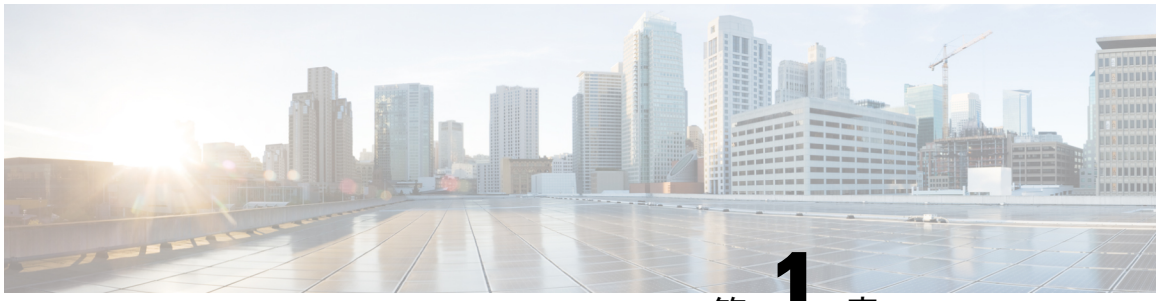
Cisco Firepower バージョン 7.1 リリースノート

初版：2021 年 12 月 15 日

最終更新：2022 年 9 月 23 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/

目 次



第 1 章

ようこそ

このドキュメントでは、以下に示すバージョン 7.1のリリース情報を記載しています。

- Cisco Firepower Threat Defense
- Cisco Firepower Management Center
- Cisco Firepower Device Manager

このドキュメントでは、お客様が導入したハードウェアと仮想アプライアンスについて説明します。Cisco Defense Orchestrator（CDO）、またはクラウド提供型の管理センターで Firepower Threat Defense を管理している場合は、「Cisco Defense Orchestrator の新機能」も参照してください。

リリースの主なポイント

全 FTD リリース

バージョン 7.1 は、FMC および FTD デバイスでのみサポートされます。ASA FirePOWER または NGIPSv デバイスではサポートされていません。

バージョン 7.1 の FMC を引き続き使用して、バージョン 6.5 ～ 7.0 を実行している古いデバイス（FTD、ASA FirePOWER および NGIPSv）を管理できます。

リリース日

表 *1*: バージョン *7.1* のリリース日

バージョン	ビルド	日付	プラットフォーム
7.1.0.2	36	2022 年 8 月 3 日	FMC/FMCv Secure Firewall 3100 シリーズ
7.1.0.1	28	2022 年 02 月 24 日	FMC/FMCv Secure Firewall 3100 シリーズを除くすべてのデバイス
7.1.0	90	2021 年 12 月 1 日	すべて（All）

推奨リリース

新しい機能と解決済みの問題を利用するには、対象となるすべてのアプライアンスを推奨リリース以上にアップグレードすることをお勧めします。シスコ サポートおよびダウンロードサイトでは、推奨リリースに金色の星が付いています。

また、新機能ガイドにも推奨リリースを示します。

- Cisco Secure Firewall Management Center の新機能（リリース別）
- Cisco Secure Firewall デバイスマネージャの新機能（リリース別）

古いアプライアンスの推奨リリース

アプライアンスが古すぎて推奨リリースを実行できず、ハードウェアを今すぐ更新しない場合は、メジャーバージョンを選択してから可能な限りパッチを適用します。一部のメジャーバージョンは長期または超長期に指定されているため、いずれかを検討してください。これらの用語の説明については、「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」を参照してください。

ハードウェアの更新に関心がある場合は、シスコの担当者またはパートナー担当者にお問い合わせください。

シスコとのデータの共有

次の機能はシスコとデータを共有します。

Cisco Success Network

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。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。

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 TACTAC 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。

初期設定およびアップグレード中に、登録するか尋ねられます。登録はいつでも変更できます。この機能は FDM で現在サポートされていません。

Web 分析トラッキング

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、ユーザーの場所、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。

デフォルトで登録されていますが、初期設定の完了後にいつでも登録を変更できます。

支援が必要な場合

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次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、Cisco 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。

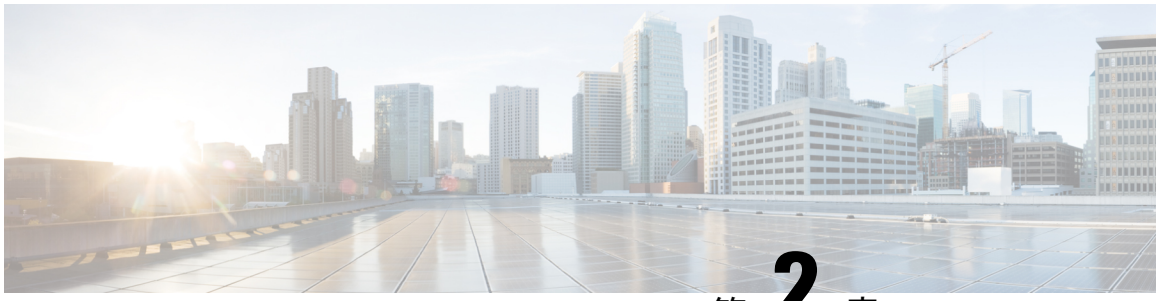
- マニュアル：http://www.cisco.com/go/threatdefense-71-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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 のユーザー 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



第 2 章

システム要件

このドキュメントでは、バージョン 7.1 のシステム要件を記載します。

FMC プラットフォーム

このセクションでは、バージョン 7.1 でサポートされている、お客様が導入したハードウェアと仮想 FMC を示します。クラウド提供型の管理センターにはバージョンはありません。

クラウド提供型の管理センターを含む、FMC とのデバイス互換性については、「FTD管理方式（9 ページ）」を参照してください。一般的な互換性情報については、Cisco Secure Firewall Management Center 互換性ガイド を参照してください。

FMC ハードウェア

バージョン 7.1 は次の FMC ハードウェアをサポートします。

- FMC 1600
- FMC 2600
- FMC 4600

また、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必要があります（Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes を参照）。

FMCv

バージョン 7.1 は、次の FMCv プラットフォームをサポートしています。

FMCv では、2、10、25、または 300 台のデバイスを管理できるライセンスを購入できます。一部のプラットフォームのみが FMCv300 をサポートすることに注意してください。さらに、

FMCv2 は高可用性をサポートしていません。サポートされているインスタンスの詳細については、Cisco Secure Firewall Management Center Virtual 入門ガイド を参照してください。

表 *2 :* バージョン *7.1 FMCv* パブリック クラウド プラットフォーム

プラットフォーム	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Amazon Web Services（AWS）	対応	対応	対応
Google Cloud Platform（GCP）	対応	—	—
Microsoft Azure	対応	—	—
Oracle Cloud Infrastrucure（OCI）	対応	対応	対応

表 *3 :* バージョン *7.1 FMCv* オンプレミス/プライベート クラウド プラットフォーム

プラットフォーム	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Cisco HyperFlex	対応	—	—
カーネルベース仮想マシン（KVM）	対応	—	—
Nutanix エンタープライズクラウド	対応	—	—
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

FTDプラットフォーム

次の表に、このリリースのサポート対象デバイスと管理方式を示します。これらの管理方法の詳細については、を参照してください。FTD管理方式 （9 ページ）一般的な互換性情報については、Cisco Secure Firewall Threat Defense 互換性ガイド を参照してください。

FTD ハードウェア

Threat Defense のハードウェアは、多様なスループット、拡張性、およびフォームファクタに対応します。

表 *4 :* バージョン *7.1 FTD* ハードウェア

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
Firepower 1010、1120、1140、1150	対応	—	対応	対応	—
Firepower 2110、2120、2130、2140	対応	—	対応	対応	—
Secure Firewall 3110、3120、3130、3140	対応	—	対応	対応	バージョン 7.1.0 リリースには、これらのデバイスのオンラインヘルプが含まれていません。FMC の場合、新しいオンラインヘルプがバージョン 7.1.0.2 に含まれています。FDM の場合は、Cisco.com に掲載されているドキュメントを参照してください。将来のリリースに新しいオンラインヘルプを含める予定です。
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	対応	—	対応	対応	FXOS 2.11.1.154 以降のビルドが必要です。
Firepower 9300：SM-24、SM-36、SM-44 モジュール Firepower 9300：SM-40、SM-48、SM-56 モジュール	対応	—	対応	対応	FXOS 2.11.1.154 以降のビルドが必要です。

プラットフォーム	FMC 互換		FDM 互換		注記
	お客様が導入	クラウド提供型	FDM のみ	FDM + CDO	
ISA 3000	対応	—	対応	対応	最新の ROMMON イメージが必要です。 Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイドを参照してください。

FTDv

仮想版 FTD の導入により、スループット要件とリモートアクセス VPN セッションの制限に基づいて、パフォーマンス階層型のスマート ソフトウェア ライセンスがサポートされます。オプションは、FTDv5（100 Mbps/50 セッション）から FTDv100（16 Gbps/10,000 セッション）までです。サポートされているインスタンス、スループット、およびその他のホスティング要件の詳細については、該当するスタートアップガイドを参照してください。

表 *5*：バージョン *7.1 FTDv* パブリック クラウド プラットフォーム

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Amazon Web Services（AWS）	対応	—	対応	対応
Microsoft Azure	対応	—	対応	対応
Google Cloud Platform（GCP）	対応	—	—	—
Oracle Cloud Infrastrucure（OCI）	対応	—	—	—

表 *6*：バージョン *7.1 FTDv* オンプレミス/プライベート クラウド プラットフォーム

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Cisco Hyperflex	対応	—	対応	対応
カーネルベース仮想マシン（KVM）	対応	—	対応	対応

デバイスのプラットフォーム	FMC 互換		FDM 互換	
	お客様が導入	クラウド提供型	FDM のみ	CDO および FDM
Nutanix エンタープライズクラウド	対応	—	対応	対応
OpenStack	対応	—	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	—	対応	対応

FTD管理方式

デバイスモデルとバージョンに応じて、いくつかのデバイス管理方法をサポートしています。

お客様が導入したFMC

すべての デバイスは、FMC によるリモート管理に対応しています。

お客様が導入したハードウェアまたは仮想FMCは、管理対象デバイスと同じまたは新しいバージョンを実行する必要があります。これは、以下を意味します。

- より新しい FMC でより古いデバイスを管理できます。通常は、メジャーバージョンをいくつか遡ることができます。ただし、導入環境全体を常に更新することをお勧めします。多くの場合、新機能の使用や問題解決の適用には、FMC とその管理対象デバイスの両方で最新リリースが必要になります。
- FMC よりも新しいバージョンのデバイスをアップグレードすることはできません。メンテナンス（3 桁）リリースの場合でも、最初に FMC をアップグレードする必要があります。

表 *7: FMC*とデバイス間の互換性

FMC バージョン	管理可能な最も古いデバイスバージョン
クラウド提供型の管理センター（バージョンなし）	7.0.3/7.2
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3

FMC バージョン	管理可能な最も古いデバイスバージョン
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1
5.4.1	5.4.1（ASA-5506-X シリーズ、ASA5508-X、および ASA5516-X の ASA FirePOWER）。 5.3.1（ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、および ASA-5585-X シリーズの ASA FirePOWER）。 5.3.0（Firepower 7000/8000 シリーズおよびレガシーデバイス）。

クラウド提供型の管理センター

クラウド提供型の管理センターは、複数のシスコ セキュリティ ソリューションの管理を統合する Cisco Defense Orchestrator（CDO）プラットフォームを通して提供されます。更新についてはシスコが行います。クラウド提供型の管理センターは、以下を実行する Threat Defense デバイスを管理できます。

- 7.0.3 以降のメンテナンスリリース
- バージョン 7.2 以降

クラウド提供型の管理センターは、バージョン 7.1 を実行している脅威防御デバイス、または任意のバージョンを実行しているデバイスを管理できません。クラウド管理を登録解除して無効にしない限り、クラウド提供型の管理センターに登録されている脅威防御デバイスをバージョン 7.0.x からバージョン 7.1 にアップグレードすることはできません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

クラウド管理デバイスは、イベントのログ記録と分析の目的でのみ、バージョン 7.2 以降のお客様導入の管理センターに追加できます。あるいは、シスコのセキュリティ分析とロギング（SaaS） を使用して、Cisco Cloud にセキュリティイベントを送信できます。

FDM

Firepower Device Manager を使用すると、単一の FTD デバイスをローカルで管理できます。

必要に応じて、FMC の代替策として、Cisco Defense Orchestrator（CDO）を追加し、複数の FTD デバイスをリモートで管理します。一部の構成では引き続き FDM が必要ですが、CDO を使用することで、展開したすべての FTD を通して一貫したセキュリティポリシーを確立して維持できます。

ブラウザ要件

ブラウザ

現在サポートされている MacOS と Microsoft Windows 上で稼働する、次の一般的なブラウザの最新バージョンでテストを実施しています。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge（Windows のみ）

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 を使用した広範なテストを実施していません。また、FMC ウォークスルーを使用した Microsoft Edge の広範なテストも実施していません。ただし、Cisco TAC 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。

ブラウザの設定と拡張

ブラウザに関係なく、JavaScript、Cookie、および TLS v1.2 が有効なままになっていることを確認する必要があります。Microsoft Edge を使用している場合は、IE モードを有効にしないでください。

一部のブラウザ拡張機能では、PKI オブジェクトの証明書やキーなどのフィールドに値を保存できないことに注意してください。これらの拡張機能には Grammarly や Whatfix Editor などがありますが、それに限りません。この問題は、これらの拡張機能によってフィールドに文字（HTML など）が挿入され、システムが無効と見なすために発生します。シスコの製品にログインしている間は、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

インターフェイス	最小解像度
FMC	1280 X 720

インターフェイス	最小解像度
FDM	1024 X 768
Firepower 4100/9300 用 Firepower Chassis Manager	1024 X 768

セキュア通信

初めてログインした場合、システムは自己署名デジタル証明書を使用して Web 通信を保護します。ブラウザに信頼されていない機関に関する警告が表示されますが、信頼ストアに証明書を追加することもできます。これにより継続できるようになりますが、自己署名証明書を、世界的に知られている、または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。

自己署名証明書の置き換えを開始する手順は、次のとおりです。

- FMC：**[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。
- FDM：[Device] をクリックしてから **[System Settings]** > **[Management Access]** リンクをクリックし、次に [Management Web Server）] タブをクリックします。

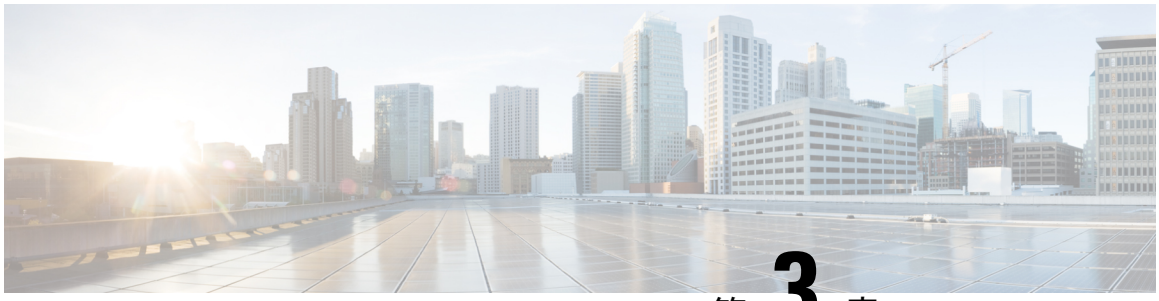
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーション ガイドを参照してください。

