AsyncOS 15.5.1 for Cisco Secure Email Gateway リリースノート（一般導入）

発行日：2024 年 4 月 30 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
Vault サービスのモニタリングとアラートの送信	電子メールゲートウェイは、初期化されているかどうかにかかわらず、Vault サービスをモニターし、そのステータスを追跡するようになりました。また、適切なアラートメッセージを送信し、ステータス情報を error_logs に記録します。 アラートログには、次のいずれかの方法でアクセスできます。 • Web インターフェイスで [システム管理（System Administration）] > [アラート（Alerts）] ページに移動し、[上位アラートの表示（View Top Alerts）] ボタンをクリックします。 • CLI で `displayalerts` コマンドを使用します。 何らかの問題によって Vault サービスの初期化に失敗した場合は、Vault サービスがダウンしていることを示すアラートメッセージを（メール、Web インターフェイス、および CLI で）受信します。Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。 **（注）** AsyncOS 15.5.1 へのアップグレード中にアップグレードが失敗した場合は、upgrade_logs で Vault サービスエラーを確認する必要があります。Vault サービスエラーがあった場合は、Vault サービスを復元するか、設定を保存せずにアップグレードプロセスを続行する必要があります。 アラートメッセージは次のようなシナリオで受信します。 • AsyncOS 15.5.1 へのアップグレード後に Vault サービスの初期化に失敗した場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。 • 電子メールゲートウェイのいずれかのサービスが初期化に失敗した Vault サービスを使用している場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。送信されるアラートメッセージは、暗号化ステータスによって異なります。暗号化ステータスは、`fipsconfig` > `encryptedconfig` サブコマンドを使用して確認できます。 Vault モニタリングメカニズム は、75 分ごとに Vault サービスをチェックします。ダウンしている場合は、Vault サービスが復元されるまでアラートメッセージを送信します。 成功した Vault 正常性チェックと初期化ログエントリの例については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Logging」の章にある「Successful Vault Health Check and Initialization」セクションを参照してください。

	Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。 **注意** 暗号化（CLI > `fipsconfig` > `encryptconfig`）が有効になっている場合は、データの損失を防ぐため、電子メールゲートウェイの設定のコピーを常に保存し、維持してください。 電子メールゲートウェイの設定を保存する方法の詳細については、電子メールゲートウェイの設定の保存（12 ページ）を参照してください。 Vault Recovery プロセスの実行方法については、Vault の問題を解決するための Vault Recovery プロセスの実行（13 ページ）を参照してください。
メッセージ終了 RFC 標準規格に違反しているメッセージの識別	電子メールゲートウェイは、メッセージ終了 RFC 標準規格（つまり <CRLF.CRLF>）に違反しているメッセージを識別してフィルタ処理し、脅威を検出するようになりました。 電子メールゲートウェイは、無効なメッセージ終了シーケンスを含むメッセージを受信すると、メッセージ終了 RFC 標準規格に準拠するメッセージを受信するまで、その接続内のすべてのメッセージ ID（MID）に **X-Ironport-Invalid-End-Of-Message** 拡張ヘッダー（X-Header）を追加します。 コンテンツフィルタでポリシーを設定し、これらのメッセージに対して必要なアクションを実行できます。 CR および LF 処理フィールドの設定の詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Listening for Connection Requests by Creation a Listener Using Web Interface」セクションを参照してください。
CLI による API サーバーの再起動	新しい CLI サブコマンド `API_SERVER` を使用して API サーバーを再起動できるようになりました。`API_SERVER` サブコマンドを使用して、API サーバーを再起動しステータスを表示できます。`API_SERVER` サブコマンドは、`diagnostic` > `SERVICES` サブコマンドの下に追加されています。 diagnostic コマンドとそのサブコマンドの詳細については、『*CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway*』の「The Commands：Reference Example」の章の「diagnostic」セクションを参照してください。

脅威検出のための脅威スキャナの設定	AsyncOS 15.0 リリースでは、着信メッセージの脅威を検出するために脅威スキャナ機能が導入されました。そのリリースでは、脅威スキャナを直接設定して脅威を検出することはできず、設定はバックエンドで行われていました。 このリリース以降、電子メールゲートウェイで着信した脅威を検出するように脅威スキャナを設定できます。脅威スキャナは受信メールポリシーごとに有効または無効にできます。脅威スキャナを有効にすると、着信メッセージがスキャンされ、スパム対策の判定に影響します。 **前提条件**：脅威スキャナを有効にするには、**グレイメールのグローバル設定**を有効にする必要があります。 脅威スキャナは、次の方法でポリシーごとに設定できます。 • **Web インターフェイス**：[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] の順に選択し、メールポリシーの [スパム対策（Anti-Spam）] 列の下にあるリンクをクリックして、[メールポリシー：スパム対策（Mail Policies: Anti-Spam）] ページを開きます。[脅威スキャナの有効化（Enable Threat Scanner）] チェックボックスをオンまたはオフにすることができます。 • **CLI**：`policyconfig` コマンドを使用します。 **インストールとアップグレードのシナリオ** 電子メールゲートウェイをインストールするか、AsyncOS 15.0 以前のバージョンから AsyncOS 15.5.1 リリースにアップグレードすると、脅威スキャナはデフォルトで無効になります。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Managing Spam and Graymail」の章にある「Defining Anti-Spam Policies」セクションを参照してください。 CLI を使用した脅威スキャナの設定の詳細については、『*CLI Reference Guide for AsyncOS 15.5.1 for Cisco Secure Email Gateway*』の「The Commands: Reference Examples」の章にある「Configuring Threat Scanner Per Policy」セクションを参照してください。

