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：2024 年 3 月 19 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について説明します。また、アップグレードによる影響についても説明します。

アップグレードと展開により、システムでトラフィックが処理されるか、他の操作をしなくても異なる動作が発生する場合、機能がアップグレードに影響を与えます。これは特に、新しい脅威検出およびアプリケーション識別機能で一般的です。または、アップグレードプロセスに特別な要件がある場合もあります。たとえば、アップグレードの前後に非標準のタスクを実行する必要がある場合があります（特定のコンフィギュレーションの編集または削除、ヘルスポリシーの適用、Web インターフェイスでの FlexConfig コマンドのやり直しなど）。

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 および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。

英語以外の言語でWebインターフェイスを使用している場合は、メンテナンスリリースやパッチで導入される機能が、次のメジャーリリースまで翻訳されない可能性があることに注意してください。

推奨リリース：バージョン 7.2.5.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最新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。バージョン 7.2.6 以降または 7.4.1 以降では、新しい推奨リリースが使用可能になると Management Center から通知され、製品のアップグレードページに推奨リリースが表示されます。

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用

語の説明については、「Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報」を参照してください。

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

バージョン 7.4.1 の Management Center 機能

表 *1* : バージョン *7.4.1* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
再導入された機能			

機能	最小の Management Center	最小の Threat Defense	詳細
再導入された機能。	機能に依存	機能に依存	

機能	最小の Management Center	最小の Threat Defense	詳細
			バージョン 7.4.1 では、奇数番号のバージョン（7.1.x、7.3.x）またはバージョン 7.4.0 のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0.x、7.2.x）のメンテナンスリリースには含まれていた機能、機能拡張および重要な修正が再度サポートされます。 再導入された機能は次のとおりです。 • バージョン 7.3 でサポートされているすべてのデバイスプラットフォーム、および Firepower 1010E（7.2 で最後にサポート）での Threat Defense のサポート。 • Management Center によるインターフェイス同期エラーの検出。アップグレードの影響。 • Web 分析プロバイダーを更新しました。アップグレードの影響。 • Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。アップグレードの影響。 • NAT ルールの編集時にネットワークグループを作成します。 • 高可用性 Management Center 用の単一のバックアップファイル。 • 統合イベントビューアからパケットトレーサを開きます。 • 展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。アップグレードの影響。 • NTP 同期の問題に関する正常性アラート。アップグレードの影響。 • 前回の展開以降の設定変更に関するレポートを表示および生成します。 • デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。

機能	最小の Management Center	最小の Threat Defense	詳細
			• 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。アップグレードの影響。 • スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。アップグレードの影響。 • アクセス制御オブジェクトの最適化を有効または無効にします。 • クラスタ制御リンク ping ツール。 • Snort 3 コアダンプの頻度を設定します。 • Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。
プラットフォーム（Platform）			
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	7.4.1	7.4.1	Cisco Secure Firewall 3130 および 3140 は次のネットワークモジュールをサポートするようになりました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド
Firepower 9300 ネットワークモジュール用の光トランシーバ。	7.4.1	7.4.1	Firepower 9300 は、次の光トランシーバをサポートするようになりました。 • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR 以下のネットワークモジュールでサポート： • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G 参照： Cisco Firepower 9300 ハードウェア設置ガイド

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100 のパフォーマンスプロファイルのサポート。	7.4.1	7.4.1	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 3100 に適用されるようになりました。以前は、この機能は Firepower 4100/9300、Cisco Secure Firewall 4200、および Threat Defense Virtual でサポートされていました。 参照：「Configure the Performance Profile」
[インターフェイス（Interfaces）]			
Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開します。	7.4.1	7.4.1	Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開できるようになりました。以前は、1 つの管理インターフェイス、1 つの診断インターフェイス、および少なくとも 2 つのデータインターフェイスが必要でした。新しいインターフェイスの要件： • Azure：管理 1、データ 2（最大 8） • GCP：管理 1、データ 3（最大 8） 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド
デバイス管理			
ユーザー定義の VRF インターフェイスでサポートされるデバイス管理サービス。	7.4.1	いずれか	Threat Defense プラットフォーム設定（NetFlow、SSH アクセス、SNMP ホスト、syslog サーバー）で設定されたデバイス管理サービスが、ユーザー定義の Virtual Routing and Forwarding（VRF）インターフェイスでサポートされるようになりました。 プラットフォームの制限：コンテナインスタンスまたはクラスタ化されたデバイスではサポートされていません。 参照：「Platform Settings」
高可用性/拡張性：Threat Defense			

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100 のマルチインスタンスモード。	7.4.1	7.4.1	Secure Firewall 3100 は、単一のデバイス（アプライアンスモード）または複数のコンテナインスタンス（マルチインスタンスモード）として展開できます。マルチインスタンスモードでは、完全に独立したデバイスとして機能する複数のコンテナインスタンスを 1 つのシャーシに展開できます。マルチインスタンスモードでは、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレード対象（シャーシのアップグレード）になることに注意してください。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [Chassis Manager]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [新しいポリシー（New Policy）] > [シャーシプラットフォーム設定（Chassis Platform Settings）]** • **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]** 新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode** プラットフォームの制限：Cisco Secure Firewall 3105 ではサポートされていません。 参照：「Multi-Instance Mode for the Secure Firewall 3100」 および Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
VMware および KVM 向け Threat Defense Virtual の 16 ノードクラスタ	7.4.1	7.4.1	VMware の仮想 Threat Defense と KVM の仮想 Threat Defense に 16 ノードクラスタを構成できるようになりました。 参照：「Clustering for Threat Defense Virtual in a Private Cloud」

機能	最小の Management Center	最小の Threat Defense	詳細
AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバー。	7.4.1	7.4.1	AWS Gateway Load Balancer（GWLB）を使用して AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバーを設定できるようになりました。 プラットフォームの制限：5 台および 10 台のデバイスライセンスでは使用できません。 参照：「Configure Target Failover for Threat Defense Clustering with GWLB in AWS」
Threat Defense 高可用性ペアの設定の不一致を検出します。	7.4.1	7.4.1	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照：「Troubleshoot Configuration Sync Failure」および Cisco Secure Firewall Threat Defense コマンドリファレンス
高可用性：Management Center			
Management Center の高可用性同期の機能拡張。	7.4.1	いずれか	Management Center の高可用性（HA）には、次の同期機能拡張が含まれています。 • 設定履歴ファイルが大きいと、遅延の大きいネットワークで同期が失敗する可能性があります。これを防ぐために、デバイス設定履歴ファイルは他の設定データと並行して同期されるようになりました。この機能拡張により、同期時間も短縮されます。 • Management Center は、設定履歴ファイルの同期プロセスをモニターし、同期がタイムアウトした場合に正常性アラートを表示するようになりました。 新規/変更された画面：次の画面でこれらのアラートを確認できます。 • [通知（Notifications）] > [メッセージセンター（Message Center）] > [正常性（Health）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ステータス （Status）]（[概要（Summary）] の下） 参照：「Viewing Management Center High Availability Status」
SD-WAN			

機能	最小の Management Center	最小の Threat Defense	詳細
[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードのアプリケーションモニタリング。	7.4.1	7.4.1	[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードでWANインターフェイスアプリケーションのパフォーマンスをモニターできるようになりました。 新規/変更された画面：**[概要（Overview）]** > **[Cisco SD-WANサマリー（SD-WAN Summary）]** > **[アプリケーション モニタリング（Application Monitoring）]** 参照：「WAN Summary Dashboard」
VPN			
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPSec フローのオフロード。	7.4.1	7.4.1	**アップグレードの影響。条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。 この機能はアップグレードにより自動的に有効になります。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4100/9300 の暗号デバッグの機能拡張。	7.4.1	7.4.1	バージョン 7.4.0 で導入された暗号デバッグの機能拡張は、Cisco Secure Firewall 3100 および Firepower 4100/9300 に適用されるようになりました。以前は、Cisco Secure Firewall 4200 でのみサポートされていました。 参照：「Troubleshooting Using Crypto Archives」
ルートベース VPN の VTI の詳細を表示します。	7.4.1	いずれか	管理対象デバイスのルートベース VPN の仮想トンネルインターフェイス（VTI）の詳細を表示できるようになりました。ダイナミック VTI の動的に作成されたすべての仮想アクセスインターフェイスの詳細も表示できます。 新規/変更された画面：[デバイス（Device）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit a device）] > [インターフェイス（Interfaces）] > [仮想トンネル（Virtual Tunnels）] タブ。 参照：「About Virtual Tunnel Interfaces」
ルーティング			

機能	最小の Management Center	最小の Threat Defense	詳細
FlexConfig を使用して、IS-ISインターフェイスで BFD ルーティングを設定します。	7.4.1	7.4.1	FlexConfig を使用して、物理、サブインターフェイス、および EtherChannel IS-IS インターフェイスで Bidirectional Forwarding Detection（BFD）ルーティングを設定できるようになりました。 参照：「Guidelines for BFD Routing」
アクセス制御：脅威の検出とアプリケーションの識別			
Zero Trust アクセスの機能拡張。	7.4.1	7.4.1（Snort 3）	Management Center には、次の Zero Trust アクセスの機能拡張が含まれています。 • アプリケーションの送信元NATを設定できます。設定されたネットワークオブジェクトまたはオブジェクトグループは、着信要求のパブリックネットワークの送信元 IP アドレスを、アプリケーション ネットワーク内のルーティング可能な IP アドレスに変換します。 • 診断ツールを使用して、Zero Trust 設定の問題をトラブルシューティングできます。 • エクスペリエンスを向上させるために、Zero Trustアプリケーションポリシーのテレメトリデータを収集するようになりました。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[Zero Trustアプリケーション（Zero Trust Application）]** 新規/変更された CLI コマンド：**show running-config zero-trust**、**show zero-trust statistics** 参照： • アプリケーションの作成 • Zero Trust セッションのモニタリング • Cisco Secure Firewall Threat Defense コマンドリファレンス • Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ
CIP 検出。	7.4.1	7.4.1（Snort 3）	セキュリティポリシーで CIP およびイーサネット/IP（ENIP）アプリケーション条件を使用することで、Common Industrial Protocol（CIP）を検出して処理できるようになりました。 参照：「Application Rule Conditions」

機能	最小の Management Center	最小の Threat Defense	詳細
CIP 安全検出。	7.4.1	7.4.1（Snort 3）	CIP Safety は、産業自動化アプリケーションの安全な動作を可能にする CIP 拡張機能です。CIP インスペクタは、CIP トラフィック内の CIP Safety セグメントを検出できるようになりました。CIP Safety セグメントを検出してアクションを実行するには、Management Center のネットワーク分析ポリシーで CIP インスペクタを有効にし、アクセス コントロール ポリシーに割り当てます。 新規/変更された画面：[ポリシー（Policies）]>[アクセス制御（Access Control）] > [ポリシーの編集（Edit a policy）] > [ルールの追加（Add Rule）]>[アプリケーション（Applications）] タブの順に選択し、検索ボックスで CIP Safety を検索します。 参照：Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
アクセス制御：アイデンティティ			

機能	最小の Management Center	最小の Threat Defense	詳細
複数の Active Directory レルム（レルムシーケンス）のキャプティブポータル サポート。	7.4.1	7.4.1	**アップグレードの影響。カスタム認証フォームの更新。** LDAP レルム、Microsoft Active Directory レルム、またはレルムシーケンスに対してアクティブ認証を設定できます。さらに、レルムまたはレルムシーケンスを使用してアクティブ認証にフォールバックするパッシブ認証ルールを設定できます。必要に応じて、アクセス制御ルールで同じ ID ポリシーを共有する管理対象デバイス間でセッションを共有できます。 さらに、以前にアクセスしたデバイスとは別の管理対象デバイスを使用してシステムにアクセスするときに、ユーザーに再認証を要求するオプションがあります。 HTTP 応答ページ認証タイプを使用する場合は、Threat Defense をアップグレードした後、カスタム認証フォームに**<select name="realm" id="realm"></select>**を追加する必要があります。これにより、ユーザーはレルムを選択できます。 制限事項：Microsoft Azure Active Directory ではサポートされていません。 新規/変更された画面： • **[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集）> [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** • **[IDポリシー（Identity policy）] >（編集）> [ルールの追加（Add Rule）] > [パッシブ認証（Passive Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** • **[IDポリシー（Identity policy）] >（編集）> [ルールの追加（Add Rule）] > [アクティブ認証（Active Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** 参照：「How to Configure the Captive Portal for User Control」

機能	最小の Management Center	最小の Threat Defense	詳細
ファイアウォール全体でキャプティブポータルアクティブ認証セッションを共有します。	7.4.1	7.4.1	以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサイトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。 • (デフォルト) 有効にすると、ユーザーはアクティブな認証アイデンティティルールに関連付けられた管理対象デバイスで認証できます。 • アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は無効にします。 新規/変更された画面：**[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集） > [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** 参照：「How to Configure the Captive Portal for User Control」
Management Center の Web インターフェイスを使用して、ダウンロード可能なアクセス制御リストを RADIUS アイデンティティソースのシスコ属性値ペア ACL とマージします。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）] > [RADIUSサーバーグループの追加（Add RADIUS Server Group）] > [ダウンロード可能ACL とシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）]** 新しい CLI コマンド： • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** 参照：「RADIUS Server Group Options」
ヘルス モニタリング			

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower 4100/9300 のシャーシレベルのヘルスアラート。	7.4.1	FXOS 2.14.1 を搭載したすべて	**アップグレードの影響。新しい正常性モジュールを有効にし、アップグレード後にデバイス正常性ポリシーを適用します。** シャーシを読み取り専用デバイスとして Management Center に登録することで、Firepower 4100/9300 のシャーシレベルのヘルスアラートを表示できるようになりました。また、Firewall Threat Defense プラットフォーム障害のヘルスモジュールを有効にして、ヘルスポリシーを適用する必要があります。アラートは、メッセージセンター、ヘルスモニター（左側のペインの [デバイス（Devices）] でシャーシを選択）、およびヘルスイベントビューに表示されます。 マルチインスタンスモードで Cisco Secure Firewall 3100 のシャーシを追加し、正常性アラートを表示することもできます。これらのデバイスの場合は、Management Center を使用してシャーシを管理します。ただし、Firepower 4100/9300 シャーシの場合は、シャーシマネージャまたは FXOS CLI を使用する必要があります。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** 参照：「Add a Chassis to the Management Center」

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center のメモリ使用率の計算、アラート、およびスワップメモリのモニタリングが改善されました。	7.4.1	いずれか	**アップグレードの影響。メモリ使用量アラートのしきい値が引き下げられる可能性があります。** Management Center のメモリ使用量の精度が向上し、デフォルトのアラートしきい値が警告は88%、重大は90%に引き下げられました。しきい値が新しいデフォルト値よりも高かった場合、アップグレードによって自動的に下げられます。この変更を有効にするために正常性ポリシーを適用する必要はありません。高メモリプロセスを終了できない場合、システムメモリが極めて少ない状態で Management Center が再起動する可能性があることに注意してください。 新規または既存の Management Center の正常性ダッシュボードに新しいスワップメモリ使用状況メトリックを追加することもできます。[メモリ（Memory）] メトリックグループを選択していることを確認します。 新規/変更された画面： • **システム（⚙） > [正常性（Health）] > [モニタリング（Monitoring）] > [Firewall Management Center][ダッシュボードの追加/編集（Add/Edit Dashboard）][メモリ（Memory）]** • **システム（⚙） > [正常性（Health）] > [ポリシー（Policy）] > [Management Center正常性ポリシー（Management Center Health Policy）] > [メモリ（Memory）]** 参照：「Using Management Center Health Monitor」
展開とポリシー管理			
変更管理。	7.4.1	いずれか	変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。 この機能を有効にするための **システム（⚙） > [設定（Configuration）] > [変更管理（Change Management）]** ページが追加されました。有効にすると、**システム（⚙） > 変更管理のワークフロー** ページが表示され、メニューに新しい **[チケット（Ticket）]**（📋）クイックアクセスアイコンが表示されます。 参照：「Change Management」
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
FXOS アップグレードに含まれるファームウェアのアップグレード。	7.4.1	いずれか	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Management Center のアップグレード後に設定変更レポートを自動的に生成します。	7.4.1	いずれか	Management Center のメジャーおよびメンテナンスアップグレード後に、設定変更に関するレポートを自動的に生成できます。このレポートは、展開しようとしている変更を理解するのに役立ちます。レポートが生成されたら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。 その他のバージョンの制限：バージョン 7.4.1 以降の Management Center のアップグレードでのみサポートされます。バージョン 7.4.1 以前のバージョンへのアップグレードはサポートされていません。 新規/変更された画面：**システム（⚙）>[設定（Configuration）]>[設定のアップグレード（Upgrade Configuration）]>[アップグレード後のレポートの有効化（Enable Post-Upgrade Report）]** 参照：「Upgrade Configuration」
管理（Administration）			
Management Center ハードウェアのハードドライブを消去します。	7.4.1	いずれか	Management Center CLI を使用してリブートし、ハードドライブデータを完全に消去できます。消去が完了したら、新しいソフトウェアイメージをインストールできます。 新規/変更された CLI コマンド： **secure erase** 参照：「Secure Firewall Management Center Command Line Reference」
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			

機能	最小の Management Center	最小の Threat Defense	詳細
トラブルシューティングファイルの生成とダウンロードは、[デバイス（Device）] および [クラスタ（Cluster）] ページから実行できます。	7.4.1	7.4.1	[デバイス（Device）] ページの各デバイス、および [クラスタ（Cluster）] ページのすべてのクラスタノードのトラブルシューティング ファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。または、**[デバイス（Devices）] > [デバイス管理（Device Management）] > その他**（⋮）> [トラブルシューティング ファイル（Troubleshoot Files）] メニューからファイル生成をトリガーできます。 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）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]** 参照：「Generate Troubleshooting Files」
クラスタへの参加に失敗した場合のノードでのトラブルシューティングファイルの自動生成。	7.4.1	7.4.1	ノードがクラスタに参加できない場合、そのノードのトラブルシューティング ファイルが自動的に生成されます。[タスク（Tasks）] または [クラスタ（Cluster）] ページからファイルをダウンロードできます。 参照：「Troubleshooting the Cluster」
デバイスまたはデバイスクラスタの CLI 出力を表示します。	7.4.1	いずれか	デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。また、任意の **show** コマンドを入力して、出力を確認できます。 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（Cluster）] > [全般（General）]** 参照：「View CLI Output」

機能	最小の Management Center	最小の Threat Defense	詳細
データプレーン障害後の迅速なリカバリ。	7.4.1	7.4.1	データプレーンプロセスがクラッシュした場合、デバイスをリブートする代わりに、データプレーンプロセスのみリロードするようになりました。データプレーンプロセスのリロードに加えて、Snort および他のいくつかのプロセスもリロードされます。 ただし、ブートアップ中にデータプレーンプロセスがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードプロセスループの発生を回避できます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 プラットフォームの制限：マルチインスタンスモードではサポートされていません。 参照：Cisco Secure Firewall Threat Defense コマンドリファレンス および『Cisco Secure Firewall ASA シリーズ コマンド リファレンス』
廃止された機能			
廃止：イベント正常性アラートの頻繁なドレイン 。	7.4.1	7.4.1	[ディスク使用量（Disk Usage）] 正常性モジュールは、イベントの頻繁なドレインでアラートを生成しなくなりました。Management Center のアップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをバージョン 7.4.1 以降にアップグレードする（アラートの送信を停止する）まで、アラートが表示され続ける場合があります。 参照：「Disk Usage and Drain of Events Health Monitor Alerts」
廃止：VPN トンネルステータス正常性モジュール。	7.4.1	いずれか	VPN トンネルステータス正常性モジュールは廃止されました。代わりに VPN ダッシュボードを使用します。 参照：「VPN Monitoring and Troubleshooting」

機能	最小の Management Center	最小の Threat Defense	詳細
廃止：ダウンロード可能なアクセス制御リストと、FlexConfig を使用した RADIUS アイデンティティソースのシスコ属性値ペア ACL のマージ。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** この機能は、Management Center の Web インターフェイスでサポートされるようになりました。

バージョン 7.4.0 の Management Center 機能

（注） バージョン 7.4.0 は、Cisco Secure Firewall Management Center および Cisco Secure Firewall 4200 でのみ使用できます。バージョン 7.4.0 Management Center は他のデバイスモデルの古いバージョンを管理できますが、Threat Defense 7.4.0 を必要とする機能には Cisco Secure Firewall 4200 を使用する必要があります。他のすべてのデバイスプラットフォームのサポートは、バージョン 7.4.1 で再開されます。

表 *2 :* バージョン *7.4.0* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
再導入された機能			
再導入された機能。	7.4.0	機能に依存	バージョン 7.4.0 では、奇数番号のバージョン（7.1.x、 7.3.x）のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0.x、7.2.x）のメンテナンスリリースに含まれていた機能、機能拡張および重要な修正が再度サポートされます。 再導入された機能は次のとおりです。 • 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）。アップグレードの影響。 • Threat Defense の高可用性のための「誤フェールオーバー」の削減。 • 国コードの地理位置情報パッケージのみをダウンロードします。アップグレードの影響。

機能	最小の Management Center	最小の Threat Defense	詳細
プラットフォーム			
Management Center 1700、2700、4700。	7.4.0	いずれか	最大 300 台のデバイス管理が可能な Cisco Secure Firewall Management Center 1700、2700、および 4700 が導入されました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide
Microsoft Hyper-V 向けの Management Center Virtual。	7.4.0	いずれか	最大 25 台のデバイスを管理できる Microsoft Hyper-V 向けの Cisco Secure Firewall Management Center Virtual を導入しました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center Virtual 入門ガイド
Cisco Secure Firewall 4200。	7.4.0	7.4.0	Cisco Secure Firewall 4215、4225、および 4245 を導入しました。 これらのデバイスは、以下の新しいネットワークモジュールをサポートしています。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR4K-XNM-2X100G） • 4 ポート 200G QSFP+ ネットワークモジュール（FPR4K-XNM-4X200G） 参照： Cisco Secure Firewall 4215、4225、4245 ハードウェア設置ガイド
Cisco Secure Firewall 4200 のパフォーマンスプロファイルのサポート。	7.4.0	7.4.0	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 4200 に適用されるようになりました。以前は、この機能は Firepower 4100/9300 および Threat Defense Virtual でのみサポートされていました。 参照：「Configure the Performance Profile」
プラットフォームの移行			
Firepower 1000/2100 から Cisco Secure Firewall 3100 への移行。	7.4.0	いずれか	Firepower 1000/2100 から Cisco Secure Firewall 3100 に設定を簡単に移行できるようになりました。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[移行（Migrate）]** プラットフォームの制限：Firepower 1010 または 1010E からの移行はサポートされていません。 参照：「About Secure Firewall Threat Defense Model Migration」

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS への移行。	7.4.0	いずれか	Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS（300 台のデバイスライセンスあり）への移行。 参照： Cisco Secure Firewall Management Center モデル移行ガイド
Firepower Management Center 1600/2600/4600 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0	いずれか	Firepower Management Center 1600/2600/4600 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。 参照： Cisco Secure Firewall Management Center モデル移行ガイド

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower Management Center 1000/2500/4500 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0 のみ	7.0.0	

機能	最小の Management Center	最小の Threat Defense	詳細
			Firepower Management Center 1000/2500/4500 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。移行するには、古い Management Center をバージョン 7.0 からバージョン 7.4.0 に一時的にアップグレードする必要があります。 **重要** バージョン 7.4.0 は、移行プロセス中に 1000/2500/4500 でのみサポートされます。Management Center のアップグレードとデバイスの移行までの間隔は最小限に抑える必要があります。 移行プロセスを要約すると、次のようになります。 **1.** アップグレードと移行の準備をします。リリースノート、アップグレードガイド、および移行ガイドに記載されているすべての前提条件を読み、理解し、条件を満たしてください。 アップグレードする前に、古い Management Center の「移行準備ができている」こと、つまり、新たに展開されていて、完全にバックアップされていること、すべてのアプライアンスが正常な状態であることなどが特に重要です。新しい Management Center も設定する必要があります。 **2.** 古い Management Center とそのすべての管理対象デバイスを少なくともバージョン 7.0.0 にアップグレードします（バージョン 7.0.5 を推奨）。 すでに最小バージョンを実行している場合は、この手順をスキップできます。 **3.** 古い Management Center をバージョン 7.4.0 にアップグレードします。 アップグレードパッケージを解凍し（ただし、展開はしない）、Management Center にアップロードします。Special Release からダウンロードします。 **4.** モデル移行ガイドの説明に従って、Management Center を移行します。 **5.** 移行が成功したことを確認します。 移行しても期待どおりに機能せず、元に戻す場合、1000/2500/4500 の一般的な操作ではバージョン 7.4.0 がサポートされていないことに注意してください。古い Management Center をサポートされているバージョンに戻すには、バージョン 7.0 に再イメージ化し、バックアップから復元して、デバイスを再登録する必要があります。

機能	最小の Management Center	最小の Threat Defense	詳細
			参照： • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Cisco Secure Firewall Management Center モデル移行ガイド 移行プロセスの任意の時点で質問がある場合、またはサポートが必要な場合は、Cisco TAC にお問い合わせください。

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower Management Center 1000/2500/4500 から クラウド提供型 Firewall Management Center へのデバイスの移行。	7.4.0 のみ	7.0.3	

機能	最小の Management Center	最小の Threat Defense	詳細
			Firepower Management Center 1000/2500/4500 からクラウド提供型 Firewall Management Centerにデバイスを移行できます。 デバイスを移行するには、オンプレミス Management Center をバージョン 7.0.3（7.0.5 を推奨）からバージョン 7.4.0 に一時的にアップグレードする必要があります。バージョン 7.0 の Management Center ではクラウドへのデバイスの移行がサポートされていないため、この一時的なアップグレードが必要です。さらに、バージョン 7.0.3 以降（7.0.5 を推奨）を実行しているスタンドアロンおよび高可用性 Threat Defense デバイスのみが移行の対象となります。クラスタの移行は現時点ではサポートされていません。 **重要** バージョン 7.4.0 は、移行プロセス中に 1000/2500/4500 でのみサポートされます。Management Center のアップグレードとデバイスの移行までの間隔は最小限に抑える必要があります。 移行プロセスを要約すると、次のようになります。 **1.** アップグレードと移行の準備をします。リリースノート、アップグレードガイド、および移行ガイドに記載されているすべての前提条件を読み、理解し、条件を満たしてください。 アップグレードする前に、古い Management Center の「移行準備ができている」こと、つまり、移行するデバイスのみ管理していること、設定の影響（VPN の影響など）を評価していること、新たに展開されていて、完全にバックアップされていること、すべてのアプライアンスが正常な状態であることなどが特に重要です。 また、クラウドテナントのプロビジョニング、ライセンス付与、および準備もする必要があります。これには、セキュリティイベントロギングの方法を含める必要があります。サポートされていないバージョンが実行されるため、分析のためにオンプレミス Management Center を保持することはできません。 **2.** オンプレミス Management Center とそのすべての管理対象デバイスを少なくともバージョン 7.0.3 にアップグレードします（バージョン 7.0.5 を推奨）。 すでに最小バージョンを実行している場合は、この手順をスキップできます。 **3.** オンプレミス Management Center をバージョン 7.4.0 にアップグレードします。 アップグレードパッケージを解凍し（ただし、展開はしない）、Management Center

機能	最小の Management Center	最小の Threat Defense	詳細
			にアップロードします。Special Release からダウンロードします。 **4.** オンプレミス Management Center を CDO にオンボードします。 **5.** 移行ガイドの説明に従って、すべてのデバイスをオンプレミス Management Center から クラウド提供型 Firewall Management Center に移行します。 移行するデバイスを選択する場合は、[オンプレミスFMCからFTDを削除する（Delete FTD from On-Prem FMC）] を選択してください。変更をコミットするか、14 日が経過するまで、デバイスは完全には削除されないことに注意してください。 **6.** 移行が成功したことを確認します。 移行しても期待どおりに機能しない場合は、14 日以内に戻すことができます。戻さない場合は自動的にコミットされます。ただし、バージョン 7.4.0 は一般的な操作ではサポートされていないことに注意してください。オンプレミス Management Center をサポートされているバージョンに戻すには、再移行したデバイスを削除し、バージョン 7.0.x に再イメージ化し、バックアップから復元して、デバイスを再登録する必要があります。 参照： • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • オンプレミス Management Center 管理対象 Cisco Secure Firewall Threat DefenseFirepower Threat Defense のクラウド提供型 Firewall Management Center への移行 移行プロセスの任意の時点で質問がある場合、またはサポートが必要な場合は、Cisco TAC にお問い合わせください。
デバイス管理			

機能	最小の Management Center	最小の Threat Defense	詳細
シリアル番号を使用して Firepower 1000/2100 および Cisco Secure Firewall 3100を Management Centerに登録するロータッチプロビジョニング。	7.4.0	Management Center がパブリックに到達可能：7.2.0 Management Center がパブリックに到達できない：7.2.4	ロータッチプロビジョニングを使用すると、Firepower 1000/2100 および Cisco Secure Firewall 3100 デバイスで初期セットアップを実行することなく、シリアル番号でデバイスを Management Center に登録できます。Management Center は、この機能のために SecureX および Cisco Defense Orchestrator と統合されています。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（Device）]** > **[シリアル番号（Serial Number）]** その他のバージョンの制限：この機能は、Management Center がパブリックに到達できない場合、バージョン 7.3.x または 7.4.0 Threat Defense デバイスではサポートされません。サポートは、バージョン 7.4.1 で再開されています。 参照：「Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)」
[インターフェイス（Interfaces）]			

