AsyncOS 12.5 for Cisco Web Security Appliances リリースノート

初版：2020 年 9 月 10 日

最終更新：2023 年 5 月 9 日

Web セキュリティアプライアンスについて

Cisco Web セキュリティ アプライアンスはインターネット トラフィックを代行受信してモニターし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネット ベースの脅威から内部ネットワークを保護します。

最新情報

AsyncOS 12.5.6-008 MD（メンテナンス導入）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、「リリース 12.5.6-008 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

AsyncOS 12.5.5-008 MD（メンテナンス導入）の新機能：更新

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、「リリース 12.5.5-008 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

（注） 現在、12.5.5-008 では、Cisco Secure Email および Web Manager の互換ビルドは利用できません。

AsyncOS 12.5.5-004 MD（メンテナンス導入）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、「リリース 12.5.5-004 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

AsyncOS 12.5.4-011 MD（メンテナンス導入）の新機能：更新

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、「リリース 12.5.4-011 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

AsyncOS 12.5.4-005 MD（メンテナンス導入）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、「リリース 12.5.4-005 の既知および修正済みの問題のリスト （26 ページ）」を参照してください。

AsyncOS 12.5.3-002 MD（メンテナンス導入）の新機能

このリリースには、多数のバグ修正が含まれています。詳細については、「リリース 12.5.3-002 の既知および修正済みの問題のリスト」を参照してください。

AsyncOS 12.5.2-011 MD（メンテナンス導入）の新機能

このリリースには、多数のバグフィックスが含まれています。詳細については、「リリース 12.5.2-011 の既知および修正済みの問題のリスト」を参照してください。

AsyncOS 12-5-2-007 MD（メンテナンス導入）の新機能

このリリースには、多数のバグフィックスが含まれています。詳細については、「リリース 12.5.2-007 の既知および修正済みの問題のリスト」を参照してください。

機能	説明
新しい URL カテゴリの更新通知	新しい URL カテゴリの更新通知がバナーに導入されました。ユーザには、今後の URL カテゴリの更新に関する電子メール通知も送信されます。

AsyncOS 12-5-1-043 GD（一般導入）の新機能：更新

このリリースには、多数のバグフィックスが含まれています。詳細については、「リリース 12.5.1-043 の既知および修正済みの問題のリスト」および「AsyncOS 12.5.1-043 GD（一般導入）の動作の変更：更新」を参照してください。

AsyncOS 12.5.1-035 GD（一般導入）の新機能

このリリースには、多数のバグフィックスが含まれています。詳細については、「リリース 12.5.1-035 の既知および修正済みの問題のリスト」を参照してください。

機能	説明
TLS 1.0/1.1 の廃止	アプライアンスを AMP ファイル レピュテーション サーバに接続するには、TLS 1.2 以降のバージョンを使用します。南・北・中央アメリカ （レガシー）cloud-sa.amp.sourcefire.com は AMP ファイル レピュテーション サーバ リストから削除されるため、南・北・中央アメリカ （レガシー）cloud-sa.amp.sourcefire.com はアプライアンスで設定できません。 アプライアンスを 12.5.1 バージョンにアップグレードする前に、以下を推奨します。 • AMP サービスが有効で、ファイル レピュテーション サーバが南・北・中央アメリカ （レガシー）cloud-sa.amp.sourcefire.com として設定されている場合は、ファイル レピュテーション サーバを南・北・中央アメリカ （cloud-sa.amp.cisco.com）に変更します。 • アプライアンスをアップグレードした後、ファイル レピュテーション サーバが南・北・中央アメリカ（cloud-sa.amp.cisco.com）として保持されているかどうかを確認します。 （注） アプライアンスをアップグレードする前にヨーロッパまたはアジア太平洋、日本、中国をファイル レピュテーション サーバとして設定した場合、上記の条件は適用されません。 詳細については、『Decommissioning Legacy File Reputation Servers for Cisco Web Security Appliances』を参照してください。
信頼できるドメインルックアップの有効化	レルムの信頼できるドメインルックアップの動作を制御するために、[信頼できるドメインのルックアップを有効にする（Enable Trusted Domain Lookup）] オプションが [Active Directory アカウント（Active Directory Account）] セクション（[ネットワーク（Network）] > [認証（Authentication）] > [レルムの追加（Add Realm）]）に追加されました。 このオプションは、デフォルトでは有効になっています。

