Cisco Cloud/Hybrid Secure Email の概要

発行日:2017年7月28日
改訂:2021 年 3 月 22 日

Cisco Systems, Inc.
www.cisco.com

Cisco は世界各国 200 箇所にオフィスを開設しています。
所在地、電話番号、FAX 番号
は当社の Web サイト
(www.cisco.com/go/offices)をご覧ください。

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Cloud/Hybrid Secure Email の概要

Cisco E メールセキュリティサービスについて

Cisco クラウド E メール セキュリティ サービスの概要

Cisco クラウド E メール セキュリティは、耐障害性が高い各地のシスコ データセンターで管理されるインフラストラクチャを提供します。このサービスは、「クラウド」または Software as a Service（SaaS）モデルに基づいた E メール セキュリティを提供します。組織では、クラウドベースのインフラストラクチャにアクセスでき、インフラストラクチャを視覚化できます。

このガイド全体で、「アプライアンス」という用語は、仮想アプライアンスを示すために使用されます。

Cisco クラウド E メール セキュリティは、包括的なサービスです。ソフトウェア、ハードウェア、およびサポートがすべてバンドルされています。このサービスには、次の特徴および機能があります。

- **外部脅威フィードの使用。**外部の脅威フィード（ETF）フレームワークは、Cisco E メール セキュリティ ゲートウェイで、TAXII プロトコルで通信される STIX 形式の外部脅威情報を使用することを可能にします。
- **送信者ドメイン レピュテーション フィルタリング。**送信者ドメイン レピュテーション（SDR）フィルタリングを使用すると、シスコの SDR サービスによって決定される SDR に基づいて、Cisco E メール セキュリティ ゲートウェイを通過するメッセージをフィルタリングできます。
- **新しいデータ損失防止（DLP）ソリューション。**シスコは、RSA DLP で作成されたすべての既存の DLP ポリシーを新しい DLP エンジンへとシームレスに移行できる、代替の DLP ソリューションを提供します。アップグレード後は、Web インターフェイスの、[メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] ページで、移行した DLP ポリシーを表示または変更できます。

（注）　Async0S 11.0 以降は、RSA Enterprise Manager の統合のサポートはありません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。

- IP レピュテーションフィルタと IronPort Anti-Spam を統合した独自のマルチレイヤアプローチによるゲートウェイでの**スパム対策**。
- Sophos および McAfee ウイルス対策スキャン エンジンによるゲートウェイでの**ウイルス対策**。
- **グレイメールの検出と安全な購読解約。**Cisco E メール セキュリティ アプライアンスでは、以下を行うことができます。
  - 統合グレイメール エンジンを使用してグレイメールを識別し、適切なポリシー制御を適用します。
  - エンド ユーザがクラウドベースの購読解約サービスを使用して不要なグレイメールを購読解約できる安全で簡単なメカニズムが提供されます。
- **Outbreak Filters™。**これは、新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対するシスコの独自保護機能です。
- **ポリシー、ウイルス、およびアウトブレイク隔離。**管理者による評価のために、疑わしいメッセージを保存する安全な場所が提供されます。
- **スパム隔離。**隔離されたスパムおよび疑わしいスパムへのエンド ユーザ アクセスが提供されます。
- **電子メール認証。**このアプライアンスは、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- **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。**高度なマルウェア防御は、次の情報に基づいて着信メッセージおよび発信メッセージに含まれる新たな標的型ファイルベースの脅威を特定します。
  - ファイル レピュテーション
  - ファイル分析（レピュテーションが不明な一部のファイルのための機能）
  - 判定のアップデート
- **URL フィルタリング。**URL フィルタリングは、着信メッセージと発信メッセージ内の URL のレピュテーションとカテゴリを取得することによって、次のような新しい機能を有効にします。
- **S/MIME セキュリティ サービス。**Cisco E メール セキュリティ アプライアンスにより、組織は S/MIME を使用して安全に通信できます。このとき、どのエンド ユーザも自分の証明書を所持する必要はありません。組織は、個人ではなく組織を識別する証明書を使用して、ゲートウェイ レベルでメッセージの署名、暗号化、検証、および復号化を処理できます。
- **E メール暗号化。**HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、Cisco E メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ホステッド キー サービスを使用してメッセージを暗号化します。
- **メッセージ トラッキング。**このアプライアンスには、Cisco E メール セキュリティ アプライアンスが処理するメッセージのステータスを簡単に検索できる、メッセージ トラッキング機能があります。

