特長と機能

Firepower バージョン 6.5.0 には以下が含まれます。

新機能

次のトピックでは、Firepower バージョン 6.5.0 で使用可能な新機能をリストしています。アップグレード パスが 1 つ以上のメジャー バージョンをスキップする場合は、『Cisco Firepower リリース ノート』で過去の新機能リストを参照してください。

Firepower Management Center/バージョン 6.5.0 の新機能

次の表に、Firepower Management Center を使用して設定された場合に Firepower バージョン 6.5.0 で使用できる新機能を示します。

表 *1* : バージョン *6.5.0* の新機能：*FMC* 導入環境

機能	説明
ハードウェアと仮想ハードウェア	
Firepower 1150 上の FTD	Firepower 1150 が導入されました。
Azure 上の FTDv がより大規模なインスタンスに対応	Microsoft Azure に導入した Firepower Threat Defense Virtual で、より大規模なインスタンス D4_v2 および D5_v2 がサポートされるようになりました。

機能	説明
VMware 上の FMCv 300	より大規模な Firepower Management Center Virtual for VMware 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	
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/変更された画面： • **[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）] > [PoE] サポートされるプラットフォーム：Firepower 1010

機能	説明
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 に一度に 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/変更された画面：**[デバイス（Devices）]** > **[NAT]** > FTD NAT ポリシーの追加/編集 > NAT ルールの追加/編集 > [PAT プール（PAT Pool）] タブ > [ブロック割り当て（Block Allocation）] オプション サポートされているプラットフォーム：すべてのFTDデバイス
Firepower 4100/9300 上の複数のコンテナインスタンスの TLS 暗号化アクセラレーション	Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。 新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることは「ありません」。代わりに、**create hw-crypto** および **scope hw-crypto** CLI コマンドを使用してください。詳細については、『Cisco Firepower 4100/9300 FXOS Command Reference』を参照してください。 新しい FXOS CLI コマンド： • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** 削除された FXOS CLI コマンド： • **show hwCrypto**（**show hw-crypto** に置き換えられました） • **config hwCrypto** 削除された FTD CLI コマンド： • **show crypto accelerator status** サポートされるプラットフォーム：Firepower 4100/9300
アクセス制御とイベント分析	

機能	説明
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/変更された画面：[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
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/変更された画面： • [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

機能	説明
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/変更された画面：[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
Cisco Firepower User Agent バージョン 2.5 の統合	Firepower バージョン 6.4.0 および 6.5.0 と統合できる Cisco Firepower User Agent バージョン 2.5 がリリースされました。 （注） Cisco Firepower User Agent ソフトウェアとアイデンティティソースについてはサポートの終了が予定されています。今すぐ Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えてください。これにより、ユーザエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。 詳細については、「Cisco Firepower Management Center Configuration Guides」ページで該当する *Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド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

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

機能	説明
設定できるドメイン数の増加（マルチテナンシー）	マルチテナンシーを実装する（管理対象デバイス、設定、およびイベントへのユーザアクセスをセグメント化する）場合、最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 個のサブドメインを作成できます。以前は、最大で 50 ドメインでした。 サポートされるプラットフォーム： FMC
ISE 接続ステータスのモニタの機能拡張	[ISE接続ステータスのモニタ（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	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/変更された画面：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] サポートされているプラットフォーム：FMC、FTD
Cisco Support Diagnostics	*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 TAC は TAC 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。 アップグレードおよび再イメージ化中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。 現時点では、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/変更された画面： • **[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 および管理対象の Firepower 4100/9300

機能	説明
FMC モデル移行	バックアップおよび復元機能を使用して、FMC が同じモデルでない場合でも、FMC 間で設定とイベントを移行できるようになりました。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による FMC の交換が容易になります。 一般に、ローエンドの FMC からハイエンドの FMC に移行することはできますが、その逆に移行することはできません。KVM および Microsoft Azure からの移行はサポートされていません。また、Cisco Smart Software Manager（CSSM）への登録を解除して再登録する必要があります。 サポート対象の移行先モデルなどの詳細については、『Firepower Management Center モデル移行ガイド』を参照してください。 サポートされるプラットフォーム： FMC
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 FTD を搭載した Firepower 4100/9300 シリーズ
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 ユーザを除き（これには `admin` ユーザが含まれます）、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 ユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。 サポートされるプラットフォーム： FMC

