電子メール パイプラインについて

この章は、次の項で構成されています。

電子メール パイプラインの概要

電子メールパイプラインは電子メールゲートウェイで処理されるため、電子メールフローです。これには 3 フェーズあります。

- 受信：着信電子メールを受信するように電子メールゲートウェイはリモートホストに接続されるため、設定された制限やその他の受信ポリシーに従います。たとえば、ホストがユーザのメールを送信できることを確認し、受信接続とメッセージ制限を適用し、メッセージの受信者を検証します。
- ワークキュー：電子メールゲートウェイは着信および発信メールを処理し、フィルタリング、セーフリスト/ブロックリストスキャン、スパム対策およびウイルス対策スキャン、アウトブレイクフィルタ、隔離などを実行します。
- 配信：発信電子メールを送信するように電子メールゲートウェイは接続されるため、設定された配信制限とポリシーに従います。たとえば、発信接続制限を適用し、指定された配信不能メッセージを処理します。

電子メール パイプラインのフロー

次の図に、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処理される様子の概要を示します。各機能は順番に処理されます（上から下へ）。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。

図 *1:* 電子メール パイプライン：電子メール接続の受信

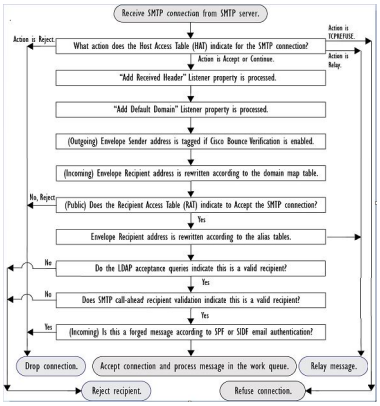


図 *2:* 電子メール パイプライン - 作業キュー

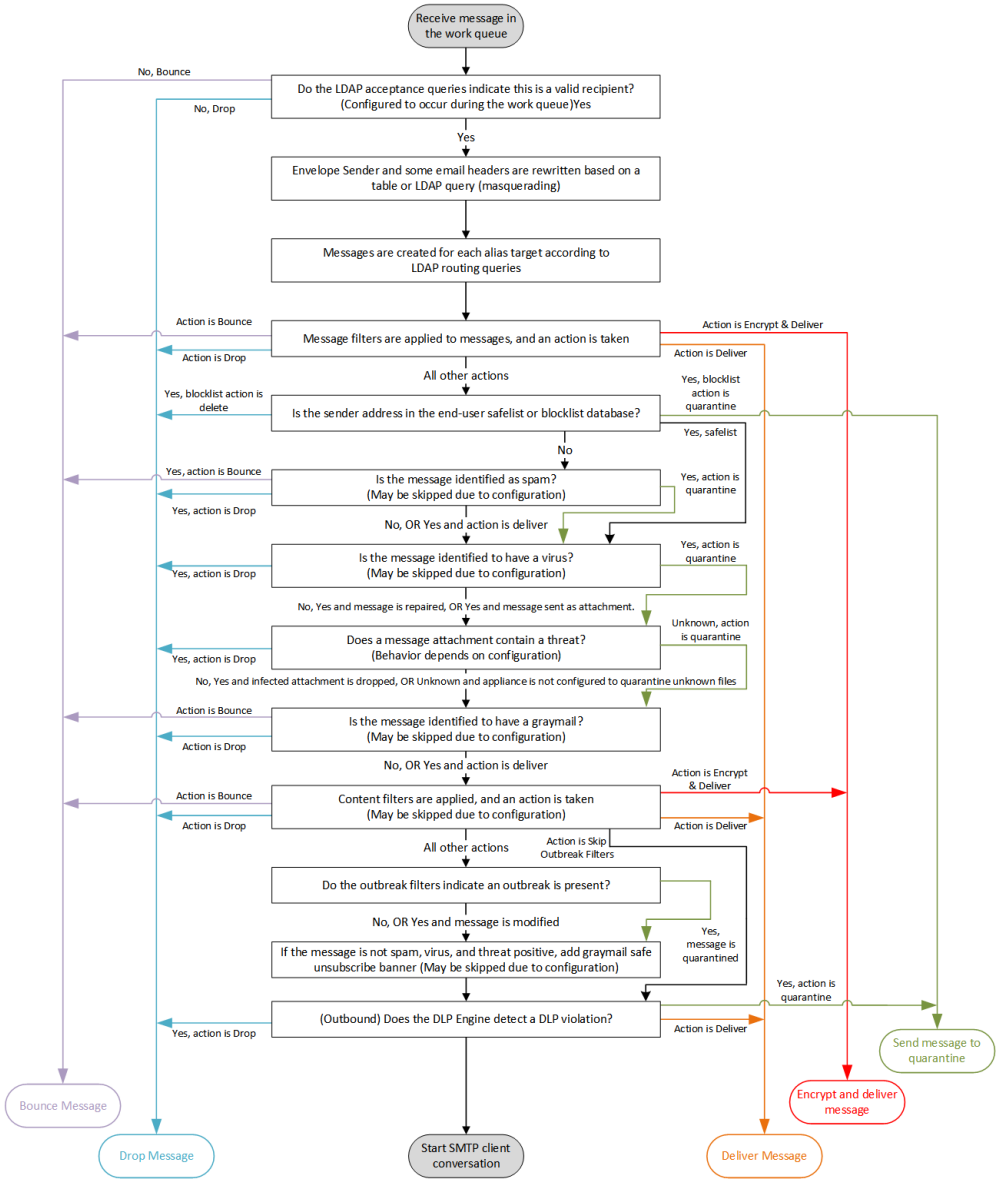
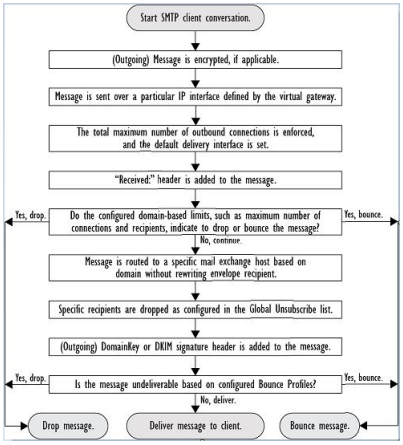