（注） 自己署名証明書を置き換えない場合は、次の手順を実行します。

- Google Chrome は、画像、CSS、JavaScript などの静的コンテンツを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。
- Mozilla Firefox は、ブラウザの更新時に自己署名証明書を信頼しなくなる場合があります。この場合は Firefox を更新できますが、一部の設定が失われることに注意してください。Mozilla の Firefox 更新サポートページを参照してください。

監視対象ネットワークからの参照

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、モニター対象ネットワーク内のユーザーが 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。



第 3 章

特長と機能

このドキュメントでは、バージョン7.1の新機能と廃止された機能について説明します。また、アップグレードによる影響についても言及します。

重要 新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

新機能

FMC バージョン 7.1 の新機能

新しい FMC で古いデバイスを管理できますが、常に環境全体を更新することを推奨します。新しいトラフィック処理機能では、FMC とデバイスの両方で最新のリリースが前提条件となります。 デバイスが明らかに関与していない機能（Web インターフェイスの外観の変更、クラウド統合）では、FMC の最新バージョンのみを必須条件としているにもかかわらず、それが保証されない場合があります。新機能の説明では、バージョンの要件が標準で想定される条件から逸脱している場合は明示しています。

表 *8 : FMC* バージョン *7.1.0* の新機能

機能	説明
デバイスのセットアップ	

機能	説明
FDM を使用して、FMC による管理用に FTD を設定します。	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。FTD CLI を使用すると、管理と FMC のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス設定は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された FDM 画面：**[システム設定（System Settings）]** > **[管理センター（Management Center）]**
デバイスのアップグレード	
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**[システム（System）]** > **[更新（Updates）]**ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）]ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、Firepower 4100/9300 のコンテナインスタンスではサポートされません。

機能	説明
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。
Snort 3 後方互換性。	Snort 3 の場合、新しい機能と解決済みのバグでは、FMC とその管理対象デバイスを完全にアップグレードしている必要があります。Snort 2 とは異なり、新しい FMC（たとえば、バージョン 7.1）から展開して、古いデバイス（たとえば、バージョン 7.0）の検査エンジンを更新することはできません。 古いデバイスに展開すると、サポートされない設定が一覧表示され、それらの設定がスキップされることが警告されます。環境全体を常に更新することをお勧めします。
デバイス管理	

機能	説明
新しい Cisco Secure Firewall 3100 の設定と機能をサポート。	次の画面と CLI コマンドは、Secure Firewall 3100 に関連付けられています。これらの新しいモデルの詳細については、バージョン 7.1 の新しいハードウェアと仮想プラットフォーム （43 ページ）を参照してください。 新規/変更された画面： • **[Devices]** > **[Device Management]** > **[Add Cluster]** • **[Devices]** > **[Device Management]** > **[More]** • **[Devices]** > **[Device Management]** > **[Cluster]** • **[Devices]** > **[Device Management]** > **[Chassis Operations]** • **[Devices]** > **[Device Management]** > **[Interfaces]** > 物理インターフェイスを編集 > [Hardware Configuration] • **[Devices]** > **[Device Management]** 新規/変更された FTD CLI コマンド： **configure network speed**、**configure raid**、**show raid**、**show ssd**
AWS インスタンスでの FTDv に対する Geneve インターフェイスサポート。	AWS ゲートウェイロードバランサ（GWLB）のシングルアームプロキシをサポートするために、Geneve カプセル化サポートが追加されました。AWS GWLB は、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて FTDv を拡張するロードバランサを組み合わせます。 このサポートには、Snort 3 が有効になっている FMC が必要であり、次のパフォーマンス階層で利用できます。 • FTDv20 • FTDv30 • FTDv50 • FTDv100
OCI 上の FTDv に対する Single Root I/O Virtualization（SR-IOV）のサポート	OCI 上の FTDv に Single Root Input/Output Virtualization（SR-IOV）を実装できるようになりました。SR-IOV により、FTDv のパフォーマンスを向上させることができます。SR-IOV モードでの vNIC としての Mellanox 5 はサポートされていません。

機能	説明
Firepower 1100 の LLDP サポート。	Firepower 1100 インターフェイスの Link Layer Discovery Protocol（LLDP）を有効に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）]** > **[ハードウェア構成（Hardware Configuration）]** > **[LLDP]** 新規/変更されたコマンド：**show lldp status**、**show lldp neighbors**、**show lldp statistics** サポートされるプラットフォーム：Firepower 1100（1120、1140、および 1150）
インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになり、インターフェイスの同期が改善されました。	インターフェイスの自動ネゴシエーションが速度とデュプレックスから独立して設定されるようになりました。また、FMC でインターフェイスを同期すると、ハードウェアの変更がより効果的に検出されます。 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）]** > **[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]** サポートされるプラットフォーム：Firepower 1000/2100、Secure Firewall 3100
信頼された DNS サーバの指定のサポート。	FTD プラットフォーム設定を使用して、DNS スヌーピングに信頼できる DNS サーバーを指定できます。これは、ドメインを IP アドレスにマッピングすることにより、最初のパケットでアプリケーションを検出するのに役立ちます。デフォルトでは、信頼できる DNS サーバーには、DNS サーバーオブジェクト内の DNS サーバーと、dhcp-pool、dhcp-relay、および dhcp-client によって検出された DNS サーバーが含まれます。
デバイス設定のインポート/エクスポート。	次の使用例で、デバイス固有の設定をエクスポートし、同じデバイスに保存された設定をインポートできます。 • デバイスを別の FMC に移動する。 • 古い設定を復元する。 • デバイスを再登録する。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[全般（General）]**
高可用性/拡張性	

機能	説明
高可用性 • AWS 用 FMCv • OCI 用 FMCv	AWS 用 FMCv および OCI 用 FMCv で高可用性がサポートされるようになりました。 FTD の展開では、2 つの同一ライセンスの FMC と、各管理対象デバイスに 1 つの FTD 権限が必要です。たとえば、FMCv10 高可用性ペアで 10 台の FTD デバイスを管理するには、2 個の FMCv10 権限と 10 個の FTD 権限が必要です。バージョン 6.5.0 ～ 7.0.x のクラシックデバイス（NGIPSv または ASA FirePOWER）のみを管理している場合は、FMCv 権限は必要ありません。 サポートされるプラットフォーム：FMCv10、FMCv25、FMCv300（FMCv2 ではサポートされません）
OCI用FTDvの自動スケール。	OCI 用 FTDv で自動スケーリングがサポートされるようになりました。 クラウドベースの展開におけるサーバレス インフラストラクチャでは、キャパシティのニーズに基づいて、自動スケールグループ内のFTDvインスタンスの数が自動的に調整されます。これには、管理側の FMC との自動登録/登録解除が含まれています。
ファイアウォールの変更に対するクラスタの展開がより迅速に完了します。	ファイアウォールの変更に対するクラスタの展開がより迅速に完了するようになりました。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
ハイアベイラビリティ グループまたはクラスタ内のルートのクリア。	以前のリリースでは、**clear route** コマンドはユニットのルーティングテーブルのみをクリアしました。現在、ハイアベイラビリティグループまたはクラスタで動作している場合、コマンドはアクティブユニットまたはコントロールユニットでのみ使用でき、グループまたはクラスタ内のすべてのユニットのルーティングテーブルをクリアします。
NAT	
変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
ルーティング	

機能	説明
仮想ルータを相互接続するための BGP 設定。	ユーザー定義の仮想ルータ間、およびグローバル仮想ルータとユーザー定義の仮想ルータ間でルートを動的にリークするように BGP 設定を構成できます。ルートのインポートおよびエクスポート機能が導入され、仮想ルータにルートターゲットのタグを付け、必要に応じて、一致したルートをルートマップでフィルタリングすることにより、仮想ルータ間でルートを交換します。この BGP 機能は、ユーザー定義の仮想ルータを選択した場合にのみ利用できます。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv4/v6] > [ルートのインポート/エクスポート（Route Import/Export）]**
ユーザー定義の仮想ルータでの BGPv6 サポート。	FTD は、ユーザー定義の仮想ルータでの BGPv6 の設定をサポートするようになりました。 新規/変更された画面：選択したユーザー定義の仮想ルータについて、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [BGPv6]**
Equal-Cost-Multi-Path（ECMP）ゾーンのサポート。	トラフィックゾーンのインターフェイスをグループ化し、FMC で Equal-Cost-Multi-Path（ECMP）ルーティングを設定できるようになりました。 ECMP ルーティングは、以前は FlexConfig ポリシーを通じてサポートされていました。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [ECMP]**
ダイレクト インターネット アクセス/ポリシーベースルーティング	

機能	説明
ポリシーベースルーティングによるダイレクト インターネット アクセス。	FMC を介してポリシーベースルーティングを設定して、アプリケーションに基づいてネットワークトラフィックを分類し、ダイレクト インターネット アクセス（DIA）を実装して、ブランチ展開からインターネットにトラフィックを送信できるようになりました。PBR ポリシーを定義し、入力インターフェイスに設定して、一致基準と出力インターフェイスを指定できます。アクセス コントロール ポリシーに一致するネットワークトラフィックは、ポリシーで設定されている優先順位または順序に基づいて、出力インターフェイスを介して転送されます。 新規/変更された画面：ポリシー ベース ルーティング ポリシーを設定するための新しいポリシーページ：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[ポリシーベースルーティング（Policy Based Routing）]** サポートされるプラットフォーム：FTD
ダイレクト インターネット アクセスとポリシーベースルーティングのための FMC REST API の機能拡張。	FMC REST API を使用して、ポリシーベースルーティングによるダイレクト インターネット アクセスを設定できます。これをサポートするために、FMC REST API に次の機能拡張が加えられました。 • ポリシーベースルーティング設定を作成、表示、編集、および削除できるようにする新しい API が追加されました。 • アプリケーションを定義する拡張アクセス制御リストの既存の API に新しいパラメータが追加されました。 • インターフェイスの優先順位を定義するデバイスインターフェイスの既存の API に新しいパラメータが追加されました。
リモートアクセス VPN	
RA VPN ポリシーのコピー。	既存のポリシーをコピーして、新しい RA VPN ポリシーを作成できるようになりました。**[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**の各ポリシーの横にコピーボタンが追加されました。

機能	説明
AnyConnect VPN SAML 外部ブラウザ。	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。
Microsoft Azure 上の SAML ID プロバイダーにおける複数のトラストポイント。	Microsoft Azure の要求に応じて、SAML ID プロバイダーに複数の RA VPN トラストポイントを追加できるようになりました。 Microsoft Azure ネットワークでは、Azure は同じエンティティ ID に対して複数のアプリケーションをサポートできます。（通常は別のトンネルグループにマップされる）各アプリケーションには、一意の証明書が必要です。この機能により、Microsoft Azure 向け FTDv で RA VPN に複数のトラストポイントを追加できます。
サイト間 VPN	
VPN フィルタ。	トンネリングされたデータパケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって許可するか拒否するかを決定するルールを使用して、サイト間 VPN フィルタを設定できるようになりました。 VPN フィルタは、トンネルから出た後の復号化後のトラフィックと、トンネルに入る前の暗号化前のトラフィックに適用されます。
IKEv2 の一意のローカルトンネル ID。	ポリシーベースとルートベースのサイト間 VPN の両方に IKEv2 トンネルごとのローカルトンネル ID を設定できるようになりました。FMC Web インターフェイスまたは REST API からローカルトンネル ID を設定できます。 このローカルトンネル ID 設定により、FTD との Umbrella SIG 統合が可能になります。

機能	説明
複数の IKE ポリシー。	ポリシーベースとルートベースのサイト間 VPN の両方に複数の IKE ポリシーを設定できるようになりました。 FMC GUI および REST API を使用して複数の IKE ポリシーを設定できます。
VPN 監視ダッシュボード。	**ベータ版。** サイト間 VPN 監視ダッシュボードは次の機能を提供します。 • 全デバイスのトンネルステータス分布の可視化 • VPN トンネルで構成されるネットワークトポロジの可視化 • トポロジ、デバイス、ステータスなどの基準に基づいてトンネルを視覚的に切り離して調べる機能 （注） サイト間監視ダッシュボードはベータ機能であり、期待どおりに動作しない場合があります。実稼働環境では使用しないでください。
セキュリティ インテリジェンス	
プロキシされたトラフィックでのセキュリティ インテリジェンスのための Snort 3 サポート。	Snort 3 では、IP アドレスが HTTP リクエストに埋め込まれている HTTP プロキシトラフィックにセキュリティ インテリジェンスを適用できるようになりました。たとえば、ユーザーが IP アドレスまたはネットワークを含むブロックリストまたは許可リストをアップロードすると、システムはプロキシ IP ではなく宛先サーバーの IP を照合します。その結果、宛先サーバーへのトラフィックを（セキュリティ インテリジェンスの設定に応じて）ブロック、監視、または許可することができます。
侵入検知と防御	

機能	説明
ルールアクションのドロップ、拒否、書き換え、およびパスに対する Snort 3 のサポート。	バージョン 7.1 FMC は、バージョン 7.0 デバイスを含む、Snort 3 を使用した FTD デバイスで次の侵入ルールアクションをサポートするようになりました。 • ドロップ：一致するパケットをドロップし、この接続でそれ以上のトラフィックをブロックしません。侵入イベントを生成します。 • 拒否：一致するパケットをドロップし、この接続の以降のトラフィックもブロックします。TCP トラフィックの場合、TCP リセットを送信します。UDP トラフィックの場合、送信元および宛先ホストに ICMP ポート到達不能を送信します。侵入イベントを生成します。 • 書き換え：ルールの置換オプションに基づいて一致するパケットを上書きします。侵入イベントを生成します。 • パス：一致するパケットが他の侵入ルールによる評価なしで通過することを許可します。侵入イベントを生成しません。 これらの新しいルールアクションを設定するには、侵入ポリシーの Snort 3 バージョンを編集し、各ルールの [ルールアクション（Rule Action）] ドロップダウンを使用します。
TLS ベースの侵入ルールに対する Snort 3 のサポート。	Snort 3 で復号化された TLS トラフィックを検査する TLS ベースの侵入ルールを作成できるようになりました。この機能により、Snort 3 侵入ルールで TLS 情報を使用できます。
SMB2 上の DCE/RPC のインスペクションに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 は、SMB2 での DCE/RPC インスペクションをサポートします。 Snort 3 デバイスへの最初のアップグレード後の展開の後、既存の DCE/RPC ルールは、SMB2 での DCE/RPC の検査を開始します。以前は、これらのルールは SMB1 での DCE/RPC のみを検査していました。
侵入ルールの推奨に対する Snort 3 のサポート。	バージョン 7.1 FMC は、バージョン 7.0 デバイスを含む、Snort 3 を使用した FTD デバイスで侵入ルールの推奨をサポートするようになりました。 この機能を設定するには、侵入ポリシーの Snort 3 バージョンを編集し、左側のペインの [すべてのルール（All Rules）] の横にある [推奨（Recommendations）] ボタンをクリックします。

