Cisco IronPort AsyncOS 7.6 for Email
上級コンフィギュレーション ガイド

2012 年 3 月 8 日

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッド タウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-26343-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco IronPort AsyncOS 7.6 for Email 上級コンフィギュレーション ガイド

CONTENTS

はじめに

『*Cisco IronPort AsyncOS 7.6 for Email 上級コンフィギュレーション ガイド*』では、Cisco IronPort 電子メール セキュリティ アプライアンスのセットアップ方法、管理方法、およびモニタ方法について説明します。これらの方法は、ネットワーキングおよび電子メールの管理に関する知識を持つ、経験豊富なシステム管理者向けに記載されています。

このマニュアルをお読みになる前に

『*Quickstart Guide*』と、アプライアンスに付属の製品リリースノートをお読みください。このマニュアルでは、お客様がすでにアプライアンスを開梱し、ラック キャビネットに設置し、電源をオンにしたものと見なします。

（注） すでにアプライアンスをネットワークに配線済みの場合は、Cisco IronPort アプライアンスのデフォルト IP アドレスが、ネットワーク上の他の IP アドレスと競合していないことを確認します。工場出荷時に管理ポートに割り当てられた IP アドレスは、`192.168.42.42` です。Cisco IronPort アプライアンスに対する IP アドレス割り当ての詳細については、*Cisco IronPort AsyncOS for Email Configuration Guide* の「Setup and Installation」の章および付録 B「アプライアンスへのアクセス」を参照してください。

ドキュメント セット

AsyncOS のドキュメント セットは、*Cisco IronPort AsyncOS for Email Configuration Guide*、『*Cisco IronPort AsyncOS CLI Reference Guide*』、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』、およびこのマニュアルの 4 つに分かれており、本マニュアルには高度な機能と設定に関する情報が記載されています。このマニュアルでは、各トピックの追加情報に関して他のマニュアルを参照することがあります。

このマニュアルの構成

第 1 章「リスナーのカスタマイズ」では、エンタープライズ電子メール ゲートウェイの設定を調整するプロセスについて説明します。この章では、ゲートウェイを通って受信する電子メールを処理するために、インターフェイスおよびリスナーを設定する際に使用できる高度な機能を詳細に説明します。

第 2 章「ルーティング機能と配信機能の設定」では、Cisco IronPort アプライアンスを通過する電子メールのルーティングと配信に影響を与える機能について説明します。

第 3 章「LDAP クエリ」では、Cisco IronPort アプライアンスと社内の Lightweight Directory Access Protocol（LDAP）サーバを接続してクエリーを実行し、受け入れる受信者（グループのメンバーシップを含む）の確認、メール ルーティングとアドレス書き換え、ヘッダーのマスカレード、および SMTP 認証のサポートを行う方法について説明します。

第 5 章「電子メール認証」では、Cisco IronPort アプライアンスで電子メール認証を設定してイネーブルにするプロセスについて詳しく説明します。Cisco IronPort AsyncOS は、複数のタイプの電子メール認証をサポートしています。これには、着信メールの Sender Policy Framework（SPF）検証、Sender ID Framework（SIDF）検証、DomainKeys Identified Mail（DKIM）検証、および発信メールの DomainKeys 署名と DKIM 署名が含まれます。

第 6 章「メッセージ フィルタを使用した電子メール ポリシーの適用」では、メッセージ フィルタを使って電子メールを処理するルールを規定する方法について説明します。これには、添付ファイル フィルタ、イメージ分析、コンテンツ ディクショナリの各機能を使ったメッセージ コンテンツの変更が含まれます。

第 7 章「高度なネットワーク構成」では、NIC ペアリング、仮想 LAN、およびその他の機能に関して説明します。

第 8 章「集中管理」では、複数のアプライアンスを管理および設定できる集中管理機能について説明します。中央集中型管理機能によって、ネットワーク内の信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーを順守しながらグローバルな管理を行うことができます。

付録 A「AsyncOS クイック リファレンス ガイド」では、CLI のほとんどのコマンドに関するクイック リファレンスを示します。

付録 B「アプライアンスへのアクセス」では、Cisco IronPort アプライアンスにアクセスし、Cisco IronPort アプライアンスのファイルを送受信する方法について説明します。

印刷時の表記法

書体または記号	意味	例
AaBbCc123	コマンド、ファイル、およびディレクトリの名前、画面に表示されるコンピュータの出力。	`Please choose an IP interface for this Listener.` `sethostname` コマンドは、Cisco IronPort アプライアンスの名前を設定します。
AaBbCc123	ユーザ入力（画面上のコンピュータ出力と対比される場合）。	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**
AaBbCc123	マニュアルのタイトル、新しい語句や用語、強調する語句。コマンドライン変数（実際の名前や値に置き換えられる部分）。	*Cisco IronPort『Quickstart Guide』*をお読みください。 Cisco IronPort アプライアンスは、発信パケットを送信するためのインターフェイスを一意に選択できる*必要があります*。 `Before you begin, please reset your password to a new value.` `Old password:` **`ironport`** `New password:` *`your_new_password`* `Retype new password:` *`your_new_password`*

Cisco IronPort カスタマー サポートへの問い合わせ

サポートは、電話、電子メール、またはオンラインで依頼できます（24 時間年中無休）。

Cloud Email Security アプライアンスに関して支援を必要とする場合、Cisco IronPort カスタマー サポートには問い合わせないでください。Cloud/Hybrid Email Security アプライアンスのサポートを受ける方法については、『*Cisco IronPort Cloud Email Security/ Hybrid Email Security Overview Guide*』を参照してください。

カスタマー サポートの営業時間（月曜から金曜までの 1 日 24 時間、ただし米国の祝日を除く）中は、依頼を受けてから 1 時間以内にエンジニアがご連絡します。

営業時間外に緊急の援助を必要とする重大な問題を報告するには、以下の方法のいずれかを使用して Cisco IronPort に連絡してください。

米国フリーダイヤル：1(877) 641- 4766

米国外：http://cisco.com/web/ironport/contacts.html

サポート ポータル：http://cisco.com/web/ironport/index.html

Cisco IronPort へのコメントの送付

弊社はドキュメントの改善を重視しています。是非お客様のご意見とご提案をお寄せください。ご意見は次の宛先に電子メールでお送りいただけます。

docfeedback@ironport.com.

電子メールの件名には次のパーツ番号を記載してください。OL-22164-01。

CHAPTER 1

リスナーのカスタマイズ

クラウド E メール セキュリティ アプライアンスでリスナーを追加、変更、削除しないことをお勧めします。

『*Cisco IronPort AsyncOS for Email Configuration Guide*』では、Cisco IronPort AsyncOS オペレーティング システムで Cisco IronPort アプライアンスを企業のインバウンド電子メール ゲートウェイとして機能させる方法について説明しました。これにより、インターネットから SMTP 接続を確立してメッセージを受信し、これらの接続を *リスナー*で処理できるようにすることで適切なシステムにメッセージをリレーできます。

*リスナー*では、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、ネットワーク内にある内部システムまたはインターネットから Cisco IronPort アプライアンスに入る電子メールだけに適用されます。Cisco IronPort AsyncOS は、メッセージを受け入れて受信者のホストにリレーするために、リスナーを使用してメッセージが満たす必要のある基準を指定します。リスナーは、指定した各 IP アドレス（システム セットアップ ウィザードまたは `systemsetup` コマンドで設定した初期アドレスを含む）を対象に特定のポート上で動作する「電子メール インジェクタ」または「SMTP デーモン」と考えることができます。

（注） 『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」の章の説明に従って GUI のシステム セットアップ ウィザード（またはコマンドライン インターフェイスの `systemsetup` コマンド）を完了し、変更を確定した場合は、少なくとも 1 つのリスナーがアプライアンスに設定されている必要があります。

この章では、GUI の [ネットワーク（Network）] メニューの [リスナー（Listeners）] ページまたは CLI の `listenerconfig` コマンドを使用して、Cisco IronPort アプライアンスに設定されたリスナーの詳細な *受信*プロパティの一部をカスタマイズする方法（新しいリスナーの作成を含む）について説明します。次の第 2 章「ルーティング機能と配信機能の設定」では、システムで設定したリスナーの配信プロパティをカスタマイズする方法について説明します。

ここでは、次の内容を説明します。

リスナーの概要

[ネットワーク（Network）] > [リスナー（Listeners）] ページおよび CLI の `listenerconfig` コマンドを使用して、リスナーを作成、編集、削除できます。Cisco IronPort AsyncOS では、メッセージを受信し、受信ホストやネットワークの内部またはインターネット上の外部の受信者のいずれかにリレーするための条件を指定する必要があります。

これらの対象となる条件はリスナーで定義されます。最終的に、これらの条件が一括されてメール フロー ポリシーが定義され、強制されます。リスナーでは、Cisco IronPort アプライアンスが電子メールを送信するシステムと通信する方法も定義されます。

各リスナーは、表 1-1 に示す条件で構成されます。

表 1-1　　リスナーの条件

名前（Name）	リスナーには、簡単に参照できるように一意の名前を付けてください。リスナー用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、複数のリスナーに同一の名前を付けることはできません。	
IP インターフェイス	リスナーは IP インターフェイスに割り当てられます。IP インターフェイスは `interfaceconfig` コマンドで定義します。リスナーを作成および割り当てる*前*に、システム セットアップ ウィザード、`systemsetup` コマンド、[IP インターフェイス（IP Interfaces）] ページ、または `interfaceconfig` コマンドを使用して IP インターフェイスを設定する必要があります。インターフェイスのインターネット プロトコル アドレスのバージョンによって、リスナーが受け入れるトラフィック タイプが決まります。IP インターフェイスに IPv4 と IPv6 の両方のアドレスがある場合、リスナーは IPv4 と IPv6 の両方のアドレスからの接続を受け入れることができます。	
メール プロトコル	電子メールの受信時に、SMTP または QMQP のいずれかのメール プロトコルを使用します（CLI の `listenerconfig` コマンドでのみ使用可能）。	
IP ポート	リスナーへの接続で使用する特定の IP ポート。デフォルトでは、SMTP ではポート 25 を使用し、QMQP ではポート 628 を使用します。	
リスナー タイプ：	**パブリック（Public）** **プライベート（Private）**	パブリック リスナーおよびプライベート リスナーは、ほとんどの設定に使用されます。一般的に、プライベート リスナーはプライベート（内部）ネットワークに使用されます。パブリック リスナーには、インターネット経由の電子メールの受信のためのデフォルトの特性があります。
	ブラックホール	「ブラックホール」リスナーは、テストやトラブルシューティングの目的で使用できます。ブラックホール リスナーの作成時に、メッセージを削除する前にそのメッセージをディスクに書き込むかどうかを選択します（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「テストとトラブルシューティング」を参照してください）。メッセージを削除する前にディスクに書き込むと、受信レートおよびキューの速度の測定に役立ちます。メッセージをディスクに書き込まないリスナーは、メッセージ生成システムからの純粋な受信レートの測定に役立ちます。このリスナーのタイプは、CLI の `listenerconfig` コマンドを使用した場合にだけ利用できます。

これらの条件に加えて、各リスナーに次の設定を行うことができます。

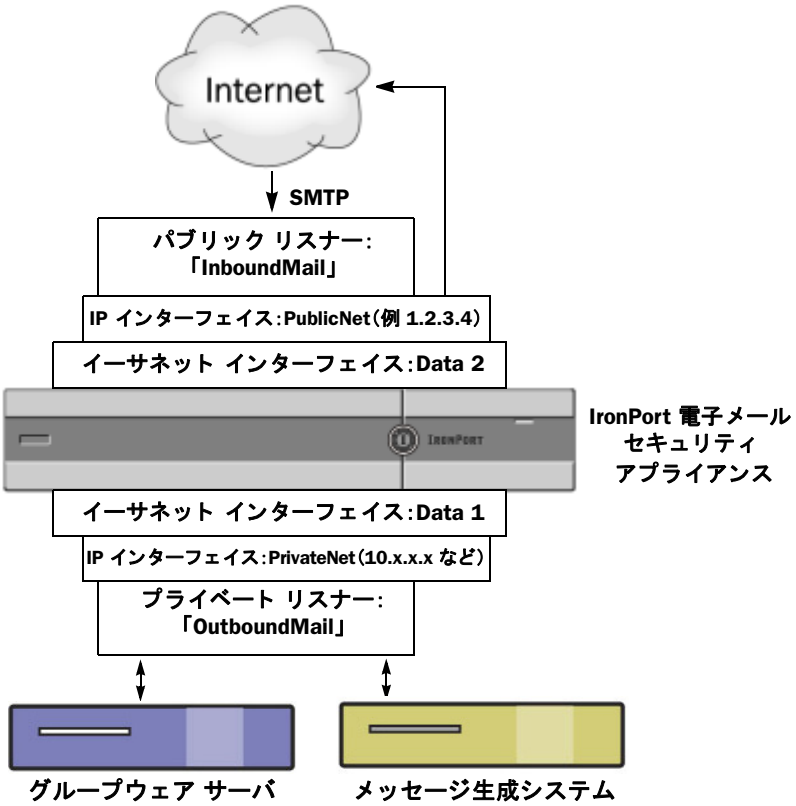
- SMTP アドレス解析オプション（SMTP の「MAIL FROM」および「RCPT TO」の解析を管理するオプションの設定。SMTP アドレス解析オプション（1-8 ページ）を参照）
- 高度な設定オプション（リスナーの動作をカスタマイズするオプションの設定。高度な設定オプション（1-11 ページ）を参照）
- LDAP オプション（このリスナーに関連付けられた LDAP クエリーを制御するオプションの設定。LDAP オプション（1-12 ページ）を参照）

また、すべてのリスナーに適用するグローバル設定があります。詳細については、リスナーのグローバル設定（1-5 ページ）を参照してください。

リスナーを作成する場合、Host Access Table（HAT; ホスト アクセス テーブル）を介してリスナーに接続できるホストを指定します。パブリック リスナーの場合、アプライアンスで受信者アクセス テーブル（RAT）を使用するためのメッセージを受け入れるすべてのドメインも定義します。RAT はパブリック リスナーのみに適用されます。ホスト アクセス テーブルおよび受信者アクセス テーブルのエントリの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Mail」の章を参照してください。

図 1-1 に、エンタープライズ ゲートウェイとして設定された Cisco IronPort アプライアンスで使用できるパブリック リスナーおよびプライベート リスナーを示します。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Enterprise Gateway Configuration」を参照してください。

図 1-1　　エンタープライズ ゲートウェイ設定のパブリック リスナーおよびプライベート リスナー



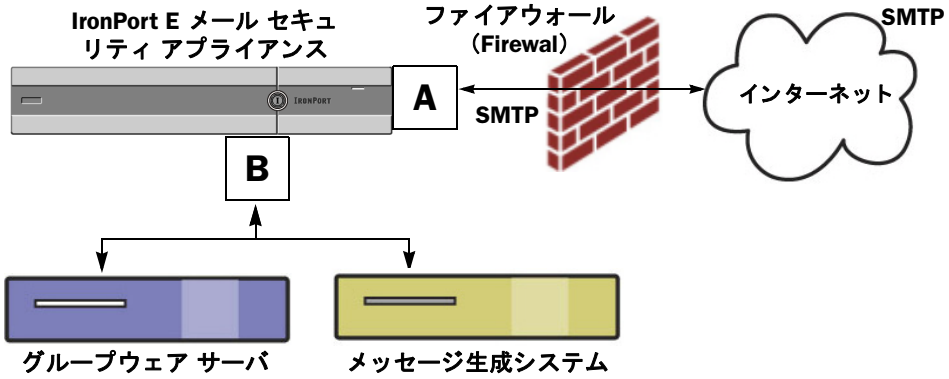
GUI を使用したリスナーの設定

GUI の [Network] メニューの [Listeners] ページを使用して、現在設定されているリスナーのリストにリスナーを追加します。

（注）『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」の章の説明に従って GUI のシステム セットアップ ウィザード（またはコマンドライン インターフェイスの `systemsetup` コマンド）を完了し、変更を確定した場合は、少なくとも 1 つのリスナーがアプライアンスに設定されている必要があります。（GUI システム セットアップ ウィザードの [リスナーの作成（Create a Listener）] セクション、または CLI の `systemsetup` コマンドで入力した設定を参照してください）。メールを受信する特定のアドレスも、その時点および最初の SMTP ルート エントリで入力されています。

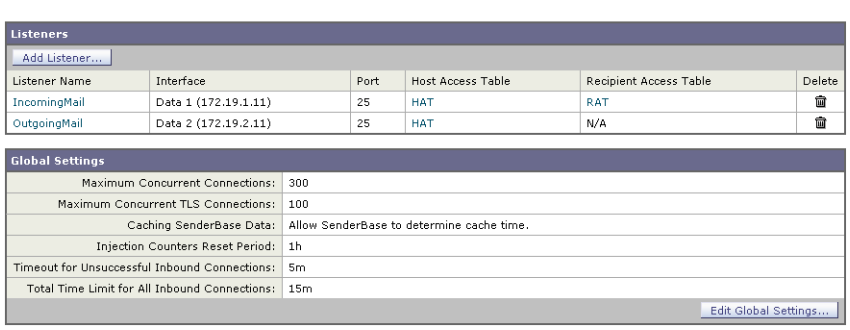
図 1-2 では、リスナー A はシステムのセットアップ時に作成された InboundMail という名前のパブリック リスナーを表します。リスナー B は、ユーザが作成したオプションのプライベート リスナーを表します。

図 1-2　新しいプライベート リスナーの作成



[Network] > [Listeners] ページを使用して、リスナーを追加、削除、または変更します。[Listeners] ページでは、リスナーのグローバル設定にもアクセスできます。

図 1-3　[Listeners] ページ



リスナーのグローバル設定

リスナーのグローバル設定は、Cisco IronPort アプライアンスで設定されたすべてのリスナーに影響します。リスナーが、インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスの両方を持つインターフェイスを使用する場合、リスナーの設定は IPv4 および IPv6 トラフィックの両方に適用されます。

次に、グローバル設定を示します

表 1-2　　リスナーのグローバル設定

グローバル設定	説明
最大同時接続数（Maximum Concurrent Connections）	リスナーに同時に接続できる最大数を設定します。デフォルト値は 300 です。リスナーが IPv4 と IPv6 の両方の接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 300 の場合、IPv4 および IPv6 接続の最大同時接続数が合計 300 を超えることはできません。
最大 TLS 同時接続数（Maximum Concurrent TLS Connections）	すべてのリスナーでの同時 TLS 接続の最大数を設定します。デフォルト値は 100 です。リスナーが IPv4 と IPv6 の両方の TLS 接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 100 の場合、IPv4 および IPv6 の TLS 接続の最大同時接続数が合計 100 を超えることはできません。
SenderBase データのキャッシング	SenderBase 情報サービスによって自動的にキャッシュ時間を決定する（推奨）ことも、独自のキャッシュ時間を指定することもできます。キャッシングをディセーブルにすることもできます。
インジェクション カウンタ リセット期間（Injection Counters Reset Period）	インジェクション制御カウンタがリセットされた場合に調整できます。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に（たとえば、60 分間隔ではなく 15 分間隔で）リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。 現在のデフォルト値は 1 時間です。最小 1 分（60 秒）から最大 4 時間（14,400 秒）までの期間を指定できます。 インジェクション制御期間（1-19 ページ）を参照してください。
受信接続のタイムアウトまでの待ち時間（Timeout Period for Unsuccessful Inbound Connections）	AsyncOS が失敗した着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 失敗した接続は SMTP カンバセーションとなり、正常なメッセージ インジェクションが発生することなく、SMTP コマンドまたは ESMTP コマンドが発行され続けます。指定したタイムアウトに達した場合は、次のエラーが送信され、接続が解除されます。 「421 Timed out waiting for successful message injection, disconnecting.」 正常なメッセージ インジェクションが発生するまで、接続に失敗したと見なされます。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 5 分です。

表 1-2　リスナーのグローバル設定(続き)

グローバル設定	説明
すべてのインバウンド接続の合計時間制限(Total Time Limit for All Inbound Connections)	AsyncOS が着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 この設定は、最大許容接続時間を適用することにより、システム リソースを保持するためのものです。この最大接続時間の約 80% が経過すると、次のメッセージが表示されます。 「421 Exceeded allowable connection time, disconnecting.」 アプライアンスは、接続が最大接続時間の 80% を超えると、接続がメッセージの途中で切断されることを防ぐために接続を切断しようとします。着信接続を最大接続時間の 80% に到達する期間開いている場合、発生する可能性がある問題です。時間制限を指定する場合、このしきい値に注意してください。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 15 分です。
HAT 遅延拒否	メッセージ受信者レベルで HAT 拒否を実行するかどうかを設定します。デフォルトでは、HAT によって拒否された接続は SMTP カンバセーションの開始時にバナー メッセージをともなって終了されます。 HAT「拒否」設定で電子メールが拒否されると、AsyncOS では SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル(RCPT TO)で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、送信側 MTA が何度も再試行される可能性も小さくなります。 HAT 遅延拒否をイネーブルにすると、次の動作が発生します。 -- MAIL FROM コマンドが許可されるが、メッセージ オブジェクトは作成されない。 -- 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。 -- SMTP AUTH を使用して MTA 送信が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。 注:CLI の `listenerconfig --> setup` コマンドからのみ設定できます。

複数のエンコーディングが含まれるメッセージの設定:localeconfig

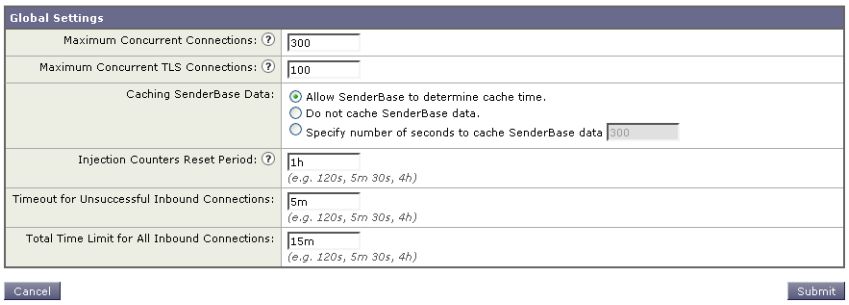
メッセージ処理中のメッセージのヘッダーおよびフッターのエンコードの変更に関する AsyncOS の動作を設定できます。この設定は GUI からは行えません。代わりに、CLI の `localeconfig` を使用して設定します。

リスナーのグローバル設定

リスナーのグローバル設定を編集するには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [リスナー（Listeners）] ページで [グローバル設定を編集（Edit Global Settings）] をクリックします。[リスナーグローバル設定を編集（Edit Listeners Global Settings）] ページが表示されます。

図 1-4　[Edit Listeners Global Settings] ページ



ステップ 2　設定を変更して [送信（Submit）] をクリックします。

ステップ 3　変更が反映された [Listeners] ページが表示されます。

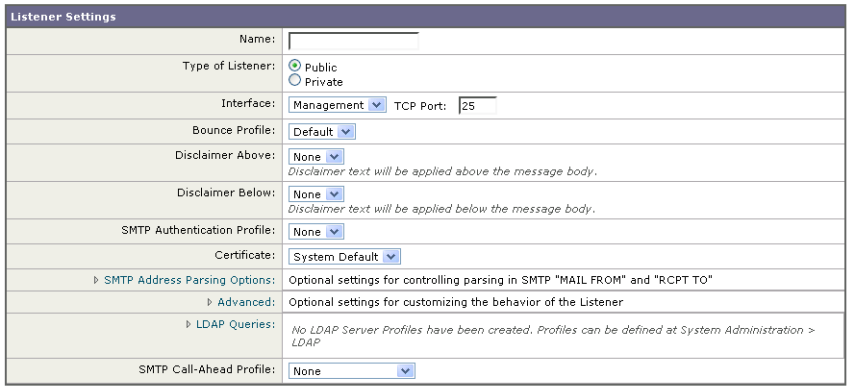
ステップ 4　変更を確定します。

リスナーの作成

新規のリスナーを追加するには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [リスナー（Listener）] ページで [リスナーを追加（Add Listener）] をクリックします。[Add Listener] ページが表示されます。

図 1-5　[Add Listener] ページ



ステップ 2　リスナーの名前を入力します。

ステップ 3　次のリスナー タイプを選択します。

ステップ 4　リスナーを作成するインターフェイスおよび TCP ポートを選択します。インターフェイスで使用する IP アドレスのバージョンによって、リスナーは IPv4 アドレス、IPv6 アドレス、または両方のバージョンからの接続を受け入れます。

ステップ 5　バウンス プロファイルを選択します（CLI の `bounceconfig` コマンドを使用して作成されたバウンス プロファイルをリストから選択できます。新しいバウンス プロファイルの作成（2-40 ページ）を参照）。

ステップ 6　電子メールの上または下に添付する免責条項を選択します（[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページまたは CLI の `textconfig` コマンドで作成された文章をリストから選択できます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「テキスト リソース」の章を参照）。

ステップ 7　SMTP 認証プロファイルを指定します。

ステップ 8　リスナーへの TLS 接続のための証明書を指定します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の `certconfig` コマンドで追加された証明書をリストから選択できます。TLS を使用した SMTP カンバセーションの暗号化（1-22 ページ）を参照）。

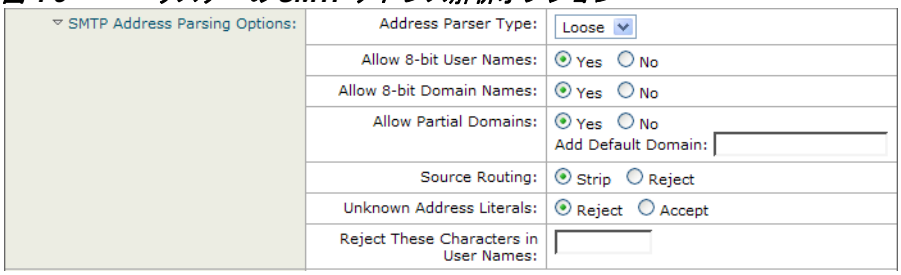
ステップ 9　必要に応じて、SMTP アドレス解析、詳細設定、および LDAP オプションを設定します（以下で説明）。

ステップ 10　変更を送信し、保存します。

SMTP アドレス解析オプション

SMTP アドレス解析オプションにアクセスするには、リスト内の [SMTP アドレス解析（SMTP Address Parsing）] をクリックしてセクションを展開します。

図 1-6　　リスナーの SMTP アドレス解析オプション



SMTP アドレス解析では、SMTP の「MAIL FROM」コマンドおよび「RCPT TO」コマンドに対する AsyncOS アドレス解析の動作の厳密性を制御します。SMTP アドレス解析には、Strict と Loose の 2 つのモードと、複数の解析オプション（アドレス解析モードとは関係なく設定される）があります。

解析モードまたは解析タイプを選択することで、アプライアンスが RFC2821 の規格に厳密に準拠するかどうかを決定できます。

Strict モード

Strict モードは RFC 2821 に準拠します。Strict モードでは、アドレス解析が RFC 2821 の規格に準拠しますが、次の例外および追加機能があります。

- 「MAIL FROM:<joe@example.com>」のように、コロンの後にスペースを挿入できます。
- ドメイン名に下線を使用できます。

- 「MAIL FROM」コマンドおよび「RCPT TO」コマンドでは、大文字と小文字が区別されます。
- ピリオドは特殊な用途に使用できません（たとえば、RFC 2821 では「J.D.」のようなユーザ名を作成できません）。

次の項で説明する追加オプションは、技術的に RFC 2821 に違反するため、イネーブルにできます。

Loose モード

Loose 解析は基本的に AsyncOS の以前のバージョンからの既存の動作です。電子メール アドレスの「検索」を最優先し、次のことを行います。

- コメントの無視。ネストされたコメント（カッコで囲まれている）がサポートされ、それらは無視されます。
- 「RCPT TO」コマンドおよび「MAIL FROM」コマンドで指定された電子メール アドレスの前後には山カッコが不要です。
- 複数のネストされた山カッコを使用できます（最も深いネスト レベルの電子メール アドレスが検索される）。

その他のオプション

2 つの解析モードに加えて、表 1-3 に示す追加項目に対する動作を指定できます。

表 1-3　SMTP アドレス解析の追加オプション

オプション	説明	デフォルト
Allow 8-bit username	イネーブルにすると、(エスケープ処理なしで)アドレスのユーザ名部分に 8 ビットの文字を使用できます。	on
Allow 8-bit domain	イネーブルにすると、アドレスのドメイン部分に 8 ビットの文字を使用できます。	on

表 1-3　SMTP アドレス解析の追加オプション（続き）

オプション	説明	デフォルト
Allow partial domain **Add Default Domain**	イネーブルにすると、部分ドメインを使用できます。部分ドメインは完全なドメインではなく、ドットなしのドメインです。 次のアドレスは、部分ドメインの例です。 – foo – foo@ – foo@bar デフォルトのドメイン機能を正常に動作させるために、このオプションをイネーブルにする*必要があります*。 デフォルトのドメインを追加:完全修飾ドメイン名ではなく、デフォルトのドメインを電子メール アドレスに使用します。[SMTP アドレス解析オプション（SMTP Address Parsing options）] で [部分ドメインを許可（Allow Partial Domains）] がイネーブルになっていない限り、このオプションはディセーブルです（SMTP アドレス解析オプション（1-8 ページ）を参照）。これは「デフォルト送信者ドメイン」を送信者のアドレスおよび完全修飾ドメイン名を含まない受信者のアドレスに追加することによって、リスナーがリレーする電子メールを変更する方法に影響します（言い換えると、リスナーの「そのままの」アドレスの処理方法をカスタマイズできます）。 従来のシステムで、送信者アドレスに企業のドメインを追加（付加）せずに電子メールを送信する場合、これを使用してデフォルトの送信者ドメインを追加できます。たとえば、従来のシステムでは電子メールの送信者として自動的に文字列「joe」のみが入力された電子メールが作成されます。デフォルトの送信者ドメインを変更すると、「@yourdomain.com」が「joe」に付加され、完全修飾送信者名 joe@yourdomain.com が作成されます。	on
Source routing: reject, strip	「MAIL FROM」アドレスおよび「RCPT TO」アドレスで送信元ルーティングが検出された場合の動作を決定します。送信元ルーティングは、複数の「@」文字を使用してルーティングを指定する、電子メール アドレスの特殊な形式です（例: @one.dom@two.dom:joe@three.dom）。「reject」を設定すると、アドレスは拒否されます。「strip」を設定すると、アドレスの送信元ルーティング部分が削除され、メッセージが通常どおり挿入されます。	discard

表 1-3　SMTP アドレス解析の追加オプション（続き）

オプション	説明	デフォルト
Reject User Names containing These Characters:	文字（たとえば、% や !）を含むユーザ名を入力すると、拒否されます。	%!:@
Unknown Address Literals (IPv6, etc.): reject, accept	システムで処理できないアドレス リテラルを受信したときの動作を決定します。現在は、IPv4 以外のすべてです。そのため、たとえば IPv6 アドレス リテラルの場合、プロトコル レベルで拒否するか、受信後すぐにハード バウンスを行うことができます。 リテラルが含まれる受信者アドレスは即時ハード バウンスの原因となります。送信者アドレスは配信される場合があります。メッセージを配信できない場合、ハード バウンスがハード バウンスされます（二重ハード バウンス）。 拒否された場合、送信者と受信者のアドレスがプロトコル レベルですぐに拒否されます。	reject

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

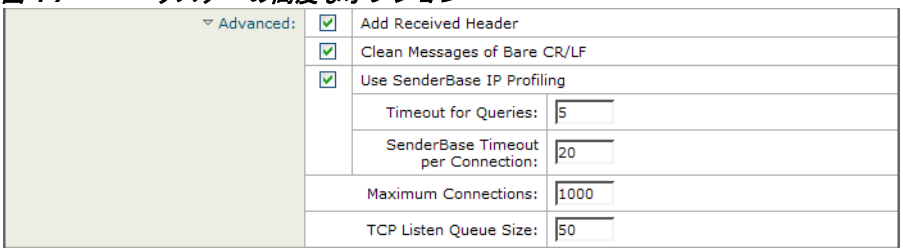
エンベロープ送信者検証をイネーブルにした場合、またはリスナーの SMTP アドレス解析オプションで部分ドメインの許可をディセーブルにした場合、リスナーのデフォルト ドメイン設定が使用されなくなります。

これらの機能は互いに排他的です。

高度な設定オプション

高度なオプションにアクセスするには、リストから [Advanced] をクリックしてセクションを展開します。

図 1-7　リスナーの高度なオプション



次に、高度な設定オプションを示します。

- [Add Received Header]: Received: ヘッダーを受信したすべての電子メールに追加します。また、リスナーは各メッセージに Received: ヘッダーを追加してリレーする電子メールを変更します。Received: ヘッダーが含まれないようにするには、このオプションを使用してディセーブルにします。

（注）　Received: ヘッダーは、ワーク キューの処理ではメッセージに追加されません。このヘッダーは配信のためにメッセージがキューから出たときに追加されます。

Received: ヘッダーをディセーブルにすると、インフラストラクチャの外部に送信されるすべてのメッセージで内部サーバの IP アドレスまたはホスト名が表示されることによって、ネットワークのトポロジが公開されないようにすることができます。Received: ヘッダーをディセーブルにする際には注意が必要です。

- [Change bare CR and LF characters to CRLF]: この新機能では、そのままの CR 文字および LF 文字が CRLF 文字に変換されます。
- SenderBase IP プロファイルを使用（Use SenderBase IP Profiling）
  - Timeout for Queries
  - SenderBase Timeout per Connection
- 最大接続数
- TCP Listen Queue Size（SMTP サーバが受け入れる前に AsyncOS で管理される接続のバックログ）

LDAP オプション

LDAP オプションにアクセスするには、リストから [LDAP Options] をクリックしてセクションを展開します。

リスナーの LDAP オプション設定は、リスナーの LDAP クエリーをイネーブルして使用します。このオプションを使用する前に、LDAP クエリーを作成しておく必要があります。クエリーの各タイプ（[Accept]、[Routing]、[Masquerade]、[Group]）には、個別のサブセクションがあります。クエリーのタイプをクリックしてサブセクションを展開します。

LDAP クエリー作成の詳細については、LDAP クエリ（3-1 ページ）を参照してください。

アクセプト クエリ

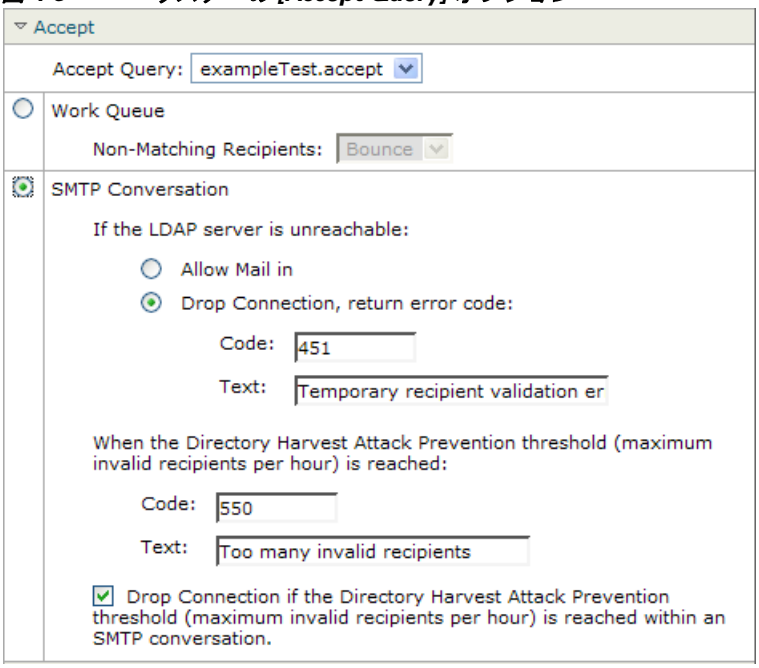
アクセプト クエリーの場合は、使用するクエリーをリストから選択します。LDAP アクセプトをワーク キューの処理中に実行するか、SMTP カンバセーションで実行するかを指定できます。

ワーク キューの処理中に LDAP アクセプトを実行する場合、一致しない受信者に対する動作として、バウンスまたはドロップに指定します。

SMTP カンバセーションで LDAP アクセプトを実行する場合、LDAP サーバに到達できない場合にメールを処理する方法を指定します。メッセージを許可するか、コードとカスタム応答で接続をドロップするかを選択できます。最後に、SMTP カンバセーションで Directory Harvest Attack Prevention（DHAP; ディレクトリ獲得攻撃防止）のしきい値に達した場合に接続をドロップするかどうかを選択します。

SMTP カンバセーションで受信者の検証を行うと、複数の LDAP クエリー間の遅延を低減できます。したがって、対話形式の LDAP アクセプトをイネーブルにした場合、ディレクトリ サーバの負荷が増大することに注意してください。

図 1-8　　リスナーの [Accept Query] オプション



詳細については、概要（3-1 ページ）を参照してください。

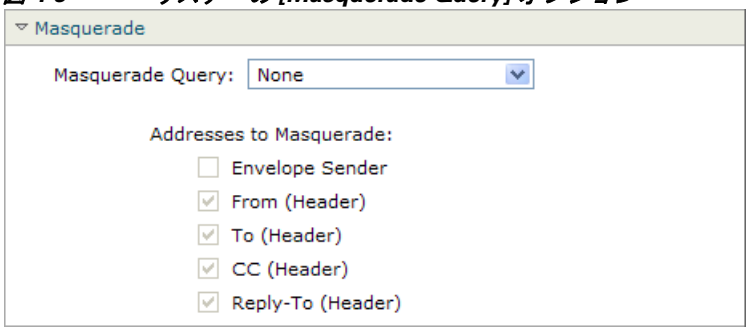
ルーティング クエリー

ルーティング クエリーの場合は、リストからクエリーを選択します。詳細については、概要（3-1 ページ）を参照してください。

マスカレード クエリー

クエリーをマスカレードするには、リストからクエリーを選択して、マスカレードするアドレスを選択します。

図 1-9　　リスナーの [Masquerade Query] オプション



詳細については、概要（3-1 ページ）を参照してください。

グループ クエリー

グループ クエリーの場合は、リストからクエリーを選択します。詳細については、概要（3-1 ページ）を参照してください。

リスナーの編集

リスナーを編集するには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [リスナー（Listeners）] ページのリストでリスナーの名前をクリックします。

ステップ 2　リスナーを変更します。

ステップ 3　変更を送信し、保存します。

リスナーの削除

リスナーを削除するには、次の手順を実行します。

ステップ 1　[Network] > [Listeners] ページで対応するリスナーの [Delete] 列にあるごみ箱のアイコンをクリックします。

ステップ 2　削除を確認します。

ステップ 3　変更を保存します。

CLI を使用したリスナーの設定

図 1-9 に、リスナーの作成および編集に関連するタスクに使用する `listenerconfig` サブコマンドの一部を示します。

表 1-4　　リスナーを作成するタスク

リスナーを作成するタスク	コマンドおよびサブコマンド	参考資料
新しいリスナーの作成	`listenerconfig -> new`	
リスナーのグローバル設定の編集	`listenerconfig -> setup`	リスナーのグローバル設定（1-5 ページ）
リスナーのバウンス プロファイルの指定	`bounceconfig, listenerconfig -> edit -> bounceconfig`	新しいバウンス プロファイルの作成（2-40 ページ）
リスナーへの免責条項の関連付け	`textconfig, listenerconfig -> edit -> setup -> footer`	『*Cisco IronPort AsyncOS for Email Configuration Guide*』で説明されています
SMTP 認証の設定	`smtpauthconfig, listenerconfig -> smtpauth`	
SMTP アドレス解析の設定	`textconfig, listenerconfig -> edit -> setup -> address`	
リスナーのデフォルト ドメインの設定	`listenerconfig -> edit -> setup -> defaultdomain`	
Received: ヘッダーの電子メールへの追加	`listenerconfig -> edit -> setup -> received`	
そのままの CR および LF 文字の CRLF への変更	`listenerconfig -> edit -> setup -> cleansmtp`	

表 1-4　　リスナーを作成するタスク（続き）

ホスト アクセス テーブルの修正	`listenerconfig -> edit -> hostaccess`	『*Cisco IronPort AsyncOS for Email Configuration Guide*』で説明されています
ローカル ドメインまたは特定のユーザ（RAT）への電子メールの受け入れ（パブリック リスナーのみ）	`listenerconfig -> edit -> rcptaccess`	『*Cisco IronPort AsyncOS for Email Configuration Guide*』で説明されています
リスナーの暗号化カンバセーション（TLS）	`certconfig, settls, listenerconfig -> edit`	TLS を使用した SMTP カンバセーションの暗号化（1-22 ページ）
証明書の選択（TLS）	`listenerconfig -> edit -> certificate`	TLS を使用した SMTP カンバセーションの暗号化（1-22 ページ）

電子メールのルーティングおよび配信設定の詳細については、第 2 章「ルーティング機能と配信機能の設定」を参照してください。

HAT の詳細パラメータ

表 1-5 では、HAT の詳細パラメータの構文を定義しています。次の値は数値であり、後に **k** を追加してキロバイトで表すか、後に **M** を追加してメガバイトで表すことができます。文字のない値はバイトと見なされます。アスタリスクが付いたパラメータは、表 1-5 に示す変数構文をサポートしています。

表 1-5　　HAT 詳細パラメータの構文

パラメータ	構文	値	値の例
接続あたりの最大メッセージ数	`max_msgs_per_session`	数字	`1000`
メッセージあたりの最大受信者数	`max_rcpts_per_msg`	数字	`10000` `1k`
最大メッセージ サイズ（Maximum message size）	`max_message_size`	数字	`1048576` `20 M`
このリスナーに許可された最大同時接続数	`max_concurrency`	数字	`1000`
SMTP バナー コード	`smtp_banner_code`	数字	`220`
SMTP バナー テキスト (*)	`smtp_banner_text`	文字列	`Accepted`
SMTP 拒否バナー コード	`smtp_banner_code`	数字	`550`
SMTP 拒否バナー テキスト (*)	`smtp_banner_text`	文字列	`Rejected`
SMTP バナーホスト名を上書き	`use_override_hostname`	`on | off | default`	`default`
	`override_hostname`	文字列	`newhostname`
TLS を使用	`tls`	`on | off | required`	`on`
anti-spam スキャンの使用	`spam_check`	`on | off`	`off`
ウイルス スキャンの使用	`virus_check`	`on | off`	`off`
1 時間あたりの最大受信者数	`max_rcpts_per_hour`	数字	`5k`

表 1-5　HAT 詳細パラメータの構文（続き）

パラメータ	構文	値	値の例
1 時間あたりのエラー コードの最大受信者数	max_rcpts_per_hour_code	数字	452
1 時間あたりのテキストの最大受信者数(*)	max_rcpts_per_hour_text	文字列	Too many recipients
SenderBase の使用	use_sb	on | off	on
SenderBase レピュテーション スコアの定義	sbrs[*value1*:*value2*]	-10.0 ～ 10.0	sbrs[-10:-7.5]
ディレクトリ獲得攻撃防止:1 時間あたりの最大無効受信大数	dhap_limit	数字	150

SenderBase 設定と HAT メール フロー ポリシー

アプライアンスへの接続を分類してメールに（レート制限が含まれる場合と含まれない場合がある）フロー ポリシーを適用するには、リスナーの Host Access Table（HAT）で次の方法を使用します。

[分類（Classification）] -> [送信者グループ（Sender Group）] -> [メールフローポリシー（Mail Flow Policy）] -> [レート制限（Rate Limiting]）

詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Configuring the Gateway to Receive Email」の章の「Sender Groups Defined by Network Owners, Domains, and IP Addresses」を参照してください。

「分類（Classification）」段階では、送信側ホストの IP アドレスを使用して、（パブリック リスナーで受信した）受信 SMTP セッションを送信者グループに分類します。送信者グループに関連付けられたメール フロー ポリシーには、レート制限をイネーブルにするパラメータがある場合があります。レート制限により、セッションあたりの最大メッセージ数、メッセージあたりの最大受信者数、最大メッセージ サイズ、リモート ホストから受け付ける最大同時接続数が制限されます。

通常、このプロセスでは、対応する名前の送信者グループの各送信者に対して受信者をカウントします。同じ時間帯に複数の送信者からメールを受信した場合、すべての送信者に対する受信者の合計数が制限値と比較されます。

このカウント方法には、次に示すいくつかの例外があります。

ステップ 1　ネットワーク オーナーによって分類が行われた場合、SenderBase 情報サービスによってアドレスの大きなブロックが小さなブロックに自動的に分割されます。

このような小さな各ブロックに対して、受信者と受信者レート制限のカウントが別々に実行されます（通常、/24 CIDR ブロックと同じですが、必ずしも同じではありません）。

ステップ 2　HAT Significant Bits 機能を使用する場合について説明します。この場合、ポリシーに関連付けられた significant bits パラメータを適用して、大きなブロックのアドレスが小さなブロックに分割されます。

このパラメータは [メールフローポリシー（Mail Flow Policy）] -> [レート制限（Rate Limiting）] フェーズに関連しています。送信者グループの IP アドレスの分類に使用する「network/bits」CIDR 表記法は、「bits」フィールドとは異なります。

デフォルトでは、SenderBase レピュテーション フィルタおよび IP プロファイリング サポートは、パブリック リスナーに対して*イネーブル*、プライベート リスナーに対して*ディセーブル*になっています。

SenderBase クエリのタイムアウト

SenderBase 情報サービス（SenderBase DNS クエリーと SenderBase 評価サービス スコア（SBRS スコア）の両方）に対してクエリーを行う方法は AsyncOS の 4.0 リリース以降で改善されています。それ以前は、設定可能な最大タイムアウト値が 5 秒であったため、SenderBase 情報サービスが到達不能または使用不可能な場合に、負荷の高い一部の Cisco IronPort アプライアンスでメール処理の遅延が生じることがありました。

新しいタイムアウト値は、`listenerconfig -> setup` コマンドを発行して SenderBase 情報サービス データのキャッシングに関するグローバル設定を変更することで最初に設定できます。SenderBase 情報サービスによって自動的にキャッシュ時間を決定する（推奨）ことも、独自のキャッシュ時間を指定することもできます。キャッシングをディセーブルにすることもできます。

リスナーの `listenerconfig -> setup` コマンドで、SenderBase 情報サービスに対する「検索」をイネーブルにします。

この例では、この機能がイネーブルになっており、（クエリーに対する、および接続ごとのすべてのクエリーに対する）デフォルトのタイムアウト値が受け入れられています。

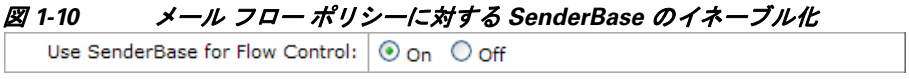
```
Would you like to enable SenderBase Reputation Filters and IP Profiling

support? [Y]> y



Enter a timeout, in seconds, for SenderBase queries. Enter '0' to

disable SenderBase Reputation Filters and IP Profiling.

[5]>



Enter a timeout, in seconds, for all SenderBase queries per connection.

[20]>
```

次に各メール フロー ポリシーについては、`listenerconfig -> hostaccess -> edit` コマンドを使用して、メール フロー ポリシーごとに SenderBase 情報サービスの「検索」を許可します。

```
Would you like to use SenderBase for flow control by default? (Yes/No/Default) [Y]>
```

GUI で次のことを実行します。

図 1-10　メール フロー ポリシーに対する SenderBase のイネーブル化



HAT Significant Bits 機能

AsyncOS の 3.8.3 リリース以降では、大きな CIDR ブロック内のリスナーのホスト アクセス テーブル（HAT）の送信者グループ エントリを管理しながら、IP アドレス単位で受信メールの追跡およびレート制限を実行できます。たとえば、着信接続がホスト「10.1.1.0/24」と一致した場合、すべてのトラフィックを 1 つの大きなカウンタに集約するのではなく、範囲内の個別のアドレスに対してカウンタが生成されます。

（注）　HAT ポリシーの significant bits オプションを有効にするには、HAT フロー制御オプションの「User SenderBase」をディセーブルにする*必要があります*（または、CLI の場合、`listenerconfig` -> setup コマンドで SenderBase 情報サービスをイネーブルにするための質問「Would you like to enable SenderBase Reputation Filters and IP Profiling support?」に **no** と回答します）。つまり、Hat Significant Bits 機能と SenderBase IP プロファイリング サポートのイネーブル化は相互に排他的です。

ほとんどの場合、この機能を使用して送信者グループを*広く*定義し（つまり、「10.1.1.0/24」や「10.1.0.0/16」のような IP アドレスの大きなグループ）、IP アドレスの小さなグループにメール フロー レート制限を*狭く*適用します。

HAT Significant Bits 機能は、次のようなシステムのコンポーネントに対応します。

HAT 設定

HAT の設定には、送信者グループとメール フロー ポリシーの 2 つの部分があります。送信者グループの設定では、送信者の IP アドレスの「分類」（送信者グループに入れる）方法を定義します。メール フロー ポリシー設定では IP アドレスからの SMTP セッションの管理方法を定義します。この機能を使用すると、IP アドレスは「CIDR ブロックで分類された」（たとえば、10.1.1.0/24）送信者グループとなり、個々のホスト（/32）として制御されます。これは「signficant_bits」ポリシー設定を使用して実行されます。

Significant Bits HAT ポリシー オプション

HAT 構文では signficant_bits 設定オプションを使用できます。HAT でデフォルト メール フロー ポリシーまたは特定のメール フロー ポリシーを編集する場合（たとえば、`listenerconfig -> edit -> hostaccess -> default` コマンドを発行する場合）、次のような質問が表示されます。

- レート制限がイネーブルになっているか
  - フロー制御のための SenderBase の使用がディセーブルになっているか
  - ディレクトリ獲得攻撃防御（DHAP）がメール フロー ポリシー（デフォルト メール フロー ポリシーまたは特定のメール フロー ポリシー）に対してイネーブルになっているか

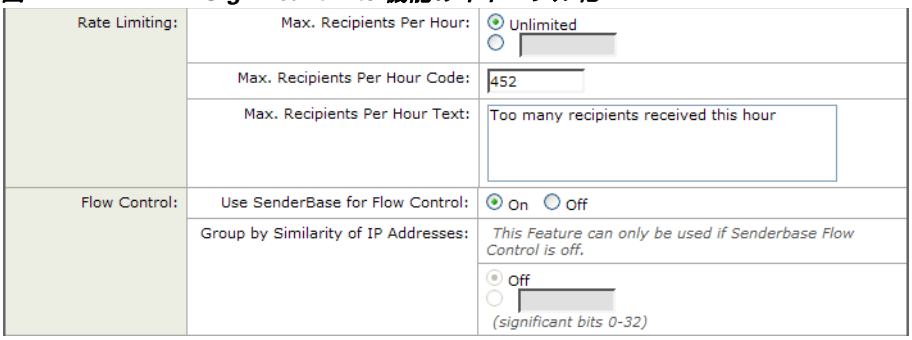
次に例を示します。

```
Do you want to enable rate limiting per host? [N]> y


Enter the maximum number of recipients per hour from a remote host.

[]> 2345


Would you like to specify a custom SMTP limit exceeded response? [Y]> n
```

```
Would you like to use SenderBase for flow control by default? [N]> n


Would you like to group hosts by the similarity of their IP addresses? [N]> y


Enter the number of bits of IP address to treat as significant, from 0 to 32.

[24]>
```

また、この機能は [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] ページの GUI にも表示されます。

図 1-11　HAT Significant Bits 機能のイネーブル化



フロー制御に SenderBase を使用するオプションが [OFF] になっているか、または [ディレクトリ獲得攻撃防御（Directory Harvest Attack Prevention）] がイネーブルになっている場合、「significant bits」値は、接続している送信者の IP アドレスに適用され、結果的に CIDR 表記法が、HAT 内の定義済みの送信者グループと一致させるためのトークンとして使用されます。CIDR ブロックで囲まれた一番右のビットは、文字列の作成時に「ゼロ設定」になります。そのため、接続が IP アドレス 1.2.3.4 から確立され、significant_bits オプションが 24 に設定されたポリシーと一致する場合、結果として生じる CIDR ブロックは 1.2.3.0/24 になります。この機能を使用すると、HAT 送信者グループ エントリ（たとえば、10.1.1.0/24）には、グループに割り当てられたポリシー内の有効ビット エントリ（上記の例では、32）とは異なる数のネットワーク有効ビット（24）が存在する可能性があります。

インジェクション制御期間

インジェクション制御カウンタがリセットされた場合に調整できるグローバル設定オプションがあります。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に（たとえば、60 分間隔ではなく 15 分間隔で）リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。

現在のデフォルト値は 3600 秒（1 時間）です。最小 1 分（60 秒）から最大 4 時間（14,400 秒）までの期間を指定できます。

GUI でグローバル設定を使用してこの期間を調整します（詳細については、リスナーのグローバル設定（1-5 ページ）を参照してください）。

また、CLI の listenerconfig -> setup コマンドを使用してこの期間を調整することもできます。

```
mail3.example.com> listenerconfig

Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.。
[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.
[300]>

Enter the global limit for concurrent TLS connections to be allowed across all listeners.
[100]>

Enter the maximum number of message header lines. 0 indicates no limit.
[1000]>

1. Allow SenderBase to determine cache time (Recommended)
2. Don't cache SenderBase data.
3. Specify your own cache time.
[1]> 3

Enter the time, in seconds, to cache SenderBase data:
```

```
[300]>


Enter the rate at which injection control counters are reset.

[1h]> 15m


Enter the timeout for unsuccessful inbound connections.

[5m]>


Enter the maximum connection time for inbound connections.

[15m]>


What hostname should Received: headers be stamped with?
1. The hostname of the Virtual Gateway(tm) used for delivering the message
2. The hostname of the interface the message is received on

[2]>


The system will always add a Message-ID header to outgoing messages that don't already
have one. Would you like to do the same for incoming messages? (Not recommended.) [N]>


By default connections with a HAT REJECT policy will be closed with a banner message at
the start of the SMTP conversation. Would you like to do the rejection at the message
recipient level instead for more detailed logging of rejected mail? [N]>


Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private


[]>
```

TLS を使用した SMTP カンバセーションの暗号化

エンタープライズ ゲートウェイ（またはメッセージ転送エージェント、つまり MTA）は、通常インターネット上で「クリアに」通信します。つまり、通信は暗号化されません。場合によっては、悪意のあるエージェントが、送信者または受信者に知られることなく、この通信を傍受する可能性があります。通信は第三者によってモニタされる可能性や、変更される可能性さえあります。

Transport Layer Security（TLS）はセキュア ソケット レイヤ（SSL）テクノロジーを改良したバージョンです。これは、インターネット上での SMTP カンバセーションの暗号化に広く使用されているメカニズムです。AsyncOS では SMTP への STARTTLS 拡張（セキュアな SMTP over TLS）がサポートされます。詳細については、RFC 3207 を参照してください（これは、廃止になった RFC 2487 に代わるバージョンです）。

AsyncOS の TLS 実装では、暗号化によってプライバシーが確保されます。これによって、X.509 証明書および証明書認証サービスからの秘密キーのインポートや、アプライアンス上で使用する自己署名証明書を作成できます。AsyncOS では、パブリック リスナーおよびプライベート リスナーに対する個々の TLS 証明書、インターフェイス上の セキュア HTTP（HTTPS）管理アクセス、LDAP インターフェイス、およびすべての発信 TLS 接続がサポートされます。

Cisco IronPort アプライアンスで TLS を正常に設定するには、次の手順を実行します。

ステップ 1　証明書を取得します。

ステップ 2　Cisco IronPort アプライアンスに証明書をインストールします。

ステップ 3　受信、配信、または両方を行うシステムで TLS をイネーブルにします。

証明書の取得

TLS を使用するには、Cisco IronPort アプライアンスに対する受信および配信のための X.509 証明書および一致する秘密キーが必要です。SMTP での受信および配信の両方には同じ証明書を使用し、インターフェイス（LDAP インターフェイス）上での HTTPS サービスや宛先ドメインへのすべての発信 TLS 接続には別の証明書を使用することも、それらのすべてに対して 1 つの証明書を使用することもできます。

既知の認証局サービスから認証および秘密キーを購入できます。認証局は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。Cisco IronPort では、サービスの重複を推奨しません。

Cisco IronPort アプライアンスでは、独自の自己署名証明書を作成して、公開証明書を取得するために認証局に送信する証明書署名要求（CSR）を生成できます。認証局は、秘密キーによって署名された信頼できる公開証明書を返送します。Web インターフェイスの [ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の `certconfig` コマンドを使用して自己署名証明書を作成し、CSR を生成して、信頼できる公開証明書をインストールします。

初めて証明書を取得または作成する場合は、インターネットで「certificate authority services SSL Server Certificates（SSL サーバ証明書を提供している認証局）」を検索して、お客様の環境のニーズに最も適したサービスを選択してください。サービスの手順に従って、証明書を取得します。

`certconfig` を使用して証明書を設定した後で、GUI の [ネットワーク（Network）] > [証明書（Certificates）] ページおよび CLI の `print` コマンドを使用して証明書のリスト全体を表示できます。`print` コマンドでは中間証明書が表示されないことに注意してください。

警告　**Cisco IronPort アプライアンスには TLS および HTTPS 機能がテスト済みであることを示すデモ証明書が同梱されますが、デモ証明書付きのサービスのいずれかをイネーブルにすることはセキュアではないため、通常の使用には推奨できません。デフォルトのデモ証明書が付属しているいずれかのサービスをイネーブルにすると、CLI に警告メッセージが表示されます。**

中間証明書

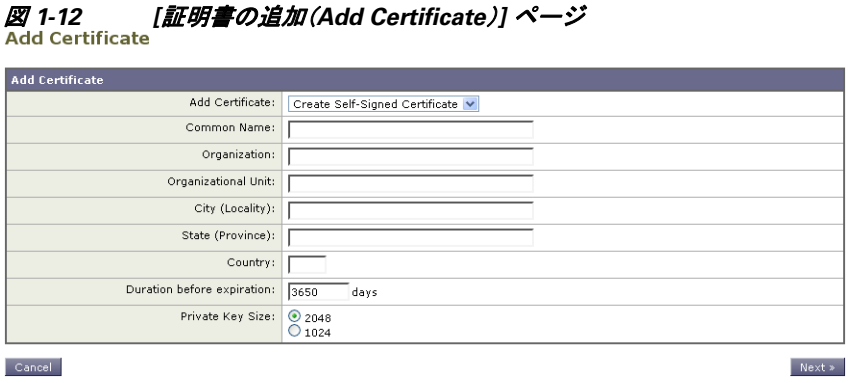
ルート証明書の検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、信頼の連鎖を効率的に作成することによって、追加の証明書を作成するために使用されます。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた godaddy.com によって証明書が発行されたとします。godaddy.com によって発行された証明書では、信頼できるルート認証局の秘密キーと同様に godaddy.com の秘密キーが検証される必要があります。

自己署名証明書の作成

自己署名証明書を作成するには、GUI の [ネットワーク（Network）] > [証明書（Certificates）] ページで [証明書の追加（Add Certificate）] をクリックします（または、CLI の `certconfig` コマンドを使用します）。[Add Certificate] ページで、[Create Self-Signed Certificate] を選択します。

図 1-12 に、[自己署名証明書の作成（Create Self-Signed Certificate）] オプションが選択された [証明書の追加（Add Certificate）] ページが表示されます。

図 1-12　[証明書の追加（Add Certificate）] ページ

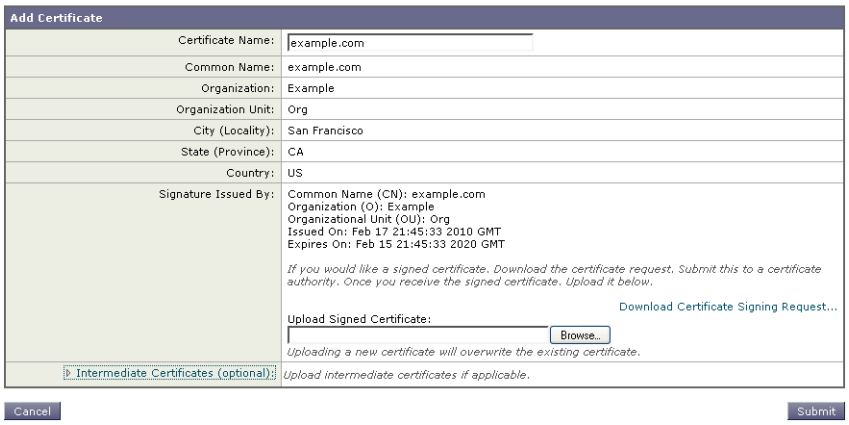


自己署名証明書に、次の情報を入力します。

共通名	完全修飾ドメイン名。
組織	組織の正確な正式名称。
組織	組織の部署名。
市（地名）	組織の本拠地がある都市。
州/県	組織の本拠地がある州、郡、または地方。
国	組織の本拠地がある 2 文字の ISO 国名コード。
失効までの期間	証明書が期限切れになるまでの日数。
秘密キー サイズ（Private Key Size）	CSR 用に生成する秘密キーのサイズ。2048 ビットおよび 1024 ビットだけがサポートされます。

[次へ(Next)] をクリックして、証明書および署名情報を確認します。図 1-13 に、自己署名証明書の例を示します。

図 1-13　[証明書(Certificate)] ページの表示



証明書の名前を入力します。AsyncOS のデフォルトでは、共通の名前が割り当てられます。

自己署名証明書の CSR を認証局に送信する場合、[証明書署名要求をダウンロード(Download Certificate Signing Request)] をクリックしてローカルまたはネットワーク マシンに PEM 形式で CSR を保存します。[送信(Submit)] をクリックして証明書を保存し、変更を確定します。

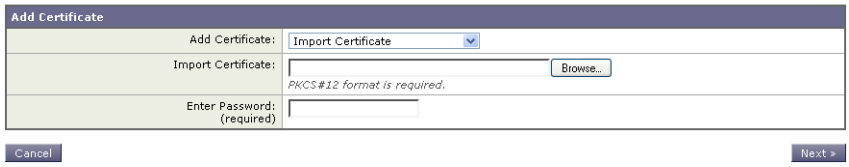
秘密キーによって署名された信頼できる公開証明書を認証局が戻すと、[証明書(Certificates)] ページの証明書の名前をクリックしてローカル マシンまたはネットワーク上のファイルへのパスを入力することで、信頼できる公開証明書をアップロードします。受信した信頼できる公開証明書が PEM 形式であるか、またはアプライアンスにアップロードする前に PEM を使用するように変換できる形式であることを確認します。(変換ツールは http://www.openssl.org の無料のソフトウェア OpenSSL に含まれています)。

認証局から証明書をアップロードすると、既存の証明書が上書きされます。自己署名証明書に関連する中間証明書をアップロードすることもできます。パブリック リスナーまたはプライベート リスナー、IP インターフェイスの HTTPS サービス、LDAP インターフェイス、または宛先ドメインへのすべての発信 TLS 接続に証明書を使用できます。

証明書のインポート

AsyncOS では PKCS #12 形式で保存された証明書をインポートしてアプライアンスで使用することもできます。GUI の [ネットワーク(Network)] > [証明書(Certificates)] ページまたは CLI の `certconfig` コマンドのいずれかを使用して、証明書をインポートできます。

図 1-14　[Add Certificate] ページ



GUI を使用して証明書をインポートするには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [証明書（Certificates）] ページの [証明書の追加（Add Certificate）] をクリックします。

ステップ 2　[Import Certificate] オプションを選択します。

ステップ 3　ネットワーク上またはローカル マシンの証明書ファイルへのパスを入力します。

ステップ 4　ファイルのパスワードを入力します。

ステップ 5　[次へ（Next）] をクリックして証明書の情報を表示します。

ステップ 6　証明書の名前を入力します。AsyncOS のデフォルトでは、共通の名前が割り当てられます。

ステップ 7　[送信（Submit）] をクリックして証明書を保存し、変更を確定します。

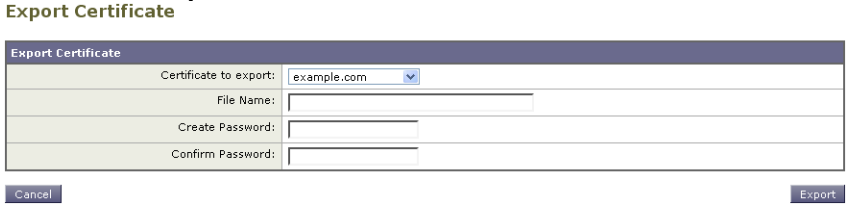
証明書のエクスポート

証明書をエクスポートするには、次のように GUI を使用して PKCS #12 形式で保存します。

ステップ 1　[ネットワーク（Network）] > [証明書（Certificates）] ページの [証明書のエクスポート（Export Certificate）] をクリックします。

[Export Certificate] ページが表示されます。

図 1-15　[Export Certificate] ページ



ステップ 2　エクスポートする証明書を選択します。

ステップ 3　証明書のファイル名を入力します。

ステップ 4　証明書ファイルのパスワードを入力します。

ステップ 5　[エクスポート（Export）] をクリックします。

Web ブラウザに、ファイルを保存するかどうかを確認するダイアログボックスが表示されます。

ステップ 6　ファイルをローカル マシンまたはネットワーク マシンに保存します。

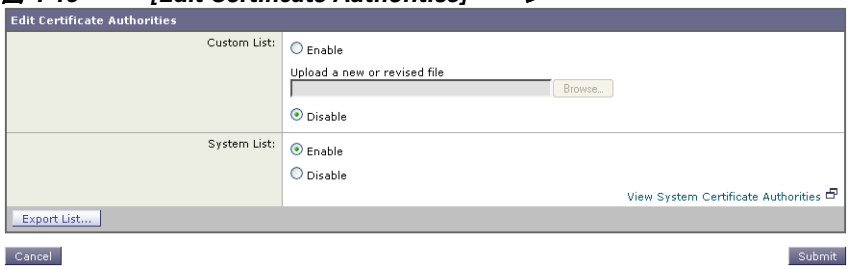
ステップ 7　さらに証明書をエクスポートするか、または [キャンセル（Cancel）] をクリックして [ネットワーク（Network）] > [証明書（Certificates）] ページに戻ります。

認証局のリストの管理

アプライアンスには信頼できる証明書のリストがあらかじめインストールされています。このリストは、リモート ドメインの証明書を検証して、ドメインのクレデンシャルを確立するために使用します。アプライアンスの信頼できる CA のカスタム リストをインポートして、あらかじめインストールされているシステム リストとともに、またはシステム リストの代わりに使用できます。GUI の [ネットワーク（Network）] > [証明書（Certificates）] > [認証局の編集（Edit Certificate Authorities）] ページ、または CLI の `certconfig > certauthority` コマンドを使用してリストを管理できます。

図 1-16 に、カスタム認証局リストとシステム認証局リストを管理する GUI の [Edit Certificate Authorities] ページを示します。

図 1-16　[Edit Certificate Authorities] ページ



システム リストに含まれている信頼できる認証局を確認するには、[認証局の編集（Edit Certificate Authorities）] ページの [システム認証局を表示（View System Certificate Authorities）] をクリックします。

カスタム認証局リストのインポート

信頼できる認証局のカスタム リストを作成して、アプライアンスにインポートできます。ファイルは PEM 形式にして、アプライアンスで信頼する認証局の証明書が含まれている必要があります。GUI を使用してリストをインポートするには、[カスタムリスト（Custom List）] の [有効（Enable）] をクリックし、ローカル マシンまたはネットワーク マシンのカスタム リストへのフル パスを入力します。変更を送信し、保存します。

システム認証局リストの無効化

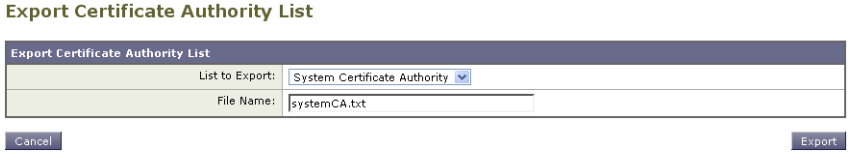
あらかじめインストールされているシステム認証局のリストはアプライアンスから削除できませんが、リモート ホストからの証明書の検証にカスタム リストのみを使用できるように、ディセーブルにすることはできます。GUI を使用してこのリストをディセーブルにするには、[Edit Certificate Authorities] ページの [System List] で [Disable] をクリックします。変更を送信し、保存します。

認証局リストのエクスポート

システム内の信頼できる認証局のサブセットのみを使用するか、既存のカスタム リストの編集を行う場合、リストを .txt ファイルにエクスポートして、認証局を追加または削除するように編集できます。リストの編集が完了したら、ファイルをカスタム リストとしてアプライアンスにインポートします。

図 1-17 に、システム リストおよびカスタム リストをエクスポートする GUI の [Export Certificate Authority List] ページを示します。

図 1-17　[Export Certificate Authority List] ページ



GUI を使用してリストをエクスポートするには、[認証局の編集（Edit Certificate Authorities）] ページで [リストのエクスポート（Export List）] をクリックします。[認証局リストのエクスポート（Export Certificate Authority List）] ページが表示されます。エクスポートするリストを選択し、リストのファイル名を入力します。[エクスポート（Export）] をクリックします。AsyncOS では、.txt ファイルとしてリストを開くか、または保存するかを確認するダイアログボックスが表示されます。

リスナー HAT の TLS のイネーブル化

暗号化が必要なリスナーに対して TLS をイネーブルにする必要があります。インターネットに対するリスナー（つまり、パブリック リスナー）には TLS をイネーブルにしますが、内部システムのリスナー（つまり、プライベート リスナー）には必要ありません。また、すべてのリスナーに対して暗号化をイネーブルにすることもできます。

リスナーの TLS に対して 3 つの異なる設定を指定できます。表 3-19 を参照してください。

表 1-6　　リスナーの TLS 設定

TLS 設定	意味
1. なし	TLS では着信接続を行えません。リスナーに対する接続では、暗号化された SMTP カンバセーションは必要ありません。これは、アプライアンス上で設定されるすべてのリスナーに対するデフォルト設定です。
2. Preferred	TLS で MTA からのリスナーへの着信接続が可能です。
3. 必須	TLS で MTA からリスナーへの着信接続が可能です。また、STARTTLS コマンドを受信するまで Cisco IronPort アプライアンスは NOOP、EHLO、または QUIT 以外のすべてのコマンドに対してエラー メッセージで応答します。この動作は RFC 3207 によって指定されています。RFC 3207 では、Secure SMTP over Transport Layer Security の SMTP サービス拡張が規定されています。TLS が「必要」であることは、送信側で TLS の暗号化を行わない電子メールが、送信前に Cisco IronPort アプライアンスによって拒否されることを意味し、このため、暗号化されずにクリア テキストで転送されることが回避されます。

デフォルトでは、プライベート リスナーとパブリック リスナーのどちらも TLS 接続を許可しません。電子メールの着信（受信）または発信（送信）の TLS をイネーブルにするには、リスナーの HAT の TLS をイネーブルにする必要があります。また、プライベート リスナーおよびパブリック リスナーのすべてのデフォルト メール フロー ポリシー設定で tls 設定が「off」になっています。

リスナーの作成時に、個々のパブリック リスナーに TLS 接続の専用の証明書を割り当てることができます。詳細については、リスナーの作成（1-7 ページ）を参照してください。

証明書の割り当て

個々のパブリック リスナーまたはプライベート リスナーに TLS 接続用の証明書を割り当てるには、[ネットワーク（Network）] > [リスナー（Listeners）] ページまたは CLI の listenerconfig -> edit -> certificate コマンドを使用します。

GUI で TLS 証明書を割り当てるには、リスナーの作成時または編集時に [Certificate] セクションで証明書を選択し、変更を送信して確定します。

図 1-18　　リスナーの証明書の選択

CLI でリスナーに証明書を割り当てるには、次の手順を実行します。

ステップ 1　`listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。

ステップ 2　`certificate` コマンドを使用して、使用できる証明書を表示します。

ステップ 3　プロンプトが表示されたら、リスナーを割り当てる証明書を選択します。

ステップ 4　リスナーの設定が完了したら、`commit` コマンドを発行して、変更をイネーブルにします。

ログ

TLS が必要であるにもかかわらず、リスナーで使用できない場合、Cisco IronPort アプライアンスによってメール ログ インスタンスで通知されます。次の条件を満たした場合、メール ログが更新されます。

- リスナーに対して TLS が [必須（required）] に設定されている。
- Cisco IronPort アプライアンスから「Must issue a STARTTLS command first」コマンドが送信された。
- 正常な受信者が受信せずに接続が終了した。

TLS 接続が失敗した理由に関する情報がメール ログに記録されます。

GUI の例

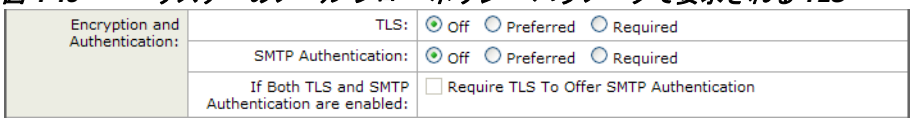
GUI でリスナーの HAT メール フロー ポリシーの TLS 設定を変更するには、次の手順を実行します。

ステップ 1　[Mail Flow Policies] ページからポリシーを変更するリスナーを選択し、編集するポリシー名のリンクをクリックします。（デフォルト ポリシー パラメータも編集可能）。

[Edit Mail Flow Policies] ページが表示されます。

ステップ 2　[暗号化と認証（Encryption and Authentication）] セクションの [TLS:] フィールドで、リスナーに必要な TLS のレベルを選択します。

図 1-19　リスナーのメール フロー ポリシー パラメータで要求される TLS



ステップ 3　変更を送信し、保存します。

選択した TLS 設定が反映されてリスナーのメール フロー ポリシーが更新されます。

CLI の例

CLI でリスナーの TLS デフォルト設定を変更するには、次の手順を実行します。

ステップ 1　`listenerconfig -> edit` コマンドを使用して、設定するリスナーを選択します。

ステップ 2　リスナーのデフォルトの HAT 設定を編集するには、`hostaccess -> default` コマンドを使用します。

ステップ 3　次の質問が表示されたら、次の選択肢のいずれかを入力して TLS 設定を変更します。

```
Do you want to allow encrypted TLS connections?

1. No

2. Preferred

3. Required

[1]> 3


You have chosen to enable TLS. Please use the 'certconfig' command to
ensure that there is a valid certificate configured.
```

この例では、リスナーで使用できる有効な証明書があるかどうかを確認するために certconfig コマンドを使用するかどうかを質問しています。証明書を作成していない場合、リスナーではアプライアンスにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。リスナーに証明書を割り当てるには、listenerconfig -> edit -> certificate コマンドを使用します。

TLS を設定すると、CLI でリスナーの概要に設定が反映されます。

```
Name: Inboundmail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: Required
```

ステップ 4　変更をイネーブルにするには、commit コマンドを発行します。

配信時の TLS および証明書検証のイネーブル化

[送信先コントロール（Destination Controls）] ページまたは destconfig コマンドを使用すると、TLS をイネーブルにして、特定のドメインに電子メールを配信するように要求できます。

TLS だけでなく、ドメインのサーバ証明書の検証も要求できます。このドメイン証明書は、ドメインのクレデンシャルを確立するために使用されるデジタル証明書に基づいています。証明プロセスには次の 2 つの要件が含まれます。

- 信頼できる認証局（CA）によって発行された証明書で終わる SMTP セッションの証明書発行者のチェーン。

- 受信マシンの DNS 名またはメッセージの宛先ドメインのいずれかと一致する証明書に表示された Common Name（CN）。

  - または -

  メッセージの宛先ドメインが、証明書のサブジェクト代替名（subjectAltName）の拡張の DNS 名のいずれかと一致している（RFC 2459 を参照）。この一致では、RFC 2818 のセクション 3.1 で説明されているワイルドカードがサポートされます。

信頼できる CA は、ID の検証および公開キーの配布に使用されるデジタル証明書を発行する、第三者機関または企業です。これによって、有効で信頼できる身元によって証明書が発行されたことがさらに保証されます。

エンベロープ暗号化の代わりに TLS 接続を介してドメインにメッセージを送信するように Cisco IronPort アプライアンスを設定できます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Cisco IronPort 電子メール暗号化」の章を参照してください。

すべての発信 TLS 接続に対してアプライアンスで使用する証明書を指定できます。証明書を指定するには、[送信先コントロール（Destination Controls）] ページの [グローバル設定の編集（Edit Global Settings）] をクリックするか、または CLI で `destconfig -> setup` を使用します。証明書はドメインごとの設定ではなく、グローバル設定です。

[送信先コントロール（Destination Controls）] ページまたは `destconfig` コマンドを使用してドメインを含める場合、指定されたドメインの TLS に 5 つの異なる設定を指定できます。TLS のエンコードにドメインとの交換が必須であるか、または推奨されるかの指定に加えて、ドメインの検証が必要かどうかも指定できます。設定の説明については、表 1-7 を参照してください。

表 1-7　配信の TLS 設定

TLS 設定	意味
デフォルト	デフォルトの TLS 設定では、リスナーからドメインの MTA への発信接続に [送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンドを使用するように設定されています。 質問の "Do you wish to apply a specific TLS setting for this domain?" に対して "no" と回答すると、値の "Default" が設定されます。
1. なし	インターフェイスからドメインの MTA への発信接続には、TLS がネゴシエートされません。
2. 推奨	Cisco IronPort アプライアンス インターフェイスからドメインの MTA への TLS がネゴシエートされます。ただし、（220 応答を受信する前に）TLS ネゴシエーションに失敗すると、SMTP トランザクションは「クリアな」（暗号化されない）ままです。証明書が信頼できる認証局によって発行された場合、検証は行われません。220 応答を受信した後にエラーが発生した場合、SMTP トランザクションはクリア テキストにフォールバックされません。
3. 必須	Cisco IronPort アプライアンス インターフェイスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証は行われません。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。ネゴシエーションに成功すると、暗号化されたセッションを経由して電子メールが配信されます。

表 1-7　配信の TLS 設定（続き）

TLS 設定	意味
4. Preferred (Verify)	Cisco IronPort アプライアンスからドメインの MTA への TLS がネゴシエートされます。アプライアンスはドメインの証明書の検証を試行します。 次の 3 つの結果が考えられます。 • TLS がネゴシエートされ、証明書が検証される。暗号化されたセッションによってメールが配信される。 • TLS がネゴシエートされるものの、証明書は検証されない。暗号化されたセッションによってメールが配信される。 • TLS 接続が確立されず、証明書は検証されない。電子メール メッセージがプレーン テキストで配信される。
5. Required (Verify)	Cisco IronPort アプライアンスからドメインの MTA への TLS がネゴシエートされます。ドメインの証明書の検証が必要です。 次の 3 つの結果が考えられます。 • TLS 接続がネゴシエートされ、証明書が検証される。暗号化されたセッションによって電子メール メッセージが配信される。 • TLS 接続がネゴシエートされるものの、信頼できる CA によって証明書が検証されない。メールは配信されない。 • TLS 接続がネゴシエートされない。メールは配信されない。

グッド ネイバー テーブルに指定された受信者ドメインの指定されたエントリがない場合、または指定されたエントリが存在するものの、そのエントリに対して指定された TLS 設定が存在しない場合、[送信先コントロール（Destination Controls）] ページまたは `destconfig -> default` サブコマンド（"No"、"Preferred"、"Required"、"Preferred (Verify)"、または "Required (Verify)"）を使用して動作を設定する必要があります。

要求された TLS 接続が失敗した場合のアラートの送信

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、Cisco IronPort アプライアンスがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。Cisco IronPort アプライアンスは、システム アラートのタイプの警告重大度レベル アラートを受信するよう設定されたすべての受信者にアラート メッセージを送信します。GUI の [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の `alertconfig` コマンド）を使用してアラートの受信者を管理できます。

TLS 接続アラートをイネーブルにするには、[送信先コントロール（Destination Controls）] ページの [グローバル設定を編集（Edit Global Settings）] をクリックまたは `destconfig -> setup` サブコマンドを使用します。これは、ドメイン単位ではなく、グローバルな設定です。アプライアンスが配信を試行したメッセージの情報については、[モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] ページまたはメール ログを使用します。

ログ

ドメインに TLS が必要であるにもかかわらず、使用できない場合、Cisco IronPort アプライアンスによってメール ログ インスタンスで通知されます。TLS 接続を使用できなかった理由も記載されています。次の条件のいずれかを満たす場合、メール ログが更新されます。

- リモート MTA で ESMTP がサポートされない（たとえば、Cisco IronPort アプライアンスからの EHLO コマンドが理解できない）。
- リモート MTA で ESMTP がサポートされるものの、「STARTTLS」が EHLO 応答でアドバタイズされる拡張のリストにない。
- リモート MTA で「STARTTLS」拡張がアドバタイズされたものの、Cisco IronPort アプライアンスで STARTTLS コマンドを送信した際にエラーが返される。

CLI の例

この例では、`destconfig` コマンドを使用して、TLS 接続の要求および「partner.com」ドメインの暗号化されたカンバセーションを実行します。リストが表示されます。

example.com の証明書は、あらかじめインストールされているデモ証明書の代わりに発信 TLS 接続で使用されます。テスト目的でデモ証明書で TLS をイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。

```
mail3.example.com> destconfig


There is currently 1 entry configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]> setup


The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure.
```

```
1. example.com

2. Demo

Please choose the certificate to apply:

[1]> 1


Do you want to send an alert when a required TLS connection fails? [N]>


There is currently 1 entry configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]> new


Enter the domain you wish to limit.

[]> partner.com


Do you wish to configure a concurrency limit for partner.com?  [Y]> n


Do you wish to apply a messages-per-connection limit to this domain? [N]> n


Do you wish to apply a recipient limit to this domain?  [N]> n
```

```
Do you wish to apply a specific bounce profile to this domain?  [N]> n


Do you wish to apply a specific TLS setting for this domain?  [N]> y


Do you want to use TLS support?

1. No

2. Preferred

3. Required

4. Preferred (Verify)

5. Required (Verify)

[1]> 3


You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there
is a valid certificate configured.

Do you wish to apply a specific bounce verification address tagging setting for this do-
main? [N]> n


Do you wish to apply a specific bounce profile to this domain? [N]> n


There are currently 2 entries configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- CLEAR - Remove all entries.
```

```
- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]> list


              Rate                Bounce        Bounce

Domain        Limiting  TLS       Verification  Profile

============  ========  =======   ============  =========

partner.com   Default   Req       Default       Default

(Default)     On        Off       Off           (Default)


There are currently 2 entries configured.


Choose the operation you want to perform:

- SETUP - Change global settings.

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- DEFAULT - Change the default.

- LIST - Display a summary list of all entries.

- DETAIL - Display details for one destination or all entries.

- CLEAR - Remove all entries.

- IMPORT - Import tables from a file.

- EXPORT - Export tables to a file.

[]>
```

HTTPS の証明書のイネーブル化

GUI の [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページまたは CLI の `interfaceconfig` コマンドのいずれかを使用して、IP インターフェイスで HTTPS サービスの証明書をイネーブルにできます。GUI を使用して IP インターフェイスを追加する場合、HTTPS サービスに使用する証明書を選択し、[HTTPS] チェックボックスをオンにして、ポート番号を入力します。

次の例では、interfaceconfig コマンドを使用して、ポート 443（デフォルト ポート）上で HTTPS サービスをイネーブルにするように IP インターフェイス PublicNet を編集します。インターフェイスのその他のすべてのデフォルトが受け入れられます。（プロンプトで Enter を入力すると、角カッコで囲まれて表示されるデフォルト値が受け入れられます。）

この例では、アプライアンスにあらかじめインストールされているデモ証明書を使用します。テスト目的でデモ証明書で HTTPS サービスをイネーブルにすることはできますが、セキュアではないため、通常の使用には推奨できません。

（注）　GUI のシステム設定ウィザードを使用して HTTPS サービスをイネーブルにできます。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「セットアップとインストール」の章の「デフォルト ルータ（ゲートウェイ）の定義、DNS 設定の構成、およびセキュア Web アクセスの有効化」を参照してください。

このコマンドからの変更が確定されると、ユーザがセキュア HTTPS の URL（https://192.168.2.1）を使用してグラフィカル ユーザ インターフェイス（GUI）にアクセスできるようになります。1

```
mail3.example.com> interfaceconfig


Currently configured interfaces:

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)


Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> edit


Enter the number of the interface you wish to edit.

[]> 3


IP interface name (Ex: "InternalNet"):

[PublicNet]>
```

```
Would you like to configure an IPv4 address for this interface (y/n)? [Y]> y


IPv4 Address (Ex: 192.168.1.2):

[192.168.2.1]>


Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[24]>


Would you like to configure an IPv6 address for this interface (y/n)? [N]>


Ethernet interface:

1. Data 1

2. Data 2

3. Management

[2]>


Hostname:

[mail3.example.com]>


Do you want to enable Telnet on this interface?  [N]>


Do you want to enable SSH on this interface?  [N]>


Do you want to enable FTP on this interface?  [N]>


Do you want to enable HTTP on this interface?  [Y]>


Which port do you want to use for HTTP?

[80]>
```

```
Do you want to enable HTTPS on this interface?  [N]> y


Which port do you want to use for HTTPS?

[443]> 443


Do you want to enable Spam Quarantine HTTP on this interface? [N]>


Do you want to enable Spam Quarantine HTTPS on this interface? [N]>


The "Demo" certificate is currently configured. You may use "Demo", but this will not be
secure. To assure privacy, run "certconfig" first.


Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the
secure service? [Y]>


Currently configured interfaces:

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)


Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>
```

CHAPTER 2

ルーティング機能と配信機能の設定

この章では、Cisco IronPort アプライアンスを通過する電子メールのルーティングおよび配信機能について説明します。リスナーを使用して電子メールを受信するようにゲートウェイを設定したら、着信（インターネットからメールを受信）と発信（社内システムからメールを送信）の両方の処理について、アプライアンスで実行されるルーティングおよび配信の設定をさらに調整できます。

この章は、次の項で構成されています。

ローカル ドメインの電子メールのルーティング

第 1 章「リスナーのカスタマイズ」では、エンタープライズ ゲートウェイ設定に対して SMTP 接続を提供するようにプライベート リスナーとパブリック リスナーをカスタマイズしました。これらのリスナーは、特定の接続を処理したり（HAT 変更経由）、特定ドメインのメールを受信したり（パブリック リスナーの RAT 変更経由）するようにカスタマイズされています。

Cisco IronPortアプライアンスでは、メールをローカル ドメイン経由で、[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページ（または `smtproutes` コマンド）を使用して指定されたホストにルーティングします。この機能は、sendmail の `mailertable` 機能に似ています。

（注）　GUI でシステム セットアップ ウィザード（またはコマンドライン インターフェイスで systemsetup コマンド）を実行し（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「セットアップとインストール」の章を参照）、変更内容を確定した場合、そのときに入力した RAT エントリごとに、アプライアンスで最初の SMTP ルート エントリが定義されています。

SMTP ルートの概要

SMTP ルートを使用すると、特定ドメインのすべての電子メールを別の Mail eXchange（MX; メール交換）ホストへリダイレクトできます。たとえば、example.com から groupware.example.com へのマッピングを作成できます。このマッピングにより、エンベロープ受信者アドレスに @example.com が含まれる電子メールは、代わりに groupware.example.com に転送されます。システムは、通常の電子メール配信のように、groupware.example.com で「MX」ルックアップを実行し、次にホストで「A」ルックアップを実行します。この代替 MX ホストは、DNS の MX レコードにリストされている必要はなく、電子メールがリダイレクトされているドメインのメンバである必要もありません。Cisco IronPort AsyncOS オペレーティング システムでは、Cisco IronPort アプライアンスで最大 4 万の SMTP ルート マッピングを設定できます。（SMTP ルートの制限（2-3 ページ）を参照）。

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。.example.com のようにドメインの一部を指定した場合は、example.com で終わるすべてのドメインがこのエントリに一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

SMTP ルート テーブルにホストがない場合は、DNS を使用して MX ルックアップが実行されます。結果は、SMTP ルート テーブルに対して再チェックされません。foo.domain の DNS MX エントリが bar.domain の場合、foo.domain に送信されるすべての電子メールが bar.domain に配信されます。bar.domain から他のホストへのマッピングを作成した場合、foo.domain へ送信される電子メールは影響を受けません。

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがその後にある場合、メールのループは作成*されません*。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

すべての電子メール配信で、SMTP ルート テーブルは、上から順に読み取られます。マッピングと一致する最も具体的なエントリが使用されます。たとえば、SMTP ルート テーブルで host1.example.com と .example.com の両方についてマッピングがある場合は、host1.example.com のエントリが使用されます。これは、具体的ではない .example.com エントリの後に出現した場合であっても、このエントリの方が具体的なエントリであるためです。そうでない場合は、エンベロープ受信者のドメインで通常の MX ルックアップが実行されます。

デフォルトの SMTP ルート

特殊キーワードの ALL を使用して、デフォルト SMTP ルートを定義することもできます。ドメインが SMTP ルート リストで前のマッピングと一致しない場合のデフォルトは、ALL エントリで指定された MX ホストにリダイレクトされます。

SMTP ルート エントリを印刷する場合、デフォルトの SMTP ルートは ALL: として一覧表示されます。デフォルトの SMTP ルートは削除できません。入力した値をクリアすることのみ可能です。

デフォルトの SMTP ルートを設定するには、[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページまたは smtproutes コマンドを使用します。

SMTP ルートの定義

ルートを構築するには、[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページ（または smtproutes コマンド）を使用します。新しいルートを作成するには、まず、永続的なルートを作成するドメインまたはドメインの一部を指定する必要があります。次に、宛先ホストを指定します。宛先ホストは、完全修飾ホスト名または IP アドレスで入力できます。IP アドレスは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）を指定できます。

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

エントリと一致するメッセージをドロップするために、特殊な宛先ホスト /dev/null を指定することもできます。（つまり、デフォルト ルートに /dev/null を指定することで、アプライアンスで受信されたメールが配信されないようにすることができます）。

受信側のドメインに複数の宛先ホストを設定できます。MX レコードと同様に、それぞれの宛先ホストにプライオリティ番号を割り当てます。最低番号が割り当てられた宛先ホストは、受信側ドメインのプライマリ宛先ホストであることを示します。一覧にある他の宛先ホストは、バックアップとして使用されます。

プライオリティが同じ宛先は、「ラウンドロビン」方式で使用されます。ラウンドロビン処理は、SMTP 接続に基づいていて、必ずしもメッセージに基づくものではありません。また、1 つ以上の宛先ホストが応答しない場合は、到達可能ないずれかのホストにメッセージが配信されます。設定されているすべての宛先ホストが応答しない場合、メールは受信側ドメインのキューに入れられ、宛先ホストへの配信が後で試みられます。（MX レコードの使用へのフェールオーバーは行われません）。

CLI で smtproutes コマンドを使用してルートを構築するときは、ホスト名または IP アドレスに続けて /pri= とその後にプライオリティを割り当てるための整数 0 ～ 65535（0 は最高のプライオリティ）を使用して、各宛先ホストにプライオリティを設定できます。たとえば、host1.example.com/pri=0 のプライオリティは、host2.example.com/pri=10 よりも高くなります。複数のエントリを指定する場合は、カンマで区切ります。

SMTP ルートの制限

最大 40,000 ルートまで定義できます。最後のデフォルト ルート ALL は、この制限内のルートとしてカウントされます。そのため、定義できるのは最大 39,999 個のカスタム ルートと、特殊なキーワード ALL を使用するルート 1 個です。

SMTP ルートと DNS

MX ルックアップを実行して、特定のドメインに対するネクスト ホップを決定するようアプライアンスに指示するには、特殊キーワード USEDNS を使用します。これは、サブドメイン宛のメールを特定ホストへルーティングする必要があるときに便利です。たとえば、example.com へのメールが企業の Exchange サーバに送信されるようにする場合、SMTP ルートは次のようになります。

```
example.com exchange.example.com
```

ただし、さまざまなサブドメイン（foo.example.com）宛のメールの場合は、次のような SMTP ルートを追加します。

```
.example.com USEDNS
```

SMTP ルートおよびアラート

[システム管理（System Administration）] > [アラート（Alerts）] ページ（または `alertconfig` コマンド）で指定されたアドレスにアプライアンスから送信されたアラートは、これらの宛先に対して定義された SMTP ルートに従います。

SMTP ルート、メール配信、およびメッセージ分裂

着信：1 つのメッセージに 10 人の受信者がいて、全員が同じ Exchange サーバに属する場合、AsyncOS では TCP 接続を 1 つ開き、メール ストアには 10 の別々のメッセージではなく、メッセージを 1 つのみ配置します。

発信：動作は同様ですが、1 つのメッセージが 10 の異なるドメインの 10 人の受信者に送信される場合、AsyncOS では 10 の MTA に対する 10 の接続を開き、それぞれ 1 つの電子メールを配信します。

