ルーティングおよび配信機能の設定

この章は、次の項で構成されています。

- ローカル ドメインの電子メールのルーティング （1 ページ）
- アドレスの書き換え （7 ページ）
- エイリアス テーブルの作成 （8 ページ）
- マスカレードの構成 （16 ページ）
- ドメイン マップ機能 （26 ページ）
- バウンスした電子メールの処理 （32 ページ）
- 宛先制御による電子メール配信の管理 （42 ページ）
- バウンス検証 （52 ページ）
- 電子メール配信パラメータの設定 （57 ページ）
- Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （60 ページ）
- グローバル配信停止機能の使用 （69 ページ）
- 確認：電子メール パイプライン （73 ページ）

ローカル ドメインの電子メールのルーティング

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

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

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

関連項目

- SMTP ルートの概要 （2 ページ）
- デフォルトの SMTP ルート （3 ページ）
- SMTP ルートの定義 （3 ページ）
- SMTP ルートの制限 （4 ページ）
- SMTP ルートと DNS （4 ページ）
- SMTP ルートおよびアラート （4 ページ）
- SMTP ルート、メール配信、およびメッセージ分裂 （4 ページ）
- SMTP ルートと発信 SMTP 認証 （5 ページ）
- GUI を使用した発信電子メール送信の SMTP ルート管理 （5 ページ）

SMTP ルートの概要

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

この機能を使用すると、ホストを「ひとかたまりにする」ことができます。.example.com などの部分ドメインを指定すると、example.com で終わるすべてのドメインがエントリに一致します。たとえば、fred@foo.example.com と wilma@bar.example.com は、両方ともマッピングに一致します。

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

つまり、再帰的なエントリは続きません。a.domain から b.domain にリダイレクトされるエントリがあり、b.domain から a.domain にリダイレクトされるエントリがその後にある場合、メー

ルのループは作成されません。この場合、a.domain に送信される電子メールは、b.domain で指定された MX ホストに配信されます。反対に、b.domain に送信される電子メールは、a.domain で指定された MX ホストに配信されます。

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

デフォルトの SMTP ルート

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

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

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

SMTP ルートの定義

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

IPv6 アドレスの場合、AsyncOS は次の形式をサポートします。

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

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

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

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

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

SMTP ルートの制限

ルートは、最大 40,000 個定義できます。ALL による最終的なデフォルト ルートは、この制限に含まれます。したがって、39,999 個までのカスタム ルートと、特別なキーワードである ALL を使用する 1 つのルートを定義できます。

SMTP ルートと DNS

特殊なキーワード USEDNS を使用すると、特定ドメインの次のホップを決定する MX ルックアップがアプライアンスで実行されます。これは、サブドメイン宛のメールを特定ホストへルーティングする必要があるときに便利です。たとえば、example.com へのメールが企業の Exchange サーバに送信されるようにする場合、SMTP ルートは次のようになります。

example.com exchange.example.com

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

.example.com USEDNS

SMTP ルートおよびアラート

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

SMTP ルート、メール配信、およびメッセージ分裂

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

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

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

SMTP ルートと発信 SMTP 認証

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

GUI を使用した発信電子メール送信の SMTP ルート管理

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

関連項目

- SMTP ルートの追加 （5 ページ）
- SMTP ルートのエクスポート （6 ページ）
- SMTP ルートのインポート （6 ページ）

SMTP ルートの追加

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

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

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

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

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

ステップ 5 変更を送信し、保存します。

SMTP ルートのエクスポート

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

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

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

SMTP ルートのインポート

ホスト アクセス テーブル（HAT）および受信者アクセス テーブル（RAT）の場合と同様に、ファイルをエクスポートおよびインポートして SMTP ルート マッピングを変更することもできます。SMTP ルートをインポートするには、次の手順に従います。

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

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

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

ステップ 4 [インポート（Import）] をクリックします。

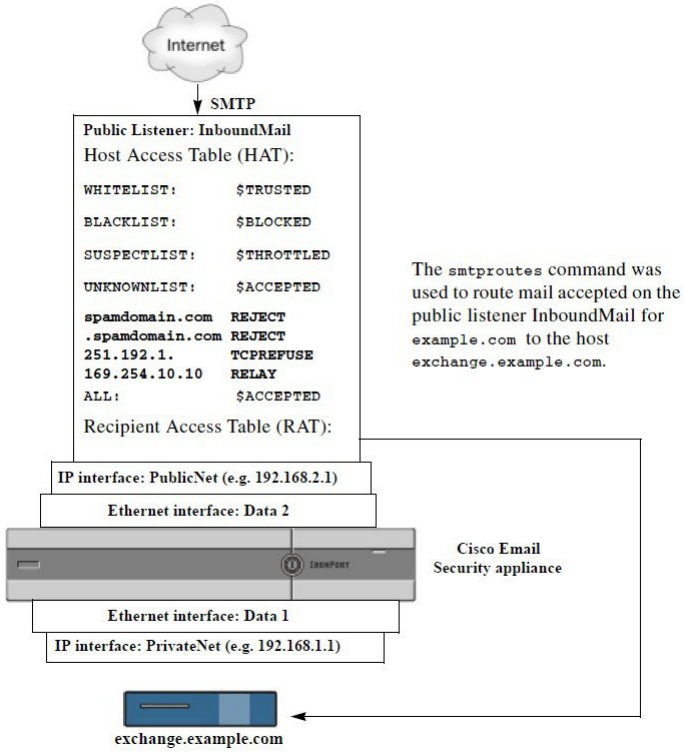
ファイル内に「コメント」を配置できます。文字「#」で始まる行はコメントと見なされ、AsyncOS によって無視されます。次に例を示します。

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

ALL:
```

次のタスク

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 *1*: パブリック リスナー用に定義された *SMTP* ルート



アドレスの書き換え

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

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

表 *1*: アドレスの書き換え方法

元のアドレス	変更後	機能	作業対象
*@anydomain	user@domain	エイリアス テーブル（エイリアス テーブルの作成（8 ページ）を参照）	• エンベロープ受信者のみ • グローバルに適用 • エイリアスを電子メール アドレスまたは他のエイリアスにマッピング

元のアドレス	変更後	機能	作業対象
*@olddomain	*@newdomain	ドメイン マッピング（ドメイン マップ機能 （26 ページ）を参照）	• エンベロープ受信者のみ • リスナーごとに適用
*@olddomain	*@newdomain	マスカレード（マスカレードの構成 （16 ページ）を参照）	• エンベロープ送信者、および To:、From:、または CC: ヘッダー • リスナーごとに適用

エイリアス テーブルの作成

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

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

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

（注） エイリアス テーブル機能により、電子メールのエンベロープ受信者が実際に書き換えられます。これは、電子メールのエンベロープ受信者を書き換えず、電子メールを指定されたドメインに再ルーティングするだけの `smtproutes` コマンド（バウンスした電子メールの処理 （32 ページ）を参照）とは異なります。

関連項目

- コマンド ラインによるエイリアス テーブルの設定 （9 ページ）
- エイリアス テーブルのエクスポートおよびインポート （10 ページ）
- エイリアス テーブルのエントリの削除 （10 ページ）

コマンド ラインによるエイリアス テーブルの設定

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

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

表 *2:* エイリアス テーブルの構文

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

左辺のエイリアスでは、次の形式を使用できます。

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

左辺 1 行あたり複数のエイリアスをカンマで区切って入力できます。

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

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

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

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

関連項目

- エイリアス テーブルの例 （10 ページ）
- aliasconfig コマンドの例 （12 ページ）

エイリアス テーブルのエクスポートおよびインポート

エイリアステーブルをインポートするには、先にFTP、SSH、およびSCPアクセスを確認し、アプライアンスにアクセスできるようにします。

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

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

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

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

エイリアス テーブルのエントリの削除

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

エイリアス テーブルの例

（注） このテーブル例のすべてのエントリは、コメントアウトされています。

```
# sample Alias Table file

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

#

# Incoming Envelope To addresses are evaluated against each

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

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

#

# Separate multiple entries with commas.
```

```
#
# Global aliases should appear before the first domain
# context. For example:
#
# admin@example.com: administrator@example.com
# postmaster@example.net: administrator@example.net
#
# This alias has no implied domain because it appears
# before a domain context:
#
# someaddr@somewhere.dom: specificperson@here.dom
#
# The following aliases apply to recipients @ironport.com and
# any subdomain within .example.com because the domain context
# is specified.
#
# Email to joe@ironport.com or joe@foo.example.com will
# be delivered to joseph@example.com.
#
# Similarly, email to fred@mx.example.com will be
# delivered to joseph@example.com
#
# [ironport.com, .example.com]
#
# joe, fred: joseph@example.com
#
# In this example, email to partygoers will be sent to
# three addresses:
#
# partygoers: wilma@example.com, fred@example.com, barney@example.com
#
# In this example, mail to help@example.com will be delivered to
```