AsyncOS 12.5.1-011 LD（限定導入）の新機能

このリリースでは、次の機能が導入されています。

機能	説明
ハイパフォーマンスのサポート	Cisco AsyncOS 12.5 リリースは、プラットフォーム S680、S690、および S695 向けに、高いパフォーマンス（HP）を備えた Web セキュリティアプライアンスを提供します。HP により、既存のハイエンドアプライアンスのトラフィック処理パフォーマンスが向上します。 （注） アプライアンスで次の機能を有効にしている場合でも、12.5 バージョンにアップグレードし、モデル（S680、S690、S695、S680F、S690F、S695F）でハイパフォーマンスモードを利用できるようになりました。 • Web トラフィック タップ（Web Traffic Tap） • ボリューム クォータと時間クォータ • 全体の帯域幅の制限（Overall Bandwidth Limits）
Web プロキシの IP スプーフィング	IP スプーフィングプロファイルを作成し、それをルーティングポリシーに追加することによって、Web プロキシ IP スプーフィングを設定できるようになりました。IP スプーフィングプロファイルがルーティングポリシーで使用されている場合、Web プロキシは送信元 IP アドレスを IP スプーフィングプロファイルで定義されたカスタム IP アドレスに変更します。 FTP プロキシ設定で、ネイティブ FTP 要求のクライアント IP スプーフィングを有効または無効にすることができるようになりました。 **前提条件**： • Web プロキシ設定（[サービス（Services）] > [Webプロキシ（Web Proxy）]）で、プロキシモードと IP スプーフィング接続タイプが選択されていることを確認します。 ユーザ ガイドの「Web 要求の代行受信」の章を参照してください。

機能	説明
YouTube 分類のサポート	セキュアなアクセス制御のため、YouTube のカスタム URL カテゴリを作成し、YouTube カスタムカテゴリでポリシーを設定できるようになりました。 **前提条件**： 次のように設定されていることを確認します。 • HTTPS プロキシを有効にします（[セキュリティサービス（Security Services）] > [HTTPSプロキシ（HTTPS Proxy）]）。 • [アクセプタブル ユース コントロール（Acceptable Use Controls）] を有効にします（[セキュリティサービス（Security Services）] > [アクセプタブル ユース コントロール（Acceptable Use Controls）]）。 • www.youtube.com と m.youtube.com を使用して、カスタムおよび外部URLカテゴリを設定します（[Webセキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）]）。 • YouTube のカスタム URL カテゴリと外部 URL カテゴリを使用して、アクションを [復号（decrypt）] にして復号ポリシーを設定します。 • YouTube 用の Google API サービスを使用して Google API キーを生成します。 ユーザ ガイドの「ポリシー アプリケーションのための URL の分類」の章を参照してください。
新しい Web インターフェイスの [システムステータス（System Status）] ダッシュボード	新しいWebインターフェイスでは、アプライアンスに新しいページ（[モニタリング（Monitoring）]>[システムステータス（System Status）]）があり、アプライアンスの現在のステータスと設定が表示されます。 > ユーザガイドの「Web Security Appliance Reports on the New Web Interface」の章を参照してください。

