

# Cisco Web セキュリティアプライアンス向け AsyncOS 14.1 リリースノート

初版：2021年6月9日

最終更新：2021年11月30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 14.1.0-047 LD \(限定導入\) の新機能：更新 \(1 ページ\)](#)
- [AsyncOS 14.1.0-041 LD \(限定導入\) の新機能：更新 \(1 ページ\)](#)
- [AsyncOS 14.1.0-032 LD \(限定導入\) の新機能 \(1 ページ\)](#)

#### AsyncOS 14.1.0-047 LD (限定導入) 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 14.1.0-047 の既知および修正済みの問題 \(14 ページ\)](#)」を参照してください。

#### AsyncOS 14.1.0-041 LD (限定導入) 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 14.1.0-041 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 14.1.0-032 LD (限定導入) 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 14.1.0-032 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。

機能	説明
Cisco Umbrella シームレス ID	

機能	説明
	<p>Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ (SWG) にパスすることができます。Cisco Umbrella SWG は、Web セキュリティアプライアンスから受信した認証済み識別情報に基づいて、Active Directory のユーザ情報をチェックします。Cisco Umbrella SWG は、ユーザを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。</p> <p>Web セキュリティアプライアンスは、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザ識別情報をパスします。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• Cisco Umbrella シームレス ID ヘッダーは、Web セキュリティアプライアンス上の同じ名前のヘッダーを上書きします。</li> <li>• Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine (ISE)、および Cisco Context Directory Agent (CDA) をサポートしていません。</li> <li>• Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。</li> <li>• Web セキュリティアプライアンスと Cisco Umbrella SWG のタイムゾーンが企業間で同じであることを確認してください。Cisco Umbrella SWG と Web セキュリティアプライアンスの時間差が 4 分を超える場合、Umbrella シームレス ID ヘッダーは Cisco Umbrella SWG 上で設定されません。</li> </ul> <p>ユーザガイドの「Cisco Umbrella シームレス ID」の項を参照してください。</p> <p><b>前提条件：</b></p> <p>Cisco Umbrella SWG Web ユーザインターフェイス上で次のタスクを実行します。</p> <ul style="list-style-type: none"> <li>• Web セキュリティアプライアンスのパブリック IP アドレスをネットワーク展開として登録します。</li> <li>• ユーザーとグループを使用してアクセスポリシーとアクセスルールを設定します ([<b>ポリシー (Policies)</b>] &gt; [<b>管理 (Management)</b>] &gt; [<b>すべてのポリシー (All Policies)</b>]) 。</li> </ul> <p>Cisco Web セキュリティアプライアンス ユーザインターフェイス上で次のタスクを実行します。</p> <ul style="list-style-type: none"> <li>• Cisco Umbrella SWG ルート証明書を Web セキュリティアプライアンスの信頼できる証明書に追加します ([<b>ネットワーク (Network)</b>] &gt; [<b>証明</b></li> </ul>

機能	説明
	<p>書管理 (Certificate Management) ] ) 。</p> <ul style="list-style-type: none"> <li>• Cisco Umbrella シームレス ID プロファイルページ ([Webセキュリティマネージャ (Cisco Security Manager) ]&gt;[Cisco UmbrellaシームレスID (Cisco Umbrella Seamless ID) ]&gt;[設定の編集 (Edit Settings) ]) で TCP Anycast IP (146.112.255.50) を設定します。</li> <li>• アップストリームプロキシグループとして適切なポートを使用して、Cisco Umbrella シームレス ID プロファイルでルーティングポリシーを設定します ([Webセキュリティマネージャ (Web Security Manager) ]&gt; [ルーティングポリシー (Routing Policies) ]) 。</li> <li>• Web セキュリティ アプライアンス ポリシーで AD 認証を有効にします。</li> <li>• 認証の復号化を有効にします。</li> </ul>

Cisco Web セキュリティアプライアンス向け AsyncOS 14.1 は、クライアントとサーバの TLSv1.2 セッション再開をサポートしています。

## AsyncOS 14.1.0-047 LD (限定導入) の動作の変更 : 更新

Cisco Umbrella シームレス ID の強化	<p>Web セキュリティアプライアンスは、ユーザーの基本認証の Active Directory から UPN 値を取得し、正しい UPN 値を Cisco Umbrella シームレス ID に送信します。この機能を利用するには、すべての Active Directory ユーザーにデフォルトまたはカスタマイズされた UPN 値を割り当てる必要があります。</p> <p>正常にログインするには、DomainName\UserName の形式で基本認証のログインを行う必要があります。</p>
-----------------------------	---