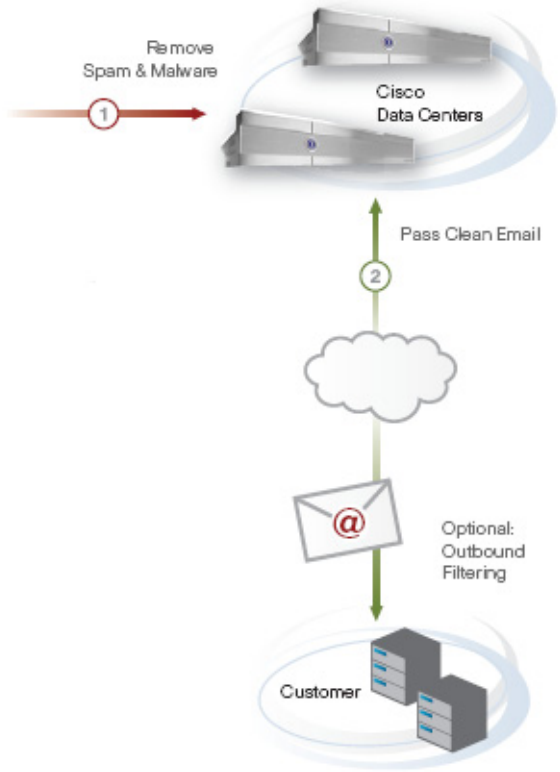
- **メール フロー モニタリング。**すべての着信メッセージおよび発信メッセージのメール フローを監視できます。企業のすべての E メール トラフィックが完全に視覚化されます。
- **アクセス制御。**送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者のアクセス制御。
- 広範な**メッセージ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。フィルタ ルールでは、メッセージまたは添付ファイルの内容、ネットワークに関する情報、メッセージ エンベロープ、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、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。
- **Transport Layer Security 上の安全な SMTP によるメッセージの暗号化。**企業インフラストラクチャと他の信頼されているホストの間で送受信されるメッセージが暗号化されます。

  統合された堅牢なレポート オプションにより、各地に導入されているインフラストラクチャからのトラフィック データが分析され、完全に統合されたセキュリティ レポートが提供されます。Cisco E メール セキュリティ アプライアンスの第 3 世代レポート技術により、世界で最も通信量が多いネットワークでも詳細に調査できます。詳細かつ正確な情報が明快かつ有益なレポートにまとめられます。このレポートは、どのレベルの組織にも適しています。

  メッセージ トラッキングにより、組織は、ダウン メッセージの処理を追跡するために、ほぼリアルタイムでメッセージを視認できます。この機能により、メッセージの正確な場所を判断することで、ヘルプ デスク コールを迅速に解決できます。フレキシブルなトラッキング インターフェイスを使用してメッセージを見つけることができます。このとき、ログ ファイル全体を検索する必要はありません。

図 1-1 は、Cisco クラウド E メール セキュリティの導入モデルを示しています。

図 1-1　　Cisco クラウド E メール セキュリティの導入



Cisco クラウド E メール セキュリティは、次のように動作します。

- E メール セキュリティ アプライアンスにより、クラスタ構成と呼ばれる他の E メール セキュリティ アプライアンスの間で構成情報が同期されます。
- E メール セキュリティ アプライアンスのクラウドベースのクラスタで、着信メールが受け入れられ、処理されます。
- クラウドベースのセキュリティ管理アプライアンスにより、クラウド E メール セキュリティ アプライアンスから、レポート データおよびトラッキング データが収集されます。このアプライアンスは、ポリシーによって隔離されたメッセージの集中地点、または E メール セキュリティ アプライアンス クラスタのスパムの集中地点として機能します。
- ポリシーに基づいてフィルタ処理されたメールは中央に隔離されます。
- システムにより、処理されたメールがグループウェア サーバまたはメール転送エージェント（MTA）に直接送信され、グループウェア サーバからの発信メールが処理され、高度なコンテンツ フィルタリングおよび E メールの暗号化が行われます。
- （オプション）E メール セキュリティ アプライアンス クラスタを介して発信メールをインターネットに送信できます。

