Cisco Firepower バージョン 6.3.0 リリース ノート

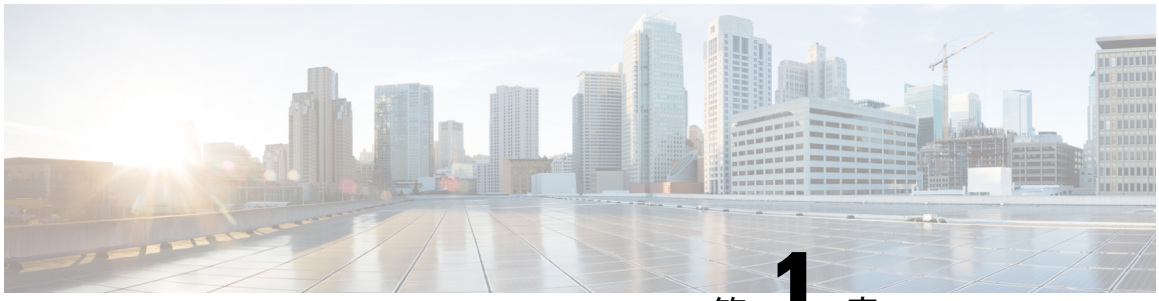
初版：2018 年 12 月 3 日

最終更新：2019 年 6 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

バージョン 6.3.0 の概要

Firepower をお選びいただき、ありがとうございます。

リリース ノートについて

リリース ノートには、アップグレードの警告や動作の変更など、バージョン 6.3.0 に関する重要なリリース固有の情報が記載されています。Firepower リリースに精通しており、Firepower 展開をアップグレードした経験がある場合でも、このドキュメントをお読みください。

Firepower 展開のアップグレードまたは新規インストール（再イメージ化）は、複雑なプロセスになる場合があります。ここで手順を説明する代わりに、リリース ノートでは適切なリソースを示しています。アップグレードとインストールの手順については、次のリンクを参照してください。

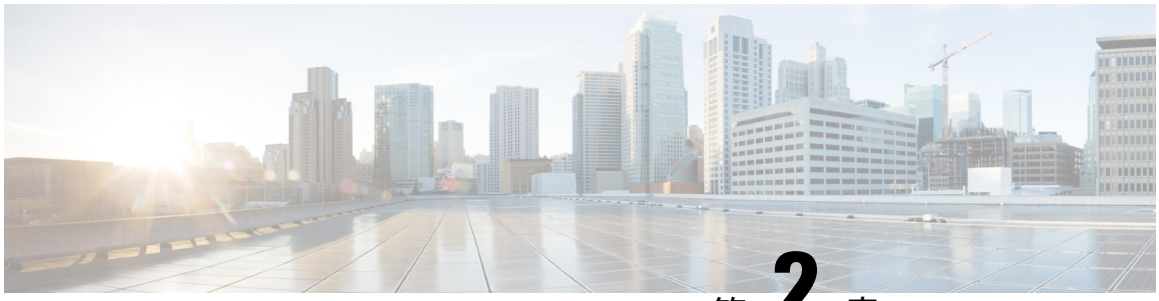
- アップグレード手順 （64 ページ）
- 設置手順 （72 ページ）

リリース日

シスコは、更新版ビルドを適宜リリースしています。各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。常に最新のビルドを使用する必要があります。以前のビルドをダウンロードした場合は使用しないでください。詳細については、「新しいビルドで解決済みの問題 （79 ページ）」を参照してください。

表 *1 :* バージョン *6.3.0* のリリース日

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：新規インストール
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	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/FMCv Firepower 4100/9300 を除くすべてのデバイス



第 2 章

互換性

この章では、Firepower バージョン 6.3.0の互換性に関する情報を提供します。

サポートされているすべての Firepower バージョン（バンドル コンポーネントと統合製品を含む）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。

Firepower Management Centerについて

バージョン 6.3.0 Firepower Management Center ソフトウェアは、物理および仮想プラットフォームでサポートされています。FMC は、すべての Firepower デバイスを管理できます。

Firepower Management Center 物理プラットフォーム：

- MC 1000、2500、4500
- MC 2000、4000
- MC 750、1500、3500

Firepower Management Center Virtual：

- VMware vSphere/VMware ESXi 6.0 および 6.5
- カーネルベース仮想マシン（KVM）
- Amazon Web Services（AWS）VPC/EC2

Firepower デバイス

バージョン6.3.0Firepowerデバイス ソフトウェアは、さまざまな物理および仮想プラットフォームでサポートされています。

- ソフトウェ アタイプ：一部の Firepower デバイスは Firepower Threat Defense（FTD）ソフトウェアを実行します。また、一部の Firepower デバイスは NGIPS/ASA FirePOWER ソフトウェアを実行します。一部のデバイスはいずれかのソフトウェアを実行できますが、両方を同時に実行することはできません。
- ローカルおよびリモート管理：すべての Firepower デバイスは、複数のデバイスを管理できる Firepower Management Center を使用したリモート管理をサポートします。また、一部のプラットフォームでは、ローカルの単一デバイス管理をサポートしています。Firepower Device Manager（FDM）、または ASDM を使用した ASA FirePOWER を使って FTD を管理することができます。一度に 1 つのデバイスに関して使用できる管理方法は 1 つだけです。
- オペレーティング システム：一部の Firepower 実装では、オペレーティング システムとソフトウェアがバンドルされます。その他の実装では、自分でオペレーティング システムをアップグレードする必要があります。バンドルされたオペレーティング システムのバージョンとビルドについては、Cisco Firepower Compatibility Guideの「Bundled Components」の情報を参照してください。

次の表は、バージョン 6.3.0 を実行している Firepower デバイスの互換性情報を示しています。ここでも、すべてのデバイスがリモート FMC 管理をサポートしていることに注意してください。

表 *2 :* バージョン *6.3.0* の *Firepower* デバイス

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
Firepower 2110、2120、2130、2140	FTD	FDM	—
Firepower 4110、4120、4140、4150 Firepower 9300 SM-24、SM-36、SM-44 モジュールを搭載	FTD	—	FXOS 2.4.1.214 以降のビルドが必要です。 個別のアップグレード。最初に FXOS をアップグレードします。 問題を解決するには、FXOS を最新のビルドにアップグレードする必要がある場合があります。判断のヒントについては、『Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)』を参照してください。

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
ISA 3000	FTD	FDM	—
ASA 5508-X、5516-X ASA 5515-X、5525-X、5545-X、5555-X	ASA FirePOWER（NGIPS）	ASDM	次のいずれかで実行されます。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.12(x) 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密にはASAのアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。
ASA 5585-X-SSP-10、-20、-40、-60	ASA FirePOWER（NGIPS）	ASDM	次のいずれかで実行されます。 • ASA 9.5(2)、9.5(3) • ASA 9.6(x) ～ 9.12(x) 個別のアップグレード。操作の順序については、『Cisco ASA Upgrade Guide』を参照してください。 ASA と ASA FirePOWER のバージョンには幅広い互換性があります。ただし、厳密にはASAのアップグレードが必要でない場合でも、問題解決のために、サポートされた最新のバージョンへのアップグレードが必要になることがあります。

デバイスのプラットフォーム	ソフトウェア	ローカル管理	OS/ハイパーバイザ
FTDv	FTD	FDM（VMware および KVM のみ）	次のいずれかで実行されます。 • VMware vSphere/VMware ESXi 6.0 または 6.5 • KVM • AWS • Microsoft Azure
NGIPSv	NGIPS	—	VMware vSphere/VMware ESXi 6.0 または 6.5 が必要
Firepower 7010、7020、7030、7050 Firepower 7110、7115、7120、7125 Firepower 8120、8130、8140 Firepower 8250、8260、8270、8290 Firepower 8350、8360、8370、8390 AMP 7150、8050、8150 AMP 8350、8360、8370、8390	NGIPS	選択した管理機能のためのローカル GUI が制限されています。	—

マネージャとデバイスの互換性

FMC で管理対象デバイスと同じバージョンかそれよりも後のバージョンを実行することを強くお勧めします。これにはパッチが含まれます。バージョンが混在する展開はサポートされていますが、新機能および解決済みの問題は、多くの場合、FMC およびその管理対象デバイス上に最新バージョンがあることが必要です。

表 *3:* バージョン *6.3.0* のマネージャとデバイスの互換性

Firepower Management Center		
バージョン 6.3.0 FMC	管理可能	バージョン 6.1 ～ 6.3.0.x のデバイス
バージョン 6.3.0 のデバイス	必須	バージョン 6.3.0 FMC
Firepower Device Manager		

バージョン 6.3.0 FDM	管理可能	1 つの FTD デバイス
ASDM		
バージョン 7.10.1 の ASDM	管理可能	バージョン 5.3.x ～ 6.3.0 ASA FirePOWER モジュール
バージョン 6.3.0 ASA FirePOWER モジュール	必須	バージョン 7.10.1 の ASDM

Web ブラウザの互換性

Firepower によってモニタされるネットワークからの Web の参照

多くのブラウザでは、デフォルトで Transport Layer Security（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、モニタ対象ネットワーク内のユーザが 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することがあります。

詳細については、『*Failures loading websites using TLS 1.3 with SSL inspection enabled*』というタイトルのソフトウェア アドバイザリを参照してください。

Firepower Web インターフェイスの使用

Firepower Web インターフェイスは、よく使われているさまざまなブラウザでテストされています。リストされていないブラウザで問題が発生した場合は、テスト済みのブラウザ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。

（注） SSL 証明書を使用すると、FMC（および 7000/8000 シリーズ デバイス）でアプライアンスとブラウザ間に暗号化チャネルを確立できます。デフォルトでは、システムに自己署名 HTTPS サーバ証明書が付属しています。この証明書を、グローバルに知られているか、内部で信頼されている認証局（CA）によって署名された証明書に置き換えることをお勧めします。カスタム サーバ証明書要求を生成し、[HTTPS証明書（HTTPS Certificates）] ページでカスタム サーバ証明書をインポートすることができます。**[システム（System）] > [設定（Configuration）]** を選択し、[HTTPS証明書（HTTPS Certificates）] をクリックします。詳細については、オンライン ヘルプまたは『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 : Firepower Web* インターフェイスでテストされたブラウザ

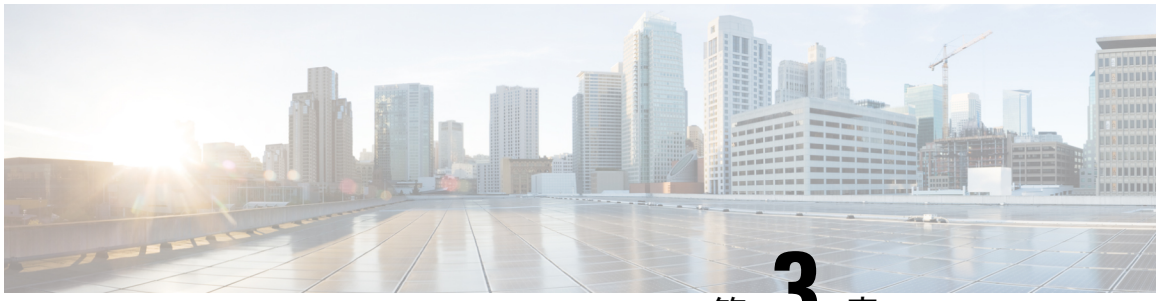
ブラウザ	必要な設定と追加の警告
Google Chrome	JavaScript、Cookie Chrome は、画像、CSS、JavaScript などの静的コンテンツを、システムによって提供される自己署名証明書とともにキャッシュしません。これにより、特に低帯域幅環境では、ページの読み込み時間が長くなります。自己署名証明書を置き替えない場合は、代わりに、自己署名証明書をブラウザまたは OS の信頼ストアに追加できます。
Mozilla Firefox	JavaScript、Cookie、TLS v1.2 これらを更新すると、Firefoxは、システムが提供する自己署名証明書を信頼しなくなる場合があります。証明書を置き換えない場合、ログイン ページがロードされないときは Firefox を更新します。Firefox の検索バーに「**`about:support`**」と入力し、[Refresh Firefox] をクリックします。一部の設定が失われます。Refresh Firefox サポート ページを参照してください。
Microsoft Internet Explorer 10 および 11（Windows）	JavaScript、Cookie、TLS v1.2、128 ビット暗号化 [Check for newer versions of stored pages] 閲覧履歴オプションについては、[Automatically] を選択してください。 [Include local directory path when uploading files to server] カスタム セキュリティ設定を無効にします（Internet Explorer 11 のみ）。 Firepower Web インターフェイスの IP アドレス/URL の互換表示を有効にします。
Apple Safari 10 および 11（MacOS）	Firepower Device Manager のみでテストされています。
Microsoft Edge（Windows）	テストされていません。

