特長と機能

このドキュメントでは、Version6.7の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

重要 新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

新機能

FMC バージョン 6.7 の新機能

新しい FMC で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、FMC とデバイスの両方で最新のリリースが前提条件となります。 デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、FMC の最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。新機能の説明では、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

表 *1 : FMC* バージョン *6.7.0* の新機能

機能	説明
プラットフォーム機能	

機能	説明
VMware 向け FMCv での高可用性のサポート。	VMware 向け FMCv は、高可用性をサポートするようになりました。ハードウェアモデルの場合と同様に、FMCv Web インターフェイスを使用して HA を確立します。 FTD の展開では、2 つの同一ライセンスの FMCv と、各管理対象デバイスに 1 つの FTD 権限が必要です。たとえば、FMCv10 HA ペアで 10 台の FTD デバイスを管理するには、2 つの FMCv10 権限と 10 の FTD 権限が必要です。クラシックデバイス（7000/8000 シリーズ、NGIPSv、ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。 この機能は、VMware 向け FMCv 2（つまり、2 つのデバイスのみ管理するようにライセンスされた FMCv）ではサポートされていません。 サポートされるプラットフォーム：VMware 向け FMCv 10、25、および 300
AWS 向け FTDv の自動スケールの改善。	バージョン 6.7.0 には、AWS 向け FTDv の次の自動スケールの改善が含まれています。 • カスタム指標パブリッシャ。新しい Lambda 関数は、自動スケールグループ内のすべての FTDv インスタンスのメモリ消費量について FMC を毎秒ポーリングし、その値を CloudWatch メトリックにパブリッシュします。 • メモリ消費に基づく新しいスケーリングポリシーを使用できます。 • FMC への SSH およびセキュアトンネル用の FTDv プライベート IP 接続。 • FMC の設定検証。 • ELB でより多くのリスニングポートを開くためのサポート。 • シングルスタック展開に変更。すべての Lambda 関数と AWS リソースは、合理化された展開のためにシングルスタックから展開されます。 サポートされているプラットフォーム：AWS の FTDv
Azure 向け FTDv の自動スケールの改善。	Azure 向け FTDv の自動スケール ソリューションには、CPU だけでなく、CPU とメモリ（RAM）に基づくスケーリングメトリックのサポートが含まれるようになりました。 サポートされているプラットフォーム：Azure の FTDv

機能	説明
Firepower Threat Defense：デバイス管理	
データインターフェイスでの FTD の管理。	専用の管理インターフェイスではなく、データインターフェイス上の FTD の FMC 管理を設定できるようになりました。 この機能は、本社の FMC からブランチオフィスの FTD を管理し、外部インターフェイスで FTD を管理する必要がある場合に、リモート展開に役立ちます。DHCP を使用して FTD でパブリック IP アドレスを受信する場合は、オプションで Web タイプの更新方式を使用して、インターフェイスのダイナミック DNS（DDNS）を設定できます。DDNS は、FTD の IP アドレスが変更された場合に FMC が完全修飾ドメイン名（FQDN）で FTD に到達できるようにします。 （注） データインターフェイスでの FMC アクセスは、クラスタリングまたはハイアベイラビリティではサポートされません。 新規/変更されたページ： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [管理（Management）]** セクション • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [FMCアクセス（FMC Access）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [DHCP] > [DDNS] > [DDNS更新方式（DDNS Update Methods）]** ページ 新規/変更された FTD CLI コマンド：**configure network management-data-interface**、**configure policy rollback** サポートされるプラットフォーム：FTD
FTD での FMC IP アドレスの更新。	FMC IP アドレスを変更する場合に、FTD CLI を使用してデバイスを更新できるようになりました。 新規/変更された FTD CLI コマンド： **configure manager edit** サポートされるプラットフォーム：FTD

機能	説明
Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期。	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。 現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、FTD が処理できるようになる前に外部ルータが FTD へのトラフィックの送信を開始することがあるためです。 この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する FTD ではサポートされません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] ページ：[論理デバイス（Logical Devices）]>[リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
Firepower 1100/2100 シリーズの SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	**アップグレードの影響。** フロー制御とリンク ステータス ネゴシエーションを無効化するように Firepower 1100/2100 シリーズ SFP インターフェイスを設定できるようになりました。 以前は、これらのデバイスで SFP インターフェイス速度（1000 または 10000 Mbps）を設定すると、フロー制御とリンク ステータス ネゴシエーションが自動的に有効になり、無効にはできませんでした。 [ネゴシエーションなし（No Negotiate）] を選択して、フロー制御とリンク ステータス ネゴシエーションを無効化できるようになりました。これにより、1 GB SFP インターフェイスまたは 10 GB SFP+ インターフェイスを設定しているかに関係なく、速度は 1000 Mbps に設定されます。10000 Mbps でネゴシエーションを無効化することはできません。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（edit interface）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）] サポートされるプラットフォーム：Firepower 1100/2100 シリーズ
Firepower Threat Defense：クラスタリング	
FMC の新しいクラスタ管理機能。	FMC を使用して、以前は CLI を使用する必要のあった次のクラスタ管理タスクを実行できるようになりました。 • クラスタユニットを有効または無効にします。 • [Device Management] ページからクラスタのステータスを表示します（ユニットごとの履歴とサマリーを含む）。 • ロールをコントロールユニットに変更します。 新規/変更されたページ： • [Devices] > [Device Management] > [More] メニュー • [Devices] > [Device Management] > [Cluster] > [General] エリア > [Cluster Live Status] リンク > [Cluster Status] サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
クラスタ導入の高速化。	クラスタの展開がより迅速に完了するようになりました。また、ほとんどの導入の失敗も、より迅速に失敗します。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの [フラットなポート範囲（Flat Port Range）] オプションがデフォルトで有効になり、設定できなくなりました。	**アップグレードの影響。** PAT アドレスがクラスタのメンバーに配布される方法が変更されます。 以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御は各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じ PAT アドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。 ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1024 ー 65535 を使用できるようになりました。以前は、[Flat Port Range] オプションを PAT プールルール（FTD NAT の [Pat Pool] タブ）で有効化することで、フラットな範囲を使用できました。[フラットなポート範囲（Flat Port Range）] オプションは無視され、PAT プールは常にフラットになります。必要に応じて [Include Reserved Ports] オプションを選択して、PAT プールに 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（[ブロック割り当て（Block Allocation）] PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 この変更は自動的に有効になります。アップグレードの前後に何もする必要はありません。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：暗号化と VPN	

機能	説明
RA VPN の AnyConnect モジュールサポート。	FTD RA VPN で AnyConnect モジュールがサポートされるようになりました。 RA VPN グループポリシーの一部として、ユーザーが Cisco AnyConnect VPN クライアントをダウンロードするときに、さまざまなオプションモジュールをダウンロードしてインストールするように設定できるようになりました。これらのモジュールは、Web セキュリティ、マルウェア保護、オフネットワークローミング保護などのサービスを提供できます。 各モジュールを、AnyConnect プロファイルエディタで作成され、AnyConnect ファイルオブジェクトとして FMC にアップロードされたカスタム設定を含むプロファイルに関連付ける必要があります。 新規/変更されたページ： • モジュールプロファイルのアップロード：新しい [File Type] オプションが [Objects] > [Object Management] > [VPN] > [AnyConnect File] > [Add AnyConnect File] に追加されました • モジュールの設定：[Client Modules] オプションが [Objects] > [Object Management] > [VPN] > [Group Policy] > [add or edit a Group Policy object] > [AnyConnect] 設定に追加されました サポートされるプラットフォーム：FTD
RA VPN の AnyConnect 管理 VPN トンネル。	FTD RA VPN は、エンドユーザーが VPN 接続を確立したときだけでなく、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルをサポートするようになりました。 この機能は、オフィスネットワークに VPN を介してユーザーが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで管理者がパッチ管理を行うのに役立ちます。社内ネットワークの接続を必要とするエンドポイントオペレーティング システム ログイン スクリプトに対するメリットもあります。 サポートされるプラットフォーム：FTD

