SMTP サーバを使用した受信者の検証

この章は、次の項で構成されています。

SMTP コールアヘッド受信者検証の概要

SMTP コールアヘッド受信者検証機能では、受信者宛ての着信メールを受け入れる前に、外部 SMTP サーバにクエリを実行します。LDAP 承認または Recipient Access Table（RAT; 受信者アクセステーブル）を使用できない場合、受信者を検証するためにこの機能を使用します。たとえば、それぞれ別のドメインを使用する多数のメール ボックスのメールをホストしていて、LDAP インフラストラクチャが各受信者を検証するために LDAP サーバにクエリーすることを許可していないとします。この場合、電子メールゲートウェイが SMTP サーバにクエリーを実行して、SMTP 通信を続ける前に受信者を検証できます。

SMTP コールアヘッド受信者検証を使用して、無効な受信者宛てのメッセージの処理を減らします。通常、無効な受信者宛てのメッセージは、ドロップする前にワーク キューを通して処理します。代わりに、電子メール パイプラインの着信および受信部分で追加処理を行わずに無効なメッセージをドロップまたはバウンスできます。

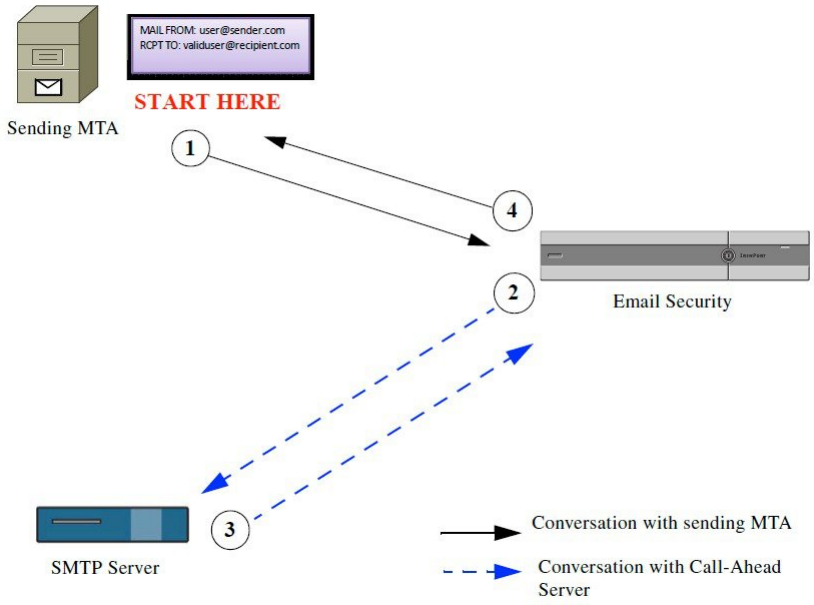
SMTP コールアヘッド受信者検証のワークフロー

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は、SMTP サーバにクエリーを実行するとき、SMTP サーバの応答を E メール セキュリティ アプライアンスに返し、ユーザの設定に基

づいて、メールを受け入れるか、コードとカスタム応答で接続をドロップすることができます。

次の図に、SMTP コールアヘッド検証通信の基本的なワークフローを示します。

***Figure 1: SMTP* コールアヘッド サーバ通信のワークフロー**



1. 送信側の MTA が SMTP 通信を開始します。
2. 電子メールゲートウェイは、SMTP サーバにクエリーを送信して受信者 validuser@recipient.com を検証する間、SMTP 通信を中断します。

Note SMTP ルートまたは LDAP ルーティング クエリーが設定されている場合、SMTP サーバへのクエリーにはこれらのルートが使用されます。

3. SMTP サーバは、電子メールゲートウェイにクエリーの応答を返します。
4. 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。

電子メールパイプラインでの処理の順序が決まっているため、特定の受信者宛てのメッセージが RAT によって拒否された場合、SMTP コールアヘッド受信者検証は発生しません。たとえば、RAT で *example.com* 宛てのメールのみを受け入れるように指定した場合、SMTP コールアヘッド受信者検証が発生する前に、*recipient@domain2.com* 宛てのメールは拒否されます。

Note HAT でディレクトリ ハーベスト攻撃防止（DHAP）を設定した場合、SMTP コールアヘッド サーバの拒否は、指定した 1 時間あたりの最大無効受信者数の中の拒否数に含まれるので注意してください。SMTP サーバによって拒否が増える場合を考慮してこの数を調整する必要があります。DHAP の詳細については、「ゲートウェイでのメール受信の設定」を参照してください。

