AsyncOS 11.0.4 for Cisco Email Security Appliances リリースノート

発行日:2021 年 3 月 24 日
改訂日:2021 年 9 月 16 日

目次

今回のリリースでの変更点

AsyncOS 11.0.4 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(23 ページ)」を参照してください。

Cisco Systems, Inc.
www.cisco.com

AsyncOS 11.0.3 の新機能

機能	説明
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。

AsyncOS 11.0.2 の新機能

機能	説明
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 > accesscontrol` コマンドを使用できます。 詳細については、『CLI Reference Guide for AsyncOS 11.0 for Email Security Appliances』の「*sshconfig*」の項を参照してください。
ファイルのレピュテーション サービス用に APJC 地域に追加された新しいデータセンター	シスコはファイルのレピュテーション サービス用に APJC 地域に次の新しいデータセンターを追加しました。 *APJC (cloud-sa.apjc.amp.cisco.com)* 新しいファイル レピュテーション サービスを使用するように、E メール セキュリティ アプライアンスを設定できます。詳細については、ユーザー ガイドまたはオンライン ヘルプの「File Reputation Filtering and File Analysis」の章を参照してください。

AsyncOS 11.0 の新機能

機能	説明
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#1643）。 ユーザー ガイドまたはオンライン ヘルプで「FIPS Management」の章を参照してください。
新しいデータ漏洩防止（DLP）ソリューション	RSA は、RSA Data Loss Prevention Suite のサポート終了（EOL）を発表しました。詳細については、https://community.rsa.com/docs/DOC-59316 を参照してください。 シスコは、RSA DLP で作成されたすべての既存の DLP ポリシーを新しい DLP エンジンへとシームレスに移行できる、代替の DLP ソリューションを提供します。アップグレード後は、Web インターフェイスの、[メールポリシー（Mail Policies）] > [DLP ポリシーマネージャ（DLP Policy Manager）] ページで、移行した DLP ポリシーを表示または変更できます。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。 **（注）** Async0S 11.0 以降は、RSA Enterprise Manager の統合のサポートはありません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。
二要素認証のサポート	Cisco E メール セキュリティ アプライアンスで、アプライアンスにログインするときにセキュアなアクセスを保証する二要素認証をサポートするようになりました。 標準の RFC に準拠している任意の標準 RADIUS サーバーを介してアプライアンスの二要素認証を設定できます。 次のいずれかの方法で、二要素認証を有効化できます。 • Web インターフェイスの [システム管理（System Administration）] > [ユーザ（Users）] ページ。ユーザー ガイドの「Distributing Administrative Tasks」の章を参照してください。 • CLI の `userconfig` > `twofactorauth` コマンド。『CLI *Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。 アプライアンスで二要素認証を有効にしている場合は、事前共有キーを使用してクラスタ マシンに参加させることができます。CLI の `clusterconfig > prepjoin` コマンドを使用して、この設定を構成します。ユーザー ガイドの「Centralized Management Using Clusters」の章を参照してください。

サービス エンジンの以前のバージョンへの手動でのロールバック	次の場合、現在のエンジンを以前のバージョンへ手動でロールバックできます。 • エンジンの更新プログラムに不具合がある。 • エンジンが適切に機能しない。 現在、次のエンジンに対し、エンジンのロールバックを実行できます。 • McAfee • Sophos • Graymail クラスタ レベルではなく、マシン レベルでのみ、エンジンのロールバックを実行できます。 Web インターフェイスで [セキュリティサービス（Security Services）] > [サービスの概要（Services Overview）] ページを使用して、次のことを実行できます。 • サービス エンジンの以前のバージョンにロールバックします。 • 手動でサービス エンジンを必要なバージョンに更新します。 詳細については、ユーザー ガイドの「System Administration」の章を参照してください。

