AsyncOS 10.1.x for Cisco Web Security Appliances リリースノート

発行日:2016 年 9 月 1 日
改定日:2020 年 1 月 20 日

目次

Cisco Systems, Inc.
www.cisco.com

最新情報

（注） **AsyncOS 10.1.x バージョンについて**：このアップグレード後、アプライアンスが Kerberos を使用して構成されている場合、認証プロセスの CPU 使用率が高くなります。同時に実行する Kerberos 認証の数を減らすか、15 分以上のサロゲート タイムアウトで IP サロゲートを使用することをお勧めします。これにより、エンド ユーザの Web 要求に対する遅延を防止できます。IP サロゲートを使用できないトラフィックについては、識別プロファイルとセッション Cookie ベースの認証サロゲートを使用します。識別プロファイルへの変更を確定するときに、エンド ユーザを再認証する必要があります。

Cisco AsyncOS 10.1.5-034（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 10.1.5-037 の既知および修正済みの問題（25 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 10.1.5-034 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。

Cisco AsyncOS 10.1.5-004（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 10.1.5-004 の既知および修正済みの問題（25 ページ）」を参照してください。

Cisco AsyncOS 10.1.4-017（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 10.1.4-017 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.4-007（MD：メンテナンス導入）の新機能

機能	説明
差分更新の有効化または無効化	CLI コマンド `updateconfig > setup` を使用して、Web レピュテーション サービスからの差分更新を有効または無効にできます。差分更新を無効にしても、アプライアンスはシスコのサーバから更新全体をダウンロードし続けます。 （注） 差分更新を無効にすると、アプライアンスで更新された Web レピュテーション情報の受信に遅延が発生します。 詳細については、ユーザ ガイドの「Web Security Appliance CLI Commands」を参照してください。

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 10.1.4-007 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.3-054（MD：メンテナンス導入）の新機能

機能	説明
Kerberos 認証ヘルパーの数の設定	CLI コマンド `modifyauthhelpers` を使用して、Kerberos 認証ヘルパーの数を設定できます。

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 10.1.3-054 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.3-039 - プロビジョニング解除

このリリースは、2018 年 7 月 12 日にプロビジョニング解除されました。

Cisco AsyncOS 10.1.2-050 - プロビジョニング解除

このリリースは、2018 年 7 月 12 日にプロビジョニング解除されました。

Cisco AsyncOS 10.1.2-036 - プロビジョニング解除

このリリースは、2017 年 12 月 14 日にプロビジョニング解除されました。

Cisco AsyncOS 10.1.1-235（MD：メンテナンス導入 - 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 10.1.1-235 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.1-234（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 10.1.1-234 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.1-230（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 10.1.1-230 の既知および修正済みの問題」を参照してください。

Cisco AsyncOS 10.1.0（GD：一般導入）の新機能

機能	説明
アーカイブ検査	特定タイプの「検査可能なアーカイブ」を許可、ブロック、または検査できます。検査可能なアーカイブとは、WSA により各ファイルのコンテンツを検査し、ファイル タイプ ブロック ポリシーを適用できるアーカイブ ファイル（圧縮ファイル）のことです。検査可能なアーカイブのリストには、ZIP、Microsoft CAB、RAR、TAR などのアーカイブ タイプが含まれています。本ユーザ ガイドの「アクセス ポリシー：オブジェクトのブロッキング」を参照してください。
中央管理型アップグレード管理	この機能により、1 つのセキュリティ管理アプライアンス（SMA）を使用して複数の WSA を同時にアップグレードできます。各 WSA に異なるソフトウェア アップグレードを適用することもできます。
TCP ウィンドウの動的サイズ変更	CLI コマンド `networktuning` を使用すると、システムの負荷と使用可能なリソースに基づいて、TCP 送信/受信スペース バッファの動的サイズ変更を有効化/無効化できます。
TCP RST（リセット）転送の有効化/無効化	TCP RST（リセット）転送を有効または無効にするために、「`Do you want to forward TCP RST sent by server to client?`」オプションを CLI `advancedproxyconfig` > `MISCELLANEOUS` に追加できます。ユーザ ガイドの「Web Security Appliance CLI Commands」を参照してください。
S600V のサポート	S600V 仮想アプライアンス モデルが OVF および KVM 導入でサポートされます。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。
ファイル レピュテーションとファイル分析のための新しいヨーロッパ リージョン サーバの追加	シスコでは、高度なマルウェア防御サービス用にヨーロッパ リージョンに 2 つの新しいサーバを追加しました。 ファイル レピュテーション サーバ：EUROPE（cloud-sa.eu.amp.cisco.com） ファイル分析サーバ：EUROPE（https://panacea.threatgrid.com） ファイル レピュテーションやファイル分析のために、これらのサーバを選択できます。本ユーザ ガイドの「ファイル レピュテーション フィルタリングとファイル分析」の章を参照してください。

