

Cisco Secure Firewall Management Center の 新機能（リリース別）

初版：2021年3月26日

最終更新：2022年6月6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。

お客様が導入した（またはオンプレミスの）新しい Management Center で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、通常は Management Center とデバイスの両方で最新のリリースが必要です。デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、Management Center の最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。このドキュメントでは、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

推奨リリース

推奨リリース：バージョン 7.2.4.x

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パッチを含む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。

Management Center バージョン 7.3 の新機能

新機能

表 1: Management Center バージョン 7.3.1 の新機能

新機能	説明
Cisco Secure Firewall 3105。	Cisco Secure Firewall 3105 を導入しました。 必要最低限の Threat Defense : 7.3.1

表 2: Management Center バージョン 7.3.0 の新機能

新機能	説明
プラットフォーム	
Management Center Virtual 300 for KVM。	KVM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。 必要最低限の Threat Defense : 任意
Cisco Secure Firewall 4100 のネットワークモジュール	次のネットワークモジュールを使用して Cisco Secure Firewall 4100 を管理できるようになりました。 <ul style="list-style-type: none"> • 2-port 100G Network Module (FPR-NM-2X100G) 必要最低限の Threat Defense : 7.3
ISA 3000 システム LED によるシャットダウンのサポート。	この機能のサポートが再開されました。ISA 3000 をシャットダウンすると、システム LED が消灯します。その後、少なくとも 10 秒間待ってからデバイスの電源を切ってください。この機能はバージョン 7.0.5 で導入されましたが、バージョン 7.1 ~ 7.2 で一時的に廃止になりました。
インターフェイス	

新機能	説明
仮想アプライアンスの IPv6 サポート。	<p>Threat Defense Virtual および Management Center Virtual は、次の環境で IPv6 をサポートするようになりました。</p> <ul style="list-style-type: none"> • AWS • Azure • OCI • KVM • VMware <p>詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドおよびCisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。</p>
VTI のループバック インターフェイスサポート。	<p>静的および動的 VTI VPN トンネルの冗長性のためにループバック インターフェイスを設定できるようになりました。ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア インターフェイスであり、IPv4 および IPv6 アドレスを持つ複数の物理インターフェイスを介して到達できます。</p> <p>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 (Devices)]>[インターフェイス (Interfaces)]>[インターフェイスの追加 (Add Interfaces)]>[ループバックインターフェイスの追加 (Add Loopback Interface)]</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure Loopback Interfaces」を参照してください。</p>
冗長マネージャアクセス データ インターフェイス。	<p>マネージャアクセスにデータインターフェイスを使用する場合、プライマリインターフェイスがダウンしたときに管理機能を引き継ぐよう、セカンダリインターフェイスを構成できます。デバイスは、SLA モニタリングを使用して、スタティックルートの実行可能性と、両方のインターフェイスを含む ECMP ゾーンを追跡し、管理トラフィックで両方のインターフェイスが使用できるようにします。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)]>[デバイス管理 (Device Management)]>[デバイス (Device)]>[管理 (Management)] • [デバイス (Devices)]>[デバイス管理 (Device Management)]>[デバイス (Devices)]>[インターフェイス (Interfaces)]>[マネージャアクセス (Manager Access)] <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure a Redundant Manager Access Data Interface」を参照してください。</p>

新機能	説明
IPv6 DHCP。	<p>IPv6 アドレッシングの次の機能がサポートされるようになりました。</p> <ul style="list-style-type: none"> • DHCPv6 アドレスクライアント：Threat Defense は、DHCPv6 サーバーから IPv6 グローバルアドレスとオプションのデフォルトルートを取得します。 • DHCPv6 プレフィックス委任クライアント：Threat Defense は DHCPv6 サーバーから委任プレフィックスを取得します。これらのプレフィックスを使用して他の Threat Defense インターフェイスのアドレスを設定し、ステートレスアドレス自動設定 (SLAAC) クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータアドバタイズメント。 • DHCPv6 ステートレスサーバー：SLAAC クライアントが Threat Defense に情報要求 (IR) パケットを送信すると、Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Threat Defense は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。 <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)]>[デバイス管理 (Device Management)]> [デバイス (Device)]>[インターフェイス (Interfaces)]>[インターフェイス (Interface)]> [IPv6]> [DHCP] • [オブジェクト (Objects)]>[オブジェクト管理 (Object Management)]> [DHCP IPv6 プール (DHCP IPv6 Pool)] <p>新規/変更された CLI コマンド：show bgp ipv6 unicast、show ipv6 dhcp、show ipv6 general-prefix</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure the IPv6 Prefix Delegation Client」、「BGP」 および「Configure the DHCPv6 Stateless Server」を参照してください。</p>

新機能	説明
<p>Azure ゲートウェイロードバランサの Threat Defense Virtual のペアプロキシ VXLAN</p>	<p>Azure ゲートウェイロードバランサで使用するために、Azure の Threat Defense Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。デバイスは、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。</p> <p>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 (Devices)]>[インターフェイス (Interfaces)]>[インターフェイスの追加 (Add Interfaces)]>[VNI インターフェイス (VNI Interface)]</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure VXLAN Interfaces」を参照してください。</p>
<p>固定ポートの前方誤り訂正 (FEC) のデフォルトが変更されました。</p>	<p>Cisco Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB 以上の SR、CSR、および LR トランシーバのデフォルトタイプが第 74 条 FC-FEC ではなく第 108 条 RS-FEC に設定されるようになりました。</p> <p>詳細については、デバイスコンフィギュレーションガイドの「Interface Overview」を参照してください。</p>
<p>高可用性/拡張性</p>	
<p>KVM および Azure 向け Management Center Virtual の高可用性。</p>	<p>KVM および Azure 向け Management Center Virtual の高可用性がサポートされるようになりました。</p> <p>Threat Defense の展開では、同じようにライセンスされた 2 つの管理センターと、管理対象デバイスごとに 1 つの Threat Defense 権限が必要です。たとえば、FMCv10 高可用性ペアで 10 台のデバイスを管理するには、2 個の FMCv10 権限と 10 個の Threat Defense 権限が必要です。バージョン 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。</p> <p>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)</p> <p>詳細については、Cisco Secure Firewall Management Center Virtual 入門ガイド、およびアドミニストレーションガイドの「High Availability」を参照してください。</p>

新機能	説明
<p>Azure 向け Threat Defense Virtual のクラスタリング。</p>	<p>Azure 向け Threat Defense Virtual を使用して、最大 16 ノードのクラスタリングを構成できるようになりました。</p> <p>新規/変更された画面 : [デバイス (Devices)] > [デバイス管理 (Device Management)]</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Clustering for Threat Defense Virtual in a Public Cloud」を参照してください。</p>
<p>Azure ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケール。</p>	<p>Azure ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケールがサポートされるようになりました。詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。</p>
<p>クラスタ化されたデバイスのバックアップと復元のサポート。</p>	<p>Management Center を使用してクラスタのバックアップを実行できるようになりました。クラスタノードを復元するには、デバイス CLI を使用する必要があります。</p> <p>新規/変更された画面 : システム (⚙️) > [ツール (Tools)] > [バックアップ/復元 (Backup/Restore)] > [管理対象デバイスのバックアップ (Managed Device Backup)]</p> <p>新規/変更された CLI コマンド : <code>restore remote-manager-backup</code></p> <p>詳細については、アドミニストレーションガイドの「Backup/Restore」を参照してください。</p>
<p>リモートアクセス VPN</p>	

新機能	説明
RA VPN ダッシュボード。	<p>デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視できるリモートアクセス VPN (RA VPN) ダッシュボードが導入されました。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できるように、ダッシュボードには次の機能があります。</p> <ul style="list-style-type: none"> • ロケーションに基づいたアクティブなユーザーセッションの可視化。 • アクティブなユーザーセッションに関する詳細情報。 • 必要に応じて、セッションを終了することによるユーザーセッションの問題の軽減。 • デバイス、暗号化タイプ、Secure Client バージョン、オペレーティングシステム、および接続プロファイルごとのアクティブなユーザーセッションの分布。 • デバイスのデバイス ID 証明書の有効期限の詳細。 <p>新規/変更された画面：[概要 (Overview)] > [ダッシュボード (Dashboards)] > [リモートアクセスVPN (Remote Access VPN)]</p> <p>詳細については、アドミニストレーションガイドの「Dashboards」を参照してください。</p>
TLS 1.3 で RA VPN 接続を暗号化します。	<p>TLS 1.3 を使用して、次の暗号で RA VPN 接続を暗号化できるようになりました。</p> <ul style="list-style-type: none"> • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 <p>Threat Defense プラットフォーム設定を使用して TLS バージョンを設定します：[デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] > [Threat Defense設定ポリシーの追加/編集 (Add/Edit Threat Defense Settings Policy)] > [SSL] > [TLSバージョン (TLS Version)]。</p> <p>この機能には、Cisco Secure Client、リリース 5 (以前は AnyConnect セキュアモビリティクライアントと呼ばれていました) が必要です。</p> <p>詳細については、デバイス コンフィギュレーションガイドの「Configure SSL Settings」を参照してください。</p>
サイト間 VPN	

新機能	説明
サイト間 VPN ダッシュボードの packets トレーサ。	<p>デバイス間の VPN トンネルのトラブルシューティングに役立つように、サイト間 VPN ダッシュボードに packets トレーサ機能を追加しました。</p> <p>[概要 (Overview)] > [ダッシュボード (Dashboards)] > [サイト間 VPN (Site to Site VPN)] を選択して、ダッシュボードを開きます。次に、調査するトンネルの横にある [表示 (View)] (👁) をクリックし、表示されるサイドペインで [packets トレーサ (Packet Tracer)] をクリックします。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Monitoring the Site-to-Site VPNs」を参照してください。</p>
サイト間 VPN を使用したダイナミック VTI のサポート。	<p>ハブアンドスポークトポロジでルートベースのサイト間 VPN を構成する場合、動的仮想トンネルインターフェイス (VTI) がサポートされるようになりました。以前は、静的 VTI のみを使用できました。</p> <p>これにより、大規模なハブアンドスポーク展開の構成が容易になります。ハブの複数のスタティック VTI 構成を単一のダイナミック VTI に置き換えることができます。また、ハブの構成を変更せずに、新しいスポークをハブに追加できます。</p> <p>新規/変更された画面：ルートベースのハブアンドスポークサイト間 VPN トポロジのハブノードエンドポイントを構成するときのオプションを更新しました。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure Endpoints for a Hub and Spoke Topology」を参照してください。</p>
Umbrella SIG 統合の改善。	<p>Threat Defense デバイスと Umbrella セキュア インターネット ゲートウェイ (SIG) の間に IPsec IKEv2 トンネルを簡単に展開できるようになりました。これにより、インターネットに向かうすべてのトラフィックを検査とフィルタリングのために Umbrella に転送できます。</p> <p>これらのトンネルを構成して展開するには、新しいタイプの静的 VTI ベースのサイト間 VPN トポロジである SASE トポロジを作成します：[デバイス (Devices)] > [VPN] > [サイト間 (Site To Site)] > [SASE トポロジ (SASE Topology)]。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Deploy a SASE Tunnel on Umbrella」を参照してください。</p>
ルーティング	

新機能	説明
<p>Management Center の Web インターフェイスから BGP の BFD を設定。</p>	<p>アップグレードの影響。</p> <p>Management Center の Web インターフェイスを使用して、BGP の Bidirectional Forwarding Detection (BFD) を設定できるようになりました。仮想ルータに属するインターフェイスでのみ BFD を有効にできることに注意してください。既存の BFD FlexConfig があり、Web インターフェイスで設定をやり直す場合は、廃止された FlexConfig を削除するまで展開できません。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [ルーティング (Routing)] > [BFD] • [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] > [BFD テンプレート (BFD Template)] • BGP ネイバー設定を構成するときに、[BFD フェールオーバー (BFD Failover)] チェックボックスが、BFD タイプ (シングルホップ、マルチホップ、自動検出、またはなし (無効)) を選択するメニューに置き換えられました。アップグレードされた Management Center の場合、古い [BFD フェールオーバー (BFD Failover)] オプションが有効になっている場合は [自動検出ホップ (auto-detect hop)] が選択され、古いオプションが無効になっている場合は [なし (none)] が選択されます。 <p>詳細については、デバイス コンフィギュレーション ガイドの「Bidirectional Forwarding Detection Routing」を参照してください。</p>
<p>VTI の IPv4 および IPv6 OSPF ルーティングのサポート。</p>	<p>VTI インターフェイスの IPv4 および IPv6 OSPF ルーティングがサポートされるようになりました。</p> <p>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)] > [ルーティング (Routing)] > [OSPF/OSFPv3] の OSPF ルーティングプロセスに VTI インターフェイスを追加できます。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「OSPF」と「Additional Configurations for VTI」を参照してください。</p>

新機能	説明
VTI の IPv4 EIGRP ルーティングのサポート。	<p>VTI インターフェイスの IPv4 EIGRP ルーティングがサポートされるようになりました。</p> <p>新規/変更された画面：VTI を EIGRP ルーティングプロセスの静的ネイバーとして定義し、VTI のインターフェイス固有の EIGRP ルーティングプロパティを設定できます。[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [ルーティング (Routing)] > [EIGRP] で VTI のサマリアドレスをアドバタイズします。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「EIGRP」と「Additional Configurations for VTI」を参照してください。</p>
ポリシーベースルーティングのためのネットワーク サービス グループの追加。	<p>最大 1024 のネットワーク サービス グループ (ポリシーベースルーティングで使用するための拡張 ACL 内のアプリケーショングループ) を設定できるようになりました。以前は、制限は 256 でした。</p>
ポリシーベースのルーティング転送アクションを設定する際の複数のネクストホップのサポート。	<p>ポリシーベースのルーティング転送アクションを設定する際に、複数のネクストホップを構成できるようになりました。トラフィックがルート基準に一致すると、システムは、成功するまで、指定した順序でトラフィックを IP アドレスに転送しようとします。</p> <p>この機能は、バージョン 7.3 以降の Management Center を備えたバージョン 7.1 以降を実行している Threat Defense デバイスで利用できます。</p> <p>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)] > [ルーティング (Routing)] > [ポリシーベースルーティング (Policy Based Routing)] > [ポリシーベースルートの追加 (Add Policy Based Route)] > [一致基準と出カインターフェイスの追加 (Add Match Criteria and Egress Interface)] の [送信先 (Send To)] メニューから [IP アドレス (IP Address)] を選択するときに、いくつかのオプションが追加されました。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure Policy-Based Routing Policy」を参照してください。</p>
<p>のアップグレード</p>	

新機能	説明
使いやすさの改善。	<p>Threat Defense アップグレードウィザードにいくつかのユーザービリティの改善を導入しました。</p> <ul style="list-style-type: none"> • ウィザードを使用して、アップグレードするデバイスを選択できるようになりました。選択したデバイス、残りのアップグレード候補、対象外のデバイス（理由付き）、アップグレードパッケージが必要なデバイスなどの間でビューを切り替えることができます。 <p>以前は、[デバイス管理（Device Management）] ページしか使用できず、プロセスの柔軟性が大幅に低くなっていました。</p> <ul style="list-style-type: none"> • ウィザードを使用して、Threat Defense アップグレードパッケージをアップロードしたり、アップグレードパッケージの場所を指定したりできるようになりました。 <p>以前は、[システムアップデート（System Updates）] ページしか使用できませんでした。</p> <ul style="list-style-type: none"> • 異なるデバイスをアップグレードする限り、異なるユーザーによる同時アップグレードワークフローが可能になりました。このシステムにより、すでに他の誰かのワークフローにあるデバイスをアップグレードすることはできません。 <p>以前は、すべてのユーザーで一度に1つのアップグレードワークフローのみが許可されていました。</p> <p>すべての Threat Defense のアップグレードについて、より小規模なアップグレードパッケージ、より高速なアップグレード、および準備状況チェックを提供します。</p> <p>詳細については、Management Center アップグレードガイドの「Upgrade Threat Defense」を参照してください。</p>

新機能	説明
無人アップグレード。	<p>Threat Defense アップグレードウィザードは、新しい [無人モード (Unattended Mode)] メニューを使用して無人アップグレードをサポートするようになりました。アップグレードするターゲットバージョンとデバイスを選択し、いくつかのアップグレードオプションを指定して、その場から離れるだけです。ログアウトしたり、ブラウザを閉じたりすることもできます。</p> <p>無人アップグレードを使用すると、システムは自動的に必要なアップグレードパッケージをデバイスにコピーし、互換性チェックと準備状況チェックを実行してアップグレードを開始します。ウィザードを手動でステップ実行する場合と同様に、アップグレードのステージに「合格」しなかったデバイス（たとえば、チェックの失敗）は、次のステージに含まれません。アップグレードが完了したら、検証とアップグレード後のタスクを開始します。</p> <p>コピーフェーズとチェックフェーズの間に無人モードを一時停止して再開できます。ただし、無人モードを一時停止しても、進行中のタスクは停止しません。開始されたコピーとチェックは完了するまで実行されます。同様に、無人モードを停止して進行中のアップグレードをキャンセルすることはできません。アップグレードをキャンセルするには、[デバイス管理 (Device Management)] ページの [アップグレード (Upgrade)] タブおよびメッセージセンターからアクセスできる [アップグレードステータス (Upgrade Status)] ポップアップを使用します。</p> <p>詳細については、Management Center アップグレードガイドの「Upgrade Threat Defense with the Wizard in Unattended Mode」を参照してください。</p>
アップグレード前のトラブルシューティング生成をスキップします。	<p>Threat Defense アップグレードウィザードから、新しい [アップグレード開始前にトラブルシューティングファイルを生成する (Generate troubleshooting files before upgrade begins)] オプションを無効にすることで、メジャーアップグレードおよびメンテナンスアップグレードの前にトラブルシューティング ファイルを自動生成することをスキップできるようになりました。これにより、時間とディスク容量を節約できます。</p> <p>脅威防御デバイスのトラブルシューティング ファイルを手動で生成するには、システム (⚙) > [正常性 (Health)] > [モニタ (Monitor)] を選択し、左側のパネルでデバイスをクリックし、[システムおよびトラブルシューティングの詳細を表示 (View System & Troubleshoot Details)]、[トラブルシューティング ファイルの生成 (Generate Troubleshooting Files)] をクリックします。</p> <p>詳細については、Management Center アップグレードガイドの「Upgrade Threat Defense」を参照してください。</p>

新機能	説明
<p>Threat Defense のアップグレード完了後の Snort 3 への自動アップグレードはオプションではなくなりました。</p>	<p>アップグレードの影響。</p> <p>Threat Defence をバージョン 7.3 以降にアップグレードする場合、[Snort 2 から Snort 3 にアップグレードする (Upgrade Snort 2 to Snort 3)] オプションは無効化できなくなりました。</p> <p>ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。</p> <p>カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスが自動アップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。</p> <p>必要最低限の Threat Defense : 任意</p>
<p>シスコからアップグレードパッケージを選択して直接ダウンロードします。</p>	<p>Management Center に直接ダウンロードする Threat Defense アップグレードパッケージを選択できるようになりました。 > [更新 (Updates)] > [製品の更新 (Product Updates)] の新しい [の更新のダウンロード (Download Threat Defense Updates)] サブタブを使用します。</p> <p>必要最低限の Threat Defense : 任意</p> <p>参照 : Management Center を含むアップグレードパッケージのダウンロード</p>

新機能	説明
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。	

新機能	説明
	<p>再イメージ化の影響。</p> <p>バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。</p> <ul style="list-style-type: none"> バージョン 7.1 ～ 7.2 インストールパッケージ： isco-ftd-fp3k.version.SPA バージョン 7.1 ～ 7.2 アップグレードパッケージ： Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar バージョン 7.3 以降の統合パッケージ： Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar <p>Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。</p> <p>Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。</p> <ul style="list-style-type: none"> Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当する アップグレードガイド を参照してください。 Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide』の「<i>Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100</i>」、次に「<i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i>」を参照してください。 ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA Upgrade Guide』を参照し、次に『Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide』の「<i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i>」を参照してください。

新機能	説明
	<ul style="list-style-type: none"> • Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。 <p>『Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティングガイド』の「Reimage the System with a New Software Version」を参照してください。</p>
アクセス制御と脅威検出	
<p>SSL ポリシーの名前が復号ポリシーに変更されました。</p>	<p>SSL ポリシーの名前を復号ポリシーに変更しました。また、インバウンドおよびアウトバウンドトラフィックの初期ルールと証明書の作成など、復号ポリシーの作成と構成を容易にするポリシーウィザードも追加しました。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • 復号ポリシーの追加または編集：[ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [復号 (Decryption)]。 • 復号ポリシーの使用：アクセス コントロール ポリシーの詳細設定の [復号ポリシー設定 (Decryption Policy Settings)]。 <p>詳細については、デバイス コンフィギュレーション ガイドの「Decryption Policies」を参照してください。</p>
<p>Snort 3 デバイスでの TLS サーバー ID 検出の改善。</p>	<p>TLS 1.3 で暗号化されたトラフィックをサーバー証明書からの情報で処理できる TLS サーバー ID 検出機能によるパフォーマンスと検査の改善がサポートされるようになりました。この機能は有効にしておくことをお勧めしますが、復号ポリシーの詳細設定にある新しい [アダプティブ TLS サーバー ID プロブを有効にする (Enable adaptive TLS server identity probe)] オプションを使用して無効にすることができます。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「TLS 1.3 Decryption Best Practices」を参照してください。</p>

新機能	説明
クラウドルックアップ結果のみを使用したURLフィルタリング。	

新機能	説明
	<p>URL フィルタリングを有効にする（または再度有効にする）と、Management Center は自動的にシスコに URL カテゴリとレピュテーションデータを照会し、データセットを管理対象デバイスにプッシュします。システムがこのデータセットを使用して Web トラフィックをフィルタリングする方法に関するオプションが増えました。</p> <p>これを行うために、[不明なURLをCisco Cloudに照会する（Query Cisco Cloud for Unknown URLs）] オプションを次の3つの新しいオプションに置き換えました。</p> <ul style="list-style-type: none"> • [ローカルデータベースのみ（Local Database Only）]：ローカル URL データセットのみを使用します。プライバシー上の理由などから、未分類の URL（ローカルデータセットにないカテゴリとレピュテーション）をシスコに送信したくない場合は、このオプションを使用します。ただし、未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致しないことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。 <p>アップグレードされた Management Center の場合、このオプションは、古い [不明なURLをCisco Cloudに照会する（Query Cisco Cloud for Unknown URLs）] が無効になっている場合に有効になります。</p> <ul style="list-style-type: none"> • [ローカルデータベースとCisco Cloud（Local Database and Cisco Cloud）]：可能な場合はローカルデータセットを使用し、Web ブラウジングを高速化します。カテゴリとレピュテーションがローカルデータセットまたは以前にアクセスした Web サイトのキャッシュにない URL をユーザーが参照すると、システムはその URL を脅威インテリジェンス評価のためにクラウドに送信し、結果をキャッシュに追加します。 <p>アップグレードされた Management Center の場合、このオプションは、古い [不明なURLをCisco Cloudに照会する（Query Cisco Cloud for Unknown URLs）] オプションが有効になっている場合に有効になります。</p> <ul style="list-style-type: none"> • [Cisco Cloudのみ（Cisco Cloud Only）]：ローカルデータセットを使用しません。カテゴリとレピュテーションが以前にアクセスした Web サイトのキャッシュにない URL をユーザーが参照すると、システムはその URL を脅威インテリジェンス評価のためにクラウドに送信し、結果をキャッシュに追加します。このオプションは、最新のカテゴリとレピュテーション情報を保証します。 <p>このオプションは、新規および再イメージ化されたバージョン 7.3 以降の Management Center のデフォルトです。Threat Defense</p>