分裂：1 つの着信メッセージに 10 人の受信者がいて、全員が別々の着信ポリシー グループ（10 グループ）に属する場合、10 人の受信者全員が同じ Exchange サーバに属していても、メッセージは分裂されます。つまり、10 の別々の電子メールが 1 つの TCP 接続で配信されます。

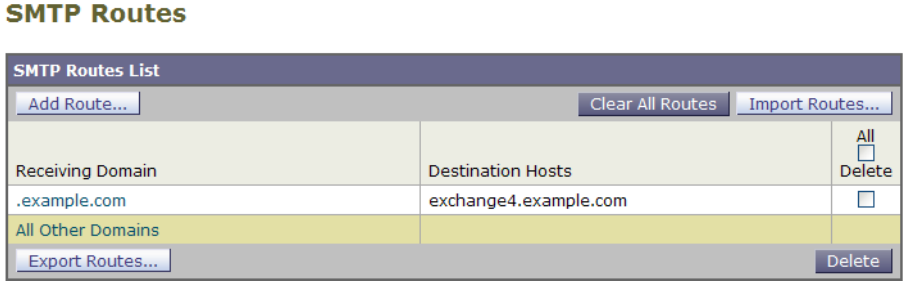
SMTP ルートと発信 SMTP 認証

発信 SMTP 認証プロファイルを作成したら、SMTP ルートに適用できます。これによって、ネットワーク エッジにあるメール リレー サーバの背後に Cisco IronPort アプライアンスが配置されている場合に、発信メールを認証できます。発信 SMTP 認証の詳細については、発信 SMTP 認証（3-41 ページ）を参照してください。

GUI を使用した SMTP ルートの管理

Cisco IronPort アプライアンスの SMTP ルートを管理するには、[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページを使用します。テーブルでマッピングの追加、変更、および削除ができます。SMTP ルート エントリをエクスポートまたはインポートすることができます。

図 2-1　[SMTP Routes] ページ

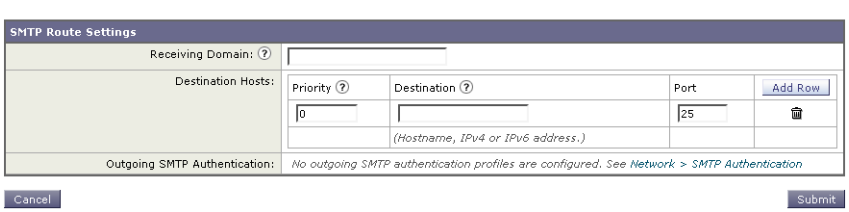


SMTP ルートの追加

SMTP ルートを追加するには、次の手順に従います。

ステップ 1　[ネットワーク（Network）] > [SMTP ルート（SMTP Routes）] ページの [ルートを追加（Add Route）] をクリックします。[Add SMTP Route] ページが表示されます。

図 2-2　[Add SMTP Route] ページ



ステップ 2　受信ドメインを入力します。ここには、ホスト名、ドメイン、IPv4 アドレス、または IPv6 アドレスを指定できます。

ステップ 3　宛先ホストを入力します。ここには、ホスト名、IPv4 アドレス、または IPv6 アドレスを指定できます。複数の宛先ホストを追加するには、[行の追加（Add Row）] をクリックし、新しい行に次の宛先ホストを入力します。

（注）　ポート番号を指定するには、宛先ホストに「<*port number*>」を追加します（例：`example.com:25`）。

ステップ 4　複数の宛先ホストを追加する場合は、`0` ～ `65535` の整数を入力してホストのプライオリティを割り当てます。`0` が最上位の優先レベルです。詳細については、SMTP ルートの定義（2-3 ページ）を参照してください。

ステップ 5　[送信（Submit）] をクリックします。[SMTP ルート（SMTP Routes）] ページが表示され、変更が反映されます。

ステップ 6　変更を保存します。

SMTP ルートの編集

SMTP ルートを編集するには、次の手順に従います。

ステップ 1　SMTP ルートのリストで、既存の SMTP ルートの名前をクリックします。[Edit SMTP Route] ページが表示されます。

ステップ 2　ルートを編集します。

ステップ 3　[送信（Submit）] をクリックします。

ステップ 4　[SMTP Routes] ページが表示され、変更が反映されます。

ステップ 5　変更を保存します。

SMTP ルートの削除

SMTP ルートを削除するには、次の手順に従います。

ステップ 1　削除する SMTP ルートの右側にあるチェックボックスをオンにします。

ステップ 2　[削除（Delete）] をクリックします。

すべての SMTP ルートを削除するには、[すべて（All）] というラベルの付いたチェックボックスをオンにして [削除（Delete）] をクリックします。

SMTP ルートのエクスポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをエクスポートするには、次の手順に従います。

ステップ 1　[SMTP ルート（SMTP Routes）] ページの [SMTP ルートをエクスポート（Export SMTP Routes）] をクリックします。[Export SMTP Routes] ページが表示されます。

ステップ 2　ファイルの名前を入力し、[送信（Submit）] をクリックします。

SMTP ルートのインポート

Host Access Table（HAT）および Recipient Access Table（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをインポートするには、次の手順に従います。

ステップ 1　[SMTP ルート（SMTP Routes）] ページの [SMTP ルートをインポート（Import SMTP Routes）] をクリックします。[Import SMTP Routes] ページが表示されます。

ステップ 2　エクスポートした SMTP ルートを含むファイルを選択します。

ステップ 3　[送信（Submit）] をクリックします。インポートによって既存の SMTP ルートがすべて置き換えられることが警告されます。テキスト ファイル内のすべての SMTP ルートがインポートされます。

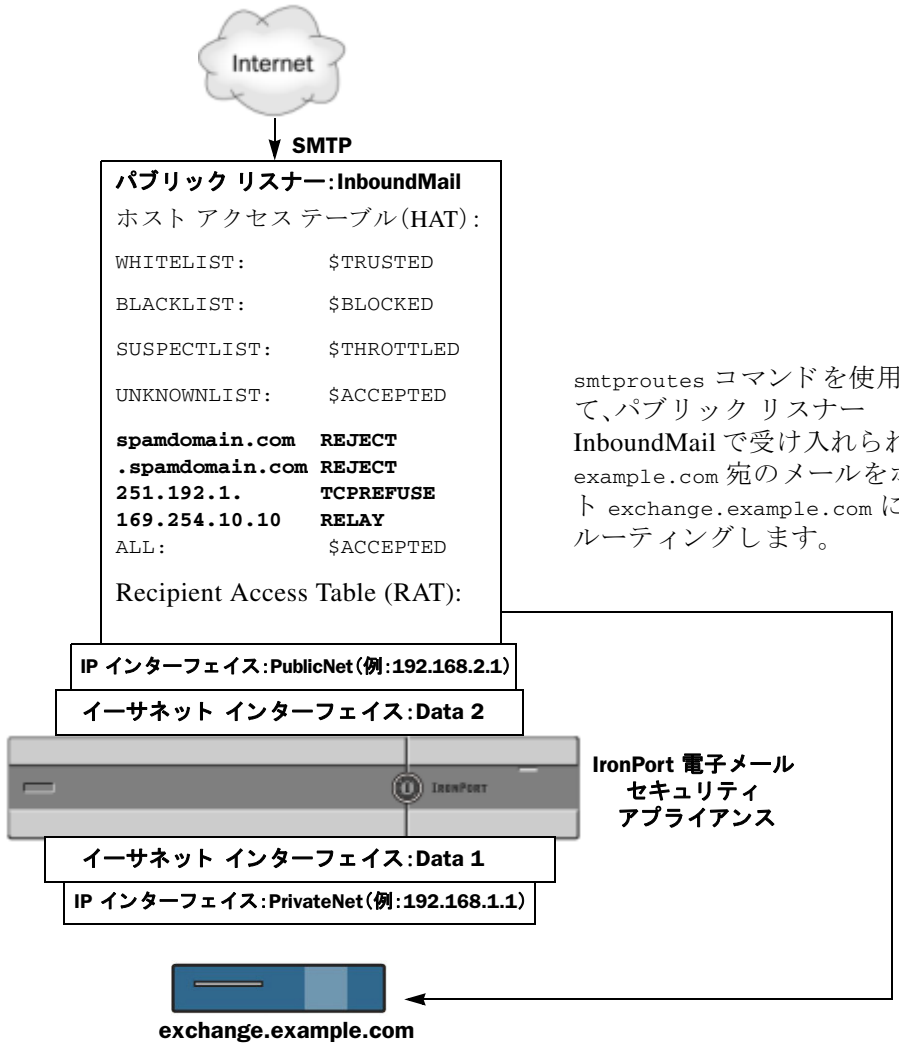
ステップ 4　[インポート（Import）] をクリックします。

ファイルには「コメント」を格納できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

```
# this is a comment, but the next line is not

ALL:
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 2-3　　パブリック リスナー用に定義された SMTP ルート



アドレスの書き換え

AsyncOS では、電子メール パイプラインでエンベロープ送信者および受信者のアドレスを書き換える方法が複数あります。アドレスの書き換えは、たとえばパートナー ドメインに送信されたメールをリダイレクトする場合や、社内インフラストラクチャを隠す（マスクする）場合に使用できます。

表 2-1 に、送信者および受信者の電子メール アドレスを書き換えるために使用される各種機能の概要を示します。

表 2-1　アドレスの書き換え方法

元のアドレス	変更後	機能	作業対象
*@anydomain	user@domain	エイリアス テーブル（エイリアス テーブルの作成（2-8 ページ）を参照）	• エンベロープ受信者のみ • グローバルに適用 • エイリアスを電子メール アドレスまたは他のエイリアスにマッピング
*@olddomain	*@newdomain	ドメイン マッピング（ドメイン マップ機能（2-28 ページ）を参照）	• エンベロープ受信者のみ • リスナーごとに適用
*@olddomain	*@newdomain	マスカレード（マスカレードの設定（2-17 ページ）を参照）	• エンベロープ送信者、および To:、From:、または CC: ヘッダー • リスナーごとに適用

エイリアス テーブルの作成

エイリアス テーブルを使用すると、1 人または複数の受信者にメッセージをリダイレクトできます。エイリアスからユーザ名や他のエイリアスへのマッピング テーブルは、一部の UNIX システムで sendmail コンフィギュレーションの `/etc/mail/aliases` 機能と同様の方法で作成できます。

リスナーが受信した電子メールのエンベロープ受信者（Envelope To または `RCPT TO` とも呼ばれます）がエイリアス テーブルで定義されているエイリアスと一致すると、電子メールのエンベロープ受信者アドレスが書き換えられます。

（注）　RAT チェックの*後*からメッセージ フィルタの*前*までに、リスナーはエイリアス テーブルをチェックし、受信者を変更します。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「電子メール パイプラインについて」の章を参照してください。

（注）　エイリアス テーブル機能により、電子メールのエンベロープ受信者が実際に書き換えられます。これは、電子メールのエンベロープ受信者を書き換えず、電子メールを指定されたドメインに再ルーティングするだけの `smtproutes` コマンド（バウンスした電子メールの処理（2-35 ページ）を参照）とは異なります。

コマンド ラインによるエイリアス テーブルの設定

エイリアス テーブルはセクションで定義します。各セクションの先頭にはドメイン コンテキスト（そのセクションに関連するドメインのリスト）があり、その後にマップのリストが続きます。

ドメイン コンテキストは、1 つ以上のドメインまたは部分ドメインのリストです。カンマで区切り、角カッコ（「[」および「]」）で囲みます。ドメインは、文字、数字、ハイフン、およびピリオドで構成される文字列です（RFC 1035、セクション 2.3.1 の「優先される名前構文」を参照）。部分ドメイン（.example.com など）は、ピリオドで始まるドメインです。部分ドメインに一致するサブ文字列で終わるようなすべてのドメインは、一致であると見なされます。たとえば、ドメイン コンテキスト .example.com は、mars.example.com および venus.example.com と一致します。ドメイン コンテキストの後には、マップ（エイリアスと受信者リスト）のリストがあります。マップは、次のように構成されます。

表 2-2　　エイリアス テーブルの構文

左辺（LHS）	区切り文字	右辺（RHS）
一致する 1 つ以上のエイリアスのリスト	コロン文字「:」	1 つ以上の受信者アドレスまたはエイリアスのリスト

左辺のエイリアスでは、次の形式を使用できます。

username	一致するエイリアスを指定します。先行する「ドメイン」属性がテーブルで指定されている必要があります。このパラメータがないと、エラーになります。
user@domain	一致する正確な電子メール アドレスを指定します。

左辺 1 行あたり複数のエイリアスをカンマで区切って入力できます。

右辺の各受信者は、user@domain 形式の完全な電子メール アドレス、または別のエイリアスを指定できます。

エイリアス ファイルには、暗黙的なドメインのない「グローバルな」エイリアス（特定ドメインではなく、グローバルに適用されるエイリアス）、エイリアスに 1 つ以上の暗黙的なドメインのあるドメイン コンテキスト、またはその両方を指定できます。

エイリアスの「チェーン」（再帰的なエントリ）を作成することはできますが、完全な電子メール アドレスで終わる必要があります。

sendmail コンフィギュレーションのコンテキストと互換性を持たせるために、メッセージをドロップするための特殊な宛先である /dev/null がサポートされています。エイリアス テーブルによってメッセージが /dev/null にマッピングされると、ドロップ済みカウンタが増分します。（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「CLI による管理およびモニタリング」の章を参照）。受信者は受け入れられますが、キューには入れられません。

エイリアス テーブルのエクスポートおよびインポート

エイリアス テーブルをインポートするには、先に付録 B「アプライアンスへのアクセス」を確認し、アプライアンスにアクセスできるようにします。

既存のエイリアス テーブルを保存するには、aliasconfig コマンドの export サブコマンドを使用します。ファイル（ファイル名は自分で指定）は、リスナーの /configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。（ファイルに不正な形式のエントリがある場合は、ファイルのインポート時にエラーが出力されます）。

エイリアス テーブル ファイルを /configuration ディレクトリに配置し、aliasconfig コマンドの import サブコマンドを使用してファイルをアップロードします。

テーブルの行の先頭でナンバー記号(#)を使用すると、その行がコメントアウトされます。

コンフィギュレーションの変更が反映されるように、必ずエイリアス テーブル ファイルをインポートした後で commit コマンドを発行してください。

エイリアス テーブルのエントリの削除

コマンドライン インターフェイス(CLI)を使用してエイリアス テーブルからエントリを削除する場合は、先にドメイン グループを選択するように求められます。「ALL (any domain)」エントリを選択すると、すべてのドメインに適用されるエイリアスの番号付きリストが表示されます。その後、削除するエイリアスの番号を選択します。

エイリアス テーブルの例

(注)　このテーブル例のすべてのエントリは、コメントアウトされています。

```
# sample Alias Table file

# copyright (c) 2001-2005, IronPort Systems, Inc.

#

# Incoming Envelope To addresses are evaluated against each

# entry in this file from top to bottom. The first entry that

# matches will be used, and the Envelope To will be rewritten.

#

# Separate multiple entries with commas.

#

# Global aliases should appear before the first domain

# context. For example:

#

#   admin@example.com: administrator@example.com

#   postmaster@example.net: administrator@example.net

#

# This alias has no implied domain because it appears

# before a domain context:

#

#   someaddr@somewhere.dom: specificperson@here.dom
```

```
#
# The following aliases apply to recipients @ironport.com and
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
# delivered to joseph@example.com
#
#   [ironport.com, .example.com]
#
#   joe, fred: joseph@example.com
#

# In this example, email to partygoers will be sent to
# three addresses:
#
#   partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
#   [example.com]
#
#   help: customercare@otherhost.dom
```

```
#
# In this example, mail to nobody@example.com is dropped.
#
#   nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
#   [example.com]
#
#   all: sales, marketing, engineering
#   sales: joe@example.com, fred@example.com, mary@example.com
#   marketing:bob@example.com, advertising
#   engineering:betty@example.com, miles@example.com, chris@example.com
#   advertising:richard@example.com, karen@advertising.com
```

aliasconfig コマンドの例

この例では、aliasconfig コマンドを使用してエイリアス テーブルを作成します。まず、**example.com** のドメイン コンテキストを指定します。次に、**customercare** のエイリアスを作成し、customercare@example.com に送信されたすべての電子メールが bob@example.com、frank@example.com、および sally@example.com にリダイレクトされるようにします。さらに、**admin** のグローバル エイリアスを作成し、admin に送信された電子メールが administrator@example.com にリダイレクトされるようにします。最後に、確認用にエイリアス テーブルが出力されます。

テーブルの出力時に、admin のグローバル エイリアスは、example.com の最初のドメイン コンテキストの*前*に出力されます。

```
mail3.example.com> aliasconfig


No aliases in table.


Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import aliases from a file.
```

```
[]> new

How do you want your aliases to apply?

1. Globally
2. Add a new domain context
[1]> 2

Enter new domain context.
Separate multiple domains with commas.
Partial domains such as .example.com are allowed.
[]> example.com

Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
    - "user" - This user in this domain context.
    - "user@domain" - This email address.
[]> customercare

Enter address(es) for "customercare".
Separate multiple addresses with commas.
[]> bob@example.com, frank@example.com, sally@example.com

Adding alias customercare: bob@example.com,frank@example.com,sally@example.com
Do you want to add another alias?  [N]> n

There are currently 1 mappings defined.
Choose the operation you want to perform:
```

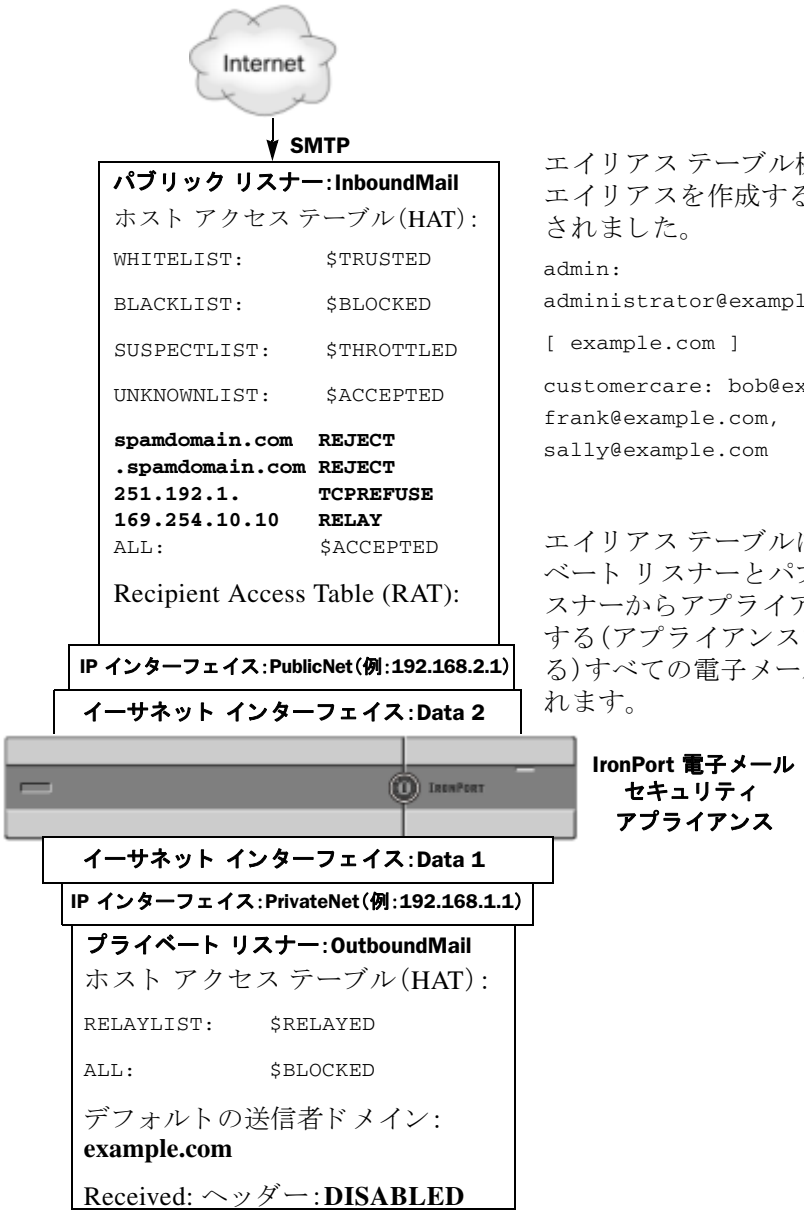
```
- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.

- CLEAR - Clear the table.

[]> new


How do you want your aliases to apply?


1. Globally

2. Add a new domain context

3. example.com

[1]> 1


Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

    - "user@domain" - This email address.

    - "user" - This user for any domain

    - "@domain" - All users in this domain.

    - "@.partialdomain" - All users in this domain, or any of its sub domains.

[]> admin


Enter address(es) for "admin".

Separate multiple addresses with commas.

[]> administrator@example.com
```

```
Adding alias admin: administrator@example.com

Do you want to add another alias?  [N]> n


There are currently 2 mappings defined.


Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.

- CLEAR - Clear the table.

[]> print


admin: administrator@example.com


[ example.com ]

customercare: bob@example.com, frank@example.com, sally@example.com


There are currently 2 mappings defined.


Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.
```

```
- CLEAR - Clear the table.

[]>
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 2-4　　アプライアンスに定義されたエイリアス テーブル



エイリアス テーブル機能は、次のエイリアスを作成するために設定されました。

```
admin:
administrator@example.com

[ example.com ]

customercare: bob@example.com,
frank@example.com,
sally@example.com
```

エイリアス テーブルは、プライベート リスナーとパブリック リスナーからアプライアンスを通過する（アプライアンスで受信される）すべての電子メールに適用されます。

マスカレードの設定

マスカレードは、作成したテーブルに従って、エンベロープ送信者（送信者または MAIL FROM とも呼ばれます）、およびリスナーで処理される電子メールの To:、From:、CC: ヘッダーを書き換える機能です。この機能の典型的な実装例は、「仮想ドメイン」です。単一のサイトから複数のドメインをホストできます。もう一つの典型的な実装は、電子メール ヘッダー内の文字列からサブドメインを「取り除く」ことで、ネットワーク インフラストラクチャを「隠す」ことです。マスカレード機能は、プライベート リスナーとパブリック リスナーの両方で利用できます。

（注）　マスカレード機能は、システム全体に対して設定するエイリアス テーブル機能とは異なり、リスナー単位で設定します。

（注）　リスナーは、LDAP 受信者受け入れクエリーの直後で LDAP ルーティング クエリーの前、メッセージがワーク キュー内にある間に、マスカレード テーブルで一致を探して受信者を変更します。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「電子メール パイプラインについて」の章を参照してください。

マスカレード機能により、エンベロープ送信者および受信した電子メールの To:、From:、CC: フィールドのアドレスが実際に書き換えられます。作成するリスナーごとに別々のマスカレード パラメータを指定できます。2 つある方法のいずれかを使用します。

ステップ 1　作成したマッピングのスタティック テーブルを使用、または

ステップ 2　LDAP クエリーを使用

この項では、スタティック テーブルを使用する方法について説明します。テーブルの形式は、一部の UNIX システムで sendmail コンフィギュレーションの /etc/mail/genericstable 機能と上位互換性があります。LDAP マスカレード クエリーの詳細については、第 3 章「LDAP クエリ」を参照してください。

マスカレードと altsrchost

一般に、マスカレード機能ではエンベロープ送信者が書き換えられ、メッセージで実行されるそれ以降のアクションは、マスカレードされたアドレスから「トリガー」されます。ただし、CLI から altscrchost コマンドを実行した場合、altscrchost マッピングは元のアドレスからトリガーされます（つまり変更後のマスカレードされたアドレスではない）。

詳細については、Virtual Gateway™ テクノロジーの使用（2-59 ページ）および確認：電子メール パイプライン（2-73 ページ）を参照してください。

スタティック マスカレード テーブルの構成

マッピングのスタティック マスカレード テーブルを設定するには、listenerconfig コマンドの edit -> masquerade サブコマンドを使用します。また、マッピングが含まれるファイルをインポートできます。マスカレード テーブルのインポート（2-19 ページ）を参照してください。このサブコマンドにより、入力アドレス、ユーザ名、およびドメインを新しいアドレスおよびドメインにマッピングするテーブルを作成および維持します。LDAP マスカレード クエリーの詳細については、第 3 章「LDAP クエリ」を参照してください。

メッセージがシステムに挿入されるときは、テーブルが参照され、ヘッダーに一致が見つかるとメッセージが書き換えられます。

ドメインのマスカレード テーブルは、次のように構成されます。

表 2-3　　マスカレード テーブルの構文

左辺（LHS）	区切り文字	右辺（RHS）
一致する 1 つ以上のユーザ名やドメインのリスト	空白文字（スペースまたはタブ文字）	書き換え後のユーザ名やドメイン

次の表に、マスカレード テーブルで有効なエントリを示します。

左辺（LHS）	右辺（RHS）
username	username@domain
このエントリは、一致するユーザ名を指定します。左辺のユーザ名に一致する着信電子メール メッセージは、一致となり、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
user@domain	username@domain
このエントリは、一致する正確なアドレスを指定します。左辺の完全なアドレスに一致する着信メッセージは、右辺のアドレスで書き換えられます。右辺は、完全なアドレスである必要があります。	
@domain	**@domain**
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
@.partialdomain	**@domain**
このエントリは、特定のドメインの任意のアドレスを指定します。左辺の元のドメインは、右辺のドメインで置き換えられますが、ユーザ名は変更ありません。	
ALL	**@domain**
ALL エントリは、そのままのアドレスに一致し、右辺のアドレスで書き換えます。右辺は、ドメインの先頭に「@」を付ける必要があります。このエントリは、テーブル内の位置に関係なく、常に優先度最低になります。 **（注）**　ALL エントリは、プライベート リスナーのみに使用できます。	

- ルールは、マスカレード テーブルでの出現順序に従って一致します。
- デフォルトでは受信時にヘッダーの From:、To:、および CC: フィールド内のアドレスが一致し、書き換えられます。エンベロープ送信者に一致して書き換えるようにオプションを設定することもできます。エンベロープ送信者および書き換え対象ヘッダーは、config サブコマンドを使用して有効と無効を切り替えます。
- テーブルの行の先頭でナンバー記号（#）を使用すると、その行がコメントアウトされます。# から行の末尾まで、すべてコメントであると見なされて無視されます。
- マスカレード テーブルは、最大で 400,000 エントリです。これは、new サブコマンドを使ってエントリ作成した場合も、ファイルからインポートした場合も同じです。

プライベート リスナー用マスカレード テーブルの例

```
# sample Masquerading file

@.example.com @example.com # Hides local subdomains in the header

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

マスカレード テーブルのインポート

従来の sendmail の `/etc/mail/genericstable` ファイルをインポートできます。`genericstable` ファイルをインポートするには、先に付録 B「アプライアンスへのアクセス」を確認し、アプライアンスにアクセスできるようにします。

`genericstable` ファイルを configuration ディレクトリに配置し、`masquerade` サブコマンドの `import` サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

`listenerconfig` -> `edit` -> *injector_number* -> `masquerade` -> `import`

または、`export` サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

`import` サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ（左辺があって右辺がない場合など）があると、ファイルのインポート時に CLI で構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更内容が反映されるように、`genericstable` ファイルをインポートした後で必ず `commit` コマンドを発行してください。

マスカレードの例

この例では、`listenerconfig` の `masquerade` サブコマンドを使用して、PrivateNet インターフェイス上にある「OutboundMail」という名前のプライベート リスナー用に、ドメイン マスカレード テーブルを作成します。

まず、マスカレードに LDAP を使用するオプションを宣言します。（LDAP マスカレード クエリーの詳細については、第 3 章「LDAP クエリ」を参照してください）。

次に、**`@.example.com`** の部分ドメイン表記が **`@example.com`** にマッピングされます。これにより、サブドメイン `.example.com` 内にある任意のマシンから送信されるすべての電子メールが `example.com` にマッピングされます。さらに、ユーザ名 **`joe`** がドメイン **`joe@example.com`** にマッピングされます。両方のエントリを確認するためにドメイン マスカレード テーブルが出力されて、`masquerade.txt` という名前のファイルにエクスポートされます。`config` サブコマンドを使用して、CC: フィールドのアドレスの書き換えが無効になり、最後に変更が確定されます。

```
mail3.example.com> listenerconfig


Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit


Enter the name or number of the listener you wish to edit.

[]> 2


Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off
```

```
Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]> masquerade


Do you want to use LDAP for masquerading?  [N]> n


Domain Masquerading Table


There are currently 0 entries.

Masqueraded headers: To, From, Cc


Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.
```

```
- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[]> @.example.com


Enter the masqueraded address or domain.

Domains like @example.com are allowed.

Full addresses such as user@example.com are allowed.

[]> @example.com


Entry mapping @.example.com to @example.com created.

Domain Masquerading Table


There are currently 1 entries.

Masqueraded headers: To, From, Cc


Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.
```

```
- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

Full addresses like "user@example.com" are allowed.

Full addresses with subdomain wildcards such as "username@.company.com" are allowed.

Domains like @example.com and @.example.com are allowed.

Hosts like @training and @.sales are allowed.

[]> joe


Enter the masqueraded address.

Only full addresses such as user@example.com are allowed.

[]> joe@example.com


Entry mapping joe to joe@example.com created.

Domain Masquerading Table


There are currently 2 entries.

Masqueraded headers: To, From, Cc


Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.
```

```
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> print

@.example.com    @example.com
joe    joe@example.com

Domain Masquerading Table

There are currently 2 entries.
Masqueraded headers: To, From, Cc

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> export

Enter a name for the exported file:
[]> masquerade.txt

Export completed.
Domain Masquerading Table
```

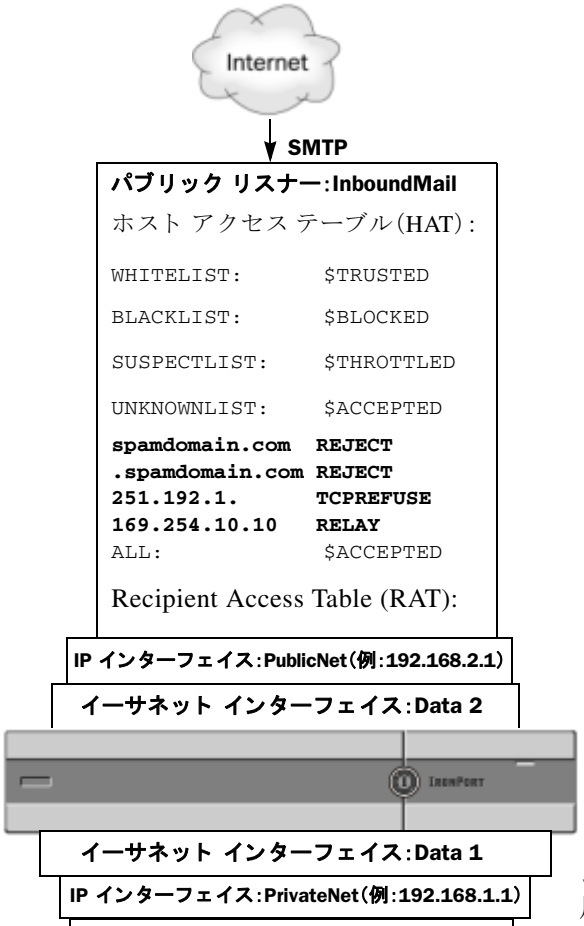
```
There are currently 2 entries.

Masqueraded headers: To, From, Cc


Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> config


Do you wish to masquerade Envelope Sender?

[N]> y


Do you wish to masquerade From headers?

[Y]> y


Do you wish to masquerade To headers?

[Y]> y


Do you wish to masquerade CC headers?

[Y]> n


Do you wish to masquerade Reply-To headers?

[Y]> n


Domain Masquerading Table
```

```
There are currently 2 entries.


- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]>


Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Footer: None
LDAP: Off


Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
```

```
- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

- LDAPACCEPT - Configure an LDAP query to determine whether a recipient address should
be accepted or bounced/dropped.

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]>


Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>


mail3.example.com> commit
```

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 2-5　　プライベート リスナー用に定義されたマスカレード



このプライベート リスナー用に、マスカレード テーブルに 2 つのエントリが追加されました。1 番めのエントリは、ネットワークのすべてのサブドメインをマスクします（例：exchange.example.com は example.com に書き換えられます）。2 番めのエントリは、そのままのアドレス joe を joe@example.com に書き換えます。

ドメイン マップ機能

リスナー用に「ドメイン マップ」を設定できます。設定するリスナーごとにドメイン マップ テーブルを作成できます。ドメイン マップ テーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロープ受信者が書き換えられます。この機能は、sendmail の「ドメイン テーブル」機能または Postfix の「仮想テーブル」機能に似ています。この機能では、エンベロープ受信者のみが影響を受け、「To:」ヘッダーは書き換えられません。

（注）　ドメイン マップ機能の処理は、RAT の直前でデフォルト ドメインの評価直後に発生します。『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「電子メール パイプラインについて」の章を参照してください。

ドメイン マップ機能でよくある実装では、複数のレガシー ドメインの着信メールを受け入れます。たとえば、会社が他の会社を買収した場合に、Cisco IronPort アプライアンスにドメイン マップを作成して買収したドメインのメッセージを受け入れ、エンベロープ受信者を会社の現在のドメインに書き換えることができます。

（注）　最大 20,000 の別個の固有ドメイン マッピングを設定できます。

表 2-4　ドメイン マップ テーブルの構文の例

左側	右側	説明
username@example.com	**username2@example.net**	右側は完全なアドレスのみ
user@.example.com	**user2@example.net**	
@example.com	**user@example.net** ***または*** **@example.net**	完全なアドレス、または完全修飾ドメイン名。
@.example.com	**user@example.net** ***または*** **@example.net**	

次の例では、`listenerconfig` コマンドの `domainmap` サブコマンドを使用して、パブリック リスナー「InboundMail」用のドメイン マップを作成します。`oldcompanyname.com` ドメインおよびそのサブドメイン宛のメールは、`example.com` ドメインにマッピングされます。マッピングは、確認のために出力されます。この例は、両方のドメインをリスナーの RAT に配置するコンフィギュレーションとは異なります。ドメイン マップ機能により、実際にエンベロープ受信者 `joe@oldcomapanyname.com` が `joe@example.com` に書き換えられます。一方、リスナーの RAT 内にドメイン `oldcompanyname.com` を置くと、`joe@oldcompanyname.com` のメールが受け入れられて、エンベロープ受信者を書き換えずにルーティングされます。また、エイリアス テーブル機能とも異なります。エイリアス テーブルでは、明示的なアドレスに解決されることが*必要*です。「*任意のユーザ名*`@domain`」を「*同じユーザ名*`@newdomain`」にマッピングするようには作成できません。

```
mail3.example.com> listenerconfig


Currently configured listeners:

1. Inboundmail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public

2. Outboundmail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private


Choose the operation you want to perform:
```

```
- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit


Enter the name or number of the listener you wish to edit.

[]> 1


Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off


Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.
```

```
- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]> domainmap


Domain Map Table


There are currently 0 Domain Mappings.

Domain Mapping is: disabled


Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import domain mappings from a file.

[]> new


Enter the original domain for this entry.

Domains such as "@example.com" are allowed.

Partial hostnames such as "@.example.com" are allowed.

Email addresses such as "test@example.com" and "test@.example.com"

 are also allowed.

[]> @.oldcompanyname.com


Enter the new domain for this entry.

The new domain may be a fully qualified

such as "@example.domain.com" or a complete

email address such as "test@example.com"

[]> @example.com
```

```
Domain Map Table


There are currently 1 Domain Mappings.

Domain Mapping is: enabled


Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display all domain mappings.

- IMPORT - Import domain mappings from a file.

- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]> print


@.oldcompanyname.com --> @example.com


Domain Map Table


There are currently 1 Domain Mappings.

Domain Mapping is: enabled


Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display all domain mappings.

- IMPORT - Import domain mappings from a file.
```

```
- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]>


Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off


Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this
listener.

- MASQUERADE - Configure the Domain Masquerading Table.
```

```
- DOMAINMAP - Configure domain mappings.

[]>
```

ドメイン マップ テーブルのインポートおよびエクスポート

ドメイン マップ テーブルをインポートまたはエクスポートするには、先に付録 B「アプライアンスへのアクセス」を確認し、アプライアンスにアクセスできるようにします。

マッピングするドメインのエントリが含まれるテキスト ファイルを作成します。エントリは空白文字（タブ文字またはスペース）で区切ります。テーブルの行の先頭でナンバー記号（#）を使用すると、その行がコメントアウトされます。

ファイルを configuration ディレクトリに配置し、`domain` サブコマンドの `import` サブコマンドを使用してファイルをアップロードします。コマンドは、次の順序で使用します。

`listenerconfig` -> `edit` -> *inejctor_number* -> `domainmap` -> `import`

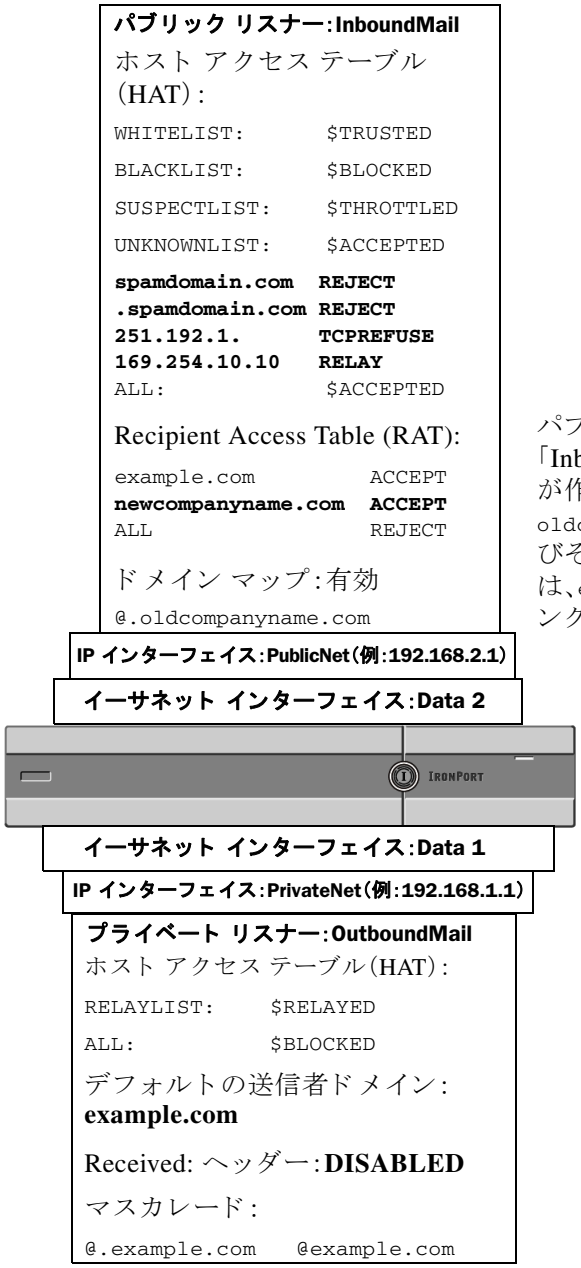
または、`export` サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

`import` サブコマンドを使用するときは、ファイルに有効なエントリのみが含まれているようにしてください。無効なエントリ（左辺があって右辺がない場合など）があると、ファイルのインポート時に CLI で構文エラーが発生します。インポート中に構文エラーが発生すると、ファイル全体でマッピングがインポートされません。

リスナーのコンフィギュレーションの変更が反映されるように、ドメイン マップ テーブル ファイルをインポートした後で `commit` コマンドを発行してください。

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 2-6　　パブリック リスナー用に定義されたドメイン マップ



パブリック リスナー「InboundMail」のドメイン マップが作成されました。oldcompanyname.com ドメインおよびそのサブドメイン宛のメールは、example.com ドメインにマッピングされます。

バウンスした電子メールの処理

バウンスした電子メールは、あらゆる電子メール配信においてやむを得ないものです。Cisco IronPort アプライアンスでは、詳細に設定できるさまざまな方法で、バウンスした電子メールを処理できます。

この項では、Cisco IronPort アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御について説明していることに注意してください。Cisco IronPort アプライアンスが発信メールに基づいて着信バウンスを制御する方法について管理するには、Cisco IronPort バウンス検証を使用します(Cisco IronPort バウンス検証(2-52 ページ)を参照)。

配信不可能な電子メールの処理

Cisco IronPort AsyncOS オペレーティング システムでは、配信不可能な電子メール（「バウンスしたメッセージ」）は、次のカテゴリに分類されます。

「カンバセーション」バウンス： 最初の SMTP カンバセーションで、リモート ドメインがメッセージをバウンスします。	
ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱいです。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コード）。
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エラー コード）。
「遅延」（または「カンバセーションでない」）バウンス： リモート ドメインは、メッセージを配信するために受け入れて、後でのみバウンスします。	
ソフト バウンス	一時的に配信不可能なメッセージ。たとえば、ユーザのメールボックスがいっぱいです。これらのメッセージは、後で再試行できます。（例：SMTP 4XX エラー コード）。
ハード バウンス	永続的に配信できないメッセージ。たとえば、そのユーザはそのドメインにはもう存在しません。これらのメッセージは、再試行されません。（例：SMTP 5XX エラー コード）。

GUI の [ネットワーク（Network）] メニューの [バウンスプロファイル（Bounce Profiles）] ページ（または `bounceconfig` コマンド）を使用して、作成するリスナーごとにハードおよびソフトのカンバセーション バウンスの Cisco IronPort AsyncOS の処理方法を設定します。バウンス プロファイルを作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または `listenerconfig` コマンド）を使用して、プロファイルを各リスナーに適用します。メッセージ フィルタを使用して、特定のメッセージにバウンス プロファイルを割り当てることもできます。（詳細については、第 6 章「メッセージ フィルタを使用した電子メール ポリシーの適用」を参照してください）。

ソフト バウンスおよびハード バウンスに関する注意

- カンバセーション ソフト バウンスの場合、ソフト バウンス イベントは、受信者への配信が一時的に失敗するたびに定義されます。単一の受信者が複数のソフト バウンス イベントを繰り返し発生させることがあります。[バウンスプロファイル（Bounce Profiles）] ページまたは `bounceconfig` コマンドを使用して、各ソフト バウンス イベントのパラメータを設定します。（バウンス プロファイルのパラメータ（2-37 ページ）を参照）。
- デフォルトでは、ハード バウンスした受信者ごとにバウンス メッセージが生成され、元の送信者に送信されます。（メッセージは、メッセージ エンベロープのエンベロープ送信者アドレスで定義されたアドレスに送信されます。Envelope From も通常エンベロープ送信者を意味します）。この機能をディセーブルにし、代わりにハード バウンスに関する情報をログ ファイルに頼ることもできます。（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「ログイン」を参照してください。）
- キュー内での最大時間または再試行の最大回数のどちらかに達すると、ソフト バウンスはハード バウンスになります。

バウンス プロファイルのパラメータ

バウンス プロファイルを設定するときは、次のパラメータを使用して、メッセージごとにカンバセーション バウンスを処理する方法を制御します。

表 2-5　バウンス プロファイルのパラメータ

最大再試行回数（Maximum number of retries）	ソフト バウンスしたメッセージを配信し直すために、ハード バウンス メッセージとして扱われるようになる前に、受信者のホストに再接続が試みられる回数。デフォルトの再試行回数は 100 です。
キューの最大時間（秒）（Maximum number of seconds in queue）	ソフト バウンスしたメッセージを配信し直すために、ハード バウンスしたメッセージとして扱われるようになる前に、受信者のホストに再接続が試みられるのに費やされる時間。デフォルトは 259,200 秒（72 時間）です。
メッセージを再試行するまでの初回待機時間（秒）（Initial number of seconds to wait before retrying a message）	ソフト バウンスしたメッセージを最初に配信し直すまでの待機時間。デフォルトは 60 秒です。初回再試行時間を大きい値に設定すると、ソフト バウンスの試行頻度が低下します。逆に頻度を上げるには、小さい値にします。
メッセージを再試行するまでの最大待機時間（秒）（Maximum number of seconds to wait before retrying a message）	ソフト バウンスしたメッセージを配信し直すまでに待機する最大時間。デフォルトは 3,600 秒（1 時間）です。これは、次の試行までの間隔ではなく、再試行回数を制御するために使用できるもう 1 つのパラメータです。初回再試行間隔の上限は、最大再試行間隔に制限されます。計算された再試行間隔が最大再試行間隔を超える場合は、最大再試行間隔が使用されます。
ハード バウンス メッセージの生成形式（Hard bounce message generation format）	ハード バウンス メッセージの生成がイネーブルかディセーブルかを指定します。イネーブルの場合は、メッセージの形式を選択できます。デフォルトでは、生成されるバウンス メッセージで DSN 形式（RFC 1894）が使用されます。バウンス メッセージに使用するカスタム通知テンプレートを選択できます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「テキスト リソース」の章を参照してください。 バウンス応答から DSN の status フィールドを解析するかどうかを選択することもできます。「はい」の場合、AsyncOS は DSN ステータス コード（RFC 3436）を検索し、そのコードを配信ステータス通知の Status フィールドで使用します。
遅延警告メッセージの送信（Send delay warning messages）	遅延の警告を送信するかどうかを指定します。イネーブルにした場合は、メッセージ間の最小間隔、および送信する最大再試行回数を指定します。 警告メッセージに使用するカスタム通知テンプレートを選択できます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「テキスト リソース」の章を参照してください。
バウンス先の受信者の指定（Specify Recipient for Bounces）	メッセージのバウンス先としてデフォルトのエンベロープ送信者アドレスではなく、別のアドレスにすることができます。
バウンスおよび遅延メッセージへの DomainKeys 署名の使用（Use DomainKeys signing for bounce and delay messages）	バウンス メッセージおよび遅延メッセージの署名に使用する DomainKeys プロファイルを選択できます。DomainKeys の詳細については、DomainKeys および DKIM 認証：概要（5-2 ページ）を参照してください。
グローバル設定（Global Settings）	

表 2-5　バウンス プロファイルのパラメータ（続き）

これらの設定を行うには、[バウンスプロファイル（Bounce Profiles）] ページの [グローバル設定を編集（Edit Global Settings）] リンクを使用するか、または CLI で `bounceconfig` コマンドでデフォルトのバウンス プロファイルを編集します。	
到達不能ホストをリトライするまでの最初の待機時間（秒）（Initial number of seconds to wait before retrying an unreachable host）	システムが到達不可能なホストへの再試行を待機する時間。 デフォルトは 60 秒です。
到達不能ホストの最大許容再試行間隔（Max interval allowed between retries to an unreachable host）	システムが到達不可能なホストへの再試行を待機する最大時間。デフォルトは 3,600 秒（1 時間）です。ホストがダウンしているために配信が最初に失敗すると、再試行値の最小秒数で開始し、ダウンしたホストに対するその後の再試行では、間隔を徐々に延ばしていきます。最大で、この最大秒数になります。

ハード バウンスと status コマンド

ハード バウンス メッセージの生成がイネーブルの場合、アプライアンスで配信用のハード バウンス メッセージが生成されるたびに、`status` および `status detail` コマンドの次のカウンタが増えていきます。

```
Counters:                          Reset          Uptime        Lifetime

    Receiving

    Messages Received              0              0             0

    Recipients Received            0              0             0

    Gen. Bounce Recipients         0              0             0
```

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「CLI による管理およびモニタリング」を参照してください。ハード バウンス メッセージの生成がディセーブルの場合、受信者でハード バウンスが発生しても、これらのカウンタはどれも増えません。

（注） メッセージ エンベロープのエンベロープ送信者アドレスは、メッセージ ヘッダーの「From:」とは異なります。Cisco IronPort AsyncOS では、ハード バウンス メッセージをエンベロープ送信者アドレスとは異なる電子メール アドレスに送信するように設定できます。

カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション

SMTP ルート マッピングおよびメッセージ フィルタ アクションは、カンバセーション バウンスの結果としてアプライアンスで生成された SMTP バウンス メッセージのルーティングには適用されません。Cisco IronPort アプライアンスでカンバセーション バウンス メッセージが受信されると、元のメッセージのエンベロープ送信者に返送する SMTP バウンス メッセージが生成されます。この場合、アプライアンスでは実際にメッセージが生成されるため、リレー用に挿入されたメッセージに適用されるすべての SMTP ルートは適用されません。

バウンス プロファイルの例

これら 2 つの例では、異なるバウンス プロファイル パラメータが使用されます。

表 2-6　例 1:バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数（Max number of retries）	2
キューの最大時間（秒）（Maximum number of seconds in queue）	259,200 秒（72 時間）
再試行するまでの初回最大時間（秒）（Initial number of seconds before retrying）	60 秒
再試行するまでの最大待機時間（秒）（Max number of seconds to wait before retrying）	60 秒

例 1 では、受信者への最初の配信は、t = 0 で実行されます。これは、メッセージが Cisco IronPort アプライアンスに挿入された直後です。デフォルトの初回再試行時間は 60 秒であるため、最初の再試行は約 1 分後の t = 60 で実行されます。再試行間隔が計算されます。再試行間隔は、最大再試行間隔である 60 秒を使用して決定されます。そのため、2 回めの再試行は、t = 約 120 で実行されます。最大再試行回数は 2 であるため、この再試行の直後にその受信者のハード バウンス メッセージが生成されます。

表 2-7　例 2:バウンス プロファイル パラメータ

パラメータ	値
最大再試行回数（Max number of retries）	100
キューの最大時間（秒）（Maximum number of seconds in queue）	100 秒
再試行するまでの初回最大時間（秒）（Initial number of seconds before retrying）	60 秒
再試行するまでの最大待機時間（秒）（Max number of seconds to wait before retrying）	120 秒

例 2 では、最初の配信は t = 0、最初の再試行は t = 60 で実行されます。2 回目の配信（t = 120 で発生するようにスケジュール）の直前にメッセージがハード バウンスされます。なぜなら、この時点でキュー内での最大時間である 100 秒を超過しているためです。

配信ステータス通知形式

システムによって生成されるバウンス メッセージは、デフォルトではハードとソフトの両方のバウンスで Delivery Status Notification（DSN; 配信ステータス通知）形式を使用します。DSN は、RFC 1894（`http://www.faqs.org/rfcs/rfc1894.html` を参照）で規定されている形式であり、「メッセージを 1 人以上の受信者に配信したときの結果をレポートするために、Message Transfer Agent（MTA; メッセージ転送エージェント）または電子的なメール ゲートウェイで使用できる MIME コンテンツ タイプを定義」します。デフォルトでは、配信ステータス通知には配信ステータスの説明、およびメッセージのサイズが 10 k よりも小さい場合は元のメッセージが含まれます。メッセージ サイズが 10 k よりも大きい場合、配信ステータス通知には、メッセージ ヘッダーのみが含まれます。メッセージ ヘッダーが 10 k を超える場合は、配信ステータス通知ではヘッダーが切り捨てられます。DSN に 10 k よりも大きいメッセージ（またはメッセージ ヘッダー）を含める場合は、`bounceconfig` コマンドの `max_bounce_copy` パラメータを使用できます（このパラメータは CLI からのみ利用できます）。

遅延警告メッセージ

システムで生成される [遅延通知メッセージ（Time in Queue Message）] でも、DSN 形式が使用されます。デフォルト パラメータを変更するには、[ネットワーク（Network）] メニューの [バウンス プロファイル（Bounce Profiles）] ページ（または `bounceconfig` コマンド）を使用して、既存のバウンス プロファイルを編集するか新規に作成し、以下のパラメータのデフォルト値を変更します。

- 遅延警告メッセージが送信される最小間隔。（The minimum interval between sending delay warning messages.）
- 遅延警告メッセージが送信される受信者あたりの最大数。（The maximum number of delay warning messages to send per recipient.）

遅延警告メッセージとハード バウンス

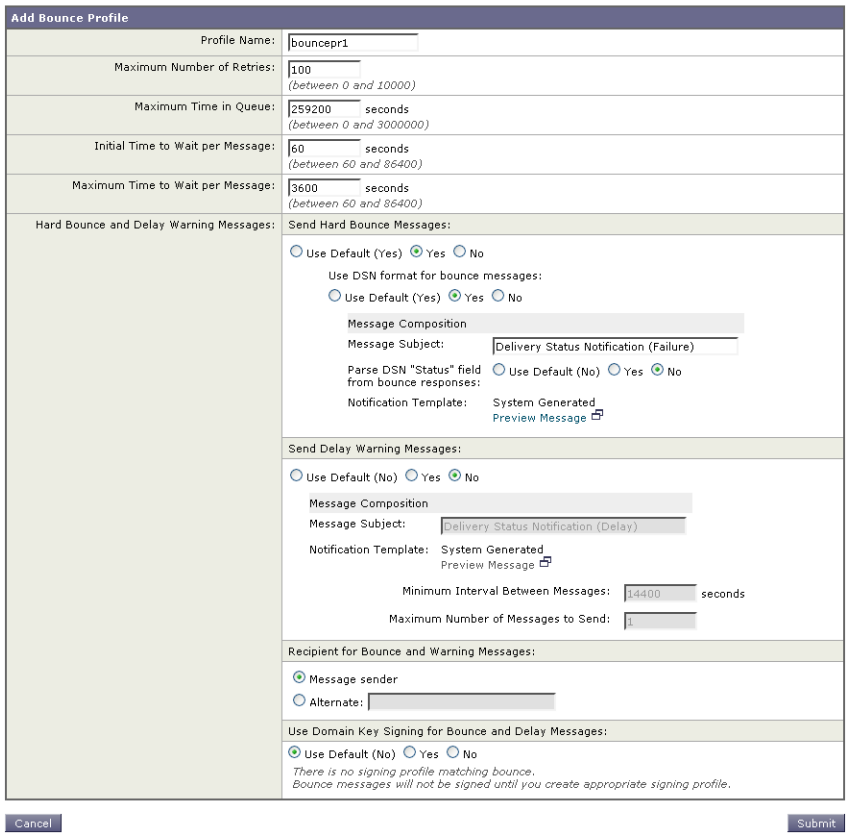
[キューでの最大保持時間（Maximum Time in Queue）] 設定と [遅延警告メッセージの送信（Send Delay Warning Messages）] の最小間隔設定の両方を非常に小さい時間に設定した場合は、同じメッセージに対して遅延警告とハード バウンスの両方を*同時に*受信することが可能です。Cisco IronPort システムでは遅延警告メッセージの送信をイネーブルにする場合は、これらの設定のデフォルト値を最小設定として使用することを推奨します。

さらに、アプライアンスによって生成される遅延警告メッセージおよびバウンス メッセージは、処理中に最大で 15 分遅延することがあります。

新しいバウンス プロファイルの作成

次の例では、[バウンスプロファイル（Bounce Profiles）] ページを使用して、`bouncepr1` という名前のバウンス プロファイルが作成されます。このプロファイルでは、ハード バウンドされたすべてのメッセージが代替アドレスである `bounce-mailbox@example.com` に送信されます。遅延警告メッセージはイネーブルです。受信者あたり警告メッセージが 1 つ送信されます。警告メッセージ間のデフォルト値は 4 時間（14400 秒）です。

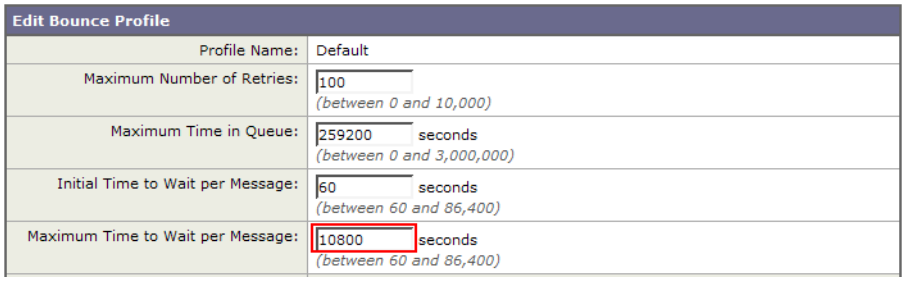
図 2-7　　バウンス プロファイルの作成



デフォルトのバウンス プロファイルの編集

バウンス プロファイルを編集するには、バウンス プロファイルのリストで名前をクリックします。デフォルトのバウンス プロファイルを編集することもできます。この例では、デフォルト プロファイルを編集して、到達不可能なホストへの再試行を待機する最大秒数を 3600（1 時間）から 10800（3 時間）に増やします。

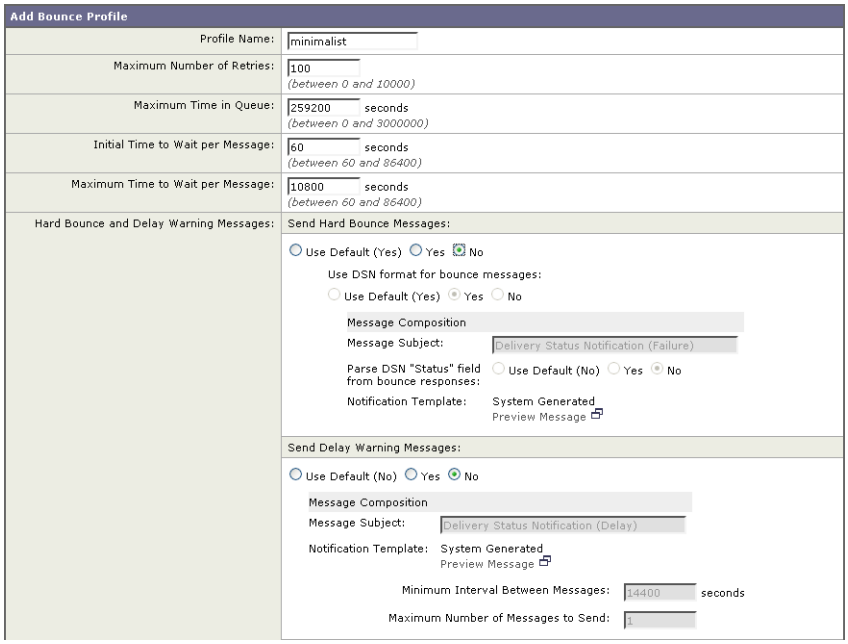
図 2-8　　デフォルトのバウンス プロファイルの編集



minimalist バウンス プロファイルの例

次の例では、minimalist という名前のバウンス プロファイルが作成されます。このプロファイルでは、メッセージがバウンスされるときに再試行されず（最大再試行回数が 0）、再試行を待機する最大時間が指定されます。ハード バウンス メッセージはディセーブルであり、ソフト バウンス警告は送信されません。

図 2-9　「minimalist」バウンス プロファイルの作成

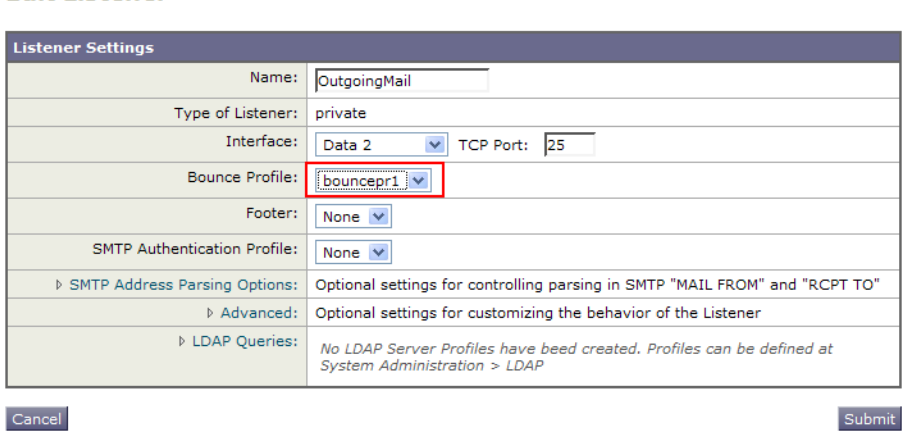


リスナーへのバウンス プロファイルの適用

バウンス プロファイルを作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページまたは listenerconfig コマンドを使用して、そのプロファイルをリスナーに適用できます。

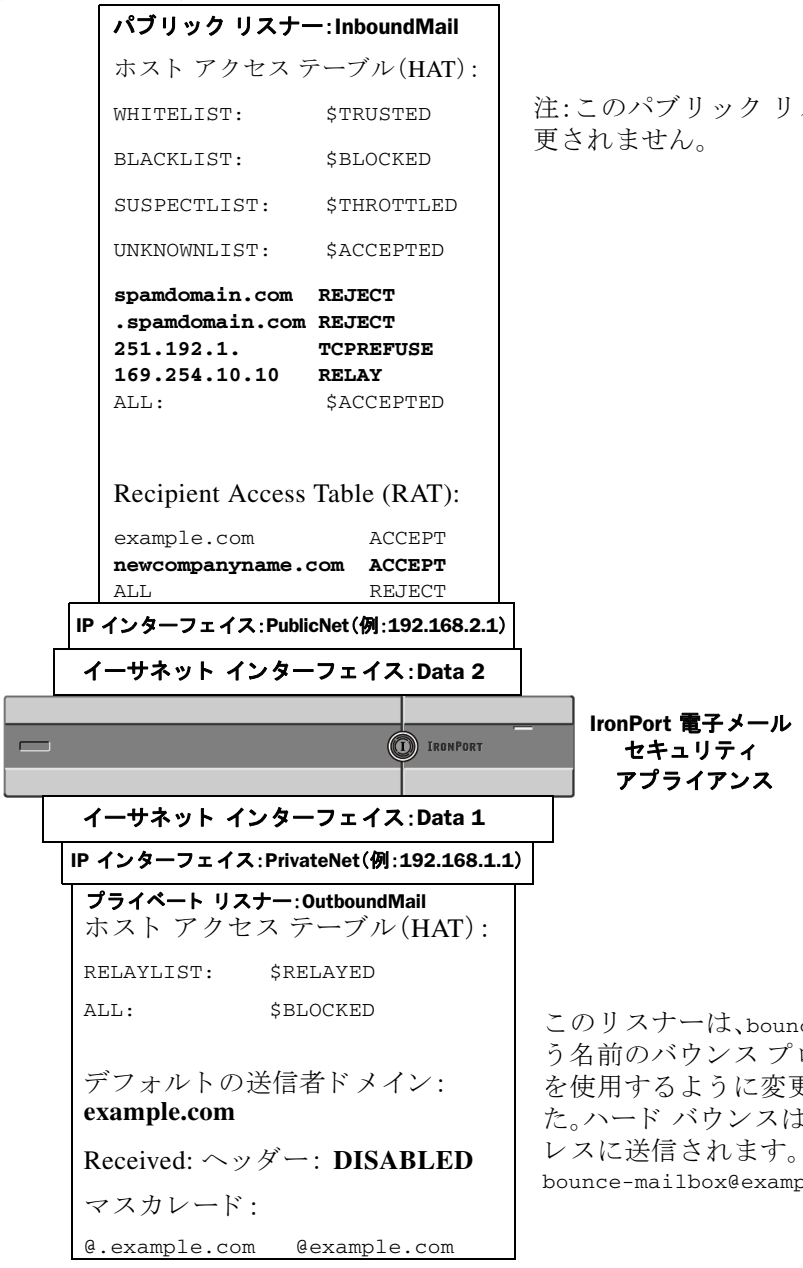
次の例では、bouncepr1 プロファイルが OutgoingMail リスナーに適用されます。

図 2-10　「minimalist」バウンス プロファイルの作成



この時点で、電子メール ゲートウェイの設定は次のようになります。

図 2-11　プライベート リスナーへのバウンス プロファイルの適用



注：このパブリック リスナーは変更されません。

このリスナーは、bouncepr1 という名前のバウンス プロファイルを使用するように変更されました。ハード バウンスは、次のアドレスに送信されます。
bounce-mailbox@example.com.

電子メール配信の管理

大量の電子メールが未管理で配信されると、受信者ドメインで混乱が生じることがあります。AsyncOS では、アプライアンスで開く接続数やアプライアンスで各宛先ドメイン宛に送信されるメッセージ数を定義することにより、メッセージ配信を詳細に管理できます。

送信先コントロール機能（GUI では [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）]、CLI では destconfig コマンド）を使用すると、次の項目を制御できます。

レート制限

- [同時接続（Concurrent Connections）]：リモート ホストに対してアプライアンスが開こうとする同時接続数。
- [接続あたりの最大メッセージ数（Maximum Messages Per Connection）]：アプライアンスが新しい接続を開始する前に、宛先ドメインに送信するメッセージ数。
- [受信者（Recipients）]：アプライアンスが特定の期間に特定のリモート ホストに対して送信する受信者数。
- [制限（Limits）]：宛先ごと、および MGA ホスト名ごとに、制限を適用する方法。

TLS

- リモート ホストに対する TLS 接続を受入、可能、必須のいずれにするか（TLS の管理（2-47 ページ）を参照）。
- TLS 接続が必要なリモート ホストに対してメッセージが配信されるときに、TLS ネゴシエーションが失敗した場合にアラートを送信するかどうか。これは、ドメイン単位ではなく、グローバルな設定です。
- リモート ホストに対するすべての発信 TLS 接続で使用する TLS 証明書の割り当て。

バウンス検証

- Cisco IronPort バウンス検証を使用して、アドレス タギングを実行するかどうか（Cisco IronPort バウンス検証（2-52 ページ）を参照）。

バウンス プロファイル（Bounce Profile）

- 特定のリモート ホストに対してアプライアンスで使用されるバウンス プロファイル（デフォルトのバウンス プロファイルは、[ネットワーク（Network）] > [バウンスプロファイル（Bounce Profiles）] ページで設定します）。

未指定のドメインに対するデフォルト設定を制御することもできます。

メール配信に使用するインターフェイスの決定

出力インターフェイスを `deliveryconfig` コマンド、メッセージ フィルタ（`alt-src-host`）、または仮想ゲートウェイを使用して指定しない場合は、出力インターフェイスは AsyncOS ルーティング テーブルによって選択されます。基本的には、「自動」を選択すると AsyncOS によって選択されます。

詳細は次のとおりです。ローカル アドレスは、インターフェイスのネットマスクをインターフェイスの IP アドレスに適用することで識別されます。どちらも、[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページまたは `interfaceconfig` コマンドを使用して（あるいはシステムのセットアップ時に）設定されます。アドレス空間が重なる場合は、より具体的なネットマスクが使用されます。宛先がローカルの場合、パケットは適切なローカル インターフェイス経由で送信されます。

宛先がローカルではない場合、パケットはデフォルトのルータ（[ネットワーク（Network）] > [ルーティング（Routing）] ページまたは `setgateway` コマンドを使用して設定）に対して送信されます。デフォルト ルータの IP アドレスはローカルです。出力インターフェイスは、ローカル アドレスの出力インターフェイスの選択ルールに従って決まります。たとえば、AsyncOS では、デフォルト ルータの IP アドレスが含まれていて最も具体的な IP アドレスおよびネットマスクが選択されます。

ルーティング テーブルは、[ネットワーク（Network）] > [ルーティング（Routing）] ページ（または routeconfig コマンド）を使用して設定されます。ルーティング テーブルで一致するエントリが、デフォルト ルートよりも優先されます。ルートが具体的になるほど、優先度が高くなります。

デフォルトの配信制限

発信宛先ドメインごとに、専用の発信キューがあります。そのため、ドメインごとに別々の同時接続制限（[送信先コントロール（Destination Controls）] テーブルで指定）があります。さらに、[送信先コントロール（Destination Controls）] テーブルで具体的に示されていない一意のドメインごとに、テーブルで設定した別の「デフォルト（Default）」制限を使用します。

[送信先コントロール（Destination Controls）] の使用

GUI で [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）] ページ、または CLI で destconfig コマンドを使用して、送信先コントロールエントリを作成、編集、および削除します。

IP アドレス バージョンの管理

ドメイン接続に使用する IP アドレスのバージョンを設定できます。E メール セキュリティ アプライアンスは両方のインターネット プロトコル バージョン 4（IPv4）およびインターネット プロトコル バージョン (IPv6) を使用します。アプライアンスのリスナーをプロトコルの両方または 1 つのバージョンを使用するように設定できます。

IPv4 または IPv6 に対して [必須（Required）] 設定を指定した場合、Cisco IronPort アプライアンスは指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションします。ドメインが IP アドレスのバージョンを使わない場合、電子メールは送信されません。IPv4 または IPv6 の [推奨（Preferred）] 設定を指定した場合、Cisco IronPort アプライアンスは最初に指定されたバージョンのアドレスを使用してドメインへの接続をネゴシエーションし、最初の試みが到達可能でない場合は他にフォール バックします。

ドメインに対する接続、メッセージ、受信者の数の管理

アプライアンスで電子メールを配信する方法を制限することにより、アプライアンスからの電子メールを扱うリモート ホストや独自の社内グループウェア サーバに負荷がかかり過ぎないようにできます。

ドメインごとに、特定の期間にシステムで超過しないようにする接続、発信メッセージ、受信者の最大数を割り当てることができます。この「グッド ネイバー」テーブルは、送信先コントロール機能（[メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）]、または destconfig コマンド（以前の setgoodtable コマンド））を使用して定義します。ドメイン名を指定するには、次の構文を使用します。

```
domain.com
```

または

```
.domain.com
```

この構文を使用すると、AsyncOS で sample.server.domain.com のようなサブドメインの送信先コントロールを指定できるようになります。詳細なサブドメイン アドレスを個別に入力する必要はありません。

接続、メッセージ、受信者については、定義する制限が各 Virtual Gateway アドレスとシステム全体のどちらに対して適用されるのかを設定します。(Virtual Gateway アドレス制限では、IP インターフェイスごとの同時接続数を管理します。システム全体の制限では、Cisco IronPort アプライアンスで許可される接続の合計数を管理します)。

また、定義する制限が指定されたドメインの各 MX レコードとドメイン全体のどちらに対して適用されるのかを設定することもできます。(多くのドメインには、電子メールの受け入れに関して複数の MX レコードがあります)。

(注) 現在のシステム デフォルトは、ドメインあたり 500 接続、接続あたり 50 メッセージです。

これらの値については、表 2-8 を参照してください。

表 2-8　[送信先コントロール(Destination Controls)] テーブルの値

フィールド	説明
同時接続 (Concurrent Connections)	Cisco IronPort アプライアンスによって特定のホストに対して行われる発信接続の最大数。(ドメインには、社内グループウェアのホストを含めることができます)。
接続あたりの最大メッセージ数 (Maximum Messages Per Connection)	新しい接続が開始されるまでに、Cisco IronPort アプライアンスから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
受信者 (Recipients)	特定の期間内に許可される受信者の最大数。[なし(None)] は、当該ドメインに対して、受信者の制限がないことを示します。 Cisco IronPort アプライアンスが受信者の数を数える最小期間(1 ～ 60 分)。期間に「0」を指定すると、この機能がディセーブルになります。 **(注)** 受信者制限を変更すると、すでにキュー内にあるすべてのメッセージのカウンタがリセットされます。アプライアンスは、新しい受信者制限に基づいてメッセージを配信します。
制限の適用 (Apply Limits)	制限がドメイン全体とそのドメインに指定された各メール交換 IP アドレスのどちらに適用されるのかを指定します。(多くのドメインで複数の MX レコードがあります)。 この設定は、接続、メッセージ、受信者の制限に適用されます。 制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。 **(注)** IP アドレスのグループを設定しても、仮想ゲートウェイを設定していない場合は、仮想ゲートウェイごとに適用制限を設定しないでください。この設定は、仮想ゲートウェイを使用するように設定されたシステムのみを対象にしています。仮想ゲートウェイの設定方法については、Virtual Gateway™ テクノロジーの使用(2-59 ページ)を参照してください。

（注）　制限が Virtual Gateway アドレスごとに適用される場合でも、システム全体の制限を仮想ゲートウェイの数で除算した値を Virtual Gateway の制限に設定することによって、システム全体の制限を効果的に実装できます。たとえば、4 つの Virtual Gateway アドレスが設定されていて、ドメイン yahoo.com に対して 100 より多くの同時接続を開かないようにするには、Virtual Gateway の制限を同時接続数 25 に設定します。

（注）　delivernow コマンドをすべてのドメインに対して実行すると、destconfig コマンドで追跡されているすべてのカウンタがリセットされます。

TLS の管理

ドメイン単位で Transport Layer Security（TLS; トランスポート層セキュリティ）を設定することもできます。[必須（Required）] 設定が指定された場合、Cisco IronPort アプライアンスのリスナーからドメインの MTA に対して TLS 接続がネゴシエートされます。ネゴシエーションに失敗すると、電子メールはその接続を介して送信されません。詳細については、配信時の TLS および証明書検証のイネーブル化（1-29 ページ）を参照してください。

TLS 接続が必要なドメインにメッセージを配信する際に TLS ネゴシエーションが失敗した場合、Cisco IronPort アプライアンスがアラートを送信するかどうかを指定できます。アラート メッセージには失敗した TLS ネゴシエーションの宛先ドメイン名が含まれます。Cisco IronPort アプライアンスは、システム アラートのタイプの警告重大度レベル アラートを受信するよう設定されたすべての受信者にアラート メッセージを送信します。GUI の [システム管理（System Administration）] > [アラート（Alerts）] ページ（または CLI の alertconfig コマンド）を使用してアラートの受信者を管理できます。

TLS 接続アラートをイネーブルにするには、[送信先コントロール（Destination Controls）] ページの [グローバル設定を編集（Edit Global Settings）] をクリックまたは destconfig -> setup サブコマンドを使用します。これは、ドメイン単位ではなく、グローバルな設定です。アプライアンスが配信を試行したメッセージの情報については、[モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）] ページまたはメール ログを使用します。

すべての発信 TLS 接続に使用する証明書を指定する必要があります。[送信先コントロール（Destination Controls）] ページの [グローバル設定を編集（Edit Global Settings）] または destconfig -> setup サブコマンドを使用して、証明書を指定します。証明書の取得方法については、証明書の取得（1-22 ページ）を参照してください。

アラートの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「システム管理」の章を参照してください。

Cisco IronPortバウンス検証タギングの管理

送信されるメールにバウンス検証のタギングが行われるかどうかを指定できます。デフォルトに対して指定することも、特定の宛先に対して指定することもできます。Cisco IronPort では、デフォルトに対してバウンス検証をイネーブルにした後で、具体的な除外対象として新しい宛先を作成することを推奨します。詳細については、Cisco IronPort バウンス検証（2-52 ページ）を参照してください。

バウンスの管理

リモート ホストに配信する接続や受信者の数を制御できるだけでなく、そのドメインで使用されるバウンス プロファイルを指定することもできます。指定すると、バウンス プロファイルは `destconfig` コマンドの 5 番めのカラムに表示されます。バウンス プロファイルを指定しない場合は、デフォルトのバウンス プロファイルが使用されます。詳細については、新しいバウンス プロファイルの作成（2-40 ページ）を参照してください。

新しい送信先コントロール エントリの追加

新規の宛先制御エントリを追加するには、次の手順を実行します。

ステップ 1　[送信先の追加（Add Destination）] をクリックします。

ステップ 2　エントリを設定します。

ステップ 3　変更を送信し、保存します。

宛先制御エントリの編集

宛先制御エントリを編集するには、次の手順を実行します。

ステップ 1　[Destination Control] ページの [Domain] カラムでドメイン名をクリックします。

ステップ 2　変更を行います。

ステップ 3　変更を送信し、保存します。

宛先制御エントリの削除

1 つ以上の宛先制御エントリを削除するには、次の手順を実行します。

ステップ 1　左側のカラムのチェックボックスをオンにして、そのエントリ（複数可）を選択します。

ステップ 2　[削除（Delete）] をクリックします。

ステップ 3　削除を確認します。

デフォルトの宛先制御エントリは削除できません。

宛先制御設定のインポートおよびエクスポート

複数のドメインを管理している場合は、すべてのドメインの送信先コントロール エントリを定義する単一の設定ファイルを作成して、アプライアンスにインポートできます。設定ファイルの形式は、Windows INI 設定ファイルと似ています。ドメインのパラメータはセクションにまとめられ、セクション名としてドメイン名が使用されます。たとえば、セクション名 `[example.com]` を使用して、ドメイン example.com のパラメータをグループにします。定義されないすべてのパラメータは、デフォルトの送信先コントロール エントリから継承されます。デフォルトの送信先コントロール エントリのパラメータを定義するには、設定ファイルに `[デフォルト(DEFAULT)]` セクションを含めます。

設定ファイルをインポートすると、アプライアンスの送信先コントロール エントリがすべて上書きされます。ただし、設定ファイルに [デフォルト(DEFAULT)] セクションが含まれていない場合、デフォルト エントリは上書きされません。その他すべての既存の送信先コントロール エントリは削除されます。

設定ファイルでは、ドメインに対して次のパラメータを定義できます。[デフォルト(DEFAULT)] セクションには bounce_profile パラメータを除くすべてのパラメータが必要です。

表 2-9　送信先コントロール設定ファイルのパラメータ

パラメータ名	説明
ip_sort_pref	ドメインに対してインターネット プロトコル バージョンを指定します。 次のいずれかの値を入力します。 • IPv6「Preferred」の場合の PREFER_V6 • IPv6「Required」の場合の REQUIRE_v6 • IPv4「Preferred」の場合の PREFER_V4 • IPv4「Required」の場合の REQUIRE_v4
max_host_concurrency	Cisco IronPort アプライアンスによって特定のホストに対して行われる発信接続の最大数。 ドメインに対してこのパラメータを定義する場合は、limit_type および limit_apply パラメータも定義する必要があります。
max_messages_per_connection	新しい接続が開始されるまでに、Cisco IronPort アプライアンスから特定のホストに対する単一発信接続に対して許可されるメッセージの最大数。
recipient_minutes	Cisco IronPort アプライアンスが受信者の数を数える期間(1 ～ 60 分)。受信者制限を適用しないようにする場合は、未定義のままにします。
recipient_limit	特定の期間内に許可される受信者の最大数。受信者制限を適用しないようにする場合は、未定義のままにします。 ドメインに対してこのパラメータを定義する場合は、recipient_minutes、limit_type、および limit_apply パラメータも定義する必要があります。
limit_type	制限がドメイン全体とそのドメインに指定された各メール交換 IP アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 • 0(または host):ドメインの場合 • 1(または MXIP):メール交換 IP アドレスの場合
limit_apply	制限がシステム全体と各 Virtual Gateway アドレスのどちらに適用されるのかを指定します。 次のいずれかの値を入力します。 • 0(または system):システム全体の場合 • 1(または VG):Virtual Gateway の場合

表 2-9　送信先コントロール設定ファイルのパラメータ（続き）

パラメータ名	説明
bounce_validation	バウンス検証アドレス タギングをオンにするかどうかを指定します。 次のいずれかの値を入力します。 • 0（または off） • 1（または on）
table_tls	ドメインの TLS 設定を指定します。詳細については、配信時の TLS および証明書検証のイネーブル化（1-29 ページ）を参照してください。 次のいずれかの値を入力します。 • 0（または off） • 1（または on）「推奨（Preferred）」の場合 • 2（または required）「必須（Required）」の場合 • 3（または on_verify）「推奨（検証）（Preferred (Verify)）」の場合 • 4（または require_verify）:「必須（検証）（Required (Verify)）」の場合 文字列には、大文字と小文字の区別はありません。
bounce_profile	使用するバウンス プロファイルの名前。[デフォルト（DEFAULT）] 送信先コントロール エントリでは使用できません。
send_tls_req_alert	必須の TLS 接続が失敗した場合にアラートを送信するかどうか。 次のいずれかの値を入力します。 • 0（または off） • 1（または on） これはグローバル設定であり、[デフォルト（DEFAULT）] 送信先コントロール エントリでのみ使用できます。
certificate	発信 TLS 接続で使用される証明書。これはグローバル設定であり、[デフォルト（DEFAULT）] 送信先コントロール エントリでのみ使用できます。 **（注）** 証明書を指定しない場合は、デモの証明書が割り当てられますが、デモの証明書を使用することはセキュアではないため、通常の使用には推奨できません。

ドメイン example1.com、example2.com、およびデフォルトの送信先コントロール エントリの例を次に示します。

```
[DEFAULT]

ip_sort_pref = PREFER_V6
```

```
max_host_concurrency = 500

max_messages_per_connection = 50

recipient_minutes = 60

recipient_limit = 300

limit_type = host

limit_apply = VG

table_tls = off

bounce_validation = 0

send_tls_req_alert = 0

certificate = example.com


[example1.com]

ip_sort_pref = PREFER_V6

recipient_minutes = 60

recipient_limit = 100

table_tls = require_verify

limit_apply = VG

bounce_profile = tls_failed

limit_type = host


[example2.com]

table_tls = on

bounce_profile = tls_failed
```

上記の例では、example1.com および example2.com について次の送信先コントロール エントリが生成されます。

```
example1.com

    IP Address Preference: IPv6 Preferred

    Maximum messages per connection: 50
```

```
    Rate Limiting:

        500 concurrent connections

        100 recipients per 60 minutes

        Limits applied to entire domain, across all virtual gateways

    TLS: Required (Verify)

    Bounce Profile: tls_failed


example2.com

    IP Address Preference: IPv6 Preferred

    Maximum messages per connection: Default

    Rate Limiting: Default

    TLS: Preferred

    Bounce Profile: tls_failed
```

[送信先コントロール(Destination Controls)] ページの [テーブルのインポート(Import Table)] ボタン、または `destconfig -> import` コマンドを使用して、設定ファイルをインポートします。[送信先コントロール(Destination Controls)] ページの [テーブルのエクスポート(Export Table)] ボタン、または `destconfig -> export` コマンドを使用して、送信先コントロール エントリを INI ファイルにエクスポートすることもできます。エクスポートされた INI ファイルには `[デフォルト(Default)]` ドメイン管理エントリも含まれています。

宛先制御と CLI

CLI で `destconfig` コマンドを使用して、送信先コントロール エントリを設定できます。このコマンドについては、*Cisco IronPort AsyncOS CLI Reference Guide* で説明します。

Cisco IronPort バウンス検証

「バウンス」メッセージは、受信側の MTA によって送信される新しいメッセージで、元の電子メールのエンベロープ送信者が新しいエンベロープ受信者として使用されます。このバウンスは、元のメッセージが配信不可能なときに(通常は、受信者アドレスが存在しないため)、通常は空のエンベロープ送信者(MAIL FROM: < >)でエンベロープ受信者に送り返されます。

スパム送信者は、誤った宛先を指定したバウンス攻撃による電子メール インフラストラクチャへの攻撃をますます増やしています。このような攻撃は、未知の正当なメール サーバによって送信される、膨大なバウンス メッセージによって行われます。基本的に、スパム送信者が使用するプロセスでは、オープン リレーおよび「ゾンビ」ネットワークを経由してさまざまなドメインで無効な可能性のあるアドレス(エンベロープ受信者)に電子メールを送信します。このようなメッセージでは、エンベロープ送信者が偽装されるため、スパムは正当なドメインから送信されたように見えます(これは「Joe job(ジョー ジョブ)」とも呼ばれます)。

次に、無効なエンベロープ受信者による着信電子メールごとに、受信側のメール サーバによって新しい電子メール（バウンス メッセージ）が生成され、一緒に無実なドメイン（エンベロープ送信者アドレスが偽装されたドメイン）の電子メール送信者宛に送信されます。その結果、このターゲット ドメインは、「誤った宛先が指定された」膨大なバウンスを受信します。このバウンス メッセージは、数百万にもおよぶことがあります。このような分散 DoS 攻撃により、電子メール インフラストラクチャがダウンして、ターゲットが正当な電子メールの送受信を行えなくなります。

誤った宛先を指定したバウンス攻撃に対処するため、AsyncOS には Cisco IronPort [バウンス検証（Bounce Verification）] が用意されています。イネーブルにすると、Cisco IronPort バウンス検証によって、その Cisco IronPort アプライアンスから送信されたメッセージのエンベロープ送信者アドレスにタグが付けられます。次に、Cisco IronPort アプライアンスで受信したバウンス メッセージで、エンベロープ受信者にこのタグが付いているかどうかがチェックされます。正当なバウンス（このタグが付いている）であれば、タグが外されて配信されます。タグが付いていないバウンス メッセージは、別の処理を行えます。

Cisco IronPort バウンス検証を使用して、発信メールに基づいて着信バウンス メッセージを管理できます。Cisco IronPort アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御については、バウンスした電子メールの処理（2-35 ページ）を参照してください。

概要：タギングと Cisco IronPort バウンス検証

バウンス検証をイネーブルにして電子メールを送信すると、Cisco IronPort アプライアンスにより、メッセージのエンベロープ送信者アドレスが書き換えられます。たとえば、MAIL FROM: `joe@example.com` が MAIL FROM: `prvs=joe=123ABCDEFG@example.com` になるとします。`123...` この例の文字列は、「バウンス検証タグ」であり、Cisco IronPort アプライアンスによって送信されるときに、エンベロープ送信者に追加されます。このタグは、バウンス検証設定で定義されたキーを使用して生成されます（キーの指定については、Cisco IronPort バウンス検証アドレスのタグ用キー（2-54 ページ）を参照してください）。このメッセージがバウンスすると、バウンス内のエンベロープ受信者アドレスに通常はこのバウンス検証タグが含まれます。

デフォルトではシステム全体でバウンス検証タギングをイネーブルまたはディセーブルにできます。特定のドメインに対してバウンス検証タギングをイネーブルまたはディセーブルにすることもできます。ほとんどの場合、デフォルトでイネーブルにしておき、除外する具体的なドメインを [送信先コントロール（Destination Controls）] テーブルに列挙します（[送信先コントロール（Destination Controls）] の使用（2-45 ページ）を参照）。

メッセージにタグ付きのアドレスがすでに含まれている場合は、別のタグが追加されません（Cisco IronPort アプライアンスがバウンス メッセージを DMZ 内の Cisco IronPort アプライアンスに配信する場合）。

着信バウンス メッセージの処理

有効なタグが含まれているバウンスは配信されます。タグが削除され、エンベロープ受信者が復元されます。これは、電子メール パイプラインのドメイン マップ処理の直後に発生します。Cisco IronPort アプライアンスでタグの付いていないバウンスやタグが無効に付いたバウンスの処理方法として、拒否するのか、それともカスタム ヘッダーを追加するのかを定義できます。詳細については、Cisco IronPort バウンス検証設定の設定（2-56 ページ）を参照してください。

バウンス検証タグが存在しない場合、タグの生成に使用されたキーが変更された場合、またはメッセージが 7 日より古い場合、そのメッセージは Cisco IronPort バウンス検証で定義された設定に従って扱われます。

たとえば、次のメール ログには、Cisco IronPort アプライアンスで拒否されたバウンス メッセージが示されています。

```
Fri Jul 21 16:02:19 2006 Info: Start MID 26603 ICID 125192

Fri Jul 21 16:02:19 2006 Info: MID 26603 ICID 125192 From: <>

Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address
<bob@example.com> rejected by bounce verification.

Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender

Fri Jul 21 16:03:51 2006 Info: Message finished MID 26603 aborted
```

（注）　非バウンス メールを独自の社内メール サーバ（Exchange など）に配信する場合は、その社内ドメインに対して Cisco IronPort バウンス検証タギングをディセーブルにしてください。

AsyncOS では、バウンスがヌルの MAIL FROM アドレス（<>）が設定されたメールであると見なされます。タグ付きのエンベロープ受信者が含まれる可能性のある非バウンス メッセージの場合は、より緩やかなポリシーが適用されます。そのような場合、7 日でのキー失効は無視され、古いキーとの一致も調べられます。

Cisco IronPort バウンス検証アドレスのタグ用キー

タギング キーは、バウンス検証タグを生成するときに Cisco IronPort アプライアンスで使用されるテキスト文字列です。ドメインから発信されるすべてのメールには一貫してタグが付けられるため、すべての Cisco IronPort アプライアンスで同じキーを使用することが理想的です。そのようにして、ある Cisco IronPort アプライアンスで発信メッセージのエンベロープ送信者にタグが付けられる場合、別の Cisco IronPort アプライアンスからバウンスを受信しても、その着信バウンスが検証および配信されます。

タグには 7 日間の猶予期間があります。たとえば、7 日間のうちにタギング キーを複数回変更できます。その場合、Cisco IronPort アプライアンスは 7 日よりも新しいこれまでのすべてのキーを使用して、タグの付いたメッセージを検証しようとします。

Cisco IronPort バウンス検証と HAT

AsyncOS には、Cisco IronPort バウンス検証に関連して、タグの付いていないバウンスを有効とするかどうかを検討する HAT 設定もあります。デフォルト設定は「いいえ」であり、タグの付いていないバウンスは無効であると見なされます。さらに、[メールポリシー（Mail Policies）] > [バウンス検証（Bounce Verification）] ページで選択されたアクションに従って、メッセージが拒否されるか、またはカスタム ヘッダーが付加されます。「はい」を選択した場合、タグの付いていないバウンスは有効であると見なされ、受け入れられます。これは、次のようなシナリオで使用できます。

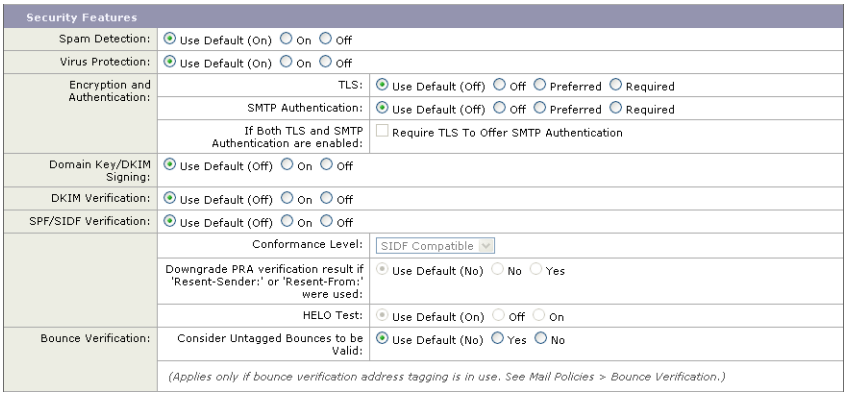
電子メールをメーリング リストに送信することを検討しているユーザがいるとします。しかし、メーリング リストでは、エンベロープ送信者の固定セットからのメッセージのみを受け入れています。そのような場合、ユーザからのタグ付きメッセージは受け入れられません（タグは定期的に変更されるため）。

そのようなユーザを救済するには、次の手順を実行します。

ステップ 1　ユーザがメールを送信しようとするドメインを [送信先コントロール（Destination Controls）] テーブルに追加し、そのドメインに対するタギングをディセーブルにします。この時点で、ユーザは問題なくメールを送信できます。

ステップ 2　ただし、そのドメインからのバウンスにはタグが付いていないため、バウンス受信を適切にサポートするには、そのドメインの送信者グループを作成し、[承認（Accept）] メール フロー ポリシーの [タグなしバウンスを有効と見なす（Consider Untagged Bounces to be Valid）] パラメータをイネーブルにします。

図 2-12　[タグなしバウンスを有効と見なす（Consider Untagged Bounces to be Valid）] HAT パラメータ



Cisco IronPort バウンス検証の使用

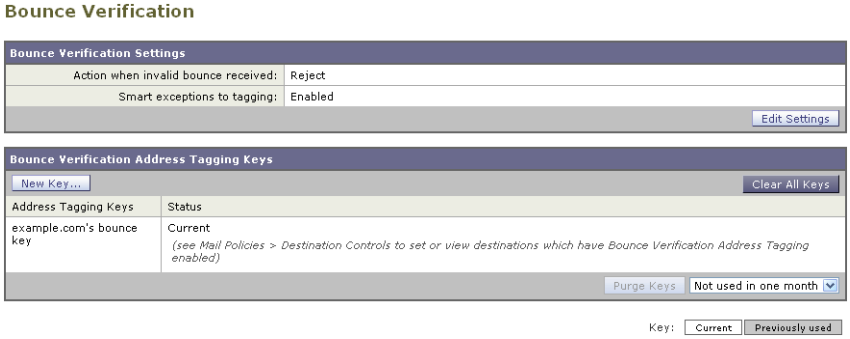
Cisco IronPort バウンス検証を設定するには、次の手順を実行します。

ステップ 1　タギング キーを入力します（[バウンス検証アドレスのタグ付けキー（Bounce Verification Address Tagging Keys）] の設定（2-56 ページ）を参照）。

ステップ 2　バウンス検証設定を編集します（Cisco IronPort バウンス検証設定の設定（2-56 ページ）を参照）。

ステップ 3　[Destination Controls] を使用して、バウンス検証をイネーブルにします（[送信先コントロール（Destination Controls）] の使用（2-45 ページ）を参照）。

図 2-13　IronPort の [バウンス検証（Bounce Verification）] ページ



[バウンス検証アドレスのタグ付けキー(Bounce Verification Address Tagging Keys)] の設定

[バウンス検証アドレスのタグ付けキー(Bounce Verification Address Tagging Keys)] のリストには、現在のキー、および過去に使用してまだ削除されていないキーが示されます。新規のキーを追加するには、次の手順を実行します。

ステップ 1　[メールポリシー(Mail Policies)] > [バウンス検証(Bounce Verification)] ページで、[キーを追加(New Key)] をクリックします。

ステップ 2　テキスト文字列を入力し、[送信(Submit)] をクリックします。

ステップ 3　変更を保存します。

キーの削除

古いアドレス タギング キーを削除するには、プルダウン メニューから削除するルールを選択し、[除去(Purge)] をクリックします。

Cisco IronPort バウンス検証設定の設定

バウンス検証設定では、無効なバウンスを受信したときに実行するアクションを指定します。バウンス検証設定を設定するには、次の手順を実行します。

ステップ 1　[設定の編集(Edit Settings)] をクリックします。[Edit Bounce Verification Settings] ページが表示されます。

ステップ 2　無効なバウンスを拒否するのか、カスタム ヘッダーをメッセージに追加するのかを選択します。ヘッダーを追加する場合は、ヘッダーの名前と値を入力します。

ステップ 3　必要に応じて、スマート例外機能をイネーブルにします。この設定を使用すると、(着信メールと発信メールの両方で 1 つのリスナーを使用している場合であっても)着信メール メッセージ、および社内メール サーバで生成されるバウンス メッセージをバウンス検証処理から自動的に除外できるようにします。

ステップ 4　変更を送信し、保存します。

Cisco IronPort バウンス検証と CLI

CLI で `bvconfig` コマンドおよび `destconfig` コマンドを使用して、バウンス検証を設定できます。これらのコマンドについては、『*Cisco IronPort AsyncOS CLI Reference Guide*』で説明します。

Cisco IronPort バウンス検証とクラスタ設定

バウンス検証は、両方の Cisco IronPort アプライアンスで同じ「バウンス キー」を使用している限り、クラスタ設定で動作します。同じキーを使用する場合は、どちらのシステムでも正当なバウンスを受け入れられる必要があります。変更後のヘッダー タグ/キーは、各 Cisco IronPort アプライアンスに固有ではありません。

電子メール配信パラメータの設定

deliveryconfig コマンドは、Cisco IronPort アプライアンスから電子メールを配信するときに使用されるパラメータを設定します。

Cisco IronPort アプライアンスは、SMTP と QMQP という複数のメール プロトコルを使用してメールを受信します。ただし、すべての発信電子メールは、SMTP を使用して配信されます。このため、deliveryconfig コマンドではプロトコルの指定が不要です。

（注）　このセクションに記載されている機能またはコマンドには、ルーティングの優先順位に影響を与えるものや、影響を受けるものが含まれています。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録 B、「ネットワークと IP アドレスの割り当て」を参照してください。

デフォルトの配信 IP インターフェイス

デフォルトで、電子メール配信には IP インターフェイスまたは IP インターフェイス グループが使用されます。現在設定されているどの IP インターフェイスまたは IP インターフェイス グループでも設定できます。特定のインターフェイスが指定されない場合は、受信者ホストと通信するときに SMTP HELO コマンドでデフォルトの配信インターフェイスと関連付けられたホスト名が使用されます。IP インターフェイスを設定するには、interfaceconfig コマンドを使用します。

電子メール配信インターフェイスの自動選択を使用するときのルールは次のとおりです。

- リモートの電子メール サーバが設定済みインターフェイスのいずれかと同じサブネット上にある場合、トラフィックは一致するインターフェイス上を流れます。
- auto-select に設定した場合、routeconfig を使用して設定したスタティック ルートが有効になります。
- そうでない場合、デフォルト ゲートウェイと同じサブネット上にあるインターフェイスが使用されます。すべての IP アドレスで宛先に対するルートが同等の場合、使用可能なうち最も効率的なインターフェイスが使用されます。

[配信可能性あり（Possible Delivery）] 機能

[配信可能性あり（Possible Delivery）] 機能がイネーブルになると、AsyncOS では、メッセージ本文が配信されてから受信者ホストがメッセージの受信を確認するまでの間にタイムアウトするすべてのメッセージを「配信可能性あり」であると見なして扱います。この機能を使用すると、受信者ホストで連続するエラーにより受信の確認が妨げられる場合に、メッセージのコピーを複数受信しなくて済みます。AsyncOS では、この受信を配信可能性ありとしてメール ログに記録し、そのメッセージを完了したものとして見なします。[配信可能性あり（Possible Delivery）] 機能は、イネーブルのままにしておくことを推奨します。

デフォルトの最大同時接続数（Default Maximum Concurrency）

アプライアンスが発信メッセージの配信で確立するデフォルトの最大同時接続数も指定できます。（システム全体のデフォルトはドメインごとに 10,000 接続です）（この制限は、リスナーあたりの最大同時発信メッセージ配信数（リスナーあたりのデフォルトは、プライベート リスナーで 600 接続、パブリック リスナーで 1000 接続です）。デフォルトよりも小さい値を設定すると、Cisco IronPort ゲートウェイが弱いネットワークを支配しないようにすることができます。たとえば、特定のファイアウォールが大量の接続をサポートしない場合、そのような環境では Cisco IronPort で Denial of Service（DoS; サービス拒否）警告が引き起こされることがあります。

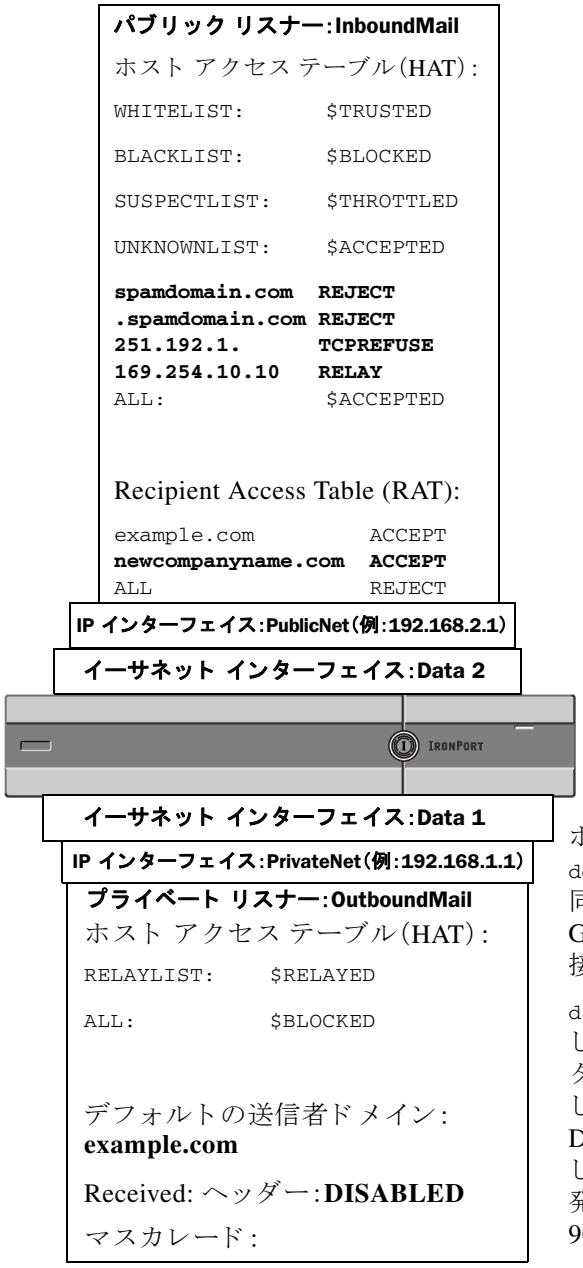
deliveryconfig の例

次の例では、deliveryconfig コマンドを使用し、[配信可能性あり（Possible Delivery）] をイネーブルにして、デフォルトのインターフェイスを [自動（Auto）] に設定します。システム全体の最大発信メッセージ配信は、9000 接続です。

```
mail3.example.com> deliveryconfig


Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[]> setup


Choose the default interface to deliver mail.

1. Auto

2. PublicNet2 (192.168.3.1/24: mail4.example.com)

3. Management (192.168.42.42/24: mail3.example.com)

4. PrivateNet (192.168.1.1/24: mail3.example.com)

5. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1


Enable "Possible Delivery" (recommended)?  [Y]> y


Please enter the default system wide maximum outbound message delivery

concurrency

[10000]> 9000


mail3.example.com>
```

これで電子メール ゲートウェイの設定は次のようになります。

図 2-14　　宛先および配信パラメータの設定



ホスト `small-isp.net` の `destconfig` エントリを使用して、同時接続数 100、または Virtual Gateway アドレスを使用して同時接続数 10 に制限されます。

`deliveryconfig` コマンドを使用して、電子メール配信用インターフェイスの自動選択を使用し、[配信可能性あり(Possible Delivery)] 機能をイネーブルにしました。システム全体の最大発信メッセージ配信は、合計で 9000 同時接続です。

Virtual Gateway™ テクノロジーの使用

この項では、Cisco IronPort Virtual Gateway™ テクノロジーとその利点、Virtual Gateway アドレスの設定方法、および Virtual Gateway アドレスのモニタおよび管理方法について説明します。

Cisco IronPort Virtual Gateway テクノロジーでは、ホストするすべてのドメインに対して異なる IP アドレス、ホスト名、およびドメインを使用してエンタープライズ メール ゲートウェイを設定し、同じ物理アプライアンス内にホストしている場合でも、それらのドメインに対して別々に企業の電子メール ポリシー強制およびスパム対策方針を作成できます。

（注） 利用できる Virtual Gateway アドレスの数は、使用する Cisco IronPort アプライアンスのモデルによって異なります。一部のアプライアンス モデルでは、ライセンス キーを使用して多くの Virtual Gateway アドレスをサポートするようにアップグレードできます。使用するアプライアンスでの Virtual Gateway アドレスの数をアップグレードする詳細については、Cisco IronPort 販売代理店にお問い合わせください。

概要

企業がカスタマーと電子メールで信頼性の高いコミュニケーションを実現できるように、シスコは独自の Virtual Gateway テクノロジーを開発しました。Virtual Gateway テクノロジーを使用すると、Cisco IronPort アプライアンスを複数の Virtual Gateway アドレスに分割し、そのアドレスを使用して電子メールを送受信できます。各 Virtual Gateway アドレスには、別々の IP アドレス、ホスト名、ドメイン、および電子メール キューが与えられます。

別々の IP アドレスとホスト名を各 Virtual Gateway アドレスに割り当てることにより、ゲートウェイ経由で配信される電子メールが受信者ホストで正しく識別され、重要な電子メールがスパムと見なされてブロックされるのを防ぐことができます。Cisco IronPort アプライアンスには、Virtual Gateway アドレスごとに SMTP HELO コマンドで正しいホスト名を付与できる高度な機能があります。そのため、受信側の Internet Service Provider（ISP; インターネット サービス プロバイダー）が逆 DNS ルックアップを実行すると、Cisco IronPort アプライアンスでは、その Virtual Gateway アドレス経由で送信された電子メールの IP アドレスと一致させることができます。多くの ISP では迷惑電子メールを検出するために逆 DNS ルックアップを使用しているため、この機能は非常に有用です。逆 DNS ルックアップでの IP アドレスが送信側ホストの IP アドレスと一致しない場合、ISP では、送信者が不正であると見なして、電子メールを破棄する頻度が高くなります。Cisco IronPort Virtual Gateway テクノロジーでは、逆 DNS ルックアップが送信側の IP アドレスと常に一致するため、メッセージが意図せずブロックされてしまうのを防げます。

各 Virtual Gateway アドレスでのメッセージも、別々のメッセージ キューに割り当てられます。受信者ホストで特定の Virtual Gateway アドレスからの電子メールをブロックしている場合、そのホスト宛のメッセージはキューに残され、最終的にはタイムアウトします。しかしブロックされていない別の Virtual Gateway キュー内にある同じドメイン宛のメッセージは、正常に配信されます。これらのキューは、配信では別のものとして扱われますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。

Virtual Gateway アドレスの設定

Cisco IronPort Virtual Gateway アドレスを設定する前に、電子メールの送信元として使用される IP アドレスのセットを割り当てる必要があります。（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ネットワークと IP アドレスの割り当て」を参照してください。）また、IP アドレスが有効なホスト名に解決されるように DNS サーバが正しく設定されている必要があります。DNS サーバが正しく設定されていれば、受信者ホストで逆 DNS ルックアップが実行されると、有効な IP/ホスト名のペアに解決されます。

仮想ゲートウェイで使用する新しい IP インターフェイスの作成

IP アドレスとホスト名が確立したら、Virtual Gateway アドレスを設定するために、まずはその IP/ホスト名のペアで新しい IP インターフェイスを作成します。それには、GUI の [ネットワーク(Network)] > [IP インターフェイス(IP Interfaces)] ページ、または CLI の `interfaceconfig` コマンドを使用します。

IP インターフェイスを設定したら、複数の IP インターフェイスをインターフェイス グループへと結合できます。これらのグループは、電子メールの配信時に「ラウンド ロビン」方式で順番に使用される Virtual Gateway アドレスに割り当てることができます。

必要な IP インターフェイスを作成したら、2 つの方法で Virtual Gateway アドレスを設定し、各 IP インターフェイスまたはインターフェイス グループから送信される電子メール キャンペーンを定義します。

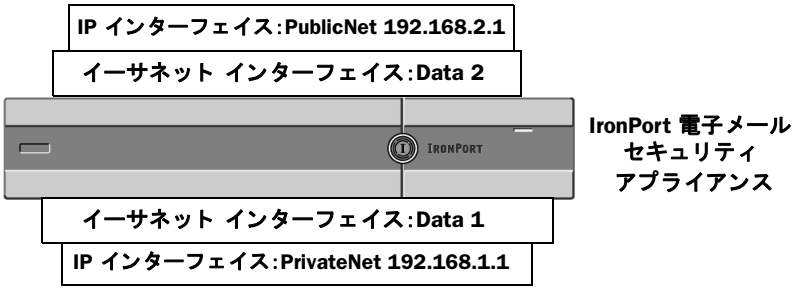
ステップ 1　`altsrchost` コマンドを使用すると、特定の送信者 IP アドレスまたはエンベロープ送信者アドレスの情報からホストの IP インターフェイス(Virtual Gateway アドレス)またはインターフェイス グループに電子メールをマッピングして配信できます。

ステップ 2　メッセージ フィルタを使用して、特定ホストの IP インターフェイス(Virtual Gateway アドレス)またはインターフェイス グループを使用してフラグ付きのメッセージを配信するためのフィルタを設定できます。送信元ホスト(Virtual Gateway アドレス)変更アクション(6-61 ページ)を参照してください。(この方法は前述の方法よりも柔軟性があり、強力です)。

IP インターフェイスを作成する詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の付録「アプライアンスへのアクセス」を参照してください。

ここまで、図 2-15 に示すように定義された次のインターフェイスを用いて、電子メール ゲートウェイの設定を使用してきました。

図 2-15　パブリック インターフェイスとプライベート インターフェイスの例



次の例では、[IP インターフェイス(IP Interfaces)] ページで管理インターフェイスの他に 2 つのインターフェイス(PrivateNet および PublicNet)が設定されていることを確認できます。

図 2-16　[IP インターフェイス(IP Interfaces)] ページ

IP Interfaces

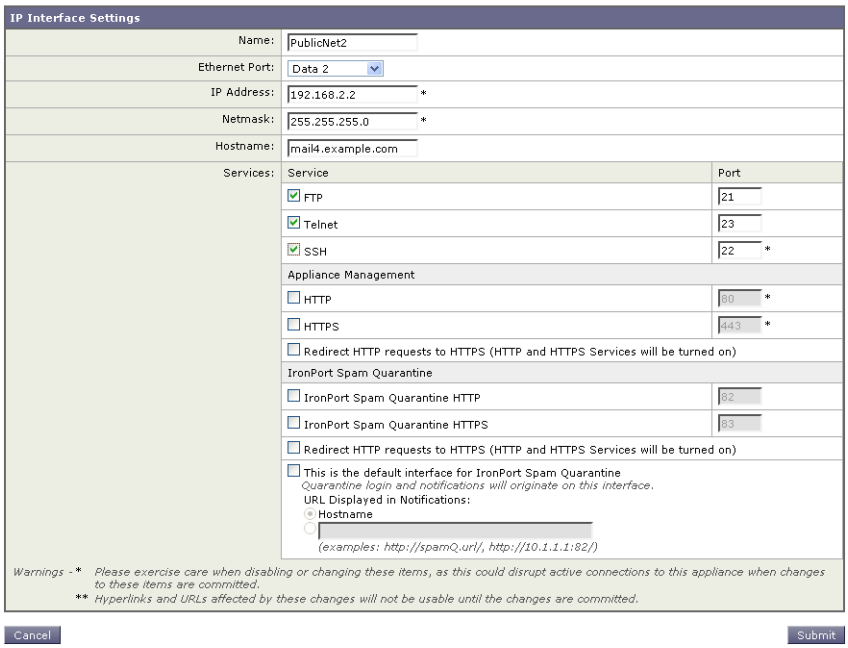
Network Interfaces and IP Addresses

Add IP Interface...

Name	IP Address	Hostname	Delete
Management	192.168.42.42/24	mail3.example.com	
PrivateNet	192.168.1.1/24	mail3.example.com	
PublicNet	192.168.2.1/24	mail3.example.com	

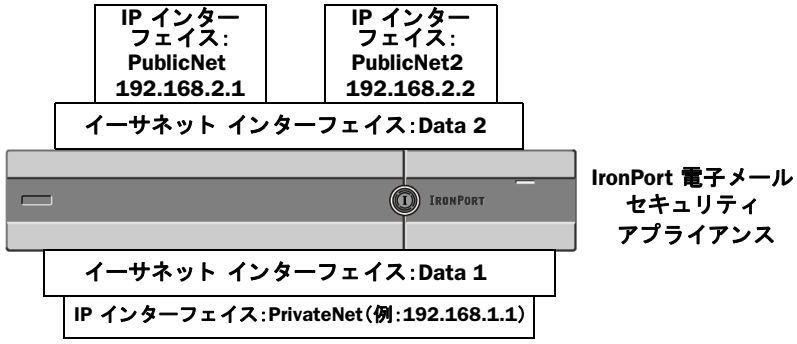
次に、[IP インターフェイスの追加(Add IP Interface)] ページを使用して、Data2 イーサネット インターフェイス上に PublicNet2 という名前の新しいインターフェイスを作成します。IP アドレス 192.168.2.2 が使用され、ホスト名 `mail4.example.com` が指定されています。さらに、FTP(ポート 21)、Telnet(ポート 23)、および SSH(ポート 22)がイネーブルになります。

図 2-17　[IP インターフェイスの追加(Add IP Interface)] ページ



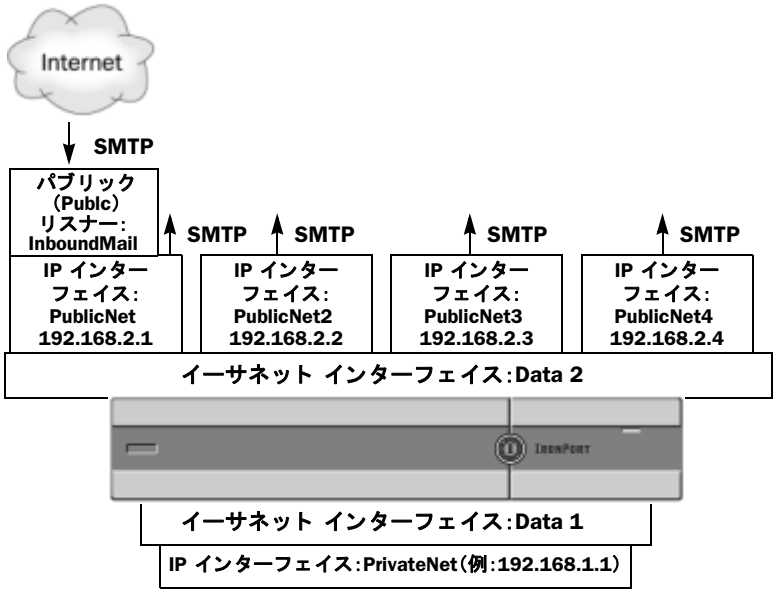
これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 2-18　別のパブリック インターフェイスの追加



Virtual Gateway アドレスを使用すると、図 2-19 に示すようなコンフィギュレーションも可能です。

図 2-19　　1 つのイーサネット インターフェイス上にある 4 つの Virtual Gateway アドレス



4 つの IP インターフェイスはそれぞれメール配信に使用できますが、インターネットからのメールを受け入れるように設定されるのはパブリック リスナー 1 つだけです。

メッセージから配信用 IP インターフェイスへのマッピング

`altsrchost` コマンドを使用すると、各 Cisco IronPort アプライアンスを、電子メールの配信元となる複数の IP インターフェイス（Virtual Gateway アドレス）にセグメント化することが最も単純で単刀直入な方法です。ただし、メッセージを特定の Virtual Gateway にマッピングする際にさらに強力で柔軟な方法が必要であれば、メッセージ フィルタの使用を検討してください。詳細については、第 6 章「メッセージ フィルタを使用した電子メール ポリシーの適用」を参照してください。

`altsrchost` コマンドを使用すると、次のいずれかに基づいて、電子メールの配信中に使用する IP インターフェイスまたはインターフェイス グループを管理できます。

- 送信者の IP アドレス
- エンベロープ送信者アドレス

電子メールの配信元にする IP インターフェイスまたはインターフェイス グループを指定するには、送信者の IP アドレスまたはエンベロープ送信者アドレスを IP インターフェイスまたはインターフェイス グループ（インターフェイス名またはグループ名で指定）とペアにするマッピング キーを作成します。

Cisco IronPort AsyncOS では、IP アドレスとエンベロープ送信者アドレスの両方をマッピング キーと比較します。IP アドレスまたはエンベロープ送信者アドレスがいずれかのキーと一致する場合、対応する IP インターフェイスが発信配信に使用されます。一致しない場合は、デフォルトの発信インターフェイスが使用されます。

一致する可能性のあるキーを優先順に示します。

送信者の IP アドレス	送信者の IP アドレスは完全一致する必要があります。 例：`192.168.1.5`
完全形式のエンベロープ送信者	エンベロープ送信者は、アドレス全体が完全一致する必要があります。 例：`username@example.com`

ユーザ名	エンベロープ送信者アドレスの @ 記号までの部分に対してユーザ名構文と一致させます。@ 記号を含める必要があります。例:username@
ドメイン	エンベロープ送信者アドレスの @ 記号で始まる部分に対してドメイン名構文と一致させます。@ 記号を含める必要があります。例:@example.com

（注） リスナーは altsrchost テーブルで情報をチェックし、マスカレード情報をチェックした*後*からメッセージ フィルタがチェックされる*前*までに、電子メールを特定のインターフェイスに転送します。

altsrchost コマンド内のサブコマンドを使用して、CLI で仮想ゲートウェイにマッピングを作成します。

構文	説明
new	新しいマッピングを手動で作成します。
print	マッピングの現在のリストを表示します。
delete	テーブルからマッピングを 1 つ削除します。

altsrchost ファイルのインポート

HAT、RAT、smtproutes、マスカレード テーブル、エイリアス テーブルと同様に、altsrchost エントリはファイルをエクスポートおよびインポートして変更できます。次の手順に従ってください。

ステップ 1　altsrchost コマンドの export サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。

ステップ 2　CLI の外部で、ファイルを取得します。（詳細については、付録 B「アプライアンスへのアクセス」を参照してください）。

ステップ 3　テキスト エディタを使用して、ファイルに新しいエントリを作成します。ルールが altsrchost テーブルに出現する順序が重要です。

ステップ 4　ファイルを保存してインターフェイスの「altsrchost」ディレクトリに配置し、インポートできるようにします。（詳細については、付録 B「アプライアンスへのアクセス」を参照してください）。

ステップ 5　altsrchost の import サブコマンドを使用して、編集したファイルをインポートします。

altsrchost の制限

最大 1,000 個の altsrchost エントリを追加できます。

altsrchost コマンド用に有効なマッピングが記載されたテキスト ファイルの例

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface
```

```
joe@ PublicInterface

192.168.1.5, DemoInterface

steve@example.com PublicNet
```

import および export サブコマンドは、1 行単位で実行され、送信者 IP アドレスまたはエンベロープ送信者アドレスの行をインターフェイス名にマッピングします。スペース以外の文字からなる 1 番めのブロックがキー、スペース以外の文字からなる 2 番めのブロックがインターフェイス名となり、カンマ(,)またはスペース( )で区切ります。コメント行はナンバー記号(#)で始まり、無視されます。

CLI を使用した altsrchost マッピングの追加

次の例では、altsrchost テーブルが出力されて、既存のマッピングがないことが示されます。その後、2 つのエントリが作成されます。

- グループウェア サーバ ホスト @exchange.example.com からのメールは、PublicNet インターフェイスにマッピングされます。
- 送信者 IP アドレス 192.168.35.35(たとえば、マーケティング キャンペーン メッセージング システム)からのメールは、PublicNet2 インターフェイスにマッピングされます。

最後に、確認のために altsrchost マッピングが出力されて、変更が確定されます。

```
mail3.example.com> altsrchost



There are currently no mappings configured.



Choose the operation you want to perform:

- NEW - Create a new mapping.

- IMPORT - Load new mappings from a file.

[]> new



Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.

[]> @exchange.example.com



Which interface do you want to send messages for @exchange.example.com from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)
```

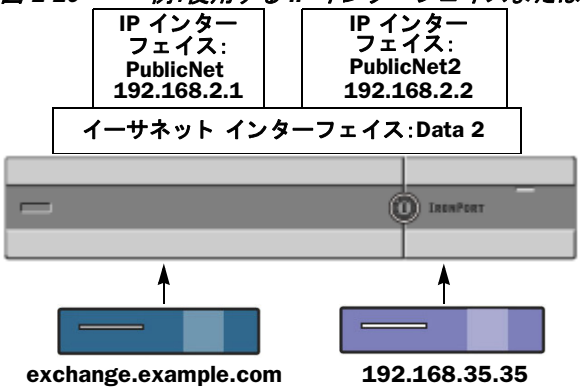
```
2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 4


Mapping for @exchange.example.com on interface PublicNet created.


Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]> new


Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping. Partial addresses such as "@example.com" or "user@" are
allowed.

[]> 192.168.35.35


Which interface do you want to send messages for 192.168.35.35 from?

1. PublicNet2 (192.168.2.2/24: mail4.example.com)

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail4.example.com)

[1]> 1
```

```
Mapping for 192.168.35.35 on interface PublicNet2 created.


Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print


1. 192.168.35.35 -> PublicNet2
2. @exchange.example.com -> PublicNet


Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>


mail3.example.com> commit
```

```
Please enter some comments describing your changes:

[]> Added 2 altsrchost mappings

Changes committed: Thu Mar 27 14:57:56 2003
```

この例におけるコンフィギュレーションの変更を図 2-20 に示します。

図 2-20　例:使用する IP インターフェイスまたはインターフェイス グループの選択



これらのマッピングを作成するように altsrchost テーブルが変更されました。@exchange.example.com からのメッセージはインターフェイス PublicNet を使用し、192.168.35.35 からのメッセージはインターフェイス PublicNet2 を使用します。

Virtual Gateway アドレスのモニタリング

Virtual Gateway アドレスごとに独自の配信用電子メール キューがありますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。Virtual Gateway キューごとに受信者ホストのステータスをモニタするには、hoststatus および hostrate コマンドを使用します。『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「使用可能なモニタリング コンポーネントの読み取り」を参照してください。

hoststatus コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。

Virtual Gateway テクノロジーを使用している場合は、各 Virtual Gateway アドレスに関する情報も表示されます。このコマンドは、返されるホスト情報のドメインを入力する必要があります。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した resetcounters コマンドからの累積です。

返される統計情報は、カウンタとゲージの 2 つのカテゴリにグループ化されます。さらに、返される他のデータには、最後のアクティビティ、MX レコード、最後の 5XX エラーがあります。

Virtual Gateway アドレスごとの配信接続の管理

一部のシステム パラメータには、システム レベルと Virtual Gateway アドレス レベルで設定が必要です。

たとえば、一部の受信者 ISP では、各クライアント ホストに許可されている接続数を制限しています。そのため、特に電子メールが複数の Virtual Gateway アドレスで配信されているときに、ISP との関係を管理することが必要です。

destconfig コマンド、および Virtual Gateway アドレスに対する影響については、電子メール配信の管理（2-43 ページ）を参照してください。

Virtual Gateway アドレスの「グループ」を作成すると、グループが 254 個の IP アドレスで構成されている場合であっても、Virtual Gateway のグッド ネイバー テーブル設定がグループに適用されます。

たとえば、254 個の発信 IP アドレスのグループを作成して、「ラウンドロビン」方式で順番に使用するようにセットアップされているとします。また、`small-isp.com` のグッド ネイバー テーブルで、同時接続数がシステムの場合は 100、Virtual Gateway アドレスの場合は 10 であるとします。このコンフィギュレーションでは、そのグループ内の 254 個の IP アドレスすべてに対して、合計で 10 よりも多くの接続が開くことは*ありません*。グループは、単一の Virtual Gateway アドレスとして扱われます。

[グローバル配信停止（Global Unsubscribe）] 機能の使用

特定の受信者、受信者ドメイン、または IP アドレスが Cisco IronPort アプライアンスからメッセージを受信しないようにするには、Cisco IronPort AsyncOS の [グローバル配信停止（Global Unsubscribe）] 機能を使用します。`unsubscribe` コマンドを使用すると、[グローバル配信停止（Global Unsubscribe）] リストにアドレスを追加/削除したり、この機能をイネーブル/ディセーブルにすることができます。「グローバルに配信停止された」ユーザ、ドメイン、電子メール アドレス、および IP アドレスのリストで、すべての受信者アドレスがチェックされます。受信者がリスト内のアドレスと一致する場合、受信者はドロップされるかハード バウンスされ、Global Unsubscribe（GUS; グローバル配信停止）カウンタが増分されます。（ログ ファイルには、一致する受信者がドロップされたのかハード バウンスされたのかが記録されます）。GUS のチェックは、電子メールを受信者に送信する直前に行われるため、システムで送信されるすべてのメッセージが検査されます。

（注）　[グローバル配信停止（Global Unsubscribe）] 機能は、メーリング リストからの名前の削除やメーリング リストの全般的な保守に代わるものではありません。この機能は、不適切なエンティティに電子メールが配信されないようにするフェールセーフ メカニズムとして動作することを目的としています。

[グローバル配信停止（Global Unsubscribe）] 機能は、プライベート リスナーおよびパブリック リスナーに適用されます。

[グローバル配信停止（Global Unsubscribe）] に含めることのできる最大アドレス数は 10,000 件です。この制限を増やすには、Cisco IronPort 販売代理店にお問い合わせください。[グローバル配信停止（Global Unsubscribe）] に追加されたアドレスは、次の 4 つのうちいずれかの形式をとります。

表 2-10　グローバル配信停止の構文

username@example.com	完全形式の電子メール アドレス この構文は、特定ドメインの特定受信者をブロックするために使用されます。
username@	ユーザ名 ユーザ名構文は、すべてのドメインで特定ユーザ名を持つすべての受信者をブロックします。構文は、ユーザ名の後にアットマーク（@）を付けます。
@example.com	ドメイン ドメイン構文は、特定ドメイン宛のすべての受信者をブロックするために使用されます。構文は、具体的なドメインの前にアットマーク（@）を付けます。

表 2-10　グローバル配信停止の構文（続き）

@.example.com	部分ドメイン 部分ドメイン構文は、特定ドメイン宛およびそのすべてのサブドメイン宛のすべての受信者をブロックするために使用されます。
10.1.28.12	IP アドレス IP アドレス構文は、特定 IP アドレス宛のすべての受信者をブロックするために使用されます。単一 IP アドレスで複数ドメインをホストしている場合に、この構文が便利です。構文は、一般的なドット区切りのオクテット IP アドレスです。

CLI を使用したグローバル配信停止へのアドレスの追加

この例では、アドレス user@example.net がグローバル配信停止リストに追加され、メッセージをハード バウンスするように機能が設定されます。このアドレスに送信されるメッセージはバウンスされます。配信の直前にメッセージがバウンスされます。

```
mail3.example.com> unsubscribe


Global Unsubscribe is enabled. Action: drop.


Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import entries from a file.

- SETUP - Configure general settings.

[]> new


Enter the unsubscribe key to add. Partial addresses such as

"@example.com" or "user@" are allowed, as are IP addresses. Partial hostnames such as
"@.example.com" are allowed.

[]> user@example.net


Email Address 'user@example.net' added.

Global Unsubscribe is enabled.
```

```
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup

Do you want to enable the Global Unsubscribe feature? [Y]> y

Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2

Global Unsubscribe is enabled. Action: bounce.

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>
```

```
mail3.example.com> commit

Please enter some comments describing your changes:

[]> Added username “user@example.net” to global unsubscribe

Changes committed: Thu Mar 27 14:57:56 2003
```

グローバル配信停止ファイルのエクスポートおよびインポート

HAT、RAT、smtproutes、スタティック マスカレード テーブル、エイリアス テーブル、ドメイン マップ テーブル、altsrchost エントリと同様に、グローバル配信停止エントリはファイルをエクスポートおよびインポートして変更できます。次の手順に従ってください。

ステップ 1　unsubscribe コマンドの export サブコマンドを使用して、既存のエントリをファイル（ファイル名は自分で指定）にエクスポートします。

ステップ 2　CLI の外部で、ファイルを取得します。（詳細については、付録 B「アプライアンスへのアクセス」を参照してください）。

ステップ 3　テキスト エディタを使用して、ファイルに新しいエントリを作成します。

ファイル内でエントリを区切るには、改行します。あらゆるオペレーティング システムの改行表現を使用できます（<CR>、<LF>、または <CR><LF>）。コメント行はナンバー記号（#）で始まり、無視されます。たとえば、次のファイルでは、単一の受信者電子メール アドレス（test@example.com）、特定ドメインのすべての受信者（@testdomain.com）、複数ドメインで同じ名前を持つすべてのユーザ（testuser@）、および特定 IP アドレスの任意の受信者（11.12.13.14）が除外されます。

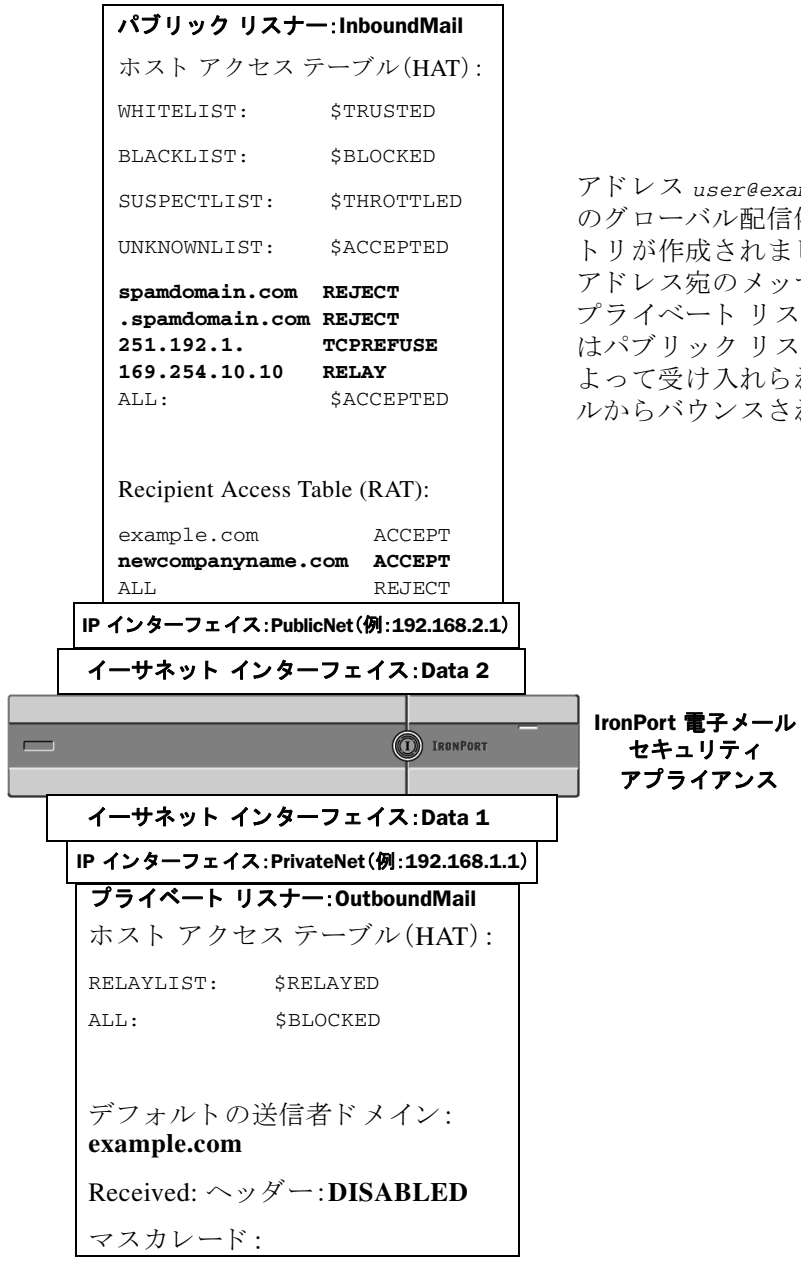
```
# this is an example of the global_unsubscribe.txt file

test@example.com

@testdomain.com

testuser@

11.12.13.14
```

ステップ 4　ファイルを保存してインターフェイスの configuration ディレクトリに配置し、インポートできるようにします。（詳細については、付録 B「アプライアンスへのアクセス」を参照してください）。

ステップ 5　unsubscribe の import サブコマンドを使用して、編集したファイルをインポートします。

これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 2-21　　グローバル配信停止の例



アドレス *user@example.net* のグローバル配信停止エントリが作成されました。このアドレス宛のメッセージは、プライベート リスナーまたはパブリック リスナーによって受け入れられたメールからバウンスされます。

確認：電子メール パイプライン

表 2-11 および表 2-12 に、受信から配信へのルーティングまで、電子メールがシステムでルーティングされる様子の概要を示します。各機能は上から順に実行されます。ここでは簡単に説明します。図 2-21 の陰付きの部分は、ワーク キュー内で発生する処理を表します。

このパイプラインに含まれる機能の設定の大部分は、`trace` コマンドを使用してテストできます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「テスト メッセージを使用したメール フローのデバッグ：トレース」を参照してください。

（注）　発信メールの場合は、ウイルス アウトブレイク フィルタ ステージの後に RSA 電子メール データ漏洩防止スキャニングが実行されます。

表 2-11　Cisco IronPort アプライアンスの電子メール パイプライン：電子メール受信機能

機能	説明
ホスト アクセス テーブル（HAT） **ホスト DNS 送信者検証（Host DNS Sender Verification）** **送信者グループ** **エンベロープ送信者検証（Envelope Sender Verification）** **送信者検証例外テーブル（Sender Verification Exception Table）** **メール フロー ポリシー（Mail Flow Policies）**	接続の ACCEPT、REJECT、RELAY、または TCPREFUSE。 最大アウトバウンド接続数。 IP アドレスあたりの最大同時インバウンド接続数。 接続あたりの最大メッセージ サイズおよびメッセージ数。 メッセージあたりおよび時間あたりの最大受信者数。 TCP リッスン キュー サイズ。 TLS：no/preferred/required SMTP AUTH：no/preferred/required 不正な形式の FROM ヘッダーを持つ電子メールのドロップ 送信者検証例外テーブル内のエントリからのメールを常に受け入れるか拒否します。 SenderBase オン/オフ（IP プロファイリング/フロー制御）
Received ヘッダー（Received Header）	受け入れた電子メールに対する Received ヘッダーの追加：オン/オフ。
デフォルト ドメイン	「素」ユーザ アドレスにデフォルト ドメインを追加します。
バウンス検証	着信バウンス メッセージを正規メッセージとして検証します。
ドメイン マップ（Domain Map）	ドメイン マップ テーブル内のドメインと一致するメッセージに含まれている各受信者のエンベロープ受信者の書き換え。
受信者アクセス テーブル（RAT）	（パブリック リスナーのみ）`RCPT TO` およびカスタム SMTP 応答内の受信者の ACCEPT または REJECT 特別な受信者にスロットリングのバイパスを許可します。
エイリアス テーブル（Alias tables）	エンベロープ受信者を書き換えます。（システム全体を対象に設定されます。`aliasconfig` は、`listenerconfig` のサブコマンドではありません）。
LDAP 受信者の受け入れ（LDAP Recipient Acceptance）	受信者受け入れの LDAP 検証は、SMTP カンバセーションで行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりにワーク キュー内で LDAP 検証を行うように設定することもできます。

表 2-12　Cisco IronPort アプライアンスの電子メール パイプライン:ルーティングおよび配信機能

ワーク キュー	LDAP 受信者の受け入れ		受信者受け入れの LDAP 検証はワーク キュー内で行われます。受信者が LDAP ディレクトリで見つからない場合、メッセージはドロップされるかバウンスされます。代わりに SMTP カンバセーション LDAP 検証を行うよう設定することもできます。
	マスカレード または LDAP マスカレード		マスカレードは、ワーク キューで行われます。マスカレードでは、スタティック テーブルを使用するか LDAP クエリーを使用して、エンベロープ送信者、To:、From:、CC: ヘッダーを書き換えます。
	LDAP ルーティング		LDAP クエリーは、メッセージ ルーティングまたはアドレス書き換えのために実行されます。グループ LDAP クエリーは、メッセージ フィルタ ルール `mail-from-group` および `rcpt-to-group` と連携して動作します。
	メッセージ フィルタ（Message Filters）*		メッセージ フィルタはメッセージの「分裂」よりも前に適用されます。* メッセージを隔離エリアに送信できます。
	アンチスパム**	受信者単位のスキャン（Per Recipient Scanning）	アンチスパム スキャン エンジンでは、メッセージを検査して、さらに処理するために判定を返します。
	アンチウイルス*		アンチウイルス スキャンでは、ウイルスを検出するためにメッセージを検査します。メッセージはスキャンされ、可能であれば、任意で修復されます。* メッセージを隔離エリアに送信できます。
	コンテンツ フィルタ*		コンテンツ フィルタが適用されます。* メッセージを隔離エリアに送信できます。
	アウトブレイク フィルタ*		アウトブレイク フィルタ機能を使用すると、ウイルス感染から保護できます。* メッセージを隔離エリアに送信できます。
	仮想ゲートウェイ		特定の IP インターフェイスまたは IP インターフェイスのグループを介してメールを送信します。
	配信制限（Delivery limits）		1. デフォルト配信インターフェイスを設定します。 2. アウトバウンド接続の合計最大数を設定します。

表 2-12　Cisco IronPort アプライアンスの電子メール パイプライン：ルーティングおよび配信機能（続き）

ドメインベースの制限値（Domain-based Limits）	ドメイン単位で、各仮想ゲートウェイおよびシステム全体の最大アウトバウンド接続数、使用するバウンス プロファイル、配信用の TLS プレファレンス：no/preferred/required を定義します。
ドメインベースのルーティング（Domain-based routing）	エンベロープ受信者を書き換えず、ドメインに基づいてメールをルーティングします。
グローバル配信停止（Global unsubscribe）	特定のリストに従って受信者をドロップします（システム全体を対象に設定）。
バウンス プロファイル（Bounce profiles）	配信不能メッセージの処理です。リスナー単位、送信先コントロール エントリ単位、およびメッセージ フィルタ経由で設定可能です。

＊これらの機能では、Quarantines という特別なキューにメッセージを送信できます。

CHAPTER 3

LDAP クエリ

クラウド E メール セキュリティ アプライアンスの LDAP 設定は変更しないことを推奨します。

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリ（Microsoft Active Directory、SunONE Directory Server、OpenLDAP などのディレクトリ）に格納されている場合は、メッセージの受け入れ、ルーティング、および認証のために LDAP サーバに対してクエリを実行するように Cisco IronPort アプライアンスを設定できます。Cisco IronPort アプライアンスは、1 つまたは複数の LDAP サーバと連携させるように設定できます。

この章では、次のトピックについて取り上げます。

概要

ここでは、実行できる LDAP クエリーのタイプ、LDAP と Cisco IronPort アプライアンスとが連携してメッセージの認証、受け入れ、ルーティングを行うしくみ、および LDAP と連携するように Cisco IronPort アプライアンスを設定する方法の概要を示します。

LDAP クエリについて

ユーザ情報がネットワーク インフラストラクチャ内の LDAP ディレクトリに格納されている場合は、次の目的で LDAP サーバに対してクエリーを実行するように Cisco IronPort アプライアンスを設定できます。

- **受け入れクエリ**。既存の LDAP インフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メール アドレスの扱い方を定義できます。詳細については、受け入れ（受信者検証）クエリー（3-20 ページ）を参照してください。
- **ルーティング（エイリアシング）**。ネットワーク内の LDAP ディレクトリで使用可能な情報に基づいてメッセージを適切なアドレスやメール ホストにルーティングするように、アプライアンスを設定できます。詳細については、ルーティング：エイリアス拡張（3-21 ページ）を参照してください。
- **マスカレード**。発信メールの場合はエンベロープ送信者、着信メールの場合はメッセージ ヘッダー（To:、Reply To:、From:、CC:など）をマスカレードできます。マスカレードの詳細については、マスカレード（3-22 ページ）を参照してください。
- **グループ クエリ**。LDAP ディレクトリ内のグループに基づいてメッセージに対するアクションを実行するように、Cisco IronPort アプライアンスを設定できます。このように設定するには、グループ クエリとメッセージ フィルタとを関連付けます。定義済みの LDAP グループに一致するメッセージに対しては、メッセージ フィルタに使用できる任意のメッセージ アクションを実行できます。詳細については、グループ LDAP クエリー（3-23 ページ）を参照してください。
- **ドメインベース クエリ**。ドメインベース クエリーを作成すると、Cisco IronPort アプライアンスは同じリスナー上でドメインごとに異なるクエリーを実行できます。E メール セキュリティ アプライアンスがドメインベース クエリを実行するときは、どのクエリを使用するかをドメインに基づいて決定し、そのドメインに関連付けられている LDAP サーバに対してクエリを実行します。
- **チェーン クエリ**。チェーン クエリーを作成すると、Cisco IronPort アプライアンスに一連のクエリーを順番に実行させることができます。チェーン クエリーが設定済みのときは、Cisco IronPort アプライアンスはシーケンス内のクエリーを 1 つずつ実行し、LDAP アプライアンスから肯定的な結果が返されると実行を停止します。
- **ディレクトリ ハーベスト防止**。LDAP ディレクトリを使用したディレクトリ ハーベスト攻撃を防ぐように Cisco IronPort アプライアンスを設定できます。ディレクトリ ハーベスト防止は、SMTP カンバセーション中に行うことも、ワーク キューの中で行うこともできます。受信者が LDAP ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。その結果、スパム送信者はメール アドレスが有効なものかどうかを区別できなくなります。LDAP によるディレクトリ ハーベスト攻撃防止（3-30 ページ）を参照してください。
- **SMTP 認証**。AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。この機能を利用すると、ユーザはリモート接続するとき（たとえば自宅や出張先にいる場合）でも、メール サーバを使用してメールを送信できるようになります。詳細については、SMTP 認証を行うための AsyncOS の設定（3-33 ページ）を参照してください。
- **外部認証**。Cisco IronPort アプライアンスにログインするユーザの認証を LDAP ディレクトリを使用して行うように、Cisco IronPort アプライアンスを設定できます。詳細については、ユーザの外部認証の設定（3-42 ページ）を参照してください。
- **スパム検疫エンドユーザ認証**。エンドユーザ隔離画面にログインするユーザを検証するように、アプライアンスを設定できます。詳細については、スパム検疫へのエンドユーザ認証のクエリー（3-45 ページ）を参照してください。

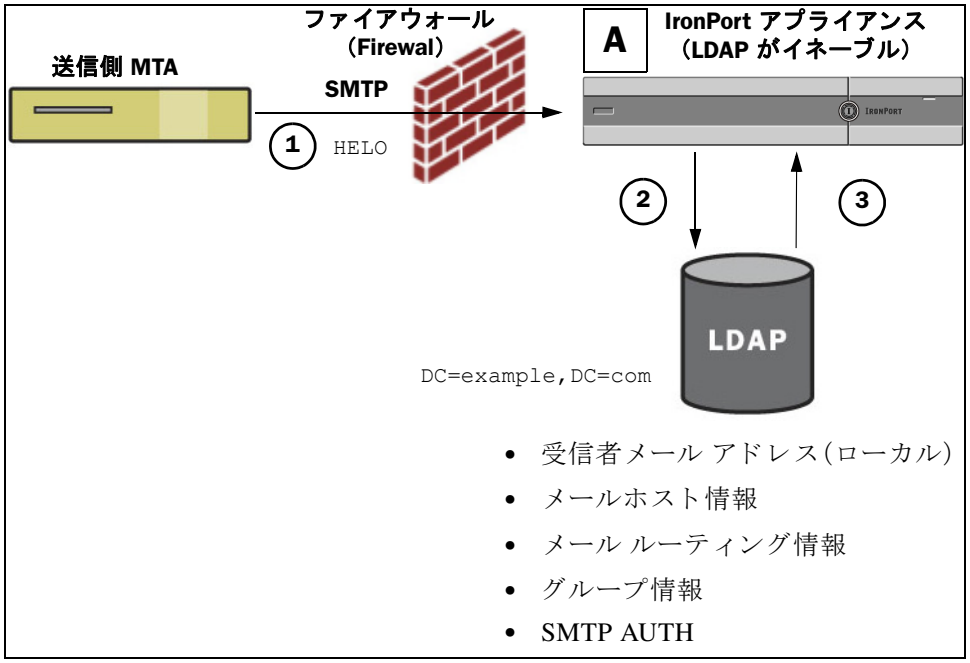
- **スパム検疫エイリアス統合。**スパムに関する電子メール通知を使用する場合、このクエリを使用してエンドユーザのエイリアスを統合すると、エンドユーザがエイリアスのメール アドレスごとに隔離通知を受け取ることはなくなります。詳細については、スパム隔離のエイリアス統合クエリ (3-46 ページ)を参照してください。
- **ユーザ識別名。**データ消失防止（DLP）のために RSA Enterprise Manager を使用する場合、このクエリは DLP 違反を含む可能性があるメッセージ送信者の識別名を取得します。E メール セキュリティ アプライアンスは、Enterprise Manager に DLP インシデント データを送信する際に識別名を含めます。詳細については、User Distinguished Name Queries, page 3-48 を参照してください。

LDAP と AsyncOS との連携の仕組み

LDAP ディレクトリと Cisco IronPort アプライアンスとを連携させると、受信者受け入れ、メッセージ ルーティング、およびヘッダー マスカレードに LDAP ディレクトリ サーバを使用できます。LDAP グループ クエリーをメッセージ フィルタとともに使用すると、メッセージが Cisco IronPort アプライアンスで受信されたときの取り扱いのルールを作成できます。

図 3-1 に、Cisco IronPort アプライアンスと LDAP がどのように連携するかを示します。

図 3-1　LDAP 設定



ステップ 1　送信側 MTA からパブリック リスナー「A」に SMTP 経由でメッセージが送信されます。

ステップ 2　Cisco IronPort アプライアンスは、LDAP サーバに対してクエリを実行します。この LDAP サーバは [システム管理（System Administration）] > [LDAP] ページ（またはグローバル `ldapconfig` コマンド）で定義されます。

ステップ 3　データが LDAP ディレクトリから受信されます。リスナーで使用するように [システム管理（System Administration）] > [LDAP] ページ（または `ldapconfig` コマンド）で定義されたクエリに応じて、次の処理が実行されます。

- メッセージを新しい受信者アドレスにルーティングするか、ドロップまたはバウンスする
- メッセージを新しい受信者のメールホストにルーティングする
- メッセージ ヘッダー From:、To:、CC: をクエリに基づいて書き換える
- メッセージ フィルタ ルール `rcpt-to-group` または `mail-from-group` で定義された、それ以降のアクション（グループ クエリと組み合わせて使用）。

（注）　Cisco IronPort アプライアンスからは、複数の LDAP サーバに接続できます。その場合、複数の LDAP サーバを使用して、ロード バランシングやフェールオーバーを行うように LDAP プロファイルを設定できます。複数の LDAP サーバと連携させる方法の詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定（3-48 ページ）を参照してください。

AsyncOS を LDAP と連携させるための設定

受け入れ、ルーティング、エイリアシング、およびマスカレードのために Cisco IronPort アプライアンスを LDAP ディレクトリと連携させるには、以下の手順に従って AsyncOS アプライアンスを設定する必要があります。

ステップ 1　**LDAP サーバ プロファイルを設定します。**サーバ プロファイルに、AsyncOS から LDAP サーバに接続するための次の情報を設定します。

- クエリ送信先となるサーバの名前とポート
- ベース DN
- サーバとのバインドのための認証要件

サーバ プロファイルの設定方法の詳細については、LDAP サーバ プロファイルの作成（3-5 ページ）を参照してください。

LDAP サーバ プロファイルを設定するときに、AsyncOS からの接続先となる LDAP サーバを 1 つまたは複数設定できます。

AsyncOS から複数のサーバに接続するように設定する方法については、AsyncOS を複数の LDAP サーバと連携させるための設定（3-48 ページ）を参照してください。

ステップ 2　**LDAP クエリを設定します。**LDAP クエリは、LDAP サーバ プロファイルで設定します。ここで設定するクエリは、実際に使用する LDAP の実装とスキーマに合わせて調整してください。

作成できる LDAP クエリのタイプについては、LDAP クエリについて（3-2 ページ）を参照してください。

クエリの記述方法については、LDAP クエリに関する作業（3-12 ページ）を参照してください。

ステップ 3　**LDAP サーバ プロファイルをパブリック リスナーまたはプライベート リスナーに対してイネーブルにします。**LDAP サーバ プロファイルをリスナーに対してイネーブルにすると、そのリスナーによって、メッセージの受け入れ、ルーティング、または送信の際に LDAP クエリが実行されるようになります。

詳細については、LDAP、LDAP クエリー、およびリスナーとの連携（3-7 ページ）を参照してください。

（注）　グループ クエリを設定するときは、AsyncOS と LDAP サーバとを連携させるためにさらに設定作業が必要です。グループ クエリの設定方法については、グループ LDAP クエリー（3-23 ページ）を参照してください。エンドユーザ認証またはスパム通知統合のクエリを設定するときは、Cisco IronPort スパム隔離機能への LDAP エンドユーザ アクセスをイネーブルにする必要があります。Cisco IronPort スパム隔離の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Cisco IronPort スパム隔離機能の設定」を参照してください。

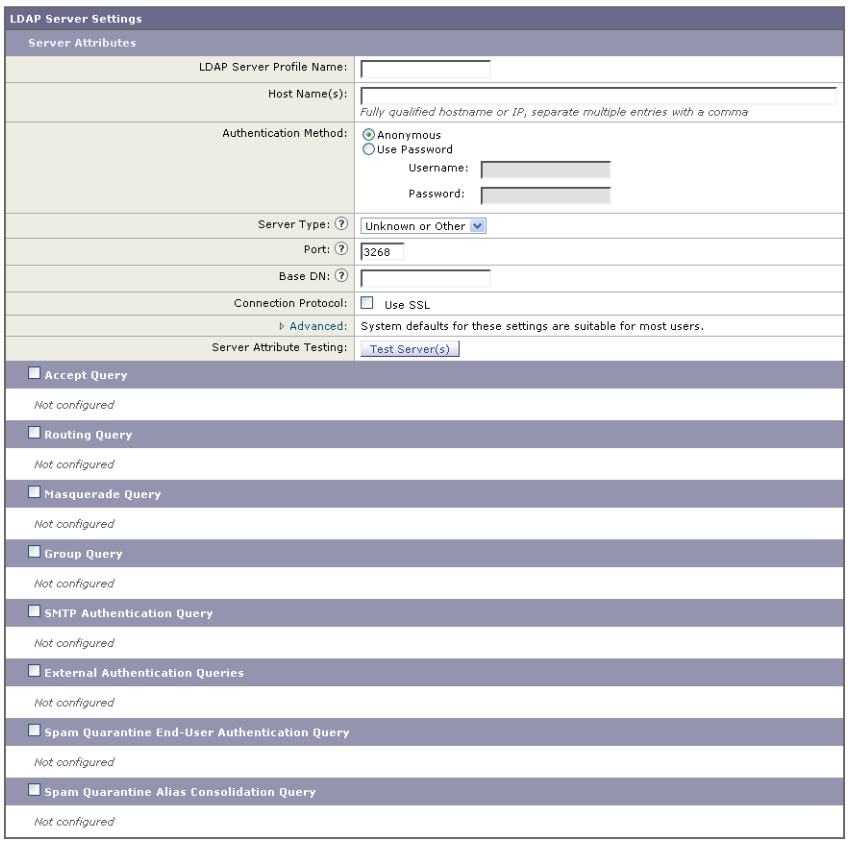
LDAP サーバ プロファイルの作成

LDAP ディレクトリを使用するように AsyncOS を設定するには、LDAP サーバに関する情報を格納する LDAP サーバ プロファイルを作成します。

LDAP サーバ プロファイルを作成するには、次の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [LDAP] ページの [LDAP サーバプロファイルを追加（Add LDAP Server Profile）] をクリックします。[LDAP サーバプロファイルを追加（Add LDAP Server Profile）] ページが表示されます。

図 3-2　　LDAP サーバ プロファイルの設定



ステップ 2　サーバ プロファイルの名前を入力します。

ステップ 3　LDAP サーバのホスト名を入力します。

複数のホスト名を入力すると、LDAP サーバのフェールオーバーやロード バランシングができるようになります。複数のエントリを指定する場合は、カンマで区切ります。詳細については、AsyncOS を複数の LDAP サーバと連携させるための設定（3-48 ページ）を参照してください。

ステップ 4　認証方式を選択します。匿名認証を使用することも、ユーザ名とパスワードを指定することもできます。

ステップ 5　LDAP サーバ タイプを、[アクティブディレクトリ（Active Directory）]、[OpenLDAP]、または [不明またはそれ以外（Unknown or Other）] から選択します。

ステップ 6　ポート番号を入力します。

デフォルト ポートは 3268 です。これは、複数台のサーバ環境でグローバル カタログへのアクセスをイネーブルにする Active Directory 用のデフォルト ポートです。

ステップ 7　LDAP サーバのベース DN（識別名）を入力します。

ユーザ名とパスワードを使用して認証する場合は、パスワードが格納されているエントリへの完全 DN がユーザ名に含まれている必要があります。たとえば、マーケティング グループに属しているユーザの電子メール アドレスが joe@example.com であるとします。このユーザのエントリは、次のようになります。

```
uid=joe, ou=marketing, dc=example dc=com
```

ステップ 8　LDAP サーバとの通信に SSL を使用するかどうかを選択します。

ステップ 9　[詳細（Advanced）] で、キャッシュの存続可能時間を入力します。この値は、キャッシュを保持する時間の長さです。

ステップ 10　保持するキャッシュ エントリの最大数を入力します。

ステップ 11　同時接続の最大数を入力します。

ロード バランシングのために LDAP サーバ プロファイルを設定する場合、これらの接続はリストで指定された LDAP サーバ間で配分されます。たとえば、同時接続数を 10 と設定し、3 台のサーバを使用して接続のロード バランシングを行う場合は、AsyncOS によってサーバへの接続が 10 ずつ作成され、接続の総数は 30 となります。

（注）　同時接続の最大数には、LDAP クエリーに使用される LDAP 接続も含まれます。ただし、Cisco IronPort スパム隔離機能に対して LDAP 認証を使用する場合は、これよりも多くの接続が開かれることがあります。

ステップ 12　[テストサーバ（Test Server(s)）] ボタンをクリックしてサーバへの接続をテストします。複数の LDAP サーバを指定した場合は、すべてのサーバのテストが実行されます。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。詳細については、LDAP サーバのテスト（3-7 ページ）を参照してください。

ステップ 13　クエリを作成します。該当するチェックボックスをオンにして、フィールドに入力します。選択できるのは、[承認（Accept）]、[ルーティング（Routing）]、[マスカレード（Masquerade）]、[グループ（Group）]、[SMTP 認証（SMTP Authentication）]、[外部認証（External Authentication）]、[スパム隔離エンドユーザ認証（Spam Quarantine End-User Authentication）]、[スパム隔離エイリアス統合（Spam Quarantine Alias Consolidation）] です。

（注）　メッセージを受信または送信するときに Cisco IronPort アプライアンスが LDAP クエリーを実行できるようにするには、該当するリスナーに対して LDAP クエリーをイネーブルにする必要があります。詳細については、LDAP、LDAP クエリー、およびリスナーとの連携（3-7 ページ）を参照してください。

ステップ 14　クエリをテストするために、[クエリのテスト（Test Query）] ボタンをクリックします。

テスト パラメータを入力して [テストの実行（Run Test）] をクリックします。テストの結果が [接続ステータス（Connection Status）] フィールドに表示されます。クエリーの定義や属性に変更を加えた場合は、[更新（Update）] をクリックします。詳細については、LDAP クエリのテスト（3-18 ページ）を参照してください。

（注）　空パスワードでのバインドを許可するように LDAP サーバが設定されている場合は、パスワード フィールドが空でもクエリーのテストは合格となります。

ステップ 15　変更を送信し、保存します。

（注）　サーバ設定の数に制限はありませんが、設定できるクエリは、サーバ 1 台につき受信者受け入れ 1 つ、ルーティング 1 つ、マスカレード 1 つ、グループ クエリ 1 つのみです。

LDAP サーバのテスト

[LDAP サーバプロファイルの追加/編集（Add/Edit LDAP Server Profile）] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。サーバ ポートへの接続に成功したか失敗したかを示すメッセージが表示されます。複数の LDAP サーバが設定されている場合は、各サーバのテストが実行されて、結果が個別に表示されます。

LDAP、LDAP クエリー、およびリスナーとの連携

メッセージを受信または送信するときに Cisco IronPort アプライアンスが LDAP クエリーを実行できるようにするには、該当するリスナーに対して LDAP クエリーをイネーブルにする必要があります。

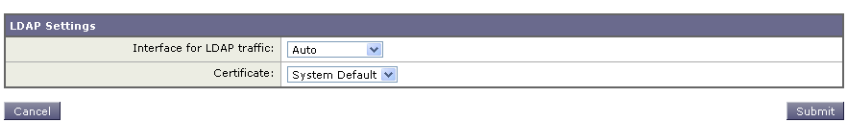
グローバル設定の構成

LDAP グローバル設定では、すべての LDAP トラフィックをアプライアンスがどのように扱うかを定義します。LDAP のグローバル設定を指定するには、次の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [LDAP] ページの [設定を編集（Edit Settings）] をクリックします。

[Edit LDAP Settings] ページが表示されます。

図 3-3　[Edit LDAP Settings] ページ



ステップ 2　LDAP トラフィックに使用する IP インターフェイスを選択します。インターフェイスの 1 つが自動的にデフォルトとして選択されます。

ステップ 3　LDAP インターフェイスに使用する TLS 証明書を選択します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の `certconfig` コマンドを使用して追加された TLS 証明書。TLS を使用した SMTP カンバセーションの暗号化（1-22 ページ）を参照してください）。

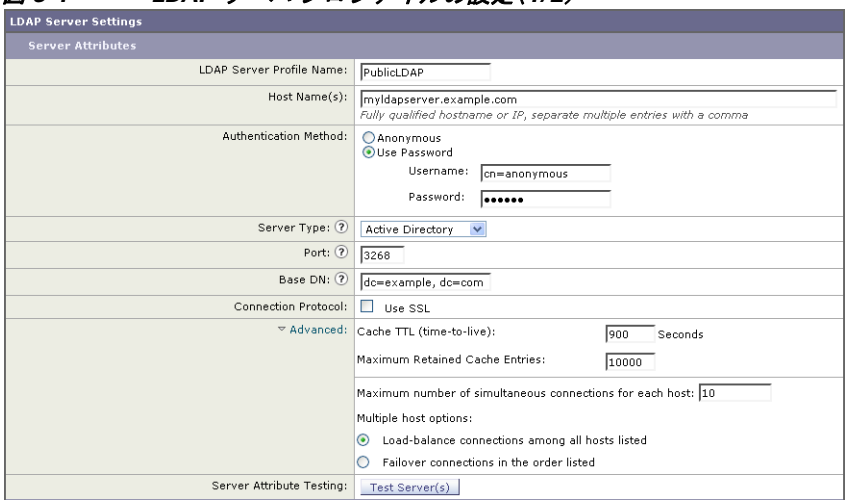
ステップ 4　変更を送信し、保存します。

LDAP サーバ プロファイル作成の例

次に示す例では、[システム管理（System Administration）] > [LDAP] ページを使用してアプライアンスのバインド先となる LDAP サーバを定義し、受信者受け入れ、ルーティング、およびマスカレードのクエリを設定します。

（注）　LDAP 接続試行のタイムアウトは 60 秒です。この時間には、DNS ルックアップと接続そのものに加えて、アプライアンス自体の認証バインド（該当する場合）も含まれます。初回の失敗後は、同じサーバ内の別のホストに対する試行がただちに行われます（2 つ以上のホストをカンマ区切りリストで指定した場合）。サーバ内にホストが 1 つしかない場合は、そのホストへの接続が繰り返し試行されます。

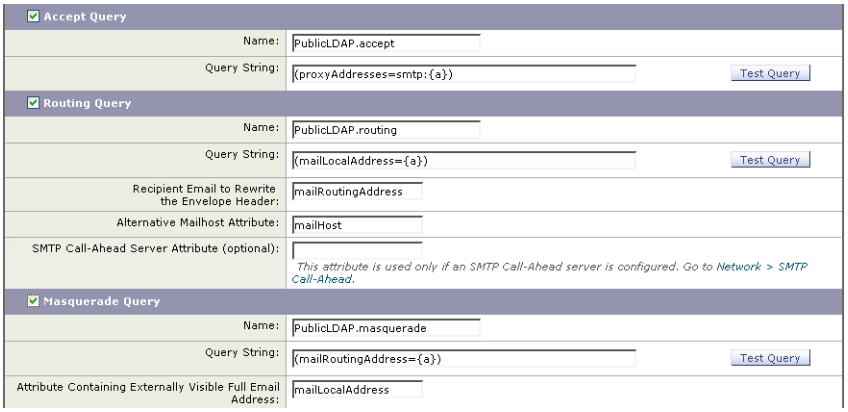
図 3-4　LDAP サーバ プロファイルの設定（1/2）



初めに、「PublicLDAP」というニックネームを `myldapserver.example.com` LDAP サーバに与えます。接続数は 10（デフォルト値）に設定されており、複数 LDAP サーバ（ホスト）のロード バランス オプションはデフォルトのままとなっています。ここで複数のホストの名前を、カンマ区切りのリストとして指定できます。クエリの送信先は、ポート 3268（デフォルト値）です。SSL は、このホストの接続プロトコルとしてはイネーブルになっていません。`example.com` のベース DN が定義されています（`dc=example,dc=com`）。キャッシュの存続可能時間は 900 秒、キャッシュ エントリの最大数は 10000 に設定されています。認証方式は、パスワード認証に設定されています。

受信者受け入れ、メール ルーティング、およびマスカレードのクエリが定義されています。クエリー名では、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

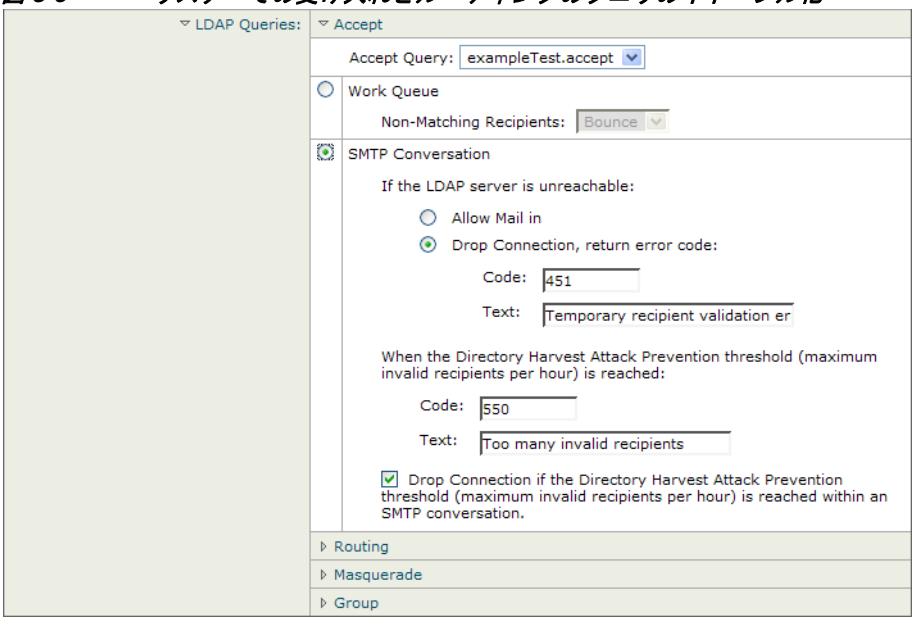
図 3-5　　LDAP サーバ プロファイルの設定(2/2)



パブリック リスナー上の LDAP クエリの有効化

この例では、受信者受け入れに対して LDAP クエリを使用するように、パブリック リスナー「InboundMail」を更新します。さらに、受信者受け入れの判定を SMTP カンバセーション中に行うように設定します(詳細については、受け入れ(受信者検証)クエリー(3-20 ページ)を参照してください)。

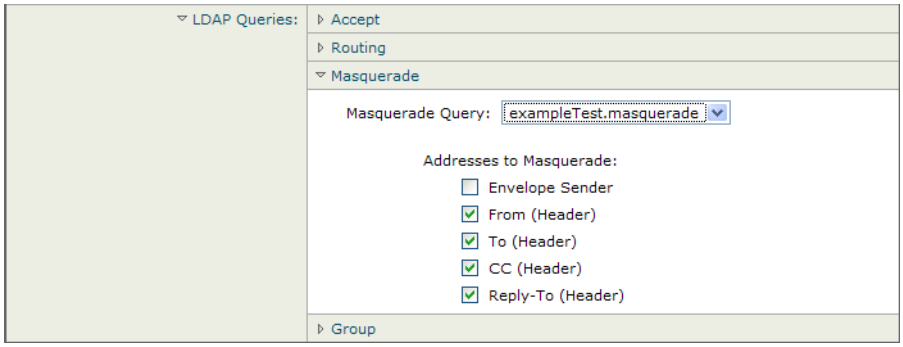
図 3-6　　リスナーでの受け入れとルーティングのクエリのイネーブル化



プライベート リスナーでの LDAP クエリのイネーブル化

この例では、LDAP クエリを使用してマスカレードを行うように、プライベート リスナー「OutboundMail」を更新します。マスカレード対象のフィールドには、From、To、CC、Reply-To があります。

図 3-7　　リスナーでのマスカレード クエリのイネーブル化



Microsoft Exchange 5.5 に対する拡張サポート

AsyncOS には、Microsoft Exchange 5.5 をサポートするための設定オプションがあります。これよりも新しいバージョンの Microsoft Exchange を使用する場合は、このオプションをイネーブルにする必要はありません。LDAP サーバを設定するときに、Microsoft Exchange 5.5 サポートをイネーブルにするかどうかを選択できます。選択するには、CLI を使用する必要があります。次に示すように、`ldapconfig -> edit -> server -> compatibility` サブコマンドを実行して、質問に「y」と答えます。

```
mail3.example.com> ldapconfig


Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.

- DELETE - Remove a server configuration.

[]> edit


Enter the name or number of the server configuration you wish to edit.

[]> 1


Name: PublicLDAP

Hostname: ldapexample.com Port 389
```

```
Authentication Type: anonymous

Base: dc=ldapexample,dc=com



Choose the operation you want to perform:

- SERVER - Change the server for the query.

- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.

- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.

- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server



Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Disabled



Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
```

```
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)
[N]> y


Do you want to configure advanced LDAP compatibility settings? (Typically not required)
[N]>


Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")


Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

LDAP クエリに関する作業

LDAP サーバ プロファイル内に、実行したい LDAP クエリのタイプごとに 1 つのエントリを作成します。LDAP クエリを作成するときは、実際に使用する LDAP サーバのクエリ構文で入力する必要があります。作成するクエリは、実際に使用する LDAP ディレクトリ サービスの実装に合わせて調整が必要であることに注意してください。特に、組織固有のニーズを満たすように新しいオブジェクト クラスや属性がディレクトリに追加されている場合です。

LDAP クエリのタイプ

次の各項で、各タイプのクエリーの例を示し、設定方法を詳しく説明します。

- **受け入れクエリ**。詳細については、受け入れ（受信者検証）クエリー（3-20 ページ）を参照してください。
- **ルーティング クエリ**。詳細については、ルーティング：エイリアス拡張（3-21 ページ）を参照してください。
- **マスカレード クエリ**。詳細については、マスカレード（3-22 ページ）を参照してください。
- **グループ クエリ**。詳細については、グループ LDAP クエリー（3-23 ページ）を参照してください。
- **ドメインベース クエリ**。詳細については、ドメインベース クエリー（3-27 ページ）を参照してください。
- **チェーン クエリ**。詳細については、チェーン クエリ（3-29 ページ）を参照してください。

次の目的のためにクエリを設定することもできます。

- **ディレクトリ ハーベスト防止**。詳細については、LDAP クエリについて（3-2 ページ）を参照してください。
- **SMTP 認証**。詳細については、SMTP 認証を行うための AsyncOS の設定（3-33 ページ）を参照してください。
- **外部認証**。詳細については、ユーザの外部認証の設定（3-42 ページ）を参照してください。
- **スパム隔離エンドユーザ認証クエリー**。詳細については、スパム検疫へのエンドユーザ認証のクエリー（3-45 ページ）を参照してください。
- **スパム隔離のエイリアス統合のクエリ**。詳細については、スパム隔離のエイリアス統合クエリ（3-46 ページ）を参照してください。

指定した検索クエリは、システム上で設定済みのすべてのリスナーに使用できます。

ベース識別名（DN）

ディレクトリのルート レベルを「ベース」と呼びます。ベースの名前は DN（Distinguishing Name）です。Active Directory（および RFC 2247 に基づく標準）のベース DN のフォーマットでは、DNS ドメインがドメイン コンポーネント（dc=）に変換されます。たとえば、example.com のベース DN は「dc=example, dc=com」です。DNS 名の各部分が順番に表現されることに注意してください。これには、実際の LDAP 設定が反映されることも、されないこともあります。

実際に使用するディレクトリに複数のドメインが含まれている場合は、クエリの対象のベースを 1 つだけ入力するのでは不都合であることもあります。そのような場合は、LDAP サーバ設定を指定するときに、ベースを「NONE」に設定します。ただし、このように設定すると検索の効率が低下します。

LDAP クエリの構文

LDAP パス内でスペースを使用できます。引用符で囲む必要はありません。CN と DC の構文では、大文字と小文字は区別されません。

```
Cn=First Last,oU=user,dc=domain,DC=COM
```

クエリに入力する変数名では、*大文字と小文字が区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **`mailLocalAddress`** と入力したときに実行されるクエリは、**`maillocaladdress`** と入力したときとは異なります。

トークン

次のトークンを LDAP クエリ内で使用できます。

- {a} ユーザ名@ドメイン名
- {d} ドメイン名
- {dn} 識別名
- {g} グループ名
- {u} ユーザ名
- {f} MAIL FROM: アドレス

（注） {f} トークンを使用できるのは、受け入れクエリーのみです。

たとえば、メールを受け入れるための Active Directory LDAP サーバに対するクエリは、次のようになります。

(|(mail={a})(proxyAddresses=smtp:{a}))

（注） 作成したクエリは、[LDAP] ページの [テスト（Test）] 機能（または `ldapconfig` コマンドの `test` サブコマンド）を使用してテストすることを強く推奨します。期待したとおりの結果が返されることを*確認してから*、リスナーに対して LDAP 機能をイネーブルにしてください。詳細については、LDAP クエリのテスト（3-18 ページ）を参照してください。

セキュア LDAP（SSL）

AsyncOS と LDAP サーバとの通信に SSL を使用するように設定できます。SSL を使用するように LDAP サーバ プロファイルを設定した場合の動作は次のようになります。

- AsyncOS は、CLI の `certconfig` で設定された LDAPS 証明書を使用します（自己署名証明書の作成（1-23 ページ）を参照）。

  LDAP サーバによっては、LDAPS 証明書の使用をサポートするように設定する作業が必要になります。

- 設定済みの LDAPS 証明書がない場合は、デモ証明書が使用されます。

ルーティング クエリー

LDAP ルーティング クエリの再帰の制限はありません。ルーティングは完全にデータ ドリブンで行われます。ただし、AsyncOS には、ルーティングの永久ループを防止するために循環参照の有無を調べる機能があります。

匿名クエリー

組織によっては、匿名クエリを許可するように LDAP ディレクトリ サーバを設定しなければならない場合があります。(匿名クエリを許可すると、クライアントが匿名でサーバにバインドしてクエリを実行できるようになります)。匿名クエリを許可するように Active Directory を設定する具体的な手順については、Microsoft サポート技術情報 320528 を参照してください。URL は次のとおりです。

```
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528
```

または、認証とクエリ実行専用のユーザを 1 つ用意します。このようにすれば、任意のクライアントから匿名クエリを受け付けるように LDAP ディレクトリ サーバを開放する必要はありません。

ここでは、次の手順について説明します。

- 「匿名」認証を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- 「匿名バインド」を許可するように Microsoft Exchange 2000 サーバをセットアップする方法。
- Cisco IronPort AsyncOS が LDAP データを Microsoft Exchange 2000 サーバから「匿名バインド」と「匿名」認証の両方を使用して取得するようにセットアップする方法。

ユーザ電子メール アドレスを問い合わせるという目的で「匿名」または「匿名バインド」認証を許可するには、Microsoft Exchange 2000 サーバに対して特定のアクセス許可を設定する必要があります。このような設定が非常に役立つのは、SMTP ゲートウェイに対する着信メール メッセージの有効性を検証するために LDAP クエリを使用する場合です。

匿名認証のセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する未認証のクエリで特定のデータを使用できるようになります。Active Directory への「匿名バインド」を許可する手順については、Active Directory の匿名バインドのセットアップ (3-16 ページ) を参照してください。

ステップ 1　必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザ オブジェクト	権限	継承	アクセス許可のタイプ
全員	内容の一覧表示	コンテナ オブジェクト	オブジェクト
全員	内容の一覧表示	組織単位オブジェクト	オブジェクト
全員	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
全員	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2　Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザ オブジェクト [全員（Everyone）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3　Cisco IronPort メッセージング ゲートウェイを設定します。

コマンドライン インターフェイス（CLI）の `ldapconfig` を使用して、次の情報を指定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：匿名

Active Directory の匿名バインドのセットアップ

ここで説明するセットアップ手順を実行すると、Microsoft Windows Active Directory 内の Active Directory サーバおよび Exchange 2000 サーバに対する匿名バインド クエリで特定のデータを使用できるようになります。Active Directory サーバの匿名バインドにより、ユーザ名 `anonymous` とブランクのパスワードが送信されます。

（注）　匿名バインドを試行するときに何らかのパスワードが Active Directory サーバに送信されると、認証に失敗することがあります。

ステップ 1　必要となる Active Directory アクセス許可を確認します。

ADSI Edit スナップインまたは LDP ユーティリティを使用して、以下の Active Directory オブジェクトの属性に対するアクセス許可を修正する必要があります。

- クエリの対象であるドメインの、ドメイン名前付けコンテキストのルート。
- 電子メール情報クエリの対象であるユーザが属している OU および CN オブジェクトのすべて。

次の表に、必要なコンテナすべてに適用されている必要のあるアクセス許可を示します。

ユーザ オブジェクト	権限	継承	アクセス許可のタイプ
匿名ログオン	内容の一覧表示	コンテナ オブジェクト	オブジェクト
匿名ログオン	内容の一覧表示	組織単位オブジェクト	オブジェクト
匿名ログオン	パブリック インフォメーション読み取り	ユーザ オブジェクト	プロパティ
匿名ログオン	電話とメールのオプションの読み取り	ユーザ オブジェクト	プロパティ

ステップ 2　Active Directory のアクセス許可を設定します。

- Windows 2000 Support Tools から ADSIEdit を開きます。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを見つけます。このフォルダに、ドメインの LDAP パスがあります。
- [ドメインネーミングコンテキスト（Domain Naming Context）] フォルダを右クリックして [プロパティ（Properties）] をクリックします。
- [セキュリティ（Security）] をクリックします。
- [詳細設定（Advanced）] をクリックします。
- [追加（Add）] をクリックします。
- ユーザ オブジェクト [匿名ログオン（ANONYMOUS LOGON）] をクリックして [OK] をクリックします。
- [権限の種類（Permission Type）] タブをクリックします。
- [適用（Apply onto）] ボックスの [継承（Inheritance）] をクリックします。
- [権限（Permission）] アクセス許可の [許可（Allow）] チェックボックスをオンにします。

ステップ 3　Cisco IronPort メッセージング ゲートウェイを設定します。

[システム管理（System Administration）] > [LDAP] ページ（または CLI の `ldapconfig`）を使用して、次の情報を設定した LDAP サーバ エントリを作成します。

- Active Directory または Exchange サーバのホスト名
- ポート 3268（Port 2）
- ドメインのルート名前付けコンテキストに一致するベース DN
- 認証タイプ：パスワード ベース（`cn=anonymous` をユーザとして使用し、パスワードはブランク）

Active Directory の実装に関する注意

- Active Directory サーバが LDAP 接続を受け付けるポートは、3268 と 389 です。グローバル カタログへのアクセス用のデフォルト ポートは 3268 です。
- Active Directory サーバが LDAPS 接続を受け付けるポートは、636 と 3269 です。Microsoft 製品で LDAPS がサポートされるのは、Windows Server 2003 以上です。

- Cisco IronPort アプライアンスは、グローバル カタログでもあるドメイン コントローラに接続してください。これは、複数のベースに対するクエリーを同じサーバを使用して実行できるようにするためです。
- クエリを正常に実行するには、Active Directory の中で、ディレクトリ オブジェクトに対する読み取り許可をグループ「Everyone」に付与する必要があります。これには、ドメイン名前付けコンテキストのルートも含まれます。
- 一般的に、多くの Active Directory 実装では、`mail` 属性エントリに一致する値の「ProxyAddresses」属性エントリが存在します。
- Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

LDAP クエリのテスト

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [クエリのテスト（Test Query）] ボタン（または CLI の `test` サブコマンド）を使用して、クエリ タイプごとに、設定した LDAP サーバに対するクエリをテストします。結果が表示されるだけでなく、クエリ接続テストの各ステージの詳細も表示されます。テストは、クエリ タイプのそれぞれに対して行うことができます。

`ldaptest` コマンドは、次の例のようにバッチ コマンドとして使用できます。

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

LDAP サーバ属性の Host Name フィールドに複数のホストを入力した場合は、Cisco IronPort アプライアンスは各 LDAP サーバに対してクエリーのテストを行います。

表 3-1 は、テスト結果の要約です。（`ldaptest` コマンドを使用することもできます）。

表 3-1　LDAP クエリのテスト

クエリのタイプ	受信者が一致する場合（PASS）	受信者が一致しない場合（FAIL）
受信者受け入れ（[承認（Accept）]、`ldapaccept`）	メッセージを受け入れます。	受信者が無効：カンバセーションまたは遅延バウンスまたはメッセージをドロップ（リスナー設定による）。 DHAP：ドロップ。
ルーティング（[ルーティング（Routing）]、`ldaprouting`）	クエリの設定に基づいてルーティングします。	このメッセージの処理を続行します。
マスカレード（[マスカレード（Masquerade）]、`masquerade`）	クエリ内で定義された変数マッピングに従ってヘッダーを変更します。	このメッセージの処理を続行します。
グループ メンバーシップ（[グループ（Group）]、`ldapgroup`）	メッセージ フィルタ ルールに対して「true」を返します。	メッセージ フィルタ ルールに対して「false」を返します。
SMTP Auth **（[SMTP 認証（SMTP Authentication）]、`smtpauth`）**	LDAP サーバから返されたパスワードを使用して認証を行います。つまり、SMTP 認証が行われます。	一致するパスワードなし：SMTP 認証の試行は失敗します。

表 3-1　LDAP クエリのテスト（続き）

クエリのタイプ	受信者が一致する場合（PASS）	受信者が一致しない場合（FAIL）
外部認証（`externalauth`）	バインド、ユーザ レコード、およびユーザのグループ メンバーシップに対して個別に「match positive」が返されます。	バインド、ユーザ レコード、およびユーザのグループ メンバーシップに対して個別に「match negative」が返されます。
スパム隔離へのエンドユーザ認証（`isqauth`）	エンドユーザ アカウントに対して「match positive」が返されます。	一致するパスワードなし：エンドユーザ認証の試行は失敗します。
スパム隔離のエイリアス統合（`isqalias`）	統合されたスパム通知の送信先である電子メール アドレスが返されます。	スパム通知を統合できません。

（注） クエリに入力する変数名では、*大文字と小文字が区別されます*。また、正しく動作するためには、LDAP 実装と一致している必要があります。たとえば、プロンプトで **`mailLocalAddress`** と入力したときに実行されるクエリは、**`maillocaladdress`** と入力したときとは異なります。Cisco IronPort Systems では、作成したすべてのクエリについて `ldapconfig` コマンドの `test` サブコマンドを使用してテストし、正しい結果が返されることを確認するよう強く推奨します。

LDAP サーバへの接続のトラブルシューティング

LDAP サーバがアプライアンスから到達不能である場合は、次のエラーのいずれかが表示されます。

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

サーバが到達不能になる原因としては、サーバ設定で入力されたポートの誤りや、ファイアウォールでポートが開いていないことが考えられます。LDAP サーバの通信には一般に、ポート 3268 または 389 が使用されます。Active Directory は、ポート 3268 を使用して、マルチサーバ環境で使用されるグローバル カタログにアクセスします（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ファイアウォール情報」を参照してください）。AsyncOS 4.0 では、SSL を使用して（通常はポート 636 で）LDAP サーバと通信する機能が追加されました。詳細については、セキュア LDAP（SSL）（3-14 ページ）を参照してください。

サーバが到達不能になる原因としてはその他に、入力されたホスト名が解決不可能であることが考えられます。

[LDAP サーバ プロファイルを追加/編集（Add/Edit LDAP Server Profile）] ページの [テスト サーバ（Test Server(s)）]（または CLI の `ldapconfig` コマンドの `test` サブコマンド）を使用して、LDAP サーバへの接続をテストできます。詳細については、LDAP サーバのテスト（3-7 ページ）を参照してください。

LDAP サーバが到達不能である場合：

- LDAP 受け入れまたはマスカレードまたはルーティングがワーク キューに対してイネーブルになっている場合は、メールはワーク キュー内に留まります。
- LDAP 受け入れはイネーブルになっておらず、他のクエリ（グローバル ポリシー チェックなど）がフィルタ内で使用されている場合は、そのフィルタの評価結果が false になります。

受け入れ（受信者検証）クエリー

既存の LDAP インフラストラクチャを使用して、着信メッセージ（パブリック リスナーでの）の受信者メール アドレスの扱い方を定義できます。ディレクトリ内のユーザ データに対する変更は、次回 Cisco IronPort アプライアンスがディレクトリ サーバに対してクエリーを実行したときに更新されます。キャッシュのサイズと、Cisco IronPort が取得したデータを保持する時間の長さは設定可能です。

（注）　特別な受信者（たとえば administrator@example.com）に対して LDAP 受け入れクエリをバイパスすることもできます。このように設定するには、受信者アクセス テーブル（RAT）を使用します。この設定の方法については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」を参照してください。

受け入れクエリの例

表 3-2 に、受け入れクエリの例を示します。

表 3-2　　一般的な LDAP 実装での LDAP クエリ文字列の例：受け入れ

クエリの対象	受信者検証
OpenLDAP	(mailLocalAddress={a}) (mail={a}) (mailAlternateAddress={a})
Microsoft Active Directory Address Book **Microsoft Exchange**	(|(mail={a})(proxyAddresses=smtp:{a}))
Sun ONE Directory Server	(mail={a}) (mailAlternateAddress={a}) (mailEquivalentAddress={a}) (mailForwardingAddress={a}) (mailRoutingAddress={a})
Lotus Notes **Lotus Domino**	(|(|(mail={a})(uid={u}))(cn={u})) (|(ShortName={u})(InternetAddress={a})(FullName={u}))

ユーザ名（左側）の検証を行うこともできます。このことが役に立つのは、ディレクトリに格納されていないドメインのメールも受け入れるようにしたい場合です。受け入れクエリを (uid={u}) に設定してください。

Lotus Notes の場合の受け入れクエリの設定

LDAPACCEPT と Lotus Notes とを組み合わせる場合は、注意が必要です。Notes LDAP に格納されているユーザの属性が次のように設定されているとします。

```
mail=juser@example.com

cn=Joe User
```

```
uid=juser

cn=123456

location=New Jersey
```

LDAP ディレクトリに存在しないユーザであるにもかかわらず、Lotus はこのユーザへの電子メールを、指定されたアドレス以外の形式（たとえば Joe_User@example.com）であっても受け入れます。したがって、AsyncOS は、このユーザの有効なユーザ メール アドレスをすべて見つけることはできません。

この解決策の 1 つは、他の形式のアドレスのパブリッシュを試みるというものです。詳細については、Lotus Notes 管理者に問い合わせてください。

ルーティング：エイリアス拡張

AsyncOS では、エイリアス拡張（複数ターゲット アドレスへの LDAP ルーティング）がサポートされます。AsyncOS によって、元のメール メッセージはエイリアス ターゲットごとに別の新しいメッセージで置き換えられます（たとえば、recipient@yoursite.com へのメッセージは、newrecipient1@hotmail.com や recipient2@internal.yourcompany.com などへの、それぞれ独立したメッセージで置き換えられます）。ルーティング クエリは、他の電子メール処理システムではエイリアシング クエリと呼ばれることもあります。

ルーティング クエリの例

表 3-3　一般的な LDAP 実装での LDAP クエリー文字列の例：ルーティング

クエリの対象	別のメールホストへのルーティング
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory Address Book **Microsoft Exchange**	該当しない可能性あり[a]

Sun ONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

a.Active Directory の実装によっては、`proxyAddresses` 属性のエントリが複数存在することがありますが、この属性の値は Active Directory によって `smtp:user@domain.com` という形式で格納されるため、このデータは LDAP ルーティング/エイリアス拡張には使用できません。ターゲット アドレスはそれぞれ別の `attribute:value` ペアに存在する必要があります。Microsoft Exchange 環境が同じインフラストラクチャ内に複数あり、互いを認識している場合は、Exchange 環境の間でメールをルーティングするときに、送信元 MTA に戻る方向のルートは通常は必要ありません。

ルーティング：MAILHOST と MAILROUTINGADDRESS

ルーティング クエリの場合は、MAILHOST の値は IP アドレスではなく、解決可能なホスト名であることが必要です。これには、内部的な DNSconfig が必要になるのが一般的です。

MAILHOST は、ルーティング クエリでは省略可能です。MAILROUTINGADDRESS は、MAILHOST が設定されていない場合は必須です。

マスカレード

マスカレードとは、電子メールのエンベロープ送信者(「送信者」または「MAIL FROM」と呼ばれることもあります)および To:、From:、CC: の各ヘッダーを、定義済みのクエリに基づいて書き換える機能です。この機能の一般的な実装例の 1 つが「仮想ドメイン」であり、これによって複数のドメインを 1 つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワーク インフラストラクチャを「隠す」ために、電子メール ヘッダーの文字列からサブドメインを取り除く(「ストリッピング」)というものがあります。

マスカレード クエリの例

表 3-4　一般的な LDAP 実装での LDAP クエリ文字列の例: マスカレード

クエリの対象	マスカレード
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory Address Book	`(proxyaddresses=smtp:{a})`

Sun ONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

「フレンドリ名」のマスカレード

ユーザ環境によっては、LDAP ディレクトリ サーバ スキーマの中に、メール ルーティング アドレスやローカル メール アドレス以外に「フレンドリ名」が含まれていることがあります。AsyncOS では、エンベロープ送信者(発信メールの場合)やメッセージ ヘッダー(受信メールの場合、To:、Reply To:、From:、CC: など)を、この「フレンドリ名」でマスカレードできます。フレンドリ アドレスには、有効な電子メール アドレスでは通常は許可されない特殊文字(引用符、スペース、カンマなど)が含まれていてもかまいません。

LDAP クエリ経由でヘッダーをマスカレードするときに、フレンドリ メール文字列全体を LDAP サーバからの結果で置き換えるかどうかを設定時に選択できます。この動作がイネーブルになっていても、エンベロープ送信者には user@domain 部分のみが使用されることに注意してください(フレンドリ名はルールに反するため)。

標準的な LDAP マスカレードのときと同様に、LDAP クエリの結果が空(長さが 0 またはすべてホワイト スペース)の場合は、マスカレードは行われません。

この機能をイネーブルにするには、LDAP ベースのマスカレード クエリをリスナーに対して設定するときに([LDAP] ページまたは `ldapconfig` コマンド)、次の質問に対して「y」と回答します。

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

たとえば、次のような LDAP エントリがあるとします。

属性	値
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com,” <joe.smith\@example.com>

この機能がイネーブルになっている場合に、LDAP クエリが (mailRoutingAddress={a}) で、マスカレード属性が (mailLocalAddress) ならば、次のように置き換えられます。

元のアドレス（From、To、CC、Reply-to）	マスカレードされたヘッダー	マスカレードされたエンベロープ送信者
admin@example.com	From: “Administrator for example.com,” <joe.smith@example.com>	MAIL FROM: <joe.smith@example.com>

グループ LDAP クエリー

LDAP ディレクトリ内で定義されたグループに受信者が属しているかどうかを、LDAP サーバに対するクエリを使用して判別できます。

LDAP グループ クエリーの設定は、次の 3 つのステップで行います。

ステップ 1　メッセージに `rcpt-to-group` または `mail-from-group` ルールを適用するメッセージ フィルタを作成します。

ステップ 2　次に、[システム管理（System Administration）] > [LDAP] ページ（または `ldapconfig` コマンド）を使用して、アプライアンスのバインド先となる LDAP サーバを定義し、グループ メンバーシップを調べるクエリを設定します。

ステップ 3　[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または `listenerconfig -> edit -> ldapgroup` サブコマンド）を使用して、このグループ クエリをリスナーに対してイネーブルにします。

グループ クエリの例

表 3-5　一般的な LDAP 実装での LDAP クエリ文字列の例：グループ

クエリの対象	グループ
OpenLDAP	OpenLDAP では、`memberOf` 属性はデフォルトではサポートされません。LDAP 管理者によって、この属性または類似の属性がスキーマに追加されていることがあります。
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
Sun ONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

たとえば、LDAP ディレクトリで「マーケティング」グループのメンバーが `ou=Marketing` と分類されているとします。この分類を使用して、このグループが送受信するメールを特別な方法で取り扱うことができます。ステップ 1 で、メッセージに作用するメッセージ フィルタを作成し、ステップ 2 と 3 で LDAP ルックアップ メカニズムを有効にします。

グループ クエリの設定

次に示す例では、マーケティング グループ（LDAP グループ「Marketing」として定義）のメンバーからのメールを代替メール配信ホスト marketingfolks.example.com に配信します。

ステップ 1　初めに、グループ メンバーシップに関して肯定的に一致するメッセージに作用する、メッセージ フィルタを作成します。この例では、作成するフィルタの中で mail-from-group ルールを使用します。メッセージのうち、エンベロープ送信者が LDAP グループ「marketing-group1」に属していることが判明したものはすべて、代替配信ホストに送信されます（フィルタの alt-mailhost アクション）。

グループ メンバーシップ フィールド変数（groupName）は、ステップ 2 で定義します。グループ属性「groupName」の値は、marketing-group1 と定義されます。

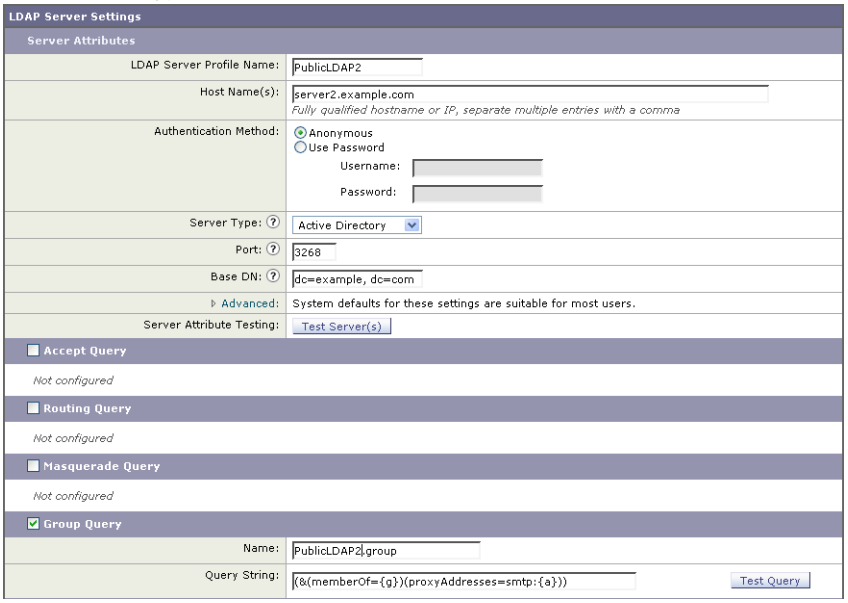
```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new


Enter filter script.  Enter '.' on its own line to end.

