Cisco Secure Firewall Threat Defense バージョン 7.2、リリースノート

初版：2022 年 6 月 6 日

最終更新：2022 年 7 月 15 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/

© 2022 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章 ようこそ 1

リリースの主なポイント 1

リリース日 2

推奨リリース 2

シスコとのデータの共有 3

支援が必要な場合 3

第 2 章 システム要件 5

Threat Defense プラットフォーム 5

Management Center プラットフォーム 7

Management Center 9

ブラウザ要件 10

第 3 章 特長と機能 13

新機能 13

Management Center バージョン 7.2 の新機能 13

Device Manager バージョン 7.2 の新機能 38

バージョン 7.2 の新しいハードウェアと仮想プラットフォーム 40

新しい侵入ルールとキーワード 41

廃止された機能 42

Management Center バージョン 7.2 で廃止済みの機能 42

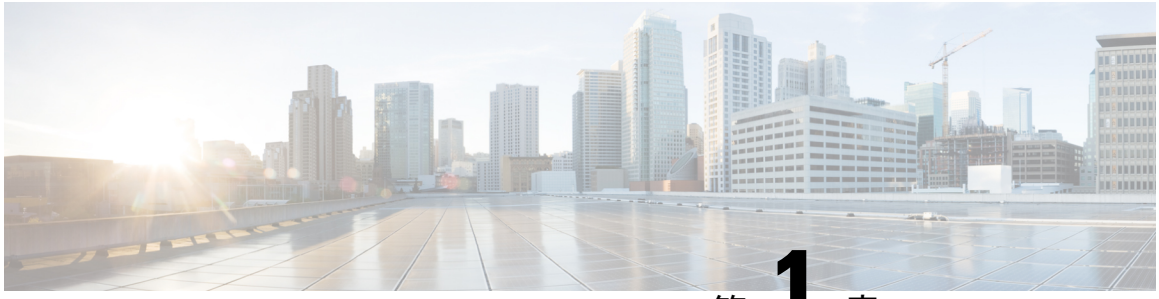
廃止された FlexConfig コマンド 43

第 4 章 ソフトウェアのアップグレード 45

アップグレードの計画 45
アップグレードする最小バージョン 46
バージョン 7.2 のアップグレードガイドライン 47
GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない 48
高可用性 Management Center の Cisco Secure Malware Analytics に再接続する 48
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 49
FXOS のアップグレードガイドライン 49
応答しないアップグレード 50
アップグレードを元に戻す 51
トラフィック フローとインスペクション 51
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 51
Management Center を使用した Threat Defense 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 52
Device Manager を使用した Threat Defense 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 55
時間とディスク容量のテスト 56
バージョン 7.2.0 の時間とディスク容量 58

第 5 章 ソフトウェアのインストール 61
設置に関するガイドライン 61
設置ガイド 64

第 6 章 未解決のバグおよび解決されたバグ 65
バージョン 7.2 で未解決のバグ 65
バージョン 7.2.0 で未解決のバグ 65
解決済みのバグ バージョン 7.2 66
バージョン 7.2.0 で解決済みのバグ 66



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 7.2 のリリース情報を記載しています。

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Cisco Secure Firewall 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 Secure Firewall 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 （1 ページ）
- リリース日 （2 ページ）
- 推奨リリース （2 ページ）
- シスコとのデータの共有 （3 ページ）
- 支援が必要な場合 （3 ページ）

リリースの主なポイント

Cisco Secure Firewall へのブランド名の変更

以下の製品は、バージョン 7.2 でブランド名が変更されました。

表 *1* : バージョン *7.2* でブランド名が変更された製品

旧製品名	変更後の製品名
Firepower Threat Defense（FTD）	Cisco Secure Firewall Threat Defense
Firepower Threat Defense Virtual（FTDv）	Cisco Secure Firewall Threat Defense Virtual
Firepower Device Manager（FDM）	Cisco Secure Firewall Device Manager

旧製品名	変更後の製品名
Firepower Management Center（FMC）	Cisco Secure Firewall Management Center
Firepower Management Center Virtual（FMCv）	Cisco Secure Firewall Management Center Virtual
Firepower Extensible Operating System（FXOS）	Cisco Secure Firewall Extensible Operating System（FXOS）
Firepower Chassis Manager	Cisco Secure Firewall Chassis Manager

