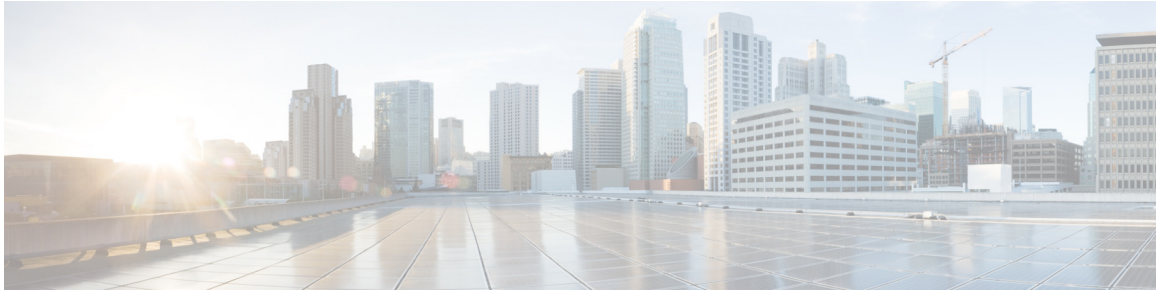

AsyncOS 15.0 for Cisco Secure Email and Web Manager（Cloud）リリースノート（一般導入）

発行日：2023 年 8 月 10 日

目次

（注） スパムの隔離ポータルにログインする際は、正確な電子メール ID とドメイン名を必ず入力してください。

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
単一ログライン（SLL）	SLL 機能は、電子メールトラッキングデータを単一ログラインまたはフラット化モデルとして作成、インデックス付け、および保存します。したがって、クエリを実行してすぐに応答を取得できます。この機能は、高速応答、低メモリ、および CPU 使用率により、トラッキングクエリまたは検索のパフォーマンスを向上させます。 この機能は、アップグレード後の電子メールトラッキングデータにのみ適用されます。
CRL ソースの設定	Secure Email and Web Manager は、ユーザーの証明書が失効していないことを確認するために、証明書検証の一環として証明書失効リスト（CRL）と呼ばれる失効した証明書のリストを確認します。サーバー上でこのリストを最新のバージョンに保つ必要があります。Secure Email and Web Manager はユーザーが作成したスケジュールでこれをダウンロードします。リストは手動で更新することもできます。 次の方法を使用して CRL ソースを設定できます。 • レガシー Web インターフェイスで、[ネットワーク（Network）] > [CRL ソース（CRL Sources）] > [CRL ソースの追加（Add CRL Source）] > [CRL（証明書失効リスト）ソースの追加（Add CRL (Certificate Revocation Lists) Source）] ウィンドウに移動します。 • CLI の `Certconfig` > `CRL` サブコマンドを使用します。 CRL ソースの設定の詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Configuring CRL Sources」のセクションを参照してください。

古い Splunk データの削除	Secure Email and Web Manager 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースとバイナリが削除されます。 （注） Secure Email and Web Manager 13.6.2 リリース以降、Splunk データベースは電子メールトラッキングデータの保存に使用されなくなりました。新しい電子メールトラッキングデータはすべて、Lucene データベースに保存されます。Secure Email and Web Manager 15.0 にアップグレードすると、Secure Email and Web Manager 13.6.2 へのアップグレード前のすべてのトラッキングデータが削除され、回復できなくなります。 （注） Splunk データベースのデバッグ情報を収集するために使用される [デバッグ（debug）] サブメニューは、CLI の `Diagnostic` > `Tracking` サブコマンドから削除されます。
最初の製造元の値にネットワーク設定をリセット	最後の Reload サブコマンド（ネットワーク設定をリセットする）の実行ステータスを表示する新しいサブコマンド `Reload Status` が `Diagnostic` コマンドに追加されました。 このコマンドの詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Diagnostic - Reload command」および「Diagnostic - Reload Status command」のセクションを参照してください。

TLS 通信中のピア証明書の X.509 検証の実行	ピア証明書の X.509 検証を実行するように Secure Email and Web Manager を設定できます。X.509 検証は、次のサービスに適用されます。 • アウトバウンド SMTP • LDAP • アップデータ • TLS を介したアラート • syslog サーバー • スマート ライセンシング サーバー • SSE コネクタ • SSE サーバー 次の方法を使用して、ピア証明書の X.509 検証を設定できます。 • Web インターフェイスの [システム管理（System Administration）] > [SSL 設定（SSL Configuration）] > [SSL 設定（SSL Configuration）] ページに移動します。 • CLI の `sslconfig` コマンドを実行します。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「X.509」のセクションを参照してください。
Secure Email and Web Manager 仮想アプライアンスモデルの新しい RAM 値	AsyncOS 15.0 リリース以降では、KVM または VMWare ESXi を介して展開された M600V Secure Email and Web Manager 仮想アプライアンスモデルに新しい RAM 値があります。 仮想アプライアンスに適用可能な新しい RAM 値の詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