受信メールの接続および異なる地理的な場所からの受信または送信メッセージの処理	Cisco E メール セキュリティ アプライアンスでは、受信メールの接続および特定の地理的な場所からの受信または送信メッセージの処理と、それらに対する適切なアクションの実行が可能になりました。たとえば次のものです。 • 特定の地域から来るメールの脅威を防ぐ。 • 特定の地域から来るメールを許可または禁止する。 この機能は次のようにして使用できます。 • **SMTP 接続レベル。**次の方法のいずれかを使用して、特定の地域からの受信メール接続を処理するために、送信者グループを設定できるようになりました。 – Web インターフェイスの、[メールポリシー(Mail Policies)] > [HAT 概要(HAT Overview)] > [送信者グループの追加(Add Sender Group)] > [送信者を追加設定(Submit and Add Senders)] > [位置情報(Geolocation)] オプション。 – CLI の `listenerconfig > hostaccess > country` コマンド。 詳細は、ユーザー ガイドの「Defining Which Hosts Are Allowed to Connect Using the Host Access Table (HAT)」の章または『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。 [地理的分散(Geo Distribution)] レポートを使用して、特定の地域からの受信メール接続の詳細を送信者の出身国に基づいて表示できます。詳細については、ユーザー ガイドの「Using Email Security Monitor」の章を参照してください。 • **コンテンツまたはメッセージ フィルタ レベル**:コンテンツまたはメッセージ フィルタを作成し、特定の地域からの受信または送信メッセージの処理、およびそのようなメッセージに対する適切なアクションを実行できます。コンテンツおよびメッセージ フィルタには、次の新しいオプションが含まれます。 – 新しいコンテンツ フィルタ条件:**地理位置情報** – 新しいメッセージ フィルタ ルール:`geolocation-rule()`。 詳細については、ユーザー ガイドの「Content Filters」または「Using Message Filters to enforce Email Policies」の章を参照してください。 [コンテンツフィルタ(Content Filters)] および [メッセージフィルタ(Message Filters)] レポートを使用して、コンテンツまたはメッセージ フィルタによって検出される、特定の位置情報からの受信または送信メッセージの詳細を表示できます。詳細については、ユーザー ガイドの「Using Email Security Monitor」の章を参照してください。 メッセージ トラッキングを使用すると、コンテンツまたはメッセージ フィルタによって検出される特定の位置情報から着信したメッセージを検索することができます。メッセージ トラッキングの [詳細設定(Advanced)] セクションで [メッセージ イベント(Message Event)] オプションに **位置情報**フィルタを使用します。 国の地理位置情報のリストはクラウドでの更新が可能です。

AMP エンジンを使用した送信メッセージのスキャン	AMP エンジンを使用して送信メッセージをスキャンするアプライアンスを設定できるようになりました。 この機能を使用して次のことができます。 • ユーザが組織のネットワークから、IP またはドメイン レピュテーションの低下につながる恐れのある、悪意のあるメッセージの送信を防ぎます。 • 悪意のある添付ファイルを含むメッセージを送信しているユーザを追跡し、それらに対して適切なアクションを実行します。 次の方法のいずれかで、アプライアンスの送信メール ポリシーを設定し、AMP エンジンによるメッセージ スキャンを許可できます。 • Web インターフェイスの [メールポリシー(Mail Policies)] > [送信メールポリシー(Outgoing Mail Policies)] ページ。ユーザー 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 の `policyconfig` コマンド。 AMP エンジンによってスキャンされた発信メッセージの詳細を表示する、次のレポートが拡張されました。 [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)] • [概要(Overview)] ページ • [送信先(Outgoing Destinations)] • [送信者(Outgoing Senders)] • [内部ユーザ(Internal Users)] ユーザー ガイドの「Using Email Security Monitor」の章を参照してください。 [メッセージトラッキング(Message Tracking)] > [メッセージイベント(Message Event)] > [高度なマルウェア防御(Advanced Malware Protection)] オプションの [メールフローの方向(Mail Flow Direction)] フィルタを使用して、AMP エンジンによってスキャンされる受信および送信メッセージを検索できます。

