



AsyncOS 12.1 for Cisco Email Security Appliances リリース ノート

発行日:2019 年 7 月 2 日
改訂日:2019 年 8 月 9 日


目次

- [今回のリリースでの変更点\(2 ページ\)](#)
- [動作における変更\(6 ページ\)](#)
- [アップグレードの方法\(9 ページ\)](#)
- [インストールおよびアップグレードに関する注意事項\(10 ページ\)](#)
- [既知および修正済みの問題\(15 ページ\)](#)
- [関連資料\(16 ページ\)](#)
- [サービスとサポート\(17 ページ\)](#)




今回のリリースでの変更点

機能	説明
新しいハードウェア サポート	<p>Cisco Email Security Appliances 向け AsyncOS 12.5 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。</p> <ul style="list-style-type: none"> • C195 • C395 • C695 • C695F <p>詳細については、次を参照してください。 https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet_c22-739910.html</p>
高度なマルウェア防御 (AMP) 隔離管理の改善	<p>AMP エンジンのスキャン プロセス実行時に、ファイルレピュテーション サービスから不明な判定を受信した添付ファイルが分類前チェックとファイル分析のために送信されます。</p> <p>分類前チェック フェーズでは、メッセージが電子メール セキュリティ アプライアンスにローカルに保存されてから、完全なファイル分析を行うために添付ファイルが送信された場合にのみ、中央集中型隔離に送信されるようになりました。</p> <p>これにより、パフォーマンスが向上し、集中型隔離の全体的な負荷が軽減されます。</p>
送信者ドメインレピュテーションを使用したメッセージのフィルタリング	<p>シスコの送信者ドメインレピュテーション (SDR) は、送信者のドメインおよびその他の属性に基づいて電子メール メッセージのレピュテーションの判定を提供するクラウド サービスです。</p> <p>このドメイン ベースのレピュテーション分析では、共有 IP、ホスティングまたはインフラストラクチャ プロバイダーのレピュテーションよりも詳しい情報を調べることでより高いスパム検出率を達成し、完全修飾ドメイン名 (FQDN) や SMTP 通信およびメッセージ ヘッダーのその他の送信者情報に関連する特徴に基づいて判定を取得します。SDR の詳細は、Cisco Talos セキュリティ インテリジェンス およびリサーチ グループ (Talos) (https://www.talosintelligence.com) までお問い合わせください。</p> <p>アプライアンスで送信者ドメインレピュテーション フィルタリングを有効にするには、ユーザ ガイドまたはオンライン ヘルプの「Sender Domain Reputation Filtering」と『<i>CLI Reference Guide for AsyncOS for Cisco Email Security Appliances</i>』を参照してください。</p>

<p>ファイル分析に向けた Cisco AMP Threat Grid クラスタリングのサポート</p>	<p>以下のいずれかの方法で、ファイル分析に向けてスタンドアロンまたはクラスタの Cisco AMP Threat Grid アプライアンスを追加できるようになりました。</p> <ul style="list-style-type: none"> • Web インターフェイスの [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ファイル分析 (File Reputation and Analysis)] ページ。ユーザガイドの「ファイルレピュテーションフィルタリングおよびファイル分析」の章を参照してください。 • CLI での <code>ampconfig</code> コマンド。『<i>CLI Reference Guide for AsyncOS for Cisco Email Security Appliances</i>』を参照してください。
<p>外部脅威フィードの消費機能</p>	<p>Cisco Email Security Appliance で、TAXII プロトコルで通信される STIX フォーマットで外部脅威情報を使用するように設定できます。アプライアンスで外部脅威情報を使用する機能によって、組織は以下のことを実施できるようになります。</p> <ul style="list-style-type: none"> • マルウェア、ランサムウェア、フィッシング攻撃、標的型攻撃などのサイバー脅威にプロアクティブに対応する。 • 外部脅威フィードまたは TAXII プロトコルで通信する STIX フォーマットで外部脅威フィードを取得可能な組織のネットワーク上の他のデバイスに登録し、アプライアンスで脅威情報を使用する。 • アプライアンスに動的な情報 (URL の動的なリストなど) をインポートし、動的な情報に基づいてメールポリシーの設定やメッセージアクションの定義を実行する。 • アプライアンスの機能を向上する。 <p>クラシック ライセンシング モードを使用していて、外部脅威フィードの機能キーをお持ちでない場合は、以下の手順でシスコの Global Licensing Operations (GLO) チームに連絡して機能キーを取得する必要があります。</p> <ol style="list-style-type: none"> 1. GLO チーム (licensing@cisco.com) に電子メールを送信し、件名を「外部脅威フィード機能キーのリクエスト」とします。その後、電子メールに製品認証キー (PAK) ファイルと発注書 (PO) の詳細を記載します。 2. GLO チームが機能キーを手動でプロビジョニングし、アプライアンスにインストール可能なライセンス キーを電子メールで送信します。 <p> (注) アプライアンスでスマート ライセンシング モードに切り替えると、自動的に外部脅威フィード機能キーが提供されます。</p> <p>この機能を設定するには、ユーザガイドまたはオンライン ヘルプの「Configuring Cisco Email Security Gateway to Consume External Threat Feeds」の章と『<i>CLI Reference Guide for AsyncOS for Cisco Email Security Appliances</i>』を参照してください。</p>

