Cisco Secure Email Gateway（クラウドおよびオンプレミス）、Cisco Secure Email and Web Manager

2024 年 5 月

目次

Cisco Secure Email

あらゆる規模のお客様が同じ困難な課題に直面しています。電子メールは最も重要なビジネス コミュニケーション ツールであると同時に、セキュリティ侵害の主要な攻撃ベクトルでもあります。Cisco Secure Email Gateway を使用すると、ユーザーは多層的なアプローチによって安全な通信を確立し、ビジネスメール詐欺（BEC）、ランサムウェア、高度なマルウェア、フィッシング、スパム、およびデータ損失に対する組織の対策を支援できます。

製品の概要

Cisco Secure Email Gateway は高度な脅威からの保護機能を備えており、脅威を迅速に検出、ブロック、および修復します。また、データ損失を防ぎ、送信中の重要な情報をエンドツーエンドの暗号化で保護します。

Cisco Secure Email Gateway を使用しているお客様は次のことができます。

- シスコの脅威調査チーム Talos™ の優れた脅威インテリジェンスを活用して、より多くの脅威を検出してブロックします。
- Cisco Secure Email Malware Defense を使用して、添付ファイルに潜み、初期段階での検出を回避するランサムウェアに対処します。
- 悪意のあるリンクを含む電子メールをドロップするか、URL をリアルタイムに分析して新たに感染したサイトへのアクセスをブロックして、フィッシングや BEC を阻止します。
- データ損失防止（DLP）機能と使いやすい電子メール暗号化により、送信メールの機密コンテンツをすべて 1 つのソリューションで保護します。
- Cisco Secure Email Threat Defense と統合して、高度な脅威検出と保護を実現します。

Cisco Secure Email and Web Manager を使用しているお客様は次のことができます。

- 一元化されたレポート、メッセージトラッキング、および検疫にアクセスします。
- 統合ダッシュボードを使用して管理作業を合理化します。

クラウド、オンプレミス、またはハイブリッド環境における導入の柔軟性を最大限に活かしたり、段階的にクラウドに移行したりできます。

Cisco XDR は、セキュリティ運用を簡素化し、対応を迅速化し、セキュリティ オペレーション センター（SOC）チームに AI 主導型のプロアクティブな脅威検出および対応能力を提供します。また、セキュリティアナリストが直面する課題に対処するように設計されており、複数のセキュリティツールからデータを取得し、機械学習と分析を適用して相関検出を実現するクラウドネイティブで拡張可能なソリューションを提供します。詳細については、cisco.com/go/xdr を参照してください。

Cisco Secure Email Gateway（クラウドおよびオンプレミス）

今日の電子メールセキュリティの脅威には、ランサムウェア、高度なマルウェア、BEC、フィッシング、スパムなどがあります。Cisco Secure Email Gateway は複数のレイヤを活用して、最大限の包括的な電子メールセキュリティを提供します。また、防御を強化するための予防策と対応策が組み込まれています。表 1 では、シスコの E メール セキュリティ ソリューションの主な機能を示します。

