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。

Firepower Management Center 展開に関する機能

（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。ユーザーエージェント設定を使用して Firepower Management Center 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、ユーザー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、シスコの担当者またはパートナーの担当者にお問い合わせください。

詳細については、『End-of-Life and End-of-Support for the Cisco Firepower User Agent』[英語] の通知、および『Firepower User Identity: Migrating from User Agent to Identity Services Engine』[英語] の技術メモを参照してください。

FMC バージョン 6.4.0 パッチの新機能

表 *1:*

機能	説明
バージョン 6.4.0.10 アップグレードがスケジュールされたタスクを延期する	**アップグレードの影響。** アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、バージョン 6.4.0.10 以降のパッチを実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 へのアップグレード、またはバージョン 6.4.0.10 をスキップするアップグレードではサポートされません。 この機能は、バージョン 6.5.0、6.6.0、または 6.6.1 でもサポートされていません。バージョン 6.6.3 および 6.7.0 では再導入されています。
バージョン 6.4.0.9 デフォルトの HTTPS サーバー証明書	**アップグレードの影響。** FMC または 7000/8000 シリーズのデバイスをバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または FMC をバージョン 6.6.0+ に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から 800 日後に期限切れになります。今後の更新はすべて、有効期間が 800 日になります。 古い証明書には、生成日に応じて、次の期限が設定されています。 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3 以前：20 年 バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。

機能	説明
バージョン 6.4.0.4 新しい syslog フィールド	次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。 • センサー UUID • 最初のパケット時間 • 接続インスタンス ID • 接続数カウンタ これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。
バージョン 6.4.0.2 FTD NAT ポリシーでのルールの競合の検出	**アップグレードの影響。** バージョン 6.4.0.2 以降のパッチ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。
バージョン 6.4.0.2 [ISE接続ステータスのモニター（ISE Connection Status Monitor）] ヘルスモジュール	新しいヘルスモジュール [ISE接続ステータスのモニター（ISE Connection Status Monitor）] は、Cisco Identity Services Engine（ISE）と FMC 間のサーバー接続のステータスをモニターします。

FMC バージョン 6.4.0 パッチで廃止された機能

表 *2*:

機能	アップグレードの影響	説明
バージョン 6.4.0.7 出力最適化	パッチを適用すると、出力最適化処理がオフになります。	CSCvq34340 を軽減するため、Firepower Threat Defense をバージョン 6.4.0.7 以降にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。 （注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。 バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。 詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。

Firepower Device Manager 展開の機能

FDM バージョン 6.4.0 パッチの新機能

表 *3:*

機能	説明
バージョン 6.4.0.10 VDB、GeoDB、および SRU 更新の手動アップロード	VDB、地理位置情報データベース、および侵入ルールの更新パッケージを手動で取得し、FDM を使用してワークステーションから FTD デバイスにアップロードできるようになりました。たとえば、FDM で Cisco Cloud から更新を取得できないエアギャップネットワークがある場合でも、必要な更新パッケージを入手できます。 ワークステーションからファイルを選択してアップロードできるように、[Device] > [Updates] ページが更新されました。 この機能はバージョン 6.5.0 ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。
バージョン 6.4.0.10 ユニバーサル永久ライセンス予約（PLR）モード	インターネットへのパスがないエアギャップネットワークがある場合は、スマートライセンスのために Cisco Smart Software Manager（CSSM）に直接登録することはできません。この場合は、ユニバーサル パーマネント ライセンス予約（PLR）モードを使用できるようになりました。このモードでは、CSSM との直接通信を必要としないライセンスを適用できます。エアギャップネットワークがある場合は、アカウント担当者に問い合わせて、CSSM アカウントでユニバーサル PLR モードを使用して必要なライセンスを取得することを許可するように依頼してください。 [Device] > [Smart License] ページに、PLR モードに切り替えたり、ユニバーサル PLR ライセンスをキャンセルしたりして登録解除する機能が追加されました。FTD API では、PLRAuthorizationCode、PLRCode、PLRReleaseCode、PLRRequestCode の新しいリソースと、PLRRequestCode、InstallPLRCode、および CancelReservation のアクションが追加されました。 この機能はバージョン 6.5.0 ではサポートされていないことに注意してください。バージョン 6.6.0 では再導入されています。バージョン 6.4.0.10 以降のパッチを実行している場合は、バージョン 6.5.0 を中間バージョンとして使用せずに、直接バージョン 6.6.0 以上にアップグレードすることをお勧めします。

機能	説明
バージョン 6.4.0.9 デフォルトの HTTPS サーバー証明書	**アップグレードの影響。** FDM をバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または6.6.0+に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から800日後に期限切れになります。今後の更新はすべて、有効期間が 800 日になります。 古い証明書には、生成日に応じて、次の期限が設定されています。 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3 以前：20 年 バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。
バージョン 6.4.0.4 新しい syslog フィールド	次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。 • センサー UUID • 最初のパケット時間 • 接続インスタンス ID • 接続数カウンタ これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。

FDM バージョン 6.4.0 パッチで廃止された機能

表 4：

機能	アップグレードの影響	説明
バージョン 6.4.0.7 出力最適化	パッチを適用すると、出力最適化処理がオフになります。	CSCvq34340 を軽減するため、Firepower Threat Defense をバージョン 6.4.0.7 以降にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。 （注） この問題が修正されているバージョン 6.6.0+ にアップグレードすることをお勧めします。機能を「有効」のままにすると、出力最適化がオンに戻ります。 バージョン 6.4.0 ～ 6.4.0.6 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。 詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。

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、新規および更新された侵入ルールとプリプロセッサルール、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。

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、Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [バージョン情報（About）] 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。

FMC の How-To ウォークスルー

デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。

（注） FMC ウォークスルーは Firefox および Chrome ブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

次の表に、一般的な問題点と解決策をいくつか示します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。

表 *5:* ウォークスルーのトラブルシューティング

問題	解決方法
ウォークスルーを開始するための [How To] リンクが見つからない。	ウォークスルーが有効になっていることを確認します。ユーザー名の下にあるドロップダウンリストから、[User Preferences] を選択し、[How-To Settings] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。

問題	解決方法
ウォークスルーがFMCと同期していない。 • 誤った手順から開始される。 • 進行が早すぎる。 • 先に進まない。	ウォークスルーが同期していない場合は、次のようにします。 • 続行します。 たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。 • ウォークスルーを終了し、別のページに移動してもう一度やり直します。 場合によっては続行できないこともあります。たとえば、手順の完了後に [Next] をクリックしないと、ウォークスルーの終了が必要になる場合があります。

シスコとのデータの共有

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、ユーザーの場所、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。

デフォルトで Web 分析トラッキングに登録しています（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、初期設定完了後はいつでも登録を変更できます。

（注） バージョン 6.2.3 から 6.6.x にアップグレードすると、Web 分析トラッキングに登録される可能性があります。登録は、意図的に登録解除した場合でも行われ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、アップグレード後に登録解除してください。

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、登録するか尋ねられます。登録はいつでも変更できます。

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、登録するか尋ねられます。登録はいつでも変更できます。

（注） この機能は、Firepower Management Center およびそこで管理される Firepower Threat Defense デバイスでサポートされます。バージョン 6.5.0 でのみ、FTD サポートは、FTD 搭載 Firepower 4100/9300 および Azure 向け FTDv に制限されます。この機能は、Firepower Device Manager ではサポートされていません。