Cisco Firepower バージョン 6.5.0 リリースノート

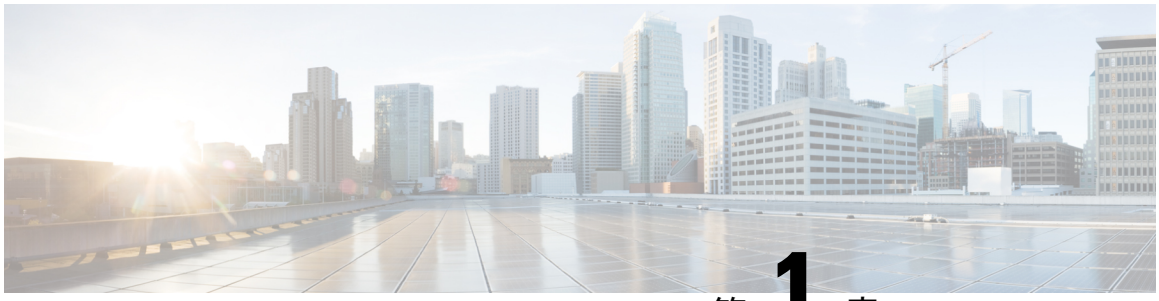
初版：2019 年 9 月 26 日

最終更新：2020 年 4 月 16 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 6.5.0 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 6.5.0 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、このドキュメントお読みください。

Firepower ソフトウェアのアップグレードまたは新規インストールは、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 （85 ページ）
- インストール手順 （94 ページ）

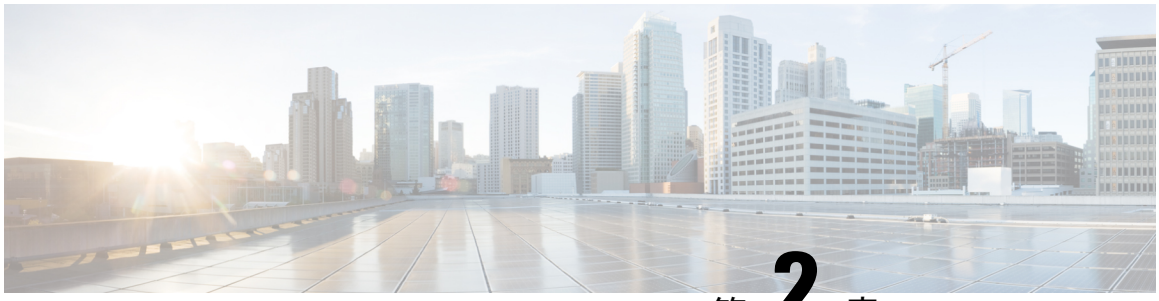
リリース日

バージョン 6.5.0 で使用可能なすべてのプラットフォームの一覧については、「互換性 （3 ページ）」を参照してください。

シスコは、更新版ビルドを適宜リリースしています。ほとんどの場合、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。最新のビルドを使用することを強くお勧めします。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 （101 ページ）を参照してください。

表 *1 :* バージョン *6.5.0* 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：再イメージ化
123	2020 年 2 月 3 日	FMC/FMCv	FMC/FMCv
120	2019 年 10 月 8 日	—	—
115	2019 年 9 月 26 日	すべてのデバイス	すべてのデバイス



第 2 章

互換性

この章では、Firepower バージョン 6.5.0の互換性に関する情報を提供します。

Firepower Management Centerについて

バージョン 6.5.0 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、混在展開を含めて、FTD または NGIPS を実行する複数のデバイスを管理できます。

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

バージョン 6.5.0 は、以下をサポートします。

- FMC 1600、2600、4600
- FMC 1000、2500、4500
- FMC 2000、4000

BIOS および RAID コントローラのファームウェアを最新の状態に保つことをお勧めします。詳細については、『Cisco Firepower Compatibility Guide』を参照してください。

Firepower Management Center Virtual （FMCv）プラットフォーム：

バージョン 6.5.0 は、以下をサポートします。

- VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 上の FMCv および FMCv 300
- カーネルベース仮想マシン（KVM）上の FMCv

- Amazon Web Services（AWS）上の FMCv
- Microsoft Azure 上の FMCv

サポートされている FMCv インスタンスについては、『Cisco Firepower Management Center Virtual 入門ガイド』を参照してください。

Firepower デバイス

バージョン 6.5.0 Firepower 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**：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。一部ではどちらを実行することもできますが、両方を同時に実行することはできません。
- **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（FMC）を使用したリモート管理をサポートします。
- **ローカル管理**：一部の Firepower デバイスは、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）で FTD を管理するか、ASDM で ASA FirePOWER を管理できます。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。
- **OS/ハイパーバイザ**：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。

サポートされている Firepower のデバイス

次の表は、バージョン 6.5.0 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 *6.5.0* 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 1010、1120、1140、1150 Firepower 2110、2120、2130、2140	FTD	FDM	—

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 4110、4120、4140、4150 Firepower 4115、4125、4145 Firepower 9300 SM-24、SM-36、SM-44 モジュールを搭載 Firepower 9300 SM-40、SM-48、SM-56 モジュールを搭載	FTD	FDM	FXOS 2.7.1.92 + 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 FXOS Release Notes, 2.7(1)』を参照してください。
ISA 3000 ASA 5508-X、5516-X ASA 5525-X、5545-X、5555-X	FTD	FDM	—
	ASA FirePOWER（NGIPS）	ASDM	ASA 9.5(2) ～ 9.14(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 5508-X および 5516-X を最新の ROMMON イメージにアップグレードすることをお勧めします。手順については、『Cisco ASA and Firepower Threat Defense Reimage Guide』を参照してください。
FTDv	FTD	FDM（AWS を除く）	次のいずれかです。 • VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 • KVM • AWS • Microsoft Azure サポートされているインスタンスについては、該当する FTDv のスタートアップガイド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
NGIPSv	NGIPS	—	VMware vSphere/VMware ESXi 6.0、6.5、または 6.7 サポートされているインスタンスについては、『Cisco Firepower NGIPSv Quick Start Guide for VMware』を参照してください。

マネージャとデバイスの互換性

FMC では、管理対象のデバイスと同じメジャーバージョンを実行している必要があります。パッチ未適用の FMC を使用してパッチを適用したデバイスを管理することもできますが、新しい機能と解決済みの問題では、多くの場合 FMC とその管理対象デバイスの「両方」で最新のパッチが必要になります。環境全体をパッチすることを強くお勧めします。

表 *3:* バージョン *6.5.0* のマネージャとデバイスの互換性

Firepower Management Center		
バージョン 6.5.0 FMC	管理可能	バージョン 6.2.3 ～ 6.5.0.x のデバイス。
バージョン 6.5.0 のデバイス	必須	バージョン 6.5.0 FMC。
Firepower Device Manager		
バージョン 6.5.0 FDM	管理可能	FTD デバイス 1 台。
ASDM		
バージョン 7.13.1 の ASDM	管理可能	バージョン 6.5.0.x 以前の ASA FirePOWER モジュール。 ASA、ASDM、および ASA FirePOWER のバージョン間には広範な互換性がありますが、ASDM の新しいバージョンでは、古い ASA デバイス上の ASA FirePOWER モジュールを管理できない場合があります。詳細については、『Cisco ASA の互換性』 を参照してください。
バージョン 6.5.0 ASA FirePOWER module	必須	バージョン 7.13.1 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。

FMC でのセキュア通信

SSL 証明書を使用すると、FMC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 Configuration Guide』を参照してください。

Firepower Web インターフェイスでテストされたブラウザ

Firepower Web インターフェイスは、現在サポートされているバージョンの MacOS と Microsoft Windows を実行している一般的なブラウザ（Google Chrome、Mozilla Firefox、および Microsoft Internet Explorer）の最新バージョンでテストされています。他のブラウザで問題が発生した場合、またはサポートが終了したオペレーティングシステムを実行している場合は、交換またはアップグレードしてください。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） Apple Safari または Microsoft Edge での広範なテストは実施されていませんが、Cisco TAC では、これらのブラウザの最新バージョンで発生した問題に関するフィードバックを求めています。

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、[Firefoxをリフレッシュ（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 11（Windows のみ）	JavaScript、Cookie、TLS v1.2、128 ビット暗号化 また、次のことを行う必要があります。 • [保存しているページの新しいバージョンがあるかどうかの確認（Check for newer versions of stored pages）] 閲覧履歴オプションについては、[自動（Automatically）] を選択してください。 • [サーバーにファイルをアップロードするときにローカルディレクトリのパスを含める（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。 • 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。 FMC ウォークスルーではテストされていません。

ブラウザ拡張機能との互換性

一部のブラウザ拡張機能（Grammarly や Whatfix Editor など）によって、PKI オブジェクトの証明書やキーなどのフィールドの値が保存されなくなる場合があります。これらの拡張機能は文字（HTML など）をフィールドに挿入するため、FMC で無効として認識されることになります。FMC の使用時はこれらの拡張機能を無効にすることをお勧めします。

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

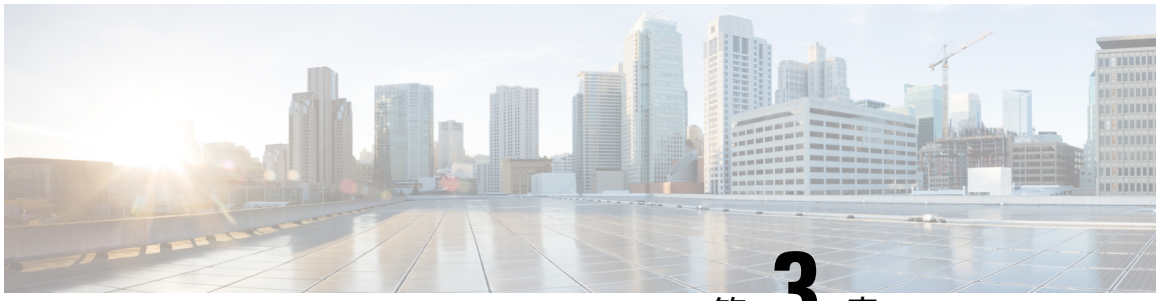
インターフェイス	解像度
Firepower Management Center	1280 X 720
Firepower Device Manager	1024 X 768
を管理している ASDM ASA FirePOWER module	1024 X 768
Firepower Chassis Manager 向け Firepower 4100/9300 シャーシ	1024 X 768

その他の互換性関連のリソース

次の表に、リリースノートとその他の互換性情報へのリンクを示します。ドキュメントの完全なロードマップについては、ドキュメントロードマップ （99 ページ）を参照してください。

表 *6 :* その他の互換性関連のリソース

説明	リソース
互換性ガイドには、バンドルコンポーネントや統合製品をなど、サポートされているハードウェアモデルとソフトウェアバージョンに関する詳細な互換性情報が記載されています。	Cisco Firepower Compatibility Guide Cisco ASA の互換性 Cisco Firepower 4100/9300 FXOS の互換性
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、リリース固有の情報が記載されています。	Cisco Firepower リリース ノート Cisco ASA リリースノート Cisco Firepower 4100/9300 FXOS リリースノート
持続性に関する速報には、管理プラットフォームやオペレーティングシステムなど、シスコ□次世代ファイアウォール製品ラインに関するサポートタイムラインが記載されています。	Cisco NGFW 製品ラインのソフトウェアリリースおよび持続性に関する速報



第 3 章

特長と機能

Firepower バージョン 6.5.0 には以下が含まれます。

新機能

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

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

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

表 *7:* バージョン *6.5.0* の新機能：*FMC* 導入環境

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

機能	説明
VMware 上の FMCv 300	より大規模な Firepower Management Center Virtual for VMware である FMCv 300 が導入されました。他の FMCv インスタンスで管理できるデバイスは 25 台ですが、この FMCv では最大 300 台のデバイスを管理できます。 FMCモデル移行機能を使用すると、性能が劣るプラットフォームから FMCv 300 に切り替えることができます。
VMware vSphere/VMware ESXi 6.7 のサポート	VMware vSphere/VMware ESXi 6.7 に FMCv、FTDv、および NGIPSv 仮想アプライアンスを展開できるようになりました。
Firepower Threat Defense	
Firepower 1010 ハードウェア スイッチのサポート	Firepower 1010 で、各イーサネットインターフェイスをスイッチポートまたはファイアウォールインターフェイスとして設定できるようになりました。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [VLANインターフェイスの追加（Add VLAN Interface）]** サポートされるプラットフォーム：Firepower 1010
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+）をサポートするようになりました。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）] > [PoE] サポートされるプラットフォーム：Firepower 1010

機能	説明
キャリアグレード NAT の拡張	キャリア グレードまたは大規模 PAT では、NAT に一度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。 新規/変更された画面：**[デバイス（Devices）]** > **[NAT]** > FTD NAT ポリシーの追加/編集 > NAT ルールの追加/編集 > [PAT プール（PAT Pool）] タブ > [ブロック割り当て（Block Allocation）] オプション サポートされているプラットフォーム：すべてのFTDデバイス
Firepower 4100/9300 上の複数のコンテナインスタンスの TLS 暗号化アクセラレーション	Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。 新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることは「ありません」。代わりに、**create hw-crypto** および **scope hw-crypto** CLI コマンドを使用してください。詳細については、『Cisco Firepower 4100/9300 FXOS Command Reference』を参照してください。 新しい FXOS CLI コマンド： • **create hw-crypto** • **delete hw-crypto** • **scope hw-crypto** • **show hw-crypto** 削除された FXOS CLI コマンド： • **show hwCrypto**（**show hw-crypto** に置き換えられました） • **config hwCrypto** 削除された FTD CLI コマンド： • **show crypto accelerator status** サポートされるプラットフォーム：Firepower 4100/9300
アクセス制御とイベント分析	

機能	説明
アクセスコントロールルールのフィルタリング	検索条件に基づいてアクセスコントロールルールをフィルタ処理できるようになりました。 新規/変更された画面：[ポリシー（Policies）]>[アクセス制御（Access Control）]>[アクセス制御（Access Control）]>ポリシーの追加/編集>フィルタボタン（[フィルタ条件に一致するルールのみを表示（show only rules matching filter criteria）]） サポートされるプラットフォーム： FMC
URL カテゴリまたはレピュテーションの異議申し立て	URLのカテゴリまたはレピュテーションについて異議を申し立てることができるようになりました。 新規/変更された画面： • [分析（Analysis）]>[接続イベント（Connection Events）]>カテゴリまたはレピュテーションを右クリック>[未処理（Dispute）] • [分析（Analysis）]>[詳細（Advanced）]>[URL]>URLの検索>[未処理（Dispute）]ボタン • [システム（System）]>[統合（Integration）]>[クラウドサービス（Cloud Services）]>[未処理（Dispute）]リンク サポートされるプラットフォーム： FMC