機能	説明
RA VPN のシングルサインオン。	FTD RA VPN は、 SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）で設定されたリモートアクセス VPN ユーザーのシングルサインオン（SSO）をサポートするようになりました。 新規/変更されたページ： • SSO サーバーへの接続：[Objects] > [Object Management] > [AAA Server] > [Single Sign-on Server] • RA VPN の一部として SSO を設定します。RA VPN 接続プロファイルを設定する際に、認証方式（AAA 設定）として [SAML] を追加しました。 サポートされるプラットフォーム：FTD
RA VPN の LDAP 許可。	FTD RA VPN は、LDAP 属性マップを使用した LDAP 認証をサポートするようになりました。 LDAP 属性マップにより、Active Directory（AD）または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。その後、リモートアクセス VPN 接続の確立中に AD または LDAP サーバーが FTD デバイスに認証を返すと、FTD デバイスは、その情報を使用して、AnyConnect クライアントが接続を完了する方法を調整できます。 サポートされるプラットフォーム：FTD

機能	説明
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN。	FTD サイト間 VPN は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートするようになりました。 ポリシーベース VPN の代替策として、仮想トンネルインターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。これは、動的または静的なルートの使用が可能です。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。トラフィックは、スタティックルートまたは BGP を使用して暗号化されます。ルーテッドセキュリティゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールを定義できます。 VTI ベースの VPN は、次の間で作成できます。 • 2 つの FTD デバイス • FTD デバイスとパブリッククラウド • FTD デバイスとサービスプロバイダーの冗長性を備えた別の FTD デバイス 新規/変更されたページ： • **[Devices] > [Device Management] > [Interfaces] > [Add Interfaces] > [Virtual Tunnel Interface]** • **[Devices] > [VPN] > [Site To Site] > [Add VPN] > [Firepower Threat Defense Device] > [Route Based (VTI)]** サポートされるプラットフォーム：FTD
サイト間 VPN に対するダイナミック RRI サポート。	FTD サイト間 VPN は、サイト間 VPN 展開で IKEv2 ベースのスタティック暗号マップでサポートされるダイナミック リバース ルート インジェクション（RRI）をサポートするようになりました。これにより、スタティックルートは、リモート トンネルエンドポイントで保護されているネットワークとホストのルーティングプロセスに自動的に挿入されます。 新規/変更されたページ：サイト間 VPN トポロジにエンドポイントを追加するときの [ダイナミック リバース ルート インジェクションの有効化（Enable Dynamic Reverse Route Injection）] 詳細オプションが追加されました。 サポートされるプラットフォーム：FTD

機能	説明
手動証明書登録の拡張機能。	署名済み CA 証明書とアイデンティティ証明書を CA 機関から互いに独立して取得できるようになりました。 証明書署名要求（CSR）を作成し、アイデンティティ証明書を取得するための登録パラメータを保存する PKI 証明書登録オブジェクトに次の変更を行いました。 • PKI 証明書登録オブジェクトの手動登録設定に [CA Only] オプションが追加されました。このオプションを有効にすると、CA 機関から署名済み CA 証明書のみを受け取り、アイデンティティ証明書は受け取りません。 • PKI 証明書登録オブジェクトの手動登録設定で、[CA Certificate] フィールドを空白のままにできるようになりました。これを行うと、署名済み CA 証明書ではなく、CA 機関からアイデンティティ証明書のみを受け取ります。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [証明書の登録（Cert Enrollment）] > [証明書の登録の追加（Add Cert Enrollment）] > [CA 情報（CA Information）] > [登録タイプ（Enrollment Type）] > [手動（Manual）] サポートされるプラットフォーム：FTD
FTD 証明書管理の拡張機能。	FTD 証明書管理に次の機能拡張が行われました。 • 証明書の内容を表示するときに、認証局（CA）のチェーンを表示できるようになりました。 • 証明書をエクスポートできるようになりました。 新規/変更されたページ： • [Devices] > [Certificates] > [Status] 列 > [View] アイコン（虫めがね） • [Devices] > [Certificates] > [Export] アイコン サポートされるプラットフォーム：FTD
アクセス制御：URL フィルタリング、アプリケーション制御、およびセキュリティ インテリジェンス	

機能	説明
TLS 1.3（TLS サーバーアイデンティティ検出）で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御。	サーバー証明書からの情報を使用して、TLS 1.3 で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御を実行できるようになりました。この機能が動作するためにトラフィックを復号化する必要はありません。 （注） 暗号化トラフィックで URL フィルタリングとアプリケーション制御を実行する場合は、この機能を有効にすることを推奨します。ただし、特に低メモリモデルでは、デバイスのパフォーマンスに影響を与える可能性があります。 新規/変更されたページ：アクセス コントロール ポリシーの [詳細（Advanced）] タブに [TLS サーバーアイデンティティ検出（TLS Server Identity Discovery）] の警告とオプションが追加されました。 新規/変更された FTD CLI コマンド：**show conn detail** コマンドの出力に B フラグが追加されました。TLS 1.3 暗号化接続では、このフラグは、アプリケーションおよび URL の検出にサーバー証明書を使用したことを示します。 サポートされるプラットフォーム：FTD
レピュテーションが不明な Web サイトへのトラフィックに対する URL フィルタリング。	レピュテーションが不明な Web サイトに対して URL フィルタリングを実行できるようになりました。 新規/変更されたページ：アクセス制御、QoS、および SSL ルールエディタに [不明なレピュテーションに適用（Apply to unknown reputation）] チェックボックスが追加されました。 サポートされるプラットフォーム：FMC

機能	説明
DNS フィルタリングにより URL フィルタリングを強化します。	**ベータ版。** *DNS*フィルタリングは、暗号化されたトラフィックを含め（ただしトラフィックを復号化せずに）トランザクションの早い段階で要求されたドメインのカテゴリとレピュテーションを決定することで、URL フィルタリングを強化します。アクセス コントロール ポリシーごとに DNS フィルタリングを有効にし、そのポリシーのすべてのカテゴリ/レピュテーション URL ルールに適用します。 （注） DNS フィルタリングはベータ機能であり、期待どおりに動作しない可能性があります。実稼働環境では使用しないでください。 新規/変更されたページ：[全般設定（General Settings）] の下のアクセス コントロール ポリシーの [詳細（Advanced）] タブに [DNS トラフィックへのレピュテーション適用の有効化（Enable reputation enforcement on DNS traffic）] オプションが追加されました。 サポートされるプラットフォーム：FMC
セキュリティ インテリジェンス フィードの更新頻度の短縮。	FMC は、5 分または 15 分ごとにセキュリティ インテリジェンス データを更新できるようになりました。以前は、最短更新頻度は 30 分でした。 カスタムフィードでこれらの短い頻度のいずれかを設定する場合は、md5 チェックサムを使用してフィードにダウンロードする更新があるかどうかを判断するようにシステムを設定する必要もあります。 新規/変更されたページ： [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワークリストとフィード（Network Lists and Feeds）] > [フィードの編集（edit feed）] > [更新頻度（Update Frequency）] に新しいオプションが追加されました。 サポートされるプラットフォーム：FMC
アクセス制御：ユーザー制御	