新機能	説明
	<p>バージョン 7.3 以降も必要であることに注意してください。このオプションを有効にすると、以前のバージョンを実行しているデバイスは、[ローカルデータベースとCisco Cloud (Local Database and Cisco Cloud)] オプションを使用します。</p> <p>新規/変更された画面：[統合 (Integration)]>[その他の統合 (Other Integrations)]>[クラウドサービス (Cloud Services)]>[URL フィルタリング (URL Filtering)]</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「URL Filtering Options」を参照してください。</p>
<p>EVE を使用して HTTP/3 および SMB over QUIC を検出します (Snort 3 のみ)。</p>	<p>Snort 3 デバイスは、暗号化された可視性エンジン (EVE) を使用して、HTTP/3 および SMB over QUIC を検出できるようになりました。次に、これらのアプリケーションに基づいてトラフィックを処理するルールを作成できます。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Encrypted Visibility Engine」を参照してください。</p>
<p>EVE によって検出された安全でないクライアントアプリケーションに基づいて IoC イベントを生成します (Snort 3 のみ)。</p>	<p>Snort 3 デバイスは、暗号化された可視性エンジン (EVE) によって検出された安全でないクライアントアプリケーションに基づいて、侵害の兆候 (IoC) 接続イベントを生成できるようになりました。これらの接続イベントの暗号化された可視性の脅威の信頼度は非常に高いです。</p> <ul style="list-style-type: none"> • イベントビューアで IoC を表示します：[分析 (Analysis)]>[ホスト/ユーザー (Hosts/Users)]>[侵害の兆候 (Indications of Compromise)] • ネットワークマップで IoC を表示します：[分析 (Analysis)]>[ホスト (Hosts)]>[侵害の兆候 (Indications of Compromise)] • 接続イベントで IoC 情報を表示します：[分析 (Analysis)]>[接続 (Connections)]>[イベント (Events)]>[接続イベントのテーブルビュー (Table View of Connection Events)]>[IOC/暗号化された可視性列 (IOC/Encrypted Visibility columns)] <p>詳細については、デバイス コンフィギュレーション ガイドの「Encrypted Visibility Engine」を参照してください。</p>

新機能	説明
<p>Snort 3 デバイスの JavaScript インспекションの改善。</p>	<p>JavaScript を正規化し、正規化されたコンテンツに対してルールを照合することで実行される JavaScript インспекションを改善しました。バージョン 7.2 で導入されたノーマライザにより、unescape 関数、decodeURI 関数、および decodeURIComponent 関数 (%XX、%uXXXX、\uXX、\u{XXXX}\xXX、10 進数コードポイント、16 進数コードポイント) 内で検査できるようになりました。また、文字列からプラス演算を削除して連結します。</p> <p>詳細については、『Snort 3 インспекタリファレンス』の「HTTP Inspect Inspector」ならびに『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。</p>
<p>Snort3 侵入ポリシーのネストされたルールグループ (MITRE ATT&CK を含む)。</p>	<p>Snort3 侵入ポリシーでルールグループをネストできるようになりました。これにより、トラフィックをより詳細に表示および処理できます。たとえば、ルールを脆弱性のタイプ、ターゲットシステム、または脅威のカテゴリ別にグループ化できます。カスタムのネストされたルールグループを作成し、ルールグループごとにセキュリティレベルとルールアクションを変更できます。</p> <p>また、Talos がキュレートした MITRE ATT&CK フレームワークでシステム提供のルールをグループ化するため、これらのカテゴリに基づいてトラフィックを処理できます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • ルールグループの表示と使用：[ポリシー (Policies)] > [侵入 (Intrusion)] > [Snort 3 バージョンの編集 (Edit Snort 3 Version)] • クラシックイベントビューでルールグループ情報を表示します：[分析 (Analysis)] > [侵入 (Intrusion)] > [イベント (Events)] > [侵入イベントのテーブルビュー (Table View of Intrusion Events)] > [ルールグループと MITRE ATT&CK 列 (Rule Group and MITRE ATT&CK columns)] • 統合イベントビューでルールグループ情報を表示します：[分析 (Analysis)] > [統合イベント (Unified Events)] > [ルールグループと MITRE ATT&CK 列 (Rule Group and MITRE ATT&CK columns)] <p>詳細については、『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。</p>
<p>アクセス制御ルールの競合分析。</p>	<p>ルールの競合分析を有効にすると、ポリシーでの以前ルールが原因で一致しない冗長ルールやオブジェクト、およびシャドウルールを特定できるようになりました。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Analyzing Rule Conflicts and Warnings」を参照してください。</p>

新機能	説明
イベントロギングおよび分析	
<p>Snort 3 デバイスの NetFlow サポート。</p>	<p>アップグレードの影響。</p> <p>Snort 3 デバイスは、NetFlow レコード (IPv4 と IPv6、NetFlow v5 と v9) を使用できるようになりました。以前は、Snort 2 デバイスのみがこれを使用していました。</p> <p>アップグレード後、ネットワーク ディスカバリ ポリシーで既存の NetFlow エクスポートと NetFlow ルールが設定されている場合、Snort 3 デバイスは NetFlow レコードの処理を開始し、NetFlow 接続イベントを生成し、NetFlow データに基づいてホストおよびアプリケーションプロトコル情報をデータベースに追加します。</p> <p>詳細については、デバイス コンフィギュレーションガイドの「Network Discovery Policies」を参照してください。</p>
統合	
<p>Cisco ACI Endpoint Update App と統合するための新しい修復モジュール</p>	<p>新しい Cisco ACI Endpoint 修復モジュールを導入しました。これを使用するには、古いモジュールを削除してから、新しいモジュールを追加して構成する必要があります。この新しいモジュールは次のことができます。</p> <ul style="list-style-type: none"> • エンドポイントセキュリティ グループ (ESG) 展開でエンドポイントを検疫します。 • 監視および分析のために、検疫されたエンドポイントからレイヤ 3 外部ネットワーク (L3Out) へのトラフィックを許可します。 • 監査専用モードで実行し、検疫ではなく通知します。 <p>詳細については、デバイス コンフィギュレーション ガイドの「APIC/Secure Firewall Remediation Module 3.0」を参照してください。</p>
ヘルス モニタリング	
<p>Management Center の Web インターフェイスでのクラスタのヘルスマニター設定。</p>	<p>Management Center の Web インターフェイスを使用して、クラスタのヘルスマニター設定を編集できるようになりました。以前のバージョンで FlexConfig を使用してこれらの設定を構成した場合、システムは展開を許可しますが、構成をやり直すように警告が表示されます。FlexConfig 設定が優先されます。</p> <p>新規/変更された画面：[デバイス (Devices)]>[デバイス管理 (Device Management)]>[クラスタの編集 (Edit Cluster)]>[クラスタのヘルスマニターの設定 (Cluster Health Monitor Settings)]</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Edit Cluster Health Monitor Settings」を参照してください。</p>

新機能	説明
<p>デバイスクラスタのヘルスマonitoringが改善されました。</p>	<p>ヘルスマonitorにクラスタダッシュボードが追加され、クラスタ全体のステータス、負荷分散メトリック、パフォーマンスメトリック、クラスタ制御リンク (CCL)、データスループットなどを表示できるようになりました。</p> <p>各クラスタのダッシュボードを表示するには、システム (⚙) > [正常性 (Health)] > [モニタリング (Monitor)] を選択し、クラスタをクリックします。</p> <p>詳細については、アドミニストレーションガイドの「Cluster Health Monitor」を参照してください。</p>
<p>ハードウェア管理センターで電源のファン速度と温度をモニタリングします。</p>	<p>ハードウェア管理センターの電源のファン速度と温度をモニタリングするハードウェア統計正常性モジュールを追加しました。アップグレードプロセスにより、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、ポリシーを適用します。</p> <p>モジュールを有効または無効にし、しきい値を設定するには、システム (⚙) > [正常性 (Health)] > [ポリシー (Policy)] で Management Center の正常性ポリシーを編集します。</p> <p>正常性ステータスを表示するには、カスタムヘルスマonitor ダッシュボードを作成します：システム (⚙) > [正常性 (Health)] > [モニタリング (Monitor)] > [Firewall Management Center] > [追加/編集 (Add/Edit)]。[ハードウェア統計 (Hardware Statistics)] メトリックグループを選択し、必要なメトリックを選択します。</p> <p>モジュールのステータスは、ヘルスマonitorの[ホーム (Home)] ページと Management Center のアラートサマリ ([ハードウェアアラーム (Hardware Alarms)] および [電源 (Power Supply)]) で表示することもできます。外部アラート応答を構成し、モジュールステータスに基づいて正常性イベントを表示できます。</p> <p>詳細については、アドミニストレーションガイドの「Hardware Statistics on Management Center」を参照してください。</p>

新機能	説明
<p>Firepower 4100/9300 の温度と電源を監視します。</p>	<p>Firepower 4100/9300 シャーシの温度と電源を監視するために、シャーシ環境ステータス正常性モジュールが追加されました。アップグレードプロセスにより、すべてのデバイス正常性ポリシーにこれら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 Firepower 4100/9300 シャーシに適用して、モニタリングを開始します。</p> <p>このモジュールを有効または無効にし、しきい値を設定するには、システム (⚙️) > [正常性 (Health)] > [ポリシー (Policy)] > [デバイスポリシー (Device Policy)] で Management Center の正常性ポリシーを編集します。</p> <p>正常性ステータスを表示するには、カスタムヘルスダッシュボードを作成します：システム (⚙️) > [正常性 (Health)] > [モニタリング (Monitor)] > [デバイスの選択 (Select Device)] > [ダッシュボードの追加/編集 (Add/Edit Dashboard)] > [カスタム相関グループ (Custom Correlation Group)]。[ハードウェア/環境ステータス (Hardware/Environment Status)] メトリックグループを選択し、次に [温度ステータス (Thermal Status)] メトリックを選択して温度を表示するか、いずれかの [電源 (Power Supply)] オプションを選択して電源ステータスを表示します。</p> <p>ヘルスマニターの [ホーム (Home)] ページと各デバイスのアラートサマリーでモジュールのステータスを表示することもできます。外部アラート応答を構成し、モジュールステータスに基づいて正常性イベントを表示できます。</p> <p>詳細については、アドミニストレーションガイドの「Hardware/Environment Status Metrics」を参照してください。</p>
<p>ライセンスング</p>	

新機能	説明
<p>ライセンス名の変更およびキャリアライセンスのサポート。</p>	<p>ライセンスの名前を次のように変更しました。</p> <ul style="list-style-type: none"> • Base は Essentials に変更 • Threat は IPS に変更 • Malware は Malware Defense に変更 • RA VPN/AnyConnect License は Cisco Secure Client に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Apex および Plus は Secure Client Premier および Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 <p>さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、およびM3UA インスペクションを設定できます。</p> <p>新規/変更された画面：システム (⚙️) > [ライセンス (Licenses)] > [スマートライセンス (Smart Licenses)]</p> <p>詳細については、アドミニストレーションガイドの「Licenses」を参照してください。</p>
<p>管理 (Administration)</p>	
<p>FlexConfig から Web インターフェイス管理に設定を移行します。</p>	<p>FlexConfig からこれらの設定を Web インターフェイス管理に簡単に移行できるようになりました。</p> <ul style="list-style-type: none"> • バージョン 7.1 以降の Web インターフェイスでサポートされる ECMP ゾーン • バージョン 7.2 以降の Web インターフェイスでサポートされる EIGRP ルーティング • バージョン 7.2 以降の Web インターフェイスでサポートされる VXLAN インターフェイス <p>移行後は、廃止された FlexConfig を削除するまで展開できません。</p> <p>新規/変更された画面：[デバイス (Devices)] > [FlexConfig] > [FlexConfig ポリシーの編集 (Edit FlexConfig Policy)] > [設定の移行 (Migrate Config)]</p> <p>詳細については、デバイス コンフィギュレーションガイドの「Migrating FlexConfig Policies」を参照してください。</p>

新機能	説明
自動 VDB ダウンロード。	<p>Management Center の初期設定では、最新の脆弱性データベース (VDB) を含むようになった、利用可能な最新のソフトウェア更新をダウンロードするための週次タスクがスケジュールされています。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。</p> <p>新規/変更された画面：システムで作成された[週次ソフトウェアダウンロード (Weekly Software Download)]のスケジュールされたタスクで、[脆弱性データベース (Vulnerability Database)]チェックボックスがデフォルトで有効になりました。</p> <p>詳細については、アドミニストレーションガイドの「Vulnerability Database Update Automation」を参照してください。</p>
任意の VDB をインストールします。	<p>VDB 357 以降、その Management Center の基準 VDB までさかのぼって任意の VDB をインストールできるようになりました。</p> <p>VDB を更新したら、構成の変更を展開します。利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、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。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。</p> <p>新しい/変更された画面：システム (⚙) >[更新 (Updates)]>[製品アップデート (Product Updates)]>[利用可能なアップデート (Available Updates)]で、古い VDB をアップロードすると、[インストール (Install)] アイコンの代わりに新しい[ロールバック (Rollback)] アイコンが表示されます。</p> <p>詳細については、アドミニストレーションガイドの「Update the Vulnerability Database」を参照してください。</p>

新機能	説明
CA バンドルの自動更新。	<p>アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLI を使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド：configure cert-update auto-update、configure cert-update run-now、configure cert-update test、show cert-update</p> <p>詳細については、Management Center アドミニストレーションガイドの「Secure Firewall Management Center Command Line Reference」と、Cisco Secure Firewall Threat Defense コマンドリファレンス を参照してください。</p>
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	
新しい How-To ウォークスルー。	<p>次の How-To が追加されました。</p> <ul style="list-style-type: none"> • 手動再登録を使用して証明書を更新する。 • 自己署名、SCEP、または EST 登録を使用して証明書を更新する。 • リモートアクセス VPN の LDAP 属性マップを構成する。 • SAML シングルサインオン サーバー オブジェクトを追加する。 • Threat Defense デバイスのパケットキャプチャを収集する。 • パケットトレースを収集して、Threat Defense デバイスのトラブルシューティングを行う。 • リモートアクセス VPN のダイナミック アクセス ポリシーを構成する。 <ul style="list-style-type: none"> • ダイナミック アクセス ポリシーを作成する。 • ダイナミック アクセス ポリシー レコードを作成する。 • ダイナミック アクセス ポリシーをリモートアクセス VPN に関連付ける。 <p>How-To を起動するには、システム (⚙️) [ハウツー (How-Tos)] を選択します。</p>

新機能	説明
新しいアクセスコントロールポリシーのユーザーインターフェイスがデフォルトになりました。	バージョン 7.2 で導入されたアクセス コントロール ポリシーのユーザーインターフェイスは、デフォルトのインターフェイスになりました。アップグレードによって切り替えられますが、元に戻すことができます。
アクセス制御ルールごとの一致基準あたりの最大オブジェクト数が 200 になりました。	1 つのアクセス制御ルールの一致基準あたりのオブジェクト数が 50 から 200 に増えました。たとえば、1 つのアクセス制御ルールに最大 200 のネットワークオブジェクトを含めることができます。
デバイスをバージョン別にフィルタ処理します。	[デバイス (Devices)] > [デバイス管理 (Device Management)] で、バージョン別にデバイスをフィルタリングできるようになりました。
スケジュールされたタスクのステータスメールが改善されました。	スケジュールされたタスクの電子メール通知は、タスクの開始時ではなく、タスクの完了時（成功または失敗に関係なく）に送信されるようになりました。これは、タスクが失敗したか成功したかを示すことができるようになったことを意味します。失敗の場合、失敗の理由と問題を修正するための修正が含まれます。
CPU コア割り当てのパフォーマンスプロファイル。	<p>データプレーンと Snort に割り当てられたシステムコアの割合を調整して、システムパフォーマンスを調整できます。この調整は、VPN と侵入ポリシーの相対的な使用に基づいています。両方を使用する場合は、コア割り当てをデフォルト値のままにします。システムを主に VPN（侵入ポリシー適用なし）または IPS（VPN 設定なし）として使用する場合、コア割り当てをデータプレーン（VPN の場合）または Snort（侵入インスペクションの場合）にスキューできます。</p> <p>[パフォーマンスプロファイル (Performance Profile)] ページがプラットフォーム設定ポリシーに追加されました。</p> <p>詳細については、デバイス コンフィギュレーション ガイドの「Configure the Performance Profile」を参照してください。</p>

新機能	説明
Cisco Success Network に送信される追加のテレメトリ。	<p>有用性を向上させるために、次のデータを Cisco Success Network に送信するようになりました。</p> <ul style="list-style-type: none"> 登録されているがアクティブに管理されていないデバイスの数、デバイスが高可用性/スケーラビリティのために構成されているかどうか、構成されたクラスタ内のノードの数などのデバイス情報。 ネットワークマップ内のホスト数、侵入イベント数、ファイル/マルウェアイベント数などのイベントおよびネットワークマップ情報。 <p>Cisco Success Network の登録はいつでも変更できます。</p> <p>詳細については、アドミニストレーションガイドの「Configure Cisco Success Network Enrollment」を参照してください。</p>
Management Center REST API	
Management Center REST API サービス/操作。	FMC REST API の変更については、API クイックスタートガイドの「 What's New in 7.3 」を参照してください。

廃止された機能

表 3: Management Center バージョン 7.3.0 で廃止済みの機能

廃止された機能	説明
サポート終了： Firepower 4110、 4120、4140、4150。	Firepower 4110、4120、4140、または 4150 ではバージョン 7.3 以降は実行できません。
サポート終了： Firepower 9300： SM-24、SM-36、 SM-44 モジュール。	SM-24、SM-36、または SM-44 モジュールを搭載した Firepower 9300 ではバージョン 7.3 以降は実行できません。

廃止された機能	説明
Firepower 1010E のサポートなし（一時的）。	バージョン 7.2.3 で導入された Firepower 1010E は、バージョン 7.3 をサポートしていません。サポートは将来のリリースで復活します。 バージョン 7.2.x の Firepower 1010E をバージョン 7.3 にアップグレードすることはできません。また、そこで再イメージ化しないでください。バージョン 7.3 を実行している Firepower 1010E デバイスがある場合は、サポートされているリリースに再イメージ化します。Firepower 1010E の管理にバージョン 7.2.3 またはバージョン 7.3.0 の Management Center を使用しないでください。代わりに、バージョン 7.2.3.1 以降またはバージョン 7.3.1 以降の Management Center を使用してください。
廃止：Snort2 デバイスの YouTube EDU コンテンツ制限。	新規または既存のアクセス制御ルールで YouTube EDU コンテンツ制限を有効にできなくなりました。既存の YouTube EDU ルールは引き続き機能します。また、ルールを編集して YouTube EDU を無効化できます。 これは、Snort 3 では利用できない Snort 2 の機能であることに注意してください。 アップグレード後に設定をやり直す必要があります。
廃止：FlexConfig を使用したクラスタのヘルスマニタの設定。	Management Center の Web インターフェイスからクラスタのヘルスマニタ設定を編集できるようになりました。編集すると、展開は許可されますが、既存の FlexConfig 設定が優先されることが警告されます。 アップグレード後に設定をやり直す必要があります。
廃止：FlexConfig を使用した BGP の BFD。	Management Center の Web インターフェイスから BGP ルーティングの Bidirectional Forwarding Detection (BFD) を設定できるようになりました。この設定をすると、廃止された FlexConfig を削除するまで展開できません。 アップグレード後に設定をやり直す必要があります。
廃止：FlexConfig を使用した ECMP ゾーン。	FlexConfig から EMCP ゾーン設定を Web インターフェイス管理に簡単に移行できるようになりました。移行後は、廃止された FlexConfig を削除するまで展開できません。 アップグレード後に設定をやり直す必要があります。
廃止：FlexConfig を使用した VXLAN インターフェイス。	FlexConfig から VXLAN インターフェイス設定を Web インターフェイス管理に簡単に移行できるようになりました。移行後は、廃止された FlexConfig を削除するまで展開できません。

Management Center バージョン 7.2 の新機能

新機能

表 4: Management Center バージョン 7.2.4 の新機能

新機能	説明
<p>Cisco Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正 (FEC) が、25 GB+ SR、CSR、および LR トランシーバの第 74 条 FC-FEC から第 108 条 RS-FEC に変更されました。</p>	<p>Cisco Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB 以上の SR、CSR、および LR トランシーバのデフォルトタイプが第 74 条 FC-FEC ではなく第 108 条 RS-FEC に設定されるようになりました。</p> <p>FEC の詳細については、「Interface Overview」を参照してください。</p>
<p>CA バンドルの自動更新。</p>	<p>アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLI を使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド : configure cert-update auto-update、configure cert-update run-now、configure cert-update test、show cert-update</p> <p>詳細については、「Secure Firewall Management Center Command Line Reference」と、Cisco Secure Firewall Threat Defense コマンドリファレンス を参照してください。</p>

新機能	説明
<p>アクセス制御のパフォーマンスの向上（オブジェクトの最適化）。</p>	<p>アップグレードの影響。7.2.4 ~ 7.2.5 への Management Center アップグレード後の最初の展開には時間がかかり、デバイスの CPU 使用率が高くなる可能性があります。</p> <p>アクセス コントロール オブジェクトの最適化により、ネットワークが重複するアクセス コントロール ルールがある場合、パフォーマンスが向上し、デバイスリソースの消費が少なくなります。</p> <p>最適化は、機能が有効になった後の最初の展開時に管理対象デバイスで行われます。ルールが多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から1時間かかることがあります。この間、デバイスの CPU 使用率も高くなる可能性があります。メンテナンスウィンドウまたはトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強くお勧めします。</p> <p>次のことを計画できます。</p> <ul style="list-style-type: none"> バージョン 7.2.4 および 7.2.5 では、この機能は、再イメージ化およびアップグレードされた Management Center に対してデフォルトで有効になっています。 この機能は、バージョン 7.3 ではサポートされていません。アップグレードまたは再イメージ化すると、この機能は無効になります。 <p>必要最低限の Threat Defense : 任意</p>