SDR サービスの有効性を向上させるための追加属性の追加	送信者ドメインのレピュテーション(SDR)サービスの有効性を向上させるため、電子メールゲートウェイには、レピュテーション分析のために Cisco TAC に送信されるテレメトリデータの一部として、デフォルトで追加属性(名前と完全な電子メールアドレス:ユーザー名とドメインを表示)が含まれるようになりました。 管理者が電子メールゲートウェイにログインすると、テレメトリデータに個人データの処理を含めるために、SDR の [追加属性を含める(Include Additional Attributes)] オプションがデフォルトで有効になっていることを通知する警告メッセージが表示されます。 **(注)** [追加属性を含める(Include Additional Attributes)] オプションは、送信者ドメインレピュテーションのフィルタ処理を有効にした場合にのみデフォルトで有効になります。 [追加属性を含める(Include Additional Attributes)] オプションを無効にする場合は、次の手順を実行します。 1. [セキュリティサービス(Security Services)] > [ドメインレピュテーション(Domain Reputation)] に移動します。 2. [グローバル設定を編集(Edit Global Settings)] をクリックし、[追加属性を含める(Include Additional Attributes)] チェックボックスをオフにします。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Sender Domain Reputation Filtering」の章にある「Enabling Sender Domain Reputation Filtering on Email Gateway」セクションを参照してください。
AWS の C5 Nitro インスタンスのサポート	AsyncOS 15.5.1 リリース以降、電子メールゲートウェイは、AWS を介して展開された **C600V** モデルの **c5.4xlarge** EC2 インスタンスタイプをサポートしています。 詳細については、『Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual on AWS EC2 Installation Guide』を参照してください。

オンプレミスユーザー向けシスコ スマート ソフトウェア ライセンシングの必須使用	Cisco Secure Email Gateway のこのリリース(AsyncOS 15.0 リリース以降のすべてのリリース)から、シスコ スマート ソフトウェア ライセンシングを使用する必要があります。 **(注)** AsyncOS 15.5.1 以降、オンプレミスユーザーのクラシックライセンスはサポートされません。クラシックライセンスモードでは、新しい機能ライセンスを注文したり、既存の機能ライセンスを更新したりすることはできなくなります。 **前提条件**:Cisco Smart Software Manager ポータルでスマートアカウントを作成し、電子メールゲートウェイでシスコ スマート ソフトウェア ライセンシングを有効にしてください。詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「System Administration」の章にある「Smart Software Licensing」セクションを参照してください。 シスコ スマート ソフトウェア ライセンシングを有効にすると、電子メールゲートウェイをこのリリースにアップグレードし、スマートライセンスモードで既存の機能ライセンスを引き続き使用できます。
個々の受信メールポリシーに Threat Defense Connector を設定します。	受信メールポリシーごとに Threat Defense Connector を設定できるようになりました。この機能を使用するには、Cisco Secure Email Gateway で Threat Defense Connector を設定して有効にしておく必要があります。 [メールポリシー(Mail Policies)] > [受信メールポリシー(Incoming Mail Policies)] に移動して、個々のメールポリシーに対して Threat Defense Connector を有効または無効にします。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Integrating Secure Email Gateway with Threat Defense」の章を参照してください。
DKIM 検証での大きなキーサイズ値のサポート	電子メールゲートウェイの DKIM 検証には、次の大きなキーサイズ値を使用できます。 • 3072 キービットサイズ • 4096 キービットサイズ 次の方法で、DKIM 検証に新しい大きなキーサイズ値を選択できます。 • **Web インターフェイス**:[メールポリシー(Mail Policies)] > [検証プロファイル(Verification Profiles)] > [プロファイルの追加(Add Profile)] または [デフォルト(Default)] に移動し、[許容最小キー:(Smallest Key to be Accepted:)] または [許容最大キー:(Largest Key to be Accepted:)] ドロップ ダウン リスト フィールドから **3072** または **4096** を選択します。 • **CLI**:`domainkeysconfig` > `keys` > `new` または `edit` > `Enter the smallest key to be accepted` または `Enter the largest key to be accepted` オプションを使用し、特定の DKIM 検証プロファイルに 3072 または 4096 に対応する必要な値を入力します。

