ホスト アクセス テーブルを使用した接続を許可するホストの定義

この章は、次の項で構成されています。

接続を許可するホストの定義の概要

設定されているすべてのリスナーに対して、リモート ホストからの着信接続を制御する一連の規則を定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうかを定義できます。AsyncOS では、ホスト アクセス テーブル（HAT）を使用してリスナーへの接続が許可されるホストを定義できます。

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。設定されたどのリスナーにも独自の HAT があります。パブリック リスナーおよびプライベート リスナーの両方に HAT を設定します。

リモート ホストからの着信接続を制御するには、次の情報を定義します。

- **リモート ホスト。**リモート ホストがリスナーに接続を試みる方法を定義します。リモート ホスト定義を送信者グループにグループ化します。たとえば、IP アドレスとホスト名の一部を使用して、送信者グループの複数のリモート ホストを定義できます。IP レピュテーションスコアでリモートホストを定義することもできます。詳細については、送信者グループへのリモート ホストの定義 （3 ページ）を参照してください。

- **アクセス ルール。**送信者グループに定義されたリモート ホストがリスナーに接続するのを許可するのか、またどのような条件下なのかを定義できます。アクセス ルールは、メール フロー ポリシーを使って定義します。たとえば、特定の送信者グループのリスナーへの接続を許可するよう定義できますが、接続ごとに最大メッセージ数だけを許可します。詳細については、メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （9 ページ）を参照してください。

[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページで、リスナーへの接続が許可されるホストを定義します。

リスナーが TCP 接続を受信すると、設定された送信者グループに対して送信元 IP アドレスを比較します。また、[HAT概要（HAT Overview）] ページにリストされている順序で送信者グループを評価します。一致が見つかると、設定済みのメール フロー ポリシーを接続に適用します。1 つの送信者グループ内に複数の条件が設定されている場合、いずれかの条件が一致すると、その送信者グループは一致します。

リスナーを作成すると、AsyncOS は、リスナーに定義済みの送信者グループとメール フロー ポリシーを作成します。定義済みの送信者グループとメール フロー ポリシーを編集して新しい送信者グループとメール フロー ポリシーを作成できます。詳細については、定義済みの送信者グループとメール フロー ポリシーの理解 （12 ページ）を参照してください。

ホストアクセステーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセステーブル情報をリスナー用の電子メールゲートウェイにインポートできます。このとき、設定されているすべてのホストアクセステーブル情報は上書きされます。詳細については、ホスト アクセス テーブルの設定の使用 （26 ページ）を参照してください。

関連項目

- デフォルト HAT エントリ （2 ページ）

デフォルト HAT エントリ

HAT は、デフォルトでは、リスナーのタイプによって異なるアクションを実行するように定義されています。

- **パブリック リスナー。**HAT は、すべてのホストからの電子メールを受け入れるように設定されます。
- **プライベート リスナー。**HAT は、指定したホストからの電子メールをリレーし、他のすべてのホストを拒否するように設定されます。

[HAT概要（HAT Overview）] では、デフォルトのエントリに「ALL」という名前が付けられます。[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページですべての送信者グループのメール フロー ポリシーをクリックしてデフォルト エントリを編集できます。

（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` および `systemsetup` コマンドは、ユーザがシステムをオープン リレーとして意図せずに設定するのを防ぎます。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。

送信者グループへのリモート ホストの定義

リモート ホストがリスナーに接続しようとする方法を定義できます。リモート ホスト定義を送信者グループにグループ化します。送信者グループは、それらの送信者からの電子メールを処理するために定義されたリモート ホストのリストです。

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（IPv4 または IPv6）
- IP 範囲
- 具体的なホスト名またはドメイン名
- IP レピュテーションサービスの「組織」分類
- IP レピュテーションスコア（IPRS）の範囲（またはスコアの欠如）
- DNS リスト クエリー応答

送信者グループの受け入れ可能なアドレスのリストの詳細については、送信者グループの構文（4 ページ）を参照してください。

SMTP サーバが電子メールゲートウェイとの SMTP 接続を試みると、リスナーは送信者グループを順番に評価し、IP レピュテーションスコア、ドメイン、または IP アドレスといった送信者グループの任意の条件に一致する場合、送信者グループに SMTP 接続を割り当てます。

（注） ダブル 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 アドレスを取得してその有効性を検証します。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。

[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページで送信者グループを定義します。

関連項目

- 送信者グループの構文 （4 ページ）
- 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 （5 ページ）
- IP レピュテーションスコアを使用した送信者グループの定義 （7 ページ）
- 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 （8 ページ）

送信者グループの構文

表 *1: 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:n:n:n:n`	IPv6 アドレス。先行ゼロを含める必要はありません。
`n:n:n:n:n:n:n:n-n:n:n:n:n:n:n:n` `n:n:n-n:n:n:n:n`	IPv6 アドレスの範囲。先行ゼロを含める必要はありません。
`n.n.n.n`	フル（完全な）IPv4 アドレス

