

セキュアWebアプライアンスのリリース変更

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[リリースごとの変更履歴](#)

[オープンソースコンポーネント](#)

[freebsd](#)

[関連情報](#)

はじめに

このドキュメントでは、さまざまなバージョンのSecure Web Appliance(SWA)の主な変更点と追加機能について説明します。

前提条件

要件

この記事には特別な要件はありません。

この文書では、次の略語を使用します。

LD：限定的な導入。

GD：一般導入。

MD：メンテナンスの導入

ED：早期導入。

HP：ホットパッチ。

CLI：コマンドラインインターフェイス。

GUI：グラフィカルユーザインターフェイス

HTTP：ハイパーテキスト転送プロトコル。

HTTPS:Hypertext Transfer Protocol Secure (ハイパーテキスト転送プロトコルによるセキュリテイ)。

ECDSA:Elliptic Curve Digital Signature Algorithm (楕円曲線デジタル署名アルゴリズム)。

PID:プロセスID。

CTR:Cisco Threat Response (シスコの脅威対策) 。

AMP : 高度なマルウェア防御。

URL:Uniform Resource Locator。

CDA : コンテキストディレクトリエージェント。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

リリースごとの変更履歴

バージョン	Type	行動の変化	機能強化/追加機能
12.0.1-268	致死量	<ul style="list-style-type: none">- システムCPUおよびメモリの要件は、12.0リリース以降から変更されています。- デフォルトでは、アプライアンスでTLSv1.3が有効になっています。- 暗号「<code>TLS_AES_256_GCM_SHA384</code>」がデフォルトの暗号リストに追加されます。	<ul style="list-style-type: none">- Cisco AsyncOS 12.0リリースは、S680、S690、およびS695プラットフォーム向けに高性能(HP)のWebセキュリティアプライアンスを提供します。- 新しいサブコマンドhighperformanceがメインのadvancedproxyconfigコマンドの下に追加され、ハイパフォーマンスモードが有効または無効になります。- SWAとCisco Threat Response(CTR)ポータル統合- アプライアンスはTLSv1.3バージョンをサポートしています。- 設定ファイルのバックアップ機能が、サブメニュー「Log Subscriptions」から「Configuration File」の「System Administration」に移動します。- アプライアンスで、HTTPSプロキシのECDSA証明書のアップロードがサポートさ

			<p>れるようになりました。</p> <ul style="list-style-type: none"> - 新しい診断CLI proxyscannermapサブコマンドがdiagnostic > proxyの下に追加されました。各プロキシと対応するスキャナプロセス間のPIDマッピングを表示します。 - 新しいオプションsearchdetailsがCLIコマンドauthcacheの下に追加されました。 - 新しいサブコマンドCTROBSERVABLEがCLIコマンドreportingconfigの下に追加され、CTR監視可能ベースインデックスを有効または無効にします。
12.0.1-334	GD		<ul style="list-style-type: none"> - メインのadvancedproxyconfigコマンドの下に新しいサブコマンドスキャナが追加され、AMPエンジンでスキャンされるMIMEタイプが除外されます。
12.0.2-004	MD	<ul style="list-style-type: none"> - TLS 1.2以降のバージョンを使用して、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します。 - AMERICAS (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。 	<ul style="list-style-type: none"> - メインCLIコマンドadvancedproxyconfig > scanners > AMPに「Enter the number of concurrent scans to be supported by AMP」という新しいオプションが追加されました。 - メインのCLIコマンドadvancedproxyconfig > scannersで、長時間実行スキャンの削除のデフォルトのスキャン不能判定をタイムアウトに変更したり、その逆を新しいCLIサブコマンドevictionから変更したりできます。
12.02-012	MD		<ul style="list-style-type: none"> - アプライアンスのWebユーザインターフェイスでアラートメッセージがトリガーされる <p>プロキシのMalloc MemoryがプロキシのMalloc Memoryの制限の90%を超えると、「Web Proxy」の重大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。</p> <ul style="list-style-type: none"> - 新しいWebインターフェイスにより、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が提供されます。