表 1. 主要な機能

機能	利点
グローバル脅威インテリジェンス	世界最大級の脅威検知ネットワークである Talos をベースとした、迅速かつ包括的な電子メール保護を受けられます。Talos は、グローバルなトラフィックアクティビティを 24 時間体制で表示し、問題点の分析、新しい脅威の検出、トラフィックトレンドのモニターを行います。Talos は、ルールを継続的に生成し、そのアップデートを E メール セキュリティ アプライアンスに適用することで、ゼロアワー攻撃を防止します。こうしたアップデートは 3 ~ 5 分おきに実行され、業界トップクラスの脅威防御を実現します。詳細については、次を参照してください。
レピュテーションフィルタリング	Talos のレピュテーション データベースに基づいたレピュテーション フィルタリングを使用して、不要な電子メールをブロックします。レピュテーションサービスは、IP アドレス、ドメイン、および Web サイトに対してキュレートされます。レピュテーションの悪い既知の内容は自動的にブロックされます。レピュテーション フィルタリングにより、大部分のスパムはネットワークに侵入する前に阻止されるため、はるかに小さいペイロードを分析することで、ソリューションを拡張できます。
スパム保護	スパムは、高度なソリューションを要する複雑な問題です。Cisco Secure Email なら簡単に保護できます。Cisco Secure Email Gateway は、多層型スキャンアーキテクチャを使用して不要な電子メールをブロックします。また、99% を超える最高水準のスパム検出率 （誤検出率は 100 万分の 1 未満）を実現しています。 Cisco Secure Email Gateway のスパム対策機能は、メッセージのコンテンツ、メッセージの構成、メッセージの送信者、およびメッセージのリンクの転送先など、メッセージのコンテキスト全体を検査します。Cisco Secure Email Gateway は、これらの要素を組み合わせることで、業界トップクラスの精度で幅広い種類の脅威を防ぎます。
ウイルス防御	Cisco Secure Email Gateway は、ゲートウェイで統合される高性能のウイルス スキャン ソリューションを提供することで、マルチベンダーによる多層型のウイルスフィルタリングを実現します。
Malware Defense（旧 AMP および Threat Grid)	Cisco Secure Email Gateway には、悪意のある攻撃者によって送信される悪意のある電子メールの添付ファイルから保護する Malware Defense が付属しています。ファイルは、既知の悪意のあるファイルを阻止するために、最初にファイルレピュテーション（SHA256 ルックアップ）と照合してチェックされます。新しいファイルや不審なファイルの場合、ファイル分析（サンドボックス分析）がゲートウェイで開始され、ファイルの動作に関する詳細な分析が数分以内に提供されます。新しい技術が出現し、新しい脅威インテリジェンスが収集された場合、ファイル レトロスペクション アラートで、IT 管理者に処理の変更を通知できます。メールボックスの自動修復（Microsoft 365 および Microsoft Exchange オンプレミス ）を使用すると、ゲートウェイがユーザーのメールボックスから感染した電子メールを自動的に修復し、ユーザーが悪意のある添付ファイルにアクセスするのを防ぎます。 Cisco Secure Email Gateway は、パスワードで保護されたファイル分析を使用することで、電子メールの本文からパスワードを抽出するか、管理者が提供するテスト用のパスワードリストを使用して、パスワードで保護されたファイルを分析できます。 お客様は追加のライセンスを購入すると、Cisco Secure Endpoint プライベートクラウドを使用して、Malware Analytics システムを完全にオンプレミスに展開できます。その結果、Cisco Secure Malware Analytics アプライアンス（Threat Grid）とともに、Malware Analytics サービス全体を完全にオンプレミスで利用できます。詳細については、次を参照してください。

機能	利点
グレイメールの検出と安全な登録解除	グレイメールには、マーケティング、ソーシャルネットワーキング、およびバルクメッセージがあります。グレイメール検出機能は、組織に届くグレイメールを正確に分類および監視します。これにより、管理者はカテゴリに応じて適切なアクションを取ることができます。多くの場合、グレイメールには登録解除リンクが含まれています。エンドユーザーはこのリンクを使用して、当該メールの配信停止を希望することを送信者に伝えます。このような登録解除メカニズムの偽装は一般的なフィッシングの手口なので、ユーザーは登録解除リンクをクリックする際は注意する必要があります。 安全な登録解除ソリューションは、以下の機能を提供します。 • 登録解除リンクを装った悪意のある脅威からのエンドユーザー保護。 • すべてのサブスクリプションを管理するための統一されたインターフェイス。 登録解除リンクを含む 電子メールに対する電子メール管理者とエンドユーザーの可視性の向上。
URL フィルタリングと制御	URL フィルタリング、電子メールと添付ファイル内の URL のスキャンによって、悪意のある URL からユーザーを保護します。URL のレピュテーションまたはカテゴリに基づいて、適切なポリシーがメッセージに適用されます。Cisco Secure Email Gateway は、短縮 URL とオープンリダイレクト URL の分析もサポートしています。URL の書き換えにより、最初のスキャン中に無害だった URL のクリック時間保護を提供します。ただし、URL レトロスペクションアラートを使用すると、Cisco Secure Email Gateway はメールボックスの自動修復（Microsoft 365 および Microsoft Exchange オンプレミス）を利用して、エンドユーザーのメールボックスからの電子メールを自動的に修復できます。
外部脅威フィード	Cisco Secure Email Gateway は、Cisco Talos に加えて、STIX over TAXII プロトコルを使用して、外部ソースから追加の脅威インテリジェンスを取得できます。
ファイル処理とマクロの検出	Cisco Secure Email Gateway は、不要な電子メールの添付ファイルの種類や内容からお客様を保護するのに役立ちます。ファイルメタデータ分析を使用することで、ファイルタイプと埋め込みマクロスクリプト（Microsoft、Adobe、または OLE タイプのマクロ）をゲートウェイで正確に認識できます。 Safe Print アクションを使用すると、Cisco Secure Email Gateway は、元のコンテンツをスクリーンショットとして含む PDF に添付ファイルを変換できます。
アウトブレイクフィルタ	アウトブレイクフィルタは、多くがフィッシングや詐欺キャンペーンである、新たなウイルスの脅威を防ぎます。Talos は、Cisco Secure Email Gateway のアウトブレイクルールセットを管理して、ゼロデイフィッシングとウイルスのリードタイムを取得するのに役立ちます。 アウトブレイク フィルタ機能を使用して、疑わしいメッセージ内の URL を書き換えることもできます。新しい URL をクリックすると、受信者は Cisco Security プロキシを介してリダイレクトされ、クリック時に悪意のあるサイトの場合はブロックページが表示され、不審なサイトの場合は Web サイトのスクリーンショットが取得されます。ユーザーは、安全だと判断した場合に Web ページへのリダイレクトを選択できます。
Web インタラクショントラッキング	Web インタラクション トラッキングは完全に統合されたソリューションであり、Cisco Secure Email Gateway によって書き換えられた URL をクリックするエンドユーザーを IT 管理者が追跡できます。レポートには次の情報が表示されます。 • 悪意のある URL をクリックした上位ユーザー • エンドユーザーがクリックした悪意のある上位 URL 日時、書き換え理由、および URL で実行されたアクション。

