特長と機能

パッチには、新機能、機能、および緊急の問題または解決済みの問題に関連する動作の変更が含まれています。

新機能

次の表に、バージョン 6.2.3.x のパッチの新機能と動作の変更の概要を示します。

表 *1 :* バージョン *6.2.3.x* の新機能

機能	バージョン	説明
FTD NAT ポリシーでのルールの競合の検出	6.2.3.13	**アップグレードの影響。** バージョン 6.2.3.13 以降 にアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つFTD NATポリシーを作成できなくなります。 これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合しているNATルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後にFTD NATポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 （注） バージョン 6.3.0 または 6.4.0 にアップグレードすると、この修正が無効になります。この問題は、バージョン 6.3.0.4 および 6.4.0.2 では対処されています。 サポートされるプラットフォーム：FMC を搭載した FTD

機能	バージョン	説明
EMS拡張機能のサポート	6.2.3.8	**アップグレードの影響。** [復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方のSSLポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になりました。EMS 拡張機能は、 RFC 7627 によって定義されています。 バージョン 6.3.0 では EMS 拡張機能のサポートが中止されていることに注意してください。FMC展開では、この機能は、デバイスのバージョンによって異なります。FMCをバージョン 6.3.0 にアップグレードしてもサポートは中止されませんが、デバイスをアップグレードすると中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。 （注） バージョン6.2.3.8は2019年1月7日にシスコサポート＆ダウンロードサイトから削除されました。バージョン 6.2.3.9 にアップグレードすると、EMS 拡張機能のサポートも有効になります。 サポートされるプラットフォーム：すべて
TLS v1.3 ダウングレード CLI コマンド	6.2.3.7	新しい CLI コマンドを使用すると、TLS v1.3 接続を TLS v1.2 にダウングレードするタイミングを指定できます。 多くのブラウザでは、デフォルトで TLS v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニタ対象ネットワーク内のユーザがTLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。 詳細については、『CiscoThreat Defense Command Reference』の「**system support ssl-client-hello-commands**」のセクションを参照してください。これらのコマンドは、Cisco TAC に問い合わせてから使用することをお勧めします。 サポートされるプラットフォーム：FTD
クラスタリングを使用したサイト間 VPN	6.2.3.3	クラスタリングを使用してサイト間VPNを設定できるようになりました。サイトツーサイト VPN は、中央集中型機能です。マスターユニットだけが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300

廃止された機能

廃止された機能が原因で、アップグレードができなかったり、アップグレード前またはアップグレード後の設定変更を必要とする場合があります。

（注） バージョン 6.6.0/6.6.x は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。ユーザエージェント設定を使用して FMC をバージョン 6.7.0 以降 にアップグレードすることはできません。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。これにより、ユーザ エージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。

詳細については、『Firepower ユーザ ID：ユーザエージェントから Identity Services Engine への移行』の技術メモを参照してください。

これらの機能はバージョン 6.2.3.x で廃止されました。

表 *2:* バージョン *6.2.3.x* で廃止された機能

機能	アップグレードの影響	プラットフォーム	説明
バージョン 6.2.3.8 パッチを削除。	なし。ただしバージョン 6.2.3.8 のままにしないでください。	任意	バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよびダウンロードサイトから削除されました。このバージョンを実行している場合は、アップグレードすることを強くお勧めします。バージョン 6.2.3.8 を実行しているデバイスは、一定時間後にトラフィックの送受信を停止する可能性があります。 バージョン 6.2.3.8 を以降のパッチにアップグレードしてから、そのパッチをアンインストールすると、バージョン 6.2.3.8 に戻ります。その時点で、ただちにアップグレードするか、バージョン 6.2.3.8 をアンインストールする必要があります。バージョン 6.2.3.8 のままにしないでください。 関連するバグ：CSCvn82378

機能	アップグレードの影響	プラットフォーム	説明
バージョン 6.2.3.1 ～ 6.2.3.3 期限切れの動的分析用のCA証明書	なし。ただし、パッチを適用する必要があります。	ネットワーク向け AMP	2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。「期限切れの動的分析用のCA証明書 （5 ページ）」を参照してください。