12.0.3-005	MD		
12.0.3-007	MD		- 新しいURLカテゴリ更新通知
12.0.4-002	MD		
12.0.5-011	MD	<p>- TLSv1.2は、アプライアンス管理Webユーザーインターフェイスではデフォルトで有効になっています</p> <p>- Session Resumptionはデフォルトで無効になっています。</p>	- CDAのサポート終了を示すメッセージがCDA設定セクションに追加されます。
12.5.1-011	致死量	<p>- 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。</p> <p>- これらのログは、詳細を含むように変更されています。</p> <p>認証が失敗すると、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。</p> <p>認証フレームワークのログには、NTLM、BASIC、SSO (透過) などの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ます</p>	<p>- Cisco AsyncOS 12.5リリースは、S680、S690、およびS695プラットフォーム向けに高性能(HP)のWebセキュリティアプライアンスを提供します。これにより、現在のハイエンドアプライアンスのトラフィックパフォーマンスが向上します。</p> <p>- 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て、モデル (S680、S690、S695、S680F、S690F、およびS695F) でハイパフォーマンスモードを使用できるようになりました。</p> <ul style="list-style-type: none"> • Webトラフィックタップ • ボリュームと時間のクォータ • 全体的な帯域幅制限 <p>- IPスプーフィングプロファイルを作成してルーティングポリシーに追加することで、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。</p> <p>- YouTubeのカスタムURLカテゴリを作成し、YouTubeのカスタムカテゴリにポリシーを設定してセキュアなアクセス制御を実現できるようになりました。</p> <p>- 新しいWebインターフェイスでは、アプライアンスの現在のステータスと設定を表示する新しいページ([モニタリング] > [システム</p>

			<p>ステータス])がアプライアンスに表示されま す。</p> <p>- Cisco Success Network(CSN)機能を使用 すると、アプライアンスの機能使用状況に関 するテレメトリを収集できます。</p> <p>- ネットワーク、ログサブスクリプション、 およびその他の構成用のREST API。</p>
12.5.1- 035	GD	<p>- TLS 1.0/1.1の廃止 :</p> <p>TLS 1.2以降のバージョンを 使用して、アプライアンスを AMPファイアレピュテーショ ンサーバに接続します。 AMPファイアレピュテーショ ンサーバリストから南・北・ 中央アメリカ (レガシー) cloud- sa.amp.sourcefire.comが削除 されているため、アプライア ンスで南・北・中央アメリカ (レガシー) cloud- sa.amp.sourcefire.comを設定 することはできません。</p>	<p>- 認証用のキャッシュサイズの設定(Network > Authentication > Authentication Settings > Credential Cache Options)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。</p>
12.5.1- 043	GD		<p>- アラート・メッセージは、アプライアンス のWebユーザー・インターフェイスに表示さ れます([System Administration] > [Alerts] > [View Top Alerts])。</p> <ul style="list-style-type: none"> • 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 • mallocメモリの100 %でプロキシが再 起動したとき <p>どちらの場合も、「Webプロキシ」の重大な アラートを受信するように構成されたすべ ての「アラート受信者」にEメール通知が送信 されます。</p>
12.5.2- 007	MD		<p>- バナーに新しいURL Categories Update通 知が導入されました。また、今後のURLカテ ゴリの更新に関する電子メール通知もユーザ</p>

			に送信されます。
12.5.2-011	MD		
12.5.3-002	MD		
12.5.4-005	MD	<p>- Cisco AsyncOS 12.5.4バージョン以降、アプライアンス管理Webユーザインターフェイスに対してTLSv1.2がデフォルトで有効になっています。</p> <p>- Cisco AsyncOS 12.5.4バージョンへのアップグレード後は、デフォルトでセッション再開が無効になります。</p> <p>- CDAのサポート終了を示すメッセージがCDA設定セクションに追加されます。</p>	
12.5.4-011	MD更新		
12.5.5-004	MD		- Cisco AsyncOS 12.5へのアップグレード後、networktuningコマンドを初めて実行するときに、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る。
12.5.5-008	MD更新		
12.5.6-008	MD		
14.0.1-014	致死量	<p>- デフォルトでは、HTTP 2.0機能は無効になっています。この機能を有効にするには、<HTTP2>コマンドを使用します。</p> <p>- AsyncOS 14.0 for Cisco Webセキュリティアプライアンスは、クライアントとサーバでTLSv1.3セッション再開をサポートします。</p>	<p>- Cisco Webセキュリティアプライアンスは、Cisco SecureXとの統合をサポートするようになりました。</p> <p>- HTTP要求用のカスタムヘッダープロファイルを設定し、ヘッダーリライトプロファイルの下に複数のヘッダーを作成できます。</p> <p>- Active Directoryのヘッダーベースの認証スキームを設定できるようになりました。クラ</p>