機能	利点
送信メールの機密コンテンツのデータセキュリティ	Cisco Secure Email は、効果的なデータ損失防止と電子メールのエンドツーエンドの暗号化を提供します。 **DLP** Cisco Secure Email の DLP により、発信メッセージを保護します。世界各国の業界や政府の規制に準拠し、機密データがネットワークから流出するのを防ぎます。政府、民間部門、および企業固有の規制を網羅した約 200 の事前構築ポリシーを含む豊富なテンプレートライブラリから選択できます。定義済みの DLP ポリシーが Cisco Secure Email Gateway に付属しているため、コンテンツ認識型のアウトバウンド電子メールポリシーを簡単に適用できます。修復の選択肢には、暗号化、フッターや免責事項の追加、ブラインドカーボンコピー（BCC）の追加、通知、検疫などがあります。複雑なポリシーを必要とする企業には、カスタマイズに必要な構築要素が用意されており、ポリシーを素早く簡単に作成できます。 **暗号化** 送信者は、メッセージの送信後もコンテンツを制御できます。送信者は電子メールの暗号化を使用してメッセージをいつでもロックできるため、受信者アドレスの誤入力、内容の間違い、時間的制約のある電子メールに関する不安がなくなります。受信者がメッセージを開封すると、暗号化されたメッセージの送信者は開封確認メッセージを受け取ります。安全性の高い返信メッセージや転送メッセージも自動的に暗号化され、エンドツーエンドのプライバシーと制御が維持されます。追加のインフラストラクチャを導入する必要はありません。セキュリティ強化のため、メッセージコンテンツはゲートウェイから受信者に直接送信され、暗号キーだけがクラウドに保存されます。 暗号化は強制的に適用するものとしてではなく、使いやすいサービスとして提供され、送信者が全面的に制御できます。
Threat Defense Connector	高度なレベルの電子メール攻撃の検出を改善するために、Threat Defense Connector を使用して、Cisco Secure Email Gateway と Cisco Secure Email Threat Defense を統合できます。Cisco Secure Email Threat Defense は、AI/ML ベースのスキャンエンジンを使用して、ゲートウェイをバイパスする可能性がある悪意のある電子メールを検出します。

Cisco Secure Email and Web Manager

Cisco Secure Email and Web Manager を使用すると、更新と設定をアプライアンスごとにではなく、一元的に管理できます。メッセージトラッキングは、複数の Cisco Secure Email Gateway からのデータ（送信者、受信者、メッセージの件名、およびその他のパラメータで分類されたデータを含む）を集約します。スパムやウイルスの判定などのスキャン結果も、ポリシー違反と同様に表示されます。また、

