AsyncOS 13.0 for Cisco Email Security Appliances リリース ノート

発行日:2019 年 9 月 23 日
改訂日:2020 年 2 月 3 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
Microsoft Exchange online、Microsoft Exchange オンプレミス、ハイブリッド、およびマルチテナント展開でのメールボックス自動修復	ファイルは常に、ユーザのメールボックスに達した後であっても、悪意のあるファイルに変化する可能性があります。AMP は、新しい情報が発生する際にこの変化を識別し、アプライアンスにレトロスペクティブ アラートを送信することができます。脅威判定が変更されたときにユーザのメールボックス内のメッセージに対して自動修復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。 アプライアンスは、次のメールボックス展開のメッセージに対して自動修復アクションを実行できます。 • Microsoft Exchange Online：Microsoft Office 365 でホストされたメールボックス • Microsoft Exchange オンプレミス：ローカルの Microsoft Exchange サーバ • ハイブリッド/マルチテナント構成：Microsoft Exchange Online 展開および Microsoft Exchange オンプレミス展開で設定されたメールボックスの組み合わせ 詳細は、ユーザガイドの「Automatically Remediating Messages in Mailboxes」の章を参照してください。
SAML 2.0 を使用したシングル サインオン（SSO）	Cisco E メール セキュリティ アプライアンスは SAML 2.0 SSO をサポートするようになりました。これにより、管理ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルでアプライアンスの Web インターフェイス（レガシー Web インターフェイスおよび新しい Web インターフェイスの両方）にログインできます。 詳細については、ユーザガイドの「Single Sign-On (SSO) Using SAML 2.0」の項を参照してください。
Common Event Format（CEF）ベースのロギングのサポート	Cisco E メール セキュリティ アプライアンスは、各メッセージ イベントを 1 つのログラインにまとめる新しいタイプのログ サブスクリプションである「統合イベント ログ」をサポートするようになりました。このログサブスクリプションを使用すると、分析のためにセキュリティ情報イベント管理（SIEM）ベンダーまたはアプリケーションに送信されるデータ（ログ情報）のバイト数を減らすことができます。 統合イベントログは、ほとんどの SIEM ベンダーによって幅広く使用されている Common Event Format（CEF）ログ メッセージ形式です。 詳細は、ユーザ ガイドの「Logging」の章を参照してください。

メッセージの添付ファイルを Safe Print で出力する機能。	悪意のあるまたは疑わしいと検出されたメッセージの添付ファイルの安全なビュー（Safe Print で出力される PDF バージョン）を提供するように電子メール ゲートウェイを構成できます。メッセージの添付ファイルの安全なビューがエンド ユーザに配信され、元の添付ファイルはメッセージから削除されます。 「Safe Print」コンテンツ フィルタ アクションを使用すると、設定されたコンテンツ フィルタ条件に一致するすべてのメッセージの添付ファイルを Safe Print で出力できます。 電子メールゲートウェイでメッセージの添付ファイルを Safe Print で出力する機能は、組織が次のことを行うのに役立ちます。 • 悪意のあるコンテンツや疑わしいコンテンツを含むメッセージの添付ファイルが組織のネットワークに侵入するのを防ぎます。 • 悪意のあるメッセージや疑わしいメッセージの添付ファイルをマルウェアの影響を受けずに表示します。 • エンドユーザの要求に応じて元のメッセージ添付ファイルを配信します。 詳細については、ユーザガイドの「Configuring Email Gateway to Safe Print Message Attachments」の章を参照してください。
Cisco Threat Response ポータルへのアプライアンスの統合	Cisco Threat Response ポータルにアプライアンスを統合すると、Cisco Threat Response ポータルで次のアクションを実行することができます。 • 組織内の複数のアプライアンスからメッセージ トラッキングのデータを確認します。 • メッセージ トラッキングで検出された脅威を特定、調査、および修正します。 • 特定した脅威を迅速に解決し、特定した脅威に対して推奨されるアクションを実行します。 • ポータルで脅威をドキュメント化して調査を保存し、ポータル内の他のデバイス間で情報を共有します。 詳細については、ユーザガイドの「Integrating with Cisco Threat Response Portal」の章を参照してください。