リリース日

表 *2:* バージョン *7.2* のリリース日

バージョン	ビルド	日付	プラットフォーム
7.2.0	82	2022-06-06	すべて

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 Device Manager 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、management center 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。

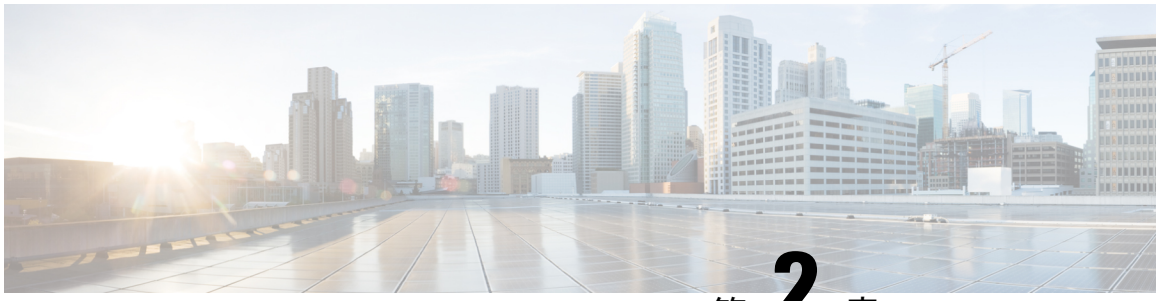
- マニュアル：http://www.cisco.com/go/threatdefense-72-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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 7.2 のシステム要件を記載します。

- Threat Defense プラットフォーム （5 ページ）
- Management Center プラットフォーム （7 ページ）
- Management Center （9 ページ）
- ブラウザ要件 （10 ページ）

Threat Defense プラットフォーム

このドキュメントでは、バージョン 7.2 でサポートされているデバイスと管理方法を記載します。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。

デバイスの管理方式

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

- Secure Firewall Management Center：複数のデバイスをリモートで管理します。

  management center は、顧客が導入したハードウェアまたは仮想プラットフォームとして、または Cisco Defense Orchestrator（CDO）プラットフォームを使用するシスコが管理するクラウド実装として利用できます。お客様が導入したハードウェアまたは仮想management center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。クラウド提供型の管理センターでは、バージョンの概念はなく、機能の更新が処理されます。

- Secure Firewall Device Manager：単一の Threat Defense デバイスをローカルで管理します。

  必要に応じて、management center の代替策として、Cisco Defense Orchestrator（CDO）を追加し、複数の Threat Defense 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 Device Manager が必要ですが、CDO を使用することで、展開したすべての Threat Defense 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。

Threat Defense 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 *3 :* バージョン *7.2 Threat Defense* ハードウェア

プラットフォーム（Platform）	Management Center 互換		Device Manager 互換		注記
	お客様が導入	クラウド提供型	Device Manager のみ	Device Manager + CDO	
Firepower 1010、1120、1140、1150	対応	対応	対応	対応	—
Firepower 2110、2120、2130、2140	対応	対応	対応	対応	—
Secure Firewall 3110、3120、3130、3140	対応	対応	対応	対応	—
Firepower 4110、4120、4140、4150 Firepower 4112、4115、4125、4145	対応	対応	対応	対応	FXOS 2.12.0.31 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	対応	FXOS 2.12.0.31 以降のビルドが必要です。
ISA 3000	対応	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。

Threat Defense Virtual

仮想版 Threat Defense 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 *4 :* バージョン *7.2 Threat Defense Virtual* 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	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Alibaba	対応	対応	—	—
Amazon Web Services（AWS）	対応	対応	対応	対応
Microsoft Azure	対応	対応	対応	対応
Google Cloud Platform（GCP）	対応	対応	対応	対応
Oracle Cloud Infrastrucure（OCI）	対応	対応	—	—

表 *5 :* バージョン *7.2 Threat Defense Virtual* 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	Management Center 互換		Device Manager 互換	
	お客様が導入	クラウド提供型	Device Manager のみ	CDO および Device Manager
Cisco Hyperflex	対応	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	対応
Nutanix エンタープライズクラウド	対応	対応	対応	対応
OpenStack	対応	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応	対応

Management Center プラットフォーム

このセクションでは、バージョン 7.2 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 management center を示します。クラウド提供型の管理センターの互換性情報について