Cisco AsyncOS 10.0.0（LD：限定導入）の新機能

機能	説明
curl コマンド	Web サーバに cURL 要求を直接またはプロキシ経由で送信します。返された要求や応答の HTTP ヘッダーから、Web ページをロードできなかった理由を判断できます。ユーザ ガイドの「Web Security Appliance CLI Commands」を参照してください。 **（注）** このコマンドは、TAC の監督のもとで管理者またはオペレータだけが使用できます。
参照元の例外	埋め込み/参照コンテンツ用に設定されたデフォルトのアクションに対する例外を定義できます。Web サイトでは、ソース ページとは分類が異なるコンテンツや、ソースとはタイプが異なるアプリケーションと見なされるコンテンツを埋め込んだり、参照することができます。デフォルトでは、ソース Web サイトの分類に関係なく、埋め込み/参照コンテンツは割り当てられたカテゴリまたはアプリケーションに選択したアクションに基づいてブロックまたはモニタされます。ユーザ ガイドの「Exceptions to Blocking for Embedded and Referred Content」を参照してください。
AMP プライベート クラウド	Cisco AMP 仮想プライベート クラウド アプライアンスを「エアギャップ」モードでオンプレミス展開し、接続している WSA にプライベート ファイル レピュテーション フィルタリングを提供できるようになりました。ユーザ ガイドの「Enabling and Configuring the File Reputation and Analysis Services」を参照してください。
AMP レポートの機能拡張	新しいレポート用パネルとディスプレイ、既存のレポート用パネルへのさらなる情報列の追加、特定のレポート間のクロスリンクなど、AMP 関連のレポート ページが拡張されました。 レトロスペクティブ アラートは、感染したファイル名や合計ユーザ数など、さらに情報を提供できるようになりました。また、レトロスペクティブ アラートのフォーマットもアップデートされ、より「読みやすく」なりました。 アクセス ログに新しいログ エントリ フィールドが追加されました。ログ エントリの末尾には次のようなファイル判定番号が付加されます。 1：不明 2：正常 3：悪意がある 4：スキャン不可
更新されたユーザ エージェントの一覧	ポリシーの定義時に選択できる使用可能なユーザ エージェントの一覧が更新され、拡張されました。この一覧は [詳細設定（Advanced）] > [ユーザエージェントによるメンバーシップ（Membership by User Agent）] にあり、多数の機能ページ（[識別プロファイル（Identification Profiles）]、[ルーティングポリシー（Routing Policies）] など）からアクセスできます。

機能	説明
中間証明書	CLI コマンド `advancedproxyconfig > HTTPS` を使用して、「中間証明書の検出」を有効にできるようになりました。WSA は、中間証明書ストアを手動で検索してダウンロードする必要性をなくして、中間証明書の検証エラーを防ぐために、この検出プロセスを使用します。ユーザ ガイドの「Web Security Appliance CLI Commands」を参照してください。
ライブ（サードパーティ）フィード	外部サーバからのデータ フィードに基づいてカスタム URL カテゴリを定義できます。これらのライブフィードのカスタム URL カテゴリは、ポリシー定義で使用できます。ユーザ ガイドの「Creating and Editing Custom URL Categories」を参照してください。

詳細については、「既知および修正済みの問題（24 ページ）」で該当する「修正済みの問題」を検索して参照してください。

動作における変更

Cisco AsyncOS 10.1.5（MD: メンテナンス導入）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。

Cisco AsyncOS 10.1.3（MD: メンテナンス導入）の動作の変更

AMP 圧縮ファイルの処理	AMP が有効になっていて、AMP からの悪意があるという判定によりアクセス ポリシーがすべての HTTP トランザクションをブロックするように設定された場合、先に MIME タイプが検出されてから、ファイルの圧縮が解除されファイルの送信をブロックまたは許可します。
VLAN の設定の変更および管理	CLI では、`etherconfig > VLAN` コマンドを使用して VLAN を編集することはできません。VLAN を編集するには、VLAN を削除して設定する必要があります。
`Find web server by:` パラメータのデフォルト値	`Find web server by:` パラメータのデフォルト値は、CLI の `advanced proxyconfig > DNS` について、次のように変更されます。 `0= Always use DNS answers in order.`