機能	説明
同時ユーザセッション数の制限	FMC に同時にログインできるユーザ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の同時セッション数を制限できます。CLI ユーザは、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/変更された画面：[システム（System）] > [設定（Configuration）] > [ユーザ設定（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	SHA1 または MD5 対称キー認証を使用して FMC と NTP サーバとの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/変更された画面：[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	

機能	説明
初期設定の改善	新規および再イメージ化された FMC では、以前の初期設定プロセスがウィザードに置き換えられます。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、毎週にスケジュール設定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『Getting Started Guide』を参照してください。スケジュールされたタスクの詳細については、『Firepower Management Center Configuration Guide』を参照してください。 サポートされるプラットフォーム： FMC

機能	説明
FMC Web インターフェイスのライトテーマ（試験版）	システムはデフォルトでクラシックテーマになっていますが、試験版の「ライト」テーマを選択することもできます。 （注） ライトテーマは試験版であるため、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/変更された画面：ユーザ名の下にあるドロップダウンリストの [ユーザ設定（User Preferences）] サポートされるプラットフォーム： FMC

機能	説明
オブジェクトの表示に関するユーザビリティの拡張	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/変更された画面： • [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/変更された画面：[要求された展開のエラーと警告（Errors and Warnings for Requested Deployment）]ダイアログボックス サポートされるプラットフォーム： FMC

機能	説明
FTD NAT ポリシー管理に関するユーザビリティの拡張	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/変更された画面：[デバイス（Devices）] > [NAT] > FTD NAT ポリシーの作成または編集 > [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
FMC REST API	
新しい REST API 機能	バージョン 6.5.0 の機能をサポートするための次の REST API オブジェクトを追加しました。 • cloudregions：地域クラウド 古い機能をサポートするための次の REST API オブジェクトを追加しました。 • categories：アクセスコントロールルールのカテゴリ • domain、inheritancesettings：ドメインとポリシーの継承 • prefilterpolicies、prefilterrules、tunneltags：プレフィルタポリシー • vlaninterfaces：VLAN インターフェイス サポートされるプラットフォーム： FMC

Firepower Device Manager/FTD バージョン 6.5.0 の新機能

リリース：2019 年 9 月 26 日

次の表は、Firepower Device Manager を使用して設定した場合に、FTD 6.5.0 で使用可能な新機能を示しています。

機能	説明
Firepower 4100/9300 での FDM のサポート。	FDM を使用して、Firepower 4100/9300 で Firepower Threat Defense を設定できるようになりました。ネイティブインスタンスのみがサポートされています。コンテナインスタンスはサポートされていません。
Microsoft Azure クラウド用 Firepower Threat Defense 仮想での FDM のサポート。	Firepower Device Manager を使用して、Microsoft Azure クラウド用 Firepower Threat Defense 仮想 で Firepower Threat Defense を設定できます。
Firepower 1150 でのサポート。	Firepower 1150 用の FTD が導入されました。
Firepower 1010 ハードウェアスイッチのサポート、PoE+ のサポート。	Firepower 1010 では、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通常のファイアウォール インターフェイスとして設定できます。各スイッチポートを VLAN インターフェイスに割り当てます。Firepower 1010 は、Ethernet1/7 と Ethernet 1/8 での Power over Ethernet+（PoE+） もサポートしています。 デフォルト設定で、Ethernet1/1 が外部として設定され、Ethernet1/2 ～ 1/8 が内部 VLAN1 インターフェイスのスイッチポートとして設定されるようになりました。バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。
インターフェイスのスキャンと置き換え。	インターフェイススキャンでは、シャーシ上で追加、削除、または復元されたインターフェイスが検出されます。設定で古いインターフェイスを新しいインターフェイスに置き換えることもできるため、インターフェイスの変更がシームレスに行えます。
インターフェイス表示の向上。	**[デバイス（Device）]**>**[インターフェイス（Interfaces）]** ページの構成が改められました。物理インターフェイス、ブリッジグループ、EtherChannel、および VLAN 用のタブが別々に設けられました。任意の対象デバイスモデルについて、モデルに関連するタブのみが表示されます。たとえば、[VLAN] タブは Firepower 1010 モデルでのみ使用できます。また、各インターフェイスの設定と使用方法に関する詳細情報がリストに表示されます。