表 5: Management Center バージョン 7.2.3 の新機能

新機能	説明
<p>Firepower 1010E。</p>	<p>Power over Ethernet (PoE) をサポートしていない Firepower 1010E を導入しました。Firepower 1010E の管理にバージョン 7.2.3 またはバージョン 7.3.0 の Management Center を使用しないでください。代わりに、バージョン 7.2.3.1 以降またはバージョン 7.3.1 以降の Management Center を使用してください。</p> <p>Firepower 1010E での PoE の詳細については、「Regular Firewall Interfaces」を参照してください。</p> <p>必要最低限の Threat Defense : 7.2.3</p>

表 6: Management Center バージョン 7.2.1 の新機能

新機能	説明
Cisco Secure Firewall 3100 のハードウェアバイパス (「fail-to-wire」) ネットワークモジュール。	<p>Cisco Secure Firewall 3100 向けに次のハードウェアバイパス ネットワーク モジュールが導入されました。</p> <ul style="list-style-type: none"> • 6 ポート 1 G SFP ハードウェアバイパス ネットワーク モジュール、SX (マルチモード) (FPR-X-NM-6X1SX-F) • 6 ポート 10 G SFP ハードウェアバイパス ネットワーク モジュール、SR (マルチモード) (FPR-X-NM-6X10SR-F) • 6 ポート 10 G SFP ハードウェアバイパス ネットワーク モジュール、LR (シングルモード) (FPR-X-NM-6X10LR-F) • 6 ポート 25 G SFP ハードウェアバイパス ネットワーク モジュール、SR (マルチモード) (FPR-X-NM-X25SR-F) • 6 ポート 25 G ハードウェアバイパス ネットワーク モジュール、LR (シングルモード) (FPR-X-NM-6X25LR-F) • 8 ポート 1 G 銅ケーブル ハードウェアバイパス ネットワーク モジュール (銅ケーブル) (FPR-X-NM-8X1G-F) <p>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)] > [物理インターフェイスの編集 (Edit Physical Interface)]</p> <p>詳細については、「Inline Sets and Passive Interfaces」を参照してください。</p>
KVM の仮想 Threat Defense を備えた Intel イーサネット ネットワーク アダプタ E810-CQDA2 ドライバ。	<p>KVM の仮想 Threat Defense で Intel イーサネット ネットワーク アダプタ E810-CQDA2 ドライバをサポートするようになりました。</p> <p>詳細については、「Getting Started with Secure Firewall Threat Defense Virtual and KVM」を参照してください。</p>

表 7: Management Center バージョン 7.2.0 の新機能

新機能	説明
プラットフォーム	

新機能	説明
Alibaba 向け Management Center Virtual および Threat Defense Virtual。	<p>Alibaba 向けの Secure Firewall Management Center Virtual および Secure Firewall Threat Defense が導入されました。Management Center を使用して、Alibaba 向け Threat Defense Virtual を管理する必要があります。デバイスマネージャーはサポートされていません。</p> <p>Alibaba インフラストラクチャの根本的な問題により、Threat Defense Virtual のインスタンスタイプ <code>ecs.g5ne.4xLarge</code> は、特に 1 秒あたりの接続数 (CPS) に関してパフォーマンスが低いことに注意してください。2xlarge または 4xlarge を推奨します。</p>
スナップショットで AWS および Azure 向け Threat Defense Virtual をすばやく展開できます。	<p>AWS または Azure インスタンスの Threat Defense Virtual のスナップショットを作成し、そのスナップショットを使用して新しいインスタンスをすばやく展開できるようになりました。この機能により、AWS および Azure の自動スケールソリューションのパフォーマンスも向上します。</p> <p>詳細については、『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。</p>
クラウド管理型の脅威防御デバイス向けの分析モード。	<p>バージョン 7.2 と同時に、Cisco クラウド提供型 Firewall Management Center を導入しました。クラウド提供型 Firewall Management Center は、Cisco Defense Orchestrator (CDO) プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。更新についてはシスコが行います。</p> <p>お客様が導入したハードウェアおよびバージョン 7.2 以降を実行している仮想管理センターでは、クラウド管理型の脅威防御デバイスを「共同管理」できますが、用途はイベントのロギングと分析に限られます。お客様が導入した管理センターからこれらのデバイスにポリシーを展開することはできません。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> クラウド管理型デバイスをお客様が導入した管理センターに追加する場合は、新しい [CDO管理対象デバイス (CDO Managed Device)] チェックボックスをオンにして、それが分析専用であることを指定します。 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択すると、分析専用のデバイスが表示されます。 <p>新規/変更された CLI コマンド：configure manager add、configure manager delete、configure manager edit、show managers</p> <p>詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理を参照してください。</p>

新機能	説明
Firewall 4100 のネットワークモジュール。	Firewall 4100 向けに次のネットワークモジュールが導入されました。 <ul style="list-style-type: none"> • 2 ポート 100 ギガビットイーサネット QSFP28 (FPR4K-NM-2X100G) • 4 ポート 100 ギガビットイーサネット QSFP28 (FPR4K-NM-4X100G)
ISA 3000 によるシャットダウンのサポート。	ISA 3000 のシャットダウンのサポートが再開されました。この機能はバージョン 7.0.2 で導入されましたが、バージョン 7.1 で一時的に廃止になりました。
高可用性/拡張性	
パブリッククラウドとプライベートクラウドの両方で Threat Defense Virtual のクラスタリング。	次の Threat Defense Virtual プラットフォームのクラスタリングを設定できるようになりました。 <ul style="list-style-type: none"> • AWS 向け Threat Defense Virtual : 16 ノードクラスタ • GCP 向け Threat Defense Virtual : 16 ノードクラスタ • KVM 向け Threat Defense Virtual : 4 ノードクラスタ • VMware 向け Threat Defense Virtual : 4 ノードクラスタ 新規/変更された画面 : <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタの追加 (Add Cluster)] • [Devices] > [Device Management] > [More] メニュー • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] 詳細については、「 Clustering for Threat Defense Virtual in a Public Cloud 」 (AWS、GCP) または「 Clustering for Threat Defense Virtual in a Private Cloud 」 (KVM、VMware) を参照してください。

新機能	説明
16 ノードクラスタのサポート。	<p>次のプラットフォームに 16 ノードクラスタを設定できるようになりました。</p> <ul style="list-style-type: none"> • Firepower 4100/9300 • AWS 向け Threat Defense Virtual • GCP 向け Threat Defense Virtual <p>Cisco Secure Firewall 3100 では、依然として 8 ノードしかサポートされません。</p> <p>詳細については、「Clustering for the Firepower 4100/9300」または「Clustering for Threat Defense Virtual in a Public Cloud」を参照してください。</p>
AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケール。	<p>CloudFormation テンプレートを使用して、AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケールをサポートできるようになりました。</p> <p>詳細については、『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。</p>
GCP 向け Threat Defense Virtual の自動スケール。	<p>GCP の内部ロードバランサ (ILB) と GCP 外部ロードバランサ (ELB) の間に Threat Defense Virtual インスタンスグループを配置することにより、GCP 向け Threat Defense Virtual の自動スケールをサポートできるようになりました。</p> <p>詳細については、『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。</p>
インターフェイス	
Firepower 2100 および Cisco Secure Firewall 3100 で LLDP をサポート。	<p>Firepower 2100 および Cisco Secure Firewall 3100 シリーズのインターフェイスで Link Layer Discovery Protocol (LLDP) を使用できるようになりました。</p> <p>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]</p> <p>新規/変更されたコマンド：show lldp status、show lldp neighbors、show lldp statistics</p> <p>詳細については、「Interface Overview」を参照してください。</p>

新機能	説明
Cisco Secure Firewall 3100のフロー制御に対応するためのフレームの一時停止。	<p>トラフィック バーストが発生している場合、バーストがNICのFIFOバッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を抑制できます。</p> <p>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)]>[ネットワーク接続 (Network Connectivity)]</p> <p>詳細については、「Interface Overview」を参照してください。</p>
Cisco Secure Firewall 3130 および 3140 のブレイクアウトポート。	<p>Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレイクアウトポートを構成できるようになりました。</p> <p>新規/変更された画面 : [デバイス (Devices)]>[デバイス管理 (Device Management)]>[シャーシの操作 (Chassis Operations)]</p> <p>詳細については、「Interface Overview」を参照してください。</p>
Management Center の Web インターフェイスから VXLAN を設定。	<p>Management Center の Web インターフェイスを使用して VXLAN インターフェイスを設定できるようになりました。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。</p> <p>以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。</p> <p>新規/変更された画面 :</p> <ul style="list-style-type: none"> • VTEP ソースインターフェイスは次の順にアクセスし、設定します : [デバイス (Devices)]>[デバイスの管理 (Device Management)]>[VTEP] • VNI インターフェイスは次の順にアクセスし、設定します。[デバイス (Devices)]>[デバイスの管理 (Device Management)]>[インターフェイス (Interfaces)]>[VPN インターフェイスを追加 (Add VNI Interface)] <p>詳細については、「Regular Firewall Interfaces」を参照してください。</p>
NAT	

新機能	説明
一度に複数の NAT ルールの有効化、無効化、削除が可能。	<p>複数の NAT ルールを選択して、すべてを同時に有効化、無効化、または削除できます。有効化および無効化の対象は手動 NAT ルールのみです。削除はすべての NAT ルールが対象になります。</p> <p>詳細については、「Network Address Translation」を参照してください。</p>
VPN	
RA VPN 接続プロファイル用の証明書と SAML 認証。	<p>RA VPN 接続プロファイル用の証明書と SAML 認証をサポートするようになりました。SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。</p> <p>新規/変更された画面：RA VPN ポリシーの接続プロファイルの認証方法を選択するときに、[証明書と SML (Certificate & SAML)] オプションを選択できるようになりました。</p> <p>詳細については、「Remote Access VPN」を参照してください。</p>
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN。	<p>ハブアンドスポークトポロジでのルートベースのサイト間 VPN のサポートが追加されました。以前は、このトポロジはポリシーベース（暗号マップ）VPN のみをサポートしていました。</p> <p>新規/変更された画面：新しい VPN トポロジを追加し、[ルートベース (VTI) (Route Based (VTI))] を選択すると、[ハブアンドスポーク (Hub and Spoke)] も選択できるようになりました。</p> <p>詳細については、「Site-to-Site VPNs」を参照してください。</p>
Cisco Secure Firewall 3100 の IPsec フローのオフロード。	<p>Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティアソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブルゲートアレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。</p> <p>FlexConfig と flow-offload-ipsec コマンドを使用して構成を変更できます。</p> <p>詳細については、「Site-to-Site VPNs」を参照してください。</p>
ルーティング	

新機能	説明
Management Center の Web インターフェイスから EIGRP を設定。	<p>Management Center の Web インターフェイスを使用して EIGRP を設定できるようになりました。デバイスのグローバル仮想ルータに属するインターフェイスでのみ EIGRP を有効にできることに注意してください。</p> <p>以前のバージョンの FlexConfig を使用して EIGRP を設定した場合、アップグレード後の展開は可能ですが、Web インターフェイスで EIGRP の設定をやり直すように警告が表示されます。新しい設定を確認したら、廃止された FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。</p> <p>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)]>[EIGRP]</p> <p>詳細については、「EIGRP」およびFlexConfig ポリシーの移行を参照してください。</p>
Firepower 1010 で仮想ルータをサポート。	<p>Firepower 1010 で最大 5 つの仮想ルータを構成できるようになりました。</p> <p>詳細については、「Virtual Routers」を参照してください。</p>
ユーザー定義の仮想ルータで VTI をサポート。	<p>仮想トンネルインターフェイスをユーザー定義の仮想ルータに割り当てることができるようになりました。これまでは、VTI はグローバル仮想ルータにしか割り当てることができませんでした。</p> <p>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)]>[仮想ルータのプロパティ (Virtual Router Properties)]</p> <p>詳細については、「Virtual Routers」を参照してください。</p>

新機能	説明
<p>パスのモニタリングによるポリシーベースのルーティング。</p>	<p>パスのモニタリング機能を使用して、デバイスの出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集できるようになりました。次に、収集したメトリックを使用して、ポリシーベースのルーティングの最適なパスを決定できます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> パスモニタリングを有効にし、収集するメトリックを選択するには、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [インターフェイス (Interfaces)] > [パスモニタリング (Path Monitoring)] に移動します。 ポリシーベースのルートを追加して転送アクションを指定する際、新規の [インターフェイスの順位付け (Interface Ordering)] オプションを使用します ([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)])。 各デバイスのヘルスマニタリングダッシュボードでパスメトリックを監視します (システム (⚙️) > [ヘルス (Health)] > [モニター (Monitor)] > [ダッシュボードの追加 (add dashboard)] > [インターフェイス: パスメトリック (Interface - Path Metrics)])。 <p>新規/変更された CLI コマンド：show policy route、show path-monitoring、clear path-monitoring</p> <p>詳細については、「Policy Based Routing」を参照してください。</p>
脅威インテリジェンス	

新機能	説明
Cisco Umbrella からの DNS ベースの脅威インテリジェンス。	<p>Cisco Umbrella から定期的に更新される情報を使用して、DNS ベースのセキュリティインテリジェンスをサポートするようになりました。二重の保護として、ローカル DNS ポリシーと Umbrella DNS ポリシーの両方を使用できます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • Umbrella への接続の設定：[統合 (Integration)] > [その他の統合 (Other Integrations)] > [クラウドサービス (Cloud Services)] > [Cisco Umbrella接続 (Cisco Umbrella Connection)] • Umbrella DNS ポリシーの設定：[ポリシー (Policies)] > [DNS] > [DNSポリシーを追加 (Add DNS Policy)] > [Umbrella DNA ポリシー (Umbrella DNA Policy)] • Umbrella DNS ポリシーのアクセスコントロールへの関連付け：[ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [ポリシーを編集 (Edit Policy)] > [セキュリティインテリジェンス (Security Intelligence)] > [Umbrella Cisco DNS ポリシー (Umbrella Cisco DNS Policy)] <p>詳細については、「DNS Policies」を参照してください。</p>
Amazon GuardDuty からの IP ベースの脅威インテリジェンス。	<p>AWS の Management Center Virtual と統合している場合、Amazon GuardDuty によって検出された悪意のある IP アドレスに基づいてトラフィックを処理できるようになりました。カスタムセキュリティインテリジェンス フィールドまたは定期的に更新されるネットワーク オブジェクト グループを介して脅威インテリジェンスがシステムで活用され、ユーザーはそれをセキュリティポリシー内で使用できます。</p> <p>詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。</p>
アクセス制御と脅威検出	

新機能	説明
<p>動的オブジェクト管理：</p> <ul style="list-style-type: none"> • クラウド提供型 Cisco Secure 動的属性コネクタ • オンプレミス Cisco Secure 動的属性コネクタ 2.0 	<p>バージョン 7.2 と同時に、Cisco Secure 動的属性コネクタの次の更新をリリースしました。</p> <ul style="list-style-type: none"> • クラウド提供型 Cisco Secure 動的属性コネクタ (CDO マネージド サービス) <ul style="list-style-type: none"> サポート対象管理センター：バージョン 7.1 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365。 <p>詳細については、<i>Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator</i> の章を参照してください。</p> • オンプレミス Cisco Secure 動的属性コネクタ 2.0 <ul style="list-style-type: none"> サポート対象管理センター：バージョン 7.0 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365、VMware。 <p>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 2.0 [英語] を参照してください。</p>
<p>Snort3 デバイスで、インスペクションをバイパスするか、エレファントフローをスロットルします。</p>	<p>インスペクションの検出およびオプションでのバイパス、もしくはエレファントフローをスロットルできるようになりました。デフォルトでは、アクセス コントロール ポリシーは、システムが 1 GB/10 秒を超える暗号化されていない接続を検出したときにイベントを生成するように設定されています。レート制限は設定可能です。</p> <p>Firepower 2100 シリーズでは、エレファントフローを検出できますが、インスペクションのバイパスやスロットルすることはできません。Snort2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスでは、引き続きインテリジェントアプリケーションバイパス (IAB) を使用します。</p> <p>新規/変更された画面：[エレファントフローの設定 (Elephant Flow Settings)] をアクセス コントロール ポリシーの [詳細 (Advanced)] タブに追加しました。</p> <p>詳細については、「Elephant Flow Detection」を参照してください。</p>

新機能	説明
Snort 3 デバイス向けの暗号化された可視性エンジン機能の拡張。	

新機能	説明
	<p>暗号化された可視性エンジン (EVE) に次の拡張機能が追加されています。</p> <ul style="list-style-type: none"> • EVE は、ホストが使用しているオペレーティングシステムを検出できます。これは、イベントとネットワークマップで報告されません。 • EVE は、高い信頼度で識別された EVE プロセスをアプリケーションに割り当てることでアプリケーショントラフィックを検出できます。これをアクセスコントロールルールで使用してネットワークトラフィックを制御できます。(バージョン 7.1 では、接続の EVE プロセスを見ることができましたが、その情報をもとに行動することはできませんでした。) <p>さらに割り当てを追加するには、カスタムアプリケーションやカスタムアプリケーションディテクタを作成します。カスタムディテクタに検出パターンを追加するときは、アプリケーションとして [暗号化された可視性エンジン (Encrypted Visibility Engine)] を選択します。次に、プロセス名と信頼度を指定します。</p> <ul style="list-style-type: none"> • EVE は QUIC トラフィックで動作するようになりました。 <p>これらの機能拡張に伴い、次の接続イベントフィールドが変更されました。</p> <p>[TLS Fingerprint Process Name] は次に [暗号化された可視性プロセス変更名 (Encrypted Visibility Process Name)] になりました。</p> <p>[TLS Fingerprint Process Confidence Score] は次に [暗号化された可視性プロセスの信頼スコア (Encrypted Visibility Process Confidence Score)] になりました。</p> <p>[TLS Fingerprint Malware Confidence] は次に [暗号化された可視性脅威の信頼度 (Encrypted Visibility Threat Confidence)] になりました。</p> <p>[TLS Fingerprint Malware Confidence Score] は次に [暗号化された可視性脅威の信頼スコア (Encrypted Visibility Threat Confidence Score)] になりました。</p> <p>検出タイプ : TLS フィンガープリント は次に 検出タイプ : 暗号化された可視性エンジン</p>

新機能	説明
	<p>れました。</p> <p>この機能には脅威ライセンスが必要になりました。</p> <p>詳細については、「Access Control Policies」および「Application Detection」を参照してください。</p>
<p>Snort 3 デバイスの TLS 1.3 インスペクション。</p>	<p>TLS 1.3 トラフィックのインスペクションがサポートされるようになりました。</p> <p>新規/変更された画面：SSL ポリシーの [詳細設定 (Advanced Settings)] タブに [TLS 1.3 復号の有効化 (Enable TLS 1.3 Decryption)] オプションが追加されました。なお、このオプションはデフォルトで無効になっています。</p> <p>詳細については、「SSL Policies」を参照してください。</p>
<p>Snort 3 デバイスのポートスキャン検出の改善。</p>	<p>改良されたポートスキャンディテクタを使用すると、ポートスキャンを検出または防止するようにシステムを簡単に設定できます。保護するネットワークを絞り込んだり、感度を設定したりできます。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスの場合、ポートスキャン検出には引き続きネットワーク分析ポリシーを使用します。</p> <p>新規/変更された画面：[脅威検出 (Threat Detection)] をアクセスコントロールポリシーの [詳細 (Advanced)] タブに追加しました。</p> <p>詳細については、「Threat Detection」を参照してください。</p>
<p>Snort 3 デバイスの VBA マクロ検査。</p>	<p>Microsoft Office ドキュメントの VBA (Visual Basic for Applications) マクロのインスペクションがサポートされるようになりました。これは、マクロを解凍し、解凍されたコンテンツに対してルールを照合することで実行されます。</p> <p>デフォルトでは、VBA マクロの解凍は、システムが提供するすべてのネットワーク分析ポリシーで無効になっています。これを有効にするには、imap、smtp、http_inspect、および pop Snort 3 インスペクタで decompress_vba 設定を使用します。</p> <p>解凍されたマクロと照合するカスタム侵入ルールを設定するには、vba_data オプションを使用します。</p> <p>詳細については、『Snort 3 インスペクタリファレンス』ならびに『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。</p>

新機能	説明
Snort 3 デバイスの JavaScript インспекションの改善。	<p>JavaScript を正規化し、正規化されたコンテンツに対してルールを照合することで実行される JavaScript インспекションを改善しました。新しいノーマライザの拡張機能には、改善されたホワイトスペースの正規化、セミコロンへの挿入、クロスサイトスクリプトの処理、識別子の正規化とデエイリアシング、ジャストインタイム (JIT) インспекション、および外部スクリプトを検査する機能が含まれます。</p> <p>デフォルトでは、新しいノーマライザは、システムが提供するすべてのネットワーク分析ポリシーで有効になっています。カスタムネットワーク分析ポリシーでパフォーマンスを調整するか、機能を無効にするには、<code>https_inspect Snort 3</code> インспекターで <code>js_norm</code> (改良されたノーマライザ) および <code>normalize_javascript</code> (従来のノーマライザ) 設定を使用します。</p> <p>正規化された JavaScript と照合するようにカスタム侵入ルールを構成するには、次のように <code>js_data</code> オプションを使用します。</p> <pre>alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)</pre> <p>詳細については、『Snort 3 インспекタリファレンス』の「HTTP Inspect Inspector」ならびに『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。</p>
Snort 3 デバイスの SMB 3 インспекションの改善。	<p>次の状況下で SMB 3 トラフィックの検査がサポートされるようになりました。</p> <ul style="list-style-type: none"> • SMB 透過フェールオーバー用に構成されたクラスタのファイルサーバーノードのフェールオーバー中。 • SMB スケールアウトを使用したクラスタの複数ファイルサーバーノード内。 • SMB ディレクトリリリースによるディレクトリ情報の変更時。 • SMB マルチチャネルによる複数の接続の分散時。 <p>詳細については、『Snort 3 インспекタリファレンス』ならびに『Cisco Secure Firewall Management Center Snort 3 Configuration Guide』を参照してください。</p>
[ポリシー管理 (Policy Management)]	

新機能	説明
<p>アクセスコントロールポリシーのロック。</p>	<p>アクセスコントロールポリシーをロックして、他の管理者が編集できないようにすることが可能になりました。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。アクセスコントロールポリシーを変更する権限を持つすべてのユーザーには、それをロックする権限があります。</p> <p>ポリシーの編集時にポリシーをロックまたはロック解除するアイコンがポリシー名の横に追加されました。さらに、他の管理者によってロックされたポリシーのロックを解除できるようにする新しい権限（アクセスコントロールポリシーロックのオーバーライド）が追加されました。この権限は、デフォルトで管理者、アクセス管理者、およびネットワーク管理者のロールで有効になっています。</p> <p>詳細については、「Access Control Policies」を参照してください。</p>
<p>オブジェクトグループ検索をデフォルトで有効化。</p>	<p>デバイスを Management Center に追加すると、[オブジェクトグループ検索 (Object Group Search)] 設定がデフォルトで有効になるようになりました。</p> <p>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)] > [詳細設定 (Advanced Settings)]</p> <p>詳細については、「Device Management」を参照してください。</p>
<p>アクセス制御ルールヒットカウントは再起動後も存続します。</p>	<p>管理対象デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。show rule hits コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。</p> <p>新規/変更された CLI コマンド : show rule hits</p> <p>詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。</p>