以前のリリースの動作の変更

このセクションでは、最新バージョンにアップグレードした後のアプライアンスの設定に影響を与える可能性がある、以前のバージョンの AsyncOS for Web の動作の変更について説明します。

プロキシ サービス用のデフォルトの暗号スイート

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。AsyncOS 10.x.x にアップグレードする場合は、「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）」を参照してください。

正規表現で使用できない特殊文字

正規表現の先頭および末尾に「.*」を使用できなくなりました。また、URL に一致させるために「./」を使用したり、その最後にドットを使用したりすることはできません。

Active Directory のユーザ名で使用できる特殊文字

AsyncOS 9.0 よりも前では、特殊文字を含むユーザ名を使用して Active Directory ドメインに参加しようとすると、エラーが生成されていました。現在はドメイン ユーザ名に次の特殊文字を使用できるようになりました：` ~ ( ) { } ! # ^ _ $ &（ただし、% はまだサポートされていないことに注意してください）。

WCCP ダイナミック サービス グループの数の制限

Web Security Appliance では、15 個を超える WCCP サービス グループを設定できません。

同時セッション数の制限

AsyncOS 8.5 以降、個々のユーザは最大 10 個の同時セッションに制限されます。この合計数には、CLI セッションと Web インターフェイス セッションの両方が含まれます。

使用できるアップグレードのリスト

AsyncOS 8.5 以降、これまでは限定リリースとして限られた数の顧客のみに提供されていたリリースを含めて、使用可能なすべてのリリースが、使用できるアップグレードのリストに表示されます。

リスト内の各リリースはリリースのタイプ（ED：早期導入、GD：一般導入、MD：メンテナンス導入など）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。

サポート要求には CCO ID とサポート契約が必要

AsyncOS 8.5 以降、アプライアンスからサポート要求をオープンするには、CCO ID とサポート契約 ID を入力する必要があります。

新しい [証明書管理（New Certificate Management）] ページ

AsyncOS 8.5 以降、証明書の管理機能は、[セキュリティサービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページから、新しいスタンドアロン ページである [ネットワーク（Network）] > [証明書管理（Certificate Management）] に移動されました。

Web トラッキング データのエクスポート

以前は、Web トラッキング データを CSV としてエクスポートする場合、データはタイムスタンプでソートされていました。AsyncOS 8.5 以降、このデータはソートされません。

SNMP モニタリング

AsyncOS 8.5 以降、次の機能は以前の実装とは異なります。

SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。認証と暗号化のパスワードは異なっている必要があります。暗号化アルゴリズムには AES（推奨）または DES を指定できます。認証アルゴリズムには SHA-1（推奨）または MD5 を指定できます。

X 認証済みグループのヘッダー形式

AsyncOS 8.5 以降、LDAP 認証と外部データ消失防止がアプライアンスで設定されている場合、AsyncOS は次の形式で X 認証済みグループのヘッダーを送信します：

LDAP:///(*LDAP server name*)/(*groupname*).

以前の形式は LDAP:///(*groupname*) でした。このソフトウェアの変更には、ポリシーの変更や、X 認証グループのヘッダーに依存するその他の自動化が必要になる場合があります。[不具合：CSCum91801]

Web トラッキングのクエリ タイムアウトを変更するための新しい CLI オプション

Web トラッキングのクエリ タイムアウトを変更するため、reportingconfig コマンドの下に新しい CLI オプションである webtrackingquerytimeout が導入されました。

（注） Webtrackingquerytimeout のデフォルト値は 120 秒であり、120 秒以上に変更できます。

次に、Web トラッキングの クエリ タイムアウトを 150 秒に変更する例を示します。

```
web.example.com > reportingconfig

Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this appliance.
[]> webtrackingquerytimeout

Timeout value for Web Tracking Queries (in Seconds)
[120] > 150

Choose the operation you want to perform:
- COUNTERS - Limit counters recorded by the reporting system.
- WEBTRACKINGQUERYTIMEOUT - Timeout value for Web Tracking Queries.
- AVERAGEOBJECTSIZE - Average HTTP Object Size used for Bandwidth Savings Calculation.
- WEBEVENTBUCKETING - Enable or Disable web transaction event bucketing.
- CENTRALIZED - Enable/Disable Centralized Reporting for this WSA appliance.
[]>
web.example.com > commit

Please enter some comments describing your changes:
[]>
Changes committed: Fri May 05 13:18:18 2017 GMT

web.example.com >
```