機能	説明
ISA 3000 の新しいデフォルト設定。	ISA 3000 のデフォルト設定が次のように変更されました。 • すべてのインターフェイスが BVI1 のブリッジグループメンバーとなりました。BVI1 には名前が付いていないため、ルーティングには参加しません。 • GigabitEthernet1/1 および 1/3 は外部インターフェイスで、GigabitEthernet1/2 および 1/4 は内部インターフェイスです。 • 内部/外部ペアごとにハードウェアバイパスが有効になります（使用可能な場合）。 • すべてのトラフィックについて、内部から外部、および外部から内部が許可されます。 バージョン 6.5 にアップグレードしても既存のインターフェイス設定が保持されます。
ASA 5515-X のサポートが終了します。最後にサポートされるリリースは FTD 6.4 です。	ASA 5515-X に FTD 6.5 をインストールすることはできません。ASA 5515-X 用に最後にサポートされるリリースは FTD 6.4 です。
Cisco ISA 3000 デバイスのアクセス制御ルールにおける Common Industrial Protocol（CIP）および Modbus アプリケーション フィルタリングのサポート。	Cisco ISA 3000 デバイスで Common Industrial Protocol（CIP）および Modbus プリプロセッサを有効にし、CIP および Modbus アプリケーションのアクセス制御ルールでフィルタを有効にすることができます。CIP アプリケーションの名前はすべて、CIP Write というように「CIP」で始まります。Modbus 用のアプリケーションは 1 つだけです。 プリプロセッサを有効にするには、CLI セッション（SSH またはコンソール）でエキスパートモードに移行し、**sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}** コマンドを発行する必要があります。展開後にプリプロセッサがオフになるため、展開のたびにこのコマンドを発行する必要があります。

機能	説明
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** および **igmp**（インターフェイスモード）コマンド、およびグローバルコマンド **ptp mode e2etransparent** と **ptp domain** を追加できるようになりました。また、FTD CLI に **show ptp** コマンドが追加されました。
EtherChannel（ポートチャネル）インターフェイス。	EtherChannel インターフェイス（ポートチャネルとも呼ばれます）を設定できます。 （注） FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス（Interfaces）] ページに表示されます。 **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページが更新され、EtherChannel の作成ができるようになりました。
FDM からシステムを再起動およびシャットダウンする機能。	新しい [再起動/シャットダウン（Reboot/Shutdown）] システム設定ページからシステムを再起動またはシャットダウンできるようになりました。以前は、FDM の CLI コンソールを使用して、あるいは SSH またはコンソールセッションから、**reboot** および **shutdown** コマンドを発行する必要がありました。これらコマンドを使用するには、管理者権限が必要です。
FDM CLI コンソールでの **failover** コマンドのサポート。	FDM CLI コンソールで **failover** コマンドを発行できるようになりました。
スタティックルート用のサービスレベル契約（SLA）モニタ。	スタティックルートとともに使用するためのサービスレベル契約（SLA）モニタオブジェクトを設定します。SLA モニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。SLA モニタオブジェクトを選択できるように、[オブジェクト（Object）] ページに [SLA モニタ（SLA Monitors）] を追加し、スタティックルートを更新しました。

機能	説明
Smart CLI および FTD API でのルーティングの変更。	今回のリリースには、Smart CLI および FTD API でのルーティング設定に対していくつかの変更が追加されています。以前のリリースでは、BGP 用として単一の Smart CLI テンプレートがありました。今回は、BGP（ルーティングプロセス設定）用と BGP 一般設定（グローバル設定）用に別々のテンプレートが用意されました。 FTD API では、新しい BGP 一般設定のメソッドを除いて、すべてのメソッドのパスが変更され、パスに「/virtualrouters」が挿入されました。 • スタティックルートメソッドのパスは、以前は /devices/default/routing/{parentId}/staticrouteentries でしたが、今後は /devices/default/routing/virtualrouters/default/staticrouteentries になります。 • BGP メソッドは、/devices/default/routing/bgpgeneralsettings と /devices/default/routing/virtualrouters/default/bgp の 2 つの新しいパスに分割されました。 • OSPF パスは、/devices/default/routing/virtualrouters/default/ospf と /devices/default/routing/virtualrouters/default/ospfinterfacesettings になりました。 FTD API を使用してルーティングプロセスを設定している場合は、コールを調べて必要に応じて修正してください。

