CHAPTER 5

電子メールを受信するためのゲートウェイの設定

GUI の System Setup Wizard（または CLI の `systemsetup` コマンド）を使用して IronPort アプライアンスの基本的な設定を行うことにより、IronPort 電子メール セキュリティ アプライアンスで電子メールを受信するために設定の調整を開始する準備ができました。ここでは、受信電子メールを処理するためにアプライアンス上でリスナーの設定を開始するときに使用できるすべての機能について詳しく説明します。

Host Access Table（HAT; ホスト アクセス テーブル）の概念について紹介しています。パブリック リスナーの Host Access Table（HAT; ホスト アクセス テーブル）と、その固有の送信者グループおよびメール フロー ポリシーは、メール フロー モニタ機能を可能にするための基礎となるフレームワークです（メール フロー モニタ機能の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」を参照してください）。

この章は、次の内容で構成されています。

- 「GUI によるリスナーの RAT の変更」（P.5-182）

リスナーによる電子メールの受信

IronPort AsyncOS オペレーティング システムを使用すると、IronPort アプライアンスをインバウンド電子メールのゲートウェイとして機能するように使用し、インターネットからの SMTP 接続を使用可能にし、メッセージの許可、適切なシステムへのメッセージの中継を行うことができます。

この構成では、これらの接続を使用可能にするために *リスナー*をイネーブルにします。リスナーは、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 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。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（`systemsetup` コマンドで設定した初期アドレスを含みます）用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。

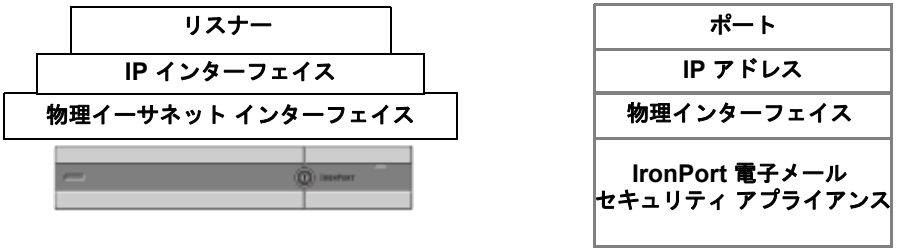
メールが単一の IP アドレス上の複数のポートに配信されるようなメール配信ポリシーの設定はできません（たとえば、通常配信用にポート 25 を設定し、IronPort のスパム検疫用にポート 6025 を設定するなど）。各配信オプションを個別の IP アドレスまたはポート上で実行することを推奨します。さらに、通常の電子メール配信用と検疫配信用には同じホスト名を使用できません。

System Setup Wizard または `systemsetup` コマンド（CLI）は、最初に IronPort アプライアンス上の使用可能な *イーサネット インターフェイス*で動作する *IP インターフェイス*を設定します。IronPort C150 アプライアンスと C160 アプライアンスでは、これらのイーサネット インターフェイスに Data1 および Data2 というラベルが付与されています。その他すべての IronPort アプライアンスでは、Data1、Data2、および Management というラベルが付与されています。これらのインターフェイスは後で [Network] メニューの [IP Interfaces] ページか `interfaceconfig` コマンドを使用して編集できます。GUI の System Setup Wizard（または `systemsetup` コマンド）を完了し、変更内容を確定した場合、すでに少なくとも 1 つのリスナーがアプライアンス上で構成されています（「手順 3：[Network]」（P.3-57）で入力した設定を参照してください）。メールを受信するためのアドレスは、その時点と、最初の SMTP ルート（[Network] > [SMTP Routes] または `smtproutes`）の入力時に入力します。

（注）　System Setup Wizard を使用して新しいリスナーを作成するとき、AsyncOS はデフォルト値でリスナーを作成します。しかし、手動でリスナーを作成する場合、AsyncOS はこれらのデフォルトの SBRS 値を使用しません。

IronPort アプライアンスの使用可能な IP インターフェイス上で動作するリスナーを設定するには、[Listeners] ページ（[Network] > [Listeners]）または `listenerconfig` コマンドを使用します。リスナーの作成と設定の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章を参照してください。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Virtual Gateway™ Technology」では、IronPort Virtual Gateway テクノロジーについて説明しています。このテクノロジーを使用すると、1 つ以上の IP アドレス（IP アドレス グループ）に対して IP インターフェイスをさらに定義してグループ化できます。

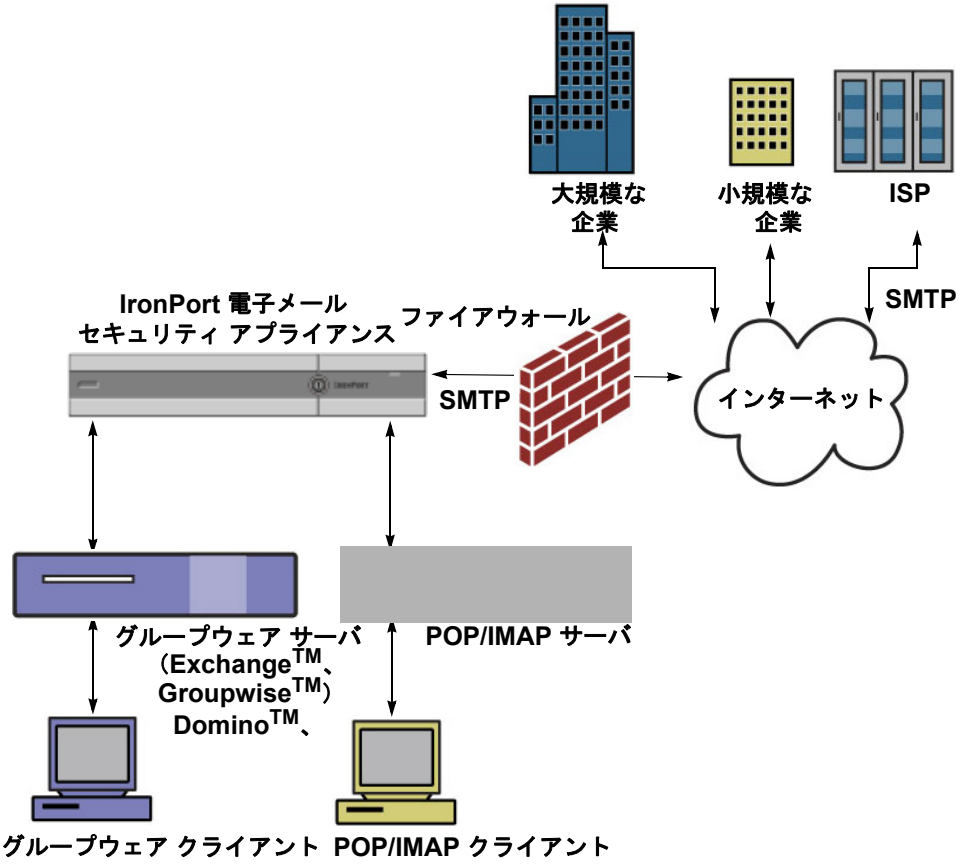
図 5-1　リスナー、IP インターフェイス、物理イーサネット インターフェイスの関係



エンタープライズ ゲートウェイ構成

この構成では、エンタープライズ ゲートウェイ構成はインターネットからの電子メールを許可し、ゲートウェイ サーバ、POP/IMAP サーバ、またはその他の MTA に電子メールを中継します。エンタープライズ ゲートウェイは、それと同時に、グループウェア サーバおよびその他の電子メール サーバからの SMTP メッセージを受け付け、インターネット上の受信者に中継します。

図 5-2　エンタープライズ ゲートウェイとしての IronPort アプライアンスの使用



この構成では、少なくとも次の 2 つのリスナーが必要です。

- インターネットからのメールを受け付けるために専用に設定されたリスナー
- 内部のグループウェアおよび電子メール サーバ（POP/IMAP）からのメールを受け付けるために専用に設定されたリスナー

パブリック リスナーとプライベート リスナー

最初のリスナーを「パブリック リスナー」、2 番めのリスナーを「プライベート リスナー」と考えます。IronPort AsyncOS は、デフォルトでインターネットから電子メールを受信する特性を持つパブリック リスナーと、内部（グループウェア、POP/IMAP などのメッセージ生成）システムからだけの電子メールの

受け入れを目的としたプライベート リスナーを区別します。パブリック リスナーとプライベート リスナーは、デフォルトでは、利用できる機能やデフォルト設定が異なっています。異なるパブリック ネットワークとプライベート ネットワーク用に個別のパブリック リスナーとプライベート リスナーを作成することで、セキュリティ、ポリシー強制、レポーティング、管理用に電子メールを区別できます。たとえば、パブリック リスナーで受信した電子メールは、デフォルトでは設定されたアンチスパム エンジンとアンチウイルス スキャン エンジンでスキャンされますが、プライベート リスナーで受信した電子メールはスキャンされません。リスナーがある同じ図を図 3-3 に示します。

図 5-3　エンタープライズ ゲートウェイ用のパブリックおよびプライベート リスナー

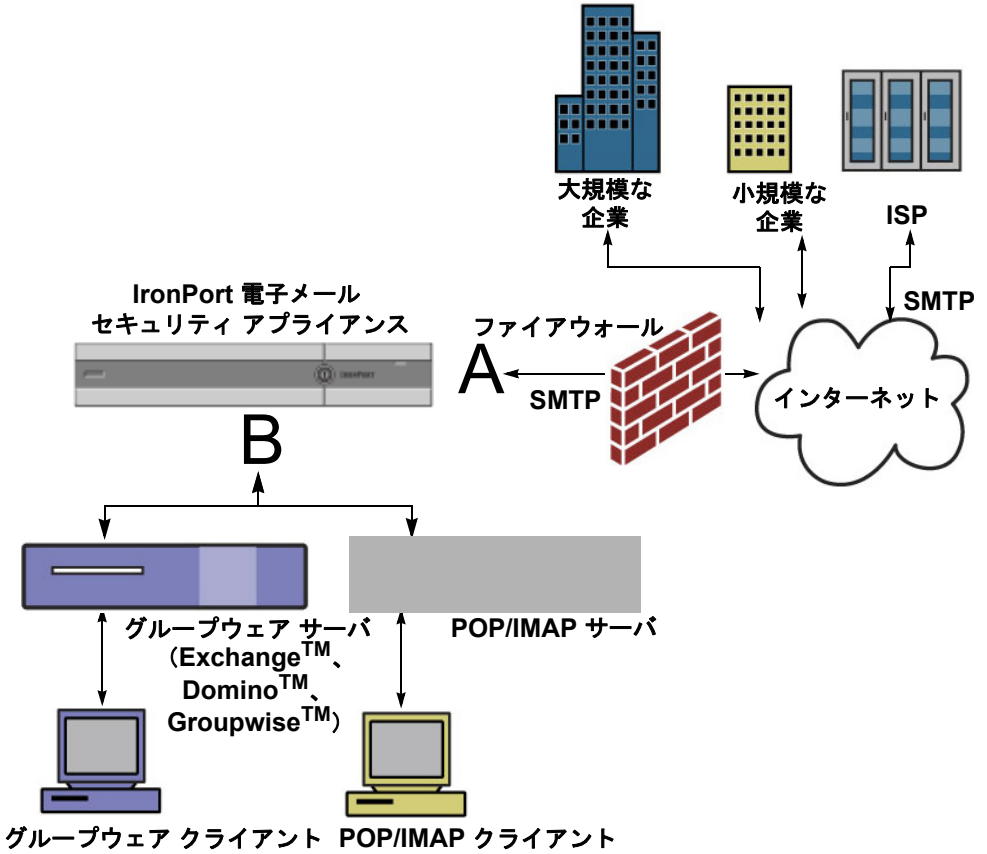


図 3-3 で、1 つのパブリック リスナー（A）と 1 つのプライベート リスナー（B）が、このエンタープライズ ゲートウェイ構成のアプライアンス上で構成されています。

さらに図 3-4 は、パブリック リスナーとプライベート リスナーのデフォルト設定の違いを示しています。パブリック リスナーは、インターネットからの電子メールを受信することを意図しています。パブリック リスナーは*多数*のホストからの接続を受信し、*限られた*数の受信者にメッセージを渡します。これとは逆に、プライベート リスナーは、内部ネットワークからの電子メールを受信することを意図しています。プライベート リスナーは限られた（既知の）数のホストからの接続を受信し、メッセージを*多数*の受信者に渡します。

C150/160 カスタマー：System Setup Wizard では、デフォルトで、インターネットからの電子メールの受信と内部ネットワークからの電子メールの中継の両方を行うための、1 つのパブリック リスナーを順を追って設定します。つまり、1 つのリスナーが両方の機能を実行できます。

それぞれの種類のリスナーの、ホスト アクセス テーブルと受信者アクセス テーブルでの違いについては後述します。

図 5-4　　パブリック リスナーとプライベート リスナー

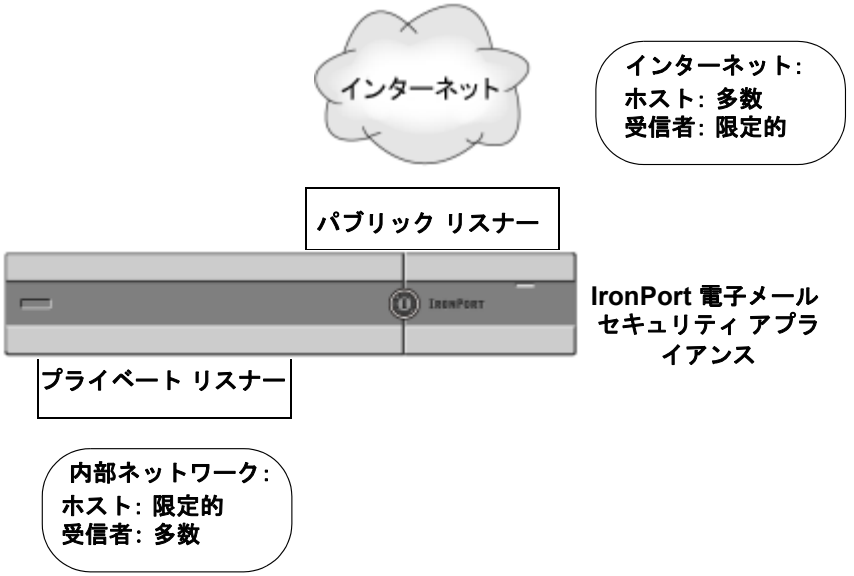
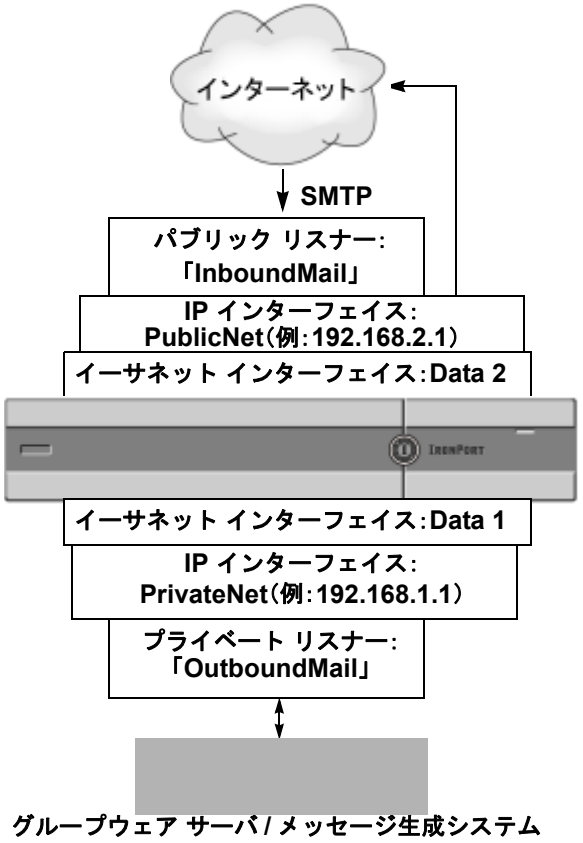


図 5-5 に、IronPort X1000/1050/1060, C60/600/650/660、および C30/300/350/360 アプライアンス上で System Setup Wizard（または CLI の `systemsetup` コマンド）によって作成される一般的な電子メール ゲートウェイ構成を示します。2 つのリスナーが作成されます。あるインターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図 5-6 に、IronPort C150/160 アプライアンス上で System Setup Wizard（または CLI の `systemsetup` コマンド）によって作成される一般的な電子メール ゲートウェイ構成を示します。1 つの IP インターフェイス上の 1 つのパブリック リスナーが、インバウンド接続とアウトバウンド接続の両方を使用可能にするために作成されます。

図 5-5　X1000/1050/1060、C60/600/650/660、C30/300/350/360 アプライアンス上のパブリック リスナーとプライベート リスナー



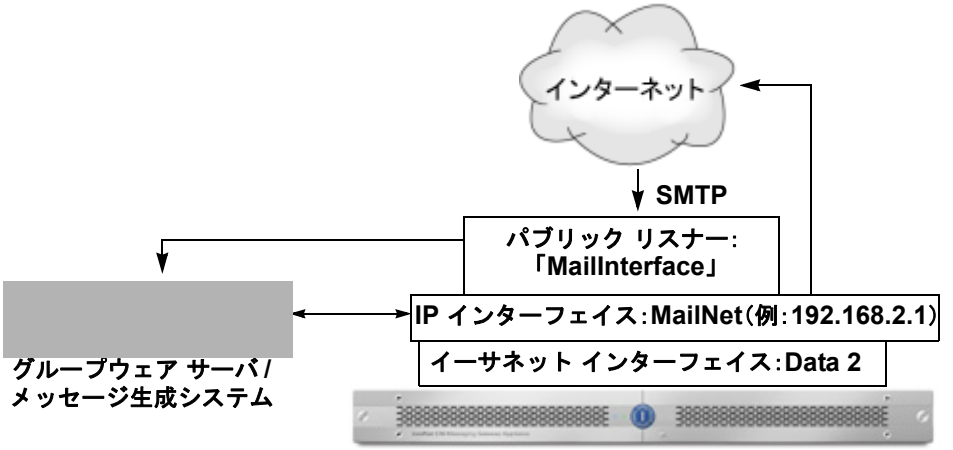
（注）　このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信します。
IP インターフェイス PublicNet は、インターネット上の宛先ホストにメッセージを送信します。