機能	説明
Web セキュリティアプライアンスにおける Cisco Success Network	Cisco Success Network（CSN）機能によって、シスコはアプライアンスの機能使用状況情報のテレメトリを収集できます。シスコはこれらの詳細情報を使用して、デバイス情報、無料の機能やライセンス供与された機能のリスト、およびそれらのアクティベーション ステータスを識別します。 （注） デフォルトでは、Cisco Success Network 機能はアプライアンスで有効になっています。必要に応じて、Web ユーザインターフェイス（[システム管理（System Administration）] > [Cisco Success Network]）または CLI コマンド **csidconfig** を使用することで、この機能を無効化できます。 **前提条件**： • Cisco Threat Response が有効になっていることを確認します。 ユーザガイドの「Integrating with Cisco Threat Response」の章を参照してください。
ネットワーク、ログサブスクリプション、およびその他の設定用の REST API	設定情報を取得し、変更（既存の情報の変更、新しい情報の追加、エントリの削除など）を、REST API を使用してアプライアンスの設定データで実行できるようになりました。 『AsyncOS API 12.5 for Cisco Web Security Appliances - Getting Started Guide』を参照してください。

動作における変更

AsyncOS 12.5.5-004 MD（メンテナンス導入）の動作の変更

networktuning	Cisco AsyncOS 12.5 へのアップグレード後、初めて networktuning コマンドを実行すると、プロキシプロセスを再起動するように求めるプロンプトが表示されます。 （注） 12.5 より前の AsyncOS バージョンでは、プロキシプロセスを再起動するためのこのプロンプトは使用できません。アップグレード前に以前のバージョンのいずれかでコマンドが実行された場合、プロンプトはトリガーされません。

AsyncOS 12.5.4-005 MD（メンテナンス導入）の動作の変更

SSL の設定	Cisco AsyncOS 12.5.4 バージョンから、TLSv1.2 は、Chrome ブラウザのバージョン 98.0.4758.80 以降をサポートするために、[システム管理者（System Administrator）] > [SSL設定（SSL Configuration）] にある [アプライアンス管理Webユーザーインターフェイス（Appliance Management Web User Interface）] に対してデフォルトで有効になっています。
セッション再開	Cisco AsyncOS 12.5.4 バージョンへのアップグレード後、セッションの再開はデフォルトで無効になります。
Context Directory Agent（CDA）	Cisco AsyncOS 12.5.4 バージョン以降、CDA のサポートの終了を示す次のメッセージが CDA 設定セクションに追加されています。 「*Context Directory Agent（CDA）のサポートが終了しました。CDAの代わりに透過的なユーザー認証用にISE/ISE-PICを設定することをお勧めします。（Context Directory Agent (CDA) has reached EOS. It is recommended configuring ISE/ISE-PIC for transparent user authentication instead of CDA.）*」

AsyncOS 12.5.1-043 GD（一般導入）の動作の変更：更新

プロキシmallocメモリ使用率に関する警告メッセージ	アプライアンスのWebユーザインターフェイスに次のアラートメッセージが表示されます（[システム管理（System Administration）]>[アラート（Alerts）]>[上位アラートの表示（View Top Alerts）]）。 • プロキシ malloc メモリがプロキシ malloc メモリ制限の 90% を超えた場合 *Proxy malloc memory reached to 90%, proxy will restart whenever max limit exceed*（プロキシ *malloc* メモリが *90%* に達しました。プロキシは最大上限を超えるたびに再起動します） • プロキシが malloc メモリの 100% に達し、再起動する場合 *Proxy malloc memory exceed the max limit, restarting proxy*（プロキシ *malloc* メモリが上限を超えたため、プロキシを再起動します） いずれの場合も、「Webプロキシ」の重要なアラートを受信するように設定されたすべての「アラート受信者」に、電子メール通知が送信されます。 重要なログメッセージにプロキシログが含まるようになりました。

AsyncOS 12.5.1-035 GD（一般導入）の動作の変更

認証のキャッシュサイズ設定	認証のキャッシュサイズ設定は、AsyncOS 12.5.1-035 以降のバージョンではサポートされていません。 AsyncOS 12.5.1-035 以降のバージョンでは、[キャッシュサイズ（Cache Size）] オプション（[ネットワーク（Network）]>[認証（Authentication）]>[認証設定（Authentication Settings）]>[クレデンシャル キャッシュ オプション（Credential Cache Options）]）がアプライアンスの Web インターフェイスから削除されました。

