Cisco Firepower Management Center の新機能（リリース別）

初版：2021 年 3 月 26 日

最終更新：2021 年 12 月 15 日

各リリースの新機能

このドキュメントでは、各リリースの新機能と廃止された機能を示します。

推奨リリース

推奨リリース：バージョン 6.6.5.1

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを推奨リリース以上にアップグレードすることをお勧めします。シスコ サポートおよびダウンロード サイトでは、推奨リリースに金色の星が付いています。

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

バージョン 7.1.0

FMC バージョン 7.1.0 の新機能

機能	説明
ハードウェアおよび仮想アプライアンス	
AWS 用 FMCv300 OCI 用 FMCv300	AWS と OCI の両方に対応する FMCv300 が導入されました。FMCv300 は、最大 300 台のデバイスを管理できます。

機能	説明
AWS 用 FTDv のインスタンス。	AWS 用 FTDv により、次のインスタンスのサポートが追加されています。 • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、m c5d.4xlarge • i3en.xlarge、i3en.2xlarge、i3en.3xlarge • inf1.xlarge、inf1.2xlarge • m5.xlarge、m5.2xlarge、m5.4xlarge • m5a.xlarge、m5a.2xlarge、m5a.4xlarge • m5ad.xlarge、m5ad.2xlarge、m5ad.4xlarge • m5d.xlarge、m5d.2xlarge、m5d.4xlarge • m5dn.xlarge、m5dn.2xlarge、m5dn.4xlarge • m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.xlarge、m5zn.2xlarge、m5zn.3xlarge • r5.xlarge、r5.2xlarge、r5.4xlarge • r5a.xlarge、r5a.2xlarge、r5a.4xlarge • r5ad.xlarge、r5ad.2xlarge、r5ad.4xlarge • r5b.xlarge、r5b.2xlarge、r5b.4xlarge • r5d.xlarge、r5d.2xlarge、r5d.4xlarge • r5dn.xlarge、r5dn.2xlarge、r5dn.4xlarge • r5n.xlarge、r5n.2xlarge、r5n.4xlarge • z1d.xlarge、z1d.2xlarge、z1d.3xlarge
Azure 用 FTDv のインスタンス。	Azure 用 FTDv により、次のインスタンスのサポートが追加されています。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

機能	説明
Device Setup	
FDMを使用して、FMCによる管理用にFTDを設定します。	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。FTD CLI を使用すると、管理と FMC のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス設定は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：**[システム設定（System Settings）]** > **[管理センター（Management Center）]**
デバイスのアップグレード	
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**[システム（System）]** > **[更新（Updates）]**ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。

機能	説明
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
Snort 3 後方互換性。	Snort 3 の場合、新しい機能と解決済みのバグでは、FMC とその管理対象デバイスを完全にアップグレードしている必要があります。Snort 2 とは異なり、新しい FMC（たとえば、バージョン 7.1.0）から展開して、古いデバイス（たとえば、バージョン 7.0.0）の検査エンジンを更新することはできません。 古いデバイスに展開すると、サポートされない設定が一覧表示され、それらの設定がスキップされることが警告されます。環境全体を常に更新することをお勧めします。
Device Management	

機能	説明
AWS インスタンスでの FTDv に対する Geneve インターフェイスサポート。	AWS ゲートウェイロードバランサ（GWLB）のシングルアームプロキシをサポートするために、Geneve カプセル化サポートが追加されました。AWS GWLB は、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて FTDv を拡張するロードバランサを組み合わせます。 このサポートには、Snort 3 が有効になっている FMC が必要であり、次のパフォーマンス階層で利用できます。 • FTDv20 • FTDv30 • FTDv50 • FTDv100
OCI 上の FTDv に対する Single Root I/O Virtualization（SR-IOV）のサポート	OCI 上の FTDv に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、FTDv のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。
Firepower 1100 の LLDP サポート。	Firepower 1100 インターフェイスの Link Layer Discovery Protocol（LLDP）を有効に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）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** > **[ハードウェア構成（Hardware Configuration）]** > **[LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 1100（1120、1140、および 1150）
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、FMC でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** > **[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 1000/2100

機能	説明
信頼された DNS サーバの指定のサポート。	FTD プラットフォーム設定を使用して、DNS スヌーピングに信頼できる DNS サーバーを指定できます。これは、ドメインを IP アドレスにマッピングすることにより、最初のパケットでアプリケーションを検出するのに役立ちます。デフォルトでは、信頼できる DNS サーバーには、DNS サーバーオブジェクト内の DNS サーバーと、dhcp-pool、dhcp-relay、および dhcp-client によって検出された DNS サーバーが含まれます。
デバイス設定のインポート/エクスポート。	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]**
高可用性/拡張性	
高可用性 • AWS 用 FMCv • OCI 用 FMCv	AWS 用 FMCv および OCI 用 FMCv で高可用性がサポートされるようになりました。 FTD の展開では、2 つの同一ライセンスの FMC 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 高可用性ペアで 10 台の FTD デバイスを管理するには、2 個の FMCv10 権限と 10 個の FTD 権限が必要です。バージョン 6.5.0 ～ 7.0.x のクラシックデバイス（NGIPSv または 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。 サポートされるプラットフォーム：FMCv10、FMCv25、FMCv300（FMCv2 ではサポートされません）
OCI 用 FTDv の自動スケール。	OCI 用 FTDv で自動スケーリングがサポートされるようになりました。 クラウドベースの展開におけるサーバレス インフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。
ファイアウォールの変更に対するクラスタの展開がより迅速に完了します。	ファイアウォールの変更に対する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。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
ハイアベイラビリティ グループまたはクラスタ内のルートのクリア。	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティグループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。
NAT	
変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
ルーティング	
仮想ルータを相互接続するための BGP 設定。	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv4/v6] > [ルートのインポート/エクスポート（Route Import/Export）]**
ユーザー定義の仮想ルータでの BGPv6 サポート。	FTD は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv6]**
Equal-Cost-Multi-Path（ECMP）ゾーンのサポート。	トラフィックゾーンのインターフェイスをグループ化し、FMC で Equal-Cost-Multi-Path（ECMP）ルーティングを設定できるようになりました。 ECMP ルーティングは、以前は FlexConfig ポリシーを通じてサポートされていました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ECMP]**
ダイレクト インターネット アクセス/ポリシーベースルーティング	

機能	説明
ポリシーベースルーティングによるダイレクト インターネット アクセス。	FMC を介してポリシーベースルーティングを設定して、アプリケーションに基づいてネットワークトラフィックを分類し、ダイレクト インターネット アクセス（DIA）を実装して、ブランチ展開からインターネットにトラフィックを送信できるようになりました。PBR ポリシーを定義し、入力インターフェイスに設定して、一致基準と出力インターフェイスを指定できます。アクセス コントロール ポリシーに一致するネットワークトラフィックは、ポリシーで設定されている優先順位または順序に基づいて、出力インターフェイスを介して転送されます。 新規/変更された画面：ポリシー ベース ルーティング ポリシーを設定するための新しいポリシーページ：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** サポートされるプラットフォーム：FTD
ダイレクト インターネット アクセスとポリシーベースルーティングのための FMC REST API の機能拡張。	FMC REST API を使用して、ポリシーベースルーティングによるダイレクト インターネット アクセスを設定できます。これをサポートするために、FMC REST API に次の機能拡張が加えられました。 • ポリシーベースルーティング設定を作成、表示、編集、および削除できるようにする新しい API が追加されました。 • アプリケーションを定義する拡張アクセス制御リストの既存の API に新しいパラメータが追加されました。 • インターフェイスの優先順位を定義するデバイスインターフェイスの既存の API に新しいパラメータが追加されました。
Remote Access VPN	
RA VPN ポリシーのコピー。	既存のポリシーをコピーして、新しい RA VPN ポリシーを作成できるようになりました。**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**の各ポリシーの横にコピーボタンが追加されました。

機能	説明
AnyConnect VPN SAML 外部ブラウザ。	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。
Microsoft Azure 上の SAML ID プロバイダにおける複数のトラストポイント。	Microsoft Azure の要求に応じて、SAML ID プロバイダに複数の RA VPN トラストポイントを追加できるようになりました。 Microsoft Azure ネットワークでは、Azure は同じエンティティ ID に対して複数のアプリケーションをサポートできます。（通常は別のトンネルグループにマップされる）各アプリケーションには、一意の証明書が必要です。この機能により、Microsoft Azure 向け FTDv で RA VPN に複数のトラストポイントを追加できます。
Site to Site VPN	
VPN フィルタ。	トンネリングされたデータパケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって許可するか拒否するかを決定するルールを使用して、サイト間 VPN フィルタを設定できるようになりました。 VPN フィルタは、トンネルから出た後の復号化後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。
IKEv2 の一意のローカルトンネル ID。	ポリシーベースとルートベースのサイト間 VPN の両方に IKEv2 トンネルごとのローカルトンネル ID を設定できるようになりました。FMC Web インターフェイスまたは REST API からローカルトンネル ID を設定できます。 このローカルトンネル ID 設定により、FTD との Umbrella SIG 統合が可能になります。
複数の IKE ポリシー。	ポリシーベースとルートベースのサイト間 VPN の両方に複数の IKE ポリシーを設定できるようになりました。 FMC GUI および REST API を使用して複数の IKE ポリシーを設定できます。

機能	説明
VPN 監視ダッシュボード。	**ベータ版。** サイト間 VPN 監視ダッシュボードは次の機能を提供します。 • 全デバイスのトンネルステータス分布の可視化 • VPN トンネルで構成されるネットワークトポロジの可視化 • トポロジ、デバイス、ステータスなどの基準に基づいてトンネルを視覚的に切り離して調べる機能 （注） サイト間監視ダッシュボードはベータ機能であり、期待どおりに動作しない場合があります。実稼働環境では使用しないでください。
セキュリティ インテリジェンス	
プロキシされたトラフィックでのセキュリティ インテリジェンスのための Snort 3 サポート。	Snort 3 では、IP アドレスが HTTP リクエストに埋め込まれている HTTP プロキシトラフィックにセキュリティ インテリジェンスを適用できるようになりました。たとえば、ユーザーが IP アドレスまたはネットワークを含むブロックリストまたは許可リストをアップロードすると、システムはプロキシ IP ではなく宛先サーバーの IP を照合します。その結果、宛先サーバーへのトラフィックを（セキュリティ インテリジェンスの設定に応じて）ブロック、監視、または許可することができます。
侵入検知と防御	

機能	説明
ルールアクションのドロップ、拒否、書き換え、およびパスに対する Snort 3 のサポート。	バージョン 7.1.0 FMC は、バージョン 7.0.0/7.0.x デバイスを含む、Snort 3 を使用した FTD デバイスで次の侵入ルールアクションをサポートするようになりました。 • ドロップ：一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。侵入イベントを生成します。 • 拒否：一致するパケットをドロップし、この接続の以降のトラフィックもブロックします。TCP トラフィックの場合、TCP リセットを送信します。UDP トラフィックの場合、送信元および宛先ホストに ICMP ポート到達不能を送信します。侵入イベントを生成します。 • 書き換え：ルールの置換オプションに基づいて一致するパケットを上書きします。侵入イベントを生成します。 • パス：一致するパケットが他の侵入ルールによる評価なしで通過することを許可します。侵入イベントを生成しません。 これらの新しいルールアクションを設定するには、侵入ポリシーの Snort 3 バージョンを編集し、各ルールの [ルールアクション（Rule Action）] ドロップダウンを使用します。
TLS ベースの侵入ルールに対する Snort 3 のサポート。	Snort 3 で復号化された TLS トラフィックを検査する TLS ベースの侵入ルールを作成できるようになりました。この機能により、Snort 3 侵入ルールで TLS 情報を使用できます。
SMB2 上の DCE/RPC のインスペクションに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1.0 は、SMB2 での DCE/RPC インスペクションをサポートします。 Snort 3 デバイスへの最初のアップグレード後の展開の後、既存の DCE/RPC ルールは、SMB2 での DCE/RPC の検査を開始します。以前は、これらのルールは SMB1 での DCE/RPC のみを検査していました。
侵入ルールの推奨に対する Snort 3 のサポート。	バージョン 7.1.0 FMC は、バージョン 7.0.0/7.0.x デバイスを含む、Snort 3 を使用した FTD デバイスで侵入ルールの推奨をサポートするようになりました。 この機能を設定するには、侵入ポリシーの Snort 3 バージョンを編集し、左側のペインの [すべてのルール（All Rules）] の横にある [推奨（Recommendations）] ボタンをクリックします。

機能	説明
ssl_version および **ssl_state** キーワードに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1.0 では、**ssl_version** および **ssl_state** 侵入ルールキーワードがサポートされています。 シスコが提供する侵入ポリシーには、これらのキーワードを使用するアクティブルールが含まれます。これらを使用して、カスタム/サードパーティルールを作成、アップロード、および展開することもできます。バージョン 7.0.x では、これらのキーワードは Snort 2 でのみサポートされていました。Snort 3 では、これらのキーワードを含むルールはトラフィックに一致しないため、アラートを生成したり、トラフィックに影響を与えたりすることはできませんでした。ルールが予期したとおりに機能していないという通知はありませんでした。バージョン 7.1.0 以降の Snort 3 デバイスへの最初のアップグレード後の展開の後、これらのキーワードを含む既存のルールはトラフィックと一致します。
Identity Services およびユーザー制御	
HTTP/2 トラフィックのインターセプトに対する Snort 3 キャプティブポータルのサポート。	キャプティブポータルを使用したユーザー認証のために、HTTP/2 トラフィックをインターセプトしてリダイレクトできるようになりました。 ブラウザがリダイレクトを受信すると、ブラウザはリダイレクトに従い、HTTP/1 キャプティブポータルと同じプロセスを使用して idhttpsd（Apache Web サーバー）で認証します。認証後、idhttpsd によりユーザーは元の URL にリダイレクトされます。
ホスト名ベースのリダイレクトに対する Snort 3 キャプティブポータルのサポート。	ID ポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスの IP アドレスではなく、完全修飾ドメイン名（FQDN）にユーザーの認証をリダイレクトできます。 FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。 新規/変更された画面：ID ポリシー設定に [ホスト名にリダイレクト（Redirect to Host Name）] オプションが追加されました。
暗号化トラフィックの処理（TLS/SSL）	

機能	説明
TLS 証明書フィード。	ライブ TLS 証明書フィードに基づいて TLS/SSL ルールを作成できるようになりました。ライブ TLS 証明書フィードを使用すると、TLS 証明書フィンガープリントの管理オーバーヘッドが削減され、より最新の情報に基づいたルールが可能になります。
拡張 TLS/SSL ポリシーオプション。	[SSLポリシー（SSL Policy）] ページの [詳細設定（Advanced Settings）] タブで、次の拡張 TLS/SSL ポリシーオプションを設定できるようになりました。 • ESNI（暗号化されたサーバー名識別）を要求するフローをブロックする • HTTP/3 アドバタイズメントを無効にする • 信頼できないサーバー証明書をクライアントに伝播する
暗号化されたセッションを可視化するための暗号化された可視性エンジン。	**ベータ版。** 暗号化された可視性エンジンを有効にすると、復号を必要とせずに暗号化されたセッションを可視化することができます。このエンジンによってトラフィックのフィンガープリントが収集され、分析されます。FMC 7.1 では、暗号化された可視性エンジンにより、TLS や QUIC などのプロトコルを含む暗号化されたトラフィックの可視性が向上します。そのトラフィックに対してアクションは適用されません。 暗号化された可視性エンジンは、デフォルトで無効になっています。これは、[実験段階の機能（Experimental Features）] セクションのアクセス コントロール ポリシーの [詳細（Advanced）] タブで有効にすることができます。 新規/変更された画面：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [*Access Control Policy name*] > [詳細（Advanced）]** **（注）** 暗号化された可視性エンジンは、可視性のために提供される実験段階のベータ機能です。誤検出を起こす可能性があります。
サービス ポリシー	
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更された画面：[サービスポリシーの追加/編集（Add/Edit Service Policy）] ウィザードの [接続設定（Connection Settings）]。

機能	説明
ネットワークディスカバリ（Network Discovery）	
ネットワーク検出の Snort 3 サポートの改善（リモートネットワーク アクセスのサポート）。	ネットワーク検出とリモートネットワーク アクセスのサポートの改善により、Snort 3 はこれらの機能について Snort 2 と同等になりました。強化された機能は次のとおりです。 • SMB トラフィックのホストとアプリケーションの検出：ネットワーク上の SMB トラフィックの場合、ホストはネットワークマップで検出され、SMB アプリケーションプロトコルと関連するオペレーティングシステム情報が検出されます。 • NetBIOS トラフィックの検出：NetBIOS トラフィックの場合、NetBIOS 名と、クライアントアプリケーションやオペレーティングシステムなどのアプリケーション関連情報が検出されます。 • ネットワーク検出ポリシーによって監視されるホスト/ネットワークのみのアプリケーションの検出：このフィルタリングロジックの機能拡張により、ネットワーク検出ルールに基づいて監視されているネットワークのアプリケーションを検出できます。 Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。
イベントロギングおよび分析	

機能	説明
エレファントフローの識別とモニタリングに対する Snort 3 のサポート。	Snort 3 を実行する FTD では、エレファントフロー（システム全体のパフォーマンスに影響を与えるのに十分な大きさのシングルセッション ネットワーク接続）を識別できるようになりました。デフォルトでは、エレファントフローの検出は自動的に有効になり、1GB/10 秒を超える接続を追跡および記録します。 接続イベントの新しい定義済み検索（Reason = Elephant Flow）を使用すると、エレファントフローをすばやく特定できます。ヘルスモニタを使用して、デバイス上のアクティブなエレファントフローを表示し、エレファントフローの発生率を CPU 使用率などの他のデバイスメトリックと関連付けるカスタム ヘルス ダッシュボードを作成することもできます。 この機能を無効にするか、サイズと時間のしきい値を設定するには、FTD CLI を使用します。 新規/変更された FTD CLI コマンド： • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
FMC からセキュアネットワーク分析クラウドに侵入イベントとレトロスペクティブ マルウェア イベントを送信します。	**アップグレードの影響。** Cisco Security Analytics and Logging（SaaS）を使用してセキュリティイベントを Stealthwatch クラウドに送信するようにシステムを設定すると、FMC は次を送信します。 • 侵入イベント。これにより、リモートで保存された侵入イベントに影響フラグデータを含めることができます。以前は、これらのイベントは FTD によってクラウドに送信され、影響フラグは含まれていませんでした。 • レトロスペクティブ マルウェア イベント。これらは、デバイスによって引き続きクラウドに送信される「元の性質」ファイルとマルウェアイベントを補完します。 この機能が有効になっている場合、FMC はアップグレードの成功後にこの情報の送信を開始します。

機能	説明
侵入イベントの新しいデータストアによるパフォーマンスの向上。	パフォーマンスを向上させるために、バージョン7.1.0では、侵入イベントに新しいデータストアを使用します。アップグレードが完了し、FMCが再起動すると、履歴イベントが、最新のイベントが先頭になるようにバックグラウンドで移行されます。 この移行の一部として、侵入インシデント、侵入イベントクリップボード、および侵入イベントのカスタムテーブルは廃止されました。詳細については、FMC バージョン 7.1.0 で廃止された機能（22 ページ）を参照してください。 また、侵入イベントテーブルに、[送信元ホストの重要度（Source Host Criticality）] と [宛先ホストの重要度（Destination Host Criticality）] という 2 つの新しいフィールドが導入されました。
接続およびセキュリティインテリジェンス イベントのNAT IPアドレスおよびポート情報。	NAT 変換の可視性を高めるために、次のフィールドが接続およびセキュリティ インテリジェンス イベントに追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port） イベントのテーブルビューでは、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [x] をクリックしてフィールド選択ツールを表示します。