MarketingGroupfilter:

  if (mail-from-group == "marketing-group1") {

      alt-mailhost ('marketingfolks.example.com');}

.

1 filters added.


Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.
```

```
- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

メッセージ フィルタ ルール mail-from-group と rcpt-to-group の詳細については、メッセージ フィルタ ルール (6-2 ページ) を参照してください。

ステップ 2　次に、[LDAP サーバプロファイルを追加(Add LDAP Server Profile)] ページを使用して、アプライアンスのバインド先となる LDAP サーバを定義し、グループ メンバーシップを調べる最初のクエリを定義します。

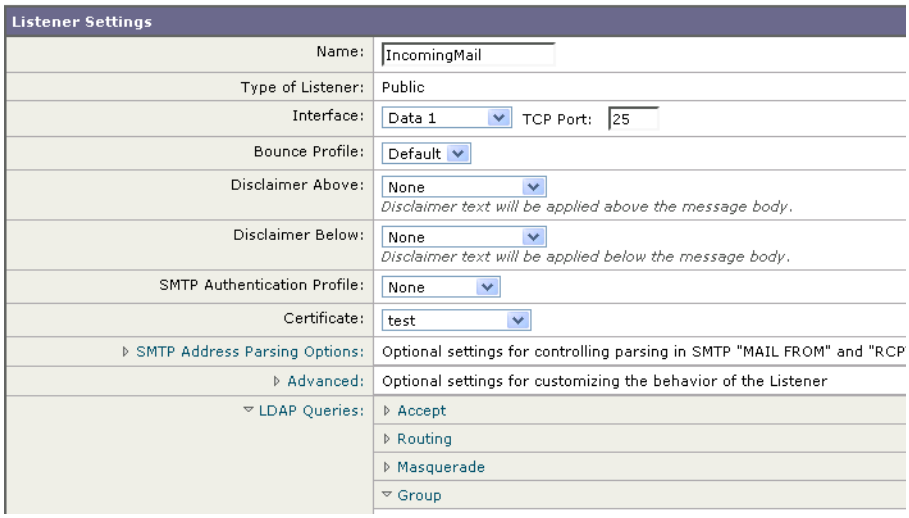
図 3-8　新しい LDAP プロファイルとグループ クエリーの追加



ステップ 3　次に、パブリック リスナー「InboundMail」で LDAP クエリを使用してグループ ルーティングを行うように更新します。[リスナーを編集(Edit Listener)] ページを使用して、前のステップで指定した LDAP クエリをイネーブルにします。

このクエリが実行されると、リスナーが受け入れたメッセージによって LDAP サーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。PublicLDAP2.group クエリはすでに、[システム管理(System Administration)] > [LDAP] ページで定義されています。

図 3-9　　リスナーでのグループ クエリの指定



この例では、変更を有効にするには commit が必要であることに注意してください。

例:グループ クエリを使用してスパムとウイルスのチェックをスキップする

メッセージ フィルタはパイプラインの初めの方で実行されるので、グループ クエリを使用すると、特定のグループについてウイルスとスパムのチェックをスキップできます。たとえば、社内の IT グループへのメッセージについては、スパムとウイルスのチェックをスキップしてすべて受信したいという要望があるとします。LDAP レコードの中に、DN をグループ名として使用するグループ エントリを作成します。このグループ名は、次の DN エントリで構成されます。

cn=IT, ou=groups, o=sample.com

LDAP サーバ プロファイルを作成し、次のグループ クエリを指定します。

(&(memberOf={g})(proxyAddresses=smtp:{a}))

次に、このクエリをリスナーに対してイネーブルにします。これで、メッセージがそのリスナーで受信されたときに、このグループ クエリがトリガーされます。

IT グループのメンバーについてはウイルスとスパムのチェックをスキップするために、次のメッセージ フィルタを作成して、着信メッセージを LDAP グループと比較して検査します。

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new



Enter filter script. Enter '.' on its own line to end.

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){
```

```
skip-spamcheck();

skip-viruscheck();

deliver();

}

.

1 filters added.
```

（注）　このメッセージ フィルタ内の rcpt-to-group には、グループ名として入力された DN（cn=IT, ou=groups, o=sample.com）が反映されています。メッセージ フィルタ内で使用しているグループ名が正しいことを確認してください。フィルタの実行時に、LDAP ディレクトリ内でその名前との比較が確実に行われるようにするためです。

リスナーが受け入れたメッセージによって LDAP サーバに対するクエリがトリガーされて、グループ メンバーシップが特定されます。メッセージ受信者が IT グループのメンバーの場合は、メッセージ フィルタの定義に従ってウイルスとスパムのチェックがいずれもスキップされて、メッセージが受信者に配信されます。フィルタで LDAP クエリの結果をチェックするには、LDAP サーバに対する LDAP クエリを作成し、その LDAP クエリをリスナーに対してイネーブルにする必要があります。

ドメインベース クエリー

ドメインベース クエリとは、LDAP クエリをタイプ別にグループ化し、特定のドメインに関連付けたうえで、特定のリスナーに割り当てたものです。ドメインベース クエリが使用されるのは、複数の LDAP サーバがそれぞれ異なるドメインに関連付けられているが、すべての LDAP サーバに対するクエリを同じリスナー上で実行する場合です。たとえば、「Bigfish」という会社が「Redfish」と「Bluefish」の 2 社を買収するとします。Bigfish は自社のドメイン Bigfish.com に加えて Redfish.com および Bluefish.com のドメインを保持し、ドメインごとに別の LDAP サーバを運用して、各ドメインに関連付けられた従業員の情報を格納します。この 3 つのドメインのメールをすべて受け入れるために、Bigfish はドメインベース クエリーを作成します。これで、Bigfish は Bigfish.com、Redfish.com、および Bluefish.com のメールを同じリスナー上で受け入れることができます。

ドメインベース クエリーを設定するには、次の手順を実行します。

ステップ 1　ドメインベース クエリで使用するドメインごとに 1 つずつ、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれに対して、ドメインベース クエリに使用するクエリを設定します（受け入れ、ルーティングなど）。詳細については、LDAP サーバ プロファイルの作成（3-5 ページ）を参照してください。

ステップ 2　ドメインベース クエリを作成します。ドメインベース クエリーを作成するときは、各サーバ プロファイルからクエリーを選択します。また、どのクエリーを実行するかを Envelope To フィールドに基づいて決定するように、Cisco IronPort アプライアンスを設定します。クエリーの作成方法の詳細については、ドメインベース クエリーの作成（3-28 ページ）を参照してください。

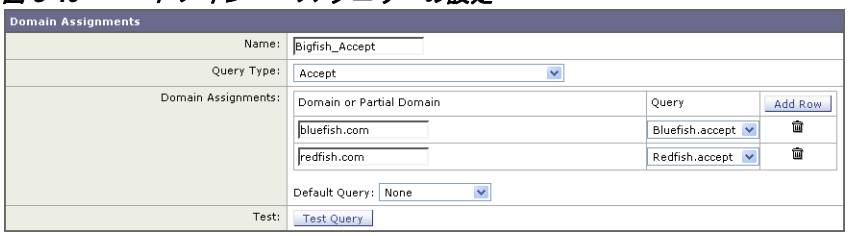
ステップ 3　ドメインベース クエリをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」を参照してください。

（注）　ドメインベース クエリーは他にも、Cisco IronPort スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Cisco IronPort スパム隔離機能の設定」を参照してください。

ドメインベース クエリーの作成

ドメインベース クエリは、[システム管理（System Administration）] > [LDAP] > [LDAP サーバプロファイル（LDAP Server Profiles）] ページで作成します。

図 3-10　　ドメインベース クエリーの設定



ステップ 1　[LDAP サーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2　[ドメイン割り当ての追加（Add Domain Assignments）] をクリックします。

ステップ 3　[Domain Assignments] ページが表示されます。

ステップ 4　ドメインベース クエリの名前を入力します。

ステップ 5　クエリのタイプを選択します。

（注）　ドメインベース クエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリー タイプを選択すると、Cisco IronPort アプライアンスはそのタイプのクエリーを利用可能なサーバ プロファイルから取得し、クエリー フィールドを生成します。

ステップ 6　[ドメイン割り当て（Domain Assignments）] フィールドに、ドメインを入力します。

ステップ 7　このドメインに関連付けるクエリを選択します。

ステップ 8　クエリのドメインがすべて追加されるまで、行を追加します。

ステップ 9　どのクエリにも一致しないときに実行する、デフォルトのクエリを入力できます。デフォルト クエリーを入力しない場合は、[なし（None）] を選択します。

ステップ 10　クエリーをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスワードまたは電子メール アドレスを [テストパラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 11　（省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注）　ドメインベース クエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 12　変更を送信し、保存します。

チェーン クエリ

チェーン クエリーは、Cisco IronPort アプライアンスによって順番に実行が試行される一連の LDAP クエリーで構成されます。Cisco IronPort アプライアンスは、この「チェーン」の中の各クエリの実行を試行し、LDAP サーバから肯定的なレスポンスが返されると（または「チェーン」の最後のクエリで否定的なレスポンスが返されるか失敗すると）実行を停止します。チェーン クエリが役立つのは、LDAP ディレクトリ内のエントリにおいて、さまざまな属性に類似の（または同一の）値が格納されている場合です。たとえば、属性 `maillocaladdress` と `mail` がユーザ電子メール アドレスを格納するために使用されているとします。この両方の属性に対して確実にクエリを実行するには、チェーン クエリを使用します。

チェーン クエリーを設定するには、次の手順を実行します。

ステップ 1　チェーン クエリ内で使用するクエリごとに、サーバ プロファイルを作成します。このサーバ プロファイルのそれぞれについて、チェーン クエリーに使用するクエリーを設定します。詳細については、LDAP サーバ プロファイルの作成（3-5 ページ）を参照してください。

ステップ 2　チェーン クエリを作成します。詳細については、チェーン クエリの作成（3-29 ページ）を参照してください。

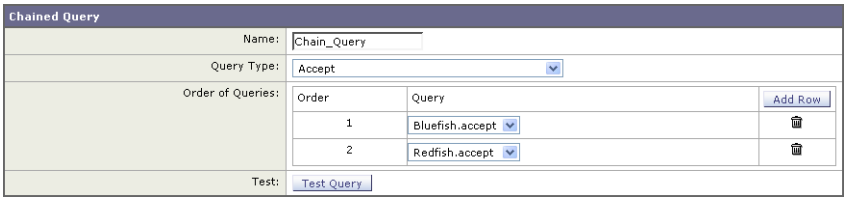
ステップ 3　チェーン クエリをパブリックまたはプライベートのリスナーに対してイネーブルにします。リスナーの設定方法の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」を参照してください。

（注）　ドメインベース クエリーは他にも、Cisco IronPort スパム隔離機能の LDAP エンドユーザ アクセスやスパム通知のために使用できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Cisco IronPort スパム隔離機能の設定」を参照してください。

チェーン クエリの作成

チェーン クエリは、[システム管理（System Administration）] > [LDAP] > [LDAP サーバプロファイル（LDAP Server Profiles）] ページで作成します。

図 3-11　　チェーン クエリーの設定



ステップ 1　[LDAP サーバプロファイル（LDAP Server Profiles）] ページの [詳細設定（Advanced）] をクリックします。

ステップ 2　[チェーン クエリを追加（Add Chain Query）] をクリックします。

[Chain query] ページが表示されます。

ステップ 3　チェーン クエリの名前を入力します。

ステップ 4　クエリー タイプを選択します。

チェーン クエリを作成するときに選択するクエリのタイプは、すべて同じでなければなりません。クエリー タイプを選択すると、Cisco IronPort アプライアンスはそのタイプのクエリーを利用可能なサーバ プロファイルから取得し、クエリー フィールドを生成します。

ステップ 5　チェーン クエリに追加するクエリを選択します。

Cisco IronPort アプライアンスによって、ここで設定した順にクエリーが実行されます。したがって、複数のクエリをチェーン クエリに追加する場合は、より限定的なクエリの後でより汎用のクエリが実行されるような順序にすることを推奨します。

ステップ 6　クエリーをテストします。[クエリのテスト（Test Query）] ボタンをクリックし、テストするユーザ ログインとパスワードまたは電子メール アドレスを [テストパラメータ（Test Parameters）] のフィールドに入力します。結果が [接続ステータス（Connection Status）] フィールドに表示されます。

ステップ 7　（省略可能）{f} トークンを受け入れクエリ内で使用する場合は、エンベロープ送信者アドレスをテスト クエリに追加できます。

（注）　チェーン クエリの作成が終了したら、このクエリをパブリックまたはプライベートのリスナーに関連付ける必要があります。

ステップ 8　変更を送信し、保存します。

LDAP によるディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃は、悪意のある送信者が、よくある名前を持つ受信者宛にメッセージを送信することによって開始します。電子メール ゲートウェイは、受信者がその場所に有効なメールボックスを持っているかどうかを調べて応答を返します。これを大量に実行すると、悪意のある送信者は、どのアドレスにスパムを送信すればよいかを、有効なアドレスの「収穫（ハーベスト）」によって特定できるようになります。

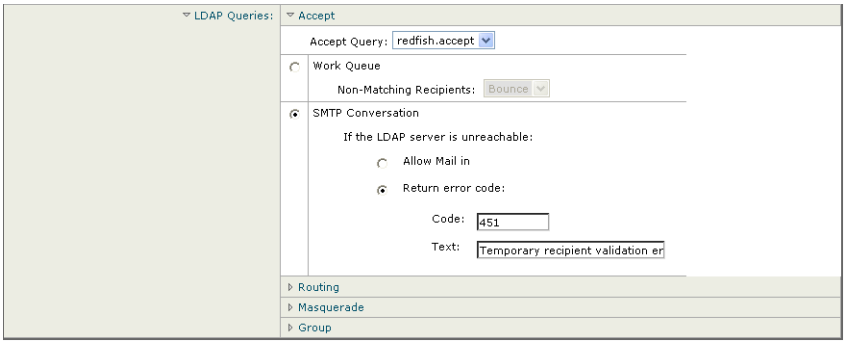
Cisco IronPort 電子メール セキュリティ アプライアンスでは、LDAP 受け入れ検証クエリーを使用すると、Directory Harvest Attack（DHA; ディレクトリ ハーベスト攻撃）を検出して防止できます。LDAP 受け入れを設定するときに、ディレクトリ ハーベスト攻撃防止を SMTP カンバセーション中に行うか、ワーク キューの中で行うかを選択できます。

SMTP カンバセーション中のディレクトリ ハーベスト攻撃防止

DHA を防止するには、ドメインだけを Recipient Access Table（RAT; 受信者アクセス テーブル）に入力しておき、LDAP 受け入れ検証を SMTP カンバセーション内で実行します。

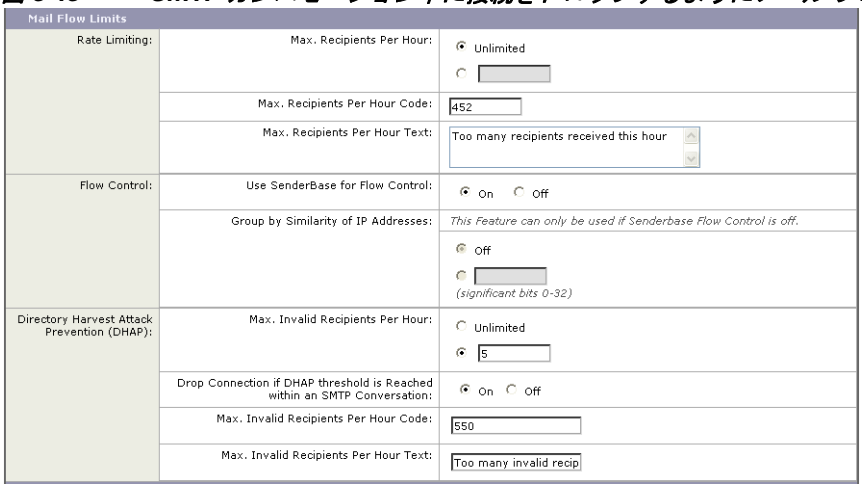
SMTP カンバセーション中にメッセージをドロップするには、LDAP 受け入れのための LDAP サーバ プロファイルを設定します。次に、LDAP 受け入れクエリを SMTP カンバセーション中に実行するようにリスナーを設定します。

図 3-12　受け入れクエリを SMTP カンバセーション中に実行するように設定



リスナーで実行する LDAP 受け入れクエリを設定したら、そのリスナーに関連付けられたメール フロー ポリシーの中の DHAP（ディレクトリ ハーベスト攻撃防止）設定を指定する必要があります。

図 3-13　SMTP カンバセーション中に接続をドロップするようにメール フロー ポリシーを設定する



リスナーに関連付けられたメール フロー ポリシーの中で、ディレクトリ ハーベスト攻撃防止のための次の項目を設定します。

- [1 時間あたりの無効な受信者の最大数（Max. Invalid Recipients Per hour）]。このリスナーがリモート ホストから受け取る無効な受信者の 1 時間あたりの最大数です。このしきい値は、RAT 拒否の総数を表します。これは、無効な LDAP 受信者宛てのため SMTP カンバセーション中にドロップされたメッセージの総数と、ワーク キュー内でバウンスされたメッセージの合計です。たとえば、しきい値を 5 と設定した場合に、検出された RAT 拒否が 2 件で、無効な LDAP 受信者宛てのためドロップされたメッセージが 3 件であるとします。この時点で、Cisco IronPort アプライアンスはしきい値に到達したと判断して、接続をドロップさせます。デフォルトでは、パブリック リスナーでの 1 時間あたりの受信者の最大数は 25 です。プライベート リスナーの場合は、1 時間あたりの受信者の最大数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。
- [SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Drop Connection if DHAP Threshold is reached within an SMTP conversation）]。ディレクトリ ハーベスト攻撃防止のしきい値に達したときに Cisco IronPort アプライアンスによって接続をドロップさせる設定をします。
- [時間コードあたりの最大受信者数（Max. Recipients Per Hour Code）]。接続をドロップするときに使用するコードを指定します。デフォルトのコードは 550 です。

- [時間テキストあたりの最大受信者数(Max. Recipients Per Hour Text)]。ドロップした接続に対して使用するテキストを指定します。デフォルトのテキストは「Too many invalid recipients」です。

しきい値に達した場合は、受信者が無効であってもメッセージのエンベロープ送信者にバウンス メッセージが送信されることはありません。

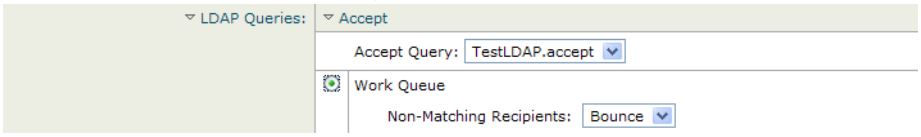
作業キュー内でのディレクトリ ハーベスト攻撃防止

ディレクトリ ハーベスト攻撃(DHA)のほとんどは、ドメインだけを受信者アクセス テーブル(RAT)に入力しておき、LDAP 受け入れ検証をワーク キュー内で実行することによって防止できます。この方法を使用すると、悪意のある送信者が、受信者が有効かどうかを SMTP カンバセーション中に知ることはできなくなります。(受け入れクエリが設定されているときは、システムはメッセージを受け入れて、LDAP 受け入れ検証をワーク キュー内で実行します)。ただし、メッセージのエンベロープ送信者には、受信者が無効である場合にバウンス メッセージが送信されます。

ワーク キュー内でディレクトリ ハーベスト攻撃防止するための設定

ディレクトリ ハーベスト攻撃を防止するには、初めに LDAP サーバ プロファイルを設定して LDAP 受け入れをイネーブルにします。LDAP 受け入れクエリをイネーブルにしたら、次のように、その受け入れクエリを使用するようにリスナーを設定すると共に、受信者が一致しない場合はメールをバウンスするように指定します。

図 3-14　受信者が一致しない場合はメッセージをバウンスするように受け入れクエリを設定



次に、メール フロー ポリシーを設定します。このポリシーでは、所定の時間内に送信 IP アドレスあたりどれだけの無効な受信者アドレスをシステムが受け入れるかを定義します。この数を超えると、システムはこの状態が DHA(ディレクトリ ハーベスト攻撃)であると判断してアラート メッセージを送信します。このアラート メッセージに含まれる情報は次のとおりです。

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name'),
dhap_limit=n, sender_group=sender_group,

listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name', 1),
sender=envelope_sender, rcpt=envelope_recipients
```

メール フロー ポリシーで指定されたしきい値に達するまでは、システムによってメッセージがバウンスされますが、それ以降は応答を返すことなく受け入れられてドロップされます。したがって、正当な送信者にはアドレスの誤りが通知されますが、悪意のある送信者は、どの受信者が受け入れられたかを判断できません。

この無効受信者カウンタの働きは、現在 AsyncOS に実装されているレート制限機能に似ています。つまり、管理者がこの機能をイネーブルにして、上限値をパブリック リスナーの HAT 内のメール フロー ポリシーの中で設定します(HAT のデフォルトのメール フロー ポリシーを含む)。

たとえば、パブリック リスナーの HAT 内のメール フロー ポリシーを CLI で作成または編集するときは、次のような質問が表示されます（listenerconfig -> edit -> hostaccess -> default | new コマンドを実行）。

```
Do you want to enable Directory Harvest Attack Prevention per host? [Y]> y


Enter the maximum number of invalid recipients per hour from a remote host.

[25]>
```

この機能は、メール フロー ポリシーを GUI で編集するときにも表示されます（対応するリスナーに対して LDAP クエリが作成済みの場合）。

図 3-15　GUI の DHAP 防止機能

1 時間あたりの無効受信者数を入力すると、そのメール フロー ポリシーに対して DHAP（ディレクトリ ハーベスト攻撃防止）がイネーブルになります。デフォルトで、パブリック リスナーでは 1 時間あたり最大 25 件の無効受信者が受け入れられます。プライベート リスナーの場合は、1 時間あたりの無効受信者数はデフォルトでは無制限です。この最大数を [無制限（Unlimited）] に設定すると、そのメール フロー ポリシーに対して DHAP はイネーブルになりません。

SMTP 認証を行うための AsyncOS の設定

AsyncOS では、SMTP 認証がサポートされています。SMTP Auth は、SMTP サーバに接続するクライアントを認証するメカニズムです。

このメカニズムを利用すると、特定の組織に所属するユーザが、その組織のメール サーバにリモートで接続している（自宅や出張先などから）ときもメール サーバを使用してメールを送信できるようになります。メール ユーザ エージェント（MUA）は、メールの送信を試行するときに認証要求（チャレンジ/レスポンス）を発行できます。

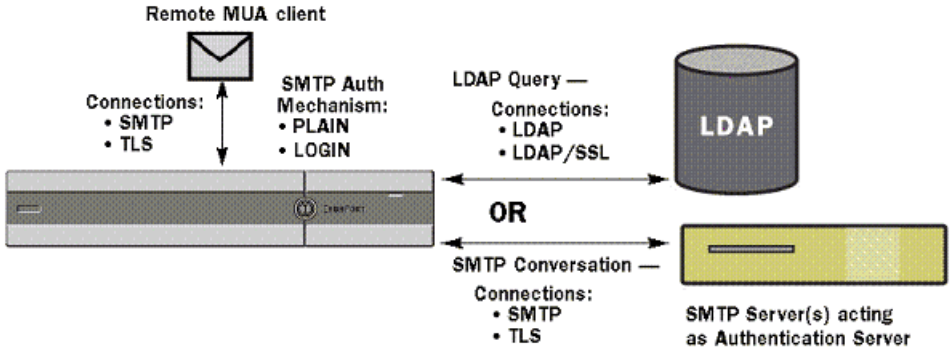
SMTP 認証は、発信メール リレーに対しても使用できます。これを利用すると、Cisco IronPort アプライアンスがネットワークのエッジではない場合に、アプライアンスからリレー サーバへのセキュア接続を確立できます。

AsyncOS は RFC 2554 に準拠しており、この中で SMTP カンバセーション内で認証コマンドを実行する方法、ネゴシエーションへのレスポンス、および生成するエラー コードが規定されています。

AsyncOS では、ユーザ クレデンシャルの認証方式として次の 2 つがサポートされています。

- LDAP ディレクトリを使用する。
- 別の SMTP サーバを使用する（SMTP Auth 転送と SMTP Auth 発信）。

図 3-16　SMTP Auth のサポート：LDAP ディレクトリ ストアまたは SMTP サーバ



SMTP 認証方式を設定したら、HAT メール フロー ポリシー内で使用される SMTP Auth プロファイルを、`smtpauthconfig` コマンドを使用して作成します（リスナーでの SMTP 認証のイネーブル化（3-38 ページ）を参照）。

SMTP 認証の設定

LDAP サーバを使用して認証を行う場合は、[LDAP サーバプロファイルを追加（Add LDAP Server Profile）] または [LDAP サーバプロファイルを編集（Edit LDAP Server Profile）] ページ（または `ldapconfig` コマンド）でクエリ タイプとして SMTPAUTH を選択して SMTP 認証クエリを作成します。設定する LDAP サーバのそれぞれについて、SMTP 認証プロファイルとして使用する SMTPAUTH クエリを 1 つ設定できます。

SMTP 認証クエリには、「LDAP バインド」と「属性としてのパスワード」の 2 種類があります。「パスワードを属性として取得」を使用するときは、Cisco IronPort アプライアンスによって LDAP ディレクトリ内のパスワード フィールドが取り出されます。このパスワードは、プレーン テキストでも、暗号化またはハッシュ化済みで格納されていてもかまいません。LDAP バインドを使用するときは、Cisco IronPort アプライアンスはクライアントが指定したクレデンシャルを使用して LDAP サーバへのログインを試行します。

パスワードを属性として指定

OpenLDAP の規定（RFC 2307 に基づく）では、コーディングのタイプを中カッコで囲み、その後にエンコードされたパスワードを続けることになっています（たとえば「{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=」）。この例では、パスワード部分はプレーン テキストのパスワードに SHA を適用してから base64 エンコーディングしたものです。

Cisco IronPort アプライアンスがパスワードを取得する前に、SASL メカニズムのネゴシエートが MUA との間で行われ、アプライアンスと MUA はどの方法を使用するかを決定します（サポートされているメカニズムは LOGIN、PLAIN、MD5、SHA、SSHA、CRYPT SASL です）。その後で、アプライアンスは LDAP データベースに対するクエリを実行してパスワードを取得します。LDAP 内では、中カッコで囲まれたプレフィックスがパスワードに付いていることがあります。

- プレフィックスが付いていない場合は、LDAP 内に格納されているパスワードがプレーン テキストであると見なされます。
- プレフィックスが付いている場合は、アプライアンスはそのハッシュ化パスワードを取得し、MUA によって指定されたユーザ名とパスワードの両方あるいはどちらかのハッシュを実行して、ハッシュ後のパスワードと比較します。Cisco IronPort アプライアンスでサポートされるハッシュ タイプは SHA1 と MD5 であり、RFC 2307 の規定に基づいて、パスワード フィールド内ではハッシュ化パスワードの前にハッシュ メカニズムのタイプが付加されます。

- LDAP サーバの中には、OpenWave LDAP サーバのように、暗号化されたパスワードの前に暗号化タイプを付加しないものもあり、代わりに暗号化タイプが別の LDAP 属性として格納されています。このような場合は、管理者が指定したデフォルトの SMTP AUTH 暗号化方式であると見なされて、そのパスワードと SMTP カンバセーションで取得されたパスワードとが比較されます。

Cisco IronPort アプライアンスは、SMTP Auth 交換から任意ユーザ名を受け取って LDAP クエリーに変換し、このクエリーを使用してクリア テキストまたはハッシュ化されたパスワード フィールドを取得します。次に、SMTP Auth クレデンシャルで指定されたパスワードに対してハッシュが必要な場合は実行し、その結果を LDAP からのパスワードと比較します（ハッシュ タイプのタグがある場合は取り除く）。一致した場合は、SMTP Auth カンバセーションが続行されます。一致しない場合は、エラー コードが返されます。

SMTP 認証クエリの設定

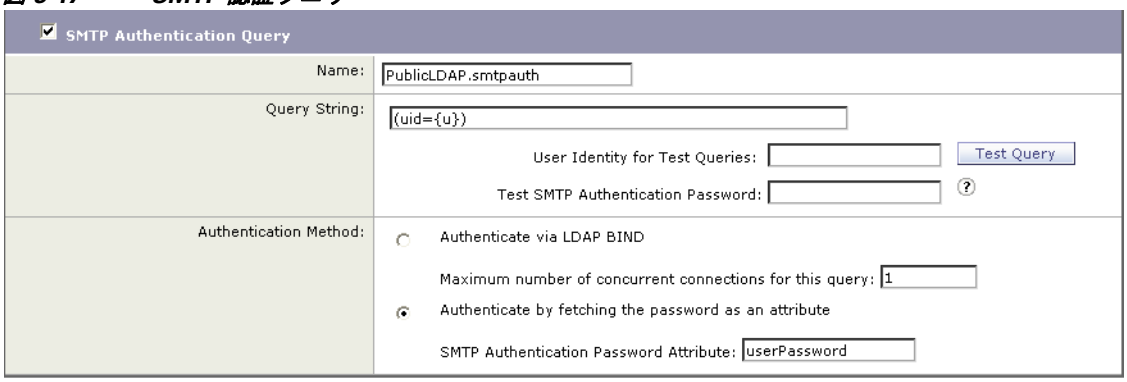
SMTP 認証クエリーを設定するときは、次の情報を指定します。

表 3-6　SMTP Auth LDAP クエリのフィールド

名前	クエリの名前
クエリー文字列（Query String）	認証を LDAP バインド経由で行うか、パスワードを属性として取得して行うかを選択できます。 [バインド（Bind）]：LDAP サーバへのログイン試行には、クライアントによって指定されたクレデンシャルを使用します（これを「LDAP バインド」と呼びます）。 SMTP Auth クエリで使用される同時接続の最大数を指定します。この数は、上の LDAP サーバ属性で指定した数を超えてはなりません。バインド認証時に大量のセッション タイムアウトが発生するのを防ぐには、ここで指定する同時接続の最大数を大きくします（一般的には、接続のほぼすべてを SMTP Auth に割り当てることができます）。バインド認証ごとに、新しい接続が 1 つ使用されます。残りの接続は、他のタイプの LDAP クエリで共有されます。 [属性としてのパスワード（Password as Attribute）]：パスワードを取得して認証を行うには、下の [SMTP Auth パスワード属性（SMTP Auth password attribute）] フィールドでパスワードを指定します。 選択した種類の認証に使用する LDAP クエリを指定します。 Active Directory のクエリの例： `(&(samaccountname={u})(objectCategory=person)(objectClass=user))`
SMTP 認証のパスワードの属性（SMTP Auth Password Attribute）	[属性としてパスワード取得した認証（Authenticate by fetching the password as an attribute）] を選択した場合は、パスワード属性をここで指定します。

次の例では、[システム管理（System Administration）] > [LDAP] ページを使用して LDAP 設定「PublicLDAP」を編集し、SMTPAUTH クエリを追加しています。クエリ文字列（`uid={u}`）は、userPassword 属性と比較するように作成されています。

図 3-17　SMTP 認証クエリ



SMTPAUTH プロファイルの設定が完了すると、そのクエリを SMTP 認証に使用するようにリスナーを設定できます。

第 2 の SMTP サーバ経由での SMTP 認証（転送を使用する SMTP Auth）

SMTP 認証カンバセーションのために指定されたユーザ名とパスワードを、別の SMTP サーバを使用して検証するようにアプライアンスを設定できます。

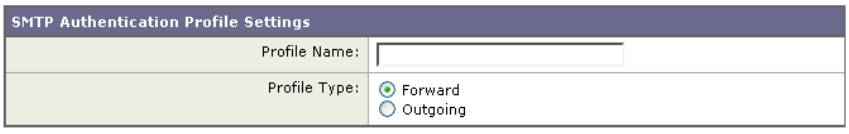
認証を行うサーバは、メールを転送するサーバとは別のものであり、SMTP 認証要求への応答だけを行います。認証に成功したときは、専用メール サーバによるメールの SMTP 転送を続行できます。この機能は、「転送を使用する SMTP Auth」と呼ばれることもあります。クレデンシャルのみが別の SMTP サーバに転送（プロキシ）されて認証が行われるからです。

SMTP 認証転送プロファイルを作成するには、次の手順を実行します。

ステップ 1　[Network] > [SMTP Authentication] リンクをクリックします。[SMTP Authentication] ページが表示されます。

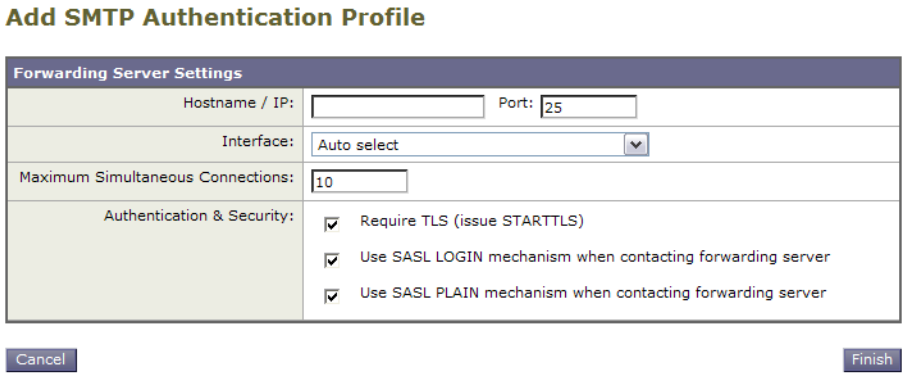
ステップ 2　[プロファイルの追加（Add Profile）] リンクをクリックします。[Add SMTP Authentication Profile: SMTP Authentication Profile Settings] ページが表示されます。SMTP 認証プロファイルの一意の名前を入力します。[プロファイルタイプ（Profile Type）] で [転送する（Forwarding）] を選択します。

図 3-18　転送 SMTP 認証プロファイルの選択



ステップ 3　[Next] ボタンをクリックします。[Add SMTP Authentication Profile: Forwarding Server Settings] ページが表示されます。

図 3-19　転送サーバ設定の追加



転送サーバのホスト名/IP アドレスとポートを入力します。認証要求の転送に使用する転送インターフェイスを選択します。同時接続の最大数を指定します。次に、アプライアンスから転送サーバへの接続に対して TLS を必須とするかどうかを設定します。使用する SASL メカニズムも、[プレーン（PLAIN）] と [ログイン（LOGIN）] から選択できます（使用できる場合）。この選択は、転送サーバごとに設定されます。

ステップ 4　変更を送信し、保存します。

認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証のイネーブル化（3-38 ページ）を参照してください。

LDAP を使用する SMTP 認証

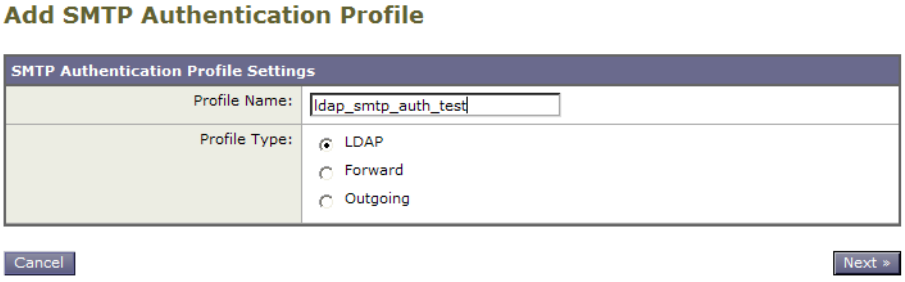
LDAP ベースの SMTP 認証プロファイルを作成するには、SMTP 認証クエリを LDAP サーバ プロファイルと共に [システム管理（System Administration）] > [LDAP] ページであらかじめ作成しておく必要があります。このプロファイルを使用して SMTP 認証プロファイルを作成します。LDAP プロファイルの作成方法の詳細については、LDAP クエリについて（3-2 ページ）を参照してください。

LDAP を使用する SMTP 認証プロファイルを設定するには、次の手順を実行します。

ステップ 1　[Network] > [SMTP Authentication] リンクをクリックします。[SMTP Authentication] ページが表示されます。

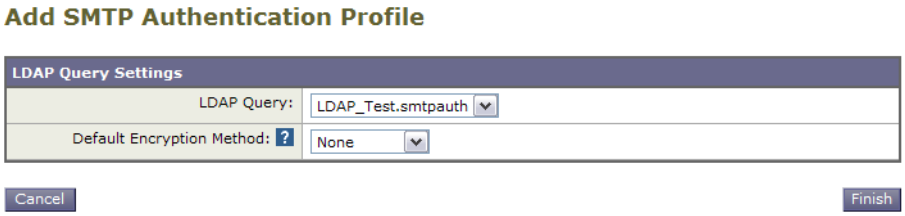
ステップ 2　[プロファイルの追加（Add Profile）] リンクをクリックします。[Add SMTP Authentication Profile: SMTP Authentication Profile Settings] ページが表示されます。SMTP 認証プロファイルの一意の名前を入力します。[プロファイルタイプ（Profile Type）] で [LDAP] を選択します。

図 3-20　LDAP SMTP 認証プロファイルの選択



ステップ 3　[Next] ボタンをクリックします。[Add SMTP Authentication Profile: LDAP Query Settings] ページが表示されます。

図 3-21　LDAP SMTP 認証プロファイルの LDAP クエリー設定の指定



ステップ 4　この認証プロファイルに使用する LDAP クエリを選択します。デフォルトの暗号化方式をドロップダウン メニューから選択します。選択肢には、[SHA]、[Salted SHA]、[Crypt]、[Plain]、[MD5] があります。LDAP サーバによって暗号化後のパスワードの前に暗号化タイプが付加される場合は、[なし（None）] を選択してください。LDAP サーバによって暗号化タイプが別エンティティとして保存される場合は（たとえば OpenWave LDAP サーバ）、暗号化方式をメニューから選択してください。デフォルトの暗号化設定は、LDAP クエリにバインドが使用される場合は使用されません。

ステップ 5　[終了（Finish）] ボタンをクリックします。

ステップ 6　[変更を確定（Commit Changes）] ボタンをクリックして必要に応じて任意のコメントを追加したら、[変更を確定（Commit Changes）] をクリックして LDAP SMTP 認証プロファイルの追加を終了します。

認証プロファイルの作成が完了すると、そのプロファイルをリスナーに対してイネーブルにできます。詳細については、リスナーでの SMTP 認証のイネーブル化（3-38 ページ）を参照してください。

リスナーでの SMTP 認証のイネーブル化

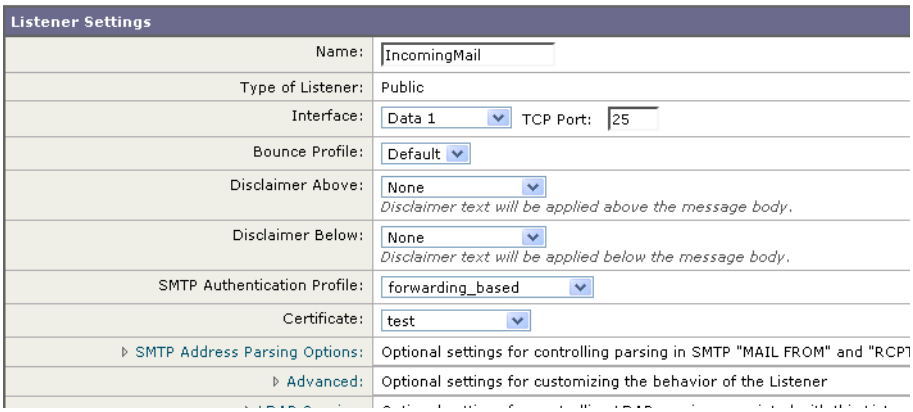
[ネットワーク（Network）] > [SMTP 認証（SMTP Authentication）] ページで、実行する認証のタイプ（LDAP ベースまたは SMTP 転送ベース）を指定して SMTP 認証「プロファイル」を作成したら、[ネットワーク（Network）] > [リスナー（Listeners）] ページ（または `listenerconfig` コマンド）を使用して、このプロファイルをリスナーに関連付ける必要があります。

（注）　認証済みのユーザには、ユーザのその時点のメール フロー ポリシーの中で RELAY 接続動作が許可されます。

（注）　1 つのプロファイル内で複数の転送サーバを指定することもできます。SASL メカニズム CRAM-MD5 と DIGEST-MD5 は、Cisco IronPort アプライアンスと転送サーバの間ではサポートされません。

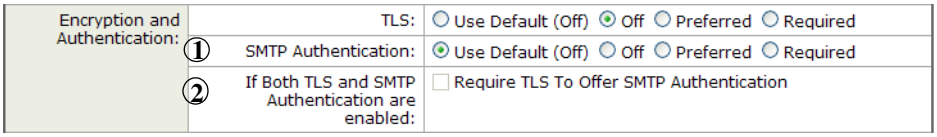
次の例では、リスナー「InboundMail」で SMTPAUTH プロファイルが使用されるように、[リスナーを編集（Edit Listener）] ページで設定しています。

図 3-22　SMTP 認証プロファイルを [リスナーを編集(Edit Listener)] ページで選択する



プロファイルを使用するようにリスナーを設定したら、そのリスナーでの SMTP 認証を許可、禁止、または必須とするようにホスト アクセス テーブルのデフォルト設定を変更できます。

図 3-23　メール フロー ポリシーでの SMTP 認証のイネーブル化



番号（Number）	説明
1.	[SMTP 認証(SMTP Authentication)] フィールドでは、リスナー レベルで SMTP 認証を制御します。[いいえ(No)] を選択した場合は、SMTP 認証に関する他の設定にかかわらず、このリスナーでは認証はイネーブルになりません。
2.	2 番めのプロンプト([SMTP 認証(SMTP Authentication)])で [必須(Required)] を選択した場合は、AUTH キーワードが発行されるのは TLS がネゴシエートされた(クライアントが別の EHLO コマンドを発行した)後となります。

SMTP 認証と HAT ポリシーの設定

送信者は送信者グループとしてまとめられ、その後で SMTP 認証ネゴシエーションが開始するので、ホスト アクセス テーブル(HAT)の設定には影響は及びません。リモート メール ホストが接続するときに、アプライアンスは初めにどの送信者グループが該当するかを特定して、その送信者グループのメール ポリシーを適用します。たとえば、リモート MTA「suspicious.com」が SUSPECTLIST という送信者グループに属している場合は、「suspicious.com」の SMTPAUTH ネゴシエーションの結果とは無関係に THROTTLE ポリシーが適用されます。

ただし、SMTPAUTH を使用して認証を受ける送信者の扱いは、「通常の」送信者とは異なります。SMTPAUTH セッションに成功した場合の接続動作は「RELAY」に変更されるので、実質的に受信者アクセス テーブル(RAT)と LDAPACCEPT はバイパスされます。その結果、送信者はメッセージを Cisco IronPort アプライアンス経由でリレーできます。したがって、適用されるレート制限やスロットリングがある場合は、引き続き有効になります。

HAT 遅延拒否

HAT 遅延拒否が設定済みのときは、HAT 送信者グループとメール フロー ポリシーの設定に基づいて本来ならばドロップされる接続も、認証に成功し、RELAY メール フロー ポリシーが許可されます。

遅延拒否を設定するには、CLI の `listenerconfig --> setup` コマンドを使用します。この動作は、デフォルトではディセーブルになっています。

次の表に、HAT の遅延拒否を設定する方法を説明します。

```
example.com> listenerconfig


Currently configured listeners:


1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private


Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.。

[]> setup


Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>


[...]


By default HAT rejected connections will be closed with a banner

message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y
```

```
Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y


Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551


Enter your custom SMTP response. Press Enter on a blank line to finish.


Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

発信 SMTP 認証

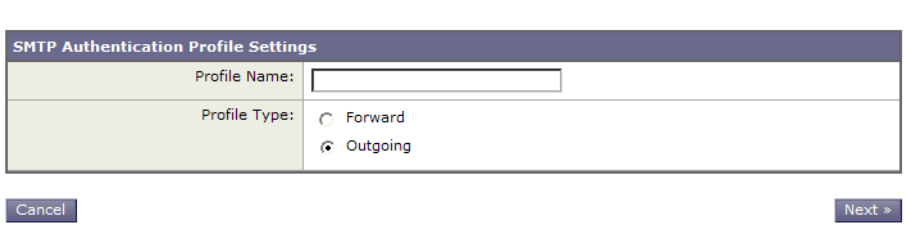
SMTP 認証は、発信メール リレーをユーザ名とパスワードを使用して検証するときにも使用できます。「発信」SMTP 認証プロファイルを作成してから、このプロファイルを全ドメインの SMTP ルートに関連付けます。メール配信試行のたびに、Cisco IronPort アプライアンスは必要なクレデンシャルを使用してアップストリーム メール リレーにログインします。PLAIN SASL フォーマットのログインのみがサポートされます。

SMTP 認証をすべての発信メールに使用するには、次の手順を実行します。

ステップ 1　[Network] > [SMTP Authentication] リンクをクリックします。[SMTP Authentication] ページが表示されます。

ステップ 2　[プロファイルの追加（Add Profile）] リンクをクリックします。[Add SMTP Authentication Profile: SMTP Authentication Profile Settings] ページが表示されます。SMTP 認証プロファイルの一意の名前を入力します。[プロファイルタイプ（Profile Type）] で [発信（Outgoing）] を選択します。[Next] ボタンをクリックします。

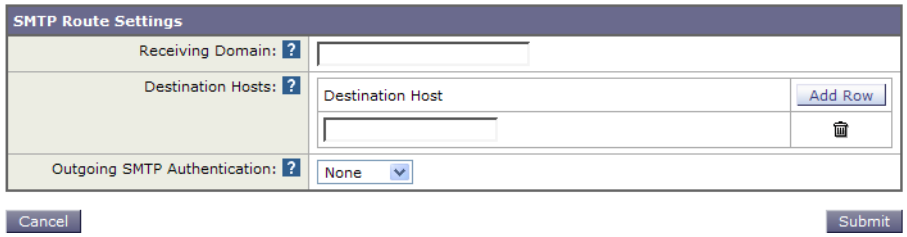
図 3-24　発信 SMTP 認証プロファイルの追加



認証プロファイルの認証用ユーザ名とパスワードを入力します。[終了（Finish）] ボタンをクリックします。[SMTP Authentication Profiles] ページに新しい発信プロファイルが表示されます。

ステップ 3　[Network] > [SMTP Routes] リンクをクリックします。[SMTP Routes] ページが表示されます。

図 3-25　発信 SMTP ルートの追加



ステップ 4　[All Other Domains] リンクをクリックします。[Edit SMTP Route] ページが表示されます。SMTP ルートの宛先ホストの名前を [宛先ホスト（Destination Host）] に入力します。これは、発信メールの配信に使用される外部メール リレーのホスト名です。

ステップ 5　発信 SMTP 認証プロファイルをドロップダウン メニューから選択します。[送信（Submit）] ボタンをクリックします。

ステップ 6　変更を保存します。

ロギングと SMTP 認証

SMTP 認証メカニズム（LDAP ベース、SMTP 転送サーバ ベース、または SMTP 発信）がアプライアンス上で設定されている場合は、以下のイベントが Cisco IronPort メール ログに記録されます。

- （情報）SMTP 認証成功：認証されたユーザと、使用されたメカニズムも記録されます。（プレーン テキストのパスワードが記録されることはありません）。
- （情報）SMTP 認証失敗：認証されたユーザと、使用されたメカニズムも記録されます。
- （警告）認証サーバに接続不可能：サーバ名とメカニズムも記録されます。
- （警告）タイムアウト イベント：転送サーバ（アップストリームの、インジェクションを行う Cisco IronPort アプライアンスと通信）が認証要求を待つ間にタイムアウトしたとき。

ユーザの外部認証の設定

ネットワーク上の LDAP ディレクトリを使用してユーザを認証するように Cisco IronPort アプライアンスを設定できます。このように設定すると、ユーザが各自の LDAP ユーザ名とパスワードを使用してログインできるようになります。LDAP サーバに対する認証クエリを設定したら、アプライアンスによる外部認証の使用をイネーブルにします（GUI の [システム管理（System Administration）] > [ユーザ（Users）] ページまたは CLI の `userconfig` コマンドを使用します）。

ユーザの外部認証を設定するには、次の手順を実行します。

ステップ 1　**ユーザ アカウントを検索するためのクエリーを作成します。**LDAP サーバ プロファイルで、LDAP ディレクトリ内のユーザ アカウントを検索するためのクエリを作成します。

ステップ 2　**グループ メンバーシップ クエリーを作成します。**ユーザが特定のディレクトリ グループのメンバーかどうかを判断するためのクエリを作成します。

ステップ 3　**LDAP サーバを使用するように外部認証をセットアップします。**この LDAP サーバをユーザ認証に使用するようにアプライアンスを設定し、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「ユーザの追加」を参照してください。

（注）　[LDAP] ページの [クエリのテスト（Test Query）] ボタン（または ldaptest コマンド）を使用して、クエリから返される結果が期待したとおりであることを確認します。詳細については、LDAP クエリのテスト（3-18 ページ）を参照してください。

ユーザ アカウント クエリ

外部ユーザを認証するために、AsyncOS はクエリを使用してそのユーザのレコードを LDAP ディレクトリ内で検索し、ユーザのフル ネームが格納されている属性を見つけます。選択したサーバ タイプに応じて、AsyncOS によってデフォルト クエリーとデフォルト属性が入力されます。アカウントが失効しているユーザは拒否するようにアプライアンスを設定することもできます。それには、RFC 2307 で規定されている属性が LDAP ユーザ レコード内で定義されている必要があります（shadowLastChange、shadowMax、および shadowExpire）。ユーザ レコードが存在するドメイン レベルのベース DN が必須です。

表 3-7 に、AsyncOS がユーザ アカウントを Active Directory サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 3-7　デフォルトのユーザ アカウント クエリ文字列と属性：Active Directory

サーバ タイプ（Server Type）	Active Directory
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=user)(sAMAccountName={u}))
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	displayName

表 3-8 に、AsyncOS がユーザ アカウントを OpenLDAP サーバ上で検索するときに使用されるデフォルトのクエリ文字列とユーザのフル ネーム属性を示します。

表 3-8　デフォルトのユーザ アカウント クエリ文字列と属性：OpenLDAP

サーバ タイプ（Server Type）	OpenLDAP
ベース DN	（ブランク）（ユーザ レコードを見つけるには具体的なベース DN を使用する必要があります）
クエリ文字列	(&(objectClass=posixAccount)(uid={u}))
ユーザのフル ネームが格納されている属性（Attribute containing the user's full name）	gecos

グループ メンバーシップ クエリ

AsyncOS は、ユーザが特定のディレクトリ グループのメンバーかどうかを判断するという目的でもクエリを使用します。ディレクトリ グループ メンバーシップ内のメンバーシップによって、そのユーザのシステム内のアクセス許可が決まります。GUI の [システム管理（System Administration）] > [ユーザ（Users）] ページ（または CLI の `userconfig`）で外部認証をイネーブルにするときに、ユーザ ロールを LDAP ディレクトリ内のグループに割り当てます。ユーザ ロールによって、そのユーザがシステム内で持つアクセス許可が決まります。外部認証されたユーザの場合は、ロールは個々のユーザではなくディレクトリ グループに割り当てられます。たとえば、IT というディレクトリ グループ内のユーザに Administrator ロールを割り当て、Support というディレクトリ グループのユーザに Help Desk User ロールを割り当てます。

1 人のユーザが複数の LDAP グループに属しており、それぞれユーザ ロールが異なる場合は、最も限定的なロールのアクセス許可が AsyncOS によってそのユーザに付与されます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

グループ メンバーシップを問い合わせるための LDAP プロファイルを設定するときに、グループ レコードが格納されているディレクトリ レベルのベース DN を入力し、グループ メンバーのユーザ名が格納されている属性と、グループ名が格納されている属性を入力します。LDAP サーバ プロファイルに対して選択されたサーバ タイプに基づいて、ユーザ名とグループ名の属性のデフォルト値とデフォルト クエリー文字列が AsyncOS によって入力されます。

（注） Active Directory サーバの場合は、ユーザが特定のグループのメンバーかどうかを判断するためのデフォルトのクエリ文字列は `(&(objectClass=group)(member={u}))` です。ただし、使用する LDAP スキーマにおいて、「memberof」のリストでユーザ名ではなく識別名が使用されている場合は、`{dn}` を `{u}` の代わりに使用できます。

表 3-9 に、AsyncOS が Active Directory サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリー文字列と属性を示します。

表 3-9　デフォルトのグループ メンバーシップ クエリ文字列と属性：Active Directory

サーバ タイプ（Server Type）	Active Directory
ベース DN	（ブランク）（グループ レコードを見つけるには具体的なベース DN を使用する必要があります）
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=group)(member={u}))` **（注）** 使用する LDAP スキーマにおいて `memberOf` リストの中でユーザ名ではなく識別名が使用されている場合は、`{u}` の代わりに `{dn}` を使用できます。
各メンバーのユーザ名（またはそのユーザのレコードの DN）が格納されている属性	`member`
グループ名が格納されている属性	`cn`

表 3-10 に、AsyncOS が OpenLDAP サーバ上でグループ メンバーシップ情報を検索するときに使用されるデフォルトのクエリ文字列と属性を示します。

表 3-10　デフォルトのグループ メンバーシップ クエリ文字列と属性:OpenLDAP

サーバ タイプ(Server Type)	OpenLDAP
ベース DN	(ブランク)(グループ レコードを見つけるには具体的なベース DN を使用する必要があります)
ユーザが特定のグループのメンバーかどうかを判断するためのクエリー文字列	`(&(objectClass=posixGroup)(memberUid={u}))`
各メンバーのユーザ名(またはそのユーザのレコードの DN)が格納されている属性	`memberUid`
グループ名が格納されている属性	`cn`

スパム検疫へのエンドユーザ認証のクエリー

スパム隔離へのエンドユーザ認証のクエリとは、ユーザが Cisco IronPort スパム隔離機能にログインするときにユーザを検証するためのクエリです。トークン {u} は、ユーザを示します(ユーザのログイン名を表します)。トークン {a} は、ユーザの電子メール アドレスを示します。LDAP クエリによって「SMTP:」が電子メール アドレスから除去されることはありません。ただし、AsyncOS はこの部分をアドレスから除去します。

Cisco IronPort スパム隔離機能のエンドユーザ アクセス検証に LDAP クエリを使用するには、[有効なクエリとして指定する(Designate as the active query)] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理(System Administration)] > [LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク(*)が表示されます。

サーバ タイプに基づいて、次のデフォルト クエリ文字列がエンドユーザ認証クエリに使用されます。

- **Active Directory:** `(sAMAccountName={u})`
- **OpenLDAP:** `(uid={u})`
- **Unknown or Other:** (ブランク)

デフォルトでは、プライマリ メール属性は Active Directory サーバの場合は `proxyAddresses`、OpenLDAP サーバの場合は `mail` です。独自のクエリとメール属性を入力できます。クエリを CLI で作成するには、`ldapconfig` コマンドの `isqauth` サブコマンドを使用します。

(注) ユーザのログイン時に各自のメール アドレス全体を入力させる場合は、`(mail=smtp:{a})` というクエリ文字列を使用します。

スパム隔離機能に対するエンドユーザ認証をイネーブルにする方法については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Cisco IronPort スパム隔離機能の設定」を参照してください。

Active Directory エンドユーザ認証の設定例

ここでは、Active Directory サーバとエンドユーザ認証クエリの設定の例を示します。この例では、Active Directory サーバに対してパスワード認証を使用し、メール属性は `mail` と `proxyAddresses` を使用し、Active Directory サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 3-11　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例:Active Directory

認証方式	パスワードを使用（検索用にバインドするための低特権のユーザを作成するか、匿名検索を設定する必要があります）
サーバ タイプ（Server Type）	Active Directory
[ポート（Port）]	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル	（ブランク）
クエリ文字列	`(sAMAccountName={u})`
メール属性	`mail,proxyAddresses`

OpenLDAP エンドユーザ認証の設定の例

ここでは、OpenLDAP サーバとエンドユーザ認証クエリの設定の例を示します。この例では、OpenLDAP サーバに対して匿名認証を使用し、メール属性は `mail` と `mailLocalAddress` を使用し、OpenLDAP サーバに対するエンドユーザ認証にはデフォルトのクエリ文字列を使用します。

表 3-12　LDAP サーバとスパム隔離へのエンドユーザ認証の設定例:OpenLDAP

認証方式	匿名（Anonymous）
サーバ タイプ（Server Type）	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	（ブランク）
クエリ文字列	`(uid={u})`
メール属性	`mail,mailLocalAddress`

スパム隔離のエイリアス統合クエリ

スパム通知を使用する場合は、スパム隔離のエイリアス統合クエリを使用して電子メール エイリアスを 1 つにまとめると、受信者がエイリアスごとに隔離通知を受け取ることはなくなります。たとえば、ある受信者がメール アドレス john@example.com、jsmith@example.com、および john.smith@example.com のメールを受け取るとします。エイリアス統合を使用すると、受信者が受け取るスパム通知は 1 通だけとなります。送信先は、このユーザのエイリアスすべてに送信されるメッセージのプライマリ電子メールアドレスとして選択されたアドレスです。

メッセージを統合してプライマリ電子メールアドレスに送信するには、受信者の代替電子メール エイリアスを検索するためのクエリを作成してから、受信者のプライマリ電子メールアドレスの属性を [メール属性（Email Attribute）] フィールドに入力します。

Cisco IronPort スパム隔離機能のスパム通知に LDAP クエリを使用するには、[有効なクエリとして指定する（Designate as the active query）] チェックボックスをオンにしてください。すでにアクティブなクエリがある場合、そのクエリはディセーブルになります。[システム管理（System Administration）] > [LDAP] ページを開いたときに、アクティブなクエリの横にアスタリスク（*）が表示されます。

Active Directory サーバの場合は、デフォルトのクエリー文字列は `(|(proxyAddresses={a})(proxyAddresses=smtp:{a}))` で、デフォルトのメール属性は `mail` です。OpenLDAP サーバの場合は、デフォルト クエリー文字列が `(mail={a})` で、デフォルト メール属性が `mail` です。独自のクエリーとメール属性を定義することもできます。属性が複数の場合は、カンマで区切ります。Cisco IronPortでは、入力するメール属性が複数ある場合は、最初のメール属性として、変動する可能性のある値を複数持つ属性（たとえば `proxyAddresses`）ではなく、値を 1 つだけ使用する一意の属性（たとえば `mail`）を入力することを推奨します。

クエリーを CLI で作成するには、`ldapconfig` コマンドの `isqalias` サブコマンドを使用します。

Active Directory エイリアス統合の設定例

ここでは、Active Directory サーバとエイリアス統合クエリの設定の例を示します。この例では、Active Directory サーバの匿名認証、Active Directory サーバのエイリアス統合用クエリー文字列、`mail` メール属性を使用します。

表 3-13　LDAP サーバとスパム隔離エイリアス統合の設定例：Active Directory

認証方式	匿名（Anonymous）
サーバ タイプ（Server Type）	Active Directory
[ポート（Port）]	3268
ベース DN（Base DN）	（ブランク）
接続プロトコル	SSL を使用する（Use SSL）
クエリ文字列	`(|(mail={a})(mail=smtp:{a}))`
メール属性	メール アドレス

OpenLDAP エイリアス統合の設定例

ここでは、OpenLDAP サーバとエイリアス統合クエリの設定の例を示します。この例では、OpenLDAP サーバの匿名認証、OpenLDAP サーバのエイリアス統合用クエリー文字列、`mail` メール属性を使用します。

表 3-14　LDAP サーバとスパム隔離エイリアス統合の設定例：OpenLDAP

認証方式	匿名（Anonymous）
サーバ タイプ（Server Type）	OpenLDAP
ポート	389
ベース DN	（ブランク）（古いスキーマでは具体的なベース DN の使用が要求されることがあります）
接続プロトコル	SSL を使用する（Use SSL）
クエリ文字列	`(mail={a})`
メール属性	メール アドレス

電子メール セキュリティ アプライアンスは、Enterprise Manager に DLP インシデント データを送信する際に、メッセージ送信者の完全な識別名を含める必要があります。Enterprise Manager 送信者名を取得するには、LDAP サーバのユーザ識別名のクエリを作成して、クエリを E メール セキュリティ アプライアンスで発信メッセージを送信するリスナーに追加します。E メール セキュリティ アプライアンスは RSA Enterprise Manager で DLP が有効になっている場合に限り、このクエリを使用します。それ以外の場合、サーバ プロファイルのオプションとして表示されません。

AsyncOS を複数の LDAP サーバと連携させるための設定

LDAP プロファイルを設定するときに、Cisco IronPort アプライアンスからの接続先となる複数の LDAP サーバをリストとして設定できます。複数の LDAP サーバを使用するには、LDAP サーバに格納されている情報が同一になるように設定する必要があります。また、構造も同一で、使用する認証情報も同一でなければなりません（レコードを統合できる製品がサード パーティから提供されています）。

冗長化した複数の LDAP サーバに接続するように Cisco IronPort アプライアンスを設定すると、LDAP のフェールオーバーまたはロード バランシングを設定できます。

複数の LDAP サーバを使用すると、次のことが可能になります。

- **フェールオーバー**。フェールオーバーのための LDAP プロファイルを設定しておくと、Cisco IronPort アプライアンスが最初の LDAP サーバに接続できなくなったときに、リスト内の次の LDAP サーバへのフェールオーバーが行われます。
- **ロード バランシング**。ロード バランシングのための LDAP プロファイルを設定しておくと、Cisco IronPort アプライアンスが LDAP クエリーを実行するときに、アプライアンスからの接続はリスト内の LDAP サーバに分散されます。

冗長 LDAP サーバを設定するには、[システム管理（System Administration）] > [LDAP] ページまたは CLI の `ldapconfig` コマンドを使用します。

サーバとクエリのテスト

[Add（または Edit）LDAP Server Profile] ページの [テストサーバ（Test Server(s)）] ボタン（または CLI の `test` サブコマンド）を使用して、LDAP サーバへの接続をテストします。複数の LDAP サーバを使用する場合は、各サーバのテストが実行されて、各サーバの結果が個別に表示されます。各 LDAP サーバでのクエリのテストも実行されて、結果が個別に表示されます。

フェールオーバー

LDAP クエリが確実に解決されるようにするには、フェールオーバーのための LDAP プロファイルを設定します。

アプライアンスは、LDAP サーバ リスト内の最初のサーバへの接続を、所定の時間が経過するまで試行します。Cisco IronPort アプライアンスがリスト内の最初の LDAP サーバに接続できない場合は、リスト内の次の LDAP サーバへの接続が試行されます。デフォルトでは、アプライアンスは常にリスト内の最初のサーバへの接続を試行し、それ以降の各サーバへの接続を、リスト内で指定されている順に試行します。Cisco IronPort アプライアンスが確実にプライマリの LDAP サーバにデフォルトで接続するようにするには、そのサーバが LDAP サーバ リストの先頭に入力されていることを確認してください。

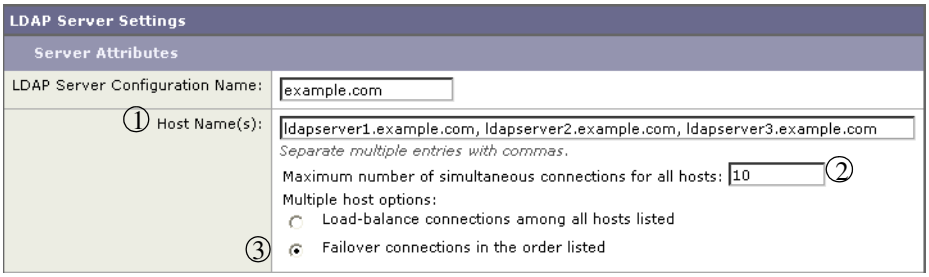
Cisco IronPort アプライアンスが 2 番め以降の LDAP サーバに接続した場合は、タイムアウトの時間に達するまで、そのサーバに接続したままになります。タイムアウトの時間に達すると、リスト内の最初のサーバへの再接続が試行されます。

LDAP フェールオーバーのための Cisco IronPort アプライアンスの設定

LDAP フェールオーバーを行うように Cisco IronPort アプライアンスを設定するには、GUI で以下の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2　LDAP サーバ プロファイルから、次の項目を設定します。



番号（Number）	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。
3	フェールオーバー モードを選択します。

ステップ 3　他の LDAP 設定を指定して変更を確定します。

ロード バランシング

LDAP 接続をグループ内の LDAP サーバ間に分散させるには、ロード バランシングのための LDAP プロファイルを設定します。

ロード バランシングのための LDAP プロファイルを設定しておくと、Cisco IronPort アプライアンスからの接続はリスト内の LDAP サーバに分散されます。接続に失敗したときやタイムアウトしたときは、Cisco IronPort アプライアンスは使用可能な LDAP サーバを判断して、使用可能なサーバに再接続します。Cisco IronPort アプライアンスは、管理者が設定した最大同時接続数に基づいて、同時に確立する接続の数を決定します。

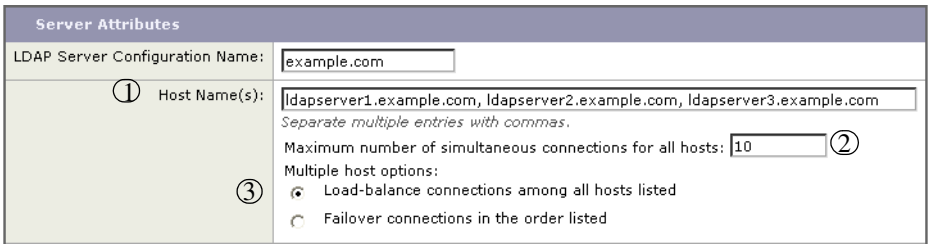
リストで指定された LDAP サーバの 1 つが応答しなくなった場合は、Cisco IronPort アプライアンスからの接続の負荷は残りの LDAP サーバに分散されます。

ロード バランシングのための Cisco IronPort アプライアンスの設定

LDAP ロード バランシングを行うように Cisco IronPort アプライアンスを設定するには、GUI で以下の手順を実行します。

ステップ 1　[システム管理（System Administration）] > [LDAP] ページで、編集する LDAP サーバ プロファイルを選択します。

ステップ 2　LDAP サーバ プロファイルから、次の項目を設定します。



番号（Number）	説明
1	LDAP サーバの一覧を表示します。
2	最大接続数を設定します。
3	ロード バランシング モードを選択します。

ステップ 3　他の LDAP 設定を指定して変更を確定します。

CHAPTER 4

SMTP サーバを使用した受信者の検証

この章では、SMTP サーバを使用した受信者の検証方法について説明します。

この章は、次の項で構成されています。

SMTP Call-Ahead 受信者検証：概要

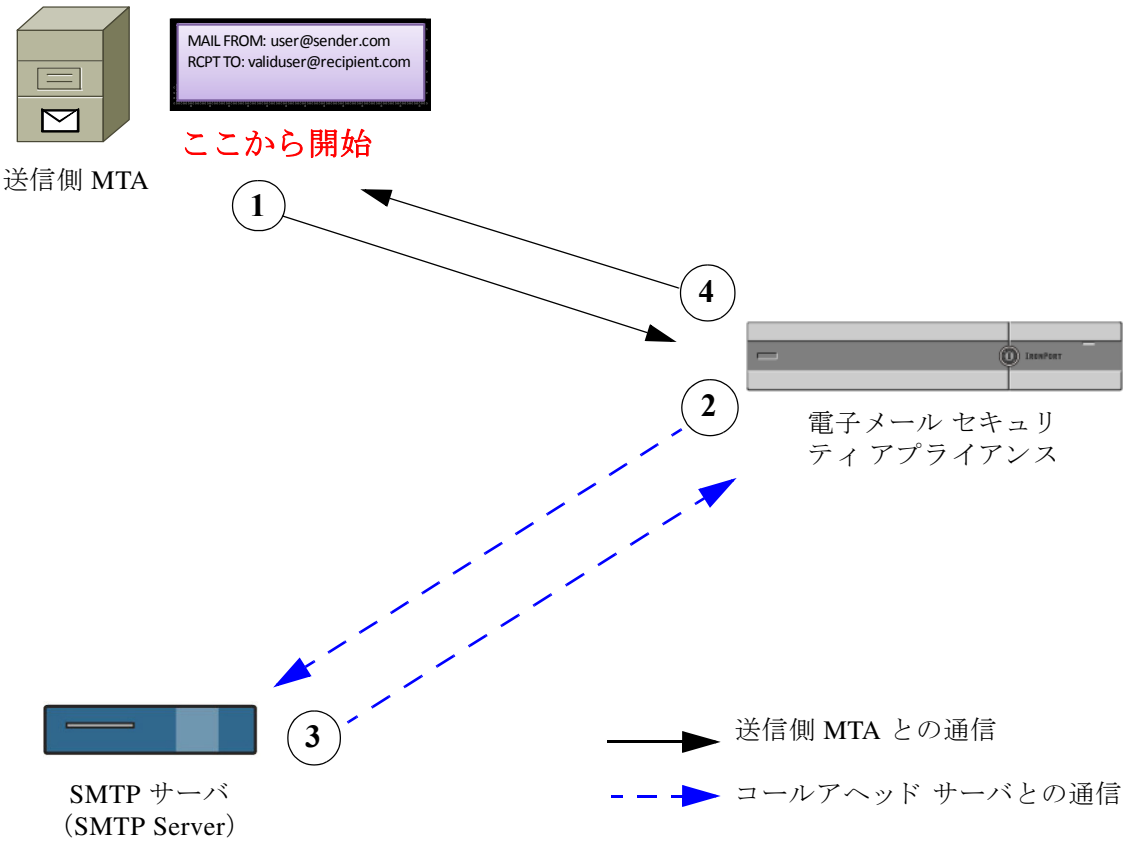
SMTP Call-Ahead 受信者検証では、受信者宛ての着信メールを受け入れる前に、外部 SMTP サーバにクエリーを実行して、受信者を検証できます。SMTP call-ahead 受信者検証は、ユーザを検証したいが、受信者検証のために LDAP 承認または受信者アクセス テーブル（RAT）を使用できない場合に役に立ちます。たとえば、顧客が大量の異なるメールボックス宛てのメールのホストとなっていて、それぞれが個別のドメインを使用しているとします。LDAP インフラストラクチャであるため、インフラストラクチャにクエリーを実行して、個々のドメインで各顧客を検証する方法はありません。この場合、顧客は SMTP Call-Ahead 受信者検証を設定して、電子メール セキュリティ アプライアンスが SMTP サーバにクエリーを実行して、SMTP 通信を続ける前に受信者を検証できます。

SMTP Call-Ahead 受信者検証では、電子メール セキュリティ アプライアンスは無効な受信者宛てのメッセージに対する大量の処理を保存できます。通常の処理では、無効な受信者宛てのメッセージは、ドロップする前に電子メール パイプラインの作業キュー フェーズを通して処理する必要があります。SMTP Call-Ahead 受信者検証機能を使用すると、電子メール パイプラインの着信および受信部分で追加処理を行わずに無効なメッセージをドロップまたはバウンスできます。

E メール セキュリティ アプライアンスで SMTP コールアヘッド受信者検証を設定すると、E メール セキュリティ アプライアンスは、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。Cisco IronPort アプライアンスは、SMTP サーバにクエリを実行するとき、SMTP サーバの応答を電子メール セキュリティ アプライアンスに返し、ユーザの設定に基づいて、メールを受け入れるか、コードとカスタム応答で接続をドロップすることができます。

図 4-1 に、SMTP コールアヘッド検証通信の基本的なワークフローを示します。

図 4-1　SMTP コールアヘッド サーバ通信のワークフロー



1. 送信側の MTA が SMTP 通信を開始します。
2. E メール セキュリティ アプライアンスは、SMTP サーバにクエリーを送信して受信者 *validuser@recipient.com* を検証する間、SMTP 通信を中断します。

   （注）　SMTP ルートまたは LDAP ルーティング クエリーが設定されている場合、SMTP サーバへのクエリーにはこれらのルートが使用されます。

3. SMTP サーバは、E メール セキュリティ アプライアンスにクエリーの応答を返します。
4. E メール セキュリティ アプライアンスは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答（および SMTP コールアヘッド プロファイルの設定）に基づいて接続を続行するかドロップします。

電子メール パイプラインでの処理の順序が決まっているため、特定の受信者宛てのメッセージが RAT によって拒否された場合、SMTP コールアヘッド受信者検証は発生しません。たとえば、RAT で *example.com* 宛てのメールのみを受け入れるように指定した場合、SMTP コールアヘッド受信者検証が発生する前に、*recipient@domain2.com* 宛てのメールは拒否されます。

（注）　HAT でディレクトリ ハーベスト攻撃防止（DHAP）を設定した場合、SMTP コールアヘッド サーバの拒否は、指定した 1 時間あたりの最大無効受信者数の中の拒否数に含まれるので注意してください。SMTP サーバによって拒否が増える場合を考慮してこの数を調整する必要があります。DHAP の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」を参照してください。

SMTP Call-Ahead 受信者検証の設定

SMTP コールアヘッド受信者検証は、SMTP コールアヘッド プロファイルを作成し、そのプロファイルをパブリック リスナーでイネーブルにして設定します。プロファイルでは、SMTP コールアヘッド受信者検証機能について、SMTP サーバとの接続方法、SMTP サーバの応答に基づいて実行するアクションなどの動作を定義します。このプロファイルをパブリック リスナーに割り当て、指定されたリスナーが受信したメッセージを SMTP コールアヘッド受信者検証を使用して処理できるようにします。

SMTP Call-Ahead 受信者検証を設定するには、次の手順を実行します。

1. **Call-Ahead サーバ プロファイルを設定します。**Call-Ahead サーバ プロファイルで、Call-Ahead サーバとの接続方法と Call-Ahead サーバの応答の処理方法を指定します。詳細については、コールアヘッド サーバ プロファイルの設定（4-3 ページ）を参照してください。
2. **パブリック リスナーで Call-Ahead サーバ プロファイルをイネーブルにします。**パブリック リスナーで Call-Ahead サーバ プロファイルをイネーブルにすると、電子メール セキュリティ アプライアンスは、SMTP Call-Ahead 受信者検証を使用して、そのリスナーで着信メールを処理できます。詳細については、パブリック リスナーでの SMTP Call-Ahead サーバ プロファイルのイネーブル化（4-6 ページ）を参照してください。
3. **LDAP ルーティング クエリーを設定します。**LDAP ルーティング クエリーを使用して、メールを異なるホストに転送する場合、SMTP Call-Ahead クエリーに対する SMTP Call-Ahead サーバの値を返すようにクエリーを設定できます。LDAP ルーティング クエリーの設定（4-7 ページ）を参照してください。

コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッド サーバ プロファイルの設定では、E メール セキュリティ アプライアンスと SMTP サーバの接続方法と SMTP サーバから返される応答の解釈方法を設定します。

SMTP Call-Ahead サーバ プロファイルを設定するには、次の手順を実行します。

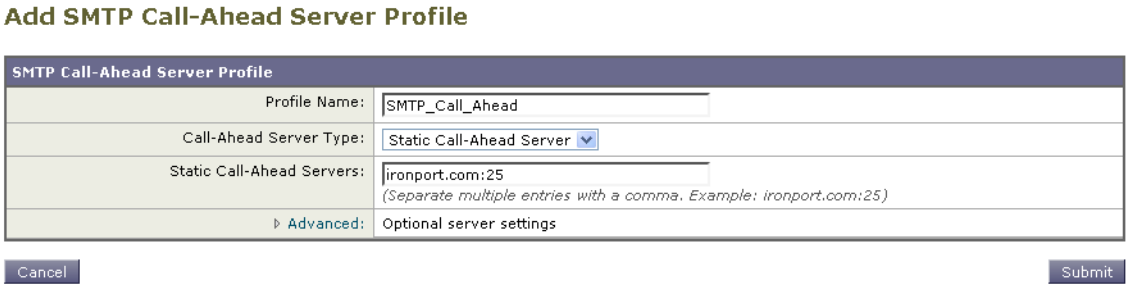
ステップ 1　[ネットワーク（Network）] > [SMTP コールアヘッド（SMTP Call-Ahead）] をクリックします。

[SMTP Call-Ahead Server Profile] ページが開きます。

ステップ 2　[プロファイルを追加（Add Profile）] をクリックします。

[Add SMTP Call-Ahead Server Profile] ページが開きます。

図 4-2　[Add SMTP Call-Ahead Server Profile] ページ



ステップ 3　プロファイルの設定値を入力します。詳細については、表 4-1SMTP コールアヘッド サーバ プロファイルの設定（4-4 ページ）を参照してください。

ステップ 4　プロファイルの高度な設定を指定します。詳細については、表 4-2 SMTP コールアヘッド サーバ プロファイルの高度な設定（4-5 ページ）を参照してください。

ステップ 5　変更を送信し、保存します。

SMTP コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッド サーバ プロファイルの設定時に、E メール セキュリティ アプライアンスと SMTP サーバの接続方法を設定する必要があります。

表 4-1 で、SMTP Call-Ahead サーバ プロファイルの基本設定を説明します。

表 4-1　SMTP コールアヘッド サーバ プロファイルの設定

設定	説明
プロファイル名（Profile Name）	コールアヘッド サーバ プロファイルの名前。
コールアヘッド サーバ タイプ（Call-Ahead Server Type）	コールアヘッド サーバへの接続方法を次から 1 つ選択します。 • [配信ホストを使用（Use Delivery Host）]。SMTP コールアヘッド クエリーに配信電子メール アドレスのホストを使用するように指定する場合は、このオプションを選択します。たとえば、メールの受信アドレスが *recipient@example.com* の場合、SMTP クエリーは *example.com* に関連付けられた SMTP サーバに対して実行されます。SMTP ルートまたは LDAP ルーティング クエリーを設定した場合、クエリー先の SMTP サーバの決定には、これらのルートが使用されます。LDAP ルーティング クエリーの設定についての詳細は、LDAP ルーティング クエリーの設定（4-7 ページ）を参照してください。 • [スタティックコールアヘッドサーバ（Static Call-Ahead Server）]。クエリー先のコールアヘッド サーバのスタティック リストを作成する場合は、このオプションを使用します。コールアヘッド サーバの名前や場所が頻繁に変わらないと思われる場合は、このオプションを使用できます。このオプションを使用すると、E メール セキュリティ アプライアンスは、リストの最初のスタティック コールアヘッド サーバからラウンドロビン方式でホストにクエリーを送信します。 **（注）** スタティック コールアヘッド サーバ タイプを選択すると、クエリーに SMTP ルートは適用されないので注意してください。その代わり MX ルックアップが実行され、その後、ホストでスタティック サーバのコールアヘッド IP アドレスを取得するためのルックアップが実行されます。
スタティックコールアヘッドサーバ（Static Call-Ahead Servers）	スタティック コールアヘッド サーバ タイプを使用する場合は、このフィールドにホストとポートの組み合わせのリストを入力します。次の構文を使用して、サーバとポートのリストを作成します。 `ironport.com:25` 複数のエントリがある場合は、カンマで区切ります。

表 4-2 に、SMTP コールアヘッド サーバ プロファイルの高度な設定を説明します。

表 4-2　SMTP コールアヘッド サーバ プロファイルの高度な設定

設定	説明
インターフェイス（Interface）	SMTP サーバと SMTP 通信を開始するときに使用されるインターフェイス。 [管理インターフェイス（Management interface）] または [自動（Auto）] のどちらを使用するかを選択します。[自動（Auto）] を選択すると、E メール セキュリティ アプライアンスは、使用するインターフェイスを自動的に検出しようとします。Cisco IronPort インターフェイスは、次の方法で SMTP サーバとの接続を試みます。 • コールアヘッド サーバが設定済みインターフェイスの 1 つと同じサブネット上にある場合、接続は一致するインターフェイスによって開始されます。 • 設定済みの任意の SMTP ルートが、クエリーのルートに使用されます。 • それ以外の場合、デフォルト ゲートウェイと同じサブネット上にあるインターフェイスが使用されます。
MAIL FROM アドレス（MAIL FROM Address）	SMTP サーバとの SMTP 通信に使用される MAIL FROM: アドレス。
検証要求タイムアウト（Validation Request Timeout）	SMTP サーバからの結果を待機する秒数。このタイムアウト値は、複数のコールアヘッド サーバにアクセスする可能性のある 1 つの受信者検証要求に対する値です。コールアヘッド サーバの応答（4-6 ページ）を参照してください。
検証エラーのアクション（Validation Failure Action）	受信者検証要求が失敗した場合（タイムアウト、サーバの障害、ネットワークの問題、または不明な応答により）に実行するアクション。E メール セキュリティ アプライアンスでのさまざまな応答の処理方法を設定できます。コールアヘッド サーバの応答（4-6 ページ）を参照してください。
一時的なエラーのアクション（Temporary Failure Action）	受信者検証要求が一時的に失敗した場合（リモート SMTP サーバから 4xx 応答が返された）に実行するアクション。メールボックスが一杯の場合、メールボックスを利用できない場合、またはサービスを利用できない場合に発生することがあります。 コールアヘッド サーバの応答（4-6 ページ）を参照してください。
セッションあたりの最大受信者数（Max. Recipients per Session）	1 つの SMTP セッションで検証する最大受信者数。 1 ～ 25,000 セッションの間で指定します。
サーバあたりの最大接続数（Max. Connections per Server）	1 台のコールアヘッド SMTP サーバへの最大接続数。 1 ～ 100 接続の間で指定します。
キャッシュ（Cache）	SMTP 応答のキャッシュのサイズ。100 ～ 1,000,000 エントリの間で指定します。
キャッシュ TTL（Cache TTL）	キャッシュ内でのエントリの存続可能時間値。このフィールドのデフォルト値は 900 秒です。60 ～ 86400 秒の間で指定します。

コールアヘッド サーバの応答

SMTP サーバからは、次の応答が返されます。

- **2xx**：コールアヘッド サーバから 2 で始まる SMTP コードを受け取った場合、受信者は受け入れられます。たとえば、応答が 250 の場合、メーリング アクションを続行できます。
- **4xx**：4 で始まる SMTP コードは、SMTP 要求の処理中に一時的な障害が発生したことを示します。後で再試行すると正常に処理されることがあります。たとえば、応答 451 は、要求されたアクションが中止されたか、処理中にローカル エラーが発生したことを示します。
- **5xx**：5 で始まる SMTP コードは、SMTP 要求の処理中に永続的な障害が発生したことを示します。たとえば、応答 550 は、要求されたアクションが実行されなかったか、メールボックスを使用できなかったことを示します。
- **タイムアウト。**コールアヘッド サーバから応答が戻されない場合、タイムアウトが発生する前に再試行する時間を設定できます。
- **接続エラー。**コールアヘッド サーバへの接続に失敗した場合、受信者アドレスへの接続を受け入れるか拒否するかを設定できます。

パブリック リスナーでの SMTP Call-Ahead サーバ プロファイルのイネーブル化

SMTP コールアヘッド サーバ プロファイルを作成したら、そのプロファイルをリスナーでイネーブルにして、リスナーが SMTP サーバ経由の着信メールを検証できるようにする必要があります。プライベート リスナーでは受信者の検証は必要ないので、SMTP コールアヘッド機能はパブリック リスナーでのみ使用できます。

リスナーで SMTP Call-Ahead サーバ プロファイルをイネーブルにするには、次の手順を実行します。

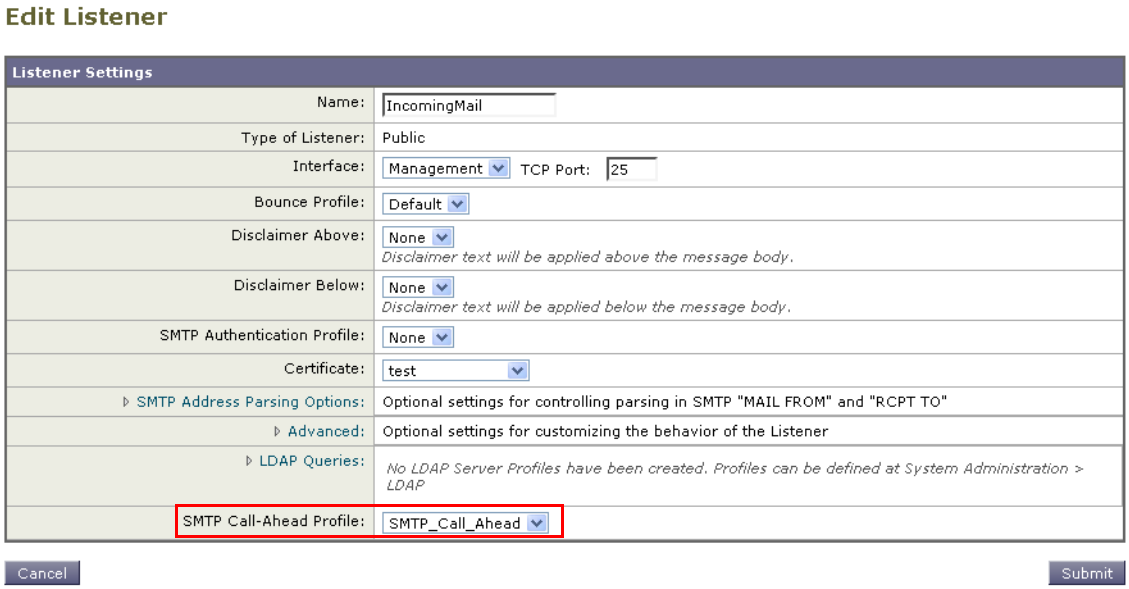
ステップ 1　[ネットワーク（Network）] > [リスナー（Listeners）] に移動します。

ステップ 2　SMTP コールアヘッド機能をイネーブルにするリスナーの名前をクリックします。

[リスナーを編集（Edit Listener）] ページが開きます。

ステップ 3　[SMTP コールアヘッドプロファイル（SMTP Call Ahead Profile）] フィールドで、イネーブルにする SMTP コールアヘッド プロファイルを選択します。

図 4-3　SMTP Call-Ahead サーバ プロファイルがイネーブルに設定された [Edit Listener] ページ



ステップ 4　変更を送信し、保存します。

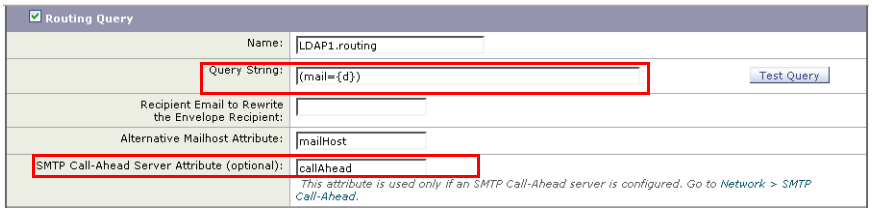
LDAP ルーティング クエリーの設定

LDAP ルーティング クエリーを使用して、メールを異なるメール ホストにルーティングする場合、AsyncOS は、代替メールホスト属性を使用して、クエリー先の SMTP サーバを決定します。ただし、この処理が不適切な場合があります。たとえば、次のスキーマでは、メール ホスト属性（`mailHost`）には、コールアヘッド SMTP サーバの属性（`callAhead`）で指定されているサーバとは異なる SMTP アドレスがあります。

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

この場合、[SMTP コールアヘッド（SMTP Call-Ahead）] フィールドを使用して、SMTP コールアヘッド クエリーを `callAhead` 属性で指定されているサーバに転送するルーティング クエリーを作成できます。たとえば、次の属性でルーティング クエリーを作成できます。

図 4-4　SMTP コールアヘッド用に設定された LDAP ルーティング クエリー:



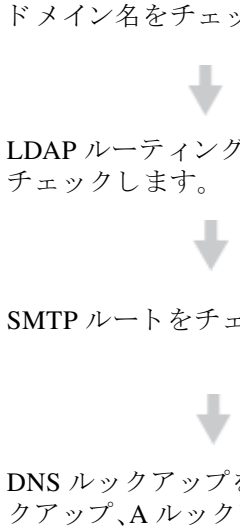
このクエリーでは、`{d}` は受信者アドレスのドメイン部分を表し、SMTP コールアヘッド サーバ属性は、クエリーに使用するコールアヘッド サーバとポートの値として、ポート 9025 の smtp2.mydomain.com、smtp3.mydomain.com を返します。

（注）　この例は、LDAP ルーティング クエリーを使用して SMTP コールアヘッド クエリーを正しい SMTP サーバに転送できるクエリーの設定例の 1 つです。この例で説明したクエリー文字列や特定の LDAP 属性を使用する必要はありません。

SMTP コールアヘッド クエリーのルーティング

SMTP コールアヘッド クエリーのルーティング時、AsyncOS は次の順序で情報をチェックします。

図 4-5　SMTP コールアヘッド クエリー ルーティングのワークフロー



ドメインに LDAP ルーティング クエリーまたは SMTP ルートが設定されていない場合、前の状態の結果は次のステージに渡されます。SMTP ルートが存在しない場合は、DNS ルックアップが実行されます。

SMTP コールアヘッド クエリーの代わりに LDAP ルーティング クエリーを使用するときに、SMTP ルートも設定されている場合、ルーティング動作は、ルーティング クエリーから返される値によって異なります。

- LDAP ルーティング クエリーからポートなしで 1 つのホスト名が返された場合、SMTP コールアヘッド クエリーは SMTP ルートを適用します。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。
- LDAP ルーティング クエリーからポートと共に 1 つのホスト名が返された場合、その SMTP ルートが使用されますが、SMTP ルートでポートが指定されていても、LDAP クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。
- LDAP ルーティング クエリーからポートと共に、またはポートなしで複数のホストが返された場合、SMTP ルートが適用されますが、SMTP ルートでポートが指定されていても、LDAP ルーティング クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

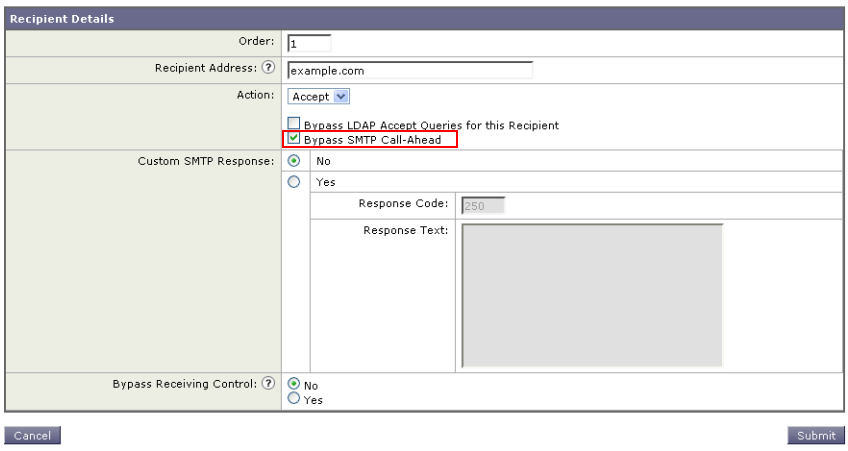
SMTP Call-Ahead 検証のバイパス

リスナーで SMTP コールアヘッド検証をイネーブルにしたまま、特定のユーザまたはユーザ グループに対して SMTP コールアヘッド検証を省略する必要がある場合があります。

SMTP コールアヘッド クエリー中にメールを遅延させてはならない受信者に対する SMTP コールアヘッド検証を省略する場合です。たとえば、有効であることが明確であり、迅速な対応を必要とするカスタマー サービスのエイリアスに RAT エントリを追加できます。

GUI から SMTP Call-Ahead 検証をバイパスするように設定するには、RAT エントリの追加または編集時に、[SMTP Call-Ahead をバイパス（Bypass SMTP Call-Ahead）] を選択します。

図 4-6　SMTP コールアヘッドをバイパスする



CHAPTER 5

電子メール認証

Cisco IronPort AsyncOS は SPF（Sender Policy Framework）、SIDF（Sender ID Framework）、DKIM（DomainKeys and DomainKeys Identified Mail）など、さまざまな形式の電子メール認証をサポートしています。

DomainKeys と DKIM は送信側で使われた署名キーに基づいて電子メールの信頼性を確認します。SPF と SIDF は DNS TXT レコードに基づいて電子メールの信頼性を検証する方法です。SPF と SIDF により、インターネット ドメインの所有者は、特別な形式の DNS レコードを使用して、そのドメインに電子メールを送信する権限のあるマシンを指定することができます。

この章は、次の項で構成されています。

電子メール認証の概要

Cisco IronPort AsyncOS は、電子メールの偽造を防止するために、さまざまな形式の電子メール認証をサポートしています。着信メールを検証するために、AsyncOS は SPF（Sender Policy Framework）、SIDF（Sender ID Framework）、DKIM（DomainKeys Identified Mail）をサポートしています。送信メールに署名するために、AsyncOS は DomainKeys と DKIM をサポートしています。

DomainKeys または DKIM 電子メール認証では、送信側が公開キー暗号化を使用して、電子メールに署名します。これにより、検証済みのドメインを使用して、電子メールの From:（または Sender:）ヘッダーのドメインと比較して、偽造を検出できます。AsyncOS の現在のバージョンでは、DomainKeys の電子メール署名をサポートし、DKIM の電子メール署名と検証の両方をサポートしています。DomainKeys と DKIM の詳細については、DomainKeys および DKIM 認証：概要（5-2 ページ）を参照してください。

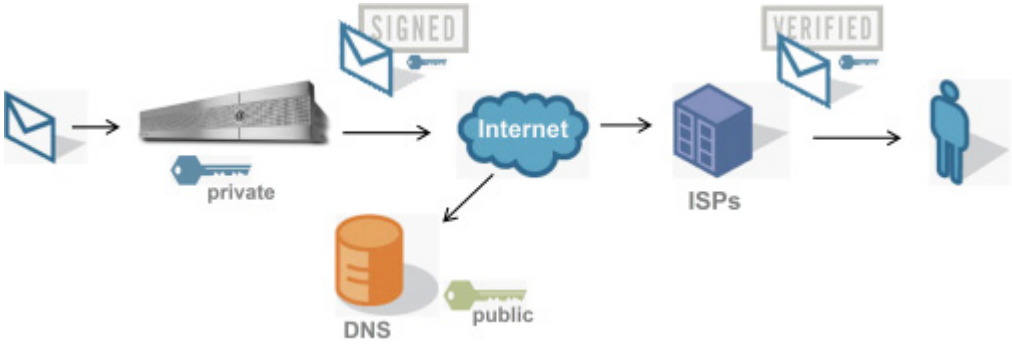
SPF および SIDF 電子メール認証により、インターネット ドメインの所有者は、特別な形式の DNS TXT レコードを使用して、それらのドメインに電子メールを送信する権限のあるマシンを指定することができます。準拠したメール受信側は、パブリッシュされた SPF レコードを使用して、メール トランザクション中に、送信側のメール転送エージェントの ID の権限をテストします。SPF および SIDF の詳細については、SPF および SIDF 検証の概要（5-22 ページ）を参照してください。

DomainKeys および DKIM 認証：概要

AsyncOS は電子メールの偽造を防止するために DomainKeys および DKIM 認証をサポートしています。DomainKeys と DKIM は、電子メールの送信元とメッセージの内容が、転送中に変更されていないことを確認するために使われるメカニズムです。DKIM は、DomainKeys 仕様に、DKIM（DomainKeys Identified Mail）と呼ばれる拡張プロトコルを作成するための IIM（Identified Internet Mail）の側面を組み合わせた拡張プロトコルです。DomainKeys と DKIM は、署名と検証の 2 つの主要部分から構成されます。AsyncOS の現在のバージョンは、DomainKeys の「署名」部分のプロセスをサポートし、DKIM の署名と検証の両方をサポートします。バウンスおよび遅延メッセージで DomainKeys および DKIM 署名を使用することもできます。

DomainKeys または DKIM 認証を使用すると、送信側は公開キー暗号化を使用して電子メールに署名します。これにより、検証済みのドメインを使用して、電子メールの From:（または Sender:）ヘッダーのドメインと比較して、偽造を検出できます。

図 5-1　　認証ワーク フロー



ステップ 1　管理者（ドメイン所有者）が公開キーを DNS 名前空間にパブリッシュします。

ステップ 2　管理者は発信メール転送エージェント（MTA）に秘密キーをロードします。

ステップ 3　そのドメインの権限のあるユーザによって送信される電子メールが、各秘密キーによってデジタル署名されます。署名は DomainKey または DKIM 署名ヘッダーとして電子メールに挿入され、電子メールが送信されます。

ステップ 4　受信側 MTA は、電子メールのヘッダーから DomainKeys または DKIM 署名と、要求された送信側ドメイン（Sender: または From: ヘッダーによって）を抽出します。DomainKeys または DKIM 署名ヘッダー フィールドから抽出された要求された署名ドメインから、公開キーが取得されます。

ステップ 5　公開キーは、DomainKeys または DKIM 署名が適切な秘密キーによって生成されているかどうかを確認するために使われます。

Yahoo! または Gmail アドレスを使用して、送信 DomainKeys 署名をテストできます。これらのサービスは無料で提供され、DomainKeys 署名されている着信メッセージを検証します。

AsyncOS の DomainKeys および DKIM 署名

AsyncOS の DomainKeys および DKIM 署名は、ドメイン プロファイルによって実装され、メール フロー ポリシー（一般に、発信「リレー」ポリシー）によってイネーブルにされます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」の章を参照してください。メッセージの署名は、メッセージ送信前にアプライアンスによって実行される最後の操作です。

ドメイン プロファイルはドメインとドメイン キー情報（署名キーと関連情報）を関連付けます。電子メールは、Cisco IronPort アプライアンスで、メール フロー ポリシーによって送信され、いずれかのドメイン プロファイルに一致する送信側電子メール アドレスが、ドメイン プロファイルに指定されている署名キーを使用して DomainKeys 署名されます。DKIM と DomainKeys の両方の署名をイネーブルにすると、DKIM 署名が使われます。DomainKeys および DKIM プロファイルは、`domainkeysconfig` CLI コマンドまたは GUI の [メールポリシー（Mail Policies）] > [ドメイン プロファイル（Domain Profiles）] および [メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページを使用して実装します。

DomainKeys および DKIM 署名は次のように機能します。ドメイン所有者はパブリック DNS（そのドメインに関連付けられた DNS TXT レコード）に格納される公開キーと、アプライアンスに格納され、そのドメインから送信されるメール（発信されるメール）の署名に使われる秘密キーの 2 つのキーを生成します。

メッセージがメッセージの送信（発信）に使われるリスナーで受信されると、Cisco IronPort アプライアンスは、ドメイン プロファイルが存在するかどうかを調べます。アプライアンスに作成された（およびメール フロー ポリシー用に実装された）ドメイン プロファイルが存在する場合、メッセージの有効な Sender: または From: アドレスがスキャンされます。どちらも存在する場合、DomainKeys には Sender: が使われます。DKIM 署名には、From: アドレスが常に使われます。それ以外の場合は、最初の From: アドレスが使われます。有効なアドレスが見つからない場合、メッセージは署名されず、イベントが mail_logs に記録されます。

（注） DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

有効な送信側アドレスが見つかった場合、送信側アドレスが既存のドメイン プロファイルに対して照合されます。一致しているものが見つかった場合、メッセージは署名されます。見つからない場合、メッセージは署名なしで送信されます。メッセージに既存の DomainKeys（「DomainKey-Signature:」ヘッダー）がある場合、メッセージは、元の署名の後に新しい送信側アドレスが追加されている場合にのみ、署名されます。メッセージに既存の DKIM 署名がある場合、新しい DKIM 署名がメッセージに追加されます。

AsyncOS はドメインに基づいて電子メールに署名するメカニズムに加えて、署名キーを管理する（新しいキーの作成または既存のキーの入力）方法を提供します。

このマニュアルのコンフィギュレーションの説明は、署名と検証の最も一般的な使用方法を示しています。着信電子メールのメール フロー ポリシーで DomainKeys および DKIM 署名をイネーブルにすることも、発信電子メールのメール フロー ポリシーで DKIM 検証をイネーブルにすることもできます。

（注） クラスタ環境にドメイン プロファイルと署名キーを設定する場合、[ドメイン キー プロファイル（Domain Key Profile）] 設定と [署名キー（Signing Key）] 設定がリンクしていることに注意します。そのため、署名キーをコピー、移動、または削除した場合、同じ操作が関連プロファイルに対して行われます。

DomainKeys および DKIM 署名の設定

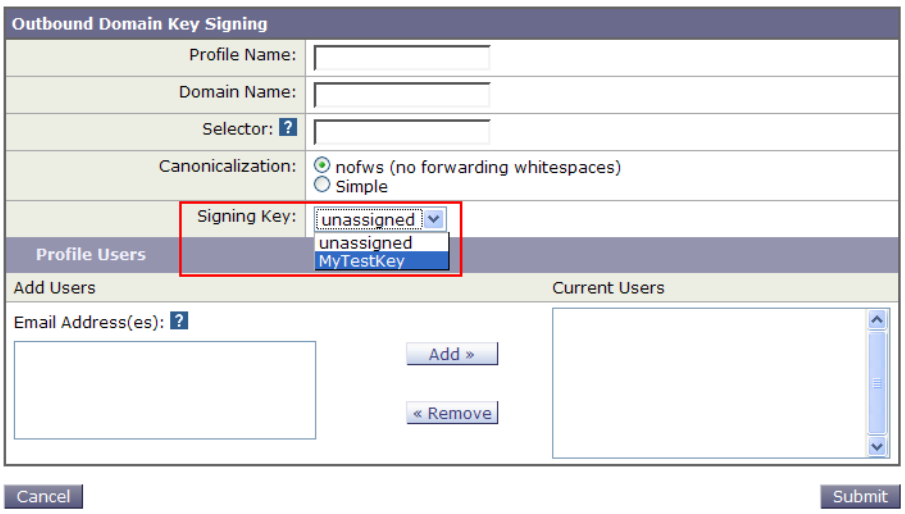
署名キー

署名キーは Cisco IronPort アプライアンスに格納されている秘密キーです。署名キーの作成時に、キー サイズを指定します。キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性もあります。Cisco IronPortアプライアンスでは 512 ～ 2048 ビットのキーをサポートしています。768 ～ 1024 ビットのキー サイズは安全であると見なされ、現在ほとんどの送信側で使われています。大きなキー サイズに基づいたキーはパフォーマンスに影響する可能性があるため、2048 ビットを超えるキーはサポートされていません。署名キーの作成方法については、新しい署名キーの作成（5-11 ページ）を参照してください。

既存のキーを入力する場合、それをフォームに貼り付けるだけです。既存の署名キーの別の使用方法は、キーをテキスト ファイルとしてインポートすることです。既存の署名キーの追加の詳細については、既存の署名キーのインポートまたは入力（5-12 ページ）を参照してください。

キーを入力すると、ドメイン プロファイルで使用できるようになり、ドメイン プロファイルの [Signing Key] リストに表示されます。

図 5-2　[Add Domain Profile] ページ（DomainKeys）：署名キー



署名キーのエクスポートとインポート

署名キーを Cisco IronPort アプライアンス上のテキスト ファイルにエクスポートできます。キーをエクスポートすると、アプライアンスに現在存在するすべてのキーがテキスト ファイルに挿入されます。キーのエクスポートの詳細については、署名キーのエクスポート（5-12 ページ）を参照してください。

エクスポートされたキーをインポートすることもできます。

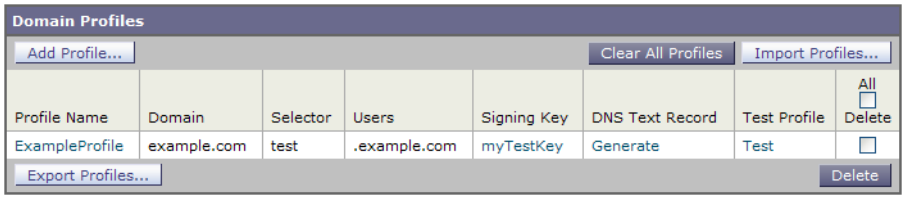
（注）　キーをインポートすると、アプライアンス上のすべての現在のキーが置き換えられます。

詳細については、既存の署名キーのインポートまたは入力（5-12 ページ）を参照してください。

公開キー

署名キーをドメイン プロファイルに関連付けると、公開キーが含まれる DNS テキスト レコードを作成できます。これは、ドメイン プロファイルのリストの [DNS テキストレコード（DNS Text Record）] 列の [生成（Generate）] リンクから（または CLI の `domainkeysconfig -> profiles -> dnstxt` から）実行します。

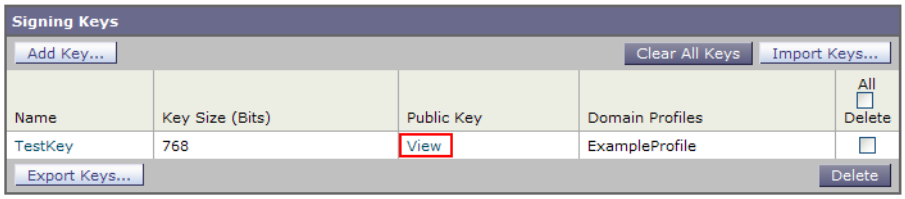
図 5-3　[ドメインプロファイル（Domain Profiles）] ページの DNS テキスト レコードの生成リンク



DNS テキスト レコードの生成の詳細については、DNS テキスト レコードの生成（5-13 ページ）を参照してください。

[署名キー（Signing Keys）] ページの [ビュー（View）] リンクから、公開キーを表示することもできます。

図 5-4　[署名キー（Signing Keys）] ページの公開キーの表示リンク



ドメイン プロファイル

ドメイン プロファイルは送信側ドメインを署名に必要なその他の情報と共に署名キーに関連付けます。ドメイン プロファイルは次の情報から構成されます。

- ドメイン プロファイルの名前。
- ドメイン名（「d=」ヘッダーに含まれるドメイン）。
- セレクタ（セレクタは公開キーのクエリーを形成するために使用されます。DNS クエリー タイプでは、この値が送信側ドメインの「_domainkey」名前空間の前に付けられます）。
- 正規化方法（署名アルゴリズムに提示するためにヘッダーと内容が準備される方法）。AsyncOS は DomainKeys に対して「simple」と「nofws」、DKIM に対して「relaxed」と「simple」をサポートしています。
- 署名キー（詳細については、署名キー（5-4 ページ）を参照してください）。
- 署名するヘッダーのリストと本文の長さ（DKIM のみ）。
- 署名のヘッダー（DKIM のみ）に含めるタグのリスト。これらのタグは次の情報を保持します。
  - 署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。
  - 公開キーを取得するために使用されるクエリー方法のカンマ区切りリスト。

  - 署名が作成されたときのタイムスタンプ。
  - 秒による署名の有効期限。
  - 垂直バーよって隔離されている（つまり、|）ヘッダー フィールドの一覧は、メッセージの署名時を示します。
- 署名（DKIM のみ）に含めるタグ。
- プロファイル ユーザのリスト（署名用にドメイン プロファイルの使用を許可されたアドレス）。

（注） プロファイル ユーザに指定されたアドレスのドメインは [ドメイン（Domain）] フィールドに指定されたドメインに一致している必要があります。

既存のすべてのドメイン プロファイルで、特定の用語を検索できます。詳細については、ドメイン プロファイルの検索（5-15 ページ）を参照してください。

DKIM 署名を持つシステムで生成されたメッセージに署名するかどうかを選択できます。詳細については、システムで生成されたメッセージへの署名（5-15 ページ）を参照してください。

ドメイン プロファイルのエクスポートとインポート

既存のドメイン プロファイルを Cisco IronPort アプライアンス上のテキスト ファイルにエクスポートできます。ドメイン プロファイルをエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキスト ファイルに挿入されます。ドメイン プロファイルのエクスポート（5-14 ページ）を参照してください。

以前にエクスポートしたドメイン プロファイルをインポートできます。ドメイン プロファイルをインポートすると、マシン上のすべての現在のドメイン プロファイルが置き換えられます。ドメイン プロファイルのインポート（5-14 ページ）を参照してください。

送信メールの署名のイネーブル化

DomainKeys および DKIM 署名は発信メールのメール フロー ポリシーでイネーブルにします。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」の章を参照してください。

発信メール フロー ポリシーで署名をイネーブルにするには、次の手順を実行します。

ステップ 1　[メール フロー ポリシー（Mail Flow Policies）] ページ（[メール ポリシー（Mail Policies）] メニューから）で、[リレー（RELAYED）] メール フロー ポリシー（送信）をクリックします。

ステップ 2　[セキュリティ サービス（Security Features）] セクションから、[オン（On）] を選択して、[DomainKeys/DKIM 署名（DomainKeys/DKIM Signing）] をイネーブルにします。

図 5-5　DomainKeys/DKIM 署名のイネーブル化

ステップ 3　変更を送信し、保存します。

バウンスおよび遅延メッセージの署名のイネーブル化

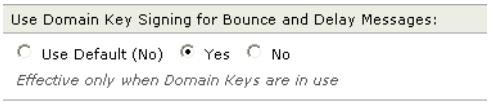
発信メッセージに署名するだけでなく、バウンスおよび遅延メッセージに署名したい場合があります。これにより、会社から受信するバウンスおよび遅延メッセージが正当なものであることを受信者に警告したい場合があります。バウンスおよび遅延メッセージの DomainKeys および DKIM 署名をイネーブルにするには、公開リスナーに関連付けられたバウンス プロファイルの DomainKeys/DKIM 署名をイネーブルにします。

バウンスおよび遅延メッセージの署名をイネーブルにするには、次の手順を実行します。

ステップ 1　署名された発信メッセージを送信する公開リスナーに関連付けられているバウンス プロファイルで、[ハード バウンスと遅延警告メッセージ（Hard Bounce and Delay Warning Messages）] に移動します。

ステップ 2　[バウンスおよび遅延メッセージに対してドメインキー署名を使用（Use Domain Key Signing for Bounce and Delay Messages）] をイネーブルにします。

図 5-6　　バウンスおよび警告メッセージの署名のイネーブル化



（注）　バウンスおよび遅延メッセージに署名するには、DomainKeys/DKIM 署名の設定（GUI）（5-7 ページ）に示されたすべての手順を完了している必要があります。

（注）　ドメイン プロファイルの [差出人：（From:）] アドレスは、バウンス返信アドレスに使用されているアドレスと一致している必要があります。これらのアドレスを一致させるには、バウンス プロファイルの返信アドレスを設定し（[システム管理（System Administration）] > [返信先アドレス（Return Addresses）]）、ドメイン プロファイルの [ユーザのプロファイリング（Profile Users）] リストで同じ名前を使用します。たとえば、バウンス返信アドレスに MAILER-DAEMON@example.com の返信アドレスを設定し、ドメイン プロファイルにプロファイル ユーザとして MAILER-DAEMON@example.com を追加します。

クラウド E メール セキュリティ アプライアンスの返信アドレスは変更しないことを推奨します。

DomainKeys/DKIM 署名の設定（GUI）

AsyncOS の DomainKeys/DKIM 署名の基本ワークフロー

ステップ 1　新規の秘密キーを作成するか、既存の秘密キーをインポートします。署名キーの作成またはインポートについては、署名キー（5-4 ページ）を参照してください。

ステップ 2　ドメイン プロファイルを作成し、キーをドメイン プロファイルに関連付けます。ドメイン プロファイルの作成については、ドメイン プロファイル（5-5 ページ）を参照してください。

ステップ 3　DNS テキスト レコードを作成します。DNS テキスト レコードの作成については、DNS テキスト レコードの生成（5-13 ページ）を参照してください。

ステップ 4　発信メールのメール フロー ポリシーで、DomainKeys/DKIM 署名をまだイネーブルにしていない場合は、イネーブルにします（送信メールの署名のイネーブル化（5-6 ページ）を参照してください）。

ステップ 5　任意で、バウンスおよび遅延メッセージの DomainKeys/DKIM 署名をイネーブルにします。バウンスおよび遅延メッセージの署名のイネーブル化については、バウンスおよび遅延メッセージの署名のイネーブル化（5-7 ページ）を参照してください。

ステップ 6　電子メールを送信します。ドメイン プロファイルに一致するドメインから送信されたメールは DomainKeys/DKIM 署名されます。さらに、バウンスおよび遅延メッセージの署名を設定した場合は、バウンスまたは遅延メッセージに署名されます。

（注）　DomainKey および DKIM プロファイルの両方を作成した（およびメール フロー ポリシーで署名をイネーブルにしている）場合、AsyncOS は DomainKeys と DKIM の両方の署名で送信メッセージを署名します。

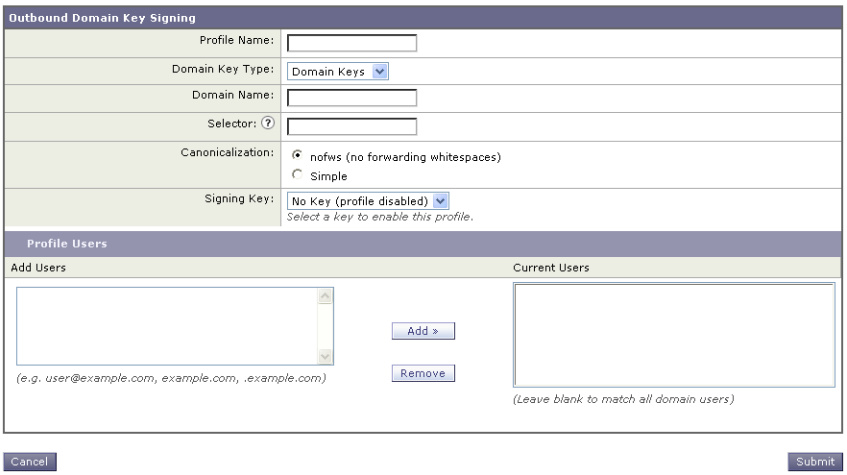
DomainKeys 署名のドメイン プロファイルの作成

DomainKeys 署名の新しいドメイン プロファイルを作成するには、次の手順を実行します。

ステップ 1　[ドメインプロファイル（Domain Profiles）] ページの [プロファイルの追加（Add Profile）] をクリックします。

ステップ 2　プロファイルの名前とドメイン キー タイプ（DomainKeys）を入力します。ドメイン キー タイプを選択すると、[Add Domain Profile] ページが表示されます。

図 5-7　[Add Domain Profile] ページ（DomainKeys）



ステップ 3　ドメイン名を入力します。

ステップ 4　セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 5　正規化（[no forwarding whitespaces] または [simple]）を選択します。

ステップ 6　署名キーを選択します（すでに署名キーを作成している場合。作成していない場合は、次の手順までスキップします）。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。新しい署名キーの作成（5-11 ページ）を参照してください。

ステップ 7　署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

ステップ 8　[送信（Submit）] をクリックします。

ステップ 9　[変更を確定（Commit Changes）] ボタンをクリックして必要に応じて任意のコメントを追加したら、[変更を確定（Commit Changes）] をクリックして新しいドメイン プロファイルの追加を終了します。

ステップ 10　この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化（5-6 ページ）を参照してください）。

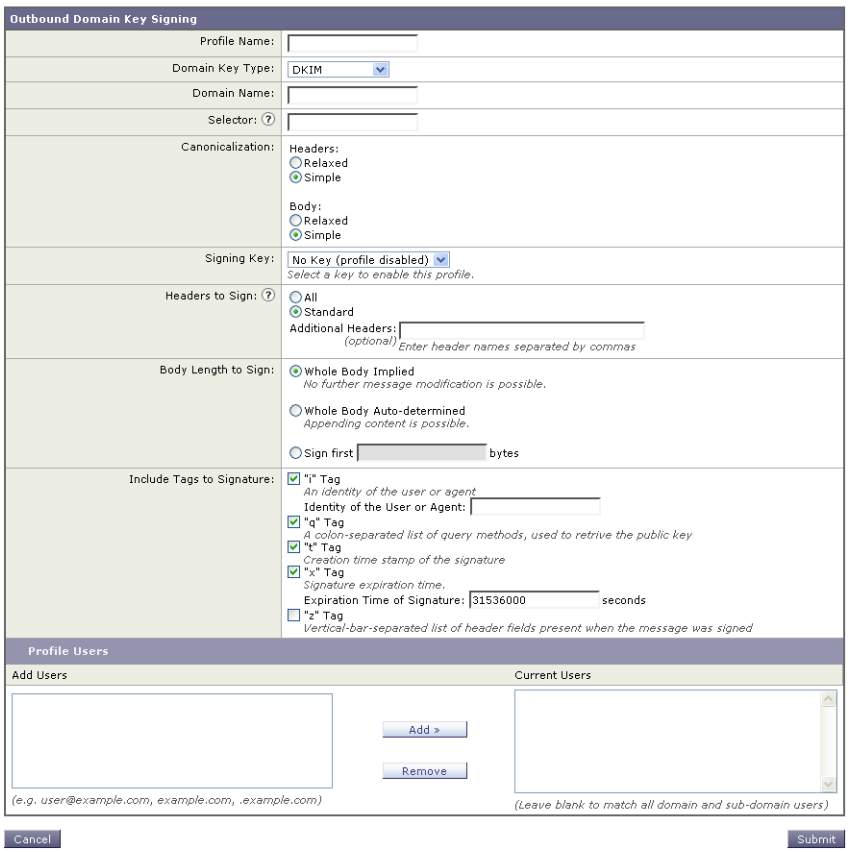
DKIM 署名の新しいドメイン プロファイルの作成

DKIM 署名の新しいドメイン プロファイルを作成するには、次の手順を実行します。

ステップ 1　[ドメインプロファイル（Domain Profiles）] ページの [プロファイルの追加（Add Profile）] をクリックします。

ステップ 2　プロファイルの名前とドメイン キー タイプ（DKIM）を入力します。ドメイン キー タイプを選択すると、[Add Domain Profile] ページが表示されます。

図 5-8　[Add Domain Profile] ページ（DKIM）



ステップ 3　ドメイン名を入力します。

ステップ 4　セレクタを入力します。セレクタは、「_domainkey」名前空間の前に付けられる任意の名前で、送信側ドメインあたり複数の同時公開キーをサポートするために使われます。セレクタ値と長さは、DNS 名前空間と電子メール ヘッダーで有効である必要があり、それらにセミコロンを含めることができないという規定が追加されます。

ステップ 5　ヘッダーの正規化を選択します。次のオプションから選択します。

- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。ヘッダー名を小文字に変更し、ヘッダーを展開して、連続した空白を 1 つの空白に短縮し、先頭と末尾の空白を取り除きます。
- [Simple]。ヘッダーは変更されません。

ステップ 6　本文の正規化を選択します。次のオプションから選択します。

- [Relaxed]。「relaxed」ヘッダー正規化アルゴリズムは、次を実行します。本文末尾の空の行を取り除き、行中の空白を 1 つの空白に短縮し、行の末尾の空白を取り除きます。
- [Simple]。本文末尾の空の行を取り除きます。

ステップ 7　署名キーを選択します（すでに署名キーを作成している場合。作成していない場合は、次の手順までスキップします）。署名キーをリストから選択させるために、少なくとも 1 つの署名キーを作成する（またはインポートする）必要があります。新しい署名キーの作成（5-11 ページ）を参照してください。

ステップ 8　署名するヘッダーのリストを選択します。次のヘッダーから選択できます。

- [すべて（All）]。AsyncOS は署名時に存在するすべてのヘッダーに署名します。送信中にヘッダーの追加や削除が予想されない場合は、すべてのヘッダーに署名することが考えられます。
- [標準（Standard）]。送信中にヘッダーの追加や削除が予想される場合は、標準ヘッダーを選択することが考えられます。AsyncOS は次の標準ヘッダーにのみ署名します（メッセージにそのヘッダーが存在しない場合、DKIM 署名は、そのヘッダーにヌル値を示します）。
  - 送信元（From）
  - Sender、Reply To-
  - Subject
  - Date、Message-ID
  - To、Cc
  - MIME-Version
  - Content-Type、Content-Transfer-Encoding、Content-ID、Content-Description
  - Resent-Date、Resent-From、Resent-Sender、Resent-To、Resent-cc、Resent-Message-ID
  - In-Reply-To、References
  - List-Id、List-Help、List-Unsubscribe、LIst-Subscribe、List-Post、List-Owner、List-Archive

（注）　[標準（Standard）] を選択した場合、署名するヘッダーを追加できます。

ステップ 9　メッセージ本文に署名する方法を指定します。メッセージ本文に署名するか、署名するバイト数を選択できます。次のオプションのいずれかを選択します。

- [本文全体を含む（Whole Body Implied）]。本文の長さを判断するために「l=」タグを使用しないでください。メッセージ全体に署名し、変更を許可しません。
- [本文全体を自動判断（Whole Body Auto-determined）]。メッセージ本文全体に署名し、送信中に本文の末尾へのデータの追加を許可します。
- [最初に署名 _ バイト（Sign first _ bytes）]。指定したバイト数まで、メッセージ本文に署名します。

ステップ 10　メッセージ署名のヘッダー フィールドに含めるタグを選択します。これらのタグに格納されている情報はメッセージ署名の検証に使用されます。次のオプションから 1 つ以上を選択します。

- ["i" タグ]。署名されたメッセージが代理したユーザまたはエージェントの ID（たとえば、メーリング リスト マネージャ）。ドメイン `@example.com` など、@ 記号が付加されたドメイン名を入力します。
- ["q" タグ]。公開キーを取得するために使用されるクエリー方法のコロン区切りリスト。現在、唯一有効な値は dns/txt です。
- ["t" タグ]。署名が作成されたときのタイムスタンプを表示します。
- ["x" タグ]。署名が終了する絶対的な日時。署名の有効期限（秒単位）を指定します。デフォルトは `31536000` 秒です。
- ["z" タグ]。垂直バーよって隔離されている（つまり、|）ヘッダー フィールドの一覧は、メッセージの署名時を示します。これには、ヘッダー フィールドの名前と値が含まれます。次に例を示します。