は、『Management Center （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。

Management Center ハードウェア

バージョン 7.2 は次の management center 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 Firepower ホットフィックス リリース ノート を参照）。

Management Center Virtual

バージョン 7.2 は、次の Management Center Virtual プラットフォームをサポートしています。

Management Center Virtual 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 *6 :* バージョン *7.2 Management Center Virtual* 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（Platform）	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
Alibaba	対応	—	—
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 *7 :* バージョン *7.2 Management Center Virtual* 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（Platform）	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	—	—

プラットフォーム（Platform）	FMCv2、10、25	FMCv300	ハイ アベイラビリティ
OpenStack	対応	—	—
VMware vSphere/VMware ESXi 6.5、6.7、または 7.0	対応	対応	対応

Management Center

すべての デバイスは、management center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 Management Center

お客様が導入したハードウェアまたは仮想management center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 management center 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、management center 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。
- management center 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 management center をアップグレードする必要があります。

表 *8 : Management Center*とデバイス間の互換性

Management Center バージョン	管理可能な最も古いデバイスバージョン
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1

Management Center バージョン	管理可能な最も古いデバイスバージョン
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 7.2.0 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）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。

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
Management Center	1280 X 720
Device Manager	1024 X 768
Firepower 4100/9300 用 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。

- Management Center：**[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。

- Device Manager ：[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。

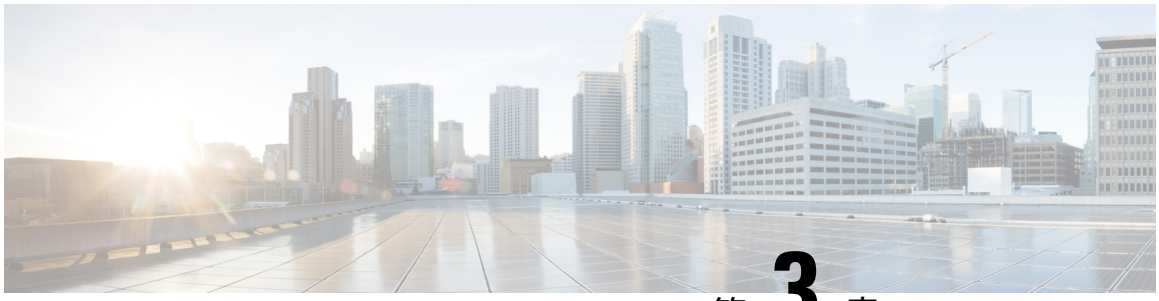
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーションガイドを参照してください。

（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7.2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 （13 ページ）
- 廃止された機能 （42 ページ）

新機能

Management Center バージョン 7.2 の新機能

新しいハードウェアまたは仮想 management center 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、management center 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、management center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 *9 : Management Center* バージョン *7.2.0* の新機能

機能	説明
プラットフォーム（Platform）	

機能	説明
スナップショットで AWS および Azure 向け Threat Defense Virtual をすばやく展開できます。	AWS または Azure インスタンスの Threat Defense Virtual のスナップショットを作成し、そのスナップショットを使用して新しいインスタンスをすばやく展開できるようになりました。この機能により、AWS および Azure の自動スケールソリューションのパフォーマンスも向上します。
AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケール。	CloudFormation テンプレートを使用して、AWS ゲートウェイロードバランサ向け Threat Defense Virtual の自動スケールをサポートするようになりました。
GCP 向け Threat Defense Virtual の自動スケール。	GCP の内部ロードバランサ（ILB）と GCP 外部ロードバランサ（ELB）の間に Threat Defense Virtua インスタンスグループを配置することにより、GCP 向け Threat Defense Virtua の自動スケールをサポートするようになりました。
クラウド管理型の脅威防御デバイス向けの分析モード。	バージョン 7.2 と同時に、クラウド提供型の Cisco Secure Firewall Management Center が導入されました。このクラウド提供型の管理センターは、Cisco Defense Orchestrator（CDO）プラットフォームを使用して、複数の Cisco セキュリティソリューションの管理を統合します。更新についてはシスコが行います。 お客様が導入したハードウェアおよびバージョン 7.2 以降を実行している仮想管理センターでは、クラウド管理型の脅威防御デバイスを「共同管理」できますが、用途はイベントのロギングと分析に限られます。お客様が導入した管理センターからこれらのデバイスにポリシーを展開することはできません。 新規/変更された画面： • クラウド管理型デバイスをお客様が導入した管理センターに追加する場合は、新しい [CDO管理対象デバイス（CDO Managed Device）] チェックボックスをオンにして、それが分析専用であることを指定します。 • [デバイス（Devices）] > [デバイス管理（Device Management）] を選択すると、分析専用のデバイスが表示されます。 新規/変更された CLI コマンド：**configure manager add**、**configure manager delete**、**configure manager edit**、**show managers** 詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理を参照してください。
高可用性/拡張性	