新機能	説明
アクセスコントロールポリシーのユーザビリティの改善。	<p>アクセスコントロールポリシーで使用できる新しいユーザーインターフェイスが追加されました。従来のユーザーインターフェイスを引き続き使用することも、新しいユーザーインターフェイスを試すこともできます。</p> <p>新しいインターフェイスは、ルールリストのテーブルビューとグリッドビュー、列を表示または非表示にする機能、高度な検索機能、無限スクロール機能を備え、アクセスコントロールポリシーが割り当てられたポリシーに関するパケットフローのビューがより明確になりました。また、ルール作成用の追加/編集ダイアログボックスがシンプルになりました。アクセスコントロールポリシーの編集時に、従来のユーザーインターフェイスと新しいユーザーインターフェイスを自由に切り替えることができます。</p> <p>詳細については、「Access Control Policies」を参照してください。</p>
イベントロギングおよび分析	

新機能	説明
<p>SecureX との統合、SecureX とのオーケストレーションの改善</p>	<p>SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合 (Integration)] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureXの有効化 (Enable SecureX)] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、および Cisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。</p> <p>この新しいページで SecureX との統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。</p> <p>Web インターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング (SaaS) を使用して Secure Network Analytics (Stealthwatch) クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、システム (⚙️) > [統合 (Integration)] > [クラウドサービス (Cloud Services)] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。</p> <p>Management Center は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップインターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。</p> <p>この機能の一部として、REST API を使用して SecureX との統合を設定できなくなりました。FMC の Web インターフェイスを使用する必要があります。</p> <p>この機能はバージョン 7.0.2 で導入され、バージョン 7.1 で一時的に廃止になりました。</p> <p>詳細については、『Cisco Secure Firewall Management Center (7.0.2 および 7.2) および SecureX 統合ガイド』を参照してください。</p>

新機能	説明
<p>セキュリティイベントのログを複数の Cisco Secure Network Analytics オンプレミス データストアに記録。</p>	<p>Cisco Secure Network Analytics Data Store (マルチノード) との統合を設定する際、セキュリティイベント用に複数のフローコレクターを追加できるようになりました。各フローコレクターを、バージョン 7.0 以降を実行している 1 つ以上の Threat Defense デバイスに割り当てます。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • セットアップ：[統合 (Integration)]>[セキュリティ分析とロギング (Security Analytics & Logging)]>[Secure Network Analytics Data Store] • 変更：[統合 (Integration)]>[セキュリティ分析およびロギング (Security Analytics & Logging)]>[デバイス割り当ての更新 (Update Device Assignments)] <p>この機能には、Cisco Secure Network Analytics バージョン 7.1.4 が必要です。</p> <p>詳細については、『Cisco Security Analytics and Logging (オンプレミス) : ファイアウォールイベント統合ガイド』を参照してください。</p>
<p>データベースアクセスの変更。</p>	<p>10 個の新しいテーブルを追加し、1 個のテーブルを廃止し、6 個のテーブルで結合を禁止しました。また、Snort 3 サポートのためにさまざまなテーブルにフィールドを追加し、可読形式でタイムスタンプと IP アドレスを提供しました。</p> <p>詳細については、『Cisco Secure Firewall Management Center Database Access Guide, Version 7.2』の新機能のトピックを参照してください。</p>
<p>eStreamer の変更。</p>	<p>新しい Python ベースの参照クライアントが SDK に追加されました。また、完全修飾イベントをリクエストできるようになりました。</p> <p>詳細については、『Cisco Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2』の新機能のトピックを参照してください。</p>
<p>アップグレード</p>	

新機能	説明
<p>デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。</p>	<p>Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレードパッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5つのパッケージの同時転送に対応できます。</p> <p>この機能は、同じスタンドアロン Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。</p> <ul style="list-style-type: none"> • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。 <p>これらのデバイス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します。アップグレードパッケージを1つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。</p> <ul style="list-style-type: none"> • 高可用性 Management Center によって管理されるデバイス。 • クラウド提供型の管理センターによって管理されているが、お客様が導入した Management Center に分析モードで追加されたデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 <p>新規/変更された CLI コマンド：configure p2psync enable、configure p2psync disable、show peers、show peer details、sync-from-peer、show p2p-sync-status</p> <p>必要最低限の Threat Defense : 7.2</p> <p>詳細については、「Copy Threat Defense Upgrade Packages between Devices」を参照してください。</p>

新機能	説明
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	<p>バージョン 7.2 以降の Management Center を使用して Threat Defense をアップグレードする場合、Snort 2 から Snort 3 へのアップグレードを実行するかどうかを選択できるようになりました。</p> <p>ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。</p> <p>このオプションは、バージョン 7.2 以降への Threat Defense のメジャーアップグレードおよびメンテナンスアップグレードでサポートされています。バージョン 7.0 または 7.1 への Threat Defense のアップグレード、または任意のバージョン向けのパッチではサポートされていません。</p>
単一ノードクラスタのアップグレード。	<p>デバイスのアップグレードページ ([デバイス (Devices)] > [デバイスのアップグレード (Device Upgrade)]) を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ (システム (⚙️) [更新 (Updates)]) ではサポートされていません。</p> <p>この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300、Secure Firewall 3100</p>

新機能	説明
CLI からの Threat Defense アップグレードの復元。	<p>Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。</p> <p>注意 CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。</p> <p>新規/変更された CLI コマンド : upgrade revert、show upgrade revert-info。</p> <p>必要最低限の Threat Defense : 7.2</p> <p>詳細については、「Revert the Upgrade」を参照してください。</p>
管理とトラブルシューティング	
Secure Firewall 3100 のパケットドロップ統計。	<p>新しい show packet-statistics 脅威防御 CLI コマンドは、ポリシーに関連しないパケットドロップに関する包括的な情報を表示します。これまでは、いくつかのコマンドを使用してこの情報を表示する必要がありました。</p> <p>詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。</p>
DNS 要求を解決するための複数の DNS サーバグループ。	<p>クライアントシステムからの DNS 要求を解決するために、複数の DNS グループを設定できます。これらの DNS サーバグループを使用して、さまざまな DNS ドメインの要求を解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバを使用するキャッチオールデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部 DNS サーバを使用する別のグループを構成できます。したがって、組織のドメイン名を使用した FQDN への接続は、内部 DNS サーバを使用して解決されますが、パブリックサーバへの接続は外部 DNS サーバを使用します。</p> <p>新規/変更された画面 : [プラットフォーム設定 (Platform Settings)] > [DNS]</p> <p>詳細については、「Platform Settings」を参照してください。</p>

新機能	説明
<p>使用タイプごとに脅威防御を使用して証明書の検証を設定します。</p>	<p>トラストポイント（脅威防御デバイス）で検証が許可される使用タイプを指定できるようになりました：IPsec クライアント接続、SSL クライアント接続、および SSL サーバー証明書。</p> <p>新規/変更された画面：証明書登録オブジェクトに [検証の使用 (Validation Usage)] オプションを追加しました：[オブジェクト (Objects)] > [オブジェクトマネージャ (Object Manager)] > [PKI] > [証明書の登録 (Cert Enrollment)]。</p> <p>詳細については、「オブジェクト管理」を参照してください。</p>
<p>展開で管理接続が失われた場合の自動ロールバック。</p>	<p>展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、configure policy rollback コマンドを使用して手動で設定をロールバックすることしかできませんでした。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [展開設定 (Deployment Settings)] • [展開 (Deploy)] > [高度な展開 (Advanced Deploy)] > [プレビュー (Preview)] • [展開 (Deploy)] > [展開履歴 (Deployment History)] > [プレビュー (Preview)] <p>詳細については、「Device Management」を参照してください。</p>
<p>設定の変更を展開するときに、レポートを生成して電子メールで送信します。</p>	<p>任意の展開タスクのレポートを生成できるようになりました。このレポートには、展開された設定に関する詳細が含まれています。</p> <p>新規/変更されたページ：[展開 (Deploy)] > [展開履歴 (Deployment History)] [アイコン (icon)] その他 (⋮) [全般的なレポート (Generate Report)]。</p> <p>詳細については、「Configuration Deployment」を参照してください。</p>

新機能	説明
<p>GeoDB を 2 つのパッケージに分割。</p>	<p>2022 年 5 月、バージョン 7.2 リリースの直前に、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>バージョン 7.2 以降の Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、またはシスコサポートおよびダウンロードサイトから 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されてインポートされます。ただし、更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、必ず両方の GeoDB パッケージを取得してインポートしてください。</p> <ul style="list-style-type: none"> • 国コードパッケージ : Cisco_GEODB_Update-date-build.sh.REL.tar • IP パッケージ : Cisco_IP_GEODB_Update-date-build.sh.REL.tar <p>地理位置情報の更新（システム (⚙️) > [更新 (Updates)] > [地理位置情報の更新 (Geolocation Updates)] ページと概要ページ ([ヘルプ (Help)] > [概要 (About)]) には、システムで現在使用されているパッケージのバージョンが一覧表示されます。</p> <p>詳細については、「Updates」を参照してください。</p>
<p>Web インターフェイスのフランス語オプション。</p>	<p>Management Center の Web インターフェイスをフランス語に切り替えることができるようになりました。</p> <p>新規/変更された画面 : システム (⚙️) > [設定 (Configuration)] > [言語 (Language)]</p> <p>詳細については、「System Configuration」を参照してください。</p>

新機能	説明
<p>Web インターフェイスの変更：展開とユーザーアクティビティの統合。</p>	<p>バージョン 7.2 では、すべてのケースで以下の Management Center メニューオプションが変更されています。</p> <p>[展開 (Deploy)]>[展開履歴 (Deployment History)] は次に [展開 (Deploy)]>[展開履歴 (Deployment History)] (右側) に移動されました。</p> <p>[展開 (Deploy)]>[展開 (Deployment)] は次に [展開 (Deploy)]>[高度な展開 (Advanced Deploy)] に移動されました。</p> <p>[分析 (Analysis)]>[ユーザー (Users)]>[アクティブなセッション (Active Sessions)] は次に [統合 (Integration)]>[ユーザー (Users)]>[アクティブなセッション (Active Sessions)] に移動されました。</p> <p>[分析 (Analysis)]>[ユーザー (Users)]>[ユーザー (Users)] は次に [統合 (Integration)]>[ユーザー (Users)]>[ユーザー (Users)] に移動されました。</p> <p>[分析 (Analysis)]>[ユーザー (Users)]>[ユーザーアクティビティ (User Activity)] は次に [統合 (Integration)]>[ユーザー (Users)]>[ユーザーアクティビティ (User Activity)] に移動されました。</p>

新機能	説明
Web インターフェイスの変更 : SecureX、脅威インテリジェンス、およびその他の統合。	

新機能	説明
	<p>バージョン 7.0.1 以前、またはバージョン 7.1 からアップグレードする場合、バージョン 7.2 では Management Center のメニューオプションが変更されます。</p> <p>(注) バージョン 7.0.2 またはそれ以降のバージョン 7.0.x メンテナンスリリースからアップグレードする場合、メニュー構造はすでに次のようになっています。</p> <p>[AMP] > [AMP管理 (AMP Management)] は次に変更されました。 [統合 (Integration)] > [AMP > [AMP管理 (AMP Management)]</p> <p>[AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)] は次に変更されました。 [統合 (Integration)] > [AMP > [ダイナミック分析接続 (Dynamic Analysis Connections)]</p> <p>[インテリジェンス (Intelligence)] > [ソース (Sources)] は次に変更されました。 [統合 (Integration)] > [インテリジェンス (Intelligence)] > [ソース (Sources)]</p> <p>[インテリジェンス (Intelligence)] > [要素 (Elements)] は次に変更されました。 [統合 (Integration)] > [インテリジェンス (Intelligence)] > [要素 (Elements)]</p> <p>[インテリジェンス (Intelligence)] > [設定 (Settings)] は次に変更されました。 [統合 (Integration)] > [インテリジェンス (Intelligence)] > [設定 (Settings)]</p> <p>[インテリジェンス (Intelligence)] > [インシデント (Incidents)] は次に変更されました。 [統合 (Integration)] > [インテリジェンス (Intelligence)] > [インシデント (Incidents)]</p>

新機能	説明
	<p>れま し た。</p> <p>システム (⚙️) > [統合 (Integration)] は次 [統合 (Integration)]>[その他 の変の統合 (Other Integrations)] 更さ れま し た。</p> <p>システム (⚙️) > [ロギング (Logging)]>[セキュリティ分析とロギング (Security Analytics and Logging)] は次 [統合 (Integration)]>[セキュ リ ティ分析とロギング (Security Analytics and Logging)] 更さ れま し た。</p> <p>システム (⚙️) > [SecureX] は次 [統合 (Integration)]> [SecureX] 更さ れま し た。</p>
Management Center REST API	
Management Center REST API サービス/操作。	FMC REST API の変更の詳細については、REST API クイックスタートガイド [英語] の「 What's New in 7.2 」を参照してください。

廃止された機能

表 8 : Management Center バージョン 7.2.0 で廃止済みの機能

廃止された機能	説明
<p>廃止 : FlexConfig を使用した EIGRP。</p>	<p>Management Center の Web インターフェイスから EIGRP ルーティングを設定できるようになりました。</p> <p>次の FlexConfig オブジェクトは不要になりました : Eigrp_Configure、Eigrp_Interface_Configure、Eigrp_Unconfigure、Eigrp_Unconfigure_all。</p> <p>および、次の関連するテキストオブジェクトが廃止されました : eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary、eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon。</p> <p>システムでは、アップグレード後に展開できますが、EIGRP 構成をやり直すように警告されます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。詳細については、「Migrating FlexConfig Policies」を参照してください。</p>
<p>廃止 : FlexConfig を使用した VXLAN。</p>	<p>Management Center の Web インターフェイスから VXLAN インターフェイスを設定できるようになりました。</p> <p>次の FlexConfig オブジェクトは不要になりました : VxLAN_Clear_Nve、VxLAN_Clear_Nve_Only、VxLAN_Configure_Port_And_Nve、VxLAN_Make_Nve_Only、VxLAN_Make_Vni。</p> <p>これらの関連するテキストオブジェクト : vxlan_Port_And_Nve、vxlan_Nve_Only、vxlan_Vni。</p> <p>以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。</p>
<p>廃止 : アップグレード前の自動トラブルシューティング。</p>	<p>時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。</p> <p>管理センターのトラブルシューティング ファイルを手動で生成するには、システム (⚙️) > [正常性 (Health)] > [モニタ (Monitor)] を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。</p>

FMC バージョン 7.1 の新機能

新機能

表 9: FMC バージョン 7.1 パッチの新機能

新機能	説明
バージョン 7.1.0.3 CA バンドルの自動更新。	<p>アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLIを使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド : configure cert-update auto-update、configure cert-update run-now、configure cert-update test、show cert-update</p> <p>詳細については、Management Center アドミニストレーションガイドの「Firepower Management Center Command Line Reference」と、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。</p>

表 10: FMC バージョン 7.1.0 の新機能

新機能	説明
プラットフォーム	

新機能	説明
Cisco Secure Firewall 3100	<p>Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。</p> <p>ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ (SED) です。SSD が 2 つある場合、ソフトウェア RAID を形成します。これらのデバイスはスバンド EtherChannel クラスタリング用に最大 8 つのユニットをサポートします。</p> <p>バージョン 7.1.0 リリースには、これらのデバイスのオンラインヘルプが含まれていないことに注意してください。バージョン 7.1.0.2 には、新しいオンラインヘルプが含まれています。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタの追加 (Add Cluster)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [詳細 (More)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [クラスタ (Cluster)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [シャーシの操作 (Chassis Operations)] • [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を編集 > [ハードウェア構成 (Hardware Configuration)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] <p>新規/変更された FTD CLI コマンド：configure network speed、configure raid、show raid、show ssd</p>
AWS 用 FMCv300 OCI 用 FMCv300	<p>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。</p>

新機能	説明
AWS 用 FTDv のインスタンス。	<p>AWS 用 FTDv により、次のインスタンスのサポートが追加されます。</p> <ul style="list-style-type: none"> • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5n.xlarge、c5n.2xlarge、c5n.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。	<p>Azure 用 FTDv により、次のインスタンスのサポートが追加されます。</p> <ul style="list-style-type: none"> • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

新機能	説明
<p>FDM を使用して、FMC による管理用に FTD を設定します。</p>	<p>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。FTDCLI 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）。</p> <p>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。</p> <p>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)]</p>
デバイスのアップグレード	
<p>正常なデバイスアップグレードを元に戻します。</p>	<p>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。</p> <p>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 (⚙️) > [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。</p> <p>この機能は、コンテナインスタンスではサポートされません。</p> <p>必要最低限の FTD : 7.1</p>

新機能	説明
<p>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。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。
<p>Snort 3 後方互換性。</p>	<p>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する必要があります。Snort 2 とは異なり、新しい FMC（たとえば、バージョン 7.1）から展開して、古いデバイス（たとえば、バージョン 7.0）の検査エンジンを更新することはできません。</p> <p>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。</p>
<p>デバイス管理</p>	

新機能	説明
<p>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。</p>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • FTDv20 • FTDv30 • FTDv50 • FTDv100
<p>OCI 上の FTDv に対する Single Root I/O Virtualization (SR-IOV) のサポート</p>	<p>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。</p>
<p>Firepower 1100 の LLDP サポート。</p>	<p>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。</p> <p>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]</p> <p>新規/変更されたコマンド : show lldp status、show lldp neighbors、show lldp statistics</p> <p>サポートされるプラットフォーム : Firepower 1100 (1120、1140、および 1150)</p>
<p>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。</p>	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム : Firepower 1000/2100、Secure Firewall 3100</p>

新機能	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。	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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)]</p>
高可用性/拡張性	
<p>高可用性</p> <ul style="list-style-type: none"> • AWS 用 FMCv • OCI 用 FMCv 	<p>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。</p> <p>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。</p> <p>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)</p>
OCI 用 FTDv の自動スケール。	<p>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。</p> <p>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。</p>
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。	<p>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。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300、Secure Firewall 3100</p>

新機能	説明
<p>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。</p>	<p>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。</p>
NAT	
<p>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。</p>	<p>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。</p>
ルーティング	
<p>仮想ルータを相互接続するための BGP 設定。</p>	<p>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。</p> <p>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)]</p>
<p>ユーザー定義の仮想ルータでの BGPv6 サポート。</p>	<p>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。</p> <p>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]</p>
<p>Equal-Cost-Multi-Path (ECMP) ゾーンをサポート。</p>	<p>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。</p> <p>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。</p> <p>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]</p>
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	

新機能	説明
<p>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。</p>	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FTD</p>
<p>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。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。
リモートアクセス VPN	
<p>RA VPN ポリシーのコピー。</p>	<p>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。</p>

新機能	説明
AnyConnect VPN SAML外部ブラウザ。	<p>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。</p> <p>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。</p>
Microsoft Azure 上の SAML ID プロバイダーにおける複数のトラストポイント。	<p>Microsoft Azure の要求に応じて、SAML ID プロバイダーに複数の RA VPN トラストポイントを追加できるようになりました。</p> <p>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。</p>
サイト間 VPN	
VPN フィルタ。	<p>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。</p> <p>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。</p>
IKEv2 の一意のローカルトンネル ID。	<p>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。</p> <p>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。</p>
複数の IKE ポリシー。	<p>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。</p> <p>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。</p>

新機能	説明
VPN 監視ダッシュボード。	<p>ベータ版。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>(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。</p>
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。	<p>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。</p>
侵入検知と防御	

新機能	説明
<p>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。</p>	<p>バージョン 7.1 FMC は、バージョン 7.0 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。</p> <ul style="list-style-type: none"> • 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せん。 • 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。 <p>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。</p>
<p>TLS ベースの侵入ルールに対する Snort 3 のサポート。</p>	<p>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。</p>
<p>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。</p>	<p>アップグレードの影響。</p> <p>Snort 3 を使用したバージョン 7.1 は、SMB2 での DCE/RPC インスペクションをサポートします。</p> <p>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。</p>
<p>侵入ルールの推奨に対する Snort 3 のサポート。</p>	<p>バージョン 7.1 FMC は、バージョン 7.0 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。</p> <p>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。</p>

新機能	説明
<p>ssl_version および ssl_state キーワードに対する Snort 3 のサポート。</p>	<p>アップグレードの影響。</p> <p>Snort 3 を使用したバージョン 7.1 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。</p> <p>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/サードパーティールールを作成、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 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。</p>
Identity Services およびユーザー制御	
<p>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をサポート。</p>	<p>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。</p> <p>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。</p>
<p>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。</p>	<p>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。</p> <p>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ー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。</p> <p>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。</p>
暗号化トラフィックの処理 (TLS/SSL)	

新機能	説明
拡張 TLS/SSL ポリシー オプション。	<p>[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。</p> <ul style="list-style-type: none"> • 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。	<p>ベータ版。</p> <p>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。</p> <p>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。</p> <p>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)]</p> <p>(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。</p>
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。	<p>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。</p> <p>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)]。</p>
ネットワーク ディスカバリ	

新機能	説明
<p>ネットワーク検出の Snort3 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）。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>Snort3 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。</p>

イベントロギングおよび分析

新機能	説明
<p>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。</p>	<p>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。</p> <p>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。ヘルスマニタを使用して、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。</p> <p>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。</p> <p>新規/変更された FTD CLI コマンド：</p> <ul style="list-style-type: none"> • 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 <i>bytes-in-MB</i> • system support elephant-flow-detection time-threshold <i>time-in-seconds</i>
<p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>

新機能	説明
<p>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。</p>	<p>パフォーマンスを向上させるために、バージョン 7.1 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。</p> <p>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。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。</p>
<p>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。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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) <p>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。</p>
<p>パケットトレーサの機能拡張。</p>	<p>バージョン 7.1 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。</p> <ul style="list-style-type: none"> • 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)] > [トラブルシューティング (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。 <p>新規/変更された FTD CLI コマンド :</p> <ul style="list-style-type: none"> • <code>packet-tracer input source_interface pcap pcap_filename</code>

新機能	説明
オブジェクト管理	
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。	<p>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。</p> <p>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。</p>
統合	
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。	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>
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	