```
# customercare@otherhost.dom. Note that mail to help@ironport.com will
# NOT be processed by the alias table because the domain context
# overrides the previous domain context.
#
# [example.com]
#
# help: customercare@otherhost.dom
#
# In this example, mail to nobody@example.com is dropped.
#
# nobody@example.com: /dev/null
#
# "Chains" may be created, but they must end in an email address.
# For example, email to "all" will be sent to 9 addresses:
#
# [example.com]
#
# all: sales, marketing, engineering
# sales: joe@example.com, fred@example.com, mary@example.com
# marketing:bob@example.com, advertising
# engineering:betty@example.com, miles@example.com, chris@example.com
# advertising:richard@example.com, karen@advertising.com
```

aliasconfig コマンドの例

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

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

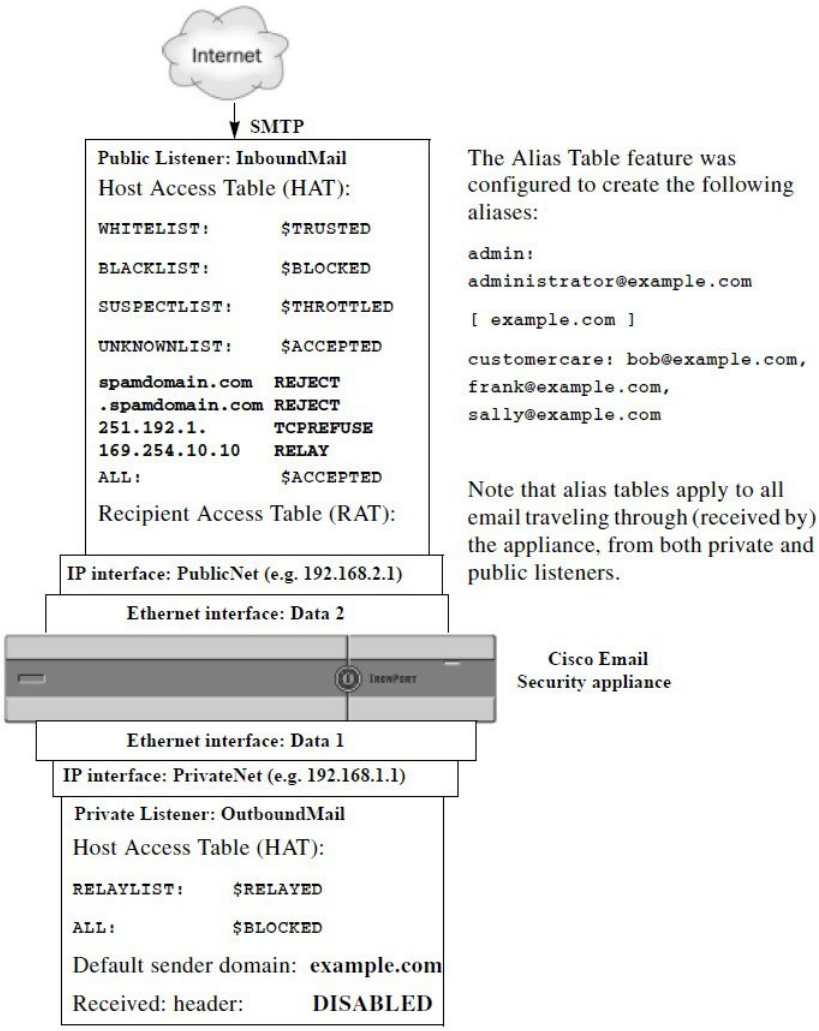
```
mail3.example.com> aliasconfig

No aliases in table.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import aliases from a file.

[]> new


How do you want your aliases to apply?

1. Globally

2. Add a new domain context


[1]> 2

Enter new domain context.

Separate multiple domains with commas.

Partial domains such as .example.com are allowed.

[]> example.com


Enter the alias(es) to match on.

Separate multiple aliases with commas.

Allowed aliases:

- "user" - This user in this domain context.

- "user@domain" - This email address.

[]> customercare


Enter address(es) for "customercare".

Separate multiple addresses with commas.

[]> bob@example.com, frank@example.com, sally@example.com


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

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

There are currently 1 mappings defined.

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.
```

```
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> new
How do you want your aliases to apply?
1. Globally
2. Add a new domain context
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n

There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
```

```
- CLEAR - Clear the table.

[]> print

admin: administrator@example.com

[ example.com ]

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

There are currently 2 mappings defined.

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display the table.

- IMPORT - Import aliases from a file.

- EXPORT - Export table to a file.

- CLEAR - Clear the table.

[]>
```

この時点で、電子メール ゲートウェイの設定は次のようになります。

図 *2:* アプライアンスに定義されたエイリアス テーブル



マスカレードの構成

マスカレードは、作成したテーブルに従って、エンベロープ送信者（送信者またはMAIL FROMとも呼ばれます）、およびリスナーで処理される電子メールの To:、From:、CC: ヘッダーを書き換える機能です。この機能の一般的な実装例の1つが「仮想ドメイン」であり、これによって複数のドメインを1つのサイトからホスティングできるようになります。他の一般的な実装としては、ネットワーク インフラストラクチャを「隠す」ために、電子メール ヘッダーの文字列からサブドメインを取り除く（「ストリッピング」）というものがあります。マスカレード機能は、プライベート リスナーとパブリック リスナーの両方で利用できます。

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

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

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

- 作成したマッピングのスタティック テーブルを使用
- LDAP クエリを使用。

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

関連項目

- マスカレードと altsrchost （17 ページ）

マスカレードと altsrchost

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

詳細については、Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ （60 ページ）および確認：電子メール パイプライン （73 ページ）を参照してください。

関連項目

- スタティック マスカレード テーブルの構成 （17 ページ）
- プライベート リスナー用マスカレード テーブルの例 （19 ページ）
- マスカレード テーブルのインポート （19 ページ）
- マスカレードの例 （19 ページ）

スタティック マスカレード テーブルの構成

マッピングのスタティック マスカレード テーブルを設定するには、listenerconfig コマンドの edit -> masquerade サブコマンドを使用します。また、マッピングが含まれるファイルをインポートできます。マスカレード テーブルのインポート （19 ページ）を参照してください。こ

のサブコマンドにより、入力アドレス、ユーザ名、およびドメインを新しいアドレスおよびドメインにマッピングするテーブルを作成および維持します。LDAPマスカレードクエリの詳細については、LDAP クエリを参照してください。

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

ドメインのマスカレード テーブルは、次のように構成されます。

表 *3:* マスカレード テーブルの構文

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

次の表に、マスカレード テーブルで有効なエントリを示します。

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

- ルールは、マスカレード テーブルでの出現順序に従って一致します。

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

プライベート リスナー用マスカレード テーブルの例

```
# sample Masquerading file

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

sales sales_team@success.com

@techsupport tech_support@biggie.com

user@localdomain user@company.com

ALL @bigsender.com
```

マスカレード テーブルのインポート

従来の sendmail の /etc/mail/genericstable ファイルをインポートできます。genericstable ファイルをインポートするには、先にFTP、SSH、およびSCP アクセスを確認し、アプライアンスにアクセスできるようにします。

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

```
listenerconfig -> edit -> listener_number -> masquerade -> import
```

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

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

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

マスカレードの例

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

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

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

```
mail3.example.com> listenerconfig

Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

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

[]> 2

Name: OutboundMail

Type: Private

Interface: PrivateNet (192.168.1.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.
```

```
- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

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

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

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

- LDAPROUTING - Configure an LDAP query to reroute messages.

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

recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.

[]> masquerade

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

Domain Masquerading Table

There are currently 0 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> new


Enter the source address or domain to masquerade.

Usernames like "joe" are allowed.