`n.n.n.`
`n.n.n.`
`n.n.`
`n.n.`
`n.`
	部分的な IPv4 アドレス

`n.n.n.n-n.`
`n.n.n.n-n.`
`n.n.n-n.`
`n.n-n.`
`n.n-n`
`n-n.`
`n-n`
	IPv4 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`
	IPv4 CIDR アドレス ブロック

`n:n:n:n:n:n:n:n/c`	IPv6 CIDR アドレス ブロック。先行ゼロを含める必要はありません

構文	意味
SBRS[n:n]SBRS[none]	IP レピュテーションスコア詳細については、IP レピュテーションスコアを使用した送信者グループの定義 （7 ページ）を参照してください。
SBO:n	ネットワークオーナー識別番号。詳細については、IP レピュテーションスコアを使用した送信者グループの定義 （7 ページ）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、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 （8 ページ）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、IP レピュテーションサービスは、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 アドレスは、送信元メール ホストの IP アドレスとして定義します。電子メールゲートウェイ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 IP バージョン 6（IPv6）アドレスをサポートします。

ドメインは、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。

ネットワーク オーナーは、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。

組織は、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。組織はネットワーク オーナー、ネットワーク オーナー内の部門、そのネットワーク オーナーの顧客のいずれかになります。

関連項目

- HAT に基づくポリシーの設定 （6 ページ）

HAT に基づくポリシーの設定

次の表に、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 *2:* 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。IP レピュテーションサービスは、電子メールの送信元について組織レベルまで独自に把握しており、電子メールゲートウェイはそれを利用して、組織に基づくポリシーを自動的に適用します。上の例で、ユーザがホスト アクセス テーブル（HAT）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、電子メールゲートウェイは、Macromedia Inc.、Alloutdeals.com、および Greatoffers.com に対して最大 10 人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 人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。

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。

- **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。**

  着信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、IP レピュテーションサービスにクエリを実行することで得られます。IP レピュテーションサービスは、送信者の相対的な規模に関する情報を提供します（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。

- **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、電子メールゲートウェイ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、電子メールゲートウェイ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、電子メールゲートウェイ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、ネットワークーナーとSENDERBASE組織の差別化を使用して、SENDERBASE内のロジックに基づき、送信者ごと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、「電子メール セキュリティ モニタの使用方法」の章を参照してください。

IP レピュテーションスコアを使用した送信者グループの定義

電子メールゲートウェイは、IP レピュテーションサービスに対してクエリを実行し、IP レピュテーションスコアを決定できます。IP レピュテーションスコアは、IP レピュテーション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、次の表に示すように、-10.0 ～ +10.0 です。

表 *3 : IP* レピュテーションスコアの定義

スコア（Score）	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）

IP レピュテーションスコアを使用して、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 電子メールゲートウェイを設定します。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。メッセージ処理の送信者グループの作成 （16 ページ）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、IP レピュテーションスコアを含めるための構文については次の表を参照してください。

表 *4: IP* レピュテーションスコアの構文

`SBRS[ n n`	IP レピュテーションスコアIP レピュテーションサービスにクエリを実行すると、送信者が識別され、スコアが範囲内で定義されます。
SBRS[none]	IP 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 IP レピュテーション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、IP レピュテーション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。

IP レピュテーションサービスにクエリを実行するようにリスナーを設定するには、[ネットワーク（Network）]>[リスナー（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、 電子メールゲートウェイが IP レピュテーションサービスにクエリ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 [メールポリシー（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、IP レピュテーションサービスに対してルックアップを使用する際のさまざまなポリシーを設定できます。

（注） メッセージフィルタを作成して IP レピュテーションスコアに「しきい値」を指定し、システムで処理されるメッセージにさらにアクションを実行できます詳細については、「アンチスパム」および「アンチウィルス」の章の「IP レピュテーションルール」、「アンチスパムシステムのバイパスアクション」、および「アンチウイルスシステムのバイパスアクション」を参照してください。

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（「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」の章の「DNS リスト ルール」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（「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」の章の「DNS リスト ルール」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。クエリのテスト、DNS クエリの一般的な設定、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 Cisco Systems 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ALLOWED_LIST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）、その内容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。

メールフローポリシーを使用した電子メール送信者のアクセス ルールの定義

メール フロー ポリシーでは SMTP カンバセーション中の送信者からリスナーへの電子メール メッセージのフローを制御または制限することができます。メール フロー ポリシーに次のパラメータ タイプを定義することで SMTP カンバセーションを制御します。

- 接続ごとの最大メッセージ数などの接続パラメータ。
- 1 時間あたりの受信者の最大数など、レート制限パラメータ。
- SMTP カンバセーション中に通信するカスタム SMTP コードと応答を変更します。
- スパム検出の有効化。
- ウイルス保護の有効化。
- TLS を使った SMTP 接続の暗号化などの暗号化。
- DKIM を使った着信メールの確認などの認証パラメータ。

最後に、メール フロー ポリシーが、リモート ホストからの接続に対し、次のいずれかのアクションを実行します。

- **承認（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。

- **拒否（REJECT）**。接続は、最初は許可されますが、接続しようとするクライアントは、4XX または 5XX SMTP のステータス コードを取得します。どの電子メールも許可されません。