機能	説明
ISE/ISE-PIC を使用した pxGrid 2.0。	**アップグレードの影響。** FMC を ISE/ISE-PIC アイデンティティソースに接続する場合は、pxGrid 2.0 を使用します。まだ pxGrid 1.0 を使用している場合は、ここで切り替えてください。このバージョンは廃止されました。 pxGrid 2.0 で使用するために、バージョン 6.7.0 では Cisco ISE 適応型ネットワーク制御（ANC）修復が導入され、相関ポリシー違反に関連する ISE 設定 ANC ポリシーが適用またはクリアされます。 pxGrid 1.0 で Cisco ISE エンドポイント保護サービス（EPS）修復を使用した場合は、pxGrid 2.0 で ANC 修復を設定して使用します。「誤った」pxGrid を使用している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。 サポートされているすべての Firepower バージョン（統合製品を含む）の詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。 新規/変更されたページ： • [Policies] > [Actions] > [Modules] > [Installed Remediation Modules] リスト • [Policies] > [Actions] > [Instances] > [Select a module type] ドロップダウンリスト サポートされるプラットフォーム：FMC
レルムシーケンス。	レルムを順序付けられたレルムシーケンスにグループ化できるようになりました。 単一のレルムを追加するのと同じ方法で、アイデンティティルールにレルムシーケンスを追加します。アイデンティティルールをネットワークトラフィックに適用すると、システムは指定された順序で Active Directory ドメインを検索します。LDAP レルムのレルムシーケンスは作成できません。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [レルムシーケンス（Realm Sequences）] サポートされるプラットフォーム：FMC

機能	説明
ISE サブネットフィルタリング。	特にメモリの少ないデバイスでは、CLI を使用して、ISE からのユーザーと IP およびセキュリティグループタグ（SGT）と IP のマッピングの受信から、サブネットを除外できるようになりました。 Snort Identity Memory Usage ヘルスモジュールは、メモリ使用率が特定のレベル（デフォルトでは 80%）を超えるとアラートを出します。 新しいデバイス CLI コマンド： **configure identity-subnet-filter** {**add** | **remove**} サポートされるプラットフォーム：FMC 管理対象デバイス
アクセス制御：侵入およびマルウェア防御	
動的分析のためのファイルの事前分類の改善。	**アップグレードの影響。** システムは、静的分析の結果（動的要素のないファイルなど）に基づいて、疑わしいマルウェアファイルを動的分析用に送信しないことを決定できるようになりました。 アップグレード後、[Captured Files] テーブルでは、これらのファイルの動的分析ステータスが [Rejected for Analysis] になります。 サポートされるプラットフォーム：FMC

機能	説明
S7Commplusプリプロセッサ。	新しい S7Commplus プリプロセッサは、広く受け入れられている S7 産業用プロトコルをサポートします。これを使用して、対応する侵入ルールとプリプロセッサルールを適用し、悪意のあるトラフィックをドロップし、侵入イベントを生成できます。 新規/変更されたページ： • プリプロセッサの有効化：ネットワーク分析ポリシーエディタで、[Settings] をクリックし（「Settings」という語をクリックします）、SCADA プリプロセッサで [S7Commplus Configuration] を有効にします。 • プリプロセッサの設定：ネットワーク分析ポリシーエディタの [Settings] で、[S7Commplus Configuration] をクリックします。 • S7Commplus プリプロセッサルールの設定：侵入ポリシーエディタで、[Rules] > [Preprocessors] > [S7 Commplus Configurations] の順にクリックします。 サポートされるプラットフォーム：ISA 3000 を含むすべての FTD デバイス
カスタム侵入ルールのインポートでルール競合の際に警告表示。	カスタム（ローカル）侵入ルールをインポートする場合、FMC がルールの競合について警告するようになりました。以前は、FMC は競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン 6.6.0.1 は除きます。 [ルールの更新（Rule Updates）] ページで、ルールのインポートに競合があった場合は、[ステータス（Status）] 列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールをインポートするためのベストプラクティスを参考にすることを推奨します。 新規/変更されたページ：**[システム（System）] > [更新（Updates）] > [ルールの更新（Rule Updates）]** に警告アイコンが追加されました。 サポートされるプラットフォーム：FMC

機能	説明
アクセス制御：TLS/SSL 暗号解読	
復号の既知キー TLS/SSL ルールのための ClientHello の変更。	**アップグレードの影響。** TLS/SSL 復号化を設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを復号の既知キーアクションを含む TLS/SSL ルールと照合しようとします。以前は、システムは ClientHello メッセージと復号 - 再署名ルールのみを照合していました。 照合は ClientHello メッセージからのデータとキャッシュされたサーバー証明書データからのデータに依存します。メッセージが一致すると、ClientHello メッセージが特定の方法で変更されます。FMC コンフィギュレーションガイドの「*ClientHello* メッセージ処理」のトピックを参照してください。 この動作の変更は、アップグレード後に自動的に行われます。復号の既知キー TLS/SSL ルールを使用する場合は、暗号化されたトラフィックが期待どおりに処理されていることを確認します。 サポートされているプラットフォーム：すべてのデバイス
イベントロギングおよび分析	
オンプレミスの Stealthwatch ソリューションによるリモートデータストレージと相互起動。	オンプレミスの Stealthwatch ソリューションである Cisco Security Analytics and Logging（On Premises）を使用して、大量の Firepower イベントデータを FMC 以外に保存できるようになりました。 FMC でイベントを表示する場合、リモートデータストレージの場所にあるイベントをすばやく相互起動して表示できます。FMC は syslog を使用して、接続、セキュリティインテリジェンス、侵入、ファイル、およびマルウェアイベントを送信します。 （注） このオンプレミスソリューションは、バージョン 6.4.0 以上を実行している FMC でサポートされます。ただし、コンテキスト相互起動には Firepower バージョン 6.7.0 以上が必要です。このソリューションは、Stealthwatch Enterprise（SWE）バージョン 7.3 を実行する必要がある Stealthwatch Management Console（SMC）用の Security Analytics and Logging On Prem アプリケーションの可用性にも依存します。 サポートされるプラットフォーム：FMC

機能	説明
Stealthwatch コンテキスト相互起動リソースを迅速に追加する。	FMC の新しいページを使用すると、Stealthwatch アプライアンスのコンテキスト相互起動リソースをすばやく追加できます。 Stealthwatch リソースを追加した後は、一般的なコンテキスト相互起動ページで管理します。ここで、Stealthwatch 以外の相互起動リソースを手動で作成および管理します。 新規/変更されたページ： • Stealthwatch リソースを追加します。[System] > [Logging] > [Security Analytics and Logging] • リソースを管理します。[Analysis] > [Advanced] > [Contextual Cross-Launch] サポート対象プラットフォーム：FMC
新しい相互起動オプションフィールドタイプ。	次のイベントデータの追加タイプを使用して、外部リソースに相互起動できるようになりました。 • アクセス コントロール ポリシー • 侵入ポリシー • アプリケーションプロトコル • クライアント アプリケーション • Web アプリケーション • ユーザー名（レルムを含む） 新規/変更されたページ： • 相互起動クエリリンクを作成または編集する際の新しい変数：[Analysis] > [Advanced] > [Contextual Cross-Launch]。 • ダッシュボードとイベントビューアの新しいデータタイプで、右クリックで相互起動が可能になりました。 サポートされるプラットフォーム：FMC