Cisco Hybrid Email Security の概要

Cisco Hybrid Email Security は、クラウドベースの E メール セキュリティの導入とアプライアンスベースの E メール セキュリティの導入（オンプレミス）を結合する固有のサービス オファリングです。これにより、組織では選択および制御の幅が最大となります。クラウドベースのインフラストラクチャは、通常、着信 E メールのクレンジングに使用され、一方オンプレミス アプライアンスでは、きめ細かい制御（データ損失防止（DLP）技術と暗号化技術による機密情報の保護）が提供されます。

このハイブリッド サービスは、Cisco クラウド E メール セキュリティ サービスと同様に包括的であり、ソフトウェア、ハードウェア、およびサポートがすべてバンドルされています。このサービスには、次の特徴および機能があります。

- **外部脅威フィードの使用。**外部の脅威フィード（ETF）フレームワークは、Cisco E メール セキュリティ ゲートウェイで、TAXII プロトコルで通信される STIX 形式の外部脅威情報を使用することを可能にします。
- **送信者ドメイン レピュテーション フィルタリング。**送信者ドメイン レピュテーション（SDR）フィルタリングを使用すると、シスコの SDR サービスによって決定される SDR に基づいて、Cisco E メール セキュリティ ゲートウェイを通過するメッセージをフィルタリングできます。
- **新しいデータ損失防止（DLP）ソリューション。**シスコは、RSA DLP で作成されたすべての既存の DLP ポリシーを新しい DLP エンジンへとシームレスに移行できる、代替の DLP ソリューションを提供します。アップグレード後は、Web インターフェイスの、[メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] ページで、移行した DLP ポリシーを表示または変更できます。

  （注）　Async0S 11.0 以降は、RSA Enterprise Manager の統合のサポートはありません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。

- IP レピュテーションフィルタと IronPort Anti-Spam を統合した独自のマルチレイヤアプローチによるゲートウェイでの**スパム対策**。
- Sophos および McAfee ウイルス対策スキャン エンジンによるゲートウェイでの**ウイルス対策**。
- **グレイメールの検出と安全な購読解約。**Cisco E メール セキュリティ アプライアンスでは、以下を行うことができます。
  - 統合グレイメール エンジンを使用してグレイメールを識別し、適切なポリシー制御を適用します。
  - エンド ユーザがクラウドベースの購読解約サービスを使用して不要なグレイメールを購読解約できる安全で簡単なメカニズムが提供されます。
- **Outbreak Filters™。**これは、新しいアップデートが適用されるまで危険なメッセージを隔離し、新しいメッセージ脅威に対する脆弱性を削減する、新しいウイルス、詐欺、およびフィッシングの拡散に対するシスコの独自保護機能です。
- **ポリシー、ウイルス、およびアウトブレイク隔離。**管理者による評価のために、疑わしいメッセージを保存する安全な場所が提供されます。
- **スパム隔離。**隔離されたスパムおよび疑わしいスパムへのエンド ユーザ アクセスが提供されます。

