特長と機能

メジャーリリースは、Firepowerソフトウェアの新機能、機能、および拡張機能を提供します。メジャーバージョンには、廃止された機能とプラットフォーム、メニューと用語の変更、動作の変更などが含まれることがあります。

廃止された機能は、バージョンをスキップするときにアップグレードの問題を引き起こす可能性が最も高いため、リリースノートには廃止された機能の履歴情報が記載されています。新機能の履歴情報については、スキップするバージョンのリリースノートを参照してください。

Firepower Management Center/バージョン 6.2.3 の新機能

次の表に、Firepower Management Centerを使用して設定された場合にFirepowerバージョン6.2.3で使用できる新機能を示します。

機能	説明
ハードウェアと仮想ハードウェア	

機能	説明
ISA 3000 の FTD	管理のために Firepower Device Manager または Firepower Management Center を使用して、ISA 3000 シリーズで Firepower Threat Defense を実行できるようになりました。 ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。ハードウェア バイパスやアラーム ポートなど、ASA でサポートされていた ISA 3000 の特別な機能は、このリリースの Firepower Threat Defense ではサポートされていません。
VMware ESXi 6.5 のサポート	Firepower Threat Defense Virtual、Firepower Management Center Virtual、および Firepower NGIPS Virtual が、VMware ESXi 6.5 でサポートされるようになりました。
Firepower Threat Defense：暗号化と **VPN**	
SSL ハードウェア アクセラレーション	特定の FirePOWER 管理対象デバイス モデルでは、パフォーマンスが大幅に向上する、ハードウェアでの SSL 暗号化および復号化のアクセラレーションをサポートしています。SSL ハードウェア アクセラレーションは、サポートするすべてのアプライアンスに対してデフォルトで無効化されています。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
Firepower Threat Defense の VPN の改善	証明書の登録操作のノンブロッキング ワーク フローでは、複数の Firepower Threat Defense デバイスで証明書の登録を並行して実行できます。 • 管理者は、[Access & Certificate] ステップで [Enroll the selected certificate object on the target devices] チェックボックスをオンにすることで、ポリシー内のすべてのデバイスに対して、リモート アクセス VPN ポリシー ウィザードで証明書を登録できるようになりました。この操作を選択した場合、ウィザードの終了後に展開のみを実行する必要があります。この設定は、デフォルトでオンになっています。 • 管理者は、デバイスでリモートアクセス VPN 証明書の登録を一度に 1 つずつ開始する必要がなくなりました。各デバイスの登録プロセスは、現在独立しており、並行して実行できます。 • PKS12 証明書の登録に失敗した場合、管理者は、登録を再試行するためにもう一度 PKS12 ファイルを再アップロードする必要はありません。これは、PKS12 ファイルが証明書の登録オブジェクトに保存されるためです。
Firepower Threat Defense：ハイアベイラビリティとクラスタリング	
Firepower Management Center のハイ アベイラビリティ メッセージ	Firepower Management Center のハイ アベイラビリティ ペアでは、UI メッセージが改善されています。UI には、Firepower Management Center のペアが確立されている間に、中間ステータス メッセージが表示されるようになり、書き換えられた UI メッセージがより直感的になりました。
内部エラーの発生後に自動的に Firepower Threat Defense クラスタに再参加	以前は、多くの内部エラー状態によって、クラスタ ユニットがクラスタから削除され、ユーザが問題を解決した後で、手動でクラスタに再参加する必要がありました。現在は、ユニットが自動的に、5 分、10 分、20 分の間隔でクラスタに再参加しようとします。内部エラーには、アプリケーション同期のタイムアウト、一貫性のないアプリケーションステータスなどがあります。 新しい/変更されたコマンド：**show cluster info auto-join** サポートされるプラットフォーム：Firepower 4100/9300