ケースブックを使用した脅威分析の実行	Cisco E メール セキュリティ アプライアンスには、ケースブックとピボット メニューのウィジェットが含まれるようになりました。 **コメント** Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック（Casebook）] ウィジェットを使用することはできません。 [ケースブック（Casebook）] ウィジェットと [ピボット メニュー（Pivot Menu）] ウィジェットを使用して、アプライアンスで次のアクションを実行できるようになりました。 • 観測対象をケースブックに追加し、脅威分析の調査を実行します。 • 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス（エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など）の監視対象をピボットし、脅威分析のために調査します。 詳細については、ユーザガイドの「Integrating with Cisco Threat Response Portal」の章を参照してください。
機能の使用状況の統計情報を収集することによるユーザエクスペリエンスの向上	シスコ E メール セキュリティ アプライアンスでは、アプライアンスの新しい Web インターフェイスで機能やインターフェイスの使用状況の統計情報が収集されるようになり、全体的なユーザエクスペリエンスの向上に役立ちます。収集されたすべてのデータは匿名化されます。この機能の選択を解除する場合は、Web インターフェイスで**[システム管理（System Administration）] > [一般設定（General Settings）] > [使用状況分析（Usage Analytics）]** ページに移動して無効にします。 詳細については、ユーザガイドの「Collecting Usage Statistics of the Appliance on the New Web Interface」の項を参照してください。
FIPS 認定	Cisco E メール セキュリティ アプライアンスは FIPS 認定され、次の FIPS 140-2 認定の暗号化モジュールを統合しました：Cisco Common Crypto Modul（FIPS 140-2 認定番号 2984）。 ユーザガイドの「FIPS Management」の章を参照してください。
メッセージ トラッキング機能拡張	メッセージの「`Reply To`」ヘッダーに基づいてメッセージを検索できるようになりました。 詳細については、ユーザガイドの「Tracking Messages」の章を参照してください。
`trailblazerconfig` CLI コマンド	`trailblazerconfig` コマンドを使用すると、新しい Web インターフェイスで HTTPS のポートを介して受信接続と送信接続をルーティングできます。 **コメント** デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。`help trailblazerconfig` コマンドを入力すると、インライン ヘルプを参照できます。 詳細については、CLI リファレンスガイドの「trailblazerconfig」の項を参照してください。

メトリックバー ウィジェット	[メトリックバー(Metrics Bar)] ウィジェットを使用すると、[高度なマルウェア防御(Advanced Malware Protection)] レポート ページで Cisco Threat Grid アプライアンスによって実行されるファイル分析のリアルタイム データを確認できます。 詳細については、ユーザガイドの「Advanced Malware Protection Page」の項を参照してください。
IP アドレスを永続的な許可リストまたはブロックリストとして分類する機能	SSH を使用してアプライアンスにアクセスするために使用する IP アドレスを永続的な許可リストまたはブロックリストに分類することができます。アプライアンスまたは ipblockd サービスが再起動された場合、永続的なブロックリストまたは許可リストの IP アドレスは保持されます。 IP アドレスを永続的なブロックリストまたは許可リストに分類するには、CLI で `sshconfig > access` 管理サブコマンドを使用できます。 詳細については、『CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances』の「sshconfig」の項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。

レポート、隔離、およびトラッキングのための新しい Web インターフェイス	アプライアンスには、現在、次を検索および表示するための新しい Web インターフェイスがあります。 • **電子メール レポート。**次のカテゴリに基づいて [レポート（Reports）] ドロップダウンから電子メール レポートを表示できます。 – 電子メール脅威のレポート – ファイルおよびマルウェアのレポート – 接続およびフローのレポート – ユーザ レポート – フィルタのレポート 詳細については、ユーザガイドの「Email Security Monitor Pages on the New Web Interface」の章を参照してください。 • **スパム隔離** – スパムやスパムの疑いがあるメッセージを、Web インターフェイス ページの [隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] で表示および検索できるようになりました。 – セーフリストやブロックリストに追加されたドメインを、Web インターフェイスの [隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [セーフリスト（Safelist）] または [ブロックリスト（Blocklist）] ページで表示、追加、および検索できます。 詳細については、ユーザガイドの「Spam Quarantine」の章を参照してください。 • **ポリシー、ウイルスおよびアウトブレイク隔離。**ポリシー隔離、ウイルス隔離、およびアウトブレイク隔離は、Web インターフェイスの [隔離（Quarantine）] > [その他の隔離（Other Quarantine）] > [検索（Search）] ページで表示および検索できます。詳細については、ユーザガイドの「Centralized Policy, Virus, and Outbreak Quarantines」の章を参照してください。 • **メッセージ トラッキング。**メッセージまたはメッセージのグループは、検索条件に応じて Web インターフェイスの **[トラッキング（Tracking）] > [検索（Search）]** ページから検索できます。詳細は、ユーザ ガイドの「Tracking Messages」の章を参照してください。 **重要：** • アプライアンスで AsyncOS API が有効になっていることを確認してください。 • AsyncOS HTTPS API ポートが複数のインターフェイスで有効になっていないことを確認します。 • デフォルトで、`trailblazerconfig` はアプライアンスで有効になっています。 – 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。 – また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。 詳細については、新しい Web インターフェイスへのアクセス（16 ページ）を参照してください。