自動更新の有効化または無効化	次のサービス エンジンの [グローバル設定(Global Settings)] ページで自動更新を有効または無効にできるようになりました。 • McAfee • Sophos • Graymail 特定のサービス エンジンの自動更新が無効な場合に、定期的にアラートを受信できるようになりました。次のいずれかの方法で、既存のアラート間隔を変更できます。 • Web インターフェイスの、[セキュリティサービス(Security Services)] > [サービスのアップデート(Service Updates)] > [無効な自動エンジン更新のアラート間隔(Alert Interval for Disabled Automatic Engine Updates)]。ユーザー ガイドの「System Administration」の章を参照してください。 • CLI の `updateconfig` コマンド。
メール ポリシーの高度なマルウェア防御によって検出された添付ファイルに関する追加操作の実行	添付ファイルが、受信または送信メール ポリシーの [高度なマルウェア防御(Advanced Malware Protection)] セクションで、「悪意がある」、「スキャン不可」または「ファイル分析のために送信された」とみなされる場合、次の追加操作を実行できます。 • メッセージの受信者の変更 • 代替宛先ホストへメッセージを送信します。 詳細については、ユーザー ガイドの「File Reputation Filtering and File Analysis」を参照してください。
AMP エンジン ログの改善	次のシナリオについての情報が、AMP エンジンのログに記録されるようになりました。 • ファイル分析サーバにアップロードされないファイル。 • アプライアンスでファイル分析サーバへの日単位のファイルのアップロード制限を超えたために、ファイル分析がスキップされたファイル。 • スキャン不可とマークされているファイル。

コンテンツ スキャンでサポートされるアーカイブ ファイル形式	アプライアンスのコンテンツ スキャナでは、次のアーカイブ ファイル形式でコンテンツ スキャンを実行できます。 • ACE アーカイブ • ALZ アーカイブ • Apple ディスク イメージ • ARJ アーカイブ • bzip2 アーカイブ • EGG アーカイブ • GNU Zip • ISO ディスク イメージ • Java アーカイブ • LZH • Microsoft キャビネット アーカイブ • RAR マルチパート ファイル • RedHat パッケージ マネージャ アーカイブ • Roshal アーカイブ（RAR） • UNIX AR アーカイブ • UNIX 圧縮アーカイブ • UNIX cpio • UNIX Tar • XZ アーカイブ • ZIP アーカイブ • 7-Zip
マクロ検出の強化	次のファイルのマクロを検出できるようになりました。 • Adobe Acrobat ポータブル ドキュメント フォーマット（PDF）ファイル内の JavaScript マクロ。 • Microsoft Office ファイル（Open XML）と OLE ファイルの Visual Basic for Applications（VBA）マクロ。 詳細については、ユーザー ガイドの「Content Filters」または「Using message Filters to Enforce Email Policies」の章を参照してください。

Web インターフェイス ログインの CRL チェック	次の方法のいずれかを使用して Web インターフェイス ログインの CRL チェックを設定できます。 • Web インターフェイスの [ネットワーク(Network)] > [CRL ソース(CRL Sources)] > [設定の編集(Edit Settings)] > [WebUI のCRL チェック(CRL check for WebUI)] オプション。ユーザー ガイドの「Authenticating SMTP Sessions Using Client Certificates」の章を参照してください。 • CLI の `certconfig > crl` コマンド このオプションが有効で、証明書が失効した場合、次のことが起こります。 • 証明書が失効したことを示すアラートを受信します。 • アプライアンスの Web インターフェイスにアクセスすることはできません。ただし、CLI を使用してアプライアンスにログインすることはできます。 アプライアンスの Web インターフェイスにアクセスできるように、CLI を介して有効な証明書をインポートし、設定する必要があります。『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。
ファイル レピュテーション判定結果値のキャッシュ有効期間の設定。	ファイル レピュテーションの判定結果値のキャッシュ有効期間は、次の方法のいずれかで設定できます。 • Web インターフェイスの [セキュリティサービス(Security Services)] > [ファイルレピュテーションと分析(File Reputation and Analysis)] > [キャッシュ設定(Cache Settings)] ページ。 • CLI の `ampconfig > cachesettings > modifytimeout` コマンド。
ファイルのレピュテーションとファイルの分析サービス用にヨーロッパ地域に追加された新しいデータセンター	シスコはファイルのレピュテーションとファイルの分析サービス用に、ヨーロッパ地域に新しいデータセンターを追加しました。 • ファイル レピュテーション サーバー用の EUROPE (cloud-sa.eu.amp.cisco.com) • ファイル分析サーバー用の EUROPE (https://panacea.threatgrid.eu) 新しいファイルのレピュテーションとファイルの分析サービスを使用するように、E メール セキュリティ アプライアンスを設定できます。詳細については、ユーザー ガイドの「File Reputation Filtering and File Analysis」を参照してください。