画面解像度の要件

表 *5 : Firepower* ユーザ インターフェイスの画面解像度の要件

インターフェイス	解像度
Firepower Management Center	幅 1280 ピクセル
7000/8000 シリーズ デバイス（制限されたローカル インターフェイス）	幅 1280 ピクセル

インターフェイス	解像度
Firepower Device Manager	幅 1024 ピクセル、高さ 768 ピクセル
ASA FirePOWER モジュールを管理している ASDM ASA FirePOWER モジュール	幅 1024 ピクセル、高さ 768 ピクセル
Firepower Chassis Manager Firepower 4100/9300 シャーシ向け Firepower Chassis Manager Firepower 4100/9300 シャーシ	幅 1024 ピクセル、高さ 768 ピクセル



第 3 章

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。 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。 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。 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）]** 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。 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）]** 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。 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）]** 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。 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）]** 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
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。 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。 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。 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 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 新規/変更された [Firepower Chassis Manager] 画面： • **[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	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。 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）]** 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/変更された画面： • **[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）] 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
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。 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
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。 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。 • 第 1 要素：任意の RADIUS または LDAP/AD サーバ • 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 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
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/変更された画面： • **[システム（System）] > [統合（Integration）] > [パケット アナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケット アナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [クエリパケットアナライザ（Query Packet Analyzer）]

機能	説明
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。 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。 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。 • 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。 • 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）。
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。 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。 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。 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 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。 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 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。 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）] > [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	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。 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。 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 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。 • **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。 新規/変更された画面：**[System] > [Configuration]** > [ユーザ設定（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。 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。 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）]** 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 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。 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。 • **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**：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。 新規/変更された画面： • **[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（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
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。 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 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。 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。 **[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。 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。 **[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。 **[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。 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。 **[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 *6* : 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。 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。
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。 • ASA 5506-X、5506H-X、5506W-X • ASA 5512-X 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 *7:* 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。 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

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 *8 : 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 コンフィギュレーション ガイド』を参照してください。

表 *9 : 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 *10 : 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。

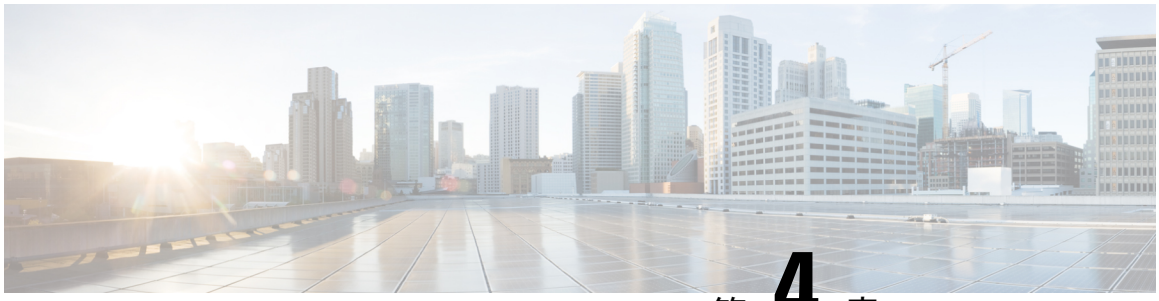
メニューの変更

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 *11 : 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）]**



第 4 章

バージョン 6.3.0 へのアップグレード

この章では、バージョン 6.3.0 の重要なリリースに固有の情報を提供します。

また、新機能、廃止された機能とプラットフォーム、メニューと用語の変更、ブラックリストに登録された FlexConfig コマンドなどの情報に関して「特長と機能 （11 ページ）」に目を通す必要があります。

バージョン6.2.3に関するガイドラインと警告バージョン6.3.0

このチェックリストには、バージョン 6.3.0 に関する新しい重要なアップグレード ガイドラインと警告が含まれています。

表 *12* : バージョン *6.3.0* の新しいガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	バージョン 6.3+ に再イメージ化すると、ほとんどのアプライアンスで LOM が無効になる。 （45 ページ）	FMC（物理） Firepower 7000/8000 シリーズ	任意	6.3.0 以降

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 4100/9300 では FXOS のアップグレードの前に FTD プッシュが必要 （43 ページ）	Firepower 4100/9300	6.1.x	6.3.0 のみ
	FMC、7000/8000 シリーズ、NGIPSv で準備状況チェックに失敗する可能性 （38 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ～ 6.1.0.6 6.2.0 ～ 6.2.0.6 6.2.1 6.2.2 ～ 6.2.2.4 6.2.3 ～ 6.2.3.4	6.3.0+
	名前が変更されたアップグレードとインストール パッケージ （42 ページ）	FMC Firepower 7000/8000 シリーズ NGIPSv	6.1.0 ～ 6.2.3.x	6.3.0+
	アプライアンスへのアクセスの更新されたセキュリティ （39 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0+
	セキュリティ インテリジェンスによって可能になるアプリケーションの識別 （39 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0+
	アップグレード後に VDB を更新して CIP 検出を有効化 （39 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0+
	無効な侵入変数セットによって展開に失敗する可能性 （40 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0+
	接続イベントと侵入イベントに関する Syslog の動作の変更 （41 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0+
	FMC および ASA FirePOWER へのバージョン 6.3.0-83 アップグレードに失敗する可能性 （45 ページ）	FMC ASDM を使用した ASA FirePOWER	6.1.0 ～ 6.2.3.x	6.3.0 のみ
	アップグレードでの TLS/SSL ハードウェア アクセラレーションの有効化 （44 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.1.0 ～ 6.2.3.x	6.3.0 のみ

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	URL フィルタリング キャッシュのタイムアウトが変更される可能性（41 ページ）	任意	6.2.3.x	6.3.0+
	MC1000、2500、および 4500 用プレインストール ホットフィックス（必須） （37 ページ）	MC1000、2500、および 4500	6.2.x	6.3.0+
	リモート アクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性（40 ページ）	FMC を使用した FTD	6.2.x	6.3.0+
	FTD/FDM アップグレード時に削除されるデータ レポート機能 （44 ページ）	FDM を使用した FTD	6.2.x	6.3.0 のみ

MC1000、2500、および4500用プレインストールホットフィックス（必須）

展開： Firepower Management Center モデル MC1000、2500、および 4500

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 +

MC1000、MC2500、または MC4500 をバージョン 6.2.x からバージョン 6.3 + にアップグレードする前に、プレインストールホットフィックスを適用する必要があります。このホットフィックスにより、RAID コントローラのファームウェアが更新されます。ホットフィックスを適用しないと、バージョン 6.3+ を実行している、影響を受けるアップグレード済み FMC でパフォーマンス上の問題が発生する可能性があります。その他のアプライアンス（バージョン 6.3+ の新しい FMC または再イメージ化された FMC を含む）にはホットフィックスを適用しないでください。

ホットフィックスは シスコ サポートおよびダウンロード サイト で入手可能であり、お使いの現在のバージョンのアップグレード パッケージおよびインストール パッケージと同じ場所にあります。ホットフィックスを適用するには、通常のアップグレード ページ（**[システム（System）] > [更新（Updates）]**）を使用します。

表 *13 :* プレインストール ホットフィックス パッケージ

現在のバージョン	ホットフィックス	パッケージ
6.3+	—	ホットフィックスを適用せずに 6.3+ にアップグレードした場合は、Cisco TAC に連絡してください。
6.2.3.x	ホットフィックス AJ	Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.2.3.999-5.sh.REL.tar
6.2.2.x	ホットフィックス BY	Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1.sh.REL.tar
6.2.1	—	バージョン 6.2.3 にアップグレードし、ホットフィックス AJ を適用します。
6.2.0.x	ホットフィックス CD	Sourcefire_3D_Defense_Center_S3_Hotfix_CD-6.2.0.999-1.sh

FMC、7000/8000シリーズ、NGIPSvで準備状況チェックに失敗する可能性

展開：FMC、7000/8000 シリーズ デバイス、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.1.0.6、バージョン 6.2.0 ～ 6.2.0.6、バージョン 6.2.1、バージョン 6.2.2 ～ 6.2.2.4、およびバージョン 6.2.3 ～ 6.2.3.4

直接アップグレード先：バージョン 6.3 +

次に示すバージョンの Firepower のいずれかからアップグレードする場合は、そこに示されているモデルで準備状態チェックを実行できません。これは、準備状況チェック プロセスが新しいアップグレード パッケージに対して互換性を持たないためです。

表 *14 :* バージョン *6.3 +* 用の準備状況チェックを備えたパッチ

準備完了チェックがサポートされない	修正された最初のパッチ
6.1.0 ～ 6.1.0.6	6.1.0.7
6.2.0 ～ 6.2.0.6	6.2.0.7
6.2.1	なし。バージョン 6.2.3.5+ にアップグレードしてください。
6.2.2 ～ 6.2.2.4	6.2.2.5
6.2.3 ～ 6.2.3.4	6.2.3.5

アプライアンスへのアクセスの更新されたセキュリティ

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

セキュリティを強化するために、バージョン 6.3 では、セキュア 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が更新されました。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。

セキュリティインテリジェンスによって可能になるアプリケーションの識別

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

バージョン 6.3 では、セキュリティ インテリジェンスの設定によりアプリケーションの検出と識別が可能になります。現在の展開で検出を無効にした場合は、アップグレード プロセスによって再び検出が有効になる可能性があります。必要がない場合（たとえば、IPS のみの展開など）に検出を無効にするとパフォーマンスが向上する可能性があります。

検出を無効にするには、次の手順を実行する必要があります。

- ネットワーク検出ポリシーからすべてのルールを削除します。
- 単純なネットワークベースの条件（ゾーン、IP アドレス、VLAN タグ、およびポート）のみを使用してアクセス制御を実行します。どんな種類のアプリケーション、ユーザ、URL、または地理位置情報の制御も行わないでください。
- （新規）デフォルトのグローバル リストなど、アクセス コントロール ポリシーのセキュリティ インテリジェンス設定からすべてのホワイトリストとブラックリストを削除することで、ネットワークと URL ベースのセキュリティ インテリジェンスを無効にします。
- （新規）DNS のデフォルトのグローバル ホワイトリストや DNS ルールのグローバル ブラックリストなど、関連付けられている DNS ポリシー内のすべてのルールを削除または無効にすることで、DNS ベースのセキュリティ インテリジェンスを無効にします。

アップグレード後に VDB を更新して CIP 検出を有効化

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3 +

脆弱性データベース（VDB）299 以降を使用しているときにアップグレードする場合、アップグレード プロセスの問題により、アップグレード後の CIP 検出を使用できなくなります。これには、2018 年 6 月から現在までにリリースされたすべての VDB に加えて、最新の VDB も含まれます。

アップグレード後は常に脆弱性データベース（VDB）を最新バージョンに更新することを推奨しますが、この場合は特に重要です。

この問題の影響を受けるかどうかを確認するには、CIPベースアプリケーションの条件を使用して、アクセス制御ルールを設定してみてください。ルール エディタで CIP アプリケーションが見つからない場合は、手動で VDB を更新します。

無効な侵入変数セットによって展開に失敗する可能性

展開：すべて

アップグレード元：バージョン 6.1 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

侵入変数セット内のネットワーク変数については、除外する IP アドレスが、含める IP アドレスのサブセットである必要があります。次の表に、有効な設定と無効な設定の例を示します。

有効	無効
含める：10.0.0.0/8 除外する：10.1.0.0/16	含める：10.1.0.0/16 除外する：172.16.0.0/12 除外する：10.0.0.0/8

バージョン 6.3.0 より前のバージョンでは、このタイプの無効な設定でネットワーク変数を正常に保存できました。現在のバージョンでは、これらの設定によって展開がブロックされ、次のエラーが表示されます。「`Variable set has invalid excluded values.`」

この場合は、正しく設定されていない変数セットを識別して編集してから展開しなおしてください。変数セットによって参照されているネットワーク オブジェクトおよびグループの編集が必要である場合もあることに注意してください。

リモート アクセス VPN のデフォルト設定の変更によって VPN トラフィックがブロックされる可能性

展開：**リモート アクセス VPN 用に設定された** Firepower Threat Defense

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 +

バージョン6.3では非表示オプションの **sysopt connection permit-vpn** のデフォルト設定が変更されています。アップグレードすると、リモート アクセス VPN がトラフィックを渡さなくなる可能性があります。この場合は、次のいずれかの手法を使用してください。

- **sysopt connection permit-vpn** コマンドを設定する FlexConfig オブジェクトを作成します。このコマンドの新しいデフォルトは **no sysopt connection permit-vpn** です。