高度なマルウェア防御レポートの拡張機能	[高度なマルウェア防御(Advanced Malware Protection)] レポートページには、次の拡張機能が追加されています • 新しいセクション - [カテゴリ別受信マルウェアファイル(Incoming Malware Files by Category)] セクションは、[カスタム検出(Custom Detection)] に分類される、AMP for Endpoints コンソールから受信したブロックされたファイル SHA の割合を表示します。 AMP for Endpoints コンソールから取得されるブロックされたファイル SHA の脅威名は、レポートの [着信マルウェア脅威ファイル(Incoming Malware Threat Files)] セクションで [シンプルカスタム検出(Simple Custom Detection)] として表示されます。 • 新しいセクション - [カテゴリ別受信マルウェアファイル(Incoming Malware Files by Category)] セクションは、[カスタムしきい値(Custom Threshold)] に分類されるしきい値設定を基にしてブロックされたファイル SHA の割合を表示します。 • レポートの [詳細(More Details)] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブロックされたファイル SHA のファイルトラジェクトリ詳細を表示できます。 • 新しい判定 - ファイルの分析後に、ファイルに動的なコンテンツが存在しないときの新しい判定 [低リスク(Low Risk)] が導入されました。判定の詳細は、レポートの [AMPにより渡された受信ファイル(Incoming Files Handed by AMP)] セクションに表示されます。 詳細については、ユーザガイドの「Email Security Monitor Pages on the New Web Interface」の章を参照してください。

スパム対策スキャン設定の強化	新しい「アグレッシブな」スキャンプロファイルがスパム対策のグローバル設定に追加されました。このプロファイルを使用して、スパムとして検出された着信または発信メッセージに、より高いプライオリティを割り当てたり、誤検出の可能性を高めたりすることができます。 **コメント** 注：アグレッシブ スキャン プロファイルのオプションが有効になっていると、スパム対策しきい値に対するメールポリシーの調整は、通常のプロファイルスキャンが使用する場合よりも大きな影響を及ぼします。したがって、スパムの捕捉率と誤検出率との最適なバランス調整のため、既存のスパム対策メールポリシーしきい値設定を確認する必要があります。 このオプションは、次のいずれかの方法で有効化できます。 • Web インターフェイスの **[セキュリティサービス（Security Services）] > [IronPort スパム対策（IronPort Anti-Spam）] > [グローバル設定の編集（Edit Global Settings）]**。ユーザガイドの「Managing Spam and Graymail」の章を参照してください。 • CLI の `antispamconfig` コマンド。『CLI Reference Guide for AsyncOS 13.0 for Email Security Appliances』を参照してください。
How-To ウィジェットで使用可能な新しいウォークスルー	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。 このリリースでは、次のウォークスルーが追加されています。 • SAML 2.0 を使用するシングルサインオン • メールボックスの自動修復を使用したメールボックス内の悪意のあるメッセージの修復 • 悪意のあるメッセージまたは疑わしいメッセージの添付ファイルの安全なビューを提供 • 統一された Common Event Format（CEF）ロギングの設定 **コメント** ウォークスルーのリストは更新可能なクラウドです。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。 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。 各リリースでサポートされているウォークスルーの完全なリストを表示するには、『Walkthroughs Supported in AsyncOS for Cisco Email Security Appliances』を参照してください。

動作における変更

レポート ページにおける変更	このリリースでは、次のレポートが新しい Web インターフェイスで変更になりました。 • [マイダッシュボード（My Dashboard）] ページは、[マイレポート（My Reports）] に名前が変更されています。 • [受信メール（Incoming Mail）] ページは、[メールフロー概要（Mail Flow Summary）] に名前が変更されています。 • [アウトブレイク フィルタ（Outbreak Filters）] レポート ページは、[アウトブレイク フィルタリング（Outbreak Filtering）] に名前が変更されています。 • [ウイルスの種類（Virus Types）] レポート ページは、[ウイルス フィルタリング（Virus Filtering）] に名前が変更されています。 • [高度なマルウェア防御（Advanced Malware Protection）]、[AMP ファイル分析（AMP File Analysis）]、[AMP 判定のアップデート（AMP Verdict Updates）]、および [メールボックスの自動修復（Mailbox Auto Remediation）] レポート ページは、[高度なマルウェア防御（Advanced Malware Protection）] として統合されています。 • [受信メールと送信者（Incoming Mail and Outgoing Senders）] レポート ページは、[メール フローの詳細（Mail Flow Details）] として統合されています。 • [TLS 接続（TLS Connections）] レポート ページは、[TLS 暗号化（TLS Encryption）] に名前が変更されています。 • [地理的分散（Geo-Distribution）] レポート ページは、[国別接続（Connection by Country）] に名前が変更されています。 • [内部ユーザ（Internal Users）] レポート ページは、[ユーザ メールの概要（User Mail Summary）] に名前が変更されています。 • [Web インタラクション トラッキング（Web Interaction Tracking）] レポート ページは、[Web インタラクション（Web Interaction）] に名前が変更されています。 詳細については、ユーザ ガイドの「Understanding the Email Reporting Pages」のセクションを参照してください。