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

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

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

```
Hosts like @training and @.sales are allowed.
[]> @.example.com
Enter the masqueraded address or domain.
Domains like @example.com are allowed.
Full addresses such as user@example.com are allowed.
[]> @example.com
Entry mapping @.example.com to @example.com created.
Domain Masquerading Table
There are currently 1 entries.
Masqueraded headers: To, From, Cc
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]> new

Enter the source address or domain to masquerade.
Usernames like "joe" are allowed.
Full addresses like "user@example.com" are allowed.
Full addresses with subdomain wildcards such as "username@.company.com" are allowed.
Domains like @example.com and @.example.com are allowed.
Hosts like @training and @.sales are allowed.
[]> joe
Enter the masqueraded address.
Only full addresses such as user@example.com are allowed.
[]> joe@example.com
Entry mapping joe to joe@example.com created.
Domain Masquerading Table
```

```
There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> print

@.example.com @example.com


joe joe@example.com

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

- IMPORT - Import all entries from a file.

- EXPORT - Export all entries to a file.

- CONFIG - Configure masqueraded headers.

- CLEAR - Remove all entries.

[]> export

Enter a name for the exported file:

[]> masquerade.txt

Export completed.

Domain Masquerading Table

There are currently 2 entries.

Masqueraded headers: To, From, Cc

Choose the operation you want to perform:
```

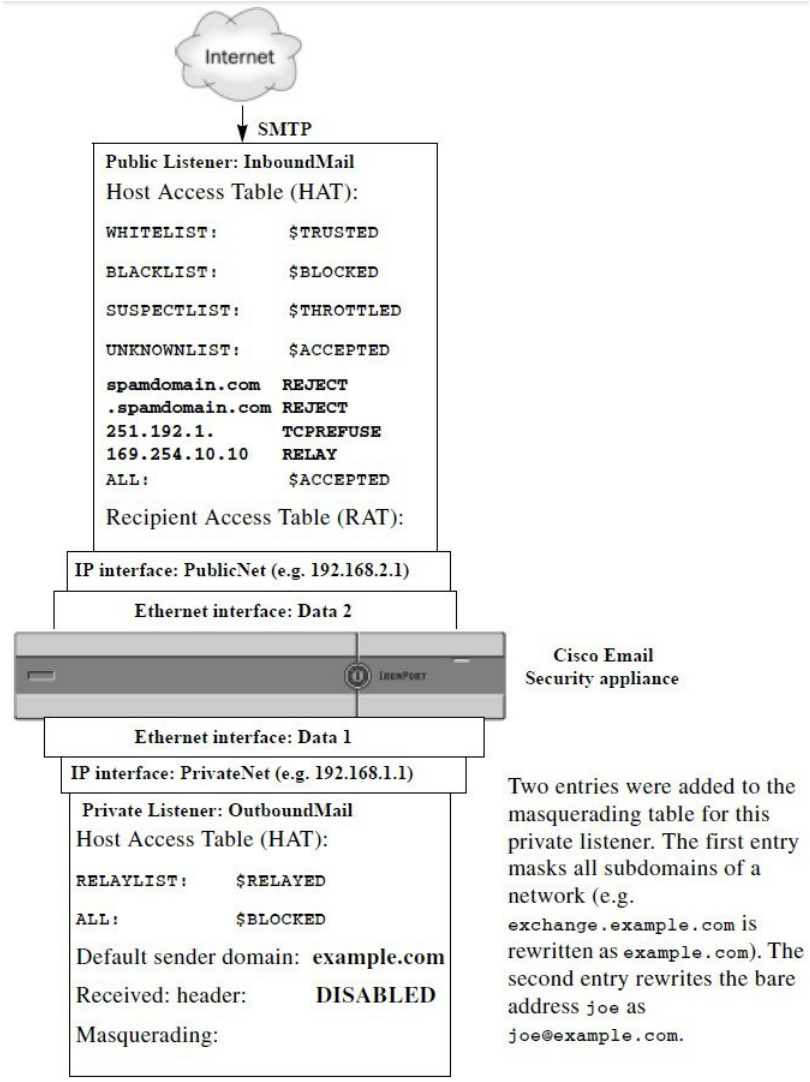
```
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.

[]> config
Do you wish to masquerade Envelope Sender?
[N]> y
Do you wish to masquerade From headers?
[Y]> y
Do you wish to masquerade To headers?
[Y]> y
Do you wish to masquerade CC headers?
[Y]> n
Do you wish to masquerade Reply-To headers?
[Y]> n
Domain Masquerading Table
There are currently 2 entries.
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import all entries from a file.
- EXPORT - Export all entries to a file.
- CONFIG - Configure masqueraded headers.
- CLEAR - Remove all entries.
[]>
Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
```

```
Protocol: SMTP

Default Domain:

Max Concurrency: 600 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

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

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

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

- LDAPROUTING - Configure an LDAP query to reroute messages.

- LDAPGROUP - Configure an LDAP query to determine whether a sender or
recipient is in a specified group.

- SMTPAUTH - Configure an SMTP authentication.


[]>

Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.
```

```
- SETUP - Change global settings.

[]>
```

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 *3:* プライベート リスナー用に定義されたマスカレード



ドメイン マップ機能

リスナー用に「ドメイン マップ」を設定できます。設定するリスナーごとにドメイン マップ テーブルを作成できます。ドメイン マップ テーブルに含まれているドメインと一致するメッセージでは、各受信者のエンベロープ受信者が書き換えられます。この機能は、sendmail の

「ドメイン テーブル」機能または Postfix の「仮想テーブル」機能に似ています。この機能では、エンベロープ受信者のみが影響を受け、「To:」ヘッダーは書き換えられません。

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

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

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

表 *4:* ドメイン マップ テーブルの構文の例

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

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

```
mail3.example.com> listenerconfig
```

```
Currently configured listeners:

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

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

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit

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

[]> 1

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Disabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

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

```
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> domainmap
Domain Map Table
There are currently 0 Domain Mappings.
Domain Mapping is: disabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import domain mappings from a file.
[]> new

Enter the original domain for this entry.
Domains such as "@example.com" are allowed.
Partial hostnames such as "@.example.com" are allowed.
Email addresses such as "test@example.com" and "test@.example.com"
are also allowed.
[]> @.oldcompanyname.com
Enter the new domain for this entry.
The new domain may be a fully qualified
such as "@example.domain.com" or a complete
email address such as "test@example.com"
[]> @example.com
Domain Map Table
There are currently 1 Domain Mappings.
Domain Mapping is: enabled
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display all domain mappings.
- IMPORT - Import domain mappings from a file.
- EXPORT - Export domain mappings to a file.
```

```
- CLEAR - Clear all domain mappings.

[]> print

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

Domain Map Table

There are currently 1 Domain Mappings.

Domain Mapping is: enabled

Choose the operation you want to perform:

- NEW - Create a new entry.

- EDIT - Modify an entry.

- DELETE - Remove an entry.

- PRINT - Display all domain mappings.

- IMPORT - Import domain mappings from a file.

- EXPORT - Export domain mappings to a file.

- CLEAR - Clear all domain mappings.