  これは、外部ユーザがリモート アクセス VPN アドレス プール内の IP アドレスになりすますことができないため、VPN でトラフィックを許可するよりも安全な方法です。欠点は VPN トラフィックが検査されないことです。つまり、侵入とファイルの保護、URL フィルタリング、その他の高度な機能がトラフィックに適用されません。

- リモート アクセス VPN アドレス プールからの接続を許可するアクセス制御ルールを作成します。

  この方法では、VPN トラフィックが確実に検査され、高度なサービスを接続に適用できます。欠点は、外部のユーザが IP アドレスをスプーフィングして、内部ネットワークにアクセスしやすくなることです。

URL フィルタリング キャッシュのタイムアウトが変更される可能性

展開：すべて

アップグレード元：バージョン 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

バージョン 6.3.0 の新機能として、GUI で URL フィルタリング キャッシュのタイムアウト値を設定できます。古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。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。

アップグレード完了後、

- FMC：**[システム（System）]** > **[統合（Integration）]** を選択し、[Cisco CSI] タブをクリックして、[キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定を確認します。
- FDM：**[システム設定（System Settings）]** > **[トラフィック設定（Traffic Settings）]** > **[URL フィルタリングの設定（URL Filtering Preferences）]** を選択し、[URL存続可能時間（URL Time to Live）] 設定を確認します。

接続イベントと侵入イベントに関する Syslog の動作の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0+

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。アクセス コントロール ポリシーの新しい [ロギング（Logging）] タブでこれらの設定にアクセスできます。

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、バージョン6.3.0+にアップグレードすると、侵入ポリシーによって、Syslogイベントが新しい[ロギング（Logging）]タブ上の宛先に送信されるためです（バージョン6.3.0以前では、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）。

また、NGIPSデバイス（7000/8000シリーズ、ASA FirePOWER、NGIPSv）から送信されるメッセージで、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。

名前が変更されたアップグレードとインストール パッケージ

展開： FMC、7000/8000 シリーズ、NGIPSv

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3 +

アップグレード、パッチ、ホットフィックス、およびインストールパッケージの命名スキーム（名前の最初の部分）は、当該プラットフォーム上で「Version 6.3.0」で始まるように変更されました。

（注） この変更により、古い物理アプライアンス（DC750、1500、2000、3500、4000のほか、7000/8000シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。バージョン5.x を現在実行していて、これらのアプライアンスのいずれかにバージョン 6.3.0 または 6.4.0 を新規インストールする必要がある場合は、シスコ サポートおよびダウンロード サイト からインストール パッケージをダウンロードした後、その名前を「古い」名前に変更します。

表 *15 :* 命名スキーム：アップグレード、パッチ、およびホットフィックス パッケージ

プラットフォーム	命名方式
FMC	**新**： Cisco_Firepower_Mgmt_Center **旧**： Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 シリーズ	**新**： Cisco_Firepower_NGIPS_Appliance **旧**： Sourcefire_3D_Device_S3
NGIPSv	**新**： Cisco_Firepower_NGIPS_Virtual **旧**： Sourcefire_3D_Device_VMware **旧**： Sourcefire_3D_Device_Virtual64_VMware

表 *16 :* 命名スキーム：インストール パッケージ

プラットフォーム	命名方式
FMC （物理）	新： Cisco_Firepower_Mgmt_Center 旧： Sourcefire_Defense_Center_M4 旧： Sourcefire_Defense_Center_S3
FMCv: VMware	新： Cisco_Firepower_Mgmt_Center_Virtual_VMware 旧： Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	新： Cisco_Firepower_Mgmt_Center_Virtual_KVM 旧： Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 シリーズ	新： Cisco_Firepower_NGIPS_Appliance 旧： Sourcefire_3D_Device_S3
NGIPSv	新： Cisco_Firepower_NGIPSv_VMware 旧： Cisco_Firepower_NGIPS_VMware

Firepower 4100/9300 では FXOS のアップグレードの前に FTD プッシュが必要

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：FXOS 2.0.1、2.1.1、または 2.3.1 上のバージョン 6.1.x

直接アップグレード先：FXOS 2.4.1 上のバージョン 6.3.0

Firepower Management Center がバージョン 6.2.3+ を実行している場合は、アップグレードの前に Firepower アップグレード パッケージを管理対象デバイスにプッシュ（コピー）することを強くお勧めします。これにより、アップグレード メンテナンス ウィンドウの長さを縮小できます。

FTD を搭載した Firepower 4100/9300 の場合、必要な付属する FXOS のアップグレードを開始する前にプッシュすることをお勧めします。また、バージョン 6.1 からバージョン 6.3+ に直接アップグレードする場合は、このプッシュが必須です。FXOS をアップグレードする前にプッシュする必要があります。

これは、Firepower 6.1 を実行したまま FXOS をバージョン 2.4.1 にアップグレードすると、デバイス管理ポートがフラップする（そのため、デバイスと FMC の間で断続的な通信上の問題が発生する）ためです。「sftunnel daemon exited」というアラームが表示される可能性があり、長時間の通信をともなうタスク（大規模なアップグレードパッケージのプッシュなど）が失敗する可能性があります。

FTD を搭載した Firepower 4100/9300 をアップグレードするには、必ず次の手順に従ってください。

1. FMC をターゲット バージョンにアップグレードします。
2. シスコ サポートおよびダウンロード サイト からデバイス アップグレード パッケージを取得し、それを FMC にアップロードします。
3. FMC を使用してアップグレード パッケージをデバイスにプッシュします。
4. プッシュが完了したら、FXOS をターゲット バージョンにアップグレードします。
5. すぐに、FMC を使用してデバイス上の Firepower ソフトウェアをアップグレードします。

   Firepower ソフトウェアをアップグレードするまでは、管理ポートのフラップが発生する可能性があることに注意してください。

FTD/FDM アップグレード時に削除されるデータ レポート機能

展開：Firepower Device Manager

アップグレード元：バージョン 6.2.x

直接アップグレード先：バージョン 6.3 のみ

短期間のデータをレポートする機能が、バージョン 6.3 のアップグレード時に削除されます。アップグレード後に、アップグレード前の日の短い時間範囲をクエリしようとすると、利用可能なデータに合わせてクエリが調整されます。たとえば、ある日の午後 1 ～ 3 時をクエリした場合、システムに 24 時間データしかないと、その日全体がレポートされます。

アップグレードでの TLS/SSL ハードウェア アクセラレーションの有効化

展開：Firepower 2100 シリーズ、Firepower 4100/9300 シャーシ

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0 のみ

アップグレード プロセスにより、対象デバイスの TLS/SSL ハードウェア アクセラレーション（TLS 暗号化アクセラレーションと呼ばれる場合もあります）が自動的に有効になります。この機能は、導入されたバージョン 6.2.3 では Firepower 4100/9300 シャーシ 上でデフォルトで無効になっており、Firepower 2100 シリーズのデバイスでは利用できませんでした。

トラフィックを復号しない管理対象デバイスで TLS/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この機能を無効にすることをお勧めします。

無効にするには、次の CLI コマンドを使用します。

```
system support ssl-hw-offload disable
```

バージョン6.3+に再イメージ化すると、ほとんどのアプライアンスでLOMが無効になる。

展開：物理 FMC、7000/8000 シリーズ デバイス

再イメージ化元：バージョン 6.0+

直接アップグレード先：バージョン 6.3 +

バージョン 6.3+ を新規インストールすると、セキュリティ上の理由から、ほとんどのアプライアンスの Lights-Out 管理（LOM）設定が自動的に削除されます。いくつかの古い FMC モデルでは、管理ネットワーク設定とともにLOM設定を保持するオプションが用意されています。

バージョン 6.3+ の再イメージ化中にネットワーク設定を削除する場合は、初期設定を実行するためにアプライアンスに物理的にアクセスできることを確認する必要があります。LOM を使用することはできません。初期設定を実行した後、LOM とLOMユーザを再度有効にすることができます。

表 *17 : LOM* 設定への再イメージ化の影響

プラットフォーム	バージョン6.2.3以前への再イメージ化	バージョン6.3+への再イメージ化
MC1000、2500、4500 MC2000、4000	削除されない	常に削除される
MC750、1500、3500	ネットワーク設定を削除すると削除される	ネットワーク設定を削除すると削除される
7000/8000 シリーズ	常に削除される	常に削除される

FMC および ASA FirePOWER へのバージョン 6.3.0-83 アップグレードに失敗する可能性

展開： Firepower Management Center、ASA FirePOWER（ローカル管理）

アップグレード元：バージョン 6.1.0 ～ 6.2.3.x

直接アップグレード先：バージョン 6.3.0-83

一部の Firepower Management Center およびローカル（ASDM）管理された ASA FirePOWER モジュールでは、バージョン 6.3.0、ビルド 83 でのアップグレードに失敗していました。この問題は、バージョン 5.4.x からアップグレードした一部のお客様に限られていました。詳細については、シスコのバグ検索ツールで CSCvn62123 を参照してください。

新しいアップグレードパッケージが利用可能になりました。バージョン6.3.0-83 アップグレードパッケージをダウンロードした場合は、使用しないでください。この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

以前に公開されたガイドラインと警告

アップグレードパスでメジャーバージョンがスキップされる場合は、このチェックリストを確認してください。いくつかの以前のメジャーバージョンからバージョン6.3.0にアップグレードできます。アップグレードする最小バージョン （51 ページ）を参照してください。

表 *18 :* 以前に公開されたガイドライン

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	アクセスコントロールではSRUから遅延ベースのパフォーマンス設定を取得可能 （48 ページ）	FMC	6.1.x	6.2.0+
	FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え （49 ページ）	FMC を使用した FTD	6.1.x	6.2.0+
	バージョン 6.2.0 からの FDM アップグレードが失敗する可能性 （48 ページ）	FDM を使用した FTD	6.2.0 のみ	6.2.2+
	レポートの結果の制限の変更 （47 ページ）	FMC	6.1.0 ～ 6.2.2.x	6.2.3+
	アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除 （46 ページ）	FTD クラスタ	6.1.x	6.2.3+
	アップグレードにより CSSM から FTD/FDM を登録解除することが可能 （47 ページ）	FDM を使用した FTD	6.2.0 ～ 6.2.2.x	6.2.3+

アップグレードの前にバージョン 6.1.x FTD クラスタからサイト ID を削除

展開： Firepower Threat Defenseクラスタ

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2.3+

Firepower Threat Defense バージョン 6.1.x クラスタは、サイト間クラスタリングをサポートしていません（バージョン 6.2.0 以降では FlexConfig を使用してサイト間機能を設定できます）。

FXOS 2.1.1 でバージョン 6.1.x クラスタを展開または再展開している場合、（サポートされていない）サイト ID の値を入力しているときは、アップグレードする前に、FXOS の各ユニットでサイト ID を削除（**0** に設定）する必要があります。そうしないと、アップグレード後、ユニットがクラスタに再度参加できなくなります。

すでにアップグレード済みの場合は、サイト ID を各ユニットから削除してからクラスタを再確立します。サイト ID を表示または変更するには、『Cisco FXOS CLI Configuration Guide』を参照してください。

レポートの結果の制限の変更

展開：Firepower Management Center

アップグレード元：バージョン 6.1 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3+

バージョン 6.2.3 では、次のように、使用できる結果の数、またはレポートの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。

表 *19*：レポートの結果の新しい制限

レポート セクション タイプ	最大レコード数：**HTML** または **CSV** レポート セクション	最大レコード数：**PDF** レポート セクション
棒グラフ 円グラフ	100（上位または下位）	100（上位または下位）
テーブル ビュー	400,000	100,000
詳細ビュー	1,000	500

Firepower Management Center 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 よりも大きい結果数を指定する場合は、アップグレード プロセスが設定を新しい最大値に下げます。

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。

アップグレードにより CSSM から FTD/FDM を登録解除することが可能

導入：FDM を使用した FTD

アップグレード元：バージョン 6.2 ～ 6.2.2.x

直接アップグレード先：バージョン 6.2.3+

Firepower Device Manager によって管理されている Firepower Threat Defense デバイスをアップグレードすると、そのデバイスが Cisco Smart Software Manager から登録解除される場合があります。アップグレードが完了したら、ライセンスのステータスを確認します。

ステップ 1 [デバイス（Device）] をクリックし、[スマートライセンスの概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 2 デバイスが登録されていない場合は、[デバイスの登録（Register Device）] をクリックします。

バージョン 6.2.0 からの FDM アップグレードが失敗する可能性

展開：FDM を使用した FTD（メモリが少ない ASA 5500-X シリーズ デバイスで実行）

アップグレード元：バージョン 6.2.0

直接アップグレード先：バージョン 6.2.2+

バージョン 6.2.0 からアップグレードする場合、アップグレードに失敗し、「`Uploaded file is not a valid system upgrade file`」というエラーが表示される可能性があります。これは、正しいファイルを使用している場合でも発生する可能性があります。