スパム隔離へのアクセスの変更	• 管理ユーザが、アプライアンスの新しい Web インターフェイスで [スパム隔離（Spam Quarantine）] ページにアクセスできるようになりました。 新しい Web インターフェイスで [隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] ページに移動して [スパム隔離（Spam Quarantine）] ページにアクセスできます。 • エンドユーザは、新しい Web インターフェイスのスパム隔離ポータルにアクセスできるようになりました。詳細については、新しい Web インターフェイスへのアクセス（16 ページ）を参照してください。 **重要**エンド ユーザのみがエンドユーザのスパム隔離ポータルにログインできます。ローカルおよび外部認証のユーザは、エンドユーザのスパム隔離ポータルにログインできません。 • 新しい Web インターフェイスで隔離されたメッセージを表示するためのリンクを含むスパム通知を受信します。アプライアンスで AsyncOS API HTTP/HTTPS ポートおよび HTTPS サービスが有効になっていることを確認してください。 • 他のインターフェイス（Data 1）でスパム隔離を使用している場合は、それをデフォルトのインターフェイスとして設定する必要があります。 **重要** `trailblazerconfig` が有効になっている場合は、（Data 1）インターフェイスで AsyncOS API ポート（HTTP/HTTPS）および HTTP/HTTPS サービスを有効にする必要があります。`trailblazerconfig` が無効になっている場合は、（Data 1）インターフェイスで AsyncOS API ポート（HTTP/HTTPS）を有効にする必要があります。
新しい Web インターフェイスでのクラスタのサポート	クラスタ構成の場合、レポートデータを表示し、新しい Web インターフェイス上のログインホストのみの隔離データを表示および検索できます。
Context Adaptive Scanning Engine（CASE）の強化	CASE の強化機能を次に示します。 • メッセージの添付ファイルに含まれる URL に関する追加のメッセージメタデータと情報を CASE で使用できます。 • アウトブレイクフィルタ隔離の終了スキャンにおける URL インテリジェンス使用率の向上により、フィッシングやその他の URL ベースの脅威の検出機能が向上しました。
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。 `<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>`
メールボックス自動修復機能の強化	このリリース以前は、悪意のあるメッセージに対する削除の修復アクションを設定すると、そのメッセージは [削除済みアイテム（Deleted Items）] などの特定のフォルダから削除されませんでした。 このリリースにアップグレードすると、メッセージはメールボックス内のすべてのフォルダから完全に削除されます。

AsyncOS 13.0 での API バージョンサポートへの変更	このリリースへのアップグレード後は、AsyncOS 13.0 は API バージョン 1.0 ではなくバージョン 2.0 のみをサポートします。
LDAP の接続設定の変更	アプライアンスで LDAP サーバプロファイルを作成する際、接続がリセットされる前に LDAP サーバへの接続が保持される最大時間（秒単位）を設定できるようになりました。60 ～ 86400 の間の値を選択します。 次のいずれかの方法で値を設定できます。 • Web インターフェイスで、**[システム管理（System Administration）] > [LDAP] > [LDAP サーバプロファイルを追加（Add LDAP Server Profile t ）]** の順に選択します。ユーザガイドの「Creating LDAP Server Profiles to Store Information About the LDAP Server」の項を参照してください。 • CLI の `ldapconfig` コマンドを使用します。『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。
自己署名証明書の変更	このリリースより前のリリースでは、アプライアンスは SHA-1 署名ハッシュ アルゴリズムを使用して自己署名証明書を作成していました。 このリリースへのアップグレード後、アプライアンスは SHA-256 署名ハッシュ アルゴリズムを使用して自己署名証明書を作成します。
ユーザ名の長さの変更	これよりも前のリリースでは、ユーザ名の長さは最大 16 文字に制限されていました。このリリースへのアップグレード後は、ユーザ名の長さは最大 32 文字までになります。
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。既存のデモンストレーション 次の設定で使用されている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