機能	説明
パケットトレーサの機能拡張。	バージョン 7.1.0 では、より使いやすくするためにパケットトレーサ インターフェイスが更新されています。さらに、次のことができるようになりました。 • メインメニューから直接パケットトレーサにアクセス：**[デバイス（Devices）] > [トラブルシュート（Troubleshoot）] > [パケットトレーサ（Packet Tracer）]** • パケットトレースの保存。 • 複数デバイスでの並列パケットトレースの実行。 • デバイスを介した PCAP の再生。 • Snort 3 デバイスの場合、L2 から L7 までのトラフィック評価のフェーズ（アプリケーション識別、ファイル/マルウェア検出、侵入検出、セキュリティ インテリジェンスなど）、および各フェーズにかかる時間に関して新しい詳細を提供する拡張出力の表示。 新規/変更された FTD CLI コマンド： • **packet-tracer input***source_interface* **pcap***pcap_filename*
オブジェクト管理（Object Management）	
HTTP、ICMP、および SSH プラットフォーム設定のネットワークオブジェクトのサポート。	Threat Defense プラットフォーム設定ポリシーで IP アドレスを設定するときに、ホストまたはネットワークのネットワークオブジェクトを含むネットワーク オブジェクト グループを使用できるようになりました。
ネットワーク ワイルドカードマスク オブジェクトの Snort 3 サポート。	[オブジェクト管理（Object Management）] ページで、ネットワーク ワイルドカード マスク オブジェクトを作成および管理できるようになりました。アクセス制御、プレフィルタ、および NAT ポリシーでネットワーク ワイルドカード マスク オブジェクトを使用できます。
オブジェクトの展開プレビューの機能拡張。	地理位置情報、ファイルリスト、およびセキュリティ インテリジェンス オブジェクトへの展開の変更をプレビューできるようになりました。 更新された画面：**[展開（Deploy）] > [展開（Deployment）]**。 [プレビュー（Preview）] 列で、デバイスの [プレビュー（Preview）] アイコンをクリックすると、ファイルリストオブジェクトへの変更が表示されます。
統合	

機能	説明
Cisco ACI Endpoint Update App バージョン 2.0 および修復モジュールのサポート。	Cisco ACI Endpoint Update App のバージョン 2.0 では、以前のバージョンに比べて次の点が改善されています。 • 最小更新間隔（アプリケーションが FMC を更新する頻度）が 10 秒になりました。以前は 30 秒でした。 • サイトプレフィックス（各 APIC テナントに関連付けられた FMC にネットワーク グループ オブジェクトを作成する文字列）が 10 文字に制限されました。以前は 5 文字でした。 この更新では、新しい Cisco ACI Endpoint 修復モジュールも利用できます。
ユーザビリティ、パフォーマンス、およびトラブルシューティング	
ヘルスモニタリングの強化。	ヘルスモニタは次のように更新されました。 • ヘルスポリシーエディタは、類似するヘルスモジュールをグループ化するようになりました。モジュールグループ全体を有効または無効にできます。 • ヘルスポリシー除外エディタが更新され、使いやすくなりました。また、アラートからデバイスまたはヘルスモジュールを除外するときに、除外の期間を 15 分から永久まで指定できるようになりました。 • ヘルス モニタ アラート エディタが更新され、使いやすくなりました。 • ヘルスポリシーの展開インターフェイスが更新され、使いやすくなりました。 （注） 更新されたヘルスモニタを使用するには、**[システム（System）] > [設定（Configuration）] > [REST API設定（REST API Preferences）]**で REST API アクセスを有効にする必要があります。 新規/変更された画面： • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの編集（Edit Policy）]** • **[システム（System）] > [ヘルス（Health）] > [除外（Exclude）]** • **[システム（System）] > [ヘルス（Health）] > [モニタアラート（Monitor Alerts）]** • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの展開（Deploy Policy）]**

機能	説明
展開履歴の機能拡張。	展開ジョブをブックマークし、ジョブの展開に関する注意を編集して、レポートを生成できるようになりました。
グローバル検索の機能拡張。	グローバル検索に次の機能が追加されました。 • FMC ウォークスルーの全文を検索できます（how-tos）。 • 拡張コミュニティリスト名または設定値を検索できます。 • ドメインごとに検索を制限できます。
新しいウォークスルー。	次のウォークスルーが追加されました。 • Snort 3 侵入ポリシーの作成。 • 個々のデバイス上での Snort 3 の有効化と無効化。 • Snort 3 ネットワーク分析ポリシーの作成。 • ネットワーク分析ポリシーのマッピングの表示。 • FTD のアップグレード。 • クラスタの作成および管理。 • FMC アクセスインターフェイスの管理からデータへの変更。 • FMC アクセスインターフェイスのデータから管理への変更。
Cisco Success Network に送信された Snort メモリ使用量テレメトリ。	有用性を向上させるために、Snort メモリおよびスワップ使用率（メモリ不足イベントを含む）に関するテレメトリを Cisco Success Network に送信するようになりました。 この情報は、Snort 2 と Snort 3 の両方に送信されます。Cisco Success Network の登録はいつでも変更できます。
Snort 3 は、フロー開始イベントとフロー終了イベントの統計情報をサポートします。	Snort 3 を使用する FTD の場合、**show snort statistics** コマンドの出力で、フロー開始イベントとフロー終了イベントに関する統計情報が報告されるようになりました。
FMC REST API	

機能	説明
FMC REST API サービス/操作。	

機能	説明

	新機能と既存の機能をサポートするために、複数の FMC REST API サービス/操作が追加されました。詳細については、Firepower Management Center REST API バージョン 7.1 クイックスタートガイド [英語] を参照してください。
	新しい FMC REST API には次のものが含まれます。
	• シャーシ管理：管理対象シャーシ、シャーシインターフェイス、ネットワークモジュール、およびブレークアウト インターフェイス用のシャーシ管理 API が追加されました。
	• 展開：ジョブ履歴の API が追加されました。
	• デバイスクラスタ：準備状況チェックを実行し、クラスタリングを変更するための API が追加されました。
	• デバイス：次の API が追加されました。
	  • FTD インターフェイスの取得
	  • Packet Tracer
	  • ルーティング
	  • 仮想 LAN
	• 正常性：トンネル API が追加されました。
	• オブジェクト：次の API が追加されました。
	  • 自律サービスパス
	  • 拡張コミュニティ リスト
	  • 拡張コミュニティ リスト
	  • 拡張アクセス リスト
	  • IPv4 プレフィックスリスト
	  • IPv6 プレフィックスリスト
	  • ポリシー リスト
	  • ルート マップ
	  • 標準アクセス リスト
	  • 標準コミュニティ リスト
	• ポリシー：自動および手動の NAT ルールを変更するための API が追加されました。

機能	説明
	• ユーザー：Duo 設定を取得および変更するための API が追加されました。 • トラブルシューティング：パケットトレーサ PCAP 機能が追加されました。 • 更新：アップグレードを元に戻すための API が追加されました。 • ネットワークマップ：ホストと脆弱性のための API が追加されました。

FMC バージョン 7.1.0 で廃止された機能

表 *1: FMC* バージョン *7.1.0* で廃止された機能

機能	アップグレードの影響	説明
侵入インシデントと侵入イベントクリップボード。	インシデントに関連するすべてのデータが削除されます。 クリップボードをデータソースとして使用するレポート テンプレート セクションは削除されます。	バージョン 7.1.0 では、侵入インシデント機能と関連する侵入イベントクリップボードが削除されています。 廃止された画面/オプション： • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • 侵入イベントワークフローページおよびパケットビューでの [コピー（Copy）] および [すべてコピー（Copy All）] • レポートテンプレートにセクションを追加する場合（[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]）、データソースとして [クリップボード（Clipboard）] テーブルを選択できなくなりました。

機能	アップグレードの影響	説明
侵入イベントのカスタムテーブル	侵入イベントテーブルのフィールドを含むカスタムテーブルは削除されます。	バージョン 7.1.0 では、侵入イベントのカスタムテーブルのサポートが終了します。 カスタムテーブルにフィールドを追加する場合（[分析（Analysis）]>[詳細設定（Advanced）]>[カスタムテーブル（Custom Tables）]）、データソースとして [侵入イベント（Intrusion Events）] テーブルを選択できなくなりました。
NGIPS ソフトウェア（ASA FirePOWER/NGIPSv）	アップグレードは禁止されています。	バージョン 7.1.0 は、FMC および FTD デバイスでのみサポートされます。ASA FirePOWER または NGIPSv デバイスではサポートされていません。 バージョン 7.1.0 FMC を引き続き使用して、バージョン 6.5.0 ～ 7.0.x を実行している古いデバイス（FTD、ASA FirePOWER および NGIPSv）を管理できます。
ASA 5508-X および 5516-X	アップグレードは禁止されています。	ASA 5508-X または 5516-X ではバージョン 7.1.0+ を実行できません。
FMC 1000、2500、4500	アップグレードは禁止されています。	FMC モデルの FMC 1000、2500、および 4500 ではバージョン 7.1.0+ を実行できません。これらの FMC を使用してバージョン 7.1.0 以降のデバイスを管理することはできません。

バージョン 7.0.1

FMC バージョン 7.0.1 の新機能

表 *2 : FMC* バージョン *7.0.1* の新機能

機能	説明
Snort 3 rate_filter インスペクタ	バージョン 7.0.1 では、Snort 3 rate_filter インスペクタが導入されています。 これにより、ルールに対する過剰な一致に対応して侵入ルールのアクションを変更できます。レートベースの攻撃を特定の期間ブロックし、イベントの生成中でも一致するトラフィックを許可するように戻すことができます。詳細については、『Snort 3 Inspector Reference』を参照してください。 （注） この機能を使用するには、FMC とデバイスの両方にバージョン 7.0.1 以降が必要です。また、lsp-rel-20210816-1910 以降を実行している必要があります。**[システム（System）] > [アップデート（Updates）] > [ルールアップデート（Rule Updates）]** で LSP を確認および更新できます。 新規/変更されたページ：カスタムネットワーク分析ポリシーの Snort 3 バージョンを編集して、インスペクタを設定します。 サポートされるプラットフォーム：FTD
ASA FirePOWER サービスを使用する ISA 3000 の新しいデフォルトパスワード	新しいデバイスの場合、admin アカウントのデフォルトパスワードは Adm!n123 になりました。以前は、デフォルトの admin パスワードは Admin123 でした。 バージョン 7.0.1 以降にアップグレードまたは再イメージ化しても、パスワードは変更されません。ただし、すべてのユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。 サポートされるプラットフォーム：ASA FirePOWER サービスを使用する ISA 3000

バージョン 7.0.0

FMC バージョン 7.0.0 の新機能

表 *3 : FMC* バージョン *7.0.0* の新機能

機能	説明
ハードウェアおよび仮想アプライアンス	
VMware vSphere/VMware ESXi 7.0 のサポート	VMware vSphere/VMware ESXi 7.0 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。 バージョン 7.0.0 でも VMware 6.0 のサポートは終了します。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードします。
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。 • Cisco HyperFlex • Nutanix エンタープライズクラウド • OpenStack

機能	説明
FTDvパフォーマンス階層型のスマートライセンス	**アップグレードの影響。** FTDv は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスをサポートするようになりました。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。 新しいデバイスを追加する前に、お使いのアカウントに必要なライセンスが含まれていることを確認してください。追加のライセンスを購入するには、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。 FTDv をバージョン 7.0.0 にアップグレードすると、デバイスが自動的に FTDv50 階層に割り当てられます。レガシー（非階層型）ライセンスを引き続き使用するには、アップグレード後に階層を [変数（Variable）] に変更します。 サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。 新規/変更されたページ： • **[デバイス（Device）] > [デバイス管理（Device Management）]** ページで FTDv デバイスを追加または編集するときに、パフォーマンス階層を指定できるようになりました。 • **[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** ページでパフォーマンス階層を一括編集できます。
Device Management	
FTD CLI **show cluster history** の改善	新しいキーワードを指定すると、**show cluster history** コマンドの出力をカスタマイズできます。 新規/変更されたコマンド：**show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] サポートされるプラットフォーム：Firepower 4100/9300
クラスタから永久に削除するための FTD CLI コマンド	FTD CLI を使用して、ユニットをクラスタから完全に削除し、その設定をスタンドアロンデバイスに変換できるようになりました。 新規/変更されたコマンド： **cluster reset-interface-mode** サポートされるプラットフォーム：Firepower 4100/9300
NAT	

機能	説明
優先順位付けされたシステム定義の NAT ルール	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。 セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。 サポートされるプラットフォーム：FTD
仮想ルーティング	
ISA 3000 の仮想ルータサポート	ISA 3000 デバイスには最大 10 台の仮想ルータを設定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：ISA 3000
Site to Site VPN	
ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。	仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。 バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダのエンドポイントに接続し、バックアップ VTI を別のサービスプロバイダのエンドポイントに接続できます。 新規/変更されたページ：ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択した場合に、サイト間 VPN ウィザードにバックアップ VTI を追加する機能が追加されました。 サポートされるプラットフォーム：FTD
Remote Access VPN	
Load balancing	RA VPN ロードバランシングがサポートされるようになりました。システムは、セッション数によってグループ化されたデバイス間でセッションを分散します。トラフィック量やその他の要因は考慮されません。 新規/変更された画面：RA VPN ポリシーの [詳細設定（Advanced Settings）] にロード バランシング 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
ローカル認証	RA VPN ユーザーのローカル認証がサポートされるようになりました。これは、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。 **1.** ローカルレルムを作成します。 ローカルユーザー名とパスワードは、ローカルレルムに保存されます。レルムを作成し（**[システム（System）] > [統合（Integration）] > [レルム（Realms）]**）、新しい **[ローカル（LOCAL）]** レルムタイプを選択すると、1つ以上のローカルユーザーを追加するように求められます。 **2.** ローカル認証を使用するように RA VPN を設定します。 RA VPN ポリシーを作成または編集し（**[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**）、そのポリシー内に接続プロファイルを作成して、その接続プロファイルでプライマリ、セカンダリ、またはフォールバック認証サーバーとして **[ローカル（LOCAL）]** を指定します。 **3.** 作成したローカルレルムを RA VPN ポリシーに関連付けます。 RA VPN ポリシーエディタで、新しい **[ローカルレルム（Local Realm）]** 設定を使用します。ローカル認証を使用する RA VPN ポリシーのすべての接続プロファイルは、ここで指定したローカルレルムを使用します。 サポートされるプラットフォーム：FTD

機能	説明
ダイナミック アクセス ポリシー	新しいダイナミック アクセス ポリシーを使用すると、変化する環境に自動的に適応するリモートアクセス VPN 認証を設定できます。 **1.** AnyConnect HostScan パッケージを AnyConnect ファイルとしてアップロードして、HostScan を設定します（**[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[VPN]>[AnyConnectファイル（AnyConnect File）]**）。**[ファイルタイプ（File Type）]** ドロップダウンリストに新しい **[HostScan パッケージ（HostScan Package）]** オプションがあります。 このモジュールはエンドポイントで実行され、ダイナミック アクセス ポリシーが使用するポスチャアセスメントを実行します。 **2.** ダイナミック アクセス ポリシーを作成します（**[デバイス（Devices）] [ダイナミック アクセス ポリシー（Dynamic Access Policy）]**）。 ダイナミック アクセス ポリシーは、ユーザーがセッションを開始するたびに評価するセッション属性（グループメンバーシップやエンドポイントセキュリティなど）を指定します。その後、その評価に基づいてアクセスを拒否または許可できます。 **3.** 作成したダイナミック アクセス ポリシーを RA VPN ポリシーに関連付けます。 リモートアクセス VPN ポリシーエディタで、新しい **[ダイナミック アクセス ポリシー（Dynamic Access Policy）]**設定を使用します。 サポートされるプラットフォーム：FTD
マルチ証明書認証	リモートアクセスVPNユーザのマルチ証明書認証をサポートするようになりました。SSL または IKEv2 EAP フェーズで AnyConnect クライアントを使用してVPNアクセスを許可するためにユーザの ID 証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。 サポートされるプラットフォーム：FTD

機能	説明
AnyConnect カスタム属性	AnyConnectカスタム属性をサポートし、AnyConnectクライアント機能を設定するためのインフラストラクチャを、これらの機能の明示的なサポートをシステムに追加することなく、提供するようになりました。 サポートされるプラットフォーム：FTD
アクセス制御	

機能	説明
FTD 用 Snort 3	

機能	説明
	新しいバージョンである 7.0.0 以降の FTD の展開では、Snort 3 がデフォルトの検査エンジンです。アップグレードされた展開では引き続き Snort 2 が使用されますが、いつでも切り替えることができます。 Snort 3 を使用する利点は次のとおりですが、これに限定されません。 • パフォーマンスの向上。 • SMBv2 インスペクションの改善。 • 新しいスクリプト検出機能。 • HTTP/2 インスペクション。 • カスタムルールグループ。 • カスタム侵入ルールを記述しやすくする構文。 • 侵入イベント内の「would have dropped」インライン結果の理由。 • VDB、SSL ポリシー、カスタム アプリケーション ディテクタ、キャプティブポータル ID ソース、および TLS サーバ ID 検出へ変更を展開するときに Snort が再起動しない。 • Cisco Success Network に送信される Snort 3 固有のテレメトリデータ、およびトラブルシューティングログの改善による、有用性の向上。 Snort 3 侵入ルールの更新は、SRU ではなく LSP（Lightweight Security Package）と呼ばれます。Snort 2 には引き続き SRU が使用されます。シスコからのダウンロードには、最新の LSP と SRU の両方が含まれており、設定に適したルールセットが自動的に使用されます。 バージョン 7.0.0 以降の FMC は、Snort 2 と Snort 3 の両方のデバイスでの展開を管理でき、各デバイスに正しいポリシーを適用します。ただし、Snort 2 とは異なり、FMC のみをアップグレードしてから展開することで、デバイス上の Snort 3 を更新することはできません。Snort 3 では、新しい機能と解決済みのバグにより、FMC 上のソフトウェアとその管理対象デバイスをアップグレードする必要があります。各ソフトウェアバージョンに含まれている Snort の詳細については、Cisco Firepower Compatibility Guideのバンドルされたコンポーネントのセクションを参照してください。 **重要** Snort 3 に切り替える前に、Firepower Management Center Snort 3 Configuration Guideを読んで理解することを強く

機能	説明
	推奨します。機能の制限と移行手順には特に注意してください。Snort 3 へのアップグレードは影響を最小限に抑えるように設計されていますが、機能は正確にマッピングされません。慎重に計画して準備することで、トラフィックが期待どおりに処理されるようにできます。 Snort 3 の Webサイト（https://snort.org/snort3）にもアクセスできます。https://snort.org/snort3 サポートされるプラットフォーム：FTD