IronPort 電子メール セキュリティ アプライアンス

IP インターフェイス PrivateNet は、内部のメール ホストにメッセージを送信します。

（注）　このプライベート リスナーは、Data1 イーサネット インターフェイス上の PrivateNet IP インターフェイスのポート 25 上で SMTP プロトコルを使用し、`.example.com` ドメイン内の内部システムからメッセージを受信します。

図 5-6　C150 アプライアンス上のパブリック リスナー



（注）　このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信し、.example.com ドメイン内の内部システムからのメッセージを中継します。
IP インターフェイス MailNet は、インターネット上の宛先ホストと内部のメール ホストにメッセージを送信します。

ホスト アクセス テーブル（HAT）: 送信者グループとメール フロー ポリシー

アプライアンス上で設定されている各リスナーには、それが受信するメッセージの動作を変更するために設定可能なプロパティがあります。「概要：電子メール パイプライン」（P.4-91）で説明したように、リスナーの動作に影響を与える最初の構成可能な機能の 1 つが Host Access Table（HAT; ホスト アクセス テーブル）です。

HAT は、リモート ホストからの着信接続を制御するリスナー用のルール セットを保持しています。作成するすべてのリスナーに独自の HAT があります。HAT は、パブリック リスナーとプライベート リスナーの両方に対して定義されます。

HAT 内のエントリは次の基本的な構文によって定義されます。

表 5-1　HAT の基本的な構文

リモート ホスト定義	ルール

*リモート ホスト定義*は、リスナーに定義しようとするリモート ホストを（たとえば単一の IP アドレスで）定義する方法です。

*ルール*は、指定したリモート ホストがリスナーに接続できるかどうかを指定します。

AsyncOS の HAT では、基本構文を拡張し、複数のリモート ホスト定義に名前を付けたものを作成できます。これを*送信者グループ*と呼びます。複数のアクセス ルールとパラメータ セットを組み合わせて名前を付けたものを、*メール フロー ポリシー*と呼びます。この拡張された構文を表 5-2 に示します。

表 5-2　HAT の高度な構文

送信者グループ：	メール フロー ポリシー：
リモート ホスト	アクセス ルール + パラメータ
リモート ホスト	
リモート ホスト	
...	

ルールが HAT に現れる順序は重要です。リスナーに接続しようとする各ホストについて、HAT が上から下に向かって読み込まれます。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

HAT に格納する定義済みエントリとカスタム エントリは、最後のホスト エントリである「ALL」の上に入力します。

デフォルト HAT エントリ

作成するすべてのパブリック リスナーについて、デフォルトでは、*すべてのホストからの電子メールを許可する*ように HAT が設定されます。作成するすべてのプライベート リスナーについて、デフォルトでは、指定したホストからの電子メールを中継し、その他すべてのホストを拒否するように HAT が設定されます。

（注） 指定したホスト以外のすべてのホストを拒否することで、`listenerconfig` コマンドと `systemsetup` コマンドでは、意図せずシステムを「オープン リレー」として設定することが防止されます。オープン リレー（「セキュアでないリレー」または「サード パーティ」リレーとも呼びます）は、第三者による電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープン リレーがあると、ローカル ユーザ向けでもローカル ユーザからでもない電子メールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。

メール フロー ポリシー：アクセス ルールとパラメータ

HAT のメール フロー ポリシーを使用すると、リスナーがリモート ホストからメールを受信する速度を制御または制限できます。また、SMTP カンバセーションの間でやりとりされる SMTP コードと応答も変更できます。

HAT には、リモート ホストからの接続に作用する次の 4 つの基本的なアクセス ルールがあります。

ステップ 1　`ACCEPT`

接続が許可された後、電子メールの許可がさらに受信者アクセス テーブル（パブリック リスナーの場合）などのリスナーの設定によって制限されます。

ステップ 2　`REJECT`

接続は最初に許可されますが、接続しようとしているクライアントに 4XX または 5XX のグリーティングが送信されます。電子メールは許可されません。

（注） SMTP カンバセーションの開始時ではなく、メッセージ受信レベル（RCPT TO）でこの拒否を実行するように AsyncOS を設定することもできます。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。この設定は、CLI の `listenerconfig --> setup` コマンドで設定します。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。

ステップ 3　`TCPREFUSE`

接続は TCP レベルで拒否されます。

ステップ 4　`RELAY`

接続は受け付けられます。すべての受信者について受信が許可され、受信者アクセス テーブルで制約されません。

- `CONTINUE`

  HAT 内のマッピングが無視され、HAT の処理が継続されます。着信接続が、CONTINUE でない後続のエントリに一致する場合、代わりにそのエントリが使用されます。CONTINUE ルールは、Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）で HAT を容易に編集できるようにするために使用します。詳細については、「新しい送信者グループの追加」（P.5-149）を参照してください。

これらの基本的なアクセス コントロール パラメータに加え、作成するリスナーで次のパラメータを使用できます。アクセス ルール（ACCEPT または REJECT）と組み合わされたパラメータは、*メール フロー ポリシー*と呼ばれます。メール フロー ポリシーは、HAT パラメータのグループ（アクセス ルールの後に、接続パラメータ、レート制限パラメータ、カスタム SMTP コードと応答、およびアンチスパム、アンチウイルス、暗号化、認証パラメータを続けたもの）を表現するための 1 つの方法です。

その後メール フロー ポリシーは、リスナーの HAT 内のエントリとして送信者グループにマップされます。

表 5-3　HAT メール フロー ポリシー パラメータ

パラメータ	説明
[Connections]	
[Maximum message size]	このリスナーで許可されるメッセージの最大サイズ。最大メッセージ サイズの最小値は 1 KB です。
[Maximum concurrent connections from a single IP]	単一の IP アドレスからこのリスナーに接続することが許可される最大同時接続数。
[Maximum messages per connection]	リモート ホストからの接続に対して、このリスナーを通じて送信できる最大メッセージ数。
[Maximum recipients per message]	このホストからのメッセージに対して許可される最大受信者数。
[SMTP Banner]	
[Custom SMTP Banner Code]	このリスナーとの接続が確立されたときに返される SMTP コード。
[Custom SMTP Banner Text]	このリスナーとの接続が確立されたときに返される SMTP バナー テキスト。
[Custom SMTP Reject Banner Code]	このリスナーにより接続が拒否されたときに返される SMTP コード。
[Custom SMTP Reject Banner Text]	このリスナーにより接続が拒否されたときに返される SMTP バナー テキスト。
[Override SMTP Banner Host Name]	デフォルトでは、SMTP バナーをリモート ホストに表示するときに、リスナーのインターフェイスに関連付けられているホスト名が含められます（たとえば、`220- hostname ESMTP`）。ここに異なるホスト名を入力することで、このバナーを変更できます。また、ホスト名フィールドを空白のままにすることで、ホスト名をバナーに表示*しない*こともできます。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
[Rate Limiting]	
[Rate Limiting: Maximum Recipients per Hour]	このリスナーが 1 台のリモート ホストから受信する、時間あたりの最大受信者数。送信者 IP アドレスあたりの受信者の数は、グローバルに追跡されます。リスナーごとに独自のレート制限しきい値が追跡されますが、すべてのリスナーが 1 個のカウンタに対して検証を行うため、同じ IP アドレス（送信者）が複数のリスナーに接続している場合、レート制限を超える可能性が高くなります。
[Rate Limiting: Max.recipient per Hour Exceeded Error Code]	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP コード。
[Rate Limiting: Max.Recipients Per Hour Exceeded Error Text]	ホストが、このリスナーに対して定義されている時間あたりの最大受信者数を超えた場合に返される SMTP バナー テキスト。
[Flow Control]	
[Use SenderBase for Flow Control]	このリスナーの IronPort SenderBase 評価サービスへの「ルックアップ」をイネーブルにします。
[Group by Similarity of IP Addresses:]（有効ビット範囲 0 ～ 32）	リスナーの Host Access Table（HAT; ホスト アクセス テーブル）内のエントリを大規模な CIDR ブロックで管理しつつ、IP アドレスごとに着信メールを追跡およびレート制限するために使用します。レート制限のために類似の IP アドレスをグループ化するための有効ビットの範囲（0 ～ 32）を定義しつつ、その範囲内の IP アドレスごとに個別のカウンタを保持します。「Use SenderBase」をディセーブルにする必要があります。HAT の有効ビットの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「HAT Significant Bits Feature」を参照してください。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
[Directory Harvest Attack Prevention (DHAP)]	
[Directory Harvest Attack Prevention: Maximum Invalid Recipients Per Hour]	このリスナーが 1 台のリモート ホストから受信する、時間あたりの最大の無効な受信者数。このしきい値は、RAT 拒否の総数と、SMTP カンバセーションでドロップされたか、ワーク キューでバウンスされた無効な LDAP 受信者へのメッセージの総数を合計したものを表します（関連付けられているリスナーの LDAP 許可設定で設定します）。LDAP 許可クエリーの DHAP の設定の詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。
[Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation]	IronPort アプライアンスは、無効な受信者のしきい値に達するとホストへの接続をドロップします。
[Max.Invalid 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。
[Max.Invalid 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。
[Drop Connection if DHAP threshold is reached within an SMTP Conversation]	SMTP カンバセーション中に DHAP しきい値に達した場合の接続のドロップをイネーブルにします。
[Max.Invalid Recipients Per Hour Code]	SMTP カンバセーション中の DHAP により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。
[Max.Invalid Recipients Per Hour Text:]	SMTP カンバセーション中の DHAP により接続をドロップするときに使用するテキストを指定します。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
[Spam Detection]	
[Anti-spam scanning]	このリスナー上でアンチスパム スキャンをイネーブルにします。
[Virus Detection]	
[Anti-virus scanning]	このリスナー上でアンチウイルス スキャンをイネーブルにします。
[Encryption and Authentication]	
[Allow TLS Connections]	このリスナーの SMTP カンバセーションで、Transport Layer Security（TLS）を拒否、優先、または義務付けします。
[SMTP Authentication]	リスナーに接続するリモート ホストからの SMTP 認証を許可、禁止、義務付けます。SMTP 認証については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。
[If Both TLS and SMTP Authentication are enabled:]	TLS に SMTP 認証を提供するよう義務付けます。
[Domain Key Signing]	
[Domain Key/ DKIM Signing]	このリスナーで DomainKeys または DKIM 署名をイネーブルにします（ACCEPT および RELAY のみ）。
[DKIM Verification]	DKIM 検証をイネーブルにします。
[SPF/SIDF Verification]	
[Enable SPF/SIDF Verification]	このリスナーで SPF/SIDF 署名をイネーブルにします。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Email Authentication」の章を参照してください。
[Conformance Level]	SPF/SIDF 準拠レベルを設定します。[SPF]、[SIDF]、[SIDF Compatible] のいずれかを選択します。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Email Authentication」の章を参照してください。

表 5-3　HAT メール フロー ポリシー パラメータ（続き）

パラメータ	説明
[Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:]	準拠レベルとして [SIDF Compatible] を選択した場合、メッセージ中に Resent-Sender: ヘッダーまたは Resent-From: ヘッダーが存在する場合に、PRA Identity 検証の結果 Pass を None にダウングレードするかどうかを設定します。このオプションはセキュリティ目的で選択します。
[HELO Test]	HELO ID に対してテストを実行するかどうかを設定します（[SPF] および [SIDF Compatible] 準拠レベルで使用します）。
[Untagged Bounces]	
[Consider Untagged Bounces to be Valid]	バウンス検証タギング（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章を参照）がイネーブルの場合にのみ適用されます。デフォルトでは、アプライアンスはタグのないバウンスを無効と見なし、バウンス検証の設定に応じて、バウンスを拒否するか、カスタム ヘッダーを追加します。タグ付きでないバウンスを有効と見なす場合、アプライアンスはバウンス メッセージを受け付けます。
[Envelope Sender DNS Verification]	
	「送信者検証」（P.5-161）を参照してください。
[Exception Table]	
[Use Exception Table]	送信者検証ドメイン例外テーブルを使用します。例外テーブルは 1 つしか使用できませんが、メール フロー ポリシーごとにイネーブルにできます。詳細については、「送信者検証例外テーブル」（P.5-165）を参照してください。

デフォルトでは、これらのパラメータは、アプライアンス上の各リスナーについて、表 5-5 および表 5-6 に示すデフォルト値に設定されます。

（注）　アンチスパムまたはアンチウイルス スキャンが HAT でグローバルにイネーブルになっている場合、メッセージが IronPort アプライアンスによって許可されるときに、アンチスパムまたはアンチウイルス スキャン用にフラグ設定されます。

メッセージを許可した後にアンチスパムまたはアンチウイルス スキャンがディセーブルにされた場合、メッセージは、ワーク キューを出るときに引き続きスキャン対象になります。

HAT 変数の構文

表 5-4 では、メール フロー ポリシーに対して定義されるカスタム SMTP およびレート制限バナーと組み合わせることでも使用できる変数のセットを定義します。変数名の大文字と小文字は区別されません（つまり、$group と $Group は同じです）。

表 5-4　HAT 変数の構文

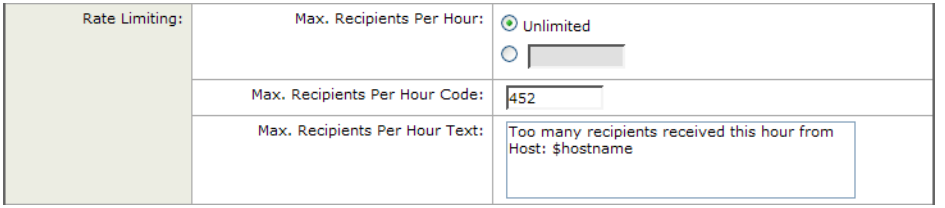
変数	定義
$Group	HAT 内の一致した送信者グループの名前で置き換えられます。送信者グループに名前がない場合、「None」が表示されます。
$Hostname	IronPort アプライアンスによって検証された場合にのみ、リモート ホスト名で置き換えられます。IP アドレスの逆引き DNS ルックアップが成功したもののホスト名が返されない場合、「None」が表示されます。逆引き DNS ルックアップが失敗した場合（DNS サーバに到達できない場合や、DNS サーバが設定されていない場合）、「Unknown」が表示されます。
$OrgID	SenderBase 組織 ID（整数値）で置き換えられます。 IronPort アプライアンスが SenderBase 組織 ID を取得できないか、SenderBase 評価サービスが値を返さなかった場合、「None」が表示されます。
$RemoteIP	リモート クライアントの IP アドレスで置き換えられます。
$HATEntry	リモート クライアントが一致した HAT のエントリで置き換えられます。

HAT 変数の使用

（注） これらの変数は、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の表 1-3 に示されている高度な HAT パラメータ smtp_banner_text および max_rcpts_per_hour_text とともに使用できます。

これらの変数を使用し、$TRUSTED ポリシー内で許可された接続のカスタム SMTP バナー応答テキストを GUI で編集できます。

図 5-7　HAT 変数の使用



または、CLI で次のように入力します。

```
Would you like to specify a custom SMTP response?  [Y]> y


Enter the SMTP code to use in the response. 220 is the standard code.

[220]> 200


Enter your custom SMTP response.  Press Enter on a blank line to finish.

You've connected from the hostname: $Hostname, IP address of: $RemoteIP,
matched the group: $Group, $HATEntry and the SenderBase Organization:
$OrgID.
```

HAT 変数のテスト

これらの変数をテストするには、既知の信頼できるマシンの IP アドレスを、IronPort アプライアンス上のリスナーの $WHITELIST 送信者グループに追加します。その後、そのマシンから telnet で接続します。SMTP 応答中で変数の置き換えを確認できます。次の例を参考にしてください。

```
# telnet IP_address_of_IronPort_Appliance

220 hostname ESMTP

200 You've connected from the hostname: hostname, IP address of:
IP-address_of_connecting_machine, matched the group: WHITELIST, 10.1.1.1
the SenderBase Organization: OrgID.
```

デフォルト メール フロー ポリシーの参照

図 5-8 に、パブリック リスナーのデフォルト ポリシー パラメータを示します。

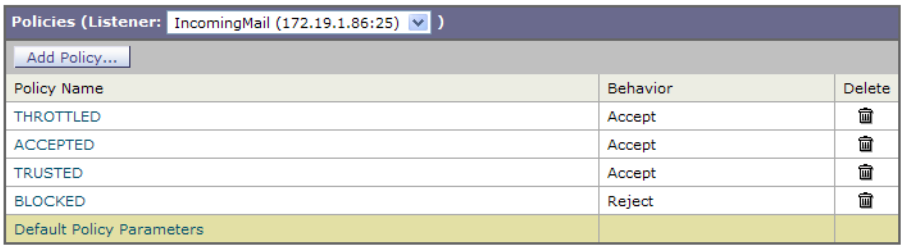
リスナーのデフォルト ポリシー パラメータを表示するには、次の手順を実行します。