機能	説明
ssl_version および **ssl_state** キーワードに対する Snort 3 のサポート。	**アップグレードの影響。** Snort 3 を使用したバージョン 7.1 では、**ssl_version** および **ssl_state** 侵入ルールキーワードがサポートされています。 シスコが提供する侵入ポリシーには、これらのキーワードを使用するアクティブルールが含まれます。これらを使用して、カスタム/サードパーティルールを作成、アップロード、および展開することもできます。バージョン 7.0.x では、これらのキーワードは Snort 2 でのみサポートされていました。Snort 3 では、これらのキーワードを含むルールはトラフィックに一致しないため、アラートを生成したり、トラフィックに影響を与えたりすることはできませんでした。ルールが予期したとおりに機能していないという通知はありませんでした。バージョン 7.1 以降の Snort 3 デバイスへの最初のアップグレード後の展開の後、これらのキーワードを含む既存のルールはトラフィックと一致します。
Identity Services およびユーザー制御	
HTTP/2 トラフィックのインターセプトに対する Snort 3 キャプティブポータルのサポート。	キャプティブポータルを使用したユーザー認証のために、HTTP/2 トラフィックをインターセプトしてリダイレクトできるようになりました。 ブラウザがリダイレクトを受信すると、ブラウザはリダイレクトに従い、HTTP/1 キャプティブポータルと同じプロセスを使用して idhttpsd（Apache Web サーバー）で認証します。認証後、idhttpsd によりユーザーは元の URL にリダイレクトされます。
ホスト名ベースのリダイレクトに対する Snort 3 キャプティブポータルのサポート。	ID ポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスの IP アドレスではなく、完全修飾ドメイン名（FQDN）にユーザーの認証をリダイレクトできます。 FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。 新規/変更された画面：ID ポリシー設定に [ホスト名にリダイレクト（Redirect to Host Name）] オプションが追加されました。
暗号化トラフィックの処理（TLS/SSL）	

機能	説明
TLS 証明書フィード。	ライブ TLS 証明書フィードに基づいて TLS/SSL ルールを作成できるようになりました。ライブ TLS 証明書フィードを使用すると、TLS 証明書フィンガープリントの管理オーバーヘッドが削減され、より最新の情報に基づいたルールが可能になります。
拡張 TLS/SSL ポリシーオプション。	[SSLポリシー（SSL Policy）] ページの [詳細設定（Advanced Settings）] タブで、次の拡張 TLS/SSL ポリシーオプションを設定できるようになりました。 • ESNI（暗号化されたサーバー名識別）を要求するフローをブロックする • HTTP/3 アドバタイズメントを無効にする • 信頼できないサーバー証明書をクライアントに伝播する
暗号化されたセッションを可視化するための暗号化された可視性エンジン。	**ベータ版。** 暗号化された可視性エンジンを有効にすると、復号を必要とせずに暗号化されたセッションを可視化することができます。このエンジンによってトラフィックのフィンガープリントが収集され、分析されます。FMC 7.1 では、暗号化された可視性エンジンにより、TLS や QUIC などのプロトコルを含む暗号化されたトラフィックの可視性が向上します。そのトラフィックに対してアクションは適用されません。 暗号化された可視性エンジンは、デフォルトで無効になっています。これは、[実験段階の機能（Experimental Features）] セクションのアクセス コントロール ポリシーの [詳細（Advanced）] タブで有効にすることができます。 新規/変更された画面：**[ポリシー（Policies）] > [アクセス制御（Access Control）] > [*Access Control Policy name*] > [詳細（Advanced）]** **（注）** 暗号化された可視性エンジンは、可視性のために提供される実験段階のベータ機能です。誤検出を起こす可能性があります。
サービス ポリシー	
初期接続の最大セグメントサイズ（MSS）を設定します。	サービスポリシーを設定して、初期接続制限に達したときに初期接続の SYN cookie を生成するためのサーバーの最大セグメントサイズ（MSS）を設定できます。これは、最大初期接続数も設定するサービスポリシーの場合に意味があります。 新規/変更された画面：[サービスポリシーの追加/編集（Add/Edit Service Policy）] ウィザードの [接続設定（Connection Settings）]。

機能	説明
ネットワークディスカバリ	
ネットワーク検出の Snort 3 サポートの改善（リモートネットワーク アクセスのサポート）。	ネットワーク検出とリモートネットワークアクセスのサポートの改善により、Snort 3 はこれらの機能について Snort 2 と同等になりました。強化された機能は次のとおりです。 • SMB トラフィックのホストとアプリケーションの検出：ネットワーク上の SMB トラフィックの場合、ホストはネットワークマップで検出され、SMB アプリケーションプロトコルと関連するオペレーティングシステム情報が検出されます。 • NetBIOS トラフィックの検出：NetBIOS トラフィックの場合、NetBIOS 名と、クライアントアプリケーションやオペレーティングシステムなどのアプリケーション関連情報が検出されます。 • ネットワーク検出ポリシーによって監視されるホスト/ネットワークのみのアプリケーションの検出：このフィルタリングロジックの機能拡張により、ネットワーク検出ルールに基づいて監視されているネットワークのアプリケーションを検出できます。 Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が常に有効になっています。
イベントロギングおよび分析	

機能	説明
エレファントフローの識別とモニタリングに対する Snort 3 のサポート。	Snort 3 を実行する FTD では、エレファントフロー（システム全体のパフォーマンスに影響を与えるのに十分な大きさのシングルセッション ネットワーク接続）を識別できるようになりました。デフォルトでは、エレファントフローの検出は自動的に有効になり、1GB/10 秒を超える接続を追跡および記録します。 接続イベントの新しい定義済み検索（Reason = Elephant Flow）を使用すると、エレファントフローをすばやく特定できます。ヘルスモニタを使用して、デバイス上のアクティブなエレファントフローを表示し、エレファントフローの発生率を CPU 使用率などの他のデバイスメトリックと関連付けるカスタム ヘルス ダッシュボードを作成することもできます。 この機能を無効にするか、サイズと時間のしきい値を設定するには、FTD CLI を使用します。 新規/変更された FTD CLI コマンド： • **show elephant-flow status** • **show elephant-flow detection-config** • **system support elephant-flow-detection enable** • **system support elephant-flow-detection disable** • **system support elephant-flow-detection bytes-threshold** *bytes-in-MB* • **system support elephant-flow-detection time-threshold** *time-in-seconds*
FMC からセキュアネットワーク分析クラウドに侵入イベントとレトロスペクティブ マルウェア イベントを送信します。	**アップグレードの影響。** Cisco Security Analytics and Logging（SaaS）を使用してセキュリティイベントを Stealthwatch クラウドに送信するようにシステムを設定すると、FMC は次を送信します。 • 侵入イベント。これにより、リモートで保存された侵入イベントに影響フラグデータを含めることができます。以前は、これらのイベントは FTD によってクラウドに送信され、影響フラグは含まれていませんでした。 • レトロスペクティブ マルウェア イベント。これらは、デバイスによって引き続きクラウドに送信される「元の性質」ファイルとマルウェアイベントを補完します。 この機能が有効になっている場合、FMC はアップグレードの成功後にこの情報の送信を開始します。

機能	説明
侵入イベントの新しいデータストアによるパフォーマンスの向上。	パフォーマンスを向上させるために、バージョン 7.1 では、侵入イベントに新しいデータストアを使用します。アップグレードが完了し、FMCが再起動すると、履歴イベントが、最新のイベントが先頭になるようにバックグラウンドで移行されます。 この移行の一部として、侵入インシデント、侵入イベントクリップボード、および侵入イベントのカスタムテーブルは廃止されました。詳細については、FMC バージョン 7.1 で廃止された機能（46 ページ）を参照してください。 また、侵入イベントテーブルに、[送信元ホストの重要度（Source Host Criticality）] と [宛先ホストの重要度（Destination Host Criticality）] という 2 つの新しいフィールドが導入されました。
接続およびセキュリティインテリジェンス イベントの NAT IP アドレスおよびポート情報。	NAT 変換の可視性を高めるために、次のフィールドが接続およびセキュリティ インテリジェンス イベントに追加されました。 • NAT 送信元 IP（NAT Source IP） • NAT 宛先 IP（NAT Destination IP） • NAT 送信元ポート（NAT Source Port） • NAT 宛先ポート（NAT Destination Port） イベントのテーブルビューでは、デフォルトでこれらのフィールドは非表示にされています。表示されるフィールドを変更するには、任意の列名の [x] をクリックしてフィールド選択ツールを表示します。

機能	説明
パケットトレーサの機能拡張。	バージョン 7.1 では、より使いやすくするためにパケット トレーサ インターフェイスが更新されています。さらに、次のことができるようになりました。 • メインメニューから直接パケットトレーサにアクセス：**[デバイス（Devices）] > [トラブルシュート（Troubleshoot）] > [パケットトレーサ（Packet Tracer）]** • パケットトレースの保存。 • 複数デバイスでの並列パケットトレースの実行。 • デバイスを介した PCAP の再生。 • Snort 3 デバイスの場合、L2 から L7 までのトラフィック評価のフェーズ（アプリケーション識別、ファイル/マルウェア検出、侵入検出、セキュリティ インテリジェンスなど）、および各フェーズにかかる時間に関して新しい詳細を提供する拡張出力の表示。 新規/変更された FTD CLI コマンド： • **packet-tracer input***source_interface* **pcap***pcap_filename*
オブジェクト管理	
HTTP、ICMP、および SSH プラットフォーム設定のネットワークオブジェクトのサポート。	Threat Defense プラットフォーム設定ポリシーで IP アドレスを設定するときに、ホストまたはネットワークのネットワークオブジェクトを含むネットワーク オブジェクト グループを使用できるようになりました。
ネットワーク ワイルドカードマスク オブジェクトの Snort 3 サポート。	[オブジェクト管理（Object Management）] ページで、ネットワーク ワイルドカード マスク オブジェクトを作成および管理できるようになりました。アクセス制御、プレフィルタ、およびNAT ポリシーでネットワーク ワイルドカード マスク オブジェクトを使用できます。
オブジェクトの展開プレビューの機能拡張。	地理位置情報、ファイルリスト、およびセキュリティ インテリジェンス オブジェクトへの展開の変更をプレビューできるようになりました。 更新された画面：**[展開（Deploy）] > [展開（Deployment）]**。[プレビュー（Preview）] 列で、デバイスの [プレビュー（Preview）] アイコンをクリックすると、ファイルリストオブジェクトへの変更が表示されます。
統合	

機能	説明
Cisco ACI Endpoint Update App バージョン 2.0 および修復モジュールのサポート。	Cisco ACI Endpoint Update App のバージョン 2.0 では、以前のバージョンに比べて次の点が改善されています。 • 最小更新間隔（アプリケーションが FMC を更新する頻度）が 10 秒になりました。以前は 30 秒でした。 • サイトプレフィックス（各 APIC テナントに関連付けられた FMC にネットワーク グループ オブジェクトを作成する文字列）が 10 文字に制限されました。以前は 5 文字でした。 この更新では、新しい Cisco ACI Endpoint 修復モジュールも利用できます。
ユーザビリティ、パフォーマンス、およびトラブルシューティング	
ヘルスモニタリングの強化。	ヘルスモニタは次のように更新されました。 • ヘルスポリシーエディタは、類似するヘルスモジュールをグループ化するようになりました。モジュールグループ全体を有効または無効にできます。 • ヘルスポリシー除外エディタが更新され、使いやすくなりました。また、アラートからデバイスまたはヘルスモジュールを除外するときに、除外の期間を 15 分から永久まで指定できるようになりました。 • ヘルス モニタ アラート エディタが更新され、使いやすくなりました。 • ヘルスポリシーの展開インターフェイスが更新され、使いやすくなりました。 （注） 更新されたヘルスモニタを使用するには、**[システム（System）] > [設定（Configuration）] > [REST API設定（REST API Preferences）]**で REST API アクセスを有効にする必要があります。 新規/変更された画面： • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの編集（Edit Policy）]** • **[システム（System）] > [ヘルス（Health）] > [除外（Exclude）]** • **[システム（System）] > [ヘルス（Health）] > [モニタアラート（Monitor Alerts）]** • **[システム（System）] > [ヘルス（Health）] > [ポリシー（Policy）] > [ポリシーの展開（Deploy Policy）]**

機能	説明
展開履歴の機能拡張。	展開ジョブをブックマークし、ジョブの展開に関する注意を編集して、レポートを生成できるようになりました。
グローバル検索の機能拡張。	グローバル検索に次の機能が追加されました。 • FMC ウォークスルーの全文を検索できます（how-tos）。 • 拡張コミュニティリスト名または設定値を検索できます。 • ドメインごとに検索を制限できます。
新しいウォークスルー。	次のウォークスルーが追加されました。 • Snort 3 侵入ポリシーの作成。 • 個々のデバイス上での Snort 3 の有効化と無効化。 • Snort 3 ネットワーク分析ポリシーの作成。 • ネットワーク分析ポリシーのマッピングの表示。 • FTD のアップグレード。 • クラスタの作成および管理。 • FMC アクセスインターフェイスの管理からデータへの変更。 • FMC アクセスインターフェイスのデータから管理への変更。
Cisco Success Network に送信された Snort メモリ使用量テレメトリ。	有用性を向上させるために、Snort メモリおよびスワップ使用率（メモリ不足イベントを含む）に関するテレメトリを Cisco Success Network に送信するようになりました。 この情報は、Snort 2 と Snort 3 の両方に送信されます。Cisco Success Network の登録はいつでも変更できます。
Snort 3 は、フロー開始イベントとフロー終了イベントの統計情報をサポートします。	Snort 3 を使用する FTD の場合、**show snort statistics** コマンドの出力で、フロー開始イベントとフロー終了イベントに関する統計情報が報告されるようになりました。

機能	説明
Web インターフェイスの変更：SecureX、脅威インテリジェンス、およびその他の統合。	

機能	説明
	バージョン 7.0.2 以降のバージョン 7.0.x メンテナンスリリースからアップグレードする場合、バージョン 7.1 では以下の FMC メニューオプションが変更されます。 （注） これらの変更は、バージョン 7.2 で元に戻ります。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [AMP] > [AMP管理（AMP Management）] [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [インテリジェンス（Intelligence）] > [ソース（Sources）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [インテリジェンス（Intelligence）] > [要素（Elements）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [インテリジェンス（Intelligence）] > [設定（Settings）] [統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）] は次に変更されまし [インテリジェンス（Intelligence）] > [インシデント（Incidents）]

機能	説明		
		た。	
	[統合（Integration）] > [その他の統合（Other Integrations）]	は次に変更されました。	**システム**（⚙） > [統合（Integration）]
	[統合（Integration）] > [セキュリティ分析とロギング（Security Analytics and Logging）]	は次に変更されました。	**システム**（⚙） > [ロギング（Logging）] > [セキュリティ分析とロギング（Security Analytics and Logging）]
	[統合（Integration）] > [SecureX]	は次に変更されました。	**システム**（⚙） > [SecureX]
FMC REST API			

機能	説明
FMC REST API サービス/操作。	

機能	説明
	新機能と既存の機能をサポートするために、複数の FMC REST API サービス/操作が追加されました。詳細については、Firepower Management Center REST API バージョン 7.1 クイックスタートガイド [英語] を参照してください。 新しい FMC REST API には次のものが含まれます。 • シャーシ管理：管理対象シャーシ、シャーシインターフェイス、ネットワークモジュール、およびブレークアウト インターフェイス用のシャーシ管理 API が追加されました。 • 展開：ジョブ履歴の API が追加されました。 • デバイスクラスタ：準備状況チェックを実行し、クラスタリングを変更するための API が追加されました。 • デバイス：次の API が追加されました。 • FTD インターフェイスの取得 • Packet Tracer • ルーティング • 仮想 LAN • 正常性：トンネル API が追加されました。 • オブジェクト：次の API が追加されました。 • 自律サービスパス • 拡張コミュニティ リスト • 拡張コミュニティ リスト • 拡張アクセス リスト • IPv4 プレフィックスリスト • IPv6 プレフィックスリスト • ポリシー リスト • ルート マップ • 標準アクセス リスト • 標準コミュニティ リスト • ポリシー：自動および手動の NAT ルールを変更するための API が追加されました。