機能	説明
National Vulnerability Database（NVD）が Bugtraq に代わって使用されるようになりました。	**アップグレードの影響。** Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データはNVDから取得されています。この変更をサポートするために、次の変更を行いました。 • [CVE ID] および [Severity] フィールドが [Vulnerabilities] テーブルに追加されました。テーブルビューで CVE ID を右クリックすると、NVDの脆弱性に関する詳細を表示できます。 • [Vulnerability Impact] フィールドが [Impact] に名前変更されました（テーブルビューのみ）。 • 使用されていない/冗長な [Bugtraq ID]、[Title, Available Exploits]、[Technical Description]、[Solution] フィールドが削除されました。 • ホストネットワークマップから [Bugtraq ID] フィルタリングオプションが削除されました。 脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。 サポートされるプラットフォーム：FMC
のアップグレード	

機能	説明
アップグレード前の互換性チェック。	

機能	説明
	アップグレードの影響。 FMC展開では、より複雑な準備状況チェックを実行したり、アップグレードを試行したりする前に、Firepowerアプライアンスがアップグレード前の互換性チェックに合格することが必要になりました。このチェックは、アップグレードが失敗する原因となる問題を検出します。これらをより早期に検出し、続行をブロックするようになりました。 検出は次のとおりです。 • FXOS を新しいリリースの付属する FXOS バージョンにアップグレードするまで、FMC を使用して Firepower 4100/9300 シャーシをバージョン 6.7.0 以降にアップグレードすることはできません。 デバイスをバージョン 6.7.0 以降にアップグレードしている限り、アップグレードはブロックされます。たとえば、Firepower バージョン 6.6.x に対して古いバージョンの FXOS がデバイスで実行されている場合でも、Firepower 4100/9300 の 6.3 → 6.6.x のアップグレードはブロックされません。 • デバイスの設定が古い場合、FMC を使用してデバイスをアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行しており、管理対象デバイスを有効なターゲットにアップグレードしている限り、アップグレードはブロックされます。たとえば、デバイスの設定が古い場合、デバイスを 6.3.0 → 6.6.x にアップグレードするとブロックされます。 • デバイスの設定が古い場合、FMC をバージョン 6.7.0 以上からアップグレードすることはできません。 FMC がバージョン 6.7.0 以降を実行している限り、アップグレードはブロックされます。以前のバージョン（バージョン 6.7.0 へのアップグレードを含む）からアップグレードする場合は、必ず自分で展開する必要があります。 インストールするアップグレードパッケージを選択すると、FMCはすべての対象アプライアンスの互換性チェック結果を表示します。新しい [Readiness Check] ページにもこの情報が表示されます。示された問題を修正するまでアップグレードできません。 新規/変更されたページ： • アップグレードパッケージの**[System]** > **[Update]** > **[Product**

機能	説明
	Updates] > **[Available Updates]** > **[Install]**アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]** サポートされるプラットフォーム：FMC、FTD

機能	説明
準備状況チェックの改善。	

機能	説明
	アップグレードの影響。 準備状況チェックにより、ソフトウェアをアップグレードするための Firepower アプライアンスの準備状況を評価できます。これらのチェックには、データベースの整合性、ファイルシステムの整合性、設定の整合性、ディスク容量などが含まれます。 FMC をバージョン 6.7.0 にアップグレードすると、FTD のアップグレード準備状況チェックが次のように改善されます。 • 準備状況チェックが高速になります。 • デバイス CLI にログインすることなく、ハイアベイラビリティおよびクラスタ化された FTD デバイスで準備状況チェックがサポートされるようになりました。 • FTD デバイスをバージョン 6.7.0 以上にアップグレードするための準備状況チェックで、デバイスにアップグレードパッケージが存在する必要はなくなりました。アップグレード自体を開始する前に、アップグレードパッケージをデバイスにプッシュすることをお勧めしますが、準備状況チェックを実行する前に行う必要はありません。 • インストールするアップグレードパッケージを選択すると、該当するすべての FTD デバイスの準備状況が FMC に表示されるようになりました。新しい [Readiness Checks] ページでは、展開内の FTD デバイスの準備状況チェックの結果を表示できます。このページから準備状況チェックを再実行することもできます。 • 準備状況チェックの結果には、推定アップグレード時間が含まれます（ただし、リブート時間は含まれません）。 • エラーメッセージの方が優れています。FMC のメッセージセンターから成功/失敗ログをダウンロードすることもできます。 FMC がバージョン 6.7.0 以上を実行している限り、これらの改善はバージョン 6.3.0 以上からの FTD アップグレードでサポートされます。 新規/変更されたページ： • アップグレードパッケージの **[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]** アイコン • **[System]** > **[Update]** > **[Product Updates]** > **[Readiness Checks]**

機能	説明
	• **[Message Center] > [Tasks]** サポートされるプラットフォーム：FTD

機能	説明
FTD アップグレード ステータス レポートとキャンセル/再試行オプションの改善。	

機能	説明
	アップグレードの影響。 [Device Management] ページで、進行中のデバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を表示できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。 デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。 また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル（[Cancel Upgrade]）することも、失敗したアップグレードを再試行（[Retry Upgrade]）することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。 （注） 失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、FMC を使用して FTD デバイスをアップグレードするときに表示される新しい自動キャンセルオプションを無効にする必要があります（[Automatically cancel on upgrade failure and roll back to the previous version]）。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。 パッチの自動キャンセルはサポートされていません。HA またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 新規/変更されたページ： • FTD アップグレードパッケージの**[System]** > **[Update]** > **[Product Updates]** > **[Available Updates]** > **[Install]**アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新しい FTD CLI コマンド： • **show upgrade status detail**

機能	説明
	• **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry** サポートされるプラットフォーム：FTD
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。** FMC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、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン 6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。 サポートされるプラットフォーム：FMC
アップグレードでディスク容量を節約するために PCAP ファイルが削除される。	**アップグレードの影響。** Firepowerアプライアンスをアップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。 サポートされるプラットフォーム：すべて
展開とポリシー管理	

機能	説明
設定のロール バック。	**ベータ版。** FTD デバイスの設定を「ロールバック」して、以前に展開した設定に置き換えることができるようになりました。 （注） ロールバックはベータ機能であり、すべての展開タイプとシナリオでサポートされているわけではありません。これは中断を伴う操作でもあります。FMC コンフィギュレーション ガイドの「ポリシー管理」の章に記載されているガイドラインと制限事項を必ず読んで理解してください。 新規/変更されたページ：[Deploy] > [Deployment History] > [Rollback] 列とアイコン。 サポートされるプラットフォーム：FTD
侵入およびファイルポリシーを（アクセス コントロール ポリシーとは無関係に）展開する。	依存する変更がない限り、アクセス コントロール ポリシーとは無関係に侵入ポリシーとファイルポリシーを選択して展開できるようになりました。 新規/変更されたページ：[展開（Deploy）] > [展開（Deployment）] サポートされるプラットフォーム：FMC
アクセス制御ルールのコメントの検索。	アクセス制御ルールのコメント内で検索できるようになりました。 新規/変更されたページ：アクセス コントロール ポリシー エディタで、[検索ルール（Search Rules）] ドロップダウンダイアログに[コメント（Comments）]フィールドが追加されました。 サポートされるプラットフォーム：FMC
FTD NAT ルールの検索とフィルタリング。	FTD NAT ポリシーでルールを検索して、IP アドレス、ポート、オブジェクト名などに基づいてルールを検索できるようになりました。検索結果には部分一致が含まれます。条件で検索すると、ルールテーブルがフィルタリングされ、一致するルールのみが表示されます。 新規/変更されたページ：FTD NAT ポリシーを編集するときに、ルールテーブルの上に検索フィールドが追加されました。 サポートされるプラットフォーム：FTD