機能	説明
パブリッククラウドとプライベートクラウドの両方で Threat Defense Virtual のクラスタリング。	次の Threat Defense Virtual プラットフォームのクラスタリングを設定できるようになりました。 • AWS 向け Threat Defense Virtual：16 ノードクラスタ • GCP 向け Threat Defense Virtual：16 ノードクラスタ • KVM 向け Threat Defense Virtual：4 ノードクラスタ • VMware 向け Threat Defense Virtual：4 ノードクラスタ 新規/変更された画面： • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタの追加（Add Cluster）] • [Devices] > [Device Management] > [More] メニュー • [デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）]
16 ノードクラスタのサポート。	次のプラットフォームに 16 ノードクラスタを設定できるようになりました。 • Firepower 4100/9300 • AWS 向け Threat Defense Virtual • GCP 向け Threat Defense Virtual Cisco Secure Firewall 3100 では、依然として 8 ノードしかサポートされません。
インターフェイス	
Firepower 2100 および Cisco Secure Firewall 3100 で LLDP をサポート。	Firepower 2100 および Cisco Secure Firewall 3100 シリーズのインターフェイスで Link Layer Discovery Protocol（LLDP）を使用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**

機能	説明
Cisco Secure Firewall 3100 でハードウェアバイパスをサポート（「fail-to-wire」）。	Cisco Secure Firewall 3100 は、ハードウェア バイパス ネットワーク モジュールの使用時に、ハードウェアバイパス機能をサポートするようになりました（バージョン 7.2 の新しいハードウェアと仮想プラットフォーム （40 ページ） を参照してください）。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）]>[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）]
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止。	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [ハードウェア構成（Hardware Configuration）] > [ネットワーク接続（Network Connectivity）]
Cisco Secure Firewall 3130 および 3140 のブレークアウトポート。	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成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）] > [シャーシの操作（Chassis Operations）]
Management Center の Web インターフェイスから VXLAN を設定。	Management Center の Web インターフェイスを使用して VXLAN インターフェイスを設定できるようになりました。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。 以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。 新規/変更された画面： • VTEP ソースインターフェイスは次の順にアクセスし、設定します：**[デバイス（Devices）] > [デバイスの管理（Device Management）] > [VTEP]** • VNI インターフェイスは次の順にアクセスし、設定します。**[デバイス（Devices）] > [デバイスの管理（Device Management）] > [インターフェイス（Interfaces）] > [VPNインターフェイスを追加（Add VNI Interface）]**

機能	説明
NAT	
一度に複数の NAT ルールの有効化、無効化、削除が可能。	複数の NAT ルールを選択して、すべてを同時に有効化、無効化、または削除できます。有効化および無効化の対象は手動 NAT ルールのみです。削除はすべての NAT ルールが対象になります。
VPN	
RA VPN 接続プロファイル用の証明書と SAML 認証。	RA VPN 接続プロファイル用の証明書と SAML 認証をサポートするようになりました。SAML 認証/承認が開始される前に、マシン証明書やユーザー証明書を認証できます。これは、ユーザー固有の SAML DAP 属性と DAP 証明書属性を使用して実行できます。 新規/変更された画面：RA VPN ポリシーの接続プロファイルの認証方法を選択するときに、[証明書と SML（Certificate & SAML）] オプションを選択できるようになりました。
ハブアンドスポークトポロジを使用したルートベースのサイト間 VPN。	ハブアンドスポークトポロジでのルートベースのサイト間 VPN のサポートが追加されました。以前は、このトポロジはポリシーベース（暗号マップ）VPN のみをサポートしていました。 新規/変更された画面：新しい VPN トポロジを追加し、[ルートベース (VTI)（Route Based (VTI)）] を選択すると、[ハブアンドスポーク（Hub and Spoke）] も選択できるようになりました。
Cisco Secure Firewall 3100 の IPsec フローのオフロード。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
ルーティング	