機能	説明
	• ユーザー：Duo 設定を取得および変更するための API が追加されました。 • トラブルシューティング：パケットトレーサ PCAP 機能が追加されました。 • 更新：アップグレードを元に戻すための API が追加されました。 • ネットワークマップ：ホストと脆弱性のための API が追加されました。

FDM バージョン 7.1 の新機能

表 *9 : FDM* バージョン *7.1.0* の新機能

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 3100	Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新しい/変更された画面：**[Devices]** > **[Interfaces]** 新しい/変更された FTD コマンド： configure network speed、configure raid、show raid、show ssd
ASA 5508-X および 5516-X のサポートは終了します。サポートされる最後のリリースは FTD 7.0 です。	ASA 5508-X または 5516-X に FTDFTD 7.1 はインストールできません。これらのモデルで最後にサポートされるリリースは FTD 7.0 です。
ファイアウォールと IPS の機能	

機能	説明
Snort 3 のネットワーク分析ポリシー（NAP）設定。	Snort 3 の実行時に、FDM を使用してネットワーク分析ポリシー（NAP）を設定できます。ネットワーク分析ポリシーはトラフィック前処理検査を制御します。インスペクタは、トラフィックを正規化し、プロトコルの異常を識別することで、トラフィックがさらに検査されるように準備します。すべてのトラフィックに使用する NAP を選択し、ネットワークのトラフィックに最適な設定をカスタマイズできます。Snort 2 の実行中は NAP を設定できません。 [ポリシー（Policies）]>[侵入（Intrusion）] の設定ダイアログボックスにネットワーク分析ポリシーが追加されました。これには、直接の変更が可能な組み込み JSON エディタと、上書きをアップロードしたり、作成したものをダウンロードしたりするためのその他の機能があります。 >
変換後の宛先としての完全修飾ドメイン名（FQDN）オブジェクトの手動 NAT サポート。	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。
改善されたアクティブ認証アイデンティティルール。	ID ポリシールールのアクティブ認証を設定して、ユーザーの接続をデバイスに入力するインターフェイスの IP アドレスではなく、完全修飾ドメイン名（FQDN）にユーザーの認証をリダイレクトできます。FQDN は、デバイス上のいずれかのインターフェイスの IP アドレスに解決される必要があります。FQDN を使用すると、クライアントが認識するアクティブ認証用の証明書を割り当てることができます。これにより、IP アドレスにリダイレクトされたときにユーザに表示される信頼できない証明書の警告を回避できます。証明書では、FQDN、ワイルドカード FQDN、または複数の FQDN をサブジェクト代替名（SAN）に指定できます。 ID ポリシー設定に [ホスト名にリダイレクト（Redirect to Host Name）] オプションが追加されました。
VPN 機能	

機能	説明
サイト間 VPN のバックアップリモートピア	リモートバックアップピアを含めるようにサイト間 VPN 接続を設定できます。プライマリリモートピアが使用できない場合、システムはバックアップピアの 1 つを使用して VPN 接続を再確立しようとします。バックアップピアごとに個別の事前共有キーまたは証明書を設定できます。バックアップピアは、ポリシーベースの接続でのみサポートされ、ルートベース（仮想トンネルインターフェイス）の接続では使用できません。 バックアップピア設定を含むように、サイト間 VPN ウィザードを更新しました。
リモートアクセス VPN（MSCHAPv2）のパスワード管理。	リモートアクセス VPN のパスワード管理を有効にできます。これにより、AnyConnect はユーザーに期限切れのパスワードの変更を求めることができます。パスワード管理がない場合、ユーザーは AAA サーバーを使用して期限切れのパスワードを直接変更する必要があります。AnyConnect はユーザーにパスワードの変更を要求しません。LDAP サーバーの場合は、パスワードの有効期限が近づいていることをユーザーに通知する警告期間を設定することもできます。 リモートアクセス VPN 接続プロファイルの認証設定に [パスワード管理を有効にする（Enable Password Management）] オプションが追加されました。
AnyConnect VPN SAML 外部ブラウザ	リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。組み込みブラウザでは実行できない Web 認証方式（生体認証など）をサポートしたい場合も、このオプションを選択します。 リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。
管理およびトラブルシューティングの機能	

機能	説明
システムインターフェイスの完全修飾ドメイン名（FQDN）から IP アドレスへのマッピングを更新するためのダイナミック ドメイン ネーム システム（DDNS）のサポート。	ダイナミックアップデートを DNS サーバーに送信するように、システムのインターフェイスに DDNS を設定できます。これにより、インターフェイスに定義された FQDN が正しいアドレスに解決され、ユーザーが IP アドレスではなくホスト名を使用して簡単にシステムにアクセスできるようになります。これは、DHCP を使用してアドレスを取得するインターフェイスに特に役立ちますが、静的にアドレス指定されたインターフェイスにも役立ちます。 アップグレード後に FlexConfig を使用して DDNS を設定した場合は、変更を再度展開する前に、FDM または FTD API を使用して設定をやり直し、FlexConfig ポリシーから DDNS FlexConfig オブジェクトを削除する必要があります。 FDM を使用して DDNS を設定し、FMC 管理に切り替えると、DDNS 構成が保持され、FMC が DNS 名を使用してシステムを検索できるようになります。 FDM で、**[System Settings]** > **[DDNS Service]**ページが追加されました。FTD API で、DDNSService および DDNSInterfaceSettings リソースが追加されました。
デバイス CLI で、**dig** コマンドが **nslookup** コマンドに置き換わります。	デバイス CLI で完全修飾ドメイン名（FQDN）の IP アドレスを検索するには、**dig** コマンドを使用します。**nslookup** コマンドは削除されます。
FDM を使用した DHCP リレー構成。	FDM を使用して DHCP リレーを構成できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。 [システム設定（System Settings）] > [DHCP] > [DHCP リレー（DHCP Relay）] ページを追加し、DHCP サーバーを新しい DHCP 見出しの下に移動しました。 > >
FDM の自己署名証明書のキータイプとサイズ。	FDM で新しい自己署名内部および内部 CA 証明書を生成するときに、キータイプとサイズを指定できます。キータイプには、RSA、ECDSA、および EDDSA があります。許可されるサイズはキータイプによって異なります。推奨される最小長よりも小さいキーサイズの証明書をアップロードすると、警告が表示されるようになりました。また、可能な場合は置き換える必要がある脆弱な証明書を見つけるために役立つ、事前定義された脆弱キー検索フィルタもあります。

機能	説明
信頼できる CA 証明書の使用検証の制限。	信頼できる CA 証明書を使用して特定のタイプの接続を検証できるかどうかを指定できます。SSL サーバー（ダイナミック DNS で使用）、SSL クライアント（リモートアクセス VPN で使用）、IPsec クライアント（サイト間 VPN で使用）、または LDAPS などの Snort 検査エンジンによって管理されていないその他の機能の検証を許可または阻止できます。これらのオプションの主な目的は、特定の証明書に対して検証できるため、VPN 接続が確立されないようにすることです。 信頼できる CA 証明書のプロパティとして [検証の使用（Validation Usage）] が追加されました。
FDM での**管理者**パスワードの生成。	FDM での初期システム設定時、または FDM で**管理者**パスワードを変更するときに、ボタンをクリックしてランダムな 16 文字のパスワードを生成できるようになりました。
起動時間と tmatch コンパイルステータス。	**show version** コマンドには、システムの起動（ブート）にかかった時間に関する情報が含まれるようになりました。設定が大きいほど、システムの起動に時間がかかることに注意してください。 新しい **show asp rule-engine** コマンドは、tmatch コンパイルのステータスを表示します。Tmatch コンパイルは、アクセスグループ、NAT テーブル、およびその他のいくつかの項目として使用されるアクセスリストに使用されます。これは、非常に大きな ACL と NAT テーブルがある場合には、CPU リソースを消費し、進行中のパフォーマンスに影響を与える可能性がある内部プロセスです。コンパイル時間は、アクセスリスト、NAT テーブルなどのサイズによって異なります。
show access-list element-count 出力の拡張。	**show access-list element-count** コマンドの出力が拡張されました。オブジェクトグループ検索を有効にして使用すると、出力には要素数のオブジェクトグループの数に関する詳細が含まれます。 さらに、**show tech-support** 出力には **show access-list element-count** と **show asp rule-engine** からの出力が含まれます。

機能	説明
FDM を使用した FMC による管理のための FTD の構成	FDM を使用して初期設定を実行すると、管理および FMC アクセス設定に加えて、管理のために FMC に切り替えたときに、FDM で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。FTD CLI を使用すると、管理と FMC のアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。 FMC に切り替えると、FDM を使用して FTD を管理できなくなります。 新規/変更された画面：[システム設定（System Settings）]、[管理センター（Management Center）] >
FTD REST API バージョン 6.2（v6）。	ソフトウェアバージョン 7.1 用の FTD REST API はバージョン 6.2 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.2 の URL バージョンパス要素は、6.0/1 と同じ v6 である点に注意してください。 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、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。

バージョン 7.1 の新しいハードウェアと仮想プラットフォーム

表 *10* : バージョン *7.1.0* の新しいハードウェアと仮想プラットフォーム

機能	説明
Cisco Secure Firewall 3100	Cisco Secure Firewall 3110、3120、3130、および 3140 が導入されました。 ファイアウォールの電源が入っているときに、再起動することなく、同じタイプのネットワークモジュールをホットスワップできます。他のモジュールの変更を行う場合には、再起動が必要です。Secure Firewall 3100 25 Gbps インターフェイスは、Forward Error Correction と、インストールされている SFP に基づく速度検出をサポートします。SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 管理センターの展開では、これらのデバイスはスパンド EtherChannel クラスタリング用に最大 8 つのユニットをサポートします。 （注） バージョン 7.1.0 リリースには、これらのデバイスのオンラインヘルプが含まれていません。FMC の場合、新しいオンラインヘルプがバージョン 7.1.0.2 に含まれています。FDM の場合は、Cisco.com に掲載されているドキュメントを参照してください。将来のリリースに新しいオンラインヘルプを含める予定です。 これらのモデルに関連する画面と CLI コマンドについては、FMC バージョン 7.1 の新機能 （13 ページ）およびFDM バージョン 7.1 の新機能 （37 ページ）を参照してください。
AWS 用 FMCv300 OCI 用 FMCv300	AWS と OCI の両方に対応する FMCv300 が導入されました。FMCv300 は、最大 300 台のデバイスを管理できます。

機能	説明
AWS 用 FTDv のインスタンス。	AWS 用 FTDv により、次のインスタンスのサポートが追加されています。 • c5a.xlarge、c5a.2xlarge、c5a.4xlarge • c5ad.xlarge、c5ad.2xlarge、c5ad.4xlarge • c5d.xlarge、c5d.2xlarge、c5d.4xlarge • c5n.xlarge、c5n.2xlarge、c5n.4xlarge • i3en.xlarge、i3en.2xlarge、i3en.3xlarge • inf1.xlarge、inf1.2xlarge • m5.xlarge、m5.2xlarge、m5.4xlarge • m5a.xlarge、m5a.2xlarge、m5a.4xlarge • m5ad.xlarge、m5ad.2xlarge、m5ad.4xlarge • m5d.xlarge、m5d.2xlarge、m5d.4xlarge • m5dn.xlarge、m5dn.2xlarge、m5dn.4xlarge • m5n.xlarge、m5n.2xlarge、m5n.4xlarge • m5zn.xlarge、m5zn.2xlarge、m5zn.3xlarge • r5.xlarge、r5.2xlarge、r5.4xlarge • r5a.xlarge、r5a.2xlarge、r5a.4xlarge • r5ad.xlarge、r5ad.2xlarge、r5ad.4xlarge • r5b.xlarge、r5b.2xlarge、r5b.4xlarge • r5d.xlarge、r5d.2xlarge、r5d.4xlarge • r5dn.xlarge、r5dn.2xlarge、r5dn.4xlarge • r5n.xlarge、r5n.2xlarge、r5n.4xlarge • z1d.xlarge、z1d.2xlarge、z1d.3xlarge
Azure 用 FTDv のインスタンス。	Azure 用 FTDv により、次のインスタンスのサポートが追加されています。 • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2

新しい侵入ルールとキーワード

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が可能です。

侵入ルールを更新（SRU/LSP）すると、新規および更新された侵入ルールとプリプロセッサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。現在の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、SRU/LSP を更新しても、そのルールはインポートされません。

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。

Snort のバージョンを確認するには、互換性ガイドの「バンドルされたコンポーネント」の項を参照するか、次のコマンドのいずれかを使用します。

- FMC：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- FDM：**show summary** CLI コマンドを使用します。

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。

廃止された機能

FMC バージョン 7.1 で廃止された機能

表 *11 : FMC* バージョン *7.1.0* で廃止された機能

機能	アップグレードの影響	説明
侵入インシデントと侵入イベントクリップボード。	インシデントに関連するすべてのデータが削除されます。 クリップボードをデータソースとして使用するレポート テンプレート セクションは削除されます。	バージョン 7.1 では、侵入インシデント機能と関連する侵入イベントクリップボードが削除されています。 廃止された画面/オプション： • [分析（Analysis）] > [侵入（Intrusions）] > [インシデント（Incidents）] • [分析（Analysis）] > [侵入（Intrusions）] > [クリップボード（Clipboard）] • 侵入イベントワークフローページおよびパケットビューでの [コピー（Copy）] および [すべてコピー（Copy All）] • レポートテンプレートにセクションを追加する場合（[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）]）、データソースとして [クリップボード（Clipboard）] テーブルを選択できなくなりました。
侵入イベントのカスタムテーブル。	侵入イベントテーブルのフィールドを含むカスタムテーブルは削除されます。	バージョン 7.1 では、侵入イベントのカスタムテーブルのサポートが終了します。 カスタムテーブルにフィールドを追加する場合（[分析（Analysis）] > [詳細設定（Advanced）] > [カスタムテーブル（Custom Tables）]）、データソースとして [侵入イベント（Intrusion Events）] テーブルを選択できなくなりました。

機能	アップグレードの影響	説明
SecureX との統合、SecureX とのオーケストレーションの改善	バージョン 7.0.2 以降でこの機能を新たに有効にした場合、バージョン 7.1 にアップグレードできません。	バージョン 7.1 では、バージョン 7.0.2 で導入された SecureX との統合およびオーケストレーションの改善を一時的に中止します。 バージョン 7.0.2 またはそれ以降のメンテナンスリリースで SecureX との統合を新たに有効にした場合は、バージョン 7.1 にアップグレードする前に、この機能を無効にする必要があります。アップグレードが正常に完了したら、以前の方法を使用して、この機能を再度有効にできます。 バージョン 7.0.0 または 7.0.1 で SecureX との統合を有効にした場合は、アップグレードの際に問題は発生しません。
地理位置情報の詳細。	なし。これは日付ベースで廃止予定です。	2022 年 5 月、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 新しい国コードパッケージのファイル名は、古いオールインワンパッケージと同じ（Cisco_GEODB_Update-*date-build*）です。これにより、バージョン 7.1 以前を実行している環境では、引き続き GeoDB の更新プログラムを取得できます。GeoDB 更新プログラムを手動でダウンロードする場合（エアギャップ展開など）、IP パッケージではなく、必ず国コードパッケージを取得してください。 **重要** この分割による地理位置情報ルールやトラフィック処理への影響はありません。これらのルールは、国コードパッケージのデータのみに依存しています。ただし、オールインワンパッケージは原則的に国コードパッケージに置き換えられるため、コンテキストデータは更新されなくなり、陳腐化されます。最新のデータを取得するには、FMC をバージョン 7.2 以降にアップグレードするか再イメージ化して、GeoDB を更新します。