機能	説明

Firepower Threat Defense のハイアベイラビリティ強化	バージョン 6.2.3 では、ハイア ベイラビリティの Firepower Threat Defense デバイスに関する次の機能が導入されています。
	• ハイアベイラビリティペアのアクティブまたはスタンバイ Firepower Threat Defense デバイスが再起動されると、Firepower Management Center は、どちらの管理対象デバイスでも正確なハイアベイラビリティステータスを表示しない場合があります。ただし、Firepower Threat Defense と Firepower Management Center 間の通信が確立されていないために、Firepower Management Center ではステータスがアップグレードされないことがあります。**[Devices]** > **[Device Management]** ページの [Refresh Node Status] オプションを使用すると、ハイアベイラビリティノードのステータスを更新して、ハイアベイラビリティペアのアクティブデバイスとスタンバイデバイスに関する正確な情報を取得できます。
	• Firepower Management Center UI の **[Devices]** > **[Device Management]** ページには、新しい [Switch Active Peer] アイコンがあります。
	• バージョン 6.2.3 には、新しい REST API オブジェクト **Device High Availability Pair Services** が含まれており、次の 4 つの機能を備えています。
	  • **DELETE ftddevicehapairs**
	  • **PUT ftddevicehapairs**
	  • **POST ftddevicehapairs**
	  • **GET ftddevicehapairs**

管理とトラブルシューティング	
Firepower Threat Defense SSH アクセスへの外部認証の追加	LDAP または RADIUS を使用して、Firepower Threat Defense への SSH アクセス用に外部認証を設定できるようになりました。 新規/変更された画面：**[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** サポートされるプラットフォーム：FTD

機能	説明
脆弱性データベース（VDB）の強化されたインストール	Firepower Management Center は、VDB をインストールする前に、インストールにより Snort プロセスが再起動し、トラフィック検査が中断され、管理対象デバイスがトラフィックを処理する方法次第でトラフィック フローが中断される可能性があるという警告を表示するようになりました。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、または Firepower ソフトウェア アップグレードの一部として、VDB がバックグラウンドでインストールされる場合。
アップグレード パッケージのプッシュ	実際のアップグレードを実行する前に、Firepower Management Center から管理対象デバイスにアップグレード パッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。 ハイア ベイラビリティ デバイス、クラスタ デバイス、またはスタック構成デバイスにプッシュすると、システムは、アップグレード パッケージを最初にアクティブ/マスター/プライマリに送信し、次にスタンバイ/スレーブ/セカンダリに送信します。 新規/変更された画面：**[System]** > **[Updates]**
Firepower Threat Defense の保守性	バージョン 6.2.3 では、 **show fail over** CLI コマンドが改善されています。新しいキーワード **-history** を使用すると、トラブルシューティングに役立つ詳細が表示されます。 • **Show fail over history** は、失敗の理由に加えて、その具体的な詳細を表示します。 • **Show fail over history details** は、ピア ユニットのフェールオーバー履歴を表示します。 （注） このコマンド出力には、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。

機能	説明
デバイス一覧のソート	**[Devices]** > **[Devices Management]** ページで、[View by] ドロップダウンリストを使用して、グループ、ライセンス、モデル、またはアクセスコントロールポリシーのいずれかのカテゴリでデバイス一覧をソートして表示できます。マルチドメイン導入では、ドメイン（その導入のデフォルトの表示カテゴリ）を基準にソートして表示することもできます。デバイスはリーフ ドメインに属している必要があります。
監査ログの改善	監査ログは、Firepower Threat Defense Platform 設定の **[Devices]** > **[Platform Settings]** ページでポリシーが変更されたかどうかを示します。
FTD CLI コマンドの更新	Firepower Threat Defense デバイスの CLI コマンドの **asa_mgmt_plane** オプションと **asa_dataplane** オプションは、**management-plane** と **data-plane** にそれぞれ名前が変更されています。
Cisco Success Network	**アップグレードの影響。** *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。 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	**アップグレードの影響。** *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。 バージョン 6.2.3 にアップグレードすると、Web 分析トラッキングが有効になります。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オプトアウトできます。
Performance	