	<p>– これらの証明書の有効期間が変更されます。</p> <ul style="list-style-type: none"> • HTTPS • ISE • SAAS • アプライアンス証明書 • デモ/管理証明書 <p>– ログサブスクリプションのログ名とファイル名が無効なためにアップグレードが失敗すると、アプライアンスのCLIおよびGUIにメッセージが表示されるようになりました。</p> <p>– デフォルトでは、ポーリング間隔は24時間に設定されています。</p> <p>– このリリースにアップグレードした後で、ベースDN (ベース識別名) フィールド ([ネットワーク] > [認証] > [レルムの追加]) が空の場合、LDAP認証の開始テストを実行できません。</p>	<p>クライアントとWebセキュリティアプライアンスはユーザを認証済みと見なし、認証やユーザクレデンシャルの入力を求めるプロンプトを再度表示しません。X-Authenticated機能は、Webセキュリティアプライアンスがアップストリームデバイスとして動作する場合に動作します。</p> <p>–</p> <p>アプライアンスのシステムステータスダッシュボードが拡張されました。</p> <ul style="list-style-type: none"> • Capacityタブ：時間範囲、システムCPUとメモリの使用量、帯域幅とRPS、機能別のCPU使用量、およびクライアント接続とサーバ接続に関する詳細を提供するタブです。 • StatusタブのProxy Traffic Characteristicsには、クライアントとサーバの接続に関する詳細情報が表示されます。 • サービス応答時間に、棒グラフの詳細と以前の日付の凡例データが含まれるようになりました。 <p>– 構成情報を取得し、アプライアンスの構成データに対して変更 (現在の情報の変更、新しい情報の追加、エントリの削除など) を行うことができます。また、管理ポリシー、アクセスポリシー、およびバイパスポリシーにREST APIを使用できます</p> <p>– Cisco AsyncOS 14.0バージョンは、TLSを介したWeb要求および応答に対してHTTP 2.0をサポートします。HTTP 2.0のサポートにはTLS ALPNベースのネゴシエーションが必要で、これはTLS 1.2バージョン以降からのみ使用可能です。</p> <p>このリリースでは、次の機能に対してHTTPS 2.0はサポートされていません。</p> <ul style="list-style-type: none"> • Webトラフィックタップ • 外部DLP • 全体の帯域幅とアプリケーションの帯
--	--	--

			<p>域幅</p> <ul style="list-style-type: none"> - HTTP 2.0の設定を有効または無効にするための新しいCLIコマンド<HTTP2>が導入されました。アプライアンスのWebユーザインターフェイスでは、HTTP 2.0を有効または無効にしたり、HTTP 2.0のドメインを制限したりすることはできません。 - HTTP 2.0の設定は、Cisco Secure Email and Web Manageではサポートされません - CLIでは、次のいずれかの機能のデフォルト証明書を使用しようとすると、新しい警告メッセージが表示されます。 <ul style="list-style-type: none"> • アプライアンス証明書 (Webユーザインターフェイスで、Network > Certificate Management > Appliance Certificateの順に移動します) • クレデンシャル暗号化証明書 (Webユーザインターフェイスで、Network > Authentication > Edit Settings > Advancedセクションに移動します) • HTTPS管理UI証明書 (コマンドラインインターフェイスでcertconfig > SETUPを使用) - certconfigの下に新しいサブコマンドOCSPVALIDATION_FOR_SERVER_CERTが追加されました。この新しいサブコマンドを使用すると、LDAPおよびアップデータサーバ証明書のOCSP検証を有効にできます。証明書の検証が有効な場合、通信に含まれる証明書が失効するとアラートを受信できます。 - アプライアンスと認証サーバ間のポーリング機能を設定するために、新しいCLIコマンドgathereredconfigが追加されました。 - アプライアンスでスマートライセンス機能を設定しながら、管理インターフェイスとデータインターフェイスのいずれかを選択できるようになりました。
14.0.1-040	致死量	- スマートソフトウェアライセンスを有効にし、Webセキュリティ	- Cisco Smart Software Managerポータルで作成されたスマートアカウントの詳細は、