（注） また、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）でこの拒否を実行するように、AsyncOS を設定できます。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` コマンドから設定されます。詳細については、CLI を使用してリスナーを作成することによる接続要求のリスニングを参照してください。

- **TCPREFUSE**。TCP レベルで接続は拒否されます。
- **リレー（RELAY）**。接続は許可されます。すべての受信者の受信は許可され、受信者アクセス テーブルで制限されません。
- **継続（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、GUI での HAT の編集を容易にするために使用されます。詳細については、メッセージ処理の送信者グループの作成 （16 ページ）を参照してください。

関連項目

- HAT 変数の構文 （10 ページ）

HAT 変数の構文

次の表では、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: 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	電子メールゲートウェイ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。

変数	定義
$OrgID	SenderBase 組織 ID（整数値）で置き換えられます。 電子メールゲートウェイが SENDERBASE 組織 ID を取得できないか、IP レピュテーション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。

関連項目

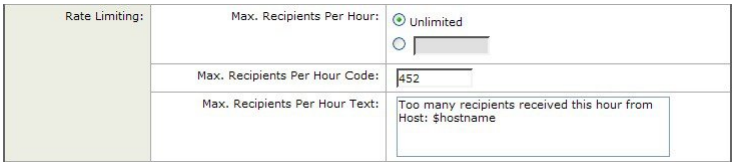
- HAT 変数の使用 （11 ページ）
- HAT 変数のテスト （12 ページ）

HAT 変数の使用

（注） これらの変数は、「ゲートウェイでのメール受信の設定」の章で説明する高度な HAT パラメータ `smtp_banner_text` と `max_rcpts_per_hour_text` と併用できます。