外部 SMTP サーバを使用した受信者の検証方法

	操作内容	詳細
ステップ 1	電子メールゲートウェイの SMTP サーバへの接続およびサーバの応答の解釈方法を決定します。	コールアヘッド サーバ プロファイルの設定, on page 3
ステップ 2	SMTP サーバが受信者を検証するようにパブリック リスナーを設定します。	リスナーでの SMTP サーバ経由の着信メール検証のイネーブル化, on page 8
ステップ 3	（任意）メールの別のホストにルーティングする際に使用する SMTP サーバを決定するには、LDAP ルーティング クエリーを更新します。	LDAP ルーティング クエリの構成, on page 8
ステップ 4	（任意）特定の受信者に対してコールアヘッド検証をバイパスするように電子メールゲートウェイを設定します	特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス, on page 10

関連項目

- コールアヘッド サーバ プロファイルの設定, on page 3

コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッドサーバプロファイルの設定では、電子メールゲートウェイと SMTP サーバの接続方法と SMTP サーバから返される応答の解釈方法を設定します。

Procedure

ステップ 1 [ネットワーク（Network）]>[SMTP コールアヘッド（SMTP Call-Ahead）] をクリックします。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 プロファイルの設定値を入力します。詳細については、表「SMTP コールアヘッド サーバ プロファイルの設定」を参照してください。

ステップ 4 プロファイルの高度な設定を指定します。詳細については、表「SMTP コールアヘッドサーバプロファイルの詳細設定」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。

What to do next

- SMTP コールアヘッド サーバ プロファイルの設定, on page 4
- コールアヘッド サーバの応答, on page 7

SMTP コールアヘッド サーバ プロファイルの設定

SMTP コールアヘッドサーバプロファイルの設定時に、電子メールゲートウェイと SMTP サーバの接続方法を設定する必要があります。

***Table 1: SMTP* コールアヘッド サーバ プロファイルの設定**

設定	説明
プロファイル名（Profile Name）	コールアヘッド サーバ プロファイルの名前。

設定	説明
コールアヘッド サーバ タイプ（Call-Ahead Server Type）	コールアヘッド サーバへの接続方法を次から 1 つ選択します。 • [配信ホストを使用（Use Delivery Host）]。SMTP コールアヘッド クエリーに配信電子メール アドレスのホストを使用するように指定する場合は、このオプションを選択します。たとえば、メールの受信アドレスが recipient@example.com の場合、SMTP クエリーは example.com に関連付けられた SMTP サーバに対して実行されます。SMTP ルートまたは LDAP ルーティング クエリーを設定した場合、クエリー先の SMTP サーバの決定には、これらのルートが使用されます。LDAP ルーティング クエリーの設定についての詳細は、LDAP ルーティング クエリの構成, on page 8を参照してください。 • [スタティック コールアヘッドサーバ（Static Call-Ahead Server）]。クエリー先のコールアヘッド サーバのスタティック リストを作成する場合は、このオプションを使用します。コールアヘッド サーバの名前や場所が頻繁に変わらないと思われる場合は、このオプションを使用できます。このオプションを使用すると、電子メール ゲートウェイは、リストの最初のスタティック コールアヘッドサーバからラウンドロビン方式でホストにクエリーを送信します。 **Note** スタティック コールアヘッド サーバ タイプを選択すると、クエリーに SMTP ルートは適用されないので注意してください。その代わり MX ルックアップが実行され、その後、ホストでスタティック サーバのコールアヘッド IP アドレスを取得するためのルックアップが実行されます。
スタティック コールアヘッドサーバ（Static Call-Ahead Servers）	スタティック コールアヘッド サーバ タイプを使用する場合は、このフィールドにホストとポートの組み合わせのリストを入力します。次の構文を使用して、サーバとポートのリストを作成します。 ironport.com:25 複数のエントリがある場合は、カンマで区切ります。