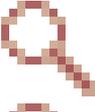
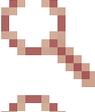
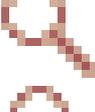
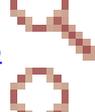
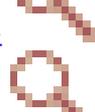
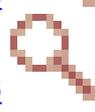
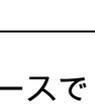
		<p>アプライアンスをCisco Smart Software Managerに登録すると、シスコクラウドサービスが提供されます。</p> <p>(Network > Cloud Service Settings)を選択すると、Cisco Cloud Servicesポータル経由でセキュアWebアプライアンスが自動的に有効化され、登録されます。</p> <p>- スマートライセンスがアプライアンスに登録されている場合、Cisco Cloud Serviceを無効にしたり、登録を解除したりすることはできません。</p> <p>- アプライアンスをCisco Smart Software Managerに登録済みで、Cisco Cloud Servicesを設定していない場合、AsyncOS 14.0.1-040にアップグレードすると、Cisco Cloud Servicesは自動的に有効になります。デフォルトでは、地域は南北アメリカとして登録されており、必要に応じて地域（ヨーロッパおよびAPJC）を変更できます。</p> <p>- スマートライセンスがアプライアンスに登録されている場合、Cisco Cloud Serviceを無効にしたり、登録を解除したりすることはできません。</p>	<p>CLIのsmartaccountinfoコマンドで表示できません。</p> <p>- Cisco Cloud Servicesの証明書の有効期限が切れているか、間もなく切れる場合、AsyncOS 14.0.1-040へのアップグレード後に、Cisco Cloud Serviceによって証明書が自動更新されます。</p> <p>- Cisco Cloud Services証明書が期限切れになった場合、CLIのcloudserviceconfig > fetchcertificateサブコマンドからCisco Talos Intelligence Servicesポータルに新しい証明書をダウンロードできます。</p> <p>- Cisco Cloud Serviceポータル(CLIでcloudserviceconfig > autoregisterサブコマンド)を使用して、Webセキュリティアプライアンスを自動登録できます。</p> <p>- CLIのupdateconfig > clientcertificateサブコマンドから、仮想アプライアンスおよびハードウェアアプライアンスの証明書をロードできます。</p> <p>- バナーに新しいURL Categories Update通知が導入されました。</p> <p>URLカテゴリの更新に関する電子メール通知もユーザに送信されます。</p>
14.0.1-053	GD		
14.0.1-503	HP		
14.0.2-012	MD	<p>- Cisco AsyncOS 14.0.2バージョンでは、Appliance Management Web User InterfaceのSystem Administrator > SSL ConfigurationでTLSv1.2がデフォルトで有効になっています。</p>	<p>- CDAのサポート終了を示すメッセージがCDA設定セクションに追加されます。</p> <p>- Test Interfaceドロップダウンリストから、Smart License Registrationのデータまたは管理インターフェイスを選択できるようになり</p>

		<p>– セッション再開はデフォルトで無効になっています。</p>	<p>ました。</p>
14.0.3-014	MD	<p>- Cisco AsyncOS 14.0へのアップグレード後、networktuningコマンドを初めて実行するときに、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る。</p>	
14.0.3-502	HP	<p>- Secure Web Applianceが高パフォーマンスモードで動作している場合、ヒープ制限の枯渇により、高い遅延とacceptハンドラが無効になります。これにより、接続数が少なくなります。</p>	
14.0.4-005	MD		
14.5.0-498	致死量	<p>– 製品のブランド変更：</p> <ul style="list-style-type: none"> • エンドポイント向けAMP、高度なマルウェア防御、AMPはセキュアエンドポイント • スレッドグリッド（ファイル分析）がマルウェア分析に変更されました <p>– 誤分類要求はHTTPS経由で送信されるため、セキュリティアラート通知を受信しません。</p> <p>- Sambaのバージョンがバージョン4.11.15にアップグレードされました。</p> <p>- Appliance Management WebユーザーインターフェイスのSystem Administrator > SSL Configurationで、TLSv1.2がデフォルトで有効になっている。</p> <p>- AsyncOS 14.5の新規インストー</p>	<p>- Secure Web Applianceは、DNSサーバから受信したDNS応答が暗号署名をサポートしていることを検証できるようになりました。</p> <p>- Secure Web Applianceは、クライアントによって開始される同時接続の数を設定値に制限します。</p> <p>- AsyncOSリリース14.5では、Cisco WebセキュリティアプライアンスはCisco Secure Web Applianceにブランド変更されました。</p> <p>– クライアントのWebブラウザにEUNページが表示されると、Decrypt Policyグループ内のアクセスログ決定タグにEUN (End user Notification)が付加されます。</p> <p>– ポリシーの複製機能を使用すると、ポリシーの設定をコピーまたは複製し、新しいポリシーを作成できます。</p> <p>– クォータプロファイルで帯域幅の値を構成し、アクセスポリシーURLカテゴリまたは全体的なWebアクティビティのクォータにクォータプロファイルをマップすることで、トラフィック帯域幅を管理できます。</p>