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 *1 : 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、 電子メールゲートウェイ上のリスナーの $ALLOWED_LIST 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。次に例を示します。

```
# telnet
IP_address_of_Email_Security_Appliance port

220 hostname
 ESMTP

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

定義済みの送信者グループとメール フロー ポリシーの理解

次の表では、パブリック リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 *6:* 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

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
ALLOWED_LIST	信頼する送信者を ALLOWED_LIST 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。	$TRUSTED

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
BLOCKED_LIST	BLOCKED_LIST送信者グループ内の送信者は、メールフローポリシー$BLOCKEDで設定されたパラメータによって拒否されます。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。	$BLOCKED
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、 SenderBase レピュテーション サービスに対してクエリーが実行されます。	$THROTTLED

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
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、Anti-Spam ソフトウェア（システムで有効になっている場合）、アンチウイルス スキャン エンジン、および IP レピュテーション 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、ウイルス スキャンを参照してください。IP レピュテーション サービスの詳細については、IP レピュテーション サービスを参照してください。	$ACCEPTED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、デフォルト HAT エントリ （2 ページ）を参照してください。	$ACCEPTED

次の表では、プライベート リスナーの作成時に設定される定義済みの送信者グループとメール フロー ポリシーをリストします。

表 *7:* 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

定義済みの送信者グループ	説明	デフォルトで設定されるメール フロー ポリシー
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） RELAYLIST 送信者グループにはシステム設定ウィザードを実行したときに電子メールのリレーが許可されるシステムが含まれます。	$RELAYED
ALL	その他すべての送信者に適用されるデフォルトの送信者グループ。詳細については、デフォルト HAT エントリ （2 ページ）を参照してください。	$BLOCKED

（注） イーサネットポートが2つしかない電子メールゲートウェイモデルのシステム設定ウィザードを実行すると、1人のリスナーだけを作成するように促されます。また、内部システム用のメールのリレーに使用される$RELAYED メール フロー ポリシーも含まれるパブリック リスナーを作成します。3 つ以上のイーサネットポートを持つ 電子メールゲートウェイモデルについては、RELAYLIST送信者グループと $RELAYED メールフローポリシーがプライベートリスナーだけに表示されます。

送信者グループからのメッセージの同様の処理

リスナーが送信者からのメッセージを処理する方法を設定するには、[メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] と [メールフローポリシー（Mail Flow Policy）] ページで行います。これは、送信者グループとメール フロー ポリシーを作成、編集、および削除することにより行います。

関連項目

- メッセージ処理の送信者グループの作成 （16 ページ）
- 既存の送信者グループへの送信者の追加 （17 ページ）

- 着信接続のために実行するルールの順序の並べ替え （17 ページ）
- 送信者の検索 （18 ページ）
- メール フロー ポリシーを使用した電子メール送信者のアクセス ルールの定義 （9 ページ）
- メール フロー ポリシーのデフォルト値の定義 （26 ページ）

メッセージ処理の送信者グループの作成

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 [送信者グループを追加（Add Sender Group）] をクリックします。

ステップ 4 送信者グループの名前を入力します。

ステップ 5 送信者グループのリストに配置する順序を選択します。

ステップ 6 （任意）たとえば、送信者グループまたはその設定についての情報などのコメントを入力します。

ステップ 7 この送信者グループを適用するメール フロー ポリシーを選択します。

（注） 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。

ステップ 8 （任意）DNS リストを選択します。

ステップ 9 （任意） IP レピュテーションスコアに情報がない送信者を含めます。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 10 （任意）DNS リストを入力します。

ステップ 11 （任意）ホスト DNS 検証設定を構成します。

詳細については、未検証の送信者へのより厳格なスロットリング設定の実行 （37 ページ）を参照してください。

ステップ 12 [送信（Submit）] をクリックして、送信者グループを作成します。

ステップ 13 新しく作成した送信者グループをクリックします。

ステップ 14 [送信者を追加（Add Sender）] をクリックして、送信者グループに送信者を追加します。

- 送信者の IP アドレスを追加します。[IPアドレス（IP Addresses）] を選択して IPv4 アドレス、IPv6 アドレス、またはホスト名を追加し、変更を送信します。

  送信者は、IP アドレスおよびホスト名の一部の範囲を含めることができます。

- 送信者の国を追加します。 [地理位置情報（Geolocation）] を選択し、変更を送信します。

ステップ 15 変更を送信し、保存します。

次のタスク

関連項目

- リスナーの IP レピュテーション フィルタリング スコアのしきい値の編集

既存の送信者グループへの送信者の追加

手順

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、[送信者グループに追加（Add to Sender Group）] リンクをクリックします。

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 変更を送信し、保存します。

（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、[送信者グループに追加（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（4 ページ）を参照してください。

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。

ステップ 4 [保存（Save）] をクリックして送信者を追加し、[受信メールの概要（Incoming Mail Overview）] ページに戻ります。

次のタスク

関連項目

- スパムフィルタからの 電子メールゲートウェイ生成メッセージの保護
- メッセージがスパムかどうかスキャンするための 電子メールゲートウェイの設定方法

着信接続のために実行するルールの順序の並べ替え

リスナーに送信者グループを追加すると、送信者グループの順序を編集する必要があります。

リスナーに接続しようとするホストごとに、HAT は上から下へ順番に読み込まれます。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。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 [順番を編集（Edit Order）] をクリックします。

ステップ 4 HAT の送信者グループの既存の行の新しい順序を入力します。

シスコはデフォルトの順序を維持することを推奨します（RELAYLIST（特定のハードウェアモデルのみ）の後に ALLOWED_LIST、BLOCKED_LIST、SUSPECTLIST、および UNKNOWNLIST が続く）。

ステップ 5 変更を送信し、保存します。