機能	説明
新しいURLカテゴリおよびレピュテーション データベース。	システムは、Cisco Talos とは別の URL データベースを使用します。新しいデータベースでは、URL のカテゴリにいくつかの違いがあります。アップグレードすると、もう存在していないカテゴリがアクセス制御や SSL 復号ルールで使用されている場合、システムはそのカテゴリを適切な新しいカテゴリに置き換えます。変更を有効にするには、アップグレード後に設定を展開します。カテゴリの変更についての詳細は、[保留中の変更（Pending Changes）] ダイアログに表示されます。引き続き希望する結果が得られることを確認するため、URL フィルタリングポリシーを調べることもできます。 アクセス制御ポリシーと SSL 復号ポリシーの [URL] タブ、および **[デバイス（Device）] > [システム設定（System Settings）] > [URLフィルタリング設定（URL Filtering Preferences）]** ページに URL ルックアップ機能を追加しました。この機能を使用すると、特定の URL に割り当てられているカテゴリを確認できます。同意しない場合は、カテゴリの異議を送信するリンクもあります。このどちらの機能も、URL に関する詳細情報を提供する外部 Web サイトを使用します。
セキュリティ インテリジェンスでは、ホスト名ではなく IP アドレスを使用する URL 要求に対して IP アドレスの評価が使用されます。	HTTP/HTTPS 要求の宛先が、ホスト名ではなく IP アドレスを使用する URL である場合は、ネットワークアドレスリストにある IP アドレスの評価が検索されます。ネットワークおよび URL リストで IP アドレスを重複させる必要はありません。これにより、エンドユーザがプロキシを使用してセキュリティ インテリジェンスの評価のブロックを回避することが困難になります。
接続イベントおよび優先度の高い侵入/ファイル/マルウェア関連イベントを Cisco Cloud に送信するためのサポート。	Cisco Cloud サーバにイベントを送信できます。このサーバから、各種のシスコ クラウドサービスがイベントにアクセスできます。次に、Cisco Threat Response などのクラウドアプリケーションを使用して、イベントを分析したり、デバイスが遭遇した可能性のある脅威を評価したりできます。このサービスを有効にすると、デバイスから、接続イベントおよび優先度の高い侵入/ファイル/マルウェア関連イベントが Cisco Cloud に送信されます。 **[デバイス（Device）] > [システム設定（System Settings）] > [クラウドサービス（Cloud Services）]** にある Cisco Threat Response の項目を「Cisco Cloudにイベントを送信（Send Events to the Cisco Cloud）」に変更しました。

機能	説明
シスコ クラウドサービスのリージョンサポート。	スマートライセンスへの登録時に、シスコ クラウドサービスリージョンの選択が求められるようになりました。このリージョンは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Cloud を通過するすべてのクラウド機能で使用されます。登録済みデバイスを以前のリリースからアップグレードすると、自動的に US リージョンに割り当てられます。リージョンを変更する必要がある場合は、スマートライセンスを登録解除して、改めて再登録して新しいリージョンを選択する必要があります。 [スマートライセンス（Smart License）] ページと初期デバイス セットアップ ウィザードで、ライセンス登録プロセスにステップを追加しました。また、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウドサービス（Cloud Services）]** ページでもリージョンを確認できます。
FTD REST API バージョン 4（v4）。	ソフトウェアバージョン 6.5 用の FTD REST API のバージョン番号が 4 になりました。API の URL の v1/v2/v3 を v4 に置き換える必要があります。v4 の API には、ソフトウェアバージョン 6.5 で追加されたすべての機能に対応する多数の新しいリソースが含まれています。使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[詳細オプション（More options）] ボタン（⋮）をクリックし、[API エクスプローラ（API Explorer）] を選択します。

機能	説明
FTD アクセス制御ルールで送信元および宛先の一致基準として使用できる TrustSec セキュリティ グループの API サポート。	FTD API を使用して、送信元または宛先のトラフィックの一致基準に TrustSec セキュリティグループを使用したアクセス コントロール ポリシー ルールを設定できます。ISE からセキュリティグループタグ（SGT）のリストがダウンロードされます。SXP の更新がないかをリッスンし、スタティック SGT から IP アドレスへのマッピングを取得するように、システムを設定できます。 GET /object/securitygrouptag メソッドを使用して、ダウンロードしたタグのリストを表示でき、SGTDynamicObject リソースを使用して 1 つ以上のタグを表す動的オブジェクトを作成できます。この動的オブジェクトをアクセス制御ルールで使用して、送信元または宛先のセキュリティ グループに基づくトラフィックの一致基準を定義できます。 セキュリティ グループに関連する ISE オブジェクトまたはアクセス制御ルールに変更を加えると、FDM でそれらのオブジェクトを編集しても変更が保持されます。ただし、FDM でルールを編集する場合、アクセスルールのセキュリティグループの基準を表示することはできません。API を使用してセキュリティグループに基づくアクセスルールを設定する場合は、その後で FDM を使用してアクセス コントロール ポリシーのルールを編集する際に注意が必要です。 AccessRule（sourceDynamicObjects および destinationDynamicObjects 属性）、IdentityServicesEngine（subscribeToSessionDirectoryTopic および subscribeToSxpTopic 属性）、SecurityGroupTag、SGTDynamicObject の各 FTD API リソースを追加または変更しました。 イベントビューアに、送信元と宛先のセキュリティグループタグと名前を列として追加しました。