機能	説明
Management Center の Web インターフェイスから EIGRP を設定。	Management Center の Web インターフェイスを使用して EIGRP を設定できるようになりました。デバイスのグローバル仮想ルータに属するインターフェイスでのみ EIGRP を有効にできることに注意してください。 以前のバージョンの FlexConfig を使用して EIGRP を設定した場合、アップグレード後の展開は可能ですが、Web インターフェイスで EIGRP の設定をやり直すように警告が表示されます。新しい設定を確認したら、廃止された FlexConfig オブジェクトまたは FlexConfig コマンドを削除できます。 このプロセスを支援するために、コマンドライン移行ツールが用意されています。詳細については、コンフィギュレーション ガイドの FlexConfig ポリシーの移行 を参照してください。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[EIGRP]**
Firepower 1010 で仮想ルータをサポート。	Firepower 1010 で最大 5 つの仮想ルータを構成できるようになりました。
ユーザー定義の仮想ルータで VTI をサポート。	仮想トンネルインターフェイスをユーザー定義の仮想ルータに割り当てることができるようになりました。これまでは、VTI はグローバル仮想ルータにしか割り当てることができませんでした。 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）]** > **[仮想ルータのプロパティ（Virtual Router Properties）]**

機能	説明
パスのモニタリングによるポリシーベースのルーティング。	パスのモニタリング機能を使用して、デバイスの出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集できるようになりました。次に、収集したメトリックを使用して、ポリシーベースのルーティングの最適なパスを決定できます。 新規/変更された画面： • パスモニタリングを有効にし、収集するメトリックを選択するには、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）** > **[パスモニタリング（Path Monitoring）]**に移動します。 • ポリシーベースのルートを追加して転送アクションを指定する際、新規の [インターフェイスの順位付け（Interface Ordering）] オプションを使用します（**[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）]**）。 • 各デバイスのヘルスモニタリングダッシュボードでパスメトリックを監視します（**システム**（⚙）>**[ヘルス（Health）]**>**[モニター（Monitor）]** > [ダッシュボードの追加（add dashboard）] > **[インターフェイス: パスメトリック（Interface - Path Metrics）]**）。 新規/変更された CLI コマンド：**show policy route**、**show path-monitoring**、**clear path-monitoring**
脅威インテリジェンス	

機能	説明
Cisco Umbrella からの DNS ベースの脅威インテリジェンス。	Cisco Umbrella から定期的に更新される情報を使用して、DNS ベースのセキュリティインテリジェンスをサポートするようになりました。二重の保護として、ローカル DNS ポリシーと Umbrella DNS ポリシーの両方を使用できます。 新規/変更された画面： • Umbrella への接続の設定：**[統合（Integration）]** > **[その他の統合（Other Integrations）]** > **[クラウドサービス（Cloud Services）]** > **[Cisco Umbrella接続（Cisco Umbrella Connection）]** • Umbrella DNS ポリシーの設定：**[ポリシー（Policies）]** > **[DNS]** > **[DNSポリシーを追加（Add DNS Policy）]** > **[Umbrella DNAポリシー（Umbrella DNA Policy）]** • Umbrella DNS ポリシーのアクセスコントロールへの関連付け：**[ポリシー（Policies）]** > **[アクセスコントロール（Access Control）]** > **[ポリシーを編集（Edit Policy）]** > **[セキュリティインテリジェンス（Security Intelligence）]** > **[Umbrella Cisco DNS ポリシー（Umbrella Cisco DNS Policy）]**
Amazon GuardDuty からの IP ベースの脅威インテリジェンス。	AWS の Management Center Virtual と統合している場合、Amazon GuardDuty によって検出された悪意のある IP アドレスに基づいてトラフィックを処理できるようになりました。カスタム セキュリティ インテリジェンス フィードまたは定期的に更新されるネットワーク オブジェクト グループを介して脅威インテリジェンスがシステムで活用され、ユーザーはそれをセキュリティポリシー内で使用できます。 詳細については、AWS クラウド向け Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。
アクセス制御と脅威検出	