- メッセージの性質、URL、およびその他の電子メール属性を追跡してレポートします。
- 電子メールセキュリティの隔離を単一のリポジトリに統合します。
- スパム対策、ウイルス対策、アウトブレイクフィルタ、ポリシー隔離などが含まれています。
- 複数のアプライアンスの管理を一元化することで、管理者は組織全体に一貫したアクセプタブル ユース ポリシーを適用できます。

（注）Cisco Secure Email and Web Manager の導入は必須ではありませんが、管理がより簡単、迅速、かつ効率的になります。

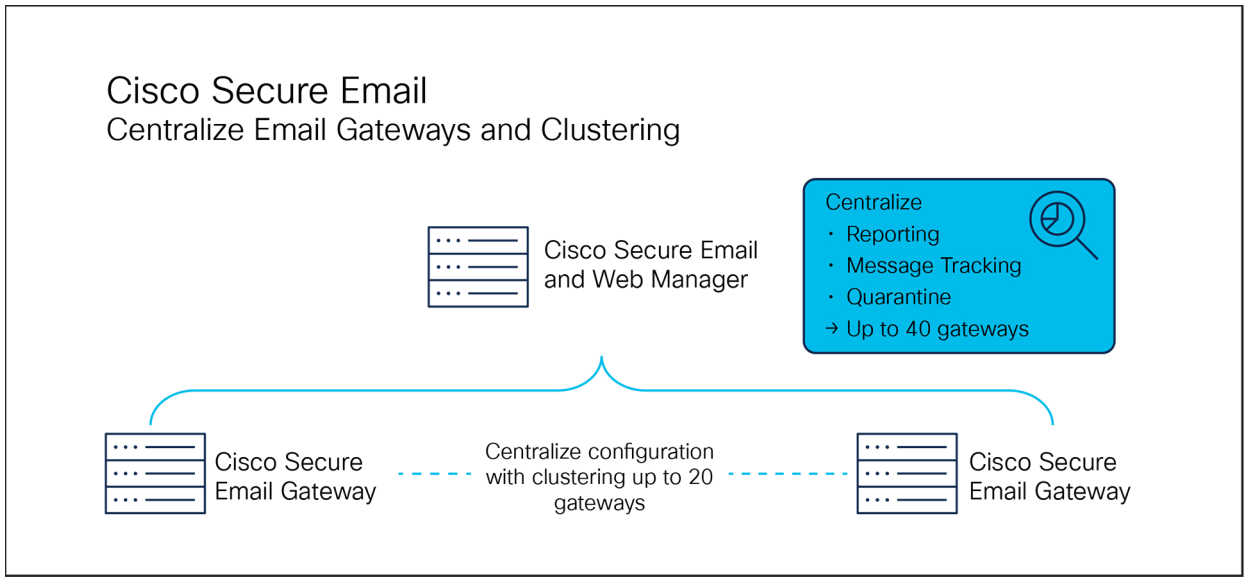


表 2. 主要な機能

機能	利点
一元化されたレポート	Cisco Secure Email and Web Manager は、複数の Cisco Secure Email Gateway からのレポートを完全に統合して集約することで、管理を簡素化します。
メッセージトラッキング	データ（送信者、受信者、メッセージの件名、およびその他のパラメータで分類されたデータを含む）は、複数の Cisco Secure Email Gateway から集約されます。スキャン結果には、各セキュリティチェックの詳細なスキャン結果、およびポリシーと設定に従って実行されたアクションが表示されます。
スパム隔離	スパムメッセージは、使いやすいセルフサービスであるシスコのスパム検疫ソリューションを使用して一元的に保存できます。複数の Cisco Secure Email Gateway を使用している大企業は、スパムトラフィックを 1 つの場所にオフロードして追跡を容易にし、従業員用の単一のアクセスポイントを提供できます。
Policy 隔離	不審なメッセージやポリシー違反メッセージは、管理ビューと管理のために一元的に保存できます。メッセージはダッシュボードから安全に確認でき、管理者の決定に従ってアクションを実行できます。複数の Cisco Secure Email Gateway で、ポリシーで隔離された電子メールを管理者アクセス用の単一のポイントにオフロードできます。

Cisco Secure Email のソフトウェアライセンス

E メール セキュリティ ソフトウェア バンドルには、Essentials、Advantage、および Premier の 3 種類があります。また、アドオン スタンドアロン オプションも用意されています（表 3 を参照）。あとは、サポートが必要なメールボックス数に適したライセンスを購入するだけです。