ステップ 1　GUI にアクセスします（「GUI へのアクセス」（P.2-19）を参照）。

ステップ 2　[Mail Policies] > [Mail Flow Policies] の順にクリックします。

[Mail Flow Policies] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されているメール フロー ポリシーが表示されます。

図 5-8　[Mail Flow Policies] ページ



ステップ 3　[Default Policy Parameters] リンクをクリックします。

[Default Policy Parameters] ページが表示されます。図 5-9 を参照してください。

図 5-9　パブリック リスナーのデフォルト ポリシー パラメータ（1/2）

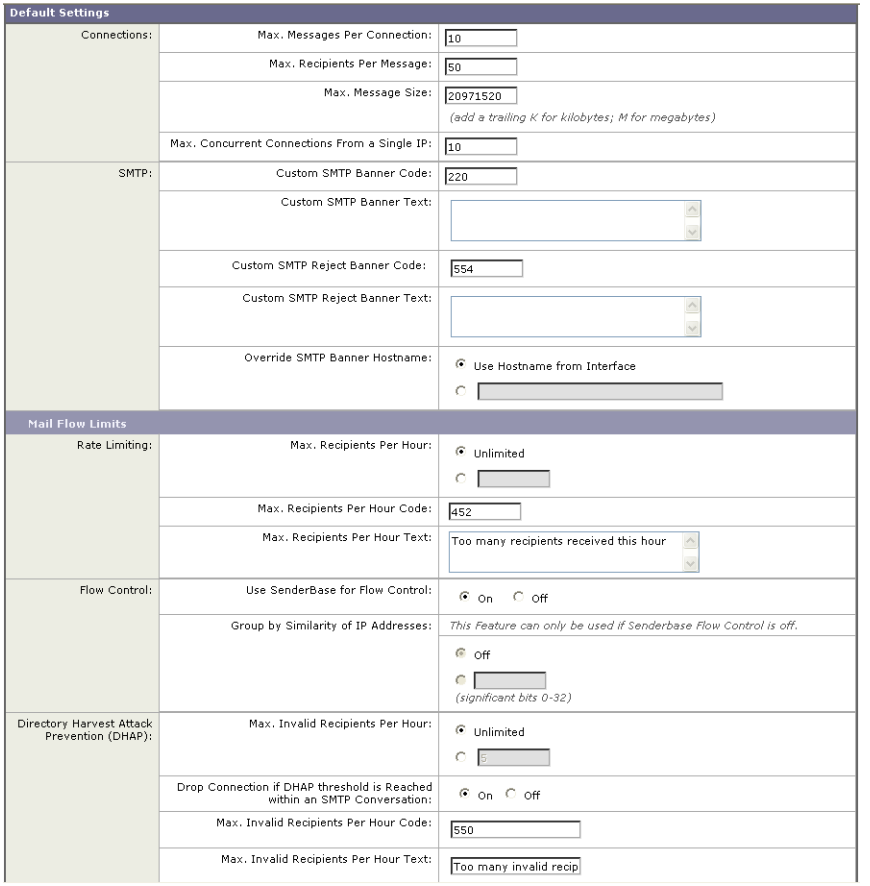
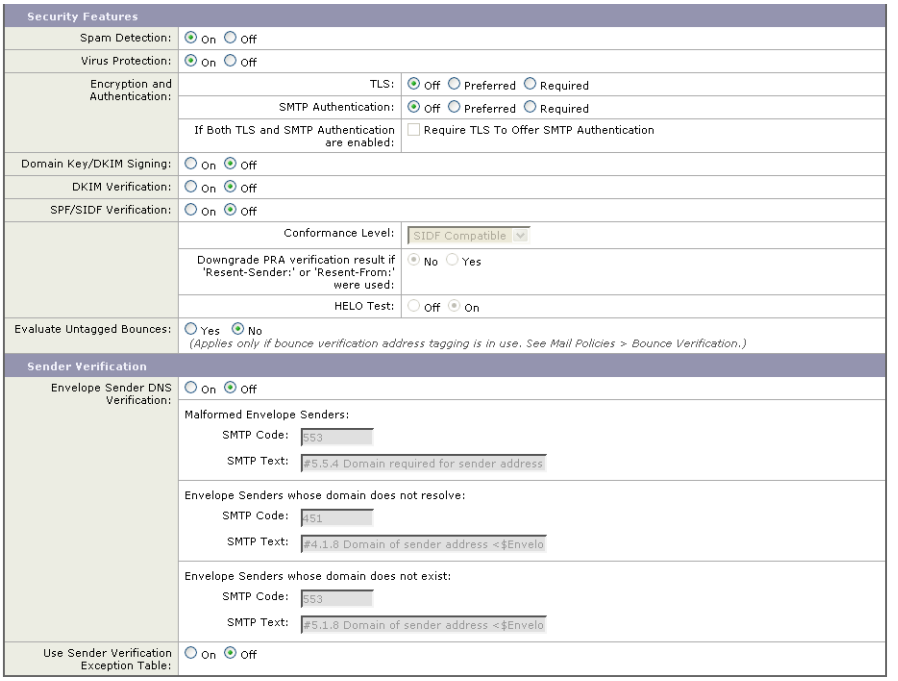


図 5-10　パブリック リスナーのデフォルト ポリシー パラメータ（2/2）



リスナーのデフォルト ポリシー パラメータ

次の表に、パブリック リスナーのデフォルト パラメータの一覧を示します。

表 5-5　パブリック リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
[Maximum message size:]	20 MB
[Max.concurrent connections allowed to this listener:]	10 接続
[Maximum messages per connection:]	10 メッセージ
[Maximum recipients per message:]	50 受信者
[SMTP Banner Code:]	220
[SMTP Banner Text:]	「*hostname* ESMTP」
[SMTP Reject Banner Code:]	554
[SMTP Reject Banner Text:]	「Access Denied」

表 5-5　パブリック リスナーの HAT デフォルト ポリシー パラメータ（続き）

パラメータ	デフォルト値
[Override SMTP Banner Hostname]	Use hostname from Interface
[Rate Limiting: Maximum Recipients per Hour:]	デフォルトなし。ユーザ定義。
[Rate Limiting: Limit Exceeded Error Code:]	452
[Rate Limiting: Limit Exceeded Error Text:]	「Too many recipients received this hour」
[Directory Harvest Attack Prevention]	OFF
[Use SenderBase:]	ON
[Group by Similarity of IP address:]	OFF
[Use anti-spam scanning:]	ON（アンチスパムがイネーブルな場合）
[Use anti-virus scanning:]	ON（アンチウイルスがイネーブルな場合）
[Allow TLS Connections:]	NO
[Override Hostname]	NO
[SMTP Auth]	OFF
[Domainkey/DKIM Signing]	OFF
[DKIM Verification]	OFF
[SPF/SIDF Verification]	OFF
[Envelope Sender DNS Verification]	OFF
[Use Exception Table]	OFF

次の表に、プライベート リスナーのデフォルト パラメータの一覧を示します。

表 5-6　プライベート リスナーの HAT デフォルト ポリシー パラメータ

パラメータ	デフォルト値
[Maximum messages per connection:]	10,000 メッセージ
[Maximum recipients per message:]	100,000 受信者
[Maximum message size:]	100 MB（104857600 バイト）
[Max.concurrent connections from a single IP]	50 接続
[SMTP Banner Code:]	220
[SMTP Banner Text:]	「*hostname* ESMTP」
[SMTP Reject Banner Code:]	554
[SMTP Reject Banner Text:]	「Access Denied」
[Override SMTP Banner Hostname]	Use hostname from Interface
[Rate Limiting: Maximum Recipients per Hour:]	Unlimited
[Rate Limiting: Limit Exceeded Error Code:]	N/A
[Rate Limiting: Limit Exceeded Error Text:]	N/A
[Use SenderBase:]	OFF
[Group by Similarity of IP address:]	OFF
[Directory Harvest Attack Prevention]	OFF
[Use anti-spam scanning:]	OFF（アンチスパムがイネーブルな場合）
[Use anti-virus scanning:]	ON（アンチウイルスがイネーブルな場合）
[Allow TLS Connections:]	NO
[Override Hostname]	NO
[SMTP Auth]	OFF
[Domainkeys/DKIM Signing]	OFF

表 5-6　プライベート リスナーの HAT デフォルト ポリシー パラメータ（続き）

パラメータ	デフォルト値
[DKIM Verification]	OFF
[SPF/SIDF Verification]	OFF
[Accept Untagged Bounces]	NO
[Envelope Sender DNS Verification]	OFF
[Use Exception Table]	OFF

送信者グループ

HAT パラメータをアクセス ルールと組み合わせることで、メール フロー ポリシーが作成されます（図 5-6「メール フロー ポリシー：アクセス ルールとパラメータ」（P.5-117）を参照）。異なる HAT パラメータをグループ化して名前を割り当てると、送信者のグループに適用できるメール フロー ポリシーが定義されます。

*送信者グループ*は、単に、複数の送信者からの電子メールを同じ方法で扱う（つまり、送信者のグループにメール フロー ポリシーを適用する）ために集められた送信者のリストです。送信者グループは、次のもので識別される送信者のリストです。

- IP アドレス
- IP 範囲
- 具体的なホスト名またはドメイン名
- SenderBase 評価サービスの「組織」分類
- SenderBase Reputation Score（SBRS; SenderBase 評価スコア）の範囲（またはスコアの欠如）
- DNS リスト クエリー応答

送信者グループを構成するリモート ホスト（送信者エントリ）を定義するための構文については、表 5-7 を参照してください。これらの送信者エントリは、リスナーの HAT 内でカンマで区切られます。メール フロー ポリシーと同様に、送信者グループに名前を割り当てます。

送信者グループおよびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。IronPort アプライアンスでは、デフォルトで、「パブリック リスナー向けの定義済みのメール フロー ポリシー」（P.5-139）に示すメール フロー ポリシーと送信者グループがあらかじめ定義されています。

第 6 章「電子メール セキュリティ マネージャ」では、定義済みの送信者グループとメール フロー ポリシーを使用して、ゲートウェイを通過するメールをすばやく高性能に分類し、リスナーの HAT に対するリアルタイムな変更を行うことができます。

（注）　二重 DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS（A）ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しない場合、または A レコードが存在しない場合は、システムは IP アドレスのみを使用して HAT 内のエントリと照合します。

送信者グループの構文

表 5-7　HAT 内でのリモート ホストの定義：送信者グループの構文

構文	意味
n.n.n.n	フル（完全な）IP アドレス
n.n.n. n.n.n n.n. n.n n. n	部分的な IP アドレス

表 5-7　HAT 内でのリモート ホストの定義：送信者グループの構文（続き）

構文	意味
n.n.n.n-n n.n.n-n. n.n.n-n n.n-n. n.n-n n-n. n-n	IP アドレスの範囲
yourhost.example.com	完全修飾ドメイン名
.partialhost	部分ホスト ドメイン内のすべてのもの
n/c n.n/c n.n.n/c n.n.n.n/c	CIDR アドレス ブロック
SBRS[n:n] SBRS[none]	SenderBase 評価スコア。詳細については、「SenderBase 評価スコアによって定義された送信者グループ」（P.5-136）を参照してください。
SBO:n	SenderBase ネットワーク オーナー識別番号。詳細については、「SenderBase 評価スコアによって定義された送信者グループ」（P.5-136）を参照してください。
dnslist[dnsserver.domain]	DNS リスト クエリー。詳細については、「HAT 内の DNS リストにクエリーを実行することで定義された送信者グループ」（P.5-138）を参照してください。
ALL	すべてのアドレスに一致する特殊なキーワード。これは、すべての送信者グループのみに適用され、常に含まれます（ただしリストされません）。

ネットワーク オーナー、ドメイン、IP アドレスで定義される送信者グループ

SMTP プロトコルには電子メールの送信者を認証するための方法が組み込まれていないため、大量の迷惑メールの送信者は、その身元を隠すためのいくつかの戦略を採用することに成功してきました。たとえば、メッセージのエンベロープ

送信者アドレスのスプーフィング、偽造した HELO アドレスの使用、単なる異なるドメイン名のローテーションなどがあります。これにより、多数のメール管理者は、「この大量の電子メールは誰が送信しているのか」という基本的な質問を自問することになります。この質問に答えるために、SenderBase 評価サービスは、接続元ホストの IP アドレスに基づいて身元ベースの情報を集約するための固有の階層を開発してきました。IP アドレスは、メッセージ中で偽造することがほとんど不可能な情報の 1 つです。

IP Address は、送信元メール ホストの IP アドレスとして定義します。

Domain は、指定した第 2 レベル ドメイン名（たとえば yahoo.com）を持つホスト名を使用するエンティティとして定義され、IP アドレスに対する逆引き（PTR）ルックアップによって決定されます。

Network Owner は、IP アドレスのブロックを管理するエンティティ（通常は会社）として定義され、American Registry for Internet Numbers（ARIN）などのグローバル レジストリやその他のソースからの IP アドレス空間の割り当てに基づいて決定されます。

Organization は、ネットワーク オーナーの IP ブロック内のメール ゲートウェイの特定のグループを最も詳細に管理するエンティティとして定義され、SenderBase によって決定されます。Organization は Network Owner、Network Owner 内の部門、その Network Owner の顧客のいずれかになります。

HAT に基づくポリシーの設定

表 5-8 に、ネットワーク オーナーと組織の例をいくつか示します。

表 5-8　ネットワーク オーナーと組織の例

例の種類	ネットワーク オーナー	組織
ネットワーク サービス プロバイダー	Level 3 Communications	Macromedia Inc. AllOutDeals.com GreatOffers.com
電子メール サービス プロバイダー	GE	GE Appliances GE Capital GE Mortgage
商用送信者	The Motley Fool	The Motley Fool

ネットワーク オーナーの規模にはかなりの幅があるため、メール フロー ポリシーの基にする適切なエンティティは組織です。SenderBase 評価サービスは、電子メールの送信元について組織レベルまで独自に理解しており、IronPort アプライアンスはそれを利用して、組織に基づいてポリシーを自動的に適用します。上の例で、ユーザが Host Access Table（HAT; ホスト アクセス テーブル）で「Level 3 Communications」を送信者グループとして指定した場合、SenderBase はそのネットワーク オーナーによって管理される個別の組織に基づいてポリシーを適用します。

たとえば、上記の表 3-7 で、ユーザが Level 3 に対して時間あたりの受信者数の制限を 10 と入力した場合、IronPort アプライアンスは、Macromedia Inc.、Alloutdeals.com、*および*Greatoffers.com に対して最大 10 個の受信者を許可します（Level 3 ネットワーク オーナーに対しては時間あたり合計 30 個の受信者になります）。このアプローチの利点は、これらの組織のいずれかがスパムを送信し始めても、Level 3 によって管理されているその他の組織には影響がないことです。これを、ネットワーク オーナー「The Motley Fool」の例と対比します。ユーザがレート制限を時間あたり 10 個の受信者に設定した場合、ネットワーク オーナー Motley Fool の合計の制限は、時間あたり 10 個の受信者になります。

IronPort メール フロー モニタ機能は、送信者を定義する方法の 1 つであり、送信者に関するメール フロー ポリシーの決定を作成するためのモニタリング ツールとなります。特定の送信者に関するメール フロー ポリシーの決定を作成するには、次のことを質問します。

ステップ 1　この送信者によって、どの IP アドレスが制御されているか。

インバウンド電子メールの処理を制御するためのメール フロー モニタ機能が使用する最初の情報が、この質問に対する答えになります。この答えは、SenderBase 評価サービスにクエリーを実行することで得られます。SenderBase 評価サービスは、送信者の相対的な規模に関する情報を提供します（SenderBase ネットワーク オーナーまたは SenderBase 組織）。この質問に答えるにあたり、次のことが仮定されます。

- 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。

ステップ 2　その規模に応じて、この送信者に接続数を全体でいくつ割り当てるべきか。

- 大規模な組織は、より多くの IP アドレスを管理し、より厳格な電子メールを送信する傾向があります。そのため、アプライアンスへの接続をより多く割り当てる必要があります。

– 多くの場合、大量の電子メールの送信元は、ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業、迷惑メールの送信元です。ISP、NSP、アウトソーシングされた電子メールの配信を管理する企業は、多数の IP アドレスを管理する組織の例であり、アプライアンスへの接続をより多く割り当てる必要があります。通常、迷惑メールの送信者は、多数の IP アドレスを管理せず、少数の IP アドレスを通じて大量のメールを送信します。このような送信者には、アプライアンスへの接続をより少なく割り当てる必要があります。

メール フロー モニタ機能は、SenderBase ネットワーク オーナーと SenderBase 組織の差別化を使用して、SenderBase 内のロジックに基づき、送信者あたりに接続を割り当てる方法を決定します。メール フロー モニタ機能の使用方法の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」の章を参照してください。

SenderBase 評価スコアによって定義された送信者グループ

IronPort アプライアンスは、SenderBase 評価サービスに対してクエリーを実行して、送信者の評価スコア（SBRS）を特定できます。SBRS は、SenderBase 評価サービスからの情報に基づき、IP アドレス、ドメイン、または組織に割り当てられた数値です。スコアの範囲は、表 5-9 に示すように、-10.0 ～ +10.0 です。

表 5-9　SenderBase 評価スコアの定義

スコア	意味
-10.0	スパムの送信元である可能性が最も高い
0	中間か、または推奨を行うための十分な情報がない
+10.0	信頼できる送信者である可能性が最も高い
なし	この送信者のデータがない（一般にスパムの送信元）