機能	説明
ダイナミックオブジェクト	ダイナミックオブジェクトは、アクセスコントロールルールで使用できます。 ダイナミックオブジェクトは、単に IP アドレスまたはサブネットのリストです（範囲なし、FQDN なし）。ただし、ネットワークオブジェクトとは異なり、ダイナミックオブジェクトへの変更はすぐに有効になり、再展開する必要はありません。これは、IP アドレスがワークロードリソースに動的にマッピングされる仮想環境やクラウド環境で役立ちます。 ダイナミックオブジェクトを作成および管理するには、Cisco Secure 動的属性コネクタを使用することをお勧めします。コネクタは、ワークロードの変更に基づいてファイアウォールポリシーを迅速かつシームレスに更新する別個の軽量アプリケーションです。そのためには、環境内のタグ付きリソースからワークロード属性を取得し、指定した基準に基づいて IP リストをコンパイルします（「動的属性フィルタ」）。次に、FMC でダイナミックオブジェクトを作成し、IP リストを入力します。ワークロードが変更されると、コネクタによってダイナミックオブジェクトが更新され、新しいマッピングに基づいてすぐにトラフィックの処理が開始されます。詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイドを参照してください。 作成したダイナミックオブジェクトは、アクセス コントロール ルール エディタの新しい [動的属性（Dynamic Attributes）] タブでアクセスコントロールルールに追加できます。このタブは、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに代わるものです。ここで、SGT 属性を使用したルールの設定を続行します。 （注） FMC でダイナミックオブジェクトを作成することもできます（**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [外部属性（External Attributes）] > [ダイナミックオブジェクト（Dynamic Objects）]**）。ただし、この場合はコンテナのみ作成されます。その後、REST API を使用してデータを入力して管理する必要があります。Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。 サポート対象プラットフォーム：FMC Cisco Secure Dynamic Attributes Connector の統合でサポートされる仮想/クラウドワークロード：Microsoft Azure、AWS、VMware

機能	説明
Active Directory ドメインのクロスドメイン信頼	Microsoft Active Directory フォレスト（相互に信頼する AD ドメインのグループ）のユーザーを使用してユーザー アイデンティティ ルールを設定できるようになりました。 新規/変更されたページ： • レルムとディレクトリを同時に設定するようになりました。 • 新しい [同期結果（Sync Results）] ページ（**[システム（System）] > [統合（Integration）] > [レルム（Realms）] > [同期結果（Sync Results）]**）に、クロスドメイン信頼関係のユーザーおよびグループのダウンロードに関連するエラーが表示されます。 サポート対象プラットフォーム：FMC
DNS フィルタリング	バージョン 6.7.0 でベータ機能として導入された DNS フィルタリングは、完全にサポートされるようになり、新しいアクセス コントロール ポリシーではデフォルトで有効になっています。 サポートされるプラットフォーム：すべて
イベントロギングおよび分析	

機能	説明
Secure Network Analytics オンプレミス展開でのイベント保存プロセスの改善	新しいシスコのセキュリティ分析とロギング（オンプレミス）アプリと新しいFMCウィザードにより、オンプレミスSecure Network Analyticsソリューションのリモートデータストレージをより簡単に設定できます。 **1.** ハードウェアまたは仮想Stealthwatchアプライアンスを展開します。 Stealthwatch Management Consoleを単独で使用することも、Stealthwatch Management Console、フローコレクタ、およびデータストアを設定することもできます。 **2.** Stealthwatch Management Consoleに新しいCisco Security Analytics and Logging（オンプレミス）アプリをインストールして、Stealthwatchをリモートデータストアとして設定することができます。 **3.** FMCで、**[システム（System）] > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics & Logging）]**ページの新しいウィザードのいずれかを使用して、Stealthwatch展開に接続します。 Stealthwatchのコンテキストクロス起動を設定するために使用したフォーカスの狭いページは、ウィザードによって置き換えられます。現在、これはウィザードのステップの1つです。 syslogを使用してFirepowerイベントをStealthwatchに送信するアップグレードされた展開では、ウィザードを使用する前にこれらの設定を無効にします。そうしないと、二重にイベントが発生します。Stealthwatchへのsyslog接続を削除するには、FTDプラットフォーム設定を使用します（**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]**）。 syslogへのイベント送信を無効にするには、アクセス制御ルールを編集します。 Stealthwatchのハードウェア要件およびソフトウェア要件を含む詳細については、オンプレミスにおけるシスコのセキュリティ分析とロギング：Firepowerイベント統合ガイドを参照してください。 サポート対象プラットフォーム：FMC

機能	説明
Secure Network Analytics オンプレミス展開でリモートに保存されたイベントを操作する	FMC を使用して、Secure Network Analytics オンプレミス展開でリモートに保存された接続イベントを操作できるようになりました。 接続イベントページ（**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**）と統合イベントビューア（**[分析（Analysis）] > [統合イベント（Unified Events）]**）の新しい**データ ソース**オプションを使用して、処理する接続イベントを選択できます。デフォルトでは、時間範囲に何も存在しない場合、ローカルに保存された接続イベントが表示されます。その場合、システムはリモートに保存されたイベントを表示します。 また、リモートで保存された接続イベントに基づいてレポートを生成できるように、レポートテンプレートにデータソースオプションが追加されました（**[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]**）。 （注） この機能は、接続イベントでのみサポートされます。クロス起動は、リモートで保存されたセキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベントを調べる唯一の方法です。統合イベントビューアでも、システムはこれらのタイプのローカルに保存されたイベントのみを表示します。 ただし、すべてのセキュリティ インテリジェンス イベントに同一の接続イベントが存在することに注意してください。これらは「IP ブロック」や「DNS ブロック」などの理由を持つイベントです。これらの重複イベントは、接続イベントページまたは統合イベントビューアで処理できますが、専用のセキュリティ インテリジェンス イベント ページでは処理できません。 サポートされるプラットフォーム：FMC。

機能	説明
すべての接続イベントを Secure Network Analytics クラウドに保存する	Cisco Security Analytics and Logging（SaaS）を使用して、すべての接続イベントを Stealthwatch クラウドに保存できるようになりました。以前は、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベント、およびそれらに関連する接続イベントに限定されていました。 クラウドに送信するイベントを変更するには、**[システム（System）] > [統合（Integration）]** を選択します。**[クラウドサービス（Cloud Services）]** タブで、**[シスコクラウドイベントの設定（Cisco Cloud Event Configuration）]** を編集します。優先順位の高い接続イベントをクラウドに送信する古いオプションは、**[すべて（All）]**、**[なし（None）]**、または **[セキュリティイベント（Security Events）]** の選択肢に置き換えられました。 （注） これらの設定は、SecureX に送信するイベントも制御します。ただし、すべての接続イベントをクラウドに送信するように選択した場合でも、SecureX はセキュリティ（優先度の高い）接続イベントのみを消費します。また、**[分析（Analysis）] > [SecureX]** で SecureX 接続自体を設定することにも注意してください。 サポート対象プラットフォーム：FMC
統合イベントビューア	統合イベントビューア（**[分析（Analysis）] > [統合イベント（Unified Events）]**）では、1 つのテーブルで接続、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアの各イベントが表示されます。これは、異なるタイプのイベント間の関係を調べるのに役立ちます。 単一の検索フィールドを使用すると、複数の条件に基づいてビューを動的にフィルタリングできます。また、**[本番稼働（Go Live）]** オプションでは、管理対象デバイスから受信したイベントがリアルタイムで表示されます。 サポート対象プラットフォーム：FMC

機能	説明
SecureX のリボン	FMC 上の SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。 SecureX に接続してリボンを有効にするには、**[分析（Analysis）] > [SecureX]** を使用します。クラウドリージョンを選択し、SecureX に送信するイベントを指定するには、引き続き **[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）]** を使用する必要があります。 詳細については、Cisco Firepower および SecureX 統合ガイドを参照してください。 サポート対象プラットフォーム：FMC
ローカルストレージをオフにすると、すべての接続イベントのレート制限が免除されます。	イベントレート制限は、FMCに送信されるすべてのイベントに適用されます。ただし、セキュリティイベント（セキュリティ インテリジェンス、侵入、ファイル、マルウェアのイベント、およびそれらに関連する接続イベント）は例外です。 バージョン7.0.0以降では、ローカル接続イベントストレージを無効にすると、セキュリティイベントだけでなく、すべての接続イベントがレート制限から除外されます。これを行うには、**[システム（System）] > [設定（Configuration）] > [データベース（Database）]** ページで **[最大接続イベント数（Maximum Connection Events）]** を 0 に設定します。 （注） **[最大接続イベント数（Maximum Connection Events）]** は、0 に設定してオフにすること以外では、接続イベントのレート制限を制御しません。このフィールドに 0 以外の数値を指定すると、優先順位の低い接続イベントがすべてレート制限されます。 ローカルイベントストレージを無効にしても、リモートイベントストレージには影響せず、接続の概要や相関にも影響しないことに注意してください。システムは、引き続き、トラフィックプロファイル、相関ポリシー、ダッシュボード表示などの機能に接続イベント情報を使用します。 サポート対象プラットフォーム：FMC

機能	説明
ファイルおよびマルウェアイベントテーブルに一緒に表示されるポートとプロトコル	ファイルおよびマルウェアイベントテーブルでは、[ポート（Port）] フィールドにプロトコルが表示されるようになり、[ポート（Port）] フィールドでプロトコルを検索できます。アップグレード前に存在したイベントの場合、プロトコルが不明な場合は「TCP」が使用されます。 新規/変更されたページ： • **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]** • **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]** サポートされるプラットフォーム：FMC
アップグレード	
アップグレードパフォーマンスとステータスレポートの改善	FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい **[アップグレード（Upgrades）]** タブでは、アップグレードステータスとエラーレポートがさらに強化されています。 サポートされるプラットフォーム：FTD

機能	説明
[アップグレード（Upgrade）] ウィザード	

機能	説明
	バージョン 7.0.0 の FMC の新しいデバイス アップグレード ページ（**[デバイス（Devices）] > [アップグレード（Upgrade）]**）には、バージョン 6.4.0 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。 開始するには、[デバイス管理（Device Management）] ページ（**[デバイス（Devices）] > [デバイス管理（Device Management）] > [アクションの選択（Select Action）]**）で新しい **[Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）]** アクションを使用します。 続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。 ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。 （注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き [システム更新（System Updates）] ページ（**[システム（System）] > [更新（Updates）]**）を使用する必要があります。また、[システム更新（System Updates）] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。 （注） バージョン 7.0.0/7.0.x では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは 1 つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1 つユニットでアップグレードを開始すると、すべてのユニットで開始されます。

機能	説明
	時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。 サポートされるプラットフォーム：FTD
より多くのデバイスを一度にアップグレードする	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7.0 以降へのアップグレードでのみ確認できます。デバイスを古いFTDリリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべてのFTDモデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。 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	

機能	説明
SD カードを使用した ISA 3000 でのゼロタッチ復元	ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。 サポートされるプラットフォーム：ISA 3000
RA およびサイト間 VPN ポリシーを選択的に展開する	バージョン 6.6.0 で導入された選択的ポリシーの展開では、リモートアクセスとサイト間 VPN ポリシーがサポートされ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）]** ページに VPN ポリシー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
新しいヘルス モジュール	次の正常性モジュールが追加されました。 • AMP 接続ステータス • AMP Threat Grid のステータス • ASP ドロップ • 高度な Snort 統計情報 • シャーシステータス FTD • イベント ストリーム ステータス • FMC アクセス設定の変更 • FMC HA ステータス（古い HA ステータスの交換） • FTD HA ステータス • ファイルシステムの整合性チェック • フロー オフロード • ヒット カウント（Hit Count） • MySQL ステータス • NTP ステータス FTD • Rabbit MQ ステータス • ルーティング統計情報 • SSE 接続ステータス • Sybase ステータス • 未解決グループモニター • VPN 統計情報 • xTLS カウンタ さらに、バージョン 6.6.3 で [アプライアンス設定のリソース使用率（Appliance Configuration Resource Utilization）] モジュールとして導入された [構成メモリ割り当て（Configuration Memory Allocation）] モジュールは、バージョン 6.7.0 では完全にはサポートされていませんでしたが、完全にサポートされます。 サポート対象プラットフォーム：FMC
セキュリティと強化	

機能	説明
AWS 導入用の新しいデフォルトパスワード	初期展開時にユーザーデータ（**[高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]**）を使用してデフォルトパスワードを定義していなければ、adminアカウントのデフォルトパスワードは AWS のインスタンス ID です。 以前は、デフォルトの admin パスワードは Admin123 でした。 サポートされているプラットフォーム：FMCv for AWS、FTDv for AWS
証明書の登録用の EST	証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。 新規/変更されたページ：**[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [CA情報（CA Information）]** タブ設定時の新しい登録オプション。 サポート対象プラットフォーム：FMC
EdDSA 証明書タイプのサポート	新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。 新規/変更されたページ：**[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [キー（Key）]** タブの設定時の新しい証明書キーオプション。 サポート対象プラットフォーム：FMC
NTP サーバーの AES-128 CMAC 認証	AES-128 CMAC キーを使用して、FMC と NTP サーバー間の接続を保護できるようになりました。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）]**。 サポートされるプラットフォーム：FMC
SNMPv3 ユーザーは、SHA-224 または SHA-384 認証アルゴリズムを使用して認証できます。	SNMPv3 ユーザーは、SHA-224 または SHA-384 アルゴリズムを使用して認証できるようになりました。 新規/変更されたページ：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）] > [認証アルゴリズムタイプ（Auth Algorithm Type）]** サポートされるプラットフォーム：FTD
ユーザービリティとパフォーマンス	

機能	説明
ポリシーとオブジェクトのグローバル検索	特定のポリシーを名前で検索し、特定のオブジェクトを名前と設定値で検索できるようになりました。この機能は、クラシックテーマでは使用できません。 新規/変更されたページ：[展開（Deploy）] メニューの左側にある [FMC] メニューバーに [検索（Search）] アイコンとフィールドの機能が追加されました。 サポート対象プラットフォーム：FMC
Intel QuickAssist Technology（QAT）を使用した FTDv でのハードウェア暗号化アクセラレーション	VMware の FTDv および KVM の FTDv でハードウェア暗号化アクセラレーション（CBC 暗号のみ）がサポートされるようになりました。この機能を使用するには、ホスティング プラットフォームに Intel QAT 8970 PCI アダプタ/バージョン 1.7 以降のドライバが必要です。リブートすると、ハードウェア暗号化アクセラレーションが自動的に有効になります。 サポートされるプラットフォーム：VMware の FTDv、KVM の FTDv
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、 **show local-host** サポートされるプラットフォーム：FTD
FMC REST API：新しいサービスと操作 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。詳細については、Firepower Management Center REST API バージョン 7.0 クイックスタートガイド [英語] を参照してください。	
デバイス	alerts：GET
統合	fmchastatuses：GET securexconfigs：GET および PUT

機能	説明
オブジェクト	anyconnectcustomattributes、anyconnectpackages、anyconnectprofiles：GET anyconnectcustomattributes/overrides：GET applicationfilters：PUT、POST、および DELETE certificatemaps：GET dnsservergroups：GET dnsservergroups/overrides：GET dynamicobjectmappings：POST dynamicobjects：GET、PUT、POST、および DELETE dynamicobjects/mappings：GET および PUT geolocations：PUT、 POST、および DELETE grouppolicies：GET hostscanpackages：GET intrusionrules、intrusionrulegroups：GET、PUT、POST、および DELETE intrusionrulesupload：POST ipv4addresspools、ipv6addresspools：GET ipv4addresspools/overrides、ipv6addresspools/overrides：GET localrealmusers：GET、PUT、POST、DELETE radiusservergroups：GET realms：PUT、POST、および DELETE sidnsfeeds、sidnslists、sinetworkfeeds、sinetworklists：GET sinkholes：GET ssoservers：GET ssoservers/overrides：GET usage：GET

機能	説明
ポリシー	accesspolicies/securityintelligencepolicies：GET dnspolicies：GET dnspolicies/allowdnsrules、dnspolicies/blockdnsrules：GET dynamicaccesspolicies：GET、PUT、POST、および DELETE identitypolicies：GET intrusionpolicies：PUT、POST、および DELETE intrusionpolicies/intrusionrulegroups、intrusionpolicies/intrusionrules：GET および PUT networkanalysispolicies：GET、PUT、POST、および DELETE networkanalysispolicies/inspectorconfigs：GET networkanalysispolicies/inspectoroverrideconfigs：GET および PUT ravpns：GET ravpns/addressassignmentsettings、ravpns/certificatemapsettings、ravpns/connectionprofiles：GET
検索（Search）	globalsearch：GET

FMC バージョン 7.0.0 で廃止された機能

表 *4 : FMC* バージョン *7.0.0* で廃止された機能

機能	アップグレードの影響	説明
キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書	Firepower Threat Defense デバイスを介したアップグレード後の VPN 接続を防止します。	バージョン 7.0.0 では、キーが 2048 ビット未満の RSA 証明書、または署名アルゴリズムで SHA-1 を使用する RSA 証明書のサポートが削除されています。 アップグレードする前に、オブジェクトマネージャを使用し、より強力なオプションを使用して PKI 証明書の登録を更新します（[オブジェクト（Objects）]>[PKI]>[証明書の登録（Cert Enrollment）]）。更新しない場合、アップグレードしても現在の設定は保持されますが、デバイスを介した VPN 接続は失敗します。 弱いオプションを使用して古い Firepower Threat Defense デバイス（バージョン 6.4.0 ー 6.7.x）のみを管理し続けるには、[デバイス（Devices）]>[証明書（Certificates）] ページで各デバイスの新しい [弱暗号化の有効化（Enable Weak-Crypto）] オプションを選択します。

機能	アップグレードの影響	説明
SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化（削除）	アップグレード後に展開ができないようにします。	バージョン 7.0.0 では、Firepower Threat Defense デバイスにおける SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化のサポートが削除されています。 Firepower Threat Defense をバージョン 7.0.0 にアップグレードすると、Firepower Management Center の設定に関係なく、これらのユーザーがデバイスから削除されます。プラットフォーム設定ポリシーでこれらのオプションを使用している場合は、Firepower Threat Defense をアップグレードする前に構成を変更して確認してください。 これらのオプションは、Threat Defense プラットフォーム設定ポリシー（[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]）で SNMPv3 ユーザーを作成または編集する際の [認証アルゴリズムタイプ（Auth Algorithm Type）] および [暗号化タイプ（Encryption Type）] ドロップダウンにあります。
AMP クラウドとのポート 32137 通信	Firepower Management Center のアップグレードを阻止します。	バージョン 7.0.0 では、パブリックおよびプライベート AMP クラウドからファイル配置データを取得するためにポート 32137 を使用する Firepower Management Center オプションが廃止されています。プロキシを設定しない限り、Firepower Management Center はポート 443/HTTPS を使用するようになりました。 アップグレードする前に、[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページで [ネットワーク用 AMP にレガシーポート 32137 を使用（Use Legacy Port 32137 for AMP for Networks）] オプションを無効にします。AMP for Networks の展開が期待どおりに機能するまで、アップグレードを続行しないでください。
[HA ステータス（HA Status）] 正常性モジュール	なし。	バージョン 7.0.0 では、[HA ステータス（HA Status）] 正常性モジュールの名前が変更されています。これからは、[FMC HA ステータス（FMC HA Status）] 正常性モジュールです。これは、新しい [FTD HA ステータス（FTD HA Status）] モジュールと区別するためです。

機能	アップグレードの影響	説明
VMware 6.0 ホスティング	Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードします。	バージョン 7.0.0 では、VMware vSphere/VMware ESXi 6.0 での仮想展開のサポートが廃止されています。 これには、FMCv、FTDv、および VMware 向け NGIPSv が含まれます。
Web インターフェイスの変更	なし	バージョン 7.0.0 では、次の点が変更されています。 • アクセス コントロール ルール エディタでは、[動的属性（Dynamic Attributes）] タブが、フォーカスの狭い [SGT/ISE 属性（SGT/ISE Attributes）] タブに置き換わります。ここで、SGT 属性を使用したルールの設定を続行します。 • **[システム（System）]** > **[SecureX]** で、SecureX 統合を設定するようになりました以前は、これらの設定は **[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** で行っていました。 • **[ヘルプ（Help）]** > **[使用方法（How-Tos）]** でウォークスルーが呼び出されるようになりました。以前は、ブラウザウィンドウの下部にある [使用方法（How-Tos）] をクリックしていました。

バージョン 6.7.0

FMC バージョン 6.7.0 の新機能

表 5:

機能	説明
ハードウェアおよび仮想アプライアンス	
Oracle Cloud Infrastructure（OCI）仮想導入	Oracle Cloud Infrastructure に FMCv と FTDv を導入しました。
Google Cloud Platform（GCP）仮想導入	Google Cloud Platform に FMCv と FTDv を導入しました。

機能	説明
VMware 向け FMCv でのハイアベイラビリティのサポート	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 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（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。Firepower Management Center Configuration Guide の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読むことを推奨します。 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、デバイスは ClientHello メッセージを特定の方法で変更します。『Firepower Management Center Configuration Guide』の「ClientHello Message Handling」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）によって Bugtraq が置き換わりました	**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
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。 サポートされてい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
コンフィギュレーション 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。『Firepower Management Center Configuration Guide』の「Policy Management」の章の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
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 FTD コンテナインスタンスをバックアップでき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：Firepower 4100/9300
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

機能	説明
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
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、『Firepower Management Center Configuration Guide』の「*Reusable Objects*」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（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。 サポート対象プラットフォーム：FMC

機能	説明
ヘルスモニターリングの強化	ヘルスモニター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。 サポート対象プラットフォーム：FMC
ユーザー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。 サポート対象プラットフォーム：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

FMC バージョン 6.7.0 で廃止された機能

表 *6*：

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 ID ソース	Firepower Management Center のアップグレードを阻止します。	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。 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。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、Cisco Firepower User Agent の製品速報 [英語]、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。https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/bulletin-c25-744508.htmlhttps://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/product-bulletin-c25-742894.htmlhttps://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/215887-firepower-user-identity-migrating-from.html 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 Firepower Management Center 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	Firepower Management Center のアップグレードを阻止します。	次のいずれかの Firepower Threat Defense 機能を使用している場合、Firepower Management Center をアップグレードできない場合があります。 • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の Firepower Management Center 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 Firepower Management Center 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 6.7.0 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 6.7.0 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 6.7.0 への Firepower Management Center のアップグレード デバイスがバージョン 6.6.3/6.6.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 6.7.0 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、Firepower Management Center 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 6.3.0～6.6.1 からバージョン 6.7.0 にアップグレードされた Firepower Management Center、またはバージョン 6.7.0 に新たにインストールされた Firepower Management Center。 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 Firepower Management Center にモジュールが有効になっているバージョン 6.6.3/6.6.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 7.0.0 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（Configuration Memory Allocation）] に変更されます。

機能	アップグレードの影響	説明
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 6.7.0 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 6.7.0 の新機能 （51 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 6.3.0 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 6.7.0 以降の Firepower Management Center 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。
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 6.7.0 では、クラシックテーマの Firepower Management Center 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 6.7.0 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 6.7.0 の新機能 （51 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。
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	アップグレードは禁止されています。	ASA 5525-X、5545-X、および 5555-X のデバイスでは、Firepower ソフトウェア（Firepower Threat Defense と ASA FirePOWER の両方）のバージョン 6.7.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。

バージョン 6.6.3

FMC バージョン 6.6.3 の新機能

表 *7:*

機能	説明
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 6.6.3 以降を実行している 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 以降のパッチからアップグレードする場合を除き、バージョン 6.6.3 へのアップグレードはサポートされません。

機能	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	バージョン 6.7.0 のアップグレードの影響。 バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールであるアプライアンス設定のリソース使用率が導入されています。 モジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。詳細については、Firepower Management Center Configuration Guideの「アクセス制御のベストプラクティス」を参照してください。 アップグレードプロセスにより、すべての正常性ポリシーにこのモジュールが自動的に追加され、有効になります。アップグレード後、正常性ポリシーを管理対象デバイスに適用して、モニターリングを開始します。 （注） このモジュールには、FMC と管理対象デバイスの両方に、バージョン 6.6.3 以降の 6.6.x リリース、またはバージョン 7.0.0 以降が必要です。 バージョン 6.7.0 では、このモジュールのサポートが部分的および一時的に廃止されています。詳細については、FMC バージョン 6.7.0 で廃止された機能 （87 ページ）を参照してください。 バージョン 7.0.0 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。

バージョン 6.6.1

FMC バージョン 6.6.1 で廃止された機能

表 *8*:

機能	アップグレードの影響	説明
ルールが競合してもカスタム侵入ルールのインポートが失敗しない	なし	バージョン 6.6.0 では、ルールの競合があった場合、Firepower Management Center はカスタム（ローカル）侵入ルールのインポートの完全な拒否を開始しました。バージョン 6.6.1 ではこの機能を廃止し、競合が発生したルールをサイレントでスキップする、バージョン 6.6.0 より前の動作に戻ります。 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。Firepower Management Center Configuration Guide の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読むことを推奨します。 バージョン 6.7.0 では、今後のリリースでのルールの競合に関する警告が追加されます。

バージョン 6.6.0

FMC バージョン 6.6.0 の新機能

表 *9*:

機能	説明
ハードウェアおよび仮想アプライアンス	
Firepower 4112 上の FTD	Firepower 4112 が導入されました。このプラットフォームでは、ASA 論理デバイスを展開することもできます。FXOS 2.8.1 が必要です。

機能	説明
AWS の展開用の大型のインスタンス	**アップグレードの影響。** FTDv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C5.xlarge • C 5.2 xlarge • C5.4xlarge FMCv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C3.4xlarge • C4.4xlarge • C5.4xlarge AWS インスタンスタイプ用の既存のすべての FMCv が廃止されました。アップグレードする前に、サイズを変更する必要があります。詳細については、バージョン 6.6.0 のアップグレードガイドラインを参照してください。 サポートされるプラットフォーム：FMCv for AWS、FTDv for AWS
クラウドベースの FTDv 展開の自動スケール	バージョン 6.6.0 では、AWS 自動スケール/Azure 自動スケールのサポートが導入されています。 クラウドベースの展開におけるサーバーレスインフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。 サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure
Firepower Threat Defense：デバイス管理	

機能	説明
DHCPを使用した初期管理インターフェイスの IP アドレスの取得	Firepower 1000/2000 シリーズと ASA-5500-X シリーズのデバイスの場合、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得するようになりました。この変更により、既存のネットワーク上に新しいデバイスを簡単に展開できるようになりました。 この機能は、論理デバイスを展開するときにIPアドレスを設定する Firepower 4100/9300 シャーシではサポートされていません。また、FTDvやISA 3000 でもサポートされていません。これらについては、引き続きデフォルトで 192.168.45.45 になります。 サポートされているプラットフォーム：Firepower 1000/2000 シリーズ、ASA-5500-X シリーズ
CLI での MTU 値の設定	FTD CLI を使用して、FTD デバイスインターフェイスの MTU（最大伝送単位）値を設定できるようになりました。デフォルト値は 1500 バイトです。MTU の最大値は次のとおりです。 • 管理インターフェイス：1500 バイト • イベントインターフェイス：9000 バイト 新しい FTD CLI コマンド： **configure network mtu** 変更された FTD CLI コマンド：**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが **configure network management-interface** コマンドに追加されました。 サポートされるプラットフォーム：FTD

機能	説明
内部 Web サーバーからのアップグレードパッケージの取得	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更されたページ：[システム（System）] > [更新（Updates）] > [更新のアップロード（Upload Update）] ボタン > [ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション サポートされるプラットフォーム：FTD
接続ベースのトラブルシューティングの機能拡張	FTD CLI 接続ベースのトラブルシューティングに次の機能拡張が加えられました（デバッギング）。 • **debug packet-module trace**：モジュールレベルのパケットトレースを有効にするために追加されました。 • **debug packet-condition**：進行中の接続のトラブルシューティングをサポートするように変更されました。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：クラスタリング	

機能	説明
マルチインスタンスクラスタ	コンテナインスタンスを使用してクラスタを作成できるようになりました。Firepower 9300 では、クラスタ内の各モジュールに 1 つのコンテナインスタンスを含める必要があります。セキュリティエンジン/モジュールごとに複数のコンテナインスタンスをクラスタに追加することはできません。 クラスタインスタンスごとに同じセキュリティモジュールまたはシャーシモデルを使用することを推奨します。ただし、必要に応じて、同じクラスタ内に異なる Firepower 9300 セキュリティ モジュール タイプまたは Firepower 4100 モデルのコンテナインスタンスを混在させ、一致させることができます。同じクラスタ内で Firepower 9300 と 4100 のインスタンスを混在させることはできません。 新しい FXOS CLI コマンド： **set port-type cluster** 新規/変更された Firepower Chassis Manager ページ： • **[論理デバイス（Logical Devices）] > [クラスタの追加（Add Cluster）]** • **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] > [タイプ（Type）] フィールド サポートされるプラットフォーム：Firepower 4100/9300
FTD クラスタでのデータユニットへのパラレル設定同期	FTD クラスタの制御ユニットは、デフォルトでスレーブユニットとの設定変更を同時に同期させるようになりました。以前は、同期が順番に行われていました。 サポートされるプラットフォーム：Firepower 4100/9300
クラスタへの参加の失敗または削除のメッセージを次のコマンドに追加。 **show cluster history**	クラスタユニットがクラスタへの参加に失敗するか、クラスタを離脱する場合のために、新しいメッセージが **show cluster history** コマンドに追加されました。 サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：ルーティング	

機能	説明
仮想ルータと VRF-Lite	複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できるようになりました。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。 仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。 作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。完全なリストについては、『Firepower Management Center Configuration Guide』の「Virtual Routing for Firepower Threat Defense」の章を参照してください。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（edit device）]>[ルーティング（Routing）]タブ 新しい FTD CLI コマンド：**show vrf**。 変更された FTD CLI コマンド：［**vrf** *name* ｜ **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更しました。 サポートされるプラットフォーム：FTD（Firepower 1010 および ISA 3000 を除く）
Firepower Threat Defense：**VPN**	

機能	説明
リモートアクセス VPN 内の DTLS 1.2	Datagram Transport Layer Security（DTLS） 1.2 を使用して、RA VPN 接続を暗号化できるようになりました。 FTD プラットフォーム設定を使用して、FTD デバイスが RA VPN サーバーとして動作するときに使用する最小 TLS プロトコルバージョンを指定します。また、DTLS 1.2 を指定する場合は、最小 TLS バージョンとして TLS 1.2 を選択する必要もあります。 Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7 以降が必要です。 新規/変更されたページ：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [SSL] > [DTLS バージョン（DTLS Version）] オプション サポートされるプラットフォーム：FTD（ASA 5508-X および ASA 5516-X を除く）
複数のピアに対するサイト間 VPN IKEv2 のサポート	IKEv1 と IKEv2 のポイントツーポイント エクストラネットおよびハブアンドスポークトポロジのために、サイト間 VPN 接続にバックアップピアを追加できるようになりました。これまで設定できたのは、IKEv1 ポイントツーポイント トポロジのバックアップピアのみでした。 新規/変更されたページ：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [ポイントツーポイントまたはハブアンドスポーク FTD VPN トポロジの追加または編集（Add or Edit a Point to Point or Hub and Spoke FTD VPN Topology）] > [エンドポイントの追加（Add Endpoint）] > [IP アドレス（IP Address）] フィールドで、カンマ区切りのバックアップピアがサポート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：FTD
セキュリティ ポリシー	

機能	説明
セキュリティポリシーの使いやすさの向上	バージョン 6.6.0 を使用すると、アクセス制御ルールとプレフィルタルールが簡単に使用できるようになります。次の作業に進んでください。 • 1回の操作（状態、アクション、ロギング、侵入ポリシーなど）で、複数のアクセス制御ルールの特定の属性を編集します。 アクセス コントロール ポリシー エディタで、関連するルールを選択し、右クリックして [編集（Edit）] を選択します。 • 複数のパラメータによってアクセス制御ルールを検索します。 アクセス コントロール ポリシー エディタで、[ルールの検索（Search Rules）] テキストボックスをクリックしてオプションを表示します。 • アクセス制御ルールまたはプレフィルタルール内のオブジェクトの詳細と使用状況を表示します。 アクセスコントロールポリシーエディタまたはプレフィルタ ポリシー エディタで、ルールを右クリックし、[オブジェクトの詳細（Object Details）] を選択します。 サポートされるプラットフォーム：FMC

機能	説明
アクセス コントロール ポリシーのオブジェクトグループ検索	動作中、FTD デバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。 オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。 オブジェクトグループ検索は、ルールがどのように定義されているかや、FMC にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] >[デバイス（Device）] タブ > [詳細設定（Advanced Settings）] > [オブジェクトグループ検索（Object Group Search）] オプション サポートされるプラットフォーム：FTD
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の時間ベースのルール	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できるようになりました。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス コントロール ルール エディタまたはプレフィルタルールエディタ • [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [タイムゾーン（Time Zone ）] • [オブジェクト（Objects）]> [オブジェクト管理（Object Management）] > [時間範囲（Time Range）] と [タイムゾーン（Time Zone）] サポートされるプラットフォーム：FTD

機能	説明
出力最適化の再有効化	**アップグレードの影響。** バージョン 6.6.0 では CSCvs86257 が修正されました。出力最適化が次のような状態だった場合があります。 • 有効になっていたがオフになり、アップグレードするとオンに戻る（機能が有効になっていた場合でも、バージョン 6.4.0 と 6.5.0 の一部のパッチでは出力最適化をオフにしていました）。 • 手動で無効にした場合は、アップグレード後に **asp inspect-dp egress-optimization** を使用して再度有効に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
イベントロギングおよび分析	
新しいデータストアによるパフォーマンスが向上	**アップグレードの影響。** パフォーマンスを向上させるために、バージョン 6.6.0 では、接続およびセキュリティインテリジェンスイベントに新しいデータストアを使用します。 アップグレードが完了し、FMC がリブートすると、履歴接続イベントとセキュリティインテリジェンスイベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。 履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。 イベントの移行の進行状況は、メッセージセンターでモニターできます。 サポート対象プラットフォーム：FMC
URL の接続イベントとセキュリティ インテリジェンス イベントを検索する場合のワイルドカードのサポート	**example.com** のパターンを持つ URL の接続イベントとセキュリティインテリジェンスイベントを検索する場合は、ワイルドカードを含めなければならなくなりました。このような検索の場合、具体的には ***example.com*** を使用します。 サポート対象プラットフォーム：FMC

機能	説明
FTD デバイスを使用した最大 30 万の同時ユーザーセッションのモニターリング	バージョン 6.6.0 では、FTD デバイスモデルの一部で、同時ユーザーセッション（ログイン）のモニターリングが新たにサポートされるようになります。 • 30 万セッション：Firepower 4140、4145、4150、9300 • 15 万セッション：Firepower 2140、4112、4115、4120、4125 他のすべてのデバイスは、2,000 に制限されている ASA FirePOWER を除き、以前の 64,000 の制限を引き続きサポートします。 新しい正常性モジュールでは、ユーザーID機能のメモリ使用率が設定可能なしきい値に達したときに、アラートを発行します。また、時間の経過に伴うメモリ使用率のグラフも表示できます。 新規/変更されたページ： • [システム（System）] > [正常性（Health）] > [ポリシー（Policy）] > [正常性ポリシーを追加または編集（Add or Edit Health Policy）] > [Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] • [システム（System）] > [正常性（Health）] > [モニター（Monitor）] > デバイスの選択 > [Snort アイデンティティメモリ使用率（Snort Identity Memory Usage）] モジュールの [グラフ（Graph）] オプション サポートされるプラットフォーム：上記の FTD デバイス
IBM QRadar との統合	IBM QRadar 向けの新しい Cisco Firepower アプリケーションをイベントデータを表示するための代替手段として使用して、ネットワークへの脅威を分析、ハント、および調査をすることができます。eStreamer が必要です。 詳細については、『Integration Guide for the Cisco Firepower App for IBM QRadar』を参照してください。 サポート対象プラットフォーム：FMC
管理とトラブルシューティング	

機能	説明
設定変更を展開するための新しいオプション	FMC メニューバーの [展開（Deploy）] ボタンが次の機能を追加するオプションが備わったメニューになりました。 • [ステータス（Status）]：デバイスごとに、変更を展開する必要があるかどうか、展開前に解決する必要がある警告またはエラーがあるかどうか、最後の展開が処理中、失敗、正常に完了のうちのどの状態かが表示されます。 • [プレビュー（Preview）]：デバイスに対して最後に展開してから行った、適用可能なすべてのポリシーとオブジェクトの変更が表示されます。 • [展開の選択（Selective Deploy）]：管理対象デバイスに対して展開するポリシーと設定から選択します。 • [展開時間の見積もり（Deploy Time Estimate）]：特定のデバイスに対して展開するためにかかる時間の見積もりが表示されます。すべての展開のみでなく、特定のポリシーや設定の見積もりを表示することができます。 • [履歴（History）]： 以前の展開の詳細が表示されます。 新規/変更されたページ： • **[展開（Deploy）] > [展開（Deployment）]** • **[展開（Deploy）] > [展開履歴（Deployment History）]** サポート対象プラットフォーム：FMC

機能	説明
初期設定による VDB の更新と、SRU の更新のスケジュール設定	新規および再イメージ化された FMC では、セットアッププロセスは次のようになりました。 • 最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。 • 毎日の侵入ルール（SRU）のダウンロードを有効にします。これらのダウンロード後は、セットアッププロセスで自動展開が有効にならないことに注意してください。ただし、この設定は変更できます。 アップグレードされた FMC は影響を受けません。 新規/変更されたページ： • [システム（System）] > [更新（Updates）] > [製品の更新（VDB の更新）（Product Updates (VDB updates)）] • [システム（System）] > [更新（Updates）] > [ルールの更新（SRU の更新）（Rule Updates (SRU updates)）] サポート対象プラットフォーム：FMC
FMC を復元するための VDB の一致は不要	バックアップからの FMC の復元に交換用 FMC 上に同じ VDB を使用する必要はなくなりました。ただし、復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。 サポート対象プラットフォーム：FMC
サブジェクト代替名（SAN）を使用した HTTPS 証明書	SAN を使用して複数のドメイン名または IP アドレスを保護する HTTPS サーバー証明書を要求できるようになりました。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更されたページ：[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）] > [新しい CSR の生成（Generate New CSR）] > [サブジェクト代替名（Subject Alternative Name）] フィールド サポート対象プラットフォーム：FMC

機能	説明
FMC ユーザーアカウントに関連付けられている実名	FMCユーザーアカウントを作成または変更するときに、実名を指定できるようになりました。これには、個人名、部署名、またはその他の識別属性を指定できます。 新規/変更されたページ：[システム（System）] > [ユーザー（Users）] > [ユーザー（Users）] > [実名（Real Name）] フィールド サポート対象プラットフォーム：FMC
追加の FTD プラットフォームでの Cisco Support Diagnostics	**アップグレードの影響。** Cisco Support Diagnostics は、すべての FMC および FTD デバイスで完全にサポートされるようになりました。以前は、サポートは FMC、FTD 搭載 Firepower 4100/9300、および Azure 向け FTDv に限定されていました。 サポートされるプラットフォーム：FMC、FTD
ユーザービリティ	
ライトテーマ	FMC はデフォルトでバージョン 6.5.0 のベータ機能として導入されたライトテーマに設定されます。バージョン 6.6.0 にアップグレードすると、ライトテーマに自動的に切り替わります。これは、ユーザー設定で従来のテーマに戻すことができます。 すべてに返信することはできませんが、ライトテーマについてのフィードバックを歓迎します。[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 からフィードバックをお送りください。 サポート対象プラットフォーム：FMC
アップグレードの残り時間の表示	FMC のメッセージセンターに、アップグレードが完了するまでのおおよその残り時間が表示されるようになりました。これには、リブート時間は含まれません。 新規/変更されたページ：メッセージセンター サポート対象プラットフォーム：FMC
セキュリティと強化	