[]>

Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain Map: Enabled

TLS: No

SMTP Authentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.
```

```
- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

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

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[]>
```

関連項目

- ドメイン マップ テーブルのインポートおよびエクスポート （31 ページ）

ドメイン マップ テーブルのインポートおよびエクスポート

ドメインマップテーブルをインポートまたはエクスポートするには、先にFTP、SSH、およびSCP アクセスを確認し、アプライアンスにアクセスできるようにします。

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

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

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

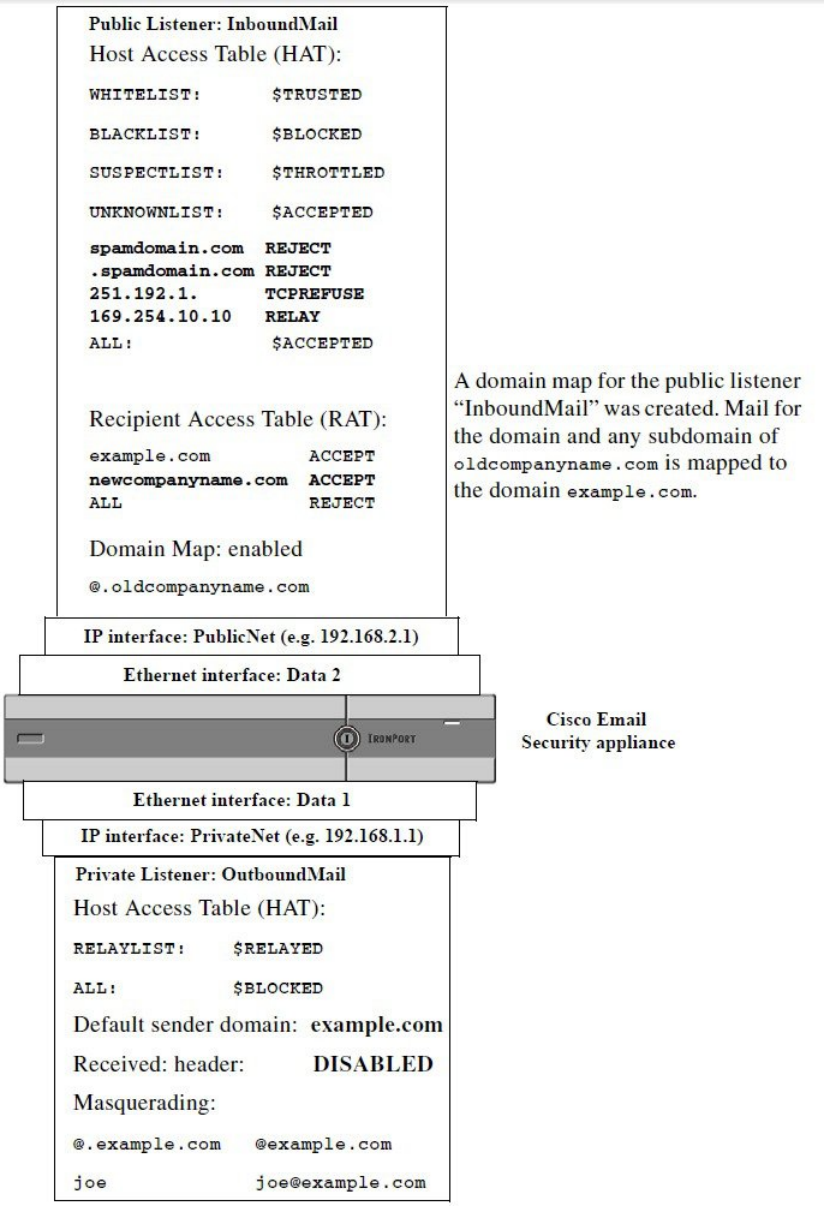
または、`export` サブコマンドを使用して既存のコンフィギュレーションをダウンロードできます。ファイル（ファイル名は自分で指定）は、configuration ディレクトリに書き込まれます。このファイルを CLI の外部で変更し、インポートし直すことができます。

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

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

これでエンタープライズ ゲートウェイの設定は次のようになります。

図 *4:* パブリック リスナー用に定義されたドメイン マップ



バウンスした電子メールの処理

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

この項では、アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御について説明していることに注意してください。アプライアンスが発信メールに基づいて着信バウ

ンスを制御する方法について管理するには、バウンス検証を使用します（バウンス検証 （43 ページ）を参照）。

関連項目

- 配信不可能な電子メールの処理 （33 ページ）
- 新しいバウンス プロファイルの作成 （41 ページ）
- リスナーへのバウンス プロファイルの適用 （41 ページ）

配信不可能な電子メールの処理

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

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

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

関連項目

- ソフト バウンスおよびハード バウンスに関する注意 （34 ページ）
- バウンス プロファイルのパラメータ （34 ページ）
- ハード バウンスと status コマンド （38 ページ）
- カンバセーション バウンスおよび SMTP ルートのメッセージ フィルタ アクション （39 ページ）
- バウンス プロファイルの例 （39 ページ）
- 配信ステータス通知形式 （40 ページ）
- 遅延警告メッセージ （40 ページ）
- 遅延警告メッセージとハード バウンス （41 ページ）

ソフト バウンスおよびハード バウンスに関する注意

- カンバセーション ソフト バウンスの場合、ソフト バウンス イベントは、受信者への配信が一時的に失敗するたびに定義されます。単一の受信者が複数のソフト バウンス イベントを繰り返し発生させることがあります。[バウンスプロファイル（Bounce Profiles）]ページまたは bounceconfig コマンドを使用して、各ソフト バウンス イベントのパラメータを設定します。（バウンス プロファイルのパラメータ （34 ページ） を参照）。
- デフォルトでは、ハード バウンスした受信者ごとにバウンス メッセージが生成され、元の送信者に送信されます。（メッセージは、メッセージエンベロープのエンベロープ送信者アドレスで定義されたアドレスに送信されます。Envelope From も通常エンベロープ送信者を意味します）。この機能をディセーブルにし、代わりにハードバウンスに関する情報をログ ファイルに頼ることもできます。（「ロギング」の章を参照。）
- キュー内での最大時間または再試行の最大回数のどちらかに達すると、ソフトバウンスはハード バウンスになります。

バウンス プロファイルのパラメータ

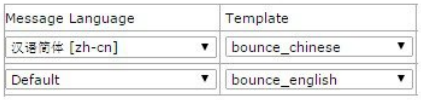
バウンスプロファイルを設定するときは、次のパラメータを使用して、メッセージごとにカンバセーション バウンスを処理する方法を制御します。

表 *5:* バウンス プロファイルのパラメータ

最大再試行回数（Maximum number of retries）	ソフトバウンスしたメッセージを配信し直すために、ハードバウンス メッセージとして扱われるようになる前に、受信者のホストに再接続が試みられる回数。デフォルトの再試行回数は 100 です。
キューの最大時間（秒）（Maximum number of seconds in queue）	ソフト バウンスしたメッセージを配信し直すために、ハード バウンスしたメッセージとして扱われるようになる前に、受信者のホストに再接続が試みられるのに費やされる時間。デフォルトは 259,200 秒（72 時間）です。

メッセージを再試行するまでの初回待機時間（秒）（Initial number of seconds to wait before retrying a message）	ソフト バウンスしたメッセージを最初に配信し直すまでの待機時間。デフォルトは 60 秒です。初回再試行時間を大きい値に設定すると、ソフト バウンスの試行頻度が低下します。逆に頻度を上げるには、小さい値にします。
メッセージを再試行するまでの最大待機時間（秒）（Maximum number of seconds to wait before retrying a message）	ソフトバウンスしたメッセージを配信し直すまでに待機する最大時間。デフォルトは 3,600 秒（1 時間）です。これは、次の試行までの間隔ではなく、再試行回数を制御するために使用できるもう 1 つのパラメータです。初回再試行間隔の上限は、最大再試行間隔に制限されます。計算された再試行間隔が最大再試行間隔を超える場合は、最大再試行間隔が使用されます。

ハード バウンス メッセージの送信（Send Hard Bounce Messages）	ハード バウンスに対してバウンス メッセージを送信するかどうかを指定します。このオプションが有効な場合は、バウンス メッセージの形式を選択できます。デフォルトでは、バウンス メッセージで DSN 形式（RFC 1894）が使用されます。 元のメッセージ（件名と本文）の言語に基づいてカスタマイズされたバウンス メッセージを送信することもできます。たとえば、中国語のメッセージには中国語でバウンス メッセージを送信し、他の言語のすべてのメッセージには英語のバウンス メッセージを送信することができます。 [通知テンプレート（Notification Template）] の下で [行の追加（Add Row）] をクリックして、メッセージの言語と使用するテンプレートを選択します。 （注） デフォルトのエントリが削除されていないことを確認します（[メッセージの言語（Message Language）] を [デフォルト（Default）] に設定）。デフォルト エントリのバウンス通知テンプレートは変更できます。 メッセージの言語は、次のシナリオではデフォルトと見なされます。 • メッセージの言語が、他の通知テンプレート エントリで選択した言語と異なる場合。 • メッセージの言語が、Cisco E メール セキュリティ アプライアンスでサポートされていない場合。 • アプライアンスがメッセージの言語を検出できない場合。 • メッセージの内容（件名と本文）が 50 バイト未満である場合。 前述の例（中国語のメッセージには中国語のバウンス メッセージを送信し、他の言語のすべてのメッセージには英語のバウンス メッセージを送信する）を設定する場合、通知テンプレートのテーブルは次のようになります。 バウンス応答から DSN の status フィールドを解析するかどうかを選択することもできます。「はい」の場合、アプライアンスは DSN ステータス コード（RFC 3436）を検索し、そのコードを配信ステータス通知の Status フィールドで使用します。

遅延警告メッセージの送信（Send Delay Warning Messages）	配信遅延に対して警告メッセージを送信するかどうかを指定します。このオプションが有効な場合は、元のメッセージ（件名と本文）の言語に基づいてカスタムの遅延警告メッセージを構成できます。たとえば、中国語のメッセージには中国語で遅延警告メッセージを送信し、他の言語のすべてのメッセージには英語の遅延警告メッセージを送信することができます。 [通知テンプレート（Notification Template）] の下で [行の追加（Add Row）] をクリックして、メッセージの言語と使用するテンプレートを選択します。 （注） デフォルトのエントリが削除されていないことを確認します（[メッセージの言語（Message Language）] を [デフォルト（Default）] に設定）。デフォルトエントリのバウンス通知テンプレートは変更できます。 メッセージの言語は、次のシナリオではデフォルトと見なされます。 • メッセージの言語が、他の通知テンプレートエントリで選択した言語と異なる場合。 • メッセージの言語が、Cisco E メール セキュリティ アプライアンスでサポートされていない場合。 • アプライアンスがメッセージの言語を検出できない場合。 • メッセージの内容（件名と本文）が 50 バイト未満である場合。 前述の例（中国語のメッセージには中国語の遅延警告メッセージを送信し、他の言語のすべてのメッセージには英語の遅延警告メッセージを送信する）を設定する場合、通知テンプレートのテーブルは次のようになります。  メッセージ間の最小間隔、および送信する最大再試行回数を指定することもできます。
バウンス先の受信者の指定（Specify Recipient for Bounces）	メッセージのバウンス先としてデフォルトのエンベロープ送信者アドレスではなく、別のアドレスにすることができます。

バウンスおよび遅延メッセージへの DomainKeys 署名の使用（Use DomainKeys signing for bounce and delay messages）	バウンス メッセージおよび遅延メッセージの署名に使用する DomainKeys プロファイルを選択できます。DomainKeys の詳細については、DomainKeys と DKIM 認証を参照してください。
グローバル設定（Global Settings）	
これらの設定を行うには、[バウンスプロファイル（Bounce Profiles）] ページの [グローバル設定を編集（Edit Global Settings）] リンクを使用するか、または CLI で `bounceconfig` コマンドを使用してデフォルトのバウンス プロファイルを編集します。	
到達不能ホストをリトライするまでの最初の待機時間（秒）（Initial number of seconds to wait before retrying an unreachable host）	システムが到達不可能なホストへの再試行を待機する時間。 ★セグメント分割★ デフォルトは 60 秒です。
到達不能ホストの最大許容再試行間隔（Max interval allowed between retries to an unreachable host）	システムが到達不可能なホストへの再試行を待機する最大時間。デフォルトは 3,600 秒（1 時間）です。ホストがダウンしているために配信が最初に失敗すると、再試行値の最小秒数で開始し、ダウンしたホストに対するその後の再試行では、間隔を徐々に延ばしていきます。最大で、この最大秒数になります。

ハード バウンスと status コマンド

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

Counters:	Reset	Uptime	Lifetime
Receiving			
Messages Received	0	0	0

Recipients Received	0	0	0
Gen. Bounce Recipients	0	0	0

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

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

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

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

バウンス プロファイルの例

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

表 *6*：例 *1*：バウンス プロファイル パラメータ

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

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

表 *1: 例 2*：バウンス プロファイル パラメータ

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

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

配信ステータス通知形式

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

遅延警告メッセージ

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

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

遅延警告メッセージとハード バウンス

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

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

新しいバウンス プロファイルの作成

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

関連項目

- デフォルトのバウンス プロファイルの編集 （41 ページ）
- minimalist バウンス プロファイルの例 （41 ページ）

デフォルトのバウンス プロファイルの編集

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

minimalist バウンス プロファイルの例

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

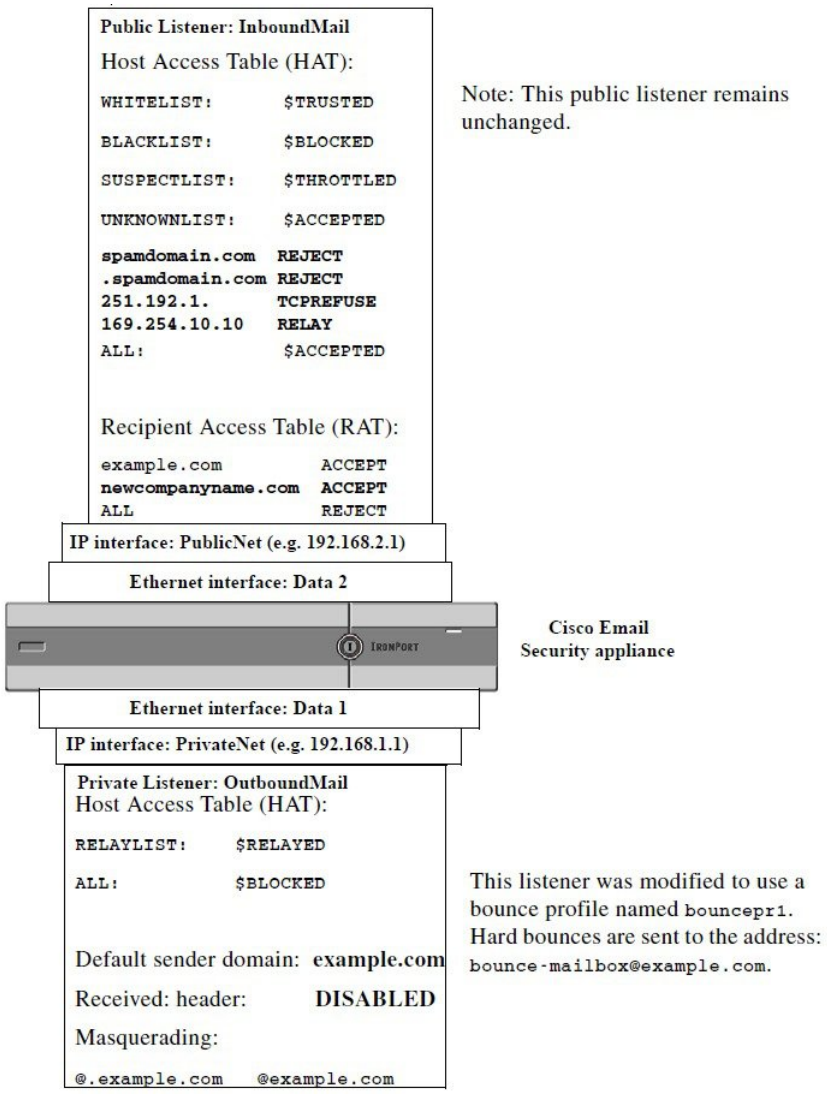
リスナーへのバウンス プロファイルの適用

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

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

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:* プライベート リスナーへのバウンス プロファイルの適用



宛先制御による電子メール配信の管理

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

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

- レート制限 （43 ページ）
- TLS （43 ページ）

- バウンス検証 （43 ページ）
- バウンス プロファイル（Bounce Profile） （43 ページ）

レート制限

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

TLS

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

バウンス検証

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

バウンス プロファイル（Bounce Profile）

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

未指定のドメインに対するデフォルト設定を制御することもできます。

関連項目

- メール配信に使用するインターフェイスの決定 （44 ページ）
- デフォルトの配信制限 （44 ページ）
- [送信先コントロール（Destination Controls）] の使用 （44 ページ）

メール配信に使用するインターフェイスの決定

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

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

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

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

デフォルトの配信制限

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

[送信先コントロール（Destination Controls）] の使用

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

関連項目

- IP アドレス バージョンの管理 （45 ページ）
- ドメインに対する接続、メッセージ、受信者の数の管理 （45 ページ）
- TLS の管理 （47 ページ）
- バウンス検証タギングの管理 （47 ページ）
- バウンスの管理 （48 ページ）

• 新しい送信先コントロール エントリの追加 （48 ページ）
• 宛先制御設定のインポートおよびエクスポート （48 ページ）
• 宛先制御と CLI （52 ページ）

IP アドレス バージョンの管理

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

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

ドメインに対する接続、メッセージ、受信者の数の管理

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

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

