# 特長と機能

Firepower バージョン 6.3.0 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 6.3.0 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。

## FMC/Firepower バージョン 6.3.0 の新機能

次の表に、Firepower Management Center を使用して設定された場合の Firepower バージョン 6.3.0 で使用可能な新機能の概要を示します。

| 機能 | 説明 |
|---|---|
| **ハードウェア** | |
| ISA 3000 および FirePOWER Services | ISA 3000 with FirePOWER Services は、バージョン 6.3.0 でサポートされています。<br>ISA 3000 with FirePOWER Services はバージョン 5.4.x でもサポートされていましたが、バージョン 6.3.0 にアップグレードすることはできません。再イメージ化する必要があります。<br>サポートされるプラットフォーム：ISA 3000 |
| **ライセンス** | |

| 機能 | 説明 |
| --- | --- |
| 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。<br>新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]**<br>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。<br>新規/変更された画面：**[システム（System）] > [ライセンス（Licenses）] > [特定のライセンス（Specific Licenses）]**<br>サポートされるプラットフォーム：FMC、FTD |
| **インターフェイス機能** | |
| サポート対象ネットワーク モジュールに対する Firepower 2100 でのハードウェア バイパス サポート | Firepower 2100 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。<br>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）]**<br>サポートされるプラットフォーム：Firepower 2100 |
| 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。<br>新規/変更された Firepower Chassis Management 画面：**[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）]**<br>新規/変更された FXOS コマンド： **set port-channel-mode**<br>サポートされるプラットフォーム：Firepower 4100/9300 |
| **アクセス制御** | |

| 機能 | 説明 |
| --- | --- |
| URL カテゴリおよびレピュテーションデータの更新間隔 | 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。<br><br>バージョン 6.3.0 にアップグレードしても、システムの動作は変更されません。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。<br><br>新規/変更された画面：**[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 |
| ハイ アベイラビリティとスケーラビリティ | |

| 機能 | 説明 |
| --- | --- |
| FTD を搭載した Firepower 4100/9300 のマルチインスタンス機能 | 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。<br><br>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。<br><br>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。<br><br>（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。<br><br>新規/変更された FMC 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）] タブ<br><br>新規/変更された [Firepower Chassis Manager] 画面：<br>• **[概要（Overview）]** > **[デバイス（Devices）]**<br>• **[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）]<br>• **[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）]**<br>• **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]**<br>• **[プラットフォームの設定（Platform Settings）]** > **[Mac プール（Mac Pool）]**<br>• **[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）]**<br><br>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**<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |

| 機能 | 説明 |
| --- | --- |
| 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。FXOS でクラスタを展開する際にネットワークを設定できるようになりました。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。<br><br>新規/変更された [Firepower Chassis Manager] 画面：**[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）]**<br><br>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<br><br>新規/変更された FXOS コマンド： **set cluster-control-link network**<br><br>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。<br><br>新規/変更された画面：<br><br>• **[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<br><br>• **[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）] リンク > [クラスタ ステータス（Cluster Status）] ダイアログ ボックス<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |
| **暗号化と VPN** | |

| 機能 | 説明 |
|---|---|
| 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。<br><br>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。<br><br>サポートされるプラットフォーム：Firepower 2100 シリーズ、Firepower 4100/9300 |
| RA VPN：RADIUS ダイナミック認証または認可変更（CoA） | ダイナミック アクセス コントロール リスト（ACL）またはユーザごとの ACL 名を使用する RA VPN のユーザ認可のために、RADIUS サーバを使用できるようになりました。<br><br>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 では、Cisco AnyConnect セキュア モビリティ クライアントを使用する RA VPN ユーザの二要素認証をサポートしています。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。<br><br>• 第 1 要素：任意の RADIUS または LDAP/AD サーバ<br>• 第 2 要素：モバイルにプッシュされる RSA トークンまたは DUO パスコード<br><br>FTD の Duo 多要素認証（MFA）の詳細については、Duo セキュリティ Web サイトの『Cisco Firepower Threat Defense (FTD) VPN with AnyConnect』のドキュメントを参照してください。<br><br>サポートされるプラットフォーム FTD |
| **イベント、ロギング、および分析** | |
| 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。<br><br>新規/変更された画面：<br><br>• **[システム（System）] > [統合（Integration）] > [パケット アナライザ（Packet Analyzer）]**<br>• **[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）]**<br>• ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）] |