機能	説明
宛先ベースのセキュリティグループタグ（SGT）を使用したユーザ制御	アクセスコントロールルール内の送信元および宛先の両方の一致基準にISE SGT タグを使用できるようになりました。SGT タグは、ISE によって取得されたタグからホスト/ネットワークへのマッピングです。 新しい接続イベントフィールド： • [宛先SGT（Destination SGT）]（syslog：DestinationSecurityGroupTag）：接続レスポンダの SGT 属性。 名前が変更された接続イベントフィールド： • [送信元SGT（Source SGT）]（syslog：SourceSecurityGroupTag）：接続イニシエータの SGT 属性。[セキュリティグループタグ（Security Group Tag）]（syslog：SecurityGroup）から変更されました。 新規/変更された画面：[システム（System）] > [統合（Integration）] > [IDソース（Identity Sources）] > [Identity Services Engine] > [セッションディレクトリのトピック（Session Directory Topic）] および [SXPのトピック（SXP Topic）] 登録オプション サポートされるプラットフォーム：すべて
Cisco Firepower User Agent バージョン 2.5 の統合	Firepower バージョン 6.4.0 および 6.5.0 と統合できる Cisco Firepower User Agent バージョン 2.5 がリリースされました。 （注） Cisco Firepower User Agent ソフトウェアとアイデンティティソースについてはサポートの終了が予定されています。今すぐ Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に切り替えてください。これにより、ユーザエージェントで使用できない機能も利用できるようになります。ライセンスを変換するには、販売担当者にお問い合わせください。 詳細については、「Cisco Firepower Management Center Configuration Guides」ページで該当する *Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。 新規/変更された FMC CLI コマンド： **configure user-agent** サポートされるプラットフォーム： FMC

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

機能	説明
設定できるドメイン数の増加（マルチテナンシー）	マルチテナンシーを実装する（管理対象デバイス、設定、およびイベントへのユーザアクセスをセグメント化する）場合、最上位のグローバルドメインの下に、2 つまたは 3 つのレベルで最大 100 個のサブドメインを作成できます。以前は、最大で 50 ドメインでした。 サポートされるプラットフォーム： FMC
ISE 接続ステータスのモニタの機能拡張	[ISE接続ステータスのモニタ（ISE Connection Status Monitor）] ヘルスモジュールで、TrustSec SXP（SGT Exchange Protocol）サブスクリプションステータスに関する問題のアラートが表示されるようになりました。 サポートされるプラットフォーム： FMC
地域のクラウド	Cisco Threat Response の統合、Cisco Support Diagnostics、または Cisco Success Network 機能を使用する場合は、地域クラウドを選択できるようになりました。デフォルトでは、アップグレードによって米国（北米）リージョンに割り当てられます。 新規/変更された画面：[システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] サポートされているプラットフォーム：FMC、FTD
Cisco Support Diagnostics	*Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TAC は TAC ケースの過程でデバイスから必要な情報を収集することもできます。 アップグレードおよび再イメージ化中に、参加を承諾するか、辞退するかを尋ねられます。また、いつでもオプトインまたはオプトアウトできます。 現時点では、Cisco Support Diagnostics のサポートは一部のプラットフォームに限定されています。 新規/変更された画面： • **[システム（System）] > [スマートライセンス（Smart Licenses）]** • **[システム（System）] > [スマートライセンス（Smart Licenses）] > [登録（Register）]** サポートされるプラットフォーム：FMC および管理対象の Firepower 4100/9300

機能	説明
FMC モデル移行	バックアップおよび復元機能を使用して、FMC が同じモデルでない場合でも、FMC 間で設定とイベントを移行できるようになりました。これにより、組織の拡大、物理実装から仮想実装への移行、ハードウェアの更新など、技術面またはビジネス面の理由による FMC の交換が容易になります。 一般に、ローエンドの FMC からハイエンドの FMC に移行することはできますが、その逆に移行することはできません。KVM および Microsoft Azure からの移行はサポートされていません。また、Cisco Smart Software Manager（CSSM）への登録を解除して再登録する必要があります。 サポート対象の移行先モデルなどの詳細については、『Firepower Management Center モデル移行ガイド』を参照してください。 サポートされるプラットフォーム： FMC
セキュリティと強化	
FXOS ベースの FTD デバイス上のアプライアンス コンポーネントの安全な消去	指定したアプライアンス コンポーネントを安全に消去する FXOS CLI を使用できるようになりました。 新しい FXOS CLI コマンド： **erase secure** サポートされるプラットフォーム：Firepower 1000/2000、および FTD を搭載した Firepower 4100/9300 シリーズ
初期設定時における FMC admin アカウントのパスワード要件の厳格化	FMC の初期設定時に、admin アカウントの「強力な」パスワードを選択することが必要になりました。設定プロセスでは、FMC Web インターフェイスと CLI の両方の admin アカウントにこの強力なパスワードが適用されます。 （注） バージョン 6.5.0+ にアップグレードしても、脆弱なパスワードを強力なパスワードに変更する必要はありません。物理 FMC 上の LOM ユーザを除き（これには admin ユーザが含まれます）、新しい脆弱なパスワードの選択は禁止されていません。ただし、すべての Firepower ユーザアカウント（特に管理者アクセス権を持つユーザアカウント）に強力なパスワードを設定することを推奨します。 サポートされるプラットフォーム： FMC

機能	説明
同時ユーザセッション数の制限	FMC に同時にログインできるユーザの数を制限できるようになりました。読み取り専用ロール、読み取り/書き込みロール、またはその両方を持つユーザの同時セッション数を制限できます。CLI ユーザは、読み取り/書き込み設定によって制限されることに注意してください。 新規/変更された画面：[システム（System）] > [設定（Configuration）] > [ユーザ設定（User Configuration）] > [許可された最大同時セッション数（Max Concurrent Sessions Allowed）] オプション サポートされるプラットフォーム： FMC
認証済み NTP サーバ	SHA1 または MD5 対称キー認証を使用して FMC と NTP サーバとの間のセキュアな通信を設定できるようになりました。システムセキュリティのために、この機能を使用することをお勧めします。 新規/変更された画面：[システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）] サポートされるプラットフォーム： FMC
ユーザビリティ	

機能	説明
初期設定の改善	新規および再イメージ化された FMC では、以前の初期設定プロセスがウィザードに置き換えられます。GUI ウィザードを使用すると、初期設定の完了時に FMC に [デバイス管理（Device Management）] ページが表示され、導入環境のライセンシングと設定をすぐに開始できます。 また、設定プロセスでは以下が自動的にスケジュールされます。 • ソフトウェアのダウンロード。導入環境に適用されるソフトウェアパッチおよび公開されているホットフィックスをダウンロードする（インストールはしない）、毎週にスケジュール設定されたタスクが作成されます。 • FMC設定のみのバックアップ。FMCの設定をバックアップしてローカルに保存する、毎週にスケジュール設定されたタスクが作成されます。 • GeoDBの更新。地理位置情報データベースの毎週の更新が有効になります。 タスクはUTCでスケジュールされるため、いつ現地で実行されるかは、日付と場所によって異なります。また、タスクはUTCでスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされたタスクは、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。 （注） 自動スケジュール設定タスクと GeoDB の更新を確認し、必要に応じて調整することを強くお勧めします。 アップグレードされた FMC は影響を受けません。初期設定ウィザードの詳細については、ご使用の FMC モデルの『Getting Started Guide』を参照してください。スケジュールされたタスクの詳細については、『Firepower Management Center Configuration Guide』を参照してください。 サポートされるプラットフォーム： FMC

機能	説明
FMC Web インターフェイスのライトテーマ（試験版）	システムはデフォルトでクラシックテーマになっていますが、試験版の「ライト」テーマを選択することもできます。 （注） ライトテーマは試験版であるため、テキストやその他の UI 要素の位置がずれていることがあります。場合によっては、応答時間が通常より長くなることもあります。ページまたは機能を使用できない問題が発生した場合は、クラシックテーマに戻してください。すべてに対応することはできませんが、フィードバックもお寄せください。[ユーザ設定(User Preferences)] ページのフィードバックリンクを使用するか、fmc-light-theme-feedback@cisco.com までお問い合わせください。 新規/変更された画面：ユーザ名の下にあるドロップダウンリストの [ユーザ設定（User Preferences）] サポートされるプラットフォーム： FMC

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

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

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

リリース：2019 年 9 月 26 日

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

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

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

機能	説明
ISA 3000 デバイスの高精度時間プロトコル（PTP）の設定。	FlexConfig を使用して、ISA 3000 デバイスで高精度時間プロトコル（PTP）を設定できます。PTP は、パケットベースネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。このプロトコルは、ネットワーク化された産業用の測定および制御システム向けとして特別に設計されています。 FlexConfig オブジェクトに、**ptp** および **igmp**（インターフェイスモード）コマンド、およびグローバルコマンド **ptp mode e2etransparent** と **ptp domain** を追加できるようになりました。また、FTD CLI に **show ptp** コマンドが追加されました。
EtherChannel（ポートチャネル）インターフェイス。	EtherChannel インターフェイス（ポートチャネルとも呼ばれます）を設定できます。 （注） FDM の Etherchannel は Firepower 1000 および 2100 シリーズにのみ追加できます。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに FDM の [インターフェイス（Interfaces）] ページに表示されます。 **[デバイス（Device）]** > **[インターフェイス（Interfaces）]** ページが更新され、EtherChannel の作成ができるようになりました。
FDM からシステムを再起動およびシャットダウンする機能。	新しい [再起動/シャットダウン（Reboot/Shutdown）] システム設定ページからシステムを再起動またはシャットダウンできるようになりました。以前は、FDM の CLI コンソールを使用して、あるいは SSH またはコンソールセッションから、**reboot** および **shutdown** コマンドを発行する必要がありました。これらコマンドを使用するには、管理者権限が必要です。
FDM CLI コンソールでの **failover** コマンドのサポート。	FDM CLI コンソールで **failover** コマンドを発行できるようになりました。
スタティックルート用のサービスレベル契約（SLA）モニタ。	スタティックルートとともに使用するためのサービスレベル契約（SLA）モニタオブジェクトを設定します。SLA モニタを使用すると、スタティックルートの状態を追跡し、失敗したルートを自動的に新しいものに交換できます。SLA モニタオブジェクトを選択できるように、[オブジェクト（Object）] ページに [SLA モニタ（SLA Monitors）] を追加し、スタティックルートを更新しました。

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

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

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

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

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

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

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

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

廃止された機能

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

廃止されたプラットフォームの販売終了およびサポート終了の通知へのリンクを含む、サポート対象のFirepowerのすべてのバージョンの詳細な互換性情報については、『Cisco Firepower Compatibility Guide』を参照してください。

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

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

バージョン6.5.0で廃止された機能

これらの機能はバージョン6.5.0で廃止されました。

表 *8 :* バージョン *6.5.0* で廃止された機能

機能	説明
FMC CLI を無効にする機能	バージョン 6.3.0 では、明示的に有効にする必要がある FMC CLI が導入されました。バージョン 6.5.0 では、新しい展開とアップグレードされた展開の両方に対して、FMC CLI が自動的に有効になります。Linux シェル（エキスパート モードとも呼ばれる）にアクセスする場合は、CLI にログインしてから、**expert** コマンドを使用する必要があります。 **注意** Cisco TAC の指示がない限り、シェルを使用して Firepower アプライアンスにアクセスしないことをお勧めします。 廃止されたオプション：[システム（System）] > [設定（Configuration）]> [コンソール設定（Console Configuration）] > [CLI アクセスの有効化（Enable CLI Access）] チェックボックス 影響を受けるプラットフォーム：FMC
TLS 1.0 および 1.1	セキュリティ強化対策： • キャプティブポータル（アクティブ認証）では、TLS 1.0 のサポートが廃止されました。 • ホスト入力で TLS 1.0 および TLS 1.1 のサポートが廃止されました。 クライアントが Firepower アプライアンスとの接続に失敗した場合は、TLS 1.2 をサポートするようにクライアントをアップグレードすることをお勧めします。 影響を受けるプラットフォーム：FMC
Firepower 4100/9300 用の TLS crypto アクセラレーション FXOS CLI コマンド	Firepower 4100/9300 の複数のコンテナ インスタンスに対して TLS crypto アクセラレーションを許可する一環として、次の FXOS CLI コマンドを削除しました。 • **show hwCrypto** • **config hwCrypto** および、この FTD CLI コマンドを削除しました。 • **show crypto accelerator status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。 影響を受けるプラットフォーム：Firepower 4100/9300

機能	説明
Cisco Security Packet Analyzer の統合	バージョン 6.5.0 では、FMC と Cisco Security Packet Analyzer の統合のサポートを終了します。 廃止された画面/オプション： • **[システム（System）] > [統合（Integration）] > [パケットアナライザ（Packet Analyzer）]** • **[分析（Analysis）] > [詳細（Advanced）] > [パケットアナライザのクエリ（Packet Analyzer Queries）]** • ダッシュボードまたはイベント ビューアでイベントを右クリックしたときの [Query Packet Analyzer] 影響を受けるプラットフォーム：FMC
Firepower Management Center モデル FMC 750、1500、3500	MC750、MC1500、および MC3500 モデルでは、Firepower Management Center ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。これらの FMC を使用してバージョン 6.5.0 以降のデバイスを管理することはできません。
Firepower ソフトウェアを搭載した ASA 5515-X および ASA 5585-X シリーズ デバイス	これらのモデルでは、Firepower ソフトウェア（FTD と ASA FirePOWER の両方）をバージョン 6.5.0+ にアップグレードしたり、このバージョンを新規インストールしたりできません。 • ASA 5515-X • ASA 5585-X-SSP-10、-20、-40、-60 ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。
Firepower 7000/8000 シリーズ デバイス	AMP モデルを含む、Firepower 7000/8000 シリーズ デバイスでは、Firepower ソフトウェアをバージョン 6.5.0 以降にアップグレードしたり、このバージョンを新規インストールしたりできません。ただし、バージョン 6.5.0 の FMC を使用して、古いデバイス（バージョン 6.2.3 ～ 6.4.x）を管理できます。

バージョン 6.4.0 で廃止された機能

これらの機能はバージョン 6.4.0 で廃止されました。

表 *9* : バージョン *6.4.0* で廃止された機能

機能	説明
SSL ハードウェア アクセラレーション FTD CLI コマンド	TLS crypto アクセラレーション機能の一部として、次の FTD CLI コマンドを削除しました。 • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** 代替手段の詳細については、新しい機能のマニュアルを参照してください。 影響を受けるプラットフォーム：FTD

バージョン 6.3.0 で廃止された機能

これらの機能はバージョン 6.3.0 で廃止されました。

表 *10* : バージョン *6.3.0* で廃止された機能

機能	説明
復号化のための EMS 拡張機能のサポート	バージョン 6.3.0 では、バージョン 6.2.3.8/6.2.3.9 で導入された EMS 拡張機能のサポートが中止されます。つまり、[復号 - 再署名（Decrypt-Resign）] と [復号 - 既知のキー（Decrypt-Known Key）] の両方の SSL ポリシーアクションが、ClientHello ネゴシエーション時に EMS 拡張機能をサポート（よりセキュアな通信が可能）しなくなります。EMS 拡張機能は、 RFC 7627 によって定義されています。 FMC 展開では、この機能は、デバイスのバージョンによって異なります。FMC をバージョン 6.3.0 にアップグレードしても、サポートされるバージョンがデバイスで実行されていれば、サポートは中止されません。ただし、デバイスをバージョン 6.3.0 にデバイスをアップグレードすると、サポートは中止されます。 サポートはバージョン 6.3.0.1 で再導入されています。 影響を受けるプラットフォーム：すべて
パッシブおよびインライン タップ インターフェイスの復号化	バージョン 6.3.0 では、パッシブ モードまたはインライン タップ モードのインターフェイスでの復号化トラフィックは、GUI を介して設定することはできますが、サポートされなくなりました。暗号化されたトラフィックのインスペクションは必然的に制限されます。