新機能	説明
ヘルスマonitoringの強化。	<p>ヘルスマonitorは次のように更新されました。</p> <ul style="list-style-type: none"> ヘルスポリシーエディタは、類似するヘルスマ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マ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。 ヘルスマonitor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。 <p>(注) 更新されたヘルスマonitorを使用するには、システム (⚙️) > [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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> システム (⚙️) > [正常性 (Health)] > [ポリシー (Policy)] > [ポリシーの編集 (Edit Policy)] システム (⚙️) > [正常性 (Health)] > [除外 (Exclude)] システム (⚙️) > [正常性 (Health)] > [アラートの監視 (Monitor Alerts)] システム (⚙️) > [正常性 (Health)] > [ポリシー (Policy)] > [ポリシーの展開 (Deploy Policy)]
展開履歴の機能拡張。	<p>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。</p>
グローバル検索の機能拡張。	<p>グローバル検索に次の機能が追加されました。</p> <ul style="list-style-type: none"> 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。

新機能	説明
新しいウォークスルー。	<p>次のウォークスルーが追加されました。</p> <ul style="list-style-type: none"> • 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。	<p>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。</p> <p>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。</p>
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。	<p>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。</p>

新機能	説明
Web インターフェイスの変更 : SecureX、脅威インテリジェンス、およびその他の統合。	

新機能	説明
	<p>バージョン 7.0.2 以降のバージョン 7.0.x メンテナンスリリースからアップグレードする場合、バージョン 7.1 では以下の FMC メニューオプションが変更されます。</p> <p>(注) これらの変更は、バージョン 7.2 で元に戻ります。</p> <p>[統合 (Integration)]>[AMP] は次 [AMP]>[AMP管理 (AMP >[AMP管理 (AMP Management)] に変 Management)] 更さ れま し た。</p> <p>[統合 (Integration)]>[AMP] は次 [AMP]>[ダイナミック分析接 >[ダイナミック分析接続 (Dynamic Analysis Connections)] に変 続 (Dynamic Analysis Connections)] 更さ れま し た。</p> <p>[統合 (Integration)]>[インテ は次 [インテリジェンス リジェンス (Intelligence)]> (Intelligence)]>[ソース [ソース (Sources)] に変 (Sources)] 更さ れま し た。</p> <p>[統合 (Integration)]>[インテ は次 [インテリジェンス リジェンス (Intelligence)]> (Intelligence)]>[要素 [要素 (Elements)] に変 (Elements)] 更さ れま し た。</p> <p>[統合 (Integration)]>[インテ は次 [インテリジェンス リジェンス (Intelligence)]> (Intelligence)]>[設定 [設定 (Settings)] に変 (Settings)] 更さ れま し た。</p> <p>[統合 (Integration)]>[インテ は次 [インテリジェンス リジェンス (Intelligence)]> (Intelligence)]>[インシデン [インシデント (Incidents)] 更さ ト (Incidents)] れま し</p>

新機能	説明
	<p>た。</p> <p>[統合 (Integration)]>[その他の統合 (Other Integrations)] は次に変更されました。</p> <p>システム (⚙️) > [統合 (Integration)]</p> <p>[統合 (Integration)]>[セキュリティ分析とロギング (Security Analytics and Logging)] は次に変更されました。</p> <p>システム (⚙️) > [ロギング (Logging)]>[セキュリティ分析とロギング (Security Analytics and Logging)]</p> <p>[統合 (Integration)]> [SecureX] は次に変更されました。</p> <p>システム (⚙️) > [SecureX]</p>

FMC REST API

FMC REST API サービス/操作。	FMC REST API の変更の詳細については、REST API クイックスタートガイド [英語] の「 What's New in 7.1 」を参照してください。
-----------------------	---

廃止された機能

表 11: FMC バージョン 7.1.0 で廃止された機能

廃止された機能	説明
サポート終了： FMC 1000、 2500、4500	FMC モデルの FMC 1000、2500、および 4500 ではバージョン 7.1 以降を実行できません。これらの FMC を使用してバージョン 7.1 以降のデバイスを管理することはできません。
サポート終了： ASA 5508-X およ び 5516-X	ASA 5508-X または 5516-X ではバージョン 7.1 以降を実行できません。

廃止された機能	説明
サポート終了： NGIPS ソフトウェア (ASA FirePOWERNGIPS)。	バージョン 7.1 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 の FMC を引き続き使用して、バージョン 6.5 ~ 7.0 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。
廃止：侵入インシデントと侵入イベントクリップボード。	<p>データと構成は削除される場合があります。</p> <p>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ました。アップグレードにより、インシデントに関連するすべてのデータが削除され、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 セクションが削除されます。</p> <p>廃止された画面/オプション：</p> <ul style="list-style-type: none"> • [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。
廃止：侵入イベントのカスタムテーブル。	<p>カスタムテーブルは削除される場合があります。</p> <p>バージョン 7.1 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。アップグレードにより、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。</p> <p>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。</p>
廃止：FlexConfig を使用した ECMP ゾーン。	<p>FlexConfig 設定は無視されます。展開ができない場合があります。</p> <p>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、Management Center の Web インターフェイスで Equal Cost Multipath (ECMP; 等コストマルチパス) ルーティングを設定できるようになりました。アップグレード後、FlexConfig を使用して設定した ECMP ゾーンは無視されます。等コストのスタティックルートが存在する状態で展開することはできず、それらのインターフェイスを ECMP ゾーンに割り当てる必要があります。</p>

廃止された機能	説明
<p>一時的に廃止： SecureX との統合、SecureX とのオーケストレーションの改善。</p>	<p>アップグレードができない場合があります。</p> <p>バージョン 7.1 では、バージョン 7.0.2 で導入された SecureX との統合およびオーケストレーションの改善を一時的に中止します。改善されたエクスペリエンスは、バージョン 7.2 で戻ります。</p> <p>バージョン 7.0.2 またはそれ以降のメンテナンスリリースで SecureX との統合を新たに有効にした場合は、バージョン 7.1 にアップグレードする前に、この機能を無効にする必要があります。アップグレードが正常に完了したら、以前の方法を使用して、この機能を再度有効にできます。バージョン 7.0.0 または 7.0.1 で SecureX との統合を有効にした場合、またはバージョン 7.2 にアップグレードする場合、アップグレードの際に問題は発生しません。</p>
<p>廃止：地理位置情報の詳細。</p>	<p>2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ (Cisco_GEODB_Update-date-build) です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合 (エアギャップ展開など)、IP パッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。</p>

FMC バージョン 7.0 の新機能

新機能

表 12: FMC バージョン 7.0.6 の新機能

新機能	説明
Web 分析プロバイダーを更新しました。	<p>アップグレードの影響。ブラウザは新しいリソースに接続します。</p> <p>Management Center を使用している間、ブラウザは Web 分析のために Google (google.com) ではなく Amplitude (amplitude.com) に接続します。</p> <p>Web 分析は、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、Management Center 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提供します。デフォルトで Web 分析に登録されていますが、初期設定の完了後にいつでも登録を変更できます。広告ブロッカーは Web 分析をブロックできるため、登録したままにする場合は、Cisco アプライアンスのホスト名/IP アドレスの広告ブロックを無効にしてください。</p> <p>必要最低限の Threat Defense : 任意</p> <p>バージョンの制限 : 振幅分析は、バージョン 7.0.0 ~ 7.0.5、7.1.0 ~ 7.2.4、または 7.3.x ではサポートされていません。サポートされているバージョンからサポートされていないバージョンにアップグレードすると、ブラウザは Google への接続を再開します。</p>

表 13: FMC バージョン 7.0.5 の新機能

新機能	説明
ISA 3000 システム LED によるシャットダウンのサポート。	<p>ISA 3000 をシャットダウンすると、システム LED が消灯します。その後、少なくとも 10 秒間待ってからデバイスの電源を切ってください。</p> <p>バージョンの制限 : バージョン 7.1 では、この機能のサポートが一時的に廃止されます。サポートは、バージョン 7.3 で再開されています。</p>

新機能	説明
CA バンドルの自動更新。	<p>アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。</p> <p>ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLIを使用して、この機能を無効にすることができます。</p> <p>新規/変更された CLI コマンド：configure cert-update auto-update、configure cert-update run-now、configure cert-update test、show cert-update</p> <p>バージョンの制限：この機能は、バージョン 7.0.0 ~ 7.0.4、7.1.0 ~ 7.1.0.2、または 7.2.0 ~ 7.2.3 ではサポートされていません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードすると、この機能は一時的に無効になり、システムはシスコへの接続を停止します。</p> <p>詳細については、『FMC configuration guide』の「Firepower Management Center Command Line Reference」、および「Cisco Secure Firewall Threat Defense コマンドリファレンス」を参照してください。</p>

表 14: FMC バージョン 7.0.3 の新機能

新機能	説明
クラウド提供型の管理センターの FTD サポート	

新機能	説明
	<p>バージョン 7.0.3 FTD デバイスは、2022 年春に導入されたクラウド提供型の管理センターによる管理をサポートします。このクラウド提供型の管理センターは、Cisco Defense Orchestrator (CDO) プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。更新についてはシスコが行います。</p> <p>次の場合は、クラウド提供型の管理センターでバージョン 7.0.3 FTD を使用する必要があります。</p> <ul style="list-style-type: none"> • 現在、お客様が導入したハードウェアまたは仮想 FMC を使用しています。 • 今すぐクラウド提供型の管理センターに移行したいと考えている。 • デバイスをバージョン 7.2 以降にアップグレードする必要はありません。バージョン 7.2 以降は、クラウド提供型の管理センターによる管理もサポートしています。 <p>この状況に当てはまる場合は、次のことを実行してください。</p> <ol style="list-style-type: none"> 1. 現在の FMC をバージョン 7.2 以降にアップグレードします。 <p>技術的にはバージョン 7.0.3 または 7.1 FMC を使用して FTD をバージョン 7.0.3 にアップグレードできますが、デバイスをクラウド提供型の管理センターに簡単に移行したり、イベントのログ記録と分析の目的でのみ（「分析のみ」）、お客様が導入した管理センターにデバイスを登録したままにしたりすることはできません。</p> 2. アップグレードされた FMC を使用して、デバイスをバージョン 7.0.3 にアップグレードします。 3. デバイスでクラウド管理を有効にします。 <p>バージョン 7.0.x デバイスの場合のみ、デバイス CLI から configure manager-cdo enable を実行してクラウド管理を有効にする必要があります。 show manager-cdo コマンドは、クラウド管理が有効になっているかどうかを表示します。</p> 4. CDO の [FTD をクラウドに移行する (Migrate FTD to cloud)] ウィザードを使用して、クラウド提供型の管理センターにデバイスを移行します。 <p>必要に応じて、お客様が導入した管理センターにデバイスを分析専用デバイスとして登録したままにします。あるいは、シスコのセキュリティ分析とロギング (SaaS) を使用して、Cisco Cloud にセキュリティイベントを送信できます。</p>

新機能	説明
	<p>クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している Threat Defense デバイス、または任意のバージョンを実行している従来のデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 7.0.x からバージョン 7.1 にアップグレードできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。</p> <p>新規/変更された CLI コマンド：configure manager add、configure manager delete、configure manager edit、show managers</p> <p>詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理を参照してください。</p>

表 15: FMC バージョン 7.0.2 の新機能

新機能	説明
ISA 3000 によるシャットダウンのサポート。	<p>ISA 3000 をシャットダウンできるようになりました。以前は、デバイスを再起動することしかできませんでした。</p> <p>(注) バージョン 7.1 では、この機能のサポートが一時的に廃止されます。サポートは、バージョン 7.2 で再開されています。</p>
ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。	<p>ダイナミックオブジェクト名でダッシュ文字を使用できるようになりました。これは、ACI エンドポイント更新アプリ（ダッシュ文字が許可されている）を使用して、テナントのエンドポイントグループを表すダイナミックオブジェクトを FMC で作成する場合に特に便利です。</p> <p>最低限の Threat Defense : 7.0.2</p>

新機能	説明
SecureX との統合、SecureX とのオーケストレーションの改善	<p>SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合 (Integration)] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureXの有効化 (Enable SecureX)] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、および Cisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。</p> <p>この新しいページで SecureX との統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。</p> <p>Web インターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング (SaaS) を使用して Secure Network Analytics (Stealthwatch) クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、システム (⚙) > [統合 (Integration)] > [クラウドサービス (Cloud Services)] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。</p> <p>Management Center は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップインターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。</p> <p>この機能の一部として、REST API を使用して SecureX との統合を設定できなくなりました。FMC の Web インターフェイスを使用する必要があります。</p> <p>バージョンの制限：この機能はバージョン 7.1 で一時的に廃止になりましたが、バージョン 7.2 で戻ります。新しい方法で SecureX との統合を有効にした場合は、バージョン 7.1.x にアップグレードする前に、この機能を無効にする必要があります。アップグレードが正常に完了したら、この機能を再度有効にできます。バージョン 7.2 以降へのアップグレードは影響を受けません。</p> <p>詳細については、Cisco Secure Firewall Management Center (7.0.2 および 7.2) および SecureX 統合ガイドを参照してください。</p>

新機能	説明
Web インターフェイスの変更 : SecureX、脅威インテリジェンス、およびその他の統合。	

新機能	説明
	<p>以下の FMC メニューオプションが変更されました。</p> <p>(注) これらの変更はバージョン 7.1 で一時的に非推奨になりましたが、バージョン 7.2 で復活しました。</p> <p>[AMP]>[AMP管理 (AMP Management)] は次に変更されました。 [統合 (Integration)]>[AMP]>[AMP管理 (AMP Management)]</p> <p>[AMP]>[ダイナミック分析接続 (Dynamic Analysis Connections)] は次に変更されました。 [統合 (Integration)]>[AMP]>[ダイナミック分析接続 (Dynamic Analysis Connections)]</p> <p>[インテリジェンス (Intelligence)]>[ソース (Sources)] は次に変更されました。 [統合 (Integration)]>[インテリジェンス (Intelligence)]>[ソース (Sources)]</p> <p>[インテリジェンス (Intelligence)]>[要素 (Elements)] は次に変更されました。 [統合 (Integration)]>[インテリジェンス (Intelligence)]>[要素 (Elements)]</p> <p>[インテリジェンス (Intelligence)]>[設定 (Settings)] は次に変更されました。 [統合 (Integration)]>[インテリジェンス (Intelligence)]>[設定 (Settings)]</p> <p>[インテリジェンス (Intelligence)]>[インシデント (Incidents)] は次に変更されました。 [統合 (Integration)]>[インテリジェンス (Intelligence)]>[インシデント (Incidents)]</p>

新機能	説明
	<p>システム (⚙️) > [統合 (Integration)]</p> <p>は次に変更されました。</p> <p>[統合 (Integration)]>[その他の統合 (Other Integrations)]</p>
	<p>システム (⚙️) > [ロギング (Logging)]> [セキュリティ分析とロギング (Security Analytics and Logging)]</p> <p>は次に変更されました。</p> <p>[統合 (Integration)]>[セキュリティ分析とロギング (Security Analytics and Logging)]</p>
	<p>システム (⚙️) > [SecureX]</p> <p>は次に変更されました。</p> <p>[統合 (Integration)]> [SecureX]</p>

表 16: FMC バージョン 7.0.1 の新機能

新機能	説明
Snort 3 の rate_filter インспекタ。	<p>Snort 3 rate_filter インспекタが導入されました。</p> <p>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。</p> <p>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спекタを設定します。</p> <p>サポートされるプラットフォーム：FTD</p> <p>バージョンの制限：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 (⚙️) > [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。</p>

新機能	説明
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	<p>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。</p> <p>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。</p> <p>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</p>

表 17: FMC バージョン 7.0.0 の新機能

新機能	説明
プラットフォーム	
VMware vSphere/VMware ESXi 7.0 のサポート。	<p>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。</p> <p>バージョン 7.0 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サポートされているバージョンにアップグレードします。</p>
新しい仮想環境。	<p>次の環境に FMCv および FTDv が導入されました。</p> <ul style="list-style-type: none"> • Cisco HyperFlex • Nutanix エンタープライズクラウド • OpenStack (FDM 管理のサポートなし)

新機能	説明
<p>FTDv パフォーマンス階層型のスマートライセンス。</p>	<p>アップグレードの影響。 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。</p> <p>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。</p> <p>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。</p> <p>FTDv をバージョン 7.0 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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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 (⚙️) > [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。
<p>高可用性/拡張性</p>	

新機能	説明
クラスタリング用の PAT ポートブロック割り当ての改善	<p>PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するには、FlexConfig を使用して cluster-member-limit コマンドを実行して、予定しているクラスタ内の最大ノード数を設定します。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。</p> <p>新規/変更されたコマンド：cluster-member-limit (FlexConfig)、show nat pool cluster [summary]、show nat pool ip detail</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
FTD CLI show cluster history の改善。	<p>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。</p> <p>新規/変更されたコマンド：show cluster history [brief] [latest] [reverse] [time]</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
クラスタから永久に削除するための FTD CLI コマンド。	<p>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。</p> <p>新規/変更されたコマンド：cluster reset-interface-mode</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
NAT	
優先順位付けされたシステム定義の NAT ルール。	<p>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す。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
仮想ルーティング	

新機能	説明
ISA 3000 の仮想ルータサポート。	<p>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。</p> <p>サポートされるプラットフォーム : ISA 3000</p>
サイト間 VPN	
<p>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)。</p>	<p>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。</p> <p>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ー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ーのエンドポイントに接続できます。</p> <p>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。</p> <p>サポートされるプラットフォーム : FTD</p>
Remote Access VPN	
ロードバランシング。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム : FTD</p>

新機能	説明
ローカル認証。	<p>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。</p> <ol style="list-style-type: none"> 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 (⚙️) > [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。 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。 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。 <p>サポートされるプラットフォーム : FTD</p>

新機能	説明
<p>ダイナミックアクセスポリシー。</p>	<p>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。</p> <ol style="list-style-type: none"> 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クセスメントを実行します。 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。 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。 <p>サポートされるプラットフォーム : FTD</p>
<p>マルチ証明書認証。</p>	<p>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。</p> <p>サポートされるプラットフォーム : FTD</p>
<p>AnyConnect カスタム属性。</p>	<p>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。</p> <p>サポートされるプラットフォーム : FTD</p>
<p>アクセス制御</p>	

新機能	説明
FTD 用 Snort 3。	

新機能	説明
	<p>新規に FTD を展開する場合、Snort 3 がデフォルトの検査エンジンになります。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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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。</p> <p>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</p>

新機能	説明
	<p data-bbox="797 289 1341 321">クが期待どおりに処理されるようになります。</p> <p data-bbox="664 359 1468 422">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</p> <p data-bbox="664 443 1143 474">サポートされるプラットフォーム : FTD</p>

新機能	説明
<p>ダイナミックオブジェクト。</p>	<p>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。</p> <p>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。</p> <p>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、を参照してください Cisco Secure 動的属性コネクタ コンフィギュレーションガイド。</p> <p>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。</p> <p>(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。</p> <p>サポート対象プラットフォーム：FMC</p> <p>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</p>

新機能	説明
Active Directory ドメインのクロスドメイン信頼。	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • レルムとディレクトリを同時に設定でき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 (⚙️) > [統合 (Integration)] > [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。 <p>サポート対象プラットフォーム：FMC</p>
DNS フィルタリング。	<p>バージョン 6.7 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。</p> <p>サポートされるプラットフォーム：すべて</p>
イベントロギングおよび分析	

新機能	説明
<p>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。</p>	<p>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。</p> <ol style="list-style-type: none"> 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 (⚙️) > [ロギング (Logging)] > [セキュリティ分析とロギング (Security Analytics & Logging)] 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。 <p>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。</p> <p>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、Cisco Security Analytics and Logging（オンプレミス）：ファイアウォールイベント統合ガイド を参照してください。</p> <p>サポート対象プラットフォーム：FMC</p>

新機能	説明
<p>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。</p>	<p>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。</p> <p>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。</p> <p>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)])。</p> <p>(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。</p> <p>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。</p> <p>サポート対象プラットフォーム : FMC</p>

新機能	説明
<p>すべての接続イベントを Secure Network Analytics クラウドに保存する。</p>	<p>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。</p> <p>クラウドに送信するイベントを変更するには、システム (⚙️) > [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。</p> <p>(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。</p> <p>サポート対象プラットフォーム：FMC</p>
<p>統合イベントビューア。</p>	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>

新機能	説明
SecureX のリボン。	<p>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。</p> <p>SecureX に接続してリボンを有効にするには、[システム (System)] > [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 (⚙️) > [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。</p> <p>詳細については、Cisco Secure Firewall Threat Defense および SecureX 統合ガイドを参照してください。</p> <p>サポート対象プラットフォーム : FMC</p>
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せん。	<p>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。</p> <p>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るようになります。これを行うには、システム (⚙️) > [設定 (Configuration)] > [データベース (Database)] で [最大接続イベント数 (Maximum Connection Events)] を 0 に設定します。</p> <p>(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。</p> <p>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。</p> <p>サポート対象プラットフォーム : FMC</p>

新機能	説明
ファイルおよびマルウェアイベントテーブルと一緒に表示されるポートとプロトコル。	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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)] <p>サポートされるプラットフォーム：FMC</p>
アップグレード	
FTD の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。	<p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
FTD の [アップグレード (Upgrade)] ウィザード。	

新機能	説明
	<p>FMCの新しいデバイスアップグレードページ ([デバイス (Devices)] > [デバイスアップグレード (Device Upgrade)]) には、バージョン 6.4 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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>(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 (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。</p> <p>(注) バージョン 7.0 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。</p> <p>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</p>

新機能	説明
	<p>ることを手動で確認します。</p> <p>サポートされるプラットフォーム：FTD</p>
<p>多くの FTD デバイスを一度にアップグレードします。</p>	<p>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。</p> <ul style="list-style-type: none"> • デバイスの同時アップグレード。 <p>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。</p> <p>重要 この改善は、FTD バージョン 6.7 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。</p> <ul style="list-style-type: none"> • デバイスモデルによるアップグレードのグループ化。 <p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
管理とトラブルシューティング	
<p>SD カードを使用した ISA 3000 でのゼロタッチ復元。</p>	<p>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 ～ 15 秒間押します。</p> <p>サポートされるプラットフォーム：ISA 3000</p>

新機能	説明
RA およびサイト間 VPN ポリシーを選択的に展開する。	<p>バージョン 6.6 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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
<p>新しいヘルスマジュール。</p>	<p>次の正常性モジュールが追加されました。</p> <ul style="list-style-type: none"> • 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 <p>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 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。</p> <p>サポート対象プラットフォーム : FMC</p>
<p>セキュリティと強化</p>	

新機能	説明
AWS 導入用の新しいデフォルトパスワード。	<p>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。</p> <p>以前は、デフォルトの admin パスワードは Admin123 でした。</p> <p>サポートされているプラットフォーム：FMCv for AWS、FTDv for AWS</p>
証明書の登録用の EST。	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
EdDSA 証明書タイプのサポート。	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
NTP サーバーの AES-128 CMAC 認証。	<p>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。</p> <p>新規/変更されたページ：システム (⚙️) >[構成（Configuration）]>[時刻の同期（Time Synchronization）]。</p> <p>サポートされるプラットフォーム：FMC</p>
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。	<p>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。</p> <p>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）]</p> <p>サポートされるプラットフォーム：FTD</p>