```
domain.com
```

または

```
.domain.com
```

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

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

また、定義した制限がドメイン全体に適用されるかどうかを設定します。

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

これらの値については、次の表で説明します。

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

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

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

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

TLS の管理

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

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

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

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

アラートの詳細については、「システム管理」の章を参照してください。

バウンス検証タギングの管理

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

バウンスの管理

リモートホストに配信する接続や受信者の数を制御できるだけでなく、そのドメインで使用されるバウンス プロファイルを指定することもできます。指定すると、バウンス プロファイルは destconfig コマンドの 5 番めのカラムに表示されます。バウンス プロファイルを指定しない場合は、デフォルトのバウンスプロファイルが使用されます。詳細については、新しいバウンス プロファイルの作成 （41 ページ）を参照してください。

新しい送信先コントロール エントリの追加

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

ステップ 2 エントリを設定します。

ステップ 3 変更を送信し、保存します。

宛先制御設定のインポートおよびエクスポート

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

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

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

表 *9*: 送信先コントロール設定ファイルのパラメータ

パラメータ名	説明
`ip_sort_pref`	ドメインに対してインターネットプロトコルバージョンを指定します。 次のいずれかの値を入力します。 • IPv6「Preferred」の場合の `PREFER_V6` • IPv6「Required」の場合の `REQUIRE_v6` • IPv4「Preferred」の場合の `PREFER_V4` • IPv4「Required」の場合の `REQUIRE_v4`

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

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

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