送信者の検索

[HAT概要（HAT Overview）] ページの上部にある [送信者を検索（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[検索（Find）] をクリックします。

メール フロー ポリシーを使用した着信メッセージのルールの定義

メール フロー ポリシーを作成する前に、次のルールとガイドラインを考慮してください。

- [デフォルトを使用（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。デフォルト値を定義するには、メール フロー ポリシーのデフォルト値の定義 （26 ページ）を参照してください。
- 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 アクセプト クエリーを設定しておく必要があります）。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] ページに移動します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 次の表で説明する情報を入力します。

表 *8:* メール フロー ポリシー パラメータ

パラメータ	説明
接続	
最大メッセージ サイズ（Maximum message size）	このリスナーが許可す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。
単一 IP からの最大同時接続数（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。
接続あたりの最大メッセージ数	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。
メッセージあたりの最大受信者数	このホストから許可されるメッセージあたりの受信者の最大数。
SMTP バナー	
カスタム SMTP バナー コード（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。
カスタム SMTP バナー テキスト（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。 （注） このフィールドには一部の変数を使用できます。詳細については、HAT 変数の構文 （10 ページ）を参照してください。
カスタム SMTP 拒否バナー コード（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。
カスタム SMTP 拒否バナー テキスト（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。

パラメータ	説明
SMTP バナー ホスト名を上書き（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電子メールゲートウェイに追加されます（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。
ホストのレート制限	
1時間あたりの最大受信者数（Max. 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。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じ IP アドレス（送信者）が複数のリスナーに接続されるとレート制限を超える可能性が高くなります。 （注） このフィールドには一部の変数を使用できます。詳細については、HAT 変数の構文 （10 ページ）を参照してください。
時間コードあたりの最大受信者数（Max. Recipients per Hour 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。
1時間あたりの最大受信者数の超過テキスト（Max. Recipients Per Hour Exceeded 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。
送信者のレート制限	
時間間隔あたりの最大受信者数（Max. Recipients per Time Interval）	このリスナーがメール送信者アドレスに基づいて一義的なエンベロープ送信者から受信する指定した期間中の最大受信者数。最大受信者数はグローバルに追跡されません。各リスナーは各レート制限のしきい値を追跡します。ただし、すべてのリスナーは単一のカウンタに対して検証するので、同じメール送信者アドレスからのメッセージが複数のリスナーによって受信されるとレート制限を超える可能性が高くなります。 デフォルトの最大受信者数を使用するか、無制限の受信者を許可するか、または別の最大受信者数を指定するか選択します。 他のメール フロー ポリシーによってデフォルトで使用される、最大受信者数と時間間隔を指定するデフォルトのメール フロー ポリシー設定を使用します。時間間隔はデフォルトのメール フロー ポリシーを使用してしか指定できません。

パラメータ	説明
送信者のレート制限超過エラー コード（Sender Rate Limit Exceeded Error Code）	SMTP コードは、エンベロープがこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
送信者のレート制限超過エラー テキスト（Sender Rate Limit Exceeded Error Text）	SMTP バナー テキストは、エンベロープの送信者がこのリスナーに対して定義された時間間隔の最大受信者数を超えた場合に返されます。
例外	特定のエンベロープ送信者を定義されているレート制限から免除する場合は、そのエンベロープ送信者を含むアドレス リストを選択します。詳細については、着信接続ルールへの送信者アドレス リストの使用 （28 ページ）を参照してください。
フロー制御（Flow Control）	
Use SenderBase for Flow Control	このリスナーに対して IP レピュテーションサービスでの「検索」を有効にします。
IP アドレスの類似性でグループ化：（有効ビット範囲 0 ～ 32）（Group by Similarity of IP Addresses: (significant bits 0-32)）	リスナーのホスト アクセス テーブル（HAT）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。[SenderBase を使用（Use SenderBase）] をディセーブルにする必要があります。HAT Significant Bits の詳細については、ルーティングおよび配信機能の設定を参照してください。
ディレクトリ獲得攻撃防御（DHAP）	
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	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 拒否と SMTP コールアヘッド サーバプロファイル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（関連付けられたリスナーの LDAP 承認設定に設定されたとおり）。LDAP アクセプト クエリーの DHAP の設定の詳細については、LDAP クエリに関する作業を参照してください。

パラメータ	説明
ディレクトリ獲得攻撃防御：SMTP 対話内で DHAP しきい値に到達した場合、接続をドロップ（Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is Reached within an SMTP Conversation）	電子メールゲートウェイは、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。
時間コードあたりの無効な受信者の最大数（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。
時間テキストあたりの無効な受信者の最大数（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。
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）	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。
時間コードあたりの無効な受信者の最大数（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。
時間テキストあたりの無効な受信者の最大数（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。

パラメータ	説明
スパム検出	
アンチスパム スキャン（Anti-spam scanning）	このリスナー上でアンチスパム スキャンを有効にします。
ウイルス検出	
アンチウイルス スキャン	このリスナー上でアンチウイルス スキャンを有効にします。
送信者ドメインのレピュテーションの検証	
送信者ドメインのレピュテーションの検証	送信者ドメインのレピュテーションの検証を有効にします。
暗号化と認証	