クロスサイト スクリプティング攻撃保護設定の変更	このリリース以前は、クロスサイト スクリプティング攻撃保護（XSS）はデフォルトで無効になっていました。 このリリースへのアップグレード後は、XSS はデフォルトで有効になります。また、CLI で `adminaccessconfig` コマンドを使用して設定を変更することもできます。
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。
SSL を使用した LDAP サーバプロファイルの変更	このリリースへのアップグレード後は、LDAP サーバプロファイルはデフォルトで SSL を使用しません。これは、セキュア LDAP が無効になっている AsyncOS バージョンからアプライアンスをアップグレードすると発生します。
DMARC 集計レポートの変更	CLI で dmarcconfig コマンドを使用して、1 日に生成できる DMARC 集約レポートの最大制限を設定できるようになりました。 1 日に生成される DMARC 集計レポートの数のデフォルト値は 1000 で、最大値は 5 万です。 メール フローへの影響を回避するため、DMARC 集計レポートの生成は、ピーク以外の時間帯にスケジュールすることを推奨します。 大量の DMARC 集計レポートを生成すると、ピーク時間帯以外の電子メール配信でわずかな遅延が発生する期間が長くなる可能性があります。
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（DLP）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。
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。
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。
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。
URL 無効化アクションの変更	このリリース以前は、URL に対して無効化アクションを適用すると、URL はクリックできなくなりますが、URL のコピーは表示できました。 このリリースへのアップグレード後は、URL に対して無効化または置換アクションを適用すると、条件に一致する URL はハイパーリンクから完全に削除されます。 **コメント** URL をクリックできないように電子メールクライアントの自動フォーマット設定が無効になっていることを確認します。
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。

新しい Web インターフェイスとレガシー Web インターフェイスの比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	アプライアンスにログインすると、[メールフロー概要(Mail Flow Summary)] ページが表示されます。	アプライアンスにログインすると、[マイダッシュボード(My Dashboard)] ページが表示されます。
レポート ドロップダウン	[レポート(Reports)] ドロップダウンで、アプライアンスのレポートを表示できます。	[モニタ(Monitor)] メニューで、アプライアンスのレポートを表示できます。
マイレポート	[レポート(Reports)] ドロップダウンから **[マイレポート(My Reports)]** を選択します。	[マイレポート(My Reports)] ページは、[モニタ(Monitor)] > [マイダッシュボード(My Dashboard)] から表示できます。
メールフロー概要	[メールフロー概要(Mail Flow Summary)] ページには、着信および送信メッセージに関するトレンド グラフやサマリー テーブルが表示されます。	[受信メール(Incoming Mail)] には、着信および発信メッセージに関するグラフやサマリー テーブルが含まれます。
高度なマルウェア防御 レポート ページ	[レポート(Reports)] ドロップダウンメニューの [高度なマルウェア防御(Advanced Malware Protection)] レポートページでは、次のセクションを使用できます。 • [概要(Overview)] • [AMP ファイル レピュテーション(AMP File Reputation)] • [ファイル分析(File Analysis)] • [ファイル レトロスペクション(File Retrospection)] • [メールボックスの自動修復(Mailbox Auto Remediation)]	アプライアンスの **[モニタ(Monitor)]** メニューには、次の [高度なマルウェア防御(Advanced Malware Protection)] レポートページがあります。 • [高度なマルウェア防御(Advanced Malware Protection)] • [AMP ファイル分析(AMP File Analysis)] • [AMP判定のアップデート(AMP Verdict Updates)] • [メールボックスの自動修復(Mailbox Auto Remediation)]
アウトブレイク フィルタ ページ	新しい Web インターフェイスの [アウトブレイクフィルタリング(Outbreak Filtering)] レポートページでは、[過去1年間のウイルスアウトブレイク(Past Year Virus Outbreaks)] および [過去1年間のウイルスアウトブレイクの概要(Past Year Virus Outbreak Summary)] は使用できません。	[モニタ(Monitor)] > [アウトブレイクフィルタ(Outbreak Filters)] ページには、[過去1年間のウイルスアウトブレイク(Past Year Virus Outbreaks)] および [過去1年間のウイルスアウトブレイクの概要(Past Year Virus Outbreak Summary)] が表示されます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
スパム隔離(管理者およびエンドユーザ)	新しい Web インターフェイスで [隔離(Quarantine)] > [スパム隔離(Spam Quarantine)] > [検索(Search)] をクリックして [スパム隔離(Spam Quarantine)] ページにアクセスします。 新しい Web インターフェイスでのスパム隔離ポータルへのエンドユーザのアクセスの詳細については、新しい Web インターフェイスへのアクセス(16 ページ)を参照してください。	スパム隔離は、**[モニタ(Monitor)] > [スパム隔離(Spam Quarantine)]** メニューから表示できます。
ポリシー、ウイルスおよびアウトブレイク隔離	新しい Web インターフェイスで [隔離(Quarantine)] > [その他の隔離(Other Quarantine)] をクリックします。 アプライアンス上でポリシー、ウイルス、およびアウトブレイク隔離のみを表示できます。	アプライアンスでは、**[モニタ(Monitor)] > [ポリシー、ウイルス、およびアウトブレイク隔離(Policy, Virus and Outbreak Quarantines)]** を使用して、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。
隔離内のメッセージに対するすべてのアクションの選択	隔離で複数(またはすべて)のメッセージを選択し、削除、遅延、リリース、移動などのメッセージアクションを実行できます。	隔離で複数のメッセージを選択して、メッセージアクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-
拒否された接続	拒否された接続を検索するには、アプライアンスで **[トラッキング(Tracking)] > [検索(Search)] > [拒否された接続(Rejected Connection)]** タブをクリックします。	-
クエリタイムアウト	アプライアンスでは、メッセージトラッキング機能の **[クエリタイムアウト(Query timeout)]** フィールドは使用できません。	メッセージトラッキング機能の [クエリ設定(Query Settings)] フィールドで、クエリのタイムアウトを設定できます。
有効なメッセージ トラッキング データ	[有効なメッセージトラッキングデータ(Message Tracking Data Availability)] ページにアクセスするには、Web インターフェイスのページの右上にある歯車アイコンをクリックします。	アプライアンスの欠落データインターバルを表示することができます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
判定チャートと最後の状態の判定	判定チャートに、アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	アプライアンスでは、メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致の詳細は、アプライアンスでは、[メッセージの詳細（Message Details）] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致の詳細は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。
メッセージの方向（受信または送信）	メッセージの方向（受信または送信）は、アプライアンスのメッセージトラッキング結果ページに表示されます。	メッセージの方向（受信または送信）は、メッセージ トラッキング結果ページには表示されません。