AsyncOS 12.5.1-011 LD（限定導入）の動作の変更

ログ サブスクリプション	次のログが変更されて、詳細が追加されました。 • 認証に失敗すると、アクセスログにユーザ名が表示されるようになりました。 • 認証フレームワークログに、失敗した認証プロトコルのクライアント IP アドレスが表示されるようになりました。 • NTLM • 基本 • SSO（透過的）

新しい Web インターフェイスへのアクセス

新しい Web インターフェイスは、モニタリング レポートとトラッキング Web サービスの新しい外観を提供します。新しい Web インターフェイスにアクセスするには、次の手順を実行します。

- レガシー Web インターフェイスにログインします。
- UI の上部に表示される [SecureWeb Applianceの外観が新しくなりました。お試しください。（SecureWeb Appliance is getting a new look. Try it!!）]をクリックします。

リンクをクリックすると、Web ブラウザの新しいタブが開き、`https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login` に移動します。ここでは、`wsa01-enterprise.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` は、新しい Web インターフェイスにアクセスするためにアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

重要

- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- 指定したアプライアンスのホスト名を DNS サーバが解決できることを確認します。
- デフォルトでは、新しい Web インターフェイスでは、TCP ポート 6080、6443、および 4431 が動作可能である必要があります。これらのポートがエンタープライズ ファイアウォールによってブロックされていないことを確認します。
- 新しい Web インターフェイスにアクセスするためのデフォルト ポートは 4431 です。これは、**trailblazerconfig** コマンドを使用してカスタマイズできます。**trailblazerconfig** コマンドの詳細については、「コマンドライン インターフェイス」を参照してください。
- 新しい Web インターフェイスでは、HTTP および HTTPS の AsyncOS API（モニタリング）ポートも必要です。デフォルトでは、これらのポートは 6080 および 6443 です。AsyncOS

API（モニタリング）ポートは、**interfaceconfig** コマンドを使用してカスタマイズすることもできます。**interfaceconfig** コマンドの詳細については、「コマンドライン インターフェイス」を参照してください。

- これらのデフォルトポートを変更した場合は、新しい Web インターフェイスのカスタマイズされたポートがエンタープライズ ファイアウォールによってブロックされていないことを確認します。
- 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。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 11.8 以降）にアクセスすることをお勧めします。
  - Google Chrome
  - Mozilla Firefox
- 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 11.8 以降）でサポートされている解像度は、1280x800 ～ 1680x1050 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。

（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。

リリースの分類

各リリースは、リリースのタイプ（ED：初期導入、GD：全面導入など）によって識別されています。これらの用語の説明については、http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdfを参照してください。

サポート対象ハードウェア

このビルドは、サポートされている既存のすべてのプラットフォーム上でのアップグレードに使用できますが、拡張パフォーマンスのサポートは次のハードウェアモデルでのみ使用できます。

- Sx80
- Sx90/F
- Sx95/F

アプライアンスをアップグレードまたは再起動する前に、接続されているファイバスイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

仮想モデル：

- S100v
- S300v

  システムの CPU およびメモリ要件は、12.5 リリース以降で変更されています。詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。
- S600v

（注） アプライアンスに付属の Cisco SFP を使用します。

アップグレードパス

AsyncOS 12.5.6-008 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.6-008 にアップグレードできます。

- 11.8.0-453
- 11.8.0-603
- 11.8.1-702
- 11.8.2-702
- 11.8.3-501
- 11.8.4-004
- 12.0.1-334
- 12.0.2-012
- 12.0.3-007
- 12.0.4-002
- 12.0.5-011
- 12.5.1-043
- 12.5.2-007
- 12.5.2-011
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-002
- 12.5.5-004
- 12.5.5-008