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

- すべての仮想アプライアンスモデル
- 次のハードウェア モデル
  - x70（Cisco Web セキュリティ アプライアンス S170 は AsyncOS 10.5 以降ではサポートされていません）
  - x80
  - x90

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

重要: アップグレード後、ルート パーティションが読み取り専用の S190、S390、および S690 アプライアンスでは、ルート パーティションの使用率を表示する ipcheck コマンドの出力が 100% を超えることがあります。これは正常であり、機能的な影響は一切ありません。

（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（17 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（17 ページ）」を参照してください。

AsyncOS 10.1.5-037（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.5-037 にアップグレードできます。

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-009
- 10.1.4-017
- 10.1.5-004
- 10.1.5-034

AsyncOS 10.1.5-034（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.5-034 にアップグレードできます。

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-009
- 10.1.4-017
- 10.1.5-004

AsyncOS 10.1.5-004（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.5-004 にアップグレードできます。

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007
- 10.1.4-009
- 10.1.4-017

AsyncOS 10.1.4-017（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.4-017 にアップグレードできます。

- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054
- 10.1.4-007

AsyncOS 10.1.4-007（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.4-007 にアップグレードできます。

- 9.1.1-074
- 9.1.2-022
- 9.1.2-041
- 9.1.3-016
- 9.1.3-024
- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 10.1.3-054

AsyncOS 10.1.3-054（MD：メンテナンス導入 - 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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.3-054 にアップグレードできます。

- 9.1.1-074
- 9.1.2-022
- 9.1.2-041
- 9.1.3-016
- 9.1.3-024
- 10.1.1-235
- 10.1.1-306
- 10.1.2-036
- 10.1.2-050
- 10.1.3-039
- 8.5.3-901

AsyncOS 10.1.1-235（MD：メンテナンス導入 - 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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.1-235 にアップグレードできます。

- 8.0.8-113
- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 9.1.2-034
- 10.1.0-204
- 10.1.1-230
- 10.1.1.-234

AsyncOS 10.1.1-234（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.1-234 にアップグレードできます。

- 8.0.8-113
- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 9.1.2-029
- 10.0.0-233
- 10.1.0-204
- 10.1.1-230

AsyncOS 10.1.1-230（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.1-230 にアップグレードできます。

- 8.0.8-118
- 8.5.3-069
- 8.5.4-038
- 9.0.1-162
- 9.1.0-157
- 9.1.1-074
- 9.1.2-022
- 10.0.0-233
- 10.1.0-204

AsyncOS 10.1.0-204（GD：一般導入）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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.1.0-204 にアップグレードできます。

- 8.0.6-119
- 8.0.7-149
- 8.0.8-113
- 8.0.8-118
- 8.5.1-104
- 8.5.2-027
- 8.5.3-069
- 8.8.0-085
- 9.0.1-162
- 9.0.1-204
- 9.1.0-070
- 9.1.0-157
- 9.1.1-074
- 9.1.1-507
- 9.1.1-508
- 9.1.1-510
- 9.1.2-010
- 10.0.0-233

AsyncOS 10.0.0-233（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（17 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（17 ページ）」を参照してください。

次のバージョンから AsyncOS for Cisco Web Security Appliances リリース 10.0.0-233 にアップグレードできます。

- 8.0.6-119
- 8.0.7-149
- 8.0.8-118
- 8.5.1-104
- 8.5.2-027
- 8.5.2-103
- 8.5.2-105
- 8.5.3-069
- 8.8.0-085
- 9.0.1-162
- 9.0.1-203
- 9.1.0-157
- 9.1.1-074
- 10.0.0-188

アップグレード前の要件

RAID コントローラのファームウェアの更新

AsyncOS ソフトウェアをアップグレードする前に、『*Cisco Update for RAID Controller Firmware (For S360/S370/S660/S670 only, reboot required) Release Notes*』の説明に従って RAID コントローラ ファームウェアを更新します。

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
- 仮想アプライアンスの展開
- 設定ファイル
- デモ セキュリティ証明書の暗号化の強度
- アップグレード後の再起動
- Cisco AsyncOS 10.0.0（LD：限定導入）の新機能