ユーザビリティとパフォーマンス

新機能	説明
ポリシーとオブジェクトのグローバル検索。	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
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。	<p>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。リポートすると、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。</p> <p>サポートされるプラットフォーム：VMware の FTDv、KVM の FTDv</p>
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。	<p>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。</p> <p>次のコマンドが変更されました：clear local-host (廃止)、show local-host</p> <p>サポートされるプラットフォーム：FTD</p>
使用方法の場所が変更されました。	<p>[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。</p>
<h3>FMC REST API</h3> <p>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。</p>	
デバイス	alerts : GET
統合	fmchastatuses : GET securexconfigs : GET および PUT

新機能	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 groupolicies : 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、sidnlists、sinetworkfeeds、sinetworklists : GET sinkholes : GET sso servers : GET sso servers/overrides : GET usage : GET

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

廃止された機能

表 18: FMC バージョン 7.0.0 で廃止された機能

廃止された機能	説明
サポートの終了 : VMware vSphere/VMware ESXi 6.0。	VMware vSphere/VMware ESXi 6.0 での仮想展開のサポートは廃止されました。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サポートされているバージョンにアップグレードします。

廃止された機能	説明
<p>廃止：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。</p>	<p>FTD 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。</p> <p>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 証明書のサポートは削除されました。</p> <p>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。</p> <p>弱いオプションを使用して古い FTD デバイス (バージョン 6.4 ~ 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。</p>
<p>廃止：SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化。</p>	<p>ユーザーを削除します。アップグレード後に展開ができないようにします。</p> <p>FTD 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ました。</p> <p>FTD をバージョン 7.0 以上にアップグレードすると、FMC の設定に関係なく、該当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、FTD 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。</p> <p>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。</p>
<p>廃止：AMP クラウドとのポート 32137 通信。</p>	<p>FMC がアップグレードされないようにします。</p> <p>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 FMC オプションは廃止されました。プロキシを設定しない限り、FMC はポート 443/HTTPS を使用するようになりました。</p> <p>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。</p>

廃止された機能	説明
廃止：HA ステータス正常性モジュール。	HA ステータス正常性モジュールの名前を <i>FMCHA</i> ステータス正常性モジュールに変更しました。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。
廃止：レガシー API エクスプローラ。	FMC REST API レガシー API エクスプローラのサポートが削除されました。
廃止：地理位置情報の詳細。	<p>2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ (<i>Cisco_GEODB_Update-date-build</i>) です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合 (エアギャップ展開など)、IP パッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。</p>

FMC バージョン 6.7 の新機能

新機能

表 19: FMC バージョン 6.7.0 の新機能

新機能	説明
プラットフォーム	
OCI および GCP の FMCv および FTDv。	<p>次の環境に FMCv および FTDv が導入されました。</p> <ul style="list-style-type: none"> • Oracle Cloud Infrastructure (OCI) • Google Cloud Platform (GCP)

新機能	説明
VMware 向け FMCv での高可用性のサポート。	<p>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。</p> <p>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。</p> <p>この機能は、VMware 向け FMCv2（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。</p> <p>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</p>
AWS 向け FTDv の自動スケールの改善。	<p>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。</p> <ul style="list-style-type: none"> • 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ル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。 <p>サポートされているプラットフォーム：AWS の FTDv</p>
Azure 向け FTDv の自動スケールの改善。	<p>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）に基づくスケール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。</p> <p>サポートされているプラットフォーム：Azure の FTDv</p>
Firepower Threat Defense：デバイス管理	

新機能	説明
データインターフェイスでの FTD の管理。	<p>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。</p> <p>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。</p> <p>(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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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 <p>新規/変更された FTD CLI コマンド：configure network management-data-interface、configure policy rollback</p> <p>サポートされるプラットフォーム：FTD</p>
FTD での FMC IP アドレスの更新。	<p>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。</p> <p>新規/変更された FTD CLI コマンド：configure manager edit</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
<p>Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期。</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>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)]</p> <p>新規/変更された FXOS コマンド : set link-state-sync enabled、show interface expand detail</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

新機能	説明
<p>Firepower 1100/2100 シリーズの SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>[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。</p> <p>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)]</p> <p>サポートされるプラットフォーム : Firepower 1100/2100 シリーズ</p>
Firepower Threat Defense : クラスタリング	
<p>FMC の新しいクラスタ管理機能。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [Devices] > [Device Management] > [More] メニュー • [Devices] > [Device Management] > [Cluster] > [General] エリア > [Cluster Live Status] リンク > [Cluster Status] <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>クラスタ導入の高速化。</p>	<p>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。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

新機能	説明
<p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>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 ～ 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。</p> <p>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 ～ 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 ～ 1023 のポート範囲を含めることができます。</p> <p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム : FTD</p>
<p>Firepower Threat Defense : 暗号化と VPN</p>	

新機能	説明
<p>RA VPN の AnyConnect モジュールサポート。</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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 <p>サポートされるプラットフォーム：FTD</p>
<p>RA VPN の AnyConnect 管理 VPN トンネル。</p>	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
RA VPN のシングルサインオン。	<p>FTD RA VPN は、SAML 2.0 準拠のアイデンティティプロバイダー (IdP) で設定されたリモートアクセス VPN ユーザーのシングルサインオン (SSO) をサポートするようになりました。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> 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。 <p>サポートされるプラットフォーム：FTD</p>
RA VPN の LDAP 許可。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	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。	<p>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。</p> <p>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。</p> <p>VTI ベースの VPN は、次の間で作成できます。</p> <ul style="list-style-type: none"> • 2 つの FTD デバイス • FTD デバイスとパブリッククラウド • FTD デバイスとサービスプロバイダーの冗長性を備えた別の FTD デバイス <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [Devices] > [Device Management] > [Interfaces] > [Add Interfaces] > [Virtual Tunnel Interface] • [Devices] > [VPN] > [Site To Site] > [Add VPN] > [Firepower Threat Defense Device] > [Route Based (VTI)] <p>サポートされるプラットフォーム：FTD</p>
サイト間 VPN に対するダイナミック RRI サポート。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
<p>手動証明書登録の拡張機能。</p>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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)]</p> <p>サポートされるプラットフォーム：FTD</p>
<p>FTD 証明書管理の拡張機能。</p>	<p>FTD 証明書管理に次の機能拡張が行われました。</p> <ul style="list-style-type: none"> • 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。 <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [Devices] > [Certificates] > [Status] 列 > [View] アイコン (虫めがね) • [Devices] > [Certificates] > [Export] アイコン <p>サポートされるプラットフォーム：FTD</p>
<p>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</p>	

新機能	説明
<p>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。</p>	<p>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。</p> <p>(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。</p> <p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
<p>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。</p>	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>

新機能	説明
<p>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。</p>	<p>ベータ版。</p> <p>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。</p> <p>(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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
<p>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。</p>	<p>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。</p> <p>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があります。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
<p>アクセス制御：ユーザー制御</p>	

新機能	説明
<p>ISE/ISE-PIC を使用した pxGrid 2.0。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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、関連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。</p> <p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム：FMC</p>
<p>レルムシーケンス。</p>	<p>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。</p> <p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>

新機能	説明
ISE サブネットフィルタリング。	<p>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。</p> <p>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。</p> <p>新しいデバイス CLI コマンド: configure identity-subnet-filter {add remove}</p> <p>サポートされるプラットフォーム: FMC 管理対象デバイス</p>
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。	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム: FMC</p>
S7Commplus プリプロセッサ。	<p>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。</p> <p>新規/変更されたページ:</p> <ul style="list-style-type: none"> • 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。 <p>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</p>

新機能	説明
<p>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。</p>	<p>カスタム（ローカル）侵入ルールの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。</p> <p>[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。</p> <p>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のインポートしようとする、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールのインポートするためのベストプラクティスを参考にすることを推奨します。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
<p>アクセス制御：TLS/SSL 暗号解読</p>	
<p>復号の既知キー TLS/SSL ルールのための ClientHello の変更。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>照合は ClientHello メッセージからのデータとキャッシュされたサーバー証明書データからのデータに依存します。メッセージが一致すると、ClientHello メッセージが特定の方法で変更されます。FMC コンフィギュレーションガイドの「ClientHello メッセージ処理」のトピックを参照してください。</p> <p>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。</p> <p>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</p>
<p>イベントロギングおよび分析</p>	

新機能	説明
<p>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。</p>	<p>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。</p> <p>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。</p> <p>(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。</p> <p>サポートされるプラットフォーム：FMC</p>
<p>Stealthwatch コンテキスト相互起動リソースを迅速に追加する。</p>	<p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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] <p>サポート対象プラットフォーム：FMC</p>

新機能	説明
<p>新しい相互起動オプションフィールドタイプ。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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) <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • 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。 <p>サポートされるプラットフォーム : FMC</p>
<p>National Vulnerability Database (NVD) が Bugtraq に代わって使用されるようになりました。</p>	<p>アップグレードの影響。</p> <p>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。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <p>サポートされるプラットフォーム : FMC</p>
<p>アップグレード</p>	

新機能	説明
アップグレード前の互換性チェック。	

新機能	説明
	<p>アップグレードの影響。</p> <p>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。</p> <p>検出は次のとおりです。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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]

新機能	説明
	サポートされるプラットフォーム : FMC、FTD

新機能	説明
準備状況チェックの改善。	<p>アップグレードの影響。</p> <p>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进行评估できます。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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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] • [Message Center] > [Tasks] <p>サポートされるプラットフォーム：FTD</p>

新機能	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。	

新機能	説明
	<p>アップグレードの影響。</p> <p>[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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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] <p>新しい FTD CLI コマンド：</p> <ul style="list-style-type: none"> • show upgrade status detail • show upgrade status continuous • show upgrade status

新機能	説明
	<ul style="list-style-type: none"> • upgrade cancel • upgrade retry <p>サポートされるプラットフォーム：FTD</p>
<p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>(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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
<p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>サポートされているプラットフォーム：すべて</p>
<p>展開とポリシー管理</p>	

新機能	説明
設定のロールバック。	<p>ベータ版。</p> <p>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。</p> <p>(注) ロールバックはベータ機能であり、すべての展開タイプとシナリオでサポートされているわけではありません。これは中断を伴う操作でもあります。FMC コンフィギュレーションガイドの「ポリシー管理」の章に記載されているガイドラインと制限事項を必ず読んで理解してください。</p> <p>新規/変更されたページ：[Deploy] > [Deployment History] > [Rollback] 列とアイコン。</p> <p>サポートされるプラットフォーム：FTD</p>
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。	<p>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。</p> <p>新規/変更されたページ：[展開 (Deploy)] > [展開 (Deployment)]</p> <p>サポートされるプラットフォーム：FMC</p>
アクセス制御ルールのコメントの検索。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
FTD NAT ルールの検索とフィルタリング。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
アクセスコントロールポリシーとプレフィルタポリシー間のルールのコピーおよび移動。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
オブジェクト一括インポート。	<p>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。</p> <p>制限事項および特定のフォーマット手順については、FMC コンフィギュレーション ガイドの「再利用可能なオブジェクト」の章を参照してください。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>
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。	<p>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。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
管理とトラブルシューティング	
FMC シングルサインオン。	<p>FMC は、サードパーティの SAML 2.0 準拠アイデンティティプロバイダー (IdP) で設定された外部ユーザーのシングルサインオン (SSO) をサポートするようになりました。IdP のユーザーまたはグループロールを FMC ユーザーロールにマッピングできます。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [Login] > [Single Sign-On] • [System] > [Users] > [SSO] <p>サポートされるプラットフォーム：FMC</p>
FMC ログアウトの遅延。	<p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
FTD コンテナインスタンスのバックアップと復元。	<p>FMC を使用してバージョン 6.7.0 以降の FTD コンテナインスタンスをバックアップおよび復元できるようになりました。</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
ヘルスマonitoringの強化。	<p>ヘルスマonitoringが次のように拡張されました。</p> <ul style="list-style-type: none"> • [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マonitorer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関連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、カスタム関連ダッシュボードを作成します。 <p>サポートされるプラットフォーム：FMC</p>

新機能	説明
ヘルスモジュールの更新。	<p>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れました。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>サポートされるプラットフォーム：FMC</p>
メッセージセンターの検索。	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
ユーザビリティとパフォーマンス	

新機能	説明
Dusk テーマ。	<p>ベータ版。</p> <p>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。</p> <p>(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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>
FMC メニューの検索。	<p>FMC メニューを検索できるようになりました。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
Firepower Management Center REST API	

新機能	説明
新しい REST API サービス。	<p>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。</p> <p>認可サービス：</p> <ul style="list-style-type: none"> • <code>ssoconfig</code>：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。 <p>ヘルスサービス：</p> <ul style="list-style-type: none"> • <code>metrics</code>：ヘルスマニターのメトリックを取得する GET 操作。 • <code>alerts</code>：ヘルスアラートを取得する GET 操作。 • <code>deploymentdetails</code>：展開の正常性の詳細を取得する GET 操作。 <p>展開サービス：</p> <ul style="list-style-type: none"> • <code>jobhistories</code>：展開履歴を取得する GET 操作。 • <code>rollbackrequests</code>：設定ロールバックを要求する POST 操作。 <p>デバイスサービス：</p> <ul style="list-style-type: none"> • <code>metrics</code>：デバイスマトリックを取得する GET 操作。 • <code>virtualtunnelinterfaces</code>：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。 <p>統合サービス：</p> <ul style="list-style-type: none"> • <code>externalstorage</code>：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。 <p>ポリシーサービス：</p> <ul style="list-style-type: none"> • <code>intrusionpolicies</code>：侵入ポリシーを変更するための POST および DELETE 操作。 <p>サービスの更新：</p> <ul style="list-style-type: none"> • <code>cancelupgrades</code>：失敗したアップグレードをキャンセルする POST 操作。 • <code>retryupgrades</code>：失敗したアップグレードを再試行する POST 操作。 <p>サポート対象プラットフォーム: FMC</p>

廃止された機能

表 20: FMC バージョン 6.7.0 で廃止された機能

廃止された機能	説明
サポート終了： Firepower ソフトウェアを使用した ASA 5525-X、5545-X、および 5555-X デバイス。	ASA 5525-X、5545-X、および 5555-X でバージョン 6.7 以降は実行できません。
廃止：Cisco Firepower User Agent ソフトウェアとアイデンティティソース。	<p>FMC がアップグレードされないようにします。</p> <p>ユーザーエージェント設定を使用して FMC をバージョン 6.7 以降にアップグレードすることはできません。</p> <p>バージョン 6.6 は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) に切り替える必要があります。ライセンスを変換するには、販売担当者にお問い合わせください。</p> <p>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。</p> <p>廃止された FTD CLI コマンド：configure user agent</p>
廃止：Cisco ISE エンドポイント保護サービス (EPS) の修復。	<p>ISE 修復が機能しなくなることがあります。</p> <p>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。</p> <p>「不正な」pxGrid を使用して FMC を ISE/ISE-PIC アイデンティティソースに接続している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。</p>

廃止された機能	説明
<p>廃止：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。</p>	<p>FMC がアップグレードされないようにします。</p> <p>次の FTD 機能のいずれかを使用している場合、FMC をアップグレードできないことがあります。</p> <ul style="list-style-type: none"> • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の FMC 展開で引き続きサポートされますが、より強力なオプションに変更することをお勧めします。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • NULL の「暗号化アルゴリズム」（暗号化なしの認証、テスト目的）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルの FMC 展開で引き続きサポートされます。ただし、IKEv2 ポリシーではサポートされなくなりました。 • ハッシュアルゴリズム：MD5。 <p>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。</p>

廃止された機能	説明
<p>廃止：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）。</p>	<p>ヘルスマニターでのアップグレード後のエラーの可能性。</p> <p>バージョン 6.7 では、バージョン 6.6.3 で導入され、後続のすべての 6.6.x リリースでサポートされるアプライアンス設定のリソース使用率の正常性モジュールに関するサポートが部分的かつ一時的に廃止されています。</p> <p>バージョン 6.7 のサポートは次のとおりです。</p> <ul style="list-style-type: none"> バージョン 6.6.3 以降からバージョン 6.7 への FMC のアップグレード <p>デバイスがバージョン 6.6.x のままである場合にのみ、モジュールのサポートが継続されます。デバイスをバージョン 6.7 にアップグレードすると、モジュールは動作を停止し、正常性モニターにエラーが表示されます。エラーを解決するには、FMC を使用してモジュールを無効にし、ポリシーを再適用します。</p> <ul style="list-style-type: none"> バージョン 6.3 ～ 6.6.1 からバージョン 6.7.0 への FMC のアップグレード、または FMC バージョン 6.7 の新規インストール。 <p>このモジュールはサポートされていません。</p> <p>モジュールがサポートされていない FMC にモジュールが有効になっているバージョン 6.6.x デバイスを追加するまれなケースでは、解決できないエラーがヘルスマ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。</p> <p>バージョン 7.0 ではフルサポートが提供され、モジュールの名前が構成メモリ割り当てに変更されています。</p>
<p>廃止：その他のヘルスマニターモジュール（永久的）。</p>	<p>バージョン 6.7 では、次のヘルスマニターモジュールが廃止されています。</p> <ul style="list-style-type: none"> 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。上記の新機能の表を参照してください。 ローカルマルウェア分析：このモジュールは、バージョン 6.3 のデバイス上の脅威データの更新モジュールに置き換えられました。バージョン 6.7 以降の FMC は、古いモジュールが適用されるデバイスを管理できなくなります。 ユーザーエージェントステータスマニター：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。
<p>廃止：クラシックテーマを使用したウォークスルー。</p>	<p>バージョン 6.7 では、クラシックテーマの FMC ウォークスルー（使用方法）が廃止されました。ユーザー設定でテーマを切り替えることができます。</p>

廃止された機能	説明
廃止：Bugtraq	<p>バージョン 6.7 では Bugtraq のデータベースフィールドとオプションが削除されます。Bugtraq 脆弱性データは使用できなくなりました。現在、ほとんどの脆弱性データは National Vulnerability Database (NVD) から取得されています。</p> <p>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。</p>
廃止：Microsoft Internet Explorer	<p>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。</p>
廃止：地理位置情報の詳細。	<p>2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ (Cisco_GEODB_Update-date-build) です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合 (エアギャップ展開など)、IP パッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。</p>

FMC バージョン 6.6 の新機能

新機能

表 21: FMC バージョン 6.6.3 の新機能

新機能	説明
<p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>(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。</p> <p>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。</p>

新機能	説明
<p>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。</p>	<p>バージョン 6.7.0 のアップグレードの影響。</p> <p>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。</p> <p>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、コンフィギュレーションガイドの「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。</p> <p>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、モニタリングを開始します。</p> <p>(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 以降が必要です。</p> <p>バージョン 6.7 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 の新機能 (120 ページ) を参照してください。バージョン 7.0 ではフルサポートが提供され、モジュールの名前が構成メモリ割り当てに変更されています。</p>

表 22: FMC バージョン 6.6.0 の新機能

新機能	説明
プラットフォーム	
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。

新機能	説明
AWS の展開用の大型のインスタンス。	<p>アップグレードの影響。</p> <p>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。</p> <ul style="list-style-type: none"> • C5.xlarge • C 5.2 xlarge • C5.4xlarge <p>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。</p> <ul style="list-style-type: none"> • C3.4xlarge • C4.4xlarge • C5.4xlarge <p>AWS インスタンスタイプの既存の FMCv はすべて廃止になりました (c3.xlarge、c3.2xlarge、c4.xlarge、c4.2xlarge)。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、リリースノートのバージョン 6.6 のアップグレードガイドラインを参照してください。</p>
クラウドベースの FTDv 展開の自動スケール。	<p>AWS 自動スケール/Azure 自動スケールのサポートが導入されました。</p> <p>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。</p> <p>サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure</p>
Firepower Threat Defense : デバイス管理	
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。	<p>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。</p> <p>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。</p> <p>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</p>

新機能	説明
CLI での MTU 値の設定。	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>新しい FTD CLI コマンド：configure network mtu</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
内部 Web サーバーからの Threat Defense アップグレードパッケージの取得。	<p>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 とそのデバイスと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。</p> <p>(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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>
接続ベースのトラブルシューティングの機能拡張。	<p>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 (デバッグ)。</p> <ul style="list-style-type: none"> • 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。 <p>サポートされるプラットフォーム：FTD</p>
Firepower Threat Defense：クラスタリング	

新機能	説明
<p>マルチインスタンスクラスタリング。</p>	<p>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。</p> <p>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。</p> <p>新しい FXOS CLI コマンド : set port-type cluster</p> <p>新規/変更された Chassis Manager ページ :</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>FTD クラスタでのデータユニットへのパラレル設定同期。</p>	<p>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。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>クラスタへの参加の失敗や削除のメッセージを show cluster history に追加。</p>	<p>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。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>Firepower Threat Defense : ルーティング</p>	

新機能	説明
仮想ルータと VRF-Lite。	<p>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。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>新しい FTD CLI コマンド：show vrf。</p> <p>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。</p> <p>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)</p>
Firepower Threat Defense : VPN	
リモートアクセス VPN 内の DTLS 1.2。	<p>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。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>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)</p>

新機能	説明
<p>複数のピアに対するサイト間 VPN IKEv2 のサポート。</p>	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム : FTD</p>
セキュリティ ポリシー	
<p>セキュリティポリシーの使いやすさの向上。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>サポートされるプラットフォーム : FMC</p>

新機能	説明
<p>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。</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>
<p>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。</p>	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • 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)] <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
出力最適化の再有効化。	<p>アップグレードの影響。</p> <p>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。</p> <ul style="list-style-type: none"> 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。 <p>サポートされるプラットフォーム：FTD</p>
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の向上。	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
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。	<p>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。</p> <p>サポート対象プラットフォーム：FMC</p>

新機能	説明
<p>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リング。</p>	<p>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）のモニタリングが新たにサポートされるようになります。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム：上記の FTD デバイス</p>
<p>IBM QRadar との統合。</p>	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
<p>管理とトラブルシューティング</p>	

新機能	説明
設定変更を展開するための新しいオプション。	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [展開 (Deploy)] > [展開 (Deployment)] • [展開 (Deploy)] > [展開履歴 (Deployment History)] <p>サポート対象プラットフォーム : FMC</p>

新機能	説明
<p>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。</p>	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>アップグレードされた FMC は影響を受けません。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> [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))] <p>サポート対象プラットフォーム：FMC</p>
<p>FMC を復元するための VDB の一致は不要。</p>	<p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
<p>サブジェクト代替名 (SAN) を使用した HTTPS 証明書。</p>	<p>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。</p> <p>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</p> <p>サポート対象プラットフォーム：FMC</p>
<p>FMC ユーザーアカウントに関連付けられている実名。</p>	<p>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。</p> <p>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</p> <p>サポート対象プラットフォーム：FMC</p>