```
[DEFAULT]

ip_sort_pref = PREFER_V6

max_host_concurrency = 500

max_messages_per_connection = 50

recipient_minutes = 60

recipient_limit = 300

limit_type = host

limit_apply = VG
```

```
table_tls = off
bounce_validation = 0
send_tls_req_alert = 0
certificate = example.com
[example1.com]
ip_sort_pref = PREFER_V6
recipient_minutes = 60
recipient_limit = 100
table_tls = require_verify
limit_apply = VG
bounce_profile = tls_failed
limit_type = host
[example2.com]
table_tls = on
bounce_profile = tls_failed
```

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

```
example1.com

IP Address Preference: IPv6 Preferred
Maximum messages per connection: 50
Rate Limiting:
500 concurrent connections
100 recipients per 60 minutes
Limits applied to entire domain, across all virtual gateways
TLS: Required (Verify)

Bounce Profile: tls_failed

example2.com

IP Address Preference: IPv6 Preferred
Maximum messages per connection: Default
Rate Limiting: Default
```

```
TLS: Preferred

Bounce Profile: tls_failed
```

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

宛先制御と CLI

CLI で destconfig コマンドを使用して、送信先コントロール エントリを設定できます。このコマンドについては、『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。

バウンス検証

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

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

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

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

タグが外されて配信されます。タグが付いていないバウンス メッセージは、別の処理を行えます。

バウンス検証を使用して、発信メールに基づいて着信バウンス メッセージを管理できます。アプライアンスで着信メールに基づいて発信バウンスを生成する方法の制御については、バウンスした電子メールの処理 （32 ページ）を参照してください。

関連項目

- 概要：タギングとバウンス検証 （53 ページ）
- バウンス検証を使用してバウンス メッセージ ストームを防止 （55 ページ）
- タグなしのバウンスされたメッセージの合法的受け入れ （54 ページ）

概要：タギングとバウンス検証

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

デフォルトではシステム全体でバウンス検証タギングをイネーブルまたはディセーブルにできます。特定のドメインに対してバウンス検証タギングをイネーブルまたはディセーブルにすることもできます。ほとんどの場合、デフォルトでイネーブルにしておき、除外する具体的なドメインを [送信先コントロール（Destination Controls）] テーブルに列挙します（[送信先コントロール（Destination Controls）] の使用 （44 ページ）を参照）。

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

関連項目

- 着信バウンス メッセージの処理 （53 ページ）
- バウンス検証アドレスのタギング キー （54 ページ）

着信バウンス メッセージの処理

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

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

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

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

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

Fri Jul 21 16:02:40 2006 Info: MID 26603 ICID 125192 invalid bounce, rcpt address
<bob@example.com> rejected by bounce verification.
Fri Jul 21 16:03:51 2006 Info: Message aborted MID 26603 Receiving aborted by sender

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

（注） 非バウンス メールを独自の社内メール サーバ（Exchange など）に配信する場合は、その社内ドメインに対してバウンス検証タギングを無効にしてください。

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

バウンス検証アドレスのタギング キー

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

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

タグなしのバウンスされたメッセージの合法的受け入れ

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

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

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

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

バウンス検証を使用してバウンス メッセージ ストームを防止

ステップ 1 タギング キーを入力します。詳細については、[バウンス検証アドレスのタグ付けキー（Bounce Verification Address Tagging Keys）] の設定 （55 ページ）を参照してください。

ステップ 2 バウンス検証設定を編集します。詳細については、バウンス検証設定値の設定 （56 ページ）を参照してください。

ステップ 3 [送信先コントロール（Destination Controls）] を使用したバウンス検証をイネーブルにします。詳細については、[送信先コントロール（Destination Controls）] の使用 （44 ページ）を参照してください。

次のタスク

関連項目

- [バウンス検証アドレスのタグ付けキー（Bounce Verification Address Tagging Keys）] の設定 （55 ページ）
- バウンス検証設定値の設定 （56 ページ）
- CLI を使用したバウンス検証の構成 （56 ページ）
- バウンス検証とクラスタ設定 （56 ページ）

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

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

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

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

ステップ 3 変更を保存します。

次のタスク

関連項目

- キーの削除 （56 ページ）

キーの削除

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

バウンス検証設定値の設定

バウンス検証設定では、無効なバウンスを受信したときに実行するアクションを指定します。

ステップ 1 [メールポリシー（Mail Policies）] > [バウンス検証（Bounce Verification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 無効なバウンスを拒否するのか、カスタム ヘッダーをメッセージに追加するのかを選択します。ヘッダーを追加する場合は、ヘッダーの名前と値を入力します。

ステップ 4 必要に応じて、スマート例外機能をイネーブルにします。この設定を使用すると、（着信メールと発信メールの両方で 1 つのリスナーを使用している場合であっても）着信メール メッセージ、および社内メール サーバで生成されるバウンス メッセージをバウンス検証処理から自動的に除外できるようにします。

ステップ 5 変更を送信し、保存します。

CLI を使用したバウンス検証の構成

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

バウンス検証とクラスタ設定

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

電子メール配信パラメータの設定

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

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

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

関連項目

- デフォルトの配信 IP インターフェイス （57 ページ）
- [配信可能性あり（Possible Delivery）] 機能 （58 ページ）
- デフォルトの最大同時接続数 （58 ページ）
- deliveryconfig の例 （58 ページ）

デフォルトの配信 IP インターフェイス

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

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

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

[配信可能性あり（Possible Delivery）] 機能

⚠

注意 この機能を有効にすると、メッセージ配信が信頼できなくなり、メッセージの損失につながることがあります。また、アプライアンスは RFC 5321 に準拠しない状態になります。詳細については、http://tools.ietf.org/html/rfc5321#section-6.1.を参照してください。

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

デフォルトの最大同時接続数

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

deliveryconfig の例

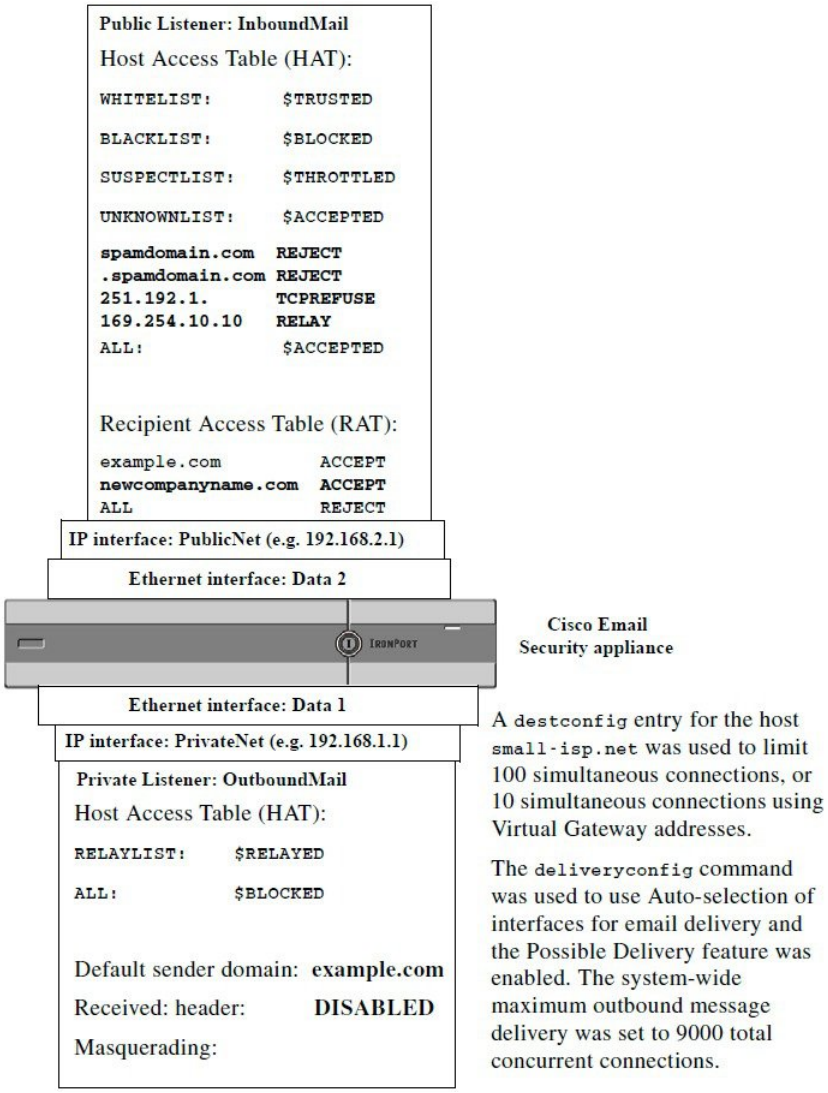
次の例では、`deliveryconfig` コマンドを使用し、[配信可能性あり（Possible Delivery）] をイネーブルにして、デフォルトのインターフェイスを [自動（Auto）] に設定します。システム全体の最大発信メッセージ配信は、9000 接続です。

```
mail3.example.com> deliveryconfig

Choose the operation you want to perform:

- SETUP - Configure mail delivery.