機能	説明
アクセス コントロール ポリシーとプレフィルタポリシー間のルールのコピーおよび移動。	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。アクセス コントロール ポリシーとそれに関連付けられたプレフィルタポリシーの間でルールを移動することもできます。 新規/変更されたページ：アクセス コントロール ポリシー エディタおよびプレフィルタ ポリシー エディタで、各ルールの右クリック メニューに [Copy] および [Move] オプションが追加されました。 サポートされるプラットフォーム：FMC
オブジェクト一括インポート。	カンマ区切り値（CSV）ファイルを使用して、ネットワーク、ポート、URL、VLAN タグ、および識別名オブジェクトを FMC に一括インポートできるようになりました。 制限事項および特定のフォーマット手順については、FMC コンフィギュレーション ガイドの「再利用可能なオブジェクト」の章を参照してください。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [オブジェクトタイプの選択（choose an object type）] > [オブジェクトタイプの追加（Add Object Type）] > [オブジェクトのインポート（Import Object）] サポートされるプラットフォーム：FMC

機能	説明
アクセス制御およびプレフィルタポリシーのインターフェイス オブジェクトの最適化。	特定のFTDデバイスでインターフェイス オブジェクトの最適化を有効にできるようになりました。 展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。 インターフェイス オブジェクトの最適化はデフォルトで無効になっています。これを有効にする場合は、[Object Group Search] も有効にする必要があります。これは、ネットワークオブジェクトに加えてインターフェイス オブジェクトにも適用されるようになり、デバイスのメモリ使用量を削減できます。 新規/変更されたページ：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[デバイス（Device）**>**[詳細設定（Advanced Settings）]** セクション > [インターフェイス オブジェクトの最適化（Interface Object Optimization）] チェックボックス サポートされるプラットフォーム：FTD
管理とトラブルシューティング	
FMC シングルサインオン。	FMC は、サードパーティの SAML 2.0 準拠アイデンティティプロバイダー（IdP）で設定された外部ユーザーのシングルサインオン（SSO）をサポートするようになりました。IdP のユーザーまたはグループロールをFMCユーザーロールにマッピングできます。 新規/変更されたページ： • **[Login]** > **[Single Sign-On]** • **[System]** > **[Users]** > **[SSO]** サポートされるプラットフォーム：FMC
FMC ログアウトの遅延。	FMC からログアウトする場合、自動的に 5 秒間のカウントダウンが行われます。[ログアウト（Log Out）] を再度クリックすると、すぐにログアウトできます。 サポートされるプラットフォーム：FMC

機能	説明
FTD コンテナインスタンスのバックアップと復元。	FMC を使用してバージョン 6.7.0 以降の FTD コンテナインスタンスをバックアップおよび復元できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300
ヘルスモニタリングの強化。	ヘルスモニタリングが次のように拡張されました。 • [Health Status] サマリーページでは Firepower Management Center と FMC が管理するすべてのデバイスの正常性を一目で確認できます。 • [Monitoring] ナビゲーションペインでは、デバイス階層を移動できます。 • 管理対象デバイスは、個別に一覧表示されるか、該当する場合は地理位置情報、高可用性、またはクラスタステータスに基づいてグループ化されます。 • ナビゲーションペインから個々のデバイスのヘルスモニターを表示できます。 • 相互に関連するメトリックを相互に関連付けるカスタムダッシュボード。CPU や Snort などの事前定義された相関グループから選択します。または、使用可能なメトリックグループから独自の変数セットを作成して、カスタム相関ダッシュボードを作成します。 サポートされるプラットフォーム：FMC

機能	説明
ヘルスモジュールの更新。	CPU 使用率ヘルスモジュールが 4 つの新しいモジュールに置き換わりました。 • CPU使用率（コアごと）：すべてのコアのCPU使用率をモニターします。 • CPU 使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU 使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 メモリ使用量を追跡するために、次のヘルスモジュールが追加されました。 • メモリ使用率データプレーン：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。 統計情報を追跡するために、次のヘルスモジュールが追加されました。 • 接続統計情報：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACEの数やIPSルールなど）をモニターします。 • Snort 統計情報：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 サポートされるプラットフォーム：FMC

機能	説明
メッセージセンターの検索。	メッセージセンターで現在のビューをフィルタリングできるようになりました。 新規/変更されたページ：メッセージセンターの [Show Notifications] スライダに [Filter] アイコンとフィールドが追加されました。 サポートされるプラットフォーム：FMC
ユーザビリティとパフォーマンス	
Dusk テーマ。	**ベータ版。** FMC Web インターフェイスのデフォルトは Light テーマですが、新しい Dusk テーマを選択することもできます。 （注） Dusk テーマはベータ機能です。ページまたは機能を使用できない問題が発生した場合は、別のテーマに切り替えてください。すべてに対応することはできませんが、フィードバックもお寄せください。[ユーザー設定 (User Preferences)] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com までお問い合わせください。 新規/変更されたページ：ユーザー名の下にあるドロップダウンリストの [ユーザー設定（User Preferences）] サポートされるプラットフォーム：FMC
FMC メニューの検索。	FMC メニューを検索できるようになりました。 新規/変更されたページ：[Deploy] メニューの左側にある [FMC] メニューバーに [Search] アイコンとフィールドが追加されました。 サポートされるプラットフォーム：FMC
Firepower Management Center REST API	

機能	説明
新しい REST API サービス。	

機能	説明
	新機能と既存の機能をサポートするために、次の FMC REST API サービス/操作が追加されました。 認可サービス： • ssoconfig：FMC シングルサインオンを取得および変更するための GET および PUT 操作。 ヘルスサービス： • メトリック：ヘルスモニターのメトリックを取得する GET 操作。 • アラート：ヘルスアラートを取得する GET 操作。 • deploymentdetails：展開の正常性の詳細を取得する GET 操作。 展開サービス： • jobhistories：展開履歴を取得する GET 操作。 • rollbackrequests：設定ロールバックを要求する POST 操作。 デバイスサービス： • メトリック：デバイスメトリックを取得する GET 操作。 • virtualtunnelinterfaces：仮想トンネルインターフェイスを取得および変更するための GET、PUT、POST、および DELETE 操作。 統合サービス： • externalstorage：外部イベントストレージ設定を取得および変更するための GET、ID による GET、および PUT 操作。 ポリシーサービス： • intrusionpolicies：侵入ポリシーを変更するための POST および DELETE 操作。 サービスの更新： • cancelupgrades：失敗したアップグレードをキャンセルする POST 操作。 • retryupgrades：失敗したアップグレードを再試行する POST 操作。

機能	説明
	サポートされるプラットフォーム：FMC

FDM バージョン 6.7 の新機能

表 *2 : FDM* バージョン *6.7.0* の新機能

機能	説明
プラットフォーム機能	
ASA 5525-X、5545-X、5555-X でのサポートが終了します。最後にサポートされていたリリースは FTD 6.6 です。	FTD 6.7 を ASA 5525-X、5545-X、5555-X にインストールすることはできません。これらのモデルで最後にサポートされていたリリースは FTD 6.6 です。
ファイアウォールと IPS の機能	
アクセス制御ルールの照合のための TLS サーバーアイデンティティ検出	TLS 1.3 証明書は暗号化されます。TLS 1.3 で暗号化されたトラフィックで、アプリケーションまたはURL フィルタリングを使用するアクセスルールに対応するには、システムが TLS 1.3 証明書を復号する必要があります。暗号化された接続が適切なアクセス制御ルールに適合していることを確認するため、[TLS Server Identity Discovery] を有効にすることを推奨します。この設定では、証明書のみが復号されます。接続は暗号化されたままになります。 [Access Control Settings]（⚙）ボタンとダイアログボックスが **[Policy]** > **[Access Control]**ページに追加されました。
外部の信頼できる CA 証明書のグループ	SSL 復号ポリシーで使用される信頼できる CA 証明書のリストをカスタマイズできるようになりました。デフォルトでは、ポリシーはすべてのシステム定義の信頼できる CA 証明書を使用しますが、カスタムグループを作成して証明書を追加したり、デフォルトグループを独自のより制限されたグループに置き換えることができます。 **[Objects]** > **[Certificates]** ページに証明書グループが追加され、SSL 復号ポリシー設定を変更して証明書グループを選択できるようにしました。