機能	説明
デフォルトの HTTPS サーバー証明書の更新期限は 800 日	**アップグレードの影響。** 現在のデフォルトの HTTPS サーバー証明書がすでに 800 日である場合を除き、バージョン 6.6.0 にアップグレードすることで証明書が更新され、有効期限がアップグレード日から 800 日後になりました。今後の更新はすべて、有効期間が 800 日になります。 古い証明書は、生成日に応じて期限切れになるように設定されていました。 サポート対象プラットフォーム：FMC
Firepower Management Center REST API	
新しい REST API 機能	バージョン 6.6.0 の機能をサポートするための次の REST API サービスが追加されました。 • bgp、bgpgeneralsettings、ospfinterface、ospfv2routes、ospfv3interfaces、ospfv3routes、virtualrouters、routemaps、ipv4prefixlists、ipv6prefixlists、aspathlists、communitylists、extendedcommunitylists、standardaccesslists、standardcommunitylists、policylists：ルーティング • virtualrouters、virtualipv4staticroutes、virtualipv6staticroutes、virtualstaticroutes：仮想ルーティング • timeranges、globaltimezones、timezoneobjects：時間ベースのルール • commands：REST API から CLI コマンドの限定的なセットを実行 • pendingchanges：保留中の改善点を展開 古い機能をサポートするために、次の REST API サービスが追加されました。 • intrusionrules、intrusionpolicies：侵入ポリシー サポート対象プラットフォーム：FMC

機能	説明
拡張アクセスリストの REST API サービス名を変更	**アップグレードの影響。** FMC REST API の extendedaccesslist（単数形）サービスは、extendedaccesslist**s**（複数形）になりました。クライアントを更新していることを確認します。古いサービス名を使用すると失敗し、無効な URL エラーが返されます。 要求タイプ：GET 特定の ID に関連付けられている拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} すべての拡張アクセスリストを取得するための URL： • 旧：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • 新：/api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** サポート対象プラットフォーム: FMC

FMC バージョン 6.6.0 で廃止された機能

表 *10*:

機能	アップグレードの影響	説明
クラウドベースの FMCv 展開でのメモリ不足のインスタンス	アップグレードは禁止されています。	パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。 • AWS での c3.xlarge • AWS での c3.2xlarge • AWS での c4.xlarge • AWS での c4.2xlarge • Azure での Standard_D3_v2 バージョン 6.6.0+ にアップグレードする前に、サイズを変更する必要があります。詳細については、バージョン 6.6.0 のアップグレードガイドラインを参照してください。 さらに、バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開におけるメモリ不足のインスタンスタイプが完全に廃止されました。以前の Firepower バージョンであっても、これらを使用して新しい FMCv インスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。
VMware 向け FTDv の e1000 インターフェイス	アップグレードされないようにします。	バージョン 6.6.0 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』を参照してください。

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	なし。ただし、今すぐ切り替える必要があります。	バージョン 6.6.0 では、次の Firepower Threat Defense セキュリティ機能は廃止されます。 • 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。 これらの機能はバージョン 6.7.0 で廃止されました。VPN で使用するために、IKE プロポーザルまたは IPSec ポリシーでこれらの機能を設定しないでください。できるだけ強力なオプションに変更してください。
接続イベントのカスタムテーブル	サポートされていないカスタムテーブルは削除する必要があります。	バージョン 6.6.0 は、接続イベントとセキュリティ インテリジェンス イベントのカスタムテーブルのサポートを終了します。アップグレード後は、これらのイベントの既存のカスタムテーブルは引き続き「利用可能」ですが、結果は返されません。これらのテーブルを削除することをお勧めします。 他のタイプのカスタムテーブルに変更はありません。 廃止されたオプション： • [分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル（Custom Tables）] > [カスタムテーブルの作成（Create Custom Table）] > [テーブル（Tables）] ドロップダウンリスト > [接続イベント（Connection Events）] と、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] のクリック

機能	アップグレードの影響	説明
イベントビューアから接続イベントを削除する機能	なし	バージョン6.6.0は、接続イベントとセキュリティインテリジェンス イベントをイベントビューアから削除するためのサポートを終了しています。データベースを消去するには、**[システム（System）]** > **[ツール（Tools）]** > **[データの消去（Data purge）]** を選択します。 廃止されたオプション： • **[分析（Analysis）]** > **[接続（Connections）]** > **[イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）] • **[分析（Analysis）]** > **[接続（Connections）]** > **[セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）]

バージョン 6.5.0

FMC バージョン 6.5.0 の新機能

表 *11* :

機能	説明
ハードウェアおよび仮想アプライアンス	
Firepower 1150 上の FTD	Firepower 1150 が導入されました。
Azure の FTDv がより大規模なインスタンスに対応	Microsoft Azure に導入した Firepower Threat Defense Virtual で、より大規模なインスタンス D4_v2 および D5_v2 がサポートされるようになりました。
VMware 向け FMCv 300	Firepower Management Center Virtual for VMware より大規模な FMCv 300 を導入しました。他の FMCv インスタンスで管理できるデバイスは 25 台ですが、この FMCv では最大 300 台のデバイスを管理できます。 FMCモデル移行機能を使用すると、性能が劣るプラットフォームから FMCv 300 に切り替えることができます。
VMware vSphere/VMware ESXi 6.7 のサポート	VMware vSphere/VMware ESXi 6.7 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。

機能	説明
Firepower Threat Defense	
Firepower 1010 ハードウェアスイッチのサポート	Firepower 1010 で、各イーサネットインターフェイスをスイッチポートまたはファイアウォール インターフェイスとして設定できるようになりました。 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）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [VLANインターフェイスの追加（Add VLAN Interface）]** サポートされるプラットフォーム：Firepower 1010
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+）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：[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）] > [PoE] サポートされるプラットフォーム：Firepower 1010
キャリアグレード NAT の拡張	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。 新規/変更されたページ：**[デバイス（Devices）] > [NAT]** > [FTD NAT ポリシーの追加/編集（add/edit FTD NAT policy）] > [NAT ルールの追加/編集（add/edit NAT rule）] > [PAT プール（PAT Pool）] タブ > [ブロック割り当て（Block Allocation）] オプション サポートされるプラットフォーム：FTD

機能	説明
Firepower 4100/9300 上の複数のコンテナインスタンスの TLS 暗号化アクセラレーション	Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。 新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、**create hw-crypto** および **scope hw-crypto** CLI コマンドを使用してください。詳細については、Cisco Firepower 4100/9300 FXOS Command Reference を参照してください。 新しい FXOS CLI コマンド： • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** 削除された FXOS CLI コマンド： • **show hwCrypto**（**show hw-crypto** に置き換えられました） • **config hwCrypto** 削除された FTD CLI コマンド： • **show crypto accelerator status** サポートされるプラットフォーム：Firepower 4100/9300
セキュリティ ポリシー	
アクセスコントロールルールのフィルタリング	検索条件に基づいてアクセスコントロールルールをフィルタ処理できるようになりました。 新規/変更されたページ：[ポリシー（Policies）]>[アクセス制御（Access Control）]>[アクセス制御（Access Control）]>ポリシーの追加/編集>フィルタボタン（[フィルタ条件に一致するルールのみを表示（show only rules matching filter criteria）]） サポートされるプラットフォーム：FMC

機能	説明
URL カテゴリまたはレピュテーションの異議申し立て	URL のカテゴリまたはレピュテーションについて異議を申し立てることができるようになりました。 新規/変更されたページ： • [分析（Analysis）] > [接続イベント（Connection Events）] > カテゴリまたはレピュテーションを右クリック > [未処理（Dispute）] • [分析（Analysis）] > [詳細（Advanced）] > [URL] > URL の検索 > [未処理（Dispute）] ボタン • [システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] > [未処理（Dispute）] リンク サポートされるプラットフォーム：FMC
宛先ベースのセキュリティグループタグ（SGT）を使用したユーザー制御	アクセスコントロールルール内の送信元および宛先の両方の一致基準に ISE SGT タグを使用できるようになりました。SGT タグは、ISE によって取得されたタグからホスト/ネットワークへのマッピングです。 新しい接続イベントフィールド： • [宛先SGT（Destination SGT）]（syslog：DestinationSecurityGroupTag）：接続レスポンダの SGT 属性。 名前が変更された接続イベントフィールド： • [送信元SGT（Source SGT）]（syslog：SourceSecurityGroupTag）：接続イニシエータの SGT 属性。[セキュリティグループタグ（Security Group Tag）]（syslog：SecurityGroup）から変更されました。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [ID ソース（Identity Sources）] > [Identity Services Engine] > [セッションディレクトリのトピック（Session Directory Topic）] および [SXP のトピック（SXP Topic）] 登録オプション サポートされるプラットフォーム：すべて

機能	説明
Cisco Firepower User Agent バージョン 2.5 の統合	Firepower バージョン 6.4.0 ～ 6.6.x と統合できる Cisco Firepower User Agent のバージョン 2.5 がリリースされました。 （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、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。 新規/変更された FMC CLI コマンド： **configure user-agent** サポートされるプラットフォーム：FMC
イベントロギングおよび分析	

機能	説明
Threat Intelligence Director の優先順位。	TID ブロッキングおよびモニターリング監視可能アクションが、セキュリティ インテリジェンス ブロック リストを使用したブロッキングおよびモニターリングよりも優先されるようになりました。 [ブロック（Block）] TID 監視可能アクションを設定した場合は、トラフィックが [ブロック（Block）] に設定されたセキュリティ インテリジェンス ブロック リストにも一致していても、次のようになります。 • 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDブロック（TID Block）] のバリアントになります。 • システムは、[ブロック済み（Blocked）] のアクション実施を伴う TID インシデントを生成します。 [モニター（Monitor）] TID 監視可能アクションを設定した場合は、トラフィックが [モニター（Monitor）] に設定されたセキュリティ インテリジェンス ブロック リストにも一致していても、次のようになります。 • 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDモニター（TID Monitor）] のバリアントになります。 • システムは、[モニター済み（Monitored）] のアクション実施を伴う TID インシデントを生成します。 以前は、どちらの場合も、システムではカテゴリが分析別に報告され、TID インシデントは生成されませんでした。 （注） システムは引き続き、トラフィックを以前と同様に効果的に処理します。以前にブロックされたトラフィックは引き続きブロックされ、モニター対象トラフィックは引き続きモニターされます。単に、どのコンポーネントが「クレジット」を取得するかが変更されます。また、生成される TID インシデントが増える場合もあります。 セキュリティ インテリジェンスと TID の両方を有効にした場合のシステム動作の詳細については、『Firepower Management Center Configuration Guide』の「TID-Firepower Management Center Action Prioritization」の情報を参照してください。 サポートされるプラットフォーム：FMC

機能	説明
packet-profile CLI コマンド	デバイスがネットワークトラフィックをどのように処理したかに関する統計情報を取得する FTD CLI を使用できるようになりました。プレフィルタポリシーによって高速パス処理されたパケット数、大規模なフローとしてオフロードされたパケット数、アクセス制御（Snort）によって完全に評価されたパケット数などを取得できます。 新しい FTD CLI コマンド： • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** サポートされるプラットフォーム：FTD
次に対応したその他のイベントタイプ Cisco SecureX Threat Response	Firepower で、Cisco SecureX Threat Response にファイルおよびマルウェアイベントや優先度の高い接続イベント（侵入、ファイル、マルウェア、およびセキュリティインテリジェンスイベントに関連するイベント）を送信できるようになりました。 FMC Web インターフェイスでは、この機能を Cisco Threat Response（CTR）と呼びます。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] サポートされるプラットフォーム：FTD（syslog経由または直接統合）および従来のデバイス（syslog 経由）
管理とトラブルシューティング	
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp**（インターフェイス モード）コマンド、グローバル コマンド **ptp mode e2etransparent**、**ptp domain** を追加できるようになりました。 新規/変更されたコマンド： **show ptp** サポートされるプラットフォーム：FTD を使用した ISA 3000

機能	説明
設定できるドメイン数の増加（マルチテナンシー）	マルチテナンシーを実装する（管理対象デバイス、設定、およびイベントへのユーザーアクセスをセグメント化する）場合、最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 個のサブドメインを作成できます。以前は、最大で 50 ドメインでした。 サポートされるプラットフォーム：FMC
ISE 接続ステータスのモニターの機能拡張	[ISE接続ステータスのモニター（ISE Connection Status Monitor）] ヘルスモジュールで、TrustSec SXP（SGT Exchange Protocol）サブスクリプション ステータスに関する問題のアラートが表示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：FMC
地域のクラウド	**アップグレードの影響。** Cisco Threat Response の統合、Cisco Support Diagnostics、または Cisco Success Network 機能を使用する場合は、地域クラウドを選択できるようになりました。 デフォルトでは、アップグレードによって米国（北米）リージョンに割り当てられます。 新規/変更されたページ：**[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** サポートされるプラットフォーム：FMC、FTD

機能	説明
Cisco Support Diagnostics	**アップグレードの影響。** （「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。 バージョン 6.5.0 では、Cisco Support Diagnostics のサポートは一部のプラットフォームに限定されています。 新規/変更されたページ： • **[システム（System）] > [スマートライセンス（Smart Licenses）]** • **[システム（System）] > [スマートライセンス（Smart Licenses）] > [登録（Register）]** サポートされるプラットフォーム：FMC、Firepower 4100/9300、および Azure 向け FTDv
FMC モデル移行	バックアップおよび復元機能を使用して、FMC が同じモデルでない場合でも、FMC 間で設定とイベントを移行できるようになりました。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による FMC の交換が容易になります。 一般に、ローエンドの FMC からハイエンドの FMC に移行することはできますが、その逆に移行することはできません。KVM および Microsoft Azure からの移行はサポートされていません。また、Cisco Smart Software Manager（CSSM）への登録を解除して再登録する必要があります。 サポート対象の移行先モデルなどの詳細については、『Firepower Management Center モデル移行ガイド』を参照してください。 サポート対象プラットフォーム：FMC
セキュリティと強化	

機能	説明
FXOS ベースの FTD デバイス上のアプライアンス コンポーネントの安全な消去	指定したアプライアンス コンポーネントを安全に消去する FXOS CLI を使用できるようになりました。 新しい FXOS CLI コマンド： **erase secure** サポートされるプラットフォーム：Firepower 1000/2000 および Firepower 4100/9300
初期設定時における FMC admin アカウントのパスワード要件の厳格化	FMC の初期設定時に、admin アカウントの「強力な」パスワードを選択することが必要になりました。設定プロセスでは、FMC Web インターフェイスと CLI の両方の admin アカウントにこの強力なパスワードが適用されます。 （注） バージョン 6.5.0+ にアップグレードしても、脆弱なパスワードを強力なパスワードに変更する必要はありません。物理 FMC 上の LOM ユーザーを除き（これには admin ユーザーが含まれます）、新しい脆弱なパスワードの選択は禁止されていません。ただし、すべての Firepower ユーザーアカウント（特に管理者アクセス権を持つユーザーアカウント）に強力なパスワードを設定することを推奨します。 サポートされるプラットフォーム：FMC
同時ユーザーセッション数の制限	FMC に同時にログインできるユーザーの数を制限できるようになりました。読み取り専用ロール、読み取り/書き込みロール、またはその両方を持つユーザーの同時セッション数を制限できます。CLI ユーザーは、読み取り/書き込み設定によって制限されることに注意してください。 新規/変更されたページ：[システム（System）] > [設定（Configuration）] > [ユーザー設定（User Configuration）] > [許可された最大同時セッション数（Max Concurrent Sessions Allowed）] オプション サポートされるプラットフォーム：FMC
認証済み NTP サーバー	SHA1 または MD5 対称キー認証を使用して FMC と NTP サーバー間のセキュアな通信を設定できるようになりました。システムセキュリティのために、この機能を使用することをお勧めします。 新規/変更されたページ：[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）] サポートされるプラットフォーム：FMC
ユーザービリティとパフォーマンス	

機能	説明
初期設定の改善	新規および再イメージ化されたFMCでは、ウィザードによって以前の初期設定プロセスが置き換えられます。GUIウィザードを使用すると、初期設定の完了時にFMCに[デバイス管理（Device Management）]ページが表示され、導入環境のライセンシング と設定をすぐに開始できます。 また、設定プロセスでは以下が自動的にスケジュールされます。 • ソフトウェアのダウンロード。導入環境に適用されるソフトウェアパッチおよび公開されているホットフィックスをダウンロードする（インストールはしない）、毎週にスケジュール設定されたタスクが作成されます。 • FMC設定のみのバックアップ。FMCの設定をバックアップしてローカルに保存する、週次のスケジュールされたタスクが作成されます。 • GeoDB の更新。地理位置情報データベースの毎週の更新が有効になります。 タスクはUTCでスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。 （注） 自動スケジュール設定タスクと GeoDB の更新を確認し、必要に応じて調整することを強くお勧めします。 アップグレードされた FMC は影響を受けません。初期設定ウィザードの詳細については、ご使用のFMCモデルのスタートアップ ガイドを参照してください。スケジュールされたタスクの詳細については、Firepower Management Center Configuration Guideを参照してください。 サポートされるプラットフォーム：FMC

機能	説明
ライトテーマ	**ベータ版。** FMC Web インターフェイスのデフォルトはクラシックテーマですが、新しいライトテーマを選択することもできます。 （注） ライトテーマはベータ機能です。テキストやその他の UI 要素の位置がずれていることがあります。場合によっては、応答時間が通常より長くなることもあります。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、クラシックテーマに戻してください。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

機能	説明
オブジェクトの表示に関するユーザービリティの拡張	次のように、ネットワーク、ポート、VLAN、および URL オブジェクトに対する「オブジェクトの表示」機能が強化されました。 • アクセス コントロール ポリシーで FTD ルーティングを設定するときに、オブジェクトを右クリックして [オブジェクトの表示（View Objects）] を選択すると、そのオブジェクトに関する詳細が表示されます。 • オブジェクトの詳細を表示しているとき、またはオブジェクトマネージャでオブジェクトを参照しているときに、[使用状況の検索（Find Usage）]（）をクリックすると、オブジェクトグループとネストされたオブジェクトにドリルダウンできるようになりました。 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）] > サポートされているオブジェクトタイプの選択 > [使用状況の検索（Find Usage）]（） • [ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセス制御（Access Control）] > ポリシーの作成または編集 > ルールの作成または編集 > サポートされている条件タイプの選択 > オブジェクトの右クリック > [オブジェクトの表示（View Objects）] • [デバイス（Devices）] > [デバイス管理（Device Management）] > FTD デバイスの編集 > [ルーティング（Routing）] > サポートされているオブジェクトの右クリック > [オブジェクトの表示（View Objects）] サポートされるプラットフォーム：FMC
設定変更の展開に関するユーザービリティの拡張	設定変更の展開に関連するエラーと警告の表示が整理されました。すぐに詳細が表示されるのではなく、[クリックしてすべての詳細を表示します（Click to view all details）] をクリックすると、特定のエラーまたは警告に関する詳細情報を表示できるようになりました。 新規/変更されたページ：[要求された展開のエラーと警告（Errors and Warnings for Requested Deployment）] ダイアログボックス サポートされるプラットフォーム：FMC

