AsyncOS 11.8.x for Cisco Web Security Appliances リリースノート

発行日:2019 年 7 月 22 日

最終更新日:2021 年 1 月 25 日

目次

Cisco Systems, Inc.
www.cisco.com

最新情報

AsyncOS 11.8.3-018 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 11.8.3-018 の既知および修正済みの問題（23 ページ）」および「Asyncos 11.8.3-018 の動作の変更（8 ページ）」を参照してください。

AsyncOS 11.8.2-009 の新機能 MD（メンテナンス導入）

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 11.8.2-009 の既知および修正済みの問題（23 ページ）」を参照してください。

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 11.8.2 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、https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/content_security_general/Decommissioning_Legacy_File_Reputation_Servers_for_Cisco_Web_Security_Appliance.pdf を参照してください。

このリリースでは、コマンド ライン インターフェイスに次の変更が加えられています。

新規コマンドライン	説明
AMP での最大同時スキャン数の設定をサポート	`AMP` でサポートされる同時スキャン数の入力オプションが、メインの CLI コマンドに新たに追加されました。 `advancedproxyconfig > scanners > AMP.` この新しい CLI オプションを使用すると、AMP でサポートされる同時スキャン数を設定できます。すべてのモデルのデフォルト値は、上限の 250 です。
長時間実行中のスキャン削除時の判定変更をサポート	新しい CLI サブコマンド `eviction` がメインの CLI コマンドに追加されました。 `advancedproxyconfig > scanners` この新しい CLI サブコマンドを使用すると、長時間実行中のスキャン削除の判定設定をデフォルトの**スキャン不能**から**タイムアウト**に、またはその逆に変更できます。

AsyncOS 11.8.1-023 の新機能 MD（メンテナンス導入）

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 11.8.1-023 の既知および修正済みの問題（23 ページ）」を参照してください。

このリリースでは、`advanced proxyconfig` CLI コマンドの下に新しい `scanners` サブコマンドが含まれています。

機能拡張	説明
AMP エンジンによるスキャンからの MIME タイプの除外が可能	新しいサブコマンド `scanners` がメインの `advanced proxyconfig` コマンドの下に追加され、AMP エンジンによるスキャン対象から MIME タイプを除外できるようになりました。`scanners` サブコマンドを使用するには、「Adaptive Scanning」機能を無効にする必要があります。 `scanners` サブコマンドを使用して、AMP エンジンでスキャンする必要のない MIME タイプを追加し、スキャンのパフォーマンスを向上させることができます。デフォルトの MIME タイプのオプションは、「image/ALL and text/ALL」です。 MIME タイプを追加するには、デフォルトのオプションの後に追加する必要があります。たとえば、ビデオと音声の MIME タイプを追加する場合は、次の形式にする必要があります。 「image/ALL and text/ALL video/ALL audio/ALL」

AsyncOS 11.8.0-453 GD（全面導入）更新の新機能

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 11.8.0-453 の既知および修正済みの問題（24 ページ）」を参照してください。

AsyncOS 11.8.0-440 GD（全面導入）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 11.8.0-440 の既知および修正済みの問題（24 ページ）」を参照してください。

AsyncOS 11.8.0-429 LD（限定導入）更新の新機能

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 11.8.0-429 の既知および修正済みの問題（24 ページ）」を参照してください。