TLS	このリスナーに対する SMTP カンバセーションのトランスポート レイヤ セキュリティ（TLS）の拒否、推奨、必須を設定します。 [推奨（Preferred）] を選択すると、ドメインおよび電子メール アドレスを指定するアドレス リストを選択することによって、特定のドメインまたは特定の電子メールアドレスを持つドメインのエンベロープ送信者に対して TLS を必須に設定できます。このリストのドメインまたはアドレスに一致するエンベロープ送信者が TLS を使用しない接続経由でメッセージを送信しようとすると、 電子メールゲートウェイは接続を拒否し、送信者は再び TLS を使用して送信を試みる必要があります。 [クライアント証明書の検証（Verify Client Certificate）] オプションは、クライアント認証が有効な場合、 電子メールゲートウェイがユーザのメールアプリケーションと TLS 接続を確立するように指示します。TLS 推奨設定にこのオプションを選択した場合、ユーザが証明書を持たない場合にも電子メールゲートウェイは非TLS接続を許可しますが、ユーザが無効な証明書を持っている場合は、接続を拒否します。TLS 必須設定の場合、このオプションを選択すると、電子メールゲートウェイが接続を許可するために有効な証明書が必要になります。 アドレス リストの作成の詳細については、着信接続ルールへの送信者アドレス リストの使用 （28 ページ）を参照してください。 TLS 接続のクライアント証明書を使用する方法については、電子メールゲートウェイからの TLS 接続の確立を参照してください。
SMTP 認証	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、「LDAP クエリー」の章で詳細を説明します。

パラメータ	説明
TLS と SMTP 認証の両方が有効化されている場合（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。
ドメイン キー/DKIM署名（Domain Key/DKIM Signing）	このリスナーでドメイン キーまたはDKIM署名を有効にします。（承認およびリレーのみ）。
DKIM検証	DKIM 検証をイネーブルにします。
S/MIME の復号と検証	
S/MIME の復号/検証	• S/MIME の復号または検証を有効にします。 • S/MIME の検証後、デジタル署名を維持するかメッセージから削除するかを選択します。トリプルラップされたメッセージの場合、内部署名のみが維持または削除されます。
S/MIME 公開キーの収集	
S/MIME公開キーの収集	S/MIME 公開キーの収集をイネーブルにします。
検証エラー時の証明書の収集	署名された着信メッセージの検証に失敗した場合、公開キーを収集するかどうかを選択します。
更新された証明書の保存	更新された公開キーを収集するかどうかを選択します。
SPF/SIDF 検証	
SPF/SIDF検証のイネーブル化（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、電子メール認証を参照してください。
準拠レベル（Conformance Level）	SPF/SIDF 準拠レベルを設定します。[SPF]、[SIDF]、[SIDF互換（SIDF Compatible）] のいずれかを選択します。詳細は、電子メール認証を参照してください。

パラメータ	説明
「Resent-Sender:」または「Resent-From:」を使用した場合、PRA 検証結果をダウングレードします:（Downgrade PRA verification result if 'Resent-Sender:' or 'Resent-From:' were used:）	準拠レベルとして [SIDF互換（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テスト（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互換（SIDF Compatible）] 準拠レベルで使用します）。
DMARC 検証	
DMARC検証のイネーブル化（Enable DMARC Verification）	このリスナーで DMARK 検証をイネーブルにします。詳細については、DMARC 検証を参照してください。
DMARC検証プロファイルを使用（Use DMARC Verification Profile）	このリスナーで使用する DMARK 検証プロファイルを選択します。
DMARCフィードバックレポート（DMARC Feedback Reports）	DMARC 集計フィードバック レポートの送信をイネーブルにします。 DMARC 集計フィードバックレポートの詳細については、DMARC 集計レポートを参照してください。 （注） DMARC を指定するには、フィードバック レポート メッセージが DMARC に準拠している必要があります。これらのメッセージに DKIM 署名が付いていることを確認するか、または適切な SPF レコードをパブリッシュする必要があります。
タグなしバウンス	
タグなしバウンスを有効と見なす（Consider Untagged Bounces to be Valid）	バウンス検証タギング（「ルーティングおよび配信機能の設定」の章で説明）がイネーブルになっている場合にだけ適用されます。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みなし、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。タグの付いていないバウンスを有効とみなすことを選択した場合、 電子メールゲートウェイはバウンスメッセージを受け入れます。

パラメータ	説明
エンベロープ送信者の DNS 検証	
	送信者の検証 （31 ページ）を参照してください。
例外テーブル	
例外テーブルを使用（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 つだけ使用できますが、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 （35 ページ）を参照してください。

（注） アンチスパムまたはアンチウイルススキャンが HAT でグローバルに有効な場合、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のために電子メールゲートウェイによって受け入れられると同時にフラグが付けられます。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 スキャンが無効にされた場合、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。

ステップ 4 変更を送信し、保存します。

メール フロー ポリシーのデフォルト値の定義

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] をクリックします。

ステップ 2 [リスナー（Listener）] フィールドで編集するリスナーを選択します。

ステップ 3 設定したメール フロー ポリシーの下の [デフォルトポリシーパラメータ（Default Policy Parameters）] リンクをクリックします。

ステップ 4 このリスナーのすべてのメール フロー ポリシーで使用するデフォルト値を定義します。

プロパティの詳細については、メール フロー ポリシーを使用した着信メッセージのルールの定義 （18 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。

ホスト アクセス テーブルの設定の使用

ホストアクセステーブルに格納されているすべての情報をファイルにエクスポートし、ファイルに格納されているホストアクセステーブル情報をリスナー用の電子メールゲートウェイにイ

ンポートできます。このとき、既存のすべてのホストアクセステーブル情報は上書きされます。

関連項目

- 外部ファイルへの ホスト アクセス テーブル設定のエクスポート （27 ページ）
- 外部ファイルからのホスト アクセス テーブル設定のインポート （27 ページ）

外部ファイルへの ホスト アクセス テーブル設定のエクスポート

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 [リスナー（Listener）] メニューで編集するリスナーを選択します。
ステップ 3 [HATをエクスポート（Export HAT）] をクリックします。
ステップ 4 エクスポートする HAT のファイル名を入力します。これは、 電子メールゲートウェイ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 5 変更を送信し、保存します。

外部ファイルからのホスト アクセス テーブル設定のインポート

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。

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] ページに移動します。
ステップ 2 [リスナー（Listener）] メニューで編集するリスナーを選択します。
ステップ 3 [HATをインポート（Import HAT）] をクリックします。
ステップ 4 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、電子メールゲートウェイの configuration ディレクトリに存在する必要があります。

ステップ 5 [送信（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 6 [インポート（Import）] をクリックします。
ステップ 7 変更を保存します。

ファイル内に「コメント」を配置できます。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。