機能	説明
動的オブジェクト管理： • クラウド提供型 Cisco Secure 動的属性コネクタ • オンプレミス Cisco Secure 動的属性コネクタ 2.0	バージョン 7.2 と同時に、Cisco Secure 動的属性コネクタの次の更新をリリースしました。 • クラウド提供型 Cisco Secure 動的属性コネクタ（CDO マネージドサービス） サポート対象管理センター：バージョン 7.1 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365。 詳細については、Cisco Defense Orchestrator のクラウド提供型ファイアウォール管理センターを使用した Firewall Threat Defense の管理 の「*Managing the Cisco Secure Dynamic Attributes Connector with Cisco Defense Orchestrator*」の章を参照してください。 • オンプレミス Cisco Secure 動的属性コネクタ 2.0 サポート対象管理センター：バージョン 7.0 以降およびクラウド提供型管理センター。 サポート対象仮想/クラウドワークロード：AWS、Azure、Azure サービスタグ、Google Cloud Connector、GitHub、Office 365、VMware。 詳細については、Cisco Secure 動的属性コネクタ コンフィギュレーション ガイド 2.0 [英語] を参照してください。
Snort 3 デバイスで、インスペクションをバイパスするか、エレファントフローをスロットルします。	インスペクションの検出およびオプションでのバイパス、もしくはエレファントフローをスロットルできるようになりました。デフォルトでは、アクセス コントロール ポリシーは、システムが 1 GB/10 秒を超える暗号化されていない接続を検出したときにイベントを生成するように設定されています。レート制限は設定可能です。 Firepower 2100 シリーズでは、エレファントフローを検出できますが、インスペクションのバイパスやスロットルすることはできません。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスでは、引き続きインテリジェント アプリケーション バイパス（IAB）を使用します。 新規/変更された画面：[エレファントフローの設定（Elephant Flow Settings）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。

機能	説明
Snort 3 デバイス向けの暗号化された可視性エンジン機能の拡張。	

機能	説明
	暗号化された可視性エンジン（EVE）に次の拡張機能が追加されています。 • EVEは、ホストが使用しているオペレーティングシステムを検出できます。これは、イベントとネットワークマップで報告されます。 • EVEは、高い信頼度で識別されたEVEプロセスをアプリケーションに割り当てることでアプリケーション トラフィックを検出できます。これをアクセスコントロールルールで使用してネットワークトラフィックを制御できます。（バージョン 7.1 では、接続の EVE プロセスを見ることができましたが、その情報をもとに行動することはできませんでした。） さらに割り当てを追加するには、カスタムアプリケーションやカスタムアプリケーションディテクタを作成します。カスタムディテクタに検出パターンを追加するときは、アプリケーションとして [暗号化された可視性エンジン（Encrypted Visibility Engine）] を選択します。次に、プロセス名と信頼度を指定します。 • EVE は QUIC トラフィックで動作するようになりました。 これらの機能拡張に伴い、次の接続イベントフィールドが変更されました。 [TLS Fingerprint Process Name] は次に変更されました。 [暗号化された可視性プロセス名（Encrypted Visibility Process Name）] [TLS Fingerprint Process Confidence Score] は次に変更されました。 [暗号化された可視性プロセスの信頼スコア（Encrypted Visibility Process Confidence Score）] [TLS Fingerprint Malware Confidence] は次に変更されました。 [暗号化された可視性脅威の信頼度（Encrypted Visibility Threat Confidence）] [TLS Fingerprint Malware Confidence Score] は次に変更されました。 [暗号化された可視性脅威の信頼スコア（Encrypted Visibility Threat Confidence Score）] 検出タイプ：TLS フィンガープリント は次に変更さ 検出タイプ：暗号化された可視性エンジン

機能	説明
	れまし た。 この機能には脅威ライセンスが必要になりました。
Snort 3 デバイスの TLS 1.3 インスペクション。	TLS 1.3 トラフィックのインスペクションがサポートされるようになりました。 新規/変更された画面：SSL ポリシーの [詳細設定（Advanced Settings）] タブに [TLS 1.3復号の有効化（Enable TLS 1.3 Decryption）] オプションが追加されました。なお、このオプションはデフォルトで無効になっています。
Snort 3 デバイスのポートスキャン検出の改善。	改良されたポートスキャンディテクタを使用すると、ポートスキャンを検出または防止するようにシステムを簡単に設定できます。保護するネットワークを絞り込んだり、感度を設定したりできます。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスの場合、ポートスキャン検出には引き続きネットワーク分析ポリシーを使用します。 新規/変更された画面：[脅威検出（Threat Detection）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。
Snort 3 デバイスの VBA マクロ検査。	Microsoft Office ドキュメントの VBA（Visual Basic for Applications）マクロのインスペクションがサポートされるようになりました。これは、マクロを解凍し、解凍されたコンテンツに対してルールを照合することで実行されます。 デフォルトでは、VBA マクロの解凍は、システムが提供するすべてのネットワーク分析ポリシーで無効になっています。これを有効にするには、imap、smtp、http_inspect、および pop Snort 3 インスペクタで decompress_vba 設定を使用します。 解凍されたマクロと照合するカスタム侵入ルールを設定するには、vba_data オプションを使用します。