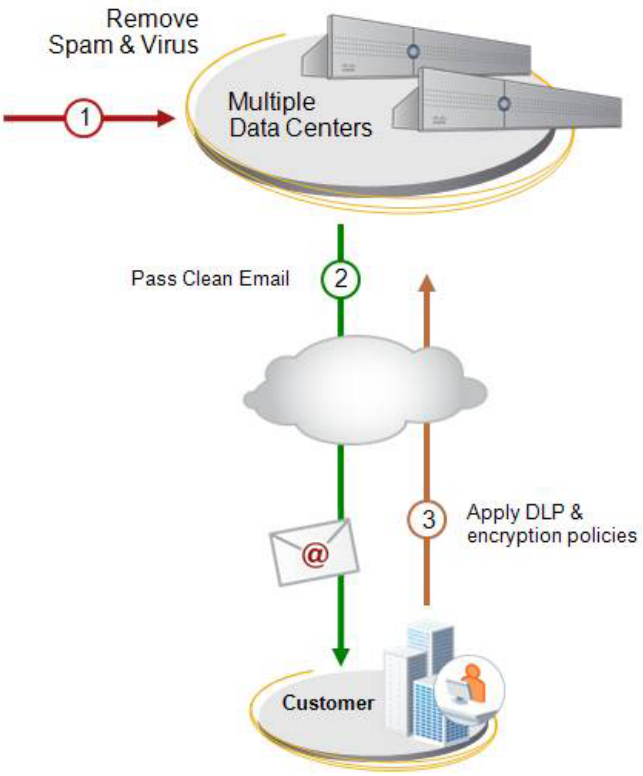
- **電子メール認証。**このアプライアンスは、発信メールに対する DomainKeys および DomainKeys Identified Mail（DKIM）の署名の他に、着信メールに対する Sender Policy Framework（SPF）、Sender ID Framework（SIDF）、DKIM の検証など、さまざまな形式の電子メール認証をサポートします。
- **ファイル レピュテーション フィルタリングとファイル分析。**高度なマルウェア防御は、次の情報に基づいて着信メッセージおよび発信メッセージに含まれる新たな標的型ファイルベースの脅威を特定します。
  - ファイル レピュテーション
  - ファイル分析（レピュテーションが不明な一部のファイルのための機能）
  - 判定のアップデート
- **URL フィルタリング。**URL フィルタリングは、着信メッセージと発信メッセージ内の URL のレピュテーションとカテゴリを取得することによって、次のような新しい機能を有効にします。
- **S/MIME セキュリティ サービス。**Cisco E メール セキュリティ アプライアンスにより、組織は S/MIME を使用して安全に通信できます。このとき、どのエンド ユーザも自分の証明書を所持する必要はありません。組織は、個人ではなく組織を識別する証明書を使用して、ゲートウェイ レベルでメッセージの署名、暗号化、検証、および復号化を処理できます。
- **E メール暗号化。**HIPAA、GLBA、および同様の規制要求に対応するために発信メールを暗号化できます。これを行うには、Cisco E メール セキュリティ アプライアンスで暗号化ポリシーを設定し、ローカル キー サーバまたはホステッド キー サービスを使用してメッセージを暗号化します。
- **E メール セキュリティ マネージャ。**アプライアンス上ですべての E メール セキュリティ サービスおよびアプリケーションを管理するための、包括的な単一ダッシュボード。電子メール セキュリティ マネージャは、ユーザ グループに基づいて電子メール セキュリティを実施でき、インバウンドとアウトバウンドの独立したポリシーを使用して、IronPort レピュテーション フィルタ、アウトブレイク フィルタ、アンチスパム、アンチウイルス、および電子メール コンテンツ ポリシーを管理できます。
- **メッセージ トラッキング。**このアプライアンスには、Cisco E メール セキュリティ アプライアンスが処理するメッセージのステータスを簡単に検索できる、メッセージ トラッキング機能があります。
- **メール フロー モニタリング。**すべての着信メッセージおよび発信メッセージのメール フローを監視できます。企業のすべての E メール トラフィックが完全に視覚化されます。
- **アクセス制御。**送信者の IP アドレス、IP アドレス範囲、またはドメインに基づいた、インバウンドの送信者のアクセス制御。
- 広範な**メッセージ フィルタリング** テクノロジーを使用して、社内ポリシーを順守させ、企業のインフラストラクチャを出入りする特定のメッセージに作用させることができます。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、メッセージをドロップ、バウンス、アーカイブ、ブラインド カーボン コピー、または変更したり、通知を生成したりできます。
- **Transport Layer Security 上の安全な SMTP によるメッセージの暗号化。**企業インフラストラクチャと他の信頼されているホストの間で送受信されるメッセージが暗号化されます。

  統合された堅牢なレポート オプションにより、各地に導入されているインフラストラクチャからのトラフィック データが分析され、完全に統合されたセキュリティ レポートが提供されます。Cisco E メール セキュリティ アプライアンスの第 3 世代レポート技術により、世界で最も通信量が多いネットワークでも詳細に調査できます。詳細かつ正確な情報が明快かつ有益なレポートにまとめられます。このレポートは、どのレベルの組織にも適しています。

メッセージ トラッキングにより、組織は、ダウン メッセージの処理を追跡するために、ほぼリアルタイムでメッセージを視認できます。この機能により、メッセージの正確な場所を判断することで、ヘルプ デスク コールを迅速に解決できます。フレキシブルなトラッキング インターフェイスを使用してメッセージを見つけることができます。このとき、ログ ファイル全体を検索する必要はありません。トラッキングは、クラウド ベース アプライアンスとオンプレミス アプライアンスの両方が対象となります。

