AsyncOS 11.7.x for Cisco Web Security Appliances リリースノート

発行:2018 年 12 月 11 日

改訂:2020 年 7 月 20 日

目次

Cisco Systems, Inc.
www.cisco.com

最新情報

AsyncOS 11.7.2-011 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 11.7.2-011 の既知および修正済みの問題(19 ページ)」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 11.7.1-049 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 11.7.1-049 の既知および修正済みの問題(19 ページ)」を参照してください。

AsyncOS 11.7.1-020 の新機能 - MD（メンテナンス導入）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 11.7.1-020 の既知および修正済みの問題(19 ページ)」を参照してください。

AsyncOS 11.7.1-006 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 11.7.1-006 の既知および修正済みの問題（19 ページ）」を参照してください。

Cisco AsyncOS 11.7.0-418 の新機能：GD（全面導入）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 11.7.0-418 の既知および修正済みの問題（20 ページ）」を参照してください。

Cisco AsyncOS 11.7.0-407 の新機能：GD（全面導入）更新

機能	説明
ISE 統合でのセキュア グループ タグと Active Directory グループのサポート	ISE 統合では、ISE から受信したセキュア グループ タグ（SGT）と Active Directory グループ（AD グループ）の情報を使用してアクセス ポリシーを作成できます。
カプセル化された URL の保護	URL カテゴリのフィルタリングは、translate.google.com を経由するすべてのトランザクションに適用され、さらにその機能を強化してすべてのトランザクションでアクションを特定し、実行します。 HTTPS プロキシを有効にして、HTTPS 要求の復号化を選択する必要があります。
Web ベースのレピュテーション スコア（WBRS）エンジンの強化	WBRS エンジンが強化され、web レピュテーションおよび URL の Web カテゴリ情報の有効性が向上しました。
カスタムおよび外部 URL カテゴリの外部ライブ フィードでフィード ファイル 30 個をサポート	URL カテゴリの定義を使用して、各ファイルが最大 5,000 のエントリを含むフィード ファイルを 30 個まで使用できます。 **コメント** 使用できる最大エントリ数は 5000 です。外部フィード エントリの数を増やすと、パフォーマンスの低下につながります。最適なパフォーマンスを得るために、各フィード ファイルに 1500 のエントリを使用することも、合計で 45,000 のエントリを使用することもできます。
レポートのサーバ名指定（SNI）情報	アプライアンスで、パススルー HTTPS トランザクションの SNI を提供できるようになりました。これにより、[Webトラッキング（Web Tracking）] ページの特定の Web サイトへのトランザクションを検索できます。

機能	説明
ISE-PIC の統合	アプライアンスを設定して、ISE-PIC バージョン 2.4 および pxGrid バージョン 2.0 で透過的にユーザを特定できるようになりました。ISE-PIC でユーザ アイデンティティ情報（ユーザ名や Active Directory グループ）を取得し、設定されたポリシー内の透過的なユーザ ID でこれらのプロファイルを使用できるようになります。 **コメント** AsyncOS 11.7 for Cisco Web Security Appliances にアップグレードする場合、正常な統合のために ISE を再設定する必要があります。以前に設定されたすべての ISE 機能は、ISE が再設定されるまで機能しません。 **コメント** AsyncOS 11.7 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。導入する ISE バージョンが ISE 2.4 未満である場合、11.7 未満の AsyncOS for Cisco Web Security Appliances を使用して続行します。 詳細については、ユーザ ガイドの「Overview of the Identity Services Engine (ISE) / ISE Passive Identity Controller (ISE-PIC) Service」のトピックを参照してください。