機能	説明
ポリシー展開の再起動の改善	バージョン 6.2.3 の機能強化として、Snort プロセスを再起動する設定が削減されました。Firepower Threat Defense デバイスでは、設定の展開により Snort プロセスが再起動し、トラフィック検査が中断され、管理対象デバイスがトラフィックを処理する方法次第でトラフィック フローが中断される可能性がある場合、展開の前に、管理 UI が警告を出すようになりました。 再起動の動作は、Firepower Device Manager を使用して管理されているデバイスでは異なることに注意してください。詳細については、Firepower Device Manager/FTD バージョン 6.2.3 の新機能 （8 ページ） を参照してください。
ポリシー適用時のトラフィック ドロップ	バージョン 6.2.3 では、**configure snort preserve-connection {enable | disable}** コマンドが Firepower Threat Defense CLI に追加されています。このコマンドは、Snort プロセスがダウンした場合に、ルーテッド インターフェイスとトランスペアレント インターフェイスで既存の接続を維持するかどうかを決定します。コマンドを無効にすると、Snort がダウンして、Snort が再開するまでドロップされたままになると、新規または既存のすべての接続がドロップされます。コマンドを有効にした場合、すでに許可されている接続は確立されたままですが、Snort が再び使用可能になるまで新しい接続を確立できません。 Firepower Device Manager で管理されている Firepower Threat Defense デバイスでは、このコマンドを永続的に無効にできないことに注意してください。次の設定の展開時に設定がデフォルトに戻ると、既存の接続がドロップされることがあります。
ローエンド アプライアンスのメモリ容量の増加	バージョン 6.1.0.7、6.2.0.5、6.2.2.2、および 6.2.3 では、Firepower ローエンド アプライアンスのメモリ容量が増加しています。これにより、ヘルス アラートの数が削減されます。
ISE pxGrid ディスカバリの高速化	ハイ アベイラビリティの ISE pxGrid に障害が発生した場合、または到達不能になった場合、Firepower Management Center は、新しいアクティブ pxGrid をより迅速に検出できるようになりました。
FMC REST API	

機能	説明
Firepower Management Center REST API の改善	新しい Firepower Management Center REST API は、ASA FirePOWER から Firepower Threat Defense への移行時に、NAT ルール、スタティック ルーティング設定、および対応するオブジェクトに対する CRUD（作成、取得、アップグレード、削除）操作の使用をサポートしています。 NAT 用に新しく導入された API • NAT ルール • Firepower Threat Defense NAT ポリシー • 自動 NAT ルール • 手動 NAT ルール Cisco ACI に Firepower Threat Defense デバイスを展開する場合、API を使用すると、APIC コントローラを介して、適切なスタティック ルートを適切に追加できるほか、特定のサービス グラフに必要なその他の設定も追加できます。また、API により、Firepower Threat Defense を ACI に挿入する最も柔軟性の高い方法である、PBR サービス グラフの挿入も可能になります。 スタティック ルート用に新しく導入された API • IPv4 スタティック ルート • IPv6 スタティック ルート • SLA モニタ

Firepower Device Manager/FTD バージョン 6.2.3 の新機能

リリース：2018年3月29日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.3 で使用できる新機能を示します。

機能	説明
SSL/TLS の復号	接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URL およびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。**[Policies]** > **[SSL Decryption]** ページおよび **[Monitoring]** > **[SSL Decryption]** ダッシュボードが追加されました。 **注目** アクティブな認証を実装するアイデンティティポリシーは、SSL 復号ルールを自動的に生成します。SSL 復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。
セキュリティ インテリジェンスのブラックリスト登録	新しい **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** ページから設定できるセキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先 URL に基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティ インテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。 また、[ポリシー（Policies）] ダッシュボードの名前を [アクセスおよびSIルール（Access And SI Rules）] に変更し、セキュリティ インテリジェンス同等のルールがアクセス ルールとともにダッシュボードに含まれるようになりました。
侵入ルールの調整	アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント（警告）をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション（ドロップまたは警告に設定）のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、**[Policies]** > **[Intrusion]** を選択します。