ライセンスには、クラウド、オンプレミス、ハイブリッドの 3 つの異なる展開オプションがあります。展開オプションごとに、それぞれのプラットフォームでソリューションを実行する権限が付与されます。

- クラウド：シスコホステッド
- オンプレミス：仮想マシン
- ハイブリッド：シスコホステッドおよび仮想マシン。

ライセンスバンドルとアドオンの比較については、こちらをクリックしてください。

期間および数量ベースのサブスクリプション ライセンス

ライセンスは、期間ベースのサブスクリプション（1 年、3 年、5 年）です。

Cisco Secure Email のポートフォリオでは、メールボックス数に基づき段階的価格を設定しています。お客様の導入に適した導入の決定は、販売代理店およびパートナーの代理店がお手伝いします。

シスコパートナーの場合、詳細については、発注ガイド を参照してください。

各ソフトウェア製品の主要なコンポーネントを表 3 に示します。

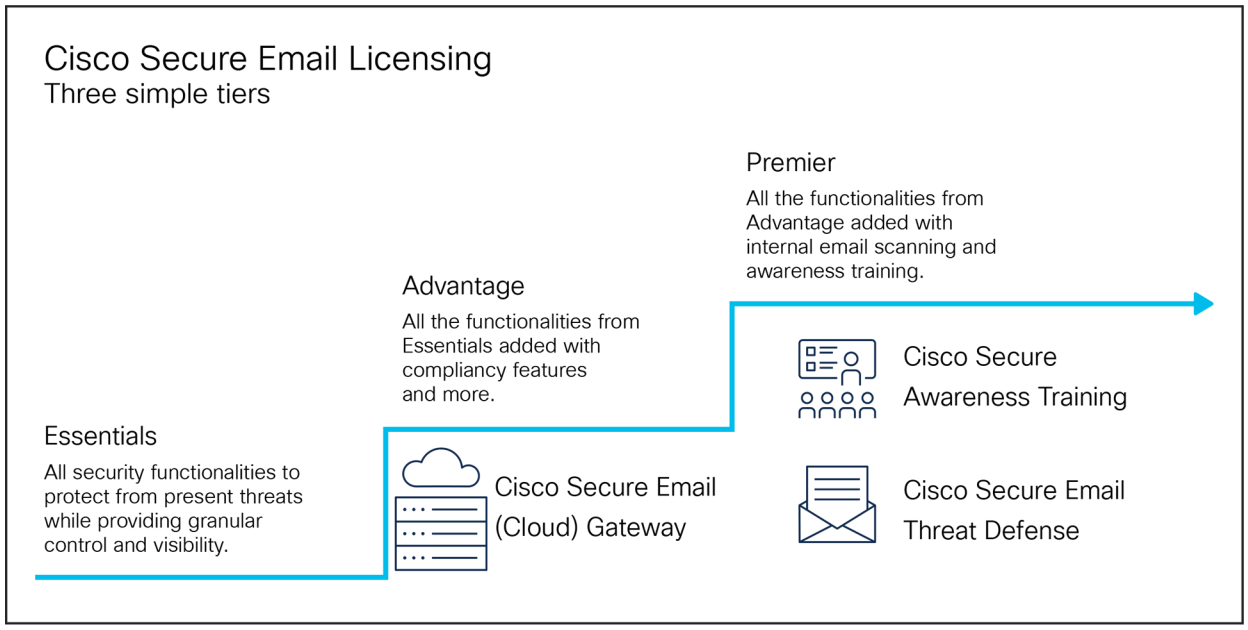


表 3. ソフトウェアのコンポーネント

バンドル	説明
Essentials	Cisco Secure Email Essentials バンドルは、電子メールベースの脅威に対する保護を提供します。また、スパム対策、Sophos ウイルス対策、Malware Defense、グレイメール検出、およびアウトブレイクフィルタが含まれています。Malware Defense には、Malware Analytics ソリューション（旧 Threat Grid）を使用したサンドボックス分析が含まれており、1 日にサンドボックス化されるファイルの数には制限があります。
Advantage	Cisco Secure Email Advantage バンドルには、Essentials のすべての機能に加えて、データ損失防止、エンベロープ暗号化、および安全な登録解除機能が含まれています。このバンドルの Malware Analytics には、ファイル送信数の制限はありません（無制限）。
Premier	Cisco Secure Email Premier バンドルは、次の 3 製品を組み合わせたものです。 • Cisco Secure Email Gateway Advantage バンドル • Cisco Secure Email Threat Defense • Cisco Secure Awareness トレーニング