機能	説明
FTD API を使用した設定のインポート/エクスポート。	FTD API を使用して、デバイス設定のエクスポートや設定ファイルのインポートを行えます。設定ファイルを編集して、インターフェイスに割り当てられている IP アドレスなどの値を変更できます。したがって、インポート/エクスポートを使用して新しいデバイス用のテンプレートを作成できます。そのため、ベースラインの構成をすばやく適用し、新しいデバイスをより迅速にオンラインにすることができます。デバイスのイメージを再作成した後、インポート/エクスポートを使用して設定を復元することもできます。または、単に一連のネットワークオブジェクトや他の項目をデバイスのグループに配布する目的で使用することもできます。 ConfigurationImportExport のリソースとメソッド (/action/configexport、/jobs/configexports、/action/downloadconfigfile、/action/uploadconfigfile、/jobs/configimports、/action/configimport、/jobs/configimports) を追加しました。
カスタムファイルポリシーの作成と選択。	FTD API を使用してカスタム ファイル ポリシーを作成し、FDM を使用してアクセス制御ルールでそれらのポリシーを選択することができます。 filepolicies、filetypes、filetypecategories、ampcloudconfig、ampservers、ampcloudconnections の各 FTD API FileAndMalwarePolicies リソースを追加しました。 また、「Block Office Document and PDF Upload, Block Malware Others」と「Block Office Documents Upload, Block Malware Others」の 2 つの定義済みポリシーを削除しました。これらのポリシーを使用している場合は、ユーザが編集できるようにアップグレード中にユーザ定義のポリシーに変換されます。
FTD API を使用したセキュリティ インテリジェンス DNS ポリシーの設定。	FTD API を使用してセキュリティ インテリジェンス DNS ポリシーを設定できます。このポリシーは FDM には表示されません。 domainnamefeeds、domainnamegroups、domainnamefeedcategories、securityintelligencednspolicies の各 SecurityIntelligence リソースを追加しました。

機能	説明
Duo LDAP を使用したリモートアクセス VPN 二要素認証。	リモートアクセス VPN 接続プロファイルの 2 番目の認証ソースとして Duo LDAP を設定し、Duo パスコード、プッシュ通知、または通話を使用して二要素認証を実現できます。FTD API を使用して Duo LDAP のアイデンティティ ソース オブジェクトを作成する必要がありますが、FDM を使用してそのオブジェクトを RA VPN 接続プロファイルの認証ソースとして選択することができます。 duoldapidentitysources のリソースとメソッドを FTD API に追加しました。
FTD リモートアクセス VPN 接続の認可に使用する LDAP 属性マップの API サポート。	カスタムの LDAP 属性マップを使用して、リモートアクセス VPN の LDAP 認証を強化することができます。LDAP 属性マップにより、顧客固有の LDAP 属性名および値がシスコの属性名および値と同等になります。これらのマッピングを使用して、LDAP 属性値に基づいてユーザにグループポリシーを割り当てることができます。これらのマップは FTD API を使用してのみ設定できます。FDM を使用して設定することはできません。ただし、API を使用してこれらのオプションを設定すれば、後で FDM で Active Directory のアイデンティティソースを編集して設定を保存できます。 LdapAttributeMap、LdapAttributeMapping、LdapAttributeToGroupPolicyMapping、LDAPRealm、LdapToCiscoValueMapping、LdapToGroupPolicyValueMapping、RadiusIdentitySource の各 FTD API オブジェクトモデルを追加または変更しました。