```
z=From:admin@example.come|To:joe@example.com|
Subject:test%20message|Date:Date:August%2026,%202011%205:30:02%20PM%20-0700
```

ステップ 11　署名のドメイン プロファイルを使用するユーザ（電子メール アドレス、ホストなど）を入力します。

（注）　ドメイン プロファイルを作成する場合、特定のユーザに関連付けるプロファイルの決定において、階層を使用することに注意してください。たとえば、example.com のプロファイルと joe@example.com の別のプロファイルを作成するとします。joe@example.com からメールが送信される場合、joe@example.com のプロファイルが使われます。しかし、メールが adam@example.com から送信される場合は、example.com のプロファイルが使われます。

ステップ 12　変更を送信し、保存します。

ステップ 13　この時点で、送信メール フロー ポリシーで DomainKeys/DKIM 署名をイネーブルにしていない場合はイネーブルにする必要があります（送信メールの署名のイネーブル化（5-6 ページ）を参照してください）。

（注）　DomainKeys と DKIM の両方のプロファイルを作成している場合、AsyncOS は送信メールに DomainKeys と DKIM の両方の署名を実行します。

新しい署名キーの作成

新しい署名キーを作成するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページで [キーを追加（Add Key）] をクリックします。[Add Key] ページが表示されます。

ステップ 2　キーの名前を入力します。

ステップ 3　[生成（Generate）] をクリックしてキー サイズを選択します。

キー サイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性があります。シスコでは、セキュリティとパフォーマンスのバランスが良い 768 ビットのキー サイズが推奨されます。

ステップ 4　[送信（Submit）] をクリックします。キーが生成されます。

ステップ 5　[変更を確定（Commit Changes）] ボタンをクリックして必要に応じて任意のコメントを追加したら、[変更を確定（Commit Changes）] をクリックして新しい署名キーの追加を終了します。

（注）　キーを割り当てるドメイン プロファイルを編集していない場合は、編集する必要がある場合があります。

署名キーのエクスポート

署名キーをエクスポートすると、Cisco IronPort アプライアンスに現在存在するすべてのキーがまとめて 1 つのテキスト ファイルにエクスポートされます。署名キーをエクスポートするには、次の手順を実行します。

ステップ 1　[署名キー（Signing Keys）] ページの [キーをエクスポート（Export Keys）] をクリックします。[Export Signing Keys] ページが表示されます。

図 5-9　[Export Signing Keys] ページ

ステップ 2　ファイルの名前を入力し、[送信（Submit）] をクリックします。

既存の署名キーのインポートまたは入力

既存のキーを入力するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページで [キーを追加（Add Key）] をクリックします。[Add Key] ページが表示されます。

ステップ 2　[貼り付けキー（Paste Key）] フィールドにキーを貼り付けます（PEM フォーマットされ、RSA キーのみである必要があります）。

ステップ 3　変更を送信し、保存します。

既存のエクスポート ファイルからキーをインポートするには、次の手順を実行します（署名キーのエクスポート（5-12 ページ）を参照）。

ステップ 1　[メールポリシー（Mail Policies）] > [署名キー（Signing Keys）] ページで [キーをインポート（Import Keys）] をクリックします。[Import Key] ページが表示されます。

ステップ 2　エクスポートされた署名キーを含むファイルを選択します。

ステップ 3　[送信（Submit）] をクリックします。インポートによってすべての既存の署名キーが置き換えられることが警告されます。テキスト ファイルのすべてのキーがインポートされます。

ステップ 4　[インポート（Import）] をクリックします。

署名キーの削除

ステップ 1　署名キーのリストから特定のキーを削除するには、次の手順を実行します。

ステップ 2　[Signing Keys] ページで、削除する各署名キーの右のチェックボックスをオンにします。

ステップ 3　[削除(Delete)] をクリックします。

ステップ 4　削除を確認します。

現在構成されているすべての署名キーを削除するには、次の手順を実行します。

ステップ 1　[署名キー(Signing Keys)] ページの [すべてのキーを消去(Clear All Keys)] をクリックします。

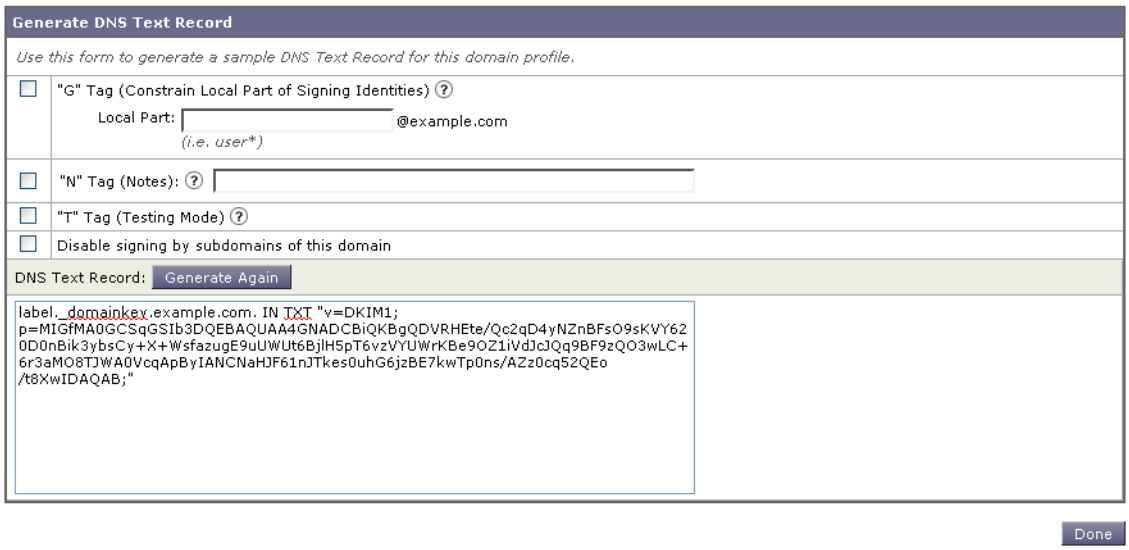
ステップ 2　削除を確認するよう求められます。

DNS テキスト レコードの生成

DNS テキスト レコードを生成するには、次の手順を実行します。

ステップ 1　対応するドメイン プロファイルの [DNS テキストレコード(DNS Text Record)] 列で [生成(Generate)] リンクをクリックします。[Generate DNS Text Record] ページが表示されます。

図 5-10　[DNS Text Record] ページ



ステップ 2　DNS テキスト レコードに含める属性のチェックボックスをオンにします。

ステップ 3　[再生成(Generate Again)] をクリックして、変更を含めてキーを再生成します。

ステップ 4　DNS テキスト レコードがテキスト フィールドに表示されます(ここでそれをコピーできます)。

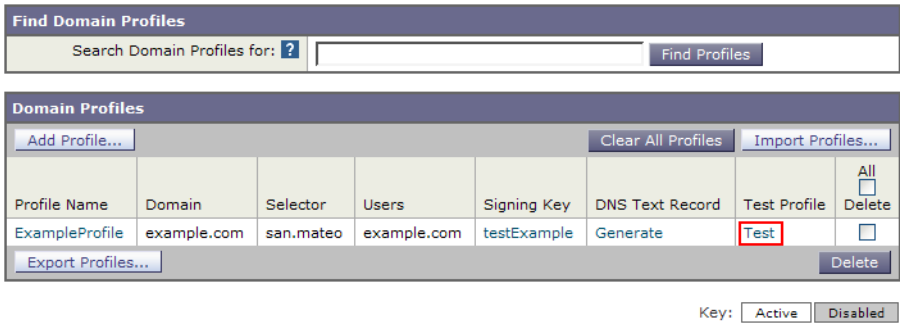
ステップ 5　[完了(Done)] をクリックします。

ドメイン プロファイルのテスト

署名キーを作成してドメイン プロファイルに関連付け、DNS テキストを生成して承認済み DNS に挿入したら、ドメイン プロファイルをテストできます。次の手順を実行します。

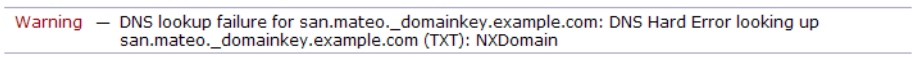
ステップ 1　[Domain Profiles] ページの [Test] をクリックします。

図 5-11　ドメイン プロファイルのテスト



ステップ 2　成功または失敗を示すメッセージがページの上部に表示されます。テストが失敗した場合、エラー テキストを含む警告メッセージが表示されます。

図 5-12　失敗したドメイン プロファイル テスト



ドメイン プロファイルのエクスポート

ドメイン プロファイルをエクスポートすると、Cisco IronPort アプライアンスに現在存在するすべてのドメイン プロファイルがまとめて 1 つのテキスト ファイルにエクスポートされます。ドメイン プロファイルをエクスポートするには、次の手順を実行します。

ステップ 1　[ドメインプロファイル（Domain Profiles）] ページの [ドメインプロファイルをエクスポート（Export Domain Profiles）] をクリックします。[Export Domain profiles] ページが表示されます。

ステップ 2　ファイルの名前を入力し、[送信（Submit）] をクリックします。

ドメイン プロファイルのインポート

既存のエクスポート ファイルからドメイン プロファイルをインポートするには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [ドメインプロファイル（Domain Profiles）] ページの [ドメインプロファイルをインポート（Import Domain Profiles）] をクリックします。[Import Domain Profiles] ページが表示されます。

ステップ 2　エクスポートされたドメイン プロファイルを含むファイルを選択します。

ステップ 3　[送信（Submit）] をクリックします。インポートによってすべての既存のドメイン プロファイルが置き換えられることが警告されます。テキスト ファイルのすべてのドメイン プロファイルがインポートされます。

ステップ 4　[インポート（Import）] をクリックします。

ドメイン プロファイルの削除

ドメイン プロファイルのリストから特定のドメイン プロファイルを削除するには、次の手順を実行します。

ステップ 1　[Domain Profiles] ページで、削除する各ドメイン プロファイルの右のチェックボックスにマークをオンにします。

ステップ 2　[削除（Delete）] をクリックします。

ステップ 3　削除を確認します。

現在構成されているすべてのドメイン プロファイルを削除するには、次の手順を実行します。

ステップ 1　[ドメインプロファイル（Domain Profiles）] ページの [すべてのプロファイルを消去（Clear All Profiles）] をクリックします。

ステップ 2　削除を確認するよう求められます。

ドメイン プロファイルの検索

すべてのドメイン プロファイルで特定の用語（一般にユーザ名やホスト名）を検索するには、次の手順を実行します。

ステップ 1　[Domain Profiles] ページの [Find Domain Profiles] フィールドに検索語を指定します。

ステップ 2　[プロファイルの検索（Find Profiles）] をクリックします。

ステップ 3　検索では、各ドメイン プロファイルの email、domain、selector、signing key name のフィールドがスキャンされます。

（注）　検索語を入力しない場合、検索エンジンはすべてのドメイン プロファイルを返します。

システムで生成されたメッセージへの署名

DKIM 署名を持つシステムで生成されたメッセージに署名するかどうか選択できます。E メール セキュリティ アプライアンスが署名するシステム生成メッセージの種類には、次のものがあります。

- Cisco IronPort スパム隔離通知
- コンテンツ フィルタで生成された通知
- 設定メッセージ
- サポート リクエスト

アプライアンスでシステム生成メッセージに署名できるようにするには、次の手順を実行します。

ステップ 1　[ドメイン署名プロファイル（Domain Signing Profiles）] ページの [システム生成メッセージの DKIM 署名（DKIM Signing of System Generated Messages）] で [設定を編集（Edit Settings）] をクリックします。[システム生成メッセージの DKIM 署名（DKIM Signing of System Generated Messages）]。

ステップ 2　[オン（On）] を選択します。

ステップ 3　変更を送信し、保存します。

ドメイン キーとロギング

DomainKeys 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:30 2007 Info: MID 371 DomainKeys: signing with dk-profile - matches
user123@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DomainKeys: cannot sign - no profile matches
user12@example.com
```

DKIM 署名時には、次のような行がメール ログに追加されます。

```
Tue Aug 28 15:29:54 2007 Info: MID 372 DKIM: signing with dkim-profile - matches
user@example.com
Tue Aug 28 15:34:15 2007 Info: MID 373 DKIM: cannot sign - no profile matches
user2@example.com
```

DKIM 検証の設定

送信メールの署名に加えて、DKIM を使用して受信メールを検証できます。

DKIM 検証を設定するには、次を実行する必要があります。

- メール フロー ポリシーの DKIM 検証プロファイルを作成します。
- 受信メールのメール フロー ポリシーで、DKIM 検証をイネーブルにします。
- 任意で、DKIM 認証条件を使用して、DKIM 検証済み電子メールに対するアクションを実行するためのコンテンツ フィルタを設定します。

DKIM 検証用に AsyncOS アプライアンスを設定すると、次のチェックが実行されます。

ステップ 1　AsyncOS は受信メールの [DKIM シグネチャ(DKIM-Signature)] フィールド、署名ヘッダーの構文、有効なタグ値、必須タグを調べます。署名がこれらのいずれかのチェックで失敗すると、AsyncOS は *permfail* を返します。

ステップ 2　署名チェックの実行後、公開 DNS レコードから公開キーが取得され、TXT レコードが検証されます。このプロセス中にエラーが検出されると、AsyncOS は *permfail* を返します。公開キーの DNS クエリーで応答を取得できない場合、*tempfail* が発生します。

ステップ 3　公開キーの取得後、AsyncOS はハッシュ値をチェックし、署名を検証します。この手順中にエラーが発生すると、AsyncOS は *permfail* を返します。

ステップ 4　チェックにすべて合格すると、AsyncOS は *pass* を返します。

（注）　メッセージ本文が指定された長さより長い場合、AsyncOS は次の判定を返します。

```
dkim = pass (partially verified [x bytes])
```

ここで *X* は検証されたバイト数を表します。

最終検証結果は、*Authentication-Results* ヘッダーとして入力されます。たとえば、次のいずれかのようなヘッダーを受け取ることがあります。

```
Authentication-Results: example1.com
    header.from=From:user123@example.com; dkim=pass (signature verified)
Authentication-Results: example1.com
```

```
    header.from=From:user123@example.com; dkim=pass (partially verified [1000 bytes])
Authentication-Results: example1.com
    header.from=From:user123@example.com; dkim=permfail (body hash did not verify)
```

（注） 現在の DKIM 検証は最初の有効な署名で停止します。最後に検出された署名を使用して、検証できません。この機能は、後のリリースで使用できるようになる可能性があります。

DKIM の検証プロファイルの管理

DKIM 検証プロファイルは E メール セキュリティ アプライアンスのメール フロー ポリシーが DKIM 署名を保証するために使用されるパラメータのリストです。たとえば、クエリーがタイムアウトする前に 30 秒取る検証プロファイルと、クエリーがタイムアウトする前に 3 秒だけ取る検証プロファイルの、2 つの検証プロファイルを作成できます。THROTTLED メール フロー ポリシーに 2 つ目の検証プロファイルを割り当てて、DDoS の場合の接続スタベーションを防止できます。検証プロファイルは次の情報で構成されます。

- 検証プロファイルの名前。
- 許容できる公開キーの最小、最大サイズ。デフォルトのキーのサイズは 512 および 2048 です。
- メッセージの中で検証できる署名の最大数。メッセージに定義した署名の最大数よりも多くの署名がある場合、アプライアンスは残りの署名の検証をスキップし、メッセージの処理を続行します。デフォルトは、5 つの署名です。
- 送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差（秒単位）。たとえば、メッセージ署名が 05:00:00 に期限切れとなり、検証者のシステム時刻が 05:00:30 である場合、時間の許容差が 60 秒であればメッセージ署名は有効なままですが、許容差が 10 秒であれば無効になります。デフォルトは 60 秒です。
- 本文の長さのパラメータを使用するかどうかを指定するオプション。
- 一時的な障害の場合に実行する SMTP アクション。
- 永続的な障害の場合に実行する SMTP アクション。

プロファイル名ですべての既存の検証プロファイルを検索できます。

Cisco IronPort アプライアンスのコンフィギュレーション ディレクトリに DKIM 検証プロファイルをテキスト ファイルとしてエクスポートできます。検証プロファイルをエクスポートすると、アプライアンスに存在するすべてのプロファイルが 1 つのテキスト ファイルに挿入されます。詳細については、DKIM 検証プロファイルのエクスポート（5-19 ページ）を参照してください。

以前エクスポートした DKIM 検証プロファイルをインポートできます。DKIM 検証プロファイルをインポートすると、マシンの現在のすべての DKIM 検証プロファイルを置き換えることになります。詳細については、DKIM 検証プロファイルのインポート（5-19 ページ）を参照してください。

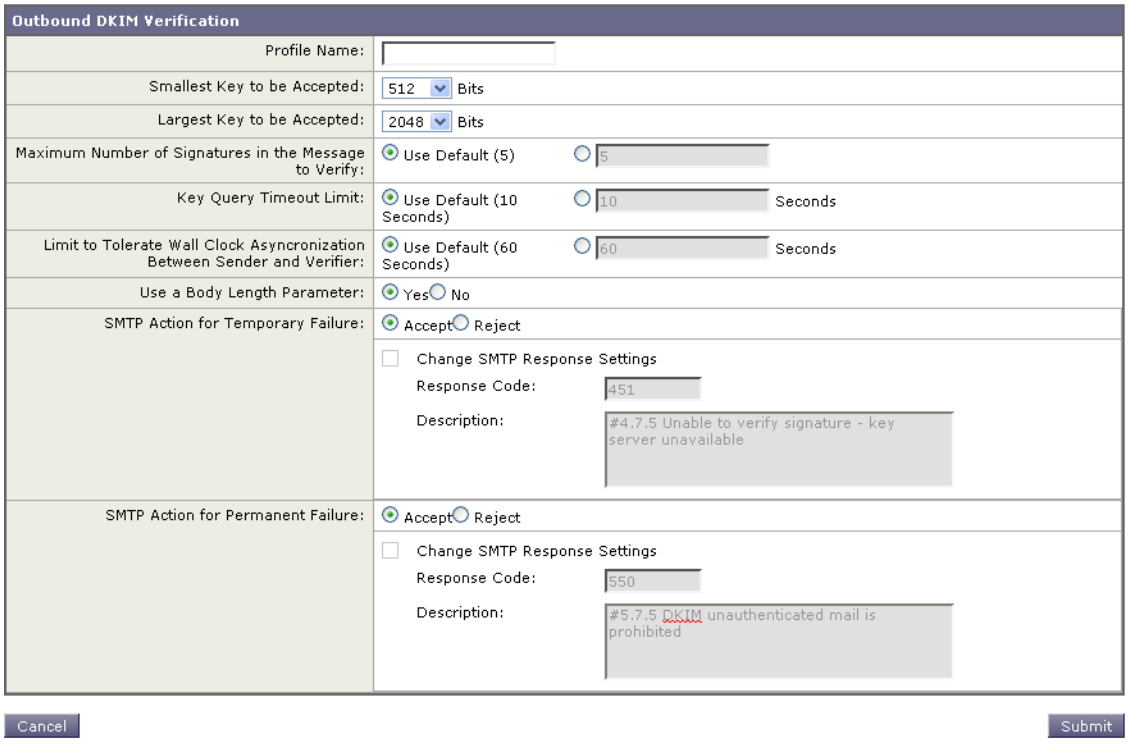
DKIM 検証プロファイルの作成

DKIM 検証プロファイルを作成するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] をクリックします。

ステップ 2　[プロファイルを追加（Add Profile）] をクリックします。[DKIM 検証プロファイルの追加（Add DKIM Verification Profiles）] ページが表示されます。

図 5-13　[DKIM 検証プロファイルの追加(Add DKIM Verification Profiles)] ページ



ステップ 3　プロファイル名を入力します。

ステップ 4　アプライアンスが許可する署名キーの最小キー サイズを選択します。

ステップ 5　アプライアンスが許可する署名キーの最大キー サイズを選択します。

ステップ 6　1 つのメッセージで検証する署名の最大数を選択します。デフォルトは 5 つの署名です。

ステップ 7　キー クエリーがタイムアウトするまでの時間(秒)を選択します。デフォルトは 10 秒です。

ステップ 8　送信者のシステム時刻と検証者のシステム時刻との間の時間の最大許容差(秒単位)を選択します。デフォルトは 60 秒です。

ステップ 9　メッセージの検証に、署名の本文の長さのパラメータを使用するかどうか選択します。

ステップ 10　署名を確認するときに一時的な障害がある場合、E メール セキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 11　署名を確認するときに永続的な障害がある場合は、E メール セキュリティ アプライアンスがメッセージを受け入れるか、拒否するかを選択します。アプライアンスがメッセージを拒否する場合、デフォルトの 451 SMTP 応答コードまたは別の SMTP 応答コードとテキストを送信するよう選択できます。

ステップ 12　変更を送信します。

新しいプロファイルが DKIM 検証プロファイルのテーブルに表示されます。

ステップ 13　変更を保存します。

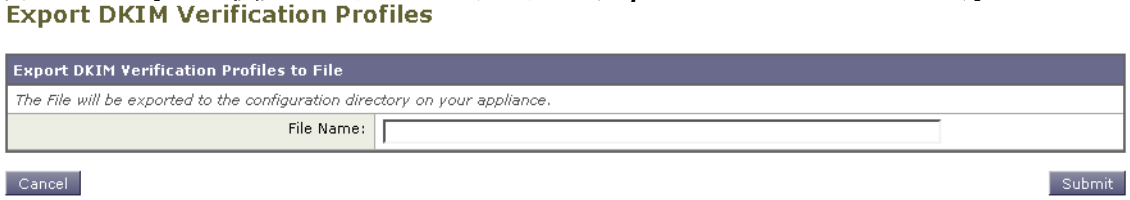
ステップ 14　この時点で着信メール フロー ポリシーで DKIM 検証をイネーブルにし、使用する検証プロファイルを選択する必要があります。

DKIM 検証プロファイルのエクスポート

DKIM 検証プロファイルをエクスポートする場合、Cisco IronPort アプライアンス上に存在するすべての DKIM 検証プロファイルが単一のテキスト ファイルとしてエクスポートされ、アプライアンスの configuration ディレクトリに保存されます。DKIM 検証プロファイルをエクスポートする手順は次のとおりです。

ステップ 1　[メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] ページの [プロファイルをエクスポート（Export Profiles）] をクリックします。[DKIM 検証プロファイルのエクスポート（Export DKIM Verification Profile）] ページが表示されます。

図 5-14　[DKIM 検証プロファイルのエクスポート（Export DKIM Verification Profile）] ページ



ステップ 2　ファイルの名前を入力し、[送信（Submit）] をクリックします。

DKIM 検証プロファイルのインポート

既存のファイルから DKIM 検証プロファイルをインポートするには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] ページの [プロファイルをインポート（Import Profiles）] をクリックします。[DKIM 検証プロファイルのインポート（Import DKIM Verification Profile）] ページが表示されます。

ステップ 2　DKIM 検証プロファイルを含むファイルを選択します。

ステップ 3　[送信（Submit）] をクリックします。インポートによってすべての既存の DKIM 検証プロファイルが置き換えられることが警告されます。

ステップ 4　[インポート（Import）] をクリックします。

DKIM 検証プロファイルの削除

DKIM 検証プロファイルのリストから特定の DKIM 検証プロファイルを削除するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] ページで、削除する各 DKIM 検証プロファイルの右にあるチェックボックスをオンにします。

ステップ 2　[削除（Delete）] をクリックします。

ステップ 3　削除を確認します。

現在設定されているすべての DKIM 検証プロファイルを削除するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [検証プロファイル（Verification Profiles）] ページの [すべてのプロファイルを消去（Clear All Profiles）] をクリックします。

ステップ 2　削除を確認します。

DKIM 検証プロファイルの検索

すべての DKIM 検証プロファイルについてプロファイル名から特定の用語を検索します。

ステップ 1　[DKIM 検証プロファイル（DKIM Verification Profiles）] ページの [次の DKIM 検証プロファイルを検索（Search DKIM Verification Profiles for）] フィールドに検索語を指定します。

ステップ 2　[プロファイルの検索（Find Profiles）] をクリックします。

検索では、各 DKIM 検証プロファイル名をスキャンします。

検索語を入力しない場合、検索エンジンはすべての DKIM 検証プロファイルを返します。

メール フロー ポリシーでの DKIM 検証の設定

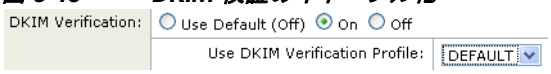
DKIM 検証は、受信メールのメール フロー ポリシーでイネーブルにします。

受信メール フロー ポリシーで検証をイネーブルにするには、次の手順を実行します。

ステップ 1　[Mail Flow Policies] ページ（[Mail Policies] メニューから）で、検証を実行するリスナーの受信メール ポリシーをクリックします。

ステップ 2　メール フロー ポリシーの [Security Features] セクションで、[On] を選択して、[DKIM Verification] をイネーブルにします。

図 5-15　DKIM 検証のイネーブル化



ステップ 3　ポリシーで使用する DKIM 検証プロファイルを選択します。

ステップ 4　変更を保存します。

DKIM 検証とロギング

DKIM 検証時には、次のような行がメール ログに追加されます。

```
mail.current:Mon Aug 6 13:35:38 2007 Info: MID 17 DKIM: no signature


mail.current:Mon Aug 6 15:00:37 2007 Info: MID 18 DKIM: verified pass
```

DKIM 検証済みメールのアクションの設定

DKIM メールを検証すると、メールに *Authentication-Results* ヘッダーが追加されますが、認証結果に関係なく、メールは受け入れられます。これらの認証結果に基づいてアクションを設定するには、コンテンツ フィルタを作成して、DKIM 検証済みメールに対するアクションを実行します。たとえば、DKIM 検証が失敗した場合、メールを配信、バウンス、ドロップ、または隔離エリアに送るように設定できます。これを実行するには、コンテンツ フィルタを使用して、アクションを設定する必要があります。

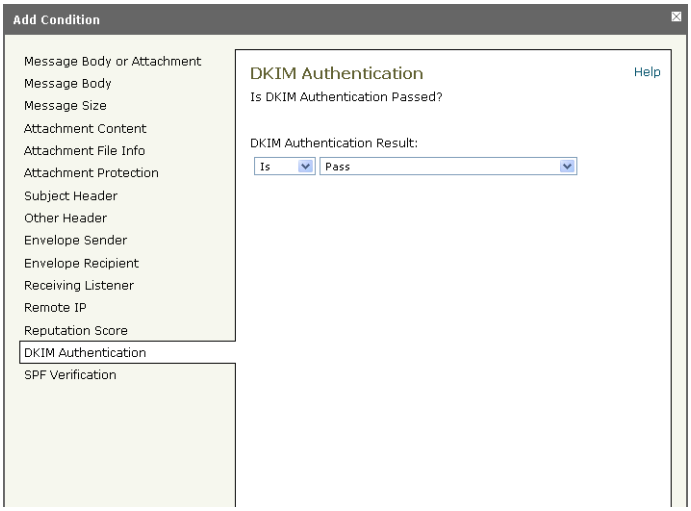
GUI からアクションを追加するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [受信フィルタ（Incoming Filters）] で [フィルタの追加（Add Filter）] をクリックします。

ステップ 2　[条件（Conditions）] セクションで [条件を追加（Add Condition）] をクリックします。

ステップ 3　[DKIM Authentication] 認証を選択します。

図 5-16　　DKIM 認証コンテンツ フィルタの条件



ステップ 4　DKIM 条件を選択します。次のオプションのいずれかを選択します。

- **[Pass]。メッセージは認証テストに合格しました。**
- [Neutral]。メッセージは署名されていません。
- [Temperror]。修復可能なエラーが発生しました。
- [Permerror]。修復不可能なエラーが発生しました。
- [Hardfail]。認証テストが失敗しました。
- [None]。認証が実行されませんでした。

ステップ 5　条件に関連付けるアクションを選択します。たとえば、DKIM 検証が失敗した場合、受信者に通知し、メッセージをバウンスさせることができます。または DKIM 検証に合格した場合、それ以上処理せずに、メッセージをすぐに配信できます。

ステップ 6　新しいコンテンツ フィルタを送信します。

ステップ 7　適切な受信メール ポリシーでコンテンツ フィルタをイネーブルにします。

ステップ 8　変更を保存します。

SPF および SIDF 検証の概要

Cisco IronPort AsyncOS は、Sender Policy Framework（SPF）および Sender ID Framework（SIDF）検証をサポートしています。SPF と SIDF は DNS レコードに基づいて電子メールの信頼性を検証する方法です。SPF と SIDF により、インターネット ドメインの所有者は、特別な形式の DNS TXT レコードを使用して、そのドメインに電子メールを送信する権限のあるマシンを指定することができます。

SPF/SIDF 認証を使用すると、送信側はそれらの名前の使用が許可されるホストを指定する SPF レコードをパブリッシュし、準拠するメール受信側はパブリッシュされた SPF レコードを使用して、メール トランザクション中に送信側のメール転送エージェントの ID の権限をテストします。

（注）　SPF チェックでは、解析と評価が必要であるため、AsyncOS のパフォーマンスに影響する場合があります。さらに、SPF チェックによって、DNS インフラストラクチャの負荷が増えることに注意してください。

SPF と SIDF を操作する場合、SIDF は SPF に似ていますが、いくつかの違いがあります。SIDF と SPF のすべての違いの説明については、RFC 4406 を参照してください。このマニュアルの目的のため、この 2 つの用語は、1 つのタイプの検証のみを適用する場合を除いて、まとめて説明しています。

AsyncOS は IPv4 アドレスと IPv6 アドレスの両方に対して SPF をサポートしています。

（注）　AsyncOS は着信リレーに対して SPF をサポートしていません。

有効な SPF レコードに関する注意

Cisco IronPort アプライアンスで SPF および SIDF を使用するには、RFC 4406 および 4408 に従って、SPF レコードをパブリッシュします。PRA ID の決定方法の定義については、RFC 4407 を確認してください。さらに、SPF レコードと SIDF レコードを作成する場合に犯しやすい誤りについては、次の Web サイトを参照してください。

```
http://www.openspf.org/FAQ/Common_mistakes
```

有効な SPF レコード

SPF HELO チェックに合格するには、各送信側 MTA に（ドメインとは別に）「v=spf1 a –all」SPF レコードを含めます。このレコードを含めないと、HELO チェックは HELO ID に None 判定を下す可能性があります。ドメインへの SPF 送信側が大量の None 判定を返した場合、これらの送信側は各送信側 MTA に「v=spf1 a –all」SPF レコードを含めていない可能性があります。

有効な SIDF レコード

SIDF フレームワークをサポートするには、「v=spf1」レコードと「spf2.0」レコードの両方をパブリッシュする必要があります。たとえば、DNS レコードは次の例のようになります。

```
example.com. TXT "v=spf1 +mx a:colo.example.com/28 -all"

smtp-out.example.com TXT "v=spf1 a -all"

example.com. TXT "spf2.0/mfrom,pra +mx a:colo.example.com/28 -all"
```

SIDF は HELO ID を検証しないため、この場合、各送信側 MTA に SPF v2.0 レコードをパブリッシュする必要はありません。

（注）　SIDF をサポートしない場合は、「spf2.0/pra ~all」レコードをパブリッシュします。

SPF レコードのテスト

RFC の確認に加えて、Cisco IronPort アプライアンスに SPF 検証を実装する前に、SPF レコードをテストすることを推奨します。openspf.org Web サイトでは、いくつかのテスト ツールが提供されています。

`http://www.openspf.org/Tools`

次のツールを使用して、電子メールが SPF レコード チェックに失敗した理由を判断できます。

`http://www.openspf.org/Why`

さらに、テスト リスナーで SPF をイネーブルにし、シスコの `trace` CLI コマンドを使用して（または GUI からトレースを実行して）、SPF 結果を表示できます。トレースを使用すると、さまざまな送信側 IP を簡単にテストできます。

Cisco IronPort E メール セキュリティ アプライアンスでの SPF の使用

Cisco IronPort アプライアンスで SPF/SIDF を使用するには、次の手順を実行します。

ステップ 1　**SPF/SIDF をイネーブルにします。**デフォルトのメール フロー ポリシーから、受信リスナーの SPF/SIDF をイネーブルにするか、さまざまな受信メール ポリシーでそれをイネーブルにできます。詳細については、SPF と SIDF のイネーブル化（5-24 ページ）を参照してください。

ステップ 2　**SPF/SIDF 検証済みメールに対して実行するアクションを設定します。**メッセージまたはコンテンツ フィルタを使用して、SPF 検証済みメールに対して実行するアクションを判断することができます。詳細については、SPF/SIDF 検証済みメールに対して実行するアクションの決定（5-30 ページ）を参照してください。

ステップ 3　**SPF/SIDF 結果をテストします。**組織では、さまざまな電子メール認証方法が使われており、各組織で SPF/SIDF の使用方法が異なることがある（たとえば、SPF または SIDF ポリシーの準拠する規格が異なる）ため、SPF/SIDF 結果をテストして、権限のある送信者からの電子メールをバウンスしたり、ドロップしたりしないようにする必要があります。コンテンツ フィルタ、メッセージ フィルタ、Content Filters レポートを組み合わせて使用し、SPF/SIDF 結果をテストできます。SPF/SIDF 結果のテストの詳細については、SPF/SIDF 結果のテスト（5-34 ページ）を参照してください。

警告　**シスコでは、グローバルな電子メール認証を強く奨励していますが、業界での採用途上にある現時点では、SPF/SIDF 認証の失敗に対して慎重な処理を行うよう提案しています。さらに多くの組織で社内公認のメール送信インフラストラクチャの制御能力が向上するまでは、シスコは電子メールのバウンスを回避し、代わりに SPF/SIDF 検証に失敗した電子メールを隔離できます。**

AsyncOS コマンドライン インターフェイス（CLI）では、Web インターフェイスよりも詳細な SPF レベルの制御設定を提供しています。SPF 判定に基づいて、アプライアンスは、リスナー単位で SMTP カンバセーションにおいてメッセージを許可または拒否できます。SPF の設定は、`listenerconfig` コマンドを使用してリスナーのホスト アクセス テーブルのデフォルト設定を編集するときに変更できます。設定の詳細については、CLI を使用した SPF および SIDF のイネーブル化（5-25 ページ）を参照してください。

SPF と SIDF のイネーブル化

SPF/SIDF を使用するには、受信リスナーでメール フロー ポリシーの SPF/SIDF をイネーブルにする必要があります。デフォルトのメール フロー ポリシーから、リスナーで SPF/SIDF をイネーブルにするか、特定の受信メール ポリシーについて SPF/SIDF をイネーブルにすることができます。

GUI によって、デフォルトのメール フロー ポリシーで SPF/SIDF をイネーブルにするには、次の手順を実行します。

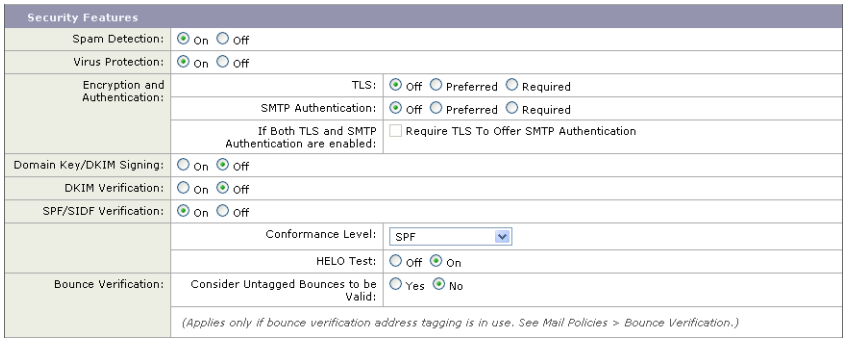
ステップ 1　[Mail Policies] > [Mail Flow Policy] をクリックします。

ステップ 2　[Default Policy Parameters] をクリックします。

ステップ 3　デフォルトのポリシー パラメータで、[セキュリティ サービス（Security Features）] セクションを表示します。

ステップ 4　[SPF/SIDF Verification] セクションで、[Yes] をクリックします。

図 5-17　メール フロー ポリシーの SPF/SIDF のイネーブル化



ステップ 5　準拠のレベルを設定します（デフォルトは SIDF 互換）。このオプションを使用して、使用する SPF または SIDF 検証の規格を判断できます。SIDF 準拠に加えて、SPF と SIDF を組み合わせた SIDF 互換を選択できます。

表 5-1　SPF/SIDF 準拠レベル

準拠レベル	説明
SPF	SPF/SIDF 検証は RFC4408 に従って動作します。 - PRA（Purported Responsible Address）ID 検証は行われません。 **注**：HELO ID に対してテストするには、この準拠オプションを選択します。
SIDF	SPF/SIDF 検証は RFC4406 に従って動作します。 - PRA ID は規格への完全準拠によって判断されます。 - SPF v1.0 レコードは spf2.0/mfrom,pra として扱われます。 - 存在しないドメインや形式が誤った ID については、Fail の判定が返されます。

表 5-1　SPF/SIDF 準拠レベル（続き）

準拠レベル	説明
SIDF 互換（SIDF Compatible）	SPF/SIDF 検証は、次の違いを*除き*、RFC4406 に従って動作します。 - SPF v1.0 レコードは spf2.0/mfrom として扱われます。 - 存在しないドメインや形式が誤った ID については、None の判定が返されます。 **注**: この準拠オプションは、OpenSPF コミュニティ（www.openspf.org）の要求に応じて導入されました。

（注） CLI からはさらに多くの設定を使用できます。詳細については、CLI を使用した SPF および SIDF のイネーブル化（5-25 ページ）を参照してください。

ステップ 6　SIDF 互換の準拠レベルを選択した場合、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうかを設定します。このオプションをセキュリティ目的で選択できます。

ステップ 7　SPF の準拠レベルを選択した場合、HELO ID に対してテストを実行するかどうかを設定します。このオプションを使用して、HELO チェックをディセーブルにすることによって、パフォーマンスが向上することがあります。これは、`spf-passed` フィルタ ルールで、PRA または MAIL FROM ID が最初にチェックされるため、便利な場合があります。アプライアンスは SPF 準拠レベルに対してのみ HELO チェックを実行します。

CLI を使用した SPF および SIDF のイネーブル化

AsyncOS CLI では各 SPF/SIDF 準拠レベルのより詳細な制御設定をサポートしています。リスナーのホスト アクセス テーブルのデフォルトの設定をする場合、リスナーの SPF/SIDF 準拠レベルと、アプライアンスが SPF/SIDF 検証結果に基づいて実行する SMTP アクション（ACCEPT または REJECT）を選択できます。アプライアンスがメッセージを拒否する場合に送信する SMTP 応答を定義することもできます。

準拠レベルに応じて、アプライアンスは HELO ID、MAIL FROM ID、または PRA ID に対してチェックを実行します。アプライアンスが、次の各 ID チェックの各 SPF/SIDF 検証結果に対し、セッションを続行する（ACCEPT）か、セッションを終了する（REJECT）かを指定できます。

- **[None]。**情報の不足のため、検証を実行できません。
- **[Neutral]。**ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- **[SoftFail]。**ドメイン所有者は、ホストが指定された ID を使用する権限がないと思うが、断言を避けたいと考えています。
- **[Fail]。**クライアントは、指定された ID でメールを送信する権限がありません。
- **[TempError]。**検証中に一時的なエラーが発生しました。
- **[Permerror]。**検証中に永続的なエラーが発生しました。

アプライアンスは、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、PRA ID の Pass 結果を None にダウングレードするように SIDF 互換準拠レベルを設定していない限り、Pass 結果のメッセージを受け入れます。アプライアンスは PRA チェックで None が返された場合に指定された SMTP アクションを実行します。

ID チェックに対して SMTP アクションを定義していない場合、アプライアンスは Fail を含むすべての検証結果を自動的に受け入れます。

イネーブルにされたいずれかの ID チェックの ID 検証結果が REJECT アクションに一致する場合、アプライアンスはセッションを終了します。たとえば、管理者は、すべての HELO ID チェック結果に基づいてメッセージを受け入れるようにリスナーを設定しますが、MAIL FROM ID チェックからの Fail 結果に対してはメッセージを拒否するようにリスナーを設定するとします。メッセージが HELO ID チェックに失敗しても、アプライアンスはその結果を受け入れるため、セッションが続行します。次に、メッセージが MAIL FROM ID チェックで失敗した場合、リスナーはセッションを終了し、REJECT アクションの STMP 応答を返します。

SMTP 応答は、アプライアンスが SPF/SIDF 検証結果に基づいてメッセージを拒否する場合に返すコード番号とメッセージです。TempError 結果は、他の検証結果と異なる SMTP 応答を返します。TempError の場合、デフォルトの応答コードは `451` で、デフォルトのメッセージ テキストは「`#4.4.3 Temporary error occurred during SPF verification`」です。他のすべての検証結果の場合のデフォルトの応答コードは `550` で、デフォルトのメッセージ テキストは「`#5.7.1 SPF unauthorized mail is prohibited`」です。TempError や他の検証結果に独自の応答コードとメッセージ テキストを指定できます。

任意で、Neutral、SoftFail、または Fail 検証結果に対して REJECT アクションが実行された場合に、SPF パブリッシャ ドメインから、サードパーティの応答を返すように、アプライアンスを設定することができます。デフォルトで、アプライアンスは次の応答を返します。

```
550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>
```

これらの SPF/SIDF 設定をイネーブルにするには、`listenerconfig -> edit` サブコマンドを使用し、リスナーを選択します。次に、`hostaccess -> default` サブコマンドを使用して、ホスト アクセス テーブルのデフォルトの設定を編集します。次のプロンプトに `yes` と答えて、SPF 制御を設定します。

```
Would you like to change SPF/SIDF settings?  [N]> yes

Would you like to perform SPF/SIDF Verification?  [Y]> yes
```

ホスト アクセス テーブルでは、次の SPF 制御設定を使用できます。

表 5-2　　CLI を使用した SPF 制御設定

準拠レベル	使用可能な SPF 制御設定
SPF のみ（SPF Only）	• HELO ID チェックを実行するかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション – HELO ID（イネーブルの場合） – MAIL FROM ID • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

表 5-2　CLI を使用した SPF 制御設定（続き）

準拠レベル	使用可能な SPF 制御設定
SIDF 互換（SIDF Compatible）	• HELO ID チェックを実行するかどうか • メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション – HELO ID（イネーブルの場合） – MAIL FROM ID – PRA Identity • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 厳格（SIDF Strict）	• 次の ID チェックの結果に基づいて実行される SMTP アクション – MAIL FROM ID – PRA Identity • SPF REJECT アクションの場合に返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

次に、ユーザが SPF Only 準拠レベルを使用して、SPF/SIDF 検証を設定する例を示します。アプライアンスは HELO ID チェックを実行し、None および Neutral 検証結果を受け入れ、その他の結果を拒否します。SMTP アクションの CLI プロンプトはすべての ID タイプで同じです。ユーザは MAIL FROM ID の SMTP アクションを定義しません。アプライアンスは、その ID のすべての検証結果を自動的に受け入れます。アプライアンスはすべての REJECT 結果に対して、デフォルトの拒否コードとテキストを使用します。

```
Would you like to change SPF/SIDF settings?  [N]> yes


Would you like to perform SPF/SIDF Verification?  [N]> yes


What Conformance Level would you like to use?

1. SPF only

2. SIDF compatible

3. SIDF strict

[2]> 1
```

```
Would you like to have the HELO check performed? [Y]> y

Would you like to change SMTP actions taken as result of the SPF verification? [N]> y

Would you like to change SMTP actions taken for the HELO identity? [N]> y

What SMTP action should be taken if HELO check returns None?
1. Accept
2. Reject
[1]> 1

What SMTP action should be taken if HELO check returns Neutral?
1. Accept
2. Reject
[1]> 1

What SMTP action should be taken if HELO check returns SoftFail?
1. Accept
2. Reject
[1]> 2

What SMTP action should be taken if HELO check returns Fail?
1. Accept
2. Reject
    [1]> 2

    What SMTP action should be taken if HELO check returns TempError?
    1. Accept
```

```
2. Reject

[1]> 2


What SMTP action should be taken if HELO check returns PermError?

1. Accept

2. Reject

[1]> 2


Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n


Would you like to change SMTP response settings for the REJECT action? [N]> n


Verification timeout (seconds)

[40]>
```

次に、リスナーのデフォルトのポリシー パラメータに SPF/SIDF 設定がどのように表示されるかを示します。

```
SPF/SIDF Verification Enabled: Yes

  Conformance Level: SPF only

  Do HELO test: Yes

  SMTP actions:

    For HELO Identity:

      None, Neutral: Accept

      SoftFail, Fail, TempError, PermError: Reject

    For MAIL FROM Identity: Accept

  SMTP Response Settings:

    Reject code: 550

    Reject text: #5.7.1 SPF unauthorized mail is prohibited.

    Get reject response text from publisher: Yes
```

```
    Defer code: 451

    Defer text: #4.4.3 Temporary error occurred during SPF verification.

  Verification timeout: 40
```

`listenerconfig` コマンドの詳細については、*Cisco IronPort AsyncOS CLI Reference Guide* を参照してください。

Received-SPF ヘッダー

AsyncOS で SPF/SIDF 検証を設定すると、電子メールに SPF/SIDF 検証ヘッダー（`Received-SPF`）が配置されます。さらに、Received-SPF ヘッダーには、次の情報が含まれます。

- **検証結果**：SPF 検証結果（検証結果（5-31 ページ）を参照してください）。
- **ID**：SPF 検証でチェックされた ID：HELO、MAIL FROM、PRA。
- **レシーバ**：検証するホスト名（チェックを実行する）。
- **クライアント IP アドレス**：SMTP クライアントの IP アドレス。
- **ENVELOPE FROM**：エンベロープ送信者メールボックス。（MAIL FROM ID は空にすることができないため、これは、MAIL FROM ID と異なることがあります）。
- **x-sender**：HELO、MAIL FROM、または PRA ID の値。
- **x-conformance**：準拠のレベル（表 5-1 SPF/SIDF 準拠レベル（5-24 ページ）を参照）と PRA チェックのダウングレードが実行されたかどうか。

次の例に、SPF/SIDF チェックに合格したメッセージに追加されるヘッダーを示します。

```
Received-SPF: Pass identity=pra; receiver=box.example.com;

    client-ip=1.2.3.4; envelope-from="alice@fooo.com";

    x-sender="alice@company.com"; x-conformance=sidf_compatible
```

（注）　`spf-status` および `spf-passed` フィルタ ルールでは、received-SPF ヘッダーを使用して、SPF/SIDF 検証の状態が判断されます。

SPF/SIDF 検証済みメールに対して実行するアクションの決定

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。次のメッセージおよびコンテンツ フィルタ ルールを使用して、SPF/SIDF 検証済みメールの状態を判断し、検証結果に基づいてメッセージへのアクションを実行できます。

- `spf-status`。このフィルタ ルールは SPF/SIDF 状態に基づいてアクションを決定します。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。
- `spf-passed`。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。

（注）　spf-passed フィルタ ルールはメッセージ フィルタでのみ使用できます。

より詳細な結果に対処する必要がある場合は、spf-status ルールを使用し、簡単なブール値を作成する必要がある場合は spf-passed ルールを使用できます。

検証結果

spf-status フィルタ ルールを使用する場合、次の構文を使用して、SPF/SIDF 検証結果に対してチェックできます。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

（注）　spf-status メッセージ フィルタ ルールは、HELO、MAIL FROM、PRA ID に対して結果をチェックする場合にのみ使用できます。spf-status コンテンツ フィルタ ルールは、ID に対してチェックする場合に使用できません。

次のいずれかの検証結果を受け取る可能性があります。

- None：情報の不足のため、検証を実行できません。
- Pass：クライアントは、指定された ID でメールを送信する権限があります。
- Neutral：ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- SoftFail：ドメイン所有者は、指定された ID を使用する権限がホストにないと思うが、断言を避けたいと考えています。
- Fail：クライアントは、指定された ID でメールを送信する権限がありません。
- TempError：検証中に一時的なエラーが発生しました。
- PermError：検証中に永続的なエラーが発生しました。

CLI での spf-status フィルタ ルールの使用

次の例に、spf-status メッセージ フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:

     if (sendergroup == "TRUSTED" and spf-status == "Pass"){

         skip-spamcheck();

     }


quarantine-spf-failed-mail:

     if (spf-status("pra") == "Fail") {

         if (spf-status("mailfrom") == "Fail"){

             # completely malicious mail

             quarantine("Policy");

         } else {

           if(spf-status("mailfrom") == "SoftFail") {

             # malicious mail, but tempting

             quarantine("Policy");

           }

         }

     } else {

       if(spf-status("pra") == "SoftFail"){

         if (spf-status("mailfrom") == "Fail"

                  or spf-status("mailfrom") == "SoftFail"){

             # malicious mail, but tempting

             quarantine("Policy");

         }

       }

     }
```

```
stamp-mail-with-spf-verification-error:

     if (spf-status("pra") == "PermError, TempError"

             or spf-status("mailfrom") == "PermError, TempError"

             or spf-status("helo") == "PermError, TempError"){

          # permanent error - stamp message subject

          strip-header("Subject");

          insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }
```

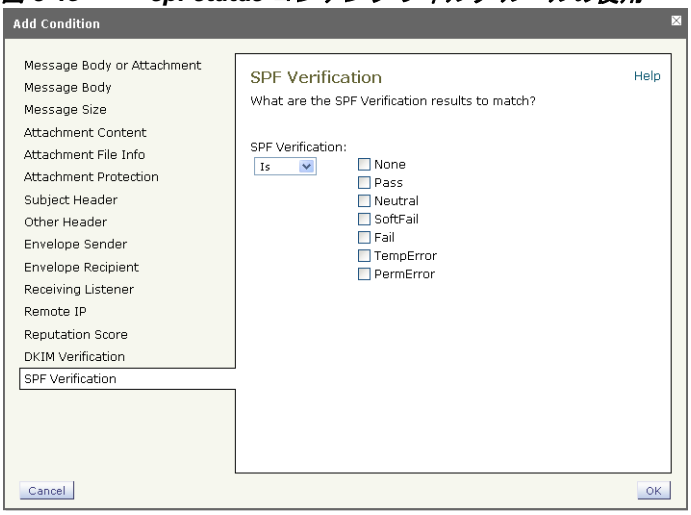
.

GUI での spf-status コンテンツ フィルタ ルール

GUI でコンテンツ フィルタから spf-status ルールをイネーブルにすることもできます。ただし、spf-status コンテンツ フィルタ ルールを使用した場合、HELO、MAIL FROM、PRA ID に対して結果をチェックできません。

GUI から spf-status コンテンツ フィルタ ルールを追加するには、[メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。次に [条件を追加（Add Condition）] ダイアログボックスから、[SPF 検証（SPF Verification）] フィルタ ルールを追加します。条件に、1 つ以上の検証結果を指定します。

図 5-18　　spf-status コンテンツ フィルタ ルールの使用



SPF 検証条件を追加したら、SPF 状態に基づいて実行するアクションを指定します。たとえば、SPF 状態が SoftFail の場合、メッセージを隔離します。

spf-passed フィルタ ルールの使用

spf-passed ルールは SPF 検証の結果をブール値として表示します。次の例に、spf-passed とマークされていない電子メールを隔離するために使用する spf-passed ルールを示します。

```
quarantine-spf-unauthorized-mail:

    if (not spf-passed) {

        quarantine("Policy");