アドオン	説明
セキュリティ管理アプライアンス（SMA）	Cisco Secure Email Manager 機能を使用すると、管理者は、複数の電子メールゲートウェイにまたがるメッセージと検疫を同時に一元的にレポートおよび検索できます。 このアドオンは、オンプレミス ゲートウェイ バンドルでのみ使用できます。クラウド ゲートウェイ バンドルの場合、Cisco Secure Cloud Email Manager は常に含まれています。
イメージアナライザ	送受信メール内の不正なコンテンツを検出し、問題となるユーザーの特定、監視、指導を可能にします。
グレイメールの安全な登録解除	グレイメールに安全な登録解除オプションをタグ付けできるようになりました。このタグは、エンドユーザーに代わって登録解除アクションを安全に管理します。また、各種グレイメール登録解除の要求をモニターします。要求はすべて、ポリシーレベルで管理できます。
インテリジェントマルチスキャン	インテリジェント マルチスキャン（IMS）は、高性能なマルチレイヤ アンチスパム ソリューションです。Cisco Anti-Spam をはじめとするアンチスパムエンジンを組み合わせることによって、スパム検出率が向上します。
McAfee ウイルス対策	McAfee ウイルス対策スキャンテクノロジーを提供します。
データ損失の防止	アウトバウンドトラフィック内の機密データの検出と、シビラティ（重大度）に基づいたさまざまなアクションを有効にします。
暗号化	Cisco Secure Email Encryption Service をアクティブにするためのライセンス。このサービスは、機密性の高い電子メールに関するエンドツーエンドの完全な暗号化オプションを提供します。
Cisco Secure Email Threat Defense	AI/ML ベースのエンジンを使用した検出を改善し、Microsoft 365 のお客様に対する、内部トラフィックの可視性と保護を強化します。

ソフトウェアライセンス契約

シスコ エンドユーザー ライセンス契約は、ソフトウェアライセンスを購入するたびに提供されます。

ソフトウェア サブスクリプションのサポート

すべての E メールセキュリティのライセンスには、ビジネスに不可欠なアプリケーションを利用可能にして、高度に安全かつピークパフォーマンスで運用するために必要なソフトウェア サブスクリプションのサポートが含まれています。このサポートによって、お客様は購入したソフトウェア サブスクリプションの全期間にわたって、以下に示すサービスを利用できます。

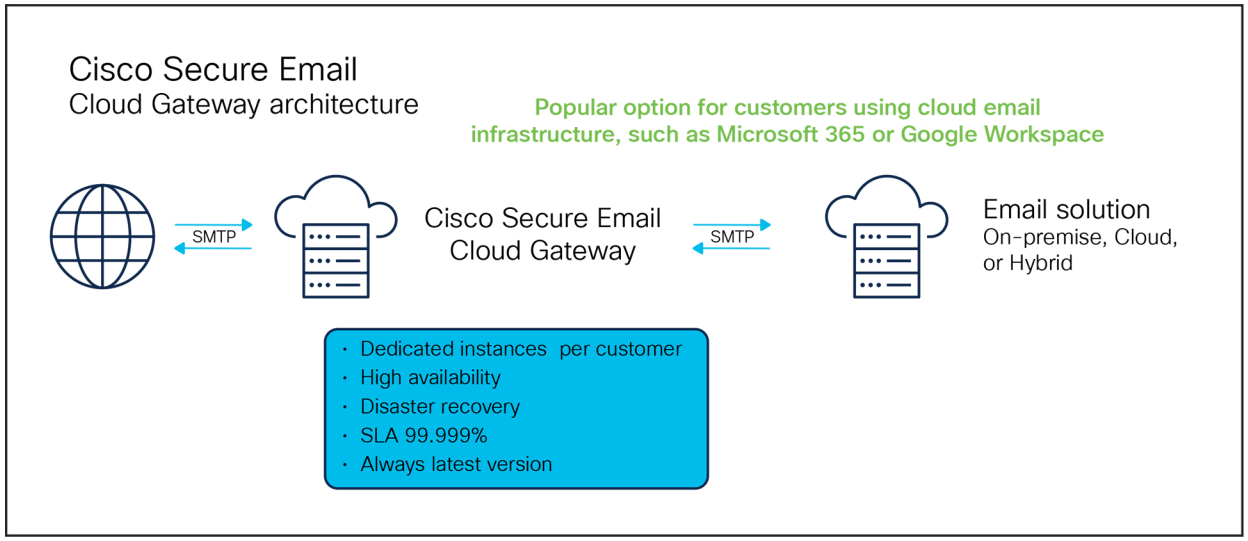
- ソフトウェア更新およびメジャーアップグレードを適用し、最新機能で最適なアプリケーションのパフォーマンスを得る
    - Cisco Technical Assistance Centerから迅速で専門的なサポートを得る
    - 社内の専門知識を構築して拡張し、ビジネスの俊敏性を高めるオンラインツールを利用する
    - 追加的な知識習得とトレーニングの機会を提供するコラボレーション性の高い学習