動作における変更

AsyncOS 11.0.3 の動作の変更

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>`
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。

AsyncOS 11.0.2 の動作の変更

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。
グレイメールの URL 書き換えの変更	アプライアンスでグレイメールと安全な配信停止が有効になっている場合、アプライアンスは、長さが 2000 文字未満の元の配信停止 URL のみを書き換えます。
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。
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。

AsyncOS 11.0 の動作の変更

RSA Enterprise Manager はサポート対象外	このリリースにアップグレードした後は、RSA Enterprise Manager はサポートされません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。
マシン レベルでのみ実行される DLP の更新	このリリースより前は、DLP の更新は、DLP が設定されたレベルで実行されていました。たとえば、DLP がクラスタ レベルで設定されている場合は、DLP の更新もそのレベルで実行されていました。 このリリースにアップグレードした後は、DLP の更新は、DLP がクラスタ、マシンまたはグループ レベルのいずれで設定されているかに関係なく、マシン レベルでのみ実行されます。
以前のバージョンの DLP エンジンおよびコンテンツ照合分類子へのロールバックの廃止	このリリースの前までは、アプライアンス上の DLP エンジンとコンテンツ照合分類子を以前のバージョンにロールバック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、アプライアンス上の DLP エンジンとコンテンツ照合分類子の以前のバージョンにロールバックすることはできなくなります。
米国運転免許証分類子の変更	このリリースより前は、Web インターフェイスの [メールポリシー(Mail Policies)] > [DLP ポリシーマネージャ(DLP Policy Manager)] > [詳細設定(Advance Settings)] ページで [米国運転免許証(US Drivers License)] 分類子フィールドを表示できました。この分類子を使用して、作成した DLP ポリシーに一致する特定の米国の州を選択または選択解除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、Web インターフェイスの [メールポリシー(Mail Policies)] > [DLP ポリシーマネージャ(DLP Policy Manager)] > [詳細設定(Advance Settings)] ページの [米国運転免許証(US Drivers License)] 分類子フィールドは使用できなくなります。作成した DLP ポリシーに一致する特定の米国の州を選択または選択解除することはできなくなります。デフォルトで、米国運転免許証分類子が米国で発行されたすべての運転免許証を検索するようになりました。
デフォルトの重大度スケール値の変更	このリリースより前は、重大度のスケール値は、デフォルトではすべてのポリシーで同じで、ポリシーごとに調整できるようになっていました。 このリリースにアップグレードした後は、デフォルトの重大度スケール値はポリシーごとに異なるようになります。
パスフレーズのリセットの変更	管理者(ユーザー)は、ロックされたユーザー アカウントのパスフレーズをシリアル コンソール ポートを介してリセットできるようになりました。 すべてのロックされた管理(ユーザー)アカウントは、パスフレーズが管理者(ユーザー)によって変更された後にのみロック解除できます。
正規表現を追加するための新しい構文	Perl 互換正規表現(PCRE)構文を使用して、コンテンツ照合分類子または DLP ポリシー テンプレート用の正規表現を追加できるようになりました。