機能	最小の Management Center	最小の Threat Defense	詳細
マージされた管理インターフェイスと診断インターフェイス。	7.4.0	7.4.0	**アップグレードの影響。アップグレード後にインターフェイスをマージします。** 7.4以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。 7.4 以降にアップグレードした場合： • 診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 • 診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 プラットフォーム設定の場合、これは次のことを意味します。 • 診断インターフェイスで、HTTP、ICMP、または SMTP を有効にすることはできなくなりました。 • SNMP については、診断インターフェイスではなく管理インターフェイスでホストを許可できます。 • Syslog サーバーについては、診断インターフェイスではなく管理インターフェイスでアクセスできます。 • Syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前で指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。 • インターフェイスを指定しない場合、DNS ルックアップは管理専用ルーティングテーブルにフォールバックしなくなりました。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** 新規/変更されたコマンド： **show management-interface convergence** 参照：「Merge the Management and Diagnostic Interfaces」

機能	最小の Management Center	最小の Threat Defense	詳細
VXLAN VTEP IPv6 のサポート。	7.4.0	7.4.0	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 は、Threat Defense Virtual クラスタ制御リンクまたは Geneve カプセル化ではサポートされていません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [VTEP] > [VTEPの追加（Add VTEP）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit 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）]** 参照：「Configure Geneve Interfaces」
BGP および管理トラフィックのループバックインターフェイスのサポート。	7.4.0	7.4.0	AAA、BGP、DNS、HTTP、ICMP、IPsec フローオフロード、NetFlow、SNMP、SSH、および syslog にループバック インターフェイスを使用できるようになりました。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [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（Loopback Interface）] 参照：「Configure Loopback Interfaces」
ループバックおよび管理タイプのインターフェイス グループ オブジェクト。	7.4.0	7.4.0	管理専用インターフェイスまたはループバック インターフェイスのみを含むインターフェイス グループ オブジェクトを作成でき、作成したグループを DNS サーバー、HTTP アクセス、SSH などの管理機能に使用できます。ループバックグループは、ループバック インターフェイスを利用できるすべての機能で使用できますが、DNS では管理インターフェイスはサポートされていない点に注意してください。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）] > [追加（Add）] > [インターフェイスグループ（Interface Group）]** 参照：「Interface」
高可用性/拡張性			

機能	最小の Management Center	最小の Threat Defense	詳細
データインターフェイスを使用して、Threat Defense ハイアベイラビリティペアを管理します。	7.4.0	7.4.0	Threat Defense ハイアベイラビリティでは、Management Center との通信に通常のデータインターフェイスを使用できるようになりました。以前は、スタンドアロンデバイスのみがこの機能をサポートしていました。 参照：「Using the Threat Defense Data Interface for Management」
SD-WAN			
WAN サマリーダッシュボード。	7.4.0	7.2.0	WAN サマリーダッシュボードには、WAN デバイスとデバイスのインターフェイスのスナップショットが表示されます。また、WAN ネットワーク、デバイス正常性に関する情報、インターフェイス接続、アプリケーション スループット、および VPN 接続に関するインサイトが表示されます。WAN リンクを監視し、予防的かつ迅速な回復措置を実行できます。 新規/変更された画面：[概要（Overview）] > [WANサマリー（WAN Summary）] 参照：「WAN Summary Dashboard」
HTTP パスのモニタリングを使用したポリシーベースのルーティング。	7.4.0	7.2.0	ポリシーベースルーティング（PBR）は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集された評価指標（RTT、ジッター、パケット損失、およびMOS）を使用できるようになりました。インターフェイスの HTTP ベースのアプリケーション モニタリング オプションは、デフォルトで有効になっています。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[インターフェイスの編集（Edit interface）] > [パスモニタリング（Path Monitoring）] > [HTTPベースのアプリケーションモニタリングの有効化（Enable HTTP based Application Monitoring）] チェックボックス。 プラットフォームの制限：クラスタ化されたデバイスではサポートされていません。 参照：「Configure Path Monitoring Settings」

機能	最小の Management Center	最小の Threat Defense	詳細
ユーザー ID と SGT を使用したポリシーベースのルーティング。	7.4.0	7.4.0	ユーザーとユーザーグループ、および PBR ポリシーの SGT に基づいてネットワークトラフィックを分類できるようになりました。PBR ポリシーの拡張 ACL を定義するときに、ID および SGT オブジェクトを選択できます。 新規/変更された画面：[オブジェクト（Objects）]>[オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] > [拡張アクセスリストの追加/編集（Add/Edit Extended Access List）] > [拡張アクセスリストエントリの追加/編集（Add/Edit Extended Access List Entry）] > [ユーザー（Users）] および [セキュリティグループタグ（Security Group Tag）] 参照：「Configure Extended ACL Objects」
VPN			
Cisco Secure Firewall 4200 向け VTI ループバックインターフェイスの IPSec フローのオフロード。	7.4.0	7.4.0	Cisco Secure Firewall 4200 では、VTI ループバックインターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされます。以前は、この機能は Secure Firewall 3100 の物理インターフェイスでサポートされていました。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 その他の要件：FPGA ファームウェア 6.2 以降 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4200 の暗号デバッグの機能拡張。	7.4.0	7.4.0	暗号デバッグの機能拡張は次のとおりです。 • 暗号アーカイブは、テキスト形式とバイナリ形式で使用できるようになりました。 • 追加の SSL カウンタをデバッグに使用できます。 • スタックした暗号化ルールは、デバイスを再起動せずに ASP テーブルから削除できます。 新規/変更された CLI コマンド： **show counters** 参照：「Troubleshooting Using Crypto Archives」
VPN：リモートアクセス			

機能	最小の Management Center	最小の Threat Defense	詳細
Secure Client のメッセージ、アイコン、画像、接続/切断スクリプトをカスタマイズします。	7.4.0	7.1.0	Secure Client をカスタマイズして、それらのカスタマイズを VPN ヘッドエンドに展開できるようになりました。サポートされている Secure Client のカスタマイズは次のとおりです。 • GUI テキストとメッセージ • アイコンとイメージ • スクリプト • バイナリ • Customized Installer Transforms • Localized Installer Transforms エンドユーザーが Secure Client から接続すると、Threat Defense によりそれらのカスタマイズがエンドポイントに配布されます。 新規/変更された画面： • [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [Secure Clientのカスタマイズ（Secure Client Customization）] • [デバイス（Device）] > [リモートアクセス（Remote Access）] > [VPNポリシーの編集（Edit VPN policy）] > [詳細設定（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customization）] 参照：「Customize Cisco Secure Client」
VPN：サイト間			
VPN ノードの IKE および IPsec セッションの詳細を簡単に表示できます。	7.4.0	いずれか	サイト間 VPN ダッシュボードで、VPN ノードの IKE および IPsec セッションの詳細を使いやすい形式で表示できます。 新規/変更された画面：[概要（Overview）] > [サイト間VPN（Site to Site VPN）] の順に選択し、[トンネルステータス（Tunnel Status）] ウィジェットの下で、トポロジにカーソルを合わせて [表示（View）] をクリックし、[CLIの詳細（CLI Details）] タブをクリックします。 参照：「Monitoring the Site-to-Site VPNs 」

機能	最小の Management Center	最小の Threat Defense	詳細
接続イベントのサイト間 VPN 情報	7.4.0	7.4.0（Snort 3）	接続イベントに、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、[VPNアクション（VPN Action）] の 3 つの新しいフィールドが含まれるようになりました。ポリシーベースおよびルートベースのサイト間 VPN トラフィックの場合、これらのフィールドにより、接続が暗号化または復号化（またはその両方）されたかどうか、および実行ユーザーが示されます。 新規/変更された画面：**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [イベントのテーブルビュー（Table View of Events）]** 参照：「Site to Site VPN Connection Event Monitoring」
NAT 変換からサイト間 VPN トラフィックを簡単に免除します。	7.4.0	いずれか	サイト間 VPN トラフィックを NAT 変換から簡単に免除できるようになりました。 新規/変更された画面： • エンドポイントの NAT 免除の有効化：**[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [サイト間VPNの追加/編集（Add/Edit Site to Site VPN）] > [エンドポイントの追加/編集（Add/Edit Endpoint）] > [ネットワークアドレス変換からVPNトラフィックを免除する（Exempt VPN traffic from network address translation）]** • NAT ポリシーのないデバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [NAT免除（NAT Exemptions）]** • 単一デバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [Threat Defense NATポリシー（Threat Defense NAT Policy）] > [NAT免除（NAT Exemptions）]** 参照：「NAT Exemption」
ルーティング			
IPv6 ネットワークで BGP のグレースフルリスタートを構成します。	7.4.0	7.3.0	管理対象デバイスのバージョン 7.3 以降の IPv6 ネットワークに対しては、BGP グレースフルリスタートを設定できます。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] > [BGP] > [IPv6] > [ネイバー（Neighbor）] > [ネイバーの追加/編集（Add/Edit Neighbor）]。 参照：「Configure BGP Neighbor Settings」

機能	最小の Management Center	最小の Threat Defense	詳細
動的 VTI による仮想ルーティング。	7.4.0	7.4.0	ルートベースのサイト間 VPN にダイナミック VTI を使用して仮想ルータを設定できるようになりました。 新規/変更された画面：[使用可能なインターフェイス（Available Interfaces）] の下の [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）] > [仮想ルータのプロパティ（Virtual Router Properties）] > [ダイナミック VTI インターフェイス（Dynamic VTI interfaces）]。 プラットフォームの制限：ネイティブモードのスタンドアロンまたは高可用性デバイスでのみサポートされます。コンテナインスタンスやクラスタ化されたデバイスではサポートされていません。 参照：「About Virtual Routers and Dynamic VTI」
アクセス制御：脅威の検出とアプリケーションの識別			

機能	最小の Management Center	最小の Threat Defense	詳細
クライアントレスの Zero Trust アクセス。	7.4.0	7.4.0（Snort 3）	Zero Trust アクセスが導入され、外部の SAML ID プロバイダー（IdP）ポリシーを使用して、ネットワークの内部（オンプレミス）または外部（リモート）から保護された Web ベースのリソース、アプリケーション、またはデータへのアクセスを認証および承認できます。 設定では、ゼロトラストアプリケーションポリシー、アプリケーショングループ、およびアプリケーションを指定します。 新規/変更された画面： • **[ポリシー（Policies）] > [Zero Trustアプリケーション（Zero Trust Application）]** • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** • **[概要（Overview）] > [ダッシュボード（Dashboard）] > [Zero Trust]** 新規/変更された CLI コマンド： • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** 参照：「Zero Trust Access」

機能	最小の Management Center	最小の Threat Defense	詳細
暗号化された可視性エンジン機能の拡張。	7.4.0	7.4.0（Snort 3）	暗号化された可視性エンジン（EVE）で、次のことができるようになりました。 • 脅威スコアに基づいて暗号化トラフィック内の悪意のある通信をブロックする。 • EVE で検出されたプロセスに基づいてクライアント アプリケーションを判断する。 • 検出のために、フラグメント化された Client Hello パケットを再構成する。 新規/変更された画面：アクセス コントロール ポリシーの詳細設定を使用して EVE を有効にし、これらの設定を行います。 参照：「Encrypted Visibility Engine」
特定のネットワークとポートをエレファントフローのバイパスまたはスロットリングから免除します。	7.4.0	7.4.0（Snort 3）	エレファントフローのバイパスまたはスロットリングから特定のネットワークとポートを免除できるようになりました。 新規/変更された画面： • アクセス コントロール ポリシーの詳細設定でエレファントフロー検出を構成するときに、[エレファントフローの修復（Elephant Flow Remediation）] オプションを有効にすると、[ルールの追加（Add Rule）] をクリックして、バイパスまたはスロットリングから免除するトラフィックを指定できるようになりました。 • システムがバイパスまたはスロットリングから免除されているエレファントフローを検出すると、[エレファントフローが免除されました（Elephant Flow Exempted）] という理由でフロー中接続イベントを生成します。 プラットフォームの制限：Firepower 2100 シリーズではサポートされていません。 参照：「Elephant Flow Detection」

機能	最小の Management Center	最小の Threat Defense	詳細
カスタム アプリケーションディテクタを使用した最初のパケットアプリケーションの識別。	7.4.0	7.4.0（Snort 3）	新しい Lua ディテクタ API が導入され、TCP セッションの最初のパケットの IP アドレス、ポート、およびプロトコルがアプリケーションプロトコル（サービス AppID）、クライアントアプリケーション（クライアント AppID）、および Web アプリケーション（ペイロード AppID）にマッピングされます。この新しい Lua API addHostFirstPktApp は、パフォーマンスの向上、再検査、およびトラフィック内の攻撃の早期検出に使用されます。この機能を使用するには、カスタムアプリケーション ディテクタの高度なディテクタで検出基準を指定して、Lua ディテクタをアップロードする必要があります。 参照：「Custom Application Detectors」
機密データの検出とマスキング。	7.4.0	7.4.0（Snort 3）	**アップグレードの影響。デフォルトポリシーの新しいルールが有効になります。** 社会保障番号、クレジットカード番号、E メールなどの機密データは、インターネットに意図的に、または誤って漏洩される可能性があります。機密データの検出は、機密データの漏洩の可能性を検出してイベントを生成するために使用され、大量の個人識別情報（PII）データが転送された場合にのみイベントを生成します。機密データの検出では、組み込みパターンを使用して、イベントの出力で PII をマスクできます。 データマスキングの無効化はサポートされていません。 参照：「Custom Rules in Snort 3」
JavaScript インスペクションの改善。	7.4.0	7.4.0（Snort 3）	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 インスペクションを改善しました。 参照：「HTTP Inspect Inspector」および Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
ファイルおよびマルウェアイベントに含まれる MITRE 情報。	7.4.0	7.4.0	ファイルおよびマルウェアイベントに MITRE 情報（ローカルマルウェア分析結果）が含まれるようになりました。以前は、この情報は侵入イベントについてのみ利用可能でした。MITRE 情報は、クラシックイベントビューと統合イベントビューの両方で表示できます。MITRE 列は、両方のイベントビューでデフォルトで非表示になっていることに注意してください。 参照：「Local Malware Analysis」および「File and Malware Event Fields」

機能	最小の Management Center	最小の Threat Defense	詳細
メモリが少ない Snort 2 デバイス用の小規模 VDB。	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	すべて（Snort 2）	**アップグレードの影響。メモリが少ないデバイスのアプリケーション ID が影響を受けます。** VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA 5506-X シリーズ、ASA-5508-X、5512-X、5515-X、5516-X、5525-X、5545-X バージョンの制限：小規模 VDB をインストールできるかどうかは、管理対象デバイスではなく Management Center のバージョンによって決まります。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 Management Center をアップグレードする場合、導入環境内にメモリの少ないデバイスが 1 つでも含まれていると、VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。 参照：「Update the Vulnerability Database」
アクセス制御：アイデンティティ			
Cisco Secure 動的属性コネクタによる動的オブジェクト管理の機能強化。	7.4.0	いずれか（Any）	次を使用した動的オブジェクト管理がサポートされるようになりました。 • Management Center の Cisco Secure 動的属性コネクタ。アップグレード • スタンドアロン アプリケーションとしての Cisco Secure 動的属性コネクタ 2.1。 参照：「Cisco Secure Dynamic Attributes Connector」および Cisco Secure Dynamic Attributes Connector コンフィギュレーション ガイド、バージョン2.1 [英語]

機能	最小の Management Center	最小の Threat Defense	詳細
ユーザー ID ソースとしての Microsoft Azure AD。	7.4.0	7.4.0	Microsoft Azure Active Directory（Azure AD）レルムと ISE を使用すると、ユーザーを認証したりユーザー制御のためにユーザーセッションを取得したりできます。 新規/変更された画面： • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [レルムを追加（Add Realm）] > [Azure AD（Azure AD）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（ Realms）] > [アクション（Actions）]（ユーザーのダウンロード、コピー、編集、削除など） サポートされている ISE バージョン：3.0 パッチ 5 以降、3.1（任意のパッチレベル）、3.2（任意のパッチレベル） 参照：「Create a Microsoft Azure Active Directory Realm」
イベントロギングおよび分析			
Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして設定できます。	7.4.0	いずれか（Any）	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** NetFlow は、パケットフローの統計情報を提供するシスコアプリケーションの 1 つです。Management Center の Web インターフェイスを使用して、Threat Defense デバイスを NetFlow エクスポータとして設定できるようになりました。既存の NetFlow 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。 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）] > [Threat Defense設定ポリシー（Threat Defense Settings policy）] > [NetFlow]** 参照：「Configure NetFlow」

機能	最小の Management Center	最小の Threat Defense	詳細
ログに記録された暗号化接続での「不明な」SSL アクションに関する詳細。	7.4.0	7.4.0	イベントレポートおよび復号ルールマッチングの有用性が向上しました。 • 暗号化された接続の SSL ハンドシェイクが完了していないかどうかを示す新しい**SSL ステータス**。ログに記録された接続の SSL ハンドシェイクが完了していない場合、接続イベントの [SSLステータス（SSL Status）] 列に「不明（不完全なハンドシェイク）（Unknown (Incomplete Handshake)）」と表示されます。 • 証明書のサブジェクト代替名（SAN）は、強化された復号ルールマッチングの認証局（CA）名を照合するときに使用されるようになりました。 新規/変更された画面： • [分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [SSLステータス（SSL Status）] • [分析（Analysis）] > [接続（Connections）] > [セキュリティ関連イベント（Security-Related Events）] > [SSLステータス（SSL Status）] 参照：「Connection and Security-Related Connection Event Fields」
ヘルス モニタリング			
OpenConfig を使用して、テレメトリを外部サーバーにストリーミング。	7.4.0	7.4.0	OpenConfig を使用して、メトリックとヘルスモニタリング情報を Threat Defense デバイスから外部サーバー（gNMI コレクタ）に送信できるようになりました。TLS により暗号化された接続を開始するように Threat Defense またはコレクタを設定できます。 新規/変更された画面：**システム（⚙）** > **[ヘルス（Health）]** > **[ポリシー（Policy）]** > **[Firewall Threat Defenseポリシー（Firewall Threat Defense Policies）]** > **[設定（Settings）]** > **[OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]** 参照：「Send Vendor-Neutral Telemetry Streams Using OpenConfig」
新しいASP ドロップメトリック。	7.4.0	7.4.0	新規または既存のデバイス正常性ダッシュボードに、600 を超える新しいASP（高速セキュリティパス）ドロップメトリックを追加できます。[ASP ドロップ（ASP Drops）] メトリックグループを選択していることを確認します。 新規/変更された画面：**システム（⚙）** > **[正常性（Health）]** > **[モニター（Monitor）]** > **[デバイス（Device）]** 参照：「show asp drop Command Usage」

機能	最小の Management Center	最小の Threat Defense	詳細
管理（Administration）			
詳細な Management Center の監査ログを syslog に送信します。	7.4.0	いずれか	構成データの形式とホストを指定することにより、構成変更を監査ログデータの一部として syslog にストリーミングできます。Management Centerは、監査構成ログのバックアップと復元をサポートしています。 新規/変更された画面：**システム**（⚙）> [設定（Configuration）] > [監査ログ（Audit Log）] > [設定変更の送信（Send Configuration Changes）]。 参照：「Stream Audit Logs to Syslog」
アクセス コントロール ポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	いずれか	カスタムユーザーロールを定義して、アクセス コントロール ポリシーおよびルールの侵入設定と、その他のアクセス コントロール ポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [アクセスコントロールポリシー（Access Control Policy）] > [アクセスコントロールポリシーの変更（Modify Access Control Policy）] > [脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。 参照：「Create Custom User Roles」
証明書の失効を確認する際の IPv6 URL のサポート。	7.4.0	7.4.0	以前は、Threat Defense は IPv4 OCSP URL のみをサポートしていました。現在、Threat Defense は IPv4 と IPv6 の両方の OCSP URL をサポートしています。 参照：「Requiring Valid HTTPS Client Certificates」および「Certificate Enrollment Object Revocation Options」

機能	最小の Management Center	最小の Threat Defense	詳細
デフォルトの NTP サーバーが更新されました。	7.4.0	いずれか	新しい Management Center の展開では、デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。Management Center を使用して、独自のデバイスに時刻を提供することを推奨します。**システム**（⚙）>**[設定（Configuration）]**>**[時刻の同期（Time Synchronization）]**で Management Center の NTP サーバーを更新できます。 参照：「Internet Access Requirements」
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			

機能	最小の Management Center	最小の Threat Defense	詳細
ユーザービリティの拡張。	7.4.0	いずれか	次の作業に進んでください。 • **システム**（⚙）**>[スマートライセンス（Smart Licenses）]** から Threat Defense クラスタのスマートライセンスを管理します。以前は、[デバイス管理（Device Management）] ページを使用する必要がありました。 参照：デバイスクラスタのライセンス • メッセージセンター通知のレポートをダウンロードします。メッセージセンターで、[通知を表示（Show Notifications）] スライダの横にある新しい [レポートのダウンロード（Download Report）] アイコンをクリックします。 参照：システムメッセージの管理 • すべての登録済みデバイスのレポートをダウンロードします。**[デバイス（Devices）]>[デバイス管理（Device Management）]**に移動し、ページの右上にある新しい [デバイスリストレポートのダウンロード（Download Device List Report）] リンクをクリックします。 参照：管理対象デバイスリストのダウンロード • ネットワークおよびポートオブジェクトを複製します。オブジェクトマネージャ（**[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]**）で、ポートまたはネットワークオブジェクトの横にある新しい [クローン（Clone）] アイコンをクリックします。その後、新しいオブジェクトのプロパティを変更し、新しい名前で保存できます。 参照：ネットワークオブジェクトの作成およびポートオブジェクトの作成 • カスタム ヘルス モニタリング ダッシュボードを簡単に作成し、既存のダッシュボードを簡単に編集できます。 参照：「Correlating Device Metrics」
Secure Firewall 4200 のパケットキャプチャでキャプチャするトラフィックの方向を指定します。	7.4.0	7.4.0	Secure Firewall 4200 では、 コマンドで新しい**direction**キーワード**capture**を使用できます。 新規/変更された CLI コマンド：**capture***capture_name***switchinterface***interface_name* [**direction** {**both** | **egress** | **ingress**}] 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	最小の Management Center	最小の Threat Defense	詳細
Snort 3 が無応答になると再起動し、HA フェールオーバーがトリガーされる可能性があります。	7.4.0	7.4.0（Snort 3）	操作の継続性を向上させるために、応答しない Snort が高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスが応答しなくなった場合に Snort 3 が再起動されるようになったために発生します。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます）。 この機能は、デフォルトでイネーブルにされています。CLI を使用してフェールオーバーを無効にするか、Snort を再起動する条件として時間や無応答スレッド数を設定できます。 新規/変更された CLI コマンド： **configure snort3-watchdog** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Success Network テレメトリ。	7.4.0	いずれか	テレメトリの変更については、『Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.4.x』を参照してください。
Management Center REST API			
Management Center REST API。	7.4.0	いずれか	Management Center 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 Version 7.4」を参照してください。
廃止された機能			

機能	最小の Management Center	最小の Threat Defense	詳細
一時的に廃止された機能。	7.4.0	いずれか	

機能	最小の Management Center	最小の Threat Defense	詳細
			バージョン 7.4.0 へのアップグレードはサポートされていますが、現在のバージョンに含まれている重要な機能や修正、機能拡張が削除されます。代わりに、バージョン 7.4.1 以降にアップグレードしてください。 バージョン 7.2.5 ～ 7.2.x では、アップグレードにより以下が削除されます。 • Management Center によるインターフェイス同期エラーの検出。アップグレードの影響。 バージョン 7.2.6 ～ 7.2.x では、アップグレードにより以下が削除されます。 • Web 分析プロバイダーを更新しました。アップグレードの影響。 • Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。アップグレードの影響。 • NAT ルールの編集時にネットワークグループを作成します。 • 高可用性 Management Center 用の単一のバックアップファイル。 • 統合イベントビューアからパケットトレーサを開きます。 • 展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。アップグレードの影響。 • NTP 同期の問題に関する正常性アラート。アップグレードの影響。 • 前回の展開以降の設定変更に関するレポートを表示および生成します。 • デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。

機能	最小の Management Center	最小の Threat Defense	詳細
			• 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。アップグレードの影響。 • スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。アップグレードの影響。 • アクセス制御オブジェクトの最適化を有効または無効にします。 • クラスタ制御リンク ping ツール。 • Snort 3 コアダンプの頻度を設定します。 • Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。
廃止：FlexConfig を使用した NetFlow。	7.4.0	いずれか	Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして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。 参照：「Configure NetFlow」

バージョン 7.3.1 の Management Center 機能

表 *3 :* バージョン *7.3.1.1* での *Management Center* の機能

機能	最小の Management Center	最小の Threat Defense	詳細
メモリが少ない Snort 2 デバイス用の小規模 VDB。	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	すべて（Snort 2）	**アップグレードの影響。 メモリが少ないデバイスのアプリケーション ID が影響を受けます。** VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA 5506-X シリーズ、ASA-5508-X、5512-X、5515-X、5516-X、5525-X、5545-X バージョンの制限：小規模 VDB をインストールできるかどうかは、管理対象デバイスではなく Management Center のバージョンによって決まります。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 Management Center をアップグレードする場合、導入環境内にメモリの少ないデバイスが 1 つでも含まれていると、VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。 参照：「Update the Vulnerability Database」

表 *4 :* バージョン *7.3.1* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3105。	7.3.1	7.3.1	Cisco Secure Firewall 3105 を導入しました。

バージョン 7.3.0 の Management Center 機能

表 *5*：バージョン *7.3.0* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
プラットフォーム			
Management Center Virtual 300 for KVM。	7.3.0	いずれか	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。高可用性はサポートされていません。
Firewall 4100 のネットワークモジュール。	7.3.0	7.3.0	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。 • 2 ポート 100G ネットワークモジュール（FPR4K-NM-2X100G） サポートされているプラットフォーム：Firepower 4112、4115、4125、4145
ISA 3000 システム LED によるシャットダウンのサポート。	7.3.0	7.0.5 7.3.0	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。

機能	最小の Management Center	最小の Threat Defense	詳細
Threat Defense Virtual 用の新しいコンピューティングシェイプと OCI 用の Management Center Virtual。	7.3.0	7.3.0	OCI 用の Threat Defense Virtual では、次のコンピューティングシェイプのサポートが追加されています。 • インテル VM.DenseIO2.8 • インテル VM.StandardB1.4 • インテル VM.StandardB1.8 • インテル VM.Standard1.4 • インテル VM.Standard1.8 • インテル VM.Standard3.Flex • インテル VM.Optimized3.Flex • AMD VM.Standard.E4.Flex OCI 用の Management Center Virtual では、次のコンピューティングシェイプのサポートが追加されています。 • インテル VM.StandardB1.4 • インテル VM.Standard3.Flex • インテル VM.Optimized3.Flex • AMD VM.Standard.E4.Flex VM.Standard2.4 および VM.Standard2.8 コンピューティングシェイプは、2022 年 2 月に注文可能期間が終了したことに注意してください。バージョン 7.3 以降を導入する場合は、別のコンピューティングシェイプにすることを推奨します。 互換性のあるコンピューティングシェイプの詳細については、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。
インターフェイス			

機能	最小の Management Center	最小の Threat Defense	詳細
仮想アプライアンスの IPv6 サポート。	7.3.0	7.3.0	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。 • AWS • Azure • OCI • KVM • VMware 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。
VTI のループバック インターフェイス サポート。	7.3.0	7.3.0	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。 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）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
冗長マネージャアクセス データ インターフェイス。	7.3.0	7.3.0	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。 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）] > [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）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
IPv6 DHCP。	7.3.0	7.3.0	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。 • 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。 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）] > [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）]** 新規/変更された CLI コマンド：**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
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	7.3.0	7.3.0	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。 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）]** 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。
高可用性/拡張性			
KVM および Azure 向け Management Center Virtual の高可用性。	7.3.0	いずれか	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。 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。 KVM でサポートされているプラットフォーム：FMCv10、FMCv25、FMCv300 Azure でサポートされているプラットフォーム：FMCv10、FMCv25 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。
Azure 向け Threat Defense Virtual のクラスタリング。	7.3.0	7.3.0	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。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	7.3.0	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。
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。	7.3.0	7.3.0	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。 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）]** 新規/変更された CLI コマンド：**restore remote-manager-backup** 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。
リモートアクセス VPN			
RA VPN ダッシュボード。	7.3.0	いずれか	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。 • 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。 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）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
TLS 1.3 で RA VPN 接続を暗号化します。	7.3.0	7.3.0	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。 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 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）]**。 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。 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。
サイト間 VPN			
サイト間 VPN ダッシュボードのパケットトレーサ。	7.3.0	いずれか	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 ダッシュボードにパケットトレーサ機能を追加しました。 **[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 [パケットトレーサ（Packet Tracer）] をクリックします。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
サイト間 VPN を使用したダイナミック VTI のサポート。	7.3.0	7.3.0	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。 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。 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。 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。
Umbrella SIG 統合の改善。	7.3.0	7.3.0	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。 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）]**。 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。
ルーティング			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center の Web インターフェイスから BGP の BFD を設定。	7.3.0	いずれか	**アップグレードの影響。** 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。 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）] > [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。 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。
VTI の IPv4 および IPv6 OSPF ルーティングのサポート。	7.3.0	7.3.0	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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
VTI の IPv4 EIGRP ルーティングのサポート。	7.3.0	7.3.0	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。 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。 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。
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。	7.3.0	7.3.0	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。
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。	7.3.0	7.1	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の基準に一致すると、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。 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）]** > **[一致基準と出力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。 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。
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
シスコからアップグレードパッケージを選択して、Management Center に直接ダウンロードします。	7.3..x のみ	いずれか	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。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 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
Threat Defense のウィザードを使用してアップグレードパッケージを Management Center にアップロードします。	7.3.x のみ	いずれか	ウィザードを使用して、脅威防御アップグレードパッケージをアップロードしたり、場所を指定したりできるようになりました。以前は（バージョンに応じて）、**システム**（⚙）>**[更新（Updates）]** または **システム**（⚙）> **[製品のアップグレード（Product Upgrades）]** を使用していました。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 参照：脅威防御のアップグレード
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。	7.3.0	いずれか	**アップグレードの影響。** 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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	7.3.0	