AsyncOS 12.5.5-008 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.5-008 にアップグレードできます。

- 11.7.2-011
- 11.8.1-702
- 11.8.2-702
- 11.8.3-021
- 11.8.3-501
- 12.0.1-334
- 12.0.5-011
- 12.5.1-043
- 12.5.2-011
- 12.5.3-004
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-005

AsyncOS 12.5.5-004 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.5-004 にアップグレードできます。

- 10.6.0-244
- 11.7.0-704
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-603
- 11.8.1-702
- 11.8.2-702
- 11.8.3-501
- 11.8.4-004
- 12.0.1-334
- 12.0.2-012
- 12.0.3-007
- 12.0.4-002
- 12.0.5-011
- 12.5.1-043
- 12.5.2-011
- 12.5.3-006
- 12.5.4-011

AsyncOS 12.5.4-011 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.4-011 にアップグレードできます。

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007
- 12.5.2-011
- 12.5.3-002
- 12.5.4-005

AsyncOS 12.5.4-005 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS 12.5.4-005 にアップグレードできます。

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007
- 12.5.2-011
- 12.5.3-002

AsyncOS 12.5.3-002 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.3-002 にアップグレードできます。

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 11.8.4-004
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.4-002
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007
- 12.5.2-011

AsyncOS 12.5.2-011 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.2-011 にアップグレードできます。

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2-007

AsyncOS 12.5.2-007 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.2-007 にアップグレードできます。

- 10.6.0-240
- 10.6.0-244
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.7.3-025
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 11.8.3-018
- 11.8.3-021
- 11.8.3-501
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043

AsyncOS 12.5.1-043 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.1-043 にアップグレードできます。

- 10.1.4-017
- 10.1.5-004
- 10.1.5-034
- 10.1.5-037
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.1-501
- 11.7.2-011
- 11.8.0-414
- 11.8.0-453
- 11.8.0-603
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.5.0-701
- 12.5.1-011
- 12.5.1-035

AsyncOS 12.5.1-035 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.1-035 にアップグレードできます。

- 10.1.4-017
- 10.1.5-004
- 10.1.5-034
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.7.2-011
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.1-702
- 11.8.2-009
- 11.8.2-702
- 12.0.1-268
- 12.0.1-334
- 12.0.2-004
- 12.5.0-701
- 12.5.1-011

AsyncOS 12.5.1-011 へのアップグレード

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 12.5.1-011 にアップグレードできます。

- 10.1.4-017
- 10.1.5-004
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.5.6-022
- 10.5.6-024
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.1-706
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.7.1-043
- 11.7.1-045
- 11.7.1-049
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 12.0.1-268
- 12.0.1-334
- 12.5.0-701

アップグレード後の要件

12.5.5-008 にアップグレードした後、次の手順を実行する必要があります。

手順

ステップ 1 管理者アクセス権を使用して、Cisco Threat Response ポータルでユーザアカウントを作成します。

新しいアカウントを作成するには、URL：https://visibility.amp.cisco.com を使用して Cisco Threat Response ポータルにログインし、[Cisco セキュリティアカウントの作成（Create a Cisco Security Account）] をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

ステップ 2 アプライアンスを Security Services Exchange（SSE）クラウドポータルに登録するには、自身の地域に対応する SSE ポータルからトークンを生成します。

SSE クラウドポータルへの登録時に、アプライアンスの Web ユーザインターフェイスから、地域に基づいて次の FQDN を選択します。

- 米国（api-sse.cisco.com）

- 欧州（api.eu.sse.itd.cisco.com）
- APJC（api.apj.sse.itd.cisco.com）

ステップ 3 Security Services Exchange ポータルのクラウドサービスにある Cisco Threat Response が有効になっていることを確認します。アプライアンスを Security Services Exchange ポータルに登録するには、FQDN api-sse.cisco.com（米国）のファイアウォールの HTTPS（インとアウト）443 ポートが開いていることを確認します。