機能	説明
パッシブ ID ルールの Active Directory レルムシーケンス	Active Directory（AD）サーバーとそのドメインの番号付きリストであるレルムシーケンスを作成し、パッシブ認証 ID ルールで使用できます。レルムシーケンスは、複数の AD ドメインをサポートしている状況で、ユーザーベースのアクセス制御を実行するときに役立ちます。各 AD ドメインの個別のルールを記述する代わりに、すべてのドメインを対象とする単一のルールを作成できます。シーケンス内の AD レルムの順序は、ID の競合が発生した場合に、その競合を解決するために使用されます。 **[Objects]** > **[Identity Sources]** ページに AD レルム シーケンス オブジェクトが追加され、そのオブジェクトをパッシブ認証アイデンティティルールのレルムとして選択できるようになりました。FTD API に **RealmSequence** リソースが追加されました。また **IdentityRule** リソースには、アクションとしてパッシブ認証を使用するルールのレルムとしてレルム シーケンス オブジェクトを選択する機能が追加されました。
TrustSec セキュリティグループタグ（SGT）グループオブジェクトの FDM サポートと、アクセス制御ルールでのそれらの使用	FTD 6.5 では、SGT グループオブジェクトを設定し、それらをアクセス制御ルールの一致基準として使用するためのサポートが FTD API に追加されました。さらに、ISE によってパブリッシュされた SXP トピックをリッスンするように ISE アイデンティティ オブジェクトを変更できます。これらの機能を FDM で直接設定できるようになりました。 新しいオブジェクトである SGT グループが追加され、それらを選択および表示できるようにアクセス制御ポリシーが更新されました。また、サブスクライブするトピックの明示的な選択を含むように ISE オブジェクトを変更しました。

機能	説明
Snort 3.0 のサポート	新しいシステムでは、Snort 3.0 がデフォルトの検査エンジンです。古いリリースから 6.7 にアップグレードした場合、アクティブな検査エンジンは Snort 2.0 のままですが、Snort 3.0 に切り替えることができます。このリリースでは、Snort 3.0 は、仮想ルータ、時間ベースのアクセス制御ルール、または TLS 1.1 以下の接続の復号化をサポートしていません。これらの機能が必要ない場合にのみ Snort 3.0 を有効にしてください。Snort 2.0 と Snort 3.0 の間を自由に切り替えることができるため、必要に応じて、変更を元に戻すことができます。バージョンを切り替えるたびにトラフィックが中断されます。 **[デバイス（Device）] > [更新（Updates）]** ページの [侵入ルール（Intrusion Rules）] グループに Snort のバージョンを切り替える機能が追加されました。FTD API では、IntrusionPolicy リソースアクション/toggleinspectionengine が追加されました。 さらに、Snort 3 ルールパッケージの更新で追加、削除、または変更された侵入ルールを示す新しい監査イベント、ルール更新イベントがあります。
Snort 3 のカスタム侵入ポリシー	Snort 3 を検査エンジンとして使用している場合は、カスタム侵入ポリシーを作成できます。これに対し、Snort 2 を使用する場合にのみ、事前定義されたポリシーを使用できます。カスタム侵入ポリシーを使用すると、ルールのグループを追加または削除し、グループレベルでセキュリティレベルを変更して、グループ内のルールのデフォルトアクション（無効化、アラート、またはドロップ）を効率的に変更できます。Snort 3 の侵入ポリシーを使用すると、Cisco Talos 提供の基本ポリシーを編集することなく、IPS/IDS システムの動作をより詳細に制御できます。 侵入ポリシーを一覧表示するように **[Policies] > [Intrusion]** ページが変更されました。新しいポリシーを作成したり、既存のポリシーを表示または編集（グループの追加/削除、セキュリティレベルの割り当て、ルールのアクションの変更など）することができます。複数のルールを選択し、それらのアクションを変更することもできます。さらに、アクセス制御ルールでカスタム侵入ポリシーを選択できます。
侵入イベント用の複数の syslog サーバー	侵入ポリシー用に複数の syslog サーバーを設定できます。侵入イベントは各 syslog サーバーに送信されます。 侵入ポリシー設定ダイアログボックスに、複数の syslog サーバーオブジェクトを選択する機能が追加されました。

機能	説明
URL レピュテーション照合にレピュテーションが不明なサイトを含めることが可能です	URL カテゴリのトラフィック一致基準を設定し、レピュテーション範囲を選択する場合に、レピュテーションが不明な URL をレピュテーション照合に含めることができます。 アクセス制御ルールと SSL 復号ルールの URL レピュテーション基準に [レピュテーションが不明なサイトを含める（Include Sites with Unknown Reputation）] チェックボックスが追加されました。
VPN 機能	
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN	VPN 接続プロファイルのローカルインターフェイスとして仮想トンネルインターフェイスを使用して、ルートベースのサイト間 VPN を作成できるようになりました。ルートベースのサイト間 VPN を使用すると、VPN 接続プロファイルを一切変更することなく、ルーティングテーブルを変更するだけで、特定の VPN 接続で保護されたネットワークを管理できます。リモートネットワークの追跡を継続し、前述の変更に対応して VPN 接続プロファイルを更新する必要はありません。その結果、クラウド サービス プロバイダーや大企業の VPN 管理が簡素化されます。 インターフェイスのリストのページに [仮想トンネルインターフェイス（Virtual Tunnel Interfaces）] タブが追加され、VTI をローカルインターフェイスとして使用できるように、サイト間 VPN ウィザードが更新されました。
FTD リモート アクセス VPN 接続を行うための Hostscan およびダイナミック アクセス ポリシー（DAP）の API サポート	Hostscan パッケージとダイナミック アクセス ポリシー（DAP）ルール XML ファイルをアップロードし、XML ファイルを作成するよう DAP ルールを設定することで、接続中のエンドポイントのステータスに関連する属性に基づいてグループポリシーをリモートユーザーに割り当てる方法を制御することができます。Cisco Identity Services Engine（ISE）がない場合は、これらの機能を使用して認可変更を実行できます。Hostscan のアップロードと DAP の設定は FTD API を使用してのみ行えます。FDM を使用して設定することはできません。Hostscan および DAP の使用方法の詳細については、AnyConnect のマニュアルを参照してください。 dapxml、hostscanpackagefiles、hostscanxmlconfigs、ravpns の各 FTD API オブジェクトモデルを追加または変更しました。