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

廃止された FlexConfig コマンド

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

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

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

Firepower Management Center を使用した FTD

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

表 *11* : *FMC* を使用した *FTD*：廃止された *FlexConfig* オブジェクト

非推奨メソッド	オブジェクト	詳細	新しいロケーション
6.3.0 以降	FlexConfig オブジェクト： • Default_DNS_Configure 関連するテキスト オブジェクト： • defaultDNSNameServerList • defaultDNSParameters	デフォルト DNS グループを設定します。デフォルト DNS グループでは、データインターフェイスの完全修飾ドメイン名を解決する際に使用できる DNS サーバを定義します。これにより、IP アドレスではなくホスト名を使用して、CLI で **ping** などのコマンドを使用することができます。	FTD プラットフォーム設定ポリシーで、データインターフェイスの DNS を設定します。
6.3.0 以降	FlexConfig オブジェクト： • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout 関連するテキスト オブジェクト： • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout	初期接続制限およびタイムアウトを設定して SYN フラッド サービス妨害（DoS）攻撃から保護します。	これらの機能は、FTD サービス ポリシーで設定します。ポリシーは、デバイスに割り当てられているアクセス制御ポリシーの [詳細設定（Advanced）] タブで確認できます。

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

表 *12* : *FMC* を使用した *FTD*：廃止された *CLI* コマンド

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

Firepower Device Manager を使用した FTD

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

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

表 *13 : FDM* を使用した *FTD* : 廃止された *CLI* コマンド

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

FMC メニューの変更

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

表 *14 : Firepower Management Center* メニューの変更

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

FMC How-To ウォークスルー

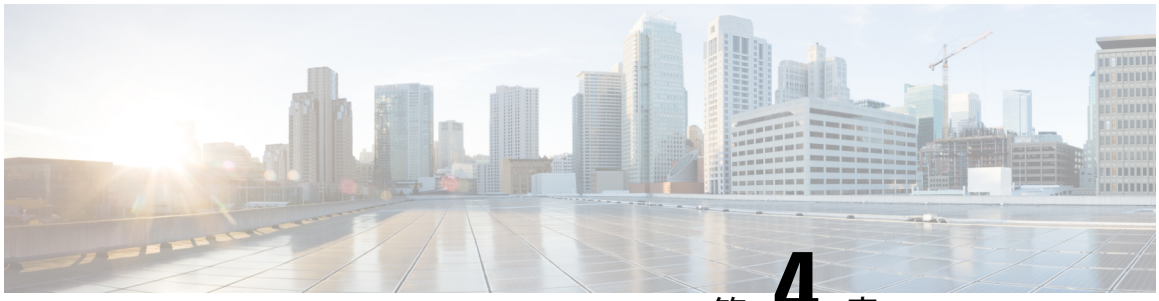
バージョン 6.3.0 では、デバイスのセットアップやポリシー設定などのさまざまな基本タスクについて順を追って説明する、FMC に関するウォークスルー（How-To とも呼ばれる）が導入されています。ブラウザウィンドウの下部にある [How To] をクリックし、ウォークスルーを選択して、手順ごとの説明に従って操作します。

（注） ウォークスルーはFirefoxおよびChromeブラウザでテストされています。別のブラウザで問題が発生した場合は、Firefox または Chrome に切り替えてください。問題が解消されない場合は、Cisco TAC にお問い合わせください。

次の表に、一般的な問題点と解決策をいくつか示します。ウォークスルーは、右上隅の [x] をクリックするといつでも終了できます。

表 *15 :* ウォークスルーのトラブルシューティング

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



第 4 章

バージョン 6.5.0 へのアップグレード

この章では、バージョン 6.5.0 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。

に関するガイドラインと警告 バージョン 6.5.0

このチェックリストには、バージョン 6.5.0 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。「以前に公開されたガイドラインと警告 （64 ページ）」および「一般的なガイドラインと警告 （70 ページ）」も確認する必要があります。

表 *16* : バージョン *6.5.0* 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
	Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要 （44 ページ）	Firepower 1000 シリーズ	6.4.0	6.5.0 以降
	バージョン 6.5.0 での出力最適化の無効化 （44 ページ）	FTD	6.2.3 ～ 6.4.0.x	6.5.0 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
	アップグレードによって北米の Cisco Cloud に展開が割り当てられる （45 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降
	Cisco 脅威インテリジェンスダイレクタ（TID） 動作の変更 （45 ページ）	FMC	6.2.3 ～ 6.4.0.x	6.5.0 以降
	FTD/FDM アップグレード時に削除される履歴データ （46 ページ）	FDM を使用した FTD	6.2.3 ～ 6.4.0.x	6.5.0 以降
	新しい URL カテゴリとレピュテーション （46 ページ）	任意（Any）	6.2.3 ～ 6.4.0.x	6.5.0 以降

Firepower 1000 シリーズ デバイスではアップグレード後に電源の再投入が必要

展開：Firepower 1000 シリーズ デバイス

アップグレード元：バージョン 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0 では、Firepower 1000/2100 および Firepower 4100/9300 シリーズ デバイス向けの FXOS CLI の「安全に消去する」機能が導入されています。

Firepower 1000 シリーズ デバイスでは、この機能を適切に動作させるには、バージョン 6.5.0+ にアップグレードした後にデバイスの電源を再投入する必要があります。自動リブートでは十分ではありません。サポートされているその他のデバイスでは、電源の再投入は必要ありません。

バージョン 6.5.0 での出力最適化の無効化

展開：FTD

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0 のみ

CSCvq34340 を軽減するため、FTD デバイスをバージョン 6.4.0.7+ または バージョン 6.5.0.2+ にパッチすると、出力最適化処理がオフになります。これは、出力最適化機能が有効になっているか、無効になっているかに関係なく発生します。

バージョン 6.5.0 へのアップグレード：

- バージョン 6.2.3.x から：出力最適化を有効にしてオンにします。

- バージョン 6.3.0.x から：出力最適化を有効にしてオンにします。
- バージョン 6.4.0.x から：現在の設定を使用します。ただし、バージョン 6.4.0.x パッチにより出力最適化がオフになっても機能が引き続き有効になっている場合は、バージョン 6.5.0 へのアップグレードにより再度オンになります。

（注） バージョン 6.5.0.2+ にパッチを適用するか、またはバージョン 6.6.0 にアップグレードことをお勧めします。バージョン 6.5.0 または 6.5.0.1 のままの場合は、FTD CLI から **no asp inspect-dp egress-optimization** を実行して出力最適化を手動で無効にする必要があります。

この問題は、出力最適化が想定のとおりに動作するバージョン 6.6.0 で修正されました。詳細については、ソフトウェアアドバイザリ『FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature』を参照してください。

アップグレードによって北米の Cisco Cloud に展開が割り当てられる

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0+

シスコ クラウドサービスのリージョンが導入されました。導入環境の地域別クラウドは、Cisco Defense Orchestrator、Cisco Threat Response、Cisco Success Network、および Cisco Support Diagnostics の各機能に使用されます。

FMC 展開の場合、デフォルトでは、アップグレードによって米国（北米）リージョンに割り当てられます。リージョンは [システム（System）] > [統合（Integration）] > [クラウドサービス（Cloud Services）] ページで変更できます。

FDM を使用した FTD の場合は、スマートライセンスに登録するときにリージョンを選択します。登録済みデバイスをアップグレードすると、米国（北米）リージョンに割り当てられます。リージョンを変更するには、Cisco Smart Software Manager（CSSM）で登録解除して再登録する必要があります。

Cisco 脅威インテリジェンスダイレクタ（TID） 動作の変更

展開：FMC

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

バージョン 6.5.0+ では、TID ブロッキングおよびモニタリング監視可能アクションが、セキュリティ インテリジェンス ブラックリストを使用したブロッキングおよびモニタリングよりも優先されるようになりました。

[ブロック（Block）] TID 監視可能アクションを設定した場合は、トラフィックが [ブロック（Block）] に設定されたセキュリティ インテリジェンス ブラックリストにも一致していても、次のようになります。

- 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDブロック（TID Block）] のバリアントになります。
- システムは、[ブロック済み（Blocked）] のアクション実施を伴う TID インシデントを生成します。

[モニタ（Monitor）] TID 監視可能アクションを設定した場合は、トラフィックが [モニタ（Monitor）] に設定されたセキュリティ インテリジェンス ブラックリストにも一致していても、次のようになります。

- 接続イベントのセキュリティ インテリジェンス カテゴリは [TIDモニタ（TID Monitor）] のバリアントになります。
- システムは、[モニタ済み（Monitored）] のアクション実施を伴う TID インシデントを生成します。

以前は、どちらの場合も、システムではカテゴリが分析別に報告され、TIDインシデントは生成されませんでした。

（注） システムは引き続き、トラフィックを以前と同様に効果的に処理します。以前にブロックされたトラフィックは引き続きブロックされ、モニタ対象トラフィックは引き続きモニタされます。単に、どのコンポーネントが「クレジット」を取得するかが変更されます。また、生成される TID インシデントが増える場合もあります。

セキュリティ インテリジェンスと TID の両方を有効にした場合のシステム動作の詳細については、『Firepower Management Center Configuration Guide』の「TID-Firepower Management Center Action Prioritization」の情報を参照してください。

FTD/FDM アップグレード時に削除される履歴データ

展開：Firepower Device Manager

アップグレード元：バージョン 6.2.3 ～ 6.4.x

直接アップグレード先：バージョン 6.5.0 以降

データベース スキーマの変更により、すべての履歴レポート データがアップグレード中に削除されます。アップグレード後、履歴データをクエリしたり、履歴データをダッシュボードに表示したりすることはできません。

新しい URL カテゴリとレピュテーション

展開：すべて

アップグレード元：バージョン 6.2.3 ～ 6.4.0.x

直接アップグレード先：バージョン 6.5.0+

Cisco Talos Intelligence Group（Talos）は、URL の分類およびフィルタ処理のために、新しいカテゴリを導入し、レピュテーションの名前を変更しました。新しい URL カテゴリの説明については、Talos の「Intelligence Categories」サイトを参照してください。

また、ルール設定オプションは同じままですが、未分類およびレピュテーションのない URL の概念が新しくなっています。

- 未分類の URL は、疑わしい（Questionable）、ニュートラル（Neutral）、好ましい（Favorable）、信頼されている（Trusted）というレピュテーションのいずれかになります。

  [未分類（Uncategorized）] の URL はフィルタ処理できますが、レピュテーションによりさらに制約を追加することはできません。これらのルールは、レピュテーションに関係なく、すべての未分類 URL と一致します。

  カテゴリのない信頼されていない（Untrusted）ルールのような設定は存在しないことに注意してください。それ以外の場合、信頼されていない（Untrusted）レピュテーションの未分類 URL は、「悪意のあるサイト（Malicious Sites）」という新しい脅威カテゴリに自動的に割り当てられます。

- レピュテーションのない URL は任意のカテゴリに属することができます。

  レピュテーションのない URL をフィルタ処理することはできません。「レピュテーションなし」に対応するオプションはルールエディタにありません。ただし、レピュテーションに [すべて（Any）] を指定して URL をフィルタ処理することは可能で、その場合はレピュテーションのない URL が含まれます。これらの URL もカテゴリで制約する必要があります。Any/Any ルールに対するユーティリティはありません。

次の表に、アップグレードでの変更点の概要を示します。これらの変更は、ほとんどのお客様にとって最小限の影響で済むように設計されており、アップグレード後の展開を妨げることもありませんが、これらのリリースノートおよび現在の URL フィルタリングの設定を確認することを強くお勧めします。慎重な計画と準備は、誤った手順を回避することに加えて、アップグレード後のトラブルシューティングにかかる時間を短縮するのに役立ちます。

表 *17:* アップグレード時の展開の変更

変更内容	詳細
URL ルールのカテゴリが変更されます。	アップグレードにより、次のポリシーで、新しいカテゴリセットのほぼ同等のルールが使用されるように URL ルールが変更されます。 • アクセス コントロール • SSL • QoS（FMC のみ） • 相関（FMC のみ） これらの変更により、余分なルールや無効になったルールが生じ、パフォーマンスが低下する可能性があります。マージされたカテゴリが設定に含まれている場合、許可またはブロックされる URL が若干変更されることがあります。 カテゴリの変更に関する詳細なリストについては、「URL カテゴリの変更 （54 ページ）」を参照してください。
URL ルールのレピュテーションの名前が変更されます。	アップグレードにより、新しいレピュテーション名を使用するように URL ルールが変更されます。 1. 信頼されていない（「高リスク」だった） 2. 疑わしい（「疑わしいサイト」だった） 3. ニュートラル（「セキュリティ リスクのある無害なサイト」だった） 4. 好ましい（「無害なサイト」だった） 5. 信頼されている（「十分に既知」だった）
URL キャッシュをクリアします。	アップグレードによって URL キャッシュがクリアされます。このキャッシュには、システムが以前にクラウドで検索した結果が含まれています。ローカル データ セットに含まれていない URL については、アクセス時間が一時的に少し長くなることがあります。
「レガシー」イベントにラベルを付けます。	すでにログに記録されているイベントの場合、アップグレードにより、関連する URL のカテゴリおよびレピュテーション情報が「レガシー」としてラベル付けされます。これらのレガシー イベントは時間の経過とともにデータベースからエージ アウトします。

URL カテゴリおよびレピュテーションのアップグレード前のアクション

アップグレードする前に、次のアクションを実行します。

表 *18* : アップグレード前のアクション

アクション	詳細
アプライアンスが Talos のリソースにアクセスできることを確認します。	アップグレード後、システムは次のシスコのリソースと通信できる必要があります。 • https://regsvc.sco.cisco.com/ - 登録 • https://est.sco.cisco.com/ - セキュア通信のための証明書を取得 • https://updates-talos.sco.cisco.com/ - クライアント/サーバマニフェストを取得 • http://updates.ironport.com/ - データベースのダウンロード（注：ポート 80 を使用） • https://v3.sds.cisco.com/ - クラウドクエリ クラウドクエリサービスは、次の IP アドレスブロックも使用します。 • IPv4 クラウドクエリ： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 クラウドクエリ： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
潜在的なルールの問題を特定します。	今後の変更点を理解します。現在の URL フィルタリング設定を調べて、アップグレード後に実行する必要があるアクションを特定します（次の項を参照）。 （注） 廃止されたカテゴリを使用する URL ルールをこの時点で変更することができます。そうしない場合、それらを使用するルールによってアップグレード後の展開が妨げられます。 FMC 展開では、アクセスコントロールのルールや下位ポリシー（SSL など）のルールを含む、ポリシーの現在の保存されている設定に関する詳細情報を提供する、アクセスコントロール ポリシー レポートを生成することを推奨します。URL ルールごとに、現在のカテゴリ、レピュテーション、関連付けられているルール アクションが表示されます。FMC で **[Policies]** > **[Access Control]** を選択し、該当するポリシーの横にあるレポート アイコン（  ）をクリックします。

URL カテゴリおよびレピュテーションのアップグレード後のアクション

アップグレード後に URL フィルタリング設定を再確認し、できるだけ早く次のアクションを実行する必要があります。展開のタイプとアップグレードによって行われた変更に応じて、一部（すべてではない）の問題が GUI でマークされることがあります。たとえば、FMC/FDM のアクセス コントロール ポリシーでは、[警告の表示（Show Warnings）]（FMC）または [問題ルールの表示（Show Problem Rules）] (FDM) をクリックできます。