AsyncOS 11.8.0-414 LD の新機能（限定導入）

機能	説明
ISE/ISE-PIC 統合の機能拡張	• セキュリティ グループ タグと Active Directory グループを使用してアクセス ポリシーを作成できます。 • ISE/ISE-PIC による透過的な識別に失敗したユーザの場合、Active Directory ベースのレルムを使用してフォールバック認証を設定できます。 • 仮想デスクトップ環境（Citrix、Microsoft 共有/リモート デスクトップ サービス）でユーザの認証を設定できます。 （注） 仮想デスクトップ環境（VDI）ユーザのフォールバック認証はサポートされていません。 （注） シスコ ターミナル サービス エージェントと Microsoft サーバ設定で、リモート デスクトップ セッションの最大数が同じであることを確認します。これにより、誤ったセッション情報が ISE から Web セキュリティ アプライアンスに送信されないようにし、新しいセッションの誤認証が回避されます。 ユーザ ガイドの「Identity Services Engine（ISE）/ISE パッシブ ID コントローラ（ISE-PIC）サービスの概要」のトピックを参照してください。
ドメイン マップ	アプライアンスを設定し、クライアント要求と宛先サーバの証明書チェックを変更せずに特定の HTTPS トラフィックのパススルーを許可できるようになりました。 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
アプライアンスの設定のロールバック	新しい CLI コマンド `rollbackconfig` が追加されました。このコマンドを使用して、以前に確定された 10 の設定のいずれかにロールバックします。ロールバック設定機能は、デフォルトで有効になっています。 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。
アプライアンス設定の自動バックアップ	新しいログ タイプ「設定履歴ログ」が追加されます。このログ タイプを使用して、コンフィギュレーション ファイルをサブスクライブし、FTP または SCP を介してリモートに配置されたバックアップ サーバに送信します。 ユーザ ガイドの「ログによるシステム アクティビティのモニタ」の章を参照してください。
外部フィードおよび O365 フィードの例外リストのサポート	[カスタムおよび外部 URL カテゴリ（Custom and External URL Categories）] のフィード ファイルからサイトと正規表現を除外できます。これは、[外部ライブフィード カテゴリ（External Live Feed Category）] にのみ適用されます。 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。
O365 Web サービス フィードのプロキシ バイパス設定	プロキシ バイパス リストには、カスタム URL カテゴリ（O365 URL）のドメイン名または IP アドレスを追加できます。カスタム URL カテゴリのドメイン名または IP アドレスを手動で追加する必要はありません。 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。
ファイル分析に向けた Cisco AMP Threat Grid クラスタリングのサポート	以下の方法で、ファイル分析に向けてスタンドアロンまたはクラスタの Cisco AMP Threat Grid アプライアンスを追加できるようになりました。 Web インターフェイスの [セキュリティ サービス（Security Services）] > [ファイル レピュテーションとファイル分析（File Reputation and Analysis）] ページ。 ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。
ファイル分析のしきい値の設定	許容されるファイル分析 スコアのしきい値の上限を設定できるようになりました。しきい値設定に基づいてブロックされるファイルは、詳細マルウェア保護レポートの [着信マルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで、[カスタムしきい値（Custom Threshold）] として表示されます。 ユーザ ガイドの「File Reputation Filtering and File Analysis」の章を参照してください。
複数の Web カテゴリを使用した URL フィルタリングの設定	複数の URL カテゴリを使用して URL フィルタリング エンジンを設定できるようになりました。複数の URL カテゴリ機能は、アクセス ポリシーのみに適用されます。 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。

機能	説明
新しい脅威カテゴリのサポート	現在、アプライアンスには新しい 22 の脅威カテゴリがあります。新しい脅威カテゴリのリストは、新しいカテゴリが使用可能になるたびに、アプライアンスの新しい Web インターフェイスで自動的に更新されます。 『Release Notes for URL Category and Threat Category Updates for Cisco Web and Email Security Appliances』を参照してください。
モニタリングおよびトラッキングのための新しい Web インターフェイス	アプライアンスには、レポートをモニタリングおよびトラッキングするための新しい Web インターフェイスが追加されました。 [モニタリング (Monitoring)] ページでは、一般的なレポートおよび脅威レポートに分類されたレポートを表示できます。 [トラッキング (Tracking)] ページでは、メッセージまたはメッセージのグループに関して、検索条件に応じて Web インターフェイスの [トラッキング (Tracking)] > [検索 (Search)] ページから検索できます。ユーザ ガイドの「メッセージ トラッキング」の章を参照してください。 詳細については、「新しい Web インターフェイスの Web セキュリティ アプライアンス レポート」の章を参照してください。 新しい Web インターフェイスにアクセスするには、ユーザ ガイドの「製品とリリースの概要」の章にある「アプライアンスの Web インターフェイスへのアクセス」のトピックを参照してください。また、「新しい Web インターフェイスへのアクセス (9 ページ)」を参照してください。

(注) Web レピュテーションエンジンの名前が Talos Intelligence Engine に変更されました。

高度なマルウェア防御の事前分類エンジンの既存バージョンは 1.0.0-113 です。高度なマルウェア防御の事前分類エンジンが最近更新され、バージョンが 1.0.0-007 から 1.0.0-113 に変更されました。

(注) アプライアンスは、工場出荷時のデフォルト モードで次のポートのみをサポートします。
- 8080
- 8443
- 22

(注) Cisco Web セキュリティアプライアンスは FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました (FIPS 140-2 認定# 2984)。