機能	説明
外部 CA 証明書の証明書失効チェックの有効化	FTD API を使用して、特定の外部 CA 証明書の証明書失効チェックを有効にすることができます。失効チェックは、リモートアクセス VPN で使用される証明書に特に役立ちます。FDM を使用して証明書の失効チェックを設定することはできません。FTD API を使用する必要があります。 ExternalCACertificate リソースに revocationCheck、crlCacheTime、および oscpDisableNonce 属性が追加されました。
安全性の低い Diffie-Hellman グループ、および暗号化アルゴリズムとハッシュアルゴリズムのサポートがなくなりました	6.6 で廃止されていた以下の機能が削除されました。それらを IKE プロポーザルまたは IPsec ポリシーで引き続き使用している場合は、アップグレード後にそれらを置き換えないと、設定変更を展開できません。VPN が正しく機能するように、サポートされる DH および暗号化アルゴリズムにアップグレードする前に VPN 設定を変更することをお勧めします。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。
リモートアクセス VPN 用のカスタムポート	リモートアクセス VPN（RA VPN）接続に使用するポートを設定できます。RA VPN に使用されているインターフェイスで FDM に接続する必要がある場合は、RA VPN 接続のポート番号を変更できます。FDM が使用するポート 443 は、デフォルトの RA VPN ポートでもあります。 RA VPN ウィザードのグローバル設定ステップが更新され、ポート設定が追加されました。
リモートアクセス VPN を認証するための SAML サーバーのサポート	SAML 2.0 サーバーをリモートアクセス VPN の認証ソースとして設定できます。サポートされている SAML サーバーは次のとおりです：Duo。 **[Objects]** > **[Identity Sources]** ページでのアイデンティティソースとして SAML サーバーが追加され、それを使用できるようにリモートアクセス VPN 接続プロファイルが更新されました。

機能	説明
AnyConnect モジュールプロファイルの FTD API サポート	FTD API を使用して、AMP イネーブラ、ISE ポスチャ、Umbrella といった AnyConnect で使用されるモジュールプロファイルをアップロードできます。これらのプロファイルは、AnyConnect プロファイル エディタ パッケージからインストールできるオフライン プロファイル エディタを使用して作成する必要があります。 AnyConnectClientProfile モデルに anyConnectModuleType 属性が追加されました。最初はモジュールプロファイルを使用する AnyConnect クライアント プロファイル オブジェクトを作成できますが、FDM で作成されたオブジェクトを変更して正しいモジュールタイプを指定するには、依然として API を使用する必要があります。
ルーティング機能	
スマート CLI による EIGRP のサポート	以前のリリースでは、FlexConfig を使用して、[Advanced Configuration] ページで EIGRP を設定しました。今回、[Routing] ページでスマート CLI を直接使用して EIGRP を設定するようになりました。 FlexConfig を使用して EIGRP を設定した場合は、リリース 6.7 にアップグレードするときに、FlexConfig ポリシーから FlexConfig オブジェクトを削除してから、スマート CLI オブジェクトで設定を再作成する必要があります。スマート CLI の更新が完了するまでは、参照用に EIGRP FlexConfig オブジェクトを保持できます。設定は自動的に変換されません。 [Routing] ページに EIGRP スマート CLI オブジェクトが追加されました。
インターフェイス機能	
ISA 3000 ハードウェアバイパスの持続性	永続化オプションを使用して、ISA 3000 インターフェイスペアのハードウェアバイパスを有効にできるようになりました。電源が回復した後、ハードウェアバイパスは手動で無効にするまで有効のままになります。持続性のないハードウェアバイパスを有効にすると、電源が回復した後にハードウェアバイパスが自動的に無効になります。ハードウェアバイパスが無効になっていると、短時間のトラフィック中断が発生する可能性があります。永続化オプションを使用すると、トラフィックの短時間の中断が発生するタイミングを制御できます。 新規/変更された画面：**[Device]** > **[Interfaces]** > **[Hardware Bypass]** > **[Hardware Bypass Configuration]**

機能	説明
Firepower 4100/9300 における FTD 動作リンク状態と物理リンク状態の同期	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、Radware vDP デコレータを使用する FTD ではサポートされません。 新規/変更された Firepower Chassis Manager 画面：[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム： Firepower 4100/9300
Firepower 1100 および 2100 SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました	自動ネゴシエーションを無効にするように Firepower 1100 および 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更画面：[Device] > [Interfaces] > [Edit Interface] > [Advanced Options] > [Speed] サポートされるプラットフォーム：Firepower 1100 および 2100
管理およびトラブルシューティングの機能	

機能	説明
失敗した FTD ソフトウェアのアップグレードをキャンセルし、以前のリリースに戻す機能	FTD のメジャーソフトウェアアップグレードが失敗するか、正常に機能しない場合は、アップグレードインストールの実行時の状態にデバイスを戻すことができます。 FDM の [System Upgrade] パネルにアップグレードを元に戻す機能が追加されました。アップグレード時に、FDM ログイン画面にアップグレードステータスが表示され、アップグレードが失敗した場合にキャンセルしたり元に戻すためのオプションが表示されます。FTD API に CancelUpgrade、RevertUpgrade、RetryUpgrade、および UpgradeRevertInfo リソースが追加されました。 FTD CLI に **show last-upgrade status**、**show upgrade status**、**show upgrade revert-info**、**upgrade cancel**、**upgrade revert**、**upgrade cleanup-revert**、および **upgrade retry** コマンドが追加されました。
データインターフェイス上の FDM/FTD API アクセス用のカスタム HTTPS ポート	データインターフェイスで FDM または FTD API アクセスに使用する HTTPS ポートを変更できます。ポートをデフォルトの 443 から変更することにより、管理アクセスと同じデータインターフェイスで設定されているその他の機能（リモートアクセス VPN など）の競合を回避できます。管理インターフェイスの管理アクセス HTTPS ポートは変更できないことに注意してください。 **[Device]** > **[System Settings]** > **[Management Access]** > **[Data Interfaces]** ページにポートを変更する機能が追加されました。
Firepower 1000 および 2100 シリーズ デバイス上の Cisco Defense Orchestrator のロータッチプロビジョニング	Cisco Defense Orchestrator（CDO）を使用して新しい FTD デバイスを管理する予定がある場合、デバイスセットアップ ウィザードを完了することなく、または FDM にログインすることさえなく、デバイスを追加できるようになりました。 新しい Firepower 1000 および 2100 シリーズ デバイスは、最初に Cisco Cloud に登録され、CDO で簡単に要求できます。CDO に入ると、CDO からデバイスをすぐに管理できます。このロータッチプロビジョニングでは、物理デバイスと直接やりとりする必要性が最小限に抑えられ、ネットワクデバイスに関する経験が浅い従業員が勤務するリモートオフィスなどの場所にとって理想的です。 Firepower 1000 および 2100 シリーズ デバイスの初期プロビジョニング方法が変更されました。また、**[System Settings]** > **[Cloud Services]** ページに自動登録が追加されました。これにより、FDM を使用して以前に管理していたアップグレード済みデバイスおよびその他のデバイスのプロセスを手動で開始できます。

機能	説明
SNMP 設定の FTD API サポート	FTD API を使用して FDM または CDO 管理対象 FTD デバイスで SNMP バージョン 2c または 3 を設定できます。 API リソースの SNMPAuthentication、SNMPHost、SNMPSecurityConfiguration、SNMPServer、SNMPUser、SNMPUserGroup、SNMPv2cSecurityConfiguration、および SNMPv3SecurityConfiguration が追加されました。 （注） FlexConfig を使用して SNMP を設定した場合は、FTD API SNMP リソースを使用して設定をやり直す必要があります。SNMP を設定するためのコマンドは、FlexConfig では使用できなくなりました。FlexConfig ポリシーから SNMP FlexConfig オブジェクトを削除するだけで、変更を展開できます。その後、API を使用して機能を再設定するときに、それらのオブジェクトを参照として使用できます。
システムに保持されるバックアップファイルの最大数が 10 から 3 に減少	システムでは、10 個ではなく最大 3 個のバックアップファイルがシステムに保持されます。新しいバックアップが作成されると、最も古いバックアップファイルが削除されます。必要な場合にシステムを回復するために必要なバージョンを入手できるように、バックアップファイルは異なるシステムにダウンロードしてください。
FTD API バージョンの後方互換性	FTD バージョン 6.7 以降、ある機能の API リソースモデルがリリース間で変更されない場合、FTD API は古い API バージョンに基づくコールを受け入れることができます。機能モデルが変更された場合でも、古いモデルを新しいモデルに変換する論理的な方法があれば、古いコールが機能します。たとえば、v4 コールを v5 システムで受け入れることができます。コールのバージョン番号として「latest（最新）」を使用する場合、「古い」コールは、このシナリオでは v5 コールとして解釈されるため、下位互換性を利用するかどうかは、API コールの構築方法によって決まります。