機能	説明
FTD サイト間 VPN 接続におけるリバース ルート インジェクションとセキュリティ アソシエーション（SA）のライフタイムの API サポート。	FTD API を使用して、サイト間 VPN 接続のリバース ルート インジェクションを有効にすることができます。逆ルート注入（RRI）とは、リモート トンネル エンドポイントによって保護されているネットワークおよびホストのルーティング プロセスに、スタティック ルートを自動的に組み込む機能です。デフォルトでは、スタティック RRI が有効になっており、接続の設定時にルートが追加されます。ダイナミック RRI は無効になっています。ダイナミック RRI では、セキュリティ アソシエーション（SA）が確立されたときにのみルートが挿入され、その後 SA が切断されたときにルートが削除されます。ダイナミック RRI は IKEv2 接続でのみサポートされています。 また、接続のセキュリティ アソシエーション（SA）のライフタイムを秒単位または送信キロバイト単位で設定することもできます。ライフタイムを期限なしに設定することもできます。デフォルトのライフタイムは、28,800 秒（8 時間）および 4,608,000 キロバイト（10 メガバイト/秒で 1 時間）です。ライフタイムに到達すると、エンドポイントで新しいセキュリティ アソシエーションと秘密キーがネゴシエートされます。 FDM を使用してこれらの機能を設定することはできません。ただし、API を使用してこれらのオプションを設定すると、後で FDM で接続プロファイルを編集して設定を保存できます。 dynamicRRIEnabled、ipsecLifetimeInSeconds、ipsecLifetimeInKiloBytes、ipsecLifetimeUnlimited、rriEnabled の各属性を SToSConnectionProfile リソースに追加しました。
IKE ポリシーの Diffie-Hellman グループ 14、15、および 16 のサポート。	DH グループ 14 を使用するように IKEv1 ポリシーを設定し、DH グループ 14、15、および 16 を使用するように IKEv2 ポリシーを設定できるようになりました。IKEv1 を使用している場合は、グループ 2 と 5 が今後のリリースで削除されるため、すべてのポリシーを DH グループ 14 にアップグレードしてください。また、IKEv2 ポリシーで DH グループ 24 を使用したり、IKE バージョンで MD5 を使用したりしないでください。これらも今後のリリースで削除されます。

機能	説明
変更を展開する際のパフォーマンスの向上。	システムの強化により、アクセス制御ルールを追加、編集、または削除した場合に、以前のリリースと比べて変更がより迅速に展開されるようになりました。 フェールオーバー用のハイアベイラビリティグループに設定しているシステムでは、展開した変更をスタンバイデバイスに同期させるプロセスが改良され、同期がより迅速に完了するようになりました。
システムダッシュボード上のCPUおよびメモリ使用率の計算の改善。	CPUとメモリの使用率を計算する方法が改善され、システムダッシュボードに表示される情報に、デバイスの実際の状態がより正確に反映されるようになりました。
FTD 6.5にアップグレードした場合に履歴レポートデータは使用できなくなる。	既存のシステムをFTD 6.5にアップグレードした場合、データベーススキーマの変更のために履歴レポートデータが使用できなくなります。そのため、アップグレード前の時点における使用状況データはダッシュボードに表示されません。

廃止された機能

このトピックでは、Firepowerバージョンで廃止された機能とプラットフォームを示します。アップグレードパスが1つ以上のメジャーバージョンをスキップする場合は、中間リリースの情報を確認する必要があります。

廃止されたプラットフォームの販売終了およびサポート終了の通知へのリンクを含む、サポート対象のFirepowerのすべてのバージョン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。

（注） Cisco Firepower User Agentソフトウェアとアイデンティティソースについてはサポートの終了が予定されています。今すぐCisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えてください。これにより、ユーザエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。

詳細については、「Cisco Firepower Management Center Configuration Guides」ページで該当する*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。

バージョン6.5.0で廃止された機能

これらの機能はバージョン6.5.0で廃止されました。

表 *2 :* バージョン *6.5.0* で廃止された機能

機能	説明
FMC CLI を無効にする機能	バージョン 6.3.0 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 6.5.0 では、新しい展開とアップグレードされた展開の両方に対して、FMC 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 影響を受けるプラットフォーム：FMC
TLS 1.0 および 1.1	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。 影響を受けるプラットフォーム：FMC
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。 影響を受けるプラットフォーム：Firepower 4100/9300

機能	説明
Cisco Security Packet Analyzer の統合	バージョン 6.5.0 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 [Query Packet Analyzer] 影響を受けるプラットフォーム：FMC
Firepower Management Center モデル FMC 750、1500、3500	MC750、MC1500、および MC3500 モデルでは、Firepower Management Center ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。これらの FMC を使用してバージョン 6.5.0 以降のデバイスを管理することはできません。
Firepower ソフトウェアを搭載した ASA 5515-X および ASA 5585-X シリーズ デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）をバージョン 6.5.0+ にアップグレードしたり、このバージョンを新規インストールしたりできません。 • ASA 5515-X • ASA 5585-X-SSP-10、-20、-40、-60 ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。
Firepower 7000/8000 シリーズ デバイス	AMP モデルを含む、Firepower 7000/8000 シリーズ デバイスでは、Firepower ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。