[]> setup

Choose the default interface to deliver mail.

1. Auto

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

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

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

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

```
[1]> 1

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

Please enter the default system wide maximum outbound message delivery

concurrency

[10000]> 9000

mail3.example.com>
```

これで電子メール ゲートウェイの設定は次のようになります。

図 *6* : 宛先および配信パラメータの設定



Virtual Gateway™ テクノロジーを使用してすべてのホストされたドメインでの構成のメール ゲートウェイ

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

Cisco Virtual Gateway テクノロジーでは、ホストするすべてのドメインに対して異なる IP アドレス、ホスト名、およびドメインを使用してエンタープライズ メール ゲートウェイを設定し、同じ物理アプライアンス内にホストしている場合でも、それらのドメインに対して別々に企業の電子メール ポリシー強制およびスパム対策方針を作成できます。すべての E メール セキュリティ アプライアンス モデルで使用可能な仮想ゲートウェイ アドレスの数値は 255 です。

関連項目

- 概要 （60 ページ）
- Virtual Gateway アドレスの設定 （61 ページ）
- Virtual Gateway アドレスのモニタ （69 ページ）
- Virtual Gateway アドレスごとの配信接続の管理 （69 ページ）

概要

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

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

各 Virtual Gateway アドレスでのメッセージも、別々のメッセージ キューに割り当てられます。受信者ホストで特定の Virtual Gateway アドレスからの電子メールをブロックしている場合、そのホスト宛のメッセージはキューに残され、最終的にはタイムアウトします。しかしブロックされていない別の Virtual Gateway キュー内にある同じドメイン宛のメッセージは、正常に配信

されます。これらのキューは、配信では別のものとして扱われますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべての Virtual Gateway キューが一体のものとして扱われます。

Virtual Gateway アドレスの設定

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

関連項目

- 仮想ゲートウェイで使用する新しい IP インターフェイスの作成 （61 ページ）
- メッセージから配信用 IP インターフェイスへのマッピング （64 ページ）
- altsrchost ファイルのインポート （65 ページ）
- altsrchost の制限 （66 ページ）
- altsrchost コマンド用に有効なマッピングが記載されたテキスト ファイルの例 （66 ページ）
- CLI を使用した altsrchost マッピングの追加 （66 ページ）

仮想ゲートウェイで使用する新しい IP インターフェイスの作成

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

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

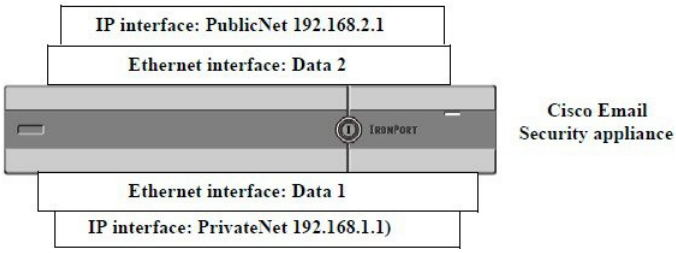
必要な IP インターフェイスを作成したら、2 つの方法で Virtual Gateway アドレスを設定し、各 IP インターフェイスまたはインターフェイス グループから送信される電子メール キャンペーンを定義します。

- altsrchost コマンドを使用すると、特定の送信者 IP アドレスまたはエンベロープ送信者アドレスの情報からホストの IP インターフェイス（Virtual Gateway アドレス）またはインターフェイス グループに電子メールをマッピングして配信できます。
- メッセージ フィルタを使用して、特定ホストの IP インターフェイス（Virtual Gateway アドレス）またはインターフェイス グループを使用してフラグ付きのメッセージを配信するためのフィルタを設定できます。送信元ホスト（Virtual Gateway アドレス）変更アクションを参照してください。（この方法は前述の方法よりも柔軟性があり、強力です）。

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

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

図 *7:* パブリック インターフェイスとプライベート インターフェイスの例



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

図 *8:* [IPインターフェイスを編集（*IP Interface*）] ページ

IP Interfaces

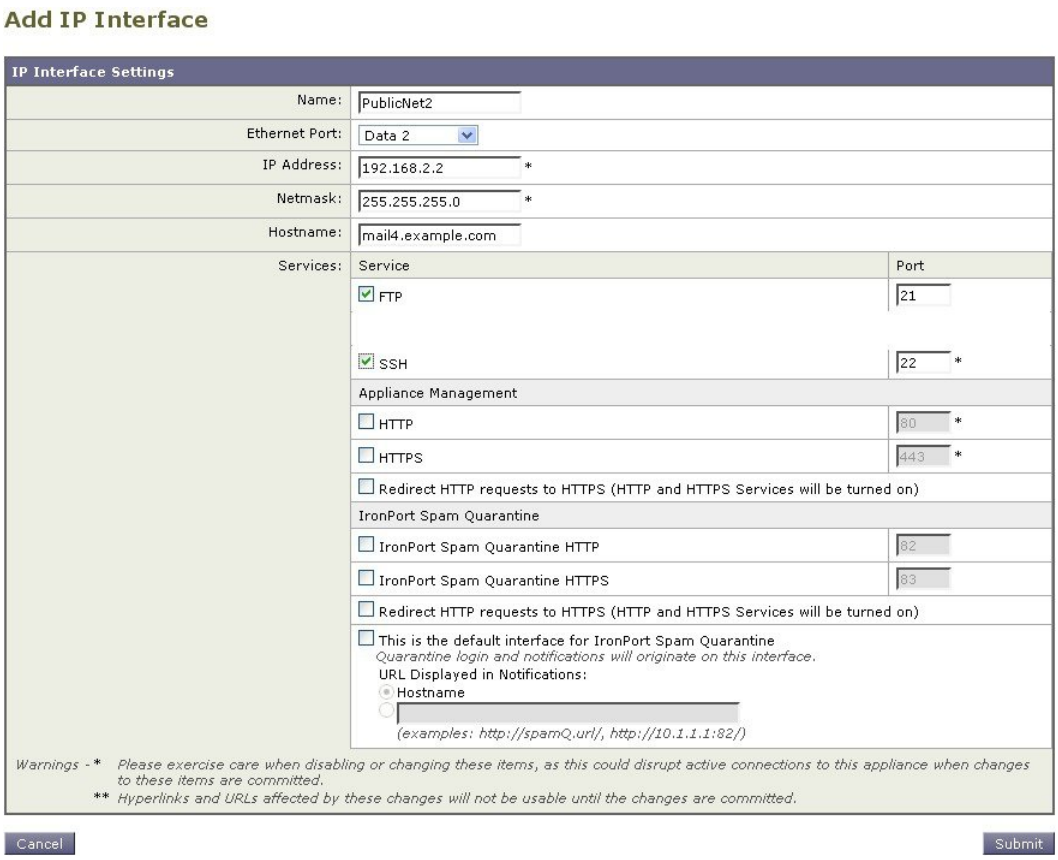
Network Interfaces and IP Addresses

Add IP Interface...