この場合は、次の回避策を試してください。

- 再度試す。
- CLI を使用してアップグレードする。
- まず 6.2.0.1 にアップグレードする。

アクセス コントロールでは SRU から遅延ベースのパフォーマンス設定を取得可能

展開：FMC

アップグレード元：6.1.x

直接アップグレード先：6.2+

バージョン 6.2+ の新しいアクセス コントロール ポリシーでは、デフォルトで、最新の侵入ルール更新（SRU）から遅延ベースのパフォーマンス設定が取得されます。この動作は、新しい [設定の適用元（Apply Settings From）] オプションによって制御されます。このオプションを設定するには、アクセス コントロール ポリシーを編集または作成して、[詳細設定（Advanced）] をクリックし、遅延ベースのパフォーマンス設定を編集します。

バージョン 6.2+ にアップグレードすると、現在の（バージョン 6.1.x）設定に従って新しいオプションが設定されます。現在の設定が次の場合、新しいオプションが設定されます。

- [デフォルト（Default）]：新しいオプションは、[インストール済みのルールの更新（Installed Rule Update）] に設定されます。アップグレードしてから展開すると、最新の SRU からの遅延ベースのパフォーマンス設定が使用されます。最新の SRU が指定する内容によって、トラフィックの処理が変更される可能性があります。
- [カスタム（Custom）]：新しいオプションは、[カスタム（Custom）] に設定されます。システムは現在のパフォーマンス設定を保持します。このオプションによって動作が変更されることはありません。

アップグレードする前に設定を確認することをお勧めします。前述したように、バージョン 6.1.x の FMC Web インターフェイスから、ポリシーの遅延ベースのパフォーマンス設定を表示し、[デフォルトに戻す（Revert To Defaults）] ボタンがグレー表示されているかどうかを確認します。ボタンがグレー表示されている場合は、デフォルト設定が使用されています。ボタンがアクティブになっている場合は、カスタム設定が設定されています。

FTD での「フェールセーフ」から「Snort フェール オープン」への置き換え

展開：FMC を使用した FTD

アップグレード元：バージョン 6.1.x

直接アップグレード先：バージョン 6.2+

バージョン 6.2 では、Snort フェール オープン設定により、FMC によって管理される Firepower Threat Defense デバイスのフェールセーフ オプションが置き換えられます。フェールセーフでは、Snort がビジー状態のときにトラフィックをドロップすることができますが、Snort がダウンしている場合、トラフィックはインスペクションなしで自動的に通過します。Snort フェール オープンでは、このトラフィックをドロップすることができます。

FTD デバイスをアップグレードすると、その新しい Snort フェール オープン設定は、以下のように、古いフェールセーフ設定に依存します。新しい設定ではトラフィックの処理が変更されることはありませんが、アップグレードの前にフェールセーフを有効または無効にするかどうかを検討してください。

表 *20 :* フェールセーフの *Snort* フェール オープンへの移行

バージョン 6.1 のフェールセーフ	バージョン 6.2 の Snort フェール オープン	動作
無効（デフォルトの動作）	[ビジー（Busy）]：無効 [ダウン（Down）]：有効	Snort プロセスがビジー状態の場合は、新規および既存の接続をドロップし、Snort プロセスがダウンしている場合は、接続をインスペクションなしで通過します。
有効	[ビジー（Busy）]：有効 [ダウン（Down）]：有効	Snort プロセスがビジー状態またはダウンしている場合、新規または既存の接続をインスペクションなしで通過します。

Snort フェール オープンでは、デバイスにバージョン 6.2 が必要であることに注意してください。バージョン 6.1.x のデバイスを管理している場合、FMC Web インターフェイスにフェールセーフ オプションが表示されます。

一般的なガイドラインと警告

これらの重要なガイドラインと制限事項は、すべてのアップグレードに適用されます。ただし、このリストは包括的なものではありません。アップグレード パスの計画、OS のアップグレード、準備状況チェック、バックアップ、メンテナンス期間など、アップグレードプロセスに関するその他の重要な情報へのリンクについては、「アップグレード手順 （64 ページ）」を参照してください。

アプライアンス アクセス

Firepower デバイスは、（インターフェイス設定に応じて）アップグレード中、またはアップグレードが失敗した場合に、トラフィックを渡すことを停止できます。Firepower デバイスをアップグレードする前に、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。Firepower Management Center 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

署名付きのアップグレード パッケージ

Firepower では、正しいファイルを使用していることを確認できるようにするために、バージョン 6.2.1+ からのアップグレードパッケージ（およびバージョン 6.2.1+ へのホットフィックス）は、署名付きの tar アーカイブ（.tar）になっています。以前のバージョンからのアップグレードでは、引き続き未署名のパッケージが使用されます。

シスコ サポートおよびダウンロードサイトからアップグレードパッケージを手動でダウンロードする場合（たとえば、メジャーアップグレードやエアギャップ展開のために）、正しいパッケージをダウンロードしていることを確認してください。 署名付きの（.tar）パッケージは解凍しないでください。

（注） 署名付きのアップグレードパッケージをアップロードした後、システムがパッケージを確認する際に、GUI のロードに数分かかることがあります。表示を高速化するには、署名付きのパッケージが不要になった後、それらのパッケージを削除します。

ASA FirePOWER デバイスでの ASA REST API の無効化

ASA FirePOWER モジュールをアップグレードする前に、ASA REST API を無効にしていることを確認します。無効にしていない場合、アップグレードが失敗することがあります。ASA CLI から：`no rest api agent`。アンインストール後に再度有効にすることができます：`rest-api agent`。

アップグレード中および後のシスコとのデータ共有

バージョン 6.2.3+ の機能には、シスコとのデータ共有が含まれます。

Cisco Network Participation 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。アップグレード中に、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。

Web 分析のトラッキングは、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、ユーザの場所、FMC 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送信します。バージョン 6.1 ～ 6.2.2.x からアップグレードする場合、アップグレードによって Web 分析トラッキングが有効になります。このデータの収集を拒否する場合は、アップグレード後にオプト アウトできます（バージョン 6.2.3.x からアップグレードする場合、アップグレード プロセスでは現在の設定が保持されます）。

応答しないアップグレード

アップグレードしているアプライアンスとの間での変更の展開、またはアップグレードしているアプライアンスの手動での再起動やシャットダウンは行わないでください。進行中のアップグレードを再開しないでください。事前のチェック中に、アップグレードプロセスが停止しているように見える場合がありますが、これは想定内の動作です。アップグレードに失敗する、アプライアンスが応答しないなど、アップグレードで問題が発生した場合には Cisco TAC にお問い合わせください。

アップグレードする最小バージョン

いくつかの以前のメジャー バージョン シーケンスからバージョン 6.3.0 に直接アップグレードできます。アップグレードするために、以前のバージョンの最新のパッチを実行する必要はありません。

表 *21 : Firepower* ソフトウェアをバージョン *6.3.0* にアップグレードするための最小バージョン

プラットフォーム	最小バージョン
Firepower Management Center Firepower 4100/9300 シリーズを除く、FMC 展開のすべての管理対象デバイス。	6.1.0
FMC を使用した Firepower 4100/9300 上の Firepower Threat Defense	FXOS 2.4.1.214+ を使用した 6.1.0（最初に FXOS をアップグレード） （注） バージョン 6.1.x からアップグレードする場合は、Firepower 4100/9300 では FXOS のアップグレードの前に FTD プッシュが必要 （43 ページ）を参照してください。
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.2.0
ASDM を使用した ASA FirePOWER	6.2.0

時間テストとディスク容量の要件

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。Firepower Management Center を使用して管理対象デバイスをアップグレードする場合、デバイスアップグレードパッケージに対して、FMC は /Volume パーティションに追加のディスク容量を必要とします。また、アップグレードを実行するための十分な時間を確保してください。

参考のために、社内の時間とディスク容量のテストに関するレポートを提供しています。

時間テストについて

ここで指定した時間の値は、社内のテストに基づいています。特定のプラットフォーム/シリーズについてテストされたすべてのアップグレードの最も遅い時間を報告していますが、複数の理由により（以下を参照）、報告された時間よりも、アップグレードにかかる時間が長くなることがあります。

基本的なテスト条件

- 展開：値は、Firepower Management Center 展開のテストから取得されています。これは、同様の条件の場合、リモートとローカルで管理されているデバイスの raw アップグレード時間が類似しているためです。
- バージョン：メジャー アップグレードの場合、以前のすべての対象メジャー バージョンからのアップグレードをテストします。パッチについては、基本バージョンおよび直前のパッチからのアップグレードをテストします。
- モデル：ほとんどの場合、各シリーズの最もローエンドのモデルでテストし、場合によってはシリーズの複数のモデルでテストします。
- 仮想設定：メモリおよびリソースのデフォルト設定を使用してテストします。

プッシュおよびリブートの除外

値は、Firepower のアップグレード スクリプト自体を実行するのにかかる時間のみを表しています。値には、ローカル管理対象デバイスまたは FMC にアップグレード パッケージをアップロードするのに必要な時間や、アップグレード パッケージを FMC から管理対象デバイスにコピー（プッシュ）するために必要な時間は含まれていません。

FMC 展開では、FMC と管理対象デバイスの間の帯域幅が不十分だと、アップグレード時間が延長されたり、アップグレードがタイムアウトする原因となる可能性があります。FMC からそのデバイスに大容量のデータを転送するための帯域幅があることを確認します。詳細については、『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

値には、再起動、準備状況チェック、オペレーティング システムのアップグレード、または設定の展開も含まれていません。

時間は単一のデバイスを対象とする

値は、デバイスごとの値です。ハイ アベイラビリティの構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは1つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンス モードで動作します。そのため、デバイス ペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。

スタック構成の 8000 シリーズ デバイスは同時にアップグレードされ、スタックは、すべてのデバイスのアップグレードが完了するまで、限定的なバージョン混在の状態で動作することに注意してください。これには、スタンドアロンデバイスのアップグレードと比べて大幅に長い時間がかかるということはありません。

影響を受ける構成とデータ

シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。

ディスク容量の要件について

容量の見積もりは、すべてのアップグレードについて報告された最大のものであり、次のようになります。

- 切り上げなし（1 MB 未満）。
- 次の 1 MB に切り上げ（1 MB ～ 100 MB）。
- 次の 10 MB に切り上げ（100 MB ～ 1 GB）。
- 次の 100 MB に切り上げ（1 GB を超える容量）。

バージョン 6.3.0 の時間とディスク容量

表 *22 :* バージョン *6.3.0* の時間とディスク容量

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
FMC	12.7 GB	29 MB	—	47 分
FMCv ：VMware 6.0	12.7 GB	29 MB	—	29 分
Firepower 2100 シリーズ	13 MB	8.8 GB	930 MB	20 分

プラットフォーム	ボリュームの容量	必要容量	FMC の容量	時間
Firepower 4100/9300 シャーシ	10 MB	7.6 GB	930 MB	6 分
ASA 5500-X シリーズ を搭載した FTD	7.9 GB	100 KB	1.1 GB	25 分
FTDv：VMware 6.0	7.3 GB	100 KB	1.1 GB	12 分
Firepower 7000/8000 シリーズ	7.0 GB	19 MB	920 MB	32 分
ASA FirePOWER	11.3 GB	22 MB	1.2 GB	63 分
NGIPSv	5.7 GB	19 MB	810 MB	16 分

トラフィック フロー、検査、およびデバイス動作

アップグレード中に発生するトラフィック フローおよびインスペクションでの潜在的な中断を特定する必要があります。これは、次の場合に発生する可能性があります。

- デバイスが再起動された場合。
- デバイス上でオペレーティング システムまたは仮想ホスティング環境をアップグレードする場合。
- デバイス上で Firepower ソフトウェアをアップグレードするか、パッチをアンインストールする場合。
- アップグレードまたはアンインストール プロセスの一部として設定変更を展開する場合（Snort プロセスが再開します）。

デバイスのタイプ、展開のタイプ（スタンドアロン、ハイアベイラビリティ、クラスタ化）、およびインターフェイスの設定（パッシブ、IPS、ファイアウォールなど）によって中断の性質が決まります。アップグレードまたはアンインストールは、保守期間中に行うか、中断による展開環境への影響が最も小さい時点で行うことを強く推奨します。

FTD アップグレード時の動作： Firepower 4100/9300 シャーシ

このセクションでは、FTD を搭載した Firepower 4100/9300 シャーシをアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower 4100/9300 シャーシ：FXOS のアップグレード