図 1-2 は、Cisco Hybrid Email Security の導入モデルを示しています。

図 1-2　　Cisco Hybrid Email Security の導入



Cisco Hybrid Email Security は、次のように動作します。

- E メール セキュリティ アプライアンスにより、クラスタ構成と呼ばれる他の E メール セキュリティ アプライアンスの間で構成情報が同期されます。
- クラウド E メール セキュリティ アプライアンスにより、着信メールが受け入れられ、処理されます。システムにより、処理されたメールがオンプレミス E メール セキュリティ アプライアンスに送信されます。このアプライアンスで、追加のコンテンツ フィルタリングが実行され、ポリシーによってメッセージがフィルタ処理されます。
- クラウドベースのセキュリティ管理アプライアンスにより、クラウド E メール セキュリティ アプライアンスとオンプレミス E メール セキュリティ アプライアンスの両方からレポート データとトラッキング データが収集されます。
- クラウドベースのセキュリティ管理アプライアンスは、クラウドベースの E メール セキュリティ アプライアンスからスパムを隔離する中央集中型の場所として機能します。
- ポリシーに基づいてフィルタ処理されたメールは、メッセージをフィルタ処理した Cisco セキュリティ管理アプライアンスに隔離されます。

- オンプレミス E メール セキュリティ アプライアンスにより、グループウェア サーバへのメールの送信、グループウェア サーバからの発信メールの処理が行われ、また高度なコンテンツ フィルタリングと E メールの暗号化が行われます。
- オンプレミス E メール セキュリティ アプライアンスにより、発信メールがインターネットに送信されます。

  マス マーケティング メーラーなど、クラウドベースのアプライアンスで、大量の発信メッセージをリレーできないようにすることを強くお勧めします。代わりに、トランザクション E メールのリレー トラフィックを制限できます。キャパシティ保証には、マーケティング通信や、プログラムまたはエンティティを生成する E メールは含まれません。

Cisco E メール セキュリティ サービスの管理

アプライアンスを使用して、クラウドベースの E メール セキュリティ サービスを直接管理および変更できます。

アプライアンスを使用して以下を実行できます。

- クラウドベースの E メール セキュリティ サービスに関する情報を表示および追跡する。
- レポートにアクセスする。
- クラウドベースのアプライアンスの設定にアクセスし、変更する。

サービスとサポート

（注）　Cisco クラウド E メール セキュリティ（CES）に関するサポートが必要な場合、Cisco TAC にお電話でご連絡ください。その際、契約番号をご用意ください。

Cisco TAC：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

従来の IronPort のサポート サイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマー サポートにアクセスすることもできます。手順については、ユーザ ガイドまたはオンライン ヘルプを参照してください。

クラウド環境の設定

E メールクラウドゲートウェイへのアクセス

Web インターフェイスおよびコマンド ライン インターフェイスへのアクセス

すべての E メールクラウドゲートウェイの Web インターフェイスには、E メールゲートウェイから直接アクセスするか、またはウェルカムレターに記載されている URL を使用してアクセスすることができます。

ウェルカムレターに記載されている詳細を使用して、コマンド ライン インターフェイス（CLI）からすべての E メールクラウドゲートウェイにアクセスできます。

Cisco Secure Email Cloud Gateway の設定

E メール認証の設定

E メールを認証するために、Sender Policy Framework（SPF）または DomainKeys Identified Mail（DKIM）を使用できます。

DKIM では、送信側が使用した署名キーに基づいて E メールの信頼性が検証されます。SPF では、DNS TXT レコードに基づいて E メールの信頼性が検証されます。SPF により、インターネットドメインの所有者は、特別な形式の DNS レコードを使用して、そのドメインに E メールを送信する権限のあるマシンを指定できます。

DKIM の設定

DKIM を設定する手順、およびコンテンツフィルタルールとメッセージフィルタルールを定義する手順については、『*User Guide for AsyncOS for Cisco Secure Email Gateway*』の次の章を参照してください。

- 電子メール認証
- 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

SPF の設定

シスコは、DNS TXT レコードの推奨 SPF エントリを提供していますが、E メールゲートウェイの受信者アクセステーブルなど、お客様が所有するドメインの DNS は管理していません。レコードの形式を以下に示します。

```
v=spf1 -exists:%{i}.spf.<unique_name>.iphmx.com -all
```