SBRS を使用して、信頼性に基づいてメール フロー ポリシーを送信者に適用するように IronPort アプライアンスを設定します。たとえば、スコアが -7.5 未満のすべての送信者を拒否することが考えられます。これは、GUI を使用して実現するのが最も簡単です。「SenderBase 評価スコアを使用した送信者グループの作成」（P.5-155）を参照してください。エクスポートした HAT をテキスト ファ

イルで編集する場合、SenderBase 評価スコアを含めるための構文については表 5-10 を参照してください。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照してください。

表 5-10　HAT 内の SenderBase 評価スコアの構文

`SBRS[`*n*`:`*n*`]`	SenderBase 評価スコア。送信者は、SenderBase 評価サービスにクエリーを実行することで識別され、スコアは範囲内で定義されます。
SBRS[none]	SBRS がないことを指定します（非常に新しいドメインには、まだ SenderBase 評価スコアがない場合があります）。

（注） GUI を通じて HAT に追加されるネットワーク オーナーは、`SBO:`*n* という構文を使用します。ここで *n* は、SenderBase 評価サービス内のネットワーク オーナーの一意の識別番号です。

SenderBase 評価サービスにクエリーを実行するようにリスナーを設定するには、[Network] > [Listeners] ページを使用するか、CLI で `listenerconfig -> setup` コマンドを使用します。また、アプライアンスが SenderBase 評価サービスにクエリーを実行するときに待つタイムアウト値を定義することもできます。その後、GUI の [Mail Policies] ページの値を使用するか、CLI の `listenerconfig -> edit -> hostaccess` コマンドを使用して、SenderBase 評価サービスに対するルックアップを使用するさまざまなポリシーを設定できます。

（注） また、SenderBase 評価スコアの「しきい値」を指定するメッセージ フィルタを作成し、システムによって処理されたメッセージをさらに操作することもできます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「SenderBase Reputation Rule」、「Bypass Anti-Spam System Action」、および「Bypass Anti-Virus System Action」を参照してください。

HAT 内の DNS リストにクエリーを実行することで定義された送信者グループ

リスナーの HAT では、特定の DNS リスト サーバに対するクエリーに一致するものとして送信者グループを定義することもできます。クエリーは、リモート クライアントの接続時に DNS を通じて実行されます。リモート リストにクエリーを実行する機能は、現在メッセージ フィルタ ルールとしても存在しますが（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「DNS List Rule」を参照）、メッセージの内容全体が受信されるのは一度だけです。

このメカニズムにより、グループ内で、DNS リストにクエリーを実行する送信者を設定し、それに応じてメール フロー ポリシーを調整できます。たとえば、接続を拒否したり、接続元ドメインの振る舞いを制限したりできます。

（注） いくつかの DNS リストは、可変の応答（たとえば「127.0.0.1」、「127.0.0.2」、「127.0.0.3」）を使用して、クエリー対象の IP アドレスに関するさまざまな事実を示すことができます。メッセージ フィルタ DNS リスト ルール（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「DNS List Rule」を参照）を使用すると、クエリーの結果をさまざまな値と比較できます。しかし、HAT 内で DNS リスト サーバにクエリーを実行する指定では、簡潔にするためにブール演算のみがサポートされています（つまり、IP アドレスがリストに現れるかどうか）。

（注） CLI のクエリーでは必ず角カッコを含めます。GUI で DNS リスト クエリーを指定する場合には角カッコは不要です。クエリーのテスト、DNS クエリーの一般的な設定、または現在の DNS リスト キャッシュのフラッシュを行うには、CLI で `dnslistconfig` コマンドを使用します。

このメカニズムは、「異常な」接続に加えて、「正常な」接続を識別するためにも使用できます。たとえば、query.bondedsender.org に対してクエリーを実行すると、その電子メール キャンペーンの健全性を保証するために IronPort Systems 社の Bonded Sender™ プログラムに供託金を積んだ接続元ホストが照合されます。デフォルトの WHITELIST の送信者グループを修正して Bonded Sender プログラムの DNS サーバにクエリーを実行し（積極的に供託金を拠出したこれら正規の電子メール送信者が一覧表示されます）、それに応じてメール フロー ポリシーを調整することもできます。

パブリック リスナー向けの定義済みのメール フロー ポリシー

アクセス ルール（ACCEPT または REJECT）と組み合わせた場合、表 5-3 (P.5-119) に示すパラメータが、作成する各パブリック リスナーの次の 4 つのメール フロー ポリシーとして事前に定義されています。

- $ACCEPTED
- $BLOCKED
- $THROTTLED
- $TRUSTED

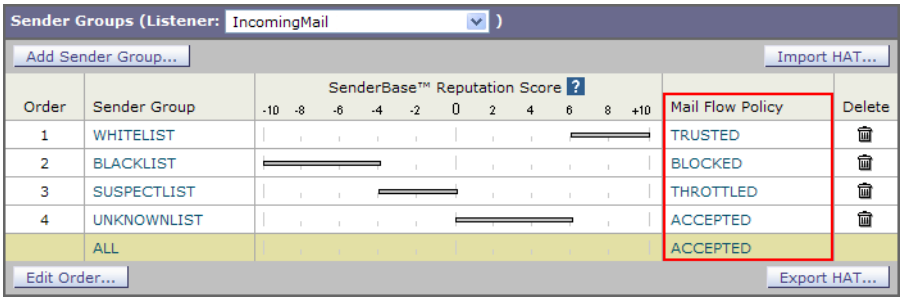
リスナーの定義済みのメール フロー ポリシーにアクセスするには、次の手順を実行します。

ステップ 1　GUI にアクセスします（「GUI へのアクセス」（P.2-19）を参照）。

ステップ 2　[Mail Policies] > [HAT Overview] の順にクリックします。

[Overview] ページが表示されます。リスナーが設定されている場合、アルファベット順で最初のリスナーに対して定義されている [Host Access Table overview] ページが表示されます。[Listener] リストから目的のリスナーを選択します。

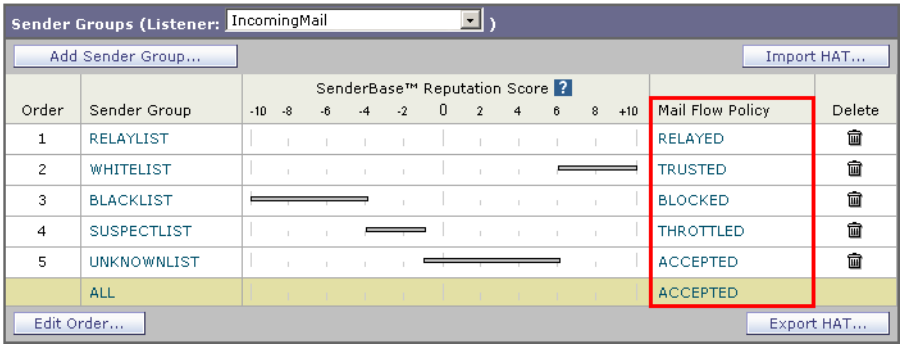
図 5-11　パブリック リスナー向けの定義済みのメール フロー ポリシー



ステップ 3　メール フロー ポリシーの名前をクリックして、そのポリシーの接続動作とパラメータを表示します。

（注）　デフォルトでは、C150/160 のユーザは、systemsetup コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。IronPort C150/160 アプライアンスで作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用されるメール フロー ポリシー $RELAYED が含まれています（図 5-12 を参照）。詳細については、「RELAYLIST」（P.5-147）を参照してください。$RELAYLIST ポリシーは、IronPort X1050/1060/1070、C650/660/670、および C350/360/370 アプライアンス上のプライベート リスナーのみで表示されます。

図 5-12　単一リスナー向けの定義済みのメール フロー ポリシー



この表で、「デフォルト」は、リスナーで定義されているデフォルト値が使用されることを意味します。

表 5-11　パブリック リスナー向けの定義済みのメール フロー ポリシー

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$ACCEPTED（All で使用）	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Default Default Default Default Default Default Default Default Default No default Default Default ON

注：$ACCEPTED ポリシーのすべてのパラメータは、CLI の systemsetup および listenerconfig コマンドでユーザが定義します。次の質問が表示されたら「**y**」を選択します。

```
Would you like to change the default host access policy?
```

これによりこれらの値を変更します。GUI を使用してこれらの値を変更するには、図 5-7「デフォルト メール フロー ポリシーの参照」（P.5-126）の手順に従います。

$BLOCKED	REJECT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	N/A N/A N/A N/A Default Default Default N/A N/A N/A N/A N/A N/A

表 5-11　パブリック リスナー向けの定義済みのメール フロー ポリシー（続き）

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$THROTTLED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase: Envelope Sender DNS Ver:	1 25 10MB 1 Default Default Default Default Default* 20 Default Default ON ON
$TRUSTED	ACCEPT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use McAfee virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	5,000 5,000 100 MB 600 Default Default Default Default OFF* -1(Disable) N/A N/A OFF

* イネーブルな場合

$ACCEPTED は名前付きポリシーであり、パブリック リスナーのデフォルトの HAT 設定と同じです。$ACCEPTED ポリシーは作成するどの送信者グループにも割り当てることができます（「新しい送信者グループの追加」（P.5-149）および「[Connections]」（P.5-119）を参照してください。また、「HAT の操作」（P.5-160）も参照してください）。

パブリック リスナー用の HAT 内の最後の ALL エントリも、主な動作として $ACCEPTED ポリシーを使用します。

各パブリック リスナーには、表 5-12 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-12　パブリック リスナー用の定義済みの送信者グループとメール フロー ポリシー

送信者グループ	使用するメール フロー ポリシー
WHITELIST	$TRUSTED
BLACKLIST	$BLOCKED
SUSPECTLIST	$THROTTLED
UNKNOWNLIST	$ACCEPTED

これら 4 つの基本的な送信者グループとメール フロー ポリシーを使用することで、パブリック リスナー上でゲートウェイに流れ込む電子メールの分類を開始するためのフレームワークが得られます。『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Using Email Security Monitor」では、ゲートウェイに流れ込む電子メールのリアルタイム フローを確認し、リスナーの HAT をリアルタイムで変更できます（IP アドレス、ドメイン、または組織の既存の送信者グループへの追加、既存のポリシーまたは定義済みのポリシーの編集、新しいメール フロー ポリシーの作成）を行うことができます。

WHITELIST

信頼する送信者を WHITELIST の送信者グループに追加します。メール フロー ポリシー $TRUSTED は、信頼できる送信者からの電子メールのレート制限をイネーブルにせず、それらの送信者からの内容をアンチスパムまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。

BLACKLIST

BLACKLIST 送信者グループ内の送信者は拒否されます（メール フロー ポリシー $BLOCKED で設定されたパラメータにより）。このグループに送信者を追加すると、SMTP HELO コマンドで 5XX SMTP 応答が返され、それらのホストからの接続が拒否されます。

SUSPECTLIST

送信者グループ SUSPECTLIST には、着信メールの速度をスロットリングする（低下させる）メール フロー ポリシーが含まれています。送信者が疑わしい場合、送信者グループ SUSPECTLIST に追加することで、メール フロー ポリシーにより次のことが指示されます。

- 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。
- リモート ホストからの時間あたりの最大受信者数は 20 に設定されます。この設定は、使用可能な最大のスロットリングであることに注意してください。このパラメータが厳しすぎる場合は、時間あたりの受信者数を増やすことができます。
- メッセージの内容はアンチスパム スキャン エンジンとアンチウイルス スキャン エンジンによってスキャンされます（これらの機能がシステムでイネーブルになっている場合）。
- 送信者に関する詳細情報を得るために、IronPort SenderBase 評価サービスに対してクエリーが実行されます。

UNKNOWNLIST

送信者グループ UNKNOWNLIST は、特定の送信者に対して使用するメール フロー ポリシーが決まっていない場合に便利です。このグループのメール フロー ポリシーでは、このグループの送信者についてメールが許可されますが、IronPort Anti-Spam ソフトウェア（システムでイネーブルになっている場合）、アンチウイルス スキャン エンジン、および IronPort SenderBase 評価サービスをすべて使用して、送信者とメッセージの内容に関する詳細情報を取得することが指示されます。このグループに属する送信者に対するレート制限もデフォルト値を使用してイネーブルになります。ウイルス スキャン エンジンの詳細については、「アンチウイルス スキャン」（P.9-304）を参照してください。SenderBase 評価サービスの詳細については、「評価フィルタリング」（P.7-246）を参照してください。

プライベート リスナー用の定義済みのメール フロー ポリシー

表 5-3 に定義されているパラメータを、アクセス ルール（RELAY または REJECT）と組み合わせた場合、作成する各*プライベート リスナー*の次の 2 つのメール フロー ポリシーとして事前に定義されます。

- $RELAYED
- $BLOCKED

これらのポリシーの要約を表 5-13 に示します。

図 5-13　プライベート リスナー用の定義済みのメール フロー ポリシー

表 5-13　プライベート リスナー用の定義済みのメール フロー ポリシー

ポリシー名	主要な動作（アクセス ルール）	パラメータ	値
$RELAYED	RELAY	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use Sophos virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Default Default Default Default Default Default Default Default Off (if enabled) -1 (Disabled) Not applicable Not applicable Default
$BLOCKED （All で使用）	REJECT	Maximum messages / session: Maximum recipients / message: Maximum message size: Maximum concurrent connections: SMTP Banner Code: SMTP Banner Text: Override Hostname: Use TLS: Use Sophos virus scanning: Maximum recipients / hour: Maximum rcpt / hour Error Code: Max recipients / hour Text: Use SenderBase:	Not applicable Not applicable Not applicable Not applicable Default Default Default Not applicable Not applicable Not applicable Not applicable Not applicable Not applicable

$BLOCKED は名前付きポリシーであり、プライベート リスナーのデフォルトの HAT 設定と同じです。プライベート リスナー用の HAT 内の最後の ALL エントリも、デフォルトの動作として $BLOCKED ポリシーを使用します。

各プライベート リスナーには、表 5-14 に示す送信者グループと対応するメール フロー ポリシーがデフォルトで定義されています。

表 5-14　プライベート リスナー用の定義済みの送信者グループとメール フロー ポリシー

送信者グループ	使用するメール フロー ポリシー
RELAYLIST	$RELAYED
ALL	$BLOCKED

この基本的な送信者グループとメール フロー ポリシーを使用することで、プライベート リスナー上でゲートウェイから出て行く電子メールの分類を開始するためのフレームワークが得られます。

RELAYLIST

中継を許可する必要があることがわかっている送信者を RELAYLIST 送信者グループに追加します。メール フロー ポリシー $RELAYED は、中継を許可する送信者からの電子メールのレート制限を行わず、それらの送信者からの内容をアンチスパム スキャン エンジンまたはアンチウイルス ソフトウェアでスキャンしない場合に設定します。

（注） GUI の System Setup Wizard（または CLI の `systemsetup` コマンド）でアウトバウンド（プライベート）リスナーを作成するときに、IronPort アプライアンスを通じた電子メールの中継を許可したシステムは、送信者グループ RELAYLIST に自動的に追加されます。「手順 3：[Network]」（P.3-57）を参照してください。

（注） デフォルトでは、C150/160 のユーザは、`systemsetup` コマンドの実行中に 1 つのパブリック リスナーのみを作成するように求められます。IronPort C150/160 アプライアンス上で作成されたパブリック リスナーにも、内部システム用にメールを中継するために使用されるメール フロー ポリシー $RELAYED が含まれます。

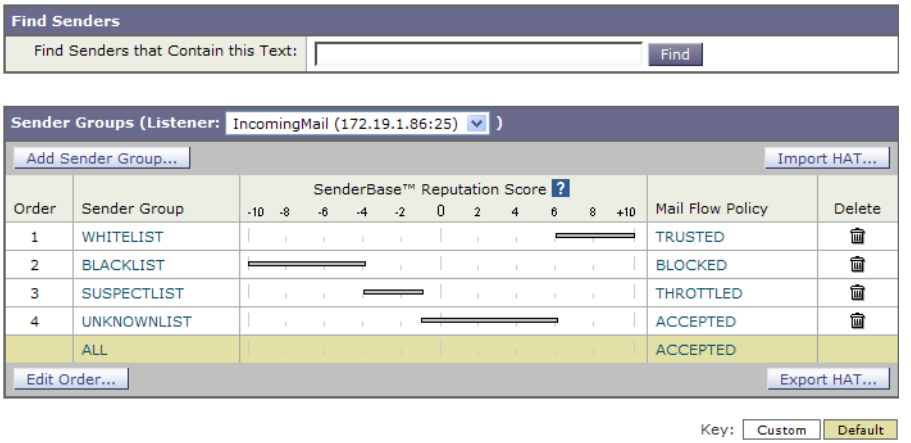
GUI による送信者グループとメール フロー ポリシーの管理

[Mail Policies] > [HAT Overview] ページと [Mail Flow Policy] ページでは、リスナーの HAT 設定を行うことができます。これらのページでは、次のことが可能です。

- 送信者グループからメール フロー ポリシーへのマッピングの参照
- 送信者グループの作成、編集、削除
- メール フロー ポリシーの作成、編集、削除
- リスナーの HAT エントリの順序変更

[Mail Policies] > [HAT Overview] リンクをクリックします。図 5-14 を参照してください。[Listener:] ドロップダウン リストから設定するリスナーを選択します。

