特長と機能

Firepower バージョン 6.4.0 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 6.4.0 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/Firepower バージョン 6.4.0 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 6.4.0 で使用可能な新機能を示します。

表 *1* : バージョン *6.4.0* 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	
FMC モデル MC1600、2600、および 4600	Firepower Management Center モデル MC1600、2600、および 4600 を導入しました。なお、これらのモデルではバージョン 6.3.x もサポートされています。
FMCv Azure 上	Microsoft Azure 上に Firepower Management Center Virtual を導入しました。

機能	説明
FTD Firepower 1010、1120、1140 上	Firepower 1010、1120、および 1140 を導入しました。
FTD Firepower 4115、4125、および 4145	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。
ASA および FTD（同じ Firepower 9300 上）	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。FXOS 2.6.1 が必要です。
ライセンス	
の新しいライセンス機能 ISA 3000	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それら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、承認された顧客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。 サポートされているプラットフォーム： ISA 3000
Firepower Threat Defense ルーティング	

機能	説明
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/変更された画面： • **[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 サポートされてい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/変更された画面：**[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 サポートされているプラットフォーム： FTD

機能	説明
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/変更された画面：**[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 サポートされているプラットフォーム： FTD
サイト間 VPN：ポイントツーポイント トポロジのためのダイナミック暗号マップ	ポイントツーポイントおよびハブアンドスポーク VPN トポロジでは、ダイナミック暗号マップを使用できるようになりました。フルメッシュ トポロジについては、ダイナミック暗号マップはまだサポートされていません。 トポロジを設定するときは、暗号マップ タイプを指定します。トポロジ内のピアの 1 つに対して、ダイナミック IP アドレスも指定する必要があります。 新規/変更された画面：**[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 サポートされているプラットフォーム： FTD

機能	説明
TLS 暗号化アクセラレーション	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 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** サポートされているプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ
イベント、ロギング、および分析	

機能	説明
ファイルおよびマルウェア イベントの syslog メッセージの改良	完全修飾ファイルおよびマルウェアのイベントデータが syslog 経由で管理対象デバイスから送信できるようになりました。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセスコントロール（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/変更された画面：**[分析（Analysis）]** > **[検索（Search）]** サポートされてい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 Threat Response（CTR）の統合	Cisco Threat Response は、脅威の迅速な検出、調査、および対応に役立つ新しい Cisco Cloud を提供しています。CTR 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。詳細については、Firepower および Cisco Threat Response の統合ガイドを参照してください。 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： FTD
Splunk の統合	Splunk のユーザは、新しい個別の Splunk アプリケーションである Cisco Firepower App for Splunk を使用してイベントを分析できます。どの機能を使用できるかは、Firepower のバージョンによって異なります。 サポートされているプラットフォーム： FMC
管理	

機能	説明
VMware の FTDv はデフォルトで vmxnet3 インターフェイスに設定される	VMware 上の 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） e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。詳細については、『Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide』の VMware インターフェイスの追加と設定の手順を参照してください。 サポートされているプラットフォーム：VMware 上の FTDv
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/変更された画面：**[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 サポートされているプラットフォーム：FMC、7000 および 8000 シリーズ

機能	説明
管理インターフェイス上のICMPv6エコー応答と宛先到達不能メッセージを無効にする機能	IPv6 を有効にすると、ICMPv6 エコー応答および宛先到達不能メッセージを無効できるようになりました。これらのパケットを無効にすることで、サービス拒否攻撃の可能性から保護します。エコー応答パケットを無効にすると、デバイスの管理インターフェイスにテスト目的で IPv6 ping を使用できなくなります。 新規/変更された画面： **[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** サポートされてい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 サーバに定義されている FTD ユーザの Service-Type 属性のサポート	FTD CLI ユーザの RADIUS の認証では、以前は RADIUS 外部認証オブジェクトにユーザ名をあらかじめ定義してから、RADIUS サーバに定義されているユーザ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 サーバで CLI ユーザ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 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/変更された画面：**[システム（System）] > [ユーザ（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）] サポートされてい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/変更された画面：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > でオブジェクトのタイプを選択し [使用状況の検索（Find Usage）]（双眼鏡）アイコン サポートされているプラットフォーム： FMC