図 *3:* 電子メール パイプライン：電子メールの配信



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。

関連項目

- 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 （4 ページ）
- Received: ヘッダー （5 ページ）
- デフォルト ドメイン （5 ページ）
- バウンス検証 （5 ページ）
- ドメイン マップ （6 ページ）
- 受信者アクセス テーブル（RAT） （6 ページ）
- エイリアス テーブル （6 ページ）
- LDAP 受信者の受け入れ （6 ページ）
- SMTP コールアヘッド受信者検証 （6 ページ）

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、エンベロープ送信者のドメイン部分はメール フロー ポリシーで DNS 検証されます。この検証は、SMTP カンバセーションの間に行われます。不正な形式のエンベロープ送信者を含むメッセージを無視できます。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。

送信者レピュテーション フィルタリングでは、IP レピュテーション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、電子メールの送信者を分類し、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、定義済みの送信者グループとメール フロー ポリシーの理解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、リスナーの使用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、リスナーの使用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、バウンス検証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、ドメイン マップ機能を参照してください。

受信者アクセス テーブル（RAT）

着信電子メールに限っては、電子メールゲートウェイ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、受信者のアドレスに基づく接続の許可または拒否の概要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、エイリアス テーブルの作成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。詳細については、リスナーの使用を参照してください。これにより、電子メールゲートウェイでは、独特な方法でディレクトリ獲得攻撃（DHAP）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 ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、LDAP クエリに関する作業を参照してください。

SMTP コールアヘッド受信者検証

電子メールゲートウェイで SMTP コールアヘッド受信者検証を設定すると、電子メールゲートウェイは、SMTP サーバに「事前に電話して」受信者を検証する間、送信側の MTA との SMTP 通信を中断します。電子メールゲートウェイが SMTP サーバに問い合わせると、SMTP サーバの応答が電子メールゲートウェイに返されます。電子メールゲートウェイは SMTP 通信を再開し、送信側の MTA に応答を送信し、SMTP サーバの応答（および SMTP コールアヘッドプロファイルの設定）に基づいて接続を続行するかドロップします。

詳細については、「SMTP サーバを使用した受信者の検証」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、ファイル レピュテーションのスキャンと分析、アウトブレイク フィルタ、および隔離が含まれます。

（注） データ漏洩防止（DLP）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、メッセージ分裂を参照してください。

関連項目

- 電子メール パイプラインとセキュリティ サービス （7 ページ）
- LDAP 受信者の受け入れ （6 ページ）
- マスカレードまたは LDAP マスカレード （8 ページ）
- LDAP ルーティング （8 ページ）
- メッセージ フィルタ （9 ページ）
- 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） （9 ページ）
- 隔離 （11 ページ）