導入先

すべての Cisco Secure Email 導入オプションで、シンプルな実装アプローチが共有されています。システム セットアップ ウィザードは、複雑な環境にも対応しており、わずか数分でシステムを起動して保護し、より安全かつ迅速に導入できます。ライセンスは、デバイスベースではなく固有のユーザーベースなので、デバイス単位ではなく固有のユーザー単位で、インバウンドおよびアウトバウンドの電子メールゲートウェイ保護を追加料金なしで適用できます。

Cloud

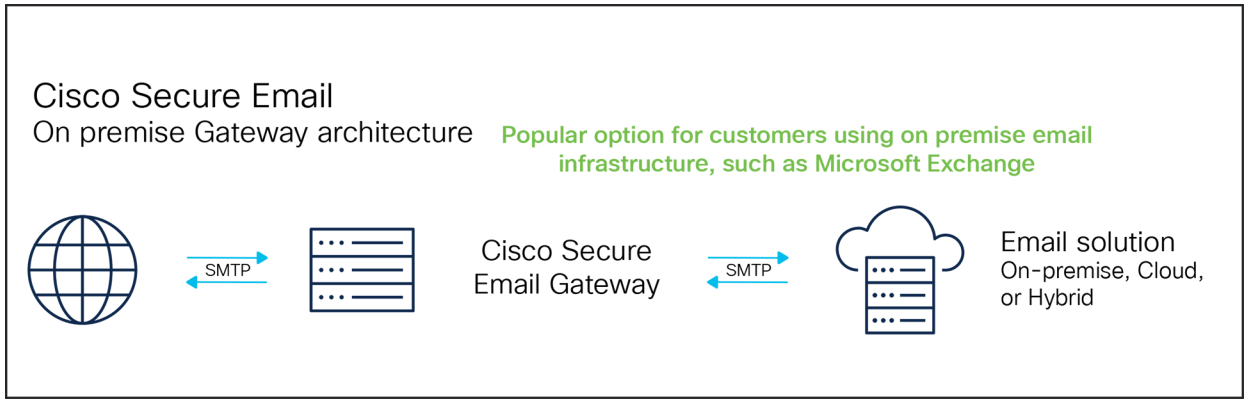
Cisco Secure Email Cloud Gateway は、E メールセキュリティの柔軟な導入モデルを提供します。共通管理できるほか、オンサイトで E メール セキュリティ インフラストラクチャを管理する必要がないので、コストを削減できます。耐障害性に優れた複数のシスコデータセンターに専用の E メールセキュリティを導入することで、最高レベルのサービス可用性とデータ保護が提供されます。お客様はクラウド インフラストラクチャへのアクセス（および可視性）を保持することができ、包括的なレポートやメッセージトラッキング機能によって、柔軟な管理が可能となります。このサービスでは、シンプルに使用できるように、ソフトウェア、コンピューティング能力、サポートがすべてバンドルされています。



オンプレミス：仮想マシン

Cisco Secure Email Gateway および Cisco Secure Email and Web Manager 仮想アプライアンスは、特に大規模な分散ネットワーク環境における E メールセキュリティの導入コストを大幅に削減します。このアプライアンスを利用すると、ネットワークマネージャは既存のネットワーク インフラストラクチャを使って必要なときに、必要な場所にインスタンスを作成できます。仮想アプライアンスは、VMware ESXi、Microsoft Hyper-V、Red Hat Virtualization、Amazon AWS、Microsoft Azure などのさまざまなハイパーバイザでサポートされています。Cisco Secure Email ソフトウェアコアバンドル（Essentials、 Advantage、および Premier）を購入すると、仮想アプライアンスの無制限ライセンスが付いてきます。