仮想アプライアンスの展開については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

互換性の詳細

セキュリティ管理のための Cisco AsyncOS との互換性

このリリースと Cisco Content Security Management 用の AsyncOS のリリースの互換性については、https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html で互換性マトリックスを参照してください。

クラウド コネクタ モードでの IPv6 と Kerberos は使用不可

アプライアンスがクラウド コネクタ モードで設定されている場合、Web インターフェイスのページに「IPv6 アドレスと Kerberos 認証用のオプションは使用できません（unavailable options for IPv6 addresses and Kerberos authentication）」と表示されます。使用できるように見えても、それらのオプションはクラウド コネクタ モードではサポートされていません。クラウド コネクタ モードでは、IPv6 アドレスまたは Kerberos 認証を使用するようにアプライアンスを設定しようとしないでください。

IPv6 アドレスの機能サポート

IPv6 アドレスをサポートする特性と機能は次のとおりです。

- コマンド ラインと Web インターフェイス。アプライアンスにアクセスするには、http://[2001:2:2::8]:8080 または https://[2001:2:2::8]:8443 を使用します。
- IPv6 データトラフィックでのプロキシアクションの実行（HTTP/HTTPS/SOCKS/FTP）
- IPv6 DNS サーバ

- WCCP 2.01（Cat6K スイッチ）とレイヤ 4 透過リダイレクション
- アップストリーム プロキシ
- 認証サービス
  - Active Directory（NTLMSSP、Basic、および Kerberos）
  - LDAP
  - SaaS SSO
  - CDA による透過的ユーザー識別（CDA との通信は IPv4 のみ）
  - クレデンシャルの暗号化
- Web レポートと Web トラッキング
- 外部 DLP サーバ（アプライアンスと DLP サーバ間の通信は IPv4 のみ）
- PAC ファイル ホスティング
- プロトコル：管理サーバを介した NTP、RADIUS、SNMP、および Syslog

IPv4 アドレスを必要とする特性と機能は次のとおりです。

- 内部 SMTP リレー
- 外部認証
- ログサブスクリプションのプッシュ方式：FTP、SCP、および Syslog
- NTP サーバー
- ローカル アップデート サーバ（アップデート用のプロキシサーバを含む）
- 認証サービス
- AnyConnect セキュア モビリティ
- Novell eDirectory 認証サーバ
- エンドユーザ 通知のカスタム ロゴのページ
- Cisco Web セキュリティアプライアンスとセキュリティ管理アプライアンス間の通信
- 2.01 より前の WCCP バージョン
- SNMP

オペレーティング システムとブラウザの Kerberos 認証の可用性

Kerberos 認証は、次のオペレーティング システムとブラウザで使用できます。

- Windows サーバ 2003、2008、2008R2、および 2012
- Mac での Safari および Firefox ブラウザの最新リリース (OSX バージョン10.5 以降)

- IE（バージョン 7 以降）と Windows 7 以降の Firefox および Chrome ブラウザの最新リリース

Kerberos 認証は、次のオペレーティング システムとブラウザでは使用できません。

- 上記に記載されていない Windows オペレーティング システム
- 上記で説明していないブラウザ
- iOS と Android

仮想アプライアンスの展開

仮想アプライアンスの展開については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

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

手順

ステップ 1 この AsyncOS リリースで仮想アプライアンスを設定します。「アップグレード後の要件」を参照してください。

（注） セキュリティサービスの更新が成功したことを確認します。

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。

ハードウェアと仮想アプライアンスの IP アドレスが異なる場合は、設定ファイルをロードする前に、[ネットワーク設定のロード（Load Network Settings）] を選択解除します。

ステップ 5 変更を確定します。

ステップ 6 [ネットワーク（Network）]>[認証（Authentication）] に移動し、ドメインに再度参加します。そうしないと、アイデンティティは機能しません。