機能	説明
侵入ポリシーに基づく自動ネットワーク分析ポリシー（NAP）割り当て	以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワークオブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック（それ以外は同じ送信元/送信先のセキュリティ ゾーンおよびネットワーク オブジェクトと一致する）に割り当てる場合、完全に一致する NAP および侵入ポリシーは取得されないことに注意してください。カスタム ネットワーク分析ポリシーは作成できません。
脅威、攻撃、およびターゲットのダッシュボード用のドリル ダウン レポート	脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。 これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポートデータが失われます。
[Web Applications] ダッシュボード	新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。
新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え	新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。
新しいマルウェア ダッシュボード	新しいマルウェアダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイル タイプの情報を参照できます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
自己署名入りの内部証明書、および内部 CA 証明書	自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成したり、アップロードできるようになりました。これらの機能を、**[Objects]** > **[Certificates]** ページで設定します。

機能	説明
インターフェイスのプロパティ編集時に DHCP サーバの設定を編集する機能	インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレス プールを簡単に再定義できます。
製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信	Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカル サポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなときに、接続を有効にできます。接続はいつでも無効にできます。 Cisco Success Network はクラウド サービスです。**[Device]** > **[System Settings]** > **[Cloud Management]** ページの名前が [Cloud Services] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。
Firepower Threat Defense 仮想 カーネルベースの仮想マシン（KVM）のハイパーバイザデバイス用の設定	Firepower Device Manager を使用して、Firepower Threat Defense 仮想 for KVM デバイス上の FTD を設定できます。以前は、VMware のみがサポートされていました。 （注） Firepower Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。
ISA 3000（Cisco 3000 シリーズ産業用セキュリティアプライアンス）デバイスの設定	Firepower Device Manager を使用して ISA 3000 デバイス上の FTD を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。

機能	説明
ルール データベースまたは VDB の更新でのオプションの展開	侵入ルール データベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。 （注） VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。
展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下	展開を開始する前に、Firepower Device Manager により、設定の更新で Snort の再起動が必要かどうかが示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうかがわかるようになったため、混乱が少ないときに展開できます。 さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。 • ユーザが SSL 復号ポリシーを有効または無効にする • 更新されたルール データベースまたは VDB がダウンロードされた • ユーザが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した
Firepower Device Manager の CLI コンソール	Firepower Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソール セッションを模倣していますが、コマンドのサブセットのみ（**show**、**ping**、**traceroute**、および **packet-tracer**）を許可します。トラブルシューティングとデバイスのモニタリングに CLI コンソールを使用します。

機能	説明
管理アドレスへのアクセスのブロックのサポート	管理IPアドレスにアクセスできないようにするため、プロトコルのすべての管理アクセスリストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアントIPアドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3へのアップグレードでは、以前からのプロトコル（HTTPSまたはSSH）用の空の管理アクセス リストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。 また、SSH または HTTPS アクセスを無効にする場合を含み、Firepower Device Manager は CLI から管理アクセスリストに加えた変更を認識します。 少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。

機能	説明
デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig	Smart CLI と FlexConfig により、まだ Firepower Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Firepower Threat Defense は、ASA 設定コマンドを使用していくつかの機能を実装します。ASA設定コマンドの知識があり、専門家ユーザの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。 • Smart CLI：（推奨される方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。 • FlexConfig：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI、変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA設定コマンドを知り、ASA設定ガイドに従う必要があります。 **注意** Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。
Firepower Threat Defense REST API、および API エクスプローラ	REST API を使用して、Firepower Device Manager を介してローカルで管理している Firepower Threat Defense デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアントプログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Firepower Device Manager にログインし、URL のパスを /#/api-explorer（https://ftd.example.com/#/api-explorer など）に変更します。