仮想アプライアンスでは、簡素化されたキャパシティプランニングでトラフィック増大にすばやく対応できます。



ハイブリッド

ハイブリッドソリューションは、最大限の柔軟性を提供します。ニーズに最適な導入オプションを組み合わせることができます。たとえば、クラウド内の Cisco Secure Email Gateway を利用して受信メッセージ内の脅威を防御しながら、機密メッセージのアウトバウンド制御をオンサイトに導入できます。また、インバウンド脅威防御をオンプレミスとクラウドに導入して、随時クラウドに移行することもできます。

Cisco Secure Email の仕様

Cisco Secure Email Cloud Gateway は、購入したユーザーライセンスに基づいて自動的にサイジングされます。クラウドゲートウェイの詳細とドキュメントについては、https://docs.ces.cisco.com/docs/ces-reference-docs を参照してください。

表 3、4、および 5 は、さまざまなハイパーバイザとクラウドプラットフォームの仮想展開の要件を表しています。正確なサイジングを行うには、選択したサイズについて、シスコのコンテンツセキュリティ担当者にご相談ください。

シスコパートナーの場合、初期サイジングの仕様について サイジングツール を参照してください。

仮想展開の詳細については、以下を参照してください。

- Cisco Secure Email Virtual Gateway および Cisco Secure Email and Web Manager 仮想アプライアンス設置ガイド [英語]
- Amazon Web Services の Amazon Elastic Compute Cloud への Cisco Secure Email Gateway、および Cisco Secure Email and Web Manager 仮想アプライアンスの展開 [英語]。
- Microsoft Azure クラウドプットフォームへの Cisco Secure Email Virtual Gateway および Cisco Secure Email and Web Manager Virtual の展開 [英語]。

表 4. VMware ESXi、Hyper V、および KVM の E メールセキュリティ仮想アプライアンスの要件。

製品	モデル	ディスク	メモリ	コア
Cisco Secure Email Virtual Gateway	C100v*	200 GB	8 GB	2
	C300v*	500 GB	16 GB	4
	C600v	500 GB	16 GB	8
Cisco Secure Email and Web Manager Virtual	M100v*	250 GB	6 ~ 8 GB	2
	M300v*	1TB	8 ~ 16 GB	4
	M600v	2TB	16 GB	8

*VMware ESXi でのみ使用できます。

表 5. Amazon AWS の E メールセキュリティ仮想アプライアンスの要件。

製品	モデル	ディスク	vRAM	vCPU	EC2 インスタンスタイプ
Cisco Secure Email Virtual Gateway	C600v	500 GB	30 GB	16	c4.4xlarge
Cisco Secure Email and Web Manager Virtual	M600v	2TB	15 GB	8	c4.2xlarge

表 6. Microsoft Azure の E メールセキュリティ仮想アプライアンスの要件。

製品	モデル	ディスク	メモリ	vCPU	Azure VMサイズ
Cisco Secure Email Virtual Gateway	C600v	500 GB	32 GB	8	Standard D8s v3
Cisco Secure Email and Web Manager Virtual	M600v	1TB	32 GB	8	Standard D8s v3

Cisco Secure Email Gateway の評価方法

- 仮想アプライアンスを試すには、このページ に移動し、記載されている手順に従ってください。
- Cisco Secure Email Cloud Gateway を試すには、シスコアカウントチームまたはパートナーに連絡して、45 日間の無料トライアルを開始してください。

シスコ セキュリティ サービス

- **アドバイザリサービス：**シスコのエキスパートが、リスク、コンプライアンス、セキュリティ、脅威管理を企業目標に合わせて調整します。

- **導入サービス：**世界中のあらゆる業界における数多くのお客様との取引で培ってきた専門知識とベストプラクティスを活用し、電子メールセキュリティをはじめとする高度なセキュリティソリューションに投資するメリットを短時間で実現して活かすお手伝いをします。
- **テクニカルサービス：**シスコは、ハードウェア、ソフトウェア、マルチベンダーソリューション、およびネットワーク環境向けのプロアクティブかつプリエンプティブなテクニカルサービスを提供しています。シスコのグローバルチームが IT 運用を推進して IT 業務を簡素化し、ビジネスの円滑な実施を支援します。

詳細情報

Cisco Secure Email の詳細については、https://www.cisco.com/go/emailsecurity を参照してください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-742868-06 06/24