表 *19*：アップグレード後の操作

アクション	詳細
廃止されたカテゴリをルールから削除します。必須。 リスト：廃止されたカテゴリ（58 ページ）。	アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらを使用するルールは展開を阻止します。 FMC では、これらのルールがマークされます。
新しいカテゴリを含めるルールを作成または変更します。 リスト：新しいカテゴリ （57 ページ）。	ほとんどの新しいカテゴリは脅威を特定します。これらのカテゴリを使用することを強くお勧めします。 FMC では、この新しいカテゴリはこのアップグレード後にマークされませんが、今後、Talos によってカテゴリが追加される場合があります。この場合は新しいカテゴリがマークされます。
マージされたカテゴリの結果として変更されたルールを評価します。 リスト：マージされたカテゴリ （59 ページ）。	影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン（51 ページ）」を参照してください。 変更内容とプラットフォームがルールの警告を処理する方法に応じて、変更がマークされることがあります。たとえば、FMC は完全に冗長および完全にプリエンプション処理されたルールをマークしますが、部分的に重複したルールはマークしません。
分割されたカテゴリの結果として変更されたルールを評価します。 リスト：カテゴリの分割 （60 ページ）。	アップグレードにより、URL ルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。これにより URL のフィルタリング方法は変更されませんが、影響を受けるルールを変更して、新しい精度を活用することができます。 これらの変更はマークされません。

アクション	詳細
名前が変更されたカテゴリまたは**変更されていない**カテゴリを把握します。 リスト：カテゴリの名前変更（62 ページ）および変更されていないカテゴリ （63 ページ）。	特に対処の必要はありませんが、これらの変更に注意する必要があります。 これらの変更はマークされません。
未分類および**レピュテーションのない** URL の処理方法を評価します。	未分類の URL とレピュテーションのない URL を使用できるようになりましたが、未分類の URL をレピュテーションでフィルタ処理することも、レピュテーションのない URL をフィルタ処理することもできません。 [未分類（Uncategorized）] カテゴリまたは [すべて（Any）] のレピュテーションでフィルタ処理されるルールが、期待どおりに動作することを確認してください。

マージされた URL カテゴリを持つルールのガイドライン

アップグレード前に URL フィルタリング設定を確認する場合は、次のシナリオとガイドラインのどちらが適用されるかを決定します。これにより、アップグレード後の設定が予想どおりに実行され、問題を解決するためのクイックアクションを実行できるようになります。

表 *20*：マージされた *URL* カテゴリを持つルールのガイドライン

ガイドライン	詳細
ルールの順序によって、トラフィックに一致するルールが決定されます。	同じカテゴリを含むルールを検討する場合は、トラフィックが、その条件を含むリスト内の最初のルールと一致することに注意してください。
同じルール内のカテゴリと異なるルール内のカテゴリ	単一のルール内でカテゴリをマージすると、ルール内の単一のカテゴリにマージされます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A とカテゴリ B を持つルールがある場合、マージ後にルールは単一のカテゴリ AB を保持します。 異なるルールのカテゴリをマージすると、マージ後に各ルールで同じカテゴリを持つルールが個別に生成されます。たとえば、カテゴリ A とカテゴリ B がマージされてカテゴリ AB になり、カテゴリ A を持つルール 1 とカテゴリ B を持つルール 2 がある場合、マージ後にルール 1 とルール 2 にはカテゴリ AB がそれぞれ含まれます。この状況を解決する方法は、ルールの順序、ルールに関連付けられたアクションとレピュテーションレベル、ルールに含まれる他の URL カテゴリ、およびルールに含まれる非 URL 条件によって異なります。

ガイドライン	詳細
関連付けられたアクション	異なるルールのマージされたカテゴリが異なるアクションに関連付けられている場合、マージ後に、同じカテゴリに対して異なるアクションを持つ 2 つ以上のルールが生成される場合があります。
関連付けられているレピュテーションレベル	マージの前に異なるレピュテーションレベルに関連付けられたカテゴリが単一のルールに含まれている場合、マージされたカテゴリは、より包括的なレピュテーションレベルに関連付けられます。たとえば、カテゴリ A が特定のルールで [すべてのレピュテーション（Any reputation）] に関連付けられており、カテゴリ B が同じルールでレピュテーションレベル [3 - セキュリティリスクのある無害なサイト（3 - Benign sites with security risks）] に関連付けられている場合、マージ後に、そのルール内のカテゴリ AB は [すべてのレピュテーション（Any reputation）] に関連付けられます。
重複および冗長カテゴリとルール	マージ後、異なるルールには、異なるアクションとレピュテーションレベルに関連付けられている同じカテゴリが含まれる場合があります。 冗長ルールは完全に重複しているとは限りませんが、ルール順序が前にある別のルールが一致する場合、トラフィックに一致しなくなる可能性があります。たとえば、ルール 1 とカテゴリ A（[すべてのレピュテーション（Any Reputation）] に適用される）を事前マージし、ルール 2 とカテゴリ B（レピュテーション 1-3 のみに適用される）を事前マージする場合、マージ後に、ルール 1 とルール 2 の両方にカテゴリ AB が含まれるようになるが、ルール順序でルール 1 の順序が前にあると、ルール 2 が一致することはありません。 FMC において、同一のカテゴリとレピュテーションを持つルールでは警告が表示されます。ただし、これらの警告は、含まれているカテゴリが同じですが、レピュテーションが異なるルールを示すことはありません。 注意：重複または冗長カテゴリを解決する方法を決定する際には、ルールのすべての条件を考慮してください。
ルール内の他の URL カテゴリ	マージされた URL を含むルールには、他の URL カテゴリも含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。
ルール内の非 URL 条件	マージされた URL カテゴリを含むルールには、アプリケーション条件などの他のルール条件も含まれている場合があります。したがって、マージ後に特定のカテゴリが複製された場合は、これらのルールを削除するのではなく、変更する必要があることがあります。

次の表の例ではカテゴリ A とカテゴリ B を使用しています。現在はカテゴリ AB にマージされています。2 つのルールの例では、ルール 1 はルール 2 よりも前に表示されます。

表 *21* : マージされた *URL* カテゴリを持つルールの例

シナリオ	アップグレード前	アップグレード後
同じルール内のマージされたカテゴリ	ルール 1 にはカテゴリ A とカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。
異なるルール内でマージされたカテゴリ	ルール 1 にはカテゴリ A が含まれる。 ルール 2 にはカテゴリ B が含まれる。	ルール 1 にはカテゴリ AB が含まれる。 ルール 2 にはカテゴリ AB が含まれる。 具体的な結果は、リスト内のルールの順序、レピュテーションレベル、および関連付けられたアクションによって異なります。また、冗長性を解決する方法を決定する際に、ルール内の他のすべての条件も考慮する必要があります。
異なるルール内でマージされたカテゴリには異なるアクションが含まれる （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ A が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ B が含まれる。 （レピュテーションは同じ）	ルール 1 には [許可（Allow）] に設定されたカテゴリ AB が含まれる。 ルール 2 には [ブロック（Block）] に設定されたカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはなく、カテゴリとレピュテーションの両方が同じであるため、マージ後に警告を表示した場合は、警告インジケータが表示されます。
同じルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 には次が含まれます。 レピュテーション Any のカテゴリ A レピュテーション 1-3 のカテゴリ B	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。

シナリオ	アップグレード前	アップグレード後
異なるルール内でマージされたカテゴリには異なるレピュテーションレベルが含まれる	ルール 1 にはレピュテーション Any のカテゴリ A が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ B が含まれる。	ルール 1 にはレピュテーション Any のカテゴリ AB が含まれる。 ルール 2 にはレピュテーション 1-3 のカテゴリ AB が含まれる。 ルール 1 は、このカテゴリのすべてのトラフィックに一致します。 ルール 2 がトラフィックに一致することはありませんが、レピュテーションが同一でないため、警告インジケータは表示されません。

URL カテゴリの変更

このテーブルを使用して、URL カテゴリの変更方法を判定します。

表 *22*：古い *URL* カテゴリのインデックス

古いカテゴリ	変更内容		古いカテゴリ	変更内容
妊娠中絶	マージされたカテゴリ （59 ページ）		[軍（Military）]	変更されていないカテゴリ （63 ページ）
乱用薬物	マージされたカテゴリ （59 ページ）		自動車	カテゴリの名前変更 （62 ページ）
アダルトとポルノ	カテゴリの分割 （60 ページ）		Music	カテゴリの名前変更 （62 ページ）
アルコールとタバコ	カテゴリの分割 （60 ページ）		ニュースとメディア	カテゴリの名前変更 （62 ページ）
ボットネット	カテゴリの名前変更 （62 ページ）		Nudity	カテゴリの名前変更 （62 ページ）
ビジネスと経済	カテゴリの分割 （60 ページ）		オンライン グリーティング カード	カテゴリの名前変更 （62 ページ）
不正	カテゴリの名前変更 （62 ページ）		オープン HTTP プロキシ	カテゴリの名前変更 （62 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
コンピュータとインターネット情報	カテゴリの分割（60 ページ）		パーク ドメイン（Parked Domains）	変更されていないカテゴリ （63 ページ）
コンピュータとインターネット セキュリティ	カテゴリの分割（60 ページ）		サーフへの支払い	マージされたカテゴリ （59 ページ）
確認済みのスパム送信元	マージされたカテゴリ （59 ページ）		ピアツーピア	カテゴリの名前変更 （62 ページ）
コンテンツ配信ネットワーク	マージされたカテゴリ （59 ページ）		個人のサイトやブログ	カテゴリの分割（60 ページ）
カルトとオカルト	カテゴリの分割（60 ページ）		個人ストレージ	カテゴリの分割（60 ページ）
出会い系（Dating）	変更されていないカテゴリ （63 ページ）		哲学と政治的主張	カテゴリの名前変更 （62 ページ）
休止サイト	カテゴリの名前変更 （62 ページ）		フィッシングとその他の不正行為	カテゴリの名前変更 （62 ページ）
動的生成コンテンツ	マージされたカテゴリ （59 ページ）		プライベート IP アドレス	廃止されたカテゴリ （58 ページ）
Educational Institutions	マージされたカテゴリ （59 ページ）		プロキシ回避とアノニマイザー	カテゴリの名前変更 （62 ページ）
エンターテイメントとアート	カテゴリの分割（60 ページ）		要検討	カテゴリの名前変更 （62 ページ）
ファッションと美容	カテゴリの名前変更 （62 ページ）		不動産（Real Estate）	変更されていないカテゴリ （63 ページ）
金融サービス	カテゴリの名前変更 （62 ページ）		レクリエーションおよび趣味	マージされたカテゴリ （59 ページ）
食品と食事	カテゴリの名前変更 （62 ページ）		参照および調査	カテゴリの分割（60 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
ギャンブル（Gambling）	カテゴリの分割（60 ページ）		宗教（Religion）	変更されていないカテゴリ（63 ページ）
ゲーム（Games）	変更されていないカテゴリ（63 ページ）		Search Engines	マージされたカテゴリ（59 ページ）
政府/自治体	マージされたカテゴリ（59 ページ）		性教育（Sex Education）	マージされたカテゴリ（59 ページ）
総額	マージされたカテゴリ（59 ページ）		シェアウェアとフリーウェア	カテゴリの名前変更（62 ページ）
ハッキング（Hacking）	マージされたカテゴリ（59 ページ）		ショッピング（Shopping）	変更されていないカテゴリ（63 ページ）
中傷と人種差別	カテゴリの名前変更（62 ページ）		ソーシャル ネットワーク（Social Network）	カテゴリの分割（60 ページ）
健康と薬	カテゴリの名前変更（62 ページ）		社会	カテゴリの分割（60 ページ）
ホームとガーデン	カテゴリの分割（60 ページ）		スパム URL	マージされたカテゴリ（59 ページ）
狩猟と釣り	カテゴリの名前変更（62 ページ）		Sports	マージされたカテゴリ（59 ページ）
法律違反	カテゴリの分割（60 ページ）		スパイウェアとアドウェア	変更されていないカテゴリ（63 ページ）
画像とビデオ検索	カテゴリの名前変更（62 ページ）		ストリーミング メディア	カテゴリの名前変更（62 ページ）
個人向け株式アドバイスとツール	カテゴリの名前変更（62 ページ）		水着と肌着	カテゴリの名前変更（62 ページ）

古いカテゴリ	変更内容		古いカテゴリ	変更内容
インターネット通信	カテゴリの分割（60 ページ）		トレーニングおよびツール	マージされたカテゴリ （59 ページ）
インターネットポータル	マージされたカテゴリ （59 ページ）		旅行（Travel）	変更されていないカテゴリ （63 ページ）
求職（Job Search）	変更されていないカテゴリ （63 ページ）		未分類	廃止されたカテゴリ （58 ページ）
キーロガーとモニタリング	マージされたカテゴリ （59 ページ）		未確認のスパム送信元	マージされたカテゴリ （59 ページ）
こども用品	カテゴリの名前変更 （62 ページ）		暴力	マージされたカテゴリ （59 ページ）
リーガル	マージされたカテゴリ （59 ページ）		武器（Weapons）	変更されていないカテゴリ （63 ページ）
ローカル情報	カテゴリの名前変更 （62 ページ）		Web 広告	マージされたカテゴリ （59 ページ）
マルウェア サイト（Malware Sites）	変更されていないカテゴリ （63 ページ）		Web ベースの電子メール	カテゴリの分割（60 ページ）
マリファナ	マージされたカテゴリ （59 ページ）		Web ホスティング サイト	カテゴリの名前変更 （62 ページ）

新しいカテゴリ

これらのテーブルには、完全に新しい URL カテゴリがリストされています。ほとんどの URL カテゴリでは脅威が特定されます。URL ルールを作成または変更して、新しい脅威カテゴリを含めることを強くお勧めします。既存の一部の URL カテゴリでは脅威が特定されることに注意してください。これらの URL カテゴリも含めることをお勧めします。脅威カテゴリのリストについては、Talos Intellience Categories のサイトを参照してください。

表 *23 :* 新しいカテゴリ

新しいカテゴリ
ダイナミックおよびレジデンシャル

表 *24 :* 新しい脅威カテゴリ

新しい脅威カテゴリ
[Bogon]
クリプトジャッキング
DNS トンネリング
ドメイン生成アルゴリズム
ダイナミック DNS
電子バンキング詐欺
エクスプロイト
高リスクサイトおよびロケーション
侵害の兆候（IOC）
リンク共有
悪意のあるサイト
モバイルの脅威
新しく発見されたドメイン
第三者中継
P2P マルウェアノード
潜在的な DNS 再バインド
TOR exit ノード

廃止されたカテゴリ

アップグレードでは、廃止されたカテゴリを使用する URL ルールは変更されません。これらのルールによって展開が防止されるため、削除または変更する必要があります。

表 *25* : 廃止されたカテゴリ

廃止されたカテゴリ
未分類
プライベート IP アドレス

マージされたカテゴリ

影響を受けたカテゴリのいずれかが含まれている各ルールに影響を受けたすべてのルールが含まれるようになります。元のカテゴリが異なるレピュテーションに関連付けられていた場合、新しいルールはさらに広い、より包含的なレピュテーションに関連付けられます。以前と同様に URL をフィルタリングするには、いくつかの設定を変更する必要があります。「マージされた URL カテゴリを持つルールのガイドライン （51 ページ）」を参照してください。

