CHAPTER 4

電子メール パイプラインの理解

電子メール パイプラインは、IronPort アプライアンスによる処理に伴う、電子メールのプロセスまたはフローです。IronPort アプライアンスの性能を最大限まで引き出すには、電子メール パイプラインの理解が不可欠です。

この章では、着信メールの電子メール パイプラインの概要を示し、各機能について簡単に説明します。この簡単な説明には、その機能の詳細説明を含む章または資料へのリンクも含まれています。

この章は、次の内容で構成されています。

概要：電子メール パイプライン

表 4-1 および表 4-2 に、システムによる受信からルーティングおよび配信までの、着信電子メールの処理の概要を示します。各機能は順序どおり（上から下）に処理されます。各機能を以下で簡単に説明します。各機能の詳細説明については、後続の章を参照してください。一部の機能については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』および『*Cisco IronPort AsyncOS for Email Daily Management Guide*』で説明されています。

表 4-2 の網掛け部分は、ワーク キュー（「ワーク キューとルーティング」（P.4-99）を参照）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、Debugging Mail Flow Using Test Messages: Trace, page -446 を参照してください。

（注）　発信メールの場合は、ウイルス感染フィルタ ステージの後に RSA 電子メール データ損失防止スキャンが行われます。

表 4-1　IronPort アプライアンスの電子メール パイプライン：電子メール受信機能

機能	説明
Host Access Table（HAT; ホスト アクセス テーブル）	接続の ACCEPT、REJECT、RELAY、または TCPREFUSE。
ホスト DNS 送信者検証	最大アウトバウンド接続数。
送信者グループ	IP アドレスあたりの最大同時インバウンド接続数。
エンベロープ送信者検証	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。
送信者検証例外テーブル	メッセージあたりおよび時間あたりの最大受信者数。
メール フロー ポリシー	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	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	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。
Recipient Access Table（RAT; 受信者アクセス テーブル）	（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。

表 4-1　IronPort アプライアンスの電子メール パイプライン：電子メール受信機能（続き）

エイリアス テーブル	エンベロープ受信者を書き換えます。（システム全体を対象に設定されます aliasconfig は、listenerconfig のサブコマンドではありません）。
LDAP 受信者の受け入れ	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 4-2　IronPort アプライアンスの電子メール パイプライン：ルーティング機能および配信機能

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 *		メッセージ フィルタは、メッセージが「分裂」される前に適用されます。* メッセージを検疫エリアに送信できます。
	セーフリスト/ブロックリスト スキャン		AsyncOS では、送信者アドレスをエンドユーザ セーフリスト/ブロックリスト データベースと照合します。送信者アドレスがセーフリストにあれば、アンチスパムのスキャンはスキップされます。受信者が複数の場合は、メッセージを分裂できます。* 送信者が Blocklist にある場合は、メッセージを検疫エリアに送信できます。
	アンチスパム **	受信者ごとのスキャン	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。
	Anti-Virus*		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。* メッセージを検疫エリアに送信できます。
	コンテンツ フィルタ *		コンテンツ フィルタが適用されます。該当するコンテンツ フィルタ条件が定義されている場合は、DKIM、SPF、および SIDF 検証が実行されます。* メッセージを検疫エリアに送信できます。
	ウイルス感染フィルタ *		ウイルス感染フィルタ機能は、ウイルス拡散からの保護に有用です。* メッセージを検疫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。

表 4-2　IronPort アプライアンスの電子メール パイプライン：ルーティング機能および配信機能（続き）

配信制限	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	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	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	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	配信不能メッセージの処理です。リスナー単位、宛先制御エントリ単位、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。

** IronPort スパム検疫にメッセージを送信できます。

着信および受信

電子メール パイプラインの受信フェーズでは、送信者のホストからの初期接続が行われます。各メッセージのドメインを設定でき、受信者が検査されて、メッセージはワーク キューに渡されます。

ホスト アクセス テーブル（HAT）、送信者グループ、およびメール フロー ポリシー

HAT では、リスナーへの接続を許可するホスト（つまり、電子メールの送信を許可するホスト）を指定できます。

送信者グループは、1 つまたは複数の送信者をグループに関連付けるために使用されるもので、メッセージ フィルタおよびその他のメール フロー ポリシーを送信者グループに対して適用できます。メール フロー ポリシーは、一連の HAT パラメータ（アクセス ルール、レート制限パラメータ、およびカスタム SMTP コードと応答）を表現する 1 つの方法です。