機能	アップグレードの影響	説明
NGIPS ソフトウェア（ASA FirePOWER、NGIPSv）。	アップグレードは禁止されています。	バージョン 7.1 は、FMC および FTD デバイスでのみサポートされます。ASA FirePOWER または NGIPSv デバイスではサポートされていません。 バージョン 7.1 の FMC を引き続き使用して、バージョン 6.5 ～ 7.0 を実行している古いデバイス（FTD、ASA FirePOWER および NGIPSv）を管理できます。

バージョン 7.1 で廃止されたハードウェアと仮想プラットフォーム

表 *12 :* バージョン *7.1.0* で廃止されたハードウェアと仮想プラットフォーム

機能	説明
ASA 5508-X および 5516-X	ASA 5508-X または 5516-X ではバージョン 7.1 以降を実行できません。
FMC 1000、2500、4500	FMC モデルの FMC 1000、2500、および 4500 ではバージョン 7.1 以降を実行できません。これらの FMC を使用してバージョン 7.1 以降のデバイスを管理することはできません。

廃止された FlexConfig コマンド

このドキュメントでは、今回のリリースで廃止された FlexConfig のオブジェクトおよびコマンドと、その他の廃止された機能が記載されています。FlexConfig が導入されたときに禁止されたコマンドを含む、禁止されたコマンドと以前のリリースで廃止になった機能の完全なリストについては、コンフィギュレーション ガイドを参照してください。

⚠

注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

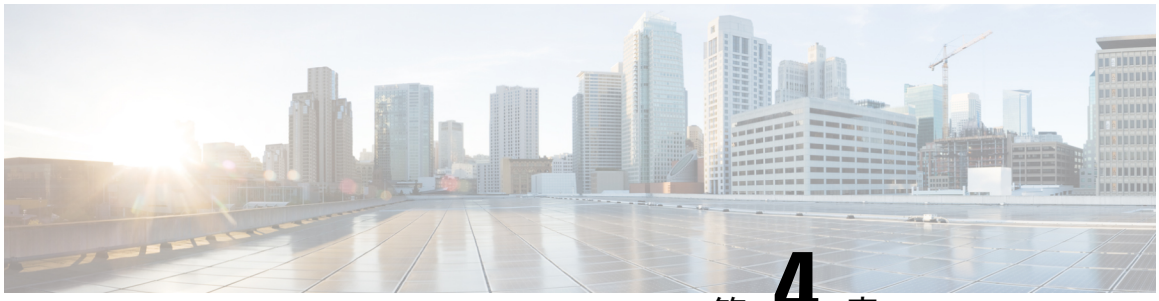
FlexConfig について

いくつかの FTD の機能は、ASA 設定コマンドを使用して設定されます。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。

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。ご使用の構成は自動的に変換されません。アップグ

レード後は、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ません。

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。



第 4 章

ソフトウェアのアップグレード

このドキュメントには、バージョン 7.1 の重要なリリース固有のアップグレードガイドラインが記載されていますが、

重要 ここに記載されているガイドラインに加えて、以下の内容も確認する必要があります。

- 未解決のバグおよび解決されたバグ （73 ページ）：アップグレードに影響するバグを回避する準備を整えます。アップグレードでバージョンがスキップされる場合は、未解決および解決済みのバグについてのリリースノートを参照するか、Cisco バグ検索ツールを使用してください。
- 特長と機能 （13 ページ）：新規および廃止された機能が原因で、アップグレード前またはアップグレード後の設定変更が必要になったり、アップグレードができなかったりする場合があります。アップグレードでバージョンがスキップされる場合は、リリースノートで履歴情報とアップグレードの影響を確認するか、該当する『New Features by Release』のガイドを参照してください。

アップグレードの計画

誤りを避けるには、注意深い計画と準備が役立ちます。この表はアップグレードの計画プロセスを要約したものです。詳細なチェックリストと手順については、該当するアップグレードガ

イドとコンフィギュレーション ガイド（http://www.cisco.com/go/threatdefense-71-docs）を参照してください。

表 *13*：アップグレードの計画フェーズ

計画フェーズ	次を含む
計画と実現可能性	展開を評価します。 アップグレードパスを計画します。 すべてのアップグレードガイドラインを読み、設定の変更を計画します。 アプライアンスへのアクセスを確認します。 帯域幅を確認します。 メンテナンス時間帯をスケジュールします。
バックアップ	ソフトウェアをバックアップします。 Firepower 4100/9300 の FXOS をバックアップします。
アップグレードパッケージ	アップグレードパッケージをシスコからダウンロードします。 システムにアップグレードパッケージをアップロードします。
関連するアップグレード	仮想展開内で仮想ホスティングをアップグレードします。 Firepower 4100/9300 の FXOS をアップグレードします。
最終チェック	設定を確認します。 NTP 同期を確認します。 ディスク容量を確認します。 設定を展開します。 準備状況チェックを実行します。 実行中のタスクを確認します。 展開の正常性と通信を確認します。

アップグレードする最小バージョン

次のように バージョン 7.1 に直接アップグレードできます。

表 *14* : バージョン *7.1* 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
FMC	6.5
FTD	6.5 Firepower 4100/9300 には FXOS 2.11.1.154 が必要です。ほとんどの場合、各メジャーバージョンで最新の FXOS ビルドを使用することを推奨します。判断のヒントについては、Cisco Firepower 4100/9300 FXOS 2.11(1) リリースノートを参照してください。

パッチを適用する最小バージョン

バージョン 7.1 にパッチを適用する場合、パッチは 4 桁目のみを変更することに注意してください。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。

バージョン 7.1 のアップグレードガイドライン

以下のチェックリストでは、該当する可能性のある新規アップグレードガイドラインや以前に公開されたアップグレードガイドラインを提供します。

表 *15* : *FMC* を使用した *FTD* のアップグレードガイドラインバージョン *7.1*

✓	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
	アップグレードする最小バージョン （52 ページ）	任意（Any）	任意（Any）	任意（Any）
	FXOS のアップグレードガイドライン （57 ページ）	Firepower 4100/9300	任意（Any）	任意（Any）
	アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0 （54 ページ）	任意（Any）	7.0.4 以降	7.1.0 のみ
	高可用性 FMC の Cisco Secure Malware Analytics に再接続する （54 ページ）	FMC	6.4.0 ～ 6.7.x	7.0 以上
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID （55 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 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
	FMCv には 28 GB の RAM が必要（55 ページ）	FMCv	6.2.3 ～ 6.5.0.x	6.6 以降

表 *16 : FDM* を使用した *FTD* のアップグレードガイドラインバージョン *7.1*

✓	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
	アップグレードする最小バージョン（52 ページ）	任意（Any）	任意（Any）	任意（Any）
	FXOS のアップグレードガイドライン（57 ページ）	Firepower 4100/9300	任意（Any）	任意（Any）
	アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0（54 ページ）	任意（Any）	7.0.4 以降	7.1.0 のみ
	アップグレードの失敗：Firepower 1010 スイッチポートでの無効な VLAN ID（55 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 以降

アップグレード禁止：バージョン 7.0.4 以降から バージョン 7.1.0

展開：すべて

アップグレード元：バージョン 7.0.4 以降のメンテナンスリリース

直接アップグレード先：バージョン 7.1.0 のみ

データストアの非互換性のため、をバージョン 7.0.4 以降からバージョン 7.1.0 にアップグレードすることができません。バージョン 7.2 以降に直接アップグレードすることをお勧めします。

高可用性 FMC の Cisco Secure Malware Analytics に再接続する

展開：動的分析のためにファイルを送信する高可用性/AMP for Networks（マルウェア検出）展開

アップグレード元：バージョン 6.4.0 ～ 6.7.x

直接アップグレード先：バージョン 7.0.0 以降

関連するバグ： CSCvu35704

バージョン 7.0.0 では、フェールオーバー後にシステムが動的分析用のファイルの送信を停止する高可用性の問題が修正されています。修正を有効にするには、Cisco Secure Malware Analytics パブリッククラウドに再度関連付ける必要があります。

高可用性ペアをアップグレードした後、プライマリ FMC で次の手順を実行します。

1. **[AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。
2. パブリッククラウドに対応するテーブル行で、 [関連付け（Associate）] をクリックします。

   ポータルウィンドウが開きます。サインインする必要はありません。再関連付けは、数分以内にバックグラウンドで行われます。

アップグレードの失敗：Firepower1010スイッチポートでの無効なVLAN ID

展開：Firepower 1010

アップグレード元：バージョン 6.4 ～ 6.6

直接アップグレード先：バージョン 6.7 以降

Firepower 1010 では、VLAN ID を 3968 ー 4047 の範囲にしてスイッチポートを設定した場合、FTD のバージョン 6.7 以降へのアップグレードは失敗します。これらの ID は内部使用専用です。

FMCv には 28 GB の RAM が必要

展開：FMCv

アップグレード元：バージョン 6.2.3 ～ 6.5

直接アップグレード先：バージョン 6.6 以降

すべての FMCv 実装には同じ RAM 要件が適用され、32 GB が推奨、28 GB が必須となりました（FMCv 300 の場合は 64 GB）。仮想アプライアンスに割り当てられたメモリが 28 GB 未満の場合、バージョン 6.6 以降へのアップグレードは失敗します。アップグレード後、メモリ割り当てを引き下げると、正常性モニターがアラートを発行します。

これらの新しいメモリ要件は、すべての仮想環境にわたって一貫した要件を適用し、パフォーマンスを向上させ、新しい機能を利用できるようにします。デフォルト設定を引き下げないことをお勧めします。使用可能なリソースによっては、パフォーマンスを向上させるために仮想アプライアンスのメモリと CPU の数を増やすことができます。詳細については、Cisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。

（注） バージョン 6.6.0 リリースの時点で、クラウドベースの FMCv の展開（AWS、Azure）でのメモリ不足インスタンスのタイプが完全に廃止されました。以前のバージョンであっても、これらを使用して新しいインスタンスを作成することはできません。既存のインスタンスは引き続き実行できます。

次の表に、メモリが不足している展開のアップグレード前の要件を示します。

表 *17* : バージョン *6.6* 以降 にアップグレードする場合の *FMCv* のメモリ要件

プラットフォーム	アップグレード前のアクション	詳細
VMware	28 GB 以上（推奨 32 GB）を割り当てます。	最初に仮想マシンの電源をオフにします。 手順については、VMware のマニュアルを参照してください。
KVM	28 GB 以上（推奨 32 GB）を割り当てます。	手順については、ご使用の KVM 環境のマニュアルを参照してください。
AWS	インスタンスのサイズを変更します。 • c3.xlarge から c3.4xlarge へ。 • c3.2.xlarge から c3.4xlarge へ。 • c4.xlarge から c4.4xlarge へ。 • c4.2xlarge から c4.4xlarge へ。 また、新規展開用に c5.4xlarge インスタンスも用意しています。	サイズを変更する前にインスタンスを停止します。これを行うと、インスタンスストアのボリューム上のデータが失われるため、最初にインスタンスストアによってバックアップされたインスタンスを最初に移行してください。さらに、管理インターフェイスに復元力のある IP アドレスがない場合は、そのパブリック IP アドレスが解放されます。 手順については、Linux インスタンスの AWS ユーザーガイドのインスタンスタイプの変更に関するマニュアルを参照してください。
Azure	インスタンスのサイズを変更します。 • Standard_D3_v2 から Standard_D4_v2 へ。	Azure ポータルまたは PowerShell を使用します。サイズを変更する前にインスタンスを停止する必要はありませんが、停止すると追加のサイズが表示される場合があります。サイズ変更により、実行中の仮想マシンが再起動されます。 手順については、Windows VM のサイズ変更に関する Azure のマニュアルを参照してください。

バージョン 7.1 パッチのアップグレードガイドライン

以下のチェックリストでは、該当する可能性のあるパッチのアップグレードガイドラインを提供します。

表 *18 : FMC* バージョン *7.1* パッチのアップグレードガイドライン

✓	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
	アップグレードする最小バージョン （52 ページ）	任意（Any）	任意（Any）	任意のパッチ
	アンインストールに対応するパッチ （59 ページ）	任意（Any）	任意（Any）	任意のパッチ

表 *19 : FDM* バージョン *7.1* パッチのアップグレードガイドライン

✓	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
	アップグレードする最小バージョン （52 ページ）	任意（Any）	任意（Any）	任意のパッチ

FXOS のアップグレードガイドライン

Firepower 4100/9300 の場合、FTD のメジャーアップグレードには FXOS のアップグレードも必要です。FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。シスコではこれらの組み合わせの拡張テストを実施するため、可能な限りこれらの組み合わせを使用してください。メンテナンスリリースとパッチで FXOS のアップグレードが必要になることはほとんどありませんが、最新の FXOS ビルドにアップグレードして、解決済みの問題を有効に活用できます。

重要なリリース固有のアップグレードガイドライン、新機能および廃止された機能、未解決のバグおよび解決済みのバグについては、Cisco Firepower 4100/9300 FXOS リリースノート を参照してください。

FTD をアップグレードするために必要な FXOS の最小バージョン

バージョン 7.1 を実行するために必要な FXOS の最小バージョンは、FXOS 2.11.1.154 です。

FXOS をアップグレードするために必要な FXOS の最小バージョン

FXOS 2.2.2 から、それ以降の任意の FXOS バージョンにアップグレードできます。

FXOS アップグレードの所要時間

FXOS のアップグレードには最長 45 分かかることがあり、トラフィックフローやインスペクションに影響を与える場合があります。詳細については、FXOS のアップグレードでのトラフィックフローとインスペクション （60 ページ）を参照してください。

応答しないアップグレード

アップグレード中は、設定の変更の実施または展開を行わないでください。システムが非アクティブに見えても、アップグレード中は手動で再起動またはシャットダウンしないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。

応答しない FMC

進行中のアップグレードは再開しないでください。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。

応答しない FTD のアップグレード

メジャーアップグレードやメンテナンスアップグレードでは、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセルし、失敗したアップグレードを再試行できます。

- FMC：[デバイス管理（Device Management）] ページおよびメッセージセンターからアクセスできる [アップグレードステータス（Upgrade Status）] ポップアップを使用します。
- FDM：[システムアップグレード（System Upgrade）] パネルを使用します。

FTD CLI を使用することもできます。

（注） デフォルトでは、FTD はアップグレードが失敗すると自動的にアップグレード前の状態に復元されます（「自動キャンセル」）。失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、アップグレードを開始するときに自動キャンセルオプションを無効にします。パッチの自動キャンセルはサポートされていません。高可用性または拡張性の展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。

この機能は、パッチまたはバージョン 6.6 以前からのアップグレードではサポートされていません。

アップグレードを元に戻すまたはアンインストールする

アップグレードに成功したにもかかわらず、システムが期待どおりに機能しない場合は、復元またはアンインストールが可能な場合があります。

- メジャーおよびメンテナンスアップグレードを FTD に復元することができます。
- アンインストールは、FMC を搭載した FTD へのパッチが対象です。FMC パッチをアンインストールすることもできます。

これらの方法のいずれも機能しない場合、以前のバージョンに戻すには、イメージを再作成する必要があります。ホットフィックスでは、復元もアンインストールもサポートされていないことに注意してください。 手順については、復元先のバージョンではなく、現在実行しているバージョンのアップグレードガイドを参照してください。