図 5-14　[Host Access Table Overview] ページ



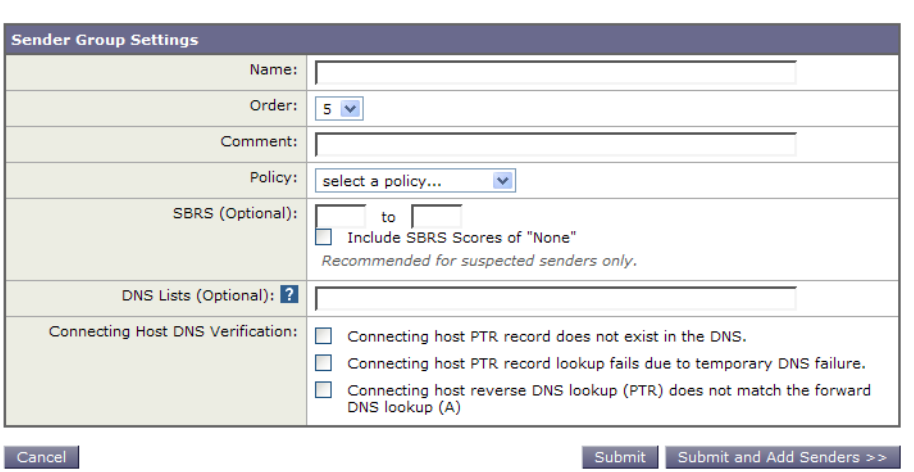
[HAT Overview] ページでは、送信者グループの追加やリスナーのメール フロー ポリシーの編集を行うことができます。

新しい送信者グループの追加

新規送信者グループを追加するには、次の手順を実行します。

ステップ 1　[HAT Overview] ページで、[Add Sender Group] をクリックします。

図 5-15　[Add Sender Group] ページ



ステップ 2　各フィールドに、送信者グループの名前を入力し、送信者グループのリストに配置する順序を選択し、コメントを入力します（任意）。

ステップ 3　このグループに適用すべきメール フロー ポリシーがわからない場合（またはまだメール フロー ポリシーが存在しない場合）は、デフォルトの「CONTINUE (no policy)」メール フロー ポリシーを使用します。そうでない場合は、ドロップダウン リストからメール フロー ポリシーを選択します。

ステップ 4　SBRS の範囲と DNS リストを選択します（任意）。また、SBRS に情報がない送信者を含めるためのチェックボックスをオンにすることもできます。これは「none」と呼ばれ、一般に疑いがあることを意味します。

ステップ 5　ホストの DNS 検証の設定を行います（「送信者検証の実装 — 設定例」（P.5-166）を参照）。

ステップ 6　[Submit] をクリックして送信者グループを保存し [Host Access Table] ページに戻るか、[Submit and Add Senders] をクリックしてグループを作成し、送信者のグループへの追加を開始します。

ステップ 7　変更を確定します。

（注）　1 つの送信者グループに重複するエントリ（同じドメインまたは IP アドレス）を入力すると、重複は廃棄されます。

送信者グループの編集

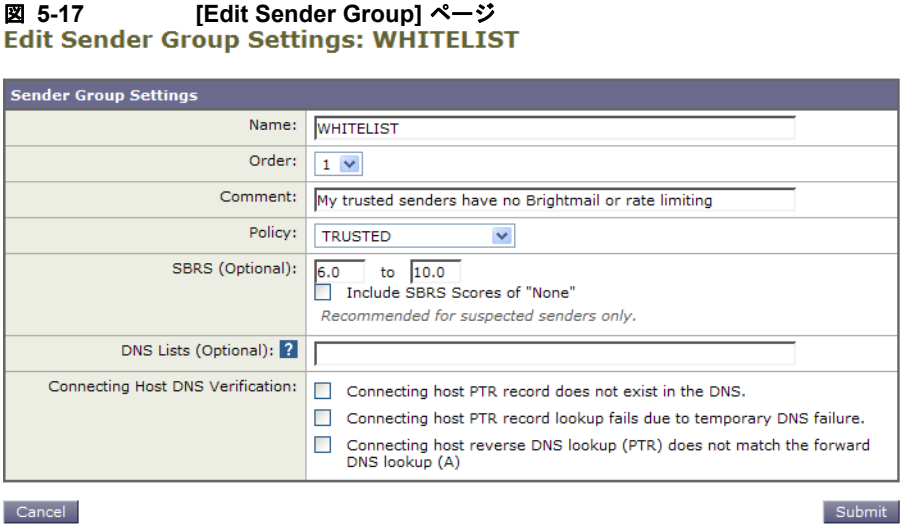
送信者グループを編集するには、次の手順を実行します。

ステップ 1　[HAT Overview] ページで、既存の送信者グループの名前をクリックします。選択した送信者グループが表示されます。

図 5-16　[Sender Group Detail] ページ

ステップ 2　[Edit Settings] をクリックします。[Edit Sender Group] ページが表示されます。

図 5-17　[Edit Sender Group] ページ



ステップ 3　送信者グループを変更し、[Submit] をクリックします。

ステップ 4　変更を確定します。

送信者グループの削除

送信者グループを削除するには、次の手順を実行します。

ステップ 1　[HAT Overview] ページで、削除する送信者グループの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。

ステップ 2　[Yes] をクリックして送信者グループを削除するか、[No] をクリックしてキャンセルします。

ステップ 3　変更を確定します。

新しいメール フロー ポリシーの追加

新しいメール フロー ポリシーを追加するには、次の手順を実行します。

ステップ 1　[Mail Policies] > [Mail Flow Policies] リンクをクリックします。[Mail Flow Policies] ページが表示されます。

ステップ 2　[Add Policy] をクリックします。[Mail Flow Policies Add Policy] ページが表示されます。

ステップ 3　メール フロー ポリシーの情報を入力します。

ステップ 4　エンベロープ送信者の DNS 検証を設定します（「送信者検証の実装 — 設定例」（P.5-166）を参照）。

ステップ 5　変更を送信して確定します。

（注）　[Use Default] オプション ボタンがオンの場合、ポリシーのデフォルト値はグレー表示されます。デフォルト値を上書きするには、[On] オプション ボタンを選択して機能または設定をイネーブルにし、新たにアクセス可能になった値を変更します。

（注）　[Custom SMTP Banner Text] および [Max. Recipients Per Hour] テキスト文字列フィールドは、「HAT 変数の構文」（P.5-124）で説明した HAT 変数をサポートしています。

（注）　一部のパラメータは特定の事前設定値に依存します（たとえば、ディレクトリ獲得攻撃の設定を行うには、LDAP 許可クエリーを設定しておく必要があります）。

メール フロー ポリシーの編集

メール フロー ポリシーを編集するには、次の手順を実行します。

ステップ 1　[Mail Flow Policy overview] ページで、ポリシーの名前をクリックします。[Mail Flow Policy Edit Policy] ページが表示されます。

ステップ 2　ポリシーを変更します。

ステップ 3　変更を送信して確定します。

メール フロー ポリシーの削除

メール フロー ポリシーを削除するには、次の手順を実行します。

ステップ 1　削除するメール フロー ポリシーの [Delete] 列にあるゴミ箱のアイコンをクリックします。削除を確認するよう求められます。

ステップ 2　[Yes] をクリックしてメール フロー ポリシーを削除するか、[No] をクリックしてキャンセルします。

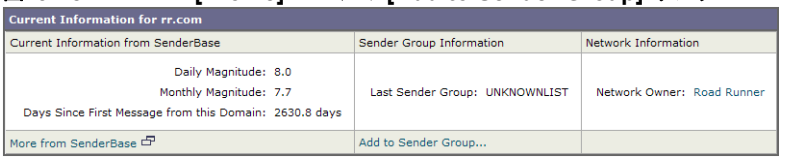
ステップ 3　変更を確定します。

送信者グループへの送信者の追加

既存の送信者グループに送信者を追加するには、次の手順を実行します。

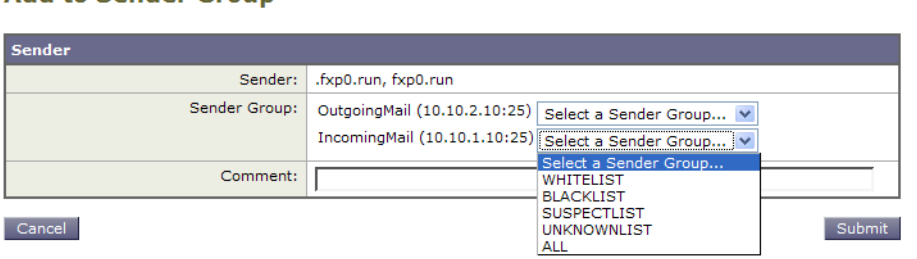
ステップ 1　ドメイン、IP、またはネットワーク オーナー プロファイル ページで、[Add to Sender Group] リンクをクリックします。

図 5-18　[Profile] ページの [Add to Sender Group] リンク



[Add to Sender Group] ページが表示されます。図 5-19 を参照してください。

図 5-19　[Add to Sender Group] ページ



ステップ 2　各リスナーに対して定義されているリストから送信者グループを選択します。

ステップ 3　[Submit] をクリックして選択した送信者グループにドメインを追加するか、[Cancel] をクリックします。

ステップ 4　変更を確定します。

（注）　ドメインを送信者グループに追加すると、実際には 2 つのドメインが GUI に表示されます。たとえば、ドメイン example.net を追加した場合、[Add to Sender Group] ページには、example.net と .example.net が追加されます。2 つめのエントリがあることで、example.net のサブドメイン内のすべてのホストが送信者グループに追加されます。詳細については、「送信者グループの構文」（P.5-132）を参照してください。

（注）　送信者グループに追加しようとしている送信者の 1 つ以上がその送信者グループにすでに存在する送信者と重複する場合、重複する送信者は追加されず、確認メッセージが表示されます。

Success — Added sender(s) to sender group(s). Some duplicates existed and were not added.

ステップ 5　[Save] をクリックして送信者を追加し、[Incoming Mail Overview] ページに戻ります。

新しい送信者グループへの送信者の追加

新しい送信者グループに送信者を追加するには、次の手順を実行します。

ステップ 1　新しい送信者グループを作成する場合、[Submit and Add Senders] をクリックします。[Add Sender] ページが表示されます。

ステップ 2　送信者を入力します。

ステップ 3　オプションで送信者のコメントを入力します。

ステップ 4　[Submit] をクリックして送信者グループにドメインを追加するか、[Cancel] をクリックします。

ステップ 5　変更を確定します。

SenderBase 評価スコアを使用した送信者グループの作成

SenderBase 評価スコアに基づいて送信者グループを作成するには、次の手順を実行します。

ステップ 1　[HAT Overview] ページで [Add Sender Group] をクリックします。

ステップ 2　[Add Sender Group] ページで、送信者グループの名前とオプションのコメントを入力します。

ステップ 3　リストからメール フロー ポリシーを選択します。

ステップ 4　[Senders] セクションで、ドロップダウン リストから [SBRS] を選択し、[Add Sender] をクリックします。

ページがリフレッシュされます。

ステップ 5　SBRS の [from:] フィールドと [to:] フィールドに範囲を入力し、オプションのコメントを入力します。

図 5-20 で、SenderBase 評価スコアが -7.5 未満の送信者は、BLOCKED メール フロー ポリシーを使用してブロックされます。

図 5-20　SenderBase 評価スコアを使用した送信者グループの作成（1）

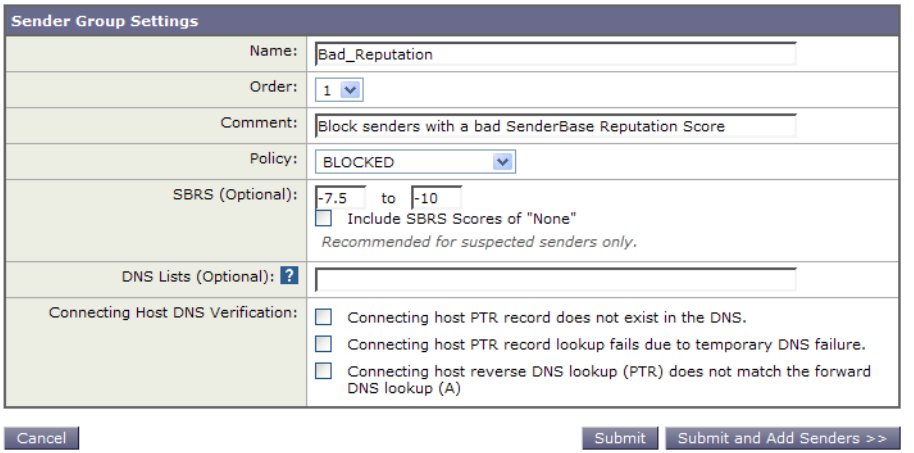
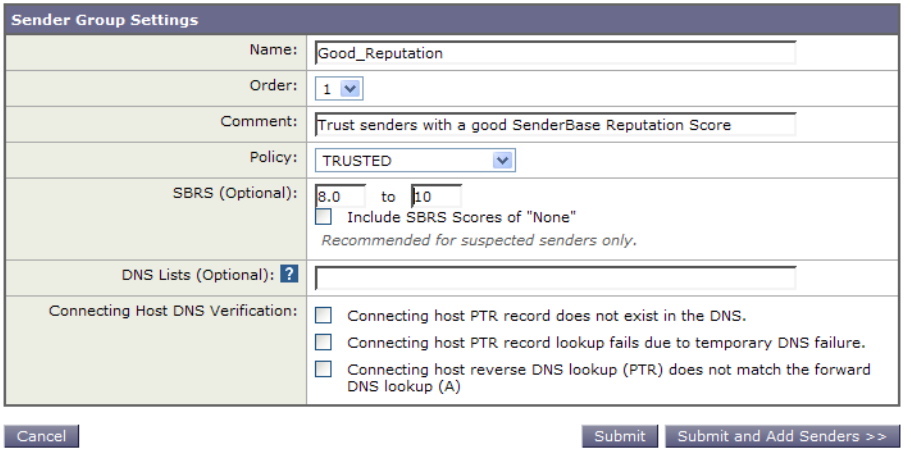


図 5-21 で、SenderBase 評価スコアが 8.0 を超えている送信者はリスナーのアンチスパム スキャンをバイパスします。

図 5-21　SenderBase 評価スコアを使用した送信者グループの作成（2）

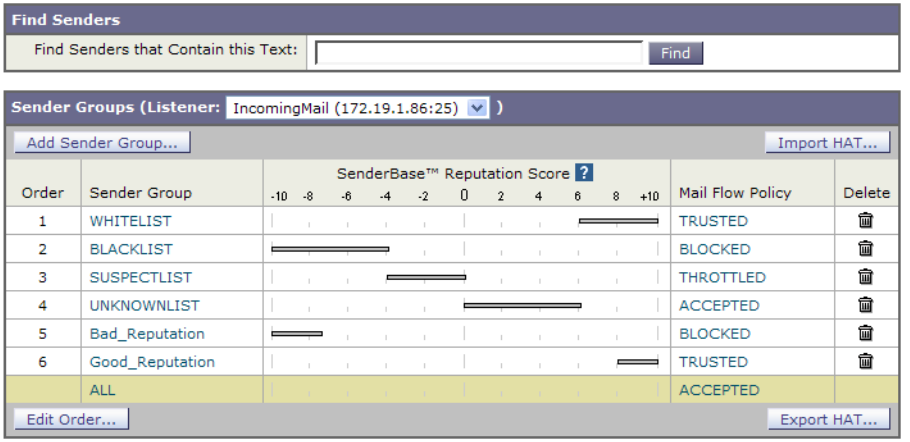


（注）　これらの同じパラメータを使用し、SenderBase 評価スコアに基づいて送信者を含めるように、TRUSTED および BLOCKED のデフォルト ポリシーを変更することもできます。詳細については、「SenderBase 評価フィルタの実装」（P.7-250）を参照してください。

ステップ 6　[Submit] をクリックし、SenderBase 評価スコアに基づいて送信者グループを作成します。

ステップ 7　変更を確定します。

図 5-22　SenderBase 評価スコアを使用したホスト アクセス テーブル



HAT の順序変更

HAT 内のエントリの順序は重要です。リスナーに接続しようとする各ホストについて、HAT が上から下に向かって読み込まれることを思い出してください。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。

たとえば、CIDR ブロックを送信者グループ A で指定し（ポリシー 1 を使用）、その CIDR ブロック内の IP アドレスに対して送信者グループ B を作成すると、送信者グループ B のポリシーは適用されません。

HAT 内のエントリの順序を編集するには、次の手順を実行します。

ステップ 1　[HAT Overview] ページで、[Edit Order] をクリックします。[Edit Sender Group Order] ページが表示されます。

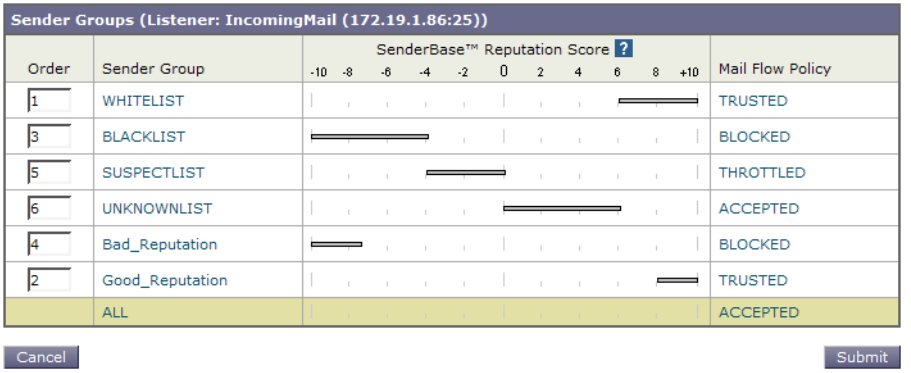
ステップ 2　HAT の既存の行の新しい順序を入力します。

ステップ 3　変更を送信して確定します。

[HAT Overview] ページがリフレッシュされ、新しい順序で表示されます。

図 5-23 に示す次の例では、信頼できる送信者が最初に処理され、ブロックされる送信者が次に処理され、不明または疑いのある送信者が最後に処理されるように順序を変更しています。