<p>ファイル分析に向けたしきい値の設定</p>	<p>許容されるファイル分析スコアのしきい値の上限を設定できるようになりました。</p> <p>しきい値設定に基づいてブロックされるファイルは、詳細マルウェア保護レポートの [Incoming Malware Threat Files] セクションで、[Custom Threshold] として表示されます。</p> <p>詳細については、ユーザガイドの「File Reputation Filtering and File Analysis」を参照してください。</p>
<p>How-To ウィジェットを使用したユーザエクスペリエンスの強化</p>	<p>How-To は、アプライアンスで複雑なタスクを実行するためにウォークスルー形式でユーザにアプリ内アシスタンスを提供する、コンテキスト型ウィジェットです。</p> <p> (注) ウォークスルーはクラウドで更新できます。ハウツーウィジェットの更新バージョンとポップアップウィンドウを表示するには、必ずブラウザのキャッシュをクリアしてください。</p> <p>詳細は、ユーザガイドまたはオンラインヘルプの「Accessing the Appliance」の章と『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。</p>
<p>脅威名に基づいた悪意のあるメッセージの表示</p>	<p>メッセージトラッキングで、脅威名に基づいて AMP エンジンに悪意があると検出された着信または発信メッセージを検索できるようになりました。</p> <p>詳細は、ユーザガイドの「Tracking Messages」の章を参照してください。</p>
<p>発信 TLS 接続に向けた、名前付きエンティティの DNS ベースの認証 (DANE) サポート</p>	<p>アプライアンスの発信 TLS 接続に向けた名前付きエンティティの DNS ベースの認証 (DANE) を有効にすることで、有効な受信者のドメインに安全にメッセージを送信できるようになりました。</p> <p>有効な受信者のドメインに安全にメッセージを送信する機能によって、宛先のドメインで DANE がサポートされていれば、組織はビジネスクリティカルな機密情報を意図した受信者に確実に送信できます。</p> <p>詳細は、ユーザガイドの「Encrypting Communication with Other MTAs」の章を参照してください。</p>
<p>偽装電子メール検出の強化</p>	<p>[Mail Policies] > [Address Lists] を選択して、完全な電子メールアドレスのみで構成された例外リストを作成し、偽装電子メール検出コンテンツフィルタをバイパスすることができます。</p> <p>アプライアンスで、設定済みのコンテンツフィルタから電子メールアドレスをスキップする場合、偽装電子メール検出ルールでこの例外リストを使用できます。詳細は、ユーザガイドの「Content Filters」の章を参照してください。</p>
<p>ログサブスクリプションの強化</p>	<p>レート制限オプションを使用して、指定した時間範囲 (秒単位) 内の、ログファイルにログ記録されるイベントの最大数を設定することができます。デフォルトの時間範囲の値は 10 秒です。</p> <p>Web インターフェイスの [System Administration] > [Log Subscriptions] ページを使用するか、CLI の logconfig コマンドを使用して、レート制限を設定します。詳細は、ユーザガイドの「Logging」の章を参照してください。</p>