アンインストールに対応するパッチ

特定のパッチをアンインストールすると、アンインストールが成功した場合でも、問題が発生する可能性があります。次のような問題があります。

- アンインストール後に設定変更を展開できない
- オペレーティングシステムと ソフトウェアの間に互換性がなくなる
- セキュリティ認定コンプライアンスが有効な状態（CC/UCAPL モード）でそのパッチが適用されていた場合、アプライアンスの再起動時に FSIC（ファイル システム整合性チェック）が失敗する

⚠

注意 セキュリティ認定の遵守が有効な場合に FSIC が失敗すると、ソフトウェアは起動せず、リモート SSH アクセスが無効になるため、ローカルコンソールを介してのみアプライアンスにアクセスできます。この問題が発生した場合は、Cisco TACにお問い合わせください。

アンインストールに対応したバージョン 7.1 のパッチ

現在、すべてのバージョン 7.1 パッチがアンインストールに対応しています。

トラフィック フローとインスペクション

デバイスのアップグレードにより、トラフィックフローとインスペクションが影響を受けます。影響が最も少ない時間帯にメンテナンス期間をスケジュールします。

FXOS のアップグレードでのトラフィックフローとインスペクション

FXOS をアップグレードするとシャーシが再起動します。高可用性や拡張性を導入する場合でも、各シャーシの FXOS を個別にアップグレードします。中断を最小限に抑えるには、1 つずつシャーシをアップグレードします。

表 *20 :* トラフィックフローとインスペクション：*FXOS* のアップグレード

導入	トラフィックの挙動	メソッド
スタンドアロン	廃棄	—
高可用性	影響なし。	**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。
	1 つのピアがオンラインになるまでドロップされる。	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。
シャーシ間クラスタ	影響なし。	**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。
	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。	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。
シャーシ内クラスタ（FirePOWER 9300 のみ）	検査なしで受け渡される。	ハードウェアバイパス有効：[Bypass: Standby] または [Bypass-Force]。
	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。	ハードウェアバイパス無効：[Bypass: Disabled]。
	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。	ハードウェア バイパス モジュールなし。

FMC を使用した FTD アップグレードのトラフィックフローとインスペクション

スタンドアロンデバイスでのソフトウェアのアップグレード

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。アップグレードの開始時にメンテナンスモードを開始すると、トラフィック インスペクションが 2 ー 3 秒中断します。イ

ンターフェイスの構成により、その時点とアップグレード中の両方のスタンドアロンデバイスによるトラフィックの処理方法が決定されます。

表 *21* : トラフィックフローとインスペクション：スタンドアロンデバイスでのソフトウェアのアップグレード

インターフェイス コンフィギュレーション		トラフィックの挙動
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。	廃棄 ISA 3000 のブリッジ グループ インターフェイスの場合に限り、FlexConfig ポリシーを使用して、停電時のハードウェアバイパスを設定できます。これにより、ソフトウェアのアップグレード中にトラフィックのドロップが発生しますが、デバイスがアップグレード後の再起動中、インスペクションなしでトラフィックが通過します。
IPS のみのインターフェイス	インラインセット、ハードウェアバイパス強制が有効：[バイパス（Bypass）]：[強制（Force）]	ハードウェアバイパスを無効にするか、スタンバイモードに戻すまで、インスペクションなしで合格。
	インラインセット、ハードウェアバイパスがスタンバイモード：[バイパス（Bypass）]：[スタンバイ（Standby）]	デバイスがメンテナンスモードの場合、アップグレード中にドロップされます。その後、デバイスがアップグレード後の再起動を完了する間、インスペクションなしで合格します。
	インラインセット、ハードウェアバイパスが無効：[バイパス（Bypass）]：[無効（Disabled）]	廃棄
	インラインセット、ハードウェア バイパス モジュールなし。	廃棄
	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。

高可用性および拡張性に関するソフトウェアのアップグレード

高可用性デバイスやクラスタ化されたデバイスのアップグレード中に、トラフィックフローや検査が中断されることはありません。高可用性ペアの場合、スタンバイ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。

クラスタの場合、データ セキュリティ モジュールを最初にアップグレードして、その後コントロールモジュールをアップグレードします。コントロール 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。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

たとえ高可用性および拡張性を備えた環境でも、復元時のトラフィックフローとインスペクションの中断を予測する必要があります。これは、すべてのユニットを同時に復元させたほうが、復元がより正常に完了するためです。同時復元とは、すべてのデバイスがスタンドアロンであるかのように、トラフィックフローと検査の中断がインターフェイスの設定のみに依存することを意味します。

ソフトウェアのアンインストール（パッチ）

スタンドアロンデバイスの場合、パッチのアンインストール中のトラフィックフローと検査の中断は、アップグレードの場合と同じになります。高可用性および拡張性の展開では、中断を最小限に抑えるために、アンインストールの順序を明確に計画する必要があります。これは、ユニットとしてアップグレードしたデバイスであっても、デバイスから個別にパッチをアンインストールするためです。

設定変更の導入

Snort プロセスを再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。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。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

表 *22:* トラフィックフローとインスペクション：設定変更の展開

インターフェイス コンフィギュレーション		トラフィックの挙動
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。	廃棄
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。	検査なしで受け渡される。 [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	廃棄
	インライン、[Snortフェールオープン：ダウン（Snort Fail Open: Down）]：有効	検査なしで受け渡される。
	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。

FDM を使用した FTD アップグレードのトラフィックフローとインスペクション

ソフトウェアのアップグレード

アップグレード中にトラフィックがドロップされます。高可用性の展開では、デバイスを1つずつアップグレードすることで、中断を最小限に抑えることができます。

ISA 3000 の場合にのみ、電源障害に対するハードウェアバイパスを設定すると、トラフィックはアップグレード中にドロップされますが、デバイスのアップグレード後の再起動中に検査なしでトラフィックが渡されます。

ソフトウェアの復元（メジャーおよびメンテナンスリリース）

復元中にトラフィックがドロップされます。高可用性の展開では、両方のユニットを同時に復元すると、復元が成功する可能性が高くなります。最初のユニットがオンラインに戻ると、トラフィックフローとインスペクションが再開されます。

設定変更の導入

Snort プロセスを再起動すると、高可用性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

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。

時間とディスク容量のテスト

参考のために、FMC およびソフトウェアのアップグレードにかかる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

特定のプラットフォームおよびシリーズでテストされたすべてのソフトウェアアップグレードの中で最長のテスト時間を報告します。次の表で説明するように、アップグレードには、複数の理由により、指定された時間よりも時間がかかる可能性があります。将来のベンチマークとして使用できるように、独自のアップグレード時間を追跡および記録することをお勧めします。

注意 アップグレード中は、設定を変更または展開しないでください。システムが非アクティブに見えても、手動で再起動またはシャットダウンしないでください。ほとんどの場合、進行中のアップグレードを再開しないでください。システムが使用できない状態になり、再イメージ化が必要になる場合があります。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応答しないアップグレード （58 ページ） を参照してください。

表 *23*：ソフトウェアアップグレードの時間テストの条件

条件	詳細
配置	デバイスアップグレードの時間は、FMC展開でのテストに基づいています。同様の条件の場合、リモートとローカルの管理対象デバイスの raw アップグレード時間は類似しています。

条件	詳細
バージョン	メジャーリリースおよびメンテナンスリリースでは、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。アップグレードでバージョンがスキップされると、通常、アップグレード時間は長くなります。
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。
仮想アプライアンス	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。ただし、仮想展開でのアップグレード時間はハードウェアに大きく依存することに注意してください。
高可用性/拡張性	特に断りのない限り、スタンドアロンデバイスでテストします。 高可用性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。
設定	シスコでは、構成およびトラフィック負荷が最小限のアプライアンスでテストを行います。 アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、また、それらがアップグレードから影響を受けるかどうか、受ける場合はどのような影響を受けるかにより、長くなる場合があります。たとえば多くのアクセス制御ルールを使用している場合、アップグレードはこれらのルールの格納方法をバックエンドで変更する必要があるため、アップグレードにはさらに長い時間がかかります。
コンポーネント	ソフトウェアアップグレード自体とその後の再起動のみの時間を報告します。これには、オペレーティングシステムのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB および侵入ルール （SRU/LSP）の更新、または設定の展開のための時間は含まれません。

ディスク容量テスト

特定のプラットフォーム/シリーズでテストされたすべてのソフトウェアアップグレードの中で最も多く使用されているディスク容量を報告します。これには、アップグレードパッケージをデバイスにコピーするために必要な容量が含まれます。

また、デバイス アップグレード パッケージ用に FMC（/Volume または /var 内）に必要な容量も報告します。FTD アップグレードパッケージ用の内部サーバーがある場合、または FDM を使用している場合は、それらの値を無視してください。

特定の場所（/var や /ngfw など）のディスク容量の見積もりを報告する場合、その場所にマウントされているパーティションのディスク容量の見積もりを報告しています。一部のプラットフォームでは、これらの場所が同じパーティション上にある場合があります。

空きディスク容量が十分でない場合、アップグレードは失敗します。

表 *24 :* ディスク容量の確認

プラットフォーム	コマンド
FMC	**[システム（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、FMC を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FTD with FMC	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
FTD with FDM	**show disk** CLI コマンドを使用します。

バージョン 7.1.0.2 の時間とディスク容量

表 *25 :* バージョン *7.1.0.2* 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	アップグレード時間	リブート時間
FMC	/var 内で 2.0 GB	/ 内で 19 MB	—	20 分	4 分
FMCv：VMware	/var 内で 2.5 GB	/ 内で 14 MB	—	21 分	[1 分（1 min）]
Secure Firewall 3100 シリーズ	—	/ngfw 内で 3.2 GB		4 分	46 分

バージョン 7.1.0.1 の時間とディスク容量

表 *26 :* バージョン *7.1.0.1* 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	アップグレード時間	リブート時間
FMC	/var 内で 2.0 GB	/ 内で 19 MB	—	18 分	8 分
FMCv：VMware	/var 内で 2.2 GB	/ 内で 14 MB	—	21 分	4 分
Firepower 1000 シリーズ	—	/ngfw 内で 5.6 GB	430 MB	10 分	11 分

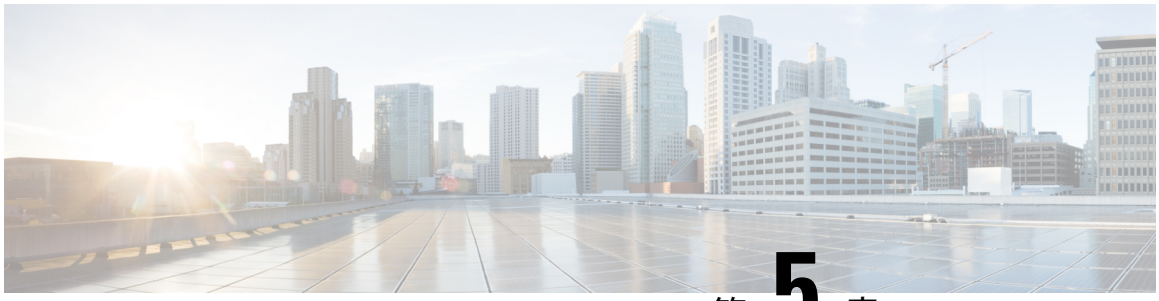
プラットフォーム	ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
Firepower 2100 シリーズ	—	/ngfw 内で 5.6 GB	420 MB	10 分	10 分
Firepower 4100 シリーズ	—	/ngfw 内で 5.6 GB	430 MB	7 分	7 分
Firepower 4100 シリーズ コンテナ インスタンス	—	/ngfw 内で 5.6 GB	430 MB	6 分	4 分
Firepower 9300	—	/ngfw 内で 5.1 GB	430 MB	7 分	8 分
ISA 3000	/ngfw/var 内で 2.0 GB	/ngfw/bin 内で 240 MB	430 MB	4 分	13 分
FTDv：VMware	/ngfw/var 内で 1.5 GB	/ngfw/bin 内で 240 MB	430 MB	4 分	4 分

バージョン 7.1.0 の時間とディスク容量

表 *27 :* バージョン *7.1.0* 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	アップグレード時間	リブート時間
FMC		/var 内で 16.9 GB	/ 内で 43 MB	—	33 分	15 分
FMCv：VMware		/var 内で 17 GB	/ 内で 50 MB で	—	34 分	5 分
Firepower 1000 シリーズ		—	/ngfw 内で 8.2 GB	930 MB	16 分	11 分
Firepower 2100 シリーズ		—	/ngfw 内で 8.3 GB	1 GB	13 分	13 分
Firepower 4100 シリーズ		—	/ngfw 内で 8.6 GB	870 MB	15 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 8.6 GB	870 MB	16 分	8 分
Firepower 9300		—	/ngfw 内で 11.2 GB	870 MB	11 分	12 分
ISA 3000	バージョン 6.5.0 ～ 6.6.0	/home 内で 9.3 GB	/ngfw 内で 256 KB	1 GB	21 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 9.3 GB	/ngfw 内で 270 KB			
	バージョン 7.0.0	/ngfw/var 内で 9.2 GB	/ngfw/bin 内で 260 KB			

プラットフォーム		ボリュームの容量	必要容量	FMC の容量	アップグレード時間	リブート時間
FTDv：VMware	バージョン 6.5.0 ～ 6.6.0	/home 内で 4.6 GB	/ngfw 内で 925 KB	1 GB	11 分	6 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.4 GB	/ngfw 内で 210 KB			
	バージョン 7.0.0	/ngfw/var 内で 5.3 GB	/ngfw/bin 内で 220 KB			



第 5 章

ソフトウェアのインストール

バージョン7.1にアップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。これは再イメージ化とも呼ばれます。

パッチ用のインストールパッケージは提供していません。特定のパッチを実行するには、適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。

- 設置に関するガイドライン （69 ページ）
- 設置ガイド （72 ページ）

設置に関するガイドライン

以下のガイドラインにより再イメージ化の一般的な問題を防ぐことができますが、包括的な解決策ではありません。詳細なチェックリストと手順については、該当するインストールガイドを参照してください。

バックアップ

再イメージ化の前に、安全なリモートロケーションにバックアップし、正常に転送されたことを確認することを強く推奨します。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。

（注） アップグレードを不要にするため再イメージ化したい場合、バージョンの制約によっては、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。

アプライアンス アクセス

アプライアンスに物理的にアクセスできない場合、現在のメジャーリリースまたはメンテナンスリリースへの再イメージ化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や以前のリリースに再イメージ化する場合は、アプライアンスに物理的にアクセスできる必要があります。Lights-Out 管理（LOM）を使用することはできません。

デバイスに関して、ユーザー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 の展開では、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。

Smart Software Manager からのの登録解除

アプライアンスまたはスイッチデバイス管理のイメージを再作成する前に、Cisco Smart Software Manager（CSSM） での登録解除が必要になる場合があります。これは、再登録を妨げる可能性のある孤立した権限付与の発生を避けるためです。

登録を解除すると、仮想アカウントからアプライアンスが削除され、クラウドおよび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。

バックアップから復元する予定がある場合は、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手動で元に戻します。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。

表 *28 : CSSM* からの登録解除シナリオ（バックアップから復元しない）

シナリオ	アクション
FMC を再イメージ化します。	手動で登録解除します。
FMC のモデルを移行します。	ソースのFMC をシャットダウンする前に、手動で登録を解除します。
FMC で FTD を再イメージ化します。	FMC からデバイスを削除すると、自動的に登録が解除されます。
FDM で FTD を再イメージ化します。	手動で登録解除します。
FMC からデバイスマネージャーに FTD を切り替えます。	FMC からデバイスを削除すると、自動的に登録が解除されます。
デバイスマネージャーから FMC に FTD を切り替えます。	手動で登録解除します。