バージョン 6.4.0 で廃止された機能

これらの機能はバージョン 6.4.0 で廃止されました。

表 *3* : バージョン *6.4.0* で廃止された機能

機能	説明
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** 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。 影響を受けるプラットフォーム：FTD

バージョン 6.3.0 で廃止された機能

これらの機能はバージョン 6.3.0 で廃止されました。

表 *4* : バージョン *6.3.0* で廃止された機能

機能	説明
復号化のための EMS 拡張機能のサポート	バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが中止されます。つまり、[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポート（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、 RFC 7627 によって定義されています。 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。 影響を受けるプラットフォーム：すべて
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	バージョン 6.3.0 では、パッシブ モードまたはインライン タップ モードのインターフェイスでの復号化トラフィックは、GUI を介して設定することはできますが、サポートされなくなりました。暗号化されたトラフィックのインスペクションは必然的に制限されます。

機能	説明
VMware 5.5 のホスティング	バージョン 6.3.0 以降の仮想展開は VMware vSphere/VMware ESXi 5.5 でテストされていません。Firepower ソフトウェアをアップグレードする前に、ホスティング環境をアップグレードすることをお勧めします。 影響を受けるプラットフォーム：FMCv、FTDv、VMware 向けの NGIPSv
Firepower ソフトウェアを搭載した ASA 5506-X シリーズおよび ASA 5512-X デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）のバージョン 6.3.0 以降へのアップグレードまたは新規インストールはできません。 • ASA 5506-X、5506H-X、5506W-X • ASA 5512-X ただし、バージョン 6.3.0 の FMC を使用して、古いデバイス（バージョン 6.1.0 ～ 6.2.3.x）を管理できます。

廃止された FlexConfig コマンド

いくつかの Firepower Threat Defense の機能は、ASA 設定コマンドを使用して設定されます。バージョン 6.2（FMC 展開）またはバージョン 6.2.3（FDM 展開）以降では、Smart CLI または FlexConfig を使用して、他の方法では Web インターフェイスでサポートされないさまざまな ASA 機能を手動で設定できます。

FTD アップグレードにより、以前に FlexConfig を使用して設定した機能について、GUI またはスマート CLI のサポートが追加されることがあります。これにより、現在使用している FlexConfig コマンドが廃止される可能性があります。既存の設定は引き続き動作し、展開も可能ですが、新しく廃止されたコマンドを使用して FlexConfig オブジェクトを割り当てたり作成したりすることはできなくなります。

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

Firepower Management Center を使用した FTD

次の表に、廃止された FlexConfig オブジェクトとそれらに関連付けられているテキスト オブジェクトを示します。事前定義されたオブジェクトの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *5 : FMC* を使用した *FTD* : 廃止された *FlexConfig* オブジェクト

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • Default_DNS_Configure 関連するテキスト オブジェクト： • defaultDNSNameServerList • defaultDNSParameters	デフォルト DNS グループを設定します。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 を設定します。
6.3.0 以降	FlexConfig オブジェクト： • 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	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）攻撃から保護します。	これらの機能は、FTD サービス ポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細設定（Advanced）] タブで確認できます。

次の表に、バージョン 6.2.3+ で、FDM を使用した FTD で新たに廃止された CLI コマンドの一覧を示します。機能がバージョン 6.2.0 に導入されたときに廃止されたコマンドを含む、廃止されたコマンドの完全なリストについては、『Firepower Management Center Configuration Guide』を参照してください。

表 *6 : FMC* を使用した *FTD* : 廃止された *CLI* コマンド

非推奨メソッド	コマンド（Command）	詳細（Details）
6.2.3 以降	**pager**	設定がブロックされます。

Firepower Device Manager を使用した FTD

次の表に、バージョン 6.3.0+ で、FDM を使用した FTD で新たに廃止された CLI コマンドの一覧を示します。機能がバージョン 6.2.3 に導入されたときに廃止されたコマンドを含む、廃止

されたコマンドの完全なリストについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』を参照してください。