機能	最小の Management Center	最小の Threat Defense	詳細
			再イメージ化の影響。 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。 • 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 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。 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。 • 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「*Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100*」、次に「*ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100*」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「*ASA→Threat Defense: Firepower 1000, 2100 Appliance*

機能	最小の Management Center	最小の Threat Defense	詳細
			Mode; Secure Firewall 3100」を参照してください。 • 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。 『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「*Reimage the System with a New Software Version*」を参照してください。
アクセス制御と脅威検出			
SSL ポリシーの名前が復号ポリシーに変更されました。	7.3.0	いずれか	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。 新規/変更された画面： • 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）]。 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。
Snort 3 デバイスでの TLS サーバー ID 検出の改善。	7.3.0	7.3.0	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プローブを有効にする（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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	7.3.0	

機能	最小の Management Center	最小の Threat Defense	詳細
			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。 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。 • [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。 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。 • [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。 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。 • [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。 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

機能	最小の Management Center	最小の Threat Defense	詳細
			以降の Management Center のデフォルトです。Threat Defense 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。 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）]** 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。
EVE を使用して HTTP/3 および SMB over QUIC を検出します（Snort 3 のみ）。	7.3.0	7.3.0（Snort 3）	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。 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。
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）。	7.3.0	7.3.0（Snort 3）	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。 • 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）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
Snort 3 デバイスの JavaScript インスペクションの改善。	7.3.0	7.3.0（Snort 3）	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 インスペク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。 詳細については、『Snort 3 インスペクタリファレンス』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。
Snort 3 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）。	7.3.0	7.0（Snort 3）	Snort 3 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。 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。 新規/変更された画面： • 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）]** 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。

機能	最小の Management Center	最小の Threat Defense	詳細
アクセス制御ルールの競合分析。	7.3.0	いずれか	ルールの競合分析を有効にすると、ポリシーでの以前の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。 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。
イベントロギングおよび分析			
Snort 3 デバイスの NetFlow サポート。	7.3.0	7.3.0（Snort 3）	**アップグレードの影響。** 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。 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 エクスポータと 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。 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。
統合			
Cisco ACI Endpoint Update App と統合するための新しい修復モジュール	7.3.0	いずれか	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。 • 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。 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。
ヘルス モニタリング			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center の Web インターフェイスでのクラスタのヘルスモニター設定。	7.3.0	いずれか	Management Center の Web インターフェイスを使用して、クラスタのヘルスモ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。 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）]>[クラスタのヘルスモニターの設定（Cluster Health Monitor Settings）] 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。
デバイスクラスタのヘルスモニタリングが改善されました。	7.3.0	いずれか	ヘルスモニター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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	いずれか	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。 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。 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）]**>**[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。 モジュールのステータスは、ヘルスモニターの [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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower 4100/9300 の温度と電源を監視します。	7.3.0	7.3.0	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。 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。 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。 ヘルスモニターの [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。 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。
ライセンシング			

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	いずれか	ライセンスの名前を次のように変更しました。 • 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 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。 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）]** 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。
管理（Administration）			

機能	最小の Management Center	最小の Threat Defense	詳細
FlexConfig から Web インターフェイス管理に設定を移行します。	7.3.0	機能に依存	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。 • 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 移行後は、廃止された FlexConfig を削除するまで展開できません。 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）]** 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。
自動 VDB ダウンロード。	7.3.0	いずれか	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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
任意の VDB をインストールします。	7.3.0	いずれか	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。 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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
CA バンドルの自動更新。	7.3.0	7.3.0	**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。** 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。 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** バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。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。 参照：『Firepower Management Center Command Line Reference』および Cisco Secure Firewall Threat Defense コマンドリファレンス 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。
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			

機能	最小の Management Center	最小の Threat Defense	詳細

新しい How-To ウォークスルー。	7.3.0	機能に依存	次の How-To が追加されました。
			• 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。
			  • 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。
			
			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。

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。	7.3.0	いずれか	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。	7.3.0	いずれか	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。	7.3.0	いずれか	**[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。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.3.0	いずれか	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。
Firepower 4100/9300 および Threat Defense Virtual での CPU コア割り当てのパフォーマンスプロファイル。	7.3.0	7.3.0	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。 [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。 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。
Cisco Success Network テレメトリ。	7.3.0	いずれか	テレメトリの変更については、『Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.3.x』を参照してください。
Management Center REST API			
Management Center REST API。	7.3.0	機能に依存	Management Center 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			

機能	最小の Management Center	最小の Threat Defense	詳細
一時的に廃止された機能。	7.3.0	機能に依存	

機能	最小の Management Center	最小の Threat Defense	詳細
			バージョン 7.3 へのアップグレードはサポートされていますが、現在のバージョンに含まれている重要な機能や修正、機能拡張が削除されます。代わりに、バージョン 7.4.1 以降にアップグレードしてください。 バージョン 7.2.3 以降では、アップグレードにより以下が削除されます。 • Firepower 1010E。を使用して無効にすることができます。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 7.3.1.1 以降の Management Center を使用してください。 バージョン 7.2.4 以降では、アップグレードにより以下が削除されます。 • 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）。アップグレードの影響。 バージョン 7.2.5 以降では、アップグレードにより以下が削除されます。 • Management Center によるインターフェイス同期エラーの検出。アップグレードの影響。 バージョン 7.2.6 以降では、アップグレードにより以下が削除されます。 • Web 分析プロバイダーを更新しました。アップグレードの影響。 • Threat Defense の高可用性のための「誤フェールオーバー」の削減。 • 国コードの地理位置情報パッケージのみをダウンロードします。アップグレードの影響。 • Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。アップグレードの影響。 • NAT ルールの編集時にネットワークグループを作成します。

機能	最小の Management Center	最小の Threat Defense	詳細
			• 高可用性 Management Center 用の単一のバックアップファイル。 • 統合イベントビューアからパケットトレーサを開きます。 • 展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。アップグレードの影響。 • NTP 同期の問題に関する正常性アラート。アップグレードの影響。 • 前回の展開以降の設定変更に関するレポートを表示および生成します。 • デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。 • 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。アップグレードの影響。 • スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。アップグレードの影響。 • アクセス制御オブジェクトの最適化を有効または無効にします。 • クラスタ制御リンク ping ツール。 • Snort 3 コアダンプの頻度を設定します。 • Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。

機能	最小の Management Center	最小の Threat Defense	詳細
サポート終了：Firepower 4110、4120、4140、4150。	—	7.3.0	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。	—	7.3.0	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：Snort 2 デバイスの YouTube EDU コンテンツ制限。	7.3.0	いずれか	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モニターの設定。	7.3.0	いずれか	Management Center の Web インターフェイスからクラスタのヘルスモニター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。	7.3.0	いずれか	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。	7.3.0	いずれか	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。	7.3.0	いずれか	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。

バージョン 7.2.6 の Management Center 機能

表 *6 :* バージョン *7.2.6* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
再導入された機能			
Web 分析プロバイダーを更新しました。	7.0.6 7.2.6 7.4.1	いずれか	**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。** 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。 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。 必要最低限の Threat Defense：任意 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 ～ 7.2.5、7.3.x、または 7.4.0 ではサポートされていません。永久サポートは、バージョン 7.4.1 で再開されています。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。
インターフェイス			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。	7.2.6 7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、Option 82 がすでに設定されている DHCP パケットを Threat Defense DHCP リレーエージェントが受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合、Threat Defense のデフォルトではそのパケットはドロップされます。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイスの追加/編集（Add/Edit Device）]** > **[DHCP]** > **[DHCP リレー（DHCP Relay）]** その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。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場合は、FlexConfig をやり直してください。 参照：「Configure the DHCP Relay Agent」
NAT			
NAT ルールの編集時にネットワークグループを作成します。	7.2.6 7.4.1	いずれか	NAT ルールの編集時に、ネットワークオブジェクトに加えてネットワークグループを作成できるようになりました。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「複数のデバイスの NAT ルールのカスタマイズ」
高可用性/拡張性			
Threat Defense の高可用性のための「誤フェールオーバー」の削減。	7.2.6 7.4.0	7.2.6 7.4.0	その他のバージョンの制限：Management Center または Threat Defense バージョン 7.3.x ではサポートされていません。 参照：「Heartbeat Module Redundancy」

機能	最小の Management Center	最小の Threat Defense	詳細
高可用性 Management Center 用の単一のバックアップファイル。	7.2.6 7.4.1	いずれか	高可用性ペアのアクティブ Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 参照：「Unified Backup of Management Centers in High Availability」
イベントロギングおよび分析			
統合イベントビューアからパケットトレーサを開きます。	7.2.6 7.4.1	いずれか	統合イベントビュー（**[分析（Analysis）] > [統合イベント（Unified Events）]**）からパケットトレーサを開けるようになりました。目的のイベントの横にある省略記号アイコン（[...]）をクリックし、[パケットトレーサで開く（Open in Packet Tracer）] をクリックします。 他のバージョンの制限：バージョン 7.2.x では、省略記号アイコンの代わりに [展開（Expand）]アイコン（[>]）アイコンを使用します。Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Working with the Unified Event Viewer」
ヘルス モニタリング			
展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。	7.2.6 7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** Disk Usage 正常性モジュールは、展開履歴（ロールバック）ファイルが Management Center で過剰なディスク容量を使用している場合にアラートを発行するようになりました。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Disk Usage for Device Configuration History Files Health Alert」
NTP 同期の問題に関する正常性アラート。	7.2.6 7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** 新しい Time Server Status 正常性モジュールは、NTP 同期に関する問題を報告します。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Time Synchronization」および「Health Modules」
展開とポリシー管理			

機能	最小の Management Center	最小の Threat Defense	詳細
前回の展開以降の設定変更に関するレポートを表示および生成します。	7.2.6 7.4.1	いずれか	前回の展開以降の設定変更に関する次のレポートを生成、表示、および（zip ファイルとして）ダウンロードできます。 • ポリシー内の追加、変更、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスのポリシー変更レポート。 • ポリシー変更レポート生成のステータスに基づいて各デバイスを分類する統合レポート。 これは、Management Center または Threat Defense デバイスのいずれかのアップグレード後に特に役立ち、展開する前にアップグレードによって加えられた変更を確認できます。 新規/変更された画面：**[展開（Deploy）] > [高度な展開（Advanced Deploy）]**。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Download Policy Changes Report for Multiple Devices」
デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。	7.2.6 7.4.1	いずれか	デバイスのロールバックのために保持する展開履歴ファイルの数を最大 10（デフォルト）まで設定できるようになったため、Management Center のディスク容量を節約できます。 新規/変更された画面：[展開（Deploy）] > **[Deployment History]**（） > [展開設定（Deployment Setting）] > [構成バージョン設定（Configuration Version Setting）] その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Set the Number of Configuration Versions」
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
アップグレードの開始ページとパッケージ管理が改善されました。	7.2.6 7.4.1	いずれか	

機能	最小の Management Center	最小の Threat Defense	詳細
			新しいアップグレードページでは、アップグレードの選択、ダウンロード、管理、および展開全体への適用が容易になります。これには、Management Center、Threat Defense デバイス、およびすべての古いNGIPSv/ASA FirePOWER デバイスが含まれます。このページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、パッケージを手動でアップロードおよび削除したりできます。 リスト/直接ダウンロードアップグレードパッケージを取得するには、インターネットアクセスが必要です。インターネットアクセスがない場合は、手動管理に限定されます。適切なメンテナンスリリースのアプライアンスが少なくとも 1 つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • **システム**（⚙）> **製品のアップグレード**では、Management Center とすべての管理対象デバイスをアップグレードし、アップグレードパッケージを管理します。 • **システム**（⚙）> **[コンテンツの更新（Content Updates）]**で、侵入ルール、VDB、およびGeoDB を更新できるようになりました。 • **[デバイスの脅威防御のアップグレード**>（**Devices Threat Defense Upgrade**）**]** を選択すると、脅威防御のアップグレードウィザードに直接移動します。 • **システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーロール（User Role）]** > **[ユーザーロールの作成（Create User Role）]** > **[メニューベースの権限（Menu-Based Permissions）]**を使用すると、[製品のアップグレード（Product Upgrades）]（システムソフトウェア）へのアクセスを許可せずに、[コンテンツの更新（Content Updates）]（VDB、GeoDB、侵入ルール）へのアクセスを許可できます。 廃止された画面/オプション： • **システム**（⚙）> **[更新（Updates）]**は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御アップグレードウィザードの [アップグレードパッケージの追加（Add Upgrade Package）] ボタンは、新しいアップグレードページへの [アップグレードパッケージの管理（Manage Upgrade Packages）] リンクに置き換えられました。

機能	最小の Management Center	最小の Threat Defense	詳細
			その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense のアップグレードウィザードからの復元の有効化。	7.2.6 7.4.1	任意（7.1 以降にアップグレードする場合）	脅威防御アップグレードウィザードからの復元を有効化できます。 その他のバージョンの制限：Threat Defense をバージョン 7.1 以降にアップグレードする必要があります。Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense アップグレードウィザードからアップグレードするデバイスを選択します。	7.2.6	いずれか	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します。 脅威防御アップグレード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。ウィザード上で、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（および理由）、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。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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。	7.2.6 7.4.1	いずれか	Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[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 Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、**[デバイス（Devices）] > [Threat Defenseアップグレード（Threat Defense Upgrade）]**によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小の Management Center	最小の Threat Defense	詳細
Threat Defense の無人アップグレード。	7.2.6	いずれか	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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
さまざまなユーザーによる同時 Threat Defense アップグレードワークフロー。	7.2.6	いずれか	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。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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
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。	7.2.6	いずれか	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。 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。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
推奨リリースの通知。	7.2.6 7.4.1	いずれか	新しい推奨リリースが利用可能になると、Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center の新しいアップグレードウィザード。	7.2.6 7.4.1	いずれか	新しいアップグレード開始ページとウィザードにより、Management Center のアップグレードを簡単に実行できます。**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]**を使用して、Management Center で適切なアップグレードパッケージを入手したら、[アップグレード（Upgrade）] をクリックして開始します。 その他のバージョンの制限：バージョン 7.2.6 以降/7.4.1 以降からの Management Center のアップグレードでのみサポートされます。バージョン 7.3.x または 7.4.0 からのアップグレードではサポートされていません。 Management Center を任意のバージョンにアップグレードするには、Management Center で現在実行しているバージョンのアップグレードガイドを参照してください。：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド。バージョン 7.4.0 を実行している場合は、バージョン 7.3.x のガイドを使用できます。
同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。	7.2.6 7.4.1	いずれか	ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
管理（Administration）			
ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。	7.2.6 7.4.1	いずれか	**アップグレードの影響。システムは新しいリソースに接続します。** Management Center では、ソフトウェア アップグレード パッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Internet Access Requirements」

機能	最小の Management Center	最小の Threat Defense	詳細
スケジュール済みタスクでは、パッチおよび VDB 更新のみダウンロードされます。	7.2.6 7.4.1	いずれか	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）> **[製品のアップグレード（Product Upgrades）]**を使用します。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Software Update Automation」

機能	最小の Management Center	最小の Threat Defense	詳細
国コードの地理位置情報パッケージのみをダウンロードします。	7.2.6 7.4.0	いずれか	**アップグレードの影響。アップグレードすると、IPパッケージが削除される可能性があります。** バージョン 7.2.6以降/7.4.0 以降では、IP アドレスを国や大陸にマッピングする地理位置情報データベース（GeoDB）の国コードパッケージのみをダウンロードするようにシステムを設定できます。コンテキストデータを含む大規模な IP パッケージはオプションになりました。 IP パッケージのダウンロードは次のとおりです。 • バージョン 7.2.0 ～ 7.2.5：常に有効。 • バージョン7.2.6～7.2.x：デフォルトでは無効になっていますが、有効にすることができます。 • バージョン 7.3.x：常に有効。 • バージョン 7.4.0 ～ 7.4.1：デフォルトで有効になっていますが、無効にすることもできます。 ダウンロードがデフォルトで無効になっているバージョンに初めてアップグレードすると、システムはダウンロードを無効にし、既存の IP パッケージを削除します。IP パッケージがないと、オプションを手動で有効にして GeoDB を更新するまで、IP アドレスのコンテキスト地理位置情報データを表示できません。 新規/変更された画面： • バージョン 7.2.6/7.4.1：**システム**（⚙）**>[コンテンツの更新（Content Updates）]>[地理位置情報の更新（Geolocation Updates）]** • バージョン 7.4.0：**システム**（⚙）**>[更新（Updates）]>[地理位置情報の更新（Geolocation Updates）]** 参照：「Update the Geolocation Database」
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			

機能	最小の Management Center	最小の Threat Defense	詳細
アクセス制御オブジェクトの最適化を有効または無効にします。	7.2.6 7.4.1	いずれか	Management Center の Web インターフェイスからアクセス制御オブジェクトの最適化を有効化または無効化できるようになりました。 新規/変更された画面：**システム**（⚙）>**[設定（Configuration）]**>**[アクセス コントロールの設定（Access Control Preferences）]**>**[オブジェクトの最適化（Object Optimization）]** その他のバージョンの制限：アクセス制御オブジェクトの最適化は、バージョン 7.2.4 ～ 7.2.5 および 7.4.0 にアップグレードまたは再イメージ化されたすべての Management Center で自動的に有効になり、バージョン 7.3.x にアップグレードまたは再イメージ化されたすべての Management Center で自動的に無効になります。バージョン 7.2.6 以降/7.4.1 以降に再イメージ化された Management Center のデフォルトでは設定可能であり、有効になっていますが、これらのリリースにアップグレードする際には現在の設定が保持されます。
クラスタ制御リンク ping ツール。	7.2.6 7.4.1	いずれか	ping を実行して、すべてのクラスタノードがクラスタ制御リンクを介して相互に到達できることを確認できます。ノードがクラスタに参加できない主な原因の 1 つは、クラスタ制御リンクの設定が正しくないことです。たとえば、クラスタ制御リンクの MTU が、接続しているスイッチの MTU よりも大きい値に設定されている可能性があります。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**その他**（⋮）>**[クラスタのライブステータス（Cluster Live Status）]** その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照：「Perform a Ping on the Cluster Control Link」

機能	最小の Management Center	最小の Threat Defense	詳細
Snort 3 はメモリ使用量が過剰になると再起動し、HA フェールオーバーがトリガーされることがあります。	7.2.6 7.4.1	7.2.6（Snort 3） 7.4.1（Snort 3）	操作の継続性を向上させるために、Snort によるメモリ使用が過剰な場合、高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスのメモリ使用が過剰な場合に Snort 3 が再起動されるようになったためです。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます）。 この機能は、デフォルトでイネーブルにされています。CLI を使用して無効にしたり、メモリしきい値を設定したりできます。 プラットフォームの制限：クラスタ化されたデバイスではサポートされていません。 新規/変更された CLI コマンド：**configure snort3 memory-monitor**、**show snort3 memory-monitor-status** その他のバージョンの制限：Management Center または Threat Defense バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Snort 3 コアダンプの頻度を設定します。	7.2.6 7.4.1	7.2.6（Snort 3） 7.4.1（Snort 3）	Snort 3 コアダンプの頻度を設定できるようになりました。Snort がクラッシュするたびにコアダンプを生成する代わりに、次回 Snort がクラッシュしたときにのみコアダンプを生成できます。または、過去 1 日あるいは 1 週間以内にクラッシュが発生していない場合に生成します。 Snort 3 コアダンプは、スタンドアロンデバイスではデフォルトで無効になっています。高可用性およびクラスタ化されたデバイスの場合、デフォルトの頻度が毎回ではなく 1 日に 1 回になりました。 新規/変更された CLI コマンド：**configure coredump snort3**、**show coredump** その他のバージョンの制限：Management Center または Threat Defense バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。	7.2.6 7.4.1	7.2.6（4200 以外） 7.4.1	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100/4200 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの [**drop** { **disable** | **mac-filter** }]。 その他のバージョンの制限：Management Center または Threat Defense バージョン 7.3.x または 7.4.0 ではサポートされていません。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
廃止された機能			
廃止：FlexConfig を使用した DHCP リレーの信頼できるインターフェイス。	7.2.6 7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 その他のバージョンの制限：この機能は、Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。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場合は、FlexConfig もやり直してください。 参照：「Configure the DHCP Relay Agent」

バージョン 7.2.5 の Management Center 機能

表 *7:* バージョン *7.2.5* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
インターフェイス			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center によるインターフェイス同期エラーの検出。	7.2.5 7.4.1	いずれか	**アップグレードの影響。アップグレード後にインターフェイスを同期する必要がある場合があります。** 場合によっては、インターフェイスが正しく設定され、デバイス上で機能している場合でも、Management Center でインターフェイスの設定が欠落していることがあります。その場合、Management Center が実行されている場合は、次のことが発生します。 • バージョン 7.2.5：[インターフェイス（Interfaces）] ページでデバイスを編集して同期するまで展開がブロックされます。 • バージョン 7.2.6 以降/7.4.1 以降：展開は警告付きで許可されますが、最初に同期しないとインターフェイス設定を編集できません。 その他のバージョンの制限：Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。Management Center は、展開をブロックしたり、設定の欠落について警告したりしません。問題が発生していると思う場合は、インターフェイスを手動で同期できます。 参照：「Sync Interface Changes with the Management Center」

バージョン 7.2.4 の Management Center 機能

表 *8 :* バージョン *7.2.4* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.4	いずれか	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。 「Interface Overview」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
CA バンドルの自動更新。	7.0.5 7.1.0.3 7.2.4	7.0.5 7.1.0.3 7.2.4	**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。** 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。 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** バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。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。 参照：『Firepower Management Center Command Line Reference』および Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	最小の Management Center	最小の Threat Defense	詳細
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）。	7.2.4	いずれか	**アップグレードの影響。7.2.4 ～ 7.2.5 または 7.4.0 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。** 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。最適化は、Management Center で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（アップグレードで有効になった場合も含む）。ルールの数が多い場合、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 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します（アップグレードによって無効になった場合も含む）。この機能が有効または無効になった後は、メンテナンス時間帯や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推奨します。 新規/変更された画面：（バージョン 7.2.6/7.4.1 が必要）：**システム**（⚙） > **[設定（Configuration）]** > **[アクセス制御の設定（Access Control Preferences）]** > **[オブジェクトグループの最適化（Object-group optimization）]**。 その他のバージョン制限：Management Center バージョン 7.3.x ではサポートされていません。 参照：「Access Control Preferences」

機能	最小の Management Center	最小の Threat Defense	詳細
メモリが少ない Snort 2 デバイス用の小規模 VDB。	6.4.0.17 7.0.6 7.2.4 7.3.1.1 7.4.0	すべて（Snort 2）	**アップグレードの影響。メモリが少ないデバイスのアプリケーション ID が影響を受けます。** VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA 5506-X シリーズ、ASA-5508-X、5512-X、5515-X、5516-X、5525-X、5545-X バージョンの制限：小規模 VDB をインストールできるかどうかは、管理対象デバイスではなく Management Center のバージョンによって決まります。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 Management Center をアップグレードする場合、導入環境内にメモリの少ないデバイスが 1 つでも含まれていると、VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。 参照：「Update the Vulnerability Database」

バージョン 7.2.3 の Management Center 機能

表 *9*：バージョン *7.2.3* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower 1010E。	7.2.3.1 7.3.1.1	7.2.3	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 7.3.1.1 以降の Management Center を使用してください。 バージョンの制限：これらのデバイスは、バージョン 7.3.x および 7.4.0 をサポートしていません。サポートは、バージョン 7.4.1 で再開されています。 参照：「Regular Firewall Interfaces」

バージョン 7.2.2 の Management Center 機能

このリリースでは、安定性、ハードニング、パフォーマンスの機能強化が導入されています。

バージョン 7.2.1 の Management Center 機能

表 *10 :* バージョン *7.2.1* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.1	7.2.1	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。 • 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） 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）] 詳細については、「Inline Sets and Passive Interfaces」を参照してください。
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。	7.2.1	7.2.1	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。 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。

バージョン 7.2.0 の Management Center 機能

表 *11* : バージョン *7.2.0* の *Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
プラットフォーム			
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。	7.2.0	7.2.0	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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
クラウド管理型の脅威防御デバイス向けの分析モード。	7.2.0	7.0.3 7.2.0	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。 バージョン 7.2 以降を実行しているオンプレミスハードウェアおよび仮想 Management Center では、クラウド管理型の Threat Defense 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。オンプレミス Management Center 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。 新規/変更された画面： • クラウド管理型デバイスをオンプレミス Management Center 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、そのデバイス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。 新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** バージョンの制限：Threat Defense バージョン 7.1 ではサポートされていません。 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。
ISA 3000 によるシャットダウンのサポート。	7.2.0	7.2.0	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			

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	7.2.0	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。 • 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： • [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。
16 ノードクラスタのサポート。	7.2.0	7.2.0	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。 • Firepower 4100/9300 • AWS 向け Threat Defense Virtual • GCP 向け Threat Defense Virtual 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。 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。
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。	7.2.0	7.2.0	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す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。

機能	最小の Management Center	最小の Threat Defense	詳細
GCP 向け Threat Defense Virtual の自動スケール。	7.2.0	7.2.0	**アップグレードの影響。GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできません。** 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 Virtua 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 Virtua の自動スケールをサポートするようになりました。 バージョンの制限：この機能のサポートに必要なインターフェイスの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。 詳細については、Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。
インターフェイス			
Firepower 2100 および Cisco Secure Firewall 3100 で LLDP をサポート。	7.2.0	7.2.0	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。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）]>[インターフェイス（Interfaces）]>[ハードウェア構成（Hardware Configuration）]>[LLDP] 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** 詳細については、「Interface Overview」を参照してください。
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。	7.2.0	7.2.0	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。 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）] 詳細については、「Interface Overview」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3130 および 3140 のブレークアウトポート。	7.2.0	7.2.0	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 ブレークアウトポートを構成できるようになりました。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）]>[シャーシの操作（Chassis Operations）] 詳細については、「Interface Overview」を参照してください。
Management Center の Web インターフェイスから VXLAN を設定。	7.2.0	いずれか	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** 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。 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。 新規/変更された画面： • 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）] 詳細については、「Regular Firewall Interfaces」を参照してください。
NAT			
複数の NAT ルールを同時に有効化、無効化、削除。	7.2.0	いずれか	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。 詳細については、「Network Address Translation」を参照してください。
VPN			

機能	最小の Management Center	最小の Threat Defense	詳細
RA VPN 接続プロファイル用の証明書と SAML 認証。	7.2.0	7.2.0	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。 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。 詳細については、「Remote Access VPN」を参照してください。
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。	7.2.0	7.2.0	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。 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。 詳細については、「Site-to-Site VPNs」を参照してください。
Cisco Secure Firewall 3100 の IPsec フローのオフロード。	7.2.0	7.2.0	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。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 詳細については、「Site-to-Site VPNs」を参照してください。
ルーティング			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center の Web インターフェイスから EIGRP を設定。	7.2.0	いずれか	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** 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。 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。 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] 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。
Firepower 1010 で仮想ルータをサポート。	7.2.0	7.2.0	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。 詳細については、「Virtual Routers」を参照してください。
ユーザー定義の仮想ルータで VTI をサポート。	7.2.0	7.2.0	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。 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）]** 詳細については、「Virtual Routers」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	7.2.0	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。 新規/変更された画面： • 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モ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）]**）。 新規/変更された CLI コマンド：**show policy route**、**show path-monitoring**、**clear path-monitoring** 詳細については、「Policy Based Routing」を参照してください。
脅威インテリジェンス			

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Umbrella からの DNS ベースの脅威インテリジェンス。	7.2.0	いずれか	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。 新規/変更された画面： • 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）] 詳細については、「DNS Policies」を参照してください。
Amazon GuardDuty からの IP ベースの脅威インテリジェンス。	7.2.0	いずれか	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。 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。
アクセス制御と脅威検出			

機能	最小の Management Center	最小の Threat Defense	詳細
動的オブジェクト管理： • 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	7.2.0	いずれか	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。 • 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） 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。 詳細については、*Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator*」の章を参照してください。 • オンプレミス Cisco Secure 動的属性コネクタ 2.0 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。 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。
Snort 3 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。	7.2.0	7.2.0（Snort 3）	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。 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。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。 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。 詳細については、「Elephant Flow Detection」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
暗号化された可視性エンジン機能の拡張。	7.2.0	7.2.0（Snort 3）	