<p>スマート ソフトウェア ライセンシングのサポート</p>	<p>スマート ソフトウェア ライセンシングを使用すると、Cisco Email Security Appliance のライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンシングをアクティブ化するには、Cisco Smart Software Manager (CSSM) でアプライアンスを登録する必要があります。CSSM は、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。</p> <p>以下は、アプライアンスでクラシック ライセンシング モードからスマート ライセンシング モードに切り替える利点です。</p> <ul style="list-style-type: none"> クラシック ライセンス モードでは困難だった、物理アプライアンスと仮想アプライアンス間の製品認証キー (PAK) ライセンスの管理が簡単に行えます。 組織内のデバイスまたはアカウント間で、ソフトウェア ライセンスを簡単に移行できます。 アプライアンスで PAK ファイルを管理したり、コピーを維持する必要がありません。 スマート ライセンシング アカウントでは、ユーザのアクセスを制限できます。 <p> 注意 アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ライセンシングモードにロールバックすることができなくなります。</p> <p>この機能を使用するには、ユーザ ガイドまたはオンライン ヘルプの「Smart Software Licensing」の章と『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。</p>
<p>DMARC 検証をスキップしたメッセージを処理するためのコンテンツ フィルタおよびメッセージ フィルタの設定</p>	<p>DMARC 検証をスキップしたメッセージに対してアクションを実行するようにアプライアンスを設定できます。</p> <p>Other Header コンテンツ フィルタで次の設定を使用して、DMARC 検証をスキップしたメッセージを分類します。</p> <ul style="list-style-type: none"> ヘッダー名を「X-Ironport-Dmarc-Check-Result」として追加します。 [Header Value] を選択して、[Equals] を選択し、validskip、invalidskip、temperror、permerror のいずれかの値を追加します。 <p>DMARC 検証をスキップしたメッセージの分類に使用するメッセージ フィルタ ルールの構文の例を次に示します。</p> <pre>Quarantine_messages_DMARC_skip: if (header("X-Ironport-Dmarc-Check-Result") == "^validskip\$") { quarantine("Policy"); }</pre> <p>コンテンツ フィルタとメッセージ フィルタで使用されるヘッダー値の詳細については、Cisco TAC にお問い合わせください。</p>
<p>シスコのコンテンツ セキュリティ管理アプライアンス接続パラメータとホスト キーを表示または削除する機能</p>	<p>smaconfig CLI コマンドを使用して、アプライアンスでシスコのコンテンツ セキュリティ管理アプライアンス接続パラメータとホスト キーを表示または削除できるようになりました。</p>

<p>インテリジェント マルチスキャンの強化</p>	<p>インテリジェント マルチスキャン (IMS) は、パフォーマンスの高いマルチレイヤ スпам対策ソリューションです。Cisco Email Security Appliance の本リリースは、最新の IMS エンジンを提供します。このエンジンは、スパム対策エンジンの様々に組み合わせることによってスパム検出率を向上します。</p> <p>最新の IMS エンジンを使用するには、IMS 機能キーを追加し、アプライアンスでライセンスを承認する必要があります。既存の IMS ユーザの場合は、IMS のすべてのメール ポリシーが移行され、最新の IMS エンジンでシームレスに機能します。</p>
<p>カスタム DLP ポリシーに向けたエンティティベースのカスタム分類子ルールの最小スコア</p>	<p>カスタム DLP ポリシーに向けてカスタム分類子を作成する際に、推奨される最小スコアを使用するか、エンティティベースのルールの最小スコアを上書きすることを選択できるようになりました。</p> <p>設定されたルールの重みに代わって、エンティティベースのルールの最小スコアを使用できます。最小スコアは部分的に一致と完全一致を区別し、それに従ってスコアを計算します。これにより、誤検出と検出漏れの数を削減できます。</p> <p>以下の方法で最小スコアを設定します。</p> <ol style="list-style-type: none"> 1. [Mail Policies] > [DLP Policy Customizations] > [Custom Classifiers Settings] セクションで、[Use recommended minimum scores for entity-based rules] チェックボックスを選択します。 2. [Mail Policies] > [DLP Policy Customizations] > [Add Custom Classifier] に移動し(または既存のカスタム分類子を確認し)、最小スコアを入力します。 <p>詳細については、ユーザ ガイドの「Data Loss Prevention」の章を参照してください。</p>

動作における変更

<p>テキスト リソースの削除における変更</p>	<p>これよりも前のリリースでは、着信メッセージやコンテンツ フィルタで参照されているテキスト リソースを削除できました。</p> <p>このリリースへのアップグレード後は、着信メッセージやコンテンツ フィルタで参照されているテキスト リソースは削除できません。</p>
<p>ロング ファイル名を使用して添付ファイルをスキャンする場合の変更</p>	<p>添付ファイルのファイル名に 256 文字以上が含まれている場合、添付ファイルと添付ファイル内のファイルはスキャン不可としてマークされ、電子メールパイプラインではそれ以上処理されません。[メッセージ トラッキング (Message Tracking)] ページと AMP ログには、次の形式で切り捨てられたファイル名が表示されます。</p> <p><元のファイル名の最初の 225 文字 + '~ too_long_name ~'+元のファイル名の最後の 10 文字></p>