表 *7: FDM* を使用した *FTD*：廃止された *CLI* コマンド

非推奨メソッド	コマンド	詳細
6.3.0 以降	**access-list**	**extended** および **standard** アクセス リストは作成できなくなりました。Smart CLI 拡張アクセス リストまたは標準アクセス リスト オブジェクトを使用してこれらの ACL を作成します。その後、それらは、サービス ポリシー トラフィック クラス用の拡張 ACL により、オブジェクト名によって ACL を参照する FlexConfig サポート コマンド（**match access-list** など）で使用できます。
6.3.0 以降	**as-path**	スマート CLI AS パス オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、自律システム パス フィルタを設定します。
6.3.0 以降	**community-list**	スマート CLI 拡張コミュニティ リスト オブジェクトまたは標準コミュニティ リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、コミュニティ リスト フィルタを設定します。
6.3.0 以降	**dns-group**	**[オブジェクト（Objects）] > [DNSグループ（DNS Groups）]** を使用して DNS グループを設定し、**[デバイス（Device）] > [システム設定（System Settings）] > [DNSサーバ（DNS Server）]** を使用してグループを割り当てます。
6.3.0 以降	**policy-list**	スマート CLI ポリシー リスト オブジェクトを作成し、それらをスマート CLI BGP オブジェクトで使用して、ポリシー リストを設定します。
6.3.0 以降	**prefix-list**	スマート CLI IPv4 プレフィックス リスト オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、IPv4 用のプレフィックス リスト フィルタリングを設定します。
6.3.0 以降	**route-map**	スマート CLI ルート マップ オブジェクトを作成し、それらをスマート CLI OSPF オブジェクトまたはスマート CLI BGP オブジェクトで使用して、ルート マップを設定します。
6.3.0 以降	**router bgp**	BGP には Smart CLI テンプレートを使用します。

FMC メニューの変更

次の表に、変更された Firepower Management Center メニュー（移動されたページ）を示します。新規および削除されたメニューオプションについては、新機能および廃止された機能のマニュアルを参照してください。

表 *8 : Firepower Management Center* メニューの変更

バージョン	新しいメニュー パス	古いメニュー パス
6.4.0	**[システム（System）] > [統合（Integration）] > [クラウド サービス（Cloud Services）]**	**[システム（System）] > [統合（Integration）] > [Cisco CSI]**
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [Whois]**	**[分析（Analysis）] > [詳細（Advanced）] > [Whois]**
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [位置情報（Geolocation）]**	**[分析（Analysis）] > [詳細（Advanced）] > [位置情報（Geolocation）]**
6.3.0	**[分析（Analysis）] > [検索（Lookup）] > [URL]**	**[分析（Analysis）] > [詳細（Advanced）] > [URL]**
6.3.0	**[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）] > [カスタムワークフロー（Custom Workflows）]**
6.3.0	**[分析（Analysis）] > [カスタム（Custom）] > [カスタムテーブル（Custom Tables）]**	**[分析（Analysis）] > [詳細（Advanced）] > [カスタムテーブル（Custom Tables）]**
6.3.0	**[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）]**	**[分析（Analysis）] > [ホスト（Hosts）] > [脆弱性（Vulnerabilities）]**
6.3.0	**[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third Party Vulnerabilities）]**	**[分析（Analysis）] > [ホスト（Hosts）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）]**

FMC How-To ウォークスルー

バージョン 6.3.0 では、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。

（注） 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。

次の表に、一般的な問題点と解決策をいくつか示します。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。

表 *9:* ウォークスルーのトラブルシューティング

問題	解決方法
ウォークスルーを開始するための [How To] リンクが見つからない。	ウォークスルーが有効になっていることを確認します。ユーザ名の下にあるドロップダウンリストから、[ユーザ設定（User Preferences）] を選択し、[設定方法（How-To Settings）] をクリックします。
ウォークスルーが予期しないタイミングで表示される。	ウォークスルーが予期しないタイミングで表示される場合は、ウォークスルーを終了します。
ウォークスルーが突然消えたり終了したりする。	ウォークスルーが消えた場合は、次のようにします。 • ポインタを移動します。 FMC で進行中のウォークスルーが表示されなくなることがあります。たとえば、別のトップレベルメニューをポイントすると表示されなくなります。 • 別のページに移動して、もう一度やり直してください。 ポインタを移動しても表示されない場合は、ウォークスルーが終了している可能性があります。
ウォークスルーが FMC と同期していない。 • 誤った手順から開始される。 • 進行が早すぎる。 • 先に進まない。	ウォークスルーが同期していない場合は、次のようにします。 • 続行します。 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。 • ウォークスルーを終了し、別のページに移動してもう一度やり直します。 場合によっては続行できないこともあります。たとえば、手順の完了後に [次へ（Next）] をクリックしないと、ウォークスルーの終了が必要になる場合があります。