URL ルールを作成または変更して、新しい脅威カテゴリ（スパム）を含めることを強くお勧めします。

表 *26* : マージされたカテゴリ

古いカテゴリ	新しくマージされたカテゴリ
Web 広告	アドバタイズメント
サーフへの支払い	
教育機関	教育
トレーニングおよびツール	
暴力	最高
総額	
政府/自治体	政府および法律
リーガル	
乱用薬物	違法ドラッグ
マリファナ	
動的生成コンテンツ	インフラストラクチャ
コンテンツ配信ネットワーク	
ハッキング	ハッキング
キーロガーとモニタリング	

古いカテゴリ	新しくマージされたカテゴリ
検索エンジン	検索エンジンおよびポータル
インターネットポータル	
性教育	性教育
妊娠中絶	
確認済みのスパム送信元	スパム（脅威カテゴリ）
スパム URL	
未確認のスパム送信元	
レクリエーションおよび趣味	スポーツおよびレクリエーション
スポーツ	

カテゴリの分割

アップグレードにより、URLルール内の古い単一のカテゴリが新しいカテゴリすべてに置き換えられ、新しいカテゴリは古いカテゴリにマッピングされます。アップグレード後、影響を受けるルールを変更して、新しい精度を活用することができます。

表 *27*：カテゴリの分割

古い単一カテゴリ	新しいカテゴリの分割
アダルトとポルノ	ポルノ（Pornography）
	アダルト（Adult）
アルコールとタバコ	アルコール（Alcohol）
	タバコ（Tobacco）
ビジネスと経済	ビジネスおよび産業（Business and Industry）
	携帯電話（Mobile Phones）
コンピュータとインターネット情報	ソフトウェア アップデート（Software Updates）
	コンピュータおよびインターネット（Computers and Internet）
	SaaS および B2B（SaaS and B2B）
	オンライン会議（Online Meetings）

古い単一カテゴリ	新しいカテゴリの分割
コンピュータとインターネット セキュリティ	コンピュータ セキュリティ（Computer Security）
	パーソナル VPN（Personal VPN）
カルトとオカルト	超常現象（Paranormal）
	占星術（Astrology）
エンターテイメントとアート	芸術（Arts）
	エンターテイメント（Entertainment）
ギャンブル（Gambling）	ギャンブル（Gambling）
	宝くじ（Lotteries）
ホームとガーデン	自然（Nature）
	DIY プロジェクト（DIY Projects）
法律違反	違法行為（Illegal Activities）
	児童虐待コンテンツ（Child Abuse Content）
	違法ダウンロード（Illegal Downloads）
インターネット通信	インターネット電話（Internet Telephony）
	チャットおよびインスタントメッセージ（Chat and Instant Messaging）
個人のサイトやブログ	個人サイト（Personal Sites）
	オンライン コミュニティ（Online Communities）
個人ストレージ	オンライン ストレージおよびバックアップ（Online Storage and Backup）
	ファイル転送サービス（File Transfer Services）
参照および調査	科学技術（Science and Technology）
	社会科学（Social Science）

古い単一カテゴリ	新しいカテゴリの分割
ソーシャル ネットワーク（Social Network）	ソーシャル ネットワーキング（Social Networking）
	プロフェッショナル ネットワーキング（Professional Networking）
社会	社会および文化（Society and Culture）
	非政府組織
Web ベースの電子メール	Web-based Email
	組織の電子メール

カテゴリの名前変更

特に対処の必要はありませんが、これらの変更に注意する必要があります。URL ルールを作成または変更して、新しい脅威カテゴリ（ボットネット、オープン HTTP プロキシ、フィッシング）を含めることを強くお勧めします。

表 *28 :* カテゴリの名前変更

古いカテゴリ名	新しいカテゴリ名
ボットネット	ボットネット（脅威カテゴリ）
不正	不正および盗用
休止サイト	非実用的
ファッションと美容	ファッション
金融サービス	金融
食品と食事	飲食
中傷と人種差別	ヘイトスピーチ
健康と薬	健康および栄養
狩猟と釣り	ハンティング
画像とビデオ検索	写真検索と画像
個人向け株式アドバイスとツール	オンライントレード
子供用品	子供向け
ローカル情報	参考資料

古いカテゴリ名	新しいカテゴリ名
自動車	乗り物
音楽	ストリーミングオーディオ
ニュースとメディア	ニュース
ヌード	性的でないヌード
オンライン グリーティング カード	デジタルポストカード
オープン HTTP プロキシ	オープン HTTP プロキシ（脅威カテゴリ）
ピアツーピア	ピアファイル転送
哲学と政治的主張	政治
フィッシングとその他の不正行為	フィッシング（脅威カテゴリ）
プロキシ回避とアノニマイザー	フィルタリング回避
要検討	ユーモア
シェアウェアとフリーウェア	フリーウェアおよびシェアウェア
ストリーミングメディア	ストリーミング ビデオ
水着と肌着	下着および水着
Web ホスティングサイト	Web ホスティング

変更されていないカテゴリ

特に対処の必要はありませんが、これらの変更に注意する必要があります。URL ルールを作成または変更して、新しい脅威カテゴリ（マルウェアサイト、スパイウェア、アドウェア）を含めることを強くお勧めします。

表 *29* : 変更されていないカテゴリ

変更されていないカテゴリ
出会い系（Dating）
ゲーム（Games）
求職（Job Search）
[軍（Military）]
パーク ドメイン（Parked Domains）

変更されていないカテゴリ
不動産（Real Estate）
宗教（Religion）
ショッピング（Shopping）
旅行（Travel）
武器（Weapons）

表 *30* : 変更されていない脅威カテゴリ

変更されていない脅威カテゴリ
マルウェアサイト（脅威カテゴリ）
スパイウェアとアドウェア（脅威カテゴリ）

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 6.5.0 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 （73 ページ）を参照してください。

表 *31* : 以前に公開されたバージョン *6.5.0* のガイドライン

✓	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
	アップグレードの失敗：コンテナ インスタンスのディスク容量不足（65 ページ）	Firepower 4100/9300	6.3.0 ～ 6.4.0.x	6.3.0.1 ～ 6.5.0
	TLS 暗号化アクセラレーションの有効化/無効にすることは不可 （66 ページ）	Firepower 2100 シリーズ Firepower 4100/9300	6.2.3 ～ 6.3.0.x	6.4.0 以降
	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（66 ページ）	任意	6.2.3.x	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
	FMC、NGIPSv で準備状況チェックに失敗する可能性（67 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 以降
	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（67 ページ）	FMC を使用した FTD	6.2.0 ～ 6.2.3.x	6.3.0 以降
	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 （68 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	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 （68 ページ）	FMC の展開	6.1.0 ～ 6.2.3.x	6.3.0 以降
	アップグレード後に VDB を更新して CIP 検出を有効化 （69 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	無効な侵入変数セットによって展開に失敗する可能性 （69 ページ）	任意	6.1.0 ～ 6.2.3.x	6.3.0 以降
	接続イベントと侵入イベントに関する Syslog の動作の変更 （70 ページ）	FMC	6.1.0 ～ 6.2.3.x	6.3.0 以降

アップグレードの失敗：コンテナインスタンスのディスク容量不足

展開：FTD を搭載した Firepower 4100/9300

アップグレード元：バージョン 6.3.0 ～ 6.4.0.x

直接アップグレード先：バージョン 6.3.0.1 ～ 6.5.0

多くの場合はメジャーアップグレード時に（場合によってはパッチ適用時に）、コンテナインスタンスを使用して設定された FTD デバイスが、ディスク容量不足のエラーにより事前チェック段階で失敗することがあります。

この問題が発生した場合には、空きディスク容量を増やしてみてください。それでも解決しない場合は、Cisco TAC にお問い合わせください。

TLS 暗号化アクセラレーションの有効化/無効にすることは不可

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 ～ 6.3.x

直接アップグレード先：バージョン 6.4.0 以降

SSL ハードウェア アクセラレーションは、*TLS* 暗号化アクセラレーションに名前が変更されました。

デバイスによっては、TLS 暗号化アクセラレーションがソフトウェアまたはハードウェアで実行される場合があります。アップグレードでは、この機能を手動で無効にした場合でも、すべての対象デバイスでアクセラレーションが自動的に有効になります。ほとんどの場合、この機能を設定することはできません。この機能は自動的に有効になり、無効にすることはできません。

バージョン *6.4.0* へのアップグレード： Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、モジュール/セキュリティ エンジンごとに、*1* つのコンテナ インスタンスに対して TLS 暗号アクセラレーションを有効にすることができます。他のコンテナインスタンスに対してアクセラレーションは無効になっていますが、ネイティブ インスタンスには有効になっています。

バージョン *6.5.0* 以降へのアップグレード：Firepower 4100/9300 シャーシのマルチインスタンス機能を使用している場合は、FXOS CLI を使用して、Firepower 4100/9300 シャーシ上の複数のコンテナ インスタンス（最大 16 個）に対して TLS 暗号アクセラレーションを有効にすることができます。新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることは「ありません」。代わりに、 **config hwCrypto enable** CLI コマンドを使用してください。

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。

FMC、NGIPSv で準備状況チェックに失敗する可能性

展開：FMC、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 6.3.0+

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 *32 :* バージョン *6.3.0* 以降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

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。

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 6.1.0 ～ 6.2.3.x、VDB 299+ 搭載

直接アップグレード先：バージョン 6.3.0+

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。

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 [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（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。

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警告は、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 （85 ページ）」を参照してください。

イベントデータと設定データのバックアップ

サポートされている場合は、アップグレードの前後にバックアップすることをお勧めします。

- アップグレード前：アップグレードが致命的なレベルで失敗した場合は、再イメージ化と復元が必要になることがあります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。最近のバックアップがある場合は、通常の操作にすばやく戻ることができます。
- アップグレード後：これにより、新しくアップグレードされた展開のスナップショットが作成されます。新しい FMC バックアップファイルがデバイスがアップグレードされたことを「認識」するように、管理対象デバイスをアップグレードした後に FMC をバックアップすることをお勧めします。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。アップグレードによって、ローカルに保存されたバックアップは消去されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。 FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。. 新しいアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

NTP 同期の確認

アップグレードする前に、時刻の提供に使用している NTP サーバと Firepower アプライアンスが同期していることを確認します。同期されていないと、アップグレードが失敗する可能性があります。FMC展開では、時刻のずれが10秒を超えている場合、[時刻同期化ステータス（Time Synchronization Status）] ヘルスモジュールからアラートが発行されますが、手動で確認する必要もあります。

時刻を確認するには、次の手順を実行します。

- FMC：[システム（System）] > [設定（Configuration）] > [時刻（Time）] を選択します。
- デバイス：**show time** CLI コマンドを使用します。

帯域幅の確認

Firepowerアプライアンスをアップグレードする（または準備状況チェックを実行する）には、アップグレードパッケージがアプライアンス上に存在する必要があります。Firepower アップグレードパッケージには、さまざまなサイズがあります。管理ネットワークに大量のデータ転送を実行するための帯域幅があることを確認します。

FMC の展開では、アップグレードパケージをアップグレード時に管理対象デバイスに転送する場合は、帯域幅が不十分だとアップグレード時間が長くなったり、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。アップグレードする前に、管理対象デバイスに Firepower アップグレードパッケージを手動でプッシュ（コピー）することをお勧めします。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のテクニカルノート）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、アップグレードパッケージとホットフィックスパッケージは「署名付き」のアーカイブになっています。 署名付きの（.tar）パッケージは解凍しないでください。

（注） 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`。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

6.2.3+ では、*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。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。

バージョン 6.2.3+ では、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。現在の設定でオプトアウトが選択されている場合でも、メジャー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、各メジャーアップグレードの後にオプトアウトしてください。

6.5.0+ では、*Cisco Support Diagnostics*（「シスコのプロアクティブサポート」とも呼ばれる）は、設定および運用上の健全性データをシスコに送信し、自動化された問題検出システムを通じてそのデータを処理して問題をプロアクティブに通知できるようにします。また、この機能により、Cisco TAC は TAC ケースの過程でデバイスから必要な情報を収集することもできます。アップグレード中に、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。

アップグレードにより侵入ルールをインポートして自動的に有効化できます。

現在の Firepower バージョンでサポートされていないキーワードが新しい侵入ルールで使用されている場合、侵入ルールデータベース（SRU）を更新しても、そのルールはインポートされません。

Firepower ソフトウェアをアップグレードし、これらのキーワードがサポートされると、新しい侵入ルールがインポートされ、IPS の設定に応じて自動的に有効化できるため、イベントの生成とトラフィックフローへの影響を開始できます。

サポートされているキーワードは、Firepower ソフトウェアに含まれている Snort のバージョンによって異なります。

- FMC：[ヘルプ（Help）] > [About（バージョン情報）] を選択します。
- FDM を使用した FTD：**show summary** CLI コマンドを使用します。
- ASDM を使用した ASA FirePOWER：[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [システム情報（System Information）] を選択します。

また、『Cisco Firepower Compatibility Guide』の「*Bundled Components*」の項で Snort バージョンを確認することもできます。

Snort リリースノートには、新しいキーワードの詳細が含まれています。https://www.snort.org/downloads でSnort ダウンロードページのリリースノートを参照できます。

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 6.5.0 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 *33 : Firepower* ソフトウェアをバージョン *6.5.0* 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。	6.2.3

プラットフォーム	最小バージョン
FMC を使用した Firepower 4100/9300 上の Firepower Threat Defense	FXOS 2.7.1.92+ を搭載した 6.2.3
FDM を使用した Firepower Threat Defense（すべてのプラットフォーム）	6.2.3
ASDM を使用した ASA FirePOWER	6.2.3

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。

（注） 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。

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、ベースバージョンから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。
- ハイアベイラビリティと拡張性：スタンドアロンデバイスでテストします。

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。

- 構成：構成とトラフィック負荷が最小限のアプライアンスでテストします。

  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。

時間はアップグレードのみを対象

値は、各プラットフォーム上で Firepower アップグレードスクリプトの実行にかかる時間のみを表しています。これらには、次の時間は含まれていません。

- 管理対象デバイスへのアップグレードパッケージの転送（アップグレード前かアップグレード中かにかかわらない）。
- 準備状況チェック。
- VDB と SRU の更新。
- 設定の展開。
- リブート（値が別途に報告される場合がある）。

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す。2020 年前半以降のリリースでは、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 6.5.0 の時間とディスク容量

表 *34 :* バージョン *6.5.0* 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	18.6 GB	24 MB	—	47 分
FMCv：VMware 6.0	18.7 GB	30 MB	—	35 分
Firepower 1000 シリーズ	1 GB	11.3 GB	1.1 GB	10 分
Firepower 2100 シリーズ	1.1 GB	12.3 GB	1 GB	12 分
Firepower 4100 シリーズ	20 MB	10.8 GB	990 MB	8 分
Firepower 9300	23 MB	10.9 GB	990 MB	8 分
ASA 5500-X シリーズ with FTD	10.4 GB	120 KB	1.1 GB	17 分
FTDv：VMware 6.0	10 GB	120 KB	1.1 GB	10 分
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 分
NGIPSv：VMware 6.0	6.6 GB	22 MB	870 MB	9 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 Chassis