		<p>ルでは、HTTPSプロキシページの期限切れおよび不一致ホスト名証明書設定値が、デフォルトでモニタではなくドロップとして選択されます。</p>	<p>- 管理ポリシー、復号化ポリシー、ルーティングポリシー、IPスプーフィングポリシー、マルウェア対策とレピュテーション、認証シーム、Cisco Smart Softwareライセンス、Cisco UmbrellaシームレスID、アイデンティティサービス、システムセットアップを設定するためのREST API。</p> <p>- ISE-SXP導入をCisco Secure Web Applianceと統合してパッシブ認証を行うことができます。これにより、SXPを介して公開されるSGTからIPへのアドレスマッピングを含む、定義されたすべてのマッピングを取得できます。</p> <p>- Cisco UmbrellaシームレスID機能を使用すると、アプライアンスは、認証が成功した後にユーザ識別情報をCisco UmbrellaセキュアWebゲートウェイ(SWG)に渡すことができます。</p> <p>- CDAのサポート終了を示すメッセージがCDA設定セクションに追加されます。</p> <p>- Test Interfaceドロップダウンリストから、Smart License Registrationのデータまたは管理インターフェイスを選択できるようになりました。</p> <p>- Cisco AsyncOS 14.5へのアップグレード後、networktuningコマンドを初めて実行するときに、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る。</p>
14.5.0-537	GD		<p>- Secure Web Appliance(CWA)のクローンオプションを使用するこれらのポリシーは、Cisco Secure Email and Web Manager(SMA)でも管理できます。</p> <ul style="list-style-type: none"> • アクセスポリシー • 識別プロファイル • 復号化ポリシー • ルーティングポリシー
14.5.1-008	MD		

14.5.1-016	MD		
14.6.0-108	致死量		<p>- AsyncOS 14.6は、Cisco UmbrellaとCisco Secure Web Appliance(SWA)のサポートを提供します。UmbrellaとセキュアWebアプライアンスの統合により、UmbrellaからセキュアWebアプライアンスへの共通のWebポリシーの導入が容易になります。</p>
15.0.0-322	致死量	<p>- FreeBSDバージョンはFreeBSD 13.0にアップグレードされました。</p> <p>- Cisco SSLバージョン1.0.2からCisco SSLバージョン1.1.1</p> <p>- 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。</p> <p>- 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。</p>	<p>- Smart Software Licensing機能に対する次の機能拡張</p> <ul style="list-style-type: none"> • ライセンス予約 • デバイスLED変換：Secure Web Applianceをスマートライセンスに登録すると、現在の有効な従来のライセンスがすべてDLC（デバイスLED変換）プロセスによってスマートライセンスに自動的に変換されます。変換されたライセンスは、CSSMポータル仮想アカウントで更新されます。 <p>- クォータプロファイルで帯域幅の値を構成してトラフィック帯域幅を管理し、クォータプロファイルを復号化ポリシーとアクセスポリシー、URLカテゴリ、または全体的なWebアクティビティのクォータにマッピングできます。</p> <p>- ポリシーの複製機能を使用すると、ポリシーの設定をコピーまたは複製し、新しいポリシーを作成できます。</p> <p>- アプリケーション検出および制御(ADC)エンジン：</p> <p>アクセプタブルユースポリシー(aup)のコンポーネント。webトラフィックを検査して、アプリケーションに使用されるwebトラフィックをより深く理解し、制御します。</p> <p>AsyncOS 15.0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。</p>