サービスとサポート (1-8 ページ) を参照してください。

DNS に SPF レコードを追加した後、SPF 検証を設定すること、およびコンテンツ フィルタ ルールとメッセージ フィルタ ルールを定義することができます。『*User Guide for AsyncOS for Cisco Secure Email Gateway*』の次の章を参照してください。

- 電子メール認証
- 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

発信 E メールのルーティング

E メールクラウドゲートウェイからの発信メールのために、クラウドベースサーバでメールがリレーされるように E メールゲートウェイを設定する必要があります。『*User Guide for AsyncOS for Cisco Secure Email Gateway*』の「Configuring Routing and Delivery Features」の章を参照してください。

ログのアーカイブ

シスコでは、E メールクラウドゲートウェイのログは保存していません。履歴ログはアーカイブされず、ログのローテーションによって上書きされる場合があります。ログを保持する場合、E メールクラウドゲートウェイでログのサブスクリプションを設定して、ログの取得方法として SCP プッシュ（またはリモートサーバの SCP）を使用します。この方法では、リモート コンピュータ上の SCP サーバに定期的にログ ファイルをプッシュします。

この方法には、SSH1 または SSH2 プロトコルを使用するリモート コンピュータ上の SSH SCP サーバが必要です。サブスクリプションには、ユーザ名、SSH キー、およびリモート コンピュータ上の宛先ディレクトリが必要です。ログ ファイルは、設定したロールオーバー スケジュールに基づいて転送されます。

ファイアウォールによりネットワークへの SSH アクセスがブロックされる場合、Cisco クラウド E メール セキュリティ データセンターからのインバウンド SSH 接続を明示的に許可することをお勧めします。

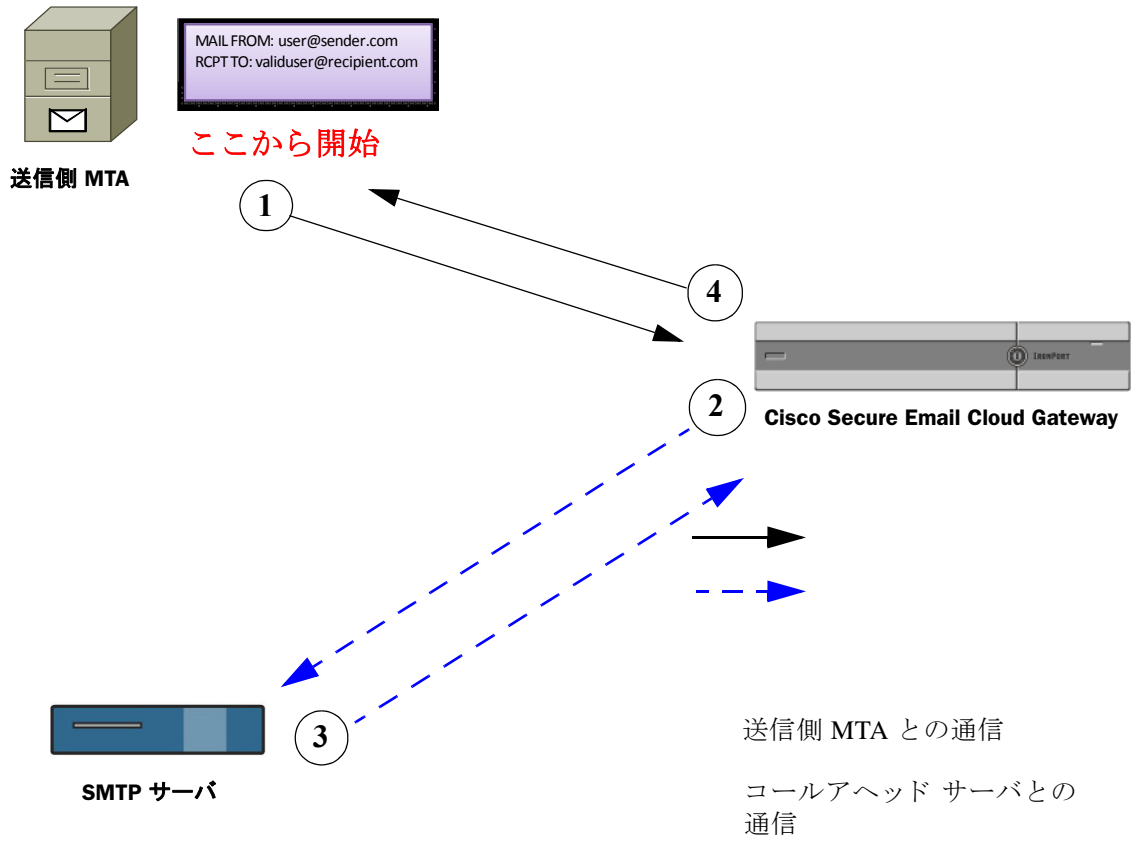
『*User Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