次の表に、SMTP コールアヘッド サーバ プロファイルの高度な設定を示します。

Table 2: SMTP コールアヘッド サーバ プロファイルの高度な設定

設定	説明
インターフェイス（Interface）	SMTP サーバと SMTP 通信を開始するときに使用されるインターフェイス。 [管理インターフェイス（Management interface）] または [自動（Auto）] のどちらを使用するかを選択します。[自動（Auto）] を選択すると、電子メールゲートウェイは、使用するインターフェイスを自動的に検出しようとします。Cisco IronPort インターフェイスは、次の方法で SMTP サーバとの接続を試みます。 • コールアヘッドサーバが設定済みインターフェイスの1つと同じサブネット上にある場合、接続は一致するインターフェイスによって開始されます。 • 設定済みの任意の SMTP ルートが、クエリーのルートに使用されます。 • それ以外の場合、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。
受信者検証の TLS サポート	TLS を使用して SMTP コールアヘッド受信者検証を実行する場合は、[イネーブル化（Enabled）] オプションボタンを選択します。 **Note** SMTP コールアヘッド受信者検証では、電子メールゲートウェイの [SSL 設定（SSL Configuration）] ページの [その他の TLS クライアントサービス（Other TLS Client Services）] オプションで選択したものと同じ TLS バージョンを使用します。 **Note** [受信者検証の TLS サポート（TLS Support for Recipient Validation）] オプションを選択した場合は、TLS を使用した SMTP コールアヘッド受信者検証を確立するために、電子メールゲートウェイに有効なクライアント証明書を追加します。 **Note** SMTP コールアヘッド受信者検証の TLS サポートでは、DEFAULT SSL 暗号リストを使用します。DEFAULT キーワードは OpenSSL DEFAULT 暗号ストリングで、通常は `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2` です。
MAIL FROMアドレス（MAIL FROM Address）	SMTP サーバとの SMTP 通信に使用される MAIL FROM: アドレス。
検証要求タイムアウト（Validation Request Timeout）	SMTP サーバからの結果を待機する秒数。このタイムアウト値は、複数のコールアヘッドサーバにアクセスする可能性のある1つの受信者検証要求に対する値です。コールアヘッドサーバの応答, on page 7を参照してください。

設定	説明
検証エラーのアクション（Validation Failure Action）	受信者検証要求が失敗した場合（タイムアウト、サーバの障害、ネットワークの問題、または不明な応答により）に実行するアクション。電子メールゲートウェイでのさまざまな応答の処理方法を設定できます。コールアヘッド サーバの応答, on page 7を参照してください。
一時的なエラーのアクション（Temporary Failure Action）	受信者検証要求が一時的に失敗した場合（リモートSMTPサーバから4xx応答が返された）に実行するアクション。メールボックスが一杯の場合、メールボックスを利用できない場合、またはサービスを利用できない場合に発生することがあります。 コールアヘッド サーバの応答, on page 7を参照してください。
セッションあたりの最大受信者数（Max. Recipients per Session）	1 つの SMTP セッションで検証する最大受信者数。 1 ～ 25,000 セッションの間で指定します。
サーバあたりの最大接続数（Max. Connections per Server）	1 台のコールアヘッド SMTP サーバへの最大接続数。 1 ～ 100 接続の間で指定します。
キャッシュ	SMTP応答のキャッシュのサイズ。100 ～ 1,000,000 エントリの間で指定します。
キャッシュTTL（Cache TTL）	キャッシュ内でのエントリの存続可能時間値。このフィールドのデフォルト値は 900 秒です。60 ～ 86400 秒の間で指定します。

コールアヘッド サーバの応答

SMTP サーバからは、次の応答が返されます。

- **2xx**：コールアヘッド サーバから 2 で始まる SMTP コードを受け取った場合、受信者は受け入れられます。たとえば、応答が250の場合、メーリングアクションを続行できます。
- **4xx**：4 で始まる SMTP コードは、SMTP 要求の処理中に一時的な障害が発生したことを示します。後で再試行すると正常に処理されることがあります。たとえば、応答451は、要求されたアクションが中止されたか、処理中にローカル エラーが発生したことを示します。
- **5xx**：5 で始まる SMTP コードは、SMTP 要求の処理中に永続的な障害が発生したことを示します。たとえば、応答 550 は、要求されたアクションが実行されなかったか、メールボックスを使用できなかったことを示します。
- **タイムアウト。**コールアヘッドサーバから応答が戻されない場合、タイムアウトが発生する前に再試行する時間を設定できます。
- **接続エラー。**コールアヘッドサーバへの接続に失敗した場合、受信者アドレスへの接続を受け入れるか拒否するかを設定できます。

- **カスタム応答**。検証エラーおよび一時エラーのためにカスタムSMTP応答（コードとテキスト）との接続を拒否するよう設定できます。

リスナーでのSMTPサーバ経由の着信メール検証のイネーブル化

SMTP コールアヘッド サーバ プロファイルを作成したら、そのプロファイルをリスナーでイネーブルにして、リスナーがSMTPサーバ経由の着信メールを検証できるようにする必要があります。プライベート リスナーでは受信者の検証は必要ないので、SMTP コールアヘッド機能はパブリック リスナーでのみ使用できます。

Procedure

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] に移動します。

ステップ 2 SMTP コールアヘッド機能をイネーブルにするリスナーの名前をクリックします。

ステップ 3 [SMTPコールアヘッドプロファイル（SMTP Call Ahead Profile）] フィールドで、イネーブルにする SMTP コールアヘッド プロファイルを選択します。