新しい DKIM 検証プロファイルでの 512 および 768 キーサイズ値の非サポート	このリリース以降、新しい DKIM 検証プロファイルを作成する際、512 および 768 のキービットサイズ値はサポートされなくなりました。 **（注）** 512 および 768 のキーサイズ値で作成された既存の DKIM 検証プロファイルは、このリリースへのアップグレードでも引き続きサポートされます。
SSL サービスの TLS 1.3 のサポート	電子メールゲートウェイで次の TLS サービスに対して TLS 1.3 を設定できるようになりました。 • GUI HTTPS • インバウンド SMTP • アウトバウンド SMTP 「GUI HTTPS」、「インバウンド SMTP」、および「アウトバウンド SMTP」の TLS サービスに TLS 1.3 を設定する場合、電子メールゲートウェイは次の TLS 暗号のみをサポートします。 • `TLS_AES_128_GCM_SHA256` • `TLS_AES_256_GCM_SHA384` • `TLS_CHACHA20_POLY1305_SHA256` **（注）** 電子メールゲートウェイでは、TLS 1.3 に使用される暗号を変更できません。 TLS 1.3 を設定すると、電子メールゲートウェイと API サービスのレガシーまたは新しい Web インターフェイス全体で TLS 通信に使用できます。
AsyncOS API を使用したファイルハッシュリスト、RAT、SMTP ルート、保存と読み込みの設定、アドレス一覧、および受信メールポリシーユーザー情報の取得	AsyncOS API を使用して、電子メールゲートウェイのファイルハッシュリスト、受信者アクセステーブル（RAT）エントリ、SMTP ルート、保存と読み込みの設定、アドレス一覧、および受信メールポリシーユーザーに関する情報を取得できるようになりました。 詳細については、『*AsyncOS 15.5.1 API for Cisco Secure Email Cloud Gateway - Getting Started Guide*』の「Configuration APIs」セクションを参照してください。
送信者レベルまたは受信者レベルでの発信メッセージに対する TLS の適用	既存の送信先コントロール設定を使用して、ドメインごとに TLS モード（TLS 必須、TLS 推奨など）を上書きできます。 送信者、受信者などの追加の条件に基づいて発信メッセージに TLS を適用する必要がある場合は、`X-ESA-CF-TLS-Mandatory` ヘッダーを使用できるようになりました。 [コンテンツフィルタ–ヘッダーの追加/編集（Content Filter – Add/Edit Header）] アクションを設定して、コンテンツフィルタ条件に基づいて [ヘッダー名:（Header Name:）] フィールドに `X-ESA-CF-TLS-Mandatory` ヘッダーを追加し、コンテンツフィルタを発信メールポリシーにアタッチできます。

メッセージ内のパスワードで保護された添付ファイルのスキャン	電子メールゲートウェイのコンテンツスキャナを設定して、着信メッセージまたは発信メッセージ内のパスワードで保護された添付ファイルの内容をスキャンできます。電子メールゲートウェイでパスワードで保護されたメッセージの添付ファイルをスキャンする機能は、組織が次のことを行うのに役立ちます。 • 限られたサイバー攻撃をターゲットとするパスワード保護されたメッセージ内の添付ファイルとしてマルウェアを使用するフィッシングキャンペーンを検出します。 • 悪意のあるアクティビティやデータのプライバシーについてパスワードで保護された添付ファイルを含むメッセージを分析します。 この機能では、英語、イタリア語、ポルトガル語、スペイン語、ドイツ語、フランス語、日本語、および韓国語がサポートされています。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Using Message Filters to Enforce Email Policies」を参照してください。
URL レトロスペクティブサービスのリージョンベースのポーリング	Cisco Secure Email Gateway が判定の更新のために接続する URL レトロスペクティブサービスのリージョンを設定できます。Cisco Secure Email Gateway ESA は、レトロスペクティブサービスのリージョンおよび関連するエンドポイントの URL を更新できます。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Setting Up URL Filtering」セクションを参照してください。
ファイル分析サーバーのリージョンの拡張	このリリース以降、ファイル分析サーバーのリージョンは、オーストラリアとカナダの 2 つの新しいリージョンをサポートします。 ファイル分析サーバーのリージョンは、次の方法で設定できます。 • **Web インターフェイス**：[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] に移動し、[グローバル設定の編集（Edit Global Settings）] をクリックします。 • **CLI**：`ampconfig` > `ADVANCED` コマンドを使用します。 詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「File Reputation Filtering and File Analysis」の章の「Enabling and Configuring File Reputation and Analysis Services」セクションを参照してください。