サーバの設定

SMTP コール アヘッド検証の使用

Cisco Secure Email Cloud では、受信者検証のために SMTP コールアヘッド検証が使用されます。これは、管理者のオーバーヘッドを最小限に抑えながら、受信者を検証するシームレスでエレガントな方法です。この方法は、既存のソリューションとしてすでに設置されているファイアウォールの設定にはほとんど影響しないか、まったく影響しません。

図 2-1　SMTP コールアヘッド サーバ通信のワークフロー



SMTP コール アヘッドは、次のように動作します。

ステップ 1　送信元の E メールシステム（MTA）により、E メールクラウドゲートウェイとの接続が開かれます。最初の SMTP プロトコル通信の一部として、送信元 E メール システムにより RCPT TO 情報が渡されます。

ステップ 2　Cisco Secure Email クラウド インフラストラクチャにより、着信接続は開かれたままとなり、SMTP サーバへのコールが開始されます。この通信の一部として、E メールクラウドゲートウェイにより、SMTP サーバ（たとえば、Microsoft Exchange）に RCPT TO 情報が渡されます。

ステップ 3　RCPT TO: のユーザが有効か無効かに基づいて、SMTP サーバは 200 番台のステータスまたは 500 番台のステータスを送信します。

MTA またはグループウェア サーバで SMTP コール アヘッドを適切に動作させるには、クラウド ベース サーバからの接続をブロックする可能性がある送信元の検証機能（たとえば、SPF チェック、TLS チェック、DHAP スキームなど）を、指定の IP アドレスについて無効にしておく必要があります。

ステップ 4　E メールクラウドゲートウェイは 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。

SMTP コールアヘッド検証の実行方法の詳細については、『*User Guide for AsyncOS for Cisco Secure Email Gateway*』を参照してください。

Cisco エンドユーザスパム隔離の使用

（注） この章は、エンドユーザ スパム隔離を有効にした場合にのみ使用してください。

Cisco エンドユーザ スパム隔離について

スパムには、以下が含まれます（ただし、これら以外にもあります）。

- 広告メール、ねずみ講、チェーン レター、および宣伝
- 不審な件名のメール、中傷的なメール、または脅迫的なメール
- 虚偽的または詐欺的なヘッダー、件名、送信者、返信先アドレス、ルーティング パス、または伝送パスが含まれるメール
- 許可なしで第三者のドメイン名を使用しているメール

スパム隔離では、適切なポリシーとテクノロジーを実装することで、スパムの影響が最小限になります。スパムとして認識されたメール メッセージは隔離されます。メッセージがスパムではない場合、それらのメッセージを隔離場所から移動し、送信者をセーフリストに追加できます。また、メッセージが実際にスパムであった場合には、アクションは不要です。隔離されたメールの容量は、メールボックスの制限容量として計算されません。また隔離されたメールは、特定の日数が経過した後に自動的に削除されます。

（注） メールが削除される前に隔離によって何日間メールが保持されるか管理者に確認してください。

スパム隔離にアクセスするために、特別なハードウェア、ソフトウェア、またはセキュリティ認証は必要ありません。ユーザは、スパムとして認識されたメッセージをリストするスパム隔離通知を定期的に受け取ります。

セーフリストとブロックリスト

どのメール メッセージをスパムとして処理するかより適切に制御するために、セーフリストとブロックリストを作成できます。セーフリストにより、特定のユーザまたはドメインがスパムとして処理されないようにすることができます。一方ブロックリストでは、特定のユーザまたはドメインが常にスパムとして処理されるようにすることができます。

（注）　セーフリストとブロックリストに追加できるエントリの最大数については、管理者に確認してください。

セーフリストとブロックリストへのアクセス（3-3 ページ）を参照してください。

スパム隔離内のメッセージの処理

スパム隔離の通知では、メッセージの詳細が示されるため、メッセージが実際にスパムであるかどうか判別できます。スパム隔離の通知から直接メッセージを処理すること、または通知の本文にあるリンクをクリックして、スパム隔離にアクセスすることができます。