図 5-23　HAT 内のエントリの順序の変更



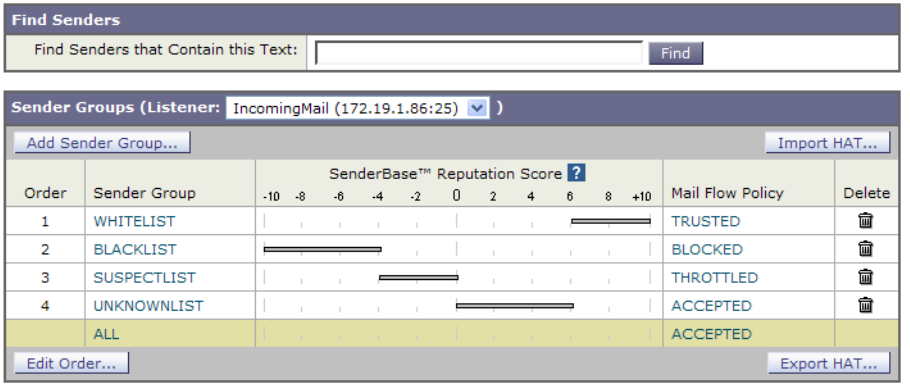
送信者の検索

[HAT Overview] ページの上部にある [Find Senders] フィールドにテキストを入力することで送信者を検索できます。検索するテキストを入力し [Find] をクリックします。

GUI によるリスナーの HAT の変更

Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）にログインし、[Mail Policies] タブをクリックします（GUI にアクセスする方法については、「GUI へのアクセス」（P.2-19）を参照してください）。左側のメニューにある [HAT Overview] リンクをクリックします。[Host Access Table Overview] ページが表示されます。

図 5-24　[Host Access Table Overview] ページ



[Host Access Table Overview] ページには、HAT 内の送信者グループが、順序、SenderBase 評価スコア範囲、関連付けられているメール フロー ポリシーとともに一覧表示されます。

[Host Access Table Overview] ページでは、次のことを行うことができます。

- 送信者グループの HAT への追加
- 送信者グループの HAT からの削除
- 既存の送信者グループの変更
- エントリの順序の変更
- ファイルからの HAT のインポート（既存のエントリの上書き）（HAT のインポートとエクスポートについては、「HAT の操作」（P.5-160）を参照してください）。
- HAT のファイルへのエクスポート
- 送信者の検索

送信者グループを編集すると、次のことが可能です。

- 送信者グループへの送信者の追加と削除
- 送信者グループの設定の編集

送信者グループの使用方法の詳細については、「GUI による送信者グループとメール フロー ポリシーの管理」（P.5-148）を参照してください。

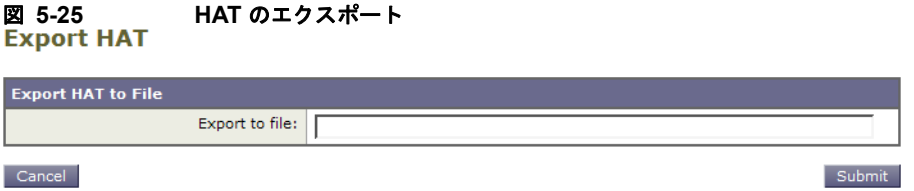
HAT の操作

HAT のエクスポート

HAT 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　[Export HAT] をクリックします。[Export Host Access Table] ページが表示されます。

図 5-25　HAT のエクスポート



ステップ 2　エクスポートする HAT のファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。

ステップ 3　変更を送信して確定します。

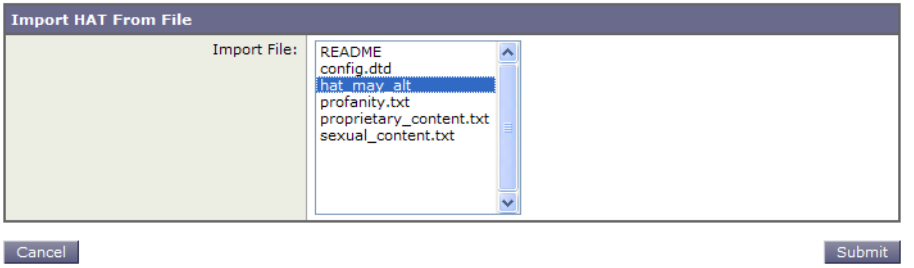
HAT のインポート

HAT をインポートすると、既存のすべての HAT エントリが現在の HAT から削除されます。

HAT をファイルからインポートするには、次の手順を実行します。

ステップ 1　[Import HAT] をクリックします。[Import Host Access Table] ページが表示されます。

図 5-26　HAT のインポート



ステップ 2　リストからファイルを選択します。

（注）　インポートするファイルは、アプライアンスのコンフィギュレーション ディレクトリに存在する必要があります。

ステップ 3　[Submit] をクリックします。既存のすべての HAT エントリを削除することを確認する警告メッセージが表示されます。

ステップ 4　[Import] をクリックします。

ステップ 5　変更を確定します。

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。次の例を参考にしてください。

```
# File exported by the GUI at 20060530T215438

$BLOCKED

    REJECT {}

[ ... ]
```

送信者検証

スパムや無用なメールは、多くの場合、DNS で解決できないドメインまたは IP アドレスを持つ送信者によって送信されます。DNS 検証とは、送信者に関する信頼できる情報を取得し、それに従ってメールを処理することを意味します。SMTP カンバセーションの前に送信者検証（送信者の IP アドレスの DNS ルッ

クアップに基づく接続のフィルタリング）を行うことは、IronPort アプライアンス上のメール パイプラインを通じて処理されるジャンク メールの量を減らすことにも役立ちます。

未検証の送信者からのメールは自動的に廃棄されます。代わりに、AsyncOS には、未検証の送信者からのメールを処理する方法を決定する送信者検証設定があります。たとえば、SMTP カンバセーションの前に未検証の送信者からのすべてのメールを自動的にブロックしたり、未検証の送信者をスロットリングしたりするように IronPort アプライアンスを設定できます。

送信者検証機能は、SMTP カンバセーションの前に実行される接続元ホストの検証と、SMTP カンバセーションの最中に実行されるエンベロープ送信者のドメイン部分の検証の 2 つで構成されます。

送信者検証：ホスト

送信者が未検証となる理由にはさまざまなものがあります。たとえば、DNS サーバが「ダウン」または応答しないか、ドメインが存在しないことが考えられます。送信者グループのホスト DNS 検証設定では、SMTP カンバセーションの前に未検証の送信者を分類し、さまざまな種類の未検証の送信者をさまざまな送信者グループに含めることができます。

IronPort アプライアンスは、着信メールについて、DNS を通じて接続元ホストの送信元ドメインを検証しようとします。この検証は、SMTP カンバセーションの前に実行されます。システムは、*二重の DNS ルックアップ*を実行することで、リモート ホストの IP アドレス（つまりドメイン）の有効性を取得および検証します。二重の DNS ルックアップは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、その後の PTR ルックアップの結果に対する正引き DNS（A）ルックアップからなります。その後、アプライアンスは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。PTR ルックアップまたは A ルックアップが失敗するか、結果が一致しない場合、システムは IP アドレスのみを使用して HAT 内のエントリを照合し、送信者は未検証と見なされます。

未検証の送信者は次の 3 つのカテゴリに分類されます。

- 接続元ホストの PTR レコードが DNS に存在しない。
- DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。
- 接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。

送信者グループの [Connecting Host DNS Verification] 設定を使用して、未検証の送信者に対する動作を指定できます（「送信者グループ SUSPECTLIST に対するホスト送信者検証の実装」（P.5-167）を参照）。

すべての送信者グループの送信者グループ設定でホスト DNS 検証をイネーブルにできますが、ホスト DNS 検証設定を送信者グループに追加するということは、そのグループに未検証の送信者を含めることになるという点に注意してください。つまり、スパムやその他の無用なメールが含まれることになります。そのため、これらの設定は、送信者を拒否またはスロットリングする送信者グループに対してのみイネーブルにすることを推奨します。たとえば、送信者グループ WHITELIST に対して DNS 検証をイネーブルにすると、未検証の送信者からのメールが、WHITELIST 内の信頼できる送信者からのメールと同じように扱われることを意味します（メール フロー ポリシーの設定内容に応じて、アンチスパムまたはアンチウイルス チェック、レート制限などのバイパスを含みます）。

送信者検証：エンベロープ送信者

エンベロープ送信者検証を使用すると、エンベロープ送信者のドメイン部分が DNS で検証されます（エンベロープ送信者のドメインが解決されるか。エンベロープ送信者のドメインの A レコードまたは MX レコードが DNS に存在するか）。タイムアウトや DNS サーバの障害など、DNS でのルックアップで一時的なエラー条件が発生した場合、ドメインは解決されません。これに対し、ドメインをルックアップしようとしたときに明確な「domain does not exist」ステータスが返された場合、ドメインは存在しません。この検証が SMTP カンバセーションの中で実行されるのに対し、ホスト DNS 検証はカンバセーションが開始される前に実行され、接続元 SMTP サーバの IP アドレスに適用されます。

詳細：AsyncOS は、送信者のアドレスのドメインに対して MX レコード クエリーを実行します。次に AsyncOS は、MX レコードのルックアップの結果に基づいて、A レコードのルックアップを行います。DNS サーバが「NXDOMAIN」（このドメインのレコードがない）を返した場合、AsyncOS はそのドメインが存在しないものとして扱います。これは「Envelope Senders whose domain does not exist」のカテゴリに分類されます。NXDOMAIN は、ルート ネーム サーバがこのドメインの権威ネームサーバを提供していないことを意味する場合があります。

しかし、DNS サーバが「SERVFAIL」を返した場合、「Envelope Senders whose domain does not resolve」として分類されます。SERVFAIL は、ドメインが存在するものの、DNS にレコードのルックアップで一時的な問題があることを意味します。

スパマーなどの不法なメール送信者が使用する一般的な手法は、MAIL FROM 情報（エンベロープ送信者内）を偽造し、受け付けられた未検証の送信者からのメールが処理されるようにすることです。これにより、MAIL FROM アドレスに送信されたバウンス メッセージが配信不能になるため、問題が生じる可能性があります。エンベロープ送信者検証を使用すると、不正な形式の（ただし空白ではない）MAIL FROM を拒否するように IronPort アプライアンスを設定できます。

各メール フロー ポリシーで、次のことが可能です。

- エンベロープ送信者の DNS 検証をイネーブルにする。
- 不正な形式のエンベロープ送信者に対し、カスタム SMTP コードと応答を渡す。エンベロープ送信者の DNS 検証をイネーブルにした場合、不正な形式のエンベロープ送信者はブロックされます。
- 解決されないエンベロープ送信者ドメインに対しカスタム応答を渡す。
- DNS に存在しないエンベロープ送信者ドメインに対しカスタム応答を渡す。

送信者検証例外テーブルを使用して、ドメインまたはアドレスのリストを格納し、そこからのメールを自動的に許可または拒否することができます（「送信者検証例外テーブル」（P.5-165）を参照）。送信者検証例外テーブルは、エンベロープ送信者検証とは独立してイネーブルにできます。そのため、たとえば、例外テーブルで指定した特別なアドレスやドメインを、エンベロープ送信者検証をイネーブルにすることなく拒否できます。また、内部ドメインまたはテスト ドメインからのメールを、他の方法で検証されない場合でも常に許可することもできます。

ほとんどのスパムは未検証の送信者から受信されますが、未検証の送信者からのメールを受け付けることが必要な理由があります。たとえば、すべての正規の電子メールを DNS ルックアップで検証できるわけではありません。一時的な DNS サーバの問題により送信者を検証できないことがあります。

未検証の送信者からのメール送信が試みられた場合、送信者検証例外テーブルとメール フロー ポリシーのエンベロープ送信者 DNS 検証設定を使用して、SMTP カンバセーション中にエンベロープ送信者が分類されます。たとえば、DNS に存在しないために検証されない送信元ドメインからのメールを受け付けてスロットリングすることができます。いったんそのメールを受け付けた後、MAIL FROM の形式が不正なメッセージは、カスタマイズ可能な SMTP コードと応答で拒否されます。これは SMTP カンバセーションの中で実行されます。

任意のメール フロー ポリシーに対し、メール フロー ポリシー設定中で、エンベロープ送信者の DNS 検証（ドメイン例外テーブルを含む）をイネーブルにできます。これには、GUI または CLI（`listenerconfig -> edit -> hostaccess -> <policy>`）を使用します。

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するか、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すると（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」の項を参照）、そのリスナーのデフォルト ドメイン設定は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。

カスタム SMTP コードと応答

エンベロープ送信者の形式が不正なメッセージ、DNS に存在しないエンベロープ送信者、DNS クエリーで解決できない（DNS サーバがダウンしているなど）エンベロープ送信者に対し、SMTP コードと応答メッセージを指定できます。

SMTP 応答には変数 `$EnvelopeSender` を含めることができます。これは、カスタム応答を送信するときにエンベロープ送信者の値に展開されます。

一般には「Domain does not exist」結果は永続的ですが、これを一時的な状態にすることができます。そのようなケースを扱うために、「保守的な」ユーザは、エラー コードをデフォルトの 5XX から 4XX に変更できます。

送信者検証例外テーブル

送信者検証例外テーブルは、SMTP カンバセーション中に自動的に許可または拒否されるドメインまたは電子メール アドレスのリストです。また、拒否されるドメインについて、オプションの SMTP コードと拒否応答を指定することもできます。IronPort アプライアンスあたりの送信者検証例外テーブルは 1 つのみであり、メール フロー ポリシーごとにイネーブルにされます。

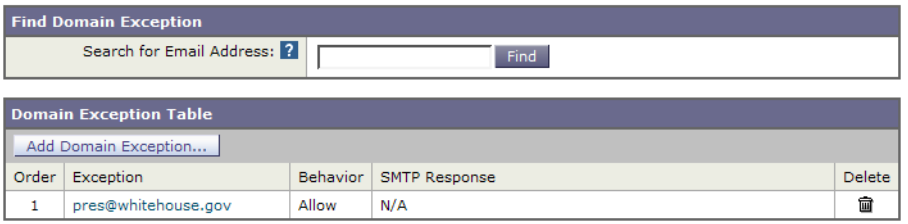
送信者検証例外テーブルは、明らかに偽物であるものの、形式が正しいドメインまたは電子メール アドレスをリストし、そこからのメールを拒否するために使用できます。たとえば、形式が正しい MAIL FROM `pres@whitehouse.gov` を送信者検証例外テーブルに格納し、自動的に拒否するように設定できます。また、内部ドメインやテスト ドメインなど、自動的に許可するドメインをリストする

こともできます。これは、Recipient Access Table（RAT; 受信者アクセス テーブル）で行われるエンベロープ受信者（SMTP RCPT TO コマンド）処理に似ています。

送信者検証例外テーブルは、GUI の [Mail Policies] > [Exception Table] ページ（または CLI の `exceptionconfig` コマンド）で定義された後、GUI（「メール フロー ポリシー ACCEPTED に対する送信者検証の実装」（P.5-171）を参照）または CLI（『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照）でポリシーごとにイネーブルにされます。

送信者検証例外テーブルのエントリの構文は次のとおりです。

図 5-27　例外テーブルのリスト



例外テーブルの変更については「GUI での送信者検証例外テーブルの作成」（P.5-172）を参照してください。

送信者検証の実装 — 設定例

ここでは、ホストとエンベロープ送信者検証の典型的で保守的な実装の例を示します。

この例では、ホスト送信者検証を実装するときに、既存の送信者グループ SUSPECTLIST とメール フロー ポリシー THROTTLED により、逆引き DNS ルックアップが一致しない接続元ホストからのメールがスロットリングされます。

新しい送信者グループ（UNVERIFIED）と新しいメール フロー ポリシー（THROTTLEMORE）が作成されます。検証されない接続元ホストからのメールは、SMTP カンバセーションの前にスロットリングされます（送信者グループ UNVERIFIED とより積極的なメール フロー ポリシー THROTTLEMORE が使用されます）。

メール フロー ポリシー ACCEPTED に対してエンベロープ送信者検証がイネーブルにされます。

表 5-15 に、送信者検証を実装するための推奨される設定を示します。

表 5-15　送信者検証：推奨される設定

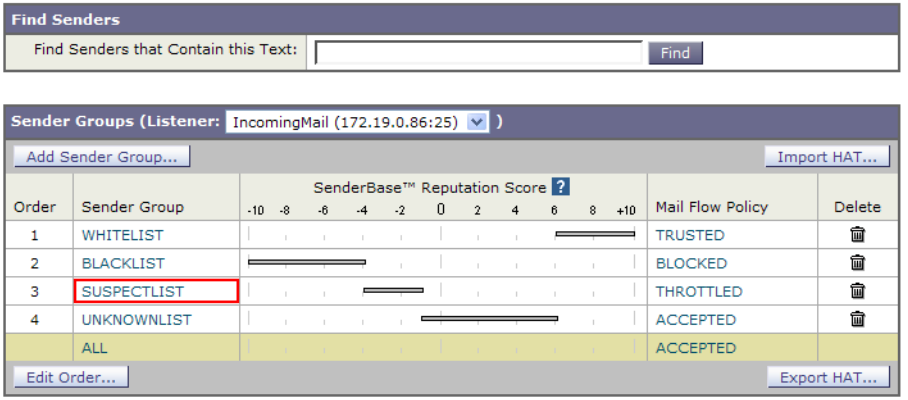
送信者グループ	ポリシー	内容
UNVERIFIED	THROTTLEMORE	SMTP カンバセーションの前 接続元ホストの PTR レコードが DNS に存在しない。
SUSPECTLIST	THROTTLED	接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。
	ACCEPTED	SMTP カンバセーション中のエンベロープ送信者検証 - 形式が不正な MAIL FROM: - エンベロープ送信者が DNS に存在しない - エンベロープ送信者が DNS で解決されない