機能	最小の Management Center	最小の Threat Defense	詳細
			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。 • 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す。 • 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。） 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。 • EVE は QUIC トラフィックで動作するようになりました。 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。 [TLS Fingerprint Process Name] は次に変更されました。 [暗号化された可視性プロセス名（Encrypted Visibility Process Name）] [TLS Fingerprint Process Confidence Score] は次に変更されました。 [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）] [TLS Fingerprint Malware Confidence] は次に変更されました。 [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）] [TLS Fingerprint Malware Confidence Score] は次に変更されました。 [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）]

機能	最小の Management Center	最小の Threat Defense	詳細
			検出タイプ：TLS フィンガープリント は次に変更されました。 検出タイプ：暗号化された可視性エンジン この機能には脅威ライセンスが必要になりました。 詳細については、「Access Control Policies」および「Application Detection」を参照してください。
TLS 1.3 インスペクション。	7.2.0	7.2.0（Snort 3）	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。 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。 詳細については、「SSL Policies」を参照してください。
ポートスキャン検出の改善。	7.2.0	7.2.0（Snort 3）	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。 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。 詳細については、「Threat Detection」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
VBAマクロインスペクション。	7.2.0	7.2.0（Snort 3）	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。 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。 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。 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。
JavaScript インスペクションの改善。	7.2.0	7.2.0（Snort 3）	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 インスペク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）インスペクション、および外部スクリプトを検査する機能が含まれます。 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、https_inspect Snort 3 インスペクターで js_norm（改良されたノーマライザ）および normalize_javascript（従来のノーマライザ）設定を使用します。 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 js_data オプションを使用します。 `alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)` 詳細については、『Snort 3 インスペクタリファレンス』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。

機能	最小の Management Center	最小の Threat Defense	詳細
SMB 3 インスペクションの改善。	7.2.0	7.2.0（Snort 3）	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。 • 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。 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。
[ポリシー管理（Policy Management）]			
アクセスコントロールポリシーのロック。	7.2.0	いずれか	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。 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。 詳細については、「Access Control Policies」を参照してください。
オブジェクトグループ検索をデフォルトで有効化。	7.2.0	いずれか	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。 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）]** 詳細については、「Device Management」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
アクセス制御ルールのヒットカウントは再起動後も存続します。	7.2.0	7.2.0	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。 新規/変更された CLI コマンド： **show rule hits** 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。
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。	7.2.0	いずれか	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。 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 ポリシーの編集中に、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。 詳細については、「Access Control Policies」を参照してください。
イベントロギングおよび分析			

機能	最小の Management Center	最小の Threat Defense	詳細
SecureX との統合、SecureX とのオーケストレーションの改善	7.2.0	いずれか	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。 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。 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。 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。 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。 バージョンの制限：この機能は、バージョン 7.0.2 以降および 7.2 以降に含まれています。バージョン 7.1 ではサポートされていません。バージョン 7.0.x で、新しい方法で SecureX との統合を有効にした場合は、この機能を無効にしない限り、バージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降にアップグレードすることをお勧めします。 参照： Cisco Secure Firewall Management Center（7.0.2 および 7.2）および SecureX 統合ガイド

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	7.0.0	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。 新規/変更された画面： • 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）] この機能には、Cisco Secure Network Analytics バージョン 7.1.4 が必要です。 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。
データベースアクセスの変更。	7.2.0	いずれか	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。 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。
eStreamer の変更。	7.2.0	いずれか	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。 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。
展開とポリシー管理			

機能	最小の Management Center	最小の Threat Defense	詳細
展開で管理接続が失われた場合の自動ロールバック。	7.2.0	7.2.0	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。 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）] > [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）] 詳細については、「Device Management」を参照してください。
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。	7.2.0	いずれか	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。 新規/変更されたページ：**[展開（Deploy）] > [Deployment History]**（）[アイコン（icon）]**その他**（）[全般的なレポート（Generate Report）]。 詳細については、「Configuration Deployment」を参照してください。
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
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」）。	7.2.0	7.2.0	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。 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。 • 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。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。 • 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 Firewall Management Center によって管理されるが、分析モードでオンプレミス Management Center に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。 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** 詳細については、「Copy Threat Defense Upgrade Packages between Devices」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	7.2.0	バージョン 7.2 以降の Management Center を使用して Threat Defense をバージョン 7.2 以降に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。 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。ヘルプについては、ご使用のバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 バージョンの制限：Threat Defense のバージョン 7.0.x または 7.1.x へのアップグレードはサポートされていません。
単一ノードクラスタのアップグレード。	7.2.0	いずれか	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。 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。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100

機能	最小の Management Center	最小の Threat Defense	詳細
CLI からの Threat Defense アップグレードの復元。	7.2.0	7.2.0	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。 **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。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。 詳細については、「Revert the Upgrade」を参照してください。
管理（Administration）			
DNS 要求を解決するための複数の DNS サーバーグループ。	7.2.0	いずれか	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 サーバー 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 サーバーを使用するキャッチオールの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 サーバー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 サーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS サーバーを使用します。 新規/変更された画面：[プラットフォーム設定（Platform Settings）] > [DNS] 詳細については、「Platform Settings」を参照してください。
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。	7.2.0	7.2.0	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。 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）]。 詳細については、「オブジェクト管理」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
GeoDB を 2 つのパッケージに分割。	7.2.0	いずれか	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。 バージョン 7.2.0 から 7.2.5 までの 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ます。バージョン 7.2.6 以降または 7.4.0 以降では、システムに IP パッケージを取得させるかどうかを設定できます。 エアギャップ展開などで更新を手動でダウンロードする場合、パッケージを個別にインポートする必要があります。 • 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 **[ヘルプ（Help）]**（?）>**[バージョン情報（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。 詳細については、「Updates」を参照してください。
Web インターフェイスのフランス語オプション。	7.2.0	いずれか	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。 新規/変更された画面：**システム**（⚙）>[設定（Configuration）]>[言語（Language）] 詳細については、「System Configuration」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	いずれか	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。 [展開（Deploy）] > [展開履歴（Deployment History）] は次に変更されました。 [展開（Deploy）] > **[Deployment History]**（右下隅） [展開（Deploy）] > [展開（Deployment）] は次に変更されました。 [展開（Deploy）] > [高度な展開（Advanced Deploy）] [分析（Analysis）] > [ユーザー（Users）] > [アクティブなセッション（Active Sessions）] は次に変更されました。 [統合（Integration）] > [ユーザー（Users）] > [アクティブなセッション（Active Sessions）] [分析（Analysis）] > [ユーザー（Users）] > [ユーザー（Users）] は次に変更されました。 [統合（Integration）] > [ユーザー（Users）] > [ユーザー（Users）] [分析（Analysis）] > [ユーザー（Users）] > [ユーザーアクティビティ（User Activity）] は次に変更されました。 [統合（Integration ）] > [ユーザー（Users）] > [ユーザーアクティビティ（User Activity）]

機能	最小の Management Center	最小の Threat Defense	詳細
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。	7.2.0	いずれか	

機能	最小の Management Center	最小の Threat Defense	詳細
			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。 （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。 [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）] [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）] [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）] [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）] [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）] [インテリジェンス は次 [統合（Integration）] > [インテ

機能	最小の Management Center	最小の Threat Defense	詳細
			（Intelligence）]>[インシデント（Incidents）] に変更されました。 リジェンス（Intelligence）]>[インシデント（Incidents）]
			システム（⚙）>[統合（Integration）] は次に変更されました。 [統合（Integration）]>[その他の統合（Other Integrations）]
			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）] は次に変更されました。 [統合（Integration）]>[セキュリティ分析とロギング（Security Analytics and Logging）]
			システム（⚙）>[SecureX] は次に変更されました。 [統合（Integration）]>[SecureX]
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			
Secure Firewall 3100 のパケットドロップ統計。	7.2.0	7.2.0	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。 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。
Cisco Success Network テレメトリ。	7.2.0	いずれか	テレメトリの変更については、『Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ、バージョン 7.2』を参照してください。
Management Center REST API			

機能	最小の Management Center	最小の Threat Defense	詳細
Management Center REST API。	7.2.0	いずれか	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			
廃止：FlexConfig を使用した EIGRP。	7.2.0	いずれか	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。 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。 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。 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。
廃止：FlexConfig を使用した VXLAN。	7.2.0	いずれか	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。 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。 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。 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。

機能	最小の Management Center	最小の Threat Defense	詳細
廃止：アップグレード前の自動トラブルシューティング。	7.2.0	いずれか	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。 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。

バージョン 7.1.0 の FMC 機能

（注） クラウド提供型 Firewall Management Center ではバージョン 7.1 デバイスを管理できません。クラウド管理対象デバイスでバージョン 7.0 を実行している場合は、バージョン 7.2 以降に直接アップグレードして、ここに記載されている機能を利用してください。

表 *12*：バージョン *7.1.0.3* の *FMC* 機能

機能	詳細
CA バンドルの自動更新。	**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。** 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。 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** バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。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。 参照：『Firepower Management Center Command Line Reference』および Cisco Secure Firewall Threat Defense コマンドリファレンス

表 *13* : バージョン *7.1.0* の *FMC* 機能

機能	詳細
プラットフォーム	
Cisco Secure Firewall 3100	Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。 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パンド 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。 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。 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）] 新規/変更された FTD CLI コマンド： **configure network speed**、**configure raid**、**show raid**、**show ssd**
AWS 用 FMCv300 OCI 用 FMCv300	AWS と OCI の両方に対応する FMCv300 が導入されました。FMCv300 は、最大 300 台のデバイスを管理できます。

機能	詳細
AWS 用 FTDv のインスタンス。	AWS 用 FTDv により、次のインスタンスのサポートが追加されています。 • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、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。	Azure 用 FTDv により、次のインスタンスのサポートが追加されています。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

機能	詳細
FDM を使用して、FMC による管理用に FTD を設定します。	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーやセキュリティ ゾーンなどの他のデフォルト設定は保持されないことに注意してください。FTD CLI を使用すると、管理と FMC のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス設定は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：[システム設定（System Settings）] > [管理センター（Management Center）]
デバイスのアップグレード	
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**システム**（⚙）> **[更新（Updates）]** ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス（Devices）]>[デバイスのアップグレード（Device Upgrade）] ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、コンテナインスタンスではサポートされません。 必要最低限の FTD：7.1

機能	詳細
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
Snort 3 後方互換性。	Snort 3 の場合、新しい機能と解決済みのバグでは、FMC とその管理対象デバイスを完全にアップグレードしている必要があります。Snort 2 とは異なり、新しい FMC（たとえば、バージョン 7.1）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。 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。
デバイス管理	
AWS インスタンスでの FTDv に対する Geneve インターフェイスサポート。	AWS ゲートウェイロードバランサ（GWLB）のシングルアームプロキシをサポートするために、Geneve カプセル化サポートが追加されました。AWS GWLB は、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて FTDv を拡張するロードバランサを組み合わせます。 このサポートには、Snort 3 が有効になっている FMC が必要であり、次のパフォーマンス階層で利用できます。 • FTDv20 • FTDv30 • FTDv50 • FTDv100
OCI 上の FTDv に対する Single Root I/O Virtualization（SR-IOV）のサポート	OCI 上の FTDv に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、FTDv のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。

機能	詳細
Firepower 1100 の LLDP サポート。	Firepower 1100 インターフェイスの Link Layer Discovery Protocol（LLDP）を有効にできるようになりました。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [LLDP] 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 1100（1120、1140、および 1150）
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、FMC でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）] サポートされるプラットフォーム：Firepower 1000/2100、Secure Firewall 3100
信頼された DNS サーバの指定のサポート。	FTD プラットフォーム設定を使用して、DNS スヌーピングに信頼できる DNS サーバーを指定できます。これは、ドメインを IP アドレスにマッピングすることにより、最初のパケットでアプリケーションを検出するのに役立ちます。デフォルトでは、信頼できる DNS サーバーには、DNS サーバーオブジェクト内の DNS サーバーと、dhcp-pool、dhcp-relay、および dhcp-client によって検出された DNS サーバーが含まれます。
デバイス設定のインポート/エクスポート。	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]
高可用性/拡張性	
高可用性 • AWS 用 FMCv • OCI 用 FMCv	AWS 用 FMCv および OCI 用 FMCv で高可用性がサポートされるようになりました。 FTD の展開では、2 つの同一ライセンスの FMC と、各管理対象デバイスに 1 つの FTD 権限が必要です。たとえば、FMCv10 高可用性ペアで 10 台の FTD デバイスを管理するには、2 個の FMCv10 権限と 10 個の FTD 権限が必要です。バージョン 6.5.0 ～ 7.0.x のクラシックデバイス（NGIPSv または ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。 サポートされるプラットフォーム：FMCv10、FMCv25、FMCv300（FMCv2 ではサポートされません）

機能	詳細
OCI 用 FTDv の自動スケール。	OCI 用 FTDv で自動スケーリングがサポートされるようになりました。 クラウドベースの展開におけるサーバレスインフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。
ファイアウォールの変更に対するクラスタの展開がより迅速に完了します。	ファイアウォールの変更に対するクラスタの展開がより迅速に完了するようになりました。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
ハイアベイラビリティ グループまたはクラスタ内のルートのクリア。	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティ グループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。
NAT	
変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
ルーティング	
仮想ルータを相互接続するための BGP 設定。	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、 [デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv4/v6] > [ルートのインポート/エクスポート（Route Import/Export）]
ユーザー定義の仮想ルータでの BGPv6 サポート。	FTD は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、 [デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv6]

機能	詳細
FMC Web インターフェイスから等コストマルチパス（ECMP）を設定します。	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** トラフィックゾーンのインターフェイスをグループ化し、FMC で Equal-Cost-Multi-Path（ECMP）ルーティングを設定できるようになりました。ECMP ルーティングは、以前は FlexConfig ポリシーを通じてサポートされていました。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[ルーティング（Routing）]**>**[ECMP]**
FMC Web インターフェイスからポリシーベースルーティングを設定します。	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** FMC Web インターフェイスからポリシーベースルーティング（PBR）を設定できるようになりました。これにより、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することができます。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。 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 7.1 以降が必要です。 • バージョン 7.0 以前を実行しているデバイスの場合は、引き続き FlexConfig を使用してポリシーベースルーティングを設定します。 FMC をバージョン 7.1 以降にアップグレードすると、ポリシーベースルーティング FlexConfig が削除されます。アップグレードする予定のないデバイスの場合は、FlexConfig を再実行し、「毎回」展開するように設定します。 • バージョン 7.1 以降を実行しているデバイスの場合、FMC Web インターフェイスを使用してポリシーベースルーティングを設定する必要があります。 デバイスをバージョン 7.1 以降にアップグレードした後、FMC Web インターフェイスでポリシーベースルーティング設定をやり直します。ポリシーベースルーティング FlexConfig は機能しません。 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）]**>**ポリシーベースルーティング（[Policy Based Routing）]**
リモートアクセス VPN	
RA VPN ポリシーのコピー。	既存のポリシーをコピーして、新しい RA VPN ポリシーを作成できるようになりました。**[デバイス（Devices）]**>**[VPN]**>**[リモートアクセス（Remote Access）]**の各ポリシーの横にコピーボタンが追加されました。

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

機能	詳細
VPN 監視ダッシュボード。	**ベータ版。** サイト間 VPN 監視ダッシュボードは次の機能を提供します。 • 全デバイスのトンネルステータス分布の可視化 • VPN トンネルで構成されるネットワークトポロジの可視化 • トポロジ、デバイス、ステータスなどの基準に基づいてトンネルを視覚的に切り離して調べる機能 （注） サイト間監視ダッシュボードはベータ機能であり、期待どおりに動作しない場合があります。実稼働環境では使用しないでください。
セキュリティ インテリジェンス	
プロキシされたトラフィックでのセキュリティ インテリジェンスのための Snort 3 サポート。	Snort 3 では、IP アドレスが HTTP リクエストに埋め込まれている HTTP プロキシトラフィックにセキュリティインテリジェンスを適用できるようになりました。たとえば、ユーザーが IP アドレスまたはネットワークを含むブロックリストまたは許可リストをアップロードすると、システムはプロキシ IP ではなく宛先サーバーの IP を照合します。その結果、宛先サーバーへのトラフィックを（セキュリティインテリジェンスの設定に応じて）ブロック、監視、または許可することができます。
侵入検知と防御	
ルールアクションのドロップ、拒否、書き換え、およびパスに対する Snort 3 のサポート。	バージョン 7.1 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。 • ドロップ：一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。侵入イベントを生成します。 • 拒否：一致するパケットをドロップし、この接続の以降のトラフィックもブロックします。TCP トラフィックの場合、TCP リセットを送信します。UDP トラフィックの場合、送信元および宛先ホストに ICMP ポート到達不能を送信します。侵入イベントを生成します。 • 書き換え：ルールの置換オプションに基づいて一致するパケットを上書きします。侵入イベントを生成します。 • パス：一致するパケットが他の侵入ルールによる評価なしで通過することを許可します。侵入イベントを生成しません。 これらの新しいルールアクションを設定するには、侵入ポリシーの Snort 3 バージョンを編集し、各ルールの [ルールアクション（Rule Action）] ドロップダウンを使用します。

機能	詳細
TLS ベースの侵入ルールに対する Snort 3 のサポート。	Snort 3 で復号化された TLS トラフィックを検査する TLS ベースの侵入ルールを作成できるようになりました。この機能により、Snort 3 侵入ルールで TLS 情報を使用できます。
SMB2 上の DCE/RPC のインスペクションに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 は、SMB2 での DCE/RPC インスペクションをサポートします。 Snort 3 デバイスへの最初のアップグレード後の展開の後、既存の DCE/RPC ルールは、SMB2 での DCE/RPC の検査を開始します。以前は、これらのルールは SMB1 での DCE/RPC のみを検査していました。
侵入ルールの推奨に対する Snort 3 のサポート。	バージョン 7.1 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。 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。
ssl_version および **ssl_state** キーワードに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 では、**ssl_version** および **ssl_state** 侵入ルールキーワードがサポートされています。 シスコが提供する侵入ポリシーには、これらのキーワードを使用するアクティブルールが含まれます。これらを使用して、カスタム/サードパーティルールを作成、アップロード、および展開することもできます。バージョン 7.0.x では、これらのキーワードは Snort 2 でのみサポートされていました。Snort 3 では、これらのキーワードを含むルールはトラフィックに一致しないため、アラートを生成したり、トラフィックに影響を与えたりすることはできませんでした。ルールが予期したとおりに機能していないという通知はありませんでした。バージョン 7.1 以降の Snort 3 デバイスへの最初のアップグレード後の展開の後、これらのキーワードを含む既存のルールはトラフィックと一致します。
Identity Services およびユーザー制御	
HTTP/2 トラフィックのインターセプトに対する Snort 3 キャプティブポータルのサポート。	キャプティブポータルを使用したユーザー認証のために、HTTP/2 トラフィックをインターセプトしてリダイレクトできるようになりました。 ブラウザがリダイレクトを受信すると、ブラウザはリダイレクトに従い、HTTP/1 キャプティブポータルと同じプロセスを使用して idhttpsd（Apache Web サーバー）で認証します。認証後、idhttpsd によりユーザーは元の URL にリダイレクトされます。

機能	詳細
ホスト名ベースのリダイレクトに対する Snort 3 キャプティブポータルのサポート。	IDポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスのIPアドレスではなく、完全修飾ドメイン名（FQDN）にユーザーの認証をリダイレクトできます。 FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDNを使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカードFQDN、または複数のFQDNをサブジェクト代替名（SAN）に指定できます。 新規/変更された画面：ID ポリシー設定に [ホスト名にリダイレクト（Redirect to Host Name）] オプションが追加されました。
暗号化トラフィックの処理（TLS/SSL）	
拡張 TLS/SSL ポリシーオプション。	[SSLポリシー（SSL Policy）] ページの [詳細設定（Advanced Settings）] タブで、次の拡張 TLS/SSL ポリシーオプションを設定できるようになりました。 • ESNI（暗号化されたサーバー名識別）を要求するフローをブロックする • HTTP/3 アドバタイズメントを無効にする • 信頼できないサーバー証明書をクライアントに伝播する
暗号化されたセッションを可視化するための暗号化された可視性エンジン。	**ベータ版。** 暗号化された可視性エンジンを有効にすると、復号を必要とせずに暗号化されたセッションを可視化することができます。このエンジンによってトラフィックのフィンガープリントが収集され、分析されます。FMC 7.1 では、暗号化された可視性エンジンにより、TLS や QUIC などのプロトコルを含む暗号化されたトラフィックの可視性が向上します。そのトラフィックに対してアクションは適用されません。 暗号化された可視性エンジンは、デフォルトで無効になっています。これは、[実験段階の機能（Experimental Features）] セクションのアクセス コントロール ポリシーの [詳細（Advanced）] タブで有効にすることができます。 新規/変更された画面：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [*Access Control Policy name*] > [詳細（Advanced）]** （注） 暗号化された可視性エンジンは、可視性のために提供される実験段階のベータ機能です。誤検出を起こす可能性があります。
サービス ポリシー	

機能	詳細
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更された画面：[サービスポリシーの追加/編集（Add/Edit Service Policy）] ウィザードの [接続設定（Connection Settings）]。
ネットワークディスカバリ	
ネットワーク検出の Snort 3 サポートの改善（リモートネットワーク アクセスのサポート）。	ネットワーク検出とリモート ネットワーク アクセスのサポートの改善により、Snort 3 はこれらの機能について Snort 2 と同等になりました。強化された機能は次のとおりです。 • SMB トラフィックのホストとアプリケーションの検出：ネットワーク上の SMB トラフィックの場合、ホストはネットワークマップで検出され、SMB アプリケーションプロトコルと関連するオペレーティングシステム情報が検出されます。 • NetBIOS トラフィックの検出：NetBIOS トラフィックの場合、NetBIOS 名と、クライアントアプリケーションやオペレーティングシステムなどのアプリケーション関連情報が検出されます。 • ネットワーク検出ポリシーによって監視されるホスト/ネットワークのみのアプリケーションの検出：このフィルタリングロジックの機能拡張により、ネットワーク検出ルールに基づいて監視されているネットワークのアプリケーションを検出できます。 Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。
イベントロギングおよび分析	

機能	詳細
エレファントフローの識別とモニタリングに対する Snort 3 のサポート。	Snort 3 を実行する FTD では、エレファントフロー（システム全体のパフォーマンスに影響を与えるのに十分な大きさのシングルセッションネットワーク接続）を識別できるようになりました。デフォルトでは、エレファントフローの検出は自動的に有効になり、1GB/10 秒を超える接続を追跡および記録します。 接続イベントの新しい定義済み検索（Reason = Elephant Flow）を使用すると、エレファントフローをすばやく特定できます。ヘルスモニタを使用して、デバイス上のアクティブなエレファントフローを表示し、エレファントフローの発生率を CPU 使用率などの他のデバイスメトリックと関連付けるカスタム ヘルス ダッシュボードを作成することもできます。 この機能を無効にするか、サイズと時間のしきい値を設定するには、FTD CLI を使用します。 新規/変更された FTD CLI コマンド： • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
FMC からセキュアネットワーク分析クラウドに侵入イベントとレトロスペクティブ マルウェア イベントを送信します。	**アップグレードの影響。** Cisco Security Analytics and Logging（SaaS）を使用してセキュリティイベントを Stealthwatch クラウドに送信するようにシステムを設定すると、FMC は次を送信します。 • 侵入イベント。これにより、リモートで保存された侵入イベントに影響フラグデータを含めることができます。以前は、これらのイベントは FTD によってクラウドに送信され、影響フラグは含まれていませんでした。 • レトロスペクティブ マルウェア イベント。これらは、デバイスによって引き続きクラウドに送信される「元の性質」ファイルとマルウェアイベントを補完します。 この機能が有効になっている場合、FMC はアップグレードの成功後にこの情報の送信を開始します。
侵入イベントの新しいデータストアによるパフォーマンスの向上。	パフォーマンスを向上させるために、バージョン 7.1 では、侵入イベントに新しいデータストアを使用します。アップグレードが完了し、FMC が再起動すると、履歴イベントが、最新のイベントが先頭になるようにバックグラウンドで移行されます。 この移行の一部として、侵入インシデント、侵入イベントクリップボード、および侵入イベントのカスタムテーブルは廃止されました。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。

機能	詳細
接続およびセキュリティ インテリジェンス イベントの NAT IP アドレスおよびポート情報。	NAT 変換の可視性を高めるために、次のフィールドが接続およびセキュリティ インテリジェンス イベントに追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port） イベントのテーブルビューでは、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [x] をクリックしてフィールド選択ツールを表示します。
パケットトレーサの機能拡張。	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。 • メインメニューから直接パケットトレーサにアクセス：**[デバイス（Devices）]**>**[トラブルシュート（Troubleshoot）]** > **[パケットトレーサ（Packet Tracer）]** • パケットトレースの保存。 • 複数デバイスでの並列パケットトレースの実行。 • デバイスを介した PCAP の再生。 • Snort 3 デバイスの場合、L2 から L7 までのトラフィック評価のフェーズ（アプリケーション識別、ファイル/マルウェア検出、侵入検出、セキュリティインテリジェンスなど）、および各フェーズにかかる時間に関して新しい詳細を提供する拡張出力の表示。 新規/変更された FTD CLI コマンド： • **packet-tracer input***source_interface***pcap***pcap_filename*
オブジェクト管理	
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。

機能	詳細
オブジェクトの展開プレビューの機能拡張。	地理位置情報、ファイルリスト、およびセキュリティ インテリジェンス オブジェクトへの展開の変更をプレビューできるようになりました。 更新された画面：**[展開（Deploy）]** > **[展開（Deployment）]**。[プレビュー（Preview）] 列で、デバイスの [プレビュー（Preview）] アイコンをクリックすると、ファイルリストオブジェクトへの変更が表示されます。
統合	
Cisco ACI Endpoint Update App バージョン 2.0 および修復モジュールのサポート。	Cisco ACI Endpoint Update App のバージョン 2.0 では、以前のバージョンに比べて次の点が改善されています。 • 最小更新間隔（アプリケーションが FMC を更新する頻度）が 10 秒になりました。以前は 30 秒でした。 • サイトプレフィックス（各 APIC テナントに関連付けられた FMC にネットワーク グループ オブジェクトを作成する文字列）が 10 文字に制限されました。以前は 5 文字でした。 この更新では、新しい Cisco ACI Endpoint 修復モジュールも利用できます。
ユーザビリティ、パフォーマンス、およびトラブルシューティング	

機能	詳細
ヘルスモニタリングの強化。	ヘルスモニタは次のように更新されました。 • ヘルスポリシーエディタは、類似するヘルスモジュールをグループ化するようになりました。モジュールグループ全体を有効または無効にできます。 • ヘルスポリシー除外エディタが更新され、使いやすくなりました。また、アラートからデバイスまたはヘルスモジュールを除外するときに、除外の期間を 15 分から永久まで指定できるようになりました。 • ヘルス モニタ アラート エディタが更新され、使いやすくなりました。 • ヘルスポリシーの展開インターフェイスが更新され、使いやすくなりました。 （注） 更新されたヘルスモニターを使用するには、**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。 新規/変更された画面： • **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。	展開ジョブをブックマークし、ジョブの展開に関する注意を編集して、レポートを生成できるようになりました。
グローバル検索の機能拡張。	グローバル検索に次の機能が追加されました。 • FMC ウォークスルーの全文を検索できます（how-tos）。 • 拡張コミュニティリスト名または設定値を検索できます。 • ドメインごとに検索を制限できます。

機能	詳細
新しいウォークスルー。	次のウォークスルーが追加されました。 • Snort 3 侵入ポリシーの作成。 • 個々のデバイス上での Snort 3 の有効化と無効化。 • Snort 3 ネットワーク分析ポリシーの作成。 • ネットワーク分析ポリシーのマッピングの表示。 • FTD のアップグレード。 • クラスタの作成および管理。 • FMC アクセスインターフェイスの管理からデータへの変更。 • FMC アクセスインターフェイスのデータから管理への変更。
Cisco Success Network に送信された Snort メモリ使用量テレメトリ。	有用性を向上させるために、Snort メモリおよびスワップ使用率（メモリ不足イベントを含む）に関するテレメトリを Cisco Success Network に送信するようになりました。 この情報は、Snort 2 と Snort 3 の両方に送信されます。Cisco Success Network の登録はいつでも変更できます。
Snort 3 は、フロー開始イベントとフロー終了イベントの統計情報をサポートします。	Snort 3 を使用する FTD の場合、**show snort statistics** コマンドの出力で、フロー開始イベントとフロー終了イベントに関する統計情報が報告されるようになりました。

機能	詳細
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。	

機能	詳細
	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。 （注）　これらの変更は、バージョン 7.2 で元に戻ります。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [AMP] > [AMP管理（AMP Management）] [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [インテリジェンス（Intelligence）] > [ソース（Sources）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [インテリジェンス（Intelligence）] > [要素（Elements）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [インテリジェンス（Intelligence）] > [設定（Settings）] [統合（Integration）] > [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。 [インテリジェンス（Intelligence）] > [インシデント（Incidents）] [統合（Integration）] > [その他の統合（Other Integrations）] は次に変更されました。 **システム**（⚙）> [統合（Integration）] [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。 **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）] [統合（Integration）] > [SecureX] は次に **システム**（⚙）> [SecureX]