メッセージがスパムである場合、何もする必要ありません。メッセージは、隔離場所で特定の日数保持された後、削除されます（日数については、管理者に確認してください）。

スパム隔離から受信トレイへのメッセージのリリース

メッセージがスパムではない場合、隔離場所から受信トレイにメッセージをリリースします。また、この送信者からのメッセージが今後隔離されないようにするために、この送信者をセーフリストに追加できます。

手順

ステップ 1　スパム隔離の通知で、リリースするメッセージの横にある [スパムではない（Not Spam）] をクリックします。

ステップ 2　表示される確認メッセージで、[送信者をセーフリストへ追加（Add Sender to Safelist）] をクリックします。

メッセージをリリースした一方で、送信者をセーフリストに追加していない場合、この送信者からの今後のメッセージは隔離される場合があります。

メッセージの詳細の表示

メッセージがスパムであるかどうか判別するために、メッセージの送信者と件名以外の詳細が必要な場合、メッセージに対してアクションを実行する前にメッセージ全体を表示できます。

手順

ステップ 1　スパム隔離の通知で、メッセージの [件名（Subject）] リンクをクリックすると、[メッセージの詳細（Message Details）] ページが表示されます。

（注）　メッセージに対してすでにアクションを実行した場合、[メッセージが見つかりません（Message Not Found）] ページが表示されます。

ステップ 2　ドロップダウン リストから、実行するアクションを選択します。オプションは、[リリース（Release）]、[リリースしてセーフリストに追加（Release and Add to Safelist）]、および [削除（Delete）] です。

アクションを実行しない場合、メッセージは、特定の日数が経過した後に、隔離場所から削除されます（日数については、管理者に確認してください）。

ステップ 3　[送信（Submit）] をクリックします。

ステップ 4　確認メッセージで、目的のアクションを確認します。

一度に複数のメッセージに対してアクションを実行

手順

ステップ 1　スパム隔離の通知で、いずれかのリンクをクリックしてスパム隔離にアクセスします。

ステップ 2　アクションを実行する対象の各メッセージの横にあるチェック ボックスを選択します。

ステップ 3　ドロップダウン リストから、実行するアクションを選択し、[実行（Submit）] をクリックします。

アクションを実行しない場合、メッセージは、特定の日数が経過した後に、隔離場所から削除されます（日数については、管理者に確認してください）。

ステップ 4　確認メッセージで、目的のアクションを確認します。

セーフリストとブロックリストへのアクセス

各エントリは、次の形式でセーフリストとブロックリストに追加できます。

- `user@domain.com`
- `server.domain.com`
- `domain.com`

送信者またはドメインを、セーフリストとブロックリストの両方に同時に追加することはできません。ただし、ドメインをセーフリストに追加し、そのドメインに所属するユーザの E メールアドレスをブロックリストに追加した場合、E メールゲートウェイは両方のルールを適用します（逆の場合も同様です）。たとえば、`example.com` をセーフリストに追加し、`george@example.com` をブロックリストに追加すると、E メールゲートウェイは、`example.com` からのすべてのメールをスパムかどうかスキャンせずに配信しますが、`george@example.com` からのメールはスパムとして処理します。

`.domain.com` などの構文を使用して、サブドメインの範囲を許可またはブロックすることはできません。ただし、`server.domain.com` などの構文を使用して特定のドメインを明示的にブロックすることは可能です。

セーフリストまたはブロックリストへのエントリの追加

手順

ステップ 1　スパム隔離の通知で、いずれかのリンクをクリックしてスパム隔離にアクセスします。

ステップ 2　[オプション（Options）] ドロップダウン リストから、[セーフリスト（Safelist）] または [ブロックリスト（Blocklist）] を選択します。

ステップ 3　E メール アドレスまたはドメインを入力し、[リストに追加（Add to List）] をクリックします。

（注）　セーフリスト エントリと異なり、ブロックリスト エントリは、エンドユーザのスパム隔離内の [オプション（Options）] メニューからのみ追加できます。

隔離内のメッセージの検索

手順

ステップ 1　スパム隔離の通知で、いずれかのリンクをクリックしてスパム隔離にアクセスします。

ステップ 2　[メッセージの検索（Search Messages）] フィールドに、検索する用語を入力し、[検索（Search）] をクリックします。