送信者グループおよびメール フロー ポリシーは合わせて、リスナーの HAT で定義されます。

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。

SMTP カンバセーションに先立って、接続元のホストが送信者グループでホスト DNS 検証の対象になった一方で、送信者検証例外テーブルにエントリを追加できます。このテーブルはメールの受け入れや拒否の基盤となるドメインと電子メール アドレスのリストで、エンベロープ送信者 DNS 検証設定値の影響は受けません。エンベロープ送信者 DNS 検証設定値にかかわらず、受け入れるか拒否するメールの送信元であるドメインおよび電子メール アドレスをリストしている送信者検証例外テーブルにエントリを追加できます。

評価フィルタリングでは、電子メール送信者を分類でき、IronPort SenderBase 評価サービスによって決定された送信者の信頼性に基づいて電子メール インフラストラクチャの利用を制限できます。

詳細については、「ホスト アクセス テーブル（HAT）：送信者グループとメール フロー ポリシー」（P.5-115）を参照してください。

Received: ヘッダー

`listenerconfig` コマンドを使用すると、リスナーで受信したすべてのメッセージに対して、デフォルトでは Received: ヘッダーを組み込まないようにリスナーを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Advanced Configuration Options」を参照してください。

デフォルト ドメイン

完全修飾ドメイン名を含んでいない送信者アドレスにデフォルト ドメインを自動的に追加するようリスナーを設定できます。これらのアドレスを「素」アドレスとも呼びます（「joe」と「joe@example.com」など）。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「SMTP Address Parsing Options」を参照してください。

バウンス検証

発信メールには特別なキーがタグ付けされます。これにより、そのメールがバウンスとして送り返された場合は、そのタグを認識したうえでメールが配信されます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「IronPort Bounce Verification」を参照してください。

ドメイン マップ

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。たとえば、joe@old.com -> joe@new.com です。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「The Domain Map Feature」を参照してください。

受信者アクセス テーブル（RAT）

インバウンド電子メールに限っては、IronPort アプライアンスでメールを受け入れるすべてのローカル ドメインのリストを、RAT によって指定できます。

詳細については、「パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ」（P.5-177）を参照してください。

エイリアス テーブル

エイリアス テーブルには、1 人または複数の受信者にメッセージをリダイレクトするメカニズムが備わっています。エイリアスはマッピング テーブルに格納されます。電子メールのエンベロープ受信者（Envelope To または RCPT TO とも呼ぶ）とエイリアス テーブルに定義されているエイリアスが一致すると、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。

エイリアス テーブルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Creating Alias Tables」を参照してください。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メール アドレス（パブリック リスナー上）を SMTP カンバセーションまたはワーク キュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、IronPort アプライアンスでは、独特な方法で Directory Harvest Attacks（DHAP; ディレクトリ獲得攻撃）に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワーク キューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリで見つからない場合は、遅延型バウンスを実行するか、メッセージ全体をドロップするようにシステムを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

ワーク キューとルーティング

ワーク キューでは、配信フェーズに移動される前の受信メッセージを処理します。処理には、マスカレード、ルーティング、フィルタリング、セーフリスト/ブロックリスト スキャン、アンチスパムおよびアンチウイルス スキャン、ウイルス感染フィルタ、および検疫が含まれます。

（注）　Data Loss Prevention（DLP; データ損失防止）スキャンは、発信メッセージだけで使用可能です。DLP メッセージ スキャンが実行されるワーク キュー内の位置については、「メッセージ分裂」（P.6-194）を参照してください。

電子メール パイプラインとセキュリティ サービス

原則として、セキュリティ サービス（アンチスパム スキャン、アンチウイルス スキャン、およびウイルス感染フィルタ）に対する変更は、すでにワーク キューにあるメッセージには影響しません。次に例を示します。

初めてパイプラインに入るメッセージについて、次のいずれかの理由により、アンチウイルス スキャンがバイパスされると仮定します。

- アプライアンスでグローバルにアンチウイルス スキャンがイネーブルにされていなかった。または、
- アンチウイルス スキャンをスキップするように HAT ポリシーで指定されていた。または、
- そのメッセージに対するアンチウイルス スキャンをバイパスさせるメッセージ フィルタが存在していた。

この場合、アンチウイルス スキャングが再イネーブル化されているかどうかを問わず、検疫エリアから解放されるときにそのメッセージのアンチウイルス スキャンは行われません。ただし、メール ポリシーに基づいてアンチウイルス スキャンがバイパスされるメッセージの場合は、検疫エリアからの解放時にアンチウイルス スキャンが行われる可能性があります。メッセージが検疫エリアにある間に、メール ポリシーの設定値が変更される可能性があるためです。たとえば、メール ポリシーによってメッセージがアンチウイルス スキャンをバイパスし、検疫されている場合に、検疫エリアからの解放以前にメール ポリシーが更新されて、アンチウイルス スキャンが組み込まれた場合、そのメッセージは、検疫エリアからの解放時にアンチウイルス スキャンが行われます。