機能	詳細
	変更されました。
FMC REST API	
FMC REST API。	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	
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。
サポート終了：NGIPS ソフトウェア（ASA FirePOWER/NGIPSv）。	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（一時的）：SecureX との統合、SecureX とのオーケストレーションの改善	**アップグレードの影響。新しい SecureX 統合が適用されている場合にバージョン 7.1.0 にアップグレードすることはできません。** この機能は、バージョン 7.0.2 以降および 7.2 以降に含まれています。バージョン 7.1 ではサポートされていません。バージョン 7.0.x で、新しい方法で SecureX との統合を有効にした場合は、この機能を無効にしない限り、バージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降にアップグレードすることをお勧めします。

機能	詳細
廃止：侵入インシデントと侵入イベントクリップボード。	**アップグレードの影響。データと構成は削除される場合があります。** 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。 廃止された画面/オプション： • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • 侵入イベントワークフローページおよびパケットビューでの [コピー（Copy）] および [すべてコピー（Copy All）] • レポートテンプレートにセクションを追加する場合（[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]）、データソースとして [クリップボード（Clipboard）] テーブルを選択できなくなりました。
廃止：侵入イベントのカスタムテーブル。	**アップグレードの影響。カスタムテーブルは削除される場合があります。** 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。 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。
廃止：FlexConfig を使用した ECMP ゾーン。	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** 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 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。
廃止：FlexConfig を使用したポリシーベースルーティング。	**アップグレードの影響。アップグレード後に、FlexConfig をやり直します。** FMC Web インターフェイスからポリシーベースルーティング（PBR）を設定できるようになりました。アップグレードの考慮事項については、FMC Web インターフェイスからポリシーベースルーティングを設定します。を参照してください

機能	詳細
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 7.0.6 の FMC 機能

表 14：

機能	詳細
Web 分析プロバイダーを更新しました。	**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。** 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。 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。 必要最低限の Threat Defense：任意 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 ～ 7.2.5、7.3.x、または 7.4.0 ではサポートされていません。永久サポートは、バージョン 7.4.1 で再開されています。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。

機能	詳細
メモリが少ない Snort 2 デバイス用の小規模 VDB。	**アップグレードの影響。 メモリが少ないデバイスのアプリケーション ID が影響を受けます。** VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA 5506-X シリーズ、ASA-5508-X、5512-X、5515-X、5516-X、5525-X、5545-X バージョンの制限：小規模 VDB をインストールできるかどうかは、管理対象デバイスではなく Management Center のバージョンによって決まります。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 Management Center をアップグレードする場合、導入環境内にメモリの少ないデバイスが 1 つでも含まれていると、VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。 参照：「Update the Vulnerability Database」
廃止された機能	
廃止：アンマネージドディスク使用率が高いアラート。	ディスク使用状況モジュールは、管理対象外のディスク使用率が高い場合にアラートを出さなくなりました。FMC をアップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをアップグレードする（アラートの送信を停止する）まで、これらのアラートが表示され続ける場合があります。 （注） バージョン 7.0 ～ 7.0.5、7.1.x、7.2.0 ～ 7.2.3、および 7.3.x は、引き続きこれらのアラートをサポートします。また、FMC がこれらのバージョンのいずれかを実行している場合、アラートが引き続き表示される場合があります。 残りのディスク使用量アラートについては、「Disk Usage and Drain of Events Health Monitor Alerts」を参照してください。

バージョン 7.0.5 の FMC 機能

表 15：

機能	詳細
ISA 3000 システム LED によるシャットダウンのサポート。	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。 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。

機能	詳細
CA バンドルの自動更新。	**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。** 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。 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** バージョンの制限：この機能は、バージョン 7.0.5 以降、7.1.0.3 以降、および 7.2.4 以降に含まれています。それ以前の 7.0、7.1、または 7.2 リリースではサポートされません。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。 参照：『Firepower Management Center Command Line Reference』および Cisco Secure Firewall Threat Defense コマンドリファレンス

バージョン 7.0.4 の FMC 機能

このリリースでは、安定性、ハードニング、パフォーマンスの機能強化が導入されています。

バージョン 7.0.3 の FMC 機能

表 *16 :* バージョン *7.0.3* の *FMC* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
クラウド提供型 Firewall Management Center への FTD のサポート。	7.2.0（分析のみサポート）	7.0.3	

機能	最小の Management Center	最小の Threat Defense	詳細
			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 Firewall Management Center による管理をサポートします。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。 次の場合は、クラウド提供型 Firewall Management Center でバージョン 7.0.3 FTD を使用する必要があります。 • 現在、お客様が導入した（「オンプレミス」）ハードウェアまたは仮想 FMC を使用している。 • クラウド提供型 Firewall Management Center に今すぐ移行する必要がある。 • バージョン 7.2 以降は クラウド提供型 Firewall Management Center による管理もサポートされているが、デバイスをこのバージョンにアップグレードする予定がない。 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。 **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。 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」）、オンプレミスの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。 **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。 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。 **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 Firewall Management Center にデバイスを移行します。 必要に応じて、オンプレミスの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

機能	最小の Management Center	最小の Threat Defense	詳細
			キュリティイベントを送信できます。 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クラシック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。 新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 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。

バージョン 7.0.2 の FMC 機能

表 *17*:

機能	詳細
ISA 3000 によるシャットダウンのサポート。	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。 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 7.2 で再開されています。
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。	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。 最低限の Threat Defense：7.0.2

機能	詳細
SecureX との統合、SecureX とのオーケストレーションの改善	**アップグレードの影響。 機能が有効な状態でバージョン 7.0.x を 7.1 にアップグレードすることはできません。** 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。 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。 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。 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。 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。 バージョンの制限：この機能は、バージョン 7.0.2 以降および 7.2 以降に含まれています。バージョン 7.1 ではサポートされていません。バージョン 7.0.x で、新しい方法で SecureX との統合を有効にした場合は、この機能を無効にしない限り、バージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降にアップグレードすることをお勧めします。 参照： Cisco Secure Firewall Management Center（7.0.2 および 7.2）および SecureX 統合ガイド

機能	詳細
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。	

機能	詳細
	以下の FMC メニューオプションが変更されました。 （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。 [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）] [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）] [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）] [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）] [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）] [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）] **システム**（⚙）> [統合（Integration）] は次に変更されました。 [統合（Integration）] > [その他の統合（Other Integrations）] **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）] は次に変更されました。 [統合（Integration）] > [セキュリティ分析とロギング（Security Analytics and Logging）] **システム**（⚙）> [SecureX] は次に [統合（Integration）] > [SecureX]

機能	詳細
	変更されました。

バージョン 7.0.1 の FMC 機能

表 *18* : バージョン *7.0.1* の *FMC* 機能

機能	詳細
Snort 3 の rate_filter インスペクタ。	Snort 3 rate_filter インスペクタが導入されました。 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。 新規/変更されたページ：カスタムネットワーク分析ポリシーの Snort 3 バージョンを編集して、インスペクタを設定します。 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。
ASA FirePOWER サービスを使用する ISA 3000 の新しいデフォルトパスワード。	新しいデバイスの場合、admin アカウントのデフォルトパスワードは Adm!n123 になりました。以前は、デフォルトの admin パスワードは Admin123 でした。 バージョン 7.0.1 以降にアップグレードまたは再イメージ化しても、パスワードは変更されません。ただし、すべてのユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。

バージョン 7.0.0 の FMC 機能

表 *19* : バージョン *7.0.0* の *FMC* 機能

機能	詳細
プラットフォーム	

機能	詳細
VMware vSphere/VMware ESXi 7.0 のサポート。	VMware vSphere/VMware ESXi 7.0 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。 バージョン 7.0 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。
新しい仮想環境。	次の環境に FMCv および FTDv が導入されました。 • Cisco HyperFlex • Nutanix エンタープライズクラウド • OpenStack FMCv の場合、これらすべての実装で FMCv2、v10、および v25 がサポートされます。 HyperFlex 用 FMCv は、FMCv10 および v25 による高可用性もサポートしています。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 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。

機能	詳細
FTDv パフォーマンス階層型のスマートライセンス。	**アップグレードの影響。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。** FTDv は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスをサポートするようになりました。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。 新しいデバイスを追加する前に、お使いのアカウントに必要なライセンスが含まれていることを確認してください。追加のライセンスを購入するには、シスコの担当者またはパートナーの担当者にお問い合わせください。 FTDv をバージョン 7.0 にアップグレードすると、デバイスが自動的に FTDv50 階層に割り当てられます。レガシー（非階層型）ライセンスを引き続き使用するには、アップグレード後に階層を [変数（Variable）] に変更します。 サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。 新規/変更されたページ： • **[デバイス（Device）] > [デバイス管理（Device Management）]** ページで FTDv デバイスを追加または編集するときに、パフォーマンス階層を指定できるようになりました。 • **システム**（⚙）**> [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。
高可用性/拡張性	
クラスタリング用の PAT ポートブロック割り当ての改善	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。 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** サポートされるプラットフォーム：Firepower 4100/9300

機能	詳細
FTD CLI **show cluster history** の改善。	新しいキーワードを指定すると、**show cluster history** コマンドの出力をカスタマイズできます。 新規/変更されたコマンド：**show cluster history** [**brief**] [**latest**] [**reverse**] [**time**] サポートされるプラットフォーム：Firepower 4100/9300
クラスタから永久に削除するための FTD CLI コマンド。	FTD CLI を使用して、ユニットをクラスタから完全に削除し、その設定をスタンドアロンデバイスに変換できるようになりました。 新規/変更されたコマンド： **cluster reset-interface-mode** サポートされるプラットフォーム：Firepower 4100/9300
NAT	
優先順位付けされたシステム定義の NAT ルール。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。 セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。 サポートされるプラットフォーム：FTD
仮想ルーティング	
ISA 3000 の仮想ルータサポート。	ISA 3000 デバイスには最大 10 台の仮想ルータを設定できるようになりました。 サポートされるプラットフォーム：ISA 3000
サイト間 VPN	
ルートベースのサイト間 VPN 向けバックアップ用仮想トンネルインターフェイス（VTI）。	仮想トンネルインターフェイスを使用するサイト間 VPN を設定する場合、トンネルのバックアップ VTI を選択できます。 バックアップ VTI を指定すると復元力が得られるため、プライマリ接続がダウンした場合でもバックアップ接続は継続して機能します。たとえば、プライマリ VTI をあるサービスプロバイダ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。 新規/変更されたページ：ポイントツーポイント接続の VPN タイプとして [ルートベース（Route-Based）] を選択した場合に、サイト間 VPN ウィザードにバックアップ VTI を追加する機能が追加されました。 サポートされるプラットフォーム：FTD
Remote Access VPN	

機能	詳細
ロード バランシング。	RA VPN ロードバランシングがサポートされるようになりました。システムは、セッション数によってグループ化されたデバイス間でセッションを分散します。トラフィック量やその他の要因は考慮されません。 新規/変更された画面：RA VPN ポリシーの [詳細設定（Advanced Settings）] にロード バランシング オプションが追加されました。 サポートされるプラットフォーム：FTD
ローカル認証。	RA VPN ユーザーのローカル認証がサポートされるようになりました。これは、プライマリまたはセカンダリ認証方式として、または設定されたリモートサーバーに到達できない場合のフォールバックとして使用できます。 **1.** ローカルレルムを作成します。 ローカルユーザー名とパスワードは、ローカルレルムに保存されます。レルムを作成し（**システム**（⚙）>**[統合（Integration）]**>**[レルム（Realms）]**）、新しい[ローカル（LOCAL）] レルムタイプを選択すると、1 つ以上のローカルユーザーを追加するように求められます。 **2.** ローカル認証を使用するように RA VPN を設定します。 RA VPN ポリシーを作成または編集し（**[デバイス（Devices）] > [VPN] > [リモートアクセス（Remote Access）]**）、そのポリシー内に接続プロファイルを作成して、その接続プロファイルでプライマリ、セカンダリ、またはフォールバック認証サーバーとして **[ローカル（LOCAL）]** を指定します。 **3.** 作成したローカルレルムを RA VPN ポリシーに関連付けます。 RA VPN ポリシーエディタで、新しい **[ローカルレルム（Local Realm）]** 設定を使用します。ローカル認証を使用する RA VPN ポリシーのすべての接続プロファイルは、ここで指定したローカルレルムを使用します。 サポートされるプラットフォーム：FTD

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

機能	詳細
FTD 用 Snort 3。	

機能	詳細
	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。 Snort 3 を使用する利点は次のとおりですが、これに限定されません。 • パフォーマンスの向上。 • SMBv2 インスペクションの改善。 • 新しいスクリプト検出機能。 • HTTP/2 インスペクション。 • カスタムルールグループ。 • カスタム侵入ルールを記述しやすくする構文。 • 侵入イベント内の「would have dropped」インライン結果の理由。 • VDB、SSL ポリシー、カスタム アプリケーション ディテクタ、キャプティブポータル ID ソース、および TLS サーバ ID 検出へ変更を展開するときに Snort が再起動しない。 • Cisco Success Network に送信される Snort 3 固有のテレメトリデータ、およびトラブルシューティングログの改善による、有用性の向上。 Snort 3 侵入ルールの更新は、SRU ではなく LSP（Lightweight Security Package）と呼ばれます。Snort 2 には引き続き SRU が使用されます。シスコからのダウンロードには、最新の LSP と SRU の両方が含まれており、設定に適したルールセットが自動的に使用されます。 FMC は、Snort 2 と Snort 3 の両方のデバイスでの展開を管理でき、各デバイスに正しいポリシーを適用します。ただし、Snort 2 とは異なり、FMC のみをアップグレードしてから展開することで、デバイス上の Snort 3 を更新することはできません。Snort 3 では、新しい機能と解決済みのバグにより、FMC 上のソフトウェアとその管理対象デバイスをアップグレードする必要があります。各ソフトウェアバージョンに含まれている Snort の詳細については、Cisco Firepower Compatibility Guide のバンドルされたコンポーネントのセクションを参照してください。 **重要** Snort 3 に切り替える前に、Firepower Management Center Snort 3 Configuration Guide を読んで理解することを強く推奨します。機能の制限と移行手順には特に注意してください。Snort 3 へのアップグレードは影響を最小限に抑えるように設計されていますが、機能は正確にマッピングされません。慎重に計画して準備することで、トラフィックが期待どおりに処理されるようにできます。 Snort 3 の Webサイト（https://snort.org/snort3）にもアクセスできます。https://snort.org/snort3

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

機能	詳細
Active Directory ドメインのクロスドメイン信頼。	Microsoft Active Directory フォレスト（相互に信頼する AD ドメインのグループ）のユーザーを使用してユーザー アイデンティティ ルールを設定できるようになりました。 新規/変更されたページ： • レルムとディレクトリを同時に設定するようになりました。 • 新しい [同期結果（Sync Results）] ページ（**システム**（⚙）>**[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。 サポート対象プラットフォーム：FMC
DNS フィルタリング。	バージョン 6.7 でベータ機能として導入された DNS フィルタリングは、完全にサポートされるようになり、新しいアクセス コントロール ポリシーではデフォルトで有効になっています。 サポートされるプラットフォーム：すべて
イベントロギングおよび分析	

機能	詳細
Secure Network Analytics オンプレミス展開でのイベント保存プロセスの改善。	新しい シスコのセキュリティ分析とロギング（オンプレミス） アプリと新しい FMC ウィザードにより、オンプレミス Secure Network Analytics ソリューションのリモートデータストレージをより簡単に設定できます。 **1.** ハードウェアまたは仮想 Stealthwatch アプライアンスを展開します。 Stealthwatch Management Console を単独で使用することも、Stealthwatch Management Console、フローコレクタ、およびデータストアを設定することもできます。 **2.** Stealthwatch Management Console に新しい Cisco Security Analytics and Logging（オンプレミス）アプリをインストールして、Stealthwatch をリモートデータストアとして設定することができます。 **3.** FMC で、**システム**（⚙） > **[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。 syslog を使用して Firepower イベントを Stealthwatch に送信するアップグレードされた展開では、ウィザードを使用する前にこれらの設定を無効にします。そうしないと、二重にイベントが発生します。Stealthwatch への syslog 接続を削除するには、FTDプラットフォーム設定を使用します（**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**）。 syslog へのイベント送信を無効にするには、アクセス制御ルールを編集します。 Stealthwatch のハードウェア要件およびソフトウェア要件を含む詳細については、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。 サポート対象プラットフォーム：FMC

機能	詳細
Secure Network Analytics オンプレミス展開でリモートに保存されたイベントを操作する。	FMC を使用して、Secure Network Analytics オンプレミス展開でリモートに保存された接続イベントを操作できるようになりました。 接続イベントページ（**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]**）と統合イベントビューア（**[分析（Analysis）] > [統合イベント（Unified Events）]**）の新しい**データソース**オプションを使用して、処理する接続イベントを選択できます。デフォルトでは、時間範囲に何も存在しない場合、ローカルに保存された接続イベントが表示されます。その場合、システムはリモートに保存されたイベントを表示します。 また、リモートで保存された接続イベントに基づいてレポートを生成できるように、レポートテンプレートにデータソースオプションが追加されました（**[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]**）。 （注） この機能は、接続イベントでのみサポートされます。クロス起動は、リモートで保存されたセキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベントを調べる唯一の方法です。統合イベントビューアでも、システムはこれらのタイプのローカルに保存されたイベントのみを表示します。 ただし、すべてのセキュリティ インテリジェンス イベントに同一の接続イベントが存在することに注意してください。これらは「IP ブロック」や「DNS ブロック」などの理由を持つイベントです。これらの重複イベントは、接続イベントページまたは統合イベントビューアで処理できますが、専用のセキュリティ インテリジェンス イベント ページでは処理できません。 サポート対象プラットフォーム：FMC
すべての接続イベントを Secure Network Analytics クラウドに保存する。	Cisco Security Analytics and Logging（SaaS）を使用して、すべての接続イベントを Stealthwatch クラウドに保存できるようになりました。以前は、セキュリティ インテリジェンス、侵入、ファイル、およびマルウェアのイベント、およびそれらに関連する接続イベントに限定されていました。 クラウドに送信するイベントを変更するには、**システム**（⚙）> [統合（Integration）] を選択します。**[クラウドサービス（Cloud Services）]** タブで、**[シスコクラウドイベントの設定（Cisco Cloud Event Configuration）]** を編集します。優先順位の高い接続イベントをクラウドに送信する古いオプションは、**[すべて（All）]**、**[なし（None）]**、または **[セキュリティイベント（Security Events）]** の選択肢に置き換えられました。 （注） これらの設定は、SecureX に送信するイベントも制御します。ただし、すべての接続イベントをクラウドに送信するように選択した場合でも、SecureX はセキュリティ（優先度の高い）接続イベントのみを消費します。また、**[分析（Analysis）] > [SecureX]** で SecureX 接続自体を設定することにも注意してください。 サポート対象プラットフォーム：FMC

機能	詳細
統合イベントビューア。	統合イベントビューア（**[分析（Analysis）]**>**[統合イベント（Unified Events）]**）では、1 つのテーブルで接続、セキュリティインテリジェンス、侵入、ファイル、およびマルウェアの各イベントが表示されます。これは、異なるタイプのイベント間の関係を調べるのに役立ちます。 単一の検索フィールドを使用すると、複数の条件に基づいてビューを動的にフィルタリングできます。また、**[本番稼働（Go Live）]** オプションでは、管理対象デバイスから受信したイベントがリアルタイムで表示されます。 サポート対象プラットフォーム：FMC
SecureX のリボン。	FMC 上の SecureX のリボンは SecureX にピボットされ、シスコのセキュリティ製品全体の脅威の状況を即座に確認できます。 SecureX に接続してリボンを有効にするには、**システム**（⚙）>**[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。 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。 サポート対象プラットフォーム：FMC
ローカルストレージをオフにすると、すべての接続イベントのレート制限が免除されます。	イベントレート制限は、FMC に送信されるすべてのイベントに適用されます。ただし、セキュリティイベント（セキュリティインテリジェンス、侵入、ファイル、マルウェアのイベント、およびそれらに関連する接続イベント）は例外です。 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した。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。 （注） **[最大接続イベント数（Maximum Connection Events）]** は、0 に設定してオフにすること以外では、接続イベントのレート制限を制御しません。このフィールドに 0 以外の数値を指定すると、優先順位の低い接続イベントがすべてレート制限されます。 ローカルイベントストレージを無効にしても、リモートイベントストレージには影響せず、接続の概要や相関にも影響しないことに注意してください。システムは、引き続き、トラフィックプロファイル、相関ポリシー、ダッシュボード表示などの機能に接続イベント情報を使用します。 サポート対象プラットフォーム：FMC

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

機能	詳細
FTD の [アップグレード（Upgrade）] ウィザード。	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。 開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [アクションの選択（Select Action）]）で新しい [Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] アクションを使用します。 続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。 ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。 （注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き **システム**（⚙） > **[更新（Updates）]**を使用する必要があります。また、[システム更新（System Updates）] ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。 （注） バージョン 7.0 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。 時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。 サポートされるプラットフォーム：FTD

機能	詳細
多くの FTD デバイスを一度にアップグレードします。	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古い FTD リリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズ デバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。 サポートされるプラットフォーム：FTD
管理とトラブルシューティング	
SD カードを使用した ISA 3000 でのゼロタッチ復元。	ローカルバックアップを実行すると、バックアップファイルが SD カードにコピーされます（カードがある場合）。交換用デバイスの設定を復元するには、新しいデバイスに SD カードを取り付け、デバイスの起動中に [リセット（Reset）] ボタンを 3 ー 15 秒間押します。 サポートされるプラットフォーム：ISA 3000
RA およびサイト間 VPN ポリシーを選択的に展開する。	バージョン 6.6 で導入された選択的ポリシーの展開では、リモートアクセスとサイト間 VPN ポリシーがサポートされるようになりました。 新規/変更されたページ：**[展開（Deploy）] > [展開（Deployment）]** ページに VPN ポリシーオプションが追加されました。 サポートされるプラットフォーム：FTD

機能	詳細
新しいヘルス モジュール。	次の正常性モジュールが追加されました。 • AMP 接続ステータス • AMP Threat Grid のステータス • ASP ドロップ • 高度な Snort 統計情報 • シャーシステータス FTD • イベント ストリーム ステータス • FMC アクセス設定の変更 • FMC HA ステータス（古い HA ステータスの交換） • FTD HA ステータス • ファイルシステムの整合性チェック • フロー オフロード • ヒット カウント（Hit Count） • MySQL ステータス • NTP ステータス FTD • Rabbit MQ ステータス • ルーティング統計情報 • SSE 接続ステータス • Sybase ステータス • 未解決グループモニター • VPN 統計情報 • xTLS カウンタ さらに、バージョン 6.6.3 で [アプライアンス設定のリソース使用率（Appliance Configuration Resource Utilization）] モジュールとして導入された [構成メモリ割り当て（Configuration Memory Allocation）] モジュールは、バージョン 6.7 では完全にはサポートされていませんでしたが、完全にサポートされます。 サポート対象プラットフォーム：FMC
セキュリティと強化	

機能	詳細
AWS 導入用の新しいデフォルトパスワード。	初期展開時にユーザーデータ（**[高度な詳細（Advanced Details）] > [ユーザーデータ（User Data）]**）を使用してデフォルトパスワードを定義していなければ、admin アカウントのデフォルトパスワードは AWS のインスタンス ID です。 以前は、デフォルトの admin パスワードは Admin123 でした。 サポートされているプラットフォーム：FMCv for AWS、FTDv for AWS
証明書の登録用の EST。	証明書の登録用の Enrollment over Secure Transport のサポートが提供されました。 新規/変更されたページ：**[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [CA情報（CA Information）]** タブ設定時の新しい登録オプション。 サポート対象プラットフォーム：FMC
EdDSA 証明書タイプのサポート。	新しい証明書キータイプ：EdDSA（キーサイズ 256）が追加されました。 新規/変更されたページ：**[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）] > [キー（Key）]** タブの設定時の新しい証明書キーオプション。 サポート対象プラットフォーム：FMC
NTP サーバーの AES-128 CMAC 認証。	AES-128 CMAC キーを使用して、FMC と NTP サーバー間の接続を保護できるようになりました。 新規/変更されたページ：**システム**（⚙）**>[構成（Configuration）]>[時刻の同期（Time Synchronization）]**。 サポートされるプラットフォーム：FMC
SNMPv3 ユーザーは、SHA-224 または SHA-384 認証アルゴリズムを使用して認証できます。	SNMPv3 ユーザーは、SHA-224 または SHA-384 アルゴリズムを使用して認証できるようになりました。 新規/変更されたページ：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SNMP] > [ユーザー（Users）] > [認証アルゴリズムタイプ（Auth Algorithm Type）]** サポートされるプラットフォーム：FTD
ユーザビリティとパフォーマンス	
ポリシーとオブジェクトのグローバル検索。	特定のポリシーを名前で検索し、特定のオブジェクトを名前と設定値で検索できるようになりました。この機能は、クラシックテーマでは使用できません。 新規/変更されたページ：[展開（Deploy）] メニューの左側にある [FMC] メニューバーに [検索（Search）] アイコンとフィールドの機能が追加されました。 サポート対象プラットフォーム：FMC

機能	詳細
Intel QuickAssist Technology（QAT）を使用したFTDvでのハードウェア暗号化アクセラレーション。	VMwareのFTDvおよびKVMのFTDvでハードウェア暗号化アクセラレーション（CBC暗号のみ）がサポートされるようになりました。この機能を使用するには、ホスティング プラットフォームにIntel QAT 8970 PCI アダプタ/バージョン1.7以降のドライバが必要です。リブートすると、ハードウェア暗号化アクセラレーションが自動的に有効になります。 サポートされるプラットフォーム：VMwareのFTDv、KVMのFTDv
多対1および1対多接続のCPU使用率とパフォーマンスが向上しました。	ダイナミックNAT / PATおよびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサやWebサーバーなど）に対して確立する場合や、1つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスとCPU使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、 **show local-host** サポートされるプラットフォーム：FTD
使用方法の場所が変更されました。	**[ヘルプ（Help）]** > **[使用方法（How-Tos）]** でウォークスルーが呼び出されるようになりました。以前は、ブラウザウィンドウの下部にある [使用方法（How-Tos）] をクリックしていました。
FMC REST API	
FMC REST API。	Management Center REST APIの変更については、『Firepower Management Center REST API バージョン7.0 クイックスタートガイド』を参照してください。
廃止された機能	
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：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。	**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。** 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。 アップグレードする前に、オブジェクトマネージャを使用し、より強力なオプションを使用してPKI証明書の登録を更新します（[オブジェクト（Objects）] > [PKI] > [証明書の登録（Cert Enrollment）]）。更新しない場合、アップグレードしても現在の設定は保持されますが、デバイスを介したVPN接続は失敗します。 弱いオプションを使用して古いFTDデバイス（バージョン6.4 ー 6.7.x）のみを管理し続けるには、[デバイス（Devices）] > [証明書（Certificates）] ページで各デバイスの新しい [弱暗号化の有効化（Enable Weak-Crypto）] オプションを選択します。

機能	詳細
廃止：SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化。	**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。** 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。 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。 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。
廃止：AMP クラウドとのポート 32137 通信。	**FMC がアップグレードされないようにします。** 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。 アップグレードする前に、**システム**（⚙）> **[統合（Integration）]** > **[クラウドサービス（Cloud Services）]**ページの [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。
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 *FMC* HA 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。

機能	詳細
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.7 の FMC 機能

表 *20 :* バージョン *6.7* の *FMC* 機能

機能	詳細
プラットフォーム	
OCI および GCP の FMCv および FTDv。	次の環境に FMCv および FTDv が導入されました。 • Oracle Cloud Infrastrucure（OCI） • Google Cloud Platform（GCP）

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

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

機能	詳細
Firepower 4100/9300 の FTD 動作リンク状態と物理リンク状態の同期。	Firepower 4100/9300 シャーシでは、FTD 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。 現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。FTD アプリケーション インターフェイスの管理状態は考慮されません。FTD からの同期がない場合は、たとえば、FTD アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、FTD のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、 FTD が処理できるようになる前に外部ルータが FTD へのトラフィックの送信を開始することがあるためです。 この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、または Radware vDP デコレータを使用する FTD ではサポートされません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] ページ：[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）] 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされるプラットフォーム：Firepower 4100/9300
Firepower 1100/2100 シリーズの SFP インターフェイスで、自動ネゴシエーションの無効化がサポートされるようになりました。	**アップグレードの影響。** フロー制御とリンク ステータス ネゴシエーションを無効化するように Firepower 1100/2100 シリーズ SFP インターフェイスを設定できるようになりました。 以前は、これらのデバイスで SFP インターフェイス速度（1000 または 10000 Mbps）を設定すると、フロー制御とリンク ステータス ネゴシエーションが自動的に有効になり、無効にはできませんでした。 [ネゴシエーションなし（No Negotiate）] を選択して、フロー制御とリンク ステータス ネゴシエーションを無効化できるようになりました。これにより、1 GB SFP インターフェイスまたは 10 GB SFP+ インターフェイスを設定しているかに関係なく、速度は 1000 Mbps に設定されます。10000 Mbps でネゴシエーションを無効化することはできません。 新規/変更されたページ：[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（edit interface）] > [ハードウェア構成（Hardware Configuration）] > [速度（Speed）] サポートされるプラットフォーム：Firepower 1100/2100 シリーズ
Firepower Threat Defense：クラスタリング	