機能	説明
Snort 3 デバイスの JavaScript インスペクションの改善。	JavaScript を正規化し、正規化されたコンテンツに対してルールを照合することで実行される JavaScript インスペクションを改善しました。新しいノーマライザの拡張機能には、改善されたホワイトスペースの正規化、セミコロンの挿入、クロスサイトスクリプトの処理、識別子の正規化とデエイリアシング、ジャストインタイム（JIT）インスペクション、および外部スクリプトを検査する機能が含まれます。 デフォルトでは、新しいノーマライザは、システムが提供するすべてのネットワーク分析ポリシーで有効になっています。カスタムネットワーク分析ポリシーでパフォーマンスを調整するか、機能を無効にするには、https_inspect Snort 3 インスペクターで js_norm（改良されたノーマライザ）および normalize_javascript（従来のノーマライザ）設定を使用します。 正規化された JavaScript と照合するようにカスタム侵入ルールを構成するには、次のように js_data オプションを使用します。 `alert tcp any any -> any any (msg:"Script detected!"; js_data; content:"var var_0000=1;"; sid:1000001;)`
Snort 3 デバイスの SMB 3 インスペクションの改善。	次の状況下で SMB 3 トラフィックの検査がサポートされるようになりました。 • SMB 透過フェールオーバー用に構成されたクラスタのファイルサーバーノードのフェールオーバー中。 • SMB スケールアウトを使用したクラスタの複数ファイルサーバーノード内。 • SMB ディレクトリリースによるディレクトリ情報の変更時。 • SMB マルチチャネルによる複数の接続の分散時。
[ポリシー管理（Policy Management）]	
アクセスコントロールポリシーのロック。	アクセス コントロール ポリシーをロックして、他の管理者が編集できないようにすることが可能になりました。ポリシーをロックすると、変更を保存する前に別の管理者がポリシーを編集して変更を保存しても、変更が無効になることはありません。アクセス コントロール ポリシーを変更する権限を持つすべてのユーザーには、それをロックする権限があります。 ポリシーの編集時にポリシーをロックまたはロック解除するアイコンがポリシー名の横に追加されました。さらに、他の管理者によってロックされたポリシーのロックを解除できるようにする新しい権限（アクセス コントロール ポリシー ロックのオーバーライド）が追加されました。この権限は、デフォルトで管理者、アクセス管理者、およびネットワーク管理者のロールで有効になっています。

機能	説明
オブジェクトグループ検索をデフォルトで有効化。	**アップグレードの影響** [オブジェクトグループ検索（Object Group Search）] の設定がデフォルトで有効になりました。バージョン 7.2 以降にアップグレードすると、この設定が有効になります。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]** > **[デバイス（Device）]** > **[詳細設定（Advanced Settings）]**
アクセス制御ルールのヒットカウントは再起動後も存続します。	管理対象デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントはHAペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 新規/変更された CLI コマンド：**show rule hits**。
アクセスコントロールポリシーのユーザビリティの改善。	アクセスコントロールポリシーで使用できる新しいユーザーインターフェイスが追加されました。従来のユーザーインターフェイスを引き続き使用することも、新しいユーザーインターフェイスを試すこともできます。 新しいインターフェイスは、ルールリストのテーブルビューとグリッドビュー、列を表示または非表示にする機能、高度な検索機能、無限スクロール機能を備え、アクセス コントロール ポリシーが割り当てられたポリシーに関するパケットフローのビューがより明確になりました。また、ルール作成用の追加/編集ダイアログボックスがシンプルになりました。アクセス コントロール ポリシーの編集中に、従来のユーザーインターフェイスと新しいユーザーインターフェイスを自由に切り替えることができます。
イベントロギングおよび分析	