動作における変更

アプリケーション SSH クライアントアルゴリズムのサポート	クラスタに電子メールゲートウェイを追加すると、次のアプリケーション SSH クライアントアルゴリズムがサポートされます。 **[非 FIPS モード]** 既存のアルゴリズムに加え、次の暗号アルゴリズム、MAC メソッド、および KEX アルゴリズムがデフォルトで Cisco Secure Email and Web Manager に追加されます。 • 暗号アルゴリズム:`aes128-ctr` • MAC メソッド:`hmac-sha2-256` • KEX アルゴリズム:`diffie-hellman-group14-sha256` **[FIPS モード]** 既存のアルゴリズムに加えて、次の暗号アルゴリズムと MAC メソッドがデフォルトで Cisco Secure Email and Web Manager に追加されます。 • 暗号アルゴリズム:`aes128-ctr` • MAC メソッド:`hmac-sha2-256`
Cisco Advanced Malware Protection エンジンによるアーカイブまたは圧縮ファイルの処理	このリリース以降、1 つ以上の構成ファイルがファイル分析の対象となる場合、Cisco Secure Email Gateway はアーカイブファイル全体を Cisco Secure Malware Analytics に送信します。構成ファイルに悪意のあるものが見つかった場合、アーカイブファイル全体がマルウェアとしてマークされます。 Cisco Secure Email Gateway が圧縮ファイルまたはアーカイブファイルの抽出に失敗した場合、ファイルは分析のために Cisco Secure Malware Analytics にアップロードされます。
プロンプトステートメントの変更:FIPS モード	このリリース以降、FIPS モードを有効にする場合、および FIPS モードで MINIMIZEDATA を有効にする場合に受信するプロンプトステートメントは、SMTP DANE ではなく SMTP のみを含むように変更されます。これらのステートメントは、FIPS 設定の MINIMIZEDATA オプションが SMTP DANE 固有のものではなく、SMTP に共通するものになるように変更されます。 **プロンプトステートメントの変更:FIPS モードの有効化** *電子メールゲートウェイの SMTP に対する FIPS 制限を最小限にしますか。[N]>* **プロンプトステートメントの変更:FIPS モードでの MINIMIZEDATA の有効化** *FIPS 制限は現在、電子メールゲートウェイの SMTP に適用されています。* *FIPS 制限を変更すると、電子メールゲートウェイがすぐに再起動します。コミットは必要ありません。* *電子メールゲートウェイの SMTP に対する FIPS 制限を最小限にしますか。[N]>*

FIPS モードでの aes192-cbc 暗号の非サポート	このリリース以降、aes192-cbc 暗号は、FIPS モードの SSH サーバーと SSH クライアントの両方でサポートされなくなります。AsyncOS 15.5.1 で FIPS モードを有効にする場合は、CLI で sshconfig ->SSHD サブコマンドを使用して aes192-cbc 暗号を削除する必要があります。 **（注）** 電子メールゲートウェイが FIPS モードで、AsyncOS 15.5.1 リリースにアップグレードされている場合、aes192-cbc 暗号はデフォルトで削除されます。

アップグレードパス

次のバージョンから、リリース 15.5.1-055 にアップグレードできます。

• 15.5.1-001	• 15.5.0-048	• 15.0.1-105
• 15.0.1-030	• 15.0.0-104	• 15.0.0-097
• 14.3.0-209	• 14.3.0-032	• 14.3.0-020
• 14.2.3-102	• 14.2.3-031	• 14.2.3-027
• 14.2.2-004	• 14.2.1-020	• 14.2.0-620

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

管理者権限を持つユーザーとしてログインして、アップグレードする必要があります。また、アップグレード後に電子メールゲートウェイを再起動する必要があります。

このリリースでサポートされているハードウェア

- このリリースでは次のハードウェアモデルがサポートされています。
  - C195
  - C395
  - C695
  - C695F

- このリリースでは次の仮想モデルがサポートされています。
  - C100v
  - C300v
  - C600v

（注） [C695 および C695F モデルの場合のみ]: アプライアンスをアップグレードまたは再起動する前に、接続されているファイバ スイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070
- C190、C390、および C690
- C380 および C680 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『*Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド*』を参照してください。このドキュメントは https://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースでは 2 TB 超のディスク領域をサポートしていないため、このリリースで 2 TB 超のディスク領域を使用する場合は、仮想電子メールゲートウェイを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシンインスタンスを導入する必要があります。

仮想電子メールゲートウェイをアップグレードしても、既存のライセンスは変更されません。

ハードウェアアプライアンスから仮想アプライアンスへの移行

ステップ 1 仮想アプライアンスの展開またはアップグレード（11 ページ）で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェアアプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされたハードウェア アプライアンスから設定ファイルを保存します。

ステップ 4 ハードウェアアプライアンスから仮想アプライアンスに設定ファイルをロードします。

ネットワーク設定に関連する適切なオプションを選択してください。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『*Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド*』に記載されています。

以下のサービスとサポート (24 ページ) も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

- 電子メールゲートウェイの設定の保存 (12 ページ)
- Vault の問題を解決するための Vault Recovery プロセスの実行 (13 ページ)
- 電子メールゲートウェイの設定の保存 (12 ページ)
- 電子メールゲートウェイで IDN ドメインを使用して設定可能な機能 (15 ページ)
- 既存の URL レピュテーション判定の新しいカテゴリと新しい名前 (17 ページ)
- Cisco Talos サービスにアクセスするためのファイアウォール設定 (17 ページ)
- Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定 (18 ページ)
- 電子メールゲートウェイでのサービスログの有効化 (18 ページ)
- クラスタレベルでのインテリジェント マルチスキャンとグレイメール設定のアップグレード (18 ページ)
- FIPS の準拠性 (18 ページ)
- 集中管理 (クラスタ化されたアプライアンス) を使用した展開のアップグレード (19 ページ)
- 直前のリリース以外のリリースからのアップグレード (19 ページ)
- 設定ファイル (19 ページ)
- アップグレード中の IPMI メッセージ (19 ページ)

電子メールゲートウェイの設定の保存

電子メールゲートウェイで暗号化が有効になっている場合は、AsyncOS 15.5.1 にアップグレードする前または後に、電子メールゲートウェイの設定のコピーを保存することをお勧めします。