動作における変更

Asyncos 11.8.3-018 の動作の変更

ログ サブスクリプション（Log Subscriptions）	ディスク容量のサイズ制限内でのみ、ログサブスクリプションを設定できるようになりました。 ディスク容量を超えるサイズ制限が設定された既存のログサブスクリプションが存在する場合、アプライアンスの Web ユーザインターフェイスと CLI に警告メッセージが表示されるようになりました。 次の操作を行うと、メッセージが表示されます。 • Web ユーザインターフェイスを介したログサブスクリプションに関する変更のコミット • [マイダッシュボード（My Dashboard）] ページで Web ユーザインターフェイスにログインまたは接続 • CLI 経由でのログインまたは接続

Asyncos 11.8.x の動作の変更

TLS バージョン	デフォルトでは、管理/データプレーンで提供される次の必須サービスの最低要件のバージョンは TLS 1.1 です。 • WSA WUI • プロキシ サービス • セキュア LDAP • RADSEC • セキュア ICAP サービス • サービスの更新 **（注）** アプライアンスが 11.8.x バージョンにアップグレードされた後、デフォルトでは TLS 1.0 が無効になります。 **（注）** TLS 圧縮機能は、セキュリティを最適化するためにデフォルトで無効になっています。この機能を有効にするには、アプライアンスを 12.0 以降のバージョンにアップグレードします。以前のバージョンで TLS 圧縮を有効にすると、アプライアンスの機能に問題が発生する可能性があります。
FTP プロキシ サービス	デフォルトでは、FTP プロキシ サービスは無効になっています。FTP プロキシがアプライアンスで有効になっている場合は、アップグレード後も有効なままになります。
認証変更の監査ログ	監査ログに、認証ポリシーに加えられた変更が表示されるようになりました。ユーザが認証ポリシー（[システム管理（System Administration）] > [ユーザ（Users）]）の権限と特権を変更した場合、同じものが監査ログに表示されます。

デフォルトの証明書有効期間の変更	アプライアンスのデフォルトの証明書有効期間が 10 年から 5 年に短縮されました。
SSH クライアント/サーバ サービスの暗号方式。	FIPS モードでは、SSH クライアント/サーバサービスでサポートされている公開キー認証暗号は、`ssh-rsa` のみです。 FIPS モードの SSH クライアントサービスでは、次の暗号方式が追加でサポートされています。 • `aes128-ctr` と `aes256-ctr` • `ecdh-sha2-nistp256`、`ecdh-sha2-nistp384`、および `ecdh-sha2-nistp521`

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、**[Web セキュリティアプライアンスをクリックして新しい外観を試してください。(Web Security appliance is getting a new look. Try it!!)]** 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、`trailerblazerconfig` 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（最新の安定バージョン）
- Mozilla Firefox（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 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。

このリリースでサポートされているハードウェア

- 次の仮想モデル：
  - S100V
  - S300V
  - S600V
- 次のハードウェア モデル：
  - x80
  - x90
  - x95

一部のハードウェアモデルでは、この AsyncOS リリースをインストールまたはアップグレードする前に、メモリをアップグレードする必要があります。詳細については、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

アップグレードの方法

AsyncOS 11.8.3-018（MD：メンテナンス導入）へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

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 AsyncOS for Cisco Web Security Appliances リリース 11.8.3-018 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
- 11.5.1-115
- 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
- 11.7.0-334
- 11.7.0-406
- 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
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429
- 11.8.0-440
- 11.8.0-446
- 11.8.0-450
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604
- 11.8.2-009
- 11.8.2-702

AsyncOS 11.8.2-009（MD - メンテナンス導入）へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

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。

Cisco Web セキュリティアプライアンス向け AsyncOS リリース 11.8.2-009 へは、次のバージョンから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
- 11.5.1-115
- 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
- 11.7.0-334
- 11.7.0-406
- 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
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429
- 11.8.0-440
- 11.8.0-446
- 11.8.0-450
- 11.8.0-453
- 11.8.1-023
- 11.8.1-028
- 11.8.1-604

AsyncOS 11.8.1-023（MD - メンテナンス導入）へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