新機能	説明
追加の FTD プラットフォームでの Cisco Support Diagnostics。	<p>アップグレードの影響。</p> <p>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。</p> <p>サポートされるプラットフォーム：FMC、FTD</p>
ユーザビリティ	
ライトテーマ。	<p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
アップグレードの残り時間の表示。	<p>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、レポート時間は含まれません。</p> <p>新規/変更されたページ：メッセージセンター</p> <p>サポート対象プラットフォーム：FMC</p>
セキュリティと強化	
デフォルトの HTTPS サーバー証明書の更新期限は 800 日。	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
Firepower Management Center REST API	

新機能	説明
<p>新しい REST API 機能。</p>	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <ul style="list-style-type: none"> • intrusionrules、intrusionpolicies : 侵入ポリシー <p>サポート対象プラットフォーム : FMC</p>
<p>拡張アクセスリストの REST API サービス名の変更。</p>	<p>アップグレードの影響。</p> <p>FMC REST API の extendedaccesslist (単数形) サービスは、extendedaccesslists (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。</p> <p>要求タイプ : GET</p> <p>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 :</p> <ul style="list-style-type: none"> • 旧 : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • 新 : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists/{objectId} <p>すべての拡張アクセスリストを取得するための URL :</p> <ul style="list-style-type: none"> • 旧 : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • 新 : /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslists <p>サポート対象プラットフォーム : FMC</p>

廃止された機能

表 23: バージョン 6.6.1 で廃止された機能

廃止された機能	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。	<p>バージョン 6.6.0 では、ルールの競合があった場合、FMC 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 より前の動作に戻ります。</p> <p>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、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーション ガイドでローカル侵入ルールのインポートするためのベストプラクティスを参考にすることを推奨します。</p> <p>バージョン 6.7 では、ルールの競合に関する警告が追加されます。</p>

表 24: バージョン 6.6.0 で廃止された機能

廃止された機能	説明
廃止：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。	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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、リリースノート バージョン 6.6 のアップグレードガイドライン を参照してください。</p> <p>さらに、バージョン 6.6 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。</p>

廃止された機能	説明
<p>廃止：VMware 向け FTDv の e1000 インターフェイス。</p>	<p>アップグレードされないようにします。</p> <p>バージョン 6.6 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。</p> <p>詳細については、『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。</p>
<p>廃止：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。</p>	<p>バージョン 6.6 では、次の FTD セキュリティ機能は廃止されます。</p> <ul style="list-style-type: none"> • 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。 <p>これらの機能はバージョン 6.7 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。</p>
<p>廃止：接続イベントのカスタムテーブル。</p>	<p>バージョン 6.6 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。</p> <p>他のタイプのカスタムテーブルに変更はありません。</p> <p>廃止されたオプション：</p> <ul style="list-style-type: none"> • [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

廃止された機能	説明
<p>廃止：イベントビューアから接続イベントを削除する機能。</p>	<p>バージョン 6.6 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。</p> <p>廃止されたオプション：</p> <ul style="list-style-type: none"> • [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)]
<p>廃止：地理位置情報の詳細。</p>	<p>2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ (<code>Cisco_GEODB_Update-date-build</code>) です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合 (エアギャップ展開など)、IP パッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。</p>

FMC バージョン 6.5 の新機能

新機能

表 25: FMC バージョン 6.5.0 パッチの新機能

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	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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

表 26: FMC バージョン 6.5.0 の新機能

機能	説明
プラットフォーム	
Firepower 1150 上の FTD。	Firepower 1150 が導入されました。
Azure 向け FTDv がより大規模なインスタンスに対応。	Microsoft Azure 向けの FTDv 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。	<p>VMware 向けのより大規模な FMCv である FMCv 300 が導入されました。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。</p> <p>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。</p>

機能	説明
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。
Firepower Threat Defense	
Firepower 1010 ハードウェア スイッチのサポート	<p>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。</p> <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [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)] <p>サポートされるプラットフォーム : Firepower 1010</p>
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	<p>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。</p> <p>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]</p> <p>サポートされるプラットフォーム : Firepower 1010</p>
キャリアグレード NAT の拡張	<p>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)。</p> <p>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</p> <p>サポートされるプラットフォーム : FTD</p>

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	<p>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。</p> <p>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、createhw-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 Secure Firewall Threat Defense コマンドリファレンスを参照してください。</p> <p>新しい FXOS CLI コマンド：</p> <ul style="list-style-type: none"> • create hw-crypto • delete hw-crypto • scope hw-crypto • show hw-crypto <p>削除された FXOS CLI コマンド：</p> <ul style="list-style-type: none"> • show hwCrypto (show hw-crypto に置き換えられました) • config hwCrypto <p>削除された FTD CLI コマンド：</p> <ul style="list-style-type: none"> • show crypto accelerator status <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
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	<p>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。</p> <p>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)])</p> <p>サポートされるプラットフォーム：FMC</p>

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	<p>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。</p> <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム : FMC</p>
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	<p>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。</p> <p>新しい接続イベントフィールド :</p> <ul style="list-style-type: none"> • [宛先SGT (Destination SGT)] (syslog : DestinationSecurityGroupTag) : 接続レスポンスの SGT 属性。 <p>名前が変更された接続イベントフィールド :</p> <ul style="list-style-type: none"> • [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。 <p>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</p> <p>サポートされるプラットフォーム : すべて</p>

機能	説明
Cisco Firepower User Agent バージョン 2.5 の統合	<p>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。</p> <p>(注) バージョン 6.6 は、Cisco Firepower User Agent ソフトウェアをアイデンティティソースとしてサポートする最後のリリースです。ユーザーエージェント設定を使用してFMCをバージョン 6.7以降にアップグレードすることはできません。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。</p> <p>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。</p> <p>新規/変更された FMC CLI コマンド : configure user-agent</p> <p>サポートされるプラットフォーム : FMC</p>
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	<p>TID ブロッキングおよびモニタ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リングよりも優先されるようになりました。</p> <p>[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。</p> <ul style="list-style-type: none"> • 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)] のバリエーションになります。 • 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。 <p>[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。</p> <ul style="list-style-type: none"> • 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)] のバリエーションになります。 • 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。 <p>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。</p> <p>(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。</p> <p>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、FMC コンフィギュレーション ガイドの「<i>TID-Firepower Management Center</i> のアクションの優先順位付け」の情報を参照してください。</p> <p>サポートされるプラットフォーム : FMC</p>

機能	説明
packet-profile CLI コマンド	<p>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。</p> <p>新しい FTD CLI コマンド：</p> <ul style="list-style-type: none"> • asp packet-profile • no asp packet-profile • show asp packet-profile • clear asp packet-profile <p>サポートされるプラットフォーム：FTD</p>
Cisco SecureX に対応したその他のイベントタイプ	<p>Firepower では、ファイルやマルウェアイベントに加えて、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 Cisco SecureX に送信できるようになりました。</p> <p>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。</p> <p>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)]</p> <p>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)</p>
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。	<p>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。</p> <p>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 e2transparent、ptp domain を追加できるようになりました。</p> <p>新規/変更されたコマンド：show ptp</p> <p>サポートされるプラットフォーム：FTD を使用した ISA 3000</p>

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）	<p>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。</p> <p>サポートされるプラットフォーム：FMC</p>
ISE 接続ステータスのモニターの機能拡張	<p>[ISE接続ステータスのモニター（ISE Connection Status Monitor）]ヘルスマジュールで、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。</p> <p>サポートされるプラットフォーム：FMC</p>
地域のクラウド	<p>アップグレードの影響。</p> <p>Cisco Threat Response の統合、Cisco Support Diagnostics、または Cisco SuccessNetwork 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。</p> <p>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。</p> <p>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）]</p> <p>サポートされるプラットフォーム：FMC、FTD</p>

機能	説明
Cisco Support Diagnostics	<p>アップグレードの影響。</p> <p>Cisco Support Diagnostics（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。</p> <p>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。</p> <p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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)] <p>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</p>
FMC モデル移行	<p>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。</p> <p>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。</p> <p>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 Model Migration Guide』を参照してください。</p> <p>サポート対象プラットフォーム：FMC</p>

機能	説明
デフォルトの HTTPS サーバー証明書。	<p>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 <code>lifespan-on-renew</code> は 3 年に戻りますが、バージョン 6.5.0.5 以降および 6.6 以降で再び 800 日に更新されます。</p> <p>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。</p> <ul style="list-style-type: none"> • 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
セキュリティと強化	
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	<p>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。</p> <p>新しい FXOS CLI コマンド : erase secure</p> <p>サポートされるプラットフォーム : Firepower 1000/2000 および Firepower 4100/9300</p>
初期設定時における FMC <code>admin</code> アカウントのパスワード要件の厳格化	<p>FMC の初期設定時に、<code>admin</code> 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 <code>admin</code> アカウントにこの強力なパスワードが適用されます。</p> <p>(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 <code>admin</code> 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。</p> <p>サポートされるプラットフォーム : FMC</p>

機能	説明
同時ユーザーセッション数の制限	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FMC</p>
認証済み NTP サーバー	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>
ユーザビリティとパフォーマンス	

機能	説明
初期設定の改善	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>(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。</p> <p>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、FMC コンフィギュレーションガイドを参照してください。</p> <p>サポートされるプラットフォーム : FMC</p>

機能	説明
ライトテーマ	<p>ベータ版。</p> <p>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。</p> <p>(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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>

機能	説明
<p>オブジェクトの表示に関するユーザビリティの拡張</p>	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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)] <p>サポートされるプラットフォーム：FMC</p>
<p>設定変更の展開に関するユーザビリティの拡張</p>	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FMC</p>

機能	説明
FTD NAT ポリシー管理に関するユーザビリティの拡張	<p>FTD NAT の設定時に、次のことが可能になりました。</p> <ul style="list-style-type: none"> • 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。 <p>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</p> <p>サポートされるプラットフォーム : FTD</p>
Firepower Management Center REST API	
新しい REST API 機能	<p>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。</p> <ul style="list-style-type: none"> • cloudregions : 地域クラウド <p>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。</p> <ul style="list-style-type: none"> • 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 <p>サポート対象プラットフォーム: FMC</p>

廃止された機能

表 27: FMC バージョン 6.5 パッチで廃止された機能

機能	説明
バージョン 6.5.0.2 廃止：出力最適化（一時的）。	<p>アップグレードの影響。</p> <p>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。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て、バージョン 6.5.0 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。ただし、CSCvq34340 を軽減するため、FTD にパッチを適用してバージョン 6.5.0.2 以降にすると、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。</p> <p>(注) この問題が修正されているバージョン 6.6+ 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 6.5.0 または 6.5.0.1 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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>

表 28: バージョン 6.5.0 で廃止された機能

機能	説明
サポート終了：FMC 750、1500、3500。	FMC モデルの FMC 1000、2500、および 4500 ではバージョン 6.5 以降を実行できません。これらの FMC を使用してバージョン 6.5+ のデバイスを管理することはできません。
サポート終了：ASA 5515-X および ASA 5585-X シリーズ	ASA 5515-X および ASA 5585-X シリーズ デバイス（SSP-10、-20、-40、および -60）では、バージョン 6.5 以降を実行できません。
サポート終了：Firepower 7000/8000 シリーズ。	AMP モデルを含む、Firepower 7000/8000 シリーズ デバイスでは、バージョン 6.5 以降を実行できません。

機能	説明
<p>廃止：FMC CLI を無効にする機能。</p>	<p>バージョン 6.3 では、明示的に有効にする必要がある FMC CLI が導入されました。バージョン 6.5 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。</p> <p>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。</p> <p>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</p>
<p>廃止：SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化。</p>	<p>バージョン 6.5 では、FTD 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。</p> <p>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。</p> <p>サポートはバージョン 7.0 で削除されます。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。</p> <p>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)]</p>
<p>廃止：TLS 1.0 および 1.1。</p>	<p>アップグレードの影響。</p> <p>セキュリティ強化対策：</p> <ul style="list-style-type: none"> • 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。 • ホスト入力での TLS 1.0 および TLS 1.1 のサポートが廃止されました。 <p>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。</p>

機能	説明
廃止：Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド。	<p>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。</p> <ul style="list-style-type: none"> • show hwCrypto • config hwCrypto <p>および、この FTD CLI コマンドを削除しました。</p> <ul style="list-style-type: none"> • show crypto accelerator status <p>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。</p>
廃止：Cisco Security Packet Analyzer の統合。	<p>バージョン 6.5 では、FMC と Cisco Security Packet Analyzer の統合のサポートを終了します。</p> <p>廃止された画面/オプション：</p> <ul style="list-style-type: none"> • [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)]

機能	説明
<p>廃止：地理位置情報の詳細。</p>	<p>2022年5月、GeoDBが2つのパッケージに分割されました。IPアドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能なIPアドレスに関連付けられた追加のコンテキストデータを含むIPパッケージです。IPパッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-date-build）です。これにより、バージョン7.1以前を実行している環境では、引き続きGeoDBの更新プログラムを取得できます。GeoDB更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IPパッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMCをバージョン7.2以降にアップグレードするか再イメージ化して、GeoDBを更新します。</p>

FMC バージョン 6.4 の新機能

新機能

表 29: FMC バージョン 6.4 パッチの新機能

新機能	説明
<p>バージョン 6.4.0.10</p> <p>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。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>(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。</p> <p>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 ~ 6.6.1 で一時的に廃止になりましたが、バージョン 6.6.3 で戻ります。</p>
<p>バージョン 6.4.0.9</p> <p>デフォルトの HTTPS サーバー証明書。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p>

新機能	説明
バージョン 6.4.0.4 新しい syslog フィールド。	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p>
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。	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>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。</p>
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)]ヘルスマジュール。	<p>新しいヘルスマジュール [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。</p>

表 30: FMC バージョン 6.4.0 の新機能

新機能	説明
プラットフォーム	
FMC 1600、2600、4600。	FMC モデル 1600、2600、および 4600 が導入されました。

新機能	説明
Azure 向け FMCv。	Microsoft Azure 向けの FMCv が導入されました。
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

VMware の FTDv は、デフォルトで vmxnet3 インターフェイスに設定されます。	<p>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。</p> <p>(注) バージョン 6.6 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 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 Secure Firewall Threat Defense Virtual スタートアップガイド』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。</p> <p>サポートされているプラットフォーム : VMware の FTDv</p>
---	--

Firepower Threat Defense : ルーティング

新機能	説明
<p>OSPFv2 ルーティングの循環（キーチェーン）認証。</p>	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム：FTD</p>
Firepower Threat Defense：暗号化と VPN	
<p>RA VPN：セカンダリ認証。</p>	<p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
<p>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。</p>	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>
<p>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。</p>	<p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
<p>TLS 暗号化アクセラレーション。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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 暗号化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。</p> <p>Firepower 4100/9300 シャーシ向けの新しい FXOS CLI コマンド：</p> <ul style="list-style-type: none"> • show hwCrypto • config hwCrypto <p>新しい FTD CLI コマンド：</p> <ul style="list-style-type: none"> • show crypto accelerator status (system support ssl-hw-status の代替) <p>削除された FTD CLI コマンド：</p> <ul style="list-style-type: none"> • system support ssl-hw-accel • system support ssl-hw-status <p>サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300</p>
イベントロギングおよび分析	
<p>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。</p>	<p>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。</p> <p>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</p> <p>サポートされているプラットフォーム：すべて</p>

新機能	説明
CVE ID による侵入イベントの検索。	<p>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。</p> <p>新規/変更されたページ : [分析 (Analysis)] > [検索 (Search)]</p> <p>サポートされるプラットフォーム : FMC</p>
[IntrusionPolicy] フィールドが syslog に含まれるようになりました。	<p>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。</p> <p>サポートされているプラットフォーム : すべて</p>
Cisco SecureX の統合。	<p>Cisco SecureX は、脅威の迅速な検出、調査、および対応に役立つクラウドサービスです。</p> <p>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。</p> <p>Cisco Secure Firewall Threat Defense および SecureX 統合ガイドを参照してください。</p> <p>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)]</p> <p>サポートされるプラットフォーム : FTD</p>
Splunk の統合。	<p>Splunk のユーザーは、新しい個別の Splunk アプリである Splunk 向け Cisco Secure Firewall (旧称Firepower) 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。</p> <p>Cisco Secure Firewall App for Splunk ユーザーガイドを参照してください。</p> <p>サポートされるプラットフォーム : FMC</p>

新機能	説明
Cisco Security Analytics and Logging (SaaS) の統合。	<p>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。</p> <p>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。</p> <p>Cisco Secure Firewall Management Center と Cisco Security Analytics and Logging (SaaS) 統合ガイドを参照してください。</p> <p>サポートされるプラットフォーム：FMC を搭載した FTD</p>
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。	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：ISA 3000</p>
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。	<p>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。</p> <p>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</p> <p>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</p> <p>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。</p>

新機能	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。	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム : FMC、Firepower 7000/8000 シリーズ</p>
管理インターフェイス上の ICMPv6 エコー応答および宛先到達不能メッセージを無効にする機能。	<p>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。</p> <p>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]</p> <p>新規/変更されたコマンド :</p> <ul style="list-style-type: none"> • configure network ipv6 destination-unreachable • configure network ipv6 echo-reply <p>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)</p>
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。	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム : FTD</p>

新機能	説明
オブジェクトの使用状況の表示。	<p>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。</p> <p>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、[使用状況の検索 (Find Usage)] (双眼鏡) アイコンの順に選択</p> <p>サポートされるプラットフォーム：FMC</p>
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。	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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)] <p>新しいコマンド：</p> <ul style="list-style-type: none"> • show rule hits • clear rule hits • cluster exec show rule hits • cluster exec clear rule hits • show cluster rule hits <p>変更されたコマンド：show failover</p> <p>サポートされるプラットフォーム：FTD</p>
URL フィルタリングヘルス モニターの改善。	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：すべて</p>

新機能	説明
<p>接続ベースのトラブルシューティング。</p>	<p>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。</p> <p>新規/変更されたコマンド：</p> <ul style="list-style-type: none"> • clear packet debugs • debug packet start • debug packet stop • show packet debugs <p>サポートされるプラットフォーム：FTD</p>
<p>Cisco Success Network の新しいモニタリング機能</p>	<p>Cisco Success Network の次のモニタリング機能を追加しました。</p> <ul style="list-style-type: none"> • 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 <p>サポート対象プラットフォーム：FMC</p>
<p>セキュリティと強化</p>	

新機能	説明
署名済みの SRU、VDB、および GeoDB の更新。	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <ul style="list-style-type: none"> • 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 <p>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。</p> <p>(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、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。</p> <p>サポートされているプラットフォーム : すべて</p>
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。	<p>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。</p> <p>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)]</p> <p>サポートされているプラットフォーム : Firepower Threat Defense</p>

新機能	説明
<p>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)。</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム : FMC</p>
ユーザビリティとパフォーマンス	
<p>Snort 再起動の改善。</p>	<p>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。</p> <p>サポートされているプラットフォーム : Firepower 4100/9300</p>

新機能	説明
<p>選択された IPS トラフィックのパフォーマンスの向上。</p>	<p>アップグレードの影響。</p> <p>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。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て、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。</p> <p>新規/変更されたコマンド：</p> <ul style="list-style-type: none"> • asp inspect-dp egress optimization • show asp inspect-dp egress optimization • clear asp inspect-dp egress optimization • show conn state egress_optimization <p>詳細については、『Cisco Secure Firewall 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。</p> <p>(注) CSCVq34340 を軽減するため、FTD デバイスにパッチを適用してバージョン 6.4.0.7 以降にすると、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。この問題が修正されているバージョン 6.6+ 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。</p> <p>詳細については、ソフトウェアアドバイザーリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。</p> <p>サポートされるプラットフォーム：FTD</p>
<p>SNMP イベントロギングの高速化。</p>	<p>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。</p> <p>サポートされているプラットフォーム：すべて</p>
<p>展開の高速化。</p>	<p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
<p>アップグレードの高速化。</p>	<p>イベント データベースが向上しました。</p> <p>サポートされているプラットフォーム：すべて</p>

新機能	説明
Firepower Management Center REST API	
新しい REST API 機能。	<p>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。</p> <ul style="list-style-type: none"> • <code>cloudeventsconfigs</code> : SecureX との連携を管理します。 • <code>ftddevicecluster</code> : シャーシのクラスタリングを管理します。 • <code>hitcounts</code> : 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。 • <code>keychain</code> : 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。 • <code>loggingsettings</code> : 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。 <p>サポートされるプラットフォーム : FMC</p>
OAS に基づく API エクスプローラ。	<p>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。</p> <p>サポート対象プラットフォーム: FMC</p>

廃止された機能

表 31: FMC バージョン 6.4.0 で廃止された機能

廃止された機能	説明
廃止 : SSL ハードウェアアクセラレーション FTD CLI コマンド。	<p>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。</p> <ul style="list-style-type: none"> • <code>system support ssl-hw-accel enable</code> • <code>system support ssl-hw-accel disable</code> • <code>system support ssl-hw-status</code>

廃止された機能	説明
廃止：地理位置情報の詳細。	<p>2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ (<code>Cisco_GEODB_Update-date-build</code>) です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IP パッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。</p>

FMC バージョン 6.3 の新機能

新機能

表 32: FMC バージョン 6.3 パッチの新機能

新機能	説明
<p>バージョン 6.3.0.4</p> <p>FTD NAT ポリシーでのルールの競合の検出</p>	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<p>バージョン 6.3.0.4</p> <p>[ISE接続ステータスのモニター (ISE Connection Status Monitor)]モジュール</p>	<p>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。</p> <p>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。</p> <p>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)]</p>
<p>バージョン 6.3.0.3</p> <p>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)</p>	<p>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。</p> <p>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。</p>

新機能	説明
バージョン 6.3.0.1 EMS 拡張機能のサポート	<p>アップグレードの影響。</p> <p>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。</p> <p>[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。</p> <p>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。</p>

表 33: FMC バージョン 6.3.0 の新機能

新機能	説明
プラットフォーム	
FMC 1600、2600、4600。	FMC モデル 1600、2600、および 4600 が導入されました。
ISA 3000 with FirePOWER Services。	<p>ISA 3000 with FirePOWER Services は、バージョン 6.3 でサポートされています (保護ライセンスのみ)。</p> <p>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、再イメージ化が必要なバージョン 6.3 にアップグレードすることはできません。</p>
Firepower 2100 のハードウェアバイパスサポート。	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム: Firepower 2100 シリーズ</p>

新機能	説明
Firepower 4100/9300 のオンモードでのデータ EtherChannel のサポート。	<p>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。</p> <p>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)]</p> <p>新規/変更された FXOS コマンド : set port-channel-mode</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
Firepower Threat Defense : HA およびクラスタリング	