    }
```

（注）　spf-status ルールと異なり spf-passed ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、spf-passed ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、spf-status ルールを使用します。

SPF/SIDF 結果のテスト

組織によって SPF/SIDF の実装方法が異なるため、SPF/SIDF 検証の結果をテストし、これらの結果を使用して、SPF/SIDF の失敗の処理方法を決定します。コンテンツ フィルタ、メッセージ フィルタ、Email Security Monitor - Content Filters レポートを組み合わせて使用し、SPF/SIDF 検証の結果をテストします。

SPF/SIDF 検証の依存度によって、SPF/SIDF 結果をテストする詳細レベルが決まります。

SPF/SIDF 結果の基本の詳細度のテスト

受信メールの SPF/SIDF 検証結果の基本評価基準を取得するため、コンテンツ フィルタと [メールセキュリティモニタ-コンテンツフィルタ（Email Security Monitor - Content Filters）] ページを使用できます。このテストでは、SPF/SIDF 検証結果のタイプごとに受信されたメッセージ数が表示されます。

基本 SPF/SIDF 検証テストを実行するには、次の手順を実行します。

ステップ 1　受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにし、コンテンツ フィルタを使用して、実行するアクションを設定します。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化（5-24 ページ）を参照してください。

ステップ 2　SPF/SIDF 検証のタイプごとに spf-status コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。spf-status コンテンツ フィルタの作成については、GUI での spf-status コンテンツ フィルタ ルール（5-33 ページ）を参照してください。

ステップ 3　多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（Content Filters）] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

SPF/SIDF 結果の高い詳細度のテスト

SPF/SIDF 検証結果のより包括的な情報を得るには、送信者の特定のグループの SPF/SIDF 検証をイネーブルにし、それらの特定の送信者の結果を確認するだけです。次に、その特定のグループのメール ポリシーを作成し、メール ポリシーで SPF/SIDF 検証をイネーブルにします。SPF/SIDF 結果の基本の詳細度のテスト（5-34 ページ）で説明するように、コンテンツ フィルタを作成し、Content Filters レポートを確認します。検証が有効であることがわかったら、この指定した送信者のグループの電子メールをドロップするかバウンスするかの決断の基準として、SPF/SIDF 検証を使用できます。

詳細な SPF/SIDF 検証テストを実行するには、次の手順を実行します。

ステップ 1　SPF/SIDF 検証のメール フロー ポリシーを作成します。受信リスナーで、メール フロー ポリシーの SPF/SIDF 検証をイネーブルにします。SPF/SIDF をイネーブルにする方法については、SPF と SIDF のイネーブル化（5-24 ページ）を参照してください。

ステップ 2　SPF/SIDF 検証の送信者グループを作成し、命名規則を使用して、SPF/SIDF 検証を示します。送信者グループの作成については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「ゲートウェイでのメール受信の設定」の章を参照してください。

ステップ 3　SPF/SIDF 検証のタイプごとに `spf-status` コンテンツ フィルタを作成します。命名規則を使用して、検証のタイプを示します。たとえば、SPF/SIDF 検証に合格したメッセージには「SPF-Passed」を使用し、検証中の一時的エラーのために合格しなかったメッセージには、「SPF-TempErr」を使用します。`spf-status` コンテンツ フィルタの作成については、GUI での spf-status コンテンツ フィルタ ルール（5-33 ページ）を参照してください。

ステップ 4　多数の SPF/SIDF 検証済みメッセージの処理後、[モニタ（Monitor）] > [コンテンツフィルタ（Content Filters）] をクリックして、各 SPF/SIDF 検証済みコンテンツ フィルタをトリガーしたメッセージ数を確認します。

CHAPTER 6

メッセージ フィルタを使用した電子メール ポリシーの適用

Cisco IronPort アプライアンスは、詳細なコンテンツ スキャンおよびメッセージ フィルタリング テクノロジーを備えているため、会社のネットワークに参加または退出するときに、会社のポリシーを適用して、特定のメッセージを処理することができます。

この章では、ポリシーの適用のために使用可能な機能（コンテンツ スキャン エンジン、メッセージ フィルタ、添付ファイル フィルタ、コンテンツ ディクショナリ）の強力な組み合わせについて説明します。

この章は、次の項で構成されています。

概要

メッセージ フィルタにより、Cisco IronPort アプライアンスでメッセージを受信したときに、それらを処理する方法を記述した特別なルールを作成できます。メッセージ フィルタは、特定の種類の電子メール メッセージに指定の特別な処理を施す必要があることを指定します。Cisco IronPort メッセージ フィルタは、指定の単語に対してメッセージ内容をスキャンすることによって社内メール ポリシーを適用することができます。この章は、次の項で構成されています。

- **メッセージ フィルタのコンポーネント**。メッセージ フィルタにより、メッセージの受信時にそれらを処理する方法を記述した特別なルールを作成できます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションにより、通知を生成したり、メッセージのドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、変更を行ったりすることができます。詳細については、メッセージ フィルタのコンポーネント（6-2 ページ）を参照してください。

- **メッセージ フィルタの処理**。AsyncOS がメッセージ フィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行されるアクションは、メッセージ フィルタの順番、メッセージの内容を変更した可能性のある事前の処理、メッセージの MIME 構造、コンテンツ マッチング用に設定されたしきい値スコア、クエリーの構造などのいくつかの要因に基づきます。詳細については、メッセージ フィルタ処理（6-4 ページ）を参照してください。
- **メッセージ フィルタ ルール**。各フィルタには、フィルタで処理できる一連のメッセージを定義するルールがあります。メッセージ フィルタを作成する場合、それらのルールを定義します。詳細については、メッセージ フィルタ ルール（6-10 ページ）を参照してください。
- **メッセージ フィルタ アクション**。各フィルタには、ルールで `true` に評価された場合に、メッセージに対して実行するアクションがあります。実行できるアクションには、最終アクション（メッセージの配信、ドロップ、バウンスなど）、またはメッセージをさらに処理できる非最終アクション（ヘッダーの除去や挿入など）の 2 つのタイプのアクションがあります。詳細については、メッセージ フィルタ アクション（6-44 ページ）を参照してください。
- **添付ファイル スキャン メッセージ フィルタ**。添付ファイル スキャン メッセージ フィルタを使用して、会社のポリシーと整合しないメッセージから添付ファイルを除去できます。元のメッセージはそのまま配信することができます。添付ファイルは、それらの特定のタイプ、フィンガープリント、内容に基づいてフィルタできます。イメージ アナライザを使用して、イメージ添付ファイルをスキャンすることもできます。イメージ アナライザは、肌の色、本文サイズ、曲率を測定して、グラフィックに不適切な内容が含まれている可能性を判断するアルゴリズムを作成します。詳細については、添付ファイルのスキャン（6-68 ページ）を参照してください。
- **CLI を使用したメッセージ フィルタの管理**。CLI は、メッセージ フィルタを操作するためのコマンドを受け入れます。たとえば、メッセージ フィルタのリストを表示、並び替え、インポート、エクスポートする必要がある場合があります。詳細については、CLI を使用したメッセージ フィルタの管理（6-79 ページ）を参照してください。
- **メッセージ フィルタの例**。この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。詳細については、メッセージ フィルタの例（6-101 ページ）を参照してください。

メッセージ フィルタのコンポーネント

メッセージ フィルタにより、メッセージの受信時にそれらを処理する方法を記述した特別なルールを作成できます。メッセージ フィルタは、メッセージ フィルタ ルールとメッセージ フィルタ アクションから構成されます。

メッセージ フィルタ ルール

メッセージ フィルタ ルールによって、フィルタで処理するメッセージを判断します。ルールは、論理結合子 AND、OR、NOT を使用して組み合わせることで、複雑なテストを作成できます。ルール式は、かっこを使用してグループ化することもできます。

メッセージ フィルタ アクション

メッセージ フィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の 2 つのタイプがあります。

- *最終*アクション（deliver、drop、bounce など）はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- *非最終*アクションは、メッセージをさらに処理することを許可するアクションを実行します。

（注） 非最終メッセージ フィルタ アクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタ アクションが適用されます。

メッセージ フィルタの構文例

フィルタ仕様の直観的な意味は次のようになります。

メッセージがルールに*一致する場合*、順番にアクションが適用されます。else 句が存在する場合、メッセージがルールに*一致しない場合*に else 句内のアクションが実行されます。

指定したフィルタ名によって、フィルタをアクティブ、非アクティブ、削除する場合に、フィルタが管理しやすくなります。

メッセージ フィルタでは次の構文を使用します。

構文例	目的
expedite:	フィルタ名
if (recv-listener == 'InboundMail' or recv-int == 'notmain')	ルールの指定

`{`
`    alt-src-host('outbound1');`
`skip_filters();`
`}`
	アクションの指定

`else`
`{`
`    alt-src-host('outbound2');`
`}`
	（任意）代替アクションの指定

代替アクションは省略できることに注意してください。

構文例	目的
expedite2:	フィルタ名
`if ((not (recv-listener == 'InboundMail')) and` **(not (recv-int == 'notmain')))**	ルールの指定

`{`
`    alt-src-host('outbound2');`
`skip_filters();`
}
	アクションの指定

複数のフィルタを順番に 1 つずつ並べて 1 つのテキスト ファイルにまとめることができます。

単一引用符または二重引用符で、フィルタの値を囲む必要があります。単一引用符または二重引用符は、値の両側に等しく組み合わせる必要があります。たとえば、式 `notify('customercare@example.com')` と `notify("customercare@example.com")` はどちらも有効ですが、式 `notify("customercare@example.com')` は構文エラーが発生します。

「`#`」文字で始まる行はコメントと見なされ、無視されます。ただし、それらは `filters -> detail` によってフィルタを表示して確認できるため、AsyncOS では保持されません。

メッセージ フィルタ処理

AsyncOS はメッセージ フィルタを処理する場合、AsyncOS がスキャンする内容、処理の順番、実行するアクションは、次のいくつかの要因に基づきます。

- **メッセージ フィルタの順番。**メッセージ フィルタは、順序付けられたリストで維持されます。メッセージの処理時に、AsyncOS は各メッセージ フィルタをそれらがリストに表示されている順番で適用します。最終アクションが行われた場合、そのメッセージに対して、それ以上のアクションは実行されません。詳細については、メッセージ フィルタの順番（6-4 ページ）を参照してください。
- **事前処理。**メッセージ フィルタが評価される前に、AsyncOS メッセージに対して実行されるアクションによって、ヘッダーが追加または削除されることがあります。AsyncOS は、処理時にメッセージに存在するヘッダーに対してメッセージ フィルタ プロセスを実行します。詳細については、メッセージ ヘッダー ルールおよび評価（6-5 ページ）を参照してください。
- **メッセージの MIME 構造。**メッセージの MIME 構造によって、「本文」として扱われるメッセージの部分と「添付ファイル」として扱われるメッセージの部分が判断されます。多くのメッセージ フィルタは、メッセージの本文部分のみに、または添付ファイル部分のみに作用するように設定されます。詳細については、メッセージ本文とメッセージ添付ファイル（6-5 ページ）を参照してください。
- **正規表現に設定されるしきい値スコア。**正規表現に一致させる場合、フィルタ アクションが実行されるまでに、一致が発生しなければならない回数を集計する「スコア」を設定します。これにより、さまざまな用語に対する応答の重み付けをすることができます。詳細については、コンテンツ スキャンの一致のしきい値（6-6 ページ）を参照してください。
- **クエリーの構造。**メッセージ フィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。さらに、システムは左から右にテストを評価しないことに注意することが重要です。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。詳細については、メッセージ フィルタ内の AND テストと OR テスト（6-9 ページ）を参照してください。

メッセージ フィルタの順番

メッセージ フィルタは順序付けられたリストに維持され、リスト内のそれらの位置によって番号付けされます。メッセージの処理時に、メッセージ フィルタが割り振られた番号順で適用されます。そのため、9 番のフィルタがメッセージに対してすでに最終アクション（バウンスなど）を実行した場合、30 番のフィルタは、メッセージの送信元ホストを変更する機会がありません。リストのフィルタの位置は、システム ユーザ インターフェイスによって変更できます。ファイルからインポートされたフィルタは、インポートされたファイル内のそれらの相対的順序に基づきます。

最終アクション後、そのメッセージに対して、それ以上のアクションは実行されません。

メッセージがフィルタ ルールに一致していても、次のいずれかの理由で、フィルタがそのメッセージに対して作用しないことがあります。

- フィルタが非アクティブである。
- フィルタが無効である。
- フィルタが、メッセージの最終アクションを実行した前のフィルタに取って代わられた。

メッセージ ヘッダー ルールおよび評価

フィルタは、ヘッダー ルールを適用する場合に、元のメッセージのヘッダーではなく、「処理済み」ヘッダーを評価します。つまり、

- 前に実行されたアクションによって、ヘッダーが追加された場合、後続のすべてのヘッダー ルールによって、それを照合できるようになります。
- 前に実行されたアクションによって、ヘッダーが取り除かれた場合、後続のすべてのヘッダー ルールで、それを照合できなくなります。
- 前に実行されたアクションによって、ヘッダーが変更された場合、後続のすべてのヘッダー ルールで、元のメッセージ ヘッダーではなく、変更済みのヘッダーが評価されます。

この動作は、メッセージ フィルタとコンテンツ フィルタの両方に共通です。

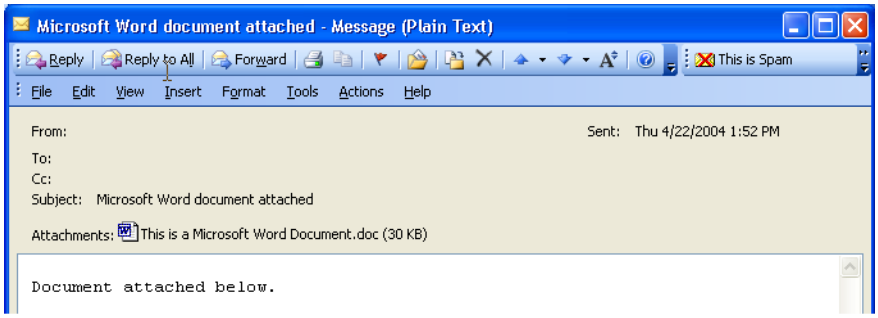
メッセージ本文とメッセージ添付ファイル

電子メール メッセージは、複数の部分から構成されます。RFC では、メッセージのヘッダーの後に続くすべてのものをマルチパート「メッセージ本文」として規定していますが、多くのユーザはまだメッセージの「本文」と「添付ファイル」を別々のものと捉えています。`body-`*variable* または `attachment-`*variable* という Cisco IronPort メッセージ フィルタを使用する場合、Cisco IronPort アプライアンスはほとんどのユーザが「本文」と「添付ファイル」として考える部分を、多くの MUA がそれらを別々にレンダリングしようと試みるのと同じように区別しようとします。

`body-`*variable* または `attachment-`*variable* メッセージ フィルタ ルールを書く目的では、メッセージ ヘッダーの後のすべてのものがメッセージ*本文*と見なされ、その内容は本文内にある MIME 部分の最初のテキスト部分と見なされます。そのコンテンツの後のすべてのもの（つまり、追加の MIME 部分）は*添付ファイル*と見なされます。AsyncOS はメッセージのさまざまな MIME 部分を評価し、添付ファイルとして処理されるファイルの部分を識別します。

たとえば、図 6-1 に、Microsoft Outlook MUA のメッセージを示します。ここでは「`Document attached below.`」という言葉がプレーン テキストのメッセージ*本文*として表示され、ドキュメント「`This is a Microsoft Word document.doc`」が*添付ファイル*として表示されています。多くのユーザが電子メールをこのように捉えている（最初の部分がプレーン テキストで 2 番めの部分がバイナリ ファイルであるマルチパート メッセージとしてではなく）ため、Cisco IronPort は、メッセージの「本文」（最初のプレーン テキスト部分）と対照的に、.doc ファイル部分（実質的に 2 番めの MIME 部分）を区別して処理するルールを作成するために、メッセージ フィルタで「添付ファイル」という用語を使用しています。ただし、RFCS 1521 および 1522 で使われている用語によると、メッセージの*本文*はすべての MIME 部分から構成されます。

図 6-1　　添付ファイルのあるメッセージ



Cisco IronPort アプライアンスは、マルチパート メッセージの*本文*と*添付ファイル*を区別しているため、想定される動作をするためには、`body-`*variable* または `attachment-`*variable* メッセージ フィルタ ルールを使用する場合に、いくつかのケースで注意が必要です。

- テキスト部分が 1 つのメッセージ（つまり、「Content-Type: text/plain」または「Content-Type: text/html」のヘッダーを含むメッセージ）がある場合、Cisco IronPort アプライアンスはメッセージ全体を本文と見なします。コンテンツ タイプが異なる場合、Cisco IronPort アプライアンスは、それを単一の添付ファイルと見なします。
- エンコードされたファイル（uuencoded など）は電子メール メッセージの本文に含まれます。これが発生した場合、エンコードされたファイルは添付ファイルとして扱われ、抽出およびスキャンされ、残りのテキストがテキスト本文として見なされます。
- 単一のテキスト以外の部分は常に*添付ファイル*と見なされます。たとえば、.zip ファイルのみで構成されるメッセージは、添付ファイルと見なされます。

コンテンツ スキャンの一致のしきい値

メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールを追加する場合、パターンが見つかる必要がある回数の最初のしきい値を指定できます。AsyncOS はメッセージをスキャンすると、メッセージおよび添付ファイルに見つかった一致の数の「スコア」を集計します。最小しきい値に満たない場合、正規表現は true と評価されません。このしきい値は次のフィルタ ルールに指定できます。

- body-contains
- only-body-contains
- attachment-contains
- every-attachment-contains
- dictionary-match
- attachment-dictionary-match

`drop-attachments-where-contains` アクションにしきい値を指定することもできます。

（注）　ヘッダーまたはエンベロープの受信者と送信者をスキャンするフィルタ ルールにしきい値を指定できません。

しきい値の構文

出現最小回数のしきい値を指定するには、パターンと、true と評価するために必要な一致の最小数を指定します。

```
if(<filter rule>('<pattern>',<minimum threshold>)){
```

たとえば、body-contains フィルタ ルールで、値「Company Confidential」が少なくとも 2 回見つかる必要があることを指定するには、次の構文を使用します。

```
if(body-contains('Company Confidential',2)){
```

デフォルトで、AsyncOS がコンテンツ スキャン フィルタを保存する場合、フィルタをコンパイルし、しきい値が割り当てられていない場合、1 のしきい値を割り当てます。

コンテンツ ディクショナリの値に対して、パターン マッチの最小数を指定することもできます。コンテンツ ディクショナリの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。

メッセージ本文と添付ファイルのしきい値スコア

電子メール メッセージは、複数の部分から構成されることがあります。メッセージ本文または添付ファイル内のパターンを検索するフィルタ ルールのしきい値を指定すると、AsyncOS は、メッセージ部分と添付ファイルの一致の数をカウントして、しきい値「スコア」を判断します。メッセージ フィルタで特定の MIME 部分を指定しない限り（attachment-contains フィルタ ルールなど）、AsyncOS はメッセージのすべての部分で見つかった一致を合計し、一致の合計がしきい値に達しているかどうかを判断します。たとえば、しきい値が 2 の body-contains メッセージ フィルタがあるとします。本文に 1 つの一致があり、添付ファイルに 1 つの一致があるメッセージを受信します。AsyncOS がこのメッセージを採点した場合、合計が 2 つの一致になり、しきい値スコアを満たしていると判断します。

同様に、複数の添付ファイルがある場合、AsyncOS は添付ファイルごとにスコアを合計して、一致のスコアを判断します。たとえば、しきい値が 3 の attachment-contains フィルタ ルールがあるとします。2 つの添付ファイルがあるメッセージを受信し、各添付ファイルに 2 つの一致が含まれます。AsyncOS はこのメッセージを 4 つの一致と採点し、しきい値スコアが満たされていると判断します。

しきい値スコアリング マルチパート/代替 MIME 部分

カウントの重複を避けるため、同じコンテンツの 2 つの表現（プレーン テキストと HTML）がある場合、AsyncOS は重複した部分からの一致を合計しません。代わりに、各部分の一致を比較して、最高値を選択します。AsyncOS はこの値をマルチパート メッセージの他の部分からのスコアに追加して、合計スコアを作成します。

たとえば、body-contains フィルタ ルールを設定し、しきい値を 4 に設定します。プレーン テキスト、HTML、および 2 つの添付ファイルを含むメッセージを受信します。メッセージは次のような構造を使用します。

```
multipart/mixed

        multipart/alternative
```

```
                text/plain

                text/html

        application/octet-stream

        application/octet-stream
```

body-contains フィルタ ルールは、メッセージの text/plain および text/html 部分を最初に採点して、このメッセージのスコアを判断します。次に、これらのスコアの結果を比較し、結果から最高のスコアを選択します。さらに、この結果を各添付ファイルからのスコアに追加して、最終スコアを判断します。メッセージに次の数の一致があるとします。

```
multipart/mixed

        multipart/alternative

                text/plain (2 matches)

                text/html (2 matches)

        application/octet-stream (1 match)

        application/octet-stream
```

AsyncOS は text/plain と text/html 部分の一致を比較するため、スコア 3 を返します。これは、フィルタ ルールをトリガーする最小しきい値を満たしていません。

コンテンツ ディクショナリを使用したしきい値のスコアリング

コンテンツ ディクショナリを使用すると、用語の「重み」を設定して、より簡単に特定の用語でフィルタ アクションをトリガーできます。たとえば、「bank」という用語ではメッセージ フィルタをトリガーせず、「bank」の後に「account」という用語があり、さらに ABA ルーティング番号が含まれていれば、フィルタ アクションをトリガーする必要があるとします。これを実現するには、重みを設定したディクショナリを使用して、特定の用語または用語の組み合わせの重要度を高くします。コンテンツ ディクショナリを使うメッセージ フィルタがフィルタ ルールの一致を評価する場合、コンテンツ ディクショナリの重みを使用して最終的なスコアを決定します。たとえば、次のコンテンツと重みを指定してコンテンツ ディクショナリを作成したとします。

表 6-1　　コンテンツ ディクショナリの例

用語/スマート ID	重み
ABA 送金番号	3
アカウント	2
バンク	1

このコンテンツ ディクショナリを dictionary-match または attachment-dictionary-match メッセージ フィルタ ルールに関連付けると、AsyncOS はメッセージ内で検出された一致する用語の各インスタンスの合計「スコア」に、この用語の重みを追加します。たとえば、メッセージ本文に用語「account」のインスタンスが 3 つ含まれているメッセージの合計スコアに、値 6 が追加されます。メッセージ フィルタのしきい値が 6 に設定されている場合、AsyncOS はこのしきい値スコアが満たされたと判断します。または、各用語のインスタンスが 1 つずつ含まれている場合も合計値は 6 になり、このスコアによってフィルタ アクションがトリガーされます。

メッセージ フィルタ内の AND テストと OR テスト

メッセージ フィルタ内で、AND または OR テストを評価する場合、AsyncOS は不要なテストを評価しません。したがって、たとえば、一方の AND テストが false の場合、もう一方のテストは評価されません。テストは左から右に評価されるわけではないため、注意してください。代わりに、AND および OR テストが評価される場合、最も価値の低いテストが最初に評価されます。たとえば、次のフィルタでは、rcpt-to-group テストよりも消費リソースの少ない remote-ip テストが必ず最初に評価されます(一般に、LDAP テストの方が消費リソースは高くなります)。

```
andTestFilter:

if (remote-ip == "192.168.100.100" AND rcpt-to-group == "GROUP")

  { ... }
```

最もコストの低いテストが最初に実行されるため、項目の順序を入れ替えても影響はありません。テストの実行順序を保証する必要がある場合は、if 文をネストさせてください。この方法は、できる限りコストの高いテストを避けるためにも推奨します。

```
expensiveAvoid:

if (<simple tests>)

  { if (<expensive test>)

    { <action> }

  }
```

次に、もう少し複雑な例で説明します。

```
if (test1 AND test2 AND test3) { ... }
```

システムは左から右に式をグループ化するため、次のようになります。

```
if ((test1 AND test2) AND test3) { ... }
```

この場合、システムが最初に行うのは、(test1 AND test2) のコストと test3 のコストの比較です。最初に 2 番めの AND を評価します。3 つのテストすべてで同じコストがかかる場合、test3 が最初に実行されます。これは、(test1 AND test2) のコストが 2 倍になるためです。

メッセージ フィルタ ルール

各メッセージ フィルタには、フィルタを適用できるメッセージのコレクションを定義するルールが含まれています。フィルタ ルールを定義して、true を返すメッセージへのフィルタ アクションを定義します。

フィルタ ルールの概要の表

表 6-2 に、メッセージ フィルタで使用できるルールをまとめます。

表 6-2　メッセージ フィルタ ルール

ルール	構文	説明
件名ヘッダー（Subject Header）	subject	件名ヘッダーが特定のパターンと一致しているか。subject ルール（6-23 ページ）を参照してください。
本文サイズ（Body Size）	body-size	本文のサイズは一定の範囲内か。本文サイズ ルール（6-26 ページ）を参照してください。
エンベロープ送信者（Envelope Sender）	mail-from	エンベロープ送信者（Envelope From, <MAIL FROM>）が指定したパターンと一致しているか。エンベロープ送信者ルール（6-25 ページ）を参照してください。
グループ内のエンベロープ送信者（Envelope Sender in Group）	mail-from-group	エンベロープ送信者（Envelope From <MAIL FROM>）が、指定した LDAP グループ内に存在するか。グループ内エンベロープ送信者ルール（6-25 ページ）を参照してください。
送信者グループ（Sender Group）	sendergroup	どの送信者グループが、リスナーのホスト アクセス テーブル（HAT）に一致するか。送信者グループ ルール（6-25 ページ）を参照してください。
グループ内エンベロープ（Envelope Recipient）	rcpt-to	エンベロープ受信者（Envelope To, <RCPT TO>）が指定したパターンと一致しているか。エンベロープ受信者ルール（6-24 ページ）を参照してください。 **注：**rcpt-to ルールはメッセージベースです。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
エンベロープ受信者（Envelope Recipient in Group）	`rcpt-to-group`	エンベロープ受信者（Envelope To, <RCPT TO>）が、指定した LDAP グループ内に存在するか。グループ内エンベロープ受信者ルール（6-24 ページ）を参照してください。 **注：**`rcpt-to-group` ルールはメッセージベースです。メッセージに複数の受信者がある場合、グループの受信者が 1 人でも検出されれば、指定されたアクションがメッセージのすべての受信者に適用されます。
リモート IP（Remote IP）	`remote-ip`	リモート ホストから送信されたメッセージは、指定した IP アドレスまたは IP ブロックに一致しているか。リモート IP ルール（6-27 ページ）を参照してください。
受信インターフェイス（Receiving Interface）	`recv-int`	メッセージは、指定された受信インターフェイス経由で届いたか。受信 IP インターフェイス ルール（6-27 ページ）を参照してください。
受信リスナー（Receiving Listener）	`recv-listener`	メッセージは、指定されたリスナー経由で届いたか。受信リスナー ルール（6-27 ページ）を参照してください。
日付（Date）	`date`	現在時刻は特定の日時の前か後か。日付ルール（6-28 ページ）を参照してください。
ヘッダー（Header）	`header(<string>)`	メッセージに特定のヘッダーが含まれているか。ヘッダーの値が特定のパターンと一致しているか。ヘッダー ルール（6-28 ページ）を参照してください。
ランダム（Random）	`random(<integer>)`	ランダム番号は一定の範囲内か。乱数ルール（6-29 ページ）を参照してください。
受信者数（Recipient Count）	`rcpt-count`	この電子メールの受信者の人数。受信者数ルール（6-30 ページ）を参照してください。
アドレス数（Address Count）	`addr-count()`	受信者の累積数。 このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が rcpt-count フィルタ ルールと異なります。アドレス数ルール（6-30 ページ）を参照してください。
SPF ステータス（SPF Status）	`spf-status`	SPF 検証ステータスの値。このフィルタ ルールでは、さまざまな SPF 検証結果をクエリできます。有効な SPF/SIDF 戻り値ごとに異なるアクションを入力できます。SPF-Status ルール（6-37 ページ）を参照してください。
SPF 合格（SPF Passed）	`spf-passed`	SPF/SIDF 検証に合格したか。このフィルタ ルールは SPF/SIDF 結果をブール値として一般化します。SPF-Passed ルール（6-38 ページ）を参照してください。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
イメージ評価（Image verdict）	`image-verdict`	イメージ スキャンの評価の結果。このフィルタ ルールを使用して、さまざまなイメージ分析の評価について問い合わせることができます。イメージ分析（6-70 ページ）を参照してください。
ワークキュー数（Workqueue count）	`workqueue-count`	ワーク キュー数と指定した値の比較結果（等しい、多い、少ない）。workqueue-count ルール（6-39 ページ）を参照してください。
本文スキャン（Body Scanning）	`body-contains(<regular expression>)`	指定したパターンと一致するテキストまたは添付ファイルがメッセージに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 エンジンは、配信ステータス部分と関連する添付ファイルをスキャンします。 本文スキャン ルール（6-30 ページ）を参照してください。
本文スキャン（Body Scanning）	`only-body-contains(<regular expression>)`	指定したパターンと一致するテキストがメッセージ本文に含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。添付ファイルはスキャンされません。本文スキャン（6-31 ページ）を参照してください。
暗号化検出（Encryption Detection）	`encrypted`	メッセージは暗号化されているか。暗号化検出ルール（6-31 ページ）を参照してください。
添付ファイル名（Attachment Filename）[a]	`attachment-filename`	指定したパターンと一致するファイル名の添付ファイルがメッセージに含まれているか。添付ファイル名ルール（6-32 ページ）を参照してください。
添付ファイルタイプ（Attachment Type）[a]	`attachment-type`	特定の MIME タイプの添付ファイルがメッセージに含まれているか。添付ファイル タイプ ルール（6-32 ページ）を参照してください。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
添付ファイルのファイルタイプ[a]（Attachment File Type）	`attachment-filetype`	フィンガープリントに基づく特定のパターンと一致するファイル タイプの添付ファイルがメッセージに含まれているか（UNIX の `file` コマンドと同様）。添付ファイルが Excel または Word ドキュメントである場合、埋め込みファイル タイプの .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、png、および Photoshop イメージを検索することもできます。 有効なフィルタを作成するには、ファイル タイプを引用符で囲む必要があります。一重引用符または二重引用符を使用できます。たとえば、.exe 添付ファイルを検索するには、次の構文を使用します。 `if (attachment-filetype == "exe")` 詳細については、添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイル MIME タイプ（Attachment MIME Type）[a]	`attachment-mimetype`	特定の MIME タイプの添付ファイルがメッセージに含まれているか。このルールは `attachment-type` ルールに似ていますが、MIME 添付ファイルで指定された MIME タイプのみが評価される点が異なります。（アプライアンスは、タイプが明示的に指定されていない場合、拡張子からファイルのタイプを「予測」することはありません）。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
保護された添付ファイル（Attachment Protected）	`attachment-protected`	パスワード保護された添付ファイルがメッセージに含まれているか。保護された添付ファイルの隔離（6-79 ページ）を参照してください。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
保護されていない添付ファイル（Attachment Unprotected）	`attachment-unprotected`	attachment-unprotected フィルタ条件は、保護されていない添付ファイルをスキャン エンジンが検出した場合に true を返します。スキャン エンジンが添付ファイルを読み取ることができた場合、そのファイルは保護されていないと見なされます。zip ファイルに保護されていないメンバが含まれている場合、その zip ファイルは保護されていないと見なされます。 **注：**attachment-unprotected フィルタ条件と attachment-protected フィルタ条件は、相互に排他的ではありません。同じ添付ファイルをスキャンすると、両方のフィルタ条件で true が返される場合があります。これは、たとえば、zip ファイルに保護されたメンバと保護されていないメンバの両方が含まれている場合に発生します。 保護されていない添付ファイルの検出（6-79 ページ）を参照してください。
添付ファイルのスキャン（Attachment Scanning ）[a]	`attachment-contains(<regular expression>)`	指定したパターンと一致するテキストまたは別の添付ファイルが、メッセージの添付ファイルに含まれているか。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 このルールは `body-contains()` ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイルのスキャン（Attachment Scanning ）	`attachment-binary-contains(<regular expression>)`	指定したパターンと一致するバイナリ データが存在する添付ファイルがメッセージに含まれているか。 このルールは `attachment-contains ()` ルールに似ていますが、バイナリ データ内のパターンのみを検索します。
添付ファイルのスキャン（Attachment Scanning ）	`every-attachment-contains(<regular expression>)`	このメッセージのすべての添付ファイルに、特定のパターンと一致するテキストが含まれているか。対象のテキストがすべての添付ファイル内に存在する必要があります。つまり実際に実行されるアクションは、各添付ファイルに対する「`attachment-contains()`」の論理 AND 演算です。本文はスキャンされません。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。 添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
添付ファイルのサイズ（Attachment Size）[a]	`attachment-size`	メッセージに含まれている添付ファイルのサイズが特定の範囲内に収まっているか。このルールは `body-size` ルールと似ていますが、このルールでは、メッセージの全体の「本文」をスキャンしないようにします。つまり、ユーザが添付ファイルとして表示する場合だけスキャンします。このサイズは、デコードする前に評価されます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
公開ブラックリスト（Public Blacklists）	`dnslist(<query server>)`	送信者の IP アドレスがパブリック ブラックリスト サーバ（RBL）内に存在するか。DNS リスト ルール（6-33 ページ）を参照してください。
SenderBase レピュテーション（SenderBase Reputation）	`reputation`	送信者の SenderBase レピュテーション スコアの値。SenderBase レピュテーション ルール（6-34 ページ）を参照してください。
SenderBase レピュテーションなし（No SenderBase Reputation）	`no-reputation`	SenderBase レピュテーションが「None」の場合に使用します。SenderBase レピュテーション ルール（6-34 ページ）を参照してください。
ディクショナリ[b]	`dictionary-match(<dictionary_name>)`	メッセージ本文に、*dictionary_name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。辞書ルール（6-35 ページ）を参照してください。
添付ディクショナリー致（Attachment Dictionary Match）	`attachment-dictionary-match(<dictionary_name>)`	添付ファイルに、*dictionary_name* で指定した名前のコンテンツ ディクショナリの正規表現が含まれているかどうかを判別します。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。辞書ルール（6-35 ページ）を参照してください。
件名ディクショナリー致（Subject Dictionary Match）	`subject-dictionary-match(<dictionary_name>)`	件名ヘッダーに、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。辞書ルール（6-35 ページ）を参照してください。
ヘッダーディクショナリー致（Header Dictionary Match）	`header-dictionary-match(<dictionary_name>, <header>)`	指定したヘッダー（大文字と小文字を区別）に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。辞書ルール（6-35 ページ）を参照してください。

表 6-2　メッセージ フィルタ ルール（続き）

ルール	構文	説明
本文ディクショナリー一致（Body Dictionary Match）	`body-dictionary-match(<dictionary_name>)`	このフィルタ条件は、辞書の用語がメッセージ本文に含まれていれば true を返します。このフィルタは、添付ファイルであると判断されない MIME 部分の用語に一致します。また、ユーザが定義したしきい値が満たされた場合も true を返します（デフォルトのしきい値は 1 です）。辞書ルール（6-35 ページ）を参照してください。
エンベロープ受信者ディクショナリー一致（Envelope Recipient Dictionary Match）	`rcpt-to-dictionary-match(<dictionary_name>)`	エンベロープ受信者に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。辞書ルール（6-35 ページ）を参照してください。
エンベロープ送信者ディクショナリー一致（Envelope Sender Dictionary Match）	`mail-from-dictionary-match(<dictionary_name>)`	エンベロープ送信者に、*dictionary name* で指定した名前のコンテンツ ディクショナリの正規表現または用語が含まれているかどうかを判別します。辞書ルール（6-35 ページ）を参照してください。
SMTP 認証済みユーザー一致（SMTP Authenticated User Match）	`smtp-auth-id-matches(<target> [, <sieve-char>])`	エンベロープ送信者のアドレスとメッセージヘッダーのアドレスが、送信者の認証済み SMTP ユーザ ID と一致するかどうかを判別します。SMTP Authenticated User Match ルール（6-39 ページ）を参照してください。
[はい（True）]	`true`	すべてのメッセージと一致します。true ルール（6-22 ページ）を参照してください。
有効（Valid）	`valid`	メッセージに解析不能または無効な MIME 部分がある場合に false を返し、それ以外の場合は true を返します。valid ルール（6-23 ページ）を参照してください。
署名済み（Signed）	`signed`	メッセージが署名済みであるかどうかを判別します。signed ルール（6-41 ページ）を参照してください。
署名証明書（Signed Certificate）	`signed-certificate(<field> [<operator> <regular expression>])`	メッセージ署名者または X.509 証明書発行者が特定のパターンと一致するかどうかを判別します。署名付き証明書ルール（6-42 ページ）を参照してください。

a. 添付ファイルのフィルタリングについては、添付ファイルのスキャン（6-68 ページ）を参照してください。
b. コンテンツ ディクショナリの詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章で説明しています。

Cisco IronPort アプライアンスに送信されるメッセージはいずれも、すべてのメッセージ フィルタで順番に処理されますが、最終アクションを指定した場合はそのアクションによりメッセージに対する以降の処理が停止されます。（メッセージ フィルタ アクション（6-3 ページ）を参照）。フィルタはすべてのメッセージに適用することもでき、ルールは論理接続子（AND、OR、NOT）を使用して結合することもできます。

ルールで使用する正規表現

ルールの定義に使用するアトミック テストの一部では、*正規表現照合*を行います。正規表現は複雑になる場合があります。次の表は、メッセージ フィルタ ルールで正規表現を適用する場合の目安として使用してください。

表 6-3　　ルールで使用する正規表現

正規表現（abc）	フィルタ ルールの正規表現が文字列と一致すると判断されるのは、正規表現の一連の指示が文字列のいずれかの部分と一致する場合です。 たとえば、正規表現「Georg」は「George Of The Jungle」、「Georgy Porgy」、「La Meson Georgette」、「Georg」の各文字列と一致します。
カレット（^） **ドル記号（$）**	ドル記号（$）を含むルールは文字列の末尾のみと一致し、キャラット（^）を含むルールは文字列の先頭のみと一致します。 たとえば、正規表現「^Georg$」は文字列「Georg」のみと一致します。 空のヘッダーを検索するには、「"^$"」と指定します。
文字、空白、アットマーク（@）	文字、空白、アットマーク（@）を含むルールは、当該の文字自体と完全に一致します。 たとえば、正規表現「^George@admin$」は文字列「George@admin」のみと一致します。
ピリオド（.）	ピリオド（.）を含むルールは任意の 1 文字（改行を除く）と一致します。 たとえば、「^...admin$ 」という正規表現は「macadmin」および「sunadmin」の各文字列とは一致しますが、「win32admin」とは一致しません。
アスタリスク（*）	アスタリスク（*）を含むルールは、「直前に指定されている文字が 0 回を含む任意の回数繰り返されている文字」と一致します。ピリオドとアスタリスクが続く場合（.*）は、任意の文字列（改行を除く）と一致します。 たとえば、「^P.*Piper$」という正規表現は、「PPiper」、「Peter Piper」、「P.Piper」、「Penelope Penny Piper」のどの文字列とも一致します。
円記号（\）	円記号は特殊文字のエスケープに使用します。したがって、\. と続けると、ピリオドそのもののみに一致し、\$ はドル記号のみに一致し、\^ はキャレット記号のみに一致します。たとえば、「^ik\.ac\.uk$」は「ik.ac.uk」という文字列のみと一致します。 **重要：**円記号はパーサーでも特殊なエスケープ文字として使用します。そのため、正規表現で円記号を使用する場合、*2* つの円記号が必要です。解析後には「実際に」使用される円記号 1 つのみが残り、正規表現システムに渡されます。上記の例を照合する場合は「^ik\\.ac\\.uk$」と入力することになります。

表 6-3　　ルールで使用する正規表現（続き）

大文字と小文字を区別しない（(?i)）	トークン (?i) は、正規表現の残りの部分で大文字と小文字が区別されないことを表します。このトークンを、大文字と小文字を区別する正規表現の先頭に配置すると、大文字と小文字が一切区別されない照合が行われます。 たとえば、「(?i)viagra」という正規表現は、「Viagra」、「vIaGrA」、「VIAGRA」と一致します。
繰り返し回数 {min,max}	1 つ前のトークンの繰り返し回数を指定する正規表現表記がサポートされています。 たとえば、「fo{2,3}」は「foo」および「fooo」とは一致しますが、「fo」や「fofo」とは一致しません。 if(header('To') == "^.{500,}") というステートメントは、500 文字以上が使用されている「To」ヘッダーを検索します。
または (|)	代替、つまり「or」演算子に相当します。A と B が正規表現の場合、「A|B」は A と B のいずれかに一致する文字列と一致します。 たとえば、「foo|bar」という表現は foo や bar とは一致しますが、foobar とは一致しません。

メッセージのフィルタリングでの正規表現の使用

フィルタを使用して、ASCII 以外の形式でエンコードされているメッセージの内容（ヘッダーと本文）の文字列とパターンを検索できます。具体的には、本システムでは次の場所にある非 ASCII 文字を検索する正規表現（regex）を使用できます。

- メッセージ ヘッダー
- MIME 添付ファイル名の文字列
- メッセージ本文:
  - MIME ヘッダーがない本文（従来の形式の電子メール）
  - エンコードを示す MIME ヘッダーがあり、MIME 部分がない本文
  - エンコードが指定されているマルチパート MIME メッセージ
  - 上記の本文のうち、MIME ヘッダーでエンコードが指定されていないもの

メッセージまたは本文の任意の部分（添付ファイルを含む）の照合に正規表現を使用できます。添付ファイルのタイプとして HTML、MS Word、Excel など多数のタイプを対象にできます。対象となる文字セットとして、gb2312、HZ、EUC、JIS、Shift-JIS、Big5、Unicode などがあります。正規表現を使用するメッセージ フィルタ ルールを作成するには、コンテンツ フィルタ GUI を使用するか（『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Email Security Manager」を参照）、テキスト エディタでファイルを作成してからシステムにインポートします。詳細については、CLI を使用したメッセージ フィルタの管理（6-79 ページ）およびスキャン パラメータの変更（6-89 ページ）を参照してください。

正規表現の使用に関するガイドライン

プレフィックスではなく文字列全体を照合する場合は、正規表現の先頭にキャレット（^）、末尾にドル記号（$）をそれぞれ配置する必要があります。

（注）　空の文字列を照合する場合に “” を使用すると、実際にはすべての文字列が一致します。代わりに、“^$” を使用してください。たとえば、subject ルール（6-23 ページ）の 2 番めの例がこれに該当します。

また、文字としてのピリオドを照合するには、正規表現でピリオドをエスケープする必要があります。たとえば、sun.com という正規表現は「thegodsunocommando」という文字列と一致しますが、^sun\.com$ という正規表現は「sun.com」という文字列のみと一致します。

技術的には、ここで使用する正規表現のスタイルは **Python re Module** モジュール スタイルの正規表現です。Python スタイルの正規表現の詳細については、http://www.python.org/doc/howto/ [英語] からアクセスできる「Python Regular Expression HOWTO」を参考にしてください。

正規表現と非 ASCII 文字セット

一部の言語では、「単語」や「単語境界」、「大文字と小文字」という概念が存在しません。

単語を構成する文字（正規表現で「\w」と表される文字）の識別などが必要になる複雑な正規表現では、ロケールが不明な場合、またはエンコードが不明な場合、問題が発生します。

n テスト

正規表現の照合テストは、シーケンス == とシーケンス != を使用して行うことができます。次に例を示します。

```
rcpt-to == "^goober@dev\\.null\\....$" (matching)


rcpt-to != "^goober@dev\\.null\\....$" (non-matching)
```

大文字と小文字の区別

特に明記されている場合を除き、正規表現では大文字と小文字が区別されます。正規表現で「foo」を検索する場合、「FOO」や「Foo」は一致しません。

効率的なフィルタの作成

次の例は、同じ処理を行う 2 つのフィルタですが、最初の例の方が CPU の使用率が高くなります。2 番めのフィルタの方が効率的な正規表現を使用しています。

```
attachment-filter: if ((recv-listener == "Inbound") AND
((((((((((((((((((((((((((((((((((((((((((((((((attachment-filename ==

"\\.386$") OR (attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.ad$"))
OR (attachment-filename == "\\.ade$")) OR (attachment-filename == "\\.adp$")) OR
(attachment-filename == "\\.asp$")) OR (attachment-filename == "\\.bas$")) OR
(attachment-filename == "\\.bat$")) OR (attachment-filename == "\\.chm$")) OR
(attachment-filename == "\\.cmd$")) OR (attachment-filename == "\\.com$")) OR
(attachment-filename == "\\.cpl$")) OR (attachment-filename == "\\.crt$")) OR
(attachment-filename == "\\.exe$")) OR (attachment-filename == "\\.hlp$")) OR
(attachment-filename == "\\.hta$")) OR (attachment-filename == "\\.inf$")) OR
(attachment-filename == "\\.ins$")) OR (attachment- filename == "\\.isp$")) OR
(attachment-filename == "\\.js$")) OR (attachment-filename == "\\.jse$")) OR
(attachment- filename == "\\.lnk$")) OR (attachment-filename == "\\.mdb$")) OR
(attachment-filename == "\\.mde$")) OR (attachment-filename == "\\.msc$")) OR
(attachment-filename == "\\.msi$")) OR (attachment-filename == "\\.msp$")) OR
(attachment-filename == "\\.mst$")) OR (attachment-filename == "\\.pcd$")) OR
(attachment-filename == "\\.pif$")) OR (attachment-filename == "\\.reg$")) OR
(attachment-filename == "\\.scr$")) OR (attachment-filename == "\\.sct$")) OR
(attachment-filename == "\\.shb$")) OR (attachment-filename == "\\.shs$")) OR
(attachment-filename == "\\.url$")) OR (attachment-filename == "\\.vb$")) OR
(attachment-filename == "\\.vbe$")) OR (attachment-filename == "\\.vbs$")) OR
(attachment-filename == "\\.vss$")) OR (attachment-filename == "\\.vst$")) OR
(attachment-filename == "\\.vsw$")) OR (attachment-filename == "\\.ws$")) OR
(attachment-filename == "\\.wsc$")) OR (attachment-filename == "\\.wsf$")) OR
(attachment-filename == "\\.wsh$"))) { bounce(); }
```

この例では、AsyncOS は正規表現エンジンを 30 回（添付ファイルタイプと recv-listener のそれぞれに 1 回ずつ）起動する必要があります。

かわりに、次のようなフィルタを作成します。

```
attachment-filter: if (recv-listener == "Inbound") AND (attachment-filename ==
"\\.(386|exe|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|l
nk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc
|wsf|wsh)$") {

    bounce();

  }
```

正規表現エンジンの起動回数は 2 回だけで、「()」の追加やスペルの誤りについて心配する必要がなくなるためフィルタの管理も大幅に簡単になります。また、最初の例に比べて CPU オーバーヘッドが低下します。

PDF と正規表現

PDF の生成方法によっては、スペースや改行がないことがあります。このような場合、スキャン エンジンは、ページ内の単語の位置に基づき、論理的なスペースと改行の挿入を試みます。たとえば、1 つの単語の中に複数のフォントやフォント サイズが混在する場合、生成される PDF コードからスキャン エンジンが単語と改行を判別するのが難しくなります。このように生成された PDF ファイルで正規表現による照合を行うと、スキャン エンジンは予期しない結果を返す場合があります。

たとえば、PowerPoint 文書に挿入した単語の中に、単語内の文字ごとに異なるフォントやフォント サイズが設定されているものがあるとします。このアプリケーションから生成された PDF をスキャン エンジンが読み取ると、論理的なスペースと改行が挿入されます。PDF の構造が原因で、「callout」という単語が「call out」または「c a l lout」と解釈されることがあります。このいずれかの表現を正規表現「callout」と照合しようとすると、一致なしという結果になります。

スマート ID

メッセージの内容をスキャンするメッセージ ルールを使用する場合、スマート ID を使用するとデータ内の特定のパターンを検出できます。

スマート ID で、データ内の次のパターンを検出できます。

- クレジット カード番号
- 米国社会保障番号
- CUSIP ナンバー
- ABA ナンバー

フィルタでスマート ID を使用するには、本文または添付ファイルのコンテンツをスキャンするフィルタ ルールで次のキーワードを使用します。

表 6-4　　メッセージ フィルタのスマート ID

キーワード	スマート ID	説明
*credit	クレジット カード番号	14、15、および 16 桁のクレジット カード番号を識別します。 注: スマート ID では enRoute および JCB カードは識別されません。
*aba	ABA 送金番号	ABA 送金番号を識別します。
*ssn	社会保障番号	米国社会保障番号を識別します。*ssn スマート ID はダッシュ、ピリオド、スペースがある社会保障番号を識別します。
*cusip	CUSIP 番号	CUSIP 番号を識別します。

スマート ID の構文

フィルタ ルールでスマート ID を使用する場合、次の例のように、本文または添付ファイルをスキャンするフィルタ ルールの中でスマート ID キーワードを引用符で囲みます。

```
ID_Credit_Cards:

if(body-contains("*credit")){

notify("legaldept@example.com");

}
.
```

また、コンテンツ ディクショナリの一部としてコンテンツ フィルタ内でスマート ID を使用することもできます。

（注） スマート ID キーワードは通常の正規表現や他のキーワードと組み合わせて使用できません。たとえば、「`*credit|*ssn`」というパターンは有効ではありません。

（注） *ssn スマート ID による誤判定を防ぐため、*ssn スマート ID は他のフィルタ条件とあわせて使用すると有用な場合があります。たとえば、「only-body-contains」フィルタ条件を使用することができます。この場合、検索文字列がメッセージ本文のすべての MIME 部分に存在する場合のみ式が true であると判定されます。たとえば、次のようなフィルタを作成できます。

```
SSN-Nohtml: if only-body-contains(“*ssn”) { duplicate-quarantine(“Policy”);}
```

メッセージ フィルタ ルールの例

次のセクションでは、メッセージ フィルタの使用例を照会します。

true ルール

`true` ルールはすべてのメッセージと一致します。たとえば、次のルールはテスト対象となるすべてのメッセージについて、IP インターフェイスを external に変更します。

```
externalFilter:

   if (true)

   {

        alt-src-host('external');

   }
```

valid ルール

valid ルールは、メッセージに解析不能または無効な MIME 部分が含まれている場合に false を返し、それ以外の場合は true を返します。たとえば、次のルールはテスト対象のメッセージのうち解析不能なメッセージをすべてドロップします。

```
not-valid-mime:

   if not valid

   {

        drop();

   }
```

subject ルール

subject ルールは、件名ヘッダーの値が指定した正規表現と一致するメッセージを選択します。

たとえば、次のフィルタは、件名が「Make Money...」という語句で始まるすべてのメッセージを廃棄します。

```
scamFilter:

   if (subject == '^Make Money')

   {

        drop();

   }
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージ ヘッダー ルールおよび評価（6-5 ページ）を参照してください。

次のフィルタは、ヘッダーが空の場合、またはメッセージにヘッダーがない場合に true を返します。

```
EmptySubject_To_filter:

if (header('Subject') != ".") OR

   (header('To') != ".") {

   drop();

}
```

（注） このフィルタは Subject ヘッダーと To ヘッダーが空の場合に true を返しますが、ヘッダーがない場合も true を返します。指定したヘッダーがメッセージ内にない場合でも、このフィルタは true を返します。

エンベロープ受信者ルール

rcpt-to ルールは、いずれかのエンベロープ受信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタは「scarface」という文字列を含む電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。

（注） rcpt-to ルールで使用する正規表現では、大文字と小文字は*区別されません*。

```
scarfaceFilter:

   if (rcpt-to == 'scarface')

   {

        drop();

   }
```

（注） rcpt-to ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

グループ内エンベロープ受信者ルール

rcpt-to-group ルールは、いずれかのエンベロープ受信者が指定した LDAP グループのメンバであるメッセージを選択します。たとえば、次のフィルタは「ExpiredAccounts」という LDAP グループ内の電子メールアドレス宛てに送信されたすべてのメッセージをドロップします。

```
expiredFilter:

   if (rcpt-to-group == 'ExpiredAccounts')

   {

        drop();

   }
```

（注） rcpt-to-group ルールはメッセージに基づいています。メッセージに複数の受信者が設定されている場合、いずれか 1 人の受信者がルールと一致していれば、指定した処理がすべての受信者に対するメッセージに適用されます。

エンベロープ送信者ルール

mail-from ルールは、エンベロープ送信者が指定した正規表現と一致するメッセージを選択します。たとえば、次のフィルタを実行すると admin@yourdomain.com により送信されたすべてのメッセージがただちに出力されます。

（注）　mail-from ルールで使用する正規表現では、大文字と小文字は*区別されません*。次の例では、ピリオドがエスケープ処理されています。

```
kremFilter:

   if (mail-from == '^admin@yourdomain\\.com$')

   {

 skip_filters();

   }
```

グループ内エンベロープ送信者ルール

mail-from-group ルールは、エンベロープ送信者が演算子の右辺で指定した LDAP グループに属している（不一致を検索する場合は、送信者の電子メール アドレスが指定した LDAP グループに*属していない*）メッセージを選択します。たとえば、次のフィルタを実行すると、「KnownSenders」という LDAP グループの電子メールアドレスにより送信されたすべてのメッセージがただちに出力されます。

```
SenderLDAPGroupFilter:

   if (mail-from-group == 'KnownSenders')

   {

 skip_filters();

   }
```

送信者グループ ルール

sendergroup メッセージ フィルタは、リスナーのホスト アクセス テーブル（HAT）でどの送信者グループが一致するかに基づいて、メッセージを選択します。このルールは「==」（一致を検索する場合）または「!=」（不一致を検索する場合）を使用して、指定した正規表現（式の右辺）との一致をテストします。たとえば、次のメッセージ フィルタ ルールは、メッセージの送信者グループが正規表現「Internal」と一致する場合に true を返し、その場合はメッセージを代替メール ホストに送信します。

```
senderGroupFilter:

      if (sendergroup == "Internal")

      {
```

```
        alt-mailhost("[172.17.0.1]");

    }
```

本文サイズ ルール

本文サイズとはメッセージのサイズのことで、ヘッダーと添付ファイルも含みます。body-size ルールは、本文サイズを指定された数値と比較し、条件に一致するメッセージを選択します。たとえば、次のフィルタは本文サイズが 5 メガバイトを超えるすべてのメッセージをバウンスします。

```
BigFilter:

   if (body-size > 5M)

   {

        bounce();

   }
```

body-size を使用すると次のような比較ができます。

例	比較の種類
body-size < 10M	より少ない
body-size <= 10M	以下
body-size > 10M	右辺と比較して大きい
body-size >= 10M	以上
body-size == 10M	等しい
body-size != 10M	等しくない

サイズ指定にはサフィクスを使用すると便利です。

数量	説明
10b	10 バイト（「10」に同じ）
13k	13 キロバイト
5M	5 メガバイト
40G	40 ギガバイト（注：Cisco IronPort では 100 メガバイトを超えるメッセージを処理できません）

リモート IP ルール

remote-ip ルールは、メッセージを送信したホストの IP アドレスが特定のパターンと一致するかどうかを確認するためのテストを実行します。IP アドレスは、インターネット プロトコル バージョン 4（IPv4）またはインターネット プロトコル バージョン 6（IPv6）を指定できます。IP アドレス パターンは、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Sender Group Syntax」に記載されている**許可ホスト**の表記（SBO、SBRS、dnslist の表記および特殊キーワード ALL を除く）を使用して指定します。

allowed hosts 表記では、IP アドレス（ホスト名ではない）の順序と数値での範囲のみを指定できます。たとえば、次のフィルタは 10.1.1.*x*（x は 50、51、52、53、54、55 のいずれか）の形式の IP アドレスから*送信されていない*すべてのメッセージをバウンスします。

```
notMineFilter:

   if (remote-ip != '10.1.1.50-55')

   {

        bounce();

   }
```

受信リスナー ルール

recv-listener ルールは、名前付きリスナーで受信したメッセージを選択します。リスナー名は、現在システム上で設定されているリスナーのいずれかのニックネームである必要があります。たとえば、次のフィルタを実行すると、expedite という名前のリスナーから受信したすべてのメッセージがただちに出力されます。

```
expediteFilter:

   if (recv-listener == 'expedite')

   {

 skip_filters();

   }
```

受信 IP インターフェイス ルール

recv-int ルールは、名前付きインターフェイス経由で受信したメッセージを選択します。インターフェイス名は、現在システムに設定されているインターフェイスのいずれかのニックネームである必要があります。たとえば、次のフィルタは、outside という名前のインターフェイスから受信したすべてのメッセージをバウンスします。

```
outsideFilter:

   if (recv-int == 'outside')

   {
```

```
        bounce();

    }
```

日付ルール

date ルールは、現在の日時と指定した時刻を照合します。date ルールは *MM/DD/YYYY hh:mm:ss* という形式のタイムスタンプがある文字列との比較を行います。このルールは、特定の日時（米国形式）の前または後に実行する処理を指定する場合に便利です。（米国以外の日付形式を使用しているメッセージを検索する場合は問題が発生することがあります）。次のフィルタは、2003 年 7 月 28 日の午後 1 時より後に campaign1@yourdomain.com から送信されたすべてのメッセージをバウンスします。

```
TimeOutFilter:

    if ((date > '07/28/2003 13:00:00') and (mail-from ==

       'campaign1@yourdomain\\.com'))

    {

        bounce();

    }
```

（注）　date ルールを $Date メッセージ フィルタ処理変数と混同しないようにしてください。

ヘッダー ルール

header() ルールは、メッセージ ヘッダーがかっこ内で引用されている特定のヘッダー（"ヘッダー名"）と一致するかどうかを確認します。このルールは subject ルールと同様に正規表現と比較することもできますが、比較を行わずに使用することもできます。この場合、メッセージにそのヘッダーがあれば「true」、なければ「false」となります。たとえば、次の例ではヘッダー X-Sample の有無、およびこのヘッダーの値に「sample text」という文字列が含まれているかどうかを確認しています。一致する場合は、メッセージがバウンスされます。

```
FooHeaderFilter:

    if (header('X-Sample') == 'sample text')

    {

        bounce();

    }
```

ヘッダーの値で検索する非 ASCII 文字を指定することができます。

次の例では、比較を行わずにヘッダー ルールを適用しています。この場合、ヘッダー X-DeleteMe が見つかると、そのヘッダーがメッセージから削除されます。

```
DeleteMeHeaderFilter:

   if header('X-DeleteMe')

   {

        strip-header('X-DeleteMe');

   }
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージ ヘッダー ルールおよび評価（6-5 ページ）を参照してください。

乱数ルール

random ルールは、0 から N-1（N はルール名の後のかっこで指定される整数値）までの乱数を生成します。このルールでは header() ルールと同様に比較を行うこともできますが、「単項」形式で単独使用することもできます。単項形式では、生成された乱数が 0 でない場合に true と評価されます。たとえば、次のフィルタはいずれも内容としては同じもので、2 分の 1 の確率で Virtual Gateway アドレス A が選択され、残り 2 分の 1 の確率で Virtual Gateway アドレス B が選択されます。

```
load_balance_a:

   if (random(10) < 5) {

        alt-src-host('interface_a');

   } else {

        alt-src-host('interface_b');

   }



load_balance_b:

   if (random(2)) {

       alt-src-host('interface_a');

   } else {

       alt-src-host('interface_b');

   }
```

受信者数ルール

rcpt-count ルールは、body-size ルールと同様に、メッセージの受信者の数を整数値と比較します。このルールを使用すると、ユーザが一度に多数のユーザに電子メールを送信することを防止でき、また大規模なメール送信キャンペーンが特定の Virtual Gateway アドレス経由で行われるようにすることができます。次の例では、受信者数が 100 件を超える電子メールが特定の Virtual Gateway アドレスを経由して送信されます。

```
large_list_filter:

   if (rcpt-count > 100) {

        alt-src-host('mass_mailing_interface');

   }
```

アドレス数ルール

addr-count() メッセージ フィルタ ルールは、1 つ以上のヘッダー文字列を対象に、各行の受信者数を計算し、受信者の累積数をレポートします。このフィルタは、エンベロープの受信者ではなくメッセージ本文のヘッダーに対して機能する点が rcpt-count フィルタ ルールと異なります。次の例では、このフィルタ ルールにより長い受信者リストが「undisclosed-recipients」というエイリアスに置き換えられています。

```
count: if (addr-count("To", "Cc") > 30) {

            strip-header("To");

            strip-header("Cc");

            insert-header("To", "undisclosed-recipients");

           }
```

本文スキャン ルール

body-contains() ルールは、受信する電子メールとその添付ファイルをスキャンし、パラメータで定義された特定のパターンの有無を確認します。これには、配信ステータス部および関連付けられている添付ファイルが含まれます。body-contains() ルールでは複数行を対象とした照合は行われません。スキャンのロジックを CLI の scanconfig コマンドで変更することにより、スキャンの対象となる、またはスキャンの対象から除外する MIM タイプを定義できます。また、スキャン結果を true と評価するために検出する必要がある一致の最小数を指定することもできます。

デフォルトでは、MIME タイプが video/*、audio/*、image/* *以外*であるすべての添付ファイルがスキャンされます。複数のファイルが含まれている .zip、.bzip、.compress、.tar、.gzip の各アーカイブ添付ファイルがスキャンされます。スキャン対象となる、「ネストされた」アーカイブ添付ファイル（.zip に格納されている .zip など）の数を設定できます。

scanconfig コマンドを使用して添付ファイルのスキャン処理を設定する方法の例などの詳細については、スキャン パラメータの変更（6-89 ページ）を参照してください。

本文スキャン

AsyncOS が本文スキャンを実行する場合、正規表現を使用して本文のテキストと添付ファイルをスキャンします。式には最小しきい値を指定することができ、スキャン エンジンがこの最小回数だけ正規表現との一致を検出すると、この式は `true` と評価されます。

AsyncOS はメッセージの各種の MIME 部分を評価し、テキスト形式になっているすべての MIME 部分をスキャンします。最初の部分で MIME タイプがテキストに指定されている場合、AsyncOS はテキスト部分を識別します。AsyncOS はメッセージで指定されたエンコードに基づいてエンコードを決定し、テキストを Unicode に変換します。その後、Unicode 領域で正規表現を検索します。メッセージでエンコードが指定されていない場合は、`scanconfig` コマンドで指定されたエンコードが使用されます。

メッセージのスキャン時に AsyncOS が MIME 部分を評価する方法の詳細については、メッセージ本文とメッセージ添付ファイル（6-5 ページ）を参照してください。

MIME 部分がテキストでない場合、AsyncOS は .zip または .tar からファイルを抽出するか、圧縮されたファイルを抽出します。データを抽出した後、スキャン エンジンはファイルのエンコードを識別し、ファイルのデータを Unicode 形式で返します。その後、AsyncOS は Unicode 領域で正規表現を検索します。

次の例では、本文のテキストと添付ファイルで「Company Confidential」という文字列を検索します。この例では、最小しきい値が 2 件に設定されているため、スキャン エンジンがこの文字列を 2 件以上検出すると、該当するメッセージをすべてバウンスし、法務部門に通知します。

```
ConfidentialFilter:

   if (body-contains('Company Confidential',2)) {

        notify ('legaldept@example.domain');

        bounce();

   }
```

メッセージの本文のみをスキャンする場合は、`only-body-contains` を使用します。

```
disclaimer:

    if (not only-body-contains('[dD]isclaimer',1) ) {

        notify('hresource@example.com');

    }
```

暗号化検出ルール

`encrypted` ルールは、メッセージの内容に暗号化データが存在するかどうかを調査します。このルールは暗号化データのデコードは行わず、メッセージの内容に暗号化データが存在するかどうかのみを調査します。このルールは、ユーザが暗号化された電子メールを送信できないようにする場合に便利です。

（注）　暗号化されたルールは、メッセージの内容の暗号化されたデータのみを検出できます。暗号化された添付ファイルは検出しません。

encrypted は true ルールと同様に、パラメータを使用せず、比較も行いません。暗号化されたデータが検出された場合に true、検出されなかった場合に false を返します。この機能を実行するにはメッセージのスキャンが必要になるため、scanconfig コマンドで定義されたスキャン設定が使用されます。オプションの設定の詳細については、スキャン パラメータの変更（6-89 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、メッセージに暗号化されたデータが含まれる場合は、該当するメッセージが BCC で法務部門宛てに送信され、バウンスされます。

```
prevent_encrypted_data:

    if (encrypted) {

         bcc ('legaldept@example.domain');

         bounce();

      }
```

添付ファイル タイプ ルール

attachment-type ルールはメッセージ内の各添付ファイルの MIME タイプを確認し、指定されたパターンと一致するかどうかを判別します。このパターンは scanconfig コマンドで使用する形式（スキャン パラメータの変更（6-89 ページ）を参照）と同じ形式である必要があり、スラッシュ（/）の左右の一方でアスタリスクをワイルドカードとして使用できます。メッセージの添付ファイルがここで指定した MIME タイプと一致する場合、このルールは「true」を返します。

この機能を実行するにはメッセージのスキャンが必要となるため、scanconfig コマンドで指定されたすべてのオプション（スキャン パラメータの変更（6-89 ページ）を参照）が適用されます。

メッセージの添付ファイルを操作するために使用できるメッセージ フィルタ ルールの詳細については、添付ファイルのスキャン（6-68 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、MIME タイプが video/* である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
bounce_video_clips:

   if (attachment-type == 'video/*') {

        bounce();

   }
```

添付ファイル名ルール

attachment-filename ルールはメッセージ内の各添付ファイルの名前を確認し、指定されたパターンと一致するかどうかを判別します。この比較では大文字と小文字は区別されます。この比較ではスペースの有無も区別されるため、ファイル名の末尾にスペースがある状態でエンコードされていると、フィルタはその添付ファイルをスキップします。メッセージの添付ファイルのいずれかが指定したファイル名と一致すると、このルールは true を返します。

次の点に注意してください。

- 各添付ファイルの名前は MIME ヘッダーからキャプチャされます。MIME ヘッダーにあるファイル名の末尾にはスペースがある場合があります。
- 添付ファイルがアーカイブの場合、Cisco IronPort はアーカイブの内部からファイル名を取得し、scanconfig ルール（スキャン パラメータの変更（6-89 ページ）を参照）を適用します。
  - 添付ファイルが 1 個の圧縮ファイル（拡張子を問わず）である場合、アーカイブであるとは見なされず、この圧縮ファイルの名前は取得されません。つまり、このファイルは attachment-filename ルールでは処理されません。このようなファイルの例としては、gzip で圧縮された実行可能ファイル（.exe）などがあります。
  - 添付ファイルが単独の圧縮ファイルである場合（foo.exe.gz など）、正規表現を使用して圧縮ファイル内の特定のファイルタイプを検索します。添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル（6-33 ページ）を参照してください。

メッセージの添付ファイルを操作するために使用できるメッセージ フィルタ ルールの詳細については、添付ファイルのスキャン（6-68 ページ）を参照してください。

次のフィルタは、リスナー経由で送信されたすべての電子メールを確認し、ファイル名が *.mp3 である添付ファイルがメッセージに含まれる場合は、該当するメッセージがバウンスされます。

```
block_mp3s:

   if (attachment-filename == '(?i)\\.mp3$') {

        bounce();

   }
```

添付ファイル名とアーカイブ ファイル内の単独の圧縮ファイル

次に、アーカイブ（gzip で作成したものなど）にある単独の圧縮ファイルを照合する例を示します。

```
quarantine_gzipped_exe_or_pif:

if (attachment-filename == '(?i)\\.(exe|pif)($|.gz$)') {

  quarantine("Policy");

}
```

DNS リスト ルール

dnslist() ルールは、クエリーに DNSBL 方式（「ip4r ルックアップ」とも呼ばれます）を使用するパブリック DNS リスト サーバを照会します。着信接続の IP アドレスは反転され（IP が 1.2.3.4 の場合は 4.3.2.1 になり）、かっこ内のサーバ名にプレフィックスとして追加されます（サーバ名の先頭がピリオドでない場合は、サーバ名とプレフィックスを区切るためのピリオドが追加されます）。DNS クエリーが生成され、システムには DNS 失敗応答（接続の IP アドレスがサーバのリストにないことを示す）または IP アドレス（アドレスが見つかったことを示す）が返されます。返される IP アドレスは*通常*、127.0.0.*x*（x は 0 ～ 255 のうちほぼすべての数）の形式になります（IP アドレス範囲は許可されていません）。一部のサーバは、リスト生成の理由に基づいてそれぞれ異なる数字を返しますが、それ以外のサーバはすべての一致に対して同じ結果を返します。

dnslist() は、header() ルールと同様に、単項または二項比較で使用できます。単独では、応答を受信すると true を返し、応答がない場合（DNS サーバが到達不能の場合など）は false を返します。

次のフィルタを実行すると、送信者が Cisco IronPort Bonded Sender 情報サービス プログラムにボンドされている場合、そのメッセージがただちに出力されます。

```
whitelist_bondedsender:

   if (dnslist('query.bondedsender.org')) {

 skip_filters();

   }
```

オプションで、等式（==）または不等式（!=）を使用して結果を文字列と比較することもできます。

次のフィルタは、サーバから「127.0.0.2」が返されるメッセージをドロップします。応答がそれ以外の内容であれば、このルールは false を返し、フィルタは無視されます。

```
blacklist:

   if (dnslist('dnsbl.example.domain') == '127.0.0.2') {

        drop();

   }
```

SenderBase レピュテーション ルール

reputation ルールは、SenderBase レピュテーション スコアを他の値と比較して確認します。>、==、<= などのすべての比較演算子を使用できます。メッセージに SenderBase レピュテーション スコアがない場合（これまでスコアがまったく確認されていないか、SenderBase レピュテーション サービス クエリー サーバから応答を取得できなかった場合）、レピュテーション スコアとの比較はすべて失敗します（数値がいずれかの値より大きいまたは小さい、いずれかの値と等しいまたは等しくないという判別ができません）。次に説明する no-reputation ルールを使用すると、SBRS スコアが「none」であるかどうかを確認できます。次の例では、SenderBase レピュテーション サービスから返されるレピュテーション スコアがしきい値の -7.5 を下回る場合に、メッセージの「Subject:」行の先頭に「*** BadRep ***」が付加されます。

```
note_bad_reps:

   if (reputation < -7.5) {

        strip-header ('Subject');

        insert-header ('Subject', '*** BadRep $Reputation *** $Subject');

   }
```

詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Reputation Filtering」と「SenderBase Reputation Score (SBRS)」を参照してください。アンチスパム システムのバイパス アクション（6-66 ページ）も参照してください。

SenderBase レピュテーション ルールによる値は -10 ～ 10 ですが、NONE という値が返される場合もあります。NONE について特に確認が必要な場合は、no-reputation ルールを使用します。

```
none_rep:

   if (no-reputation) {

       strip-header ('Subject');

        insert-header ('Subject', '*** Reputation = NONE *** $Subject');

   }
```

辞書ルール

メッセージ本文に、「*dictonary_name*」という名前のコンテンツ ディクショナリにある正規表現または用語が含まれている場合、dictionary-match(<*dictonary_name*>) ルールは true と評価されます。該当のディクショナリが存在しない場合は、ルールは false と評価されます。ディクショナリの定義（大文字と小文字の区別や単語境界の設定など）の詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。

次のフィルタは、Cisco IronPort が「secret_words」という辞書にある単語を含むメッセージをスキャンすると、管理者にブラインド カーボン コピーを送信します。

```
copy_codenames:

   if (dictionary-match ('secret_words')) {

       bcc('administrator@example.com');

       }
```

次の例では、メッセージの本文に、「secret_words」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。only-body-contains 条件とは異なり、body-dictionary-match 条件では、すべてのコンテンツ部分がそれぞれ個別に辞書に一致する必要はありません。各コンテンツ部分のスコア（マルチパート/代替部分も考慮されます）は合計されます。

```
quarantine_data_loss_prevention:

   if (body-dictionary-match ('secret_words'))

       {

       quarantine('Policy');

       }
```

次のフィルタでは、件名が指定した辞書にある単語と一致すると隔離されます。

```
quarantine_policy_subject:

    if (subject-dictionary-match ('gTest'))
```

```
        {
        quarantine('Policy');
        }
```

次の例では、「To」ヘッダーの電子メール アドレスを照合し、管理者にブラインド コピーを送信しています。

```
headerTest:
    if (header-dictionary-match ('competitorsList', 'to'))
        {
        bcc('administrator@example.com');
        }
```

`attachment-dictionary-match(<dictonary_name>)` ルールは上記の `dictionary-match` ルールと同様に機能しますが、検索対象は添付ファイルです。

次のフィルタでは、メッセージの添付ファイルに「secret_words」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:
   if (attachment-dictionary-match ('secret_words'))
       {
       quarantine('Policy');
       }
```

`header-dictionary-match(<dictonary_name>, <header>)` ルールは上記の dictionary-match ルールと同様に機能しますが、検索対象は *<header>* で指定したヘッダーです。ヘッダー名の大文字と小文字は区別されないため、たとえば「subject」でも「Subject」でも機能します。

次のフィルタでは、メッセージの「cc」ヘッダーに「ex_employees」という辞書にあるいずれかの単語が含まれていると、そのメッセージが Policy という隔離エリアに送信されます。

```
quarantine_codenames_attachment:
   if (header-dictionary-match ('ex_employees', 'cc'))
       {
       quarantine('Policy');
       }
```

辞書用語内でワイルドカードを使用することができます。電子メール アドレスのピリオドをエスケープする必要はありません。

SPF-Status ルール

SPF/SIDF 検証されたメールを受信する場合、SPF/SIDF 検証の結果によって異なるアクションを実行することが必要になる場合があります。spf-status ルールを使用すると、複数の SPF 検証結果との照合が可能になります。詳細については、検証結果（5-31 ページ）を参照してください。

SPF/SIDF 検証結果との照合を行うには、次の構文を使用します。

```
if (spf-status == "Pass")
```

1 つの条件で複数の状態判定に対してチェックする場合、次の構文を使用できます。

```
if (spf-status == "PermError, TempError")
```

さらに、次の構文を使用して、HELO、MAIL FROM、PRA ID に対して検証結果をチェックすることもできます。

```
if (spf-status("pra") == "Fail")
```

次の例に、spf-status フィルタの使用例を示します。

```
skip-spam-check-for-verified-senders:

     if (sendergroup == "TRUSTED" and spf-status == "Pass"){

         skip-spamcheck();

     }



quarantine-spf-failed-mail:

     if (spf-status("pra") == "Fail") {

         if (spf-status("mailfrom") == "Fail"){

             # completely malicious mail

             quarantine("Policy");

         } else {

           if(spf-status("mailfrom") == "SoftFail") {

             # malicious mail, but tempting

             quarantine("Policy");

           }
```

```
        }
    } else {
      if(spf-status("pra") == "SoftFail"){
        if (spf-status("mailfrom") == "Fail"
                or spf-status("mailfrom") == "SoftFail"){
            # malicious mail, but tempting
            quarantine("Policy");
        }
      }
    }


stamp-mail-with-spf-verification-error:
    if (spf-status("pra") == "PermError, TempError"
            or spf-status("mailfrom") == "PermError, TempError"
            or spf-status("helo") == "PermError, TempError"){
        # permanent error - stamp message subject
        strip-header("Subject");
        insert-header("Subject", "[POTENTIAL PHISHING] $Subject"); }
.
```

SPF-Passed ルール

次の例に、spf-passed とマークされていない電子メールを隔離するために使用する `spf-passed` ルールを示します。

```
quarantine-spf-unauthorized-mail:
    if (not spf-passed) {
        quarantine("Policy");
    }
```

（注）　spf-status ルールと異なり spf-passed ルールは SPF/SIDF 検証値を簡単なブール値に単純化します。次の検証結果は、spf-passed ルールに合格していないものとして扱われます。None、Neutral、Softfail、TempError、PermError、Fail。より詳細な結果に基づいて、メッセージへのアクションを実行するには、spf-status ルールを使用します。

workqueue-count ルール

workqueue-count ルールは、ワークキュー数を特定の値と照合します。>、==、<= などのすべての比較演算子を使用できます。

次のフィルタは、ワークキュー数を確認し、指定した値より多ければスパムの確認を省略します。

```
 wqfull:

if (workqueue-count > 1000) {

 skip-spamcheck();

}
```

SPF/SIDF の詳細については、SPF および SIDF 検証の概要（5-22 ページ）を参照してください。

SMTP Authenticated User Match ルール

Cisco IronPort アプライアンスがメッセージの送信に SMTP 認証を使用している場合、smtp-auth-id-matches *(<target> [, <sieve-char>])* ルールはメッセージのヘッダーとエンベロープ送信者を送信者の SMTP 認証ユーザ ID と照合し、スプーフィングされたヘッダーを含む送信メッセージを識別します。このフィルタを使用すると、なりすましの可能性のあるメッセージを隔離またはブロックできます。

smtp-auth-id-matches ルールは、SMTP 認証 ID を次の比較対象と比較します。

ターゲット（Target）	説明
*EnvelopeFrom	SMTP 対話のエンベロープ送信者のアドレス（MAIL FROM）を比較します。
*FromAddress	From ヘッダーから解析されたアドレスを比較します。From ヘッダーには複数のアドレスを使用できるため、そのうち 1 つが一致すれば一致と見なされます。
*Sender	Sender ヘッダーで指定されているアドレスを比較します。
*Any	ID にかかわらず、認証済み SMTP セッション中に作成されたメッセージと一致します。
*None	認証済み SMTP セッション中に作成されなかったメッセージと一致します。認証がオプションの場合に便利です（推奨）。

フィルタによる照合は厳密ではありません。大文字と小文字は区別されません。オプションで *sieve-char* パラメータが指定されている場合、特定の文字の後に続くアドレスの最後の部分は比較時に無視されます。たとえば、パラメータに「+」が含まれている場合、アドレス joe+folder@example.com のうち「+」より後の部分がフィルタでは無視されます。アドレスが joe+smith+folder@example.com の場合は、「+folder」のみが無視されます。SMTP 認証ユーザ ID 文字列が単純なユーザ名で、完全修飾電子メール アドレスでない場合は、比較対象のユーザ名部分のみが照合されます。ドメイン部分は別のルールで検証する必要があります。

また、$SMTPAuthID 変数を使用して SMTP 認証ユーザ ID をヘッダーに挿入することができます。

次の表は、SMTP 認証 ID と電子メールの比較の例で、smtp-auth-id-matches フィルタ ルールによる比較で一致するかどうかを示しています。

SMTP 認証 ID	ふるい文字	比較するアドレス	一致の可否
someuser		otheruser@example.com	なし
someuser		someuser@example.com	○
someuser		someuser@another.com	○
SomeUser		someuser@example.com	○
someuser		someuser+folder@example.com	なし
someuser	+	someuser+folder@example.com	○
someuser@example.com		someuser@forged.com	なし
someuser@example.com		someuser@example.com	○
SomeUser@example.com		someuser@example.com	○

次のフィルタは、認証済み SMTP セッション中に作成されたすべてのメッセージを確認し、From ヘッダーのアドレスとエンベロープ送信者が SMTP 認証ユーザ ID と一致するか検証します。アドレスと ID が一致すると、フィルタはドメインを許可します。一致しない場合、アプライアンスはメッセージを隔離します。

```
Msg_Authentication:

if (smtp-auth-id-matches("*Any"))

{

    # Always include the original authentication credentials in a

    # special header.

    insert-header("X-Auth-ID","$SMTPAuthID");



    if (smtp-auth-id-matches("*FromAddress", "+") and

        smtp-auth-id-matches("*EnvelopeFrom", "+"))

    {

        # Username matches.  Verify the domain

        if header('from') != "(?i)@(?:example\\.com|alternate\\.com)" or
```

```
            mail-from != "(?i)@(?:example\\.com|alternate\\.com)"

        {

            # User has specified a domain which cannot be authenticated

            quarantine("forged");

        }

    } else {

        # User claims to be an completely different user

        quarantine("forged");

    }

}
```

signed ルール

signed ルールはメッセージの署名を確認します。このルールは、メッセージの署名の有無を示すブール値を返します。このルールは、署名が ASN.1 DER エンコーディング ルールに従っているか、および CMS 署名データ型構造（RFC 3852、セクション 5.1）に準拠しているかを評価します。署名がコンテンツと一致するかどうかは検証されず、証明書の有効性も確認されません。

次の例では、signed ルールを使用してヘッダーを署名済みメッセージに挿入します。

```
signedcheck: if signed { insert-header("X-Signed", "True"); }
```

次の例では、signed ルールを使用して、特定の送信者グループから受信した未署名のメッセージの添付ファイルをドロップします。

```
Signed: if ((sendergroup == "NOTTRUSTED") AND NOT signed) {

 html-convert();

    if (attachment_size > 0)

    {

        drop_attachments("");

    }

}
```

署名付き証明書ルール

signed-certificate ルールは、X.509 証明書発行者またはメッセージ署名者が、指定した正規表現と一致している S/MIME メッセージを選択します。このルールが対応しているのは X.509 証明書のみです。

このルールの構文は signed-certificate (<field> [<operator> <regular expression>]) です。各項目の内容は次のとおりです。

- <field>:引用符で囲まれた文字列 "issuer"(発行者)または "signer"(署名者)。
- <operator>:== または !=。
- <regular expression>:発行者または署名者を照合するための値。

メッセージに複数の署名が使用されている場合、いずれかの発行者または署名者が正規表現と一致すると true が返されます。このルールを一番短い形で signed-certificate("issuer") および signed-certificate("signer") のように指定すると、S/MIME メッセージに発行者または署名者が設定されている場合に true が返されます。

署名者

メッセージ署名者に関して、このルールは X.509 証明書の subjectAltName 拡張から rfc822Name 名のシーケンスを抽出します。署名証明書に subjectAltName フィールドがない場合、またはこのフィールドに rfc822Name 名がない場合、signed-certificate("signer") ルールは false を返します。まれではありますが、rfc822Name 名が複数使用されている場合、このルールはすべての名前を正規表現と照合しようと試み、最初に一致した時点で true を返します。

発行元(Issuer)

発行者は X.509 証明書の空でない識別名です。AsyncOS は証明書から発行者を取得し、LDAP-UTF8 Unicode 文字列に変換します。次に例を示します。

- C=US,S=CA,O=IronPort
- C=US,CN=Bob Smith

X.509 証明書では発行者フィールドが必要なため、signed-certificate("issuer") は S/MIME メッセージに X.509 証明書があるかどうかを評価します。

正規表現でのエスケープ処理

LDAP-UTF8 では、正規表現で使用できるエスケープ方式が定義されています。LDAP-UTF8 での文字のエスケープ処理の詳細については、『Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names』(http://www.ietf.org/rfc/rfc4514.txt)を参照してください。

signed-certificate ルールでのエスケープ ルールは、LDAP-UTF8 で定義されたエスケープ ルールとは異なり、エスケープ処理が必要な文字のみをエスケープします。LDAP-UTF8 では、エスケープ処理なしで表示できる文字をオプションでエスケープすることができます。たとえば、次の 2 つの文字列は、LDAP-UTF8 のエスケープ ルールではいずれも「Example, Inc.」を正しく表すものとされます。

- Example\, Inc.
- Example\,\ Inc\.

ただし、signed-certificate ルールは Example\, Inc. とのみ一致します。スペースやピリオドのエスケープ処理は LDAP-UTF8 では許可されていますが、必要ではないため、正規表現では許可されません。signed-certificate ルールで使用する正規表現を作成する場合は、エスケープ処理がなくても表示できる文字はエスケープしないでください。

$CertificateSigners アクション変数

アクション変数 $CertificateSigners は、署名証明書の subjectAltName 要素から取得した、カンマ区切り形式の署名者のリストです。1 人の署名者に複数の電子メールアドレスがある場合、重複を除去した上でリストに収録されます。

たとえば、Alice が自分の 2 つの証明書でメッセージに署名したとします。Bob は自分の 1 つの証明書でメッセージに署名しています。すべての証明書は 1 件の社内機関により発行されています。メッセージが S/MIME スキャンを通過すると、抽出されるデータには 3 つの項目が含まれます。

```
[
  {
    'issuer': 'CN=Auth,O=Example\, Inc.',
    'signer': ['alice@example.com', 'al@private.example.com']
  },
  {
    'issuer': 'CN=Auth,O=Example\, Inc.',
    'signer': ['alice@example.com', 'al@private.example.com']
  },
  {
    'issuer': 'CN=Auth,O=Example\, Inc.',
    'signer': ['bob@example.com', 'bob@private.example.com']
  }
]
```

$CertificateSigners 変数は次のように拡張されます。

```
"alice@example.com, al@private.example.com, bob@example.com, bob@private.example.com"
```

例

次の例では、証明書発行者が米国にいる場合、新しいヘッダーが挿入されます。

```
Issuer: if signed-certificate("issuer") == "(?i)C=US" {
    insert-header("X-Test", "US issuer");
}
```

次の例では、署名者のドメインが example.com でない場合、管理者に通知されます。

```
NotOurSigners: if signed-certificate("signer") AND

      signed-certificate("signer") != "example\\.com$" {

    notify("admin@example.com");

}
```

次の例では、メッセージに X.509 証明書がある場合、ヘッダーが追加されます。

```
AnyX509: if signed-certificate ("issuer") {

    insert-header("X-Test", "X.509 present");

}
```

次の例では、メッセージの証明書に署名者がない場合、ヘッダーが追加されます。

```
NoSigner: if not signed-certificate ("signer") {

    insert-header("X-Test", "Old X.509?");

}
```

メッセージ フィルタ アクション

メッセージ フィルタの目的は、選択されたメッセージに対してアクションを実行することです。

アクションには、次の 2 つのタイプがあります。

- *最終*アクション（deliver、drop、bounce など）はメッセージの処理を終了し、後続のフィルタによるさらなる処理を許可しません。
- *非最終*アクションは、メッセージをさらに処理することを許可するアクションを実行します。

非最終メッセージ フィルタ アクションは、累積的です。各フィルタが異なるアクションを指定する複数のフィルタにメッセージが一致する場合、すべてのアクションが累積され、適用されます。ただし、同じアクションを指定する複数のフィルタにメッセージが一致する場合、前のアクションが上書きされ、最後のフィルタ アクションが適用されます。

フィルタ アクション一覧表

メッセージ フィルタでは次の表 6-5 に示すアクションを電子メール メッセージに適用できます。

表 6-5　メッセージ フィルタ アクション

操作	構文	説明
送信元ホストの変更	`alt-src-host`	メッセージの送信に使用する送信元ホスト名と IP インターフェイス（Virtual Gateway アドレス）を変更します。送信元ホスト（Virtual Gateway アドレス）変更アクション（6-61 ページ）を参照してください。
受信者の変更	`alt-rcpt-to`	メッセージの受信者を変更します。受信者変更アクション（6-60 ページ）を参照してください。
メール ホストの変更	`alt-mailhost`	メッセージの送信先メール ホストを変更します。配信ホスト変更アクション（6-61 ページ）を参照してください。
通知	`notify`	メッセージに関する報告を別の受信者に送信します。通知およびコピー通知アクション（6-55 ページ）を参照してください。
コピーの通知	`notify-copy`	`notify` アクションと同様ですが、`bcc-scan` アクションのようにコピーを送信します。通知およびコピー通知アクション（6-55 ページ）を参照してください。
BCC	`bcc`	メッセージをコピーし（メッセージ レプリケーション）、このコピーを匿名で別の受信者に送信します。ブラインド カーボン コピー アクション（6-57 ページ）を参照してください。
BCC（スキャン処理あり）	`bcc-scan`	メッセージを秘密で他の受信者に送信し、そのメッセージを新しいメッセージであるかのようにワークキューで処理します。ブラインド カーボン コピー アクション（6-57 ページ）を参照してください。
アーカイブ	`archive`	メッセージを mbox 形式のファイルにアーカイブします。アーカイブ アクション（6-62 ページ）を参照してください。
検疫	`quarantine (`*`quarantine_name`*`)`	*quarantine_name* で指定した隔離エリアにメッセージを送信するようフラグを設定します。隔離および複製アクション（6-59 ページ）を参照してください。
複製（隔離）	`duplicate-quarantine (`*`quarantine_name`*`)`	指定された隔離エリアにメッセージのコピーを送信します。隔離および複製アクション（6-59 ページ）を参照してください。
ヘッダーの削除	`strip-header`	メッセージの配信前に、指定したヘッダーをメッセージから削除します。ヘッダー削除アクション（6-63 ページ）を参照してください。
ヘッダーの挿入	`insert-header`	メッセージの配信前に、ヘッダーと値の対をメッセージに挿入します。ヘッダー挿入アクション（6-63 ページ）を参照してください。
ヘッダー テキストの編集	`edit-header-text`	指定したヘッダー テキストを、フィルタ条件として指定した文字列に置き換えます。ヘッダー テキスト編集アクション（6-64 ページ）を参照してください。

表 6-5　メッセージ フィルタ アクション（続き）

操作	構文	説明
本文の編集	`edit-body-text()`	メッセージ本文から正規表現に一致する部分を削除し、指定したテキストに置き換えます。このフィルタは、メッセージ本文内の URL などの特定のコンテンツを削除および置換する場合に使用できます。本文編集アクション（6-64 ページ）を参照してください。
HTML の変換	`html-convert()`	メッセージ本文から HTML タグを削除し、メッセージのプレーン テキスト部分を残します。このフィルタは、メッセージ内のすべての HTML テキストをプレーン テキストに変換する場合に使用します。HTML 変換アクション（6-65 ページ）。
バウンス プロファイルの割り当て	`bounce-profile`	特定のバウンス プロファイルをメッセージに割り当てます。バウンス プロファイル アクション（6-66 ページ）を参照してください。
アンチスパム システムのバイパス	`skip-spamcheck`	Cisco IronPort システムのアンチスパム システムがメッセージに適用 *されない* ようにします。アンチスパム システムのバイパス アクション（6-66 ページ）を参照してください。
アンチウイルス システムのバイパス	`skip-viruscheck`	Cisco IronPort システムのアンチウィルス システムがメッセージに適用 *されない* ようにします。アンチウイルス システムのバイパス アクション（6-67 ページ）を参照してください。
ウイルス アウトブレイク フィルタのスキャニング処理のスキップ	`skip-vofcheck`	このメッセージがウイルス アウトブレイク フィルタでスキャニング処理されないようにします。アンチウイルス システムのバイパス アクション（6-67 ページ）を参照してください。
添付ファイルのドロップ（名前別）	`drop-attachments-by-name`	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイルのドロップ（タイプ別）	`drop-attachments-by-type`	メッセージの添付ファイルのうち、指定した MIME タイプまたはファイル拡張子に該当する MIME タイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイルのドロップ（ファイル タイプ別）	`drop-attachments-by-filetype`	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル（zip、tar）内に該当するファイルがある場合、この添付ファイルはドロップされます。詳細については、添付ファイルのスキャン（6-68 ページ）を参照してください。

表 6-5　メッセージ フィルタ アクション（続き）

操作	構文	説明
添付ファイルのドロップ（MIME タイプ別）	`drop-attachments-by-mimetype`	メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。このアクションではファイル拡張子による MIME タイプの判別は行われず、アーカイブの内容の確認もされません。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイルのドロップ（サイズ別）	`drop-attachments-by-size`	メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ（バイト単位）以上のサイズであるファイルをすべてドロップします。アーカイブや圧縮ファイルの場合、このアクションでは非圧縮状態でのサイズは計測されず、デコードを行う前の実際の添付ファイルのサイズが計測されます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
添付ファイルのドロップ（内容別）	`drop-attachments-where-contains`	メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。パターンの発生回数が、しきい値で指定した最小回数以上である必要があります。アーカイブ ファイル（zip、tar）は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。 オプション コメントは、ドロップされた添付ファイルの置換に使用されるテキストを変更します。添付ファイルのフッターは、単純にメッセージに追加されるだけです。
添付ファイルのドロップ（辞書との一致別）	`drop-attachments-where-dictionary-match`	辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。
フッターの追加	`add-footer(`*`footer-name`*`)`	フッターをメッセージに追加します。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」章の「Message Disclaimer Stamping」を参照してください。
配信時の暗号化	`encrypt-deferred`	配信時にメッセージを暗号化します。メッセージはそのまま次の処理に進み、すべての処理が完了した時点で暗号化され、配信されます。

表 6-5　メッセージ フィルタ アクション（続き）

操作	構文	説明
メッセージ タグの追加	`tag-message(tag-name)`	RSA Email DLP ポリシー フィルタリングで使用するカスタム用語をメッセージに追加します。RSA Email DLP ポリシーを設定して、スキャン対象をメッセージ タグがあるメッセージに限定することができます。メッセージ タグは受信者側では表示されません。メッセージ タグ追加アクション（6-67 ページ）、および『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Data Loss Prevention」の章を参照してください。
ログ エントリの追加	`log-entry`	カスタマイズしたテキストを、IronPort テキスト メール ログに `INFO` レベルで追加します。このテキストにはアクション変数を使用することができます。ログ エントリはメッセージ トラッキングに表示されます。ログ エントリ追加アクション（6-68 ページ）を参照してください。
***残りのメッセージ フィルタをスキップ**	`skip-filters`	メッセージに対して他のメッセージ フィルタによる処理は行われず、メッセージは電子メール パイプラインをそのまま通過します。「残りのメッセージ フィルタをスキップ」アクション（6-53 ページ）を参照してください。
***メッセージのドロップ**	切断	メッセージをドロップし、廃棄します。ドロップ アクション（6-54 ページ）を参照してください。
***メッセージのバウンス**	`bounce`	メッセージを送信者に戻します。バウンス アクション（6-54 ページ）を参照してください。
***すぐに暗号化して配信**	`encrypt`	送信メッセージの暗号化に Cisco IronPort 電子メール暗号化を使用します。暗号化アクション（6-54 ページ）を参照してください。

***最終アクション**

添付ファイル グループ

特定のファイル タイプ（「exe」など）や一般的な添付ファイルのグループを `attachment-filetype` ルールや `drop-attachments-by-filetype rules` ルールで指定できます。AsyncOS は添付ファイルを 表 6-6 に記載されているグループに分類します。

特定のファイル タイプの添付ファイルを含まないメッセージと照合させる `!=` 演算子を使うメッセージ フィルタを作成する場合は、フィルタで除外するファイル タイプの添付ファイルが少なくとも 1 つあると、フィルタはメッセージへのアクションを実行しません。たとえば、次のフィルタは *.exe* ファイル タイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {

                drop();

           }
```

メッセージに複数の添付ファイルがある場合、E メール セキュリティ アプライアンスは他の添付ファイルが .exe ファイルでない場合でも、添付ファイルの少なくとも 1 つが .exe ファイルの場合はメッセージをドロップしません。

表 6-6　添付ファイル グループ

添付ファイル グループ名	スキャン対象のファイル タイプ
マニュアル	• doc、docx • mdb • mpp • ole • pdf • ppt、pptx • rtf • wps • x-wmf • xls、xlsx
実行可能ファイル	• exe • java • msi • pif **（注）** Executable グループをフィルタリングすると、.dll ファイルと .scr ファイルもスキャンされます。これらのファイル タイプは個別にスキャンできません。
圧縮	• ace（ACE アーカイバ圧縮ファイル） • arc（SQUASH 圧縮アーカイブ） • arj（Robert Jung ARJ 圧縮アーカイブ） • binhex • bz（Bzip 圧縮ファイル） • bz2（Bzip 圧縮ファイル） • cab（Microsoft キャビネット ファイル） • gzip*（圧縮ファイル - UNIX gzip） • lha（圧縮アーカイブ [LHA/LHARC/LHZ]） • sit（圧縮アーカイブ - Macintosh ファイル [Stuffit]） • tar*（圧縮アーカイブ） • unix（UNIX 圧縮アーカイブ） • zip*（圧縮アーカイブ - Windows） • zoo（ZOO 圧縮アーカイブ ファイル） * これらのファイルは「本文スキャン」の対象にすることができます。

表 6-6　添付ファイル グループ（続き）

添付ファイル グループ名	スキャン対象のファイル タイプ
テキスト（Text）	• txt • html • xml
画像	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff
メディア	• aac • aiff • asf • avi • flash • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

アクション変数

bcc()、bcc-scan()、notify()、notify-copy()、add-footer()、insert-headers() の各アクションには、アクションの実行時に元のメッセージの情報に自動的に置き換えられる所定の変数を使用しているパラメータがあります。これらの特殊な変数は*アクション変数*と呼ばれます。Cisco IronPort アプライアンスでは次のアクション変数がサポートされています。

表 6-7　　メッセージ フィルタ アクション変数

変数	構文	説明
すべてのヘッダー（All Headers）	$AllHeaders	メッセージのヘッダーを返します。
本文サイズ（Body Size）	$BodySize	メッセージのサイズをバイト単位で返します。
証明書の署名者（Certificate Signers）	$CertificateSigners	署名付き証明書の subjectAltName 要素から取得した署名者を返します。詳細については、$CertificateSigners アクション変数（6-43 ページ）を参照してください。
日付（Date）	$Date	現在の日付を MM/DD/YYYY 形式で返します。
ドロップされたファイル名（Dropped File Name）	$dropped_filename	直近にドロップされたファイル名のみを返します。
ドロップされたファイル名（Dropped File Names）	$dropped_filenames	ドロップされたファイルのリストを表示します（$filenames と同様です）。
ドロップされたファイル タイプ（Dropped File Types）	$dropped_filetypes	ドロップされたファイルのタイプを表示します（$filetypes と同様です）。
エンベロープ送信者（Envelope Sender）	$EnvelopeFrom	メッセージのエンベロープ送信者（Envelope From、<MAIL FROM>）を返します。
エンベロープ受信者（Envelope Recipients）	$EnvelopeRecipients	メッセージのすべてのエンベロープ受信者（Envelope To、<RCPT TO>）を返します。
ファイル名（File Names）	$filenames	メッセージの添付ファイルの名前のリストをカンマ区切りで返します。
ファイルサイズ（File Sizes）	$filesizes	メッセージの添付ファイルのサイズのリストをカンマ区切りで返します。
ファイルタイプ（File Types）	$filetypes	メッセージの添付ファイルのタイプのリストをカンマ区切りで返します。
フィルタ名（Filter Name）	$FilterName	処理中のフィルタの名前を返します。
GMT 日時（GMTimeStamp）	$GMTimeStamp	メッセージの Received: 行に表示される現在の日時を GMT 形式で返します。
HAT グループ名（HAT Group Name）	$Group	メッセージの送信時に送信者が属していた送信者グループの名前を返します。送信者グループに名前がない場合は、文字列「>Unknown<」が挿入されます。

表 6-7　メッセージ フィルタ アクション変数(続き)

変数	構文	説明
一致した内容 (Matched Content)	`$MatchedContent`	スキャン フィルタ ルール(`body-contains` などのフィルタ ルールやコンテンツ ディクショナリを含む)をトリガーした内容を返します。
メールフローポリシー (Mail Flow Policy)	`$Policy`	メッセージの送信時に送信者に適用された HAT ポリシーの名前を返します。事前に定義されているポリシー名が使用されていない場合、文字列「`>Unknown<`」が挿入されます。
ヘッダー(Header)	`$Header['string']`	引用符で囲まれたヘッダーの値を返します(元のメッセージに該当するヘッダーがある場合)。二重引用符が使用される場合もあります。
ホストネーム	`$Hostname`	Cisco IronPort アプライアンスのホスト名を返します。
内部メッセージ ID (Internal Message ID)	`$MID`	内部でメッセージを識別するため使用されているメッセージ ID(MID)を返します。RFC822「Message-Id」の値とは異なるため注意してください(「Message-Id」を取得するには $Header を使用します)。
受信リスナー (Receiving Listener)	`$RecvListener`	メッセージを受信したリスナーのニックネームに置き換えられます。
受信インターフェイス (Receiving Interface)	`$RecvInt`	メッセージを受信したインターフェイスのニックネームを返します。
リモート IP アドレス (Remote IP Address)	`$RemoteIP`	Cisco IronPort アプライアンスにメッセージを送信したシステムの IP アドレスを返します。
リモートホストアドレス (Remote Host Address)	`$remotehost`	Cisco IronPort アプライアンスにメッセージを送信したシステムのホスト名を返します。
SenderBase レピュテーション スコア	`$Reputation`	送信者の SenderBase レピュテーション スコアを返します。レピュテーション スコアがない場合は「`None`」に置き換えられます。
Subject	`$Subject`	メッセージの件名を返します。
時刻(Time)	`$Time`	現在地の時間帯での現在時刻を返します。
タイムスタンプ (Timestamp)	`$Timestamp`	メッセージの Received: 行に表示される現在の日時を現在地の時間帯に従って返します。