送信者グループ SUSPECTLIST に対するホスト送信者検証の実装

GUI で、[Mail Policies] タブの [HAT Overview] をクリックします。既存の送信者グループの一覧が表示されます。送信者グループ SUSPECTLIST に対するホスト DNS 検証をイネーブルにして設定するには、次の手順を実行します。

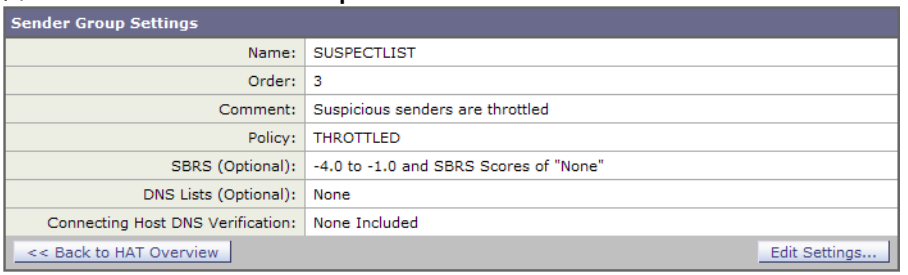
ステップ 1　[HAT Overview] ページで、送信者グループのリスト中の [SUSPECTLIST] をクリックします。

図 5-28　[HAT Overview] ページ



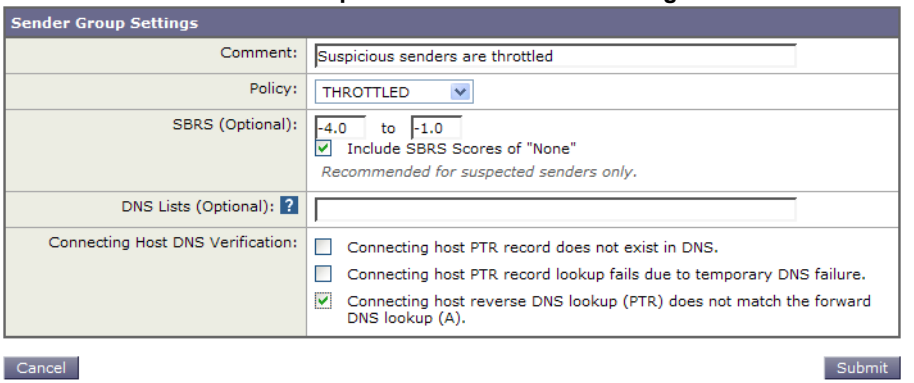
ステップ 2　[Sender Group: SUSPECTLIST] ページが表示されます。

図 5-29　Sender Group: SUSPECTLIST



ステップ 3　[Edit Settings] をクリックします。[Edit Settings] ダイアログが表示されます。

図 5-30　Sender Group: SUSPECTLIST: Edit Settings



ステップ 4　リストから [THROTTLED] ポリシーを選択します。

ステップ 5　[Connecting Host DNS Verification] の中の [Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)] チェックボックスをオンにします。

ステップ 6　変更を送信して確定します。

逆引き DNS ルックアップが失敗した送信者は送信者グループ SUSPECTLIST に一致し、メール フロー ポリシー THROTTLED のデフォルト アクションが実行されます。

（注）　また、CLI でホスト DNS 検証を設定することもできます。詳細については、「CLI でのホスト DNS 検証のイネーブル化」（P.5-176）を参照してください。

送信者検証の実装

まず、新しいメール フロー ポリシーを作成し（この例では THROTTLEMORE という名前を付けます）、より厳格なスロットリング設定を行います。

ステップ 1　[Mail Flow Policies] ページで [Add Policy] をクリックします。

ステップ 2　メール フロー ポリシーの名前を入力し、[Connection Behavior] として [Accept] を選択します。

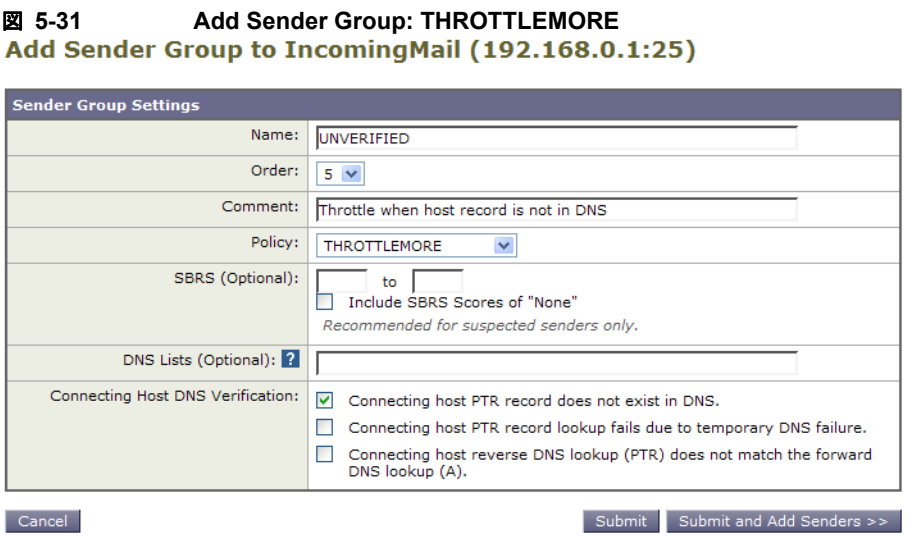
ステップ 3　メールをスロットリングするようにポリシーを設定します。

ステップ 4　変更を送信して確定します。

次に、新しい送信者グループを作成し（この例では、UNVERIFIED という名前を付けます）、THROTTLEMORE ポリシーを使用するように設定します。

ステップ 1　[HAT Overview] ページで [Add Sender Group] をクリックします。

図 5-31　Add Sender Group: THROTTLEMORE

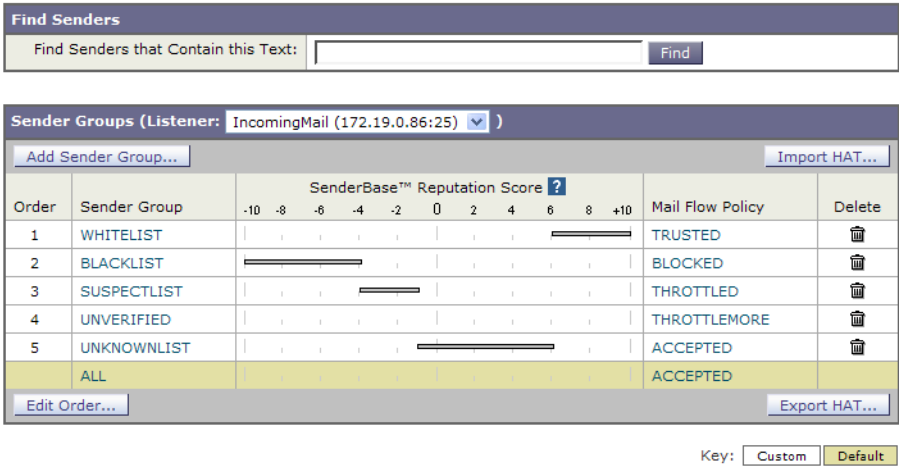


ステップ 2　リストから [THROTTLEMORE] ポリシーを選択します。

ステップ 3　[Connecting Host DNS Verification] 中の [Connecting host PTR record does not exist in DNS] チェックボックスをオンにします。

ステップ 4　変更を送信して確定します。これで [HAT Overview] ページは次のようになります。

図 5-32　[HAT Overview]



次の手順では、未検証の送信者を扱うようにメール フロー ポリシー ACCEPTED を設定します。

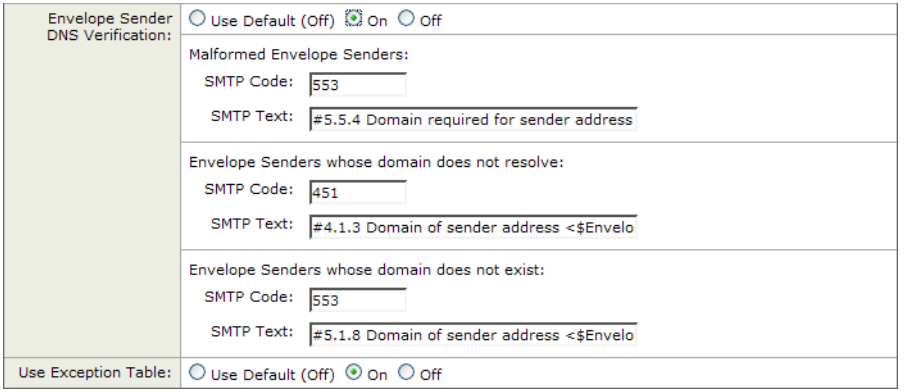
メール フロー ポリシー ACCEPTED に対する送信者検証の実装

GUI で、[Mail Policies] タブの [Mail Flow Policies] をクリックします。既存のメール フロー ポリシーの一覧が表示されます。メール フロー ポリシー ACCEPTED に対してエンベロープ送信者の DNS 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] ページで、メール フロー ポリシー [ACCEPTED] をクリックします。

ステップ 2　メール フロー ポリシーの最後にスクロールします。

図 5-33　メール フロー ポリシー ACCEPTED のエンベロープ送信者の DNS 検証の設定



ステップ 3　[On] を選択し、このメール フロー ポリシーに対するエンベロープ送信者の DNS 検証をイネーブルにします。

ステップ 4　カスタム SMTP コードと応答を定義することもできます。

ステップ 5　[Use Domain Exception Table] で [On] を選択することで、ドメイン例外テーブルをイネーブルにします。

ステップ 6　変更を送信して確定します。

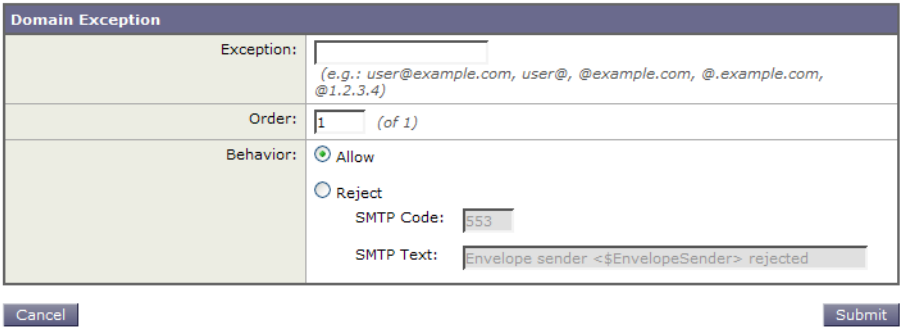
最後の手順として、送信者検証例外テーブルを作成し、送信者検証設定に対する例外を列挙します。

GUI での送信者検証例外テーブルの作成

[Mail Policies] > [Exception Table] ページを使用して、送信者検証例外テーブルを設定します。例外テーブルは、[Use Exception Table] がオンになっているすべてのメール フロー ポリシーにグローバルに適用されることに注意してください。

ステップ 1　[Mail Policies] > [Exception Table] ページで [Add Domain Exception] をクリックします。[Add Domain Exception] ページが表示されます。

図 5-34　例外テーブルへのアドレスの追加



ステップ 2　電子メール アドレスを入力します。具体的なアドレス（pres@whitehouse.gov）、名前（user@）、ドメイン（@example.com または @.example.com）、または IP アドレスを角カッコで囲んだアドレス（user@[192.168.23.1]）を入力できます。

ステップ 3　そのアドレスからのメッセージを許可するか拒否するかを指定します。メールを拒否する場合、SMTP コードとカスタム応答を指定することもできます。

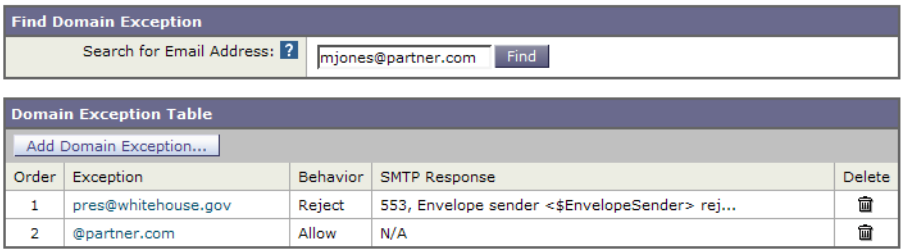
ステップ 4　変更を送信して確定します。

送信者検証例外テーブル内でのアドレスの検索

特定のアドレスが例外テーブルのいずれかのエントリに一致するかどうかを判定するには、次の手順を実行します。

ステップ 1　[Exception Table] ページの [Find Domain Exception] セクションに電子メール アドレスを入力し、[Find] をクリックします。

図 5-35　例外テーブル中の一致エントリの検索



ステップ 2　テーブル中のいずれかのエントリにアドレスが一致した場合、最初に一致したエントリが表示されます。

図 5-36　例外テーブル中の一致エントリの一覧表示

送信者検証設定のテスト

これで送信者検証設定を完了したため、IronPort アプライアンスの動作を確認できます。

DNS 関連の設定のテストは、本書の範囲を超えていることに注意してください。

エンベロープ送信者検証の設定のテスト

THROTTLED ポリシーのさまざまな DNS 関連の設定をテストすることは難しい場合がありますが、形式が不正な MAIL FROM 設定をテストできます。

ステップ 1　IronPort アプライアンスへの Telnet セッションを開きます。

ステップ 2　SMTP コマンドを使用して、形式が不正な MAIL FROM（ドメインなしの「admin」など）を使用したテスト メッセージを送信します。

（注）　デフォルト ドメインを使用するか、メールを送受信するときに部分ドメインを明示的に許可するように IronPort アプライアンスを設定した場合や、アドレス解析をイネーブルにした場合は（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」を参照）、ドメインがないかドメインの形式が正しくない電子メールを作成、送信、受信できない場合があります。

ステップ 3　メッセージが拒否されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance port

220 hostname ESMTP

helo example.com

250 hostname

mail from: admin

553 #5.5.4 Domain required for sender address
```

SMTP コードと応答が、メール フロー ポリシー THROTTLED のエンベロープ送信者検証設定で設定したものになっていることを確認します。

送信者検証例外テーブルのテスト

送信者検証例外テーブルに列挙されている電子メール アドレスからのメールに対し、エンベロープ送信者検証が実行されないことを確認するには、次の手順を実行します。

ステップ 1　アドレス admin@zzzaaazzz.com を、例外テーブルに動作「Allow」で追加します。

ステップ 2　変更を確定します。

ステップ 3　IronPort アプライアンスへの Telnet セッションを開きます。

ステップ 4　SMTP コマンドを使用して、送信者検証例外テーブルに入力した電子メール アドレス（admin@zzzaaazzz.com）からテスト メッセージを送信します。

ステップ 5　メッセージが許可されることを確認します。

```
# telnet IP_address_of_IronPort_Appliance port

220 hostname ESMTP

helo example.com

250 hostname
```

```
mail from: admin@zzzaaazzz.com

250 sender <admin@zzzaaazzz.com> ok
```

その電子メール アドレスを送信者検証例外テーブルから削除すると、エンベロープ送信者のドメイン部分が DNS で検証されないため、その送信者からのメールが拒否されます。

送信者検証とロギング

次のログ エントリは、送信者検証の判断例を示します。

エンベロープ送信者検証

形式が不正なエンベロープ送信者

```
Thu Aug 10 10:14:10 2006 Info: ICID 3248 Address: <user> sender rejected,
envelope sender domain missing
```

ドメインが存在しない（NXDOMAIN）

```
Wed Aug  9 15:39:47 2006 Info: ICID 1424 Address: <user@domain.com>
sender rejected, envelope sender domain does not exist
```

ドメインが解決されない（SERVFAIL）