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。

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。WSA には、http://[2001:2:2::8]:8080 または https://[2001:2:2::8]:8443 を使用してアクセスできます。
- 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（WSA と DLP サーバ間の通信は IPv4 のみ）
- PAC ファイル ホスティング

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+)
- IE(バージョン 7+)と Windows 7 および XP 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(19 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。

設定ファイル

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS for Web をアップグレードすると、設定は `/configuration/upgrade` ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

一般的に、古い AsyncOS リリースの設定ファイルは、新しい AsyncOS リリースと互換性がありません。その逆も同様です。

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 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

AsyncOS for Web をアップグレードした後、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

- 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。「アップグレード前の要件（17 ページ）」を参照してください。
- 管理者としてログインします。

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 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 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（Upgrades 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、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(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(22 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(23 ページ)
- 正規表現のエスケープされていないドット(23 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 10.x.x に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。

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

このセクションの要件は AsyncOS 8.8 で導入されました。

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

次の情報は、このリリースのオンライン ヘルプおよび/またはユーザ ガイドの補足情報です。

Sophos ではアーカイブ ファイルのスキャンがなくなる

AsyncOS 9.0 では、Sophos スキャナでアーカイブ（.zip）ファイルのスキャンが無効になっています。

エンドユーザ通知への Javascript の追加

標準 Javascript を任意のタイプのエンドユーザ通知に追加する必要がある場合は、ユーザ ガイドまたはオンライン ヘルプに記載されている、通知ページの HTML ファイルを編集するための手順に従ってください。（通知の [カスタムメッセージ（Custom Message）] ボックスに入力した JavaScript は、Web ユーザのインターフェイスでは削除されます。）必ずサポートされているクライアント ブラウザでスクリプトをテストし、期待どおりに動作することを確認してください。

レピュテーションの評価と分析のために送信できるファイル

ファイルのレピュテーションの評価と分析のためにファイルを送信する基準は、随時変更される場合があります。基準はシスコに登録しているお客様のみが使用できます。詳細については、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』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-user-guide-list.html
から入手できます。

このドキュメントにアクセスするには、シスコの顧客アカウントとサポート契約が必要です。登録するには、https://tools.cisco.com/RPF/register/register.do にアクセスしてください。

クラウドでのファイル分析の詳細の表示

この機能を設定する最新の手順はユーザ ガイドの PDF に記載されています。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html から入手できます。

カスタムおよびデフォルト カテゴリの異なるクライアントの「Hello」動作

パケット キャプチャをスキャンすると、カスタム カテゴリおよびデフォルト（Web）カテゴリの HTTPS 復号化パススルー ポリシーに対して別々の時間で「Client Hello」ハンドシェイクが送信されます。

デフォルト カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信する前に Client Hello が送信され、接続が失敗します。カスタム URL カテゴリを介した HTTPS ページのパススルーでは、要求元から Client Hello を受信した後に Client Hello が送信され、接続が成功します。

対応策として、SSL 3.0 のみと互換性がある Web ページのパススルー アクションを使用して、カスタム URL カテゴリを作成することができます。

その他の情報

ユーザ ガイドの PDF は、オンライン ヘルプよりも最新のものである場合があります。この製品のユーザ ガイドの PDF 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（28 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://tools.cisco.com/RPF/register/register.do 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 10.1.5-037 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=10.1.5-037&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.5-034 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=10.1.5-037&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282941570&rls=10.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.5-004 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=10.1.5-004&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.5&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.4-017 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=10.1.4-017&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.4-007 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=10.1.4-007&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.4&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.3-054 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 = 10.1.3-054 & sb = fr & svr = 2nH & bt = custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.3&sb=afr&sts=open&svr=2nH&bt=custV この URL には、ステータスが**オープン**の既知の問題について、すべてのリストが表示されます。[フィルタ（Filter）] で、[ステータス（Status）] を [その他（Other）] に変更し、オープンのステータスで表示されていない問題を確認します。

リリース 10.1.1-235 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=10.1.1-235&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.1-234 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=10.1.1-234&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.1-230 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=10.1.1-230&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.1&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.1.0-204 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=10.1.0-204&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.1.0&sb=afr&sts=open&svr=3nH&bt=custV

リリース 10.0.0-233 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=10.0.0-233&sb=fr&svr=3nH&bt=custV
既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282521310&rls=10.0.0&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、出荷リリースの既知および解決済みの不具合に関する最新情報を検索します。

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://tools.cisco.com/RPF/register/register.do 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(10.1 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、[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。

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。

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。