AsyncOS 12.5.2 for Cisco Email Security Appliances リリースノート

発行日: 2020 年 7 月 7 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

AysncOS 12.5.2 の新機能

このリリースには複数のバグ修正が含まれています。詳細については、「既知および修正済みの問題（19 ページ）」を参照してください。

AysncOS 12.5.1 の新機能

このリリースには複数のバグ修正が含まれています。詳細については、「既知および修正済みの問題（19 ページ）」を参照してください。

AysncOS 12.5.0 の新機能

機能	説明
新しいハードウェア サポート	Cisco Email Security Appliances 用 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。 • C195 • C395 • C695 • C695F 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
高度なマルウェア防御（AMP）隔離管理の改善	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。 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。 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。

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	Cisco Sender Domain Reputation（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。 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。 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『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。
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	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。 • 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「File Reputation Filtering and File Analysis」の章を参照してください。 • CLI での `ampconfig` コマンド。『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。

外部脅威フィードの消費機能	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。 • 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。 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。 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。 **（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。 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『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。
ファイル分析に向けたしきい値の設定	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。 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 [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで、[カスタムしきい値（Custom Threshold）] として表示されます。 詳細については、ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。

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	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。 **（注）** ウォークスルーはクラウドで更新できます。How-To 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。 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。
脅威名に基づいた悪意のあるメッセージの表示	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。 詳細は、ユーザ ガイドの「Tracking Messages」の章を参照してください。
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	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。 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。 詳細は、ユーザ ガイドの「EncryptingCommunication with Other MTAs」の章を参照してください。
偽装電子メール検出の強化	[メールポリシー（Mail Policies）] > [アドレスリスト（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。 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。
ログ サブスクリプションの強化	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）内での、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。 Web インターフェイスの [システム管理（System Administration）] > [ログサブスクリプション（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。

スマート ソフトウェア ライセンシングのサポート	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。 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。 • 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。 ⚠ **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 ラインセンシング モードにロールバックすることができなくなります。 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。
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	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。 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。 • ヘッダー名を「`X-Ironport-Dmarc-Check-Result`」として追加します。 • [ヘッダー値（Header Value）] を選択して、[等しい（Equals）] を選択し、`validskip`、`invalidskip`、`temperror`、`permerror` のいずれかの値を追加します。 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。 `Quarantine_messages_DMARC_skip: if (header("X-Ironport-Dmarc-Check-Result") == "^validskip$") { quarantine("Policy"); }` 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。
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	`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。

インテリジェント マルチスキャンの強化	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 スパム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。 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。
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	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。 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。 以下の方法で最小スコアを設定します。 1. [メールポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] > [カスタム分類子設定（Custom Classifiers Settings）] セクションで、[エンティティベースのルールで推奨される最小スコアを使用（Use recommended minimum scores for entity-based rules）] チェックボックスを選択します。 2. [メールポリシー（Mail Policies）] > [DLP ポリシーのカスタマイズ（DLP Policy Customizations）] > [カスタム分類子の追加（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。 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。

動作における変更

AsyncOS 12.5.2 の動作の変更

コンテンツスキャナの変更点	アプライアンスのコンテンツスキャナは、受信および送信メッセージ内のパスワードで保護された zip 添付ファイル内の、最初にネストされたレベルでファイル名を抽出できるようになりました。

AsyncOS 12.5.1 の動作の変更

パスフレーズ設定への変更	ログインパスフレーズを自動的に生成するオプションが削除されます。選択したパスフレーズをここで手動で入力する必要があります。
データベースサイズの制限に達したときのアラートの変更	このリリースにアップグレードした後、メッセージの詳細と過去のファイルの詳細を保存するデータベース内のメッセージが 2GB のサイズに達するとアラートが送信されます。 データベースの分析と修正措置の実施については、シスコカスタマーサポートにお問い合わせください。

AsyncOS 12.5.0 の動作の変更

テキスト リソースの削除における変更	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。 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。
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	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。 `<First 225 characters of original filename+'~too_long_name~'+the last ten characters of original filename>`
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	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。 • 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	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。 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。
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	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。