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。

Cisco Web セキュリティアプライアンス向けの AsyncOS リリース 11-8-1-023 へは次のバージョンから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
- 10.6.0-240
- 10.6.0-244
- 11.5.1-115
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 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
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429
- 11.8.0-440
- 11.8.0-446
- 11.8.0-450
- 11.8.0-453

AsyncOS 11.8.0-453（GD：全面導入）更新へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

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。

Cisco Web セキュリティアプライアンス向けの AsyncOS リリース 11-8-0-453 へは次のバージョンから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
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.5.3-504
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.7.1-006
- 11.7.1-020
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429
- 11.8.0-440
- 11.8.0-446
- 11.8.0-450

AsyncOS 11.8.0-440（GD：全面導入）へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

Cisco Web セキュリティアプライアンス向け AsyncOS リリース 11-8-0-440 へは次のバージョンから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
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.7.0-704
- 11.8.0-348
- 11.8.0-414
- 11.8.0-429

AsyncOS 11.8.0-429（LD：限定導入）更新へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

Cisco Web セキュリティアプライアンス向け AsyncOS リリース 11-8-0-429 へは、次のバージョンから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
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.8.0-348
- 11.8.0-414

AsyncOS 11.8.0-414（LD：限定導入）へのアップグレード

（注） アップグレード プロセスを開始する前に、「アップグレード前の要件（15 ページ）」と「インストールおよびアップグレードに関する注意事項（16 ページ）」を参照してください。

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 11-8-0-414 にアップグレードできます。

- 10.1.4-017
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 10.6.0-240
- 10.6.0-244
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.5.3-007
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407
- 11.7.0-418
- 11.8.0-348

（注） Cisco Web セキュリティ アプライアンスの AsyncOS 11.8 にアップグレードした後、TLS v1.1 が Web ユーザ インターフェイスにアクセスできるようにするには、ブラウザを有効にする必要があります。

アップグレード前の要件

AsyncOS 11.8 for Cisco Web Security Appliances は、ISE リリース 2.4 のみをサポートしています。

その他の要件は次のとおりです。

CTA ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード

AsyncOS 11.0 から 11.5 へのアップグレード

AsyncOS 11.0 バージョンで CTA ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cta_log」であること。
- ログの取得方法が「scp_push」であること。
- [CTA が有効（CTA Enable）] チェックボックスがオンになっていること。11.5 バージョンにアップグレードした後でのみ、CTA ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準ログと見なされます。

AsyncOS 11.0 より前のリリースから 11.5 へのアップグレード

AsyncOS 11.0 より前のリリースで CAT ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cta_log」であること。
- ログの取得方法が「scp_push」であること。11.5 バージョンにアップグレードした後でのみ、CTA ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準ログと見なされます。

Cloudlock ログ サブスクリプションを使用した以前のバージョンの AsyncOS から AsyncOS 11.5 へのアップグレード

AsyncOS の以前のリリースで Cloudlock ログをすでに設定している場合に AsyncOS 11.5 バージョンにアップグレードするには、次の条件を満たす必要があります。

- ログ名が「cloudlock_log」であること。
- ログの取得方法が「scp_push」であること。11.5 バージョンにアップグレードした後でのみ、Cloudlock ログと見なされます。
- 上記の条件のいずれかが満たされていない場合、アップグレード後にログは標準的な W3C ログと見なされます。

AsyncOS 11.5.x 以前のバージョンから AsyncOS 11.8 へのアップグレード

AsyncOS バージョン 11.5.x 以前から AsyncOS 11.8 にアップグレードする前に、次の条件を満たしている必要があります。

- アプライアンスが AsyncOS 11.5.x 以前のバージョンで実行されている場合は、AsyncOS 11.8 にアップグレードする前に、アプライアンスのすべてのセキュリティ エンジンを更新する必要があります。
- AsyncOS バージョン 11.5.x 以前の既存のアプライアンスのセキュリティ エンジンを更新できない場合は、最初にアプライアンスを AsyncOS 11.7.0 にアップグレードし、次に AsyncOS 11.8 バージョンにアップグレードします。

（注） アプライアンスで WBRS エンジンを無効にし、非同期 11.5.x バージョンから直接 AsyncOS 11.8 にアップグレードした場合は、Cisco TAC にお問い合わせください。アプライアンスがリモートからアクセス可能であることを確認します。