機能	説明
FTD NAT ポリシー管理に関するユーザービリティの拡張	FTD NAT の設定時に、次のことが可能になりました。 • NAT ポリシーの警告とエラーをデバイス別に表示できます。警告とエラーによって、トラフィックやフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。 • ページあたり最大 1000 個の NAT ルールを表示できます。デフォルトは 100 です。 新規/変更されたページ：[デバイス（Devices）]>[NAT]>[FTD NAT ポリシーの作成または編集（create or edit FTD NAT policy）]>[警告を表示（Show Warnings）] および [ページあたりのルール数（Rules Per Page）] オプション サポートされるプラットフォーム：FTD
Firepower Management Center REST API	
新しい REST API 機能	バージョン 6.5.0 の機能をサポートするための次の REST API オブジェクトを追加しました。 • cloudregions：地域クラウド 古い機能をサポートするための次の REST API オブジェクトを追加しました。 • categories：アクセスコントロールルールのカテゴリ • domain、inheritancesettings：ドメインとポリシーの継承 • prefilterpolicies、prefilterrules、tunneltags：プレフィルタポリシー • vlaninterfaces：VLAN インターフェイス サポートされるプラットフォーム：FMC

FMC バージョン 6.5.0 パッチの新機能

表 *12*：

機能	説明
バージョン 6.5.0.5 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 で現在デフォルト設定されているの HTTPS サーバー証明書の有効期間がすでに 800 日の場合を除き、バージョン 6.5.0.5+ にアップグレードすると証明書が更新されて、アップグレードの日から 800 日後に期限切れになります。その後の更新はすべて、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。 • 6.5.0 ～ 6.5.0.4：3 年 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年

FMC バージョン 6.5.0 で廃止された機能

表 *13*：

機能	アップグレードの影響	説明
Firepower Management Center CLI を無効にする機能	なし	バージョン 6.3.0 では、明示的に有効にする必要がある Firepower Management Center CLI が導入されました。バージョン 6.5.0 では、新しい展開とアップグレードされた展開の両方に対して、CLI が自動的に有効になります。Linux シェル（エキスパートモードとも呼ばれる）にアクセスする場合は、CLI にログインしてから、**expert** コマンドを使用する必要があります。 **注意** Cisco TAC の指示がない限り、シェルを使用して Firepower アプライアンスにアクセスしないことをお勧めします。 廃止されたオプション：**[システム（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）] > [CLI アクセスの有効化（Enable CLI Access）] チェックボックス**

機能	アップグレードの影響	説明
SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化（廃止）	なし。ただし、今すぐ切り替える必要があります。	バージョン 6.5.0 では、Firepower Threat Defense における SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化が廃止されます。 これらの設定はアップグレード後も引き続き機能しますが、展開時に警告が表示されます。また、これらのオプションを使用して新しいユーザーを作成したり、既存のユーザーを編集したりはできません。 今後のリリースでサポート対象外となります。 プラットフォーム設定ポリシーでこれらのオプションを引き続き使用する場合は、より強力なオプションに切り替えることをお勧めします。 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）] > [SNMP] > [ユーザー（Users）]
TLS 1.0 および 1.1	クライアントがアップグレードされたアプライアンスとの接続に失敗することがあります。	セキュリティ強化対策： • キャプティブポータル（アクティブ認証）では、TLS 1.0 のサポートが廃止されました。 • ホスト入力で TLS 1.0 および TLS 1.1 のサポートが廃止されました。 クライアントが Firepower アプライアンスとの接続に失敗した場合は、TLS 1.2 をサポートするようにクライアントをアップグレードすることをお勧めします。
Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド	なし	Firepower 4100/9300 の複数のコンテナ インスタンスに対して TLS crypto アクセラレーションを許可する一環として、次の FXOS CLI コマンドを削除しました。 • **show hwCrypto** • **config hwCrypto** および、この FTD CLI コマンドを削除しました。 • **show crypto accelerator status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。

機能	アップグレードの影響	説明
Cisco Security Packet Analyzer の統合	なし。ただし、統合はサポートされていません。	バージョン 6.5.0 では、Firepower Management Center と Cisco Security Packet Analyzer の統合のサポートを終了します。 廃止された画面/オプション： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）]
デフォルトの HTTPS サーバー証明書	なし	バージョン 6.4.0.9 以降からアップグレードする場合、デフォルトの HTTPS サーバー証明書の lifespan-on-renew は 3 年に戻りますが、バージョン 6.6.0 以降で再び 800 日に更新されます。 現在のデフォルトの HTTPS サーバー証明書は、いつ生成されたかに応じて、次のように期限切れになるように設定されています。 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年
Firepower Management Center モデル FMC 750、1500、3500	アップグレードは禁止されています。	FMC 750、FMC 1500、および FMC 3500 では、Firepower Management Center ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。これらの Firepower Management Center を使用してバージョン 6.5.0 以降のデバイスを管理することはできません。
Firepower ソフトウェアを搭載した ASA 5515-X および ASA 5585-X シリーズ デバイス	アップグレードは禁止されています。	ASA 5515-X および ASA 5585-X シリーズのデバイス（SSP-10、-20、-40、および -60）では、Firepower ソフトウェア（Firepower Threat Defense と ASA FirePOWER の両方）のバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。

機能	アップグレードの影響	説明
Firepower 7000/8000 シリーズ デバイス	アップグレードは禁止されています。	AMP モデルを含む、Firepower 7000/8000 シリーズ デバイスでは、Firepower ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。

バージョン 6.4.0

FMC バージョン 6.4.0 の新機能

表 *14*：

機能	説明
ハードウェアおよび仮想アプライアンス	
FMC モデル：FMC 1600、2600、および 4600	Firepower Management Center モデル FMC 1600、2600、および 4600 を導入しました。
FMCv on Azure	Firepower Management Center Virtual for Microsoft Azure を導入しました。
Firepower 1010、1120、1140 上の FTD	Firepower 1010、1120、および 1140 を導入しました。
Firepower 4115、4125、4145 上の FTD	Firepower 4115、4125、および 4145 が導入されました。
Firepower 9300 SM-40、SM-48、および SM-56 のサポート	新しい 3 つのセキュリティ モジュール（SM-40、SM-48、SM-56）を導入しました。 FXOS バージョン 2.6.1 では、同じシャーシ内に異なるタイプのセキュリティモジュールを混在できます。
同じ Firepower 9300 上の ASA および FTD	FXOS 2.6.1 では、ASA および FTD 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。
Firepower Threat Defense：デバイス管理	

機能	説明
VMware の FTDv はデフォルトで vmxnet3 インターフェイスに設定される	VMware の FTDv は、仮想デバイスを作成するときにデフォルトで vmxnet3 インターフェイスに設定されるようになりました。以前は、デフォルトは e1000 でした。Vmxnet3 のデバイス ドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワーク パフォーマンスが向上します。 （注） バージョン 6.6.0 では、e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、バージョン 6.6.0 以降へのアップグレードはできません。今すぐ実行することをお勧めします。詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』の VMware インターフェイスの追加と設定の手順を参照してください。 サポートされているプラットフォーム：VMware の FTDv
Firepower Threat Defense：ルーティング	
OSPFv2 ルーティングの循環（キーチェーン）認証	OSPFv2 ルーティングを設定すると、循環（キーチェーン）認証を使用できるようになりました。 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）]** > **[キーチェーン（Key Chain）]** オブジェクト • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [インターフェイス（Interface）] タブ > [インターフェイスの追加/編集（add/edit interface）] > [認証（Authentication）] オプション • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [エリア（Area）] タブ > [エリアの追加/編集（add/edit area）] > [仮想リンク（Virtual Link）] サブタブ > [仮想リンクの追加/編集（add/edit virtual link）]> [認証（Authentication）] オプション 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：セカンダリ認証	セカンダリ認証（二重認証とも呼ばれる）は、2 つの異なる認証サーバーを使用して、RA VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、AnyConnect VPN のユーザーは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。 RA VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。 新規/変更されたページ：**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** >[設定の追加/編集（add/edit configuration）] > [接続プロファイル（Connection Profile）] > [AAA] 領域 サポートされるプラットフォーム：FTD
サイト間 VPN：エクストラネット エンドポイントのダイナミック IP アドレス	エクストラネットエンドポイントにダイナミック IP アドレスを使用するように、サイト間 VPN を設定できるようになりました。ハブアンドスポーク導入環境では、ハブをエクストラネット エンドポイントとして使用できます。 新規/変更されたページ：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [エンドポイント（Endpoints）] タブ > [エンドポイントの追加（add endpoint）] > [IP アドレス（IP Address）] オプション サポートされるプラットフォーム：FTD
サイト間 VPN：ポイントツーポイント トポロジのためのダイナミック暗号マップ	ポイントツーポイントおよびハブアンドスポーク VPN トポロジでは、ダイナミック暗号マップを使用できるようになりました。フル メッシュ トポロジについては、ダイナミック暗号マップはまだサポートされていません。 トポロジを設定するときは、暗号マップ タイプを指定します。トポロジ内のピアの 1 つに対して、ダイナミック IP アドレスも指定する必要があります。 新規/変更されたページ：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [IPsec] タブ > [暗号マップタイプ（Crypto Map Type）] オプション サポートされるプラットフォーム：FTD

機能	説明
TLS 暗号化アクセラレーション	**アップグレードの影響。** SSL ハードウェア アクセラレーションは、TLS 暗号化アクセラレーションに名前が変更されました。デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。バージョン 6.4.0 のアップグレードプロセスでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。 ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。ただし、Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、モジュール/セキュリティ エンジンごとに、*1* つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナ インスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。 Firepower 4100/9300 シャーシ向けの新しい FXOS CLI コマンド： • **show hwCrypto** • **config hwCrypto** 新しい FTD CLI コマンド： • **show crypto accelerator status**（**system support ssl-hw-status** の代替） 削除された FTD CLI コマンド： • **system support ssl-hw-accel** • **system support ssl-hw-status** サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300
イベントロギングおよび分析	

機能	説明
ファイルおよびマルウェア イベントの syslog メッセージの改良	完全修飾ファイルおよびマルウェアのイベントデータが syslog 経由で管理対象デバイスから送信できるようになりました。 新規/変更されたページ：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [ロギング（Logging）] タブ > [ファイルおよびマルウェアの設定（File and Malware Settings）] 領域 サポートされているプラットフォーム：すべて
CVE ID による侵入イベントの検索	特定の CVE エクスプロイトの結果として生成された侵入イベントを検索できるようになりました。 新規/変更されたページ：**[分析（Analysis）]** > **[検索（Search）]** サポートされるプラットフォーム：FMC
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	侵入イベントの syslog メッセージは、イベントをトリガーした侵入ポリシーを指定す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：すべて
Cisco SecureX Threat Response 統合	Cisco SecureX Threat Response は、脅威の迅速な検出、調査、および対応に役立つ Cisco Cloud を提供しています。 この機能を使用すると、Firepower Threat Defense などの複数の製品から集約されたデータを使用してインシデントを分析できます。FMC Web インターフェイスでは、この機能を Cisco Threat Response（CTR）と呼びます。 Cisco Firepower および SecureX 統合ガイドを参照してください。 新規/変更されたページ：**[システム（System）]** > **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]** サポートされるプラットフォーム：FTD
Splunk の統合	Splunk のユーザーは、新しい個別の Splunk アプリケーションである Cisco Secure Firewall（f.k.a. Firepower）App for Splunk を使用してイベントを分析できます。どの機能を使用できるかは、Firepower のバージョンによって異なります。 Cisco Firepower App for Splunk User Guide を参照してください。 サポートされるプラットフォーム：FMC

機能	説明
Cisco Security Analytics and Logging（SaaS）の統合	Firepower イベントを Stealthwatch Cloud に送信して保存したり、必要に応じて、Firepower イベントデータを Stealthwatch Cloud によるセキュリティ分析に利用できるようにすることが可能です。 Cisco Security Analytics and Logging（SaaS）（SAL（SaaS）とも呼ばれる）により、Firepower デバイスは、イベントを syslog メッセージとしてネットワーク上の仮想マシンにインストールされた Security Events Connector（SEC）に送信します。この SEC は、イベントを Stealthwatch Cloud に転送して保存します。Web ベースの Cisco Defense Orchestrator（CDO）ポータルを使用して、イベントを表示および操作します。購入するライセンスによっては、Stealthwatch ポータルを使用して、その製品の分析機能にアクセスすることもできます。 Firepower Management Center および Cisco Security Analytics and Logging（SaaS）統合ガイド を参照してください。 サポートされるプラットフォーム：FMC を搭載した FTD
管理とトラブルシューティング	
ISA 3000 の新しいライセンス機能	ASA FirePOWER および FTD の導入環境では、 ISA 3000 は URL フィルタリングおよびマルウェアのライセンスと各ライセンスの関連機能をサポートするようになりました。 FTD のみ、ISA 3000 は、承認されたお客様向けに特定のライセンスの予約をサポートするようになりました。 サポートされるプラットフォーム：ISA 3000
管理対象デバイスのスケジュールされたリモート バックアップ	FMC を使用して、特定の管理対象デバイスのリモートバックアップをスケジュールできるようになりました。以前、スケジュールされたバックアップをサポートしていたのは Firepower 7000/8000 シリーズのデバイスのみで、デバイスのローカル GUI を使用する必要がありました。 新規/変更されたページ：**[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** > [タスクの追加/編集（add/edit task）] > [ジョブタイプ：バックアップ（Job Type: Backup）] を選択 > [バックアップのタイプ（Backup Type）] を選択 サポートされるプラットフォーム：FTD の物理プラットフォーム、VMware 向け FTDv、Firepower 7000/8000 シリーズ 例外：FTD のクラスタ化されたデバイスまたはコンテナ インスタンスはサポートされていません。

機能	説明
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用するとサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更されたページ：**[システム（System）]** > **[設定（Configuration）]** > **[管理インターフェイス（Management Interfaces）]** > **[インターフェイス（Interfaces）]** 領域 > [インターフェイスの編集（edit interface）] > [IPv6 DAD] チェックボックス サポートされるプラットフォーム：FMC、Firepower 7000/8000 シリーズ
管理インターフェイス上の ICMPv6 エコー応答と宛先到達不能メッセージを無効にする機能	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更されたページ：**[システム（System）]** > **[設定（Configuration）]** > **[管理インターフェイス（Management Interfaces）]** > **[ICMPv6]** 新規/変更されたコマンド： • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** サポートされるプラットフォーム：FMC（Web インターフェイスのみ）、管理対象デバイス（CLI のみ）

機能	説明
RADIUS サーバーに定義されている FTD ユーザーの Service-Type 属性のサポート	FTD CLI ユーザーの RADIUS 認証では、以前は RADIUS 外部認証オブジェクトにユーザー名を事前に定義してから、RADIUS サーバーに定義されているユーザー名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバーで CLI ユーザーを定義できるようになりました。また、Basic と Config の両方のユーザー ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェルアクセスフィルタを空白のままにしてください。 新規/変更されたページ：**[システム（System）]** > **[ユーザー（Users）]** > **[外部認証（External Authentication）]** タブ > [外部認証オブジェクトの追加/編集（add/edit external authentication object）] > [シェルアクセスフィルタ（Shell Access Filter）] サポートされるプラットフォーム：FTD
オブジェクトの使用状況の表示	オブジェクト マネージャでネットワーク、ポート、VLAN、またはURL オブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示できるようになりました。 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）] > でオブジェクトタイプ、[使用状況の検索（Find Usage）]（双眼鏡）アイコンの順に選択 サポートされるプラットフォーム：FMC

機能	説明
アクセス制御ルールと事前フィルタ ルールのヒット カウント	FTD デバイスのアクセス制御ルールと事前フィルタ ルールのヒット カウントにアクセスできるようになりました。 新規/変更されたページ： • **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒットカウントの分析（Analyze Hit Counts）] • **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[事前フィルタ（Prefilter）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒットカウントの分析（Analyze Hit Counts）] 新しいコマンド： • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** 変更されたコマンド： **show failover** サポートされるプラットフォーム：FTD
URL フィルタリングヘルスモニターの改善	URL フィルタリング モニター アラートの時間しきい値を設定できるようになりました。 新規/変更されたページ：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** > [ポリシーの追加/編集（add/edit policy ）] > [URL フィルタリングモニター（URL Filtering Monitor）] サポートされるプラットフォーム：すべて

機能	説明
接続ベースのトラブルシューティング	接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大 7 レベルまでサポートし、lina ログと Snort ログで一貫したログ収集メカニズムを使用できます。 新規/変更されたコマンド： • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** サポートされるプラットフォーム：FTD
Cisco Success Network の新しいモニターリング機能	Cisco Success Network の次のモニターリング機能を追加しました。 • CSPA（Cisco Security Packet Analyzer）のクエリ情報 • FMC で有効になっているコンテキストクロス起動インスタンス • TLS/SSL インスペクション イベント • Snort の再起動 サポート対象プラットフォーム：FMC
セキュリティと強化	

機能	説明
署名済みの SRU、VDB、および GeoDB の更新	Firepowerは正しい更新ファイルを使用していることが確認できるため、バージョン 6.4.0 以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）に使用します。以前のバージョンでは、引き続き未署名の更新が使用されます。シスコサポートおよびダウンロードサイトから手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。 ただし、SRU、VDB、および GeoDB の更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。バージョン 6.4.0 以降の署名付きの更新ファイルの先頭は "Sourcefire" ではなく "Cisco" で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar バージョン 5.x ～ 6.3 の更新ファイルでは、引き続き古い命名方式が使用されています。 • SRU：Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB：Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB：Sourcefire_Geodb_Update-*date-build*.sh シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。 （注） 古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。 サポートされているプラットフォーム：すべて

機能	説明
SNMPv3ユーザーは、SHA-256認証アルゴリズムを使用して認証できます	SNMPv3 ユーザーは、SHA-256 アルゴリズムを使用して認証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）] > [SNMP] > [ユーザー（Users）] > [認証アルゴリズムタイプ（Auth Algorithm Type）] サポートされているプラットフォーム：Firepower Threat Defense
2048 ビットの証明書キーが必要になりました（セキュリティ強化）	**アップグレードの影響。** AMP for Endpoints や Cisco Threat Intelligence Detector（TID）などの外部データソースへのセキュアな接続を行う場合、FMC では、少なくとも 2048 ビット長のキーを使用したサーバー証明書の生成が必要になりました。以前に 1024 ビットキーを使用して生成された証明書は機能しなくなります。 このセキュリティ拡張機能は、バージョン 6.3.0.3 で導入されました。バージョン 6.1.0 から 6.3.0.2 にアップグレードする場合、影響を受ける可能性があります。接続できない場合は、データソースでサーバー証明書を再生成します。必要に応じて、データソースへの FMC 接続を再設定します。 サポートされるプラットフォーム：FMC
ユーザービリティとパフォーマンス	
Snort 再起動の改善	バージョン 6.4.0 より以前では、Snort の再起動中、暗号化された接続のうち、「復号しない」 SSL ルールまたはデフォルトポリシーアクションに一致したものがシステムによってドロップされていました。現在は、大きなフロー オフロードまたは Snort preserve-connection を無効にしていない限り、ルーテッド/透過トラフィックはドロップされずにインスペクションなしで通過します。 サポートされているプラットフォーム：Firepower 4100/9300

機能	説明
選択された IPS トラフィックのパフォーマンスの向上	**アップグレードの影響。** 出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。この機能は、すべての FTD プラットフォームでデフォルトで有効になっています。 バージョン 6.4.0 のアップグレードプロセスでは、対象デバイスでの出力最適化が有効になります。詳細については、『Cisco Firepower Threat Defense コマンド リファレンス』を参照してください。出力最適化に関する問題をトラブルシューティングCisco TACするには、にお問い合わせください。 サポートされるプラットフォーム：FTD 新規/変更されたコマンド： • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization**
SNMP イベント ロギングの高速化	外部 SNMP トラップ サーバーに侵入イベントと接続イベントを送信する際のパフォーマンスが向上しました。 サポートされているプラットフォーム：すべて
展開の高速化	アプライアンスの通信と展開フレームワークが向上しました。 サポートされるプラットフォーム：FTD
アップグレードの高速化	イベント データベースが向上しました。 サポートされているプラットフォーム：すべて
Firepower Management Center REST API	