LDAP サーバー証明書の検証	LDAP サーバー証明書を検証するには、次のいずれかの方法を使用します。 • Web インターフェイスの [システム管理(System Administration)] > [LDAP] > [LDAP 設定を編集(Edit LDAP Settings)] ページ • CLI の `ldapconfig` > `setup` コマンド。
クラウド ドメイン パラメータの変更	このリリースより前は、Web インターフェイスまたは CLI を使用してクラウド ドメイン パラメータを設定できました。 このリリースにアップグレードした後は、Web インターフェイスまたは CLI を使用してクラウド ドメイン パラメータを設定することはできなくなります。
最大 HTTP ヘッダー サイズの設定	アプライアンスに送信される HTTP 要求の HTTP ヘッダーの最大サイズを設定するため、CLI で `adminaccessconfig > maxhttpheaderfieldsize` コマンドを使用できます。 HTTP ヘッダー フィールドのサイズの既定値は 4096(4 KB)、最大値は 33554432(32 MB)です。
クラスタ通信中のホスト キー検証の変更。	クラスタ通信中のホスト キーの検証は SSH-RSA のみに基づいて実行されるようになりました。 詳細については、クラスタ通信と SCP プッシュのための SSH-RSA キー(20 ページ)を参照してください。
アンチウイルス アラート タイプおよび高度なマルウェア防御アラート タイプのアラート重大度を個別に選択する機能	Web インターフェイスまたは CLI で、アンチウイルス アラート タイプおよび高度なマルウェア防御アラート タイプのアラート重大度を個別に選択できるようになりました。
アンチスパムの新しいデフォルトのメッセージ スキャンしきい値	次に、アンチスパム エンジンを介してメッセージをスキャンするための新しいデフォルトしきい値を示します。 • サイズが 1 MB より小さいメッセージは、アンチスパム エンジンによってスキャンされます。 • サイズが 2 MB を超えるメッセージは、アンチスパム エンジンによってスキャンされません。
ユーザー名の長さの変更	これよりも前のリリースでは、ユーザー名の長さは最大 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、ユーザー名の長さは最大 32 文字までになります。

コンテンツ スキャンの変更	コンテンツ スキャナがフル コンテンツ スキャンに割り当てられたメモリ使用量を超えた場合、アプライアンス内のコンテンツ スキャナが Microsoft Excel 添付ファイルに対し部分的なスキャンを実行するようになりました。部分的なスキャンでは、Microsoft Excel 添付ファイル内の数字、日付、および重複する内容のスキャンがスキップされます。 部分的なスキャンであることを示すため、スキャンされたメッセージには `X-Attachment-Scan = Partial` ヘッダーが追加されます。このようなメッセージに対して適切なアクションを実行するには、`X-Attachment-Scan = Partial` ヘッダーを検出するメッセージ フィルタまたはコンテンツ フィルタを使用します。 次に、メッセージ フィルタを使用して、部分的にスキャンされたメッセージを検出および隔離する例を示します。 *`PartialContentScan: if (header("X-Attachment-Scan") == "^partial$") {quarantine("Policy");}`*
偽装メールの検出の変更	このリリースより前は、偽造メッセージの検出には、メッセージの From: ヘッダー内のユーザーの名前およびユーザー ID が使用されていました。 このリリースにアップグレードした後は、偽造メッセージの検出には、メッセージの From: ヘッダー内のユーザーの名前だけが使用されるようになります。 次の例では、偽装メッセージの検出に、ユーザーの名前（Jim Ross）のみを使用しています。 Jim Ross <jimr@example.com> メッセージの From: ヘッダーに電子メール アドレス（jimr@example.com）のみが含まれている場合は、偽装メッセージの検出にはユーザー ID（jimr）が使用されます。