ファイル分析のための コンフィギュレーション ファイルの ロード中の変更	<p>次に、Web インターフェイスで [コンフィギュレーション ファイル (Configuration File)] > [ロード設定 (Load Configuration)] オプションを使用してファイル分析用のコンフィギュレーション ファイルをロードするときの動作の変更を示します。</p> <ul style="list-style-type: none"> • ファイルグループの下にあるファイルタイプは、コンフィギュレーションファイルに従って選択され、その他のファイルタイプは未選択状態のままになります。 • [ロード設定 (Load Configuration)] オプションを使用して、新しいファイルタイプを追加したり、ファイルタイプのグループを変更したりできません。
メッセージの DMARC 検証のバイ パスの変更	<p>このリリースより前のリリースでは、アドレス一覧に設定されている完全な電子メールアドレスに基づいて、送信者からのメッセージの DMARC 検証をスキップすることができました。</p> <p>このリリースにアップグレードした後は、アドレス一覧に設定されている完全な電子メールアドレスまたはドメインに基づいて、送信者からのメッセージの DMARC 検証をスキップできます。</p>
最初のログインに 対するデフォルト パスフレーズの使用 の変更	<p>AsyncOS 12.0 システムの新しい仮想アプライアンスまたはハードウェアアプライアンスをインストールする場合、Web インターフェイスまたは CLI を使用して初めてアプライアンスにログインするときにデフォルトのパスフレーズを変更する必要があります。</p>
ドメイン キー/ DKIM 検証の設定の 変更	<p>このリリースより前のリリースでは、アプライアンスが FIPS モードになっている場合、2048 ビットの DKIM キーのみを使用して、着信メッセージを検証することができました。</p> <p>このリリースにアップグレードした後は、アプライアンスが FIPS モードになっている場合、1024、1536、または 2048 ビットの DKIM キーを使用して着信メッセージを検証できます。</p>
USEDNS キーワード を使用した SMTP ルート設定に対する 変更	<p>このリリースより前のリリースでは、宛先ポートとしてデフォルトのポート (25) のみを使用して、USEDNS キーワードで SMTP ルートを設定することができました。</p> <p>このリリースにアップグレードした後は、任意の有効な宛先ポートを使用して、USEDNS キーワードで SMTP ルートを設定できます。</p>
URL フィルタリング アクション中に 検出された復号化 エラーによるス キャン不可メッ セージの処理	<p>Cisco Email Security Appliance は、URL フィルタリング アクション中に検出された複合化エラーのためにスキャンされないメッセージを処理できるようになりました。</p> <p>Web インターフェイスの [Security Services] > [Scan Behavior] > [Edit Global Settings] ページを使用して、このようなメッセージに対して次のいずれかのアクションを設定できます。</p> <ul style="list-style-type: none"> • メッセージの件名を変更する。 • メッセージにカスタム ヘッダーを追加する。 • メッセージの受信者を変更する。 • 代替宛先ホストにメッセージを送信する。 • メッセージを隔離する。 <p>詳細は、Cisco Email Security Appliance のユーザガイドの「Configuring Scan Behavior」の章を参照してください。</p>