```
# File exported by the GUI at 20060530T215438
$BLOCKED
    REJECT {}
[ ... ]
```

着信接続ルールへの送信者アドレス リストの使用

メール フロー ポリシーは、レート制限の除外、および必須 TLS 接続などのエンベロープ送信者グループに適用する特定の設定にアドレス リストを使用できます。アドレス リストは、電子メールアドレス、ドメイン、部分ドメインおよびIPアドレスで構成できます。GUIで[メールポリシー（Mail Policies）]>[アドレスリスト（Address Lists）]のページを使用するか、またはCLIの`addresslistconfig`コマンドを使用し、アドレスリストを作成できます。[アドレスリスト（Address Lists）]ページには、アドレスリストを使用するメールフローポリシーと共に、電子メールゲートウェイのすべてのアドレスリストが表示されます。

手順

ステップ 1 [メールポリシー（Mail Policies）]>[アドレスリスト（Address Lists）]を選択します。

ステップ 2 [アドレスリストの追加（Add Address List）]をクリックします。

ステップ 3 アドレス リストの名前を入力します。

ステップ 4 アドレス リストの説明を入力します。

ステップ 5 （任意）アドレス リストで完全な電子メール アドレスを使用することを義務付けるには、[完全電子メールアドレスのみ（Full Email Addresses only）]を選択します。

ステップ 6 アドレス リストを作成するには、次のオプションのいずれかを選択します。

- アドレスリストで完全な形式の電子メールアドレスを使用することを義務付ける場合は、[完全電子メールアドレスのみ（Full Email Addresses only）]を選択します。
- アドレスリストでドメインを使用することを義務付ける場合は、[ドメインのみ（Domains only）]を選択します。
- アドレス リストで IP アドレスを使用することを義務付ける場合は、[IPアドレスのみ（IP Addresses only）]を選択します。

ステップ 7 追加するアドレスを入力します。次の形式を使用できます。

- 完全な電子メール アドレス：`user@example.com`
- 電子メール アドレスの一部：`user@`

  （注） [完全Eメールアドレスのみ許可（Allow only full Email Addresses）]を選択した場合は、電子メール アドレスの一部は使用できません。

- 電子メール アドレスの IP アドレス：`@[1.2.3.4]`
- ドメインのすべてのユーザ：`@example.com`

- 部分ドメインのすべてのユーザ：`@.example.com`

ドメインおよび IP アドレスは @ 文字で開始する必要があることに注意してください。

カンマで電子メールアドレスを区切ります。新しい行を使ってアドレスを区切る場合、AsyncOS は自動的にエントリをカンマで区切られたリストに変換します。

ステップ 8 変更を送信し、保存します。

SenderBase 設定とメール フロー ポリシー

電子メールゲートウェイへの接続を分類し、メールフローポリシーを適用するには（レート制限が含まれる場合と含まれない場合がある）、リスナーは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、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 （5 ページ）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。

- ネットワークオーナーによって分類が行われた場合、IP レピュテーション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）。

- 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、IP レピュテーションフィルタおよび IP プロファイリングのサポートが、パブリックリスナーに対しては有効で、プライベートリスナーに対しては無効です。

関連項目

- HAT Significant Bits 機能 （30 ページ）

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」を無効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 情報サービスを有効にするための質問「Would you like to enable 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 （30 ページ）
- Significant Bits HAT ポリシー オプション （30 ページ）
- インジェクション制御期間 （31 ページ）

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。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 に表示されます。

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。

`listenerconfig` コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

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。`listenerconfig` コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

送信者の検証

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、電子メールゲートウェイ上のメールパイプラインを介し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 電子メールゲートウェイを設定できます。

送信者検証機能は、次のコンポーネントで構成されます。

- **接続ホストの検証（Verification of the connecting host）**。これは、SMTP カンバセーションの前に実行されます。詳細については、送信者検証：ホスト （32 ページ）を参照してください。

- **エンベロープ送信者のドメイン部分の検証（Verification of the domain portion of the envelope sender）**。これはSMTPカンバセーションの中で実行されます。詳細については、送信者検証：エンベロープ送信者 （33 ページ）を参照してください。

関連項目

- 送信者検証：ホスト （32 ページ）
- 送信者検証：エンベロープ送信者 （33 ページ）
- 送信者検証の実装 — 設定例 （35 ページ）
- 未検証送信者からのメッセージの設定テスト （39 ページ）
- 送信者検証とロギング （40 ページ）

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。

電子メールゲートウェイは、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。ダブル DNS ルックアップの実行によって、リモート ホストの IP アドレス（つまり、ドメイン）が取得され、有効性が検証されます。ダブル 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、 電子メールゲートウェイは 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 [接続ホストのDNS検証（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 を使用した未検証の送信者からのメッセージのスロットリング （36 ページ）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 ALLOWED_LIST に対してホスト DNS 検証を有効にすると、未検証の送信者からのメールが、ALLOWED_LIST 内の信頼できる送信者からのメールと同様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）。ドメインは、DNS で確認試行がタイムアウトまたは DNS サーバの障害などの一時的なエラー状態が発生したかを解決できません。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「存在しないドメインのエンベロープ送信者」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。

（注） DNS 応答が「NOERROR」の場合、送信者検証は MX レコードのないドメインを拒否します。

ただし DNS サーバが「SERVERFAIL」を返した場合、DNS サーバは「応答がないドメインのエンベロープ送信者」カテゴリに分類されます。SERVFAIL は、ドメインが存在しないが、DNS でレコードのルックアップ中に一時的な問題が発生していることを示します。

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 を拒否するように電子メールゲートウェイを設定できます。

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 （35 ページ）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。

関連項目

- 部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM （34 ページ）
- カスタム SMTP コードと応答 （34 ページ）
- 送信者検証：エンベロープ送信者 （33 ページ）