電子メール パイプラインとセキュリティ サービス

Cisco Secure Email Cloud Gateway のセキュリティサービスは、イネーブルにして変更しないことを推奨します。

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、およびアウトブレイク 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 スキャンが再イネーブル化されているかどうかを問わず、隔離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、隔離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。メッセージが隔離エリアにある間に、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、隔離されている場合に、隔離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、隔離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。詳細については、リスナーの使用を参照してください。これにより、電子メールゲートウェイでは、独特な方法でディレクトリ獲得攻撃（DHAP）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ディレクトリ内で見つからない場合に、遅延バウンスを実行するか、そのメッセージ全体をドロップするかを設定できます。

詳細については、LDAP クエリに関する作業を参照してください。

マスカレードまたは LDAP マスカレード

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とも呼ぶ）およびプライベートまたはパブリック リスナーによって処理される電子メールの 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、マスカレードの構成を参照してください。

LDAP クエリーによるマスカレードの詳細については、LDAP クエリに関する作業を参照してください。

LDAP ルーティング

ネットワーク内のLDAPディレクトリに格納されている情報に基づいてメッセージを適切なアドレスやメールホストへルーティングするように、電子メールゲートウェイを設定できます。

詳細については、LDAP クエリに関する作業を参照してください。

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、隔離、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、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。

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隔離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に関する詳細については、スパム隔離を参照してください。

スパム対策

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。

スパム対策スキャンはスパム隔離にメールを配信するように設定できます（オンボックスまたはオフボックス）。スパム隔離からリリースされるメッセージは電子メールパイプラインで処理する以降のワーク キューをとばし、宛先キューに直接進みます。

詳細については、スパムおよびグレイメールの管理を参照してください。

アンチウイルス

電子メールゲートウェイには、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、電子メールゲートウェイを設定できます。ウイルスが検出された場合に次の処置を行うように電子メールゲートウェイを設定できます。

- 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
- X-Header 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

メッセージが隔離エリア（隔離 （11 ページ）を参照）から解放されると、ウイルスがスキャンされます。アンチウィルス スキャンの詳細については、アンチウイルスを参照してください。

グレイメールの検出と安全な購読解約

グレイメールメッセージを検出し、エンドユーザに代わって安全な購読解約を実行するように電子メールゲートウェイを設定できます。実行できるアクションは、アンチウイルス スキャンで実行できるアクションに似ています。

詳細については、スパムおよびグレイメールの管理を参照してください。

ファイル レピュテーション スキャンおよびファイル分析

メッセージの添付ファイルをスキャンし、新たな脅威や標的型の脅威が含まれているかどうかを確認するように、電子メールゲートウェイを設定できます。実行できるアクションは、アンチウイルス スキャンで実行できるアクションに似ています。

詳細については、「ファイル レピュテーション フィルタリングとファイル分析」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 フィルタを参照してください。

アウトブレイク フィルタ

シスコのアウトブレイク 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。シスコ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 という名前の隔離エリアに送信できます。

Outbreak 隔離エリア内のメッセージは、他のすべての隔離エリア内のメッセージと同じように処理されます。隔離エリアおよびワーク キューの詳細については、隔離 （11 ページ）を参照してください。

詳細については、アウトブレイク フィルタを参照してください。

隔離

着信メッセージまたは発信メッセージをフィルタして隔離エリアに入れることができます。隔離エリアは、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。隔離エリア内のメッセージは、隔離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、メッセージを隔離エリアに送信できます。

- スパム フィルタ
- メッセージ フィルタ
- ウイルス対策
- アウトブレイク フィルタ
- コンテンツ フィルタ
- ファイル分析（高度なマルウェア防御）

メッセージが隔離エリアから配信されると、脅威が再度スキャンされます。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離
- スパム隔離

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。

関連項目

- 仮想ゲートウェイ （12 ページ）

仮想ゲートウェイ

Virtual Gateway テクノロジーを使用すると、電子メールゲートウェイを複数の 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、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、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電子メールゲートウェイ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、電子メール配信パラメータの設定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、[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 `destconfig` コマンド）から定義します。

詳細については、宛先制御による電子メール配信の管理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、[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。

詳細については、ローカル ドメインの電子メールのルーティングを参照してください。

グローバル登録解除

特定の受信者、受信者ドメイン、または IP アドレスに対する電子メールゲートウェイ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、グローバル配信停止機能の使用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 AsyncOS で処理する方法を設定するには、[ネットワーク（Network）]>[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、[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、バウンスした電子メールの処理を参照してください。