シャーシ間クラスタリングまたはハイ アベイラビリティ ペアの構成がある場合でも、各シャーシの FXOS を個別にアップグレードします。アップグレードの実行方法により、FXOS のアップグレード時にデバイスがトラフィックを処理する方法が決定されます。

表 *23 : FXOS* アップグレード中のトラフィックの動作

展開	方法	トラフィックの動作
スタンドアロン	—	切断
ハイ アベイラビリティ	**ベスト プラクティス**：スタンバイで FXOS を更新し、アクティブ ピアを切り替えて新しいスタンバイをアップグレードします。	影響なし
	スタンバイでアップグレードが終了する前に、アクティブ ピアで FXOS をアップグレードします。	1 つのピアがオンラインになるまでドロップされる
シャーシ間クラスタ（6.2 以降）	**ベスト プラクティス**：少なくとも 1 つのモジュールを常にオンラインにするため、一度に 1 つのシャーシをアップグレードします。	影響なし
	ある時点ですべてのモジュールを停止するため、シャーシを同時にアップグレードします。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる
シャーシ内クラスタ（Firepower 9300 のみ）	Fail-to-wire 有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]。（6.1 以降）	インスペクションなしで転送
	Fail-to-wire 無効：[バイパス：無効（Bypass: Disabled）]。（6.1 以降）	少なくとも 1 つのモジュールがオンラインになるまでドロップされる
	fail-to-wire モジュールなし。	少なくとも 1 つのモジュールがオンラインになるまでドロップされる

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *24 : Firepower* ソフトウェア アップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	切断
IPS のみのインターフェイス	インライン セット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1+）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インライン セット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1+）	ドロップ
	インライン セット、fail-to-wire モジュールなし	ドロップ
	インライン セット、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

ハイ アベイラビリティ ペア：FirePOWER ソフトウェア アップグレード

ハイ アベイラビリティ ペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

クラスタ：FirePOWER ソフトウェア アップグレード

Firepower Threat Defense クラスタのデバイスで FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼

働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

スレーブ セキュリティ モジュールを最初にアップグレードして、その後マスターをアップグレードします。アップグレード中、セキュリティ モジュールはメンテナンス モードで稼働します。

マスター セキュリティ モジュールをアップグレードする間、通常、トラフィック インスペクションと処理は続行しますが、システムはロギング イベントを停止します。ロギング ダウンタイム中に処理されるトラフィックのイベントは、アップグレードが完了した後、非同期のタイムスタンプ付きで表示されます。ただし、ロギングダウンタイムが大きい場合、システムはログ記録する前に最も古いイベントをプルーニングすることがあります。

（注） バージョン6.2.0、バージョン6.2.0.1、またはバージョン6.2.0.2からシャーシ間クラスタをアップグレードすると、各モジュールがクラスタから削除されるときに、トラフィックインスペクションで2～3秒のトラフィック中断が発生します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、デバイスがトラフィックを処理する方法に応じて異なります。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Configurations that Restart the Snort Process when Deployed or Activated*」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。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。

表 *25 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォール インターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップ

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インライン セット、[フェールセーフ（Failsafe）] が有効または無効（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インライン セット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2+）	ドロップ
	インライン セット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	インライン セット、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

FTD アップグレード時の動作：その他のデバイス

このセクションでは、Firepower 2100 シリーズ、ASA 5500-X シリーズ、ISA 3000、および FTDv で Firepower Threat Defense をアップグレードするときのデバイスとトラフィックの動作を説明します。

スタンドアロン FTD デバイス：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *26 : Firepower* ソフトウェア アップグレード中のトラフィックの動作：スタンドアロン *FTD* デバイス

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	切断

インターフェイスの設定		トラフィックの動作
IPS のみのインターフェイス	インライン セット、fail-to-wire が有効：[バイパス：スタンバイ（Bypass: Standby）] または [バイパス：強制（Bypass-Force）]（6.1+）	次のいずれかを行います。 • ドロップ（6.1 から 6.2.2.x） • インスペクションなしで転送（6.2.3 以降）
	インライン セット、fail-to-wire が無効：[バイパス：無効（Bypass: Disabled）]（6.1+）	ドロップ
	インライン セット、fail-to-wire モジュールなし	ドロップ
	インライン セット、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

ハイ アベイラビリティ ペア：FirePOWER ソフトウェア アップグレード

ハイ アベイラビリティ ペアのデバイスの FirePOWER ソフトウェアをアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

スタンバイ側のデバイスが最初にアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレードプロセスによって元の役割に切り替わります。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Configurations that Restart the Snort Process when Deployed or Activated*」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snortプロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。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。

表 *27 : FTD* 展開時のトラフィックの動作

インターフェイスの設定		トラフィックの動作
ファイアウォールインターフェイス	EtherChannel、冗長、サブインターフェイスを含むルーテッドまたはスイッチド スイッチドインターフェイスは、ブリッジグループまたはトランスペアレントインターフェイスとしても知られています。	ドロップ
IPS のみのインターフェイス	インライン セット、[フェールセーフ（Failsafe）] が有効または無効（6.0.1 ～ 6.1.0.x）	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
	インライン セット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：無効（6.2+）	ドロップ
	インライン セット、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効（6.2+）	インスペクションなしで転送
	インライン セット、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
	パッシブ、ERSPAN パッシブ	中断なし、インスペクションなし

FirePOWER 7000/8000 シリーズのアップグレード時の動作

次のセクションでは、Firepower 7000/8000 シリーズデバイスをアップグレードする際のデバイスおよびトラフィックの動作について説明します。

スタンドアロン 7000/8000 シリーズ：Firepower ソフトウェアのアップグレード

インターフェイスの設定により、アップグレード中にスタンドアロンデバイスがトラフィックを処理する方法が決定されます。

表 *28 :* アップグレード中のトラフィックの動作：スタンドアロン *7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、ハードウェア バイパスが有効（[バイパスモード：バイパス（Bypass Mode: Bypass）]）	インスペクションなしで転送。ただし、トラフィックは、次の 2 つのポイントで一時的に中断します。 • アップグレード プロセスの開始時に、リンクがダウンしてから復旧（フラップ）し、ネットワーク カードがハードウェア バイパスに切り替わるとき。 • アップグレードが完了した後、リンクが復旧し、ネットワーク カードがバイパスから切り替わるとき。インスペクションはエンドポイントの再接続後に再開され、デバイス インターフェイスとのリンクを再確立します。
インライン、ハードウェア バイパス モジュールなし、またはハードウェア バイパスが無効（[バイパスモード：非バイパス（Bypass Mode: Non-Bypass）]）	ドロップ
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップ

7000/8000 シリーズ ハイ アベイラビリティ ペア：Firepower ソフトウェアのアップグレード

ハイ アベイラビリティ ペアのデバイス（またはデバイス スタック）をアップグレードする間に、トラフィック フローまたはインスペクションが中断されることはありません。継続稼働できるように、一度に1つずつアップグレードされます。アップグレード中、デバイスはメンテナンス モードで稼働します。

最初にアップグレードするピアは、展開によって異なります。

- ルーテッドまたはスイッチド：最初にスタンバイがアップグレードされます。デバイスの役割が切り替わり、新しくスタンバイになったデバイスがアップグレードされます。アップグレードの完了時には、デバイスの役割は切り替わったままです。アクティブ/スタンバイの役割を維持する場合、アップグレード前に役割を手動で切り替えます。それにより、アップグレード プロセスによって元の役割に切り替わります。
- アクセス制御のみ：最初にアクティブがアップグレードされます。アップグレードの完了時に、アクティブとスタンバイの以前の役割がデバイスで維持されます。

8000 シリーズ スタック：Firepower ソフトウェア アップグレード

8000 シリーズ スタックでは、デバイスは同時にアップグレードされます。プライマリ デバイスがアップグレードを完了してスタックが動作を再開するまで、トラフィックはスタックがスタンドアロンデバイスであったかのように影響を受けます。すべてのデバイスがアップグレードを完了するまで、スタックは、制限付きの混合バージョンの状態で動作します。

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Configurations that Restart the Snort Process when Deployed or Activated*」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、Snort プロセスを再起動すると、HA/スケーラビリティ用に設定されたものを含め、すべての Firepower デバイスでトラフィック インスペクションが中断されます。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。

表 *29 :* 展開時のトラフィックの動作：*7000/8000* シリーズ

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）]が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）]が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし
ルーテッド、スイッチド	ドロップ

ASA FirePOWER アップグレード時の動作

Snort プロセスを再起動する特定の設定を展開する場合を含め、モジュールが FirePOWER ソフトウェア アップグレード中にトラフィックを処理する方法を決定する、ASA FirePOWER モジュールへのトラフィック リダイレクトに関する ASA サービス ポリシーです。

表 *30 : ASA FirePOWER* アップグレード中のトラフィックの動作

トラフィック リダイレクト ポリシー	トラフィックの動作
フェール オープン（**sfr fail-open**）	インスペクションなしで転送
フェール クローズ（**sfr fail-close**）	ドロップ

トラフィック リダイレクト ポリシー	トラフィックの動作
モニタのみ（**sfr {fail-close}|{fail-open} monitor-only**）	パケットをただちに出力、コピーへのインスペクションなし

ASA FirePOWER 展開時のトラフィックの動作

Snort プロセスが再起動している間のトラフィックの動作は、ASA FirePOWER モジュールをアップグレードする場合と同じです。

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Configurations that Restart the Snort Process when Deployed or Activated*」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。 さらに、Snort プロセスを再起動すると、トラフィック インスペクションが中断されます。サービスポリシーにより、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通過するかが決定されます。

NGIPSv アップグレード時の動作

このセクションでは、NGIPSv をアップグレードするときのデバイスとトラフィックの動作を説明します。

Firepower ソフトウェア アップグレード

インターフェイスの設定により、アップグレード中に NGIPSv がトラフィックを処理する方法が決定されます。

表 *31 : NGIPSv* アップグレード中のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン	ドロップ
インライン、タップ モード	パケットをただちに出力、コピーへのインスペクションなし
パッシブ	中断なし、インスペクションなし

展開時のトラフィックの動作

アップグレード プロセス中には、設定を複数回展開します。Snort は、通常、アップグレード直後の最初の展開時に再起動されます。展開の前に、特定のポリシーまたはデバイス設定を変更しない限り、それ以外の展開時に再起動されることはありません。詳細については、

『Firepower Management Center コンフィギュレーション ガイド』の「*Configurations that Restart the Snort Process when Deployed or Activated*」を参照してください。

展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、Snortプロセスを再起動すると、トラフィック インスペクションが中断されます。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。

表 *32 : NGIPSv* 展開時のトラフィックの動作

インターフェイスの設定	トラフィックの動作
インライン、[フェールセーフ（Failsafe）] が有効または無効	インスペクションなしで転送 [フェールセーフ（Failsafe）] が無効で、Snort がビジーでもダウンしていない場合、いくつかのパケットがドロップすることがあります。
インライン、タップ モード	すぐにパケットを出力し、バイパス Snort をコピーする
パッシブ	中断なし、インスペクションなし

アップグレード手順

リリース ノートにはアップグレード手順は含まれていません。これらのリリース ノートに記載されているガイドラインと警告を読んだ後、次のいずれかを参照してください。

- Cisco Firepower Management Center Upgrade Guide：管理対象デバイスや付随するオペレーティング システムを含む、FMC 展開のアップグレード
- Cisco ASA Upgrade Guide：ASDM を使用した ASA FirePOWER モジュールのアップグレード
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager：FDM を使用した FTD のアップグレード

アップグレード パッケージ

アップグレード パッケージは、シスコ サポートおよびダウンロード サイトで入手できます。

- FMCv を含む Firepower Management Center：https://www.cisco.com/go/firepower-software
- Firepower Threat Defense（ISA 3000）：https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense（FTDv を含む他のすべてのモデル）：https://www.cisco.com/go/ftd-software

- FirePOWER 7000 シリーズ： https://www.cisco.com/go/7000series-software
- FirePOWER 8000 シリーズ： https://www.cisco.com/go/8000series-software
- ASA with FirePOWER Services（ASA 5500-X シリーズ）： https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services（ISA 3000）： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