Vault Recovery プロセスを実行して Vault サービスを復元した後、保存した電子メールゲートウェイの設定をロードして、デバイスの以前の設定を復元できます。

次の方法を使用してデバイスの設定を保存できます。

- [システム管理(System Administration)] > [設定ファイル(Configuration File)] に移動し、[コンフィギュレーションファイルでパスフレーズを暗号化する(Encrypt passphrases in the Configuration Files)] を選択します。
- CLI で `saveconfig` コマンドを使用し、**2** をタイプして [パスフレーズを暗号化する(Encrypt passphrases)] オプションを選択します。

Vault の問題を解決するための Vault Recovery プロセスの実行

AsyncOS 15.5.1 にアップグレードする前または後に、(ハードウェア、オンプレミス、CES、AWS、KVM、Azure、または Hyper-V の)電子メールゲートウェイで Vault 関連の問題が発生した場合は、その問題を解決するために Vault Recovery プロセスを実行する必要があります。次の手順を使用して Vault Recovery を実行します。

1. 次のログイン情報を使用して、直接 SSH 接続を介して電子メールゲートウェイにログインします。

   ユーザー名:**enablediag**

   パスワード:**管理者ユーザーのパスワード**
2. `recovervault` コマンドを実行します。
3. プロンプトが表示されたら、次の一連のサブコマンドを入力します。
   a. `yes`
   b. `1 (encryption enabled) or 2 (encryption disabled)`
4. 管理者ユーザーのログイン情報を使用して電子メールゲートウェイにログインし、Vault Recovery プロセスが完了したらデバイスを再起動します。
5. (**クラスタセットアップの場合のみ**)Vault が回復し、デバイスの再起動が完了したら、電子メールゲートウェイをクラスタに再参加させます。
6. (**暗号化が有効になっている場合のみ**)以前に保存したデバイスの設定のコピーをロードして、以前の設定を復元します。
7. Vault サービスのアラートがないか、電子メールゲートウェイを数時間モニターします。

電子メールゲートウェイが回復し、Vault が再初期化されます。これで、問題なくデバイスに接続できます。

(注) **暗号化無効**

このシナリオでは、すべてのシステム設定が保持されます。

暗号化有効

このシナリオでは、次の暗号化された変数がデフォルトの工場出荷時の値にリセットされます。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード

- DK/DKIM 署名キー
- 発信 SMTP 認証パスワード
- PostX 暗号化キー
- PostX 暗号化プロキシ パスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード
- アップデータ サーバの URL
- 認証 API のクライアントログイン情報
- Cisco Advanced Malware Protection プロキシパスワード
- SAML 証明書のパスフレーズ

以前の設定を復元する場合は、以前に保存した設定ファイルをロードする必要があります。

（注） 認証 API のクライアントログイン情報は構成ファイルに保存されないため、API を呼び出して新しいクライアントログイン情報を作成する必要があります。

ログ（enablediag ユーザーの場合）:

```
Available Commands:
help -- View this text.
quit -- Log out.
service -- Enable or disable access to the service system.
network -- Perform emergency configuration of the diagnostic network interface.
clearnet -- Resets configuration of the diagnostic network interface.
ssh -- Configure emergency SSH daemon on the diagnostic network interface.
clearssh -- Stop emergency SSH daemon on the diagnostic network interface.
tunnel -- Start up tech support tunnel to IronPort.
print -- Print status of the diagnostic network interface.
recovervault -- Recover vault, it will only restore the encrypted variables to factory
values, will not touch anything related to configurations if encryption is disabled .
resetappliance -- Reset appliance reverts the appliance to chosen build with factory
default settings with default IP. No network configuration would be preserved.
reboot -- Reboot the appliance.

S/N 42189A47B0D50A645948-CEC55115B364
Service Access currently ENABLED (0 current service logins)
esa1.hc303-10.smtpi.com> recovervault

Are you sure you want to recover vault?  [N]> y
Encryption is enabled [1]>
Encryption is not enabled [2]>
```

ファイル レピュテーション サービスのアクティブ化の前提条件 - Cisco Secure Endpoint プライベート クラウド

このリリースにアップグレードする前に、ファイル レピュテーション サービスのアクティブ化に関する次の前提条件を満たしていることを確認してください。

- Cisco Secure Endpoint プライベート クラウドを 3.8.1 以上のバージョンにアップグレードした
- アップグレードプロセス中にプロンプトが表示されたとき、Cisco Secure Endpoint の「コンソールのホスト名」と「アクティベーションコード」の詳細を入力した。

電子メールゲートウェイで IDN ドメインを使用して設定可能な機能

前提条件:

国際化ドメイン名（IDN）機能を使用する前に、次の前提条件を満たしていることを確認してください。

- すべての着信メッセージには UTF-8 でエンコードされた IDN が必要です。
  たとえば、電子メールゲートウェイにメッセージを送信する MTA は IDN をサポートし、メッセージ内のドメインが UTF-8 形式であることを確認する必要があります。
- すべての発信メッセージには UTF-8 でエンコードされた IDN が必要であり、宛先サーバーはそれに応じて IDN を受け入れ、サポートする必要があります。
  たとえば、電子メールゲートウェイからのメッセージを受け入れる MTA は UTF-8 形式でエンコードされた IDN とドメインをサポートする必要があります。
- 該当するすべての DNS レコードで、Punycode 形式を使用して IDN を設定する必要があります。
  たとえば、IDN に MX レコードを設定する場合、DNS レコードのドメインは Punycode 形式である必要があります。