| 機能 | 説明 |
| --- | --- |
| 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。<br><br>新規/変更された画面：**[分析（Analysis）] > [詳細（Advanced）] > [コンテキストクロス起動（Contextual Cross-Launch）]** |
| ユニファイド syslog の設定 | 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。バージョン 6.3.0 では、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イベントと侵入イベントのロギングに影響を与えます。<br><br>FTD デバイスでは、一部の syslog プラットフォーム設定が接続イベントと侵入イベントのメッセージに適用されるようになりました。リストについては、『*Firepower Management Center Configuration Guide*』の「Platform Settings for Firepower Threat Defense」の章を参照してください。<br><br>サポートされるプラットフォーム：機能に応じて異なる |
| 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。<br><br>• FTD デバイスからのメッセージには、イベントタイプ ID 番号が含まれるようになりました。<br><br>• 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。<br><br>• 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）。 |
| 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 ポートのみで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。<br><br>サポートされるプラットフォーム FTD |
| **管理とトラブルシューティング** | |

| 機能 | 説明 |
|---|---|
| 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サーバクレデンシャルは 3 年で期限が切れます。<br><br>バージョン 6.3.0 にアップグレードされる前に生成されたデフォルトのサーバ証明書をアプライアンスが使用している場合、サーバ証明書は最初に生成されたときから 20 年後に期限切れとなります。デフォルトの HTTPS サーバ証明書を使用している場合、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。<br><br>新規/変更された画面：**[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<br><br>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*<br><br>サポート対象プラットフォーム：物理 FMC、7000 および 8000 シリーズ デバイス |
| 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。<br><br>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）]** > [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<br><br>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 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。<br><br>新規/変更された画面：<br>• **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）]**<br>• **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DNSサーバグループ（DNS Server Group）]**<br>• **[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]<br><br>サポートされるプラットフォーム FTD |

| 機能 | 説明 |
|---|---|
| CLI FMC | 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。<br><br>新規/変更されたコマンド：**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。<br><br>新規/変更された画面：**[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<br><br>サポートされるプラットフォーム：FMC（FMCv を含む） |
| 向上したログイン セキュリティ | ログイン セキュリティを向上させるために FMC ユーザ設定が追加されました。<br><br>• **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。<br><br>• **パスワード再利用の制限**：再利用を防止するために、FMC ユーザのパスワード履歴を追跡します。<br><br>• **ログイン失敗の最大数と一時的にユーザをロックアウトする分単位の時間の設定**：FMC ユーザが一時的にブロックされる前に、そのユーザが誤った 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。<br><br>新規/変更された画面：**[System] > [Configuration]** > [ユーザ設定（User Configuration）]<br><br>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。<br><br>サポートされるプラットフォーム：管理対象デバイス |
| 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。<br><br>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 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 |

| 機能 | 説明 |
|---|---|
| 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。<br><br>新規/変更された画面：**[システム（System）] > [ツール（Tools）] > [バックアップ/復元（Backup/Restore）]**<br><br>新規/変更された CLI コマンド： **restore**<br><br>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 上の 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 | 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。<br><br>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。<br><br>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）]** > [タスクの追加または編集（add or edit a task）] > [展開ポリシーのジョブタイプの選択（choose Job Type of Deploy Policies）] |
| 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。<br><br>• **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。<br><br>• **レルム**：ダウンロードされずに、ユーザが FMC にレポートされるか、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がログインしました。<br><br>新規/変更された画面：<br><br>• **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）]**<br><br>• **[システム（System）] > [ヘルス（Health）] > [モニタ（Monitor）]**<br><br>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。<br><br>新規/変更された CLI コマンド：**file-size**、**show capture**<br><br>サポートされるプラットフォーム：Firepower 4100/9300 |
| **Firepower Management Center REST API** | |

| 機能 | 説明 |
|---|---|
| 新しいオブジェクト | FMC REST API は、サイト間 VPN トポロジおよび HA デバイス フェールオーバーのために、新しいオブジェクトをサポートします。<br>サイト間 VPN トポロジの新しいオブジェクト：ftds2svpns、endpoints、ipsecsettings、advancedsettings、ikesettings、ikev1ipsecproposals、ikev1policies、ikev2ipsecproposals、ikev2policies<br>HA デバイス フェールオーバーの新しいオブジェクト：failoverinterfacemacaddressconfigs、monitoredinterfaces |
| 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。 |