ドメイン キー/DKIM 検証の設定の変更	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。 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。
USEDNS キーワードを使用した SMTP ルート設定に対する変更	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。 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。
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	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。 Web インターフェイスの [セキュリティサービス(Security Services)] > [スキャン動作(Scan Behavior)] > [グローバル設定を編集(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。 • 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。 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。
デモ証明書の変更	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。 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。 • 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
メモリ ページ スワッピングのしきい値の変更	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。 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。 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。

暗号化されたメッセージのエンベロープ設定の変更	このリリースより前のリリースでは、[セキュリティサービス（Security Services）] > [Cisco IronPort メール暗号化（Cisco Ironport Email Encryption）] > [暗号化エンベローププロファイルの追加（Add Encryption Envelope Profile）] ページの [暗号化アプレットの使用（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。 このリリースにアップグレードした後は、[セキュリティサービス（Security Services）] > [Cisco IronPort メール暗号化（Cisco Ironport Email Encryption）] > [暗号化エンベローププロファイルの追加（Add Encryption Envelope Profile）] ページの [暗号化アプレットの使用（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。
SSL 設定の変更	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。
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	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。 • [ファイル名（Filename）] オプションを選択して、[等しくない（Does Not Equal）]、[含まない（Does Not Contain）]、[次で終わらない（Does Not End With）]、または [始まらない（Does Not Begin）] オプションを選択し、ファイル名を入力する。 • [ファイルタイプ（File type）] オプションを選択して、[異なる（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 タイプ（MIME type）] オプションを選択して、[異なる（Is Not）] オプションを選択し、MIME タイプを入力する。 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。
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	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。 • 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） 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。 • 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	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るようになりました。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。

アップグレード パス

リリース 12.5.2-011 へのアップグレード（メンテナンス導入）

次のバージョンからリリース 12.5.2-011 にアップグレードできます。

- 11.0.1-027
- 11.0.2-044
- 11.0.3-242
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-071
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066

- 12.5.1-037
- 12.5.1-044

リリース 12.5.1-037 へのアップグレード（メンテナンス導入）

次のバージョンから、リリース 12.5.1-037 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
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804
- 11.1.3-009
- 11.5.0-058
- 11.5.0-071
- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-031

リリース 12.5.1-031 へのアップグレード（メンテナンス導入）

次のバージョンから、リリース 12.5.1-031 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
- 11.0.3-251
- 11.1.1-042
- 11.1.2-023
- 11.1.2-802
- 11.1.2-804

- 11.1.3-009
- 11.5.0-058
- 11.5.0-071
- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066

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
- 11.0.3-238
- 11.0.3-242
- 11.1.1-042

- 11.1.2-023
- 11.5.0-058
- 11.5.0-071
- 11.5.0-076
- 11.5.0-077
- 12.0.0-419
- 12.1.0-087
- 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 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（14 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/ja_jp/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（21 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（16 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（16 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（16 ページ）
- 設定ファイル（16 ページ）
- アップグレード中の IPMI メッセージ（16 ページ）
- TLS 1.0 での Cisco Email Encryption サービスのサポート（16 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、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

TLS 1.0 での Cisco Email Encryption サービスのサポート

TLS 1.0 での Cisco Email Encryption サービスのサポートは 2020 年 6 月までに無効化されます。Cisco Email Encryption サービスの Easy Open 機能を使用している場合は、アプライアンスを AsyncOS 12.5.1 以降のバージョンにアップグレードすることが必須です。

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（19 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（14 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（15 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 [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。[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（18 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（18 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（18 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 [最大タイムアウト（maximum timeout）] および [最大メッセージ（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 スパム隔離

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

12.5.2 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.2&sb=afr&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=12.5.2-011&sb=fr&sts=fd&svr=3nH&bt=custV

12.5.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5.1&sb=afr&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=12.5.1-037&sb=fr&sts=fd&svr=3nH&bt=custV

12.5.0 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=12.5&sb=afr&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ログイン情報でログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [E メールセキュリティ(Email Security)] > [Cisco E メールセキュリティアプライアンス(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 [リリース(Release)] フィールドに、リリースのバージョン(たとえば、12.5.1)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、[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。

（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

Cisco Content Security 製品のマニュアル	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/ja_jp/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/ja_jp/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/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 IronPort Encryption	http://www.cisco.com/c/ja_jp/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：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、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。