			<ul style="list-style-type: none"> - ADC設定用のREST API - 管理者は、デフォルトのユーザ名v3get以外のカスタムSNMPv3ユーザ名の設定を選択できます。 - カスタムヘッダーの最大長は16kです。 - セキュア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。
15.0.0-335	GD	<ul style="list-style-type: none"> -デバイス主導の変換 – スマートライセンスでSecure Web Applianceを登録すると、現在の有効な従来のライセンスはすべて、DLC (デバイス主導の変換) プロセスによって自動的にスマートライセンスに変換されます。変換されたライセンスは、CSSMポータル上の仮想アカウントで更新されます。 - デフォルトでは、AVCは有効になっています。 - 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。 - FreeBSD 13.0はCisco SSLバージョン1.1.1とのみ互換性があります。 FreeBSD 13.0へのSSH接続でサポートできるのは、Cisco SSH互換の暗号、MacおよびKexアルゴリズムだけです。 - AsyncOS15.0 GDリリースの一部として、Secure Web ApplianceのDCA機能が無効にな 	<ul style="list-style-type: none"> - ライセンス予約 : Cisco Smart Software Manager(CSSM)ポータルに接続しなくても、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通信することなく、セキュリティの高いネットワーク環境にセキュアなWebアプライアンスを導入するユーザにとって有益です。 - クォータプロファイルで帯域幅の値を構成し、クォータプロファイルを復号化ポリシーおよびアクセスポリシーのURLカテゴリまたは全体的なWebアクティビティのクォータにマッピングすることで、トラフィック帯域幅を管理できます。 - クローンポリシー機能を使用すると、ポリシーの設定をコピーまたはクローンし、新しいポリシーを作成できます。 - Application Discovery and Control(ADC)エンジンをサポートします。これは、アクセプタブルユースポリシーコンポーネントであり、Webトラフィックを検査して、アプリケーションに使用されるWebトラフィックをより深く理解し、制御します。 これで、AVCまたはADCエンジンのいずれかを使用してWebトラフィックを監視できます。 - ADCエンジンは高性能モードをサポートします。 - 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の取得

		<p>っています。このバージョンにアップグレードした後で、セキュリティサービス>アクセプタブルユースコントロールの順に選択し、DCAチェックボックスをオンにすると、この機能を有効にできます。</p> <p>- マルチプロキシSWA(S690、S695、S1000V)では、プロキシMallocメモリのSNMP OIDに対するSNMPWALK/SNMPGET操作はサポートされていません。</p>	<p>、および変更（現在の情報の変更、新しい情報の追加、エントリの削除など）の実行が可能になりました。</p> <p>-Adminでは、デフォルトのユーザ名v3get以外のカスタムSNMPv3ユーザ名の設定を選択できます。</p> <p>- Web要求に対するカスタムヘッダーの最大長は16kです。</p> <p>- セキュア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</p>
15.0.0-364	HP	<p>次の不具合に対する修正が含まれています。</p> <p>Cisco Bug ID CSCvz26149 </p> <p>Cisco Bug ID CSCwf78874 </p> <p>Cisco Bug ID CSCwf84371 </p> <p>Cisco Bug ID CSCwh31573 </p> <p>Cisco Bug ID CSCwh37834 </p> <p>Cisco Bug ID CSCwh41379 </p> <p>Cisco Bug ID CSCwh48523 </p> <p>Cisco Bug ID CSCwh71926 </p>	
15.1.0-287	致死量	<p>- AsyncOS 15.1以降のリリースでは、スマートソフトウェアライセンスが必須です。</p> <p>- Cisco UmbrellaとCisco Secure Web Applianceの統合により、UmbrellaからSecure Web Applianceへの共通のWebポリシーの導入が容易になります。また</p>	

		、Umbrellaダッシュボードを使用してポリシーを設定し、ログを表示できます。	
--	--	--	--

オープンソースコンポーネント

SWAで使用されるオープンソースコンポーネントの変更のリストを次に示します。

バージョン	11.8.X (2015年 9月)	12.0.X (2015年 9月)	12.5.X (2015年 9月)	14.0.X (2015年 9月)	14.5.X (2015年 9月)	14.6.X (2015年 9月)
freebsd	10.4	10.4	10.4	11.2	11.2	11.2

関連情報

- [AsyncOS 12.0 for Cisco Webセキュリティアプライアンスのリリースノート – Cisco](#)
- [AsyncOS 12.5 for Cisco Webセキュリティアプライアンスのリリースノート – Cisco](#)
- [AsyncOS 14.0 for Cisco Webセキュリティアプライアンスのリリースノート – Cisco](#)
- [AsyncOS 14.5 for Cisco Secure Web Applianceのリリースノート：シスコ](#)
- [コンテンツセキュリティのリリース用語は何ですか。\(cisco.com\) を設定できます。](#)
- [Cisco Secure Email & Web仮想アプライアンスインストールガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)
- [AsyncOS 15.1 for Cisco Secure Web Applianceのリリースノート：シスコ](#)
- [AsyncOS 15.0ホットパッチ1に関するCisco Secure Webアプライアンス向けリリースノート – シスコ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。