非 ASCII 文字セットとメッセージ フィルタ アクション変数

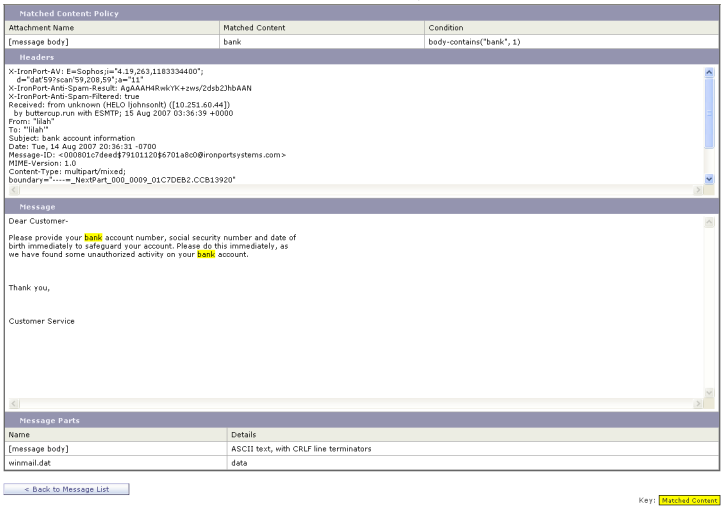
このシステムでは、ISO-2022 スタイル文字コード(ヘッダー値で使用されるエンコードのスタイル)を含むアクション変数の拡張をサポートしています。また、通知内で多言語テキストを使用できます。これらの内容が統合されて通知が生成され、UTF-8 形式の、引用符で囲まれた印刷可能なメッセージとして送信されます。

一致した内容の表示

Attachment Content 条件、Message Body または Attachment 条件、Message 本文条件、または Attachment 内容条件と一致するメッセージに対して隔離アクションを設定した場合、隔離されたメッセージ内の一致した内容を表示できます。メッセージ本文を表示すると、一致した内容が黄色で強調表示されます。また、$MatchedContent アクション変数を使用して、一致した内容をメッセージの件名に含めることができます。

メッセージ フィルタまたはコンテンツ フィルタのルールをトリガーしたローカル隔離内のメッセージを表示すると、フィルタ アクションを実際にはトリガーしなかった内容が（フィルタ アクションをトリガーした内容と共に）GUI で表示されることがあります。GUI の表示は、該当コンテンツを特定するための目安として使用するもので、該当コンテンツの完全なリストであるとは限りません。これは、GUI で使用される内容一致ロジックが、フィルタで使用されるものほど厳密ではないため起こります。この問題は、メッセージ本文内での強調表示に対してのみ当てはまります。メッセージの各パート内の一致文字列をそれに対応するフィルタ ルールと共に一覧表示するテーブルは正しく表示されます。

図 6-2　　ポリシー隔離エリア内で表示された一致内容



メッセージ フィルタ アクションの例

「残りのメッセージ フィルタをスキップ」アクション

skip-filters アクションを実行すると、メッセージ フィルタによるメッセージの処理がスキップされ、メッセージは電子メール パイプラインを通過します。アプライアンスでアンチスパム スキャンとアンチウイルス スキャンが使用できる場合、skip-filters アクションを実行したメッセージはこれらのスキャンの対象となります。skip-filters アクションは、メッセージ フィルタのデフォルトの最終アクションです。

次のフィルタは、customercare@example.com に通知を送信し、boss@admin 宛てのメッセージをただちに送信します。

```
bossFilter:

   if(rcpt-to == 'boss@admin$')
```

```
   {
        notify('customercare@example.com');
 skip-filters();
   }
```

ドロップ アクション

drop アクションを実行すると、メッセージは送信されずに破棄されます。メッセージは送信者には戻されず、メッセージの本来の宛先にも送信されず、それ以外の処理も一切行われません。

次のフィルタは、まず george@whitehouse.gov に通知を送信し、件名が「SPAM」で始まるメッセージを破棄します。

```
spamFilter:
   if(subject == '^SPAM.*')
   {
        notify('george@whitehouse.gov');
        drop();
   }
```

バウンス アクション

bounce アクションは、メッセージを送信者（エンベロープ送信者）に戻し、それ以降の処理は行いません。

次のフィルタは、@yahoo\\.com で終わる電子メール アドレスから送信されたすべてのメッセージを返送します（バウンスします）。

```
yahooFilter:
   if(mail-from == '@yahoo\\.com$')
   {
        bounce();
   }
```

暗号化アクション

encrypt アクションは、設定された暗号化プロファイルを使用して、電子メール受信者に暗号化されたメッセージを送信します。

次のフィルタは、メッセージの件名に [encrypt] という語句が含まれている場合に、そのメッセージを暗号化します。

```
Encrypt_Filter:

  if ( subject == '\\[encrypt\\]' )

   {

       encrypt('My_Encryption_Profile');

   }
```

（注）　このフィルタ アクションを使用するには、ネットワークに Cisco IronPort 暗号化アプライアンスがあるか、ホスト キー サービスが設定されている必要があります。また、このフィルタ アクションを使用するには、暗号化プロファイルの設定が必要です。

通知およびコピー通知アクション

notify および notify-copy アクションは、指定した電子メールに対して、メッセージの概要を電子メールで送信します。notify-copy アクションは、bcc-scan アクションと同様に、元のメッセージのコピーも送信します。通知概要には次の内容が含まれます。

- メッセージのメール転送プロトコル対話から取得したエンベロープ送信者およびエンベロープ受信者（MAIL FROM および RCPT TO）指定の内容。
- メッセージのヘッダー。
- メッセージを検出したメッセージ フィルタの名前。

受信者、件名行、送信元アドレス、および通知テンプレートを指定できます。次のフィルタは、サイズが 4 MB を超えるメッセージを選択し、一致するメッセージのそれぞれについて通知メッセージを admin@example.com に送信し、最後にメッセージを破棄します。

```
bigFilter:

   if(body-size >= 4M)

   {

        notify('admin@example.com');

        drop();

   }
```

または

```
bigFilterCopy:

   if(body-size >= 4M)

   {

        notify-copy('admin@example.com');
```

```
        drop();

    }
```

エンベロープ受信者パラメータとして、有効な任意の電子メール アドレス（上の例では admin@example.com）を指定できます。また、メッセージのすべてのエンベロープ受信者を指定するアクション変数 $EnvelopeRecipients（アクション変数（6-51 ページ）を参照）を指定することもできます。

```
bigFilter:

    if(body-size >= 4M)

    {

        notify('$EnvelopeRecipients');

        drop();

    }
```

notify アクションでは最大で 3 つのオプション引数を使用でき、件名ヘッダー、エンベロープ送信者、通知メッセージに使用する定義済みテキスト リソースを指定できます。これらのパラメータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合や通知テンプレートを指定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（アクション変数（6-51 ページ）を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、件名は「Message Notification」に設定されています。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する $EnvelopeFrom アクション変数を指定することもできます。

通知テンプレート パラメータは、既存の通知テンプレートの名前になります。詳細については、通知（6-76 ページ）を参照してください。

次の例は前の例を拡張したものですが、件名が「[bigFilter] Message too large」となるように変更し、リターンパスを元の送信者に設定し、「message.too.large」テンプレートを使用しています。

```
bigFilter:

    if (body-size >= 4M)

    {

        notify('admin@example.com', '[$FilterName] Message too large',

               '$EnvelopeFrom', 'message.too.large');

        drop();

    }
```

また、$MatchedContent アクション変数を使用して、送信者または管理者にコンテンツ フィルタがトリガーされたことを通知することもできます。$MatchedContent アクション変数は、フィルタをトリガーしたコンテンツを表示します。たとえば、次のフィルタは、電子メールに ABA アカウント情報が含まれる場合に、管理者に通知します。

```
ABA_filter:

if (body-contains ('*aba')){

notify('admin@example.com','[$MatchedContent]Account Information Displayed');

}
```

Notification Template

[テキスト リソース（Text Resources）] ページまたは textconfig CLI コマンドを使用して、notify() および notify-copy() アクションで使用するテキスト リソースとなるカスタム通知テンプレートを設定できます。カスタム通知テンプレートを作成しない場合、デフォルトのテンプレートが使用されます。デフォルトのテンプレートにはメッセージ ヘッダーが含まれますが、デフォルトではカスタム通知テンプレートにはメッセージ ヘッダーは含まれません。カスタム通知にメッセージ ヘッダーを含めるには、$AllHeaders アクション変数を使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」の章を参照してください。

次の例では、メッセージのサイズが大きい場合に次のフィルタがトリガーされると、本来の受信者に対して、メッセージが大きすぎることを示す電子メールが送信されます。

```
bigFilter:

   if (body-size >= 4M)

   {

        notify('$EnvelopeRecipients', '[$FilterName] Message too large',

              '$EnvelopeFrom', 'message.too.large');

        drop();

   }
```

ブラインド カーボン コピー アクション

bcc アクションは、メッセージの無記名コピーを、指定した受信者に送信します。この処理はメッセージ レプリケーションとも呼ばれています。元のメッセージにはコピーに関する通知は含まれず、無記名コピーが受信者にバウンスされることはないため、メッセージの元の送信者と受信者はコピーが送信されたことを関知しない場合があります。

次のフィルタは、johnny から sue に送信される各メッセージのブラインド カーボン コピーを mom@home.org に送信します。

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))
```

```
{

     bcc('mom@home.org');

}
```

bcc アクションでは最大で 3 つのオプション引数を使用でき、コピーしたメッセージに使用する件名ヘッダーとエンベロープ送信者、および alt-mailhost を指定できます。これらのパラメータはこの順序で指定する必要があるため、エンベロープ送信者を設定する場合は件名を指定する必要があります。

件名パラメータにはアクション変数（アクション変数（6-51 ページ）を参照）を指定できます。この変数は元のメッセージから取得したデータで置き換えられます。デフォルトでは、元のメッセージの件名（$Subject と同じ内容）が設定されます。

エンベロープ送信者パラメータとして、有効な任意の電子メールアドレスを指定できます。また、メッセージのリターンパスを元のメッセージと同じに設定する $EnvelopeFrom アクション変数を指定することもできます。

次の例は前の例を拡張したもので、件名は「[Bcc] <original subject>」に設定され、リターンパスは badbounce@home.org に設定されています。

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

        bcc('mom@home.org', '[Bcc] $Subject', 'badbounce@home.org');

   }
```

4 番めのパラメータは alt-mailhost です。

```
momFilterAltM:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

      bcc('mom@home.org', '[Bcc] $Subject', '$EnvelopeFrom',
'momaltmailserver.example.com');

   }
```

警告　**Bcc()、notify()、bounce() の各フィルタ アクションを実行すると、ネットワーク内にウイルスが侵入する場合があります。ブラインド カーボン コピー フィルタ アクションは、元のメッセージの完全なコピーであるメッセージを新規作成します。通知フィルタ アクションは、元のメッセージのヘッダーを含むメッセージを新規作成します。まれにではありますが、ヘッダーにウイルスが含まれている場合があります。バウンス フィルタ アクションは、元のメッセージの最初の 10 キロバイトを含むメッセージを新規作成します。3 つのうちいずれの場合についても、新しいメッセージはアンチウイルス スキャンやアンチスパム スキャンの処理対象とはなりません。**

複数のホストに送信する場合は、bcc() アクションを複数回呼び出すことができます。

```
multiplealthosts:

   if (recv-listener == "IncomingMail")

   {

    insert-header('X-ORIGINAL-IP', '$remote_ip');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.4');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.5');

    bcc ('$EnvelopeRecipients', '$Subject', '$EnvelopeFrom', '10.2.3.6');

   }
```

bcc-scan() アクション

bcc-scan アクションは bcc アクションと同様に機能しますが、送信されるメッセージは新しいメッセージとして扱われるため、電子メール パイプライン全体を経由して送信されます。

```
momFilter:

   if ((mail-from == '^johnny$') and (rcpt-to == '^sue$'))

   {

        bcc-scan('mom@home.org');

   }
```

隔離および複製アクション

quarantine(‘quarantine_name’) アクションは、隔離エリアと呼ばれるキューに入れるメッセージにフラグを設定します。隔離の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」を参照してください。duplicate-quarantine(‘quarantine_name’) アクションを実行すると、メッセージのコピーが指定されている隔離エリアにただちに配置されます。隔離エリア名の大文字と小文字は区別されます。

隔離フラグの付けられたメッセージは、電子メール パイプラインの残りの処理を継続します。メッセージがパイプラインの末尾に到達すると、メッセージに 1 つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。それ以外の場合は配信されます。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

したがって、メッセージ フィルタに quarantine() アクションがあり、その後に bounce() または drop() アクションが続く場合、最後のアクションによりメッセージはパイプラインの末尾に到達しないため、メッセージは隔離エリアに配置されません。メッセージ フィルタに隔離アクションが含まれる場合も同様ですが、メッセージはアンチスパムまたはアンチウイルス スキャン、またはコンテンツ フィルタによりドロップされます。最後の skip_filters() アクションにより、メッセージは残りのメッセージ フィルタをスキップしますが、コンテンツ フィルタはそのまま適用される場合があります。たとえば、メッセージ フィルタがメッセージに隔離フラグを設定し、同時に最後の skip-filters() アクションも設定している場合、電子メール パイプラインの他のアクションによりメッセージがドロップされる場合を除き、メッセージは残りのメッセージ フィルタをすべてスキップした上で隔離されます。

次の例では、メッセージに「secret_word」という辞書にあるいずれかの単語が含まれていると、そのメッセージは Policy 隔離エリアに送信されます。

```
quarantine_codenames:

   if (dictionary-match ('secret_words'))

       {

       quarantine('Policy');

       }
```

次の例では、ある会社に .mp3 ファイル形式の添付ファイルをすべてドロップする公式ポリシーがあるものと仮定しています。受信メッセージに .mp3 形式の添付ファイルがある場合、この添付ファイルは削除され、残りのメッセージ（本文と他の添付ファイル）は本来の受信者に送信されます。元のメッセージにすべての添付ファイルが添付されているコピーが隔離（Policy 隔離エリアに送信）されます。ブロックされた添付ファイルを受信する必要がある場合、本来の受信者はメッセージを隔離エリアから解放するよう要求することができます。

```
strip_all_mp3s:

  if (attachment-filename == '(?i)\\.mp3$') {

        duplicate-quarantine('Policy');

        drop-attachments-by-name('(?i)\\.mp3$');

   }
```

受信者変更アクション

alt-rcpt-to アクションは、メッセージの配信時にメッセージのすべての受信者を指定した受信者に変更します。

次のフィルタは、エンベロープ受信者のアドレスに .freelist.com が含まれているすべてのメッセージを送信し、そのメッセージの受信者を system-lists@myhost.com:

```
freelistFilter:

   if(rcpt-to == '\\.freelist\\.com$')

   {

        alt-rcpt-to('system-lists@myhost.com');

   }
```

配信ホスト変更アクション

alt-mailhost アクションは、選択したメッセージのすべての受信者の IP アドレスを、指定した数値 IP アドレスまたはホスト名に変更します。

（注）　alt-mailhost アクションを実行すると、アンチスパム スキャンによりスパムと分類されたメッセージが隔離されないようにすることができます。alt-mailhost アクションは隔離アクションに優先して実行され、指定したメール ホストにメッセージを送信します。

次のフィルタは、すべての受信者について、受信者のアドレスをホスト example.com に変更します。

```
localRedirectFilter:

   if(true)

   {

        alt-mailhost('example.com');

   }
```

これにより、joe@anywhere.com に送信されるメッセージの Envelope To アドレスが joe@anywhere.com になり、メッセージは example.com のメールホストに送信されます。smtproutes コマンドで指定された追加ルーティング情報は、引き続きメッセージのルーティングに適用されます。（ローカル ドメインの電子メールのルーティング（2-1 ページ）を参照）。

（注）　alt-mailhost アクションではポート番号を指定できません。この操作を行うには、かわりに SMTP ルートを追加します。

次のフィルタは、すべてのメッセージを 192.168.12.5 にリダイレクトします。

```
local2Filter:

   if(true)

   {

        alt-mailhost('192.168.12.5');

   }
```

送信元ホスト（Virtual Gateway アドレス）変更アクション

alt-src-host アクションは、メッセージの送信元ホストを指定した送信元に変更します。送信元ホストは、メッセージの送信元となる IP インターフェイス、または IP インターフェイスのグループにより構成されます。IP インターフェイスのグループが選択された場合、システムは電子メールの配信時に、グループ内のすべての IP インターフェイスを送信元インターフェイスとして使用する処理を繰り返します。つまり、これにより 1 台の Cisco IronPort E メール セキュリティ アプライアンスに複数の Virtual Gateway アドレスを設定できます。詳細については、Virtual Gateway™ テクノロジーの使用（2-59 ページ）を参照してください。

IP インターフェイスは、現在システムで設定されている IP インターフェイスまたは IP インターフェイス グループだけに変更できます。次のフィルタは、IP アドレスが 1.2.3.4 であるリモート ホストから受信したすべてのメッセージに対して、発信（配信）IP インターフェイス outbound2 を使用する仮想ゲートウェイを作成します。

```
externalFilter:

   if(remote-ip == '1.2.3.4')

   {

        alt-src-host('outbound2');

   }
```

次のフィルタは、IP アドレスが 1.2.3.4 のリモート ホストから受信したすべてのメッセージに対して、IP インターフェイス グループ Group1 を使用します。

```
groupFilter:

   if(remote-ip == '1.2.3.4')

   {

        alt-src-host('Group1');

   }
```

アーカイブ アクション

archive アクションは、元のメッセージ（すべてのメッセージ ヘッダーと受信者を含む）のコピーを、アプライアンス上の mbox 形式のファイルに保存します。このアクションでは、メッセージを保存するログ ファイルの名前がパラメータとして使用されます。システムはフィルタの作成時に、指定したファイル名で自動的にログ サブスクリプションを作成します。また、既存のフィルタ ログ ファイルを指定することもできます。フィルタとフィルタ ログ ファイルの作成後は、filters -> logconfig サブコマンドでフィルタ ログ オプションを編集できます。

（注）　logconfig コマンドは filters のサブコマンドです。このサブコマンドの完全な説明については、CLI を使用したメッセージ フィルタの管理（6-79 ページ）を参照してください。

mbox 形式は標準の UNIX メールボックス形式で、メッセージを簡単に表示するためのユーティリティが多数用意されています。大部分の UNIX システムでは、「mail -f *mbox.filename*」と入力するとファイルを表示できます。mbox 形式はプレーン テキストであるため、普通のテキスト エディタを使用してメッセージの内容を表示することができます。

次の例では、エンベロープ送信者が joesmith@yourdomain.com と一致する場合に、メッセージのコピーが joesmith というログに保存されます。

```
logJoeSmithFilter:

   if(mail-from == '^joesmith@yourdomain\\.com$')
```

```
{
     archive('joesmith');
}
```

ヘッダー削除アクション

strip-header アクションは、メッセージの特定のヘッダーを調べ、配信する前に該当する行をメッセージから削除します。ヘッダーが複数ある場合は、ヘッダーのすべてのインスタンス（「Received:」ヘッダーなど）が削除されます。

次の例では、すべてのメッセージで送信前に X-DeleteMe ヘッダーが削除されます。

```
stripXDeleteMeFilter:
   if (true)
   {
        strip-header('X-DeleteMe');
   }
```

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージ ヘッダー ルールおよび評価（6-5 ページ）を参照してください。

ヘッダー挿入アクション

insert-header アクションは、メッセージに新しいヘッダーを挿入します。AsyncOS は、挿入したヘッダーが規格を満たしているかどうかを検証しません。生成されるメッセージが電子メールのインターネット規格を満たしているかどうかは、ユーザが自分で確認する必要があります。

次の例では、X-Company というヘッダーがメッセージにない場合に、このヘッダーに My Company Name という値が設定されます。

```
addXCompanyFilter:
   if (not header('X-Company'))
   {
        insert-header('X-Company', 'My Company Name');
   }
```

insert-header() アクションでは、ヘッダーのテキストに非 ASCII 文字を使用できます。ただし、ヘッダー名には（規格遵守のため）ASCII 文字しか使用できません。可読性を最大限に高めるため、トランスポート エンコードは Quoted-Printable となります。

（注） strip-headers アクションと insert-header アクションを組み合わせることにより、元のメッセージにある任意のメッセージ ヘッダーを書き換えることができます。場合によっては、同じヘッダーを複数回使用することができますが（Received: など）、それ以外の場合は同じヘッダーを複数回使用すると MUA が混乱する場合があります（Subject: ヘッダーを複数回使用する場合など）。

ヘッダーに関する操作を行う場合、ヘッダーの現在の値には処理中に行われた変更（メッセージのヘッダーの追加、削除、変更を行うフィルタ処理など）が含まれている点に注意してください。詳細については、メッセージ ヘッダー ルールおよび評価（6-5 ページ）を参照してください。

ヘッダー テキスト編集アクション

edit-header-text アクションを実行すると、正規表現の置換機能を使用して、指定したヘッダー テキストを書き換えることができます。このフィルタはヘッダー内で正規表現と一致するテキストを検索し、指定した正規表現に置き換えます。

たとえば、電子メールに次のような件名ヘッダーがあるものとします。

```
Subject: SCAN Marketing Messages
```

次のフィルタは、「SCAN」というテキストを削除し、「Marketing Messages」というテキストをヘッダー内に残します。

```
Remove_SCAN: if true

   {

      edit-header-text ('Subject', '^SCAN\\s*','');

}
```

フィルタはメッセージを処理した後、次のヘッダーを返します。

```
Subject: Marketing Messages
```

本文編集アクション

edit-body-text() メッセージ フィルタの機能は Edit-Header-Text() フィルタと同様ですが、メッセージのヘッダーではなく本文が処理対象です。

edit-body-text() メッセージ フィルタは次の構文を使用します。最初のパラメータは検索のための正規表現で、2 番めのパラメータは置換のためのテキストです。

```
Example: if true {

edit-body-text("parameter 1",

"parameter 2");

       }
```

edit-body-text() メッセージ フィルタはメッセージ本文のみが処理対象です。特定の MIME 部分がメッセージの「本文」と見なされるか「添付ファイル」と見なされるかの詳細については、メッセージ本文とメッセージ添付ファイル（6-5 ページ）を参照してください。

次の例では、メッセージから URL が削除され、「URL REMOVED」というテキストに置き換えられています。

```
URL_Replaced: if true {



 edit-body-text("(?i)(?:https?|ftp)://[^\\s\">]+", "URL REMOVED");

       }
```

次の例では、メッセージの本文から社会保障番号が削除され、「XXX-XX-XXXX」というテキストに置き換えられています。

```
ssn: if true {

  edit-body-text("(?!000)(?:[0-6]\\d{2}|7(?:[0-6]\\d|7[012]))([
-]?)(?!00)\\d\\d\\1(?!0000)\\d{4}",

"XXX-XX-XXXX");

}
```

（注）　現時点では、edit-body-text() フィルタではスマート ID を使用できません。

HTML 変換アクション

RFC 2822 では電子メール メッセージのテキスト形式が規定されていますが、RFC 2822 メッセージ内の他のコンテンツのトランスポートを実現するための拡張機能（MIME など）があります。AsyncOS は html-convert() メッセージ フィルタを使用して、次の構文により HTML をプレーン テキストに変換できます。

```
Convert_HTML_Filter:

if (true)

{

html-convert();

}
```

Cisco IronPort メッセージ フィルタは、特定の MIME 部分がメッセージの「本文」であるか「添付ファイル」であるかを判別します。html-convert() メッセージ フィルタはメッセージ本文のみが処理対象です。メッセージの本文と添付ファイルの詳細については、メッセージ本文とメッセージ添付ファイル（6-5 ページ）を参照してください。

html-convert() フィルタが文書内の HTML を削除する方式は、形式によって異なります。

メッセージがプレーン テキスト（text/plain）である場合、メッセージは変更されずにフィルタを通過します。メッセージが単純な HTML メッセージ（text/html）である場合、すべての HTML タグはメッセージから削除され、残りの本文が HTML メッセージにかわり使用されます。各行の再フォーマットは行われず、HTML がプレーン テキストになることはありません。構造が MIME（multipart/alternative 構造）で、同じコンテンツに text/plain 部分と text/html 部分が含まれている場合、フィルタはメッセージの text/html 部分を削除して text/plain 部分を残します。その他の MIME タイプ（multipart/mixed など）では、すべての HTML 本文部分のタグが削除され、メッセージに再挿入されます。

メッセージ フィルタでは、html-convert() フィルタ アクションは処理対象のメッセージにタグを設定するだけで、メッセージ構造の変更は直ちには行われません。メッセージの変更は、すべての処理が完了した後に行われます。これにより、変更前に他のフィルタ アクションが元のメッセージを処理することができます。

バウンス プロファイル アクション

bounce-profile アクションは、設定済みのバウンス プロファイルをメッセージに割り当てます。（バウンスした電子メールの処理（2-35 ページ）を参照）。メッセージを配信できない場合、バウンス プロファイルで設定されたバウンス オプションが使用されます。この機能は、リスナーの設定から割り当てられているバウンス プロファイル（割り当てられている場合）に優先して適用されます。

次のフィルタの例では、送信される電子メールのうち、ヘッダーに「X-Bounce-Profile: fastbounce」があるすべての電子メールにバウンス プロファイル「fastbounce」が割り当てられます。

```
fastbounce:

   if (header ('X-Bounce-Profile') == 'fastbounce') {

        bounce-profile ('fastbounce');

   }
```

アンチスパム システムのバイパス アクション

skip-spamcheck アクションは、システムに設定されたコンテンツベースのアンチスパム フィルタリングをすべてバイパスするようシステムに指示します。コンテンツベースのアンチスパム フィルタリングが設定されていない場合、またはメッセージがあらかじめスパム スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、メッセージの SenderBase レピュテーション スコアが高い場合に、メッセージに対するコンテンツベースのアンチスパム フィルタリングがバイパスされます。

```
whitelist_on_reputation:

   if (reputation > 7.5)

   {

        skip-spamcheck();

   }
```

アンチウイルス システムのバイパス アクション

skip-viruscheck アクションは、システムに設定されたウイルス保護システムをすべてバイパスするようシステムに指示します。アンチウイルス システムが設定されていない場合、またはメッセージがあらかじめウイルス スキャンの対象に設定されていない場合は、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、アンチスパム システムとアンチウイルス システムによる処理がバイパスされています。

```
internal_mail_is_safe:

   if (recv-listener == 'private_listener')

   {

        skip-spamcheck();

        skip-viruscheck();

   }
```

ウイルス アウトブレイク フィルタのスキャニング処理バイパス アクション

skip-vofcheck アクションは、メッセージのウイルス アウトブレイク フィルタによるスキャニング処理がバイパスされるようシステムに指示します。ウイルス アウトブレイク フィルタのスキャニング処理がイネーブルになっていない場合、このアクションを実行してもメッセージに影響はありません。

次の例では、「private_listener」というリスナーで受信したメッセージに対して、ウイルス アウトブレイク フィルタのスキャニング処理がバイパスされています。

```
internal_mail_is_safe:

   if (recv-listener == 'private_listener') Outbreak Filters

   {

        skip-vofcheck();

   }
```

メッセージ タグ追加アクション

tag-message アクションは、RSA Email DLP ポリシー フィルタリングで使用するカスタム用語を送信メッセージに挿入します。RSA Email DLP ポリシーを設定して、スキャン対象をメッセージ タグがあるメッセージに限定することができます。メッセージ タグは受信者側では表示されません。タグ名には、[a-zA-Z0-9_-.] の範囲の文字のうち任意のものを組み合わせて使用できます。

メッセージのフィルタリングに使用する DLP ポリシーの設定については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Data Loss Prevention」の章を参照してください。

次の例では、件名に「[Encrypt]」が含まれるメッセージにメッセージ タグを挿入しています。Cisco IronPort Email Encryption が使用できる場合は、メッセージの配信前にメッセージをこのメッセージ タグで暗号化する DLP ポリシーを作成できます。

```
Tag_Message:

   if (subject == '^\\[Encrypt\\]')

   {

        tag-message('Encrypt-And-Deliver');

   }
```

ログ エントリ追加アクション

log-entry アクションは、カスタマイズしたテキストを、IronPort テキスト メール ログに INFO レベルで追加します。このテキストにはアクション変数を使用することができます。このアクションを使用すると、デバッグ時に便利なテキストや、メッセージ フィルタがアクションを実行した理由に関する情報を挿入できます。ログ エントリはメッセージ トラッキングにも表示されます。

次の例では、メッセージに会社の機密情報が含まれていると判断されたためメッセージがバウンスされたことを示すログ エントリが挿入されます。

```
CompanyConfidential:

   if (body-contains('Company Confidential'))

   {

        log-entry('Message may have contained confidential information.');

        bounce();

   }
```

添付ファイルのスキャン

AsyncOS は企業ポリシーに準拠していないメッセージの添付ファイルを削除でき、一方で元のメッセージはそのまま配信することができます。

添付ファイルのフィルタリングは、特定のファイル タイプ、フィンガープリント、添付ファイルの内容に基づいて行うことができます。フィンガープリントを使用して添付ファイルの正確な種類を判別することにより、ユーザは悪意のある添付ファイルの拡張子（.exe など）を一般的な拡張子（.doc など）に変更して、名前が変更されたファイルが添付ファイル フィルタを通過できるようにすることができなくなります。

添付ファイルのコンテンツをスキャンすると、Stellent 添付ファイル スキャン エンジンは添付ファイルからデータを抽出し、正規表現による検索を実行します。添付ファイルのデータとメタデータの両方が検査対象となります。Excel または Word 文書をスキャンする場合、添付ファイル スキャン エンジンは .exe、.dll、.bmp、.tiff、.pcx、.gif、.jpeg、.png、Photoshop 画像の各埋め込みファイルも検出できます。

添付ファイルのスキャンで使用するメッセージ フィルタ

表 6-8 に記載されているメッセージ フィルタ アクションは*最終でない*アクションです。(添付ファイルはドロップされ、メッセージの処理が続行されます)。

オプションのコメントは、フッターのようにメッセージに追加されるテキストで、メッセージ フィルタ アクション変数(添付ファイルのスキャン メッセージ フィルタの例(6-76 ページ)を参照)を使用することもできます。

表 6-8　　添付ファイルのスキャンで使用するメッセージ フィルタ アクション

操作	構文	説明
添付ファイルのドロップ(名前別)	`drop-attachments-by-name (<regular expression>[, <optional comment>])`	メッセージの添付ファイルのうち、指定した正規表現と一致する名前のファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。添付ファイルのスキャン メッセージ フィルタの例(6-76 ページ)を参照してください。
添付ファイルのドロップ(タイプ別)	`drop-attachments-by-type (<MIME type>[, <optional comment>])`	メッセージの添付ファイルのうち、指定した MIME タイプまたはファイル拡張子に該当する MIME タイプのファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。
添付ファイルのドロップ(ファイル タイプ別)	`drop-attachments-by-filetype (<fingerprint name>[, <optional comment>])`	メッセージの添付ファイルのうち、指定したファイルの「フィンガープリント」と一致するファイルをすべてドロップします。アーカイブ形式の添付ファイル(zip、tar)内に該当するファイルがある場合、この添付ファイルはドロップされます。詳細については、表 6-6 添付ファイル グループ(6-49 ページ)を参照してください。
添付ファイルのドロップ(MIME タイプ別)	`drop-attachments-by-mimetype (<MIME type>[, <optional comment>])`	メッセージの添付ファイルのうち、特定の MIME タイプのファイルをすべてドロップします。このアクションではファイル拡張子による MIME タイプの判別は行われず、アーカイブの内容の確認もされません。
添付ファイルのドロップ(サイズ別)	`drop-attachments-by-size (<number>[, <optional comment>])`	メッセージの添付ファイルのうち、ロー エンコード形式で指定したサイズ(バイト単位)以上のサイズであるファイルをすべてドロップします。アーカイブ ファイルまたは圧縮ファイルの場合、このアクションは、圧縮前のサイズを検証せず、実際の自体のサイズが計測されます。
添付ファイルのスキャン	`drop-attachments-where-contains (<regular expression>[, <optional comment>])`	メッセージの添付ファイルのうち、指定した正規表現を含むファイルをすべてドロップします。アーカイブ ファイル(zip、tar)は、中に含まれているファイルのいずれかが正規表現と一致する場合にドロップされます。

表 6-8　添付ファイルのスキャンで使用するメッセージ フィルタ アクション（続き）

操作	構文	説明
添付ファイルのドロップ（辞書との一致別）	`drop-attachments-where-dictionary-match(<dictionary name>)`	このフィルタ アクションは、辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。添付ファイルのスキャン メッセージ フィルタの例（6-76 ページ）を参照してください。

イメージ分析

メッセージによってはイメージを含むものがあり、適切でないコンテンツがないかスキャンすることが必要になる場合があります。イメージ分析エンジンを使用すると、電子メール内の適切でないコンテンツを検索できます。イメージ分析は、アンチウイルスおよびアンチスパム スキャン エンジンの補完または代替を目的とするものではありません。この機能は、電子メール内の適切でないコンテンツを特定することにより、許容範囲での使用を促進するためのものです。イメージ分析スキャン エンジンを使用すると、メールの隔離と分析、および傾向の認識ができます。

AsyncOS でイメージ分析を設定すると、イメージ分析フィルタ ルールを使用して、疑わしい電子メールや適切でない電子メールに対してアクションを実行することができます。イメージ スキャンでは、JPEG、BMP、PNG、TIFF、GIF、TGA、ICO、PCX の各添付ファイルのタイプをスキャンできます。イメージ アナライザは、スキン カラー、本体サイズ、曲率を測定するアルゴリズムを使用し、画像に適切でないコンテンツが含まれる可能性を判定します。イメージ添付ファイルをスキャンすると、Cisco IronPort フィンガープリントによりファイル タイプが特定され、イメージ アナライザはイメージ コンテンツを分析するアルゴリズムを使用します。イメージが別のファイルに埋め込まれている場合、Stellent スキャン エンジンによりファイルが抽出されます。Stellent スキャン エンジンは、Word、Excel、PowerPoint 文書などの各種のファイル タイプからイメージを抽出できます。イメージ分析の結果は、メッセージ全体で計算されます。メッセージにイメージがない場合、メッセージのスコアは 0 となります。これは分析結果が「Clean」であることを表します。そのため、イメージがないメッセージに対する分析結果は「Clean」となります。

（注） PDF ファイルのイメージは抽出されません。

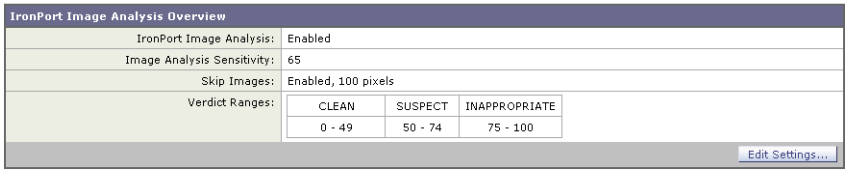
GUI からイメージ分析をイネーブル化するには、次の手順を実行します。

ステップ 1　[セキュリティ サービス（Security Services）] > [IronPort イメージ分析（IronPort Image Analysis）] の順に進みます。

ステップ 2　[有効（Enable）] をクリックします。

成功したことを示すメッセージが表示され、分析結果設定が表示されます。

図 6-3　Cisco IronPort イメージ分析の概要



イメージ分析フィルタ ルールを使用すると、次の各分析結果に基づいてアクションを決定できます。

- [正常（Clean）]: イメージに適切でないコンテンツはありません。イメージ分析の結果はメッセージ全体で計算されるため、イメージがないメッセージをスキャンすると分析結果は [正常（Clean）] となります。
- [疑わしい（Suspect）]: イメージに適切でないコンテンツがある可能性があります。
- [不適切（Inappropriate）]: イメージに適切でないコンテンツがあります。

これらの計算結果には、イメージ アナライザのアルゴリズムにより、適切でないコンテンツがある可能性を示す数値が割り当てられます。

次の値が推奨されます。

- [正常（Clean）]: 0 ～ 49
- [疑わしい（Suspect）]: 50 ～ 74
- [不適切（Inappropriate）]: 75 ～ 100

精度を設定することによりイメージ スキャンを微調整できます。これにより、誤判定を減らすことができます。たとえば、誤判定が発生している場合は、精度を低くします。逆に、イメージ スキャンで適切でないコンテンツが検出されていない場合は、精度を高く設定します。精度設定は 0（一切検出しない）と 100（精度が最高である）の間の値です。デフォルトの精度の 65 に設定することを推奨します。

スキャン値の設定

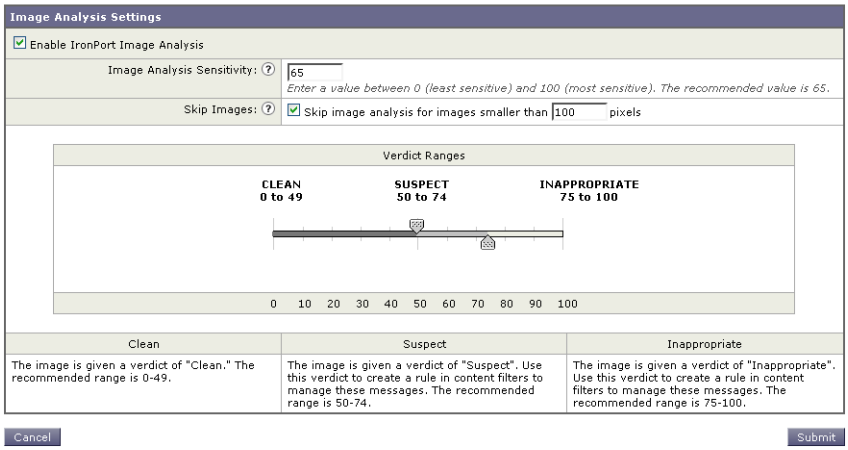
スキャン値を設定するには、次の手順を実行します。

ステップ 1　[セキュリティ サービス（Security Services）] > [IronPort イメージ分析（IronPort Image Analysis）] の順に進みます。

ステップ 2　[Edit Settings] をクリックします。

[Edit IronPort Image Analysis Settings] ページが表示されます。

図 6-4　IronPort イメージ分析設定の編集



ステップ 3　イメージ分析の精度を設定します。デフォルトの精度の 65 に設定することを推奨します。

ステップ 4　[正常（Clean）]、[疑わしい（Suspect）]、および [不適切（Inappropriate）] の評価を設定します。

値の範囲を設定する場合、値が重ならないようにしてください。また、すべて整数を使用してください。

ステップ 5　任意で、最小サイズの要件を満たさないイメージのスキャンをバイパスするように、AsyncOS を設定します（推奨）。デフォルトで、この設定は 100 ピクセルに設定されています。100 ピクセル未満のイメージをスキャンすると、誤検知が発生する可能性があります。

`imageanalysisconfig` コマンドを使用して、CLI からイメージ分析設定をイネーブルにすることもできます。

```
test.com> imageanalysisconfig


IronPort Image Analysis: Enabled

Image Analysis Sensitivity: 65

Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)

Skip small images with size less than 100 pixels (width or height)


Choose the operation you want to perform:

- SETUP - Configure IronPort Image Analysis.

[]> setup


IronPort Image Analysis: Enabled

Would you like to use IronPort Image Analysis? [Y]>
```

```
Define the image analysis sensitivity. Enter a value between 0 (least

sensitive) and 100 (most sensitive). As sensitivity increases, so does the false positive
rate. The default setting of 65 is recommended.

[65]>



Define the range for a CLEAN verdict. Enter the upper bound of the CLEAN range by
entering a value between 0 and 98. The default setting of 49 is recommended.

[49]>



Define the range for a SUSPECT verdict. Enter the upper bound of the SUSPECT range by
entering a value between 50 and 99. The default setting of 74 is recommended.

[74]>



Would you like to skip scanning of images smaller than a specific size? [Y]>



Please enter minimum image size to scan in pixels, representing either height or width of
a given image.

[100]>
```

評価結果の表示

特定のメッセージのレピュテーション スコアを確認するには、メール ログを参照します。メール ログにはイメージ名またはファイル名、特定のメッセージの添付ファイルのスコアが表示されます。また、ログにはファイル内のイメージがスキャン可能かどうかについての情報も表示されます。このログには、各イメージではなく、各メッセージの添付ファイルの結果に関する情報が表示されます。たとえば、メッセージに JPEG イメージを含む zip ファイルが添付されていた場合、ログのエントリには JPEG の名前ではなく、zip ファイルの名前が表示されます。また、zip ファイルに複数のイメージが含まれている場合、ログ エントリにはすべてのイメージの最大スコアが表示されます。「unscannable」の通知は、いずれかのイメージがスキャンできないことを意味します。

ログには、スコアがどのように特定の評価（[正常（clean）]、[疑わしい（suspect）]、または [不適切（inappropriate）]）に反映されるかに関する情報はありません。ただし、メール ログを使用して特定のメッセージの配信を追跡できるため、メッセージに対して実行されたアクションによって、メールに不適切なイメージまたは疑わしいイメージが含まれていたかどうかがわかります。

たとえば、次のメール ログでは、イメージ分析スキャンの結果、メッセージ フィルタ ルールによってドロップされた添付ファイルを示しています。

```
Thu Apr 3 08:17:56 2009 Debug: MID 154 IronPort Image Analysis: image 'Unscannable.jpg'
is unscannable.

Thu Apr 3 08:17:56 2009 Info: MID 154 IronPort Image Analysis: attachment
'Unscannable.jpg' score 0 unscannable



Thu Apr 3 08:17:56 2009 Info: MID 6 rewritten to MID 7 by
drop-attachments-where-image-verdict filter 'f-001'



Thu Apr 3 08:17:56 2009 Info: Message finished MID 6 done
```

イメージ分析メッセージ フィルタの使用

イメージ分析をイネーブルにしたら、メッセージ フィルタを作成して、さまざまなメッセージの評価に対してさまざまなアクションを実行する必要があります。たとえば、問題ないと評価されたメッセージを配信し、不適切なコンテンツを含むと判断されたメッセージを隔離する必要があるとします。

（注） シスコでは、不適切または疑わしいと評価されたメッセージをドロップまたはバウンスしないことを推奨します。代わりに、後で確認してトレンド分析について把握するために、違反したメッセージのコピーを隔離します。

次のフィルタは、コンテンツが不適切または疑わしい場合にタグを付けられるメッセージを示しています。

```
image_analysis: if image-verdict == "inappropriate" {

strip-header("Subject");

insert-header("Subject", "[inappropriate image] $Subject");

}

 else {

if image-verdict == "suspect" {

strip-header("Subject");

insert-header("Subject", "[suspect image] $Subject");

}

}
```

イメージ分析コンテンツ フィルタの使用

イメージ分析をイネーブルにすると、コンテンツ フィルタを作成してイメージ分析の評価に基づいて添付ファイルを削除するか、さまざまなメッセージの評価に対してさまざまなアクションを実行するようにフィルタを設定できます。たとえば、不適切なコンテンツを含むメッセージを隔離することに決定したとします。

イメージ分析の評価に基づいて添付ファイルを削除するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 2　[フィルタを追加（Add Filter）] をクリックします。

ステップ 3　コンテンツ フィルタの名前を入力します。

ステップ 4　[アクション（Actions）] で、[アクションを追加（Add Action）] をクリックします。

ステップ 5　[ファイル情報によって添付ファイルを除去（Strip Attachment by File Info）] で、[イメージ分析判定（Image Analysis Verdict is）] をクリックします。

ステップ 6　次のイメージ分析の評価から選択します。

- 疑わしい（Suspect）
- 不適切（Inappropriate）
- 不適切もしくは疑わしい（Suspect or Inappropriate）
- スキャン不可（Unscannable）
- 正常（Clean）

イメージ分析の評価に基づくアクションを設定するには、次の手順を実行します。

ステップ 1　[メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] をクリックします。

ステップ 2　[フィルタを追加（Add Filter）] をクリックします。

ステップ 3　コンテンツ フィルタの名前を入力します。

ステップ 4　[条件（Conditions）] で、[条件を追加（Add Condition）] をクリックします。

ステップ 5　[添付ファイルのファイル情報（Attachment File Info）] で、[イメージ分析判定（Image Analysis Verdict）] をクリックします。

ステップ 6　次のいずれかの評価を選択します。

- 疑わしい（Suspect）
- 不適切（Inappropriate）
- 不適切もしくは疑わしい（Suspect or Inappropriate）
- スキャン不可（Unscannable）
- 正常（Clean）

ステップ 7　[アクションを追加（Add Action）] をクリックします。

ステップ 8　イメージ分析の評価に基づいてメッセージに対して実行するアクションを選択します。

ステップ 9　変更を送信し、保存します。

通知

GUI の [テキストリソース(Text Resources)] ページまたは textconfig CLI コマンドを使用して、カスタム通知テンプレートをテキスト リソースとして設定することもできます。これも、添付ファイルのフィルタ ルールと組み合わせて使用すると便利なツールです。通知テンプレートは非 ASCII 文字をサポートしています(テンプレートを作成するとき、エンコードを選択するように要求されます)。

次の例では、最初に textconfig コマンドを使用して、strip.mp3 という名前の通知テンプレートを作成します。これは、通知メッセージの本文に挿入されます。次に、添付ファイルのフィルタ ルールを作成し、.mp3 ファイルがメッセージから削除された場合、予定していた受信者宛てに .mp3 ファイルが削除されたことを通知する電子メールが送信されるように設定できます。

```
drop-mp3s:

if (attachment-type == '*/mp3')

{ drop-attachments-by-filetype('Media');

  notify ('$EnvelopeRecipients', 'Your mp3 has been removed', '$EnvelopeFrom',
'strip.mp3');

}
```

詳細については、通知およびコピー通知アクション(6-55 ページ)を参照してください。

添付ファイルのスキャン メッセージ フィルタの例

次に、添付ファイルに対して実行されるアクションの例を示します。

ヘッダーの挿入

この例では、添付ファイルに指定したコンテンツが含まれている場合に、AsyncOS がヘッダーを挿入します。

次の例では、あるキーワードが含まれるかどうか、メッセージのすべての添付ファイルをスキャンします。すべての添付ファイルにキーワードが存在する場合、カスタムの X-Header が挿入されます。

```
attach_disclaim:

    if (every-attachment-contains('[dD]isclaimer') ) {

        insert-header("X-Example-Approval", "AttachOK");

    }
```

次の例では、特定のバイナリ データのパターンがあるかどうか、添付ファイルをスキャンします。フィルタは attachment-binary-contains フィルタ ルールを使用して、PDF ドキュメントが暗号化されていることを示すパターンを検索します。バイナリ データ内にそのパターンが存在する場合、カスタム ヘッダーが挿入されます。

```
match_PDF_Encrypt:

if (attachment-filetype == 'pdf' AND

attachment-binary-contains('/Encrypt')){

strip-header (‘Subject’);

insert-header (‘Subject’, ‘[Encrypted] $Subject’);

}
```

ファイル タイプによる添付ファイルのドロップ

次の例では、添付ファイルの「executable」グループ（.exe、.dll、および .scr）がメッセージから削除され、削除されたファイルの名前を列挙するテキストがメッセージに追加されます（$dropped_filename アクション変数を使用）。drop-attachments-by-filetype アクションは添付ファイルを確認し、3 文字のファイル拡張子だけではなく、ファイルのフィンガー プリントに基づいて添付ファイルを削除します。1 つのファイル タイプ（「mpeg」）を指定したり、あるファイル タイプのすべてのメンバ（「Media」）を参照したりできます。

```
strip_all_exes: if (true) {

                    drop-attachments-by-filetype ('Executable', “Removed attachment:
$dropped_filename”);

                }
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、同じ「executable」グループの添付ファイル（.exe、.dll、および .scr）が、削除されます。

```
strip_inbound_exes: if (mail-from != "@example\\.com$") {

                        drop-attachments-by-filetype ('Executable');

                    }
```

次の例では、エンベロープ送信者がドメイン example.com 内に存在しないメッセージから、ファイル タイプの特定のメンバ（「wmf」）および同じ「executable」グループの添付ファイル（.exe、.dll、および .scr）が削除されます。

```
strip_inbound_exes_and_wmf: if (mail-from != "@example\\.com$") {

                        drop-attachments-by-filetype ('Executable');

                        drop-attachments-by-filetype ('x-wmf');

                    }
```

次の例では、添付ファイルの「executable」事前定義グループが、より多くの添付ファイルの名前を含むように拡張されています（このアクションでは、添付ファイルのファイル タイプは確認*されません*）。

```
strip_all_dangerous: if (true) {

                    drop-attachments-by-filetype ('Executable');

                      drop-attachments-by-name('(?i)\\.(cmd|pif|bat)$');

                     }
```

drop-attachments-by-name アクションでは、非 ASCII 文字をサポートしています。

（注）　drop-attachments-by-name アクションは、MIME ヘッダーでキャプチャされたファイル名に対して正規表現照合を実行します。MIME ヘッダーからキャプチャされたファイル名は、最後にスペースが存在する場合があります。

次の例では、添付ファイルがメッセージに .exe 実行ファイルのファイル タイプでない場合はドロップされます。ただし、フィルタは、除外するファイル タイプを備えた少なくとも 1 つの添付ファイルがあるメッセージへのアクションを実行しません。たとえば、次のフィルタは *.exe* ファイル タイプではない添付ファイルを含むメッセージをドロップします。

```
exe_check: if (attachment-filetype != "exe") {

                    drop();

                }
```

メッセージに複数の添付ファイルがある場合、E メール セキュリティ アプライアンスは他の添付ファイルが .exe ファイルでない場合でも、添付ファイルの少なくとも 1 つが .exe ファイルの場合はメッセージをドロップしません。

ディクショナリの一致による添付ファイルのドロップ

この drop-attachments-where-dictionary-match アクションでは、辞書の用語との一致に基づいて添付ファイルを削除します。添付ファイルであると判断される MIME 部分の用語が辞書の用語と一致する場合（かつ、ユーザ定義のしきい値に達している場合）、添付ファイルが電子メールから削除されます。次の例では、「secret_words」辞書内の単語が添付ファイル内で検出されると、添付ファイルが削除されます。一致のしきい値は 1 に設定されている点に注意してください。

```
Data_Loss_Prevention: if (true) {

drop-attachments-where-dictionary-match("secret_words", 1);

}
```

保護された添付ファイルの隔離

attachment-protected フィルタでは、メッセージ内の添付ファイルがパスワード保護されているかをテストします。受信メールに対してこのフィルタを使用して、添付ファイルがスキャン可能かどうかを確認できます。この定義に従い、1 つの暗号化されたメンバと複数の暗号化されていないメンバーを含む zip ファイルは、保護されていると見なされます。同様に、オープン パスワードが設定されていない PDF ファイルは、コピーや印刷がパスワード保護されていたとしても、保護されているとは見なされません。次の例では、保護された添付ファイルが隔離エリア「Policy」に送信されます。

```
quarantine_protected:

if attachment-protected

{

quarantine("Policy");

}
```

保護されていない添付ファイルの検出

attachment-unprotected フィルタは、メッセージ内の添付ファイルがパスワード保護されていないかをテストします。このメッセージ フィルタは、attachment-protected フィルタと補完関係にあります。このフィルタを送信メールに使用して、保護されていないメールを検出することができます。次の例では、AsyncOS が送信リスナーで保護されていない添付ファイルを検出し、メッセージを隔離しています。

```
quarantine_unprotected:

if attachment-unprotected

{

quarantine("Policy");

}
```

CLI を使用したメッセージ フィルタの管理

CLI を使用して、メッセージ フィルタの追加、削除、アクティブ化/非アクティブ化、インポート/エクスポート、ログ オプションの設定が可能です。次の表で、コマンドとサブコマンドについてまとめて説明します。

表 6-9　メッセージ フィルタ サブコマンド

構文	説明
filters	メイン コマンド。このコマンドは対話形式で、詳細情報を入力するよう要求されます（たとえば、new、delete、import など）。

表 6-9　メッセージ フィルタ サブコマンド（続き）

構文	説明
new	新しいフィルタを作成します。場所を指定しない場合、現在のシーケンスにフィルタが追加されます。場所を指定した場合、シーケンスの特定の場所にフィルタが挿入されます。詳細については、新しいメッセージ フィルタの作成（6-81 ページ）を参照してください。
delete	名前またはシーケンス番号を指定して、フィルタを削除します。詳細については、メッセージ フィルタの削除（6-81 ページ）を参照してください。
移動	既存のフィルタを並べ替えます。詳細については、メッセージ フィルタの移動（6-81 ページ）を参照してください。
設定	フィルタをアクティブまたは非アクティブ状態に設定します。詳細については、メッセージ フィルタのアクティベーションとディアクティベーション（6-82 ページ）を参照してください。
import	フィルタの現在のセットを、ファイル（アプライアンスの /configuration ディレクトリ）内に保存されている新しいセットに置き換えます。詳細については、メッセージ フィルタのインポート（6-85 ページ）を参照してください。
export	フィルタの現在のセットを（アプライアンスの /configuration ディレクトリ内の）ファイルにエクスポートします。詳細については、メッセージ フィルタのエクスポート（6-86 ページ）を参照してください。
list	1 つ以上のフィルタに関する情報を一覧表示します。詳細については、メッセージ フィルタ リストの表示（6-86 ページ）を参照してください。
detail	特定のフィルタに関する詳細情報（フィルタ ルール自体の本文など）を出力します。詳細については、メッセージ フィルタの詳細の表示（6-86 ページ）を参照してください。
logconfig	フィルタの logconfig サブメニューを入力すると、`archive()` フィルタ アクションからログ サブスクリプションを編集できます。詳細については、フィルタ ログ サブスクリプションの設定（6-87 ページ）を参照してください。

（注）　フィルタを有効にするには、`commit` コマンドを発行する必要があります。

パラメータには、次の 3 つのタイプがあります。

表 6-10　フィルタ管理パラメータ

seqnum	フィルタのリスト内の位置に基づいてフィルタを表す整数です。たとえば、*seqnum* が 2 の場合、リスト内の 2 番めのフィルタを表します。
filtname	フィルタの表示名。
range	range は、複数のフィルタを表す場合に使用することがあり、「*X-Y*」の形式で表されます。X と Y は、範囲を指定するための最初と最後の *seqnums* です。たとえば、「`2-4`」は、2、3、4 番めの位置にあるフィルタを表します。X または Y のいずれかを省略すると、無制限のリストを表します。たとえば、「`-4`」は最初から 4 つのフィルタを表し、「`2-`」は、先頭以外のすべてのフィルタを表します。キーワード `all` を使用して、フィルタ リスト内のすべてのフィルタを表すこともできます。

新しいメッセージ フィルタの作成

```
new [seqnum|filtname|last]
```

新しいフィルタを挿入する位置を指定します。省略するか、キーワード `last` を指定すると、入力されたフィルタがフィルタ リストの最後に追加されます。シーケンス番号は連続させる必要があります。現在のリストの範囲を超える *seqnum* は入力できません。不明な *filtname* を入力すると、有効な *filtname*、*seqnum*、または `last` を入力するように求められます。

フィルタを入力したら、手動でフィルタ スクリプトを入力する必要があります。入力を終了したら、その行自体にピリオド(.)を入力してエントリを終了します。

次の条件ではエラーが発生します。

- シーケンス番号が現在のシーケンス番号の範囲を超えている。
- フィルタに付けた *filtname* が一意ではない。
- フィルタに付けた *filtname* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステム リソースを参照するアクションを実行するフィルタ。

メッセージ フィルタの削除

```
delete [seqnum|filtname|range]
```

指定したフィルタを削除します。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

メッセージ フィルタの移動

```
move [seqnum|filtname|range seqnum|last]
```

最初のパラメータで指定したフィルタを、2 番めのパラメータで指定した場所に移動します。2 番めのパラメータがキーワード `last` である場合、フィルタはフィルタ リストの最後に移動されます。複数のフィルタを移動する場合、それらのフィルタの相対的な順序は変わりません。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。
- シーケンス番号が現在のシーケンス番号の範囲を超えている。
- 移動してもシーケンスが変更されない。

メッセージ フィルタのアクティベーションとディアクティベーション

指定されるメッセージ フィルタは、*active* または *inactive* のいずれかであり、さらに *valid* または *invalid* のいずれかです。メッセージ フィルタは、*active* と *valid* の両方の状態である場合にのみ処理に使用されます。CLI を通じて、既存のフィルタを active から inactive に変更します（その後、再び戻します）。存在しない（または削除された）リスナーまたはインターフェイスを参照している場合、そのフィルタは invalid です。

（注） フィルタが inactive であるかどうかは、構文から判断できます。AsyncOS では、inactive であるフィルタのフィルタ名に続くコロンが、感嘆符に変更されます。フィルタを入力またはインポートするときにこの構文を使用すると、AsyncOS はフィルタを inactive としてマークします。

たとえば、次のように無害な「filterstatus」という名前のフィルタを入力します。`filter -> set` サブコマンドを使用して、このフィルタを inactive にします。フィルタの詳細が表示され、コロンが感嘆符に変わっている点に注目してください（以下の例で、太字で示されています）。

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new


Enter filter script.  Enter '.' on its own line to end.

filterstatus: if true{skip_filters();}

.

1 filters added.


Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.
```

```
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name
  1   Y      Y   filterstatus

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> set

Enter the filter name, number, or range:
[all]> all

Enter the attribute to set:
[active]> inactive

1 filters updated.
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> detail

Enter the filter name, number, or range:
[]> all



Num Active Valid Name
  1   N      Y   filterstatus
filterstatus! if (true) {
 skip_filters();
              }



Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
```

```
- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

メッセージ フィルタのアクティベーションまたはディアクティベーション

```
set [seqnum|filtname|range] active|inactive
```

指定したフィルタを指定した状態に設定します。状態のルールは次のとおりです。

- active：選択したフィルタの状態を active に設定します。
- inactive：選択したフィルタの状態を inactive に設定します。

次の条件ではエラーが発生します。

- 指定した *filtname* のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

（注） inactive であるフィルタは、構文からも判断できます。ラベル（フィルタ名）の後のコロンが、感嘆符（!）に変更されます。CLI から手動で入力された、またはインポートされたフィルタにこの構文が含まれる場合、自動的に inactive とマークされます。たとえば、`mailfrompm!` が、`mailfrompm:` の代わりに表示されます。

メッセージ フィルタのインポート

```
import filename
```

処理されるフィルタを含むファイルの名前です。このファイルは、アプライアンスの FTP/SCP ルート ディレクトリの configuration ディレクトリ内に存在する必要があります（`interfaceconfig` コマンドを使用してインターフェイスの FTP/SCP アクセスをイネーブルにしている場合）。ファイルは取り込まれて解析され、エラーが存在すれば報告されます。現在のフィルタ セット内に存在するすべてのフィルタは、インポートされたフィルタに置き換わります。詳細については、付録 B「アプライアンスへのアクセス」を参照してください。現在のフィルタ リストをエクスポートし（メッセージ フィルタのエクスポート (6-86 ページ)を参照）、そのファイルを編集してインポートすることを推奨します。

メッセージ フィルタをインポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- ファイルが存在しない。
- フィルタ名が一意ではない。

- フィルタに付けた *filtname* が予約語である。
- フィルタに構文エラーが発生している。
- インターフェイスなど、存在しないシステム リソースを参照するアクションを実行するフィルタ。

メッセージ フィルタのエクスポート

```
export filename [seqnum|filtname|range]
```

既存のフィルタ セットを、アプライアンスの FTP/SCP ルート ディレクトリにある configuration ディレクトリ内のファイルに所定の形式で出力します。詳細については、付録 B「アプライアンスへのアクセス」を参照してください。

メッセージ フィルタをエクスポートする場合、使用するエンコードを選択するよう求められます。

次の条件ではエラーが発生します。

- 指定した名前のフィルタが存在しない。
- 指定したシーケンス番号のフィルタが存在しない。

非 ASCII 文字セットの表示

このシステムでは、CLI で非 ASCII 文字が UTF-8 で表示されます。お使いのターミナル/ディスプレイが UTF-8 をサポートしていない場合、フィルタが正常に表示されません。

フィルタ内の非 ASCII 文字を管理する最も良い方法は、フィルタをテキスト ファイルで編集してから、そのテキスト ファイルをアプライアンスにインポートすることです（メッセージ フィルタのインポート（6-85 ページ）を参照）。

メッセージ フィルタ リストの表示

```
list [seqnum|filtname|range]
```

指定したフィルタの本文を出力せずに、概要を表形式で表示します。表示される情報は次のとおりです。

- フィルタ名
- フィルタ シーケンス番号
- フィルタの active/inactive 状態
- フィルタの valid/invalid 状態

次の条件ではエラーが発生します。

- 範囲の指定が不正である。

メッセージ フィルタの詳細の表示

```
detail [seqnum|filtname|range]
```

フィルタの本文や追加の状態情報など、指定したフィルタの情報をすべて表示します。

フィルタ ログ サブスクリプションの設定

logconfig

サブメニューを入力し、archive() アクションによって生成されたメールボックス ファイルのフィルタ ログ オプションを設定できます。これらのオプションは、通常の logconfig コマンドで使用されるオプションとよく似ていますが、ログを参照するフィルタを追加または削除することによってのみ、ログを作成または削除できます。

各フィルタ ログ サブスクリプションには次のデフォルト値が設定されています。この値は、logconfig サブコマンドを使用して変更できます。

- 取得方法:FTP Poll
- ファイル サイズ:10MB
- ファイルの最大数:10

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」を参照してください。

```
mail3.example.com> filters


Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> logconfig


Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll


Choose the operation you want to perform:
```

```
- EDIT - Modify a log setting.

[]> edit


Enter the number of the log you wish to edit.

[]> 1


Choose the method to retrieve the logs.

1. FTP Poll

2. FTP Push

3. SCP Push

[1]> 1


Please enter the filename for the log:

[joesmith.mbox]>


Please enter the maximum file size:

[10485760]>


Please enter the maximum number of files:

[10]>


Currently configured logs:

1. "joesmith" Type: "Filter Logs" Retrieval: FTP Poll


Enter "EDIT" to modify or press Enter to go back.

[]>
```

スキャン パラメータの変更

scanconfig コマンドは、スキャンでスキップするタイプなど、本文と添付ファイルのスキャン動作を制御します。

（注）　zip などの圧縮ファイルに含まれる MIME タイプをスキャンする場合、スキャン リストに「compressed」または「zip」または「application/zip」リストを含める必要があります。

scanconfig の使用

次の例では、scanconfig コマンドで次のパラメータを設定します。

- video/*、audio/*、image/* の MIME タイプでは、コンテンツはスキャンされません。
- ネストされた（再帰的な）アーカイブ添付ファイルは、最大 10 レベルまでスキャンされます。（デフォルトは 5 レベル）。
- スキャンされる添付ファイルの最大サイズは、25 MB です。これより大きいファイルはすべてスキップされます。（デフォルトは 5 MB）。
- 添付ファイルのメタデータ スキャンをイネーブルにします。スキャン エンジンが添付ファイルをスキャンするとき、メタデータを正規表現でスキャンします。これがデフォルトの設定です。
- 添付ファイルのスキャンのタイムアウトは、60 秒に設定されます。デフォルトは 30 秒です。
- スキャンされなかった添付ファイルは、検索パターンに一致しないと見なされます。（デフォルトの動作）。
- メッセージの application/(x-)pkcs7-mime（符号化署名）部分は、multipart/signed（クリア署名）に変換され、メッセージのコンテンツが処理されます。デフォルトでは、符号化署名されたメッセージは変換されません。

（注）　[assume the attachment matches the search pattern] を「Y」に設定すると、スキャンできないメッセージはメッセージ フィルタ ルールによって true と評価されます。これにより、辞書に一致しないメッセージの検疫など、予想外の動作が発生することがあります。このようなメッセージは、コンテンツが正しくスキャンできないという理由で検疫されていました。

```
mail3.example.com> scanconfig


There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.
```

```
- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> setup


1. Scan only attachments with MIME types or fingerprints in the list.

2. Skip attachments with MIME types or fingerprints in the list.

Choose one:

[2]> 2


Enter the maximum depth of attachment recursion to scan:

[5]> 10


Enter the maximum size of attachment to scan:

[5242880]> 10m


Do you want to scan attachment metadata? [Y]> Y


Enter the attachment scanning timeout (in seconds):

[30]> 60


If a message has attachments that were not scanned for any reason (e.g. because of size,
depth limits, or scanning timeout), assume the attachment matches the search pattern?
[N]>


If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:

1. Deliver
```

```
2. Bounce

3. Drop

[1]> 1


Configure encoding to use when none is specified for plain body text or anything with
MIME type plain/text or plain/html.

1. US-ASCII

2. Unicode (UTF-8)

3. Unicode (UTF-16)

4. Western European/Latin-1 (ISO 8859-1)

5. Western European/Latin-1 (Windows CP1252)

6. Traditional Chinese (Big 5)

7. Simplified Chinese (GB 2312)

8. Simplified Chinese (HZ GB 2312)

9. Korean (ISO 2022-KR)

10. Korean (KS-C-5601/EUC-KR)

11. Japanese (Shift-JIS (X0123))

12. Japanese (ISO-2022-JP)

13. Japanese (EUC)

[1]>


Scan behavior changed.


There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.
```

```
- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> SMIME


Do you want to convert opaque-signed messages to clear-signed? This will provide the
clear text content for various blades to process. [N]> Y



There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:

- NEW - Add a new entry.

- DELETE - Remove an entry.

- SETUP - Configure scanning behavior.

- IMPORT - Load mappings from a file.

- EXPORT - Save mappings to a file.

- PRINT - Display the list.

- CLEAR - Remove all entries.

- SMIME - Configure S/MIME unpacking.

[]> print


1. Fingerprint   Image

2. Fingerprint   Media

3. MIME Type     audio/*

4. MIME Type     image/*
```

```
5. MIME Type     video/*



There are currently 5 attachment type mappings configured to be SKIPPED.


Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[]>
```

メッセージのエンコードの変更

localeconfig コマンドを使用して、メッセージ処理中のメッセージのヘッダーおよびフッターのエンコードの変更に関する AsyncOS の動作を設定できます。

```
example.com> localeconfig


Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Only try encoding from
message body


Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup
```

```
If a header is modified, encode the new header in the same encoding as

the message body? (Some MUAs incorrectly handle headers encoded in a

different encoding than the body. However, encoding a modified header

in the same encoding as the message body may cause certain characters in the modified
header to be lost.) [Y]>


If a non-ASCII header is not properly tagged with a character set and

is being used or modified, impose the encoding of the body on the

header during processing and final representation of the message?

(Many MUAs create non-RFC-compliant headers that are then handled in

an undefined way. Some MUAs handle headers encoded in character sets

that differ from that of the main body in an incorrect way. Imposing the encoding of the
body on the header may encode

the header more precisely. This will be used to interpret the content of headers for
processing, it will not modify or rewrite the header

 unless that is done explicitly as part of the processing.) [Y]>


Footers or headings are added in-line with the message body whenever

possible. However, if the footer or heading is encoded differently

than the message body,and if imposing a single encoding will cause

loss of characters, it will be added as an attachment. The system will

always try to use the message body's encoding for the footer or

heading. If that fails, and if the message body's encoding is US-

ASCII, the system can try to edit the message body to use the footer's

or heading's encoding. Should the system try to impose the footer's

or headings's encoding on the message body? [N]> y


Behavior when modifying headers: Use encoding of message body

Behavior for untagged non-ASCII headers: Impose encoding of message
```

```
body. Behavior for mismatched footer or heading encoding: Try both

body and footer or heading encodings



Choose the operation you want to perform:

- SETUP - Configure multi-lingual settings.
```

最初のプロンプトは、ヘッダーが（たとえばフィルタによって）変更されていた場合、メッセージ ヘッダーのエンコードをメッセージ本文に一致するように変更するかどうかを指定します。

2 番めのプロンプトは、ヘッダーの文字セットが適切にタグで指定されていない場合、ヘッダーに対してメッセージ本文のエンコードを強制する必要があるかどうかを制御します。

3 番めのプロンプトは、免責事項のスタンプ（および複数のエンコード）がメッセージ本文でどのように機能するかを制御するために使用されます。詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Text Resources」章の「Disclaimer Stamping and Multiple Encodings」を参照してください。

サンプル メッセージ フィルタの作成

次の例では、`filter` コマンドを使用して新しいフィルタを 3 つ作成します。

- 最初のフィルタの名前は、**big_messages** です。これは `body-size` ルールを使用して、10 MB より大きいメッセージをドロップします。
- 2 番めのフィルタの名前は、**no_mp3s** です。これは `attachment-filename` ルールを使用して、`.mp3` ファイル拡張子が付いた添付ファイルを含むメッセージをドロップします。
- 3 番めのフィルタの名前は、**mailfrompm** です。これは `mail-from` ルールを使用して、`postmaster@example.com` からのメールをすべて調べ、`administrator@example.com` のブラインド カーボン コピーを作成します。

`filter -> list` サブコマンドを使用し、フィルタのリストを表示して、フィルタがアクティブで有効であることを確認します。次に、`move` サブコマンドを使用して、最初と最後のフィルタの位置を入れ替えます。最後に、変更を確定してフィルタを有効にします。

```
mail3.example.com> filters



Choose the operation you want to perform:

- NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new
```

```
Enter filter script.  Enter '.' on its own line to end.
big_messages:
    if (body-size >= 10M) {
       drop();
    }
.
1 filters added.


Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new


Enter filter script.  Enter '.' on its own line to end.
no_mp3s:
    if (attachment-filename == '(?i)\\.mp3$') {
        drop();
     }
.
1 filters added.
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new

Enter filter script.  Enter '.' on its own line to end.
mailfrompm:
    if (mail-from == "^postmaster$")
     { bcc ("administrator@example.com");}
.
1 filters added.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
```

```
- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> list


Num Active Valid Name

  1   Y      Y   big_messages

  2   Y      Y   no_mp3s

  3   Y      Y   mailfrompm


Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]> move


Enter the filter name, number, or range to move:

[]> 1


Enter the target filter position number or name:

[]> last


1 filters moved.
```

```
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list


Num Active Valid Name
  1   Y      Y   no_mp3s
  2   Y      Y   mailfrompm
  3   Y      Y   big_messages
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
```

```
[]> move

Enter the filter name, number, or range to move:
[]> 2

Enter the target filter position number or name:
[]> 1

1 filters moved.

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

Num Active Valid Name
  1   Y      Y   mailfrompm
  2   Y      Y   no_mp3s
  3   Y      Y   big_messages

Choose the operation you want to perform:
```

```
- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>


mail3.example.com> commit


Please enter some comments describing your changes:

[]> entered and enabled 3 filters: no_mp3s, mailfrompm, big_messages
```

メッセージ フィルタの例

この項では、実際のフィルタの例を示し、各フィルタについて簡単に説明します。

オープンリレー防止フィルタ

このフィルタは、次のように、%、余分な @、および ! 文字が電子メール アドレスに含まれるメッセージをバウンスします。

- user%otherdomain@validdomain
- user@otherdomain@validdomain:
- domain!user@validdomain

```
sourceRouted:

if (rcpt-to == "(%|@|!)(.*)@") {

  bounce();

}
```

Cisco IronPort アプライアンスは、従来の Sendmail/Qmail システムを活用するためによく使用される、このようなサード パーティ製のリレー ハックの影響を受けません。これらの記号の多く（% など）は正当な電子メール アドレスの一部である可能性があるため、Cisco IronPort アプライアンスはこれらを有効なアドレスとして受け入れ、設定済みの受信者リストと照合し、次の内部サーバに渡します。Cisco IronPort アプライアンスは、これらのメッセージを外部にリレーしません。

このようなフィルタは、このタイプのメッセージをリレーできるように誤って設定されたオープンソース MTA を使用しているユーザを保護するために所定の場所に設定されます。

（注）　このようなタイプのアドレスを処理するように、リスナーを設定することもできます。詳細については、SMTP アドレス解析オプション（1-8 ページ）を参照してください。

ポリシー適用フィルタ

件名に基づき通知するフィルタ

このフィルタは、件名に特定の用語が含まれているかどうかに基づいて通知を送信します。

```
search_for_sensitive_content:

if (Subject == "(?i)plaintiff|lawsuit|judge" ) {

    notify ("admin@company.com");

}
```

競合他社に送信されたメールの BCC およびスキャン

このフィルタは、競合他社に送信されたメッセージをスキャンし、ブラインド コピーを作成します。辞書と header-dictionary-match() ルールを使用して、柔軟性の高い競合他社のリストを指定できます（辞書ルール（6-35 ページ）を参照）。

```
competitorFilter:

if (rcpt-to == '@competitor1.com|@competitor2.com') {

    bcc-scan('legal@example.com');

}
```

特定のユーザをブロックするフィルタ

このフィルタを使用すると、特定のアドレスからの電子メールをブロックします。

```
block_harrasing_user:

if (mail-from == "ex-employee@hotmail\\.com") {

    notify ("admin@company.com");
```

```
    drop ();

}
```

メッセージのアーカイブおよびドロップ フィルタ

ファイルタイプが一致するメッセージのみをログ記録およびドロップします。

```
drop_attachments:

if (mail-from != "user@example.com") AND (attachment-filename ==

'(?i)\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$')

{

  archive("Drop_Attachments");

  insert-header("X-Filter", "Dropped by: $FilterName MID: $MID");
drop-attachments-by-name("\\.(asp|bas|bat|cmd|cpl|exe|hta|ins|isp|js)$");

}
```

大きい「To:」ヘッダーのフィルタ

「To」ヘッダーが非常に大きいメッセージを検索します。

`archive()` 行を使用して適切なアクションを検証し、drop() をイネーブルまたはディセーブルにして安全性を高めます。

```
toTooBig:

if(header('To') == "^.{500,}") {

   archive('tooTooBigdropped');

   drop();

}
```

空白の「From:」フィルタ

空白の「From」ヘッダーを特定します。

このフィルタは、「from」アドレスが空白であるさまざまな形式に対応できます。

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND header("From") == "^$|<\\s*>") {

  drop ();

}
```

また、Envelope From が空欄のメッセージをドロップする場合は、次のフィルタを使用します。

```
blank_mail_from_stop:

if (recv-listener == "InboundMail" AND (mail-from == "^$|<\\s*>" OR header ("From") ==
"^$|<\\s*>"))

{

  drop ();

}
```

SRBS フィルタ

SenderBase レピュテーション フィルタ:

```
note_bad_reps:

if (reputation < -2)  {

  strip-header ('Subject');

  insert-header ('Subject', '***BadRep $Reputation *** $Subject');

}
```

SRBS 変更フィルタ

特定のドメインの SenderBase Reputation Score（SBRS; SenderBase レピュテーション スコア）しきい値を変更します。

```
mod_sbrs:

if ( (rcpt-count == 1) AND (rcpt-to == "@domain\\.com$") AND (reputation < -2) ) {

    drop ();

}
```

ファイル名の正規表現フィルタ

このフィルタは、メッセージ本文のサイズの範囲を指定し、正規表現に一致する添付ファイルを検索します（このパターンに一致するファイル名は、「readme.zip」、「readme.exe」、「attach.exe」、など）。

```
filename_filter:

if ((body-size >= 9k) AND (body-size <= 20k)) {

   if (body-contains ("(?i)(readme|attach|information)\\.(zip|exe)$")) {
```

```
      drop ();

   }

}
```

ヘッダー内の SenderBase レピュテーション スコアの表示フィルタ

ヘッダーのログが記録されるので、メール ログで表示できます（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」を参照）。

```
Check_SBRS:

if (true) {

  insert-header('X-SBRS', '$Reputation');

}
```

ポリシーのヘッダーへの挿入フィルタ

どのメール フロー ポリシーが接続を受け入れたかを示します。

```
Policy_Tracker:

if (true) {

  insert-header ('X-HAT', 'Sender Group $Group, Policy $Policy applied.');

}
```

多数の受信者のバウンス フィルタ

3 つ以上の固有ドメインから 50 人を超える受信者が指定されている発信電子メール メッセージをすべてバウンスします。

```
bounce_high_rcpt_count:

if ( (rcpt-count > 49) AND (rcpt-to != "@example\\.com$") ) {

  bounce-profile ("too_many_rcpt_bounce"); bounce ();

}
```

ルーティングおよびドメイン スプーフィング

仮想ゲートウェイ フィルタの使用

仮想ゲートウェイを使用してトラフィックを区分します。システムに 2 つのインターフェイス「public1」と「public2」が存在するとします。デフォルトの配信インターフェイスは「public1」です。これにより、発信トラフィックはすべて 2 番めのインターフェイスを介すように強制されます。バウンスおよびその他同様のタイプのメールはフィルタを通過しないため、そのようなメールは public1 から配信されます。

```
virtual_gateways:

if (recv-listener == "OutboundMail") {

    alt-src-host ("public2");

}
```

配信とインジェクションのリスナーが同じフィルタ

配信と受信に同じリスナーを使用します。このフィルタでは、パブリック リスナー「listener1」で受信したメッセージを、インターフェイス「listener1」から送信できます（設定したパブリック インジェクタごとに、固有のフィルタをセットアップする必要があります）。

```
same_listener:

if (recv-inj == 'listener1') {

  alt-src-host('listener1');

}
```

単一インジェクタ フィルタ

単一のリスナーでフィルタを機能させます。たとえば、システム全体で実行するのではなく、メッセージ フィルタを処理する専用のリスナーを指定します。

```
textfilter-new:

if (recv-inj == 'inbound' and body-contains("some spammy message")) {

  alt-rcpt-to ("spam.quarantine@spam.example.com");

}
```

スプーフィング ドメインのドロップ フィルタ（単一のリスナー）

スプーフィング ドメイン（内部のアドレスからであると偽り、単一のリスナーで機能する）が使用されている電子メールをドロップします。以下の IP アドレスは、架空のドメイン mycompany.com を表しています。

```
DomainSpoofed:

if (mail-from == "mycompany\\.com$") {

  if ((remote-ip != "1.2.") AND (remote-ip != "3.4.")) {

    drop();

  }

}
```

スプーフィング ドメインのドロップ フィルタ（複数のリスナー）

前述と同じですが、複数のリスナーを使用して動作します。

```
domain_spoof:

if ((recv-listener == "Inbound") and (mail-from == "@mycompany\\.com")) {

archive('domain_spoof');

drop ();

}
```

別のスプーフィング ドメインのドロップ フィルタ

概要:ドメイン スプーフィング対策フィルタ:

```
reject_domain_spoof:

if (recv-listener == "MailListener") {

  insert-header("X-Group", "$Group");

  if ((mail-from == "@test\\.mycompany\\.com") AND (header("X-Group") != "RELAYLIST")) {

    notify("me@here.com");

    drop();

    strip-header("X-Group");

}
```

ルーピングの検出フィルタ

このフィルタを使用して、メール ループを発生させている要因を検出、停止、および判断します。このフィルタは、Exchange サーバまたはそれ以外の場所で発生している構成の問題を判断するために役立ちます。

```
External_Loop_Count:

if (header("X-ExtLoop1")) {

  if (header("X-ExtLoopCount2")) {

    if (header("X-ExtLoopCount3")) {

      if (header("X-ExtLoopCount4")) {

        if (header("X-ExtLoopCount5")) {

          if (header("X-ExtLoopCount6")) {

            if (header("X-ExtLoopCount7")) {

              if (header("X-ExtLoopCount8")) {

                if (header("X-ExtLoopCount9")) {

                   notify ('joe@example.com');

                   drop();

                }

              else {insert-header("X-ExtLoopCount9", "from
                   $RemoteIP");}}

            else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}

          else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}

        else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}

      else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}

    else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}

  else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}

else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}

else {insert-header("X-ExtLoop1", "1"); }
```

（注） デフォルトでは、AsyncOS は自動的にメールのループを検出し、100 回ループしたメッセージをドロップします。

CHAPTER 7

高度なネットワーク構成

この章では、NIC ペアリング、VLAN、Direct Server Return など、一般に etherconfig コマンドを使って利用できる高度なネットワーク構成について説明します。この章は、次の項で構成されています。

イーサネット インターフェイスのメディア設定

イーサネット インターフェイスのメディア設定にアクセスするには、etherconfig コマンドを使用します。個々のイーサネット インターフェイスが現在の設定と共に一覧表示されます。インターフェイスを選択すると、可能なメディア設定が表示されます。例については、メディア設定の編集例（7-2 ページ）を参照してください。

etherconfig を使ったイーサネット インターフェイスのメディア設定の編集

etherconfig コマンドを使って、イーサネット インターフェイスのデュプレックス設定（全二重/半二重）や速度（10/100/1000 Mbps）を設定できます。デフォルトでは、インターフェイスが自動的にメディア設定を選択しますが、場合によってはこの設定を上書きする必要があります。

（注） 『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「セットアップとインストール」の章の説明に従って GUI のシステム設定ウィザード（またはコマンドライン インターフェイスの systemsetup コマンド）を実行し、変更を確定していれば、アプライアンス上でデフォルトのイーサネット インターフェイス設定が構成されているはずです。

（注） 一部の Cisco IronPort C3x、C6x、X10x アプライアンスには、光ファイバ ネットワーク インターフェイス オプションが装備されています。その場合は、各アプライアンス上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。これらのギガビット光ファイバ インターフェイスは、異種混在構成で銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。ネットワーク インターフェイス カードのペアリング/チーミング（7-3 ページ）を参照してください。

メディア設定の編集例

```
mail3.example.com> etherconfig


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]> media


Ethernet interfaces:

1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d

2. Data 2 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e

3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da


Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]> edit


Enter the name or number of the ethernet interface you wish to edit.

[]> 2


Please choose the Ethernet media options for the Data 2 interface.

1. Autoselect

2. 10baseT/UTP half-duplex

3. 10baseT/UTP full-duplex

4. 100baseTX half-duplex

5. 100baseTX full-duplex

6. 1000baseTX half-duplex
```

```
7. 1000baseTX full-duplex

[1]> 5


Ethernet interfaces:

1. Data 1 (Autoselect: <100baseTX full-duplex>) 00:06:5b:f3:ba:6d

2. Data 2 (100baseTX full-duplex: <100baseTX full-duplex>) 00:06:5b:f3:ba:6e

3. Management (Autoselect: <100baseTX full-duplex>) 00:02:b3:c7:a2:da


Choose the operation you want to perform:

- EDIT - Edit an ethernet interface.

[]>


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]>
```

ネットワーク インターフェイス カードのペアリング/チーミング

NIC ペアリングで 2 つの物理データ ポートを組み合わせることにより、NIC からアップストリームのイーサネット ポートへのデータ パスに障害が発生した場合に、バックアップ イーサネット インターフェイスを提供できます。ペアリングでは、基本的に各イーサネット インターフェイスをプライマリ インターフェイスおよびバックアップ インターフェイスとして設定します。プライマリ インターフェイスに障害が発生した場合(つまり、NIC とアップストリーム ノード間のキャリアが途切れた場合)は、バックアップ インターフェイスがアクティブになり、アラートが送信されます。Cisco IronPort のマニュアルでは、「NIC ペアリング」と「NIC チーミング」は同義語です。

十分な数のデータ ポートがあれば、複数の NIC ペアを作成できます。ペアを作成するときは、任意のデータ ポートを組み合わせることができます。次に例を示します。

- Data 1 と Data 2
- Data 3 と Data 4

- Data 2 と Data 3
- など

C1x アプライアンスと M シリーズ アプライアンスでは、NIC ペアリングを使用できません。一部の C3x、C6x、X10x アプライアンスには、光ファイバ ネットワーク インターフェイス オプションが装備されています。その場合は、各アプライアンス上の使用可能なインターフェイスのリストに 2 つの追加イーサネット インターフェイス（Data 3 と Data 4）が表示されます。これらのギガビット光ファイバ インターフェイスは、異種混在構成で銅線（Data 1、Data 2、および Management）インターフェイスとペアにすることができます。

NIC ペアリングと VLAN

VLAN（仮想ローカル エリア ネットワーク（VLAN）（7-8 ページ）を参照）は、プライマリ インターフェイスにのみ設定できます。

NIC ペアの名前

NIC ペアを作成するときは、そのペアを参照するときに使用する名前を指定する必要があります。バージョン 4.5 よりも前の AsyncOS で作成した NIC ペアには、アップグレード後、自動的に「Pair 1」というデフォルト名が指定されます。

NIC ペアリングに関して生成されたアラートは、特定の NIC ペアを名前で参照します。

NIC ペアリング/チーミングの設定とテスト

イーサネットのメディア設定を確認したら、`etherconfig` コマンドを使って NIC ペアリングを設定します。ペアを参照するときに使用する名前を入力するように求められます。

アクティブなインターフェイスを切り替えるには、`failover` サブコマンドを使用します。プライマリ NIC がオンライン状態に戻っても、自動的にプライマリ NIC には切り替わりません。その場合は、（`failover` コマンドを使用して）明示的にプライマリ NIC に切り替えるか、バックアップ NIC に障害が発生するまで、バックアップ インターフェイスがアクティブな状態を維持します。NIC ペアリングに対する failover サブコマンドの使用（7-6 ページ）を参照してください。

NIC ペアを削除するには、`delete` サブコマンドを使用します。

NIC ペアリングを設定するときは、`failover` を除くすべての設定変更で確定が必要であることに注意してください。`failover` コマンドは、NIC ペアリングの設定を確定した後 15 秒ごとに行われるポーリングの次の間隔で強制的にフェールオーバーを実行します。

NIC ペアリングと既存のリスナー

リスナーが割り当てられたインターフェイスで NIC ペアリングをイネーブルにすると、バックアップ インターフェイスに割り当てられた全リスナーの削除、再割り当て、ディセーブル化のいずれかを選択するように求められます。

etherconfig コマンドを使った NIC ペアリングのイネーブル化

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]> pairing

Paired interfaces:

Choose the operation you want to perform:

- NEW - Create a new pairing.

[]> new

Please enter a name for this pair (Ex: "Pair 1"):

[]> Pair 1

Warning: The backup (Data 2) for the NIC Pair is currently configured with one or more
IP addresses.  If you continue, the Data 2 interface will be deleted.

Do you want to continue? [N]> y

The interface you are deleting is currently used by listener "OutgoingMail".

What would you like to do?

1. Delete: Remove the listener and all its settings.

2. Change: Choose a new interface.

3. Ignore: Leave the listener configured for interface "Data 2" (the listener will be
disabled until you add a new interface named "Data 2" or edit the listener's settings).

[1]>
```

```
Injector OutgoingMail deleted for mail3.example.com.

Interface Data 2 deleted.

Paired interfaces:

1. Pair 1:

        Primary (Data 1) Active, Link is up

        Backup (Data 2) Standby, Link is up


Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]>


mail3.example.com> commit
```

（注）　NIC ペアを作成したら、必ずテストしてください。詳細については、NIC ペアリングの確認（7-8 ページ）を参照してください。

NIC ペアリングに対する failover サブコマンドの使用

この例では、手動のフェールオーバーを実行し、Data 2 インターフェイスを強制的にプライマリインターフェイスにします。CLI で変更を確認するには、status サブコマンドを実行する必要があります。

```
mail3.example.com> etherconfig


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.
```

```
[]> pairing


Paired interfaces:

1. Pair 1:

        Primary (Data 1) Active, Link is up

        Backup (Data 2) Standby, Link is up


Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]> failover


Paired interfaces:

1. Pair 1:

        Primary (Data 1) Active, Link is up

        Backup (Data 2) Standby, Link is up


Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]> status


Paired interfaces:

1. Pair 1:

        Primary (Data 1) Standby, Link is up

        Backup (Data 2) Active, Link is up
```

```
Choose the operation you want to perform:

- FAILOVER - Manually failover to other port.

- DELETE - Delete a pairing.

- STATUS - Refresh status.

[]>


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]>
```

NIC ペアリングの確認

NIC ペアリングが正常に機能していることを確認する必要があります。次の手順を実行します。

ステップ 1　CLI で ping コマンドを使って、ペアになっているインターフェイスをテストします。NIC ペアと同じサブネット上に存在し、独立したソースによって ping が返されたことが確認されている IP アドレスに対して、次のように ping を実行します。

```
mail3.example.com> ping x.x.x.x
```

ステップ 2　failover コマンドを実行します（`etherconfig -> pairing -> failover`）。15 秒間待ちます。

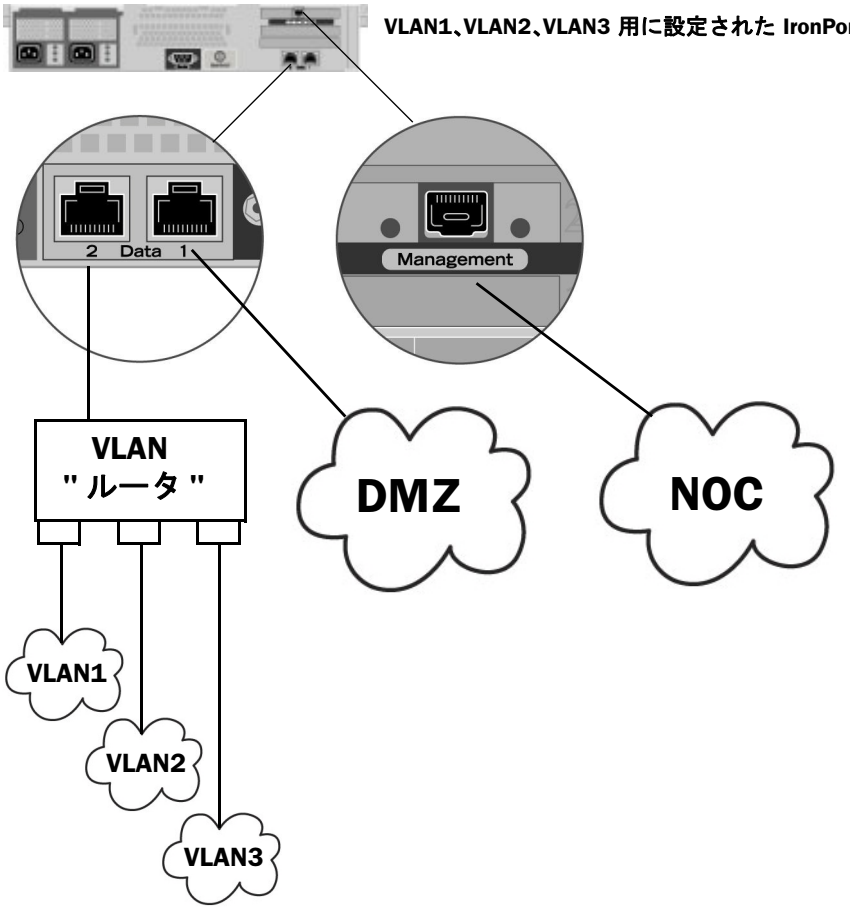
ステップ 3　バックアップ NIC がアクティブなインターフェイスになったら、再度 CLI の ping コマンドを使って、ペアになっているインターフェイスをテストします。

ステップ 4　最後に、再度 failover を実行して NIC ペアをデフォルトの（プライマリ インターフェイスがアクティブな）状態に戻します。

仮想ローカル エリア ネットワーク（VLAN）

VLAN は物理データ ポートにバインドされた仮想ローカル エリア ネットワークです。VLAN を設定することにより、Cisco IronPort アプライアンスが接続できるネットワークの数を、装備されている物理的なインターフェイスの数よりも増やすことができます。たとえば、Cisco IronPort C6x アプライアンスには Data 1、Data 2、および管理の 3 つのインターフェイスがあります。VLAN を使って、既存のリスナーに対応する別個の「ポート」上に追加のネットワークを定義できます。（詳細については、付録 B「アプライアンスへのアクセス」を参照してください）。任意の物理ネットワーク ポート上に複数の VLAN を設定できます。図 7-1 に、Data 2 インターフェイスに複数の VLAN を設定する例を示します。

図 7-1　VLAN を使用したアプライアンス上の使用可能なネットワーク数の増加



VLAN を使ってネットワークを分割することにより、セキュリティを向上させたり、管理作業を軽減したり、帯域幅を拡大したりできます。VLAN は、「VLAN DDDD」という形式の名前を持つ動的な「データ ポート」として表示されます。「DDDD」は最大 4 桁の ID です（たとえば、VLAN 2、VLAN 4094 など）。AsyncOS は、最大 30 の VLAN をサポートします。同じ Cisco IronPort アプライアンス上で重複する VLAN ID は設定できません。

VLAN と物理ポート

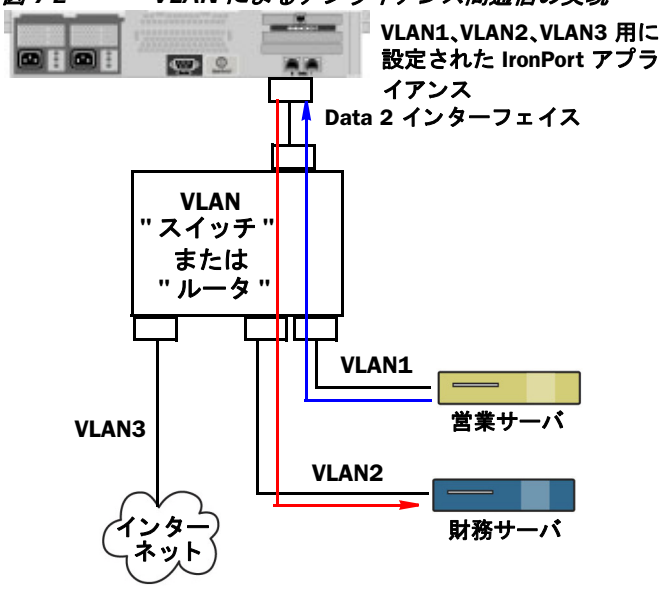
物理ポートは、VLAN に配置するために IP アドレスを設定する必要がありません。VLAN を作成した物理ポートに VLAN 以外のトラフィックを受信する IP アドレスを設定できるため、VLAN のトラフィックと VLAN 以外のトラフィックの両方を同じインターフェイスで受信できます。

VLAN は、一部のCisco IronPort X10x、C3x、および C6x アプライアンスで使用可能な光ファイバ データ ポートを含むすべての「Data」ポートと「Management」ポート上に作成できます。

VLAN は、NIC ペアリング（ペアになっている NIC で使用可能）や Direct Server Return（DSR）と併用できます。

図 7-2 は、VLAN の制限事項のために直接通信できない 2 台のメール サーバが Cisco IronPort アプライアンス経由でどのようにメールを送信するかを示す使用例です。青い線は、営業ネットワーク（VLAN1）からアプライアンスに送信されたメールを示しています。アプライアンスはこのメールを通常どおりに処理し、配信時に VLAN の宛先情報を含むタグをパケットに追加します（赤い線）。

図 7-2　VLAN によるアプライアンス間通信の実現



VLAN の管理

VLAN の作成、編集、および削除を行うには、`etherconfig` コマンドを使用します。作成した VLAN は、[ネットワーク（Network）] > [インターフェイス（Interfaces）] ページまたは CLI の `interfaceconfig` コマンドを使って設定できます。すべての変更を保存することを忘れないでください。

etherconfig コマンドによる新しい VLAN の作成

この例では、Data 1 ポート上に 2 つの VLAN（VLAN 31 と VLAN 34）を作成します。

```
mail3.example.com> etherconfig

Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]> vlan


VLAN interfaces:


Choose the operation you want to perform:
```

```
- NEW - Create a new VLAN.