アップグレード パス

リリース 11.0.4-004 へのアップグレード - MD（メンテナンス導入）更新

次のバージョンから、リリース 11.0.4-004 にアップグレードすることができます。

- 11.0.4-003
- 11.0.3-251

リリース 11.0.4-003 へのアップグレード : MD（メンテナンス導入）

次のバージョンから、リリース 11.0.4-003 にアップグレードすることができます。

- 11.0.2-037
- 11.0.2-044
- 11.0.3-238
- 11.0.3-251

リリース 11.0.3-251 へのアップグレード - MD（メンテナンス導入）更新

次のバージョンから、リリース 11.0.3-251 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

リリース 11.0.3-238 へのアップグレード - MD（メンテナンス導入）

（注） リリース 11.0.3-238 から AsyncOS バージョン 12.0.0-419 にアップグレードすることはできません。

次のバージョンから、リリース 11.0.3-238 にアップグレードすることができます。

- 9.1.2-053
- 9.7.2-145
- 9.8.1-015
- 9.8.1-021
- 11.0.1-027
- 11.0.1-301
- 11.0.1-602
- 11.0.2-037
- 11.0.2-038
- 11.0.2-044

リリース 11.0.2-044 へのアップグレード - MD（メンテナンス導入）更新

次のバージョンから、リリース 11.0.2-044 にアップグレードすることができます。

- 9.1.2-053
- 9.8.1-021
- 9.8.1-015
- 11.0.1-027
- 11.0.1-301
- 11.0.2-037
- 11.0.2-038

リリース 11.0.2-037 へのアップグレード - MD（メンテナンス導入）

次のバージョンから、リリース 11.0.2-037 にアップグレードすることができます。

- 9.1.2-053
- 9.7.2-145
- 9.8.1-021
- 9.8.1-015
- 10.0.3-003
- 11.0.0-274
- 11.0.1-027
- 11.0.1-030
- 11.0.1-301
- 11.0.1-401
- 11.0.1-505

リリース 11.0.0-274 へのアップグレード - GD（一般導入）更新

次のバージョンから、リリース 11.0.0-274 にアップグレードすることができます。

- 9.7.2-145
- 10.0.1-103
- 10.0.2-020
- 10.0.3-003
- 11.0.0-264
- 11.0.0-272

リリース 11.0.0-260 へのアップグレード - LD（限定導入）更新

次のバージョンから、リリース 11.0.0-260 にアップグレードすることができます。

- 9.1.1-038
- 9.1.2-036
- 9.7.1-066
- 9.7.2-065
- 9.7.2-131
- 9.7.2-148
- 10.0.0-203
- 10.0.1-103
- 10.0.2-020
- 11.0.0-074
- 11.0.0-105
- 11.0.0-255

リリース 11.0.0-105 へのアップグレード - LD（限定導入）

次のバージョンから、リリース 11.0.0-105 にアップグレードすることができます。

- 9.1.1-038
- 9.1.2-036
- 9.7.1-066
- 9.7.2-065
- 9.7.2-131
- 9.7.2-148
- 10.0.0-203
- 10.0.1-103

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。

アップグレードするには、管理者としてログイン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
  - C380、C390、C680、または C690
  - C170 または C190
  - 一部の C370、C370D、C670、または X1070 アプライアンス

    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

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（17 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 (25 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。

RSA DLP Suite および RSA Enterprise Manager はサポート対象外

RSA は、RSA Data Loss Prevention Suite (DLP) のサポート終了 (EOL) を発表しました。シスコは、RSA DLP で作成されたすべての既存の DLP ポリシーを新しい DLP エンジンへとシームレスに移行できる、代替の DLP ソリューションを提供します。アップグレード後は、Web インターフェイスの [セキュリティ サービス (Security Services)] > [データ損失の防止 (Data Loss Prevention)] ページで、移行した DLP ポリシーを表示または変更できます。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。