管理からデバイスを削除します。

FMC の展開で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、FMC からデバイスを削除します。バックアップからの復元を予定している場合は、これを行う必要はありません。

表 *29*：管理からデバイスを削除するシナリオ（バックアップから復元しない）

シナリオ	アクション
FMC を再イメージ化します。	管理からデバイスを削除します。
FTD を再イメージ化します。	管理から任意のデバイスを削除します。
デバイスマネージャーから FMC に FTD を切り替えます。	管理から任意のデバイスを削除します。

FXOS をダウングレードするための FTD ハードウェアの完全な再イメージ化

FXOS オペレーティングシステムを使用する FTD ハードウェアモデルの場合、以前のソフトウェアバージョンに再イメージ化するには、FXOS がソフトウェアにバンドルされているか、個別にアップグレードされているかに関係なく、完全な再イメージ化が必要になる場合があります。

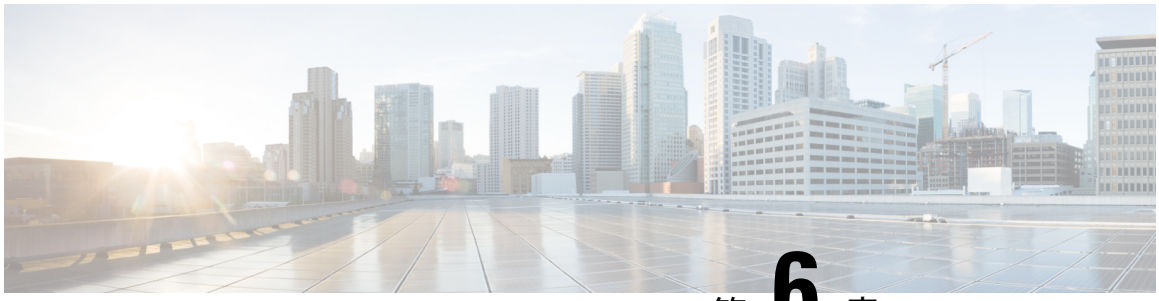
表 *30*：完全な再イメージ化のシナリオ

モデル	詳細
Firepower 2100 シリーズ Secure Firewall 3100 シリーズ	**erase configuration** メソッドを使用してイメージを再作成すると、FXOS がソフトウェアとともにダウングレードされ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。これらのデバイスの完全な再イメージ化を実行することを推奨します。
Firepower 4100/9300	FTD を復元しても FXOS はダウングレードされません。 Firepower 4100/9300 の場合、FTD のメジャーバージョンには特別に認定および推奨されている付随の FXOS バージョンがあります。FTD の以前のバージョンに戻った後、推奨されていないバージョンの FXOS（新しすぎる）を実行している可能性があります。 新しいバージョンの FXOS は旧バージョンの FTD と下位互換性がありますが、シスコでは推奨の組み合わせについて拡張テストを実施しています。FXOS を手動ではダウングレードできないため、このような状況下で推奨の組み合わせを稼働するには、完全な再イメージ化が必要になります。

設置ガイド

表 *31* : 設置ガイド

プラットフォーム	ガイド
FMC	
FMC 1600、2600、4600	Cisco Firepower Management Center 1600、2600、4600 スタートアップガイド
FMCv	Cisco Secure Firewall Management Center Virtual 入門ガイド
FTD	
Firepower 1000/2100	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイド
Cisco Secure Firewall 3100	Cisco Secure Firewall 3100 スタートアップガイド
Firepower 4100/9300	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』
ISA 3000	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド
FTDv	Cisco Secure Firewall Threat Defense Virtual スタートアップガイド



第 6 章

未解決のバグおよび解決されたバグ

利便性を考え、このドキュメントにはバージョン 7.1 の未解決のバグと解決済みのバグの一覧を記載しています。

重要 バグリストは 1 回自動生成され、その後は更新されません。バグ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。メンテナンスリリースまたはパッチの未解決のバグも記載していません。サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。

バージョン 7.1 で未解決のバグ

バージョン 7.1.0 で未解決のバグ

表 *32* : バージョン *7.1.0* で未解決のバグ

不具合 ID	タイトル
CSCvz38976	7.1/Firepower Threat Defense デバイスが大規模なパケットを転送できないことがある/フラグメント化の失敗
CSCvz83796	複数のシスコ製品が Snort ルールでの SMBv2 に対するサービス妨害の脆弱性の影響を受ける
CSCvz96487	認証条件のある SSL ルールにより、予期しないハンドシェイクエラーが発生することがある
CSCwa23353	レートフィルタを 7.1 FMCv の管理下にある 7.0.1 FTDv に展開すると、サポートされていない設定として表示される

不具合 ID	タイトル
CSCwa33452	7.1.0/7.2.0 の回帰中に Azure D5 で FTD データプレーン（Lina）コアを検出

解決済みのバグ バージョン 7.1

バージョン 7.1.0.2 で解決済みのバグ

バージョン 7.1.0.2 は、Cisco Secure Firewall 3100 および FMC の限定リリースです。バージョン 7.1.0.1 で修正されたすべてのバグ（Cisco Secure Firewall 3100 では対象外でした）は、バージョン 7.1.0.2 でも修正されています。FMC の場合、新しいオンラインヘルプがバージョン 7.1.0.2 に含まれています。

バージョン 7.1.0.1 で解決済みのバグ

表 *33* : バージョン *7.1.0.1* で解決済みのバグ

不具合 ID	タイトル
CSCvz77254	ホットフィックスパッチのアップグレードで古い Snort3 バイナリが消去されない
CSCwa70008	期限切れの証明書により、セキュリティインテリジェンスの更新が失敗する
CSCwa58060	updates-talos.sco.cisco.com から ICMP 応答が受信されない場合、LSP のダウンロードが失敗する
CSCwa51862	プロキシを使用すると LSP ダウンロードが実行されない

バージョン 7.1.0 で解決済みのバグ

表 *34* : バージョン *7.1.0* で解決済みのバグ

不具合 ID	タイトル
CSCvq26114	FMC への SSH ログインが繰り返し試行されると（DOS）、cron ジョブ（スケジュールされたタスク）が停止する
CSCvr11958	AWS FTD：「ERROR: failed to set interface to promiscuous mode」により展開が失敗する

不具合 ID	タイトル
CSCvs37955	セキュリティモジュールの確認中の「物理ハードウェアを取り外さずに」に関する紛らわしいメッセージ
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
CSCvs50538	SSLエンジンが判定を返さない場合、ファイアウォールエンジンはSSLハンドシェイクからの情報にフォールバックする必要がある
CSCvs73924	同じプロトコルが認証に設定されている場合、シャーシマネージャはAAAサーバーを変更できないことを示す必要がある
CSCvu12734	ブート時に FTD と ASA デバイスの両方でウォッチドッグのトレースバックが発生
CSCvu23149	データベーステーブル rule_opts の SID_GID_ORD インデックスの破損が原因で、FMC でバックアップの生成に失敗する
CSCvu97242	FTD 2100：クラッシュ時に Corefile と crashinfo の両方が切り捨てられ、不完全になることがある
CSCvu98260	特定のシナリオで HA が nsf を有効にすると、DRP データベースに古いルートが表示されます
CSCvv24647	FTD 2100 - SNMP：不正な値がイーサネット統計ポーリングに返される
CSCvv40916	展開中に、AbstractBaseDeploymentValidationHandler.validatePreApply に 3 分の遅延が発生する。
CSCvv59676	Snort2：TLS の証明書キャッシュのアグレッシブプルーニングを実装してメモリを解放する
CSCvv87594	FXOS：jQuery の脆弱性
CSCvv89715	Firepower 8000 シリーズスタックの Fastpath ルールが FMC からランダムに消える
CSCvw22435	FXOS 2.8.1 で「copy ftp: workspace:」を使用すると「該当するファイルまたはディレクトリがありません」のエラーが発生
CSCvw30887	サービス（bcm_usd hap reset）を使用したリセットの HA ポリシーが原因で FXOS がクラッシュする
CSCvw62255	Firepower 4100 で WSP-Q40GLR4L トランシーバと Arista スイッチを使用すると、「リンクが接続されていない（Link not connected）」エラーが発生する

不具合 ID	タイトル
CSCvw62435	AnyConnect は、セキュリティゾーン/インターフェイスグループが VTI によって使用されるインターフェイスで共存できない
CSCvw63283	FTD が EU または APJC に登録されている場合でも、クラウドサービスのリンクが Cisco Prime Network Analysis Module（NAM）の CTR ポータルにユーザーをリダイレクトする
CSCvw67974	FXOS のアップグレード後に公開キー認証を使用した SSH アクセスが失敗する
CSCvw77924	シャーシのリロード後に ASCII 文字「"」が設定された RADIUS キーが FXOS で機能しない
CSCvw79465	FXOS アップグレードが FTD イメージに対して適切な互換性チェックを実行しない
CSCvw90634	FP2100 ASA：9.15.1.1 へのアップグレード後にネットワークモジュールがダウン/ダウンの 1 Gbps SFP
CSCvw93159	Firepower 2100：ASA および FTD が「Local disk 2 missing on server 1/1」というメッセージを生成する
CSCvw95181	FXOS のアップグレードが、「does not support application instances of deployment type container」というエラーで失敗する
CSCvx04436	複数の SFDaCo プロセスの実行は禁止されているが、pidfile が 2 番目のインスタンスのブロックに失敗
CSCvx16317	管理のコンテキストが変更されると、マルチコンテキスト ASA から connect fxos admin で FXOS にアクセスできない
CSCvx24555	アイデンティティ ポリシー ルールの検証は、FMC のパフォーマンスに影響を与えることがある
CSCvx26927	CH をセグメント化して再送信した際に TLS サイトがロードされない
CSCvx27744	バージョンアップグレード情報の取得に失敗すると、6.6.1 以降の FTD でポリシーの展開が失敗することがある
CSCvx32017	スマートライセンスに [コンプライアンス違反（Out of Compliance）] と表示されるが、どのライセンスタイプか示されない。
CSCvx33904	1.9.5p2 より前の sudo には、ヒープベースのバッファオーバーフローがあり、特権昇格を使用できる
CSCvx43150	FMC で、RMA 後のメンバーデバイスの登録プロセスが失敗する
CSCvx44283	FDM UI での静的ルートチェックの制限が多い

不具合 ID	タイトル
CSCvx48862	Java エラーが原因で FCM に新しいクラスタノード設定を保存できない
CSCvx54562	FTD の高いシステムオーバーヘッドのメモリ
CSCvx57417	スマートトンネルコード署名証明書の更新
CSCvx62422	clustered_device テーブル内のデバイスのライセンスページがスタックする
CSCvx64683	NAP ポートスキャンの ignore_scanners フィールドに空白文字があるため、致命的な Snort クラッシュが発生する可能性がある
CSCvx67856	FTD7.0：システムでアングレースフルリブートが発生すると、Prometheus プロセスが起動しない
CSCvx68803	FMC（API）が、不正なリクエストにより 400 ではなく 500 HTTP コードを返す
CSCvx70480	ポリシーにアクセスすると 403 エラーが発生 -> FMC（4600）から FMCv にユーザーロールをエクスポートした後のアクセス制御
CSCvx75445	バイパススタンバイを使用してインラインセットを作成するオプションが Firepower 2130 にない
CSCvx75743	FMC 監査ログの重大度の不整合
CSCvx76665	2100 および 1010 で表示される「インターフェイスのアップデートに失敗しました」というエラーメッセージ
CSCvx78238	ASA のトラフィックでのマルチコンテキストの Firepower サービスが不適切なインターフェイスに移動する
CSCvx80830	Radius サーバーが dACL を送信し、vpn-simultaneous-logins が 1 に設定されていると、同じユーザーからの VPN 接続が失敗する
CSCvx82705	OpenSSL の 2021 年 3 月の脆弱性に対する SSP の評価
CSCvx82957	Smart CLI のロードに時間がかかる
CSCvx86177	FMC データベースを外部からポーリングするために使用される inet6_ntoa と unix_timestamp 関数がエラーを返す
CSCvx89113	新しいオブジェクトグループの作成中、IPv4 と IPv6 アドレスが混在するオブジェクトグループを検索できない
CSCvx89827	FPR 2110 でバンコクタイムゾーンを設定できない
CSCvx92932	SFDataCorrelator プロセス終了が原因で、FMC にイベントがない

不具合 ID	タイトル
CSCvx94732	Firepower Threat Defense（FTD）ヘルスモニターアラート：/ngfw で管理対象外ディスク使用率が高い
CSCvx95652	ASAv Azure：一定期間の実行後、一部またはすべてのインターフェイスがトラフィックの通過を停止する場合がある
CSCvy01482	アップグレード後にレルムの同期結果ページがフリーズする
CSCvy02240	Cisco Firepower Threat Defense イーサネット産業用プロトコルのポリシーバイパスの脆弱性
CSCvy02950	TS でスタックとクラスタ EO の履歴が必要
CSCvy03115	展開可能な構成のダウンロードを試みて、FDM UI がクラッシュした
CSCvy03907	アクセス コントロール ポリシーの作成および編集が「ルール名は既に存在します」というエラーで失敗する
CSCvy06393	ソースフィード追加時の UI エラー
CSCvy07957	FMC - [コンテキストエクスプローラで開く（Open in context explorer）] リダイレクト/オプションでデータを取得できない
CSCvy08351	侵入および相関の電子メールアラートがメールサーバーに送信されなくなる
CSCvy08908	Java によってポート転送アプリケーションがブロックされる
CSCvy10789	LDAP パスワードで FTD 2110 ASCII 文字を使用できない
CSCvy13229	FDM - GUI にアクセスできない（tomcat が開いているファイル記述子が多すぎる）
CSCvy13543	Cisco Firepower Threat Defense ソフトウェアの SSH 接続で確認されたサービス拒否攻撃に対する脆弱性
CSCvy14721	CH パケットの宛先ポートが送信元ポート以下であるときに FTD によって SSL トラフィックがドロップされる
CSCvy15396	スタンバイ FMC で ClamAV のダウンロードが失敗すると、/var ディレクトリに大量のログが生成される
CSCvy16004	差分計算の遅延により、展開で問題が発生し、FTD で HA アプリの同期タイムアウト発生の可能性がある
CSCvy16559	Cisco Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性
CSCvy16573	Cisco Firepower Threat Defense のコマンドインジェクションの脆弱性