機能	説明
署名済みの SRU、VDB、および GeoDB の更新（セキュリティの拡張）	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以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）に使用します。以前のバージョンでは、引き続き未署名の更新が使用されます。シスコ サポートおよびダウンロード サイト から手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。 ただし、SRU、VDB、および GeoDB の更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。バージョン 6.4 以降の署名付きの更新ファイルの先頭は「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar バージョン 5.x ～ 6.3 の更新ファイルでは、引き続き古い命名方式が使用されています。 • SRU：Sourcefire_Rule_Update-*date-build*-vrt.sh • VDB：Sourcefire_VDB_Fingerprint_Database-4.5.0-*version*.sh • GeoDB：Sourcefire_Geodb_Update-*date-build*.sh シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。 （注） 古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。 サポートされているプラットフォーム：すべて

機能	説明
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/変更された画面：**[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 サポートされているプラットフォーム：FTD の物理プラットフォーム、VMware 用 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。
モニタリングおよびトラブルシューティング	
URL フィルタリング モニタの改善	URL フィルタリング モニタ 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/変更された画面：**[システム（System）]** > **[健全性（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（URL Filtering Monitor）] サポートされているプラットフォーム：すべて

機能	説明
アクセス制御ルールと事前フィルタ ルールのヒット カウント	FTD デバイスのアクセス制御ルールと事前フィルタ ルールのヒット カウントにアクセスできるようになりました。 新規/変更された画面： • **[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（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** に HA ピア間のヒット カウントの同期に関連するオブジェクトのスタティック カウン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： FTD
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** サポートされているプラットフォーム： FTD

機能	説明
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 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。いつでもオプトインまたはオプトアウトできます。 サポートされているプラットフォーム： FMC
Firepower Management Center REST API	
新しい REST API 機能	バージョン 6.4 の機能をサポートするための REST API オブジェクトを追加しました。 • cloudeventsconfigs：Cisco Threat Response の統合を管理します。 • ftddevicecluster：シャーシのクラスタリングを管理します。 • hitcounts：アクセス制御ルールと事前フィルタ ルールのヒット カウント統計情報を管理します。 • keychain：OSPFv2 ルーティングの設定時に、認証のローテーションに使用されるキーチェーン オブジェクトを管理します。 • loggingsettings：アクセス コントロール ポリシーのロギング設定を管理します。 サポートされてい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 は OpenAPI 仕様（OAS）に基づいて、新しい API エクスプローラを使用します。OAS の一部として、CodeGen を使用してサンプル コードを生成するようになりました。必要に応じて、レガシー API エクスプローラにもアクセスできます。 サポートされているプラットフォーム： FMC
パフォーマンス	

機能	説明
Snort 再起動の改善	バージョン 6.4 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
選択された IPS トラフィックのパフォーマンスの向上	出力最適化は、選択された IPS トラフィックを対象としたパフォーマンス機能です。この機能は、すべての FTD プラットフォームでデフォルトで有効になっています。 バージョン 6.4 のアップグレード プロセスでは、対象デバイスでの出力最適化が有効になります。詳細については、『Cisco Firepower Threat Defense コマンド リファレンス（Cisco Firepower Threat Defense Command Reference）』を参照してください。出力最適化に関する問題をトラブルシューティング Cisco TACするには、にお問い合わせください。 サポートされているプラットフォーム： FTD 新規/変更されたコマンド： • **asp inspect-dp egress optimization** • **show asp inspect-dp egress optimization** • **clear asp inspect-dp egress optimization** • **show conn state egress_optimization**
SNMP イベント ロギングの高速化	外部 SNMP トラップ サーバ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。 サポートされてい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 Device Manager/FTD バージョン 6.4.0 の新機能

リリース日：2019 年 4 月 24 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.4.0 で使用できる新機能を示します。