機能	説明
新しい REST API 機能	バージョン 6.4.0 の機能をサポートするための REST API オブジェクトを追加しました。 • cloudeventsconfigs：Cisco SecureX Threat Response の統合を管理します。 • ftddevicecluster：シャーシのクラスタリングを管理します。 • hitcounts：アクセス制御ルールと事前フィルタ ルールのヒット カウント統計情報を管理します。 • keychain：OSPFv2 ルーティングの設定時に、認証のローテーションに使用されるキーチェーン オブジェクトを管理します。 • loggingsettings：アクセス コントロール ポリシーのロギング設定を管理します。 サポートされるプラットフォーム：FMC
OAS に基づく API エクスプローラ	バージョン 6.4.0 は OpenAPI 仕様（OAS）に基づいて、新しい API エクスプローラを使用します。OAS の一部として、CodeGen を使用してサンプル コードを生成するようになりました。必要に応じて、レガシー API エクスプローラにもアクセスできます。 サポートされるプラットフォーム：FMC

FMC バージョン 6.4.0 パッチの新機能

表 *15 :*

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。その後の更新はすべて、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 で廃止された機能

表 *16 :*

機能	アップグレードの影響	説明
SSL ハードウェアアクセラレーション FTD CLI コマンド	なし。	TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。 • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。
Web インターフェイスの変更	なし	バージョン 6.4.0 では、次のページの場所が変更されています。 **[システム（System）]> [統合（Integration）]> [クラウドサービス（Cloud Services）]** は次に変更されました。 **[システム（System）]> [統合（Integration）]> [Cisco CSI]**

FMC バージョン 6.4.0 パッチで廃止された機能

表 *17*：

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。

バージョン 6.3.0

FMC バージョン 6.3.0 の新機能

表 *18*：

機能	説明
ハードウェア	
FMC モデル：FMC 1600、2600、および 4600	Firepower Management Center モデル FMC 1600、2600、および 4600 を導入しました。
ISA 3000 with FirePOWER Services	ISA 3000 with FirePOWER Services は、バージョン 6.3.0 でサポートされています（保護ライセンスのみ）。 ISA 3000 with FirePOWER Services はバージョン 5.4.x でもサポートされていましたが、バージョン 6.3.0 にアップグレードすることはできません。再イメージ化する必要があります。

機能	説明
Firepower Threat Defense：デバイス管理	
サポート対象ネットワークモジュールに関する Firepower 2100 シリーズでのハードウェア バイパス サポート	Firepower 2100 シリーズ デバイスは、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能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：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[インターフェイス（Interfaces）]**>**[物理インターフェイスの編集（Edit Physical Interface）]** サポートされるプラットフォーム：Firepower 2100 シリーズ
オン モードでのデータ EtherChannel のサポート	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された Firepower Chassis Management ページ：**[インターフェイス（Interfaces）]**>**[すべてのインターフェイス（All Interfaces）]**>**[ポートチャネルの編集（Edit Port Channel）]**>**[モード（Mode）]** 新規/変更された FXOS コマンド： **set port-channel-mode** サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：**HA** およびクラスタリング	

機能	説明
FTD を搭載した Firepower 4100/9300 のマルチインスタンス機能	

機能	説明
	単一のセキュリティ エンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーションインスタンスを展開できるだけでした。 柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2 台の個別のシャーシ上でコンテナ インスタンスを使用してハイ アベイラビリティを使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチコンテキストモードに似ています。FTD では、マルチ コンテキスト モードを使用できません。 新規/変更された FMC ページ：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]**> [デバイスの編集（edit device）] > [インターフェイス（Interfaces）] タブ 新規/変更された Firepower Chassis Manager ページ： • **[概要（Overview）]** > **[デバイス（Devices）]** • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] • **[インターフェイス（Interfaces）]** > **[すべてのインターフェイス（All Interfaces）]** > **[タイプ（Type）]** • **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** • **[プラットフォームの設定（Platform Settings）]** > **[Mac プール（Mac Pool）]** • **[プラットフォームの設定（Platform Settings）]**> **[リソースのプロファイル（Resource Profiles）]** 新規/変更された FXOS コマンド：**connect ftd***name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**create resource-profile**、**create**

機能	説明
	subinterface、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** サポートされるプラットフォーム：Firepower 4100/9300
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された Firepower Chassis Manager ページ：**[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）] > [クラスタ情報（Cluster Information）]** 新規/変更されたオプション：[CCL サブネット IP（CCL Subnet IP）] フィールド 新規/変更された FXOS コマンド： **set cluster-control-link network** サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
FMC への FTD クラスタ追加の改善	FMC にクラスタの任意のユニットを追加できるようになりました。他のクラスタ ユニットは自動的に検出されます。以前は、各クラスタユニットを個別のデバイスとして追加し、FMC でグループ化してクラスタにする必要がありました。クラスタ ユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新規/変更されたページ： • **[デバイス（Devices）] > [デバイス管理（Device Management）]** > [追加（Add）] ドロップダウンメニュー > [デバイス（Devices）] > [デバイスの追加（Add Device）] ダイアログボックス • **[デバイス（Devices）] > [デバイス管理（Device Management）]** > [クラスタ（Cluster）] タブ > [全般（General）] 領域 > [クラスタの登録ステータス（Cluster Registration Status）] > [現在のクラスタの概要（Current Cluster Summary）] リンク > [クラスタステータス（Cluster Status）] ダイアログボックス サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：暗号化と VPN	
SSL ハードウェア アクセラレーション	追加の FTD デバイスが SSL ハードウェア アクセラレーションをサポートするようになりました。また、このオプションはデフォルトで有効になっています。 バージョン 6.3.0 にアップグレードすると、対象デバイスの SSL ハードウェア アクセラレーションが自動的に有効になります。トラフィックを復号せずに SSL ハードウェア アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。トラフィックを復号しないデバイスでは SSL ハードウェア アクセラレーションを無効に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：Firepower 2100 シリーズ、Firepower 4100/9300
RA VPN：RADIUS ダイナミック認証または認可変更（CoA）	ダイナミック アクセス コントロール リスト（ACL）またはユーザーごとの ACL 名を使用する RA VPN のユーザー認可のために、RADIUS サーバーを使用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：FTD

機能	説明
RA VPN：二要素認証	Firepower Threat Defense で、Cisco AnyConnect セキュア モビリティ クライアントを使用する RA VPN ユーザーの二要素認証をサポートするようになりました。二要素認証プロセスでは、次の要素がサポートされています。 • 第 1 要素：任意の RADIUS または LDAP/AD サーバー • 第 2 要素：RSA トークンまたは DUO パスコードがモバイルにプッシュされる FTD の Duo 多要素認証（MFA）の詳細については、Duo セキュリティ Web サイトの『CiscoFirepower Threat Defense (FTD) VPN with AnyConnect』のドキュメントを参照してください。 サポートされるプラットフォーム：FTD
セキュリティ ポリシー	

機能	説明
Firepower Threat Defense サービスポリシー	Firepower Threat Defense サービスポリシーをアクセス コントロール ポリシーの高度なオプションの一部として設定できるようになりました。特定のトラフィッククラスにサービスを適用するには、FTD サービスポリシーを使用します。 サポートされる機能は次のとおりです。 • TCP ステート バイパス • TCP シーケンス番号のランダム化 • パケットの存続可能時間（TTL）値のカウントダウン • デッド接続検出 • トラフィッククラスおよびクライアントごとの最大接続数および最大初期接続数の制限設定 • 初期接続、ハーフクローズ接続、およびアイドル接続のタイムアウト （注） バージョン 6.3.0 よりも前では、接続関連のサービスルールは TCP_Embryonic_Conn_Limit と TCP_Embryonic_Conn_Timeout の事前定義の FlexConfig オブジェクトを使用して設定できました。これらのオブジェクトを削除し、FTD サービスポリシーでルールを作り直す必要があります。これらの接続関連機能（**set connection** コマンド）の実装にカスタム FlexConfig オブジェクトを作成した場合は、それらのオブジェクトも削除し、FTD サービスポリシー経由で機能を実装する必要があります。これを行わないと、展開の問題が発生する可能性があります。 『Firepower Management Center Configuration Guide』の「*Threat Defense Service Policies*」の章には、サービスポリシーと FlexConfig やその他の機能との関係について詳細が記載されています。 新規/変更されたページ：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > [ポリシーの編集/作成（edit/create policy）] > [詳細（Advanced）] タブ > [Threat Defense サービスポリシー（Threat Defense Service Policy）] サポートされるプラットフォーム：FTD

機能	説明
URL カテゴリおよびレピュテーション データの更新間隔	**アップグレードの影響。** URL データを強制的に期限切れにすることができるようになりました。セキュリティとパフォーマンスのトレードオフがあります。間隔を短くすると、現在のデータをより多く使用することになり、間隔を長くすると、ユーザーによる Web ブラウジングを高速化できます。 Cisco TAC と連携して URL フィルタリング キャッシュのタイムアウト値を変更している場合、アップグレードによってその値が変更される可能性があります。それ以外では、この設定はデフォルトでは無効になっています（現在の動作）。つまり、キャッシュされた URL データが期限切れになることはありません。 新規/変更されたページ：**[システム（System）] > [統合（Integration）] > [Cisco CSI] > [キャッシュされた URL の期限切れ（Cached URLs Expire）]** 設定 サポートされるプラットフォーム：FMC
イベントロギングおよび分析	
Cisco Security Packet Analyzer 統合	Cisco Security Packet Analyzer と統合すると、イベントを調べて分析の結果を表示したり、詳細な分析のために結果をダウンロードしたりできます。 新規/変更されたページ： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）] サポートされるプラットフォーム：FMC

機能	説明
コンテキスト クロス起動	ダッシュボードまたはイベント ビューアでイベントを右クリックすると、事前定義またはカスタマイズされた、パブリックまたはプライベートURLベースのリソースの関連情報を検索できます。 新規/変更されたページ：**[分析（Analysis）] > [詳細（Advanced）] > [コンテキスト相互起動（Contextual Cross-Launch）]** サポートされるプラットフォーム：FMC
ユニファイド syslog の設定	**アップグレードの影響。** バージョン6.3.0では、システムがSyslogを介して接続イベントと侵入イベントをログに記録する方法が変更され、一元化されています。 以前は、イベントのタイプに応じて、複数の場所で syslog を使用してイベントロギングを設定していました。アクセスコントロール ポリシーで syslog メッセージングを設定できるようになりました。これらの設定は、アクセス制御、SSL、プレフィルタ、侵入ポリシーのほか、セキュリティ インテリジェンスの接続入イベントと侵入イベントのロギングに影響を与えます。 アップグレードによって接続イベント ログの既存の設定が変更されることはありません。ただし、Syslog 経由では「期待されなかった」侵入イベントの受信が突然開始される可能性があります。これは、侵入ポリシーがアクセス コントロール ポリシーで指定された宛先に syslog イベントを送信するようになったためです。（以前は、外部ホストではなく、管理対象デバイス自体の syslog にイベントを送信するように侵入ポリシーで syslog アラートを設定できました）。 FTD デバイスでは、一部の syslog プラットフォーム設定が接続イベントと侵入イベントのメッセージに適用されるようになりました。リストについては、『Firepower Management Center Configuration Guide』の「*Platform Settings for Firepower Threat Defense*」の章を参照してください。 NGIPS デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）については、RFC 5425 で指定されている ISO 8601 タイムスタンプ形式が使用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

機能	説明
接続イベントと侵入イベントの完全な syslog メッセージ	接続イベント、セキュリティインテリジェンスイベント、および侵入イベントの syslog メッセージの形式には、次のような変更があります。 • FTD デバイスからのメッセージに、イベントタイプ ID 番号が含まれるようになりました。 • 空の値または不明な値を持つフィールドは含まれなくなったため、メッセージが短くなり、重要なデータが切り捨てられる可能性が低くなります。 • タイムスタンプでは、RFC 5425 syslog 形式で指定された ISO 8601 タイムスタンプ形式が使用されるようになりました（FTD の場合はオプションで、従来の場合は必須）。 サポートされるプラットフォーム：すべて
FTD デバイスのその他の syslog の改善	TCP または UDP プロトコルを使用して、同じ IP アドレスを介して、同じインターフェイス（データまたは管理）からすべての syslog メッセージを送信できます。セキュアな syslog はデータ ポートでのみサポートされていることに注意してください。また、メッセージのタイムスタンプに RFC 5424 形式を使用することもできます。 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	
承認された顧客向けのエクスポート管理機能	スマート アカウントで制限付き機能を使用する資格を持たない顧客は、期間ベースのライセンスを承認を受けて購入することができます。 新規/変更されたページ：**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** サポートされるプラットフォーム：FMC、FTD
承認された顧客向けの特定のライセンス予約	顧客は特定のライセンスの予約機能を使用して、エアギャップ ネットワークにスマート ライセンスを展開できます。FMC は、Cisco Smart Software Manager または Smart Software サテライトサーバーにアクセスせずに、指定した期間中に仮想アカウントからライセンスを予約します。 新規/変更されたページ：**[システム（System）]** > **[ライセンス（Licenses）]** > **[特定のライセンス（Specific Licenses）]** サポートされるプラットフォーム：FMC、FTD（ISA 3000 を除く）

機能	説明
SNMP ホストの IPv4 範囲、サブネット、および IPv6 のサポート	IPv4 範囲、IPv4 サブネット、および IPv6 ホスト ネットワーク オブジェクトを使用して、Firepower Threat Defense デバイスにアクセスできる SNMP ホストを指定できるようになりました。 新規/変更されたページ：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**> [FTD ポリシーの作成または編集（create or edit FTD policy）] > [SNMP] > [ホスト（Hosts）] タブ サポートされるプラットフォーム：FTD
完全修飾ドメイン名（FQDN）を使用したアクセス制御	完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを作成して、これらのオブジェクトをアクセス制御ルールとプレフィルタ ルールで使用できるようになりました。FQDN オブジェクトを使用するには、DNS サーバー グループと DNS プラットフォームも設定して、システムがドメイン名を解決できるようにする必要があります。 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）]** > **[ネットワーク（Network）]** • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[DNSサーバーグループ（DNS Server Group）]** • **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** > [FTDポリシーの作成または編集（create or edit FTD policy）] > [DNS] サポートされるプラットフォーム：FTD

機能	説明
FMC の CLI	FMC の CLI では、いくつかの基本的なコマンド（パスワードの変更、バージョンの表示、再起動など)がサポートされています。デフォルトでは、FMC CLI は無効になっており、SSH を使用して FMC にログインすると、Linux シェルにアクセスします。 新規/変更されたクラシック CLI コマンド：**system lockdown-sensor** コマンドは **system lockdown** に変更されています。このコマンドは、デバイスと FMC の両方で動作するようになりました。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）] > [CLI アクセスの有効化（Enable CLI Access）]** チェックボックス サポートされるプラットフォーム：FMC（FMCv を含む）
デバイス設定のコピー	デバイス設定とポリシーを 1 つのデバイスから別のデバイスにコピーできます。 新規/変更されたページ：**[デバイス（Devices）]>[デバイス管理（Device Management）]**>[デバイスの編集（edit the device）] > [全般（General）] 領域 > [デバイス設定の取得/プッシュ（Get/Push Device Configuration）] アイコン サポートされるプラットフォーム：FMC
FTD デバイス設定のバックアップ/復元	FMC Web インターフェイスを使用して、一部の FTD デバイスの設定をバックアップできます。 新規/変更されたページ：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]** 新規/変更された CLI コマンド： **restore** サポートされるプラットフォーム：すべての物理 FTD デバイス、VMware 向け FTDv

機能	説明
展開タスクをスケジュールするときに最新のデバイスへの展開をスキップ	**アップグレードの影響。** 設定変更を展開するタスクをスケジュールするときに、**最新のデバイスへの展開をスキップする**ことを選択できるようになりました。このパフォーマンス強化設定はデフォルトで有効になっています。 アップグレード プロセスでは、既存のスケジュール済みタスクでこのオプションが自動的に有効になります。スケジュールされた展開を最新のデバイスに強制的に適用するには、スケジュールされたタスクを編集する必要があります。 新規/変更されたページ：**[システム（System）] > [ツール（Tools）] > [スケジューリング（Scheduling）]** > [タスクの追加または編集（add or edit a task）] で [展開ポリシー（Deploy Policies）] の [ジョブタイプ（Job Type）] を選択 サポートされるプラットフォーム：FMC
新しいヘルス モジュール	新しいヘルス モジュールは、次の場合にアラートを表示します。 • **デバイスでの脅威データの更新**：管理対象デバイスで脅威特定データの更新に失敗しました。 • **レルム**：ユーザーがダウンロードされずに、FMC にレポートされたか、または、FMC が認識していないレルムに対応するドメインにユーザーがログインしました。 新規/変更されたページ： • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]** • **[システム（System）] > [ヘルス（Health）] > [モニター（Monitor）]** サポートされるプラットフォーム：FMC
設定可能なパケット キャプチャ サイズ	最大 10 GB のパケット キャプチャを保存できるようになりました。 新規/変更された CLI コマンド：**file-size**、**show capture** サポートされるプラットフォーム：Firepower 4100/9300
セキュリティと強化	

機能	説明
HTTPS 証明書	現在、システムとともに提供されるデフォルトの HTTPS サーバー クレデンシャルは 3 年で期限が切れます。 バージョン 6.3.0 にアップグレードされる前に生成されたデフォルトのサーバー証明書をアプライアンスが使用している場合、サーバー証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバー証明書を使用している場合、システムはその証明書を更新する機能を提供しています。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）] > [HTTPS 証明書の更新（Renew HTTPS Certificate）]** ボタン 新規/変更されたクラシック CLI コマンド：**show http-cert-expire-date**、**system renew-http-cert***new_key* サポートされるプラットフォーム：物理 FMC、7000/8000 シリーズ デバイス
向上したログイン セキュリティ	**アップグレードの影響。** ログイン セキュリティを向上させるために FMC ユーザー設定が追加されました。 • **成功したログインを追跡**：特定の期間内に各 FMC アカウントで実行された、成功したログインの回数を追跡します。 • **パスワード再利用の制限**：再利用を防止するために、FMC ユーザーのパスワード履歴を追跡します。 • **ログイン失敗の最大数**と**一時的にユーザーをロックアウトする分単位の時間の設定**：FMC ユーザーが一時的にブロックされる前に、そのユーザーが誤った Web インターフェイス ログイン クレデンシャルを連続して入力できる回数を制限します。 セキュアな SSH アクセスのためにサポートされる暗号と暗号化アルゴリズムのリストも更新されました。暗号エラーのために SSH クライアントが Firepower アプライアンスとの接続に失敗する場合は、クライアントを最新バージョンに更新してください。 新規/変更されたページ： **[System] > [Configuration]** > [ユーザー設定（User Configuration）] サポートされるプラットフォーム：FMC

機能	説明
デバイスでの SSH ログイン失敗の制限	ユーザーが SSH 経由でデバイスにアクセスし、ログイン試行を 3 回続けて失敗すると、デバイスは SSH セッションを終了します。 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
Firepower Management Center REST API	
新しい REST API サービス	次の機能をサポートするために、REST API サービスが追加されました。 • サイト間 VPN トポロジ：ftds2svpns、endpoints、ipsecsettings、advancedsettings、ikesettings、ikev1ipsecproposals、ikev1policies、ikev2ipsecproposals、ikev2policies • HA デバイスフェールオーバー：failoverinterfacemacaddressconfigs、monitoredinterfaces サポートされるプラットフォーム：FMC
バルク オーバーライド	特定のオブジェクトに対してバルク オーバーライドを実行できるようになりました。完全なリストについては、『Cisco Firepower Management Center REST API Quick Start Guide』を参照してください。