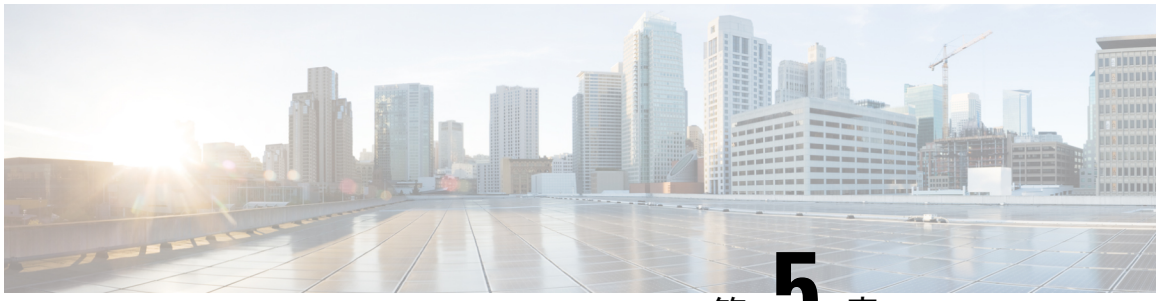
バージョン 6.2.1+ からのアップグレード パッケージは、署名付きの tar アーカイブ（.tar）です。解凍しないでください。

表 *33* : バージョン *6.2.1+* からのアップグレード パッケージ

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh.REL.tar
Firepower 2100 シリーズ	Cisco_FTD_SSP_FP2K_Upgrade-*version-build*.sh.REL.tar
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Upgrade-*version-build*.sh.REL.tar
FTD を搭載した ASA 5500-X シリーズ FTD を搭載した ISA 3000 Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-*version-build*.sh.REL.tar
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh.REL.tar

表 *34* : バージョン *6.1.x* または *6.2.0.x* からのアップグレード パッケージ

プラットフォーム	パッケージ
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh
Firepower 4100/9300 シャーシ	Cisco_FTD_SSP_Upgrade-*version-build*.sh
FTD を搭載した ASA 5500-X シリーズ Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-*version-build*.sh
Firepower 7000/8000 シリーズ	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh



第 5 章

新規インストール バージョン 6.3.0

Firepower アプライアンスをアップグレードできない（または必要なアップグレード パスを実行したくない）場合は、Firepower のメジャー リリースを新規インストールできます。

新規インストールの決定

次の表を使用して、新規インストール（再イメージ化とも呼ばれます）する必要がある場合のシナリオを特定します。これらのすべてのシナリオ（ローカルとリモート間のデバイス管理の切り替えを含む）では、デバイス設定が失われます。

（注） Firepower アプライアンスを再イメージ化する前に、またはその管理を切り替える前に、必ずライセンスの問題に対処してください。Cisco Smart Licensing を使用している場合は、孤立した権限付与の発生を防ぐために、Cisco Smart Software Manager から手動で登録解除する必要がある場合があります。手動で登録を解除しない場合、Smart Licensing でデバイスが登録されていると、デバイスを登録できないことがあります。

表 *35 :* シナリオ：新規インストールが必要ですか。

シナリオ	ソリューション	ライセンシング
FMC で管理されているデバイスをより古い Firepower バージョンからアップグレードします。	古いバージョンからのアップグレード パスには中間バージョンが含まれる場合があります。特に、FMC とデバイスのアップグレードを交互に行う必要がある大規模展開の環境では、この複数の手順のプロセスを完了するために時間がかかる場合があります。 この時間を短縮するために、アップグレードする代わりに、古いデバイスを再イメージ化することができます。 **1.** FMC からデバイスを削除します。 **2.** FMC のみをターゲット バージョンにアップグレードします。 **3.** デバイスを再イメージ化します。 バージョン 5.x のデバイスをバージョン 6.3+ に再イメージ化する必要がある場合は、「新規インストールに関するガイドラインと制約事項（69 ページ）」を参照してください。 **4.** デバイスを FMC に再度追加します。	FMC からデバイスを削除すると、デバイスが登録解除されます。デバイスを再度追加した後、ライセンスを再割り当てします。
FTD 管理を FDM から FMC（ローカルからリモート）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。	管理を切り替える前に、デバイスを登録解除します。デバイスを FMC に追加した後、ライセンスを再割り当てします。
FTD 管理を FMC から FDM（リモートからローカル）に変更します。	**configure manager** CLI コマンドを使用します。『Command Reference for Firepower Threat Defense』を参照してください。 **例外**：デバイスが実行中であるか、バージョン6.0.1からアップグレードされています。この場合は、再イメージ化します。	FMC からデバイスを削除し、デバイスを登録解除します。FDM を使用して再登録します。
ASDM と FMC 間の ASA FirePOWER 管理を変更します。	他の管理方法の使用を開始します。	クラシック ライセンスについては、セールス担当者にお問い合わせください。ASA FirePOWER ライセンスは、特定のマネージャに関連付けられています。

シナリオ	ソリューション	ライセンシング
ASA FirePOWER を同じ物理デバイス上の FTD に置き替えます。	再イメージ化します。	クラシック ライセンスをスマート ライセンスに変換します。『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。
NGIPSv を FTDv に置き換えます。	再イメージ化します。	新しいスマート ライセンスについては、セールス担当者にお問い合わせください。

新規インストールに関するガイドラインと制約事項

誤りを避けるには、注意深い計画と準備が役立ちます。Firepower リリースに精通していて、Firepower アプライアンスを再イメージ化したことがある場合でも、これらのガイドラインと制限事項に加えて、「設置手順 （72 ページ）」にリンクされている手順を必ず参照してください。

イベント データと設定データのバックアップ

イベント データと設定データを外部の場所にバックアップすることを強くお勧めします。再イメージ化すると、システム パスワード（Admin123）などのほとんどの設定が工場出荷時の初期状態に戻されます。

ただし、再イメージ化してアップグレードする必要がない場合は、バックアップを使用して古い設定をインポートできないことに注意してください。同じ VDB を使用している同じモデルおよび Firepower バージョンのアプライアンスのみからバックアップを復元できます。

Firepower Management Center からのデバイスの削除

再イメージ化する前に、必ずリモート管理からデバイスを削除してください。現状は、次のとおりです。

- FMC を再イメージ化する場合、すべてのデバイスを管理から削除します。
- 単一のデバイスを再イメージ化するか、リモートからローカル管理に切り替える場合、その単一のデバイスを削除します。

ライセンスの問題の対処

Firepower アプライアンスを再イメージ化する前に、ライセンスの問題に対処してください。Cisco Smart Software Manager からの登録解除が必要になる場合があります。または、新しいライセンスについてセールス担当者に問い合わせる必要がある場合があります。シナリオに応じて必要な操作を決定するには、「新規インストールの決定」を参照してください。

ライセンスの詳細については、次を参照してください。

- 『Cisco Firepower System Feature Licenses Guide』
- 『Frequently Asked Questions (FAQ) about Firepower Licensing』
- 設定ガイドのライセンスの章。

再イメージ化の実行中および実行後のアプライアンスへのアクセス

再イメージ化により、ほとんどの設定が工場出荷時の初期状態に戻ります。

アプライアンスに物理的にアクセスできない場合、再イメージ化プロセスによって管理ネットワークの設定を維持できます。これにより、再イメージ化した後、アプライアンスに接続して、初期設定を実行できます。ネットワーク設定を削除する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

デバイスに関して、ユーザの位置からのトラフィックがデバイスの管理インターフェイスにアクセスするためにデバイス自体を通過する必要がないことを確認してください。FMC 展開では、デバイスを経由せずに FMC 管理インターフェイスにアクセスできる必要もあります。

再イメージ化の実行中および実行後のシスコとのデータ共有

バージョン 6.2.3+ の機能には、シスコとのデータ共有が含まれます。

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。

Web 分析のトラッキングは、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、ユーザの場所、FMC 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送信します。 Web 分析トラッキングはデフォルトでオンになっています。ただし、初期設定の完了後にいつでもオプト アウトできます。

以前のメジャー バージョンへの Firepower 2100 シリーズ デバイスの再イメージ化

Firepower 2100 シリーズ デバイスを以前のメジャー バージョンに戻す必要がある場合は、完全な再イメージ化を実行することを推奨します。消去設定方式を使用すると、Firepower Threat Defense ソフトウェアに加えて、FXOS が復元しない場合があります。この場合、特にハイ アベイラビリティ展開では、障害が発生する可能性があります。

詳細については、『*Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense*』の「Reimage Procedures」の章を参照してください。

バージョン 6.3.0 へのバージョン 5.x ハードウェアの再イメージ化

バージョン 6.3+ のインストール パッケージの名前が変更されていると、古い物理アプライアンス（DC750、1500、2000、3500、4000 のほか、7000/8000 シリーズ デバイスと AMP モデル）の再イメージ化に関する問題が発生します。バージョン 5.x を現在実行していて、これらのアプライアンスのいずれかにバージョン 6.3 を新規インストールする必要がある場合は、シスコ サポートおよびダウンロード サイト からインストール パッケージをダウンロードした後、そ

の名前を「古い」名前に変更します。名前が変更されたアップグレードとインストール パッケージ （42 ページ）を参照してください。

FMC（Defense Center）をバージョン 5.x からより新しいバージョンに再イメージ化した後、古いデバイスを管理することはできません。また、これらのデバイスを再イメージ化してから、FMC に再度追加する必要があります。シリーズ 2 デバイスは EOL であり、Firepower ソフトウェアの過去バージョン 5.4.0.x を実行できないことに注意してください。それらのデバイスを置き換える必要があります。

スマート ライセンスの登録解除

Firepower Threat Defense デバイスは、ローカル（Firepower Device Manager）またはリモート（Firepower Management Center）で管理されているかどうかに関係なく、Cisco Smart Licensing を使用します。ライセンス供与された機能を使用するには、Cisco Smart Software Manager（CSSM）で登録する必要があります。再イメージ化または管理の切り替えを行う前に、孤立した権限付与を発生させないように手動で登録を解除する必要があります。

登録を解除すると、仮想アカウントからアプライアンスが削除され、関連付けられたライセンスが解放されるため、ライセンスを再割り当てできるようになります。アプライアンスを登録解除すると、適用モードになります。アプライアンスの現在の設定とポリシーはそのまま機能しますが、変更を加えたり展開したりすることはできません。

次の操作を行う前に、CSSM から登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- FDM によってローカルで管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FDM から FMC 管理に切り替える。

次の操作を行う場合、CSSM から登録解除しないでください。

- FMC によって管理されている Firepower Threat Defense デバイスを再イメージ化する。
- Firepower Threat Defense デバイスを FMC から FDM 管理に切り替える。

上記の 2 つのケースでは、FMC からデバイスを削除すると、デバイスが自動的に登録解除されます。FMC からデバイスを削除すれば、手動で登録解除する必要はありません。

ヒント NGIPS デバイスのクラシック ライセンスは、特定のマネージャ（ASDM/FMC）に関連付けられており、CSSM を使用して制御されません。クラシック デバイスの管理を切り替える場合、または NGIPS 展開から FTD 展開に移行する場合は、セールス担当者にお問い合わせください。

Firepower Management Centerの登録解除

FMC を再イメージ化する前に Cisco Smart Software Manager から Firepower Management Center の登録を解除します。これは、管理対象の Firepower Threat Defense デバイスの登録も解除します。

FMCが高可用性に設定されている場合、ライセンスの変更が自動的に同期されます。他のFMCの登録を解除する必要はありません。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[System]** > **[Licenses]** > **[Smart Licenses]**を選択します。

ステップ 3 [スマートライセンスのステータス（Smart License Status）] の横の停止記号 （）をクリックします。

ステップ 4 警告を読み、登録解除することを確認します。

FDM を使用した FTD デバイスの登録解除

再イメージ化するか、またはリモート（FMC）管理に切り替える前に、ローカルの管理対象 Firepower Threat Defense デバイスの登録を Cisco Smart Software Manager から解除します。

高可用性のために設定されているデバイスの場合は、その装置を登録解除するために、高可用性ペアにあるその他の装置にログインする必要があります。

ステップ 1 Firepower Device Manager にログインします。

ステップ 2 [デバイス（Device）] をクリックし、[スマートライセンス概要（Smart License summary）] の [設定の表示（View Configuration）] をクリックします。

ステップ 3 歯車ドロップダウンリストから [デバイスの登録解除（Unregister Device）] を選択します。

ステップ 4 警告し、登録を解除することを確認します。

設置手順

リリース ノートとアップグレード ガイドにはインストール手順は含まれていません。代わりに、次のドキュメントのいずれかを参照してください。インストール パッケージは シスコ サポートおよびダウンロード サイト から入手できます。

表 *36 : Firepower Management Center* のインストール手順

FMC プラットフォーム	ガイド
FMC 1000、2500、4500	『Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500』：Firepower Management Center の工場出荷時の初期状態への復元
FMC 750、1500、2000、3500、4000	『Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000』：Firepower Management Center の工場出荷時の初期状態への復元
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