機能	説明
(Cisco AMP Threat Grid へのファイルのアップロードを減らす)事前分類の有効性の改善	アプライアンスのファイル分析サービスでは、Cisco AMP Threat Grid でサポートされているすべてのファイルの種類をサポートしています。 • ファイル分析用の動的なコンテンツのみを含むファイルをアップロードできます。これは、管理者が毎日のファイルのアップロード制限をトラッキングするのに役立ちます。これまでは、オンボックスの事前分類エンジンにより、ファイルが分析用として送信される前に限定的な範囲でフィルタ処理されていました。今回、新しいクラウドベースの Threat Grid 事前分類エンジンが追加され、リスクの低いファイルをフィルタし取り除くようになりました。これにより、悪意がある可能性のあるファイルの送信制限を保存することで有効性が向上します。 • ファイル分析のためのファイルのアップロードを低減できます。 この機能を設定するには、ユーザ ガイドの「Enabling and Configuring File Reputation and Analysis Services」のトピックを参照してください。 **コメント** プライベート クラウド ファイル分析サーバのバージョン 2.4 またはそれ以前のバージョンを使用している場合は、ファイル分析に新しいファイル タイプを有効にしないことをお勧めします。 ファイルの分析後に、ファイルに動的なコンテンツが存在しないときの新しい判定 [低リスク(Low Risk)] が導入されました。[高度なマルウェア防御(Advanced Malware Protection)] レポートの [AMPにより渡された受信ファイル(Incoming Files Handed by AMP)] セクションに判定の詳細を表示できます。 **コメント** 低リスクのファイルは分析用として AMP Threat Grid に送信されないため、SHA の [レポート(Reporting)] の [ファイル分析(File Analysis)] ページで検索できません。
ログイン履歴の設定	ログイン履歴を保持する日数を設定するため、新しいサブコマンド `loginhistory`が CLI コマンド `adminaccessconfig` に追加されています。 デフォルト値は 1 日です。 これは FIPS モードおよび非 FIPS モードのときに使用可能です。

機能	説明
最大同時ログイン セッション数の設定	コマンドライン インターフェイスやWeb インターフェイスを使用したアプライアンスの同時セッションの最大数を設定するため、新しいサブコマンド `maxsessions` が CLI コマンド `adminaccessconfig` に追加されます。 FIPS モードのデフォルト値は 3 で、非 FIPS モードの場合は 10 です。 これは FIPS モードおよび非 FIPS モードのときに使用可能です。
スマート ソフトウェア ライセンシングのサポート	スマート ソフトウェア ライセンシングを使用すると、Cisco Web セキュリティ アプライアンスのライセンスをシームレスに管理およびモニタできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager（CSSM）でアプライアンスを登録する必要があります。CSSM は、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。 ⚠ **注意** アプライアンスでスマート ライセンシング モードを有効にすると、クラシック ラインセンシング モードに復帰できなくなります。 詳細については、ユーザ ガイドの「Smart Software Licensing」のトピックを参照してください。

機能	説明
ウォークスルーを使用したユーザ エクスペリエンスの強化	アプライアンスには、特定の設定タスクを実行するためのウォークスルーが用意されています。このリリースでは、次のウォークスルーがサポートされています。 • Active Directory - NTLM を使用したエンド ユーザの認証 • Active Directory – Kerberos を使用したエンド ユーザの認証 • HTTPS トラフィックの復号化 • ISE または ISE-PIC を使用した透過的なユーザ識別の設定 **コメント** ウォークスルーのリストは更新可能なクラウドです。ハウツー ウィジェットの更新バージョンとポップアップ ウィンドウを表示するには、必ずブラウザのキャッシュをクリアしてください。 ウォークスルーを有効にする方法については、ユーザガイドの「Additional Security Settings for Accessing the Appliance」のトピックを参照してください。
仮想アプライアンスの柔軟なディスク サイズのサポート	このリリースの AsyncOS では仮想アプライアンスのディスク サイズの柔軟性がサポートされています。詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

AsyncOS 11.7.0-406 の新機能：プロビジョニング解除

このリリースは、2019 年 5 年 23 日にプロビジョニング解除されました。

動作における変更

AsyncOS 11.7 の動作の変更

ログ サブスクリプション名	ログ サブスクリプション名の非 ASCII 文字と空白はサポートされていません。サポートされていない文字がログ サブスクリプション ファイル名に含まれている場合、アップグレードは失敗します。