動作における変更

SSH サーバーとクライアントの設定の変更	[アップグレードのシナリオ] Cisco Secure Email and Web Manager を下位の AsyncOS バージョンから AsyncOS 15.0 バージョン以降にアップグレードする場合は、次の SSH サーバーとクライアントの設定の変更が適用されます。 [SSH サーバー設定の変更] • 次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムは、デフォルトで Secure Email and Web Manager から削除されます。 – **暗号アルゴリズム**:`rijndael-cbc@lysator.liu.se`、`3des-cbc`、`blowfish-cbc`、`cast128-cbc`、`arcfour`、`arcfour128`、および `arcfour256` – **MAC メソッド**:`hmac-md5`、`umac-64@openssh.com`、`hmac-ripemd160`、`hmac-ripemd160@openssh.com`、`hmac-sha1-96`、`hmac-md5-96` – **KEX アルゴリズム**:`diffie-hellman-group-exchange-sha256`、`diffie-hellman-group-exchange-sha1`、`diffie-hellman-group1-sha1` – **ホストキーアルゴリズム**:`rsa1` • [最小サーバーキーサイズ(Minimum Server Key Size)] オプションは、デフォルトで Secure Email and Web Manager の CLI から削除されます。 • ホストキーアルゴリズム:`rsa-sha2-256` は、デフォルトで Secure Email and Web Manager に追加されます。 [SSH クライアント設定の変更] • 次の暗号アルゴリズム:`aes128-gcm@openssh.com` および `aes256-gcm@openssh.com` は、デフォルトで Secure Email and Web Manager に追加されます。 • ホストキーアルゴリズム:`rsa-sha2-256` は、デフォルトで Secure Email and Web Manager に追加されます。

SSH サーバーとクライアントの設定の変更	[バナーテキストの変更] [システムアップグレード（System Upgrade）] バナーテキストに、アップグレードプロセス後に暗号、キー、Kex、および MAC の脆弱なアルゴリズムがシステムによって削除されることを通知する注記が追加されます。
	[新規インストールシナリオ] 次の SSH サーバー設定の変更は、Cisco Secure Email and Web Manager 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。 Secure Email and Web Manager では、次の暗号アルゴリズム、MAC メソッド、およびホストキーアルゴリズムがサポートされています。 • **暗号アルゴリズム**：`aes128-ctr`、`aes192-ctr`、`aes256-ctr`、`aes128-cbc`、`aes192-cbc`、および `aes256-cbc` • **MAC メソッド**：`hmac-sha1` • **ホストキーアルゴリズム**：`rsa-sha2-256`、`ssh-rsa`、および `ssh-dss`（デフォルトでは無効） （注） CLI で `sshconfig` > `sshd` > `setup` サブコマンドを使用して、`ssh-dss` 暗号アルゴリズムを手動で有効にする必要があります。 • **KEX アルゴリズム**：`diffie-hellman-group14-sha1`、`ecdh-sha2-nistp256`、`ecdh-sha2-nistp384`、および `ecdh-sha2-nistp521`

X.509 証明書の変更	[アップグレードのシナリオ] Secure Email and Web Manager 15.0 以降のバージョンにアップグレードすると、安全性の低い署名アルゴリズムを使用した X.509 証明書はアップグレード後に削除されることが通知されます。 通知メッセージ 注:安全性の低い署名アルゴリズムを使用した x509 証明書は、アップグレード後に削除されます(設定されている場合)。
	[新規インストールシナリオ] 次の X.509 証明書用署名アルゴリズムの変更は、Cisco Secure Email and Web Manager 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。 • x509 証明書の次の署名アルゴリズムは、サポートされなくなりました:`sha1withrsaencryption`、`dsawithsha1`、`sha224withrsaencryption`、`ecdsa-with-sha1`、`ecdsa-with-sha224`、`md2withrsaencryption`、`md4withrsaencryption`、`md5withrsaencryption`、`ripemd128withrsaencryption`、`ripemd160withrsaencryption`、および `ripemd256withrsaencryption`。 • ECDSA 署名アルゴリズムを持つ x509 証明書の以下の曲線はサポートされていません:`secp224r1`、`secp192r1`、`brainpoolP160r1`、`brainpoolP192r1`、`secp160r1`、`secp160r2`、`secp192k1`、`secp224k1`、`secp256k1`、`sect163k1`、`sect163r2`、`sect193r1`、`sect193r2`、`sect233k1`、`sect233r1`、`sect239k1`、`sect283k1`、`sect283r1`、`sect409k1`、`sect409r1`、`sect571k1`、および `sect571r1`.