このリリースでは、電子メールゲートウェイ内で IDN ドメインを使用して設定できるのは次の機能**のみ**です。

- **SMTP ルートの設定:**
  - IDN ドメインを追加または編集します。
  - IDN ドメインを使用して SMTP ルートをエクスポートまたはインポートします。
- **DNS の設定:** IDN ドメインを使用して DNS サーバーを追加または編集します。
- **リスナーの設定:**
  - インバウンドリスナーまたはアウトバウンドリスナーのデフォルトドメインの IDN ドメインを追加または編集します。
  - HAT テーブルまたは RAT テーブルで IDN ドメインを追加または編集します。
  - IDN ドメインを使用して HAT テーブルまたは RAT テーブルをエクスポートまたはインポートします。
- **メールポリシーの設定:**
  - [着信メールポリシー（Incoming Mail Policies）] の送信者（[送信者を追跡する（Following Senders）] オプションまたは [送信者を追跡しない（Following Senders are）] オプション）と受信者（[受信者を追跡する（Following Recipients）] または [受信者を受信しない（Recipients are not）] オプション）の IDN ドメインを使用してドメインを追加または編集します。

  - [発信メールポリシー(Outgoing Mail Policies)] の送信者([送信者を追跡する(Following Senders)] オプションまたは [送信者を追跡しない(Following Senders are)] オプション)と受信者([受信者を追跡する(Following Recipients)] または [受信者を受信しない(Recipients are not)] オプション)の IDN ドメインを使用してドメインを追加または編集します。
  - [着信メールポリシー(Incoming Mail Policies)] または [送信メールポリシー(Outgoing Mail Policies)] で IDN ドメインを使用した送信者または受信者の検索
  - IDN ドメインを使用して送信者判定の例外を定義します。
  - IDN ドメインを使用してアドレスリストを作成します。
  - 宛先の制御に IDN ドメインを使用して宛先ドメインを追加または編集します。
- **バウンスプロファイルの設定:**IDN ドメインを使用して代替電子メールアドレスを追加または編集します。
- **送信者ドメインレピュテーションの設定:**IDN ドメインの送信者ドメイン レピュテーション スコアを定義します。
- **IP レピュテーションの設定:**IDN ドメインの IP レピュテーションスコアを定義します。
- **LDAP の設定:**IDN ドメインを使用して、LDAP グループクエリを作成し、クエリを受け入れ、クエリをルーティングし、クエリをマスカレードします。
- **レポートの設定:**IDN データ(ユーザー名、電子メールアドレス、ドメイン)をレポートに表示します。
- **メッセージトラッキングの設定:**メッセージトラッキングに IDN データ(ユーザー名、電子メールアドレス、およびドメイン)を表示します。
- **ポリシー、ウイルス、およびアウトブレイク隔離の設定:**
  - ウイルス対策エンジンによる判定に従って、マルウェアを送信する可能性のある IDN ドメインを含むメッセージを表示します。
  - スパムまたはマルウェアの可能性があるとアウトブレイクフィルタによって検出された IDN ドメインを含むメッセージを表示します。
  - メッセージフィルタ、コンテンツフィルタ、および DLP メッセージアクションによって検出された IDN ドメインを含むメッセージを表示します。
- **スパムの隔離の設定:**
  - スパム、または疑いのあるスパムとして検出された IDN ドメインを含むメッセージを表示します。
  - IDN ドメインを含む電子メールアドレスをセーフリストとブロックリストのカテゴリに追加します。

  (注) 現在、IDN ドメインを持つ受信者は、[スパムの管理(Spam Quarantine)] 設定ページの [エンドユーザーの隔離アクセス(End-User Quarantine Access] セクションでエンドユーザー認証方式が [なし(None)] に設定されている場合にのみ、エンドユーザーの隔離にアクセスできます。

- [SPF 構成設定(SPF Configuration Settings)]:IDN ドメインを使用してメッセージの SPF 検証を実行します。
- [DKIM 構成設定(DKIM Configuration Settings)]:IDN ドメインを使用して DKIM 署名とメッセージの検証を実行します。
- [DMARC 構成設定(DMARC Configuration Settings)]:IDN ドメインを使用してメッセージの DMARC 検証を実行します。

既存の URL レピュテーション判定の新しいカテゴリと新しい名前

次の表に、電子メールゲートウェイの既存の URL レピュテーション判定の新しいカテゴリと新しい名前を示します。

現在の URL レピュテーション判定名	新しい Cisco Talos URL レピュテーション判定名	スコア範囲	説明
クリーン	信頼できる	+6.0 ～ +10.0	優れた安全性を示す動作を表示します。
ニュートラル	好ましい	+0.1 ～ +5.9	一定のレベルの安全性を示す動作を表示します。
	ニュートラル	-3.0 ～ 0.0	好ましい動作や望ましくない動作は表示されません。ただし、この判定は評価の結果です。
	要検討	-5.9 ～ -3.1	リスクを示す可能性のある動作、または望ましくない動作を表示します。
悪意のある	信頼できない	-10.0 ～ -6.0	非常に悪い、悪意のある、または望ましくない動作を表示します。
スコアなし	不明	スコアなし	この判定は、これまで評価されなかった場合や、脅威レベルの判定をアサートできない場合に表示されます。