```
Wed Aug  9 15:44:27 2006 Info: ICID 1425 Address: <user@domain.com>
sender rejected, envelope sender domain could not be resolved
```

CLI でのホスト DNS 検証のイネーブル化

CLI でホスト DNS 検証をイネーブルにするには、`listenerconfig->edit->hostaccess` コマンドを使用します（詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください）。

表 5-16 に、未検証の送信者の種類と対応する CLI 設定を示します。

表 5-16　送信者グループ設定と対応する CLI 値

接続元ホストの DNS 検証	同等の CLI 設定
接続元ホストの PTR レコードが DNS に存在しない。	`nx.domain`
DNS の一時的な障害により接続元ホストの PTR レコードのルックアップに失敗した。	`serv.fail`
接続元ホストの逆引き DNS ルックアップ（PTR）が正引き DNS ルックアップ（A）に一致しない。	`not.double.verified`

パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ

パブリック リスナーを作成するとき、Recipient Access Table（RAT; 受信者アクセス テーブル）を使用して、アプライアンスがメッセージを受け付けるすべてのローカル ドメインを定義します。多くのエンタープライズ ゲートウェイは、複数のローカル ドメインのメッセージを受け付けるように設定されます。たとえば、会社名が変更されたとします。その場合、`currentcompanyname.com` および `oldcompanyname.com` 宛の電子メール メッセージを受信する必要があります。この場合、両方のローカル ドメインをパブリック リスナーの RAT に含めることになります（注：ドメイン マップ機能はあるドメインから別のドメインにメッセージをマップできます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Domain Features」の章とドメイン マップ機能の項を参照してください）。

（注） System Setup Wizard または `systemsetup` コマンドを完了し、`commit` コマンドを実行済みの場合、1 つのパブリック リスナーがアプライアンス上ですでに設定されています（「手順 3：[Network]」（P.3-57）で入力した設定を参照してください）。そのときに入力した、メールを許可するデフォルト ローカル ドメインまたは具体的なアドレスは、そのパブリック リスナーの RAT の最初のエントリとして設定されます。

受信者アクセス テーブル（RAT）

受信者アクセス テーブルは、パブリック リスナーが許可する受信者を定義します。このテーブルでは、アドレス（部分アドレス、ユーザ名、ドメイン、またはホスト名）と、それを許可するか拒否するかを指定します。オプションで、その受信者の RCPT TO コマンドに対する SMTP 応答を含めたり、特定のエントリでスロットリング制御をバイパスしたりできます。

RAT エントリは次の基本的な構文によって定義されます。

表 5-17　RAT の基本的な構文

受信者定義	ルール	（任意）カスタム SMTP 応答

ルール

RAT には、SMTP カンバセーションの中でやりとりするときに受信者に対して実行する、次の 2 つの基本的な動作があります。

ACCEPT	受信者は許可されます。
REJECT	受信者は拒否されます。

受信者の定義

RAT では、受信者または受信者のグループを定義できます。受信者は、完全な電子メール アドレス、ドメイン、部分ドメイン、またはユーザ名で定義できます。

division.example.com	完全修飾ドメイン名。
.partialhost	「partialhost」ドメイン内のすべて。
user@domain	完全な電子メール アドレス。

user@	指定したユーザ名を含むすべてのアドレス。
user@[*IP_address*]	特定の IP アドレスのユーザ名。IP アドレスは文字「[]」で囲む必要があることに注意してください。 「user@*IP_address*」（角カッコ文字なし）は有効なアドレスではないことに注意してください。有効なアドレスを作成するために、メッセージを受信したときに角カッコが追加され、受信者が RAT で一致するかどうかに影響が出ることがあります。

（注） GUI の System Setup Wizard の手順 4 でドメインを受信者アクセス テーブルに追加する場合（「手順 3：[Network]」（P.3-57）を参照）、サブドメインを指定するための別のエントリを追加することを検討してください。たとえば、ドメイン example.net を入力する場合、.example.net も入力したほうがよい場合があります。第 2 のエントリにより、example.net のすべてのサブドメイン宛のメールが受信者アクセス テーブルに一致するようになります。RAT で .example.com のみを指定した場合、.example.com のすべてのサブドメイン宛のメールを許可しますが、サブドメインがない完全な電子メール アドレス受信者（たとえば joe@example.com）宛のメールは許可されません。

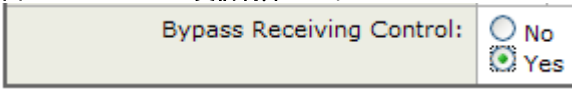
特別な受信者でのスロットリングのバイパス

受信者エントリで、リスナーでイネーブルになっているスロットリング制御メカニズムを受信者がバイパスすることを指定できます。

この機能は、特定の受信者のメッセージを制限しない場合に便利です。たとえば、多くのユーザは、メール フロー ポリシーで定義されている受信制御に基づいて送信元ドメインがスロットリングされている場合でも、リスナー上でアドレス「postmaster@domain」の電子メールを受信します。リスナーの RAT 中で受信制御をバイパスするようにこの受信者を指定することで、同じドメイン中の他の受信者用のメール フロー ポリシーを保持しつつ、リスナーは受信者「postmaster@domain」の無制限のメッセージを受信できます。受信者は、送信元ドメインが制限されている場合に、システムが保持している時間あたりの受信者のカウンタでカウントされません。

GUI で特定の受信者が受信制御をバイパスするように指定するには、RAT エントリを追加または編集するときに、[Bypass Receiving Control] で [Yes] を選択します。

図 5-37　受信制御のバイパス



CLI で特定の受信者が受信制御をバイパスするように指定するには、listenerconfig -> edit -> rcptaccess コマンドを使用して受信者を入力するときに、次の質問に「yes」と答えます。

```
Would you like to bypass receiving control for this entry?  [N]> y
```

特別な受信者での LDAP 許可のバイパス

LDAP 許可クエリーを設定する場合、特定の受信者について許可クエリーをバイパスすることが必要な場合があります。この機能は、customercare@example.com のように、ある受信者宛に受信した電子メールについて、LDAP クエリーの中で遅延させたりキューに格納したりしないことが望ましい場合に便利です。

LDAP 許可クエリーの前にワーク キュー内で受信者アドレスを書き換えるように設定した場合（エイリアシングまたはドメイン マップの使用など）、書き換えられたアドレスは LDAP 許可クエリーをバイパスしません）。たとえば、エイリアス テーブルを使用して customercare@example.com を bob@example.com および sue@example.com にマップします。customercare@example.com について LDAP 許可のバイパスを設定した場合、エイリアシングが実行された後に、bob@example.com および sue@example.com に対して LDAP 許可クエリーが実行されます。

GUI で LDAP 許可をバイパスするように設定するには、RAT エントリを追加または編集するときに [Bypass LDAP Accept Queries for this Recipient] を選択します。

CLI で LDAP 許可クエリーをバイパスするように設定するには、listenerconfig -> edit -> rcptaccess コマンドを使用して受信者を入力するときに、次の質問に「yes」と答えます。

```
Would you like to bypass LDAP ACCEPT for this entry? [Y]> y
```

LDAP 許可をバイパスするように RAT エントリを設定する場合、RAT エントリの順序が、受信者アドレスの一致のしかたに影響を与えることに注意してください。条件を満たす最初の RAT エントリを使用して受信者アドレスが一致します。たとえば、RAT エントリ postmaster@ironport.com と ironport.com があるとし

ます。postmaster@ironport.com のエントリについては LDAP 許可クエリーをバイパスするように設定し、ironport.com のエントリを ACCEPT に設定します。postmaster@ironport.com 宛のメールを受信した場合、LDAP 許可がバイパスされるのは、postmaster@ironport.com のエントリが ironport.com のエントリよりも前にある場合のみです。ironport.com のエントリが postmaster@ironport.com のエントリの前にある場合、RAT はこのエントリを介して受信者アドレスと一致し、ACCEPT アクションが適用されます。

デフォルト RAT エントリ

作成するすべてのパブリック リスナーについて、デフォルトでは、*すべての受信者からの電子メールを拒否*するように RAT が設定されます。

ALL	REJECT

[Recipient Access Table Overview] リストでは、デフォルト エントリの名前は [All Other Recipients] になります。

（注） デフォルトでは、RAT はすべての受信者を*拒否し*、誤ってインターネット上に*オープン リレー*が作成されないようにします。オープンリレー（「セキュアでないリレー」または「サードパーティ リレー」とも呼びます）は、第三者による電子メール メッセージのリレーを許す SMTP 電子メール サーバです。オープンリレーがあると、ローカル ユーザ向けでもローカル ユーザからでもないメールを処理することにより、非良心的な送信者がゲートウェイを通じて大量のスパムを送信することが可能になります。作成するパブリック リスナーの受信者アクセス テーブルのデフォルト値を変更するときには注意してください。

デフォルトの「ALL」エントリを RAT から削除してはなりません。

テキスト ファイルとしてテキスト リソースをインポートおよびエクスポートする方法

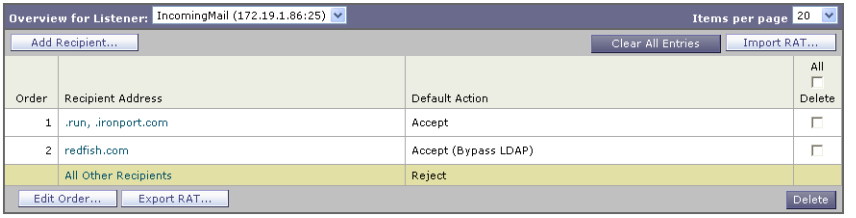
アプライアンスのコンフィギュレーション ディレクトリにアクセスする必要があります。インポートするテキスト ファイルは、アプライアンス上のコンフィギュレーション ディレクトリに存在する必要があります。エクスポートされたテキスト ファイルは、コンフィギュレーション ディレクトリに配置されます。

コンフィギュレーション ディレクトリへのアクセスの詳細については、付録 A「アプライアンスへのアクセス」を参照してください。

GUI によるリスナーの RAT の変更

GUI から RAT を変更するには、[Mail Policies] > [Recipient Access Table (RAT)] をクリックします。[Recipient Access Table Overview] ページが表示されます。

図 5-38　[Recipient Access Table Overview] ページ



[Recipient Access Table Overview] ページには、RAT 内のエントリの一覧が、その順序、デフォルトのアクション、エントリが LDAP 許可クエリーをバイパスするように設定されているかどうかとともに表示されます。

[Recipient Access Table Overview] では、次のことを行うことができます。

- RAT へのエントリの追加
- RAT からのエントリの削除
- 既存の RAT エントリの変更
- エントリの順序の変更
- ファイルからの RAT エントリのインポート（既存のエントリの上書き）
- RAT エントリのファイルへのエクスポート

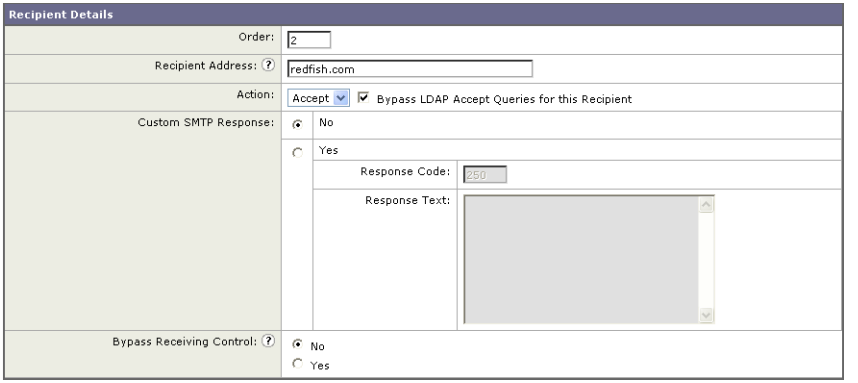
RAT は、Command Line Interface（CLI; コマンド ライン インターフェイス）を使って直接編集できます。定義したリスナーの RAT をカスタマイズするには、`listenerconfig` コマンドの `edit -> rcptaccess -> new` サブコマンドを使用して、設定する各パブリック リスナーについて、許可されるローカル ドメインを RAT に追加します。詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。

新しい RAT エントリの追加

RAT に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　[Add Recipient] をクリックします。[Add to Recipient Access Table] ページが表示されます。

図 5-39　　RAT エントリの追加



ステップ 2　エントリの順序を選択します。

ステップ 3　受信者アドレスを入力します（有効なエントリの詳細については、「受信者の定義」（P.5-178）を参照してください）。

ステップ 4　受信者を許可するか拒否するかを選択します。

ステップ 5　オプションで、受信者に対する LDAP 許可クエリーをバイパスすることを選択できます（「特別な受信者での LDAP 許可のバイパス」（P.5-180）を参照）。

ステップ 6　このエントリに対してカスタム SMTP 応答を使用する場合は、[Custom SMTP Response] で [Yes] を選択します。応答コードとテキストを入力します。

ステップ 7　オプションで、スロットリングをバイパスすることを設定できます（「特別な受信者でのスロットリングのバイパス」（P.5-179）を参照）。そのためには、[Bypass Receiving Control] で [Yes] を選択します。

ステップ 8　変更を送信して確定します。

RAT エントリの削除

RAT 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　削除する各エントリの [Delete] 列のチェックボックスをオンにします。

ステップ 2　[Delete] をクリックします。

ステップ 3　チェックボックスをオンにしたエントリが RAT から削除されます。

ステップ 4　変更を確定します。

RAT エントリの変更

RAT エントリを変更するには、次の手順を実行します。

ステップ 1　[Recipient Access Table Overview] で RAT エントリをクリックします。[Edit Recipient Access Table] ページが表示されます。

ステップ 2　エントリを変更します。

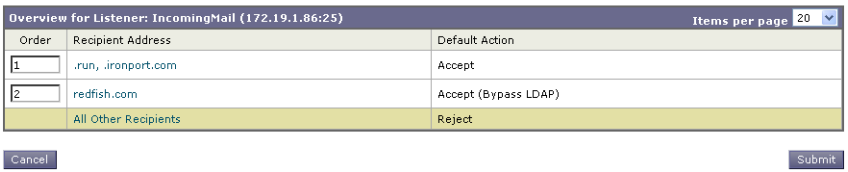
ステップ 3　変更を確定します。

RAT エントリの順序の変更

RAT 内のエントリの順序を変更するには、次の手順を実行します。

ステップ 1　[Edit Order] をクリックします。[Edit Recipient Access Table Order] ページが表示されます。

図 5-40　RAT エントリの順序の変更



ステップ 2　[Order] 列の値を調整して順序を変更します。

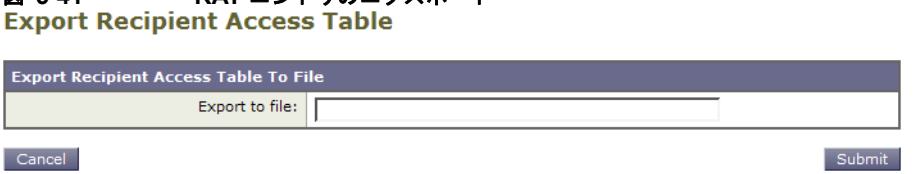
ステップ 3　変更を確定します。

RAT エントリのエクスポート

RAT エントリ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　[Export RAT] をクリックします。[Export Recipient Access Table] ページが表示されます。

図 5-41　RAT エントリのエクスポート



ステップ 2　エクスポートするエントリのファイル名を入力します。これは、アプライアンスの設定ディレクトリに作成されるファイルの名前になります。

ステップ 3　変更を送信して確定します。

RAT エントリのインポート

RAT をインポートすると、既存のすべての RAT エントリが RAT から削除されます。

一連の RAT エントリ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　[Import RAT] をクリックします。[Import Recipient Access Table] ページが表示されます。

図 5-42　RAT エントリのインポート

ステップ 2　リストからファイルを選択します。

（注）　インポートするファイルは、アプライアンスのコンフィギュレーション ディレクトリに存在する必要があります。

ステップ 3　[Submit] をクリックします。既存の RAT エントリをすべて削除することを確認する警告メッセージが表示されます。

ステップ 4　[Import] をクリックします。

ステップ 5　変更を確定します。

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。次の例を参考にしてください。

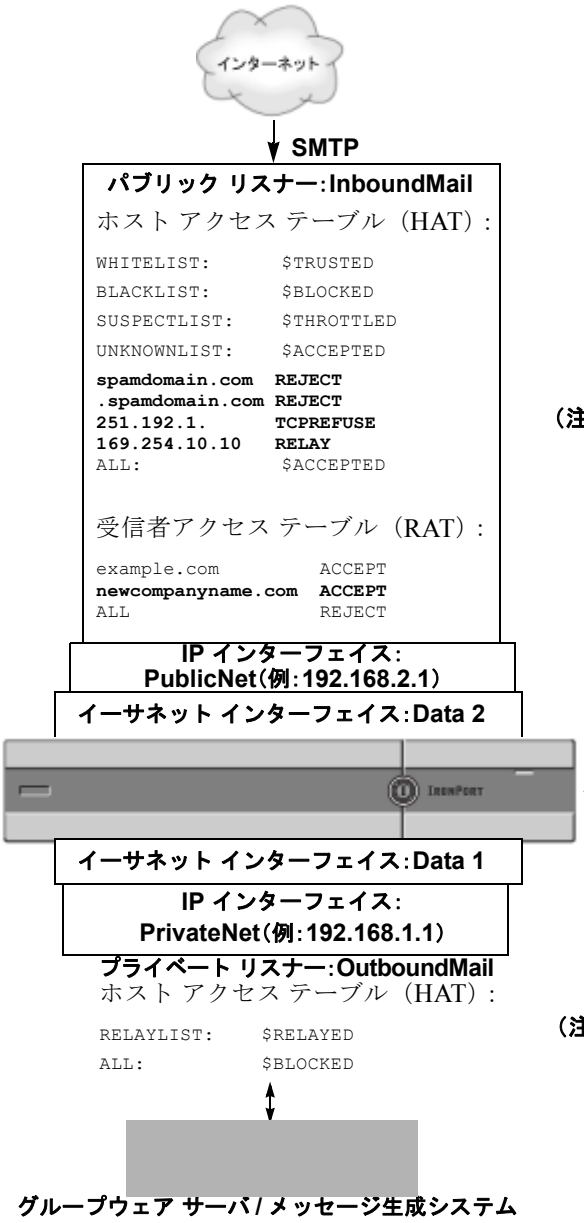
```
# File exported by the GUI at 20060530T220526

.example.com  ACCEPT

ALL  REJECT
```

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 5-43　パブリック リスナーの RAT の編集



（注） このパブリック リスナーの RAT は、ドメイン newcompanyname.com の接続を許可するために変更されています。カスタム SMTP 応答も作成されています。

（注） このプライベート リスナーは変更されていません。プライベート リスナーには RAT がありません。

図 5-44 は、図 5-4 に示した図を展開したものであり、リスナーの HAT（該当する場合）と RAT の処理シーケンスと、それぞれのデフォルト値が含まれています。

図 5-44　パブリック リスナーとプライベート リスナー