機能	説明
FTD REST API バージョン 6（v6）	ソフトウェアバージョン 6.7 用の FTD REST API はバージョン 6 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。 使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

バージョン 6.7 の新しいハードウェアと仮想プラットフォーム

表 *3 :* バージョン *6.7.0* の新しいハードウェアと仮想プラットフォーム

機能	説明
新しい仮想環境。	次の環境に FMCv および FTDv が導入されました。 • Oracle Cloud Infrastrucure（OCI） • Google Cloud Platform（GCP）

新し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/LSP）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/LSP 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。

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- FMC：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- FDM：**show summary** CLI コマンドを使用します。

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。

廃止された機能

FMC バージョン 6.7 で廃止された機能

表 *4 : FMC* バージョン *6.7.0* で廃止された機能

機能	アップグレードの影響	説明
Cisco Firepower User Agent software ソフトウェアとアイデンティティソース。	FMC がアップグレードされないようにします。	ユーザーエージェント設定を使用して FMC をバージョン 6.7 以降 にアップグレードすることはできません。 バージョン 6.6 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。Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替える必要があります。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、Cisco Firepower User Agent のサポート終了 [英語] 通知、およびFirepower ユーザー ID：ユーザーエージェントから Identity Services Engine への移行 [英語] の技術メモを参照してください。 廃止された FTD CLI コマンド： **configure user agent**
Cisco ISE エンドポイント保護サービス（EPS）の修復。	ISE 修復が機能しなくなることがあります。	Cisco ISE エンドポイント保護サービス（EPS）の修復は、pxGrid 2.0 では機能しません。代わりに、新しい Cisco ISE Adaptive Network Control（ANC）修復を設定して使用します。 「不正な」pxGrid を使用して FMC を ISE/ISE-PIC アイデンティティソースに接続している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	FMC がアップグレードされないようにします。	次の FTD 機能のいずれかを使用している場合、FMC をアップグレードできないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の FMC 展開で引き続きサポートされますが、より強力なオプションに変更することをお勧めします。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • NULL の「暗号化アルゴリズム」（暗号化なしの認証、テスト目的）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルの FMC 展開で引き続きサポートされます。ただし、IKEv2 ポリシーではサポートされなくなりました。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。

機能	アップグレードの影響	説明
アプライアンス設定のリソース使用率の正常性モジュール（一時的に廃止）。	ヘルスモニターでのアップグレード後のエラーの可能性	バージョン 6.7 では、バージョン 6.6.3 で導入され、後続のすべての 6.6.x リリースでサポートされるアプライアンス設定のリソース使用率の正常性モジュールに関するサポートが部分的かつ一時的に廃止されています。 バージョン 6.7 のサポートは次のとおりです。 • バージョン 6.6.3 以降からバージョン 6.7 への FMC のアップグレード デバイスがバージョン 6.6.x のままである場合にのみ、モジュールのサポートが継続されます。デバイスをバージョン 6.7 にアップグレードすると、モジュールは動作を停止し、正常性モニターにエラーが表示されます。エラーを解決するには、FMC を使用してモジュールを無効にし、ポリシーを再適用します。 • バージョン 6.3 ー 6.6.1 からバージョン 6.7.0 への FMC のアップグレード、または FMC バージョン 6.7 の新規インストール。 このモジュールはサポートされていません。 モジュールがサポートされていない FMC にモジュールが有効になっているバージョン 6.6.x デバイスを追加するまれなケースでは、解決できないエラーがヘルスモニターに表示されます。このエラーは無視しても問題ありません。 バージョン 7.0 ではフルサポートが提供され、モジュールの名前が 構成メモリ割り当てに変更されています。
その他の正常性モジュール（永久的に廃止）。	なし。	バージョン 6.7 では、次のヘルスモジュールが廃止されています。 • CPU 使用率：4 つの新しいモジュールに置き換えられました。FMC バージョン 6.7 の新機能 （1 ページ）を参照してください。 • ローカルマルウェア分析：このモジュールは、バージョン 6.3 のデバイス上の脅威データの更新モジュールに置き換えられました。バージョン 6.7 以降の FMC は、古いモジュールが適用されるデバイスを管理できなくなります。 • ユーザー エージェント ステータス モニター：Cisco Firepower ユーザーエージェントはサポートされなくなりました。

機能	アップグレードの影響	説明
クラシックテーマを使用したウォークスルー。	なし。	バージョン 6.7 では、クラシックテーマの FMC ウォークスルー（使用方法）が廃止されました。ユーザー設定でテーマを切り替えることができます。
Bugtraq	脆弱性データをエクスポートする場合は、アップグレード後に統合が期待どおりに機能していることを確認します。	バージョン 6.7 では Bugtraq のデータベースフィールドとオプションが削除されます。Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データは National Vulnerability Database（NVD）から取得されています。 詳細については、FMC バージョン 6.7 の新機能 （1 ページ）を参照してください。
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。

FDM バージョン 6.7 で廃止された機能

表 *5 : FDM* バージョン *6.7.0* で廃止された機能

機能	アップグレードの影響	説明
安全性の低い Diffie-Hellman グループ、暗号化アルゴリズム、およびハッシュアルゴリズム。	アップグレード後に展開ができないようにします。	次の FTD 機能のいずれかを使用している場合、アップグレード後の展開ができないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。

機能	アップグレードの影響	説明
FlexConfig コマンド。	アップグレード後に展開ができないようにします。 アップグレード後に設定をやり直す必要があります。	バージョン 6.7 では、FDM を使用する FTD の次の FlexConfig CLI コマンドは廃止されます。 • **router eigrp**：[ルーティング（Routing）] ページの **[デバイス（Device）] > [ルーティング（Routing）] > [EIGRP]** で直接スマート CLI EIGRP オブジェクトを作成して、使用できます。 • **snmp-server**：FTD API を使用して SNMP バージョン 2c または 3 を設定できるようになりました。 関連付けられている FlexConfig オブジェクトを削除するまで、アップグレード後に展開することはできません。
バックアップファイルの保持。	なし。アップグレードによって、ローカルのバックアップは常に消去されます。	バージョン 6.7 では、保存されるバックアップファイルの数が 10 から 3 に減ります。 安全なリモートロケーションにバックアップし、正常に転送が行われることを確認することをお勧めします。アップグレードによって、ローカルに保存されたバックアップは消去されます。
Microsoft Internet Explorer	ブラウザを切り替える必要があります。	Microsoft Internet Explorer を使用して Firepower Web インターフェイスをテストすることはなくなりました。Google Chrome、Mozilla Firefox、または Microsoft Edge に切り替えることをお勧めします。

バージョン 6.7 で廃止されたハードウェアと仮想プラットフォーム

表 *6 :* バージョン *6.7.0* で廃止されたハードウェアと仮想プラットフォーム

機能	説明
Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス。	ASA 5525-X、5545-X、および 5555-X でバージョン 6.7 以降は実行できません。

廃止された FlexConfig コマンド

このドキュメントでは、今回のリリースで廃止された 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と以前のリリースで廃止になった機能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 FTD の機能は、ASA 設定コマンドを使用して設定されます。Smart 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。

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。