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 Chassis：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 *35 : 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	—	ドロップされる
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 *36 : 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。	ドロップされる
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 以降）	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 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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、6.2.0.1、または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。

ハイアベイラビリティとクラスタリング ヒットレス アップグレードの要件

ヒットレスアップグレードの実行には、次の追加要件があります。

フローオフロード：フローオフロード機能でのバグ修正により、FXOSとFTDのいくつかの組み合わせはフローオフロードをサポートしていません。『Cisco Firepower Compatibility Guide』を参照してください。ハイアベイラビリティまたはクラスタ化された展開でヒットレスアップグレードを実行するには、常に互換性のある組み合わせを実行していることを確認する必要があります。

アップグレードパスに FXOS の2.2.2.91、2.3.1.130、またはそれ以降のアップグレード（FXOS 2.4.1. x、2.6.1 などを含む）が含まれている場合、次のパスを使用します。

1. FTD を 6.2.2.2 以降にアップグレードします。
2. FXOS を 2.2.2.91、2.3.1.130、またはそれ以降にアップグレードします。
3. FTD を最終バージョンにアップグレードします。

たとえば、FXOS 2.2.2.17/FTD 6.2.2.0 を実行していて、FXOS 2.6.1/FTD 6.4.0 にアップグレードする場合は、次を実行できます。

1. FTD を 6.2.2.5 にアップグレードします。
2. FXOS を 2.6.1 にアップグレードします。
3. FTD を 6.4.0 にアップグレードします。

バージョン 6.1.0 へのアップグレード：FTD ハイアベイラビリティペアのバージョン 6.1.0 へのヒットレスアップグレードを実行するには、プレインストールパッケージが必要です。詳細については、『Firepower System Release Notes Version 6.1.0 Preinstallation Package』を参照してください。

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 Configuration Guide』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 *37 : 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。	ドロップされる

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 以降）	ドロップされる
	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 1000/2100 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 *38 : 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。	ドロップされる

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 以降）	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 以降）	ドロップされる
	インラインセット、fail-to-wire モジュールなし	ドロップされる
	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 Configuration Guide』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 *39 : 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。	ドロップされる
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 以降）	ドロップされる
	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

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 module 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 *40 : 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**）	ドロップされる
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 module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 Configuration Guide』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 *41 : 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	ドロップされる
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 Configuration Guide』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 *42 : 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 module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

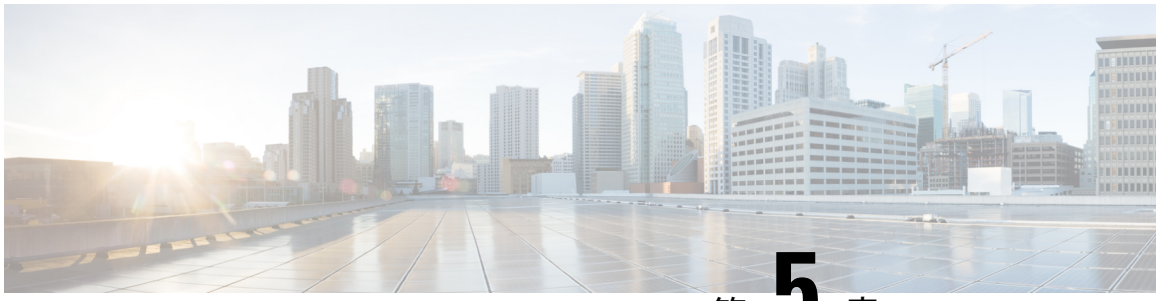
アップグレード パッケージは、シスコ サポートおよびダウンロード サイトで入手できます。

- 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
- 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

署名付きの（.tar）パッケージは解凍しないでください。

表 *43 :* のアップグレード パッケージ バージョン *6.5.0*

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 1000 シリーズ	Cisco_FTD_SSP_FP1K_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 仮想	Cisco_FTD_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



第 5 章

新規インストール バージョン 6.5.0

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） 管理の再イメージ化または切り替えを行う前に、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（CSSM）から手動で登録解除することが必要になる場合があります。これらが生じると再登録できない場合があります。

表 *44*：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。 **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。
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 Configuration Guide』を参照してください。

シナリオ	ソリューション	ライセンシング
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。
障害が発生した FMC または FTD デバイスをバックアップから復元します。	RMA のシナリオでは、工場出荷時の初期状態の設定での交換になります。ただし、交換がすでに設定されている場合は、復元する前に再イメージ化することをお勧めします。	再イメージ化を行う前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。これを行った場合は、復元後に再度登録を解除してから再登録する必要があります。 代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC 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、「インストール手順 （94 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

サポートされている場合は、再イメージ化の前にバックアップすることを強くお勧めします。

（注） 再イメージ化してアップグレードする必要がない場合、バージョンの制約により、バックアップを使用して古い設定をインポートすることはできません。設定は手動で再作成する必要があります。

安全なリモートロケーションにバックアップし、正常に転送が行われることを確認する必要があります。再イメージ化によって、システムパスワードを含むほとんどの設定が工場出荷時の初期状態に戻ります。アプライアンスに残っているすべてのバックアップが削除されます。特に、バックアップファイルは暗号化されていないため、不正アクセスを許可しないでください。バックアップ ファイルが変更されていると、復元プロセスは失敗します。

バックアップの最初のステップとして、アプライアンスモデルとバージョンを、パッチレベルを含めて書き留めておいてください。FMC の場合は、VDB のバージョンを書き留めておきます。 Firepower 4100/9300 シャーシの場合は、FXOS のバージョンを書き留めておきます。新し

いアプライアンスや再イメージ化したアプライアンスにバックアップを復元する必要がある場合は、新しいアプライアンスを最初に更新する必要がある場合があるため、これは重要です。

（注） バックアップと復元は、複雑なプロセスになる可能性があります。手順をスキップしたり、セキュリティ上の問題を無視しないでください。誤りを避けるには、注意深い計画と準備が役立ちます。バックアップと復元の要件、ガイドライン、制限事項、およびベストプラクティスの詳細については、ご使用の Firepower 製品のコンフィギュレーション ガイドを参照してください。

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

再イメージ化されたアプライアンスを手動で設定する予定がある場合は、再イメージ化する前に、リモート管理からデバイスを削除します。

- FMC を再イメージ化する場合は、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、またはリモートからローカルでの管理に切り替える場合は、その単一のデバイスを削除します。

FMC または FTD デバイスの再イメージ化後にバックアップから復元する場合は、デバイスをリモート管理から削除する必要はありません。

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。状況により、Cisco Smart Software Manager からの登録解除が必要になります。また場合によっては、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

アプライアンス 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。

（注） 以前のメジャーバージョンに再イメージ化すると、ネットワーク設定が自動的に削除されます。このようなまれなケースでは、物理的アクセスが必要です。

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。

シスコとのデータの共有

一部の機能にシスコとのデータ共有が含まれます。

バージョン 6.2.3+ では、*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。

バージョン 6.2.3+ では、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（EULA に承諾すると、Web 分析トラッキングに同意したことになります）。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。また、この機能を再度有効にする可能性があるメジャーアップグレード後は、もう一度オプトアウトする必要があります。

以前のメジャー バージョンへの Firepower 1000/2100 シリーズ デバイスの再イメージ化

Firepower 1000/2100 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お勧めします。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 トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）に記載されている再イメージ化の手順を参照してください。

バージョン 6.3.0 以降へのバージョン 5.x ハードウェアの再イメージ化

バージョン 6.3 以降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（FMC 2000 および 4000）の再イメージ化に関する問題が発生します。現在バージョン 5.x を実行していて、バージョン 6.5.0 を新規にインストールする必要がある場合は、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。『Cisco Firepower Release Notes, Version 6.3.0』の「Renamed Upgrade and Installation Packages」の情報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。後で再イメージ化または管理の切り替えを行うことにした場合は、孤立した権限付与を発生させないように登録を解除する必要があります。これらが生じると再登録できない場合があります。

（注） FMC または FTD デバイスをバックアップから復元する必要がある場合は、再イメージ化の前に登録を解除しないでください。また、FMC からデバイスを削除しないでください。代わりに、バックアップを実行した後に行われたライセンス変更を元に戻します。復元が完了したら、ライセンスを再設定します。ライセンスの競合や孤立した権限付与に気付いた場合は、Cisco TAC にお問い合わせください。

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、クラウドとクラウドサービスからアプライアンスが登録解除され、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 から手動で登録解除します。

- FTD デバイスを管理する Firepower Management Center を再イメージ化する。
- モデルの移行中にソース Firepower Management Center をシャットダウンする。
- 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。

FMC からデバイスを削除すると、CSSM から自動的に登録解除されます。これにより、次のことが可能になります。

- 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。

の登録解除 Firepower Management Center

バックアップから復元する予定がない限り、再イメージ化する前に CSSM から Firepower Management Center の登録を解除してください。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 **[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（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。

を使用した FTD デバイスの登録解除 FDM

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（Smart License）] のサマリーで [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。

インストール手順

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 *45 : 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 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 1000、2500、4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMC 750、1500、3500 FMC 2000、4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide：Restoring a Firepower Management Center to Factory Defaults
FMCv および FMCv 300	『Cisco Firepower Management Center Virtual 入門ガイド』

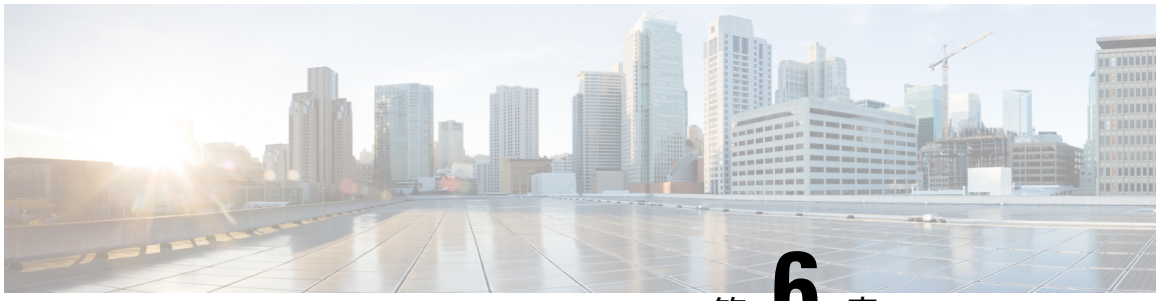
表 *46 : Firepower Threat Defense* のインストール手順

FTD プラットフォーム	ガイド
Firepower 1000/2100 シリーズ	Cisco ASA and Firepower Threat Defense Reimage Guide Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）
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 スタートアップガイド 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	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM スタートアップガイド
FTDv：AWS	Cisco Firepower Threat Defense Virtual for the AWS Cloud スタートアップガイド

FTD プラットフォーム	ガイド
FTDv：Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

表 *47 : 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
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：Managing the ASA FirePOWER Module



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。

新規および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 6.5.0 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 （99 ページ）」を参照してください。

Firepower コンフィギュレーション ガイドとオンライン ヘルプ

- 『Firepower Management Center Configuration Guide, Version 6.5』およびオンラインヘルプ
- 『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.5.0』およびオンライン ヘルプ
- 『Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.5』およびオンラインヘルプ
- Cisco Firepower Threat Defense Command Reference

FXOS コンフィギュレーション ガイドとリリース ノート

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.7(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.7(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.7(1)

アップグレード ガイド

- Cisco Firepower Management Center Upgrade Guide

- Cisco Firepower 4100/9300 Upgrade Guide
- Cisco ASA Upgrade Guide

移行ガイド

- Firepower Management Center モデル移行ガイド （新規）

スタートアップ ガイド

- Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
- Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
- Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
- 『Cisco Firepower Management Center Virtual 入門ガイド』
- Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide
- Cisco ISA 3000 スタートアップガイド （新規）
- Cisco Firepower 1010 スタートアップガイド
- Cisco Firepower 1100 シリーズ スタートアップガイド
- Cisco Firepower 2100 シリーズ スタートアップ ガイド （新規）
- Cisco Firepower 4100 スタートアップガイド
- Cisco Firepower 9300 Getting Started Guide

API および統合ガイド

- Firepower Management Center REST API バージョン 6.5.0 クイックスタートガイド
- Cisco Firepower Threat Defense REST API ガイド （Cisco Firepower Threat Defense REST API Guide）
- Firepower System Event Streamer Integration Guide, Version 6.5.0
- Firepower System Host Input API Guide v6.5
- Cisco Firepower User Agent Configuration Guide, version 2.5
- Firepower および Cisco Threat Response の統合ガイド

互換性ガイド

- Cisco Firepower Compatibility Guide
- Cisco ASA の互換性

- Cisco Firepower 4100/9300 FXOS の互換性

ライセンスおよびオープン ソース

- Cisco Firepower システム機能ライセンス
- 『Frequently Asked Questions (FAQ) about Firepower Licensing』
- Firepower Version 6.5.0 で使用されているオープン ソース

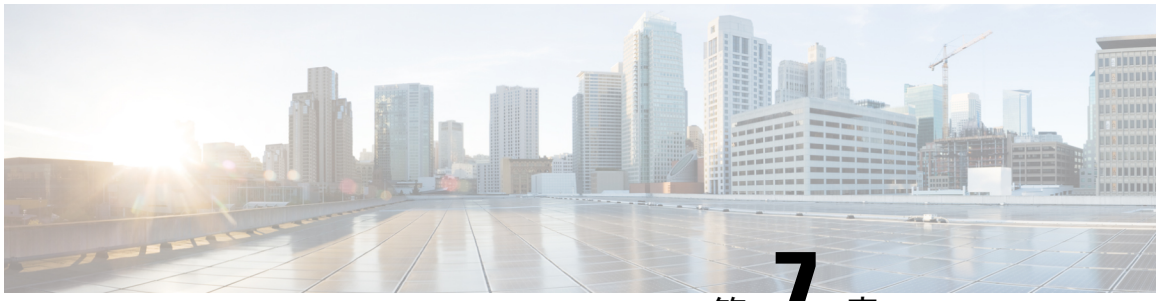
トラブルシューティングおよび設定の例

- Cisco Firepower Threat Defense Syslog メッセージ
- Firepower 4100/9300 のマルチインスタンス機能の使用 （**新規**）
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability
- Cisco FXOS トラブルシューティングガイド（Firepower Threat Defense を実行している Firepower 1000/2100 シリーズ向け）

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。

- Cisco Firepower ドキュメント一覧
- Cisco ASA シリーズ ドキュメント一覧
- Cisco FXOS ドキュメント一覧



第 7 章

解決済みの問題

便宜上、これらのリリースノートには、このバージョンの解決済みのバグが記載されています。

このリストは1回自動生成され、その後は更新されません。特定の解決済みの問題がシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco バグ検索ツール を「信頼できる情報源」と考えてください。

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6.5.0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
- ASA with FirePOWER サービス
- 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。ほとんどの場合、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。最新のビルドを使用することを強くお勧めします。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。新しいビルドで問題が解決する場合は、代わりに、アップグレードまたはホットフィックスが機能するかどうかを確認します。それ以外の場合は、Cisco TAC にご連絡ください。公的に利用可能な Firepower のホットフィックスへのクイックリンクについては、Cisco Firepower ホットフィックス リリース ノートを参照してください。