表 *2:*

機能	説明
Firepower 1000 シリーズ デバイス設定	Firepower Device Manager を使用して、Firepower 1000 シリーズ デバイスで Firepower Threat Defense を設定できます。 Power over Ethernet（PoE）ポートを通常のイーサーネット ポートとして使用することはできますが、PoE に関連するプロパティを有効にしたり設定することはできないことにご注意ください。
ISA 3000 のハードウェア バイパス	ISA 3000 のハードウェアバイパスは、**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページで設定できるようになりました。リリース 6.3 では、FlexConfig を使用してハードウェアバイパスを設定する必要がありました。FlexConfig を使用している場合は、[インターフェイス（Interfaces）] ページの設定をやり直し、FlexConfig から hardware bypass コマンドを削除してください。ただし、TCP シーケンス番号のランダム化を無効にするための FlexConfig 部分の使用は引き続き推奨されます。
FDM CLI コンソールからシステムを再起動およびシャットダウンする機能	FDM で CLI コンソールを使用して、**reboot** および **shutdown** コマンドを発行できるようになりました。以前は、システムを再起動またはシャットダウンするために、デバイスに対して個別の SSH セッションを開く必要がありました。これらコマンドを使用するには、管理者権限が必要です。
RADIUS を使用した FTD CLI ユーザの外部認証および認可。	FTD CLI にログインするユーザを、外部 RADIUS サーバを使用して認証および認可できます。外部ユーザに設定（管理者）または基本（読み取り専用）のアクセス権を付与できます。 **[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理アクセス（Management Access）]** ページの [AAA設定（AAA Configuration）] タブに SSH の設定を追加しました。

機能	説明
ネットワーク範囲オブジェクトとネストされたネットワーク グループ オブジェクトのサポート	IPv4 または IPv6 アドレスの範囲、および他のネットワーク グループ（つまり、ネストされたグループ）を含むネットワーク グループ オブジェクトを指定するネットワーク オブジェクトを作成できるようになりました。 これらの機能を含めるためにネットワーク オブジェクトとネットワーク グループ オブジェクトの [追加/編集（Add/Edit）] ダイアログボックスが変更されました。また、当該タイプのアドレス指定がポリシーのコンテキスト内で妥当かどうかにより、これらのオブジェクトの使用を許可するためにさまざまなセキュリティ ポリシーが変更されました。
オブジェクトとルールの全文検索オプション	オブジェクトおよびルールでは、全文検索を実行できます。多数の項目を含むポリシーまたはオブジェクト リストを検索することで、ルールまたはオブジェクト内の任意の場所で検索文字列を含むすべての項目を検索できます。 ルールを含むすべてのポリシー、および [オブジェクト（Objects）] リストのすべてのページに検索ボックスが追加されました。さらに、API でサポートされているオブジェクトの GET コールで **filter=fts~***search-string* オプションを使用して、全文検索に基づいて項目を取得できます。
FDM 管理対象 FTD デバイスでサポートされている API バージョンのリストの取得	GET/api/versions（ApiVersions）メソッドを使用して、デバイスでサポートされる API バージョンのリストを取得できます。API クライアントを使用すると、サポートされているバージョンで有効なコマンドとシンタックスを使用してデバイスと通信し、デバイスを設定できます。
FTD REST API バージョン 3（v3）	ソフトウェア バージョン 6.4 向けの FTD REST API のバージョン番号が 3 になりました。API URL の v1/v2 は v3 に置き換える必要があります。v3 の API には、ソフトウェア バージョン 6.4 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、ログインした後に、Firepower Device Manager の URL の最後を **/#/api-explorer** に変更します。