Async0S 11.0 以降は、RSA Enterprise Manager の統合のサポートはありません。RSA Enterprise Manager で作成した DLP ポリシーがある場合は、アップグレード後、アプライアンスでこれらのポリシーを作り直す必要があります。

C170 および C100V モデルのパフォーマンスの低下

C170 または C100V モデルで AsyncOS 11.0 にアップグレードすると、特定の設定でパフォーマンスが低下する可能性があります。詳細については、以下を参照してください。

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCve27500

FIPS の準拠性

AsyncOS 11.0 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#1643）。

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

上記のいずれかのバージョンから AsyncOS 11.0.0-264 にアップグレードする場合、以前のバージョンに戻すことはできません。

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、または X1060 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 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 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

クラスタ通信と SCP プッシュのための SSH-RSA キー

クラスタ通信

クラスタ通信中のホスト キーの検証は SSH-RSA のみに基づいて実行されるようになりました。SSH-RSA キーをアプライアンスに追加しない場合、AsyncOS 11.0 にアップグレードした後にクラスタ通信が失敗します。

SCP プッシュ

SSH-RSA キーを持たないリモート コンピュータ上の SCP サーバーに定期的にログ ファイルをプッシュするように SCP プッシュを設定すると、AsyncOS 11.0 にアップグレードした後に SCP プッシュが失敗します。

アプライアンスへの SSH-RSA キーの追加（クラスタ通信）

はじめる前に

すべてのアプライアンスがクラスタに接続されていることを確認してください。

手順

ステップ 1 CLI を使用していずれかのアプライアンスにログインします。

ステップ 2 次のバッチ コマンドを入力します。

logconfig ssh hostkey scan <hostname_or_IP_address>

例：IP アドレスを使用した SSH-RSA キーの追加

```
Cluster cluster_example)> logconfig ssh hostkey scan 10.1.1.1

Adding key type rsa for host 10.1.1.1:
10.1.1.1 ssh-rsa AAB3Nx34TAQA...
Adding key type dsa for host 10.1.1.1:
10.1.1.1.1 ssh-dss AAB3NzaC1kc3AAcbAOY…
```

例：ホスト名を使用した SSH-RSA キーの追加

```
(Cluster cluster_example)> logconfig ssh hostkey scan mail1.example.com

Adding key type rsa for mail1.example.com:
mail1.example.com ssh-rsa ADFTghYAB……

Adding key type dsa for host mail1.example.com:
mail1.example.com ssh-dss AB3NzaC1kc3MAA…
```

ステップ 3 同じアプライアンスで、クラスタ内の他のすべてのアプライアンスのホスト名または IP アドレスを使用して、ステップ 2 を繰り返します。

ステップ 4 変更を保存します。

このリリースへのアップグレード

はじめる前に

- 既知および修正済みの問題（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（16 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（17 ページ）を参照してください。

手順

E メール セキュリティ アプライアンス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 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。

アップグレード後の注意事項

AsyncOS 11.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 11.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

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（23 ページ）
- 既知および修正済みの問題のリスト（23 ページ）
- 関連資料（25 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	**AsyncOS 11.0.4**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=11.0.4&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.3	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.3&sb=afr&sts=open&svr=3nH&bt=custV
	AsyncOS 11.0.2	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.2*&sb=afr&bt=custV
	AsyncOS 11.0.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.1-027&sb=afr&bt=custV
	AsyncOS 11.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.0&sb=afr&bt=custV

修正済みの問題	**AsyncOS 11.0.4**	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941569&rls=11.0.4-004&sb=fr&sts=fd&svr=3nH&bt=custV
	AsyncOS 11.0.3	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.3-251&sb=fr&sts=fd&svr=3nH&bt=custV
	AsyncOS 11.0.2	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.2-044&sb=fr&bt=custV
	AsyncOS 11.0.1	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.1-027&sb=fr&bt=custV
	AsyncOS 11.0	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=11.0.0&sb=fr&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(Release)] フィールドに、リリースのバージョン(たとえば、11.0.4)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：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。