## AsyncOS 14.1.0-041 LD (限定導入) の動作の変更 : 更新

Cisco Umbrella シームレス ID の強化	<p>Web セキュリティアプライアンスは、認証されたユーザの UPN 値を Active Directory から取得し、Cisco Umbrella シームレス ID でユーザに正しい Web ポリシーを適用できるようにします。この機能を利用するには、すべての Active Directory ユーザにデフォルトまたはカスタマイズされた UPN 値を割り当てる必要があります。</p>
-----------------------------	---

## 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、をクリックすると、Cisco Web セキュリティアプライアンスが新しい外観になります。[試してみてください (Try it!!)] リンク。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 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：一般導入など）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せん。

- Sx90
- Sx95/F モデル



(注) Sx80 モデルは、AsyncOS バージョン 14.0 以降ではサポートされていません。

仮想モデル：

- S100v
- S300v
- S600v

## アップグレードパス

- [AsyncOS 14.1.0-047 へのアップグレード](#) (6 ページ)
- [AsyncOS 14.1.0-041 へのアップグレード](#) (7 ページ)
- [AsyncOS 14.1.0-032 へのアップグレード](#) (7 ページ)

## AsyncOS 14.1.0-047 へのアップグレード

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 14.1.0-047 にアップグレードできます。



(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。

- 14.1.0-041
- 14.1.0-032

### AsyncOS 14.1.0-041 へのアップグレード

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 14.1.0-041 にアップグレードできます。



(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。

- 14.1.0-032

### AsyncOS 14.1.0-032 へのアップグレード

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 14.1.0-032 にアップグレードできます。



(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。

- |              |              |              |              |
|--------------|--------------|--------------|--------------|
| • 11.7.3-025 | • 11.8.0-453 | • 12.0.1-268 | • 12.5.1-011 |
|              | • 11.8.1-023 | • 12.0.1-334 | • 12.5.1-035 |
|              | • 11.8.1-028 | • 12.0.2-004 | • 12.5.1-043 |
|              | • 11.8.1-511 | • 12.0.2-012 | • 14.0.0-467 |
|              | • 11.8.1-604 |              | • 14-0-1-014 |
|              | • 11.8.1-702 |              |              |
|              | • 11.8.2-009 |              |              |
|              | • 11.8.2-702 |              |              |
|              | • 11.8.3-021 |              |              |
|              | • 11.8.3-501 |              |              |

## 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、14.1.0-047 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。



(注) すでに Cisco Threat Response に登録している場合、この手順は適用されません。

### 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 ユーザー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](https://api.sse.cisco.com))

欧州 ([api.eu.sse.itd.cisco.com](https://api.eu.sse.itd.cisco.com))

APJC ([api.apj.sse.itd.cisco.com](https://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](https://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
- クラウドコネクタモードでの IPv6 と Kerberos は使用不可
- IPv6 アドレスの機能サポート



- アップグレード後の要件

## セキュリティ管理のための Cisco AsyncOS との互換性

Cisco コンテンツセキュリティ管理リリース向け AsyncOS とこのリリースとの互換性については、  
<http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html>  
 にある互換性のマトリックスを参照してください。



(注) このリリースは、現在使用可能なセキュリティ管理リリースと互換性がなく、使用することはできません。互換性のあるセキュリティ管理リリースは間もなく利用可能になります。

## 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](http://[2001:2:2::8]:8080) または [https://\[2001:2:2::8\]:8443](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
- 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 ログのページ
- 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」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。

(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

- 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。

```
HTTPSSS:NL:NL:NL:EXPI:IES:SEC:AMTA:SP:IDEA:DEF:SAE269A:PEZ66A:DEF:AS2394TAS26@M9AB4TAS18@M9AZ6TIS:GAKO:FOY35:SA25
```

**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。その後、アプライアンスに SSH 接続し、新しいキーを使用して接続を受け入れます。
- 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、ユーザガイド (PDF) の「File Reputation Filtering and File Analysis」の章を参照してください (この PDF は AsyncOS 8.8 のオンライン ヘルプよりも最新です)。

## 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ます。その影響についてのアラートがユーザーに送信され、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](http://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](#)」に表示される URL にアクセスしてください。

## 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](#)
- [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 14.1.0-047 の既知および修正済みの問題 \(14 ページ\)](#)
- [リリース 14.1.0-041 の既知および修正済みの問題 \(15 ページ\)](#)
- [リリース 14.1.0-032 の既知および修正済みの問題 \(15 ページ\)](#)

### リリース 14.1.0-047 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 14.1.0-041 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 14.1.0-032 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 Web Security Appliance User Guide』	<a href="http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html">http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html</a>
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ガイド	<a href="https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html">https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html</a>
仮想アプライアンス インストールガイド	<a href="https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html">https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html</a>

## 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](http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html) 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> 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/](http://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、ネットワークボジ図、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。

© 2021 Cisco Systems, Inc. All rights reserved.