機能	説明
アクセス制御ルールのヒットカウント	アクセスコントロールルールのヒットカウントを表示できます。ヒットカウントには、接続がルールに一致した頻度が示されます。 ヒットカウント情報が含まれるようにアクセスコントロールポリシーを更新しました。FTD API では、HitCounts リソースと **includeHitCounts** および **filter=fetchZeroHitCounts** オプションが GET アクセスポリシールールのリソースに追加されました。
ダイナミック アドレス指定と証明書認証のためのサイト間 VPN の強化	ピアの認証に事前共有キーではなく証明書を使用したサイト間 VPN 接続を設定できるようになりました。リモートピアに不明な（ダイナミック）IP アドレスが設定されている接続も設定できます。サイト間 VPN ウィザードと IKEv1 ポリシーオブジェクトにオプションが追加されました。
リモート アクセス VPN での RADIUS サーバと認可変更のサポート	リモートアクセス VPN（RA VPN）ユーザの認証、認可、およびアカウンティングに RADIUS サーバを使用できるようになりました。また、Cisco ISE RADIUS サーバの使用時、認証後にユーザの認証を変更するために、ダイナミック認証とも呼ばれる Change of Authentication（CoA）を設定できます。 RADIUS サーバとサーバ グループ オブジェクトに属性を追加し、RA VPN 接続プロファイル内の RADIUS サーバグループを選択できるようになりました。
リモートアクセス VPN の複数の接続プロファイルとグループ ポリシー	複数の接続プロファイルを設定し、そのプロファイルで使用するグループ ポリシーを作成できます。 接続プロファイルおよびグループ ポリシーが別々のページとなるように **[デバイス（Device）]** > **[リモートアクセス VPN（Remote Access VPN）]** ページを変更し、グループ ポリシーを選択できるように RA VPN 接続ウィザードを更新しました。以前はウィザードで設定していた一部の項目がグループポリシーで設定されるようになりました。
証明書ベースの 2 番目の認証ソース、およびリモート アクセス VPN での二要素認証のサポート	ユーザ認証に証明書を使用し、セカンダリ認証ソースを設定して、接続を確立する前にユーザを 2 回認証させることができます。また、2 つ目の要素として RSA トークンまたは Duo パスコードを使用して二要素認証を設定できます。 これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。

機能	説明
複数のアドレス範囲を持つ IP アドレス プールとリモート アクセス VPN 向けの DHCP アドレス プールのサポート	サブネットを指定する複数のネットワークオブジェクトを選択することで、複数のアドレス範囲を持つアドレスプールを設定できるようになりました。さらに、DHCP サーバでアドレスプールを設定し、そのサーバを使用して RA VPN クライアントにアドレスを提供できます。認証に RADIUS を使用する場合は、代わりに RADIUS サーバでアドレスプールを設定できます。 これらの追加オプションの設定をサポートするように RA VPN 接続ウィザードを更新しました。必要に応じて、接続プロファイルではなくグループポリシーでアドレスプールを設定できます。
Active Directory レルムの強化	1 つのレルムに最大 10 の冗長 Active Directory（AD）サーバを含められるようになりました。また、複数のレルムを作成したり、不要になったレルムを削除したりできます。さらに、レルム内のユーザのダウンロードの制限は、以前のリリースの 2,000 から 50,000 に増えています。 複数のレルムとサーバをサポートするように、**[オブジェクト（Objects）] > [アイデンティティ ソース（Identity Sources）]** ページを更新しました。レルム内のすべてのユーザにルールを適用するため、アクセス制御と SSL 復号化ルールのユーザの基準でレルムを選択することができます。アイデンティティ ルールと RA VPN 接続プロファイルでレルムを選択することもできます。
ISE サーバの冗長性サポート	パッシブ認証向けの ID ソースとして Cisco Identity Services Engine（ISE）を設定する際に、ISE ハイアベイラビリティ設定がある場合は、セカンダリ ISE サーバを設定できるようになりました。 ISE アイデンティティ オブジェクトにセカンダリサーバの属性が追加されました。
ファイル/マルウェア イベントを外部 syslog サーバに送信	アクセスコントロールルールに設定されたファイルポリシーによって生成される、ファイルおよびマルウェアイベントを受信するように外部 syslog サーバを設定できるようになりました。ファイルイベントにはメッセージ ID 430004 を使用し、マルウェアイベントには 430005 を使用します。 **[デバイス（Device）] > [システム設定（System Settings）] > [ログの設定（Logging Settings）]** ページにファイル/マルウェア syslog サーバのオプションが追加されました。