新しい Web インターフェイスへのアクセス

新しい Web インターフェイスでは、新しいレポートのモニタリング、隔離、およびメッセージの検索が可能です。

前提条件

- アプライアンスの新しい Web インターフェイスは、AsyncOS API HTTP/HTTPS ポート（6080/6443）および trailblazer HTTPS ポート（4431）を使用します。4431 以外のカスタムポートで trailblazer を有効にするには、CLI で `trailblazerconfig enable <port number>` コマンドを使用します。
- また、対応するファイアウォールルールとプロキシルールを変更して、ポートにアクセスできるようにする必要もあります。trailblazer HTTPS ポートがファイアウォールで開かれていることを確認します。
- **[ネットワーク（Network）] > [IP インターフェイス（IP Interfaces ｔ）]** で AsyncOS API HTTP と AsyncOS API HTTPS ポートが有効になっていることを確認します。デフォルトの AsyncOS API HTTP/HTTPS ポートは 6080/6443 です。

新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

- `trailblazerconfig` CLI コマンドが有効になっている場合は、`https://example.com:<trailblazer-https-port>/ng-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている trailblazer の HTTPS ポートです。

- アプライアンスにログインし、**[新しくなった E メール セキュリティ アプライアンスをお試しくださいお試しください。(Security Management Appliance is getting a new look. Try it !)]** をクリックして、新しい Web インターフェイスに移動します。

新しい Web インターフェイスは新しいブラウザウィンドウで開きます。それにアクセスするには、再度ログインする必要があります。アプライアンスから完全にログアウトする場合は、アプライアンスの新しい Web インターフェイスとレガシー Web インターフェイスの両方からログアウトする必要があります。

HTML ページのシームレスなナビゲーションとレンダリングのために、次のブラウザを使用してアプライアンスの新しい Web インターフェイス(AsyncOS 13.0 以降)にアクセスすることをお勧めします。

- Google Chrome(最新の安定バージョン)
- Mozilla Firefox(最新の安定バージョン)

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス(AsyncOS 13.0 以降)でサポートされている解像度は、1280 X 800 ～ 1680 X 1050 です。すべてのブラウザに対して最適に表示される解像度は 1440x900 です。

