AsyncOS 15.0 for Cisco Secure Web Appliance リリースノート

最終更新：2025 年 2 月 18 日

Secure Web Appliance について

Cisco Secure Web Appliance 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 15.0.1-004（メンテナンス導入）の新機能 （1 ページ）
- AsyncOS 15.0.0-355（一般導入）の新機能 （1 ページ）

AsyncOS 15.0.1-004（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 15.0.1-004 の既知および修正済みの問題 （15 ページ）」を参照してください。

AsyncOS 15.0.0-355（一般導入）の新機能

このリリースでは次の機能が導入されました。

機能	説明
スマート ソフトウェア ライセンシングの機能強化	スマート ソフトウェア ライセンシング機能に加えられた拡張機能は次のとおりです。 • ライセンス予約：Cisco Smart Software Manager（CSSM）ポータルに接続せずに、Cisco Secure Web Appliance で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Web Appliance を展開するユーザーにとって有益です。 詳細については、ユーザーガイドの「Overview of smart licensing」および「Reserving Feature Licenses」セクションを参照してください。 • Device Led Conversion（DLC）：Cisco Secure Web Appliance をスマートライセンスに登録すると、既存の有効なクラシックライセンスはすべて、Device Led Conversion（DLC）プロセスを使用して自動的にスマートライセンスに変換されます。これらの変換されたライセンスは、CSSM ポータルのバーチャルアカウントで更新されます。 詳細については、ユーザーガイドの「Overview of smart licensing」セクションを参照してください。 （注） • AsyncOS バージョン 15.0 は、クラシックライセンスがサポートされる最後のリリースです。AsyncOS の次のメジャーリリースでは、スマートライセンスのみがサポートされます。
詳細な帯域幅制御	クォータプロファイルで帯域幅の値を設定し、暗号化ポリシーおよびアクセスポリシー URL カテゴリまたは全体的な Web アクティビティクォータでクォータプロファイルをマッピングすることにより、トラフィックの帯域幅を管理できます。 詳細については、ユーザーガイドの「Defining Time, Volume, and Bandwidth Quotas」セクションを参照してください。
ポリシーの複製	ポリシーの複製機能を使用すると、ポリシーの既存の構成をコピーまたは複製して、新しいポリシーを作成できます。 詳細については、ユーザーガイドの「Policy Configuration」セクションを参照してください。

機能	説明
アプリケーションの検出および制御（ADC）エンジン	サポートされるADC エンジンは、アクセプタブル ユース ポリシーのコンポーネントであり、アプリケーションで使用されるWeb トラフィックを深く理解し、管理できるように、Web トラフィックを検査します。 AsyncOS 15.0 以降では、AVC または ADC エンジンを使用してWeb トラフィックを監視できます。デフォルトでは、AVC は有効になっています。ADC エンジンは、高性能モードをサポートします。 詳細については、ユーザーガイドの「Configuring the URL Filtering Engine」および「Policy Configuration」セクションを参照してください。
ADC 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アクセスポリシー設定データで実行できます。 詳細については、『AsyncOS API 15.0 for Cisco Secure Web Appliance - Getting Started Guide』を参照してください。
拡張機能	
SNMP3 のデフォルト以外のユーザー名	AsyncOS 15.0 以降、管理者は、デフォルトユーザー名 [v3get] 以外のカスタム SNMPv3 ユーザ名の設定を選択できます。 詳細については、ユーザーガイドの「Monitoring System Health and Status using SNMP」セクションを参照してください。
カスタムヘッダー	カスタムヘッダーの最大長は 16k です。 詳細については、ユーザーガイドの「Adding Custom Headers To Web Requests」セクションを参照してください。
安全なトンネルインターフェイスとリモートアクセス接続を選択するオプション	トンネルとリモートアクセス接続の確立に使用するインターフェイスを選択できます。 詳細については、ユーザーガイドの「Enabling remote access to the appliance」セクションを参照してください。

機能	説明
プラットフォームのアップグレード	AsyncOS 15.0 から、FreeBSD バージョンが FreeBSD 13.0 にアップグレードされました。 以下がアップグレードされました。 • Cisco SSL バージョン 1.0.2 から Cisco SSL バージョン 1.1.1。 • AVC、WBRSD、DCA、Beaker などの Talos エンジンがアップグレードされました。 • Webroot や McAfee などのスキャナエンジンがアップグレードされました。 （注） FreeBSD 13.0 は、Cisco SSL バージョン 1.1.1 のみと互換性があります。 FreeBSD 13.0 への SSH 接続では、Cisco SSH 互換の暗号、mac、および kex アルゴリズムのみがサポートされます。

AsyncOS 15.0.0-355 GD（一般導入）の動作の変更

Cisco Secure Web Appliance のデータセンター アーキテクチャ（DCA）機能は、AsyncOS15.0 GD リリースの一部として無効になり、今後のリリースではサポートされなくなります。したがって、有効にすることは推奨しません。

既知の制限事項

このリリースでは、次の制限事項があります。

- プロキシ Malloc メモリの SNMP OID の SNMPWALK/SNMPGET 操作は、マルチプロキシ SWA（S690、S695、S1000V）ではサポートされていません。