アップグレードの前にアップグレード後の要件を確認

既存の機能の中には、変更を加えるまではアップグレード後に機能しないものがあります。ダウンタイムを最小限に抑えるため、アップグレード前にこれらの要件について理解し、準備します。「重要：アップグレード後に必要なアクション」を参照してください。

インストールおよびアップグレードに関する注意事項

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

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 ロゴのページ
- 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。

(注) 次に、Microsoft Hyper-V generation 1 プラットフォームに導入された仮想 Web セキュリティ アプライアンス(FreeBSD 10. x)の制限事項を示します。

- `etherconfig` CLI コマンドを使用して、仮想アプライアンス インターフェイスを変更することはできません。
- `ifconfig` CLI コマンドは、デュプレックスモードで動作している場合でも、仮想アプライアンス インターフェイスのステータスを Unknown またはシンプレックスとして表示します。

ただし、上記の制限により、アプライアンスのパフォーマンスに影響はありません。

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

ステップ 1 「仮想アプライアンスの展開（18 ページ）」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。

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。

デモ セキュリティ証明書の暗号化の強度

デモ セキュリティ証明書の暗号化強度は、AsyncOS 8.5 へのアップグレードの前後で 1024 ビットです。AsyncOS 9.1.1 へアップグレードすると、2048 ビットになります。AsyncOS 10.5 以降では、FIPS モードが有効になっている場合、デモ セキュリティ証明書の強度は 4096 ビットに変更されます。

アップグレード後の再起動

アップグレード後に Web Security Appliance を再起動する必要があります。

AsyncOS for Web のアップグレード

はじめる前に

アップグレード前の要件を満たします。「アップグレード前の要件（15 ページ）」を参照してください。

ステップ 1 管理者としてログインします。

ステップ 2 [システム管理（System Administration）] > [設定ファイル（Configuration File）] ページで、Web Security Appliance 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 3 [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（Upgrades Options）] をクリックします。

ステップ 4 必要に応じて、[ダウンロード（Download）] または [ダウンロードとインストール（Download and Install）] を選択します。

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 5 [続行（Proceed）] をクリックして、アップグレードまたはダウンロードを開始します。表示される質問に答えます。

[ダウンロードのみ(Download only)] を選択した場合は、AsyncOS アップグレード イメージがアプライアンスにダウンロードされ、管理者はダウンロードしたイメージを後でインストールすることを選択できます。

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)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、Web Security 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。

通常、デフォルトでは新しい機能は有効になっていません。

(注) Nexus 56128P スイッチインターフェイスを使用して Cisco Web セキュリティアプライアンス S690F をアップグレードまたは再起動すると、10G ファイバインターフェイスのリンクステータスに「down」と表示されます。この問題を解決するには、次の手順を実行します。

1. CLI コマンド `etherconfig` > `media` を使用して、アプライアンス インターフェイスの「*media*」を **10Gbase-SR** に設定します。
2. コミットしてアプライアンスを再起動します。

(注) ファイバインターフェイス上で、1G SFP から 10G SFP(またはその逆)へのすべての SFP スワップを行った後、S695F Cisco Web セキュリティアプライアンスをリブートします。これにより、目的の帯域幅の変更に合わせてドライババッファの設定が適切に調整されます。

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(21 ページ)
- 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(21 ページ)
- 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(22 ページ)
- ファイル分析:分析対象のファイル タイプの確認(22 ページ)
- 正規表現のエスケープされていないドット(22 ページ)

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:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA
```

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。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport に示されているセキュリティの脆弱性がアプライアンスに存在していれば、アップグレード時に修正されます。

(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、高度なマルウェア保護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）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（25 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

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

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 11.8.3-018 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8.3-018&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=11.8&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.2-009 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.2-009&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.1-023 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.1-023&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.0-453 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-453&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.0-440 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-440&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.0-429 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-429&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.8.0-414 の既知および修正済みの問題

修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0-414&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.8.0&sb=afr&sts=open&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

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。

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://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(release)] フィールドに、リリースのバージョン(たとえば、11.8.0)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

この製品のドキュメントは http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html から入手できます。

仮想アプライアンスのドキュメントは、次の URL から入手できます。

https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html

Cisco コンテンツ セキュリティ管理アプライアンスのドキュメントは http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html から入手できます。

AsyncOS 11.5. for Cisco Web Security Appliances の暗号リストは次の URL から入手できます。

https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-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://community.cisco.com/t5/web-security/bd-p/5786-discussions-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 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

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。