X.509 証明書の変更	[証明書のアップロードシナリオ] 安全性の低い署名アルゴリズムを使用して X.509 証明書をアップロードすると、ABC アルゴリズムを使用した X.509 証明書の安全性が低いことを示すエラーメッセージが表示されます。 エラー メッセージ エラー：ripemd160WithRSA ダイジェストを使用した x509 証明書は低い安全性です。（Error: The x509 certificates with ripemd160WithRSA digest are less secure.）
	[構成ファイルのロードシナリオ] **CLI を使用した構成ファイルのロード** CLI を使用して構成ファイルをロードすると、安全性の低い署名アルゴリズムを使用した X.509 証明書が削除されるという警告が表示されます。 警告メッセージ 警告：次の x509 証明書は、署名アルゴリズムの安全性が低いため削除されます：['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']。（WARNING: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].） **GUI を使用した構成ファイルのロード** GUI を使用して構成ファイルをロードすると、安全性の低い署名アルゴリズムを使用した X.509 証明書が削除されるという警告が表示されます。 警告メッセージ 警告：次の x509 証明書は、署名アルゴリズムの安全性が低いため削除されます：['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']。（Warnings: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].）
最初の製造元の値にネットワーク設定をリセット	このリリースより前は、`Diagnostic` > `Reload` サブコマンドを使用して、すべてのユーザー設定を削除し、デバイス全体をリセットしていました。 このリリースにアップグレードした後、以前の機能とともに、このサブコマンドはネットワーク設定を最初の製造元の値にリセットします。
JWT トークン：エラーメッセージの変更	このリリース以前は、JSON Web トークン（JWT）トークンを使用して API 要求を行う際に JWT トークンが期限切れになっていると、期限切れトークンのエラーメッセージが表示されました。 このリリースにアップグレードした後は、JWT トークンを使用して API 要求を行う際に、使用された JWT トークンが 12 時間より古い場合、無効なトークンまたは期限切れのトークンのエラーメッセージが表示されます。期限切れトークンのエラーメッセージは、トークン生成から最大 12 時間しか表示されません。

SPoG 機能の変更	SPoG を有効または無効にすると、新しい Web インターフェイスに同時にログインしているすべてのユーザーのセッションが無効になり、サーバーへの新しい要求によってログアウトされます。ユーザーは再度ログインする必要があります。 また、Cisco Secure Email and Web Manager が SPoG に追加されており、現在同じ Cisco Secure Email and Web Manager の新しい Web インターフェイスにログインしている場合は、JWT 検証のフローが変更されたため、ログアウトされます。 （注） SPoG 機能は、SPoG クラスタの下の Cisco Secure Email and Web Manager がすべて同じバージョンである場合にのみ動作します。
メッセージ追跡：修復アクションの変更	このリリース以前は、[修復アクションの確認（Confirm Remediation Action）] ダイアログボックスの [修復バッチ名（Remediation Batch Name）] および [説明（Description）] フィールドに、小文字と大文字のアルファベットおよび 0 ～ 9 までの数字に加えて任意の特殊文字を入力できました。 このリリース以降は、[修復アクションの確認（Confirm Remediation Action）] ダイアログボックスの [修復バッチ名（Remediation Batch Name）] および [説明（Description）] フィールドに入力できるのは、小文字と大文字のアルファベット、0 ～ 9 までの数字、および「_」「-」のみです。その他の特殊文字は使用できません。
Secure Email and Web Manager と syslog サーバー間の通信で TLSv1.0 のサポートなし	このリリース以前は、Secure Email and Web Manager は、syslog サーバーで有効になっている TLS バージョンに関係なく、TLSv1.0 を使用して syslog サーバーと通信していました。 このリリース以降、Secure Email and Web Manager は、syslog サーバーで有効になっている最も高い TLS バージョンを使用します。たとえば、syslog サーバーの最も高い TLS バージョンが 1.2 の場合、Secure Email and Web Manager は TLSv1.2 を使用して syslog サーバーと通信します。 （注） TLSV1.0 は、安全でない TLS 方式であるため、現在はサポートされていません。
フェーズ 2 バックアッププロセスの通知メッセージ	このリリース以前は、フェーズ 2 バックアッププロセスのサービスタスクが進行中で、完了までに 2 時間を超えた場合、管理者に通知メッセージが送信されませんでした。 このリリースにアップグレードした後、フェーズ 2 バックアッププロセスでサービスタスクが進行中で、完了までに 2 時間を超える場合、バックアッププロセスのステータスと、完了までに時間がかかるサービス名を知らせる通知メッセージが管理者に送信されます。
[タイムゾーン（Time Zone）] -> [国（Country）] フィールドの変更	このリリース以降、[タイムゾーン（Time Zone）] -> [国（Country）] フィールドで使用可能な [米国（United States）] オプションは、[アメリカ合衆国（United States of America）] に変更されました。