機能	説明
内部バッファのログおよびカスタムイベントのログフィルタのサポート	内部バッファをシステムロギングの宛先として設定できるようになりました。さらに、イベントログフィルタを作成して、syslog サーバおよび内部バッファロギングの宛先に対して生成されるメッセージをカスタマイズできます。 イベント ログ フィルタ オブジェクトを [オブジェクト（Objects）] ページに追加し、このオブジェクトを使用する機能が **[デバイス（Device）] > [システム設定（System Settings）] > [ログの設定（Logging Settings）]** ページに追加されました。内部バッファ オプションも [ログの設定（Logging Settings）] ページに追加しました。
Firepower Device Manager の Web サーバ向けの証明書	Firepower Device Manager の設定インターフェイスへの HTTPS 接続に使用される証明書を設定できるようになりました。Web ブラウザがすでに信頼している証明書をアップロードすることで、デフォルトの内部証明書を使用するときに、Untrusted Authority メッセージを回避できます。**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）] > [管理Webサーバ（Management Web Server）]** ページが追加されました。
Cisco Threat Response のサポート	Cisco Threat Response のクラウドベースのアプリケーションに侵入イベントを送信するようにシステムを設定できます。Cisco Threat Response を使用して、侵入を分析できます。 Cisco Threat Response を **[デバイス（Device）] > [システム設定（System Settings）] > [クラウド サービス（Cloud Services）]** ページに追加しました。

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 コンフィギュレーション ガイド [英語] 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 6.4.0 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。
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。

バージョン 6.2.0 で廃止された機能

これらの機能はバージョン 6.2.0 で廃止されました。

表 *5 :* バージョン *6.2.0* で廃止された機能

機能	説明
ネストされた相関ルール	

機能	説明
	バージョン 6.2.0 では、ネストされた相関ルールのサポートが終了します。ある相関ルールが別の相関ルールのトリガーとなっている場合、その相関ルールはネストされています。 たとえば、どちらも侵入イベントのトリガーであるルール A とルール B を作成する場合、「ルール A は true」をルール B の制約として使用できます。この設定では、ルール A はルール B 内にネストされています。 **自動設定の変更** アップグレードプロセスは、ネストされたルール（ルール A）からネストされたルール（ルール B）へ設定をコピーしてネストされたルールを削除することで、特定のネストされた相関ルールを「フラット化」します。また、アップグレードは、ホストプロファイル/ユーザ資格とスヌーズ/非アクティブ期間を、ネストされたルールからネスト ルールへコピーします。 非アクティブ期間を除いて、これらのすべての設定について、設定がネスト ルールに存在しない場合にのみ、システムはネストされたルールからネストルールへ設定をコピーできます。システムがネストされたルールからネストルールへ非アクティブ期間をコピーするときは、結果として生じるルールがネスト構成にもともと含まれる両方のルールの設定を使用するように、ネスト ルールの非アクティブ期間を保持します。 **アップグレードの失敗の回避** アップグレードする前に、ネストされた相関ルールを「フラット化」できることを確認してください。そうなっていなければ、アップグレードは失敗します。ネストされたルールとネスト ルールに特定の競合がある場合は、アップグレードによりネストされたルールをフラット化できないことに注意してください。アップグレードの失敗を回避するには、アップグレードの前に、以下のように相関ルールを変更します。 • ネストされた構成内で 1 つのルールだけがこれらの設定を指定するように、ホスト プロファイル資格、ユーザ資格、スヌーズ期間の設定をネストされたルールまたはネスト ルールから削除します。 • 接続トラッカーを任意のネストされたルールから削除します。 • ホスト プロファイル資格、ユーザ資格、スヌーズ期間、非アクティブ期間を、true にする必要がないネストされたルールから削除します。つまり、ネスト ルール内の OR 演算子を使用して他のルールの条件にリンクされているネストされたルールから、これらの要素を削除します。

機能	説明
	影響を受けるプラットフォーム：FMC

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 *6 : 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。

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： • 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 *7 : 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	詳細
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 *8 : 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（Command）	詳細（Details）
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。

非推奨メソッド	コマンド（Command）	詳細（Details）
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 *9 : 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]**

バージョン	新しいメニュー パス	古いメニュー パス
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 *10 :* 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。