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は次の方法でアクセスできます。

- レガシー Web インターフェイスにログインし、[Secure Web Appliance をクリックして新しい外観を試してみてください（Secure Web Appliance is getting a new look. Try it!!）] のリンクをクリックします。この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 ファイアウォールで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** CLI コマンドを使用してカスタマイズできます。**trailblazerconfig** CLI コマンドの詳細については、ユーザガイドの「コマンドライン インターフェイス」の章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** CLI 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** CLI コマンドの詳細については、ユーザ ガイドの「コマンドライン インターフェイス」の章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 ファイアウォールで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。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 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 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。

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。

このリリースでサポートされているハードウェア

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。

- Sx90/F
- Sx95/F

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
- S1000v

（注）
- アプライアンスに付属の Cisco SFP を使用します。
- AsyncOS バージョン 15.0 は、Sx90/F モデルでサポートされる最後のリリースになります。

アップグレードパス

- AsyncOS 15.0.1-004 へのアップグレード （6 ページ）
- AsyncOS 15.0.0-355 へのアップグレード （7 ページ）

AsyncOS 15.0.1-004 へのアップグレード

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 15.0.1-004 にアップグレードできます。

- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2.011
- 12.5.3-002
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-008
- 12.5.5-501
- 12.5.6-008
- 12.7.0-033
- 14.0.1-053
- 14.0.2-012
- 14.0.3-014
- 14.0.4-005
- 14.0.4-007
- 14.1.0-041
- 14.1.0-047
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-008
- 14.5.1-016
- 14.5.1-607
- 14.5.2-011
- 14.5.3-033
- 14.6.0-108
- 15.0.0-302
- 15.0.0-322
- 15.0.0-355
- 15.0.0-364
- 15.0.0-608
- 15.0.0-612

AsyncOS 15.0.0-355 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。
- AsyncOS 15.0 は連邦情報処理標準（FIPS）モードをサポートしていないため、FIPS モードを有効にした状態で AsyncOS 15.0 にアップグレードすることは推奨しません。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 15.0.0-355 にアップグレードできます。

- 11.8.0-453
- 11.8.1-023
- 11.8.3-021
- 11.8.4-004
- 12.0.1-334
- 12.0.2-004
- 12.0.2-012
- 12.0.3-005
- 12.0.3-007
- 12.0.3-503
- 12.0.4-002
- 12.0.5-011
- 12.5.1-011
- 12.5.1-035
- 12.5.1-043
- 12.5.2.011
- 12.5.3-002
- 12.5.3-006
- 12.5.4-005
- 12.5.4-011
- 12.5.5-004
- 12.5.5-005
- 12.5.5-008
- 12.5.5-501
- 12.5.6-008
- 12.7.0-033
- 14-0-1-014
- 14.0.1-040
- 14.0.1-053
- 14.0.2-012
- 14.0.3-014
- 14.0.4-005
- 14.1.0-032
- 14.1.0-041
- 14.1.0-047
- 14.5.0-498
- 14.5.0-537
- 14.5.0-673
- 14.5.1-008
- 14.5.1-016
- 14.6.0-108
- 15.0.0-302
- 15.0.0-322

アップグレード後の要件

アプライアンスを Cisco Threat Response に登録していない場合は、15.0.0-355 にアップグレードした後で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 （9 ページ）
- クラウド コネクタ モードでの IPv6 と Kerberos は使用不可 （9 ページ）
- IPv6 アドレスの機能サポート （10 ページ）
- アップグレード後の要件 （8 ページ）

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 「アップグレード後の要件 （8 ページ）」に記載されている手順に従って、この AsyncOS リリースを使用して仮想アプライアンスを設定します。

（注）
セキュリティサービスの更新が正常にインストールされ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バージョンの AsyncOS 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の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。

仮想アプライアンスとハードウェアの 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 変更を保存します。

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

- 管理者としてログインします。
- 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。

手順

ステップ 1 **[システム管理（System Administration）]** > **[構成ファイル（Configuration File）]**ページで、Secure Web Appliance から XML 構成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）] のいずれかを選択します。

ステップ 4 利用可能なリストから、アップグレードを選択します。

ステップ 5 [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 6 [ダウンロードとインストール（Download and install）] を選択した場合は、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、Cisco Secure Web Appliance 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。

アップグレード後に必要な重要アクション

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：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

Web サイト（www.cisco.com）にあるユーザ ガイドは、オンライン ヘルプよりも最新である場合があります。この製品のユーザ ガイドとその他のドキュメントを入手するには、オンライン ヘルプの [PDFの表示（View PDF）] ボタンをクリックするか、「関連資料 （16 ページ）」に示す URL にアクセスしてください。

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 15.0.1-004 の既知および修正済みの問題 （15 ページ）
- リリース 15.0.0-355 の既知および修正済みの問題 （15 ページ）

リリース 15.0.1-004 の既知および修正済みの問題

- 修正済みの問題
- 既知の問題

リリース 15.0.0-355 の既知および修正済みの問題

- 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）]** 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

資料	参照先
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
Secure Web Appliance のリリースノート、ISE 互換性マトリックス、および暗号	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-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、Cisco TAC にお問い合わせください。TAC に連絡する前に、仮想ライセンス番号（VLN）番号を準備してください。

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、『Cisco Secure Web Appliance User Guide』の「Troubleshooting」セクション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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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。

© 2024 Cisco Systems, Inc. All rights reserved.

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。