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。 アップグレードパスでバージョンをスキップする場合は、中間リリースの廃止された機能を確認してください。

（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。

バージョン 6.2.3 で廃止された機能

以下の機能はバージョン 6.2.3 で廃止されました。

表 *1*：バージョン *6.2.3* 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
pager FlexConfig コマンド	アップグレード後に設定をやり直す必要があります。	FDM を使用した FTD	バージョン 6.2.3 では、FDM を使用した FTD の場合、**pager** FlexConfig CLI コマンドがブロックされます。
期限切れの動的分析用のCA証明書	なし。ただし、パッチまたはアップグレードが必要です。	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 （18ページ）」を参照してください。

バージョン 6.2.0 で廃止された機能

これらの機能はバージョン 6.2.0 で廃止されました。

表 *2:* バージョン *6.2.0* 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
ネストされた相関ルール	アップグレードが失敗する可能性があります。	FMC	

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 6.2.0 では、ネストされた相関ルールのサポートが終了します。ある相関ルールが別の相関ルールのトリガーとなっている場合、その相関ルールはネストされています。たとえば、どちらも侵入イベントのトリガーであるルール A とルール B を作成する場合、「ルール A は true」をルール B の制約として使用できます。この設定では、ルールAはルール B 内にネストされています。 **自動設定の変更** アップグレードプロセスは、ネストされたルール（ルールA）からネストされたルール（ルール B）へ設定をコピーしてネストされたルールを削除することで、特定のネストされた相関ルールを「フラット化」します。また、アップグレードは、ホストプロファイル/ユーザ資格とスヌーズ/非アクティブ期間を、ネストされたルールからネストルールへコピーします。 非アクティブ期間を除いて、これらのすべての設定について、設定がネスト ルールに存在しない場合にのみ、システムはネストされたルールからネスト ルールへ設定をコピーできます。システムがネストされたルールからネスト ルールへ非アクティブ期間をコピーするときは、結果として生じるルールがネスト構成にもともと含まれる両方のルールの設定を使用するように、ネスト ルールの非アクティブ期間を保持します。 **アップグレードの失敗の回避** アップグレードする前に、ネストされた相関ルールを「フラット化」できることを確認してください。そうなっていなければ、アップグレードは失敗します。ネストされたルールとネスト ルールに特定の競合がある場合は、アップグレードによりネストされたルールをフラット化できないことに注意してください。アップグレードの失敗を回避するには、アップグレードの前に、以下のように相関ルールを変更します。 • ネストされた構成内で 1 つのルールだけ

機能	アップグレードの影響	プラットフォーム	説明
			がこれらの設定を指定するように、ホスト プロファイル資格、ユーザ資格、スヌーズ期間の設定をネストされたルールまたはネスト ルールから削除します。 • 接続トラッカーを任意のネストされたルールから削除します。 • ホスト プロファイル資格、ユーザ資格、スヌーズ期間、非アクティブ期間を、true にする必要がないネストされたルールから削除します。つまり、ネスト ルール内の OR 演算子を使用して他のルールの条件にリンクされているネストされたルールから、これらの要素を削除します。

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。	

廃止された FlexConfig コマンド

このリリースノートでは、廃止された機能 （15 ページ）に、各バージョンの廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。

FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドの完全なリストについては、コンフィギュレーション ガイドを参照してください。

注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

いくつかの Firepower Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。バージョン 6.2.0（FMC 展開）またはバージョン 6.2.3（FDM 展開）以降では、スマート CLI

または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

FTD アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。ご使用の構成は自動的に変換されません。アップグレード後は、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできません。

アップグレード後、FlexConfig ポリシーおよび FlexConfig オブジェクトを確認してください。廃止されたコマンドが含まれている場合、メッセージは問題を示します。設定をやり直すことをお勧めします。新しい設定を確認したら、問題のある FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。

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ッセサルール、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。