ステップ 4 変更を送信し、保存します。

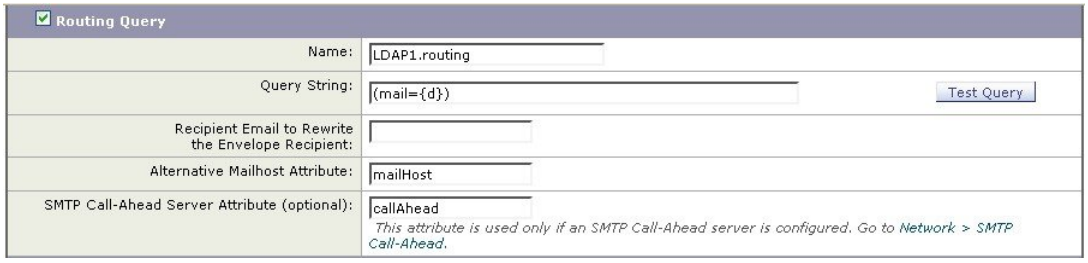
LDAP ルーティング クエリの構成

LDAP ルーティング クエリーを使用して、メールを異なるメール ホストにルーティングする場合、AsyncOS は、代替メールホスト属性を使用して、クエリー先のSMTPサーバを決定します。ただし、この処理が不適切な場合があります。たとえば、次のスキーマでは、メール ホスト属性（mailHost）には、コールアヘッドSMTPサーバの属性（callAhead）で指定されているサーバとは異なる SMTP アドレスがあります。

```
dn: mail=cisco.com, ou=domains
mail: cisco.com
mailHost: smtp.mydomain.com
policy: ASAV
callAhead: smtp2.mydomain.com,smtp3.mydomain.com:9025
```

この場合、[SMTPコールアヘッド（SMTP Call-Ahead）] フィールドを使用して、SMTP コールアヘッド クエリーを callAhead 属性で指定されているサーバに転送するルーティング クエリーを作成できます。たとえば、次の属性でルーティング クエリーを作成できます。

Figure 2: SMTP コールアヘッド用に設定された *LDAP* ルーティング クエリー



このクエリーでは、{d} は受信者アドレスのドメイン部分を表し、SMTP コールアヘッド サーバ属性は、クエリーに使用するコールアヘッド サーバとポートの値として、ポート 9025 の smtp2.mydomain.com、smtp3.mydomain.com を返します。

Note この例は、LDAP ルーティング クエリーを使用して SMTP コールアヘッド クエリーを正しい SMTP サーバに転送できるクエリーの設定例の 1 つです。この例で説明したクエリー文字列や特定の LDAP 属性を使用する必要はありません。

SMTP コールアヘッド クエリのルーティング

SMTP コールアヘッドクエリーのルーティング時、AsyncOS は次の順序で情報をチェックします。

1. ドメイン名をチェックします。
2. LDAP ルーティング クエリーをチェックします。
3. SMTP ルートをチェックします。
4. DNS ルックアップを実行します（MX ルックアップ、A ルックアップの順に実行）。

ドメインに LDAP ルーティング クエリーまたは SMTP ルートが設定されていない場合、前の状態の結果は次のステージに渡されます。SMTP ルートが存在しない場合は、DNS ルックアップが実行されます。

SMTP コールアヘッド クエリーの代わりに LDAP ルーティング クエリーを使用するときに、SMTP ルートも設定されている場合、ルーティング動作は、ルーティング クエリーから返される値によって異なります。

- LDAP ルーティング クエリーからポートなしで 1 つのホスト名が返された場合、SMTP コールアヘッドクエリーは SMTP ルートを適用します。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。
- LDAP ルーティング クエリーからポートと共に 1 つのホスト名が返された場合、その SMTP ルートが使用されますが、SMTP ルートでポートが指定されていても、LDAP クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

- LDAP ルーティング クエリーからポートと共に、またはポートなしで複数のホストが返された場合、SMTP ルートが適用されますが、SMTP ルートでポートが指定されていても、LDAP ルーティング クエリーによって返されたポートが使用されます。SMTP ルートがホスト名として宛先ホストだけ指定した場合、SMTP サーバの IP アドレスを取得するように、DNS ルックアップが実行されます。

特定のユーザまたはグループの SMTP コールアヘッド検証のバイパス

リスナーで SMTP コールアヘッド検証をイネーブルにしたまま、特定のユーザまたはユーザグループに対して SMTP コールアヘッド検証を省略する必要がある場合があります。

SMTP コールアヘッド クエリー中にメールを遅延させてはならない受信者に対する SMTP コールアヘッド検証を省略する場合です。たとえば、有効であることが明確であり、迅速な対応を必要とするカスタマー サービスのエイリアスに RAT エントリを追加できます。

SMTP コールアヘッド検証のバイパスを GUI から設定するには、RAT エントリを追加または編集するときに [SMTPコールアヘッドをバイパス（Bypass SMTP Call-Ahead）] を選択します。