<p>デモ証明書の変更</p>	<p>このリリース以前は、アプライアンスが TLS 接続を有効にするデモ証明書で事前に設定されています。</p> <p>このリリースにアップグレードすると、アプライアンスは TLS 接続を有効にする一意の証明書を生成します。次の設定で使用されている既存のデモ証明書は新しい証明書に置き換えられます。</p> <ul style="list-style-type: none"> • メール配信 • LDAP • ネットワーキング • URL フィルタリング • SMTP サービス
<p>メモリ ページ スワッピングのしきい値の変更</p>	<p>このリリースより前のリリースでは、メモリ ページ スワッピングのデフォルトのしきい値レベルは、ページ数に基づいて測定されていました。</p> <p>このリリースにアップグレードした後は、メモリ ページ スワッピングのしきい値をパーセンテージで測定するようにアプライアンスを設定できます。</p> <p>メモリ ページ スワッピングのデフォルトのしきい値は 10 % に設定されます。</p>
<p>暗号化されたメッセージのエンベロープ設定の変更</p>	<p>このリリースより前のリリースでは、[Security Services] > [Cisco Ironport Email Encryption] > [Add Encryption Envelope Profile] ページの [Use Encryption Applet] オプションがデフォルトで有効になっており、ブラウザ環境でメッセージの添付ファイルが開かれていました。</p> <p>このリリースにアップグレードした後は、[Security Services] > [Cisco Ironport Email Encryption] > [Add Encryption Envelope Profile] ページの [Use Encryption Applet] オプションがデフォルトで無効になります。これにより、キー サーバでメッセージの添付ファイルが復号化され、ブラウザ環境に依存せずに添付ファイルを開くことができます。</p>
<p>SSL 設定の変更</p>	<p>このリリースにアップグレードすると、TLS v1.0 方式と v1.2 方式を同時に有効にはできません。ただし、SSL 設定を行うことで、これらの方式は TLS v1.1 方式と共に有効にできます。</p>
<p>Attachment File Info コンテンツ フィルタまたはメッセージ フィルタの変更</p>	<p>次のいずれかの条件に基づいて、アプライアンスで 'Attachment File Info' コンテンツ フィルタまたはメッセージ フィルタを設定します。</p> <ul style="list-style-type: none"> • [Filename] オプションを選択して、[Does Not Equal]、[Does Not Contain]、[Does Not End With]、または [Does Not Begin] オプションを選択し、ファイル名を入力する。 • [File type] オプションを選択して、[Is not] オプションを選択し、ドロップダウン リストからファイル タイプを選択する。 • [MIME type] オプションを選択して、[Is Not] オプションを選択し、MIME タイプを入力する。 <p>アプライアンスは、上記のいずれかの条件に基づいて、添付ファイルがあるかどうかにかかわらず、メッセージに対して設定されたアクションを実行するようになりました。</p>

データ損失防止 (DLP) でサポートされる文字エンコーディングの変更	<p>データ損失防止では、中国語、日本語、韓国語のマルチバイト プレーン テキストファイルに対して、次の文字エンコーディングがサポートされるようになりました。</p> <ul style="list-style-type: none"> • 中国語(繁体字) (Big5) • 中国語(簡体字) (GB2312) • 韓国語(KS-C-5601/EUC-KR) • 日本語(Shift-JIS (X0123)) • 日本語(EUC) <p>ただし、データ損失防止 (DLP) は、次の文字エンコーディングをサポートしません。</p> <ul style="list-style-type: none"> • 日本語(ISO-2022-JP) • 韓国語(ISO2022-KR) • 中国語(簡体字) (HZGB2312)
メール ポリシー設定の変更	<p>このリリースへのアップグレード後、アプライアンスが着信メッセージと発信メッセージのメッセージ ヘッダーをチェックする際の優先順位を設定できます。最初に、アプライアンスはすべてのメール ポリシーで優先順位の最も高いメッセージ ヘッダーをチェックします。いずれのメール ポリシーとも一致するヘッダーがない場合、アプライアンスはすべてのメール ポリシーの優先順位リスト内の次のメッセージ ヘッダーを検索します。いずれのメール ポリシーとも一致するメッセージ ヘッダーがない場合は、デフォルトのメール ポリシー設定が使用されます。</p>

アップグレードの方法

- [リリース 12.5.0-066 へのアップグレード - GD\(一般導入\) \(9 ページ\)](#)
- [リリース 12.5.0-059 へのアップグレード - LD\(限定的な導入\) \(10 ページ\)](#)

リリース 12.5.0-066 へのアップグレード - GD(一般導入)

次のバージョンから、リリース 12.5.0-066 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-044
- 11.0.3-238
- 11.0.3-242
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-077

- 12.0.0-419
- 12.1.0-089
- 12.5.0-051
- 12.5.0-059

リリース 12.5.0-059 へのアップグレード - LD(限定的な導入)

次のバージョンから、リリース 12.5.0-059 にアップグレードすることができます。

- 11.0.1-027
- 11.0.2-044
- 11.0.3-242
- 11.1.1-042
- 11.1.2-023
- 11.5.0-058
- 11.5.0-071
- 11.5.0-077
- 12.0.0-419
- 12.1.0-089
- 12.5.0-051

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アプライアンス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

- すべての仮想アプライアンス モデル
- 次のハードウェア モデル: C190、C195、C380、C390、C395、C680、C690、C695、および C695F。

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 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 Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは <http://www.cisco.com/c/en/us/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が 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンス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。