AsyncOS for Web のアップグレード

始める前に

- RAID コントローラ ファームウェアの更新を含むアップグレード前の要件を実行します。
- 管理者としてログインします。

手順

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] ページで、Web セキュリティアプライアンスから XML コンフィギュレーション ファイルを保存します。

ステップ 2 [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] ページで、[アップグレードオプション（Upgrade Options）] をクリックします。

ステップ 3 [ダウンロードとインストール（Download and install）] または [ダウンロードのみ（Download only）] のいずれかを選択できます。

使用可能なアップグレードのリストから選択します。

ステップ 4 [続行（Proceed）] をクリックします。

[ダウンロードのみ（Download only）] を選択した場合は、アップグレードがアプライアンスにダウンロードされます。

ステップ 5 （[ダウンロードとインストール（Download and install）] を選択した場合） アップグレードが完了したら、[今すぐリブート（Reboot Now）] をクリックして、Web セキュリティアプライアンスをリブートします。

（注） ブラウザがアップグレードしたバージョンの AsyncOS に新しいオンライン ヘルプのコンテンツをロードすることを確認するには、ブラウザを終了してから開いてオンライン ヘルプを表示します。これにより、期限切れのコンテンツのブラウザ キャッシュがクリアされます。

重要：アップグレード後に必要なアクション

アップグレード後にアプライアンスが正常に機能し続けるようにするには、次の事項に対処する必要があります。

- シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更
- 仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更
- ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更
- ファイル分析：分析対象のファイル タイプの確認
- 正規表現のエスケープされていないドット

シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更

AsyncOS 9.1.1 以降では、プロキシサービスに使用可能なデフォルトの暗号スイートは、セキュアな暗号スイートのみを含むように変更されます。

ただし、AsyncOS 9.x.x 以降のリリースからアップグレードする場合、デフォルトのプロキシサービスの暗号スイートは変更されません。セキュリティを強化するために、アップグレード