機能	詳細
FMC の新しいクラスタ管理機能。	FMC を使用して、以前は CLI を使用する必要のあった次のクラスタ管理タスクを実行できるようになりました。 • クラスタユニットを有効または無効にします。 • [Device Management] ページからクラスタのステータスを表示します（ユニットごとの履歴とサマリーを含む）。 • ロールをコントロールユニットに変更します。 新規/変更されたページ： • [Devices] > [Device Management] > [More] メニュー • [Devices] > [Device Management] > [Cluster] > [General] エリア > [Cluster Live Status] リンク > [Cluster Status] サポートされるプラットフォーム：Firepower 4100/9300
クラスタ導入の高速化。	クラスタの展開がより迅速に完了するようになりました。また、ほとんどの導入の失敗も、より迅速に失敗します。 サポートされるプラットフォーム：Firepower 4100/9300

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

機能	詳細
RA VPN の AnyConnect モジュールサポート。	FTD RA VPN で AnyConnect モジュールがサポートされるようになりました。 RA VPN グループポリシーの一部として、ユーザーが Cisco AnyConnect VPN クライアントをダウンロードするときに、さまざまなオプションモジュールをダウンロードしてインストールするように設定できるようになりました。これらのモジュールは、Web セキュリティ、マルウェア保護、オフネットワークローミング保護などのサービスを提供できます。 各モジュールを、AnyConnect プロファイルエディタで作成され、AnyConnect ファイルオブジェクトとして FMC にアップロードされたカスタム設定を含むプロファイルに関連付ける必要があります。 新規/変更されたページ： • モジュールプロファイルのアップロード：新しい [File Type] オプションが [Objects] > [Object Management] > [VPN] > [AnyConnect File] > [Add AnyConnect File] に追加されました • モジュールの設定：[Client Modules] オプションが [Objects] > [Object Management] > [VPN] > [Group Policy] > [add or edit a Group Policy object] > [AnyConnect] 設定に追加されました サポートされるプラットフォーム：FTD
RA VPN の AnyConnect 管理 VPN トンネル。	FTD RA VPN は、エンドユーザーが VPN 接続を確立したときだけでなく、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルをサポートするようになりました。 この機能は、オフィスネットワークに VPN を介してユーザーが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで管理者がパッチ管理を行うのに役立ちます。社内ネットワークの接続を必要とするエンドポイント オペレーティング システム ログイン スクリプトに対するメリットもあります。 サポートされるプラットフォーム：FTD
RA VPN のシングルサインオン。	FTD RA VPN は、 SAML 2.0 準拠のアイデンティティ プロバイダー（IdP）で設定されたリモートアクセス VPN ユーザーのシングルサインオン（SSO）をサポートするようになりました。 新規/変更されたページ： • SSO サーバーへの接続：[Objects] > [Object Management] > [AAA Server] > [Single Sign-on Server] • RA VPN の一部として SSO を設定します。RA VPN 接続プロファイルを設定する際に、認証方式（AAA 設定）として [SAML] を追加しました。 サポートされるプラットフォーム：FTD

機能	詳細
RA VPN の LDAP 許可。	FTD RA VPN は、LDAP 属性マップを使用した LDAP 認証をサポートするようになりました。 LDAP 属性マップにより、Active Directory（AD）または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。その後、リモートアクセス VPN 接続の確立中に AD または LDAP サーバーが FTD デバイスに認証を返すと、FTD デバイスは、その情報を使用して、AnyConnect クライアントが接続を完了する方法を調整できます。 サポートされるプラットフォーム：FTD
仮想トンネルインターフェイス（VTI）とルートベースのサイト間 VPN。	FTD サイト間 VPN は、仮想トンネルインターフェイス（VTI）と呼ばれる論理インターフェイスをサポートするようになりました。 ポリシーベース VPN の代替策として、仮想トンネルインターフェイスが設定されたピア間に VPN トンネルを作成することができます。これは、各トンネルの終端に IPsec プロファイルが付加されたルートベースの VPN をサポートします。これは、動的または静的なルートの使用が可能です。VTI を使用することにより、静的暗号マップのアクセス リストを設定してインターフェイスにマッピングすることが不要になります。トラフィックは、スタティックルートまたは BGP を使用して暗号化されます。ルーテッド セキュリティ ゾーンを作成し、そこに VTI インターフェイスを追加し、VTI トンネルを介して復号化されたトラフィック制御のアクセス制御ルールを定義できます。 VTI ベースの VPN は、次の間で作成できます。 • 2 つの FTD デバイス • FTD デバイスとパブリッククラウド • FTD デバイスとサービスプロバイダーの冗長性を備えた別の FTD デバイス 新規/変更されたページ： • **[Devices] > [Device Management] > [Interfaces] > [Add Interfaces] > [Virtual Tunnel Interface]** • **[Devices] > [VPN] > [Site To Site] > [Add VPN] > [Firepower Threat Defense Device] > [Route Based (VTI)]** サポートされるプラットフォーム：FTD

機能	詳細
サイト間 VPN に対するダイナミック RRI サポート。	FTD サイト間 VPN は、サイト間 VPN 展開で IKEv2 ベースのスタティック暗号マップでサポートされるダイナミック リバース ルート インジェクション（RRI）をサポートするようになりました。これにより、スタティックルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティングプロセスに自動的に挿入されます。 新規/変更されたページ：サイト間 VPN トポロジにエンドポイントを追加するときの [ダイナミック リバース ルート インジェクションの有効化（Enable Dynamic Reverse Route Injection）] 詳細オプションが追加されました。 サポートされるプラットフォーム：FTD
手動証明書登録の拡張機能。	署名済み CA 証明書とアイデンティティ証明書を CA 機関から互いに独立して取得できるようになりました。 証明書署名要求（CSR）を作成し、アイデンティティ証明書を取得するための登録パラメータを保存する PKI 証明書登録オブジェクトに次の変更を行いました。 • PKI 証明書登録オブジェクトの手動登録設定に [CA Only] オプションが追加されました。このオプションを有効にすると、CA 機関から署名済み CA 証明書のみを受け取り、アイデンティティ証明書は受け取りません。 • PKI 証明書登録オブジェクトの手動登録設定で、[CA Certificate] フィールドを空白のままにできるようになりました。これを行うと、署名済み CA 証明書ではなく、CA 機関からアイデンティティ証明書のみを受け取ります。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [PKI] > [証明書の登録（Cert Enrollment）] > [証明書の登録の追加（Add Cert Enrollment）] > [CA 情報（CA Information）] > [登録タイプ（Enrollment Type）] > [手動（Manual）] サポートされるプラットフォーム：FTD
FTD証明書管理の拡張機能。	FTD 証明書管理に次の機能拡張が行われました。 • 証明書の内容を表示するときに、認証局（CA）のチェーンを表示できるようになりました。 • 証明書をエクスポートできるようになりました。 新規/変更されたページ： • [Devices] > [Certificates] > [Status] 列 > [View] アイコン（虫めがね） • [Devices] > [Certificates] > [Export] アイコン サポートされるプラットフォーム：FTD
アクセス制御：URL フィルタリング、アプリケーション制御、およびセキュリティ インテリジェンス	

機能	詳細
TLS 1.3（TLS サーバーアイデンティティ検出）で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御。	サーバー証明書からの情報を使用して、TLS 1.3 で暗号化されたトラフィックの URL フィルタリングとアプリケーション制御を実行できるようになりました。この機能が動作するためにトラフィックを復号化する必要はありません。 （注） 暗号化トラフィックで URL フィルタリングとアプリケーション制御を実行する場合は、この機能を有効にすることを推奨します。ただし、特に低メモリモデルでは、デバイスのパフォーマンスに影響を与える可能性があります。 新規/変更されたページ：アクセス コントロール ポリシーの [詳細（Advanced）] タブに [TLS サーバーアイデンティティ検出（TLS Server Identity Discovery）] の警告とオプションが追加されました。 新規/変更された FTD CLI コマンド：**show conn detail** コマンドの出力に B フラグが追加されました。TLS 1.3 暗号化接続では、このフラグは、アプリケーションおよび URL の検出にサーバー証明書を使用したことを示します。 サポートされるプラットフォーム：FTD
レピュテーションが不明な Web サイトへのトラフィックに対する URL フィルタリング。	レピュテーションが不明な Web サイトに対して URL フィルタリングを実行できるようになりました。 新規/変更されたページ：アクセス制御、QoS、および SSL ルールエディタに [不明なレピュテーションに適用（Apply to unknown reputation）] チェックボックスが追加されました。 サポートされるプラットフォーム：FMC
DNS フィルタリングにより URL フィルタリングを強化します。	**ベータ版。** *DNS* フィルタリングは、暗号化されたトラフィックを含め（ただしトラフィックを復号化せずに）トランザクションの早い段階で要求されたドメインのカテゴリとレピュテーションを決定することで、URL フィルタリングを強化します。アクセス コントロール ポリシーごとに DNS フィルタリングを有効にし、そのポリシーのすべてのカテゴリ/レピュテーション URL ルールに適用します。 （注） DNS フィルタリングはベータ機能であり、期待どおりに動作しない可能性があります。実稼働環境では使用しないでください。 新規/変更されたページ：[全般設定（General Settings）] の下のアクセス コントロール ポリシーの [詳細（Advanced）] タブに [DNS トラフィックへのレピュテーション適用の有効化（Enable reputation enforcement on DNS traffic）] オプションが追加されました。 サポートされるプラットフォーム：FMC

機能	詳細
セキュリティ インテリジェンス フィードの更新頻度の短縮。	FMC は、5 分または 15 分ごとにセキュリティ インテリジェンス データを更新できるようになりました。以前は、最短更新頻度は 30 分でした。 カスタムフィードでこれらの短い頻度のいずれかを設定する場合は、md5 チェックサムを使用してフィードにダウンロードする更新があるかどうかを判断するようにシステムを設定する必要もあります。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [セキュリティ インテリジェンス（Security Intelligence）] > [ネットワーク リストとフィード（Network Lists and Feeds）] > [フィードの編集（edit feed）] > [更新頻度（Update Frequency）] に新しいオプションが追加されました。 サポートされるプラットフォーム：FMC
アクセス制御：ユーザー制御	
ISE/ISE-PIC を使用した pxGrid 2.0。	**アップグレードの影響。** FMC を ISE/ISE-PIC アイデンティティ ソースに接続する場合は、pxGrid 2.0 を使用します。まだ pxGrid 1.0 を使用している場合は、ここで切り替えてください。このバージョンは廃止されました。 pxGrid 2.0 で使用するために、バージョン 6.7.0 では Cisco ISE 適応型ネットワーク制御（ANC）修復が導入され、相関ポリシー違反に関連する ISE 設定 ANC ポリシーが適用またはクリアされます。 pxGrid 1.0 で Cisco ISE エンドポイント保護サービス（EPS）修復を使用した場合は、pxGrid 2.0 で ANC 修復を設定して使用します。「誤った」pxGrid を使用している場合、ISE 修復は起動しません。ISE Connection Status Monitor ヘルスモジュールは、不一致を警告します。 サポートされているすべての Firepower バージョン（統合製品を含む）の詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。 新規/変更されたページ： • [Policies] > [Actions] > [Modules] > [Installed Remediation Modules] リスト • [Policies] > [Actions] > [Instances] > [Select a module type] ドロップダウンリスト サポートされるプラットフォーム：FMC

機能	詳細
レルムシーケンス。	レルムを順序付けられたレルムシーケンスにグループ化できるようになりました。 単一のレルムを追加するのと同じ方法で、アイデンティティルールにレルムシーケンスを追加します。アイデンティティルールをネットワークトラフィックに適用すると、システムは指定された順序で Active Directory ドメインを検索します。LDAP レルムのレルムシーケンスは作成できません。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [レルムシーケンス（Realm Sequences）] サポートされるプラットフォーム：FMC
ISE サブネットフィルタリング。	特にメモリの少ないデバイスでは、CLI を使用して、ISE からのユーザーと IP およびセキュリティグループタグ（SGT）と IP のマッピングの受信から、サブネットを除外できるようになりました。 Snort Identity Memory Usage ヘルスモジュールは、メモリ使用率が特定のレベル（デフォルトでは 80%）を超えるとアラートを出します。 新しいデバイス CLI コマンド： **configure identity-subnet-filter** {**add** | **remove**} サポートされるプラットフォーム：FMC 管理対象デバイス
アクセス制御：侵入およびマルウェア防御	
動的分析のためのファイルの事前分類の改善。	**アップグレードの影響。** システムは、静的分析の結果（動的要素のないファイルなど）に基づいて、疑わしいマルウェアファイルを動的分析用に送信しないことを決定できるようになりました。 アップグレード後、[Captured Files] テーブルでは、これらのファイルの動的分析ステータスが [Rejected for Analysis] になります。 サポートされるプラットフォーム：FMC

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

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

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

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

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

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

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

機能	詳細
アップグレードがスケジュールされたタスクを延期する。	**アップグレードの影響。** FMCアップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン6.4.0.10以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。 サポートされるプラットフォーム：FMC
アップグレードでディスク容量を節約するために PCAP ファイルが削除される。	**アップグレードの影響。** Firepower アプライアンスをアップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。 サポートされているプラットフォーム：すべて
展開とポリシー管理	
設定のロール バック。	**ベータ版。** FTDデバイスの設定を「ロールバック」して、以前に展開した設定に置き換えることができるようになりました。 （注） ロールバックはベータ機能であり、すべての展開タイプとシナリオでサポートされているわけではありません。これは中断を伴う操作でもあります。FMC コンフィギュレーション ガイドの「ポリシー管理」の章に記載されているガイドラインと制限事項を必ず読んで理解してください。 新規/変更されたページ：[Deploy] > [Deployment History] > [Rollback] 列とアイコン。 サポートされるプラットフォーム：FTD
侵入およびファイルポリシーを（アクセス コントロール ポリシーとは無関係に）展開する。	依存する変更がない限り、アクセス コントロール ポリシーとは無関係に侵入ポリシーとファイルポリシーを選択して展開できるようになりました。 新規/変更されたページ：[展開（Deploy）] > [展開（Deployment）] サポートされるプラットフォーム：FMC

機能	詳細
アクセス制御ルールのコメントの検索。	アクセス制御ルールのコメント内で検索できるようになりました。 新規/変更されたページ：アクセス コントロール ポリシー エディタで、[検索ルール（Search Rules）] ドロップダウンダイアログに [コメント（Comments）] フィールドが追加されました。 サポートされるプラットフォーム：FMC
FTD NAT ルールの検索とフィルタリング。	FTD NAT ポリシーでルールを検索して、IP アドレス、ポート、オブジェクト名などに基づいてルールを検索できるようになりました。検索結果には部分一致が含まれます。条件で検索すると、ルールテーブルがフィルタリングされ、一致するルールのみが表示されます。 新規/変更されたページ：FTD NAT ポリシーを編集するときに、ルールテーブルの上に検索フィールドが追加されました。 サポートされるプラットフォーム：FTD
アクセス コントロール ポリシーとプレフィルタポリシー間のルールのコピーおよび移動。	あるアクセス コントロール ポリシーから別のアクセス コントロール ポリシーにアクセス制御ルールをコピーできます。アクセス コントロール ポリシーとそれに関連付けられたプレフィルタポリシーの間でルールを移動することもできます。 新規/変更されたページ：アクセス コントロール ポリシー エディタおよびプレフィルタポリシー エディタで、各ルールの右クリックメニューに [Copy] および [Move] オプションが追加されました。 サポートされるプラットフォーム：FMC
オブジェクト一括インポート。	カンマ区切り値（CSV）ファイルを使用して、ネットワーク、ポート、URL、VLAN タグ、および識別名オブジェクトを FMC に一括インポートできるようになりました。 制限事項および特定のフォーマット手順については、FMC コンフィギュレーション ガイドの「再利用可能なオブジェクト」の章を参照してください。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [オブジェクトタイプの選択（choose an object type）] > [オブジェクトタイプの追加（Add Object Type）] > [オブジェクトのインポート（Import Object）] サポートされるプラットフォーム：FMC

機能	詳細
アクセス制御およびプレフィルタポリシーのインターフェイス オブジェクトの最適化。	特定の FTD デバイスでインターフェイス オブジェクトの最適化を有効にできるようになりました。 展開時に、アクセス制御とプレフィルタポリシーで使用されるインターフェイスグループとセキュリティゾーンは、送信元/宛先インターフェイスペアごとに個別のルールを生成します。インターフェイス オブジェクトの最適化を有効にすると、システムはアクセス制御/プレフィルタルールごとに 1 つのルールを展開します。これにより、デバイス設定の簡素化および展開のパフォーマンス向上が可能になります。 インターフェイス オブジェクトの最適化はデフォルトで無効になっています。これを有効にする場合は、[Object Group Search] も有効にする必要があります。これは、ネットワークオブジェクトに加えてインターフェイス オブジェクトにも適用されるようになり、デバイスのメモリ使用量を削減できます。 新規/変更されたページ：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**>**[デバイス（Device）** > **[詳細設定（Advanced Settings）]** セクション > [インターフェイス オブジェクトの最適化（Interface Object Optimization）] チェックボックス サポートされるプラットフォーム：FTD
管理とトラブルシューティング	
FMC シングルサインオン。	FMC は、サードパーティの SAML 2.0 準拠アイデンティティ プロバイダー（IdP）で設定された外部ユーザーのシングルサインオン（SSO）をサポートするようになりました。IdP のユーザーまたはグループロールを FMC ユーザーロールにマッピングできます。 新規/変更されたページ： • **[Login]** > **[Single Sign-On]** • **[System]** > **[Users]** > **[SSO]** サポートされるプラットフォーム：FMC
FMC ログアウトの遅延。	FMC からログアウトする場合、自動的に 5 秒間のカウントダウンが行われます。[ログアウト（Log Out）] を再度クリックすると、すぐにログアウトできます。 サポート対象プラットフォーム：FMC
FTD コンテナインスタンスのバックアップと復元。	FMC を使用してバージョン 6.7.0 以降の FTD コンテナインスタンスをバックアップおよび復元できるようになりました。 サポートされるプラットフォーム：Firepower 4100/9300

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

機能	詳細
ヘルスモジュールの更新。	CPU 使用率ヘルスモジュールが 4 つの新しいモジュールに置き換わりました。 • CPU 使用率（コアごと）：すべてのコアの CPU 使用率をモニターします。 • CPU使用率データプレーン：デバイス上のすべてのデータプレーンプロセスの平均 CPU 使用率をモニターします。 • CPU 使用率 Snort：デバイス上の Snort プロセスの平均 CPU 使用率をモニターします。 • CPU 使用率システム：デバイス上のすべてのシステムプロセスの平均 CPU 使用率をモニターします。 メモリ使用量を追跡するために、次のヘルスモジュールが追加されました。 • メモリ使用率データプレーン：データプレーンプロセスで使用される割り当て済みメモリの割合をモニターします。 • メモリ使用率 Snort：Snort プロセスによって使用される割り当て済みメモリの割合をモニターします。 統計情報を追跡するために、次のヘルスモジュールが追加されました。 • 接続統計情報：接続統計情報と NAT 変換カウントをモニターします。 • クリティカルプロセス統計情報：クリティカルプロセスの状態、リソース消費量、再起動回数をモニターします。 • 展開された設定の統計情報：展開された設定に関する統計情報（ACE の数や IPS ルールなど）をモニターします。 • Snort 統計情報：イベント、フロー、およびパケットの Snort 統計情報をモニターします。 サポートされるプラットフォーム：FMC
メッセージセンターの検索。	メッセージセンターで現在のビューをフィルタリングできるようになりました。 新規/変更されたページ：メッセージセンターの [Show Notifications] スライダに [Filter] アイコンとフィールドが追加されました。 サポート対象プラットフォーム：FMC
ユーザビリティとパフォーマンス	

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

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

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

機能	詳細
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。	**FMC がアップグレードされないようにします。** 次の FTD 機能のいずれかを使用している場合、FMC をアップグレードできないことがあります。 • Diffie-Hellman グループ：2、5、および 24。 グループ 5 は、IKEv1 の FMC 展開で引き続きサポートされますが、より強力なオプションに変更することをお勧めします。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • NULL の「暗号化アルゴリズム」（暗号化なしの認証、テスト目的）は、IKEv1 と IKEv2 の両方の IPsec プロポーザルの FMC 展開で引き続きサポートされます。ただし、IKEv2 ポリシーではサポートされなくなりました。 • ハッシュアルゴリズム：MD5。 IKE プロポーザルまたは IPsec ポリシーでこれらの機能を使用している場合は、アップグレードする前に VPN 設定を変更して確認します。
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）。	**ヘルスモニターでのアップグレード後のエラーの可能性。** バージョン 6.7 では、バージョン 6.6.3 で導入され、後続のすべての 6.6.x リリースでサポートされるアプライアンス設定のリソース使用率の正常性モジュールに関するサポートが部分的かつ一時的に廃止されています。 バージョン 6.7 のサポートは次のとおりです。 • バージョン 6.6.3 以降からバージョン 6.7 への FMC のアップグレード デバイスがバージョン 6.6.x のままである場合にのみ、モジュールのサポートが継続されます。デバイスをバージョン 6.7 にアップグレードすると、モジュールは動作を停止し、正常性モニターにエラーが表示されます。エラーを解決するには、FMC を使用してモジュールを無効にし、ポリシーを再適用します。 • バージョン 6.3 ー 6.6.1 からバージョン 6.7.0 への FMC のアップグレード、または FMC バージョン 6.7 の新規インストール。 このモジュールはサポートされていません。 モジュールがサポートされていない FMC にモジュールが有効になっているバージョン 6.6.x デバイスを追加するまれなケースでは、解決できないエラーがヘルスモニターに表示されます。このエラーは無視しても問題ありません。 バージョン 7.0 ではフルサポートが提供され、モジュールの名前が 構成メモリ割り当て に変更されています。

機能	詳細
廃止：その他のヘルスモジュール（永久的）。	バージョン 6.7 では、次のヘルスモジュールが廃止されています。 • CPU 使用率：4 つの新しいモジュールに置き換えられました。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 モニター：Cisco Firepower ユーザーエージェントはサポートされなくなりました。
廃止：クラシックテーマを使用したウォークスルー。	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。
廃止：Bugtraq	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。 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。
廃止：Microsoft Internet Explorer	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。
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.6 の FMC 機能

新機能

表 *21 : FMC* バージョン *6.6.3* の新機能

機能	詳細
アップグレードがスケジュールされたタスクを延期する。	**アップグレードの影響。** アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、バージョン 6.6.3 以降を実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 以降のパッチからアップグレードする場合を除き、バージョン 6.6.3 へのアップグレードはサポートされません。
アプライアンス設定のリソース使用率の正常性モジュール。	**バージョン 6.7.0 のアップグレードの影響。** バージョン 6.6.3 では、デバイスのメモリ管理が改善され、新しい正常性モジュールであるアプライアンス設定のリソース使用率が導入されています。 モジュールは、展開された設定のサイズに基づき、デバイスのメモリが不足するリスクがある場合にアラートを出します。アラートには、設定に必要なメモリ量と、使用可能なメモリ量を超過した量が示されます。アラートが出た場合は、設定を再評価してください。ほとんどの場合、アクセス制御ルールまたは侵入ポリシーの数または複雑さを軽減できます。詳細については、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。 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。 （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。 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、バージョン 6.7 の FMC 機能 （181 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。

表 *22 : FMC* バージョン *6.6.0* の新機能

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。
AWS の展開用の大型のインスタンス。	**アップグレードの影響。** FTDv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C5.xlarge • C 5.2 xlarge • C5.4xlarge FMCv for AWS により、次の大型のインスタンスのサポートが追加されています。 • C3.4xlarge • C4.4xlarge • C5.4xlarge AWS インスタンスタイプの既存の 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。
クラウドベースの FTDv 展開の自動スケール。	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。 クラウドベースの展開におけるサーバーレスインフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内の FTDv インスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。 サポートされているプラットフォーム：FTDv for AWS、FTDv for Azure
Firepower Threat Defense：**デバイス管理**	
DHCP を使用した初期管理インターフェイスの IP アドレスの取得。	Firepower 1000/2000 シリーズと ASA-5500-X シリーズのデバイスの場合、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得するようになりました。この変更により、既存のネットワーク上に新しいデバイスを簡単に展開できるようになりました。 この機能は、論理デバイスを展開するときに IP アドレスを設定する Firepower 4100/9300 シャーシではサポートされていません。また、FTDv や ISA 3000 でもサポートされていません。これらについては、引き続きデフォルトで 192.168.45.45 になります。 サポートされているプラットフォーム：Firepower 1000/2000 シリーズ、ASA-5500-X シリーズ

機能	説明
CLI での MTU 値の設定。	FTD CLI を使用して、FTD デバイスインターフェイスの MTU（最大伝送単位）値を設定できるようになりました。デフォルト値は 1500 バイトです。MTU の最大値は次のとおりです。 • 管理インターフェイス：1500 バイト • イベントインターフェイス：9000 バイト 新しい FTD CLI コマンド： **configure network mtu** 変更された FTD CLI コマンド：**mtu-event-channel** キーワードと **mtu-management-channel** キーワードが **configure network management-interface** コマンドに追加されました。 サポートされるプラットフォーム：FTD
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。	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6.0+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6.0 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更されたページ：[システム（System）]>[更新（Updates）]>[更新のアップロード（Upload Update）] ボタン>[ソフトウェア更新ソースの指定（Specify Software Update Source）] オプション サポートされるプラットフォーム：FTD
接続ベースのトラブルシューティングの機能拡張。	FTD CLI 接続ベースのトラブルシューティングに次の機能拡張が加えられました（デバッギング）。 • **debug packet-module trace**：モジュールレベルのパケットトレースを有効にするために追加されました。 • **debug packet-condition**：進行中の接続のトラブルシューティングをサポートするように変更されました。 サポートされるプラットフォーム：FTD
Firepower Threat Defense：クラスタリング	

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

機能	説明
仮想ルータと VRF-Lite。	複数の仮想ルータを作成して、インターフェイスグループの個別のルーティングテーブルを管理できるようになりました。各仮想ルータには独自のルーティングテーブルがあるため、デバイスを流れるトラフィックを明確に分離できます。 仮想ルータは、Virtual Routing and Forwarding の「Light」バージョンである VRF-Lite を実装しますが、この VRF-Lite は Multiprotocol Extensions for BGP（MBGP）をサポートしていません。 作成できる仮想ルータの最大数は 5 ~ 100 の範囲で、デバイスのモデルによって異なります。完全なリストについては、『Firepower Management Center Configuration Guide』の「Virtual Routing for Firepower Threat Defense」の章を参照してください。 新規/変更されたページ：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ 新しい FTD CLI コマンド：**show vrf**。 変更された FTD CLI コマンド：［**vrf** *name* ｜ **all**］キーワードセットを CLI コマンド **clear ospf**、**clear route**、**ping**、**show asp table routing**、**show bgp**、**show ipv6 route**、**show ospf**、**show route**、**show snort counters** に追加し、必要に応じて出力が仮想ルータ情報を表示するように変更しました。 サポートされるプラットフォーム：FTD（Firepower 1010 および ISA 3000 を除く）
Firepower Threat Defense：**VPN**	
リモートアクセス VPN 内の DTLS 1.2。	Datagram Transport Layer Security（DTLS） 1.2 を使用して、RA VPN 接続を暗号化できるようになりました。 FTD プラットフォーム設定を使用して、FTD デバイスが RA VPN サーバーとして動作するときに使用する最小 TLS プロトコルバージョンを指定します。また、DTLS 1.2 を指定する場合は、最小 TLS バージョンとして TLS 1.2 を選択する必要もあります。 Cisco AnyConnect セキュア モビリティ クライアント バージョン 4.7 以降が必要です。 新規/変更されたページ：[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）] > [SSL] > [DTLS バージョン（DTLS Version）] オプション サポートされるプラットフォーム：FTD（ASA 5508-X および ASA 5516-X を除く）

機能	説明
複数のピアに対するサイト間 VPN IKEv2 のサポート。	IKEv1 と IKEv2 のポイントツーポイント エクストラネットおよびハブアンドスポークトポロジのために、サイト間 VPN 接続にバックアップピアを追加できるようになりました。これまで設定できたのは、IKEv1 ポイントツーポイント トポロジのバックアップピアのみでした。 新規/変更されたページ：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [ポイントツーポイントまたはハブアンドスポーク FTD VPN トポロジの追加または編集（Add or Edit a Point to Point or Hub and Spoke FTD VPN Topology）] > [エンドポイントの追加（Add Endpoint）] > [IP アドレス（IP Address）] フィールドで、カンマ区切りのバックアップピアがサポートされるようになりました。 サポートされるプラットフォーム：FTD
セキュリティ ポリシー	
セキュリティポリシーの使いやすさの向上。	バージョン 6.6.0 を使用すると、アクセス制御ルールとプレフィルタルールが簡単に使用できるようになります。次の作業に進んでください。 • 1 回の操作（状態、アクション、ロギング、侵入ポリシーなど）で、複数のアクセス制御ルールの特定の属性を編集します。 アクセス コントロール ポリシー エディタで、関連するルールを選択し、右クリックして [編集（Edit）] を選択します。 • 複数のパラメータによってアクセス制御ルールを検索します。 アクセス コントロール ポリシー エディタで、[ルールの検索（Search Rules）] テキストボックスをクリックしてオプションを表示します。 • アクセス制御ルールまたはプレフィルタルール内のオブジェクトの詳細と使用状況を表示します。 アクセス コントロール ポリシー エディタまたはプレフィルタ ポリシー エディタで、ルールを右クリックし、[オブジェクトの詳細（Object Details）] を選択します。 サポートされるプラットフォーム：FMC