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、レポートのモニタリング、検疫、およびメッセージ検索機能が新しくなりました。

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。

- URL `https://example.com:4431/ng-login` を使用できます。

  `example.com` はアプライアンスのホスト名を示します。
- アプライアンスにログインし、[セキュリティ管理アプライアンスの外観が新しくなりましたので、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 12.0 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）
- Safari（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 12.0 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 1440 X 900 です。

（注） 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。

エンドユーザーは、新しい Web インターフェイスのスパムの隔離にアクセスできます。スパムの隔離にログインするには、次の URL を使用します。

`https://example.com:4431/euq-login`

example.com はアプライアンスのホスト名を示します。

（注） HTTP/HTTPS ポートおよび AsyncOS API 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。

アップグレード パス

リリース 15.0.0-334 へのアップグレード（一般導入）

次のバージョンからリリース 15.0.0-334 にアップグレードできます。

- 14.3.0-120
- 14.3.0-124
- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

リリース 15.0.0-333 へのアップグレード（限定導入）更新

次のバージョンからリリース 15.0.0-333 にアップグレードできます。

- 15.0.0-317
- 14.3.0-120
- 14.3.0-124
- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

リリース 15.0.0-317 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-317 にアップグレードできます。

- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224
- 14.3.0-120
- 14.3.0-124

- 14.3.0-126
- 15.0.0-281

インストールおよびアップグレードに関する注意事項

重要な追加資料

関連する E メールセキュリティおよび Web セキュリティのリリースのリリースノートも確認する必要があります。

この情報へのリンクについては、関連資料（14 ページ）を参照してください。

アップグレード前の要件

既存のデータベースのバックアップ

Cisco Secure Email and Web Manager をアップグレードする前に、Cisco Secure Email and Web Manager の既存のデータベースをバックアップします。

Secure Email and Web Manager のディザスタリカバリの詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Backing Up Security Management Appliance」のセクションを参照してください。バックアッププロセスをスケジュールする詳細な手順については、ユーザーガイドの「Common Administrative Tasks」の章の「Scheduling Single or Recurring Backups」のセクションを参照してください。

アップグレード後の要件

スパム通知 URL の変更

Cisco Secure Email and Web Manager 15.0 へのアップグレード後、保存されているスパム通知 URL を使用してもログインできない場合は、スパム通知メールに記載されている新しい URL を使用してください。

このリリースでサポートされる VM

このリリースでは、次の VM がサポートされています。

- M100V
- M300V
- M600V

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問題に関する情報を検索します。

- バグ検索ツールの要件（13 ページ）
- 既知および修正済みの問題のリスト（13 ページ）
- 既知および解決済みの問題に関する情報の検索（13 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=282941571&rls=15.0.0&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=282941571&rls=15.0.0&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問題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://bst.cloudapps.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（15.0 など）を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

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

(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

次の表の主要なドキュメントに加えて、ナレッジベースおよびシスコサポートコミュニティを含む他のリソースに関する情報は、オンラインヘルプおよびユーザーガイドの「More Information」の章に記載されています。

Cisco Secure 製品のマニュアル:	入手場所
Cisco Secure Email and Web Manager	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
コンテンツ セキュリティ製品用コマンドライン 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 Email 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、ユーザーガイドまたはオンラインヘルプを参照してください。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

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。