コメント シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

エンドユーザは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできます。

コメント エンドユーザは、インターフェイス ポート 82/83 を使用して新しい Web インターフェイスのスパム隔離ポータルにログインすることはできません。

- `trailblazerconfig` CLI コマンドが有効になっているときに、`https://example.com:<trailblazer-https-port>/euq-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている先駆者の HTTPS ポートです。

アップグレード パス

リリース 13.0.0-392 へのアップグレード - GD(全面導入)

次のバージョンから、リリース 13.0.0-392 にアップグレードすることができます。

- 11.0.3-238
- 11.0.3-242
- 11.0.3-251

- 11.1.0-135
- 11.1.2-023
- 11.1.3-009
- 11.5.0-076
- 12.0.0-419
- 12.1.0-071
- 12.1.0-087
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-031
- 12.5.1-037
- 13.0.0-314
- 13.0.0-375

リリース 13.0.0-375 へのアップグレード - LD（限定的な導入）更新

次のバージョンから、リリース 13.0.0-375 にアップグレードすることができます。

- 11.0.0-274
- 11.1.3-009
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-031
- 12.5.1-037
- 13.0.0-314

リリース 13.0.0-314 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 13.0.0-314 にアップグレードすることができます。

- 11.1.3-009
- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066

- 13.0.0-252
- 13.0.0-285
- 13.0.0-305

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
- C190、C195、C390、C395、C690、C695、および C695F のハードウェアモデル。

  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
- 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 (19 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 (29 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 モードの AsyncOS の以前のバージョンから FIPS モードの AsyncOS 13.0 へのアップグレード (21 ページ)
- AsyncOS 11.x から AsyncOS 13.x へのアップグレード (21 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 (23 ページ)
- FIPS の準拠性 (23 ページ)
- AsyncOS の以前のバージョンへの復元 (23 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 (23 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 (23 ページ)
- 設定ファイル (24 ページ)
- アップグレード中の IPMI メッセージ (24 ページ)
- メールボックス自動修復 (MAR) 設定時の変更 (24 ページ)
- TLS 1.0 での Cisco Email Encryption サービスのサポート (24 ページ)

FIPS モードの AsyncOS の以前のバージョンから FIPS モードの AsyncOS 13.0 へのアップグレード

集中型のポリシー、ウイルス、アウトブレイク検疫が有効になっている状態で FIPS モードのアプライアンスをアップグレードすると、アップグレード後に集中型のポリシー、ウイルス、アウトブレイク隔離が無効になります。集中型のポリシー、ウイルス、アウトブレイク検疫は、電子メール向け AsyncOS 13.0 で FIPS が変更されたため無効になっています。電子メール向け AsyncOS 13.0 以降では、FIPS モードのアプライアンスは、2048 ビットサイズの証明書を使用して、集中型のポリシー、ウイルス、アウトブレイク検疫を有効にします。以前の AsyncOS バージョンには、サイズが 1024 ビットの証明書があります。

集中型のポリシー、ウイルス、アウトブレイク検疫を有効にする手順は次のとおりです。

ステップ 1 Cisco セキュリティコンテンツ管理アプライアンスを AsyncOS 13.0 にアップグレードします。

ステップ 2 Cisco E メール セキュリティ アプライアンスを AsyncOS 13.0 にアップグレードします。

アップグレード後、ポリシー、ウイルス、およびアウトブレイク検疫の集中型設定が無効になります。

ステップ 3 アップグレードした AysncOS 13.0 の Cisco セキュリティ コンテンツ管理アプライアンスで CLI コマンド *updatepvocert* を実行します。
集中型のポリシー、ウィルス、およびアウトブレイク検疫の CA 証明書は 2048 ビットに更新されます。

ステップ 4 アップグレードした AysncOS 13.0 Cisco E メール セキュリティで、集中型のポリシー、ウイルス、アウトブレイク検疫が有効になっているかどうかを確認します。詳細については『*Cisco Security Content Management Appliance User Guide*』を参照してください。

AsyncOS 11.x から AsyncOS 13.x へのアップグレード

アプライアンスがクラスタ環境内にあり、ホストキー検証に SSH DSS キーを使用している場合は、AsyncOS 11.x から 13.x にアップグレードした後、クラスタ通信が失敗します。ホストキーを検証するには、アプライアンスに SSH RSA キーを追加する必要があります。