FMC バージョン 6.3.0 パッチの新機能

表 *19*：

機能	説明
バージョン 6.3.0.4 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 6.3.0.4 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 にアップグレードすると、この修正が無効になります。これは、バージョン 6.4.0.2 で再度修正されました。
バージョン 6.3.0.4 [ISE接続ステータスのモニター（ISE Connection Status Monitor）] モジュール	新しいモジュールである [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。 バージョン 6.4.0 にアップグレードすると、このモジュールが無効になります。サポートは、バージョン 6.4.0.2 で再開されています。 新規/変更された画面：[システム（System）]>[ポリシー（Policy）]>ポリシーの作成または編集>[ISE接続ステータスのモニター（ISE Connection Status Monitor）]
バージョン 6.3.0.3 2048 ビットの証明書キーが必要になりました（セキュリティ強化）	AMP for Endpoints や Cisco Threat Intelligence Detector（TID）などの外部データソースへのセキュアな接続を行う場合、FMC では、少なくとも 2048 ビット長のキーを使用したサーバー証明書の生成が必要になりました。以前に 1024 ビットキーを使用して生成された証明書は機能しなくなります。 接続できない場合は、データソースでサーバー証明書を再生成します。必要に応じて、データソースへの FMC 接続を再設定します。

機能	説明
バージョン 6.3.0.1 EMS 拡張機能のサポート	**アップグレードの影響。** バージョン 6.3.0.1 では EMS 拡張機能のサポートが再導入されます。これは、バージョン 6.2.3.8/6.2.3.9 で導入されましたが、バージョン 6.3.0 には含まれていませんでした。 [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、再び 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す。EMS 拡張機能は、RFC 7627 によって定義されています。 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。ベストプラクティスは展開全体をアップグレードすることですが、デバイスにパッチを適用するだけでも、この機能はサポートされます。

FMC バージョン 6.3.0 で廃止された機能

表 20 :

機能	アップグレードの影響	説明
復号化のための EMS 拡張機能のサポート	パッチまたはアップグレードを行うまで、EMS 拡張機能のサポートは中止されます。	バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが中止されます。つまり、[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（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、RFC 7627 によって定義されています。 Firepower Management Center 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。Firepower Management Center をバージョン 6.3.0 にアップグレードしても、サポートされるバージョンがデバイスで実行されていれば、サポートは中止されません。ただし、デバイスをバージョン 6.3.0 にデバイスをアップグレードすると、サポートは中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。

機能	アップグレードの影響	説明
パッシブおよびインライン タップ インターフェイスの復号化	システムは、パッシブ展開でトラフィックの復号化を停止します。	バージョン 6.3.0 では、パッシブ モードまたはインライン タップ モードのインターフェイスでの復号化トラフィックは、GUI を介して設定することはできますが、サポートされなくなりました。暗号化されたトラフィックのインスペクションは必然的に制限されます。
デフォルトの DNS グループの FlexConfig オブジェクト	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 6.3.0 では、FMC を使用する Firepower Threat Defense の場合、次の FlexConfig オブジェクトが廃止されます。 • Default_DNS_Configure 関連するテキストオブジェクト： • defaultDNSNameServerList • defaultDNSParameters これらによって、デフォルト DNS グループを設定できました。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバーを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。 FTD プラットフォーム設定ポリシーで、データインターフェイスの DNS を設定できるようになりました（**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）]** > [FTD ポリシーの作成または編集（Create or edit FTD policy）] > [DNS]）。

機能	アップグレードの影響	説明
初期接続制限およびタイムアウト FlexConfig オブジェクト	アップグレード後の展開の問題。 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 6.3.0 では、FMC を使用する Firepower Threat Defense の場合、次の FlexConfig オブジェクトが廃止されます。 • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 関連するテキストオブジェクト： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout これらによって、初期接続制限およびタイムアウトを設定して SYN フラッドサービス妨害（DoS）攻撃から保護できました。 FTD サービスポリシーでこれらの機能を設定できるようになりました（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [詳細（Advanced）] タブ > [Threat Defense サービスポリシー（Threat Defense Service Policy）]）。 **注意** **set connection** コマンドを使用して接続関連サービスルールを実装した場合は、関連付けられたオブジェクトを削除し、FTD サービスポリシーを使用して機能を実装する必要があります。これを行わないと、展開の問題が発生する可能性があります。

機能	アップグレードの影響	説明
Web インターフェイスの変更	なし	

機能	アップグレードの影響	説明
		バージョン 6.3.0 では、次のメニューオプションが変更されています。 **[分析（Analysis）] > [詳細（Advanced）] > [Whois]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [Whois]** **[分析（Analysis）] > [詳細（Advanced）] > [位置情報（Geolocation）]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [位置情報（Geolocation）]** **[分析（Analysis）] > [詳細（Advanced）] > [URL]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [URL]** **[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]** は次に変更されました。 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]** **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]** は次に変更されました。 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムテーブル（Custom Tables）]** **[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）]** は次に変更されました。 **[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）]**

機能	アップグレードの影響	説明
		[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）] は次に変更されました。 **[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third Party Vulnerabilities）]**
VMware 5.5 のホスティング	Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードします。	バージョン 6.3.0 以降の仮想展開は VMware vSphere/VMware ESXi 5.5 でテストされていません。これには、FMCv、FTDv、および VMware 向け NGIPSv が含まれます。
Firepower ソフトウェアを搭載した ASA 5506-X シリーズおよび ASA 5512-X デバイス	アップグレードは禁止されています。	ASA 5506-X、5506H-X、5506W-X、および 5512-X のデバイスでは、Firepower ソフトウェア（Firepower Threat Defense と ASA FirePOWER の両方）のバージョン 6.3.0 以降にアップグレードしたり、このバージョンを新規インストールすることはできません。

バージョン 6.2.3

FMC バージョン 6.2.3 の新機能

表 *21 :*

機能	説明
ハードウェアおよび仮想アプライアンス	

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**	
Firepower 4100/9300 の SSL ハードウェア アクセラレーション	FTD を搭載した Firepower 4100/9300 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 暗号化および復号のアクセラレーションをサポートするようになりました。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。 （注） この機能は、バージョン 6.4.0 以降では TLS 暗号化アクセラレーションに名前が変更されました。 サポートされるプラットフォーム：Firepower 4100/9300

機能	説明
証明書の登録の改善	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。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：ハイアベイラビリティとクラスタリング	
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、ユーザー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 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。 サポートされるプラットフォーム：FMC

機能	説明
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
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。 サポートされるプラットフォーム：FMC
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。 高可用性デバイス、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、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。 新規/変更された画面：**[システム（System）] > [更新（Updates）]** サポートされるプラットフォーム：FMC

機能	説明
Firepower Threat Defense の有用性	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。 サポートされるプラットフォーム：FTD
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。 サポートされるプラットフォーム：FMC
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。 サポートされるプラットフォーム：FTD を搭載した FMC
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。 サポートされるプラットフォーム：FTD
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。 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。 サポート対象プラットフォーム：FMC

機能	説明
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。 初期設定では、デフォルトで Web 分析トラッキングに登録されますが、その後はいつでも登録を変更できます。アップグレードでは、Web 分析トラッキングに登録または再登録することもできます。 サポート対象プラットフォーム：FMC
パフォーマンス	
FTD デバイスの Snort の再起動が減少	バージョン 6.2.3 では、FTD 設定の変更による、FTD デバイスの Snort プロセスの再起動が減少します。 FMC 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、管理対象デバイスでのトラフィック処理方法によっては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、警告が出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：FTD
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。

機能	説明
ISE pxGrid ディスカバリの高速化	高可用性の ISE pxGrid 展開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、新しいアクティブな pxGrid をより迅速に検出できるようになりました。
FMC REST API	
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 モニター

FMC バージョン 6.2.3 パッチの新機能

表 *22*：

機能	説明
バージョン 6.2.3.13 FTD NAT ポリシーでのルールの競合の検出	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。 サポートされているプラットフォーム：Firepower Threat Defense
バージョン 6.2.3.8 EMS 拡張機能のサポート	[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。 （注） バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよび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。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ます。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。 サポートされるプラットフォーム：すべて

機能	説明
バージョン 6.2.3.7 FTD の TLS v1.3 ダウングレード CLI コマンド	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、モニター対象ネットワーク内のユーザーが 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、Cisco Firepower Threat Defense コマンド リファレンスで **system support** コマンド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。 サポートされているプラットフォーム：Firepower Threat Defense
バージョン 6.2.3.3 クラスタリングを使用したサイト間 VPN	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。サイト間 VPN は、中央集中型機能です。制御ユニットのみが 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

FMC バージョン 6.2.3 で廃止された機能

表 *23*：

機能	アップグレードの影響	説明
レポートの結果の新しい制限	アップグレードすることで、レポートの設定を変更できます。	バージョン 6.2.3 では、使用できる、またはレポートセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。 HTML または CSV レポートセクションの新しい制限は次のとおりです。 • 棒グラフと円グラフ：100（上部または下部） • テーブルビュー：400,000 • 詳細ビュー：1,000 PDF レポートセクションの新しい制限は次のとおりです。 • 棒グラフと円グラフ：100（上部または下部） • テーブルビュー：100,000 • 詳細ビュー：500 Firepower Management Center をアップグレードする前に、レポートテンプレート内のセクションで最大HTMLまたはCSVよりも大きい結果数を指定する場合は、アップグレードプロセスが設定を新しい最大値に下げます。 PDF レポートを生成するレポートテンプレートの場合、テンプレート セクションの PDF の制限を超えると、アップグレード プロセスは出力形式を HTML に変更します。PDF の生成を続行するには、結果数を PDF の最大に下げます。アップグレード後にこれを行った場合、出力形式の設定を PDF に戻します。
AMP for Networks による動的分析用の期限切れ 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。	2018 年 6 月 15 日、一部の AMP for Networks 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（178 ページ）を参照してください。

FMC バージョン 6.2.3 パッチで廃止された機能

表 24：

機能	アップグレードの影響	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。	2018 年 6 月 15 日、一部の AMP for Networks 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 （178 ページ） を参照してください。

日付ベースの機能

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 *25* : 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。	

リリース日

表 *26* : バージョン *7.1.0* の日付

バージョン	ビルド	日付	プラットフォーム
7.1.0	90	2021 年 12 月 1 日	すべて（All）

表 *27* : バージョン *7.0.0/7.0.x* の日付

バージョン	ビルド	日付	プラットフォーム
7.0.1	84	2021-10-07	すべて（All）
7.0.0	94	2021 年 5 月 26 日	すべて

表 *28* : バージョン *7.0.0/7.0.x* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
7.0.0.1	15	2021 年 7 月 15 日	すべて

表 *29* : バージョン *6.7.0* の日付

バージョン	ビルド	日付	プラットフォーム
6.7.0	65	2020 年 11 月 2 日	すべて

表 *30* : バージョン *6.7.0* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.7.0.2	24	2021 年 5 月 11 日	すべて（All）
6.7.0.1	13	2021 年 3 月 24 日	すべて

表 *31* : バージョン *6.6.0/6.6.x* の日付

バージョン	ビルド	日付	プラットフォーム
6.6.5	81	2021 年 8 月 3 日	すべて（All）
6.6.4	64	2021 年 4 月 29 日	Firepower 1000 シリーズ
	59	2021 年 4 月 26 日	FMC/FMCv Firepower 1000 シリーズを除くすべてのデバイス
6.6.3	80	2020 年 3 月 11 日	すべて
6.6.1	91	2020 年 9 月 20 日	すべて
	90	2020 年 9 月 8 日	—

バージョン	ビルド	日付	プラットフォーム
6.6.0	90	2020 年 5 月 8 日	Firepower 4112
		2020 年 4 月 6 日	FMC/FMCv Firepower 4112 を除くすべてのデバイス

表 *32* : バージョン *6.6.0/6.6.x* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.6.5.1	15	2021 年 12 月 6 日	すべて（All）
6.6.0.1	7	2020 年 7 月 22 日	すべて

表 *33* : バージョン *6.5.0* の日付

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.5.0	123	2020 年 2 月 3 日	FMC/FMCv	FMC/FMCv
6.5.0	120	2019 年 10 月 8 日	—	—
6.5.0	115	2019 年 9 月 26 日	すべてのデバイス	すべてのデバイス

表 *34* : バージョン *6.5.0* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.5.0.5	95	2021 年 2 月 9 日	すべて
6.5.0.4	57	2020 年 3 月 2 日	すべて
6.5.0.3	30	2020 年 2 月 3 日	利用できなくなりました。
6.5.0.2	57	2019 年 12 月 19 日	すべて

バージョン	ビルド	日付	プラットフォーム
6.5.0.1	35	2019 年 11 月 20 日	利用できなくなりました。

表 *35* : バージョン *6.4.0* の日付

バージョン	ビルド	日付	プラットフォーム
6.4.0	113	2020 年 3 月 3 日	FMC/FMCv
6.4.0	102	2019 年 6 月 20 日	Firepower 4115、4125、4145 SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300
		2019 年 6 月 13 日	Firepower 1010、1120、1140
		2019 年 4 月 24 日	Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 シリーズ NGIPSv

表 *36* : バージョン *6.4.0* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.4.0.13	57	2021 年 12 月 2 日	すべて
6.4.0.12	112	2021 年 5 月 12 日	すべて（All）
6.4.0.11	11	2021 年 1 月 11 日	すべて（All）

バージョン	ビルド	日付	プラットフォーム
6.4.0.10	95	2020 年 10 月 21 日	すべて
6.4.0.9	62	2020 年 5 月 26 日	すべて
6.4.0.8	28	2020 年 1 月 29 日	すべて
6.4.0.7	53	2019 年 12 月 19 日	すべて
6.4.0.6	36	2019 年 10 月 16 日	利用できなくなりました。
6.4.0.5	23	2019 年 9 月 18 日	すべて
6.4.0.4	34	2019 年 8 月 21 日	すべて
6.4.0.3	29	2019 年 7 月 17 日	すべて
6.4.0.2	35	2019 年 7 月 3 日	FMC/FMCv FTD/FTDv（FirePOWER 1000 シリーズ以外）
	34	2019 年 6 月 27 日	—
		2019 年 6 月 26 日	Firepower 7000/8000 シリーズ ASA FirePOWER NGIPSv

バージョン	ビルド	日付	プラットフォーム
6.4.0.1	17	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 6 月 20 日	Firepower 4115、4125、4145 SM-40、SM-48、および SM-56 モジュールを搭載した Firepower 9300
		2019 年 5 月 15 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv Firepower 2110、2120、2130、2140 Firepower 4110、4120、4140、4150 SM-24、SM-36、および SM-44 モジュールを搭載した Firepower 9300 ASA 5508-X、5515-X、5516-X、5525-X、5545-X、5555-X ASA 5585-X-SSP-10、-20、-40、-60 ISA 3000 FTDv Firepower 7000/8000 シリーズ NGIPSv

表 ***37 :*** バージョン ***6.3.0*** の日付

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.3.0	85	2019 年 1 月 22 日	Firepower 4100/9300	Firepower 4100/9300
6.3.0	84	2018 年 12 月 18 日	FMC/FMCv ASA FirePOWER	—

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.3.0	83	2019 年 6 月 27 日	—	FMC 1600、2600、4600
		2018 年 12 月 3 日	Firepower 4100/9300 を除くすべての FTD デバイス Firepower 7000/8000 NGIPSv	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv Firepower 4100/9300 を除くすべてのデバイス

表 *38* : バージョン *6.3.0* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.3.0.5	35	2019 年 11 月 18 日	Firepower 7000/8000 シリーズ NGIPSv
	34	2019 年 11 月 18 日	FMC/FMCv すべての FTD デバイス ASA FirePOWER
6.3.0.4	44	2019 年 8 月 14 日	すべて
6.3.0.3	77	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 5 月 1 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス
6.3.0.2	67	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 3 月 20 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス

バージョン	ビルド	日付	プラットフォーム
6.3.0.1	85	2019 年 6 月 27 日	FMC 1600、2600、4600
		2019 年 2 月 18 日	FMC 750、1000、1500、2000、2500、3500、4000、4500 FMCv すべてのデバイス

表 *39* : バージョン *6.2.3* の日付

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.2.3	113	2020 年 6 月 1 日	FMC/FMCv	FMC/FMCv
6.2.3	111	2019 年 11 月 25 日	—	FTDv: AWS, Azure
6.2.3	110	2019 年 6 月 14 日	—	—
6.2.3	99	2018 年 9 月 7 日	—	—
6.2.3	96	2018 年 7 月 26 日	—	—
6.2.3	92	2018 年 7 月 5 日	—	—
6.2.3	88	2018 年 6 月 11	—	—
6.2.3	85	2018 年 4 月 9 日	—	—
6.2.3	84	2018 年 4 月 9 日	Firepower 7000/8000 シリーズ NGIPSv	—

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
6.2.3	83	2018 年 4 月 2 日	FTD/FTDv ASA FirePOWER	FTD：物理プラットフォーム FTDv：VMware、FVM Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3	79	2018 年 3 月 29 日	—	—

表 *40*：バージョン *6.2.3* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.2.3.17	30	2021 年 6 月 21 日	すべて
6.2.3.16	59	2020 年 7 月 13 日	すべて
6.2.3.15	39	2020 年 2 月 5 日	FTD/FTDv
	38	2019 年 9 月 18 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.14	41	2019 年 7 月 3 日	すべて
	36	2019 年 6 月 12 日	すべて
6.2.3.13	53	2019 年 5 月 16 日	すべて
6.2.3.12	80	2019 年 4 月 17 日	すべて

バージョン	ビルド	日付	プラットフォーム
6.2.3.11	55	2019 年 3 月 17 日	すべて
	53	2019 年 3 月 13 日	—
6.2.3.10	59	2019 年 2 月 7 日	すべて
6.2.3.9	54	2019 年 1 月 10 日	すべて
6.2.3.8	51	2019 年 1 月 2 日	利用できなくなりました。
6.2.3.7	51	2018 年 11 月 15 日	すべて
6.2.3.6	37	2018 年 10 月 10 日	すべて
6.2.3.5	53	2018 年 11 月 6 日	FTD/FTDv
	52	2018 年 12 月 9 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
6.2.3.4	54	2018 年 8 月 13 日	すべて
6.2.3.3	76	2018 年 7 月 11 日	すべて
6.2.3.2	46	2018 年 6 月 27 日	すべて
	54	2018 年 6 月 6 日	—

バージョン	ビルド	日付	プラットフォーム
6.2.3.1	47	2018 年 6 月 28 日	すべて
	45	2018 年 6 月 21 日	—
	43	2018 年 5 月 2 日	—

表 *41* : バージョン *6.2.2* の日付

バージョン	ビルド	日付	プラットフォーム
6.2.2	81	2017 年 9 月 5 日	すべて

表 *42* : バージョン *6.2.2* のパッチの日付

バージョン	ビルド	日付	プラットフォーム
6.2.2.5	57	2018 年 11 月 27 日	すべて
6.2.2.4	43	2018 年 9 月 21 日	FTD/FTDv
	34	2018 年 7 月 9 日	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018 年 6 月 15 日	—
6.2.2.3	69	2018 年 6 月 19 日	すべて
	66	2018 年 4 月 24 日	—
6.2.2.2	109	2018 年 2 月 28 日	すべて

バージョン	ビルド	日付	プラットフォーム
6.2.2.1	80	2017 年 12 月 5 日	Firepower 2100 シリーズ
	78	2017 年 11 月 20 日	—
	73	2017 年 11 月 6 日	FMC/FMCv Firepower 2100 シリーズを除くすべてのデバイス

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。