Cisco Talos サービスにアクセスするためのファイアウォール設定

電子メールゲートウェイを Cisco Talos サービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります（以下の表を参照）。

（注） HTTPS アップデータプロキシ設定は、Cisco Talos サービスへの接続に使用されます。

ホスト名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに接続するには、次のホスト名用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります。

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

詳細については、ユーザーガイドの「Firewall」の章を参照してください。

電子メールゲートウェイでのサービスログの有効化

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。

Cisco Secure Email Gateway は、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アップグレードプロセス中に、次のいずれかから電子メールゲートウェイでサービスログを有効にする方法を選択できます。

- Web インターフェイスの [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] ページで、[サービスログ（Service Logs）] に [同意する（I Agree）] オプションを選択します。
- upgrade CLI コマンドの「*サービスログをデフォルトで有効にして続行しますか？ [Y]（Do you agree to proceed with Service Logs being enabled by default? [y]）*」に「**Yes**」と入力します。

詳細については、ユーザーガイドの「Improving Phishing Detection Efficacy using Service Logs」の章を参照してください。

クラスタレベルでのインテリジェント マルチスキャンとグレイメール設定のアップグレード

AsyncOS 15.0 にアップグレードする前に、インテリジェント マルチスキャンとグレイメールの設定が同じクラスタレベルに存在していることを確認します。クラスタレベルが異なっている場合は、アップグレード後にインテリジェント マルチスキャンとグレイメールの設定を確認する必要があります。

FIPS の準拠性

AsyncOS 15.0 リリースは FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました（FIPS 140-2 認定#4036）。

集中管理（クラスタ化されたアプライアンス）を使用した展開のアップグレード

クラスタに C380 または C680 ハードウェアアプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x80 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x80 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー（AsyncOS X.0）またはマイナー（AsyncOS X.x）リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース（AsyncOS X.x.x）には、バグ修正のみが含まれています。

設定ファイル

通常、シスコは、以前のメジャーリリースに関して、設定ファイルの下位互換性をサポートしていません。マイナーリリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコカスタマーサポートでご確認ください。

アップグレード中の IPMI メッセージ

CLI を使用して電子メールゲートウェイをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。これは既知の問題です。

障害 ID：CSCuz28415

このリリースへのアップグレード

はじめる前に

- ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。
- 既知および修正済みの問題のリスト（23 ページ）とインストールおよびアップグレードに関する注意事項（10 ページ）を確認してください。
- 仮想電子メールゲートウェイをアップグレードする場合は、仮想アプライアンスのアップグレード（11 ページ）を参照してください。

手順

次の手順を実行して電子メールゲートウェイをアップグレードします。

ステップ 1 電子メールゲートウェイから、XML 構成ファイルを保存します。

ステップ 2 セーフリスト/ブロックリスト機能を使用している場合は、電子メールゲートウェイからセーフリスト/ブロックリストデータベースをエクスポートします。

ステップ 3 すべてのリスナーを一時停止します。

ステップ 4 ワークキューが空になるまで待ちます。

ステップ 5 [システム管理(System Administration)] タブで、[システムアップグレード(System Upgrade)] ページを選択します。

ステップ 6 [利用可能なアップグレード(Available Upgrades)] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。

ステップ 7 [アップグレードの開始(Begin Upgrade)] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。

ステップ 8 アップグレードが完了したら、[今すぐリブート(Reboot Now)] ボタンをクリックして電子メールゲートウェイを再起動します。

ステップ 9 すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[システム管理(System Administration)] > [SSL 構成(SSL Configuration)] ページを使用するか、CLI で `sslconfig` コマンドを使用します。手順については、ユーザーガイドまたはオンラインヘルプの「System Administration」の章を参照してください。
- 「パフォーマンスアドバイザリ (22 ページ)」を確認してください。
- SSH キーを変更した場合は、アップグレード後に電子メールゲートウェイと Cisco Secure Email and Web Manager 間の接続を再認証します。

アップグレード後の注意事項

スマート ソフトウェア ライセンシングを有効にした HTTP または HTTPS プロキシの設定

スマート ソフトウェア ライセンシングを有効にしているときに、ドメインまたはレルムを含むユーザー名を使用した認証で HTTP または HTTPS プロキシを設定すると、エンジンの更新に失敗します。この動作は既知の問題です。

不具合 ID:CSCwi11926

この問題を解決し、エンジンの更新を正常に実行するには、次の手順を実行する必要があります。

1. [セキュリティサービス(Security Services)] > [サービスの更新(Service Updates)] ページでの認証によって HTTP または HTTPS プロキシを設定します。

（注） 入力するユーザー名にドメインまたはレルムが含まれていないことを確認してください。たとえば、[ユーザー名（Username）] フィールドには、ドメイン\ユーザー名ではなくユーザー名のみを入力します。