同様に、誤ってアンチスパム スキャンをグローバルに（または HAT で）ディセーブルにし、メールがワーク キューに入った後で気付いたとします。その時点でアンチスパムをイネーブルにしても、ワーク キューにあるメッセージについてはアンチスパム スキャンは行われません。

LDAP 受信者の受け入れ

既存の LDAP インフラストラクチャを使用して、着信メッセージの受信者電子メール アドレス（パブリック リスナー上）を SMTP カンバセーションまたはワーク キュー内で処理する方法を定義できます。『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Customizing Listeners」の章の「Accept Queries」を参照してください。これにより、IronPort アプライアンスでは、独特な方法で Directory Harvest Attacks（DHAP; ディレクトリ獲得攻撃）に対処できます。システムでは、メッセージを受け入れて、SMTP カンバセーションまたはワーク キューで LDAP 受け入れ検証を実行します。受信者が LDAP ディレクトリで見つからない場合は、遅延型バウンスを実行するか、メッセージ全体をドロップするようにシステムを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

マスカレードまたは LDAP マスカレード

マスカレードは、管理者が作成するテーブルに従って、プライベート リスナーで処理される電子メールのエンベロープ送信者（Sender または `MAIL FROM` とも呼ぶ）と To:、From:、CC: のヘッダーを書き換える機能です。スタティック マッピング テーブルと LDAP クエリーの 2 通りのうちいずれかによって、作成したリスナーごとに異なるマスカレード パラメータを指定できます。

スタティック マッピング テーブルによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章にある「Configuring Masquerading」を参照してください。

クエリーによるマスカレードの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

LDAP ルーティング

ネットワーク上の LDAP ディレクトリで使用可能な情報に基づいて、適切なアドレスやメール ホストにメッセージをルーティングするように IronPort アプライアンスを設定できます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」を参照してください。

メッセージ フィルタ

メッセージ フィルタでは、受信直後のメッセージおよび添付ファイルの処理方法を記述した特別なルールを作成できます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、メッセージ ヘッダー、またはメッセージ本文に基づいてメッセージを識別します。フィルタ アクションでは、メッセージのドロップ、バウンス、アーカイブ、検疫、ブラインド カーボン コピー、または変更を行うことができます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章を参照してください。

複数受信者メッセージは、このフェーズの後に、電子メール セキュリティ マネージャに先立って「分裂」されます。メッセージの分裂とは、電子メール セキュリティ マネージャによる処理のために、単一の受信者を設定した電子メールの分裂版コピーを作成することを指します。

電子メール セキュリティ マネージャ（受信者単位のスキャン）

セーフリスト/ブロックリスト スキャン

エンドユーザ セーフリストおよびブロックリストは、エンドユーザによって作成されて、アンチスパム スキャンに先行して検査されるデータベースに格納されます。各エンドユーザは、常にスパムとして扱うか、決してスパムとして扱わないドメイン、サブドメイン、または電子メール アドレスを指定できます。送信者アドレスがエンドユーザ セーフリストに含まれている場合、アンチスパム スキャンはスキップされます。送信者アドレスがブロックリストに含まれている

場合、メッセージは、管理者設定値に応じて検疫するかドロップすることができます。セーフリストおよびブロックリストの設定の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

アンチスパム

アンチスパム機能には、IronPort Anti-Spam スキャンが含まれます。アンチスパム スキャンは、インターネット全体にわたるサーバ側のアンチスパム保護を提供します。アンチスパム スキャンでは、スパム攻撃によってユーザに不便が生じ、ネットワークが蹂躙されたり損傷したりする前に、スパム攻撃を活発に識別し、危険を除去します。その結果、ユーザのプライバシーを侵害することなく、ユーザの受信箱に届く前に、不要なメールを削除できます。

アンチスパム スキャンは、IronPort スパム検疫（オンボックスまたはオフボックス）にメールを配信するように設定できます。IronPort スパム検疫から解放されたメッセージは、電子メール パイプラインの以降のすべてのワーク キュー処理をスキップして、宛先キューに直接移動されます。

詳細については、第 8 章「アンチスパム」を参照してください。

アンチウイルス

IronPort アプライアンスには、統合されたウイルス スキャン エンジンが含まれています。「メール ポリシー」ごとを基本に、メッセージおよび添付ファイルをスキャンしてウイルスを検出するように、アプライアンスを設定できます。ウイルスが検出された場合に次の処置を行うようにアプライアンスを設定できます。

- 添付ファイルの修復の試行
- 添付ファイルのドロップ
- 件名ヘッダーの変更
- 追加の X-Hader の追加
- 異なるアドレスまたはメールホストへのメッセージの送信
- メッセージのアーカイブ
- メッセージの削除