[]> new


VLAN ID for the interface (Ex: "34"):

[]> 34


Enter the name or number of the ethernet interface you wish bind to:

1. Data 1

2. Data 2

3. Management

[1]> 1


VLAN interfaces:

1. VLAN   34 (Data 1)


Choose the operation you want to perform:

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.

- DELETE - Delete a VLAN.

[]> new


VLAN ID for the interface (Ex: "34"):

[]> 31


Enter the name or number of the ethernet interface you wish bind to:

1. Data 1

2. Data 2

3. Management

[1]> 1
```

```
VLAN interfaces:

1. VLAN   31 (Data 1)

2. VLAN   34 (Data 1)


Choose the operation you want to perform:

- NEW - Create a new VLAN.

- EDIT - Edit a VLAN.

- DELETE - Delete a VLAN.

[]>


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]>
```

interfaceconfig コマンドによる VLAN 上の IP インターフェイスの作成

この例では、VLAN 31 イーサネット インターフェイス上に新しい IP インターフェイスを作成します。

（注） インターフェイスに変更を加えると、アプライアンスとの接続が閉じることがあります。

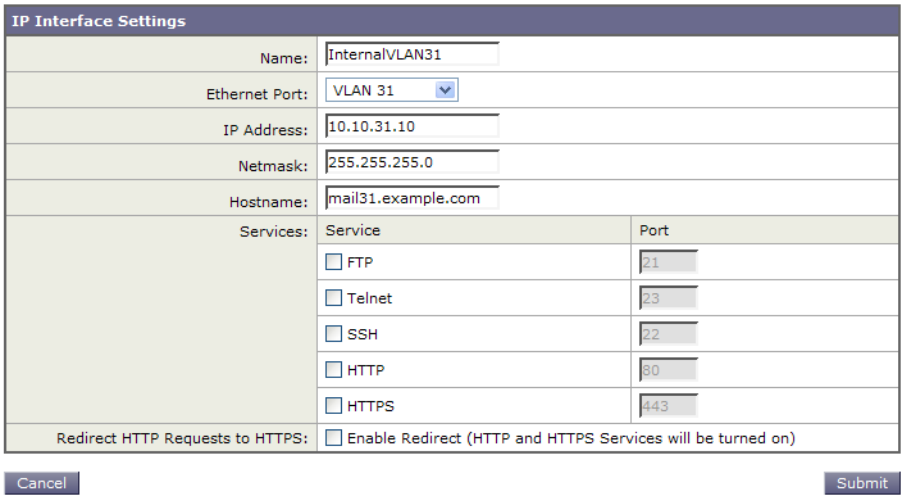
```
mail3.example.com> interfaceconfig


Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. Management (10.10.0.10/24: example.com)


Choose the operation you want to perform:
```

```
- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]> new


Please enter a name for this IP interface (Ex: "InternalNet"):

[]> InternalVLAN31


Would you like to configure an IPv4 address for this interface (y/n)? [Y]>


IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.31.10


Netmask (Ex: "255.255.255.0" or "0xffffff00"):
[255.255.255.0]>


Would you like to configure an IPv6 address for this interface (y/n)? [N]>


Ethernet interface:

1. Data 1

2. Data 2

3. Management

4. VLAN   31

5. VLAN   34

[1]> 4


Hostname:

[]> mail31.example.com
```

```
Do you want to enable Telnet on this interface? [N]>

Do you want to enable SSH on this interface? [N]>

Do you want to enable FTP on this interface? [N]>

Do you want to enable HTTP on this interface? [N]>

Do you want to enable HTTPS on this interface? [N]>



Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalVLAN31 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]>

mail3.example.com> commit
```

[ネットワーク（Network）] > [リスナー（Listeners）] ページを使って VLAN を設定することもできます。

図 7-3　GUI で新しい IP インターフェイスを作成するときに VLAN を使用する



Direct Server Return

Direct Server Return（DSR）は、同じ Virtual IP（VIP; 仮想 IP）を共有する複数の Cisco IronPort アプライアンス間で負荷を分散するための軽量負荷分散メカニズムをサポートする機能です。

DSR は、Cisco IronPort アプライアンスの「ループバック」イーサネット インターフェイス上に作成された IP インターフェイスを介して実装されます。

（注）　Cisco IronPort アプライアンスの負荷分散の設定は、このマニュアルでは取り上げません。

Direct Server Return のイネーブル化

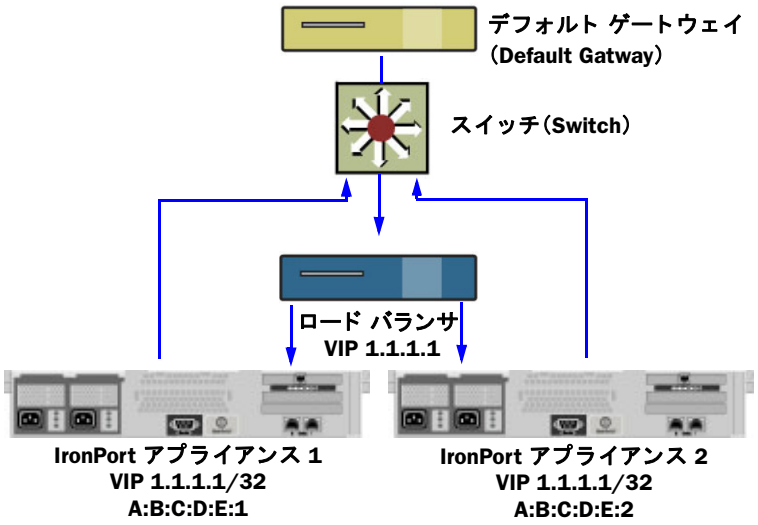
DSR をイネーブルにするには、参加している各アプライアンスの「ループバック」イーサネット インターフェイスをイネーブルにします。次に、CLI の `interfaceconfig` コマンドまたは GUI の [ネットワーク（Network）] > [インターフェイス（Interfaces）] ページを使ってループバック インターフェイス上に Virtual IP（VIP; 仮想 IP）を持つ IP インターフェイスを作成します。最後に、CLI の `listenerconfig` コマンドまたは GUI の [ネットワーク（Network）] > [リスナー（Listeners）] ページを使って新しい IP インターフェイス上にリスナーを作成します。すべての変更を保存することを忘れないでください。

（注）　ループバック インターフェイスを使用した場合、アプライアンスはそのインターフェイスの ARP 応答を発行しません。

DSR をイネーブルにするときは、次のルールが適用されます。

- すべてのシステムが同じ仮想 IP（VIP）アドレスを使用します。
- すべてのシステムがロード バランサと同じスイッチおよびサブネット上にある必要があります。

図 7-4　DSR を使用したスイッチ上の複数の Cisco IronPort アプライアンス間でのロード バランス



etherconfig コマンドによるループバック インターフェイスのイネーブル化

イネーブルになったループバック インターフェイスは、他のインターフェイス（Data 1 など）と同じように扱われます。

```
mail3.example.com> etherconfig


Choose the operation you want to perform:

- MEDIA - View and edit ethernet media settings.

- PAIRING - View and configure NIC Pairing.

- VLAN - View and configure VLANs.

- LOOPBACK - View and configure Loopback.

[]> loopback


Currently configured loopback interface:


Choose the operation you want to perform:

- ENABLE - Enable Loopback Interface.

[]> enable


Currently configured loopback interface:
```

```
1. Loopback


Choose the operation you want to perform:
- DISABLE - Disable Loopback Interface.
[]>


Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- PAIRING - View and configure NIC Pairing.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
[]>
```

interfaceconfig コマンドによるループバック上の IP インターフェイスの作成

ループバック インターフェイス上に IP インターフェイスを作成します。

```
mail3.example.com> interfaceconfig


Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)


Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> new
```

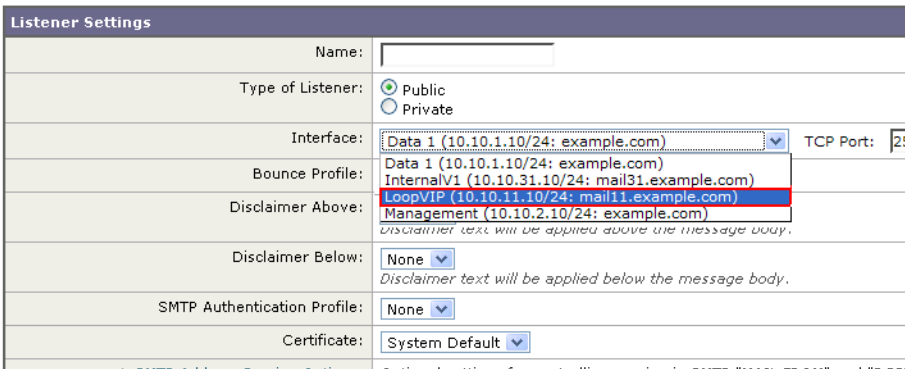
```
Please enter a name for this IP interface (Ex: "InternalNet"):

[]> LoopVIP


Would you like to configure an IPv4 address for this interface (y/n)? [Y]>


IPv4 Address (Ex: 10.10.10.10):

[]> 10.10.1.11


Netmask (Ex: "255.255.255.0" or "0xffffff00"):

[255.255.255.0]> 255.255.255.255


Would you like to configure an IPv6 address for this interface (y/n)? [N]>


Ethernet interface:

1. Data 1

2. Data 2

3. Loopback

4. Management

5. VLAN   31

6. VLAN   34

[1]> 3


Hostname:

[]> example.com


Do you want to enable Telnet on this interface? [N]>


Do you want to enable SSH on this interface? [N]>
```

```
Do you want to enable FTP on this interface? [N]>


Do you want to enable HTTP on this interface? [N]>


Do you want to enable HTTPS on this interface? [N]>


Currently configured interfaces:

1. Data 1 (10.10.1.10/24: example.com)

2. InternalV1 (10.10.31.10/24: mail31.example.com)

3. LoopVIP (10.10.1.11/24: example.com)

4. Management (10.10.0.10/24: example.com)


Choose the operation you want to perform:

- NEW - Create a new interface.

- EDIT - Modify an interface.

- GROUPS - Define interface groups.

- DELETE - Remove an interface.

[]>


mail3.example.com> commit
```

新しい IP インターフェイス上のリスナーの作成

GUI または CLI を使って新しい IP インターフェイス上にリスナーを作成します。たとえば、図 7-5 に示すように、新たに作成した IP インターフェイスを GUI の [リスナーを追加（Add Listener）] ページで選択できます。

図 7-5　新しいループバック IP インターフェイス上のリスナーの作成



CHAPTER 8

集中管理

Cisco IronPort の中央集中型管理機能（ライセンス キーを使って実行可能）を使用して複数のアプライアンスを同時に管理、設定することにより、管理に要する時間を短縮し、ネットワーク全体で設定の一貫性を確保することができます。複数のアプライアンスを管理するためにハードウェアを追加購入する必要はありません。中央集中型管理機能によって、ネットワーク内の信頼性、柔軟性、およびスケーラビリティが向上し、ローカル ポリシーを順守しながらグローバルな管理を行うことができます。

クラスタ とは、設定情報を共有する一連のマシンのことです。クラスタの内部では、マシン（Cisco IronPort アプライアンス）が *グループ* に分割されます。どのクラスタにも 1 つ以上のグループがあります。個々のマシンは、必ずいずれかのグループのメンバになります。管理者ユーザは、システムのさまざまな要素をクラスタ単位、グループ単位、またはマシン単位で設定できます。これにより、Cisco IronPort アプライアンスを、ネットワーク、地域、部署、または論理的な関係に基づいて分割できます。

クラスタは *ピアツーピア* アーキテクチャで実装されるため、クラスタ内にマスター/スレーブの関係は存在しません。どのマシンにログインしても、クラスタの制御と管理を行うことができます。（ただし、一部のコンフィギュレーション コマンドは制限されます。制限コマンド（8-15 ページ）を参照してください）。

ユーザ データベースはクラスタ内のすべてのマシン間で共有されます。つまり、ユーザのセットと管理者（および対応するパスワード）はクラスタ全体で 1 つしか存在しません。クラスタに参加するすべてのマシンは 1 つの管理者パスワードを共有します。これをクラスタの *管理パスワード* と呼びます。

この章は次のトピックで構成されています。

クラスタの要件

- クラスタ内の各マシンには、DNS で解決可能なホスト名が必要です。代わりに IP アドレスを使用することもできますが、両者を混在させることはできません。

  DNS とホスト名の解決（8-19 ページ）を参照してください。クラスタの通信は、通常、マシンの DNS ホスト名を使って開始されます。

- 1 つのクラスタは、全体として同じシリーズのマシンで構成されている必要があります（X シリーズと C シリーズには互換性があります）。

  たとえば、Cisco IronPort X1000、C60、C600、C30、C300、および C10 アプライアンスを同じクラスタに含めることはできますが、C60 と A60 アプライアンスを同じクラスタに含めることはできません。互換性のないアプライアンスを既存のクラスタに追加しようとすると、そのアプライアンスをクラスタに追加できない理由を示すエラー メッセージが表示されます。

- 1 つのクラスタは、全体として同じバージョンの AsyncOS を実行しているマシンで構成されている必要があります。

  クラスタのメンバをアップグレードする方法については、クラスタ内のマシンのアップグレード（8-13 ページ）を参照してください。

- 各マシンは、SSH（通常はポート 22）と Cluster Communication Service（CCS）の *いずれか* を使ってクラスタに参加できます。

  クラスタ通信（8-19 ページ）を参照してください。

- クラスタに参加したマシンは、SSH または CCS 経由で通信できます。使用するポートは設定可能です。SSH は通常ポート 22 上でイネーブルになっており、CCS はデフォルトでポート 2222 上でイネーブルになっていますが、どちらのサービスも別のポートに設定できます。

  アプライアンスに対して開く必要がある通常のファイアウォール ポートに加えて、クラスタ化されたマシンが CCS 経由で通信する場合は、各マシンが CCS ポート経由で相互に接続できる必要があります。クラスタ通信（8-19 ページ）を参照してください。

- マシンのクラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、CLI（コマンド ライン インタフェース）の `clusterconfig` コマンドを使用する必要があります。

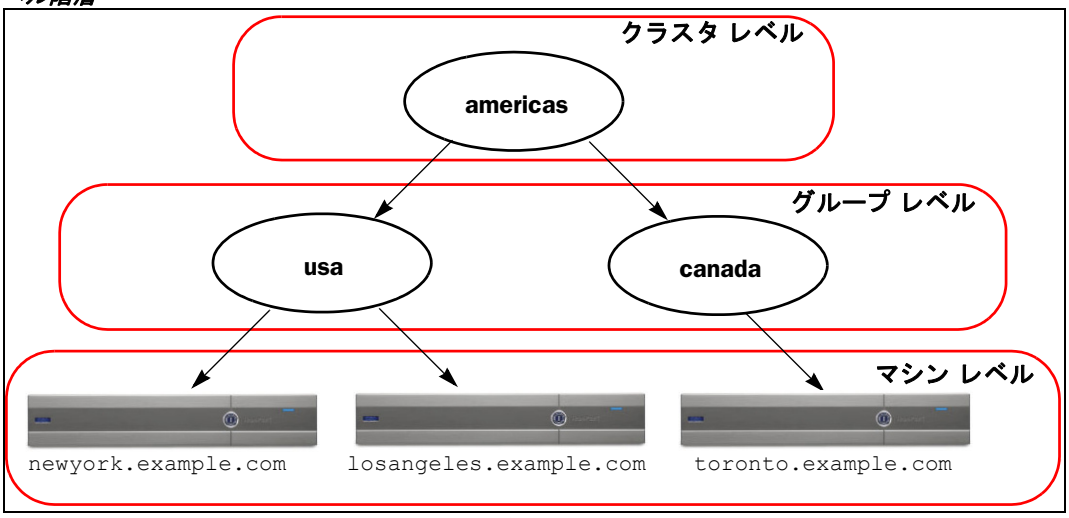
  クラスタを作成した後は、クラスタ以外の設定を GUI または CLI から管理できます。

  クラスタの作成とクラスタへの参加（8-4 ページ）およびGUI でのクラスタの管理（8-16 ページ）を参照してください。

クラスタの構成

クラスタでは、設定情報が 3 つのグループ（*レベル*）に分かれています。最上位レベルはクラスタの設定、中位レベルはグループの設定、最下位レベルはマシンごとの設定をそれぞれ表します。

図 8-1　クラスタのレベル階層



各レベルには、設定が可能なメンバが 1 つ以上存在します。これらを *モード* と呼びます。モードは特定のレベルに含まれる名前の付いたメンバを表します。たとえば、「usa」グループは図に示した 2 つのグループ モードの 1 つです。レベルは一般的な用語ですが、モードは具体的なものを示します。モードは常に名前で参照されます。図 8-1 に示したクラスタには 6 つのモードがあります。

設定は特定のレベルで設定されますが、それらは常に**特定のモードに対して**設定されます。すべてのモードに対する設定を 1 つのレベルで設定する必要はありません。クラスタ モードは特別なケースです。クラスタは 1 つしか存在しないため、クラスタ モードの設定はすべてクラスタ レベルで設定されると言えます。

通常、ほとんどの設定はクラスタ レベルで設定する必要があります。ただし、下位レベルで個別に設定された設定は上位レベルで設定された設定よりも *優先* されます。したがって、クラスタ モードの設定をグループ モードやマシン モードの設定で上書きできます。

たとえば、最初にクラスタ モードでグッド ネイバー テーブルを設定し、クラスタ内のすべてのマシンでその設定を使用するとします。次に、このテーブルをマシン モードでマシン `newyork` 用に設定します。この場合、クラスタ内の他のすべてのマシンは引き続きクラスタ レベルで定義されたグッド ネイバー テーブルを使用しますが、マシン `newyork` はクラスタの設定をマシン モードの個別の設定で上書きします。

特定のグループやマシン用にクラスタの設定を上書きする機能によって、非常に柔軟な設定が可能になります。ただし、多くの設定をマシン モードで個別に設定すると、クラスタの当初の目的である管理のしやすさが大きく損なわれます。

初期設定

ほとんどの機能については、新しいモードで設定を始めたときのデフォルトの初期設定は空です。設定が空であることとモードの設定が存在しないことは明確に区別されます。例として、1 つのグループと 1 台のマシンからなる非常に簡単なクラスタを考えます。LDAP クエリーがクラスタ レベルで設定されているとします。グループ レベルとマシン レベルでは何も設定されていません。

クラスタ	(ldap queries: a, b, c)
グループ	
マシン (Machine)	

ここで、グループに対して新しい LDAP クエリーの設定を作成したとします。その結果は次のようになります。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: None)
マシン (Machine)	

すると、クラスタ レベルの設定がグループ レベルの設定で上書きされますが、新しいグループ設定は初期状態では空です。グループ モードには、独自に設定された LDAP クエリーが実際には存在しません。このグループ内のマシンは、この「空の」LDAP クエリーをグループから継承します。

次に、このグループに次のような LDAP クエリーを追加します。

クラスタ	(ldap queries: a, b, c)
グループ	(ldap queries: d)
マシン (Machine)	

これで、クラスタ レベルで設定されたクエリーとは別に、グループにもクエリーが設定されました。マシンはグループのクエリーを継承します。

クラスタの作成とクラスタへの参加

クラスタの作成とクラスタへの参加は、グラフィカル ユーザ インターフェイス（GUI）からはできません。クラスタの作成、クラスタへの参加、およびクラスタの設定を行うには、コマンドライン インターフェイス（CLI）を使用する必要があります。クラスタの作成後は、GUI と CLI のどちらからも設定を変更できます。

クラスタを作成する *前に*、必ず中央集中型管理ライセンス キーをイネーブルにしてください。

（注） Cisco IronPort アプライアンスには、中央集中型管理機能の評価キーは付属していません。中央集中型管理機能をイネーブルにするには、30 日間の評価を要求するか、キーを購入する必要があります。キーをイネーブルにするには、CLI の `featurekey` コマンドまたは [システム管理（System Administration）] > [ライセンスキー（Feature Keys）] ページを使用します。

clusterconfig コマンド

マシン上でクラスタの作成やクラスタへの参加を行うには、`clusterconfig` コマンドを使用します。

- 新しいクラスタを *作成* すると、そのクラスタのすべての初期設定はそのクラスタを作成したマシンから継承されます。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。
- マシンがクラスタに *参加* すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。つまり、そのマシン固有の設定（IP アドレスなど）を除くすべての設定が消失し、そのマシンが参加したクラスタ、グループ、またはその両方の設定に置き換わります。マシンがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成するときにそのスタンドアロンの設定が使用され、マシン レベルの設定は保持されません。

現在のマシンがまだクラスタに含まれていない場合は、clusterconfig コマンドを実行すると、既存のクラスタに参加するか、新しいクラスタを作成するかのオプションが表示されます。

```
newyork.example.com> clusterconfig


Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 2


Enter the name of the new cluster.

[]> americas


New cluster committed: Wed Jun 22 10:02:04 2005 PDT

Creating a cluster takes effect immediately, there is no need to commit.


Cluster americas


Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.
```

```
- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

この時点で、新しいクラスタにマシンを追加できます。これらのマシンは、SSH または CCS を使用して通信できます。

既存のクラスタへの参加

既存のクラスタに参加するには、クラスタに追加するホスト上で clusterconfig コマンドを実行します。SSH と CCS のどちらを使用してクラスタに参加するかを選択できます。

既存のクラスタにホストを参加させるには、次の要件を満たす必要があります。

- クラスタ内のマシンの SSH ホスト キーを検証できること
- クラスタ内のマシンの IP アドレスを知っており、そのマシンに（SSH や CCS 経由で）接続できること
- クラスタに属するマシン上の管理ユーザの管理者パスワードを知っていること

（注） クラスタにマシンを追加する前に、追加しようとしているすべてのマシンに中央集中型管理ライセンス キーをインストールする必要があります。あらかじめ中央集中型管理のライセンス キーがシステムにインストールされており、クラスタがすでに存在する場合は、CLI の systemsetup コマンドによるシステム設定ウィザードを使って既存のクラスタに参加することもできます。管理者パスワードの変更、アプリケーションのホスト名の設定、およびネットワーク インターフェイスと IP アドレスの設定の後で、クラスタの作成とクラスタへの参加のいずれかを選択するプロンプトが表示されます。

SSH を使った既存クラスタへの参加

次の表に、SSH オプションを使ってマシン「losangeles.example.com」をクラスタに追加する例を示します。

```
losangeles.example.com> clusterconfig



Do you want to join or create a cluster?

1. No, configure as standalone.

2. Create a new cluster.

3. Join an existing cluster over SSH.

4. Join an existing cluster over CCS.

[1]> 3
```

```
While joining a cluster, you will need to validate the SSH host key of the remote
machine to which you are joining. To get the public host key

fingerprint of the remote host, connect to the cluster and run: logconfig ->
hostkeyconfig -> fingerprint.



WARNING: All non-network settings will be lost. System will inherit the values set at
the group or cluster mode for the non-network settings. Ensure that the cluster settings
are compatible with your network settings (e.g. dnsconfig settings)



Do you want to enable the Cluster Communication Service on

losangeles.example.com? [N]> n



Enter the IP address of a machine in the cluster.

[]> IP address is entered



Enter the remote port to connect to. The must be the normal admin ssh

port, not the CCS port.

[22]> 22



Enter the admin password for the cluster.

The administrator password for the clustered machine is entered



Please verify the SSH host key for IP address:

Public host key fingerprint: xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

Is this a valid key for this host? [Y]> y



Joining cluster group Main_Group.

Joining a cluster takes effect immediately, there is no need to commit.

Cluster americas



Choose the operation you want to perform:
```

```
- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>

(Cluster americas)>
```

CCS を使った既存クラスタへの参加

SSH を使用できない場合は、代わりに CCS を使用します。CCS の唯一の利点は、そのポートではクラスタ通信しか行われない（ユーザ ログインや SCP などは行われない）ことです。CCS を使って既存のクラスタにマシンを追加するには、clusterconfig の prepjoin サブコマンドを使ってクラスタに追加するマシンの準備を行います。次の例では、マシン「newyork」上で prepjoin コマンドを実行して、クラスタに追加するマシン「losangeles」の準備を行っています。

prepjoin コマンドを実行してから、クラスタに追加するホストの CLI で「clusterconfig prepjoin print」と入力し、現在クラスタに含まれているホストのコマンドラインにキーをコピーすることにより、クラスタに追加するホストのユーザ キーを取得します。

```
Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.
```

```
- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]> prepjoin


Prepare Cluster Join Over CCS


No host entries waiting to be added to the cluster.


Choose the operation you want to perform:

- NEW - Add a new host that will join the cluster.

[]> new


Enter the hostname of the system you want to add.

[]> losangeles.example.com


Enter the serial number of the host mail3.example.com.

[]> unique serial number is added


Enter the user key of the host losangeles.example.com. This can be obtained by typing
"clusterconfig prepjoin print" in the CLI on mail3.example.com. Press enter on a blank
line to finish.

unique user key from output of prepjoin print is pasted


Host losangeles.example.com added.

Prepare Cluster Join Over CCS


1. losangeles.example.com (serial-number)


Choose the operation you want to perform:
```

```
- NEW - Add a new host that will join the cluster.

- DELETE - Remove a host from the pending join list.

[]>


(Cluster americas)> commit
```

マシンがクラスタに追加された後は、clusterconfig コマンドを使ってクラスタのさまざまな設定が可能です。

```
(Cluster Americas)> clusterconfig


Cluster americas


Choose the operation you want to perform:

- ADDGROUP - Add a cluster group.

- SETGROUP - Set the group that machines are a member of.

- RENAMEGROUP - Rename a cluster group.

- DELETEGROUP - Remove a cluster group.

- REMOVEMACHINE - Remove a machine from the cluster.

- SETNAME - Set the cluster name.

- LIST - List the machines in the cluster.

- LISTDETAIL - List the machines in the cluster with detail.

- DISCONNECT - Temporarily detach machines from the cluster.

- RECONNECT - Restore connections with machines that were previously detached.

- PREPJOIN - Prepare the addition of a new machine over CCS.

[]>
```

グループの追加

すべてのクラスタには 1 つ以上のグループが含まれている必要があります。新しいクラスタを作成すると、「Main_Group」という名前のデフォルトのグループが自動的に作成されます。しかし、クラスタ内に追加のグループを作成することもできます。次の例は、既存のクラスタ内に追加のグループを作成し、そのグループにマシンを割り当てる方法を示しています。

ステップ 1　clusterconfig コマンドを実行します。

ステップ 2　addgroup サブコマンドを選択し、新しいグループの名前を入力します。

ステップ 3　setgroup サブコマンドを使用して、新しいグループに割り当てるマシンを選択します。

クラスタの管理

CLI でのクラスタの管理

クラスタに含まれるマシンでは、CLI を異なる *モード* に切り替えることができます。モードはあるレベルに含まれる特定の（名前の付いた）メンバを表していることを思い出してください。

CLI のモードに応じて、設定が変更される正確な場所が決まります。デフォルトは、ユーザがログインしたマシン（「ログイン ホスト」）を示す「マシン」モードです。

別のモードに切り替えるには、clustermode コマンドを使用します。次に例を示します。

表 8-1　クラスタの管理

コマンドの例	説明
clustermode	クラスタ モードへの切り替えを確認するプロンプトが表示されます。
clustermode group northamerica	グループ「northamerica」用のグループ モードに切り替わります。
clustermode machine losangeles.example.com	マシン「losangeles」用のマシン モードに切り替わります。

次のように、CLI プロンプトの表示が現在のモードに変わります。

```
(Cluster Americas)>
```

または

```
(Machine losangeles.example.com)>
```

マシン モードでは、プロンプトにマシンの完全修飾ドメイン名が表示されます。

設定のコピーと移動

すべての非制限コマンド（制限コマンド（8-15 ページ）を参照）に、新しい操作として CLUSTERSHOW と CLUSTERSET が追加されました。CLUSTERSHOW は、コマンド設定のモードを表示するときに使用します（新たに追加された操作（8-15 ページ）を参照）。CLUSTERSET 操作は、（現在のコマンドで設定できる）現在の設定をモード間またはレベル間で（たとえば、あるマシンからあるグループへ）移動またはコピーするときに使用します。

コピー すると、現在のモードの設定が保持されます。*移動* すると、現在のモードの設定がリセット（クリア）されます。つまり、移動した後は、現在のモードに設定が設定されなくなります。

たとえば、(destconfig コマンドで)グループ「northamerica」にグッド ネイバー テーブルを設定し、クラスタ全体にこの設定を適用する場合は、destconfig コマンド内で clusterset 操作を使って現在の設定をクラスタ モードにコピー(または移動)できます。(新しい設定の実験 (8-12 ページ)を参照)。

警告　設定を移動またはコピーするときは、依存関係に矛盾が生じないように注意してください。たとえば、免責事項のスタンプが設定されたリスナーを別のマシンに移動またはコピーしても、その新しいマシンに同じ免責事項が設定されていない場合、新しいマシンでは免責事項のスタンプがイネーブルになりません。

新しい設定の実験

クラスタの最も効果的な使用方法の 1 つは、新しい設定を実験することです。まず、分離された環境で、マシン モードでの変更を行います。次に、設定に問題がなければ、設定変更を上位のクラスタ モードに移動し、すべてのマシンに適用します。

次の例は、あるマシンでリスナーの設定を変更し、準備ができたらその設定をクラスタの残りのマシンにパブリッシュする手順を示しています。通常、リスナーはクラスタ レベルで設定されるため、この例では最初に設定をあるマシンのマシン モードに格下げしてから、設定の変更を行い、テストしています。このような実験的な変更は、クラスタ内の他のマシンで同じ変更を行う前に、1 つのマシン上でテストする必要があります。

ステップ 1　clustermode cluster コマンドを使ってクラスタ モードに変更します。

clustermode コマンドは、モードをクラスタ、グループ、およびマシン レベルに変更するときに使用する CLI コマンドです。

ステップ 2　listenerconfig を実行して、クラスタに設定されたリスナーの設定を表示します。

ステップ 3　実験するマシンを選び、clusterset コマンドを使って設定をクラスタから「下位の」マシン モードにコピーします。

ステップ 4　次のように clustermode コマンドを使って実験マシンのマシン モードに移行します。

```
clustermode machine newyork.example.com
```

ステップ 5　実験マシンのマシン モードで listenerconfig コマンドを実行し、実験マシンに固有の変更を行います。

ステップ 6　変更を確定します。

ステップ 7　実験マシン上で設定変更の実験を続行し、必ず変更を確定します。

ステップ 8　新しい設定を他のすべてのマシンに適用する準備ができたら、clusterset コマンドを使って設定を上位のクラスタ モードに移動します。

ステップ 9　変更を確定します。

クラスタからの脱退(削除)

マシンをクラスタから永続的に削除するには、clusterconfig の REMOVEMACHINE 操作を使用します。マシンをクラスタから永続的に削除すると、その設定は「平板化」され、そのマシンはクラスタに含まれていたときと同じように動作します。たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

クラスタ内のマシンのアップグレード

クラスタには、異なるバージョンの AsyncOS を実行しているマシンを接続できません。AsyncOS のアップグレードを行う前に、clusterconfig コマンドを使ってクラスタ内の各マシンを切断する必要があります。すべてのマシンをアップグレードしたら、clusterconfig コマンドを使ってクラスタを再接続します。マシンを同じバージョンにアップグレードする間は、2 つのクラスタを別個に稼働させることができます。また、GUI の [アップグレード（Upgrades）] ページでクラスタ化されたマシンをアップグレードすることもできます。

（注） クラスタから個々のマシンを切断する前にアップグレード コマンドを使用すると、AsyncOS によってクラスタ内のすべてのマシンが切断されます。マシンをアップグレードする前に、各マシンをクラスタから切断することを推奨します。各マシンを切断してアップグレードしている間、他のマシンは引き続きクラスタとして動作します。

CLI を使ってクラスタ内のマシンをアップグレードするには、次の手順を実行します。

ステップ 1　クラスタ内のマシン上で、clusterconfig の disconnect 操作を使用します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig disconnect losangeles.example.com と入力します。commit は必要ありません。

ステップ 2　必要に応じて、suspendlistener コマンドを使ってアップグレード処理中の新しい接続やメッセージの受信を停止します。

ステップ 3　upgrade コマンドを実行して、AsyncOS を新しいバージョンにアップグレードします。

（注） クラスタ内のマシンをすべて切断するように求める警告または確認メッセージは無視してください。マシンがすでに切断されているため、この時点で AsyncOS によってクラスタ内の他のマシンが切断されることはありません。

ステップ 4　マシンの AsyncOS のバージョンを選択します。アップグレードが完了すると、マシンが再起動します。

ステップ 5　アップグレードされたマシン上で resume コマンドを使って新しいメッセージの受信を開始します。

ステップ 6　クラスタ内のマシンごとにステップ 1 ～ 5 を繰り返します。

（注） クラスタからマシンを切断すると、そのマシンを使って他のマシンの設定を変更できなくなります。クラスタの設定を変更することはできますが、設定の同期が取れなくなるため、マシンが切断されている間は設定を変更しないでください。

ステップ 7　すべてのマシンをアップグレードした後で、アップグレードされたマシンごとに clusterconfig の reconnect 操作を実行してマシンを再接続します。たとえば、マシン losangeles.example.com を切断するには、clusterconfig reconnect losangeles.example.com と入力します。クラスタに接続できるのは、同じバージョンの AsyncOS を実行しているマシンだけです。

設定ファイル コマンド

設定情報は、クラスタ内の個々のシステムに保存されます。([システム管理(System Administration)] > [設定ファイル(Configuration File)] ページまたは exportconfig コマンドを使って)マシン モードで設定ファイルをエクスポートすると、現在設定中のマシンのローカル ディスクにファイルがエクスポートされます。クラスタ モードまたはグループ モードでは、現在ログインしているマシンにファイルが保存されます。ファイルのエクスポート先となるマシンは、ユーザに通知されます。

(注)　[システム管理(System Administration)] > [設定ファイル(Configuration File)] ページまたは loadconfig コマンドを使ってクラスタ *全体*(またはクラスタ化されたマシン)の設定をあらかじめ保存しておき、後でその設定を一連の(同じまたは異なる)マシンに復元する方法はサポートされていません。

設定のリセット

クラスタに含まれるマシン上で(ローカル マシン モード限定で)、([システム管理(System Administration)] > [設定ファイル(Configuration File)] ページまたは resetconfig コマンドを使って)設定をリセットすると、そのマシンは工場出荷時のデフォルト設定に戻ります。そのマシンがそれまでクラスタに含まれていた場合は、設定をリセットすることで、その設定がクラスタからも自動的に削除されます。

CLI コマンドのサポート

すべてのコマンドがクラスタに対応

AsyncOS のすべての CLI コマンドがクラスタ対応になりました。一部のコマンドは、クラスタ モードで実行したときの動作がやや異なります。たとえば、次のコマンドをクラスタに含まれるマシン上で実行すると、コマンドの動作が変更されます。

commit および clearchanges コマンド

commit

commit コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてで確定します。

commitdetail

commitdetail コマンドは、クラスタ内のすべてのマシンに反映された設定変更の詳細を表示します。

clearchanges

clearchanges(clear)コマンドは、現在のモードに関係なく、すべての変更をクラスタの 3 つのレベルのすべてでクリアします。

新たに追加された操作

CLUSTERSHOW

各コマンドに、コマンド設定時のモードを表示する CLUSTERSHOW 操作が追加されました。

下位レベルの既存の設定で上書きされる操作を実行する CLI コマンドを入力すると、通知メッセージが表示されます。たとえば、クラスタ モードでコマンドを入力すると、次のような通知メッセージが表示されることがあります。

```
Note: Changes to these settings will not affect the following groups and machines
because they are overriding the cluster-wide settings:

East_Coast, West_Coast

facilities_A, facilities_B, receiving_A
```

グループ モードの設定を編集した場合も、同じようなメッセージが表示されます。

制限コマンド

ほとんどの CLI コマンドとそれに対応する GUI ページは、任意のモード（クラスタ、グループ、マシン）で実行できます。しかし、一部のコマンドとページは 1 つのモードだけに制限されています。

システム インターフェイスには（GUI と CLI のどちらにも）、コマンドが制限されること、およびどのように制限されるかが必ず明示されます。コマンドを設定するための適切なモードに簡単に切り替えることができます。

- GUI では、[モードを変更（Change Mode）] メニューまたは [この機能の設定は現在、次で定義されています:（Settings for this features are currently defined at:）] リンクを使ってモードを切り替えます。
- CLI では、clustermode コマンドを使ってモードを切り替えます。

次のコマンドは、*クラスタ モード*に制限されます。

表 8-2　クラスタ モードに制限されるコマンド

clusterconfig	**sshconfig**
clustercheck	**userconfig**
passwd	

上記のコマンドをグループ モードまたはマシン モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

（注） passwd コマンドは、ゲスト ユーザが使用できるようにするための特例です。ゲスト ユーザがクラスタ内のマシン上で passwd コマンドを実行すると、警告メッセージは表示されず、ユーザのモードを変更せずにクラスタ レベルのデータに対して操作が行われます。他のすべてのユーザに対しては、上記の（他の制限されるコンフィギュレーション コマンドと同じ）動作が行われます。

次のコマンドは、*マシン モード* に制限されます。

antispamstatus	etherconfig	resume	suspenddel
antispamupdate	featurekey	resumedel	suspendlistener
antivirusstatus	hostrate	resumelistener	techsupport
antivirusupdate	hoststatus	rollovernow	tophosts
bouncerecipients	interfaceconfig	routeconfig	topin
deleterecipients	ldapflush	sbstatus	trace
delivernow	ldaptest	setgateway	version
diagnostic	nslookup	sethostname	vofflush
dnsflush	quarantineconfig	settime	vofstatus
dnslistflush	rate	shutdown	workqueue
dnslisttest	reboot	status	
dnsstatus	resetcounters	suspend	

上記のコマンドをクラスタ モードまたはグループ モードで実行しようとすると、警告メッセージが表示され、適切なモードに切り替えることができます。

次のコマンドは、さらに*ログイン ホスト*（ユーザがログインしているマシン）に制限されます。これらのコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

表 8-3　　ログイン ホスト モードに制限されるコマンド

last	resetconfig	tail	アップグレード
ping	supportrequest	telnet	who

GUI でのクラスタの管理

GUI では、クラスタの作成、クラスタへの参加、およびクラスタ固有の設定の管理（`clusterconfig` コマンドと同等の操作）を行うことはできませんが、クラスタ内のマシンの参照、設定の作成や削除、およびクラスタ間、グループ間、マシン間での設定のコピーや移動（つまり、`clustermode` および `clusterset` と同等の操作）を行うことができます。

GUI に最初にログインすると、[受信メールの概要（Incoming Mail Overview）] ページが表示されます。現在のマシンがクラスタのメンバとして設定されている場合は、中央集中型管理機能が GUI でイネーブルになっていることも通知されます。

[受信メールの概要（Incoming Mail Overview）] ページは、表示しているメール フロー モニタリングのデータがローカル マシンに格納されるため、ログイン ホストに制限されるコマンドの例です。別のマシンの [受信メールの概要（Incoming Mail Overview）] レポートを表示するには、そのマシンの GUI にログインする必要があります。

アプライアンス上でクラスタリングがイネーブルになっている場合は、ブラウザのアドレス フィールドの URL に注意してください。この URL には、必要に応じて `machine`、`group`、または `cluster` という単語が含まれています。たとえば、最初にログインしたときの [受信メールの概要（Incoming Mail Overview）] ページの URL は次のように表示されます。

`https://`*hostname*`/`**machine/***serial_number*`/monitor/incoming_mail_overview`

（注） [モニタ（Monitor）] メニューの [受信メールの概要（Incoming Mail Overview）] ページと [受信メールの詳細（Incoming Mail Details）] ページは、ログイン マシンに制限されます。

[メールポリシー(Mail Policies)]、[セキュリティサービス(Security Services)]、[ネットワーク(Network)]、[システム管理(System Administration)] の各タブには、ローカル マシンに制限されないページが表示されます。[メールポリシー(Mail Policies)] タブをクリックすると、GUI 内の中央集中型管理情報が変更されます。

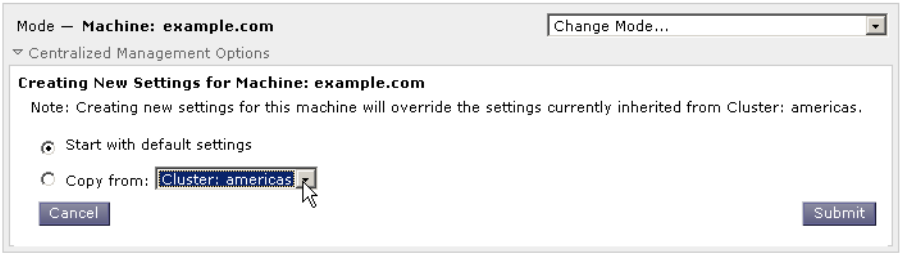
図 8-2　GUI の中央集中型管理機能:設定が規定されていない場合

図 8-2 では、このマシンの現在の機能に関する設定がクラスタ モードから継承されています。継承された設定は薄いグレーで表示(プレビュー)されます。これらの設定を保持することも、クラスタ レベルの設定をこのマシン用に上書きして変更することも可能です。

(注)　継承された設定(プレビュー表示)には、常にクラスタから継承した設定が表示されます。グループ レベルとクラスタ レベルの間で依存するサービスをイネーブルまたはディセーブルにするときは注意してください。詳細については、設定のコピーと移動(8-11 ページ)を参照してください。

[設定を上書き(Override Settings)] リンクをクリックすると、この機能に対応する新しいページが表示されます。このページでは、マシン モードの新しい設定を作成できます。デフォルト設定をそのまま使用することもできますが、別のモードですでに設定している場合は、それらの設定をこのマシンにコピーすることもできます。

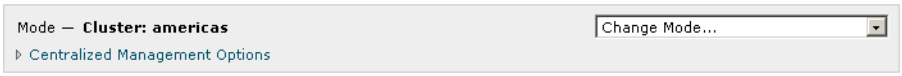
図 8-3　GUI の中央集中型管理機能:新しい設定の作成



または、図 8-2 に示すように、この設定がすでに規定されているモードに移動することもできます。これらのモードは、中央集中型管理ボックスの下部にある [この機能の設定は現在、次で定義されています: (Settings for this feature are currently defined at:)] に表示されます。ここには、設定が実際に規定されているモードだけが表示されます。別のモードで規定された (別のモードから継承された) 設定のページを表示すると、ページ上にそれらの設定が表示されます。

表示されたいずれかのモード (たとえば、図 8-2 に示す [クラスタ: 南/北/中央アメリカ (Cluster: Americas)] リンク) をクリックすると、そのモードの設定を表示して管理できる新しいページが表示されます。

図 8-4　　GUI の中央集中型管理機能: 定義された設定



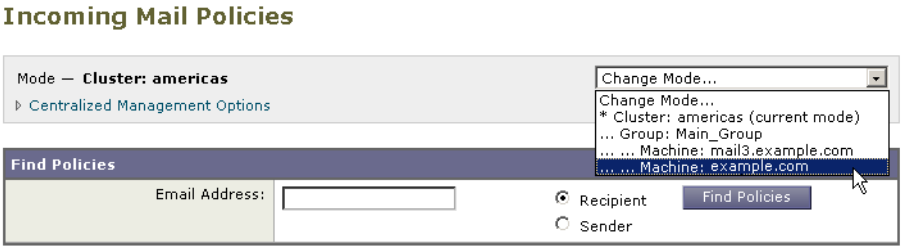
特定のモードで設定を規定すると、中央集中型管理ボックスがすべてのページに最小化された状態で表示されます。[集約管理オプション (Centralized Management Options)] リンクをクリックすると、ボックスが展開され、現在のモードで現在のページに関して設定できるオプションのリストが表示されます。[設定を管理 (Manage Settings)] ボタンをクリックすると、現在の設定を別のモードにコピーまたは移動したり、設定を完全に削除したりできます。

たとえば、図 8-5 では、[集約管理オプション (Centralized Management Options)] リンクがクリックされ、設定可能なオプションが表示されています。

図 8-5　　GUI の中央集中型管理機能: 設定の管理

ボックスの右側には [モードを変更 (Change Mode)] メニューが表示されます。このメニューには現在のモードが表示され、このメニューを使っていつでも他のモード (クラスタ、グループ、またはマシン) に移動できます。

図 8-6　　[モードを変更 (Change Mode)] メニュー



別のモードを表すページに移動すると、中央集中型管理ボックスの左側にある「モード —」というテキストが一時的に黄色で点滅し、モードが変更されたことを知らせます。

特定のタブに含まれる一部のページは、マシン モードに制限されています。ただし、(現在のログイン ホストに制限される) [受信メールの概要 (Incoming Mail Overview)] ページとは異なり、これらのページはクラスタ内のどのマシンでも使用できます。

図 8-7　　中央集中型管理機能：マシンに制限される機能

[モードを変更(Change Mode)] メニューから管理するマシンを選択します。テキストが一時的に点滅し、モードが変更されたことを知らせます。

クラスタ通信

クラスタ内のマシンは、*メッシュ ネットワーク*を使って相互に通信します。デフォルトでは、すべてのマシンが他のすべてのマシンに接続します。1 つのリンクが切断されても、他のマシンが更新を受信できなくなることはありません。

デフォルトでは、クラスタ内のすべての通信が SSH を使って保護されます。各マシンは、ルートテーブルのコピーをメモリ内に保持し、リンクの切断と確立に応じてメモリ内のテーブルを変更します。また、クラスタに含まれる他のすべてのマシンに対して定期的に(1 分間隔で)「ping」を実行します。これにより、リンクの最新状態を確認し、ルータや NAT がタイムアウトした場合でも接続を維持します。

(注)　クラスタ内の 2 台のアプライアンス間の接続は、1 台のアプライアンスが許可される最大 SSH 接続数を超えて開こうとする場合、ドロップされる可能性があります。アプライアンスは数秒以内に自動的にクラスタを再接続するため、手動の設定は必要ありません。

DNS とホスト名の解決

マシンをクラスタに接続するには、DNS が必要です。クラスタの通信は、通常、(マシン上のインターフェイスのホスト名ではなく)マシンの DNS ホスト名を使って開始されます。ホスト名を解決できないマシンは、形式的にはクラスタに含まれていても、実際にはクラスタ内の他のマシンと通信できません。

ホスト名がアプライアンス上の SSH または CCS をイネーブルにした正しい IP インターフェイスを指すように、DNS を設定する必要があります。これは非常に重要です。DNS が SSH または CCS をイネーブルにしていない別の IP アドレスを参照すると、ホストが見つかりません。中央集中型管理では、インターフェイスごとのホスト名ではなく、`sethostname` コマンドで設定した「メイン ホスト名」が使用されます。

IP アドレスを使ってクラスタ内の他のマシンに接続する場合は、接続先のマシンが接続元の IP アドレスの逆ルックアップを実行できる必要があります。DNS 内にその IP アドレスがないために逆ルックアップがタイムアウトすると、そのマシンはクラスタに接続できません。

クラスタリング、完全修飾ドメイン名、およびアップグレード

AsyncOS をアップグレードすると、DNS の変更によって接続が失われることがあります。(クラスタ内のマシン上のインターフェイスのホスト名ではなく)クラスタ内のマシンの完全修飾ドメイン名を変更する必要がある場合は、AsyncOS をアップグレードする*前に*、`sethostname` を使ってホスト名の設定を変更し、そのマシンの DNS レコードを更新する必要があることに注意してください。

クラスタ通信のセキュリティ

Cluster Communication Security（CCS）は、標準の SSH サービスに似たセキュア シェル サービスです。シスコが CCS を実装したのは、クラスタ通信に標準の SSH を使用することに対する懸念に応えるためです。マシン間の SSH 通信では、同じポートで（管理者などの）通常のログインを開きます。多くの管理者は、クラスタ化されたマシン上で通常のログインを開くことを好みません。

ヒント：CCS はデフォルトですが、クラスタ化されたマシン間のポート 22 の通信がファイア ウォールによってブロックされない場合は、CCS をイネーブルにしないでください。クラスタリングでは、すべてのマシン間でフル メッシュの SSH トンネル（ポート 22 上）が使用されます。いずれかのマシンですでに CCS をイネーブルにした場合は、クラスタからすべてのマシンを削除し、最初からやり直してください。クラスタ内の最後のマシンを削除すると、クラスタが削除されます。

CCS は、管理者が CLI へのログインではなく、クラスタ通信を開始できるように強化されています。デフォルトでは、このサービスはディセーブルです。アプライアンスの中央集中型管理機能をイネーブルにすると、`interfaceconfig` コマンドで他のサービスをイネーブルにするためのプロンプトが表示されたときに、CCS をイネーブルにするかどうかの選択を求められます。次に例を示します。

```
Do you want to enable SSH on this interface? [Y]>



Which port do you want to use for SSH?

[22]>



Do you want to enable Cluster Communication Service on this interface?

[N]> y



Which port do you want to use for Cluster Communication Service?

[2222]>
```

CCS のデフォルトのポート番号は 2222 です。必要な場合は、これを別の開いている未使用のポート番号に変更できます。マシンの参加が完了し、参加したマシンにクラスタのすべての設定データが適用されると、次の質問が表示されます。

```
Do you want to enable Cluster Communication Service on this interface? [N]> y



Which port do you want to use for Cluster Communication Service?

[2222]>
```

クラスタの整合性

中央集中型管理をイネーブルにすると、「クラスタ対応」のマシンはクラスタ内の他のマシンへのネットワーク接続を継続的に確認します。この確認は、クラスタ内の他のマシンに対する定期的な「ping」によって行われます。

特定のマシンとの通信の試行がすべて失敗すると、通信を試行したマシンはリモート ホストが切断されたことを示すメッセージをログに記録します。システムはリモート ホストがダウンしたことを示すアラートを管理者に送信します。

マシンがダウンしても、確認用の ping は引き続き送信されます。マシンがクラスタのネットワークに再び参加すると、それまでオフラインだったマシンが更新をダウンロードできるように、同期コマンドが実行されます。この同期コマンドは、一方のマシンに含まれる変更がもう一方のマシンに含まれるかどうかも判定します。含まれない場合は、それまでダウンしていたマシンが更新をサイレントでダウンロードします。

切断/再接続

マシンは、クラスタから切断できます。時折、たとえばマシンをアップグレードするために、マシンを意図的に切断することがあります。切断は、たとえば停電やソフトウェアまたはハードウェアのエラーのために突発的に起きることもあります。1 台のアプライアンスがセッションで許可されている SSH 接続の最大数を超えて開こうとする場合も、切断が起きることがあります。クラスタから切断されたマシンに直接アクセスしてマシンを設定することはできますが、切断されたマシンを再接続するまでは、クラスタ内の他のマシンに変更が反映されません。

マシンをクラスタに再接続すると、そのマシンはただちにすべてのマシンに再接続しようとします。

理論的には、クラスタから 2 台のマシンを切断した場合、同じような変更が各マシンのローカル データベースに同時に確定される可能性があります。これらのマシンをクラスタに再接続すると、これらの変更の同期が試行されます。競合がある場合は、最新の変更が記録されます（他の変更はすべて破棄されます）。

アプライアンスは、変更されるすべての変数を確定時にチェックします。確定データには、バージョン情報、連番 ID、その他の比較可能な情報が含まれます。変更しようとしているデータが以前の変更と競合することがわかった場合は、変更を破棄するオプションが表示されます。たとえば、次のようなメッセージが表示されます。

```
(Machine mail3.example.com)> clustercheck



This command is restricted to "cluster" mode.  Would you like to switch to "cluster"
mode? [Y]> y



Checking Listeners (including HAT, RAT, bounce profiles)...

Inconsistency found!

  Listeners (including HAT, RAT, bounce profiles) at Cluster enterprise:

    mail3.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on
mail3.example.com
```

```
    test.example.com was updated Mon Sep 12 10:59:17 2005 PDT by 'admin' on
mail3.example.com



How do you want to resolve this inconsistency?

1. Force entire cluster to use test.example.com version.

2. Force entire cluster to use mail3.example.com version.

3. Ignore.

[1]>
```

変更を破棄しなかった場合、変更は（確定されませんが）保持されます。変更を現在の設定に照らして確認し、その後の処理方法を決めることができます。

また、いつでも clustercheck コマンドを使ってクラスタが正常に動作していることを確認できます。

```
losangeles> clustercheck



Do you want to check the config consistency across all machines in the cluster? [Y]> y



Checking losangeles...

Checking newyork...

No inconsistencies found.
```

互いに依存する設定

クラウド E メール セキュリティ アプライアンスでは次の設定を行わないことをお勧めします。

中央集中型管理環境では、互いに依存する設定が異なるモードで設定されることがあります。設定モデルの高い柔軟性によって複数のモードで設定できるため、個々のマシンでどの設定が使用されるかは継承の法則に基づいて決まります。しかし、一部の設定は他の設定に依存しており、依存する設定の適用範囲は同じモードの設定に制限されません。したがって、あるレベルで特定のマシン用に設定された設定を参照する設定を別のレベルで設定することも可能です。

互いに依存する設定の最も一般的な例は、ページ上の別のクラスタ セクションからデータを取得する選択フィールドに関するものです。たとえば、次の機能をそれぞれ異なるモードで設定できます。

- LDAP クエリーの使用
- ディクショナリまたはテキスト リソースの使用
- バウンス プロファイルまたは SMTP 認証プロファイルの使用。

中央集中型管理には、制限コマンドと非制限コマンドがあります。(制限コマンド (8-15 ページ)を参照)。非制限コマンドは、通常、クラスタ全体で共有できるコンフィギュレーション コマンドです。

`listenerconfig` コマンドは、クラスタ内のすべてのマシンに設定できるコマンドの例です。非制限コマンドは、クラスタ内のすべてのマシンに反映できるため、マシンごとにデータを変更する必要がないコマンドです。

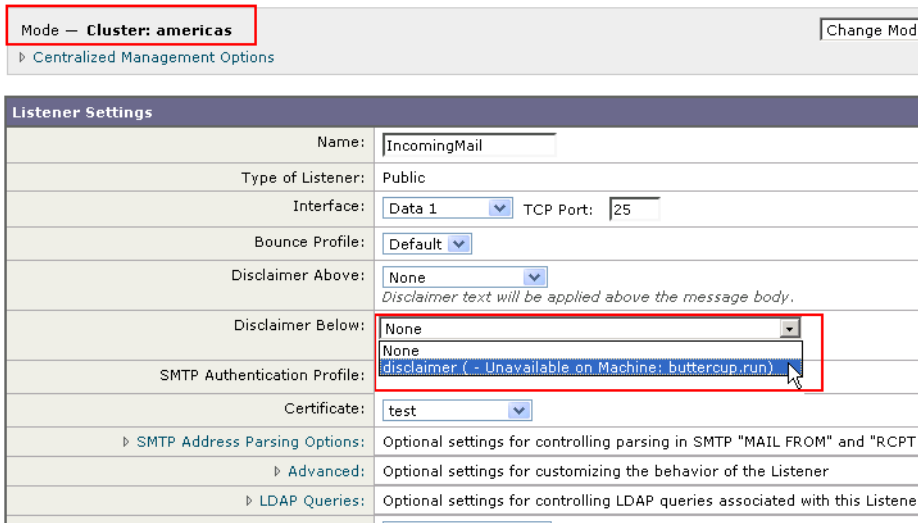
一方、制限コマンドは特定のモードだけに適用されるコマンドです。たとえば、ユーザを特定のマシン用に設定することはできません。ユーザはクラスタ全体に 1 セットしか設定できません(そうしないと、同じログイン名でリモート マシンにログインすることができなくなります)。同じように、メール フロー モニタのデータ、システム概要のカウンタ、およびログファイルは、マシン単位でしか保持されないため、これらのコマンドやページはマシンだけに制限する必要があります。

定期レポートはクラスタ全体で同じに設定できますが、レポートの表示はマシン別に行われます。したがって、GUI の [定期レポート(Scheduled Reports)] ページは 1 つでも、設定はクラスタ モードで行い、レポートの表示はマシン モードで行う必要があります。

[システム時刻(System Time)] のページには、`settz`、`ntpconfig`、`settime` の各コマンドが含まれ、制限コマンドと非制限コマンドが混在しています。この場合、`settime` は(時間の設定がマシンに固有のものであるため)マシン モードだけに制限する必要がありますが、`settz` と `ntpconfig` はクラスタ モードまたはグループ モードで設定できます。

次の例を考えてみます。

図 8-8　　互いに依存する設定の例



この図では、リスナー「IncomingMail」がマシン レベルでのみ設定された「disclaimer」という名前のフッターを参照しています。使用可能なフッター リソースのドロップダウン リストには、クラスタでは使用できるのにマシン「buttercup.run」では使用できないフッターが表示されています。このジレンマを解消するには、次の 2 つの方法があります。

- フッター「disclaimer」をマシン レベルからクラスタ レベルに格上げする
- リスナーをマシン レベルに格下げして、相互依存を解消する

中央集中型管理されたシステムの特長を最大限に活かすためには、1 つめの方法を推奨します。クラスタ化されたマシンの設定を調整するときは、設定間の相互依存に注意してください。

ベスト プラクティスとよく寄せられる質問

ベスト プラクティス

クラスタを作成すると、現在ログインしているマシンが自動的に最初のマシンとしてクラスタに追加され、Main_Group にも追加されます。マシン レベルの設定は、できる限りクラスタ レベルに移動されます。グループ レベルの設定は存在せず、マシン レベルに残された設定は、クラスタ レベルでは意味を成さないのでクラスタ化できません。例として、IP アドレスやライセンス キーなどがあります。

設定はできる限りクラスタ レベルに残します。クラスタ内の 1 つのマシンにだけ異なる設定が必要な場合は、そのクラスタ設定をそのマシンのマシン レベルにコピーします。この場合は、設定を移動しないでください。工場出荷時のデフォルト値がない設定（HAT テーブル、SMTPROUTES テーブル、LDAP サーバ プロファイルなど）を移動すると、クラスタ設定を継承するシステムに空のテーブルが作成され、電子メールが処理されなくなるおそれがあります。

マシンにクラスタ設定を再度継承させるには、CM の設定を管理し、マシンの設定を削除します。マシンがクラスタ設定を上書きするかどうかは、次のメッセージが表示されたときにわかります。

```
Settings are defined:

To inherit settings from a higher level: Delete Settings for this feature at this mode.

You can also Manage Settings.

Settings for this feature are also defined at:

Cluster: xxx
```

または、次のメッセージが表示されます。

```
Delete settings from:

    Cluster: xxx

    Machine: yyyy.domain.com
```

コピーと移動の違い

コピーする必要がある場合：クラスタに設定を作成し、グループまたはマシンには設定を作成しないか、別の設定を作成する場合。

移動する必要がある場合：クラスタには設定を作成せず、グループまたはマシンに設定を作成する場合。

適切な CM の設計方法

LIST 操作で CM マシンのリストを出力すると、次のように表示されます。

```
cluster = CompanyName

Group Main_Group:

    Machine lab1.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

    Machine lab2.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)

Group Paris:

    Machine lab3.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
```

```
    Machine lab4.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
Group Rome:
    Machine lab5.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
    Machine lab6.example.com (Serial #: XXXXXXXXXXXX-XXXXXXX)
```

現在変更しているレベルを忘れないように注意してください。たとえば、(RENAMEGROUP を使って)Main_Group の名前を変更した場合は、次のように表示されます。

```
cluster = CompanyName
Group London:
    Machine lab1.cable.nu (Serial #: 000F1FF7B3F0-CF2SX51)
    ...
```

しかし、最初にグループ レベルで London のシステムを変更すると、クラスタ レベルを基本的な設定を行うための通常の設定レベルとして使用しなくなるため、このような設定は管理者にとって混乱の元です。

ヒント:グループにクラスタと同じ名前を付けること(クラスタ「London」とグループ「London」など)は推奨しません。グループ名としてサイト名を使用する場合、クラスタに場所を表す名前を付けることは推奨しません。

正しい方法は、前述のように、できるだけ多くの設定をクラスタ レベルに残すことです。ほとんどの場合、プライマリ サイトや主要なマシン群を Main_Group に残し、グループを追加のサイト用に使用してください。これは、両方のサイトを「同等」に扱う場合にも当てはまります。CM にはプライマリ/セカンダリ サーバやマスター/スレーブ サーバがなく、クラスタ化されたすべてのマシンがピアになることを思い出してください。

ヒント:追加のグループを使用する場合は、マシンをクラスタに追加する前にグループを簡単に準備できます。

手順:サンプル クラスタの設定

このサンプル クラスタを設定するには、clusterconfig を実行する前に、すべてのマシン上ですべての GUI からログアウトします。プライマリ サイトのいずれかのマシン上で clusterconfig を実行します。次に、他のローカル マシンとリモート マシンのうち、(IP アドレスなどのマシン専用の設定を除いて)できるだけ多くの設定を共有する必要があるマシンだけをこのクラスタに追加します。clusterconfig コマンドを使ってリモート マシンをクラスタに追加することはできません。リモート マシン上の CLI を使って clusterconfig(既存のクラスタへの参加)を実行する必要があります。

前述の例では、lab1 にログインし、clusterconfig を実行して CompanyName という名前のクラスタを作成しています。同じ要件のマシンは 1 つしかないので、lab2 にログインし、saveconfig で既存の設定を保存します(この設定は lab1 の設定のほとんどを継承して大幅に変更されます)。次に、lab2 上で clusterconfig を使って既存のクラスタに参加します。他にも同じようなポリシーと設定を必要とするマシンがこのサイトにある場合は、上記の手順を繰り返します。

CONNSTATUS を実行して、DNS でホスト名が正しく解決されることを確認します。マシンがクラスタに追加されると、新しいマシンのほとんどの設定は lab1 から継承され、古い設定は消失します。追加されたマシンが運用マシンである場合は、これまでの設定の代わりに新しい設定を使ってメールが引き続き処理されるかどうかを予測する必要があります。マシンをクラスタから削除しても、そのマシンが古い専用の設定に戻ることはありません。

次に、例外となるマシンの数を数えます。例外が 1 台しかない場合は、マシン レベルの設定をいくつか追加すればよく、そのマシン用に追加のグループを作成する必要はありません。そのマシンをクラスタに追加し、設定をマシン レベルにコピーする作業を始めます。このマシンが既存の運用マシンである場合は、設定をバックアップし、前述のように電子メール処理の変更を検討する必要があります。

前述の例のように、例外が 2 台以上ある場合は、それらのマシンがクラスタで共有されない設定を共有するかどうかを判断します。共有する場合は、これらのマシン用のグループを 1 つ以上作成します。共有しない場合は、各マシンでマシン レベルの設定を作成すればよく、追加のグループを作成する必要はありません。

前述の例では、クラスタにすでに含まれているいずれかのマシン上で CLI の `clusterconfig` を実行し、ADDGROUP を選択する必要があります。この作業を 2 回行います（Paris に対して 1 回、Rome に対して 1 回）。

これで、GUI と CLI を使ってクラスタ用の設定とすべてのグループ（まだマシンがないグループも含む）用の設定を作成できます。各マシンのマシン固有の設定を作成できるようになるのは、マシンをクラスタに追加した *後* です。

上書き（例外）用の設定を作成する最適な方法は、上位レベル（クラスタなど）から下位レベル（グループなど）に設定をコピーすることです。

たとえば、クラスタを作成した後の `dnsconfig` の初期設定は次のようになりました。

```
Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: No

Group Rome: No

Machine lab2.cable.nu: No
```

この DNS の設定を「グループにコピー」すると、次のようになります。

```
Configured at mode:

Cluster: Yes

Group Main_Group: No

Group Paris: Yes

Group Rome: No

Machine lab2.cable.nu: No
```

ここで、Paris グループ レベルの DNS の設定を編集すると、Paris グループの他のマシンはその設定を継承します。Paris グループ以外のマシンは、マシン固有の設定がない限り、クラスタの設定を継承します。DNS の設定に加えて、SMTPROUTES の設定もグループ レベルで作成するのが一般的です。

ヒント：CLI のさまざまなメニューで CLUSTERSET 機能を使用するときは、設定をすべてのグループにコピーする特別なオプションを使用できます。このオプションは GUI では使用できません。

ヒント：完成されたリスナーは、グループまたはクラスタから自動的に継承されるため、通常はクラスタ内の最初のシステム上でのみリスナーを作成します。これによって管理作業が大幅に軽減されます。ただし、そのためには *グループまたはクラスタ全体でインターフェイスに同じ名前を付ける必要があります。*

設定をグループ レベルで正しく規定した後は、マシンをクラスタに追加し、このグループに含めることができます。これには次の 2 つの手順が必要です。

まず、残りの 4 つのシステムをクラスタに追加するため、各システム上で `clusterconfig` を実行します。大きく複雑なクラスタほど、追加処理にかかる時間も長くなり、数分かかることもあります。LIST および CONNSTATUS サブコマンドを使って追加処理の進行状況をモニタできます。追加処理が完了したら、SETGROUP を使ってマシンを Main_Group から Paris および Rome に移動します。クラスタに追加されたすべてのマシンが最初に Paris や Rome の設定ではなく Main_Group の設定を継承することは避けられません。これは、新しいシステムがすでに稼働中である場合、メール フローのトラフィックに影響する可能性があります。

ヒント：試験用マシンを運用マシンと同じクラスタに含めないでください。試験用システムには新しいクラスタ名を使用してください。これによって、予期しない変更（たとえば、誰かが試験用システムを変更し、誤って運用メールを消失するなど）に対する防御層が追加されます。

GUI でクラスタのデフォルト以外の CM 設定を使用する場合のオプションの要約

設定の上書き（デフォルトの設定から開始）。たとえば、SMTPROUTES 設定のデフォルトの設定は空のテーブルであり、テーブルを最初から作成できます。

設定の上書き（ただし、クラスタ「xxx」またはグループ「yyy」から現在継承している設定のコピーから開始）。たとえば、SMTPROUTES テーブルの新しいコピーをグループ レベルで使用できます。このテーブルは、初期状態ではクラスタのテーブルとまったく同じです。（SETGROUP で）同じグループに追加されたすべての Cisco IronPort アプライアンスにこのテーブルが適用されます。このグループに含まれないマシンでは、引き続きクラスタ レベルの設定が使用されます。この独立したテーブルで SMTPROUTES を変更しても、他のグループ、クラスタの設定を継承するマシン、および個々のマシン レベルで設定が規定されているマシンには影響しません。これが最も一般的な選択です。

中央集中型管理オプションのサブメニューである [設定を管理（Manage Settings）]。このメニューでは、上記のように設定をコピーできますが、設定を移動または削除することもできます。SMTPROUTES をグループまたはマシン レベルに移動すると、ルート テーブルはクラスタ レベルでは空になり、より具体的なレベルに存在することになります。

[設定を管理（Manage Settings）]。同じ SMTPROUTES の例で削除オプションを使用した場合も、クラスタの SMTPROUTES テーブルが空になります。SMTPROUTES をグループ レベルまたはマシン レベルですでに設定している場合は、これで問題ありません。クラスタ レベルの設定を削除し、グループまたはマシンの設定だけに依存することは推奨しません。クラスタ全体の設定は、新しく追加したマシンに対するデフォルトとして有用であり、これを保持することによって、管理する必要があるグループまたはサイトの設定の数が 1 つ減ります。

セットアップと設定に関する質問

Q：中央集中型管理のライセンス キーを受け取るにはどうすればよいですか。

A：Cisco IronPort アプライアンスをクラスタに追加する前に、すべてのアプライアンスに中央集中型管理用の一意のライセンス キーをインストールする必要があります。キーを入手するには、Cisco IronPort のカスタマー サポートに連絡してください。個々のキーをインストールするには、[システム管理（System Administration）] > [ライセンス キー（Feature Keys）] ページ（GUI）または `featurekey` コマンド（CLI）を使用します。

Q: 設定が完了し、リスナーやユーザからメールを受信しているスタンドアロンのアプライアンスがあります。中央集中型管理のライセンス キーを適用し、新しいクラスタを作成すると、これまでの設定はどうなりますか。

A: アプライアンスがすでに「スタンドアロン」モードで設定されている場合は、クラスタを作成したときにそのスタンドアロンの設定が使用されます。つまり、`clusterconfig -> create cluster` コマンドを使って新しいクラスタを作成すると、最初にすべての設定がクラスタ レベルで設定されます。次にクラスタに参加したマシンは、これらの設定をすべて受け取ります。

Q: これまでスタンドアロンとして設定されていたマシンがあり、既存のクラスタに参加しました。これまでの設定はどうなりますか。

A: マシンがクラスタに参加すると、そのマシンのすべてのクラスタ化可能な設定がクラスタ レベルから継承されます。クラスタに参加した時点で、ローカルで設定されたネットワーク以外の設定は消失し、クラスタや関連するグループの設定で上書きされます。(これにはユーザ/パスワードのテーブルも含まれ、パスワードとユーザはクラスタ内で共有されます)。

Q: クラスタ化されたマシンがあり、それをクラスタから(永続的に)削除しました。これまでの設定はどうなりますか。

A: マシンをクラスタから永続的に削除すると、その設定階層は「平板化」され、そのマシンは引き続きクラスタに含まれていたときと同じように動作します。マシンに継承されたすべての設定が、スタンドアロンとして設定されたマシンに適用されます。

たとえば、クラスタ モードのグローバル配信停止テーブルしかない場合にマシンをクラスタから削除すると、そのグローバル配信停止テーブルのデータがマシンのローカル設定にコピーされます。

一般的な質問

Q: 中央集中型管理されるマシン間でログ ファイルは集約されますか。

A: いいえ。ログ ファイルは引き続き個々のマシンごとに保持されます。セキュリティ管理アプライアンスを使って複数のマシンのメール ログを集約し、トラッキングやレポート作成に利用できます。

Q: ユーザ アクセスはどうなりますか。

A: Cisco IronPort アプライアンスはクラスタ全体で 1 つのデータベースを共有します。特に、`admin` アカウントはクラスタ全体で 1 つしかありません。

Q: データセンターをクラスタ化するにはどうすればよいですか。

A: データセンターは、それ自体をクラスタにせずに、クラスタ内の「グループ」にするのが理想的です。しかし、データセンター間で共有する設定が多くない場合は、各データセンターを別個のクラスタにした方がうまくいく場合があります。

Q: オフラインのシステムを再接続するとどうなりますか。

A: クラスタにシステムを再接続すると、システム間の同期が試行されます。

ネットワークに関する質問

Q:中央集中型管理機能は「ピアツーピア」アーキテクチャと「マスター/スレーブ」アーキテクチャのどちらですか。

A:すべてのマシンにすべてのマシン用のあらゆるデータ(使用されないマシン固有の設定を含む)があるため、中央集中型管理機能は「ピアツーピア」アーキテクチャと見なすことができます。

Q:ピアにならないようにアプライアンスをセットアップするにはどうすればよいですか。「スレーブ」システムを設定する必要があります。

A:このアーキテクチャでは、本物の「スレーブ」マシンは設定できません。しかし、マシン レベルで HTTP アクセス(GUI)と SSH/Telnet アクセス(CLI)をディセーブルにすることは可能です。このように GUI アクセスや CLI アクセスができないマシンは、clusterconfig コマンドでのみ 設定可能です(つまり、ログイン ホストではなくなります)。これはスレーブを設定するのに似ていますが、ログイン アクセスを再度イネーブルにすると、この設定は無効になります。

Q:複数のセグメント化されたクラスタを作成できますか。

A:クラスタを「島」のように分離することは可能です。実際、たとえばパフォーマンス上の理由などで、このようなクラスタを作成するのが有益な場合もあります。

Q:クラスタ化されたアプライアンスのうち、1 台の IP アドレスとホスト名を再設定したいのですが、再設定した場合、再起動コマンドを実行できるようになる前に GUI/CLI セッションが終了しませんか。

次の手順に従ってください。

a. 新しい IP アドレスを追加します。
b. リスナーを新しいアドレスに移動します。
c. クラスタを脱退します。
d. ホスト名を変更します。
e. どのマシンから表示した `clusterconfig` の接続リストにも、古いマシン名が表示されないことを確認します。
f. すべての GUI セッションがログアウトしたことを確認します。
g. (`interfaceconfig` または [ネットワーク(Network)] > [リスナー(Listeners)] を使って)どのインターフェイスでも CCS がイネーブルになっていないことを確認します。
h. マシンを再びクラスタに追加します。

Q:送信先コントロール機能をクラスタ レベルで適用できますか。それともこの機能はローカル マシン レベル専用ですか。

クラスタ レベルでも設定できますが、制限はマシン単位で適用されます。したがって、接続を 50 個に制限すると、クラスタ内のそれぞれのマシンにその制限が設定されます。

計画と設定

Q:クラスタをセットアップするときに、効率を最大限に高め、問題を最小限に抑えるにはどうすればよいですか。

1. 初期の計画
   - できるだけ多くの項目をクラスタ レベルで設定します。

- 例外のみをマシン単位で管理します。
- データセンターが複数ある場合は、たとえば、グループを使ってクラスタ共通でもマシン固有でもない特性を共有します。
- 各アプライアンスのインターフェイスとリスナーに同じ名前を使用します。

2. 制限コマンドに注意してください。
3. 設定間の相互依存に注意してください。

   たとえば、`listenerconfig` コマンドは、(クラスタ レベルでも)マシン レベルにしか存在しないインターフェイスに依存します。クラスタ内のどのマシンにもマシン レベルのインターフェイスが存在しない場合、そのリスナーはイネーブルになります。

   インターフェイスの削除も `listenerconfig` に影響します。
4. 設定に注意してください。

   すでに設定されているマシンがクラスタに参加すると、そのマシン単独の設定は消失します。前に設定した設定の一部を再び適用する場合は、クラスタに参加する前にすべての設定をメモしてください。

   「切断された」マシンは、まだクラスタに含まれています。マシンを再接続すると、オフライン中に行った変更がクラスタの他のマシンと同期化されます。

   マシンをクラスタから永続的に削除すると、そのマシンはクラスタのメンバとして持っていたすべての設定を保持します。しかし、考えを変えて再びそのマシンをクラスタに追加すると、そのマシンのスタンドアロンの設定はすべて消失します。この場合、設定を意図した状態に復元することはほぼ不可能です。

   `saveconfig` コマンドを使って設定の記録を取ってください。

APPENDIX **A**

AsyncOS クイック リファレンス ガイド

この付録のクイック リファレンス ガイドは、適切な CLI コマンドとその目的を調べるときに使用します。

表 A-1　　CLI コマンド（確定が不要なもの）

antispamstatus	Anti-Spam ステータスを表示します。
antispamupdate	スパム定義を手動で更新します。
antivirusstatus	Anti-Virus ステータスを表示します。
antivirusupdate	ウイルス定義を手動で更新します。
bouncerecipients	キューからメッセージをバウンスします。
clearchanges ***または*** **clear**	変更をクリアします。
commit	変更を確定します。
commitdetail	最後の確定に関する詳細情報を表示します。
diagnostic	ハードウェアおよびソフトウェアのトラブルシーティング ユーティリティです。
deleterecipients	キューからメッセージを削除します。
delivernow	メッセージのスケジュールを即時配信用に再設定します。
dnsflush	DNS キャッシュからすべてのエントリをクリアします。
dnslistflush	現在の DNS リスト キャッシュをフラッシュします。
dnslisttest	DNS ベースのリスト サービスの DNS ルックアップをテストします。
dnsstatus	DNS 統計情報を表示します。
encryptionstatus	PXE エンジンとドメイン マッピング ファイルのバージョンを表示します。
encryptionupdate	PXE エンジンの更新を要求します。
featurekey	システム機能キーを管理します。
help ***または*** **h** ***または*** **?**	ヘルプ
hostrate	特定のホストのアクティビティをモニタします。
hoststatus	特定のホスト名のステータスを取得します。
last	システムに最近ログインしたユーザを表示します。
ldapflush	キャッシュされている LDAP の結果をフラッシュします。

表 A-1　CLI コマンド（確定が不要なもの）（続き）

ldaptest	1 つの LDAP クエリー テストを実行します。
mailconfig	現在の設定を電子メール アドレスに送信します。
netstat	ネットワーク接続、ルーティング テーブル、およびいくつかのネットワーク インターフェイス統計情報を表示します。
nslookup	ネームサーバに問い合わせます。
outbreakflush	キャッシュされている発生ルールをクリアします。
outbreakstatus	現在のアウトブレイク ルールを表示します。
outbreakupdate	ウイルス感染フィルタ ルールを更新します。
packetcapture	ネットワーク経由で送受信されたパケットを傍受して表示します。
ping	ネットワーク ホストに対して ping を実行します。
quit *または* **q** *または* **exit**	終了します。
rate	メッセージのスループットをモニタします。
reboot	システムを再起動します。
redirectrecipients	すべてのメッセージを別のリレー ホストにリダイレクトします。
resetconfig	工場出荷時のデフォルト設定に戻します。
resetcounters	システム内のすべてのカウンタをリセットします。
resume	受信と配信を再開します。
resumedel	配信を再開します。
resumelistener	受信を再開します。
rollovernow	ログ ファイルをロール オーバーします。
saveconfig	設定をディスクに保存します。
sbstatus	SenderBase クエリーのステータスを表示します。
settime	システム クロックを手動で設定します。
showconfig	すべての設定値を表示します。
showmessage	メッセージを表示します。
showrecipients	キューからメッセージを表示します。
shutdown	システムをシャットダウンして電源を切ります。
status	システム ステータス
supportrequest	Cisco IronPort のカスタマー サポートにメッセージを送信します。
suspend	受信と配信を中断します。
suspenddel	配信を中断します。
suspendlistener	受信を中断します。
systemsetup	最初のシステム設定。
tail	ログ ファイルの最新部分を継続的に表示します。
techsupport	Cisco IronPort のカスタマー サービスがシステムにアクセスできるようにします。

表 A-1　CLI コマンド（確定が不要なもの）（続き）

telnet	リモート ホストに接続します。
tlsverify	リモート ホストに対する発信 TLS 接続を確立し、TLS 接続の問題をデバッグします。
tophosts	キューのサイズの順に上位のホストを表示します。
topin	着信接続の数の順に上位のホストを表示します。
trace	システムを通過するメッセージのフローを追跡します。
traceroute	リモート ホストへのネットワーク ルートを表示します。
tzupdate	タイムゾーン ルールを更新します。
updatenow	すべてのコンポーネントを更新します。
upgrade	アップグレードをインストールします。
version	システムのバージョン情報を表示します。
who	ログイン中のユーザのリストを表示します。
whoami	現在のユーザ ID を表示します。
workqueue	作業キューの一時停止ステータスを表示および変更します。

表 A-2 に示すコマンドの実行結果を有効にするには、commit コマンドを実行する必要があります。

表 A-2　CLI コマンド（確定が必要なもの）

addressconfig	システムで生成するメールの From: アドレスを設定します。
adminaccessconfig	ネットワーク アクセス リストとバナー ログインを設定します。
alertconfig	電子メール アラートを設定します。
aliasconfig	電子メール エイリアスを設定します。
altsrchost	Virtual Gateway(tm) のマッピングを設定します。
antispamconfig	Anti-Spam ポリシーを設定します。
antivirusconfig	Anti-Virus ポリシーを設定します。
bounceconfig	バウンスの動作を設定します。
bvconfig	Cisco IronPort バウンス検証を設定します。
certconfig	セキュリティの証明書とキーを設定します。
clusterconfig	クラスタ関連の設定を実行します。
deliveryconfig	メール配信を設定します。
destconfig	送信先コントロールを設定します。
dictionaryconfig	コンテンツ ディクショナリを設定します。
dnsconfig	DNS のセットアップを設定します。
dnslistconfig	DNS リスト サービスのサポートを設定します。
domainkeysconfig	DomainKeys のサポートを設定します。
etherconfig	イーサネットの設定値を設定します。
exceptionconfig	ドメイン例外テーブルを設定します。

表 A-2　CLI コマンド（確定が必要なもの）（続き）

filters	メッセージ処理オプションを設定します。
incomingrelayconfig	着信リレーを設定します。
interfaceconfig	イーサネット IP アドレスを設定します。
listenerconfig	メール リスナーを設定します。
ldapconfig	LDAP サーバを設定します。
loadconfig	設定ファイルをロードします。
localeconfig	多言語対応の設定値を設定します。
logconfig	ログ ファイルへのアクセスを設定します。
ntpconfig	NTP タイム サーバを設定します。
outbreakconfig	感染フィルタを設定します。
password または passwd	パスワードを変更する
policyconfig	受信者単位または送信者ベースのポリシーを設定します。
quarantineconfig	システムの隔離を設定します。
routeconfig	IP ルーティング テーブルを設定します。
scanconfig	添付ファイルのスキャン ポリシーを設定します。
senderbaseconfig	SenderBase の接続設定値を設定します。
setgateway	デフォルト ゲートウェイ（ルータ）を設定します。
destconfig	発信ホストの制限値と配信の設定値を設定します。
sethostname	マシンの名前を設定します。
settz	ローカル タイム ゾーンを設定します。
sievechar	Sieve 電子メール フィルタリングの文字を設定します。
smtpauthconfig	SMTP 認証プロファイルを設定します。
smtproutes	永続的なドメイン転送を設定します。
snmpconfig	SNMP の設定
sshconfig	SSH キーを設定します。
sslconfig	SSL の設定値を設定します。
stripheaders	削除するメッセージ ヘッダーを設定します。
textconfig	テキスト リソースを設定します。
unsubscribe	グローバル配信停止リストを更新します。
updateconfig	システム更新パラメータを設定します。
userconfig	ユーザ アカウントと外部の認証ソースへの接続を管理します。

APPENDIX B

アプライアンスへのアクセス

アプライアンスに作成したインターフェイスには、さまざまなサービスを通してアクセスできます。

デフォルトでは、各インターフェイスに対して次のサービスが有効または無効に設定されています。

表 B-1　インターフェイスに対してデフォルトでイネーブルになるサービス

		デフォルトで有効かどうか	
サービス	**デフォルト ポート**	**管理インターフェイス[a]**	**新規作成されたインターフェイス**
FTP	21	いいえ	いいえ
Telnet	23	はい	いいえ
SSH	22	はい	いいえ
HTTP	80	はい	いいえ
HTTPS	443	はい	いいえ

a. ここに示す「管理インターフェイス」は、Cisco IronPort C10 アプライアンスの Data 1 インターフェイスのデフォルト設定でもあります。

- グラフィカル ユーザ インターフェイス（GUI）を使用してアプライアンスにアクセスする必要がある場合は、インターフェイスで HTTP、HTTPS、またはその両方をイネーブルにする必要があります。
- 設定ファイルのアップロードまたはダウンロードを目的としてアプライアンスにアクセスする必要がある場合は、インターフェイスで FTP または Telnet をイネーブルにする必要があります。
- Secure Copy（scp）を使用しても、ファイルをアップロードまたはダウンロードできます。

FTP アクセス

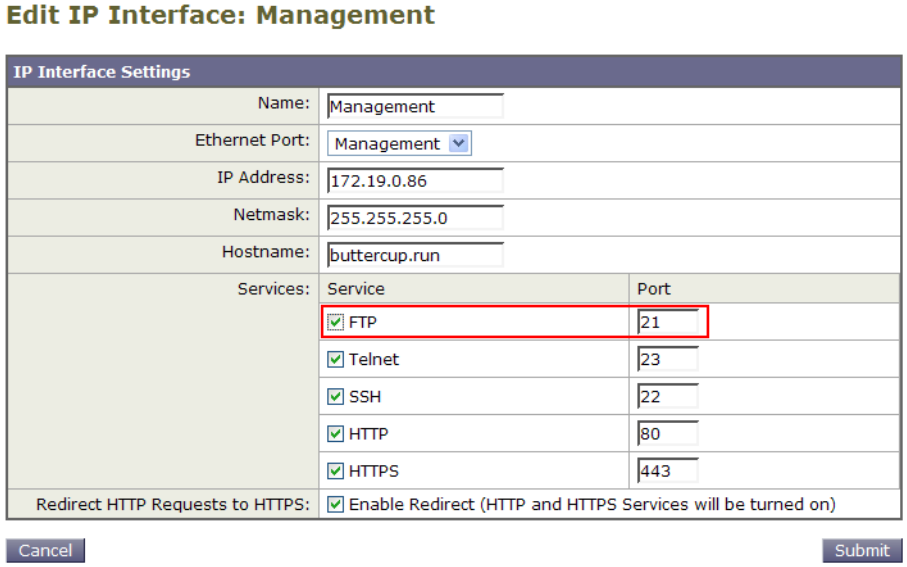
FTP 経由でアプライアンスにアクセスするには、次の手順を実行します。

ステップ 1　[ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] ページまたは `interfaceconfig` コマンドを使用して、インターフェイスに対して FTP アクセスをイネーブルにします。

WARNING:　サービスを `interfaceconfig` コマンドでディセーブルにすると、CLI との接続が解除されることがあります。これは、アプライアンスにどのように接続しているかによって異なります。管理ポートで別のプロトコル、シリアル インターフェイス、またはデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。

この例では、管理インターフェイスがポート 21（デフォルト ポート）で FTP アクセスをイネーブルにするように編集されています。

図 B-1　[IP インターフェイスを編集（Edit IP Interface）] ページ



（注）　次の手順に進む前に、忘れずに変更を確定してください。

ステップ 2　FTP 経由でインターフェイスにアクセスします。インターフェイスに対して正しい IP アドレスを使用していることを確認します。次に例を示します。

```
$ ftp 192.168.42.42
```

（注）　ブラウザの多くは、FTP 経由でもインターフェイスにアクセスできます。

ステップ 3　実行しようとする特定のタスクのディレクトリを参照します。FTP 経由でインターフェイスにアクセスしたら、次のディレクトリを参照し、ファイルをコピーおよび追加（「GET」および「PUT」）できます。次の表を参照してください。

ディレクトリ名	説明
/configuration	以下のコマンドからのデータがこのディレクトリにエクスポートされるか、このディレクトリからデータがインポート（保存）されます。 • **仮想ゲートウェイ マッピング**（altsrchost） • XML **形式の設定データ**（saveconfig、loadconfig） • **ホスト アクセス テーブル**（HAT）（hostaccess） • **受信者アクセス テーブル**（RAT）（rcptaccess） • SMTP **ルート エントリ**（smtproutes） • **エイリアス テーブル**（aliasconfig） • **マスカレード テーブル**（masquerade） • **メッセージ フィルタ**（filters） • **グローバル配信停止データ**（unsubscribe） • trace **コマンドのテスト メッセージ** • **セーフリスト/ブロックリスト バックアップ ファイル**（*slbl<タイムスタンプ><シリアル番号>.csv 形式で保存*）
/antivirus	Anti-Virus エンジンのログ ファイルが保存されるディレクトリです。このディレクトリにあるログ ファイルを検査して、ウイルス定義ファイル（scan.dat）の成功した最終ダウンロードを手動で確認できます。
/configuration /system_logs /cli_logs /status /reportd_logs reportqueryd_logs /ftpd_logs /mail_logs /asarchive /bounces /error_logs /avarchive /gui_logs /sntpd_logs /RAID.output /euq_logs /scanning /antispam /antivirus /euqgui_logs /ipmitool.output	logconfig コマンドと rollovernow コマンドを使用する**ロギング**用に自動的に作成されます。各ログの詳しい説明については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」を参照してください。 ログ ファイル タイプの違いについては、「ログ ファイル タイプの比較」を参照してください。

ステップ 4　ご使用の FTP プログラムを使用して、適切なディレクトリに対するファイルのアップロードおよびダウンロードを行います。

secure copy（scp）アクセス

クライアント オペレーティング システムでセキュア コピー（scp）コマンドがサポートされている場合は、前述の表に示すディレクトリ間でファイルをコピーできます。たとえば次の例では、ファイル /tmp/test.txt は、クライアント マシンからホスト名が mail3.example.com のアプライアンスの configuration ディレクトリにコピーされます。

コマンドを実行すると、ユーザ（admin）のパスワードを求めるプロンプトが表示されることに注意してください。この例を参考用としてだけ示します。特殊なオペレーティング システムの secure copy の実装方法によって異なる場合があります。

```
% scp /tmp/test.txt admin@mail3.example.com:configuration

The authenticity of host 'mail3.example.com (192.168.42.42)' can't be established.

DSA key fingerprint is 69:02:01:1d:9b:eb:eb:80:0c:a1:f5:a6:61:da:c8:db.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'mail3.example.com ' (DSA) to the list of known hosts.

admin@mail3.example.com's password: (type the password)

test.txt             100% |***************************|  1007       00:00

%
```

この例では、同じファイルがアプライアンスからクライアント マシンにコピーされます。

```
% scp admin@mail3.example.com:configuration/text.txt .

admin@mail3.example.com's password: (type the password)

test.txt             100% |***************************|  1007       00:00

%
```

Cisco IronPort アプライアンスに対するファイルの転送および取得には、セキュア コピー（scp）を FTP に代わる方法として使用できます。

（注） operators グループおよび administrators グループのユーザだけが、アプライアンスへのアクセスに secure copy（scp）を使用できます。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」章の「Adding Users」を参照してください。

シリアル接続によるアクセス

シリアル接続を使用してアプライアンスに接続する場合(『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Connecting to the Appliance」を参照)、シリアル ポート コネクタのピン番号については図 B-2、シリアル ポート コネクタのピン割り当てとインターフェイス信号については表 B-2 を参照してください。

図 B-2　　シリアル ポートのピン番号

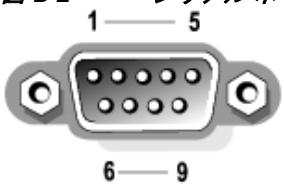


表 B-2　　シリアル ポートのピン割り当て

ピン	信号	I/O	定義
1	DCD	I	データ キャリア検出
2	SIN	I	シリアル入力
3	SOUT	O	シリアル出力
4	DTR	O	データ ターミナル レディ
5	GND	適用対象外	信号用接地
6	DSR	I	データ セット レディ
7	RTS	I	送信要求
8	CTS	O	送信可
9	RI	I	リング インジケータ
Shell	適用対象外	適用対象外	シャーシ アース

INDEX

シンボル

数値

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

め

も

ら

り

る