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（「ゲートウェイでのメール受信の設定」の章の「SMTPアドレス解析オプション」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。 電子メールゲートウェイ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有効化されます。

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、受信者アクセステーブル（RAT）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 [メールポリシー（Mail Policies）]>[例外テーブル（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 を使用した未検証送信者への送信メッセージの定義 （37 ページ）を参照）または CLI（『*CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway*』を参照）でポリシーごとに有効化されます。

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。

例外テーブルの変更については送信者の電子メールアドレスに基づいた送信者検証ルールからの未検証送信者の除外 （38 ページ）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。

次の表に、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 9: 送信者検証：推奨される設定

送信者グループ	ポリシー	含める
UNVERIFIED SUSPECTLIST	THROTTLEMORE THROTTLED	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。 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。

関連項目

- 送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング （36 ページ）
- 未検証の送信者へのより厳格なスロットリング設定の実行 （37 ページ）
- メール フロー ポリシー ACCEPTED を使用した未検証送信者への送信メッセージの定義 （37 ページ）
- 送信者の電子メールアドレスに基づいた送信者検証ルールからの未検証送信者の除外 （38 ページ）
- 送信者検証例外テーブル内でのアドレスの検索 （38 ページ）

送信者グループ SUSPECTLIST を使用した未検証の送信者からのメッセージのスロットリング

手順

ステップ 1 [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] を選択します。

ステップ 2 送信者グループのリストで [SUSPECTLIST] をクリックします。

ステップ 3 [設定を編集（Edit Settings）] をクリックします。

ステップ 4 リストから [スロットル（THROTTLED）] ポリシーを選択します。

ステップ 5 [接続ホストのDNS検証（Connecting Host DNS Verification）] の中の [接続ホスト逆引きDNS検索（PTR）が転送DNS検索（A）と一致しない（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、保存します。

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。

未検証の送信者へのより厳格なスロットリング設定の実行

手順

ステップ 1 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。

a) [メールフローポリシー（Mail Flow Policies）] ページで [ポリシーを追加（Add Policy）] をクリックします。
b) メール フロー ポリシーの名前を入力し、[接続動作（Connection Behavior）] として [承認（Accept）] を選択します。
c) 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。
d) 変更を送信し、保存します。

ステップ 2 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。

a) [HAT概要（HAT Overview）] ページで [送信者グループを追加（Add Sender Group）] をクリックします。
b) リストから [THROTTLEMORE] ポリシーを選択します。
c) [接続ホストのDNS検証（Connecting Host DNS Verification）] 中の [接続ホストのPTRレコードがDNSに存在しません（Connecting host PTR record does not exist in DNS）] チェックボックスをオンにします。
d) 変更を送信し、保存します。

メール フロー ポリシー **ACCEPTED** を使用した未検証送信者への送信メッセージの定義

手順

ステップ 1 [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] を選択します。

ステップ 2 [メールフローポリシー（Mail Flow Policies）] ページで、メール フロー ポリシー [承認（ACCEPTED）] をクリックします。

ステップ 3 [送信者の検証（Sender Verification）] セクションまでスクロールします。

ステップ 4 [エンベロープ送信者 DNS の検証（Envelope Sender DNS Verification）] セクションで、次を実行します。

- [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。
- 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 [ドメイン例外テーブルの使用（Use Domain Exception Table）] セクションで [オン（On）] を選択して、ドメイン例外テーブルを有効にします。

ステップ 6 変更を送信し、保存します。

送信者の電子メール アドレスに基づいた送信者検証ルールからの未検証送信者の除外

手順

ステップ 1 [メールポリシー（Mail Policies）] > [例外テーブル（Exception Table）] を選択します。

（注） 例外テーブルは、[例外テーブルを使用（Use Exception Table）] がイネーブルに設定され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ます。

ステップ 2 [メールポリシー（Mail Policies）] > [例外テーブル（Exception Table）] ページで [ドメイン例外を追加（Add Domain Exception）] をクリックします。

ステップ 3 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 4 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 5 変更を送信し、保存します。

送信者検証例外テーブル内でのアドレスの検索

手順

ステップ 1 [例外テーブル（Exception Table）] ページの [ドメイン例外の検索（Find Domain Exception）] セクションに電子メール アドレスを入力します。

ステップ 2 [検索（Find）] をクリックします。

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。

未検証送信者からのメッセージの設定テスト

これで送信者検証設定を完了したため、電子メールゲートウェイ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。

関連項目

- 形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信 （39 ページ）
- 送信者検証ルールから除外するアドレスからのメッセージの送信 （39 ページ）

形式が不正な MAIL FROM 送信者アドレスのテスト メッセージの送信

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。

手順

ステップ 1 電子メールゲートウェイへの 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電子メールゲートウェイを設定した場合や、アドレス解析をイネーブルにした場合は（「ゲートウェイでのメール受信の設定」の章を参照）、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_Email_Security_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。

送信者検証ルールから除外するアドレスからのメッセージの送信

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。

手順

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 変更を保存します。

ステップ 3 電子メールゲートウェイへの 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_Email_Security_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。

関連項目

- エンベロープ送信者検証 （40 ページ）

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
```

翻訳について
このドキュメントは、米国シスコ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。