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

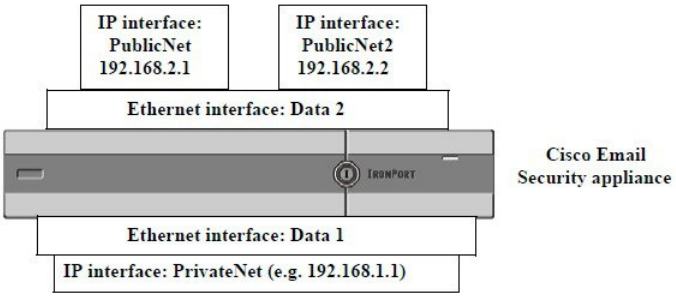
次に、[IPインターフェイスの追加（Add IP Interface）] ページを使用して、Data2 イーサネットインターフェイス上に PublicNet2 という名前の新しいインターフェイスを作成します。IP アドレス 192.168.2.2 が使用され、ホスト名 mail4.example.com が指定されています。さらに、FTP（ポート 21）および SSH（ポート 22）がイネーブルになります。

図 *9 : [IP*インターフェイスの追加（***Add IP Interface***）*]* ページ



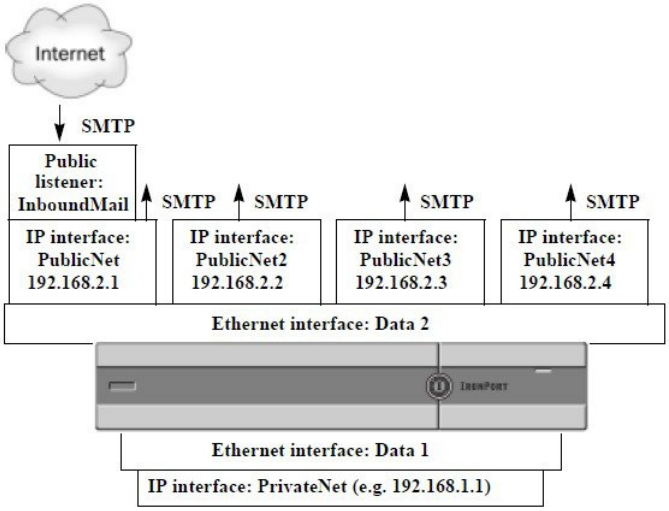
これで電子メール ゲートウェイのコンフィギュレーションは次のようになります。

図 *10 :* 別のパブリック インターフェイスの追加



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

図 *11 : 1* つのイーサネット インターフェイス上にある *4* つの *Virtual Gateway* アドレス



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

メッセージから配信用 IP インターフェイスへのマッピング

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

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

- 送信者の IP アドレス
- エンベロープ送信者アドレス

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

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

一致する可能性のあるキーを優先順に示します。

送信者の IP アドレス	送信者の IP アドレスは完全一致する必要があります。 例：`192.168.1.5`

完全形式のエンベロープ送信者	エンベロープ送信者は、アドレス全体が完全一致する必要があります。 例：`username@example.com`
[ユーザ名（Username）]	エンベロープ送信者アドレスの `@` 記号までの部分に対してユーザ名構文と一致させます。`@` 記号を含める必要があります。例：`username@`
[ドメイン（Domain）]	エンベロープ送信者アドレスの `@` 記号で始まる部分に対してドメイン名構文と一致させます。`@` 記号を含める必要があります。例：`@example.com`

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

`altsrchost` コマンド内のサブコマンドを使用して、CLI で Virtual Gateway にマッピングを作成します。

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

altsrchost ファイルのインポート

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

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

ステップ 2 CLI の外部で、ファイルを取得します。（詳細については、FTP、SSH、および SCP アクセスを参照してください）。

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

ステップ 4 ファイルを保存してインターフェイスの「altsrchost」ディレクトリに配置し、インポートできるようにします。（詳細については、FTP、SSH、および SCP アクセスを参照してください）。

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

altsrchost の制限

altsrchost エントリは、最大 1,000 個まで定義できます。

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

```
# Comments to describe the file

@example.com DemoInterface

paul@ PublicInterface

joe@ PublicInterface

192.168.1.5, DemoInterface

steve@example.com PublicNet
```

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

CLI を使用した altsrchost マッピングの追加

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

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

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

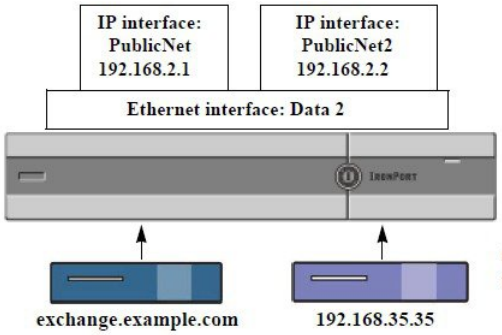
```
mail3.example.com> altsrchost

There are currently no mappings configured.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- IMPORT - Load new mappings from a file.

[]> new

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

[]> @exchange.example.com

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

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

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

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

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

[1]> 4

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

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.


[]> new


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


[]> 192.168.35.35

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

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

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

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

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

[1]> 1


Mapping for 192.168.35.35 on interface PublicNet2 created.

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

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

```
- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]> print

1. 192.168.35.35 -> PublicNet2

2. @exchange.example.com -> PublicNet

Choose the operation you want to perform:

- NEW - Create a new mapping.

- EDIT - Modify a mapping.

- DELETE - Remove a mapping.

- IMPORT - Load new mappings from a file.

- EXPORT - Export all mappings to a file.

- PRINT - Display all mappings.

- CLEAR - Remove all mappings.

[]>

mail3.example.com> commit

Please enter some comments describing your changes:

[]> Added 2 altsrchost mappings

Do you want to save the current configuration for rollback? [Y]> n

Changes committed: Fri May 23 11:42:12 2014 GMT
```

この例におけるコンフィギュレーションの変更を次の図に示します。

図 *12 :* 例：使用する *IP* インターフェイスまたはインターフェイス グループの選択



Virtual Gateway アドレスのモニタ

Virtual Gatewayアドレスごとに独自の配信用電子メール キューがありますが、システム管理、ロギング、レポートの機能では、全体的な観点からすべてのVirtual Gatewayキューが一体のものとして扱われます。Virtual Gateway キューごとに受信者ホストのステータスをモニタするには、hoststatus および hostrate コマンドを使用します。「CLI による管理およびモニタリング」の章の「モニタリングに使用できるコンポーネントの読み取り」を参照してください。

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

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

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

Virtual Gateway アドレスごとの配信接続の管理

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

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

destconfig コマンド、および仮想ゲートウェイ アドレスに対する影響については、宛先制御による電子メール配信の管理 （42 ページ）を参照してください。

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

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

グローバル配信停止機能の使用

特定の受信者、受信者ドメイン、またはIPアドレスがアプライアンスからメッセージを受信しないようにするには、AsyncOSの[グローバル配信停止（Global Unsubscribe）]機能を使用し

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

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

[グローバル配信停止（Global Unsubscribe）] には最大 10,000 アドレスを指定できます。[グローバル配信停止（Global Unsubscribe）] に追加されたアドレスは、次の 4 つのうちいずれかの形式をとります。

表 *10* : グローバル配信停止の構文

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

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

関連項目

- CLI を使用したグローバル配信停止へのアドレスの追加 （71 ページ）
- グローバル配信停止ファイルのエクスポートおよびインポート （72 ページ）

CLI を使用したグローバル配信停止へのアドレスの追加

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

```
mail3.example.com> unsubscribe

Global Unsubscribe is enabled. Action: drop.

Choose the operation you want to perform:

- NEW - Create a new entry.

- IMPORT - Import entries from a file.

- SETUP - Configure general settings.

[]> new

Enter the unsubscribe key to add. Partial addresses such as

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

"@.example.com" are allowed.

[]> user@example.net

Email Address 'user@example.net' added.

Global Unsubscribe is enabled.

Choose the operation you want to perform:

- NEW - Create a new entry.

- DELETE - Remove an entry.

- PRINT - Display all entries.

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

```
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>

mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added username "user@example.net" to global unsubscribe
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

グローバル配信停止ファイルのエクスポートおよびインポート

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

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

ステップ 2 CLI の外部で、ファイルを取得します。（詳細については、FTP、SSH、および SCP アクセスを参照してください）。

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

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

```
# this is an example of the global_unsubscribe.txt file
test@example.com
@testdomain.com
testuser@
11.12.13.14
```

ステップ 4 ファイルを保存してインターフェイスの configuration ディレクトリに配置し、インポートできるようにします。（詳細については、FTP、SSH、および SCP アクセスを参照してください）。

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

確認：電子メール パイプライン

次の表に、受信から配信へのルーティングまで、電子メールがシステムでルーティングされる様子の概要を示します。各機能は上から順に実行されます。ここでは簡単に説明します。「表：*E* メール セキュリティ アプライアンスの電子メール パイプライン：ルーティングおよび配信機能」の影付きの部分は、ワーク キューで実行される処理を表します。

このパイプラインに含まれる機能の設定の大部分は、trace コマンドを使用してテストできます。詳細については、「トラブルシューティング」の章の「テスト メッセージを使用したメール フローのデバッグ：トレース」を参照してください。

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

表 *11 : E* メール セキュリティ アプライアンスの電子メール パイプライン：電子メール受信機能

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

表 *12 : E* メール セキュリティ アプライアンスの電子メール パイプライン：ルーティングおよび配信機能

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

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

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