この表を使用して、プラットフォームで新しい バージョン 6.5.0 ビルドが使用可能かどうかを確認します。

表 *48* : バージョン *6.5.0* の新しいビルド

新しいビルド	リリース日	パッケージ	プラットフォーム	解決済み
123	2020 年 2 月 3 日	アップグレード 再イメージ化	FMC/FMCv	CSCvr95287：Cisco Firepower Management Center LDAP 認証バイパスの脆弱性 以前のビルドを実行している場合は、最新バージョンの 6.5.0 パッチを適用します。
120	2019 年 10 月 8 日	—	—	CSCvr47499：800_post/1028_latency_settings_upgrade.pl で Firepower FMC のアップグレードに失敗する マルチドメイン展開で FMC をアップグレードするためのこのビルドは、使用できなくなりました。

バージョン 6.5.0 で解決済みの問題

表 *49* : バージョン *6.5.0* で解決済みの問題

不具合 ID	タイトル
CSCvc88690	5.4.x AC 管理者およびルートルールグループは現在も 6.x ユーザロールであり、完全な権限を持っている
CSCvd80045	[正常性ポリシー（Health Policy）] ページからのドメインの切り替え中にエラーが発生する
CSCvd87211	設定されたキャプチャを削除しようとすると ASA がトレースバックする
CSCvh16358	CLI でコマンドをキャンセルできない
CSCvh78264	Clamupdates には、FMC に明示的な HTTP プロキシが設定されている場合でも、稼働中の DNS が必要になる

不具合 ID	タイトル
CSCvi23774	Firepower の推奨更新では、無効な状態に移行したサードパーティの脆弱性が考慮されない
CSCvi28409	FTP プロトコルを使用するファイルのいくつかで、キャプチャされたファイルのダウンロードが FMC 上で動作していない
CSCvi34123	拡張機能：リストの先頭に _ が含まれている DNS リストを追加できない
CSCvi93955	セキュリティヘッダーが検出されませんでした - CWE-693（Security Header Not Detected - CWE-693）：保護メカニズムの障害
CSCvi95403	レベル 5 の通知文字列がない
CSCvj53804	ICMP イベントドメイン ID が破損しているため、6.2.3 への SW アップグレードが失敗した
CSCvj73432	NTP が Eth1 インターフェイスから Eth0 IP アドレスを送信する
CSCvj74441	ASDM 上の CLI を介した SRU のインストールでは、/etc/sf/sru_versions.conf のバージョンの詳細が更新されない
CSCvk55766	デバイスをプラットフォーム設定ポリシーに割り当てようとすると、一連のデバイスがランダムにポリシーから消える
CSCvk63804	スケジューリングによる推奨ルールの更新を行っているときに機密データ検出が有効になる
CSCvk66669	FPR2100：SSL プロトコルを設定しても、FDM GUI 証明書の設定が変更されない
CSCvm31905	OpenSSH Bailout によるユーザの列挙の遅延の脆弱性
CSCvm77115	無効な TSC 値による Lina のトレースバック
CSCvm80434	多くのユーザが使用している FMC GUI でのパフォーマンスの低下
CSCvm84357	ファイルイベントの送信元と宛先がアクティブな転送モードに対して正しくない
CSCvm89006	FTD：FTD converged_cli の設定コマンド「configure user add」の syslog
CSCvn31390	コンピューティング プロセッサ PortSmash サイドチャネル情報開示の脆弱性
CSCvn31886	TLS 1.3 を使用した SSL インスペクションにより、セッションがキャッシュされないアクションを実行するためにトラフィックが復号されない
CSCvn57267	セキュリティ インテリジェンスに重複するオブジェクトが含まれている

不具合 ID	タイトル
CSCvn73998	等号が含まれている OSPFv2 MD5 パスワードが 2 回目の展開時に削除される
CSCvn78076	Firepower：[システム（System）] > [モニタリング（Monitoring）] > [統計情報（Statistics）] で、[メモリ使用量（Memory Usage）] に関連して誤解を招く統計情報が表示される
CSCvn80464	アラート設定では、使用中のポリシーを正しく追跡しない
CSCvo06680	[ヘルプ (Help)] ドロップダウンで、[Sourcefire のサポート（Sourcefire support）] ページが現在も表示されている
CSCvo11077	Cisco ASA ソフトウェアと FTD ソフトウェアの IKEv1 サービス拒否攻撃に対する脆弱性
CSCvo30347	UI のバグ：拡張アクセスリストオブジェクトのドラッグアンドドロップが機能しない
CSCvo37273	スタティックルートに設定されているオブジェクトネットワークを検証するための検証チェックが FMC UI に追加される
CSCvo39231	CSM 側のエントリが古いため、FMC からデバイスリストが [ポリシーの展開（Deploy Policy）] タブに挿入されない
CSCvo39356	スレッド名でのトレースバック：IP アドレスの割り当て
CSCvo40478	FMC ダッシュボードに FMC の最新の製品更新として誤った値が表示される
CSCvo43260	強制展開では、登録されたすべてのデバイスを受け入れるのではなく、現在のデバイスのみをロードするようにする必要がある
CSCvo43311	「トポロジに未知のエンドポイントが存在します（Unknown endpoint present in the topology）」というエラーで VPN サイト間ポリシーを保存できない
CSCvo48400	FTD をアップグレードすると、成功していない場合でも成功したと表示される
CSCvo49295	RabbitMQ は常にエラー「case_clause,undefined」で開始できない
CSCvo57287	FMC： APIUser クレデンシャルを使用して RESTAPI UI にログインできない
CSCvo59424	FMC UI では、FTD クラスタの診断インターフェイスに IP アドレスを割り当てることができない
CSCvo59683	EOAttributes テーブル内の古いオブジェクトの数が多いと、高 CPU 使用率/バックアップ障害が発生する

不具合 ID	タイトル
CSCvo61418	イベントテーブルのサイズと数が大きいと、FMC イベントの復元に失敗する
CSCvo66732	パッチの更新中に自動的に SRU をダウンロードすると、更新に失敗する場合がある
CSCvo70169	[FMC 6.3] ルールの競合により機能していないと表示される
CSCvo74786	プロセスマネージャが異常終了時に Mojo プロセスを追跡しない
CSCvo74802	プロセスマネージャが管理対象外のプロセスを想定どおりに処理しない
CSCvo74833	追跡されていないファイルが原因で、Firepower デバイスの管理対象外ディスク容量が大きくなる
CSCvo76866	2100 でのトレースバック：ウォッチドッグ
CSCvo77024	https://nvd.nist.gov/vuln/detail/CVE-2015-9251 により、FMC Jquery をアップグレードする必要がある
CSCvo80725	「エラー：ip_multicast_ctl によるチャネルの取得に失敗（ERROR: ip_multicast_ctl failed to get channel）」により vFTD 6.4 が OSPF 隣接関係を確立できない
CSCvo92100	FMC では、プラットフォーム設定の SNMP のコミュニティ文字列にスペースを使用できる
CSCvo92913	Cisco Firepower Management Center RSS のクロスサイト スクリプティングの脆弱性
CSCvp01677	203.0.113.0/25 ネットワークの管理インターフェイス上にルートを設定すると、デバイスが再起動します。
CSCvp04610	無効な GID とデータベースの同期の問題が原因で syncd プロセスが終了する
CSCvp06526	短い CPU アフィニティに一致するように sfhassd スレッド CPU アフィニティを管理する
CSCvp12526	SSL セッションを再開しようとすると、ビジー状態のデバイスで失敗する可能性がある
CSCvp26173	FMC：ホスト入力クライアント、TCP 8307 ポートの TLS 1.0 を永続的に無効にする
CSCvp26548	オブジェクトの検証に失敗したため、FDM のアップグレードが失敗する

不具合 ID	タイトル
CSCvp29803	Apache HTTP サーバモジュールでスクリプトが任意のコードを実行する脆弱性
CSCvp31204	SNMP コミュニティ文字列に特殊文字を使用できない
CSCvp33439	REST API を使用して SI DNS ポリシーを設定した後に FTD での展開が失敗する
CSCvp39970	/var/opt/CSCOpx/MDC/tomcat/log/stdout.logs によってログメッセージが過剰に書き込まれ、ディスクがいっぱいになる場合がある
CSCvp43987	正常性ポリシーの実行時間間隔は、正常性モニタプロセスのアラームしきい値よりも小さくする必要がある
CSCvp50929	バックアップの復元後に、誤ったライセンスキーが FMC に表示される
CSCvp55941	ファイル復帰ブロックがランダムにスローされて、SMB 共有からのファイルへのアクセスに関する問題が発生する
CSCvp58287	接続イベントの「ワークフローの切り替え」における FMC GUI のバグ
CSCvp66802	6.4.0.1-14 のアップグレード中に QP-HA が失敗する
CSCvp66941	ユーザに既存のセッションがあり、その中にスペースを含むパスワードがある場合は FMC ログインが失敗する
CSCvp70833	ASA/FTD：同じサービスの NAT ルールがエラー「エラー：NAT がポートを予約できません（ERROR: NAT unable to reserve ports）」を 2 回表示する
CSCvp81615	ドメインを削除すると、ルーティング設定が削除される
CSCvp82265	FMC HA の形成後に記録された不正な uuidprefix がオブジェクトの編集中にエラーを発生させる
CSCvp87623	CAC（HTTPS クライアント証明書）の使用時に更新をアップロードすると「更新要求エンティティが大きすぎます（update request entity too large）」というエラーが発生する
CSCvp90060	最新の Firepower SRU の更新（24.05.2019）後に RDP 接続が失敗する
CSCvp99327	スマートサテライトにスマートライセンスを登録しようとした後に FMC UI が応答しなくなる
CSCvp99930	プライマリがアクティブの間に sftunnel の例外で展開が失敗する
CSCvq05335	NFS リモートストレージが応答しないため、ブートプロセスで FMC がスタックする
CSCvq07624	REST API に設定されている S2S VPN に一致しない ID がある

不具合 ID	タイトル
CSCvq09093	VPN 事前展開の検証がデバイスごとに約 20 秒かかる
CSCvq11637	6.4 FDM デバイスが TCP syslog を送信していない
CSCvq12173	パラメータとしてエコー応答 ICMP(1):0 で設定されたルールが起動しない
CSCvq14954	管理専用のスレーブユニットはクラスタに参加できない
CSCvq18237	ドキュメンテーションのバグ：FMC HA 設定ガイド：ソフトウェア要件が誤っている
CSCvq21935	6.3.0.3 を実行している FTD が DATAPATH でトレースバックする
CSCvq24258	大規模なアプライアンスで Mojo サーバのワーカー数が増加する
CSCvq25791	ファイルポリシーの詳細設定でクリーンリストを有効にしても正しく記述されない。
CSCvq27739	SSH サーバが上書きされたファイルのコピーを保存するように設定されている場合は、リモート SSH ストレージへのバックアップが失敗する
CSCvq29969	再生成されていない場合でも、Firepower 推奨ルール数が変更される
CSCvq30298	deploy.stats ファイルのローテーションが行われず、サイズが大幅に大きくなる可能性がある
CSCvq34160	fp1000 シリーズプラットフォームへの ASDM 接続の確立時のトレースバックとリロード
CSCvq36042	ハートビートが失われてリロードが発生する
CSCvq43453	サブドメインの変数セットで使用されている場合、ポートオブジェクトにオーバーライドを追加できない
CSCvq45000	NAT が設定されている場合に FP 8000 センサーへのポリシーの展開が失敗する
CSCvq46443	Cisco Firepower Management Center に蓄積されたクロスサイトクリプティングの脆弱性
CSCvq48073	パケットがバイパスされる可能性があるため、PPM はデフォルトで有効にならないようにする必要がある
CSCvq53902	Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性
CSCvq53915	Cisco Firepower Management Center のクロスサイト スクリプティングの複数の脆弱性

不具合 ID	タイトル
CSCvq55941	Cisco Firepower Management Center ソフトウェアに蓄積されたクロスサイトスクリプティングの脆弱性
CSCvq56257	キャッシュされたマルウェアの処置が想定どおりに期限切れにならないことがある
CSCvq59702	ハンドシェイクメッセージの喪失後にデバイスからの接続イベントが停止する
CSCvq61601	FTD での OpenSSL の脆弱性 CVE-2019-1559
CSCvq67271	子アクセスポリシーの ID によって特定ルールを取得すると、「404：見つかりませんでした（404: Not Found）」ステータスが返される。
CSCvq70485	「securityzones」REST API が低速になる
CSCvq71217	CSCvn30118 の後、mysql-server.err によりローテーションが失敗して、ディスク使用率が高くなる
CSCvq71351	FMC：インラインセットの編集時にページがスタックする
CSCvq75634	管理インターフェイスの設定により、即時トレースバックとリロードが発生する
CSCvq76533	MC4000 の F_RNA_EVENT_LIMIT は 2000 万である必要がある
CSCvq76785	認証に未処理のエラーがあると、ユーザ名とパスワードがログに出力される
CSCvq79042	サーバからの DNS 応答が大きく、切り捨てられているため、FQDN ACL エントリが不完全になる
CSCvq81516	FMC で 12 時～午後 1 時（UTC）の間の VPN イベントが表示されない
CSCvq83019	ACPolicy に多数のアプリケーション フィルタ オブジェクトが使用されている場合に、ポリシー展開タスクの挿入の処理に長時間かかる
CSCvq83168	FMC ではサーバアドレスの後にインターフェイスを使用できないため、管理 VRF を使用した DNS ルックアップを実行できない
CSCvq87068	削除した URL オブジェクトが ngfw.rules から削除されない
CSCvq87585	50,000 回繰り返して ping を実行した後で CLISH が応答しなくなり、CPU コアの使用率が高くなる
CSCvq87703	アクティブデバイスが正しいピア状態を報告しない
CSCvq88644	tcp-proxy でのトレースバック

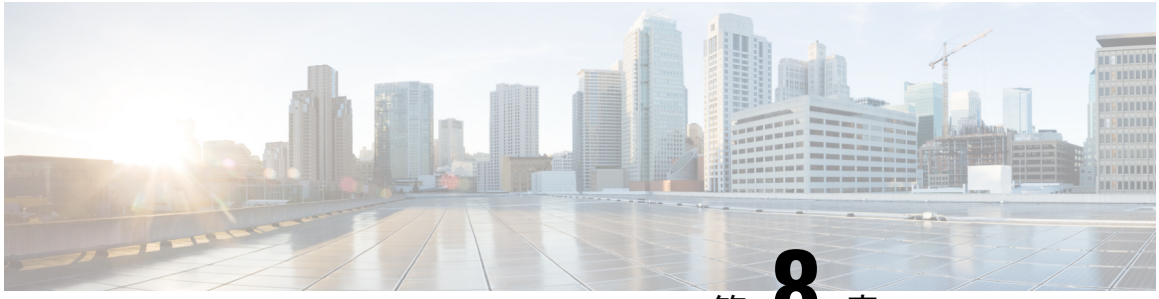
不具合 ID	タイトル
CSCvq89794	FDM：ユーザダウンロードが LDAPS で機能しない
CSCvq94729	デルタ CLI の LINA ONLY セクションでのエラー時に展開のロールバックによってトラフィックの瞬間的なドロップが発生する
CSCvq97346	UI で NAT ルールを移動し、展開すると、FDM バックエンドから NAT ルールが削除される
CSCvr00892	外部データベースアクセスで where 句が機能しない
CSCvr04954	スタックユニット：NDPolicy obj err をロードできない別のドメインでのアップグレード後に展開が失敗する
CSCvr07421	セキュリティゾーン内にインターフェイスが 400 以上あると、deployDB の不適切な形成により、ポリシーの展開が失敗する
CSCvr07460	暗号 PKI の動作に関連して ASA がトレースバックおよびリロードする
CSCvr11395	スケジュール済みの展開時にデバイスグループから展開された一部のデバイスのみ
CSCvr13278	リロード後に PPPoE セッションが起動しない。
CSCvr17735	SI 更新時の SFDataCorrelator で CPU の使用率が高くなる
CSCvr19922	クラスタ：特定の状況下で BGP ルートが同期しなくなる場合がある
CSCvr20893	ポリシーの展開後に ids_event_proce プロセスで HA ペアの FTD がクラッシュする
CSCvr23986	メモリが不足しており、MIB ウォークが頻繁に実行される状態では、Cisco ASA & FTD デバイスがリロードする場合がある
CSCvr29978	ルールを変更してすぐに保存すると、設定が削除されることがある
CSCvr30694	FMC：FMC が HA 同期の失敗を検出する
CSCvr35956	ServerKeyExchange と ClientKeyExchange の組み合わせが失敗する場合のダブルフリーのブロックが原因で lina がトレースバックする
CSCvr36369	展開に進む前に、CD はファイルコピー応答で障害が発生している NodeID を考慮する必要がある
CSCvr39556	libclamav.so のセグメンテーション違反（SFDataCorrelator のコンテキスト内）
CSCvr43341	FDM 6.5.0：トランクインターフェイスを使用してアップグレードした場合、FPR1000 GUI が応答しなくなる