注 クラスタマシンでホストキー検証に SSH RSA キーを使用している場合、クラスタ通信は失敗しません。

ステップ 1 クラスタ内のすべてのアプライアンスで使用されている SSH DSS キーを削除する手順は次のとおりです。

a. CLI を使用してクラスタ内のいずれかのアプライアンスにログインします。

b. *logconfig* コマンドを入力します。次の例では *logconfig* コマンドを使用して SSH DSS ホストキーを削除しています。

```
mail1.example.com:
logconfigChoose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.-
DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
```

```
[]> hostkeyconfig
Currently installed host keys:
1. 10.10.2.21 ssh-dss AAAAB3NzaC1kc3MAAACBAKW24h8U6GiAu+5...D9D66DqZM=
2. 10.10.2.28 ssh-dss AAAAB3NzaC1yc2EAAAADAQABAAABAQC+bgQ...J2jsmTC2i=
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]> delete
Enter the number of the key you wish to delete.
[]> 1
Currently installed host keys:
1. 10.10.2.28 ssh-dss AAAAB3NzaC1yc2EAAAADAQABAAABAQC+bgQ...J2jsmTC2i=
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display system host keys.
- FINGERPRINT - Display system host key fingerprints.
- USER - Display system user keys.
[]>
```

c. クラスタ内に含まれる他のすべてのアプライアンスに対してステップ a ～ b を繰り返します。

ステップ 2 クラスタ内に含まれるアプライアンスの現在の設定を保存します。

ステップ 3 すべてのマシンをクラスタから接続解除します。

ステップ 4 各マシンを AsyncOS 11.x から 13.x へ個別にアップグレードします

ステップ 5 次の手順でいずれかのマシンを再度クラスタに接続し、SSH RSA ホストキーを追加します。

a. CLI を使用してクラスタ内のいずれかのアプライアンスにログインします。

b. `clusterconfig` コマンドを入力します。
次の例では `clusterconfig` コマンドを使用して、最初のマシンを再度クラスタに接続し、SSH RSA ホストキーを追加しています。

```
(Machine mail1.example.com) [Disconnected]> clusterconfig
This command is restricted to "cluster" mode. Would you like to switch to "cluster"
mode? [Y] > Y
This machine (mail.example.com) is currently disconnected from the cluster.
Do you want to reconnect to the cluster? [Y] > Y
This machine (mail.example.com) is not able to communicate with the cluster.
Host keys need to be updated
Continue? [Y] > Y
Is this the first machine being connected back into the cluster? [N] > Y
Host keys updated successfully....
Commit sent to 1 of 2 machines. 詳細情報を確認するには、「commitdetail」コマンドを実行します。
```

c. クラスタ内に含まれる他のすべてのアプライアンスに対してステップ a ～ b を繰り返します。

ステップ 6 クラスタ内のいずれかのマシンにログインし、他のすべてのマシンをクラスタに再接続します。

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 13.0 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 13.0 GD は FIPS 認定され、次の FIPS 140-2 認定の暗号化モジュールを統合しました: Cisco Common Crypto Modul（FIPS 140-2 認定番号 2984）。

AsyncOS の以前のバージョンへの復元

次の AsyncOS バージョンは、内部テスト インターフェイスの脆弱性（http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa）の影響を受けます。

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047
- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

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、C380、C680、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、x70、および 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、x60、x70、および 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

メールボックス自動修復（MAR）設定時の変更

お使いのアプライアンスですでに MAR が設定されている場合は、アップグレードする前に Microsoft Azure ポータルでお使いのアプリケーションのアクセス許可を Outlook API から Graph API に変更してください。

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（27 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（19 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（19 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（26 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

FIPS モードの AsyncOS 13.0 でのポリシー、ウイルス、およびアウトブレイク検疫の集中型設定の有効化

非 FIPS モードの以前のバージョンの AsyncOS から AsyncOS 13.0 にアップグレードしても、アプライアンスはポリシー、ウイルス、およびアウトブレイク検疫の集中型設定を保持します。アップグレード後、FIPS モードを有効にすると、ポリシー、ウイルス、およびアウトブレイク検疫の集中型設定が自動的に無効になります。AsyncOS 13.0 以降では、FIPS モードのアプライアンスは 2048 ビットの CA 証明書を使用してポリシー、ウイルス、およびアウトブレイク検疫の集中型設定を有効にするため、ポリシー、ウイルス、およびアウトブレイク検疫の集中型設定は無効になっています。以前の AsyncOS バージョンには、1024ビットの CA 証明書があります。

ポリシー、ウィルス、およびアウトブレイク検疫の集中型設定を有効にするには、FIPS モードの AsyncOS の以前のバージョンから FIPS モードの AsyncOS 13.0 へのアップグレード（21 ページ）を参照してください。

AsyncOS 13.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 13.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]>
```

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 13.0 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。

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（27 ページ）
- 既知および修正済みの問題のリスト（27 ページ）
- 既知および解決済みの問題に関する情報の検索（27 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=13.0&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=13.0&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 [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（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、[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

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/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。