# Firepower Device Manager/FTD バージョン 6.3.0 の新機能

**リリース日：2018 年 12 月 3 日**

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.3.0 で使用できる新機能を示します。

| 機能 | 説明 |
|---|---|
| 高可用性設定。 | 2 つのデバイスをアクティブ/スタンバイ高可用性ペアとして設定できます。高可用性またはフェールオーバー セットアップは、プライマリ デバイスの障害時にセカンダリ デバイスで引き継ぐことができるように、2つのデバイスを結合します。これにより、デバイスの障害時にネットワーク運用を維持できます。デバイスは、同じモデルで、同じ数と同じタイプのインターフェイスを備えており、同じソフトウェア バージョンを実行している必要があります。ハイ アベイラビリティは [デバイス（Device）] ページから設定できます。 |
| パッシブ ユーザ アイデンティティ取得のサポート。 | パッシブ認証を使用するようにアイデンティティ ポリシーを設定できます。パッシブ認証では、ユーザにユーザ名とパスワードを求めることなくユーザ アイデンティティを収集します。システムは、ユーザが指定したアイデンティティ ソース（Cisco Identity Services Engine（ISE）/Cisco Identity Services Engine Passive Identity Connector（ISE PIC）を指定可能）からマッピングを取得します。または、リモート アクセス VPN ユーザからログインを取得します。<br>変更には、**[ポリシー（Policies）] > [アイデンティティ（Identity）]** でのパッシブ認証ルールのサポートと、または **[オブジェクト（Objects）] > [アイデンティティ ソース（Identity Sources）]** の ISE 設定が含まれます。 |

| 機能 | 説明 |
|---|---|
| リモートアクセスVPNおよびユーザ アイデンティティに関するローカル ユーザのサポート。 | Firepower Device Manager から直接ユーザを作成できるようになりました。その後、これらのローカルユーザアカウントを使用して、リモートアクセスVPNへの接続を認証できます。ローカルユーザデータベースは、プライマリまたはフォールバック認証ソースとして使用できます。さらに、ローカル ユーザ名がダッシュボードに反映され、それらをポリシーでのトラフィック照合に利用できるように、アイデンティティ ポリシーでパッシブ認証ルールを設定できます。<br><br>**[オブジェクト（Objects）]** > **[ユーザ（Users）]** ページが追加されました。また、リモート アクセス VPN ウィザードが更新され、フォールバック オプションが追加されました。 |
| アクセス コントロール ポリシーでのVPNトラフィック処理のデフォルト動作の変更（**sysopt connection permit-vpn**）。 | アクセス コントロール ポリシーによる VPN トラフィックの処理方法に対するデフォルト動作が変更されました。6.3以降では、アクセス コントロール ポリシーによりすべての VPN トラフィックが処理されるのがデフォルトです。これにより、URLフィルタリング、侵入防御、およびファイルポリシーを含む高度なインスペクションをVPNトラフィックに適用することができます。VPN トラフィックを許可するアクセス制御ルールを設定する必要があります。または、FlexConfig を使用して **sysopt connection permit-vpn** コマンド設定することもできます。このコマンドは、VPN 終端トラフィックがアクセス コントロール ポリシー（および高度なインスペクション）をバイパスするようにシステムに指示します。 |
| FQDN ベースのネットワーク オブジェクトのサポートと、DNS ルックアップに関するデータ インターフェイスのサポート。 | 静的IPアドレスではなく完全修飾ドメイン名（FQDN）によってホストを指定するネットワーク オブジェクト（およびグループ）を作成できるようになりました。システムは、アクセス制御ルールで使用される FQDN オブジェクトに関して、FQDN から IP アドレスへのマッピングのルックアップを定期的に実行します。これらのオブジェクトはアクセス制御ルールのみで使用できます。<br><br>オブジェクト ページに DNS グループ オブジェクトが追加されました。また、**[システム設定（System Settings）]** > **[DNS サーバ（DNS Server）]** ページが、データ インターフェイスにグループを割り当てることができるように変更され、アクセス制御ルールが、FQDN ネットワーク オブジェクトを選択できるように変更されました。さらに、管理インターフェイスの DNS 設定では、DNS サーバ アドレスのセット リストの代わりに DNS グループが使用されるようになりました。 |