新機能	説明
Firepower 4100/9300 のマルチインスタンス機能。	

新機能	説明
	<p>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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>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</p> <p>新規/変更された Firepower Chassis Manager ページ :</p> <ul style="list-style-type: none"> • [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)] <p>新規/変更された FXOS コマンド : connect ftdname、connect module telnet、create bootstrap-key PERMIT_EXPERT_MODE、create resource-profile、create 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</p>

新機能	説明
<p>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</p>	<p>サポートされるプラットフォーム : Firepower 4100/9300</p> <p>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。</p> <p>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)]</p> <p>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</p> <p>新規/変更された FXOS コマンド : set cluster-control-link network</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>FMC への FTD クラスタ追加の改善</p>	<p>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ります。ことに注意してください。</p> <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [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 <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
<p>Firepower Threat Defense : 暗号化と VPN</p>	

新機能	説明
SSLハードウェアアクセラレーション	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300</p>
RA VPN：RADIUS ダイナミック認証または認可変更（CoA）	<p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
RA VPN：二要素認証	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>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『Cisco Firepower Threat Defense (FTD) VPN with AnyConnect』のドキュメントを参照してください。</p> <p>サポートされるプラットフォーム：FTD</p>
セキュリティ ポリシー	

新機能	説明
Firepower Threat Defense サービスポリシー	<p>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。</p> <p>サポートされる機能は次のとおりです。</p> <ul style="list-style-type: none"> • 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 <p>(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。</p> <p>FMC コンフィギュレーション ガイドの「<i>Threat Defense</i> サービスポリシー」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。</p> <p>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)]</p> <p>サポートされるプラットフォーム : FTD</p>

新機能	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	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FMC</p>
イベントロギングおよび分析	
Cisco Security Packet Analyzer 統合	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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)] <p>サポートされるプラットフォーム：FMC</p>
コンテキストクロス起動	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>

新機能	説明
ユニファイド syslog の設定	<p>アップグレードの影響。</p> <p>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。</p> <p>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イベントと侵入イベントのロギングに影響を与えます。</p> <p>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）。</p> <p>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、FMC コンフィギュレーション ガイドで「<i>Firepower Threat Defense</i> のプラットフォーム設定」の章を参照してください。</p> <p>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。</p> <p>サポートされるプラットフォーム：すべて</p>
接続イベントと侵入イベントの完全な syslog メッセージ	<p>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。</p> <ul style="list-style-type: none"> • 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）。 <p>サポートされるプラットフォーム：すべて</p>

新機能	説明
FTDデバイスのその他の syslog の改善	<p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
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キスポート管理機能	<p>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せん。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC、FTD</p>
承認された顧客向けの特定のライセンス予約	<p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC、FTD (ISA 3000 を除く)</p>
SNMP ホストの IPv4 範囲、サブネット、および IPv6 のサポート	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
完全修飾ドメイン名 (FQDN) を使用したアクセス制御	<p>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。</p> <p>新規/変更されたページ：</p> <ul style="list-style-type: none"> • [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] <p>サポートされるプラットフォーム：FTD</p>
FMC の CLI	<p>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。</p> <p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FMC (FMCv を含む)</p>
デバイス設定のコピー	<p>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。</p> <p>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</p> <p>サポートされるプラットフォーム：FMC</p>

新機能	説明
FTD デバイス設定のバックアップ/復元	<p>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。</p> <p>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)]</p> <p>新規/変更された CLI コマンド : restore</p> <p>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</p>
展開タスクをスケジュールするとき最新のデバイスへの展開をスキップ	<p>アップグレードの影響。</p> <p>設定変更を展開するタスクをスケジュールするとき、最新のデバイスへの展開をスキップ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。</p> <p>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。</p> <p>新規/変更されたページ : [システム (System)]>[ツール (Tools)]>[スケジュールリング (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</p> <p>サポートされるプラットフォーム : FMC</p>
新しいヘルスマジュール	<p>新しいヘルスマジュールは、次の場合にアラートを表示します。</p> <ul style="list-style-type: none"> • 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。 <p>新規/変更されたページ :</p> <ul style="list-style-type: none"> • [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)] <p>サポートされるプラットフォーム : FMC</p>
設定可能なパケットキャプチャサイズ	<p>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。</p> <p>新規/変更された CLI コマンド : file-size、show capture</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

新機能	説明
Web インターフェイスの変更。	

新機能	説明
	<p>バージョン 6.3 では、次のメニューオプションが変更されています。</p> <p>[分析 (Analysis)] > [詳細 (Advanced)] > [Whois] は次に変更されました。</p> <p>[分析 (Analysis)] > [検索 (Lookup)] > [Whois]</p> <p>[分析 (Analysis)] > [詳細 (Advanced)] > [位置情報 (Geolocation)] は次に変更されました。</p> <p>[分析 (Analysis)] > [検索 (Lookup)] > [位置情報 (Geolocation)]</p> <p>[分析 (Analysis)] > [詳細 (Advanced)] > [URL] は次に変更されました。</p> <p>[分析 (Analysis)] > [検索 (Lookup)] > [URL]</p> <p>[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。</p> <p>[分析 (Analysis)] > [検索 (Lookup)] > [カスタム ワークフロー (Custom Workflows)]</p> <p>[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。</p> <p>[分析 (Analysis)] > [検索 (Lookup)] > [カスタム テーブル (Custom Tables)]</p> <p>[分析 (Analysis)] > [ホスト (Hosts)] > [脆弱性 (Vulnerabilities)] は次に変更されました。</p> <p>[分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [脆弱性 (Vulnerabilities)]</p> <p>[分析 (Analysis)] > [ホスト (Hosts)] > [サードパーティ] は次に変更されました。</p> <p>[分析 (Analysis)] > [脆弱性 (Vulnerabilities)] > [サード]</p>

新機能	説明
	<p>の脆弱性 (Third-Party Vulnerabilities)] 更されまし た。パーティの脆弱性 (Third Party Vulnerabilities)]</p>
セキュリティと強化	
HTTPS 証明書	<p>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。</p> <p>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証明書をアプライアンスが使用している場合、サーバ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 サーバ証明書を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。</p> <p>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</p> <p>新規/変更されたクラシック CLI コマンド : <code>show http-cert-expire-date、system renew-http-cert new_key</code></p> <p>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</p>

新機能	説明
向上したログインセキュリティ	<p>アップグレードの影響。</p> <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FMC</p>
デバイスでの SSH ログイン失敗の制限	<p>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。</p> <p>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</p>
ユーザビリティとパフォーマンス	

新機能	説明
How-To ウォークスルー	<p>デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMCに関するウォークスルー（How-Toとも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。</p> <p>(注) FMC ウォークスルーは Firefox および Chrome ブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。</p> <p>次に、一般的な問題点と解決策をいくつか示します。</p> <ul style="list-style-type: none"> <p>問題： ウォークスルーを開始するためのリンクが見つからない。</p> <p>解決策： ウォークスルーが有効になっていることを確認します。ユーザー名の下にあるドロップダウンリストから、[ユーザー設定 (User Preferences)] を選択し、[設定方法 (How-To Settings)] をクリックします。</p> <p>問題： ウォークスルーが予期しないタイミングで表示される。</p> <p>解決策： ウォークスルーを終了します。</p> <p>問題： ウォークスルーが突然消えたり終了したりする。</p> <p>解決策： ポインタを移動するか、別のページに移動してからやり直してください。</p> <p>問題： ウォークスルーがFMCと同期していない（間違ったステップで開始する、時期尚早に進む、進まない）。</p> <p>解決策： 続行を試みます。たとえば、フィールドに無効な値を入力してエラーが表示された場合は、ウォークスルーが先に進行することがあります。戻ってエラーを解決してタスクを完了することが必要になる場合があります。ただし、続行できない場合もあります。たとえば、手順の完了後に [Next] をクリックしないと、ウォークスルーを終了し、別のページに移動して、再試行する必要が生じる場合があります。</p>

Firepower Management Center REST API

新機能	説明
新しい REST API サービス	<p>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。</p> <ul style="list-style-type: none"> • サイト間 VPN トポロジ : ftds2svpns、endpoints、ipseccsettings、advancedsettings、ikesettings、ikev1ipsecproposals、ikev1policies、ikev2ipsecproposals、ikev2policies • HA デバイスフェールオーバー : failoverinterfacemacaddressconfigs、monitoredinterfaces <p>サポートされるプラットフォーム : FMC</p>
バルク オーバーライド	<p>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。</p>

廃止された機能

表 34: バージョン 6.3.0 で廃止された機能

廃止された機能	説明
サポートの終了 : VMware vSphere/VMware ESXi 5.5。	バージョン 6.3 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。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サポートされているバージョンにアップグレードします。
サポート終了 : ASA 5512-X および 5506-X シリーズ。	ASA 5506-X、5506H-X、5506W-X、および 5512-X では、バージョン 6.3 以降を実行できません。

廃止された機能	説明
<p>廃止：復号化のためのEMS拡張機能のサポート（一時的）。</p>	<p>アップグレードの影響。</p> <p>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一時的に中止されます。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。</p> <p>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。</p> <p>サポートはバージョン 6.3.0.1 で再導入されています。</p>
<p>廃止：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。</p>	<p>アップグレードの影響。</p> <p>バージョン 6.3 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。</p>

廃止された機能	説明
<p>廃止：FlexConfig を使用したデフォルトの DNS グループ。</p>	<p>バージョン 6.3 では、FMC を使用する FTD の場合、次の FlexConfig オブジェクトが廃止されます。</p> <ul style="list-style-type: none"> • Default_DNS_Configure <p>関連するテキストオブジェクト：</p> <ul style="list-style-type: none"> • defaultDNSNameServerList • defaultDNSParameters <p>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。</p> <p>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]）。</p>

廃止された機能	説明
<p>廃止：FlexConfig を使用した初期接続制限およびタイムアウト。</p>	<p>アップグレード後の展開の問題が発生する可能性があります。</p> <p>バージョン 6.3 では、FMC を使用する FTD の場合、次の FlexConfig オブジェクトが廃止されます。</p> <ul style="list-style-type: none"> • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout <p>関連するテキストオブジェクト：</p> <ul style="list-style-type: none"> • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout <p>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。</p> <p>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）]）。</p> <p>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。</p>

廃止された機能	説明
<p>廃止：地理位置情報の詳細。</p>	<p>2022年5月、GeoDBが2つのパッケージに分割されました。IPアドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能なIPアドレスに関連付けられた追加のコンテキストデータを含むIPパッケージです。IPパッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-date-build）です。これにより、バージョン7.1以前を実行している環境では、引き続きGeoDBの更新プログラムを取得できます。GeoDB更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IPパッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみ依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMCをバージョン7.2以降にアップグレードするか再イメージ化して、GeoDBを更新します。</p>

FMC バージョン 6.2.3 の新機能

表 35: FMC バージョン 6.2.3 パッチの新機能

新機能	説明
<p>バージョン 6.2.3.13</p> <p>FTD NAT ポリシーでの ルールの競合の検出</p>	<p>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。</p> <p>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。</p> <p>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。</p> <p>(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。</p> <p>サポートされるプラットフォーム：FTD</p>
<p>バージョン 6.2.3.8</p> <p>EMS 拡張機能のサポ ート</p>	<p>[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。</p> <p>(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。</p> <p>サポートされるプラットフォーム：すべて</p>

新機能	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	<p>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。</p> <p>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。</p> <p>詳細については、Cisco Secure Firewall 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 に問い合わせしてから使用することをお勧めします。</p> <p>サポートされるプラットフォーム：FTD</p>
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	<p>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。</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>

表 36: FMC バージョン 6.2.3 の新機能

新機能	説明
プラットフォーム	
ISA 3000 の FTD。	<p>ISA 3000 シリーズで FTD を実行できるようになりました。</p> <p>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 FTD ではサポートしていません。</p>
VMware ESXi 6.5 のサポート。	VMware vSphere/VMware ESXi 6.5 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。
Firepower Threat Defense : 暗号化と VPN	

新機能	説明
Firepower 4100/9300 の SSL ハードウェア アクセラレーション	<p>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。</p> <p>(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。</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>
証明書の登録の改善	<p>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 FTD デバイスで証明書の登録を並行して実行できます。</p> <ul style="list-style-type: none"> • 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。 <p>サポートされるプラットフォーム : FTD</p>
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 FTD クラスタに再参加します。	<p>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。</p> <p>新しい/変更されたコマンド : show cluster info auto-join</p> <p>サポートされるプラットフォーム : Firepower 4100/9300</p>

新機能	説明
FTDのハイアベイラビリティのハードニング	<p>バージョン 6.2.3 では、ハイアベイラビリティの FTD デバイスに関する次の機能が導入されています。</p> <ul style="list-style-type: none"> • 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 FTD デバイスが再起動されると、FMC 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、デバイスと FMC の間の通信がまだ確立されていないため、ステータスが FMC で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。 • FMC UI の [デバイス (Devices)]>[デバイス管理 (Device Management)] ページには、新しい [アクティブペアの切り替え (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。 <ul style="list-style-type: none"> • DELETE ftddevicepairs • PUT ftddevicepairs • POST ftddevicepairs • GET ftddevicepairs
管理とトラブルシューティング	
FMC ハイアベイラビリティメッセージング	<p>FMC 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、FMC 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。</p> <p>サポート対象プラットフォーム：FMC</p>
FTD SSH アクセス用に追加された外部認証	<p>LDAP または RADIUS を使用して、FTD デバイスへの 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。</p> <p>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)]</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
脆弱性データベース (VDB) の強化されたインストール	<p>FMC 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。</p> <p>次のようなときに警告が表示される可能性があります。</p> <ul style="list-style-type: none"> • 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。 <p>サポートされるプラットフォーム：FMC</p>
アップグレードパッケージのプッシュ	<p>実際のアップグレードを実行する前に、FMC 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。</p> <p>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。</p> <p>新規/変更された画面：[システム (System)] > [更新 (Updates)]</p> <p>サポートされるプラットフォーム：FMC</p>
FTD サービスアビリティ	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>(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。</p> <p>サポートされるプラットフォーム：FTD</p>

新機能	説明
デバイス一覧のソート	<p>[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。</p> <p>サポートされるプラットフォーム：FMC</p>
監査ログの改善	<p>監査ログは、FTD プラットフォーム設定の [デバイス (Devices)] > [プラットフォーム設定 (Platform Settings)] ページでポリシーが変更されたかどうかを示すようになりました。</p> <p>サポートされるプラットフォーム：FTD を搭載した FMC</p>
FTD CLI コマンドの更新	<p>FTD デバイスの CLI コマンドの <code>asa_mgmt_plane</code> オプションと <code>asa_dataplane</code> オプションは、<code>management-plane</code> と <code>data-plane</code> にそれぞれ名前が変更されています。</p> <p>サポートされるプラットフォーム：FTD</p>
Cisco Success Network	<p>アップグレードの影響。</p> <p>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。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
Web 分析トラッキング	<p>アップグレードの影響。</p> <p>Web 分析は、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、Management Center 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提供します。</p> <p>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。</p> <p>サポート対象プラットフォーム：FMC</p>
パフォーマンス	

新機能	説明
FTD デバイスの Snort の再起動が減少	<p>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。</p> <p>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。</p> <p>サポートされるプラットフォーム：FTD</p>
ポリシー適用時のトラフィック ドロップ	<p>バージョン 6.2.3 では、configure snort preserve-connection {enable disable} コマンドが FTD 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。</p> <p>FDM で管理されている FTD 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。</p>
ローエンドアプライアンスのメモリ容量の増加	<p>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。</p>
ISE pxGrid ディスカバリの高速化	<p>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、FMC 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。</p>

新機能	説明
<p>レポートの結果の新しい制限。</p>	<p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>PDF レポートセクションの新しい制限は次のとおりです。</p> <ul style="list-style-type: none"> • 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 <p>FMC 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 よりも大きい結果の数を指定する場合、アップグレードプロセスにより設定が新しい最大値に下がります。</p> <p>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。</p>
Firepower Management Center REST API	

新機能	説明
FMC REST API の改善	<p>新しいFMC REST API は、ASA FirePOWER から FTD 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。</p> <p>NAT 用に新しく導入された API</p> <ul style="list-style-type: none">• NAT ルール• FTD NAT ポリシー• 自動 NAT ルール• 手動 NAT ルール <p>Cisco ACI に FTD 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、FTD 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。</p> <p>スタティック ルート用に新しく導入された API</p> <ul style="list-style-type: none">• 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

廃止された機能

表 37: FMC バージョン 6.2.3 で廃止された機能

廃止された機能	説明
AMP for Networks による動的分析用の期限切れ CA 証明書。	<p>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な 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 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。</p> <p>バージョン 6.3 以降にアップグレードしない場合、次のようにパッチを適用すると、新しい証明書を取得して動的分析を再度有効にできます。</p> <ul style="list-style-type: none"> • バージョン 6.2.3 → バージョン 6.2.3.4 へのパッチ • バージョン 6.2.2 → バージョン 6.2.2.4 へのパッチ • バージョン 6.2.1 → 利用可能なパッチはありません • バージョン 6.2 → バージョン 6.2.0.6 へのパッチ • バージョン 6.1 → バージョン 6.1.0.7 へのパッチ • バージョン 6.0 → 利用可能なパッチはありません <p>ホットフィックスを適用することもできます。利用可能なホットフィックスについては、Cisco Secure Firewall Threat Defense/Firepower ホットフィックス リリース ノート を参照してください。CSCvj07038 : 「Firepower デバイスは Threat Grid 証明書を信頼する必要がある」に該当するバージョンとプラットフォームのホットフィックスを見つけます。</p> <p>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 <code>fmc.api.threatgrid.com</code> (<code>panacea.threatgrid.com</code> 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。</p> <p>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ることに注意してください。</p>

廃止された機能	説明
廃止：地理位置情報の詳細。	<p>2022年5月、GeoDBが2つのパッケージに分割されました。IPアドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能なIPアドレスに関連付けられた追加のコンテキストデータを含むIPパッケージです。IPパッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。</p> <p>新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-date-build）です。これにより、バージョン7.1以前を実行している環境では、引き続きGeoDBの更新プログラムを取得できます。GeoDB更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IPパッケージではなく、必ず国コードパッケージを取得してください。</p> <p>重要 この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータだけに依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMCをバージョン7.2以降にアップグレードするか再イメージ化して、GeoDBを更新します。</p>

リリース日

表 38:バージョン 7.3 日付

バージョン	ビルド	日付	プラットフォーム
7.3.1	19	2023年3月14日	すべて (All)
7.3.0	69	2022年11月29日	すべて (All)

表 39:バージョン 7.2 のリリース日

バージョン	ビルド	日付	プラットフォーム
7.2.5	208	2023-07-27	すべて
7.2.4.1	43	2023-07-27	すべて (All)

バージョン	ビルド	日付	プラットフォーム
7.2.4	169	2023-05-10	Management center
	165	2023-05-03	デバイス
7.2.3.1	13	2023-04-18	Management center
7.2.3	77	2023年2月 27日	すべて (All)
7.2.2	54	2022年11 月29日	すべて (All)
7.2.1	40	2022年10 月03日	すべて (All)
7.2.0.1	12	2022年8月 10日	すべて
7.2.0	82	2022-06-06	すべて

表 40:バージョン 7.1 のリリース日

バージョン	ビルド	日付	プラットフォーム
7.1.0.3	108	2022年3月 15日	すべて (All)
7.1.0.2	36	2022年8月 3日	FMC/FMCv Secure Firewall 3100 シリーズ
7.1.0.1	28	2022年02 月24日	FMC/FMCv Secure Firewall 3100 シリーズを除くすべてのデバイス
7.1.0	90	2021年12 月1日	すべて (All)

表 41:バージョン 7.0 のリリース日

バージョン	ビルド	日付	プラットフォーム
7.0.6	236	2023-07-18	すべて (All)

バージョン	ビルド	日付	プラットフォーム
7.0.5.1	5	2023-04-26	NGIPsv セキュリティ認定コンプライアンスが有効になっているデバイスの場合 (CC/UCAPL モード)。バージョン 7.0.5 FMC で使用します。
7.0.5	72	2022 年 11 月 17 日	すべて (All)
7.0.4	55	2022 年 8 月 10 日	すべて
7.0.3	37	2022-06-30	すべて
7.0.2.1	10	2022-06-27	すべて
7.0.2	88	2022 年 5 月 5 日	すべて (All)
7.0.1.1	11	2022 年 02 月 17 日	すべて (All)
7.0.1	84	2021-10-07	すべて (All)
7.0.0.1	15	2021 年 7 月 15 日	すべて
7.0.0	94	2021 年 5 月 26 日	すべて

表 42:バージョン 6.7のリリース日

バージョン	ビルド	日付	プラットフォーム
6.7.0.3	105	2022 年 02 月 17 日	すべて (All)
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
6.7.0	65	2020 年 11 月 2 日	すべて

表 43:バージョン 6.6 のリリース日

バージョン	ビルド	日付	プラットフォーム
6.6.7.1	54	2023 年 1 月 26 日	すべて (All)
6.6.7	223	2022 年 7 月 14 日	すべて (All)
6.6.5.2	14	2022 年 03 月 24 日	すべて
6.6.5.1	15	2021 年 12 月 6 日	すべて (All)
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	—
6.6.0.1	7	2020 年 7 月 22 日	すべて
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 44:バージョン 6.5のリリース日

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
6.5.0.5	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	—
6.5.0.1	35	2019年11月20日	利用できなくなりました。	—
6.5.0	123	2020年2月3日	FMC/FMCv	FMC/FMCv
	120	2019年10月8日	—	—
	115	2019年9月26日	すべてのデバイス	すべてのデバイス

表 45:バージョン 6.4のリリース日

バージョン	ビルド	日付	プラットフォーム
6.4.0.16	50	2022年11月21日	すべて
6.4.0.15	26	2022-05-31	すべて (All)
6.4.0.14	67	2022年02月18日	すべて
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

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
	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 46: バージョン 6.3 のリリース日

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
6.3.0.5	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	—

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
6.3.0.3	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	—
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	—
6.3.0	85	2019年1月22日	Firepower 4100/9300	Firepower 4100/9300
	84	2018年12月18日	FMC/FMCv ASA FirePOWER	—
	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 47: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
6.2.3.18	50	2022年02月16日	すべて	—
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	—
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。	—

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
6.2.3.7	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9月12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	—	—
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	—	—

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
	111	2019年11月25日	—	FTDv: AWS, Azure
	110	2019年6月14日	—	—
	99	2018年9月7日	—	—
	96	2018年7月26日	—	—
	92	2018年7月5日	—	—
	88	2018年6月11日	—	—
	85	2018年4月9日	—	—
	84	2018年4月9日	Firepower 7000/8000 シリーズ NGIPSv	—
	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
79	2018年3月29日	—	—	

表 48: 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
6.2.2.5	57	2018年11月27日	すべて

バージョン	ビルド	日付	プラットフォーム
6.2.2.4	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
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
6.2.2	81	2017年9月5日	すべて

翻訳について

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。