不具合 ID	タイトル
CSCvr47499	800_post/1028_latency_settings_upgrade.pl で Firepower FMC のアップグレードに失敗する
CSCvr51955	Estreamer は、長時間ぶわたって ACK を受信しない場合に接続を終了する必要がある
CSCvr52109	複数のデバイスへの展開後、FTD が正しいアクセス制御ルールに一致しないことがある
CSCvr53058	tcp-intercept と AC ポリシーのモニタを設定すると、AC ポリシーのルックアップが SYN+ACK パケットに対して実行される
CSCvr54250	レルムが設定されていない場合でも user_ip_map ファイルの数が多い
CSCvr59927	SRU インストールが進行中の場合、展開が失敗する
CSCvr61241	ファイルアップロード機能を実装する情報システムでは、ファイルサイズを検証する必要がある
CSCvr61492	REST API コールに関連し、デバイスのロードが低速になる
CSCvr72665	FMC の 6.3/6.4 へのアップグレードで、既存の廃止済み flexconfig を削除しないようにする必要がある
CSCvr73115	ポリシーインポート後の初期 FTD の展開によって未使用オブジェクトが発生し、ポリシーサイズが膨張する
CSCvr78166	「実行コンフィギュレーションの取得に失敗しました（failed to retrieve running configuration）」という理由で、展開が FTD 上で失敗した
CSCvr79008	不正なユーザ名の正規化を実行しているすべてのディレクトリサーバを FMC が非効率的に照会するため、セッション処理が遅延する
CSCvr80621	SecurID RSA を使用した FMC 外部認証は、バナーが有効になっている場合に失敗する
CSCvr82133	FMC を 6.5 にアップグレードした後、ルートを追加できず、また、[デバイス管理（Device Management）] ページからインターフェイスを選択できない
CSCvr84572	FMC 6.5：FMC でのユーザのログインの失敗が監査ログのエントリに記録されない
CSCvr86213	CD は、クラスタノードリリースの Lina の状態の Cluster-Msg-Delivery-Confirmation を無視する必要がある。
CSCvr88123	マルチ展開により、侵入イベントが突然ドロップする

不具合 ID	タイトル
CSCvr89663	トレースバック：スレッド名 pix_flash_config_thread で WM1010 がリブートループに陥る
CSCvr90768	FTD：低速リンクを通じた展開は失敗する場合がある
CSCvr90965	Azure で FTDv 展開を行うと、「no dns domain-lookup any」により回復不能なトレース状態が発生する。
CSCvr92617	SecurityIntelligenceEoConvertor の NPE によって、Lucene のインデックスの作成が失敗する
CSCvr95287	Cisco Firepower Management Center LDAP 認証バイパスの脆弱性
CSCvr97009	URL カテゴリを使用する場合、QoS（レート制限）が適用されない
CSCvs00023	CLISH CLI からの「shutdown」コマンドでポートマネージャがクラッシュする
CSCvs04067	Catalina へのアップグレード後、Mac 上の Chrome では FMC デバイスにアクセスできない。
CSCvs07668	SIP インスペクションが有効になっていると、スレッド DATAPATH-1-15076 で FTD がトレースバックし、リロードする。
CSCvs09533	3 つ以上のインラインセットを介してトラフィックを処理すると、FP2100 がトレースバックし、リロードする
CSCvs10443	6.5 CloudEvent コードが、6.4 コードが理解しない方法で config ファイルを書き込む
CSCvs10526	FTD での SSE 試行のスロットル
CSCvs12288	SSL ポリシーが有効になっている状態で debug_policy_all が設定されていると Snort が予期せず終了する
CSCvs19968	スタックし、HA FTD ポリシー展開エラーが発生しないようにコンソールを修正する
CSCvs22503	「ポリシーイベントの逆シリアル化に失敗しました（Failed to deserialize policy event）」の後に eStreamer が繰り返し終了する
CSCvs22608	Snort ルールのプロファイリングから無効化した SID に関して引き続き検出される
CSCvs25607	制約事項に netmap_num を追加するとパフォーマンスが低下する
CSCvs26402	NAT ポリシー設定範囲の制限が非サービス CMDS にも適用される

不具合 ID	タイトル
CSCvs34854	FMC がアクセスリスト CLI の差分の後ろに参照インターフェイス CLI の差分を生成する
CSCvs37013	octeon_init がスタックし、HA FTD ポリシー展開エラーを発生させないようにする
CSCvs40531	AnyConnect 4.8 が FPR1000 シリーズで動作していない
CSCvs47201	デバイスレコードに対して GET ALL を実行すると、「isPartOfContainer」が返される。HA とクラスタの一部であるデバイスでは偽
CSCvs55471	特定の AC ルールが無効になっている状態の ACP にポリシーの侵入イベントが適用される
CSCvs55990	ローカル/FDM で管理されている FTD 上に設定された SI DNS を使用した展開が失敗する
CSCvs61392	Firepower デバイスで、ポリシーが正常に展開された後、ハードウェアルールが更新されない
CSCvs70703	[DOC]『Cisco Firepower Compatibility Guide』に誤った RAID ファームウェアコマンドが示されている
CSCvs74452	マルウェアシードファイルのロード中に SFDatacorrelator と Snort がコアを繰り返し生成する
CSCvs77334	「別のユニットのインスペクションエンジンが Snort とディスクの障害により失敗しました（Inspection engine in other unit has failed due to snort and disk failure）」というエラーにより FTD がフェールオーバーする
CSCvs78252	TCP シーケンス番号のランダム化が有効になっている場合に、FTD 6.5 Ubuntu と Mac が SCP 転送を完了できない
CSCvs80330	ADI プロセスを重複して実行すると、正常性ステータスファイルが消去される可能性がある
CSCvs81504	WR6 と WR8 のコミット ID が CCM レイヤで更新される（Sprint 77）
CSCvs86257	FMC のアップグレードが 800_post/1025_vrf_policy_upgrade.pl で失敗する
CSCvt02409	FPR9300 3 ノードクラスタのネストされた VLAN トラフィックで 9.12.2.151 snp_cluster_ingress がトレースバックする
CSCvt27920	FTD でポリシーの展開に失敗する
CSCvt45989	ASAv HA Azure：既存の仮想ネットワークを使用すると、Azure での ASAv HA ペアの展開が常に失敗する

不具合 ID	タイトル
CSCvt48941	「APP SYNC のタイムアウトにより HA の状態の進行に失敗しました（HA state progression failed due to APP SYNC timeout）」により、FTD スタンバイユニットが HAスイッチオーバー に参加しない
CSCvt51987	ASA での 80 サイズのブロックの枯渇によりトラフィックが停止する



第 8 章

既知の問題

便宜上、これらのリリースノートには、このバージョンの既知のバグが記載されています。

このリストは1回自動生成され、その後は更新されません。特定の既知の問題がシステムでどのように分類または更新されたかとその時期によっては、リリースノートに記載されない場合があります。Cisco バグ検索ツール を「信頼できる情報源」と考えてください。

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6.5.0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 サービス
- 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 6.5.0 既知の問題

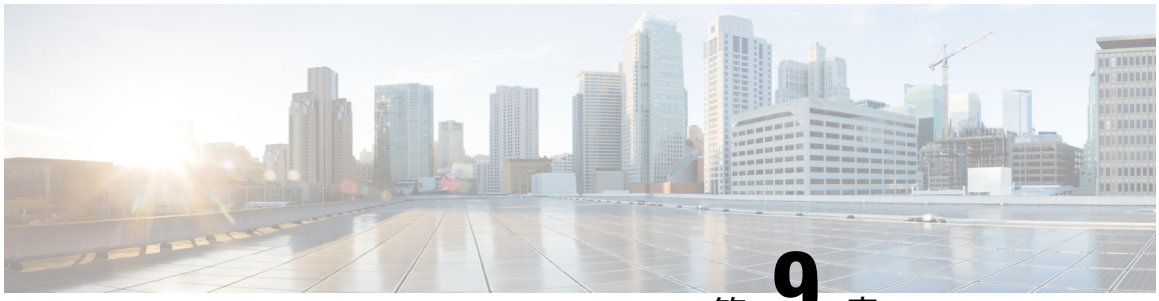
表 *50* : バージョン *6.5.0* の既知の問題

不具合 ID	タイトル
CSCvq03466	ハードウェアバイパスが有効化された状態での ISA 3000 FTD の展開が失敗する

不具合 ID	タイトル
CSCvq11310	6.5 SRTS の実行中に FTD のパフォーマンスが約 5% 低下した
CSCvq30293	FTD のバージョンのダウングレード後にブートストラップ設定が更新されません。
CSCvq47804	FDM からのシャットダウン後に FXOS セキュリティモジュールの電源が投入されない
CSCvq91091	1024B および MaxCPS のテスト時の 6.5 で、ASA 55xx シリーズのパフォーマンスが想定よりも低い
CSCvr09194	FXOS のアップグレード後に core.run_hm.pl が見つかる
CSCvr17786	HitCount が「true」、filter が「fetchZeroHitCount」に設定されたアクセスポリシーの API GET コールで、すべてのルールが返される
CSCvr21119	SSD を安全に消去するために 6.4 から 6.5 にアップグレードした場合は FP1000 ユニットでは電源の再投入が必要だった
CSCvr23986	メモリが不足しており、MIB ウォークが頻繁に実行される状態では、Cisco ASA & FTD デバイスがリロードする場合がある
CSCvr24059	送信元 SGT の相関が FMC および FTD 6.5 で機能しない
CSCvr34163	FTD がルーテッドモードまたはトランスペアレントモードの場合は、侵入イベントの下に VLAN ID が表示されないはずである
CSCvr35470	vFMC - 6.5.0-97 の CloudAgent コア
CSCvr37728	ごくまれに、ISE に再接続した後に ADI プロセスがクラッシュし、コアが生成されることがある
CSCvr39516	modexp-octeon での malloc 障害によって lina のセグメンテーション違反またはリロードが発生する
CSCvr39818	FTD：インターフェイス IP をスタティックから DHCP に切り替えると、FTD で異なる DHCP クライアント ID が使用される
CSCvr46892	モードの切り替え後にインターフェイスがシャットダウンされたままになる
CSCvr47499	800_post/1028_latency_settings_upgrade.pl で Firepower FMC のアップグレードに失敗する
CSCvr98881	トレースバック：FTD ZeroMQ メモリアサーション
CSCvs02233	OpenSSH auth-gss2.c の情報漏えいの脆弱性
CSCvs02234	OpenSSH Bailout によるユーザの列挙の遅延の脆弱性

不具合 ID	タイトル
CSCvs07425	接続を複数回クリアした後の最大接続テストが 6,000 万接続に到達しない
CSCvs08696	2.7.1 へのアップグレード後、Firepower シャーシマネージャがスマートエージェントが無効になっていると表示する
CSCvs25517	ACP を取得するための FMC API と GUI の競合状態
CSCvs31114	FTD 6.5 以降のバイパス失効チェックをサポートしていないことに関する警告
CSCvs44109	FMC：PPPoE パスワードの制限が厳しすぎる。基盤となるコードと一致している必要がある
CSCvs61555	Snort の不適切な削除によりポリシー展開が失敗し、侵入ポリシーエディタがハングする
CSCvs67534	圧縮（zip）されたマルウェアのダウンロードが初めて可能になった
CSCvs71825	/var/log/firstboot.S96ovf-data.pl にクリアテキストのインストールパスワードがある
CSCvs79606	「dns server-group DefaultDNS」CLI が無効にならない
CSCvs82115	「beakerd」プロセスが予期せず終了する。原因として、コアダンプが考えられる
CSCvt22254	FDM が更新サーバに到達できない場合、復元後に自動展開が失敗する
CSCvt35770	アップグレード後のバージョン不一致エラーによりポリシーの展開が失敗する
CSCvt39078	FMC と FTD の間の URL カテゴリの不一致。
CSCvt41201	FDM：DNS 値を変更しても、グループポリシーの値は更新されない
CSCvt43309	URL ライセンスがないセンサーがある場合は、URL フィルタライセンスによりすべてのセンサーでポリシー展開できない
CSCvt45206	アップグレード前に存在していたイベントを検索すると、イベント検索が失敗することがある
CSCvt48260	アクティブユニットを検出したときの fover_parse と ブートループでスタンバイ ASA がレースバックする
CSCvt49308	スレッド名での ASA のトレースバック：CRL 処理中の CERT API のメモリリーク
CSCvt52782	ASA トレースバックスレッド名：webvpn_task

不具合 ID	タイトル
CSCvt54182	FTD が SSL 複合を実行するように設定されている場合に LINA コアが生成される
CSCvt54279	FDM：オブジェクトのライセンス名がないために展開が失敗する。Sensitive_data には URLFILTERING ライセンスが必要
CSCvt54286	FTD-UI：自己署名証明書の UI にハードコード化された 5 年の有効期限がある
CSCvt59253	プロセス名 LINA での ASA 9.13.1.7 のトレースバックとリロード
CSCvt63484	9.13(1)7 の igb_saleen_io_sfp_mod_poll_thre プロセスにより ASA の CPU 使用率が高くなる
CSCvt63501	150 Mb を超えるファイルをアップロードしているときに WM で確認されたプロセス失敗のヒープが見られる
CSCvt63746	FDM /ngfw/var/sf/fwcfg/zones.conf が空になっている
CSCvt67638	メタデータを抽出できないエラーにより復元が失敗する
CSCvt74147	スレッド Lic HA クラスタでのトレースバック
CSCvt74893	FMCv イーサネットドライバが vmxnet3 TCP のパフォーマンス侵害を示している
CSCvt77578	HA の形成が失敗した場合でも、FDM GUI にプライマリ上でのハイアベイラビリティの成功が示される
CSCvt77813	Cisco_uridb* ファイルが原因で、/ngfw での管理対象外ディスクの使用率が高くなる



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/
- シスコ通知サービス：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