| 機能 | 説明 |
| --- | --- |
| TCP Syslog のサポートと、管理インターフェイスを介して診断 Syslog メッセージを送信する機能。 | 以前のリリースでは、診断 Syslog メッセージは（接続および侵入メッセージとは対照的に）常にデータ インターフェイスを使用していました。すべてのメッセージが管理インターフェイスを使用するようにSyslogを設定できるようになりました。最終的な送信元IPアドレスは、データインターフェイスを管理インターフェイスのゲートウェイとして使用するかどうかによって異なります。使用する場合は、IP アドレスがデータインターフェイスのものになります。UDP ではなく TCP をプロトコルとして使用するように Syslog を設定することもできます。<br><br>**[オブジェクト（Objects）] > [Syslogサーバ（Syslog Servers）]** からSyslogサーバを追加/編集できるようにダイアログボックスが変更されました。 |
| RADIUS を使用した Firepower Device Manager ユーザの外部認証および認可。 | Firepower Device Manager 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許可できます。外部ユーザに管理、読み取り/書き込み、または読み取り専用のアクセス権を付与できます。Firepower Device Manager は 5 つの同時ログインをサポートできます。6 つ目のセッションにより、最も古いセッションが自動的にログオフされます。必要に応じて、Firepower Device Manager のユーザ セッションを強制的に終了させることができます。<br><br>**[オブジェクト（Objects）] > [アイデンティティソース（Identity Sources）]** ページにRADIUSサーバおよびRADIUSサーバ グループ オブジェクトが追加され、それらのオブジェクトを設定できるようになりました。**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス（Management Access）]** に [AAA設定（AAA Configuration）] タブが追加され、サーバ グループを使用できるようになりました。さらに、**[モニタリング（Monitoring）] > [セッション（Sessions）]** ページにはアクティブ ユーザのリストが表示され、管理ユーザはセッションを終了させることができます。 |
| 保留中の変更のビューと展開の改善。 | 展開ウィンドウが変更され、展開される保留中の変更がより明確に表示されるようになりました。また、変更を破棄し、変更をクリップボードにコピーして、変更を YAML 形式のファイルでダウンロードするオプションが追加されました。さらに、監査ログで簡単に見つけることができるように、展開ジョブに名前を付けることが可能になりました。 |

| 機能 | 説明 |
|---|---|
| 監査ログ。 | 展開、システムタスク、設定の変更、管理ユーザのログイン/ログアウトなどのイベントを記録する監査ログを表示できます。**[デバイス（Device）] > [デバイス管理（Device Administration）] > [監査ログ（Audit Log）]** ページが追加されました。 |
| 設定をエクスポートする機能。 | 記録を保持するためにデバイス設定のコピーをダウンロードできます。ただし、この設定をデバイスにインポートすることはできません。この機能は、バックアップ/復元に代わるものではありません。**[デバイス（Device）] > [デバイス管理（Device Administration）] > [設定のダウンロード（Download Configuration）]** ページが追加されました。 |
| 未知の URL に関する URL フィルタリングの改善。 | アクセス制御ルールでカテゴリベースの URL フィルタリングを実行する場合、ユーザは、カテゴリとレピュテーションが URL データベースに定義されていない URL にアクセスする可能性があります。以前は、Cisco Collective Security Intelligence（CSI）からそれらの URL のカテゴリとレピュテーションのルックアップを実行するオプションを手動で有効にする必要がありました。現在は、このオプションがデフォルトで有効になっています。さらに、ルックアップの結果に関して存続可能時間（TTL）を設定できるようになりました。これにより、システムは、未知の URL ごとにカテゴリまたはレピュテーションを更新できるようになりました。**[デバイス（Device）] > [システム設定（System Settings）] > [URLフィルタリングの設定（URL Filtering Preferences）]** ページが更新されました。 |
| デフォルトで、セキュリティインテリジェンス ロギングが有効になりました。 | セキュリティインテリジェンス ポリシーは6.2.3 で導入され、ロギングはデフォルトで無効になっていました。6.3.0 以降、ロギングはデフォルトで有効になります。6.2.3 からアップグレードした場合、ロギング設定は有効または無効なまま保持されます。ポリシー適用結果を表示したい場合は、ロギングを有効にします。 |