2. スマート ソフトウェア ライセンシングを有効にして登録した後、ライセンスを要求します。
3. [今すぐアップグレード（Update Now）] をクリックして、エンジンの更新を開始します。

これで、エンジンが正常に更新されました。

FIPS モードでの TLS メール配信の失敗

DHE 暗号のネゴシエーション時に FIPS モードでの TLS メール配信に失敗した場合は、`fipsconfig` CLI コマンドで `MINIMIZEDATA` サブコマンドを使用して MINIMIZEDATA を有効にする必要があります。`fipsconfig` -> `MINIMIZEDATA` サブコマンドの詳細については、『*User Guide for AsyncOS 15.5.1 for Secure Email Gateway*』の「Minimizing FIPS Restriction on SMTP in FIPS Mode」セクションを参照してください。

Cisco Secure Endpoint プライベート クラウドのファイル レピュテーション サービスのアクティブ化

ファイル レピュテーション サービスをアクティブにするには、システムセットアップに基づいて次のいずれかの手順に従います。

- [クラスタモード]: 新しいファイル レピュテーション サービスがすでに設定されている電子メールゲートウェイに接続します。
- [スタンドアロンモード]: 次の手順を実行します。

  1. Web インターフェイスで、[セキュリティサービス（Security Services）] > [ファイルレピュテーションと分析（File Reputation and Analysis）] ページに移動します。

  2. [グローバル設定を編集（Edit Global Settings）] ボタンをクリックします。

  3. [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] パネルをクリックします。

  4. [ファイルレピュテーションサーバー（File Reputation Server）] ドロップダウンリストから [プライベートレピュテーションクラウド（Private reputation cloud）] オプションを選択します。

  5. 所定のフィールドにコンソールのホスト名とアクティベーションコードを入力します。

  6. [送信（Submit）] をクリックし、変更をコミットします。

DLP サービスステータスチェック

このリリースにアップグレードした後、DLP サービスで問題が発生する可能性があります。

ソリューション：CLI で `diagnostic` > `services` > `DLP` > `status` サブコマンドを使用して、電子メールゲートウェイの DLP サービスのステータスを確認します。DLP サービスが実行されていない場合は、既知の問題リストにある CSCvy08110 の不具合の「回避策」セクションを参照してください。既知の問題を表示する方法の詳細については、既知および修正済みの問題のリスト (23 ページ) を参照してください。

電子メールゲートウェイでのパスワードで保護された添付ファイルのスキャン

パスワード保護された添付ファイルをスキャンするように電子メールゲートウェイのコンテンツスキャナを設定する場合、電子メールトラフィックにパスワード保護された添付ファイルが高い割合で含まれていると、パフォーマンスに影響を与える可能性があります。

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 15.0 にアップグレードした後のインテリジェント マルチスキャン（IMS）およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタレベルで構成されている場合、電子メールゲートウェイはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタレベルで IMS を設定し、マシンレベルでグレイメールを設定すると、電子メールゲートウェイは IMS のグローバル設定をマシンレベルにコピーします。
- スキャンメッセージの最大メッセージサイズとタイムアウト値が異なる場合、電子メールゲートウェイは最大タイムアウトおよび最大メッセージサイズの値を使用して、IMS とグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージサイズ値として 2M を使用します。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されている電子メールゲートウェイの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20% 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツセキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダーにお問い合わせください。

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=afr&svr=3nH&rls=15.5.0,15.5.1&prdNam=Cisco%20Secure%20Email%20Gateway
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&kw=*&bt=custV&sb=fr&svr=3nH&rls=15.5.1-055&prdNam=Cisco%20Secure%20Email%20Gateway

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://tools.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択（Select from list）] > [セキュリティ（Security）] > [電子メールセキュリティ（Email Security）] > [Cisco Secure Email Gateway] の順にクリックし、[OK] をクリックします。

ステップ 4 [リリース（release）] フィールドに、リリースのバージョン（15.5.1-055 など）を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示（Show Bugs）] ドロップダウンから、[これらのリリースで修正済み（Fixed in these Releases）] を選択します。
- 既知の問題のリストを表示するには、[バグの表示（Show Bugs）] ドロップダウンから [これらのリリースに影響（Affecting these Releases）] を選択し、[ステータス（Status）] ドロップダウンから [開く（Open）] を選択します。

ご不明な点がある場合は、ツールの右上にある [ヘルプ（Help）] または [フィードバック（Feedback）] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索（search）] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

ソフトウェア ライフサイクル サポート ステートメント

ソフトウェアのタイムベースのリリースモデルおよびソフトウェアリリースのサポートタイムラインについては、「Software Lifecycle Support Statement」を参照してください。

関連資料

マニュアルの内容（Cisco Content Security 製品）	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco Secure Email and Web Manager	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンス用 CLI リファレンス ガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco Secure Email Encryption Service	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html [英語]

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：https://www.cisco.com/c/ja_jp/support/web/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、電子メールゲートウェイ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、ユーザーガイドまたはオンラインヘルプを参照してください。

このドキュメントは、米国シスコ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。