機能	説明
アクセス コントロール ポリシーのオブジェクトグループ検索。	動作中、FTDデバイスは、アクセスルールで使用されるネットワークオブジェクトの内容に基づいて、アクセス制御ルールを複数のアクセスコントロールリストのエントリに展開します。オブジェクトグループ検索を有効にすることで、アクセス制御ルールの検索に必要なメモリを抑えることができます。 オブジェクトグループ検索を有効にした場合、システムによってネットワークオブジェクトは拡張されませんが、オブジェクトグループの定義に基づいて一致するアクセスルールが検索されます。 オブジェクトグループ検索は、ルールがどのように定義されているかや、FMC にどのように表示されるかには影響しません。アクセス制御ルールと接続を照合するときに、デバイスがアクセス制御ルールを解釈して処理する方法のみに影響します。オブジェクトグループ検索はデフォルトで無効になっています。 新規/変更されたページ：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[デバイス（Device）] タブ >[詳細設定（Advanced Settings）]>[オブジェクトグループ検索（Object Group Search）] オプション サポートされるプラットフォーム：FTD
アクセス コントロール ポリシーとプレフィルタポリシーの時間ベースのルール。	適用するルールの絶対時間または反復時間、あるいは時間範囲を指定できるようになりました。このルールは、トラフィックを処理するデバイスのタイムゾーンに基づいて適用されます。 新規/変更されたページ： • アクセス コントロール ルール エディタまたはプレフィルタルールエディタ • [デバイス（Devices）]>[プラットフォーム設定（Platform Settings）]>[Threat Defense ポリシーの追加/編集（Add/Edit Threat Defense Policy）]>[タイムゾーン（Time Zone）] • [オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[時間範囲（Time Range）] と [タイムゾーン（Time Zone）] サポートされるプラットフォーム：FTD
出力最適化の再有効化。	**アップグレードの影響。** バージョン 6.6.0 では CSCvs86257 が修正されました。出力最適化が次のような状態だった場合があります。 • 有効になっていたがオフになり、アップグレードするとオンに戻る（機能が有効になっていた場合でも、バージョン 6.4.0 と 6.5.0 の一部のパッチでは出力最適化をオフにしていました）。 • 手動で無効にした場合は、アップグレード後に **asp inspect-dp egress-optimization** を使用して再度有効にすることをお勧めします。 サポートされるプラットフォーム：FTD

機能	説明
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。	**アップグレードの影響。** パフォーマンスを向上させるために、バージョン 6.6.0 では、接続およびセキュリティ インテリジェンス イベントに新しいデータストアを使用します。 アップグレードが完了し、FMC がリブートすると、履歴接続イベントとセキュリティ インテリジェンスイベントがバックグラウンドで移行され、リソースが制限されます。FMC モデル、システム負荷、および保存したイベント数に応じて、数時間から最大で 1 日かかることがあります。 履歴イベントは、経過時間ごとに、最新のイベントが最初に以降されます。移行されていないイベントは、クエリ結果やダッシュボードに表示されません。移行が完了する前に接続イベントデータベースの制限に達した場合（アップグレード後のイベントの場合など）、最も古い履歴イベントは移行されません。 イベントの移行の進行状況は、メッセージセンターでモニターできます。 サポート対象プラットフォーム：FMC
URL の接続イベントとセキュリティ インテリジェンス イベントを検索する場合のワイルドカードのサポート。	**example.com** のパターンを持つ URL の接続イベントとセキュリティ インテリジェンスイベントを検索する場合は、ワイルドカードを含めなければならなくなりました。このような検索の場合、具体的には ***example.com*** を使用します。 サポート対象プラットフォーム：FMC

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

機能	説明
設定変更を展開するための新しいオプション。	FMC メニューバーの [展開（Deploy）] ボタンが次の機能を追加するオプションが備わったメニューになりました。 • [ステータス（Status）]：デバイスごとに、変更を展開する必要があるかどうか、展開前に解決する必要がある警告またはエラーがあるかどうか、最後の展開が処理中、失敗、正常に完了のうちのどの状態かが表示されます。 • [プレビュー（Preview）]：デバイスに対して最後に展開してから行った、適用可能なすべてのポリシーとオブジェクトの変更が表示されます。 • [展開の選択（Selective Deploy）]：管理対象デバイスに対して展開するポリシーと設定から選択します。 • [展開時間の見積もり（Deploy Time Estimate）]：特定のデバイスに対して展開するためにかかる時間の見積もりが表示されます。すべての展開のみでなく、特定のポリシーや設定の見積もりを表示することができます。 • [履歴（History）]： 以前の展開の詳細が表示されます。 新規/変更されたページ： • **[展開（Deploy）] > [展開（Deployment）]** • **[展開（Deploy）] > [展開履歴（Deployment History）]** サポート対象プラットフォーム：FMC
初期設定による VDB の更新と、SRU の更新のスケジュール設定。	新規および再イメージ化された FMC では、セットアッププロセスは次のようになりました。 • 最新の脆弱性データベース（VDB）の更新をダウンロードしてインストールします。 • 毎日の侵入ルール（SRU）のダウンロードを有効にします。これらのダウンロード後は、セットアッププロセスで自動展開が有効にならないことに注意してください。ただし、この設定は変更できます。 アップグレードされた FMC は影響を受けません。 新規/変更されたページ： • [システム（System）] > [更新（Updates）] > [製品の更新（VDB の更新）（Product Updates (VDB updates)）] • [システム（System）] > [更新（Updates）] > [ルールの更新（SRU の更新）（Rule Updates (SRU updates)）] サポート対象プラットフォーム：FMC

機能	説明
FMC を復元するための VDB の一致は不要。	バックアップからの FMC の復元に交換用 FMC 上に同じ VDB を使用する必要はなくなりました。ただし、復元すると、既存の VDB がバックアップファイル内の VDB に置き換えられます。 サポート対象プラットフォーム：FMC
サブジェクト代替名（SAN）を使用した HTTPS 証明書。	SAN を使用して複数のドメイン名または IP アドレスを保護する HTTPS サーバー証明書を要求できるようになりました。SAN の詳細については、RFC 5280、セクション 4.2.1.6 を参照してください。 新規/変更されたページ：[システム（System）] > [設定（Configuration）] > [HTTPS 証明書（HTTPS Certificate）] > [新しい CSR の生成（Generate New CSR）] > [サブジェクト代替名（Subject Alternative Name）] フィールド サポート対象プラットフォーム：FMC
FMC ユーザーアカウントに関連付けられている実名。	FMC ユーザーアカウントを作成または変更するときに、実名を指定できるようになりました。これには、個人名、部署名、またはその他の識別属性を指定できます。 新規/変更されたページ：[システム（System）] > [ユーザー（Users）] > [ユーザー（Users）] > [実名（Real Name）] フィールド サポート対象プラットフォーム：FMC
追加の FTD プラットフォームでの Cisco Support Diagnostics。	**アップグレードの影響。** Cisco Support Diagnostics は、すべての FMC および FTD デバイスで完全にサポートされるようになりました。以前は、サポートは FMC、FTD 搭載 Firepower 4100/9300、および Azure 向け FTDv に限定されていました。 サポートされるプラットフォーム：FMC、FTD
ユーザビリティ	
ライトテーマ。	FMC はデフォルトでバージョン 6.5.0 のベータ機能として導入されたライトテーマに設定されます。バージョン 6.6.0 にアップグレードすると、ライトテーマに自動的に切り替わります。これは、ユーザー設定で従来のテーマに戻すことができます。 すべてに返信することはできませんが、ライトテーマについてのフィードバックを歓迎します。[ユーザー設定（User Preferences）] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com からフィードバックをお送りください。 サポート対象プラットフォーム：FMC
アップグレードの残り時間の表示。	FMC のメッセージセンターに、アップグレードが完了するまでのおおよその残り時間が表示されるようになりました。これには、リブート時間は含まれません。 新規/変更されたページ：メッセージセンター サポート対象プラットフォーム：FMC

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

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

廃止された機能

表 *23 : FMC* バージョン *6.6.1* で廃止された機能

機能	詳細
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。	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。 既存のルールと同じ SID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。FMC コンフィギュレーションガイドでローカル侵入ルールをインポートするためのベストプラクティスを参考にすることを推奨します。 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。

表 *24 : FMC* バージョン *6.6.0* で廃止された機能

機能	詳細
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。	パフォーマンス上の理由から、次の FMCv インスタンスはサポートされなくなりました。 • AWS での c3.xlarge • AWS での c3.2xlarge • AWS での c4.xlarge • AWS での c4.2xlarge • Azure での Standard_D3_v2 バージョン 6.6.0+ にアップグレードする前に、サイズを変更する必要があります。詳細については、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。 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。
廃止：VMware 向け FTDv の e1000 インターフェイス。	**アップグレードされないようにします。** バージョン 6.6 では、VMware 向け FTDv の e1000 インターフェイスのサポートを終了します。vmxnet3 または ixgbe インターフェイスに切り替えるまで、アップグレードすることはできません。または、新しいデバイスを展開できます。 詳細については、『Cisco Secure Firewall Threat Defense Virtual スタートアップガイド』を参照してください。
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。	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。 • Diffie-Hellman グループ：2、5、および 24。 • 強力な暗号化の輸出規制を満たすユーザー向けの暗号化アルゴリズム：DES、3DES、AES-GMAC、AES-GMAC-192、AES-GMAC-256。輸出規制を満たしていないユーザーの場合、DES は引き続きサポートされます（これが唯一のオプションです）。 • ハッシュアルゴリズム：MD5。 これらの機能はバージョン 6.7 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。

機能	詳細
廃止：接続イベントのカスタムテーブル。	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。 他のタイプのカスタムテーブルに変更はありません。 廃止されたオプション： • [分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル （Custom Tables）] > [カスタムテーブルの作成（Create Custom Table）] > [テーブル（Tables）] ドロップダウンリスト > [接続イベント（Connection Events）] と、[セキュリティ インテリジェンス イベント（Security Intelligence Events）] のクリック
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。	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。 廃止されたオプション： • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** > [削除（Delete）] と [すべて削除（Delete All）] • **[分析（Analysis）] > [接続（Connections）] > [セキュリティ インテリジェンス イベント（Security Intelligence Events）]** > [削除（Delete）] と [すべて削除（Delete All）]
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.5 の FMC 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	詳細
バージョン 6.5.0.5	**アップグレードの影響。**
デフォルトの HTTPS サーバー証明書	FMC で現在デフォルト設定されているの HTTPS サーバー証明書の有効期間がすでに 800 日の場合を除き、バージョン 6.5.0.5+ にアップグレードすると証明書が更新されて、アップグレードの日から 800 日後に期限切れになります。その後の更新はすべて、有効期間が 800 日になります。 古い証明書には、生成日に応じて、次の期限が設定されています。 • 6.5.0 ～ 6.5.0.4：3 年 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年

表 *26 : FMC* バージョン *6.5.0* の新機能

機能	詳細
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。	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。 FMC モデル移行機能を使用すると、性能が劣るプラットフォームから FMCv 300 に切り替えることができます。
VMware vSphere/VMware ESXi 6.7 のサポート	VMware vSphere/VMware ESXi 6.7 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。
Firepower Threat Defense	

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

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

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

機能	詳細
Cisco Firepower User Agent バージョン 2.5 の統合	Firepower バージョン 6.4.0 ～ 6.6.x と統合できる Cisco Firepower User Agent のバージョン 2.5 がリリースされました。 （注） バージョン 6.6 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。 詳細については、Cisco Firepower User Agent のサポート終了 [英語] 通知、および Firepower ユーザー ID：ユーザーエージェントから Identity Services Engine への移行 [英語] の技術メモを参照してください。 新規/変更された FMC CLI コマンド： **configure user-agent** サポートされるプラットフォーム：FMC
イベントロギングおよび分析	

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

機能	詳細
packet-profile CLI コマンド	デバイスがネットワークトラフィックをどのように処理したかに関する統計情報を取得するFTDCLIを使用できるようになりました。プレフィルタポリシーによって高速パス処理されたパケット数、大規模なフローとしてオフロードされたパケット数、アクセス制御（Snort）によって完全に評価されたパケット数などを取得できます。 新しい FTD CLI コマンド： • **asp packet-profile** • **no asp packet-profile** • **show asp packet-profile** • **clear asp packet-profile** サポートされるプラットフォーム：FTD
Cisco SecureX に対応したその他のイベントタイプ	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。 FMC Web インターフェイスでは、この機能を Cisco Threat Response（CTR）と呼びます。 新規/変更されたページ：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] サポートされるプラットフォーム：FTD（syslog 経由または直接統合）および従来のデバイス（syslog 経由）
管理とトラブルシューティング	
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTPは、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp**（インターフェイス モード）コマンド、グローバル コマンド **ptp mode e2etransparent**、**ptp domain** を追加できるようになりました。 新規/変更されたコマンド： **show ptp** サポートされるプラットフォーム：FTD を使用した ISA 3000
設定できるドメイン数の増加（マルチテナンシー）	マルチテナンシーを実装する（管理対象デバイス、設定、およびイベントへのユーザーアクセスをセグメント化する）場合、最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 個のサブドメインを作成できます。以前は、最大で 50 ドメインでした。 サポートされるプラットフォーム：FMC

機能	詳細
ISE 接続ステータスのモニターの機能拡張	[ISE接続ステータスのモニター（ISE Connection Status Monitor）] ヘルスモジュールで、TrustSec SXP（SGT Exchange Protocol）サブスクリプション ステータスに関する問題のアラートが表示されるようになりました。 サポートされるプラットフォーム：FMC
地域のクラウド	**アップグレードの影響。** Cisco Threat Response の統合、Cisco Support Diagnostics、または Cisco Success Network 機能を使用する場合は、地域クラウドを選択できるようになりました。 デフォルトでは、アップグレードによって米国（北米）リージョンに割り当てられます。 新規/変更されたページ：**[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）]** サポートされるプラットフォーム：FMC、FTD
Cisco Support Diagnostics	**アップグレードの影響。** Cisco Support Diagnostics（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TACTAC ケースの過程でデバイスから必要な情報を収集することもできます。 初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。 バージョン 6.5.0 では、Cisco Support Diagnostics のサポートは一部のプラットフォームに限定されています。 新規/変更されたページ： • **[システム（System）] > [スマートライセンス（Smart Licenses）]** • **[システム（System）] > [スマートライセンス（Smart Licenses）] > [登録（Register）]** サポートされるプラットフォーム：FMC、Firepower 4100/9300、および Azure 向け FTDv

機能	詳細
FMC モデル移行	バックアップおよび復元機能を使用して、FMC が同じモデルでない場合でも、FMC 間で設定とイベントを移行できるようになりました。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による FMC の交換が容易になります。 一般に、ローエンドの FMC からハイエンドの FMC に移行することはできますが、その逆に移行することはできません。KVM および Microsoft Azure からの移行はサポートされていません。また、Cisco Smart Software Manager（CSSM）への登録を解除して再登録する必要があります。 サポート対象の移行先モデルなどの詳細については、『Cisco Secure Firewall Management Center モデル移行ガイド』を参照してください。 サポート対象プラットフォーム：FMC
デフォルトの HTTPS サーバー証明書。	バージョン 6.4.0.9 以降からアップグレードする場合、デフォルトの HTTPS サーバー証明書の lifespan-on-renew は 3 年に戻りますが、バージョン 6.5.0.5 以降および 6.6 以降で再び 800 日に更新されます。 現在のデフォルトの HTTPS サーバー証明書は、いつ生成されたかに応じて、次のように期限切れになるように設定されています。 • 6.4.0.9 以降のパッチ：800 日 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3：20 年
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	指定したアプライアンス コンポーネントを安全に消去する FXOS CLI を使用できるようになりました。 新しい FXOS CLI コマンド： **erase secure** サポートされるプラットフォーム：Firepower 1000/2000 および Firepower 4100/9300

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

機能	詳細
初期設定の改善	新規および再イメージ化された FMC では、ウィザードによって以前の初期設定プロセスが置き換えられます。GUI ウィザードを使用すると、初期設定の完了時に FMC に [デバイス管理（Device Management）] ページが表示され、導入環境のライセンシング と設定をすぐに開始できます。 また、設定プロセスでは以下が自動的にスケジュールされます。 • ソフトウェアのダウンロード。導入環境に適用されるソフトウェアパッチおよび公開されているホットフィックスをダウンロードする（インストールはしない）、毎週にスケジュール設定されたタスクが作成されます。 • FMC 設定のみのバックアップ。FMC の設定をバックアップしてローカルに保存する、週次のスケジュールされたタスクが作成されます。 • GeoDB の更新。地理位置情報データベースの毎週の更新が有効になります。 タスクは UTC でスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクは UTC でスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。 （注） 自動スケジュール設定タスクと GeoDB の更新を確認し、必要に応じて調整することを強くお勧めします。 アップグレードされた FMC は影響を受けません。初期設定ウィザードの詳細については、ご使用の FMC モデルのスタートアップガイドを参照してください。スケジュールされたタスクの詳細については、FMC コンフィギュレーション ガイドを参照してください。 サポートされるプラットフォーム：FMC
ライトテーマ	**ベータ版。** FMC Web インターフェイスのデフォルトはクラシックテーマですが、新しいライトテーマを選択することもできます。 （注） ライトテーマはベータ機能です。テキストやその他の UI 要素の位置がずれていることがあります。場合によっては、応答時間が通常より長くなることもあります。ページまたは機能を使用できない問題が発生した場合は、クラシックテーマに戻してください。すべてに対応することはできませんが、フィードバックもお寄せください。[ユーザー設定（User Preferences）] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com"> までお問い合わせください。 新規/変更されたページ：ユーザー名の下にあるドロップダウンリストの [ユーザー設定（User Preferences）] サポートされるプラットフォーム：FMC

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

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

廃止された機能

表 *27* : *FMC* バージョン *6.5.0* パッチで廃止された機能

機能	詳細
バージョン 6.5.0.2 廃止：出力最適化（一時的）。	**アップグレードの影響。** 出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。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。 （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。 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。 サポートされるプラットフォーム：FTD

表 *28* : *FMC* バージョン *6.5.0* で廃止された機能

機能	詳細
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	詳細
廃止：FMC CLI を無効にする機能。	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。 **注意** Cisco TAC の指示がない限り、シェルを使用して Firepower アプライアンスにアクセスしないことをお勧めします。 廃止されたオプション：**[システム（System）] > [設定（Configuration）] > [コンソール設定（Console Configuration）] > [CLI アクセスの有効化（Enable CLI Access）] チェックボックス**
廃止：SNMPv3 ユーザー向けの MD5 認証アルゴリズムと DES 暗号化。	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。 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。 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。 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）]
廃止：TLS 1.0 および 1.1。	**アップグレードの影響。** セキュリティ強化対策： • キャプティブポータル（アクティブ認証）では、TLS 1.0 のサポートが廃止されました。 • ホスト入力で TLS 1.0 および TLS 1.1 のサポートが廃止されました。 クライアントが Firepower アプライアンスとの接続に失敗した場合は、TLS 1.2 をサポートするようにクライアントをアップグレードすることをお勧めします。
廃止：Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド。	Firepower 4100/9300 の複数のコンテナ インスタンスに対して TLS crypto アクセラレーションを許可する一環として、次の FXOS CLI コマンドを削除しました。 • **show hwCrypto** • **config hwCrypto** および、この FTD CLI コマンドを削除しました。 • **show crypto accelerator status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。

機能	詳細
廃止：Cisco Security Packet Analyzer の統合。	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。 廃止された画面/オプション： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）]
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.4 の FMC 機能

新機能

表 *29 : FMC* バージョン *6.4.0* パッチの新機能

機能	詳細
バージョン 6.4.0.17 メモリが少ないデバイス用の小規模 VDB。	VDB 363 以降では、メモリが少ないデバイスに小規模 VDB（別称：*VDB lite*）がインストールされるようになりました。この小規模 VDB には同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 必要最低限の Threat Defense：任意 メモリが少ないデバイス：ASA 5506-X シリーズ、ASA-5508-X、5512-X、5515-X、5516-X、5525-X、5545-X バージョンの制限：小規模 VDB をインストールできるかどうかは、管理対象デバイスではなく FMC のバージョンによって決まります。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 FMC をアップグレードする場合、導入環境内にメモリの少ないデバイスが 1 つでも含まれていると、VDB 363 以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。
バージョン 6.4.0.10 アップグレードがスケジュールされたタスクを延期する。	**アップグレードの影響。** アップグレードは、スケジュールされたタスクを延期するようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、バージョン 6.4.0.10 以降のパッチを実行している Firepower アプライアンスでサポートされています。バージョン 6.4.0.10 へのアップグレード、またはバージョン 6.4.0.10 をスキップするアップグレードではサポートされません。この機能はバージョン 6.5.0 ～ 6.6.1 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。

機能	詳細
バージョン 6.4.0.9 デフォルトの HTTPS サーバー証明書。	**アップグレードの影響。** FMC または 7000/8000 シリーズのデバイスをバージョン 6.4.0 ～ 6.4.0.8 から以降のバージョン 6.4.0.x のパッチに（または FMC をバージョン 6.6.0+ に）アップグレードすると、デフォルトの HTTPS サーバー証明書が更新されます。この証明書は、アップグレードの日から 800 日後に期限切れになります。その後の更新はすべて、有効期間が 800 日になります。 古い証明書には、生成日に応じて、次の期限が設定されています。 • 6.4.0 ～ 6.4.0.8：3 年 • 6.3.0 およびすべてのパッチ：3 年 • 6.2.3 以前：20 年 バージョン 6.5.0 ～ 6.5.0.4 では、更新時の有効期限が 3 年に戻ることに注意してください。ただし、バージョン 6.5.0.5 および 6.6.0 では 800 日に更新されます。
バージョン 6.4.0.4 新しい syslog フィールド。	次の新しい syslog フィールドは、一意の接続イベントをまとめて識別します。 • センサー UUID • 最初のパケット時間 • 接続インスタンス ID • 接続数カウンタ これらのフィールドは、侵入、ファイル、およびマルウェアイベントの syslog にも表示され、接続イベントをこれらのイベントに関連付けることができます。
バージョン 6.4.0.2 FTD NAT ポリシーでのルールの競合の検出。	**アップグレードの影響。** バージョン 6.4.0.2 以降のパッチにアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つ FTD NAT ポリシーを作成できなくなります。これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合している NAT ルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後に FTD NAT ポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。

機能	詳細
バージョン 6.4.0.2 [ISE接続ステータスのモニター（ISE Connection Status Monitor）] ヘルスモジュール。	新しいヘルスモジュール [ISE接続ステータスのモニター（ISE Connection Status Monitor）] は、Cisco Identity Services Engine（ISE）と FMC 間のサーバー接続のステータスをモニターします。

表 *30 : FMC* バージョン *6.4.0* の新機能

機能	詳細
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。
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。	VMware の FTDv は、仮想デバイスを作成するときにデフォルトで vmxnet3 インターフェイスに設定されるようになりました。以前は、デフォルトは e1000 でした。Vmxnet3 のデバイス ドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワーク パフォーマンスが向上します。 （注） バージョン 6.6 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。 サポートされているプラットフォーム：VMware の FTDv
Firepower Threat Defense：ルーティング	

機能	詳細
OSPFv2 ルーティングの循環（キーチェーン）認証。	OSPFv2 ルーティングを設定すると、循環（キーチェーン）認証を使用できるようになりました。 新規/変更されたページ： • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[キーチェーン（Key Chain）]** オブジェクト • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [インターフェイス（Interface）] タブ > [インターフェイスの追加/編集（add/edit interface）] > [認証（Authentication）] オプション • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit device）] > [ルーティング（Routing）] タブ > [OSPF 設定（OSPF settings）] > [エリア（Area）] タブ > [エリアの追加/編集（add/edit area）] > [仮想リンク（Virtual Link）] サブタブ > [仮想リンクの追加/編集（add/edit virtual link）]> [認証（Authentication）] オプション サポートされるプラットフォーム：FTD
Firepower Threat Defense：**暗号化と VPN**	
RA VPN：セカンダリ認証。	セカンダリ認証（二重認証とも呼ばれる）は、2 つの異なる認証サーバーを使用して、RA VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、AnyConnect VPN のユーザーは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。 RA VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。 新規/変更されたページ：**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]** > [設定の追加/編集（add/edit configuration）] > [接続プロファイル（Connection Profile）] > [AAA] 領域 サポートされるプラットフォーム：FTD
サイト間 VPN：エクストラネット エンドポイントのダイナミック IP アドレス。	エクストラネット エンドポイントにダイナミック IP アドレスを使用するように、サイト間 VPN を設定できるようになりました。ハブアンドスポーク導入環境では、ハブをエクストラネット エンドポイントとして使用できます。 新規/変更されたページ：**[デバイス（Devices）]** > **[VPN]** > **[サイト間（Site To Site）]** > [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [エンドポイント（Endpoints）] タブ > [エンドポイントの追加（add endpoint）] > [IP アドレス（IP Address）] オプション サポートされるプラットフォーム：FTD

機能	詳細
サイト間 VPN：ポイントツーポイント トポロジのためのダイナミック暗号マップ。	ポイントツーポイントおよびハブアンドスポーク VPN トポロジでは、ダイナミック暗号マップを使用できるようになりました。フル メッシュ トポロジについては、ダイナミック暗号マップはまだサポートされていません。 トポロジを設定するときは、暗号マップ タイプを指定します。トポロジ内のピアの 1 つに対して、ダイナミック IP アドレスも指定する必要があります。 新規/変更されたページ：**[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] >** [FTD VPN トポロジの追加/編集（add/edit FTD VPN topology）] > [IPsec] タブ > [暗号マップ タイプ（Crypto Map Type）] オプション サポートされるプラットフォーム：FTD
TLS暗号化アクセラレーション。	**アップグレードの影響。** SSL ハードウェア アクセラレーションは、TLS暗号化アクセラレーションに名前が変更されました。デバイスによっては、TLS暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。バージョン 6.4.0 のアップグレードプロセスでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。 ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。ただし、Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、モジュール/セキュリティ エンジンごとに、*1* つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナ インスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。 Firepower 4100/9300 シャーシ向けの新しい FXOS CLI コマンド： • **show hwCrypto** • **config hwCrypto** 新しい FTD CLI コマンド： • **show crypto accelerator status**（**system support ssl-hw-status** の代替） 削除された FTD CLI コマンド： • **system support ssl-hw-accel** • **system support ssl-hw-status** サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300
イベントロギングおよび分析	

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

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

機能	詳細
管理インターフェイスで重複アドレス検出（DAD）を無効にする機能。	IPv6 を有効にすると、DAD を無効にすることができます。DAD を使用するとサービス拒否攻撃の可能性が拡大するため、DAD は無効にすることができます。この設定を無効にした場合は、すでに割り当てられているアドレスがこのインターフェイスで使用されていないことを手動で確認する必要があります。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [インターフェイス（Interfaces）]** 領域 > [インターフェイスの編集（edit interface）] > [IPv6 DAD] チェックボックス サポートされるプラットフォーム：FMC、Firepower 7000/8000 シリーズ
管理インターフェイス上の ICMPv6 エコー応答および宛先到達不能メッセージを無効にする機能。	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更されたページ：**[システム（System）] > [設定（Configuration）] > [管理インターフェイス（Management Interfaces）] > [ICMPv6]** 新規/変更されたコマンド： • **configure network ipv6 destination-unreachable** • **configure network ipv6 echo-reply** サポートされるプラットフォーム：FMC（Web インターフェイスのみ）、管理対象デバイス（CLI のみ）
RADIUS サーバーに定義されている FTD ユーザーの Service-Type 属性のサポート。	FTD CLI ユーザーの RADIUS 認証では、以前は RADIUS 外部認証オブジェクトにユーザー名を事前に定義してから、RADIUS サーバーに定義されているユーザー名とリストが一致していることを手動で確認する必要がありました。Service-Type 属性を使用して RADIUS サーバーで CLI ユーザーを定義できるようになりました。また、Basic と Config の両方のユーザー ロールも定義できます。このメソッドを使用するには、外部認証オブジェクトのシェル アクセス フィルタを空白のままにしてください。 新規/変更されたページ：**[システム（System）] > [ユーザー（Users）] > [外部認証（External Authentication）]** タブ > [外部認証オブジェクトの追加/編集（add/edit external authentication object）] > [シェルアクセスフィルタ（Shell Access Filter）] サポートされるプラットフォーム：FTD
オブジェクトの使用状況の表示。	オブジェクト マネージャでネットワーク、ポート、VLAN、または URL オブジェクトが使用されているポリシー、設定、およびその他のオブジェクトを表示できるようになりました。 新規/変更されたページ：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > でオブジェクトタイプ、[使用状況の検索（Find Usage）]（双眼鏡）アイコンの順に選択 サポートされるプラットフォーム：FMC