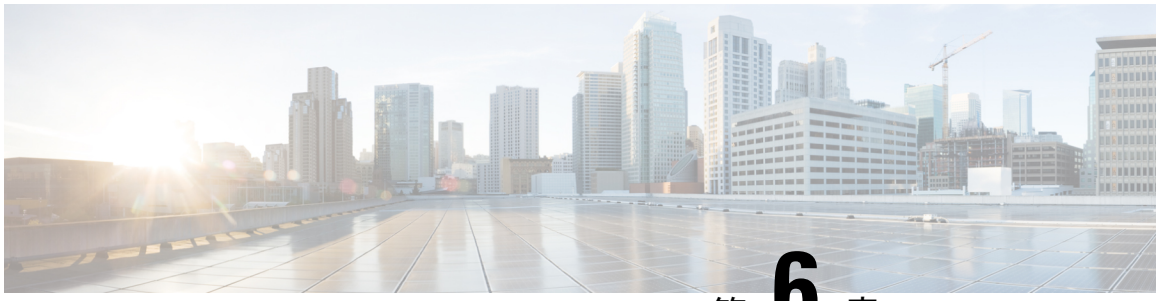
表 *37 : Firepower Threat Defense* のインストール手順

FTD プラットフォーム	ガイド
Firepower 2100 シリーズ	『Cisco ASA and Firepower Threat Defense Reimage Guide』 『Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense』
Firepower 4100/9300 シャーシ	『Cisco Firepower 4100/9300 FXOS Configuration Guides』：イメージ管理に関する章 Cisco Firepower 4100 Getting Started Guide 『Cisco Firepower 9300 Getting Started Guide』
ASA 5500-X シリーズ	『Cisco ASA and Firepower Threat Defense Reimage Guide』
ISA 3000	『Cisco ASA and Firepower Threat Defense Reimage Guide』
FTDv: VMware	VMware 向け Cisco Firepower Threat Defense Virtual スタートアップ ガイド
FTDv: KVM	Cisco Firepower Threat Defense Virtual スタートアップ ガイド（KVM 導入向け）
FTDv：AWS	『Cisco Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud』
FTDv：Azure	『Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide』

表 *38 : FirePOWER 7000/8000* シリーズ、*NGIPSv*、および *ASA FirePOWER* インストール手順

NGIPS プラットフォーム	ガイド
Firepower 7000 シリーズ	『Cisco Firepower 7000 Series Getting Started Guide』：デバイスの工場出荷時の初期状態への復元

NGIPS プラットフォーム	ガイド
Firepower 8000 シリーズ	『Cisco Firepower 8000 Series Getting Started Guide』：デバイスの工場出荷時の初期状態への復元
NGIPSv	『Cisco Firepower NGIPSv Quick Start Guide for VMware』
ASA FirePOWER	『Cisco ASA and Firepower Threat Defense Reimage Guide』 『ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide』：ASA FirePOWER モジュールの管理



第 6 章

資料

次のトピックでは、Firepower のドキュメントへのリンクを記載しています。

更新されたドキュメント

次の Firepower ドキュメントが更新されたか、バージョン 6.3.0 で新たに利用可能になっています。更新されていない、またはこのリリースで新しく使用可能になったドキュメントへのリンクについては、ドキュメント ロードマップ （77 ページ） を参照してください。

Firepower 構成ガイドとオンライン ヘルプ

- 『Firepower Management Center Configuration Guide, Version 6.3』とオンライン ヘルプ
- 『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.3.0』とオンライン ヘルプ
- 『Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.3』とオンライン ヘルプ
- 『Cisco Firepower Threat Defense Command Reference』

FXOS 構成ガイドとリリース ノート

- 『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.4(1)』
- 『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.4(1)』
- 『Cisco Firepower 4100/9300 FXOS Command Reference』
- 『Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)』

アップグレード ガイド

- Cisco Firepower Management Center Upgrade Guide

- Cisco ASA アップグレード ガイド

ハードウェア設置ガイド

- 『Cisco Firepower 2100 Series Hardware Installation Guide』

クイック スタート ガイド

クイック スタート：Firepower Management Center

- 『Cisco Firepower Management Center Virtua lDeployment Guide』（新）

クイック スタート：FMC を使用した Firepower Threat Defense

- 『Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Management Center Quick Start Guide』
- 『Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide』
- 『Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide』
- 『Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide』

クイック スタート：FDM を使用した Firepower Threat Defense

- 『Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Device Manager Quick Start Guide』
- 『Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Device Manager Quick Start Guide』
- 『Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for VMware Deployment Quick Start Guide』
- 『Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide』

API および統合ガイド

- 『Firepower Management Center REST API Quick Start Guide, Version 6.3.0』
- 『Firepower System Event Streamer Integration Guide, Version 6.3.0』
- 『Firepower System Database Access Guide v6.3』

互換性ガイド

- Cisco Firepower Compatibility Guide
- 『Cisco ASA Compatibility Guide』

- 『Cisco FXOS Compatibility Guide』

ライセンスおよびオープン ソース

- 『Cisco Firepower System Feature Licenses』
- 『Frequently Asked Questions (FAQ) about Firepower Licensing』
- 『Open Source Used in Firepower Version 6.3.0』

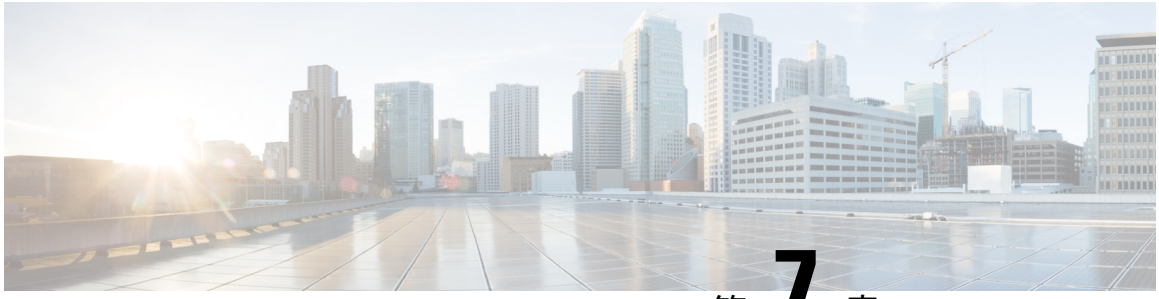
トラブルシューティングおよび設定の例

- 『Cisco Firepower Threat Defense Syslog Messages』
- 『How to Manage a Device with the Firepower Management Center』（新）

ドキュメント ロードマップ

ドキュメント ロードマップでは、現在使用可能なドキュメントおよび従来のドキュメントへのリンクを示します。

- 『Navigating the Cisco Firepower Documentation』
- 『Navigating the Cisco ASA Series Documentation』
- 『Navigating the Cisco FXOS Documentation』



第 7 章

解決済みの問題

この Firepower バージョンが最初にリリースされたとき、ここに記載されているバグは解決済みだと確認されました。

解決済みの問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新の解決済みバグ リストを取得することができます。これらの一般的なクエリには、バージョン 6.3.0を実行している Firepower 製品の解決済みのバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense Virtual
- ASA with FirePOWER Services
- NGIPSv

検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

新しいビルドで解決済みの問題

シスコは、更新版ビルドを適宜リリースしています。各プラットフォームの最新のビルド番号のみが、シスコ サポートおよびダウンロード サイト で入手可能です。常に最新のビルドを使用する必要があります。以前のビルドをダウンロードした場合は使用しないでください。

同じ Firepower バージョンに対して、1 つのビルドから別のビルドにアップグレードすることはできません。現在インストールされている「古い」ビルドで問題が発生した場合は、アップ

グレード、パッチ、またはホットフィックスで問題に対処できるかどうかを判断します。これらが利用できない場合は、再イメージ化する必要があります。

表 *39* : バージョン *6.3.0* の新しいビルド

新しいビルド	リリース日	プラットフォーム	パッケージ	解決済み
85	2019 年 1 月 22 日	Firepower 4100/9300	アップグレード 新規インストール	CSCvo02577：SSL HW 復号化によるバッファ枯渇 Firepower 4100/9300 デバイスで Firepower Threat Defense にバージョン 6.3.0-83 をすでにインストールしているか、これらのバージョンにアップグレードしている場合は、ホットフィックス B を適用します。
84	2018 年 12 月 18 日	FMC/FMCv ASA FirePOWER	アップグレード	CSCvn62123：一部の FMC およびローカル（ASDM）管理された ASA FirePOWER モジュールでは、バージョン 6.3.0-83 でのアップグレードに失敗していました。この問題は、バージョン 5.4.x からアップグレードした一部のお客様に限られていました。 この問題のためにすでにアップグレードに失敗した場合は、Cisco TAC に連絡してください。

バージョン 6.3.0 で解決済みの問題

不具合 ID	タイトル
CSCuy27743	MySQL のドロップが原因で、初回起動中に VDB のインストールが失敗する
CSCvb15074	削除された、またはアウトオブバンドで追加されたインターフェイスの FMC ヘルス通知がスタックする
CSCvb38753	ssl ルールでアプリケーションが設定されている場合、クライアント hello が dnd によって変更される
CSCvb73266	アップグレードが失敗した状態のときにデバイスに展開すると、多くの問題が発生する
CSCvc94589	OpenSSL Jan 2017 の sfims の評価
CSCvc99840	Firepower Management Center と同期していない管理対象デバイスの ID

不具合 ID	タイトル
CSCvd09003	変数セットの競合のチェックが、ネットワーク グループで機能しない
CSCvd66558	インスペクション エンジン（Snort）のパフォーマンス統計情報には、ゼロ以外のドロップがある場合でも、0 ドロップが表示される
CSCvd83685	Firepower 管理コンソールで廃止されたデフォルトの SSH 設定
CSCve03169	（1/2）LDAP参加のための不正なレルム設定の場合、シャットダウン中にADI プロセスが応答しない
CSCve13357	ネットワーク オブジェクト グループに対して、検索フィルタが適切に機能しない
CSCve13816	いくつかのセキュリティ脆弱性に対処するために MEMCACHED ソフトウェアのアップグレードが必要
CSCve50642	「The devicesthat captured file xxx are not available」が表示され、ファイルイベントからのファイルのダウンロードが失敗する
CSCve64511	#sql-*.ibd 一時テーブルのために、410_check_disk_space でのアップグレードに失敗する可能性がある
CSCve87925	FMC：OSPF インターフェイス リストでの不整合インターフェイス
CSCvf46888	DNS/URL セキュリティ インテリジェンスのブラックリストが期待どおりに機能しない
CSCvf57596	ポリシーの展開が失敗した後、ActionQueueScrape プロセスが終了しなかった
CSCvf80217	Rest API エクスプローラでは、「/deployment/deployabledevices」の下にデバイス id が表示されない
CSCvf81997	クラスタのバンドル/バンドル解除を繰り返した後、QP バックプレーンがダウンした
CSCvf88111	Pigtail を手動で終了しない場合、Pigtail は自己終了する必要がある
CSCvf90086	物理 int の削除後にサブインターフェイスが設定された場合の展開の失敗
CSCvf97412	.REL.tar アップグレード ファイルにより、GUI の [システム（System）] > [更新（Updates）] ページが低速または応答不能になる
CSCvf98187	FDM：サイト間トンネルの事前共有キーで「;」を使用できない
CSCvg10718	トラフィック プロファイルとの相関ポリシーが機能しない
CSCvg17746	6.2.1-341 から 6.2.3-10587 にアップグレードした後、FXOS CLI と FTD CLI が異なるバージョンを表示する