| 機能 | 説明 |
|---|---|
| パッシブ モードインターフェイス | インターフェイスはパッシブ モードで設定できます。パッシブに機能する場合、インターフェイスは（ハードウェア デバイスの）スイッチそのものまたは（Firepower Threat Defense Virtual の）プロミスキャス VLAN に設定されたモニタリング セッションで送信元ポートからのトラフィックを単にモニタします。<br><br>パッシブ モードを使用すると、アクティブなファイアウォールとして展開した場合の Firepower Threat Defense Virtual デバイスの動作を評価できます。また、IDS（侵入検知システム）サービスが必要な実稼働ネットワーク（脅威について知る必要があるが、デバイスに脅威をアクティブに防止させない）でパッシブ インターフェイスを使用できます。物理インターフェイスの編集時やセキュリティ ゾーンの作成時にパッシブ モードを選択できます。 |
| OSPF に関する Smart CLI の機能拡張と、BGP のサポート。 | Smart CLI の OSPF 設定機能が拡張されました。これには、標準/拡張 ACL、ルート マップ、AS パス オブジェクト、IPv4/IPv6 プレフィックス リスト、ポリシー リスト、および標準/拡張コミュニティ リストに関する新しい Smart CLI オブジェクト タイプが含まれます。また、Smart CLI を使用して BGP ルーティングを設定できるようになりました。これらの機能は、**[デバイス（Device）] > [詳細設定（Advanced Configuration）]** ページから使用できます。 |
| ISA 3000 デバイスに関する機能拡張。 | ISA 3000 のアラーム、ハードウェア バイパス、および SD カードによるバックアップ/復元の各機能を設定できるようになりました。アラームとハードウェア バイパスの設定には FlexConfig を使用します。SD カードについては、Firepower Device Manager のバックアップ/復元ページが更新されました。 |
| FTD 6.3 以降での ASA 5506-X、5506W-X、5506H-X、および 5512-X のサポートの削除。 | Firepower Threat Defense の 6.3 以降のリリースを ASA 5506-X、5506W-X、5506H-X、および 5512-X にインストールすることはできません。これらのプラットフォームに関してサポートされる FTD の最後のリリースは 6.2.3 です。 |
| FTD REST API バージョン 2（v2）。 | ソフトウェア バージョン 6.3 用の FTD REST API のバージョン番号が 2 になりました。API の URL の v1 を v2 に置き換える必要があります。v2 の API には、ソフトウェア バージョン 6.3 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 |
| --- | --- |
| 製品の使用情報をシスコに提供するための Web 分析。 | ページのヒットに基づいて製品の使用情報を匿名でシスコに提供する Web 分析を有効にできます。この情報は、シスコが機能の使用状況パターンを確認し、製品を改善するのに使用されます。すべての使用状況データは匿名で、センシティブデータは送信されません。Web分析はデフォルトで有効になっています。<br>**[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 Web 分析が追加されました。 |
| Snortが再起動されない脆弱性データベース（VDB）の更新のインストール。 | VDB の更新のインストール時に Snort が自動的に再起動されなくなりました。ただし、Snortは、引き続き、次回の設定展開時に再起動します。 |
| Snort が再起動されない侵入ルール（SRU）データベースの更新の展開。 | 侵入ルール（SRU）の更新をインストールした後は、新しいルールを有効にするために設定を展開する必要があります。SRU の更新の展開時に Snort が再起動されなくなりました。 |

# 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、サポートされているすべてのFirepower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。

表 *1* : 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（6.3.0 のみ） | 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しなくなり、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。<br><br>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。<br><br>サポートはバージョン 6.3.0.1 で再導入されています。 |
| 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+ 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。 |
| 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）をバージョン 6.3+ 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。<br>• ASA 5506-X、5506H-X、5506W-X<br>• ASA 5512-X<br><br>ただし、新しいFMCで古いデバイスを管理することはできます。 |

表 *2 :* 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。<br><br>**自動設定の変更**<br><br>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 プロファイルまたはユーザ資格とスヌーズまたは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。<br><br>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。<br><br>**アップグレードの失敗の回避**<br><br>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。<br><br>• 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。<br><br>• 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。<br><br>• 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 |

| 機能 | 説明 |
| --- | --- |
| | 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。 |

# 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、新たに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 コンフィギュレーション ガイド』を参照してください。

**表 *3: 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：<br>• Default_DNS_Configure<br><br>関連するテキスト オブジェクト：<br>• defaultDNSNameServerList<br>• 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：<br>• TCP_Embryonic_Conn_Limit<br>• TCP_Embryonic_Conn_Timeout<br><br>関連するテキスト オブジェクト：<br>• tcp_conn_misc<br>• tcp_conn_limit<br>• 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 コンフィギュレーション ガイド』を参照してください。

**表 *4 : 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 *5 : 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。 |

| 非推奨メソッド | コマンド | 詳細 |
|---|---|---|
| 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。 |

# 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 *6 : 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 |
|---|---|---|
| 6.3.0 | **[分析（Analysis）] > [検索（Lookup）] > [Whois]** | **[分析（Analysis）] > [詳細（Advanced）] > [Whois]** |

| 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）] > [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）]** |