仮想アプライアンスをアップグレードすると、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。 |
| ステップ 5 | 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/en/us/support/security/email-security-appliance/products-installation-guides-list.html> にある『*Cisco Content Security Virtual Appliance Installation Guide*』に記載されています。以下のサービスとサポート (17 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。

- [FIPS の準拠性 \(12 ページ\)](#)
- [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 \(12 ページ\)](#)
- [直前のリリース以外のリリースからのアップグレード \(12 ページ\)](#)
- [設定ファイル \(12 ページ\)](#)
- [アップグレード中の IPMI メッセージ \(12 ページ\)](#)

FIPS の準拠性

AsyncOS 12.5 リリースは、FIPS 準拠のリリースではありません。アプライアンスで FIPS モードを有効にしている場合は AsyncOS 12.5 にアップグレードする前に FIPS モードを無効にする必要があります。

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 C160、C360、C660、X1060、C170、C370、C670、または X1070 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ます。x60 および x70 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、x60 および x70 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。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 を使用してアプライアンス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\(15 ページ\)](#)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。
- 仮想アプライアンス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

Email Security Appliance をアップグレードするには、次の手順を実行します。

-
- ステップ 1** アプライアンスから、XML 設定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、アプライアンスからセーフリスト/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** [System Administration] タブで、[System Upgrade] ページを選択します。
 - ステップ 6** [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** [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、[Reboot Now] ボタンをクリックしてアプライアンスを再起動します。
 - 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。[System Administration] > [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 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\(14 ページ\)](#)を確認してください。

アップグレード後の注意事項

- [インテリジェント マルチスキャンおよびグレイメール グローバル設定の変更\(14 ページ\)](#)
- [AsyncOS 12.x へのアップグレード後のクラスタ レベルでの DLP 設定の不整合\(14 ページ\)](#)

インテリジェント マルチスキャンおよびグレイメール グローバル設定の変更

AsyncOS 12.1 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 レベルで設定されている場合、アプライアンス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、アプライアンスは IMS 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、アプライアンスは [maximum timeout] および [maximum message size] の値を使用して、IMS および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。

AsyncOS 12.x へのアップグレード後のクラスタ レベルでの DLP 設定の不整合

AsyncOS 12.x にアップグレードした後、アプライアンスがクラスタ モードになっていて、DLP が設定されている場合、CLI を使用して `clustercheck` コマンドを実行すると、DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次の例に示すように、`clustercheck` コマンドで「How do you want to resolve this inconsistency?」というプロンプトを使用します。

```
(Cluster)> clustercheck
Checking DLP settings...
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

パフォーマンス アドバイザリ

DLP

- 着信メッセージに対してスパム対策およびウイルス対策スキャンがすでに実行されているアプライアンスで発信メッセージの DLP を有効にすると、10 % 未満のパフォーマンス低下が発生する可能性があります。
- 発信メッセージだけを実行し、スパム対策およびウイルス対策が実行されていないアプライアンスで DLP を有効にすると、前のシナリオと比べてパフォーマンスがさらに低下する可能性があります。

SBNP

SenderBase Network Participation では、コンテキスト適応スキャン エンジン (CASE) を使用してデータを収集し、IronPort 情報サービスを駆動するようになりました。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。

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пам隔離

C シリーズまたは X シリーズのアプライアンスに対して IronPort スпам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アプライアンスの場合、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、いっばいに近いときに IronPort スпам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 \(15 ページ\)](#)
- [既知および修正済みの問題のリスト \(15 ページ\)](#)
- [既知および解決済みの問題に関する情報の検索 \(16 ページ\)](#)

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/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5&sb=af&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.0-066&sb=fr&sts=fd&svr=3nH&bt=custV

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** [Select from list] > [Security] > [Email Security] > [Cisco Email Security Appliance] の順にクリックし、[OK] をクリックします。
- ステップ 4** [Releases] フィールドに、リリースのバージョン(たとえば、11.1)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、[Show Bugs] ドロップダウンから [Affecting these Releases] を選択し、[Status] ドロップダウンから [Open] を選択します。
-



(注)

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。

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 コンテンツ セキュリティ管理	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco E メール セキュリティ	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html

マニュアルの内容 (Cisco Content Security 製品)	参照先
Cisco コンテンツ セキュリティ アプライアンスの CLI リファレンス ガイド	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco IronPort 暗号化	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

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: 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。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク ポジ図とその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2019 Cisco Systems, Inc. All rights reserved.