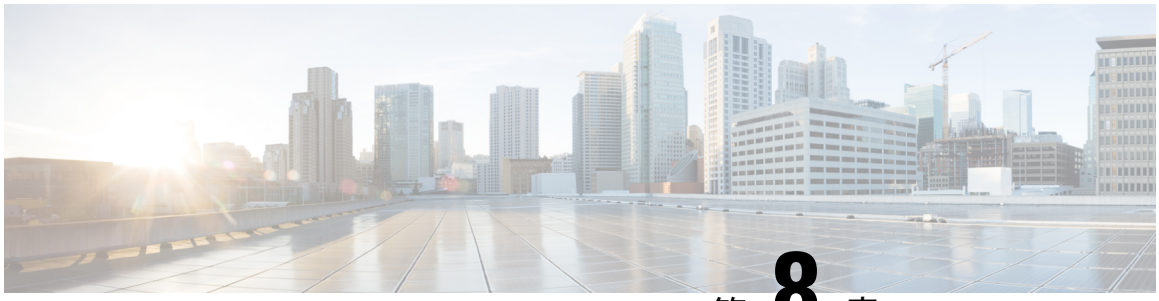
不具合 ID	タイトル
CSCvg38760	シリーズ 3 デバイスでのエクスポートでエラーが発生する
CSCvg48641	AD レルムが LDAP レルムとして設定されている場合、警告メッセージが表示されない
CSCvg50013	AQ で作成されたクラム更新タスクが繰り返され、同じトランザクションに対して成功と失敗の両方の状態になる
CSCvg62301	デバイスの登録中に、ポリシー検出に失敗し、デバイスの登録が解除されることがある
CSCvg74236	接続イベントに関する syslog アラートが設定されている場合、SI イベントの syslog メッセージが送信されない
CSCvg80052	「Lina によって有効化されるトレース」ログの最適化
CSCvg82265	アップグレード後に AMP サーバの公開キーが置き換えられる
CSCvg85671	テキスト ホスト属性を使用したホスト プロファイル限定では、修飾子値としてテキストを使用できない
CSCvg90384	セッションが終了したときの「最上位」プロセスでの高い CPU 使用率
CSCvg98063	FMC 設定ガイドのアップグレード/更新手順が最新ではない
CSCvh02424	センサーで ngfw ルールが誤った順序で展開されている
CSCvh12042	デバイスのインターフェイスが古くなっているため、展開に失敗した
CSCvh14518	FMC：PID にホスト名が含まれていると、スマート ライセンスの登録に失敗する可能性がある
CSCvh23351	AC ポリシーで [リセットしてブロック（Block with Reset）] が選択されている場合、HTTP ブロック応答ページでリセット パケットが送信されない
CSCvh59997	ENH：特定の Firepower Threat Defense syslog ロギング メッセージのログを無効にする機能
CSCvh64413	FTD は Radius サーバを使用して RA VPN ユーザを認証するときに、「0.0.0.0」NAS-IP-Address 属性を送信する
CSCvh77456	Cisco Firepower Threat Defense ソフトウェアの FTP インスペクションにおけるサービス妨害の脆弱性
CSCvh87031	FTD クラスタで SNMPv3 ユーザを展開し、ローカライズされたコマンドを送信する
CSCvh95456	Cisco 適応型セキュリティ アプライアンスのアプリケーション レイヤ プロトコルのインスペクションにおける DoS に対する脆弱性

不具合 ID	タイトル
CSCvi03103	BGP ASN によってポリシーの展開が失敗する
CSCvi08114	重複する事前フィルタ ポリシー ルールが作成される場合がある
CSCvi09176	削除されたセンサーのオーバーライドが、ネットワーク オブジェクトに残される
CSCvi12574	IKE 事前共有パスワードに「スペース」がある場合、FTD VPN サイト間展開が失敗する
CSCvi12915	スマート ライセンス ページにライセンスが表示されない
CSCvi21735	登録でホスト名ルックアップの表示名が誤って使用されている
CSCvi28420	DNS SI が MX および SOA DNS クエリの NXDOMAIN を送信しない
CSCvi56320	BS/QP の FTD 管理インターフェイスの MTU は、9000 ではなく 1500 に設定する必要がある
CSCvi56663	特定の非 ascii 文字のために、ダウンロードしたユーザが通常のユーザ id を取得できない可能性がある
CSCvi61649	.TMM ファイルによってテーブルの最適化がクラッシュとしてマークされる
CSCvi61815	外部データベース アクセスのロギングが機能していない
CSCvi66676	search.info の破損によりオブジェクトの検索が誤動作する
CSCvi74664	Firepower/NGIPS は、ユーザ/カスタム snmp 設定の追加をサポートしていない
CSCvi80603	センサー SFDC スタックがスナップショットを待機しているが、ユーザ ip の更新を受信しない
CSCvi81741	FMC/FTD FlexObject では「http」を編集できない
CSCvi89398	「スタンバイ」の FTD HA ペアの両方のメンバで FTD HA の中断が失敗する
CSCvi92640	復元後、FMC が SSH を介してリモート ストレージ サーバを確立できない
CSCvi93701	RA-VPN トラフィックが snort に転送されない
CSCvi93824	準備状況チェックを複数回開始すると、通知がスタックする
CSCvj08370	FTD ソフトウェアを搭載した FP 2100 シリーズ：LACP モードを FMC から変更することはできない

不具合 ID	タイトル
CSCvj17008	1 つ以上の IP を含む IPS イベントの元のクライアント IP 検索を拒否すると、XFF なしのイベントが除外される
CSCvj20333	エラーが発生し、KP での展開に失敗した：MIO インターフェイスの削除は許可されない
CSCvj20963	復号可能な暗号スイートのリスト
CSCvj33218	FTD 6.2.2.1：BGP ネットワーク ステートメント オブジェクトが適切にプッシュされない
CSCvj36786	FMC に、最後の IGMP 設定済みインターフェイスが表示されない
CSCvj43939	FMC GUI から flow-export を設定するときに無効な設定エラーが発生する
CSCvj46057	アップグレード中にデータ インターフェイスで仮想 mac を使用する FTD HA が原因で、トラフィックが停止する
CSCvj56728	ClamAV Integar オーバーフローに関する Denial of Service（DoS）の脆弱性
CSCvj67055	IKEv2 から IKEv1 S2S 設定にダウングレードすると、展開が失敗する
CSCvj76407	SSL ポリシーを有効にすると、HA 展開での導入が 2 分遅くなる
CSCvj78206	ネットワークを個別に追加する場合、すべてのオブジェクトを表示できない
CSCvj80556	[FMC] > [タスク（Tasks）] でタスクがスピンし続ける
CSCvj87081	接続イベントなし、または起動時に SFDataCorrelator が予期せず終了する、または purge_extra_users
CSCvj89445	GUI で展開ステータスが一致してない
CSCvk02250	「show memory binsize」および「show memory top-usage」で正しい情報が表示されない（修正完了）
CSCvk03749	トレースバックとリロード（プロセス名：lina）
CSCvk10127	センサー インターフェイスが no-auto-neg/10m/full-duplex にリセットされる
CSCvk12234	GUI：IKEv1 ポリシー スイッチの認証タイプをデフォルト値に変更する
CSCvk12245	GUI：ACP 編集からネットワーク グループを追加するときに、ネットワーク オブジェクトの [追加（Add）] ボタンが機能しない
CSCvk16858	Panic:appAgent_reply_processor_thread-Error: miovif_add_interface_map

不具合 ID	タイトル
CSCvk20497	「不明なオブジェクト」として表示されるネットワーク分析ポリシー
CSCvk20603	List.pm は、FTD デバイスに「警告」メッセージを出力してはならない
CSCvk31035	KVM（FTD）：外部からの Web サーバのマッピングが他のプラットフォームと一貫した動作をしない
CSCvk33923	FMC から管理対象の FTD デバイスを削除した後のディスク使用率が高い
CSCvk34567	delete_rules.pl スクリプトを使用してローカル ルールを削除できない
CSCvk34648	高スループットの LAN 間 VPN トラフィックによりデータ キー再生成で Firepower 2100 トンネルがフラップする
CSCvk38322	バージョン 6.2.3 の Firepower Web UI は、Internet Explorer 11 の互換表示と互換性がない
CSCvk54376	復元は、FMC HA が一時停止するまで許可されない
CSCvk58543	FMC が hm_notifyd を受信し、ヘルス アラートを終了する
CSCvk62871	パッシブ モードの Firepower 2100 FTP クライアントがサーバとのデータ チャネルを確立できない
CSCvk67239	「Thread Name: Logger Page fault: Address not mapped」での FTD または ASA のトレースバックとリロード
CSCvk69823	FMC または FTD のいずれでも変更を加えていないにもかかわらず、FlexConfig オブジェクトがデバイスにプッシュされる
CSCvk72508	QoS ルールは、ユーザ定義のアプリケーション フィルタでは機能しない
CSCvk76274	FMC API が HA FTD のスタンバイ装置から適切な情報を取得していない
CSCvm03730	FMC の [SLAモニタオブジェクト（SLA Monitor Object）] メニューに [インターフェイス名（Interface Name）] フィールドがない
CSCvm07046	「Netflow_Delete_Destination」を flexconfig ポリシーに保存するときのエラー メッセージ
CSCvm10968	CVE-2018-5391 不適切な IP フラグメント処理を通じたリモート Denial of Service（DoS）
CSCvm39670	ユーザ名の文字制限
CSCvm48220	update_snort_attrib_table プロセスでの HA スタンバイの不正なチェックの修正

不具合 ID	タイトル
CSCvm59386	/ngfw ディレクトリのディスク使用率が高いため、ポリシーの展開に失敗する
CSCvm81052	無効な証明書チェーンが原因で、ローカル マルウェア検出の更新が FMC にダウンロードされない
CSCvn11219	「Not a directory」というエラー メッセージが表示され、ポリシーの展開に失敗した



第 8 章

既知の問題

この Firepower バージョンが最初にリリースされたとき、ここに記載されているバグの存在が確認されました。

既知の問題の検索

サポート契約がある場合は、Cisco Bug Search Tool を使用して Firepower 製品の最新のオープン バグ リストを取得することができます。これらの一般的なクエリには、バージョン 6.3.0を実行している Firepower 製品の未解決のバグが表示されます。

- Firepower Management Center
- Firepower Management Center Virtual
- ASA with FirePOWER Services
- NGIPSv

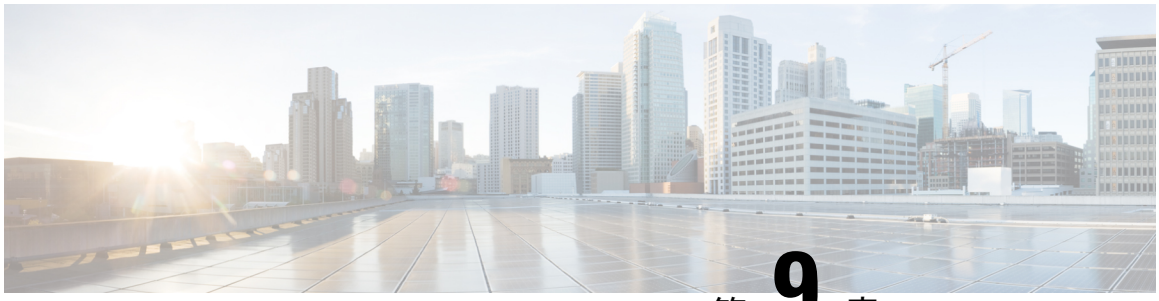
検索では、特定の Firepower プラットフォームとバージョンに影響するバグに絞り込むことができます。バグ ID ごとに検索したり、特定のキーワードを検索することもできます。

バージョン 6.3.0 の既知の問題

表 *40* : バージョン *6.3.0* の既知の問題

不具合 ID	タイトル
CSCvk74150	FDM HA を切り替えた後、6.3.0-1376 で展開に 25 分以上かかる
CSCvm29525	LOM ユーザの最大数を作成した後、ipmitool を使用してリモートでログインできない

不具合 ID	タイトル
CSCvm32307	ポート チャネル サブインターフェイスでパケット キャプチャを実行するためのオプションが必要
CSCvm37935	デフォルトの PPM しきい値が低いため、仮想デバイスでルールの評価が中断されることがある
CSCvm53619	フェールオーバー インターフェイスの MAC アドレスが正しく更新されない
CSCvn12381	4140 マルチインスタンスが 4 つのインスタンスで正しくロードバランシングされない
CSCvn19074	MSP：CIP Write アプリケーションのリセットでブロックするアクセス制御ルールがブロックしない
CSCvn19289	curl の複数の脆弱性
CSCvn32308	セカンダリの自己バックアップを復元するには、ライセンスを再登録する必要がある
CSCvn44222	6.3.0-79：6.3.0-79 から 6.4.0-1058 への HA アップグレードの実行中にアップグレードが失敗した
CSCvn46121	デフォルト アクションが syslog に記録される場合、セキュリティ インテリジェンス IP モニタ イベントが syslog に送信されない
CSCvn52181	FMC4500：ベースラインにおけるコンソールでの IPv6 設定および NTP に関連する障害の検出
CSCvn53145	ポリシーの展開で「Variable set has invalid execulded values」がスローされた



第 9 章

支援が必要な場合

Firepower をお選びいただき、ありがとうございます。

オンライン リソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービス リクエストをオープンしたりするためのオンライン リソースを提供しています。これらのリソースは、Firepower ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- Cisco Notification Service：https://www.cisco.com/cisco/support/notifications.html

シスコ サポートおよびダウンロード サイトの大部分のツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンライン リソースを使用して問題を解決できない場合は、Cisco TAC にお問い合わせください。

- Cisco TAC の電子メール アドレス：tac@cisco.com
- Cisco TAC の電話番号（北米）：1.408.526.7209 または 1.800.553.2447
- Cisco TAC の連絡先（世界全域）：Cisco Worldwide Support の連絡先