不具合 ID	タイトル
CSCvy17030	FMC の接続イベントページに「エラー：このクエリを処理できません。サポートに問い合わせてください。」と表示される
CSCvy17365	REST API ログインページの問題
CSCvy19136	証明書認証が使用される場合に Web ポータルで永続的なリダイレクトが発生する
CSCvy19453	MAC アドレスのみを持つ冗長な新しいホストイベントを含む SFDataCorrelator のパフォーマンスの問題
CSCvy20605	diskmanager プロセスの更新中に警告ヘルスアラートがトリガーされてはいけない
CSCvy21334	「スイッチオーバーなし」の場合、アクティブは CoA アップデートをスタンバイに送信しようとする
CSCvy22765	同期デーモンが終了。同期のクラッシュ。 var/sf/tds/cloud-events.json が空になる。
CSCvy23126	6.6.1 への FMC アップグレードが 800_post/097_upgrade_ssl_inspection.pl.log で失敗する
CSCvy24435	https://FMCIP/login.cgi で.cgi を使用すると、期限切れのパスワードで FMC GUI にアクセス可能になる
CSCvy24921	SNMPv3：構成が変更されるたびに SNMP EngineID が変更される
CSCvy26511	ローエンドプラットフォームの管理対象外ディスクアラートのしきい値を調整
CSCvy30016	SSL 復号ポリシーにより、Snort のパフォーマンスが低下する場合がある
CSCvy30101	SSL 復号を使用すると、Snort2 のメモリ使用量が予想される制限を超えて増加する可能性がある
CSCvy30392	テーブル ids_event_msg_map の破損した int_id インデックスが原因で、FMC でのバックアップ生成に失敗する
CSCvy31400	FTD のアップグレード後、FMC で 1 Gbps SFP の物理インターフェイスの自動ネゴシエーションが無効になることがある
CSCvy31424	QP FTD アプリケーションが、FXOS/FTD アップグレード後に古い affinity.conf が原因で起動に失敗する
CSCvy31521	syslog-ng モニターを FMC と NGIPS に追加する

不具合 ID	タイトル
CSCvy31793	バックアップのディスク容量が不足しても、バックアップ時に ibdatafix.sh が無人モードで失敗しない
CSCvy33044	デバイスのユーザーアカウント数の制限に近い状態が続く場合、ユーザーセッションの処理レートが低い
CSCvy33879	FTD：repair_users.pl が FTD のリブート失敗の原因となる rogue.firstboot ファイルを作成する
CSCvy34333	ASA のアップグレードに失敗した場合、プラットフォームとアプリケーションの間でバージョンステータスの同期が解除される
CSCvy34941	誤ったアラーム「ヘルスモニタリングが予定より大幅に遅れている」
CSCvy35416	並列展開が異なる子ドメインに対してトリガーされると、グローバルドメインからの展開に失敗する
CSCvy36694	Azure の FTDv 6.7 が GigabitEthernet インターフェイスで 1000 の速度を設定できない
CSCvy37484	device_policy_ref のエントリが大きいため、デバイス管理ページを開くときにパフォーマンスが低下する
CSCvy38558	6.6.1 にアップグレードした後、BGP コンフィギュレーションで編集/保存すると、無効なスキャンタイムエラーがスローされる
CSCvy39191	FMC への API 呼び出しを実行すると、T-ufin で内部サーバーエラー 500 が発生する
CSCvy39791	Lina のトレースバックとコアファイルサイズが 40G を超えており、圧縮に失敗する
CSCvy41157	復元後に HA 構成に失敗する
CSCvy41757	Cisco Firepower Threat Defense ソフトウェアにおける CLI 任意ファイルの書き込みの脆弱性
CSCvy43349	別の ACP のベースとして ACP を追加中に内部エラーがスローされる
CSCvy43447	マルチインスタンス FTD の Lic TMR スレッドでの FTD トレースバックとリロード
CSCvy43911	FDM：OSPF インターフェイス SmartCLI が更新の保存に失敗し、編集時に新しいフィールドが表示される
CSCvy44566	AQ メモリ消費が原因でアプリ設定の検証中に FTD 展開が失敗する
CSCvy44752	インターフェイスの作成に失敗

不具合 ID	タイトル
CSCvy47786	展開プレビューで、ACP ルールに対して変更されていない/追加されていないコメントが表示される
CSCvy47927	スケジュールされた Firepower 推奨ルールに対して複数のポリシーを選択できない
CSCvy48730	ASA/FTD がスレッド名「Unicorn Proxy Thread」でトレースバックおよびリロードすることがある
CSCvy48764	公開キー認証による SSH アクセスにはユーザーパスワードが必要
CSCvy50009	インストールの準備状況チェックの実行時に誤ったエラーが報告される
CSCvy52617	展開のたびに FMC 6.7 が VTI の IPSec プロファイルを変更し、トンネルのフラッピングを引き起こす
CSCvy53301	「展開中の内部エラー」により FDM で HA 構成に失敗する
CSCvy55054	Cisco 適応型セキュリティアプライアンスと Firepower Threat Defense ソフトウェアの DoS の脆弱性
CSCvy55676	内部エラーが原因で FMC 展開に失敗
CSCvy57905	VTI トンネルインターフェイスが、HA の KP および WM プラットフォームでリロード後もダウンしたままになる
CSCvy59958	プロセス hmlsd（SF::Messaging::smartSend）での継続的なメモリリーク
CSCvy63463	特殊文字が原因でユーザーの削除でエラーが発生
CSCvy63464	FTD 1100/2100 シリーズがクロックを 2033 に設定してリブートする
CSCvy65248	Azure D5_v2 インスタンスの FTDv：CPU 使用率が最大になる前にインターフェイスがドロップする
CSCvy66065	複数のシスコ製品の Snort ルールにおけるサービス妨害の脆弱性
CSCvy66849	Rest API 呼び出しスクリプトが 5 分ごとに実行されると、デバイスが登録解除される
CSCvy66942	9300/4100 スーパーバイザで REST API LTP を使用して FPR4100/9300 IPv6 設定を適用することができない
CSCvy68166	7.0 へのアップグレード後にレルムページがロードされない
CSCvy68859	侵入ルールの LSP およびカテゴリフィルタで DB 接続が解放されない
CSCvy68974	プロセスで使用されているメモリが 3 GB の制限を超えているため、ActionQueue プロセスが OOM Killer によって強制終了される

不具合 ID	タイトル
CSCvy69189	vpnfol_sync/Bulk-sync keytab がスタックしているため、FTD HA がバルク状態のままになる
CSCvy69787	AWS TenGigabit インターフェイス上の ASAv が 10000Mbps ではなく 1000mbps を学習している
CSCvy71478	ASALinaCliUtilShow を使用して LINA に対して行われた要求に対する応答が遅延する
CSCvy72118	navl 属性のコピー中に snort CPU 使用率が高くなる（断片化されたメタデータ）
CSCvy72185	FXOS Apache HTTP サーバーの複数の脆弱性（CVE-2020-11993）と（CVE-2020-9490）
CSCvy73930	AC ルール名の特殊文字による構文エラーが原因の EventHandler 展開エラー
CSCvy74984	デフォルトの外部ルートが使用されると、Azure 上の ASAv がメタデータサーバーへの接続を失う
CSCvy78573	cloudagent は、ルックアップのために長さゼロの URL を Beaker に送信してはいけない
CSCvy79015	800_post/800_manager_install_lsp.pl で FMC 6.7 から 7.0 へのアップグレードに失敗する
CSCvy79186	Pull_Upgrade ジョブがスタックし、デバイスのアップグレードをブロックする
CSCvy82655	REST API：一括 AC ルールの作成が処理不可能なエンティティ（422）で失敗する
CSCvy83116	FTD 1000 スタンバイが HA への再参加に失敗し、「CD App Sync エラーは SSP 設定の生成に失敗しました」というメッセージが表示される
CSCvy84733	SFR 6.7 から 7.0 へのアップグレード：Syslog の機能が停止
CSCvy86780	エラーにより LSP のインストールを完了できない再度実行してください。（Please try again.）」
CSCvy86817	カスタム CCL IP サブネットが設定されている場合、Cruz ASIC CLU フィルタに誤った src/dst IP サブネットが存在する
CSCvy88381	FMC データベースの外部ポーリング時に INET6_NTOA(location_ip) で障害が発生する
CSCvy89440	s2sCryptoMap 設定の損失

不具合 ID	タイトル
CSCvy93480	Cisco ASA および FTD ソフトウェアの IKEv2 サイト間 VPN で確認されたサービス拒否攻撃に対する脆弱性
CSCvy95329	AC ルールエントリが見つからないため、アクセスルールが正しく一致しない
CSCvy95554	group_fsp_reference テーブルのデータベースのマージで障害が発生したため、LDAP をダウンロードできない
CSCvy96325	FTD/ASA：ACP に新しい ACE エントリを追加すると、LINA の ACE 要素が削除および再追加される
CSCvy96698	FXOS portmgr で速度値を 2 回チェックするスプリアス ステータス アクションを解決する
CSCvy98027	FXOS で物理インターフェイスが動作しているのにアプリケーションインターフェイスがダウンする
CSCvy98458	FP21xx のトレースバック「Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header」
CSCvy99373	AD で adSamAccountName を解決するときにADI セッション処理が遅延する
CSCvz00254	アップグレードのインポート中にサイト間VPNが無効な状態になり、FDM 6.7.0 から 7.0.0 へのアップグレードに失敗する
CSCvz00934	トンネルの送信元を（FMC アクセス）データインターフェイスとして使用して VTI を設定できない
CSCvz01766	スタンバイ FDM の GUI が空白になる
CSCvz05468	プラットフォーム内の複数の SSH ホストエントリが最初に有効化/展開する機能として設定されている場合、LINA で SSH が切断される
CSCvz05687	DND フローのフラグメント化された証明書の要求に失敗
CSCvz05767	FP-1010 HA リンクがダウンするか、新しいホストがデバイスに接続できない
CSCvz05921	2100 SFP インターフェイスの自動ネゴシエーション設定のチェックボックスオプションが利用できない
CSCvz06848	snmp-server community 検証でエラーが発生し、FDM 管理 FTD でソフトウェアのアップグレードに失敗する
CSCvz12770	クロックリセットの問題が原因で、ポリシー展開が 0% で失敗する

不具合 ID	タイトル
CSCvz14616	SFDataCor プロセスがスタックしているため、接続イベントがない
CSCvz14628	FMC 2500 を 6.6.5-78 にアップグレードした場合、イベントデータベース「eventdb」をパージする際に、手動の介入が必要になる
CSCvz15676	Firepower 1010 デバイスで、ASA アプリをアップグレードした後、デバイスがフェイルセーフモードになる
CSCvz15755	FTD：アップグレード後にポートチャネルが起動せず、コアファイルが生成される場合がある
CSCvz17046	16 ノードクラスタセットアップをアップグレードまたはリロードしようとすると、ASAv がクラッシュしました
CSCvz17534	FTD のバックアップ復元 CLI で VPN 設定が復元されない
CSCvz18341	FMC：remove_peers の実行時に、EM_peers テーブルのピア/デバイス UUID の削除/クリーンアップが必要
CSCvz19634	FTD ソフトウェアのアップグレードが 200_pre/505_revert_prep.sh で失敗することがある
CSCvz20544	Anyconnect プロファイルのループ処理で、ASA および FTD がトレースバックおよびリロードする場合がある
CSCvz20679	FTDv - Lina のトレースバックおよびリロード
CSCvz26998	プロセスが同じログイン情報を使用すると、FMC REST API 呼び出しが HTTP エラー コード 500 を返す
CSCvz28103	FDM で DHCP リレー設定を保存すると、flex-config/smart CLI エラーが発生する
CSCvz28145	「別のユーザーの別の操作により、この操作が妨げられました。しばらくしてからやり直してください。」というエラーが表示される
CSCvz31184	FPR4100/9300 のパッシブ/インラインインターフェイスで、プレフィルタを使用したサポートされていないフローオフロードの検証を検出
CSCvz32386	FMC が同じ暗号マップのエントリに PFS21 および IKEv1 設定をプッシュするときの FTD 展開エラー
CSCvz33190	SecurityIntelligence URL フィード：SSL ピア証明書のダウンロードに失敗したか、SSH リモート キーが正しくない
CSCvz33468	ASA/FTD：手動 NAT ルールでオブジェクトグループを変更した後、NAT が送信元アドレスの変換を停止する

不具合 ID	タイトル
CSCvz34831	ASA が DACL のダウンロードに失敗した場合、試行を停止しない
CSCvz36862	FMC ポリシーの展開で、フェーズ 3 にかかる時間が 15 分を超える
CSCvz36933	ポリシーの展開時にセンサーの SNMP プロセスが再起動することがある
CSCvz38361	直接接続されていないネイバーのために BGP パケットがドロップされる
CSCvz40098	FTD HA：ヘルスモニターページに「デバイス詳細の取得エラー エラー：検証に失敗しました」と表示される
CSCvz46333	内部ソケット接続の損失による FTD ポリシー展開の失敗
CSCvz46680	FMC で管理対象デバイスのインベントリ詳細と適用ポリシーが空白で表示される
CSCvz49289	ポートを除外する FMC 6.6 接続イベントがプロトコルも除外する
CSCvz50270	ダイナミック PAT ルールの変更を検証するために、FMC GUI に検証チェックを追加
CSCvz50712	TLS サーバー検出は、AnyConnect 展開のプローブに誤った送信元 IP アドレスを使用
CSCvz51175	SNMP の管理状態が無効になっているときに FTD HA が形成されない
CSCvz53372	「config log-events-to-ramdisk disable」の実行後、Snort が D 状態になる
CSCvz53606	セキュリティ ゾーン オブジェクトへのどの変更でセキュリティゾーン UUID を変更するかを指定する
CSCvz53993	SSL フローでの Snort によるランダムなパケットのブロック
CSCvz55302	低メモリ状態での SSL null チェックによる FTD/ASA のトレースバックとリロード
CSCvz57917	/ngfw のアンマネージドディスクの使用率が高くなり、パッケージ フォルダ内が module-xxxx-x86_64.tgz ファイルで一杯になる
CSCvz59464	IPReputation フィード エラー メッセージ：メソッドが許可されていません
CSCvz61477	同じ RADIUS サーバーが認証サーバーおよび許可サーバーとして使用されている場合、RAVPN 認証に失敗する
CSCvz61767	SNMPv2 または SNMPv1 が設定されたポリシーが展開されない
CSCvz63444	FMC カスタムウィジェットがポーリングし続けてデータを返さない
CSCvz64548	デバイス上の SFTunnel がイベントメッセージを処理しない

不具合 ID	タイトル
CSCvz65181	Cisco Firepower Threat Defense ソフトウェアの セキュリティインテリジェンスにおける DNS フィードバイパスの脆弱性
CSCvz66506	FMC HA に登録された FPR2100 で継続的に ADI のトレースバックとリロードが発生
CSCvz71569	プロセス ZeroMQ のメモリ不足状態が原因で FTD のトレースバックとリロードが発生
CSCvz76745	クラウドベースのマルウェアイベントによる SFDataCorrelator メモリの増加
CSCvz77037	mojo-server の SSL エラーで FMC ユーザーインターフェイスのアクセスに失敗することがある
CSCvz80981	バージョン 7.0 を実行している SFR モジュールで SNMPv3 が機能しない
CSCvz81342	Diskmanager が AMP ファイルのキャプチャファイルをプルーニングしない
CSCvz81934	CSCvx95884 によって導入された「修正」を元に戻す
CSCvz82433	外部 DB アクセスを介して FMC データベースにクエリを試行しているが、侵入イベントのインターフェイス値が欠落している
CSCvz85493	FTD の backup.log のサイズが 50 GB 以上で制御不能になり、/ngfw が 100% になる
CSCvz89545	アップグレード後の SSL VPN のパフォーマンスの低下と重大な安定性に関する問題
CSCvz90654	「APP SYNC のタイムアウトにより HA の状態の進行に失敗」が原因で、FTD フェールオーバーユニットが HA スイッチオーバー に参加しない
CSCvz96462	VPN セッションはないが、IP アドレスが「使用中」になる
CSCvz97196	ページャーがブロックされているため、ldap-naming-attribute ページャーを使用して Flexconfig オブジェクトを作成できない
CSCwa20516	FMC ポリシーの展開に 14 分以上かかる
CSCze92695	LDAP ユーザーパスワードが /etc/sf/authconfig*.con... にクリアテキストで保存されている

翻訳について
このドキュメントは、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。