機能	詳細
アクセス制御ルールと事前フィルタルールのヒットカウント。	FTD デバイスのアクセス制御ルールと事前フィルタ ルールのヒット カウントにアクセスできるようになりました。 新規/変更されたページ： • **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒットカウントの分析（Analyze Hit Counts）] • **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[事前フィルタ（Prefilter）]** > [ポリシーの追加/編集（add/edit policy）] > [ヒットカウントの分析（Analyze Hit Counts）] 新しいコマンド： • **show rule hits** • **clear rule hits** • **cluster exec show rule hits** • **cluster exec clear rule hits** • **show cluster rule hits** 変更されたコマンド： **show failover** サポートされるプラットフォーム：FTD
URL フィルタリング ヘルス モニターの改善。	URLフィルタリングモニターアラートの時間しきい値を設定できるようになりました。 新規/変更されたページ：**[システム（System）]** > **[正常性（Health）]** > **[ポリシー（Policy）]** > [ポリシーの追加/編集（add/edit policy ）] > [URL フィルタリングモニター（URL Filtering Monitor）] サポートされるプラットフォーム：すべて
接続ベースのトラブルシューティング。	接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大 7 レベルまでサポートし、lina ログと Snort ログで一貫したログ収集メカニズムを使用できます。 新規/変更されたコマンド： • **clear packet debugs** • **debug packet start** • **debug packet stop** • **show packet debugs** サポートされるプラットフォーム：FTD

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

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

機能	詳細
選択された IPS トラフィックのパフォーマンスの向上。	**アップグレードの影響。** 出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。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。 新規/変更されたコマンド： • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization** 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。 （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。 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。 サポートされるプラットフォーム：FTD
SNMP イベントロギングの高速化。	外部 SNMP トラップ サーバーに侵入イベントと接続イベントを送信する際のパフォーマンスが向上しました。 サポートされているプラットフォーム：すべて
展開の高速化。	アプライアンスの通信と展開フレームワークが向上しました。 サポートされるプラットフォーム：FTD
アップグレードの高速化。	イベント データベースが向上しました。 サポートされているプラットフォーム：すべて
Firepower Management Center REST API	

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

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

機能	詳細
廃止：SSL ハードウェア アクセラレーション FTD CLI コマンド。	TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。 • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status**

機能	詳細
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.3 の FMC 機能

新機能

表 *32 : FMC* バージョン *6.3.0* パッチの新機能

機能	詳細
バージョン 6.3.0.4	**アップグレードの影響。**
FTD NAT ポリシーでのルールの競合の検出	バージョン 6.3.0.4 以降のパッチにアップグレードすると、競合するルール（「重複」ルールまたは「オーバーラップ」ルールとも呼ばれます）を持つ FTD NAT ポリシーを作成できなくなります。これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合している NAT ルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後に FTD NAT ポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 バージョン 6.4.0 にアップグレードすると、この修正が無効になります。これは、バージョン 6.4.0.2 で再度修正されました。

機能	詳細
バージョン 6.3.0.4 [ISE接続ステータスのモニター（ISE Connection Status Monitor）] モジュール	新しいモジュールである [ISE接続ステータスのモニター（ISE Connection Status Monitor）] は、Cisco Identity Services Engine（ISE）と FMC 間のサーバー接続のステータスをモニターします。 バージョン 6.4.0 にアップグレードすると、このモジュールが無効になります。サポートは、バージョン 6.4.0.2 で再開されています。 新規/変更された画面：[システム（System）]>[ポリシー（Policy）]>ポリシーの作成または編集 > [ISE接続ステータスのモニター（ISE Connection Status Monitor）]
バージョン 6.3.0.3 2048 ビットの証明書キーが必要になりました（セキュリティ強化）	AMP for Endpoints や Cisco Threat Intelligence Detector（TID）などの外部データソースへのセキュアな接続を行う場合、FMC では、少なくとも 2048 ビット長のキーを使用したサーバー証明書の生成が必要になりました。以前に 1024 ビットキーを使用して生成された証明書は機能しなくなります。 接続できない場合は、データソースでサーバー証明書を再生成します。必要に応じて、データソースへの FMC 接続を再設定します。
バージョン 6.3.0.1 EMS 拡張機能のサポート	**アップグレードの影響。** バージョン 6.3.0.1 では EMS 拡張機能のサポートが再導入されます。これは、バージョン 6.2.3.8/6.2.3.9 で導入されましたが、バージョン 6.3.0 には含まれていませんでした。 [復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、再び ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になります。EMS 拡張機能は、 RFC 7627 によって定義されています。 FMC 展開では、この機能は、デバイスのバージョンによって異なります。ベストプラクティスは展開全体をアップグレードすることですが、デバイスにパッチを適用するだけでも、この機能はサポートされます。

表 *33 : FMC* バージョン *6.3.0* の新機能

機能	詳細
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。	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）。 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。

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

機能	詳細
Firepower 4100/9300 のマルチインスタンス機能。	単一のセキュリティ エンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナ インスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブ アプリケーション インスタンスを展開できるだけでした。 柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2台の個別のシャーシ上でコンテナインスタンスを使用してハイアベイラビリティを使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。FTD では、マルチ コンテキスト モードを使用できません。 新規/変更された FMC ページ：**[デバイス（Devices）] > [デバイス管理（Device Management）]**> [デバイスの編集（edit device）] > [インターフェイス（Interfaces）] タブ 新規/変更された Firepower Chassis Manager ページ： • **[概要（Overview）] > [デバイス（Devices）]** • **[インターフェイス（Interfaces）]**> **[すべてのインターフェイス（All Interfaces）]**> **[新規追加（Add New）]** ドロップダウンメニュー > [サブインターフェイス（Subinterface）] • **[インターフェイス（Interfaces）]**> **[すべてのインターフェイス（All Interfaces）]**> **[タイプ（Type）]** • **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）]** • **[プラットフォームの設定（Platform Settings）] > [Macプール（Mac Pool）]** • **[プラットフォームの設定（Platform Settings）]**>**[リソースのプロファイル（Resource Profiles）]** 新規/変更された FXOS コマンド：**connect ftd***name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**create resource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** サポートされるプラットフォーム：Firepower 4100/9300

機能	詳細
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これでFXOSでクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンクインターフェイスIPアドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された Firepower Chassis Manager ページ：**[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** > **[クラスタ情報（Cluster Information）]** 新規/変更されたオプション：[CCL サブネット IP（CCL Subnet IP）] フィールド 新規/変更された FXOS コマンド： **set cluster-control-link network** サポートされるプラットフォーム：Firepower 4100/9300
FMC への FTD クラスタ追加の改善	FMCにクラスタの任意のユニットを追加できるようになりました。他のクラスタユニットは自動的に検出されます。以前は、各クラスタユニットを個別のデバイスとして追加し、FMC でグループ化してクラスタにする必要がありました。クラスタ ユニットの追加も自動で実行されるようになりました。ユニットは手動で削除する必要があることに注意してください。 新規/変更されたページ： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [追加（Add）] ドロップダウンメニュー > [デバイス（Devices）] > [デバイスの追加（Add Device）] ダイアログボックス • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [クラスタ（Cluster）] タブ > [全般（General）] 領域 > [クラスタの登録ステータス（Cluster Registration Status）] > [現在のクラスタの概要（Current Cluster Summary）] リンク > [クラスタステータス（Cluster Status）] ダイアログボックス サポートされるプラットフォーム：Firepower 4100/9300
Firepower Threat Defense：**暗号化と VPN**	
SSL ハードウェア アクセラレーション	追加の FTD デバイスが SSL ハードウェア アクセラレーションをサポートするようになりました。また、このオプションはデフォルトで有効になっています。 バージョン 6.3.0 にアップグレードすると、対象デバイスの SSL ハードウェア アクセラレーションが自動的に有効になります。トラフィックを復号せずに SSL ハードウェア アクセラレーションを使用すると、パフォーマンスに影響を与えることがあります。トラフィックを復号しないデバイスでは SSL ハードウェア アクセラレーションを無効にすることをお勧めします。 サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300

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

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

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

機能	詳細
ユニファイド syslog の設定	**アップグレードの影響。** バージョン 6.3.0 では、システムが Syslog を介して接続イベントと侵入イベントをログに記録する方法が変更され、一元化されています。 以前は、イベントのタイプに応じて、複数の場所で syslog を使用してイベント ロギングを設定していました。アクセス コントロール ポリシーで syslog メッセージングを設定できるようになりました。これらの設定は、アクセス制御、SSL、プレフィルタ、侵入ポリシーのほか、セキュリティ インテリジェンスの接続入イベントと侵入イベントのロギングに影響を与えます。 アップグレードによって接続イベント ログの既存の設定が変更されることはありません。ただし、Syslog 経由では「期待されなかった」侵入イベントの受信が突然開始される可能性があります。これは、侵入ポリシーがアクセス コントロール ポリシーで指定された宛先に syslog イベントを送信するようになったためです。（以前は、外部ホストではなく、管理対象デバイス自体の syslog にイベントを送信するように侵入ポリシーで syslog アラートを設定できました）。 FTD デバイスでは、一部の syslog プラットフォーム設定が接続イベントと侵入イベントのメッセージに適用されるようになりました。リストについては、FMC コンフィギュレーション ガイドで「*Firepower Threat Defense* のプラットフォーム設定」の章を参照してください。 NGIPS デバイス（7000/8000 シリーズ、ASA FirePOWER、NGIPSv）については、RFC 5425 で指定されている ISO 8601 タイムスタンプ形式が使用されるようになりました。 サポートされるプラットフォーム：すべて
接続イベントと侵入イベントの完全な syslog メッセージ	接続イベント、セキュリティ インテリジェンス イベント、および侵入イベントの syslog メッセージの形式には、次のような変更があります。 • FTD デバイスからのメッセージに、イベントタイプ ID 番号が含まれるようになりました。 • 空の値または不明な値を持つフィールドは含まれなくなったため、メッセージが短くなり、重要なデータが切り捨てられる可能性が低くなります。 • タイムスタンプでは、RFC 5425 syslog 形式で指定された ISO 8601 タイムスタンプ形式が使用されるようになりました（FTD の場合はオプションで、従来の場合は必須）。 サポートされるプラットフォーム：すべて
FTD デバイスのその他の syslog の改善	TCP または UDP プロトコルを使用して、同じ IP アドレスを介して、同じインターフェイス（データまたは管理）からすべての syslog メッセージを送信できます。セキュアな syslog はデータ ポートでのみサポートされていることに注意してください。また、メッセージのタイムスタンプに RFC 5424 形式を使用することもできます。 サポートされるプラットフォーム：FTD

機能	詳細
管理とトラブルシューティング	
承認された顧客向けのエクスポート管理機能	スマートアカウントで制限付き機能を使用する資格を持たない顧客は、期間ベースのライセンスを承認を受けて購入することができます。 新規/変更されたページ：**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** サポートされるプラットフォーム：FMC、FTD
承認された顧客向けの特定のライセンス予約	顧客は特定のライセンスの予約機能を使用して、エアギャップネットワークにスマートライセンスを展開できます。FMC は、Cisco Smart Software Manager または Smart Software サテライトサーバーにアクセスせずに、指定した期間中に仮想アカウントからライセンスを予約します。 新規/変更されたページ：**[システム（System）]** > **[ライセンス（Licenses）]** > **[特定のライセンス（Specific Licenses）]** サポートされるプラットフォーム：FMC、FTD（ISA 3000 を除く）
SNMP ホストの IPv4 範囲、サブネット、および IPv6 のサポート	IPv4 範囲、IPv4 サブネット、および IPv6 ホスト ネットワーク オブジェクトを使用して、Firepower Threat Defense デバイスにアクセスできる SNMP ホストを指定できるようになりました。 新規/変更されたページ：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]**> [FTD ポリシーの作成または編集（create or edit FTD policy）] > [SNMP] > [ホスト（Hosts）] タブ サポートされるプラットフォーム：FTD
完全修飾ドメイン名（FQDN）を使用したアクセス制御	完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを作成して、これらのオブジェクトをアクセス制御ルールとプレフィルタ ルールで使用できるようになりました。FQDN オブジェクトを使用するには、DNS サーバー グループと DNS プラットフォームも設定して、システムがドメイン名を解決できるようにする必要があります。 新規/変更されたページ： • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[ネットワーク（Network）]** • **[オブジェクト（Objects）]**> **[オブジェクト管理（Object Management）]**> **[DNSサーバーグループ（DNS Server Group）]** • **[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > [FTDポリシーの作成または編集（create or edit FTD policy）] > [DNS] サポートされるプラットフォーム：FTD

機能	詳細
FMC の CLI	FMC の CLI では、いくつかの基本的なコマンド（パスワードの変更、バージョンの表示、再起動など) がサポートされています。デフォルトでは、FMC CLI は無効になっており、SSH を使用して FMC にログインすると、Linux シェルにアクセスします。 新規/変更されたクラシック CLI コマンド：**system lockdown-sensor** コマンドは **system lockdown** に変更されています。このコマンドは、デバイスと FMC の両方で動作するようになりました。 新規/変更されたページ：**[システム（System）]** > **[設定（Configuration）]** > **[コンソール設定（Console Configuration）]** > **[CLI アクセスの有効化（Enable CLI Access）]** チェックボックス サポートされるプラットフォーム：FMC（FMCv を含む）
デバイス設定のコピー	デバイス設定とポリシーを 1 つのデバイスから別のデバイスにコピーできます。 新規/変更されたページ：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > [デバイスの編集（edit the device）] > [全般（General）] 領域 > [デバイス設定の取得/プッシュ（Get/Push Device Configuration）] アイコン サポートされるプラットフォーム：FMC
FTD デバイス設定のバックアップ/復元	FMC Web インターフェイスを使用して、一部の FTD デバイスの設定をバックアップできます。 新規/変更されたページ：**[システム（System）]** > **[ツール（Tools）]** > **[バックアップ/復元（Backup/Restore）]** 新規/変更された CLI コマンド： **restore** サポートされるプラットフォーム：すべての物理 FTD デバイス、VMware 向け FTDv
展開タスクをスケジュールするときに最新のデバイスへの展開をスキップ	**アップグレードの影響。** 設定変更を展開するタスクをスケジュールするときに、**最新のデバイスへの展開をスキップする**ことを選択できるようになりました。このパフォーマンス強化設定はデフォルトで有効になっています。 アップグレードプロセスでは、既存のスケジュール済みタスクでこのオプションが自動的に有効になります。スケジュールされた展開を最新のデバイスに強制的に適用するには、スケジュールされたタスクを編集する必要があります。 新規/変更されたページ：**[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]** > [タスクの追加または編集（add or edit a task）] で [展開ポリシー（Deploy Policies）] の [ジョブタイプ（Job Type）] を選択 サポートされるプラットフォーム：FMC

機能	詳細
新しいヘルス モジュール	新しいヘルス モジュールは、次の場合にアラートを表示します。 • **デバイスでの脅威データの更新**：管理対象デバイスで脅威特定データの更新に失敗しました。 • **レルム**：ユーザーがダウンロードされずに、FMC にレポートされたか、または、FMC が認識していないレルムに対応するドメインにユーザーがログインしました。 新規/変更されたページ： • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]** • **[システム（System）] > [ヘルス（Health）] > [モニター（Monitor）]** サポートされるプラットフォーム：FMC
設定可能なパケット キャプチャ サイズ	最大 10 GB のパケット キャプチャを保存できるようになりました。 新規/変更された CLI コマンド：**file-size**、**show capture** サポートされるプラットフォーム：Firepower 4100/9300

機能	詳細
Web インターフェイスの変更。	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。 **[分析（Analysis）] > [詳細（Advanced）] > [Whois]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [Whois]** **[分析（Analysis）] > [詳細（Advanced）] > [位置情報（Geolocation）]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [位置情報（Geolocation）]** **[分析（Analysis）] > [詳細（Advanced）] > [URL]** は次に変更されました。 **[分析（Analysis）] > [検索（Lookup）] > [URL]** **[分析（Analysis）] > [詳細（Advanced）] > [カスタムワークフロー（Custom Workflows）]** は次に変更されました。 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムワークフロー（Custom Workflows）]** **[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]** は次に変更されました。 **[分析（Analysis）] > [カスタム（Custom）] > [カスタムテーブル（Custom Tables）]** **[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）]** は次に変更されました。 **[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）]** **[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）]** は次に変更されました。 **[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third Party Vulnerabilities）]**
セキュリティと強化	

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

機能	詳細
How-To ウォークスルー	デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。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。 （注） FMC ウォークスルーは Firefox および Chrome ブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。 次に、一般的な問題点と解決策をいくつか示します。 • **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。 **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。 • **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。 **解決策**：ウォークスルーを終了します。 • **問題**：ウォークスルーが突然消えたり終了したりする。 **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。 • **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）。 **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。
Firepower Management Center REST API	
新しい REST API サービス	次の機能をサポートするために、REST API サービスが追加されました。 • サイト間 VPN トポロジ：ftds2svpns、endpoints、ipsecsettings、advancedsettings、ikesettings、ikev1ipsecproposals、ikev1policies、ikev2ipsecproposals、ikev2policies • HA デバイスフェールオーバー：failoverinterfacemacaddressconfigs、monitoredinterfaces サポートされるプラットフォーム：FMC

機能	詳細
バルク オーバーライド	特定のオブジェクトに対してバルク オーバーライドを実行できるようになりました。完全なリストについては、『Cisco Firepower Management Center REST API Quick Start Guide』を参照してください。

廃止された機能

表 *34 : FMC* バージョン *6.3.0* で廃止された機能

機能	詳細
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：復号化のための EMS 拡張機能のサポート（一時的）。	**アップグレードの影響。** 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。 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。 サポートはバージョン 6.3.0.1 で再導入されています。
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。	**アップグレードの影響。** 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。

機能	詳細
廃止：FlexConfig を使用したデフォルトの DNS グループ。	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。 • Default_DNS_Configure 関連するテキストオブジェクト： • defaultDNSNameServerList • defaultDNSParameters これらによって、デフォルト DNS グループを設定できました。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバーを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。 FTD プラットフォーム設定ポリシーで、データインターフェイスの DNS を設定できるようになりました（**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > [FTD ポリシーの作成または編集（Create or edit FTD policy）] > [DNS]）。
廃止：FlexConfig を使用した初期接続制限およびタイムアウト。	**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。** 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。 • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 関連するテキストオブジェクト： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout これらによって、初期接続制限およびタイムアウトを設定して SYN フラッドサービス妨害（DoS）攻撃から保護できました。 FTD サービスポリシーでこれらの機能を設定できるようになりました（**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > [ポリシーの追加/編集（add/edit policy）] > [詳細（Advanced）] タブ > [Threat Defense サービスポリシー（Threat Defense Service Policy）]）。 **注意** **set connection** コマンドを使用して接続関連サービスルールを実装した場合は、関連付けられたオブジェクトを削除し、FTD サービスポリシーを使用して機能を実装する必要があります。これを行わないと、展開の問題が発生する可能性があります。

機能	詳細
廃止：地理位置情報の詳細。	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。 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。 **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。

バージョン 6.2.3 の FMC 機能

新機能

表 *35 : FMC* バージョン *6.2.3* パッチの新機能

機能	詳細
バージョン 6.2.3.13 FTD NAT ポリシーでのルールの競合の検出	バージョン 6.2.3.13 以降にアップグレードすると、競合するルール（重複ルールまたはオーバーラップルールとも呼ばれます）を持つ FTD NAT ポリシーを作成できなくなります。これは、競合する NAT ルールが順序どおりに適用されていなかった問題を修正するものです。 現在競合している NAT ルールがある場合は、アップグレード後に展開することができます。ただし、NAT ルールは引き続き順序どおりに適用されません。 そのため、アップグレード後に FTD NAT ポリシーを調べることをお勧めします。それには、ポリシーを編集して再保存を試みます（変更は必要ありません）。ルールが競合している場合は保存ができません。問題を修正して保存し、それから展開します。 （注） バージョン 6.3.0 または 6.4.0 にアップグレードすると、この修正が無効になります。この問題は、バージョン 6.3.0.4 および 6.4.0.2 では対処されています。 サポートされるプラットフォーム：FTD
バージョン 6.2.3.8 EMS 拡張機能のサポート	[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポートし、よりセキュアな通信が可能になりました。EMS 拡張機能は、RFC 7627 によって定義されています。 （注） バージョン 6.2.3.8 は 2019 年 1 月 7 日にシスコ サポートおよびダウンロードサイトから削除されました。バージョン 6.2.3.9 にアップグレードすると、EMS 拡張機能のサポートも有効になります。バージョン 6.3.0 では EMS 拡張機能のサポートが中止されています。FMC 展開では、この機能は、デバイスのバージョンによって異なります。FMC をバージョン 6.3.0 にアップグレードしてもサポートは中止されませんが、デバイスをアップグレードすると中止されます。サポートはバージョン 6.3.0.1 で再導入されています。 サポートされるプラットフォーム：すべて

機能	詳細
バージョン 6.2.3.7 FTD の TLS v1.3 ダウングレード CLI コマンド	新しい CLI コマンドを使用すると、TLS v1.3 接続を TLS v1.2 にダウングレードするタイミングを指定できます。 多くのブラウザでは、デフォルトで TLS v1.3 が使用されています。暗号化されたトラフィックを処理するために SSL ポリシーを使用していて、モニター対象ネットワーク内のユーザーが TLS v1.3 を有効にしてブラウザを使用している場合、TLS v1.3 をサポートする Web サイトのロードに失敗します。 詳細については、Cisco 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 に問い合わせてから使用することをお勧めします。 サポートされるプラットフォーム：FTD
バージョン 6.2.3.3 クラスタリングを使用したサイト間 VPN	クラスタリングを使用してサイト間 VPN を設定できるようになりました。サイト間 VPN は、中央集中型機能です。制御ユニットのみが VPN 接続をサポートします。 サポートされるプラットフォーム：Firepower 4100/9300

表 *36 : FMC* バージョン *6.2.3* の新機能

機能	詳細
プラットフォーム	
ISA 3000 の FTD。	ISA 3000 シリーズで FTD を実行できるようになりました。 ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。ハードウェアバイパスやアラームポートなど、ASA でサポートされていた ISA 3000 の特別な機能は、このリリースの FTD ではサポートされていません。
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**	
Firepower 4100/9300 の SSL ハードウェア アクセラレーション	FTD を搭載した Firepower 4100/9300 は、パフォーマンスが大幅に向上する、ハードウェアでの SSL 暗号化および復号のアクセラレーションをサポートするようになりました。SSL ハードウェア アクセラレーションは、サポートするすべてのアプライアンスに対してデフォルトで無効化されています。 （注） この機能は、バージョン 6.4.0 以降では TLS 暗号化アクセラレーションに名前が変更されました。 サポートされるプラットフォーム：Firepower 4100/9300

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

機能	詳細

FTDのハイアベイラビリティのハードニング	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。
	• 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 [アクティブピアの切り替え（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。
	  • **DELETE ftddevicehapairs**
	  • **PUT ftddevicehapairs**
	  • **POST ftddevicehapairs**
	  • **GET ftddevicehapairs**

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	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。 サポート対象プラットフォーム：FMC
FTD SSH アクセス用に追加された外部認証	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。 新規/変更された画面：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[外部認証（External Authentication）]** サポートされるプラットフォーム：FTD

機能	詳細
脆弱性データベース（VDB）の強化されたインストール	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。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、または Firepower ソフトウェア アップグレードの一部として、VDB がバックグラウンドでインストールされる場合。 サポートされるプラットフォーム：FMC
アップグレード パッケージのプッシュ	実際のアップグレードを実行する前に、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。 高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。 新規/変更された画面：**[システム（System）] > [更新（Updates）]** サポートされるプラットフォーム：FMC
FTD サービスアビリティ	バージョン 6.2.3 では、 **show fail over** CLI コマンドが改善されています。新しいキーワード **-history** を使用すると、トラブルシューティングに役立つ詳細が表示されます。 • **Show fail over history** は、失敗の理由に加えて、その具体的な詳細を表示します。 • **Show fail over history details** は、ピア ユニットのフェールオーバー履歴を表示します。 （注） このコマンド出力には、フェールオーバーでのピア ユニットの状態変化や、その状態変化の理由が含まれます。 サポートされるプラットフォーム：FTD

機能	詳細
デバイス一覧のソート	**[Devices]** > **[Devices Management]** ページで、[View by] ドロップダウンリストを使用して、グループ、ライセンス、モデル、またはアクセス コントロール ポリシーのいずれかのカテゴリでデバイス一覧をソートして表示できます。マルチドメイン導入では、ドメイン（その導入のデフォルトの表示カテゴリ）を基準にソートして表示することもできます。デバイスはリーフ ドメインに属している必要があります。 サポートされるプラットフォーム：FMC
監査ログの改善	監査ログは、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。 サポートされるプラットフォーム：FTD を搭載した FMC
FTD CLI コマンドの更新	FTD デバイスの CLI コマンドの **asa_mgmt_plane** オプションと **asa_dataplane** オプションは、**management-plane** と **data-plane** にそれぞれ名前が変更されています。 サポートされるプラットフォーム：FTD
Cisco Success Network	**アップグレードの影響。** Cisco Success Network は、テクニカル サポートを提供するために不可欠な使用状況に関する情報と統計情報をシスコに送信します。 初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。 サポート対象プラットフォーム：FMC
Web 分析トラッキング	**アップグレードの影響。** 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。 初期設定では、デフォルトで Web 分析トラッキングに登録されますが、その後はいつでも登録を変更できます。アップグレードでは、Web 分析トラッキングに登録または再登録することもできます。 サポート対象プラットフォーム：FMC
パフォーマンス	
FTD デバイスの Snort の再起動が減少	バージョン 6.2.3 では、FTD 設定の変更による、FTD デバイスの Snort プロセスの再起動が減少します。 FMC では、設定の展開により Snort プロセスが再起動し、トラフィック検査が中断され、管理対象デバイスでのトラフィック処理方法によってはトラフィックフローが中断される可能性がある場合、展開の前に、警告が出されるようになりました。 サポートされるプラットフォーム：FTD

機能	詳細
ポリシー適用時のトラフィック ドロップ	バージョン 6.2.3 では、**configure snort preserve-connection {enable | disable}** コマンドが 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。 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。
ローエンド アプライアンスのメモリ容量の増加	バージョン 6.1.0.7、6.2.0.5、6.2.2.2、および 6.2.3 では、Firepower ローエンド アプライアンスのメモリ容量が増加しています。これにより、ヘルス アラートの数が削減されます。
ISE pxGrid ディスカバリの高速化	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。
レポートの結果の新しい制限。	**アップグレードすることで、レポートの設定を変更できます。** バージョン 6.2.3 では、使用できる、またはレポートセクションに含めることができる結果の数が制限されています。テーブルおよび詳細ビューでは、PDF レポートに HTML または CSV レポートよりも少ないレコードを含めることができます。 HTML または CSV レポートセクションの新しい制限は次のとおりです。 • 棒グラフと円グラフ：100（上部または下部） • テーブルビュー：400,000 • 詳細ビュー：1,000 PDF レポートセクションの新しい制限は次のとおりです。 • 棒グラフと円グラフ：100（上部または下部） • テーブルビュー：100,000 • 詳細ビュー：500 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。 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。

機能	詳細
Firepower Management Center REST API	
FMC REST API の改善	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。 NAT 用に新しく導入された API • NAT ルール • FTD NAT ポリシー • 自動 NAT ルール • 手動 NAT ルール 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。 スタティック ルート用に新しく導入された API • IPv4 スタティック ルート • IPv6 スタティック ルート • SLA モニター

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

機能	詳細
AMP for Networks による動的分析用の期限切れ CA 証明書。	2018 年 6 月 15 日、一部の Firepower 展開では、動的分析のためにファイルを送信できなくなりました。これは、AMP Threat Grid クラウドとの通信に必要だった CA 証明書が期限切れになったために発生しました。バージョン 6.3 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。 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。 • 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 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。 パッチまたはホットフィックスを初めてインストールする場合は、ファイアウォールで、FMC とその管理対象デバイスの両方から `fmc.api.threatgrid.com`（`panacea.threatgrid.com` を置き換える）へのアウトバウンド接続が許可されていることを確認してください。 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。

機能	詳細
廃止：地理位置情報の詳細。	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。 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。 **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。

リリース日

表 *38* : バージョン *7.4* 日付

バージョン	ビルド	日付	プラットフォーム
7.4.1	172	2023 年 12 月 13 日	すべて
7.4.0	81	2023 年 9 月 7 日	Management center Cisco Secure Firewall 4200 シリーズ

表 *39* : 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
7.3.1.1	83	2023 年 8 月 24 日	すべて
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 *40* : 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
7.2.6	167	2024-03-19	すべて
7.2.5.1	29	2023 年 11 月 14 日	すべて
7.2.5	208	2023-07-27	すべて（All）
7.2.4.1	43	2023-07-27	すべて（All）
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 *41* : 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 *42* : 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
7.0.6.1	36	2023 年 11 月 13 日	すべて
7.0.6	236	2023-07-18	すべて（All）
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 *43* : 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

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

表 *44* : 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 *45* : 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 *46* : 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
6.4.0.17	26	2023 年 9 月 28 日	すべて（All）
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）

バージョン	ビルド	日付	プラットフォーム
6.4.0.11	11	2021 年 1 月 11 日	すべて（All）
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 *47* : 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 *48 :* 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	—	—
	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 *49 :* 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。