期限切れの動的分析用の CA 証明書

展開：動的分析のためにファイルを送信する AMP for Networks（マルウェア検出）展開

影響を受けるバージョン：バージョン 6.0+

解決：CSCvj07038

2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。これは、AMP Threat Grid クラウドとの通信に必要だった CA 証明書が期限切れになったために発生しました。バージョン6.3.0は、新しい証明書を使用する最初のメジャーバージョンです。

（注） バージョン6.3.0+にアップグレードしない場合は、新しい証明書を取得して動的分析を再度有効にするために、パッチまたはホットフィックスを適用する必要があります。ただし、その後、パッチまたはホットフィックスが適用された展開をバージョン6.2.0またはバージョン6.2.3にアップグレードすると、古い証明書に戻るため、パッチまたはホットフィックスを再度適用する必要があります。

パッチまたはホットフィックスを初めてインストールする場合は、ファイアウォールで、FMCとその管理対象デバイスの両方から `fmc.api.threatgrid.com`（`panacea.threatgrid.com` を置き換える）へのアウトバウンド接続が許可されていることを確認してください。管理対象デバイスは、動的分析のためにファイルをクラウドに送信します。FMC は結果を照会します。

次の表に、メジャー バージョン シーケンスとプラットフォームごとに、古い証明書を使用するバージョンと、新しい証明書を使用するパッチおよびホットフィックスを示します。パッチおよびホットフィックスは、シスコサポートおよびダウンロードサイトで入手できます。

表 *3:* 新しい *CA* 証明書を使用するパッチとホットフィックス

古い証明書を使用するバージョン	新しい証明書を使用する最初のパッチ	新しい証明書を使用するホットフィックス	
6.2.3 ～ 6.2.3.3	6.2.3.4	ホットフィックス G	FTD デバイス
		ホットフィックス H	FMC、NGIPS デバイス
6.2.2 ～ 6.2.2.3	6.2.2.4	ホットフィックス BN	すべてのプラットフォーム
6.2.1	なし。アップグレードが必要です。	なし。アップグレードが必要です。	
6.2.0 ～ 6.2.0.5	6.2.0.6	ホットフィックス BX	FTD デバイス
		ホットフィックス BW	FMC、NGIPS デバイス
6.1.0 ～ 6.1.0.6	6.1.0.7	ホットフィックス EM	すべてのプラットフォーム
6.0.x	なし。アップグレードが必要です。	なし。アップグレードが必要です。	

侵入ルールとキーワード

アップグレードにより侵入ルールをインポートして自動的に有効化が可能です。

侵入ルールを更新（SRU）すると、更新された新しい侵入ルールおよびプリプロセサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、SRU を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。

- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

また、『Cisco Firepower Compatibility Guide』の「Bundled Components」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

Cisco Success Network

バージョン 6.2.3 では、 *Cisco Success Network* は、テクニカルサポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。

初期設定およびアップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。

Web 分析トラッキング

バージョン 6.2.3 では、 *Web* 分析のトラッキングは、これに限定されませんが、ページでの操作、ブラウザのバージョン、製品のバージョン、ユーザの場所、FMC の管理 IP アドレスまたはホスト名を含む、個人を特定できない使用状況データをシスコに送信します。

Web 分析トラッキングはデフォルトでオンになっています（バージョン 6.5.0 以降の EULA に承諾すると、Web分析トラッキングに同意したことになります）。ただし、初期設定の完了後にいつでもオプトアウトできます。

（注） バージョン 6.2.3 から 6.6.x へのアップグレードでは、Web 分析トラッキングを有効化（または再有効化）できます。これは、現在の設定がオプトアウトであっても発生する可能性があります。このデータの収集を拒否する場合は、アップグレードの後にオプトアウトしてください。

Cisco Support Diagnostics

バージョン 6.5.0 以降では、 *Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。

初期設定およびアップグレード中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。