後に、デフォルトのプロキシサービス暗号スイートをシスコが推奨する暗号スイートに変更することをお勧めします。次の手順を実行します。

手順

ステップ 1 Web インターフェイスを使用してアプライアンスにログインします。

ステップ 2 [システム管理（System Administration）]>[SSL設定（SSL Configuration）] をクリックします。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [プロキシサービス（Proxy Services）] で、[使用する暗号（CIPHER(s) to Use）] フィールドを次のフィールドに設定します。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-
DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:TLS_AES_256_GCM_SHA384
```

注意 上記の文字列を改行またはスペースを含まない単一の文字列として貼り付けてください。

ステップ 5 変更を送信し、保存します。

CLI で **sslconfig** コマンドを使用して、上記の手順を実行することもできます。

仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更

このセクションの要件は AsyncOS 8.8 で導入されました。

次のセキュリティ脆弱性は、アプライアンスに存在する場合、アップグレード中に修正されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport

（注） このパッチは、2015 年 6 月 25 日より前にダウンロードまたはアップグレードされた仮想アプライアンス リリースにのみ必要です。

アップグレード前にこの問題を修正しなかった場合は、修正されたことを示すメッセージがアップグレード中に表示されます。このメッセージが表示された場合、アップグレード後にアプライアンスを完全な動作順序に戻すには次のアクションを実行する必要があります。

- SSH ユーティリティの既知のホスト リストから、アプライアンスの既存のエントリを削除します。新しいキーが作成されたら、ssh 経由でアプライアンスに接続し、接続を承認します。
- SCP プッシュを使用して、リモートサーバ（Splunk を含む）にログを転送する場合は、リモートサーバからアプライアンスの古い SSH ホストキーをクリアします。
- 展開に Cisco コンテンツ セキュリティ管理アプライアンスが含まれている場合は、そのアプライアンスのリリース ノートに記載されている重要な手順を参照してください。

ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更

複数のコンテンツ セキュリティ アプライアンス（Web、電子メール、または管理）を展開しており、組織内の任意のアプライアンスからアップロードされたすべてのファイルについてクラウド内の詳細なファイル分析結果を表示する場合は、アップグレード後に各アプライアンスでアプライアンス グループを設定する必要があります。アプライアンスグループを設定するには、「File Reputation Filtering and File Analysis」を参照してください。

ファイル分析：分析対象のファイル タイプの確認

AsyncOS 8.8 でファイル分析クラウドサ ーバの URL が変更されました。その結果、分析可能なファイルタイプがアップグレード後に変更された可能性があります。変更がある場合は、アラートが表示されます。分析用に選択したファイルタイプを確認するには、[セキュリティサービス（Security Services）] > [マルウェア対策およびレピュテーション（Anti-Malware and Reputation）] を選択し、Advanced Malware Protection の設定を確認します。

正規表現のエスケープされていないドット

正規表現のパターンマッチングエンジンにアップグレードすると、システムの更新後に既存のパターン定義でエスケープされていないドットに関するアラートが表示されることがあります。ドットの後に 64 文字以上を返すパターン内のエスケープされていないドットは、Velocity パターンマッチングエンジンによって無効化され、その影響についてのアラートがユーザーに送信されます。パターンを修正または置換するまで、更新のたびにアラートは送信され続けます。一般に、長い正規表現内のエスケープされていないドットは問題を引き起こす可能性があるため、避ける必要があります。

マニュアルの更新

この製品のユーザーガイドおよびその他のマニュアルは、「関連資料」から入手できます。

既知および修正済みの問題

- バグ検索ツールの要件
- 既知および修正済みの問題のリスト
- 既知および解決済みの問題に関する情報の検索

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

- リリース 12.5.6-008 の既知および修正済みの問題のリスト （26 ページ）
- リリース 12.5.5-008 の既知および修正済みの問題のリスト （26 ページ）
- リリース 12.5.5-004 の既知および修正済みの問題のリスト （26 ページ）

リリース 12.5.6-008 の既知および修正済みの問題のリスト

リリース 12.5.5-008 の既知および修正済みの問題のリスト

リリース 12.5.5-004 の既知および修正済みの問題のリスト

リリース 12.5.4-011 の既知および修正済みの問題のリスト

リリース 12.5.4-005 の既知および修正済みの問題のリスト

リリース 12.5.3-002 の既知および修正済みの問題のリスト

リリース 12.5.2-011 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 12.5.2-007 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 12.5.1-043 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 12.5.1-035 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

リリース 12.5.1-011 の既知および修正済みの問題のリスト

- 修正済みの問題
- 既知の問題

既知および解決済みの問題に関する情報の検索

Cisco Bug Search Tool を使用して、既知および解決済みの不具合に関する現在の情報を検索します。

始める前に

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）] > [Webセキュリティ（Web Security）] > [Cisco Webセキュリティアプライアンス（Cisco Web Security Appliance）] > [Cisco Secure Web Appliance] をクリックし、[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（x.x.x 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、[リリース（Releases）] 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、[リリース（Releases）] 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

資料	参照先
Cisco Secure Web Appliance ユーザーガイド	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
シスコのコンテンツセキュリティ管理アプライアンスユーザーガイド	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
仮想アプライアンスインストールガイド	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html
Cisco Secure Email and Web Manager と Cisco Secure Web Appliance の互換性マトリックス	https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html
API ガイド	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-programming-reference-guides-list.html

サポート

シスコサポートコミュニティ

シスコサポートコミュニティは、シスコのお客様、パートナー、および従業員向けのオンラインフォーラムです。Webセキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコユーザーと情報を共有したりできます。

Webセキュリティと関連管理については、シスコサポートコミュニティにアクセスしてください。

https://supportforums.cisco.com/community/5786/web-security

カスタマー 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 [英語] を参照してください。

従来の IronPort のサポートサイト：http://www.cisco.com/web/services/acquisitions/ironport.html [英語] を参照してください。

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。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

翻訳について
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。