拡張 Web ベース レピュテーション スコア（WBRS）エンジンに固有のバージョン CLI コマンドの出力への変更	拡張 Web ベース レピュテーション スコア（WBRS）エンジンに固有のバージョン CLI コマンドの出力は若干異なって見えますが、すべての機能と有効性は変わりません。
	次に、出力例を示します。
	`Cisco Web 利用の制御： Web 分類エンジン：1.12.4.944（未更新）`
	`Web レピュテーション IP フィルタ：1529708330（未更新）`
	`Web レピュテーション ルール：1528401763（未更新）`
	`Web レピュテーション URL クエリ データベース：1529706637（未更新）`
	`Web レピュテーション エンジン：1.12.4.944（未更新）`
	[Web レピュテーション URL クエリデータベース（Web Reputation URL Queries Database）] 行は、11.7 より前のバージョンの [レピュテーションプレフィックスフィルタ（Reputation Prefix Filters）] を表します。

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

次のモデルがあります。

- S000V
- S100V
- S300V
- S600V
- x90
- x80

アップグレード パス

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。

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（11 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（13 ページ）を参照してください。

11.7.2-011 へのアップグレードパス - MD（メンテナンス導入）

Cisco Web セキュリティアプライアンス向け AsyncOS のリリース 11.7.2-011 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
- 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
- 11.7.1-049

11.7.1-049 のアップグレードパス - MD（メンテナンス導入）

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 のリリース 11.7.1-049 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
- 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

11.7.1-020 のアップグレードパス - MD（メンテナンス導入）更新

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 のリリース 11.7.1-020 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
- 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

11.7.1-006 のアップグレードパス - MD（メンテナンス導入）

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 のリリース 11.7.1-006 にアップグレードできます。

- 10.1.1-235
- 10.1.4-017
- 10.1.5-004
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 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

11.7.0-418 のアップグレード パス：GD（一般導入）更新

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 11.7.0-418 にアップグレードできます。

- 10.1.1-235
- 10.1.4-017
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 10.5.5-005
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11-5-3-003
- 11.5.3-016
- 11.7.0-334
- 11.7.0-406
- 11.7.0-407

11.7.0-407 のアップグレード パス：GD（一般導入）更新

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 11.7.0-407 にアップグレードできます。

- 10.1.1-235
- 10.1.4-017
- 10.5.2-072
- 10.5.3-025
- 10.5.4-018
- 11.5.1-125
- 11.5.1-504
- 11.5.1-603
- 11.5.2-020
- 11.7.0-334
- 11.7.0-406

注 仮想アプライアンス向けの AsyncOS 11.7.0-407 リリースへのアップグレードは、レポートおよび Web トラッキング データベースの破損の原因となる不具合によりサポートされていません。仮想アプライアンスに対するこの修正を含む更新リリースは、2019 年 6 月末までにリリースされます。

アップグレード前の要件

AsyncOS 11.7 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（12 ページ）
- 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（12 ページ）
- アップグレードの前にアップグレード後の要件を確認（12 ページ）

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。

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。

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（15 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コンフィギュレーション 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（11 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。

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（17 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（17 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（18 ページ）
- ファイル分析：分析対象のファイル タイプの確認（18 ページ）
- 正規表現のエスケープされていないドット（18 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-E
CDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES12 8-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（21 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 11.7.2-011 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=11.7.2-011&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.2&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.7.1-049 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=11.7.1-049&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.7.1-020 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=11.7.1-020&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.7.1-006 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=11.7.1-006&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.7.0-418 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=11.7.0-418&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.0&sb=afr&sts=open&svr=3nH&bt=custV

リリース 11.7.0-407 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=11.7.0-407&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=11.7.0&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、11.7.0)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：https://www.cisco.com/c/ja_jp/support/web/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。