メッセージが検疫エリア（「検疫」（P.4-103）を参照）から解放されると、ウイルスがスキャンされます。アンチウイルス スキャンの詳細については、第 9 章「アンチウイルス」を参照してください。

コンテンツ フィルタ

受信者ごとまたは送信者ごとを基準に、メッセージに適用するコンテンツ フィルタを作成できます。コンテンツ フィルタは、電子メール パイプラインで後ほど適用される点、つまり、1 つのメッセージが、各電子メール セキュリティ マネージャ ポリシーに対応する個々の複数のメッセージに「分裂」された後で適用される点を除いては、メッセージ フィルタとほぼ同じです。コンテンツ フィルタ機能は、メッセージ フィルタ処理およびアンチスパムとアンチウイルス スキャンがメッセージに対して実行された後で適用されます。

コンテンツ フィルタの詳細については、「コンテンツ フィルタの概要」（P.6-198）を参照してください。

ウイルス感染フィルタ

IronPort のウイルス感染フィルタ機能には、新たな拡散に対抗するための重要な第 1 層となるように活発に動作する特別なフィルタが含まれています。IronPort の発行するアウトブレイク ルールに基づいて、特定のファイル タイプの添付ファイルを持つメッセージを Outbreak という名前の検疫エリアに送信できます。

Outbreak 検疫エリア内のメッセージは、他のすべての検疫エリア内のメッセージと同じように処理されます。検疫エリアおよびワーク キューの詳細については、「検疫」（P.4-103）を参照してください。

詳細については、第 10 章「ウイルス感染フィルタ」を参照してください。

検疫

IronPort AsyncOS では、着信メッセージまたは発信メッセージをフィルタして、検疫エリアに入れることができます。検疫エリアは、メッセージの保持と処理に使用される特別なキュー、言い換えるとリポジトリです。検疫エリア内のメッセージは、検疫の設定方法に基づいて配信するか削除できます。

次のワーク キュー機能では、メッセージを検疫エリアに送信できます。

- メッセージ フィルタ
- アンチウイルス
- ウイルス感染フィルタ
- コンテンツ フィルタ

メッセージが検疫エリアから解放されると、ウイルスが再度スキャンされます。

詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

配信

電子メール パイプラインの配信フェーズでは、接続の制限、バウンス、および受信者など、電子メール処理の最終フェーズを主とします。

仮想ゲートウェイ

IronPort Virtual Gateway テクノロジーを利用すると、IronPort アプライアンスを複数の仮想ゲートウェイ アドレスに分割できます。このアドレスから電子メールの送受信が行われます。各仮想ゲートウェイ アドレスには、個別の IP アドレス、ホスト名、およびドメインと電子メール配信キューが割り当てられます。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Using Virtual Gateway Technology」を参照してください。

配信制限

配信時に使用する IP インターフェイスに基づく配信の制限およびアプライアンスでアウトバウンド メッセージ配信に適用する最大同時接続数を設定するには、`deliveryconfig` コマンドを使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Set Email Delivery Parameters」を参照してください。

ドメインベースの制限値

各ドメインに対して、一定期間でシステムが超えることができない、接続および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、[Mail Policies] > [Destination Controls] ページ（または `destconfig` コマンド）から定義します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Controlling Email Delivery」を参照してください。

ドメインベースのルーティング

エンベロープ受信者を書き換えることなく、特定のドメイン宛てのすべての電子メールを特定の Mail Exchange（MX）ホストにリダイレクトするには、[Network] > [SMTP Routes] ページ（または `smtproutes` コマンド）を使用します。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Routing Email for Local Domains」を参照してください。

グローバル配信停止

特定の受信者、受信者ドメイン、または IP アドレスに対する IronPort アプライアンスからのメッセージの配信を確実に停止するには、グローバル配信停止を使用します。グローバル配信停止をイネーブルにすると、すべての受信者アドレスが、グローバル配信停止対象のユーザ、ドメイン、電子メール アドレス、および IP アドレスのリストと照合されます。一致する電子メールは送信されません。

詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Using Global Unsubscribe」を参照してください。

バウンス制限

作成する各リスナーのカンバセーションのハード バウンスおよびソフト バウンスを IronPort AsyncOS で処理する方法を設定するには、[Network] > [Bounce Profiles] ページ（または `bounceconfig` コマンド）を使用します。バウンス プロファイルを作成し、各リスナーにプロファイルを適用するには、[Network] > [Listeners] ページ（または `listenerconfig` コマンド）を使用します。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。

バウンス プロファイルの詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Configuring Routing and Delivery Features」の章の「Directing Bounced Email」を参照してください。