機能	説明
SecureX との統合、SecureX とのオーケストレーションの改善	SecureX との統合プロセスが合理化されました。すでに SecureX アカウントを持っている場合は、新しい [統合（Integration）] > [SecureX] ページで該当するクラウドリージョンを選択し、[SecureXの有効化（Enable SecureX）] をクリックして、SecureX に対して認証するだけです。イベントをクラウドに送信するオプション、およびCisco Success Network と Cisco Support Diagnostics を有効にするオプションも、この新しいページに移動されました。 この新しいページでSecureXとの統合を有効にすると、システムのクラウド接続のライセンス管理が Cisco Smart Licensing から SecureX に切り替わります。SecureX を「従来の」方法ですでに有効にしている場合、このクラウド接続管理による利点を得るには、無効にしてから再度有効にする必要があります。 Webインターフェースで示されていない場合でも、このページでは対象のクラウドリージョンや、シスコのセキュリティ分析とロギング（SaaS） を使用して Secure Network Analytics（Stealthwatch）クラウドに送信するイベントタイプも管理することを覚えておいてください。以前のバージョンでは、このオプションは、**システム**（⚙）> [統合（Integration）] > [クラウドサービス（Cloud Services）] にありました。SecureX を有効にしても、Secure Network Analytics クラウドとの通信には影響しません。両方にイベントを送信できます。 management center は SecureX オーケストレーションもサポートするようになりました。これは、セキュリティツール全体のワークフローを自動化するために使用できる強力なドラッグアンドドロップインターフェイスです。SecureX を有効にすると、オーケストレーションを有効にできます。 この機能は、バージョン7.0.2以降のメンテナンスリリースでもサポートされています。バージョン 7.1 ではサポートされていません。

機能	説明
セキュリティイベントのログを複数の Cisco Secure Network Analytics オンプレミスデータストアに記録。	Cisco Secure Network Analytics Data Store（マルチノード）との統合を設定する際、セキュリティイベント用に複数のフローコレクターを追加できるようになりました。各フローコレクターを、バージョン 7.0 以降を実行している 1 つ以上の Threat Defense デバイスに割り当てます。 新規/変更された画面： • セットアップ：**[統合（Integration）]** > **[セキュリティ分析とロギング（Security Analytics & Logging）]** > **[Secure Network Analytics Data Store]** • 変更：**[統合（Integration）]** > **[セキュリティ分析およびロギング（Security Analytics & Logging）]** > **[デバイス割り当ての更新（Update Device Assignments）]** この機能には、Cisco Secure Network Analytics バージョン 7.1.4 が必要です。
データベースアクセスの変更。	10 個の新しいテーブルを追加し、1 個のテーブルを廃止し、6 個のテーブルで結合を禁止しました。また、Snort 3 サポートのためにさまざまなテーブルにフィールドを追加し、可読形式でタイムスタンプと IP アドレスを提供しました。 詳細については、『Cisco Secure Firewall Management Center Database Access Guide, Version 7.2』の新機能のトピックを参照してください。
eStreamer の変更。	新しい Python ベースの参照クライアントが SDK に追加されました。また、完全修飾イベントをリクエストできるようになりました。詳細については、『Cisco Secure Firewall Management Center Event Streamer Integration Guide, Version 7.2』の新機能のトピックを参照してください。
アップグレード	

機能	説明
デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	management center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレード パッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、management center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。 この機能は、同じスタンドアロン management center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。 • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。 バージョン 7.1 以降の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ます。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。 • 高可用性 management center によって管理されるデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • 分析モードで management center に追加された CDO 管理対象デバイス。 • management center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	説明
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	バージョン 7.2 以降の Management Center を使用して Threat Defense をアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 このオプションは、バージョン 7.2 以降への Threat Defense のメジャーアップグレードおよびメンテナンスアップグレードでサポートされています。バージョン 7.0 または 7.1 への Threat Defense のアップグレード、または任意のバージョン向けのパッチではサポートされていません。
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（**[デバイス（Devices）]** > **[デバイスのアップグレード（Device Upgrade）]**）を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**[システム（System）]** > **[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100

機能	説明
CLI からの Threat Defense アップグレードの復元。	Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべて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。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 **注意** CLIから復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。
管理とトラブルシューティング	
Secure Firewall 3100 のパケットドロップ統計。	新しい **show packet-statistics** 脅威防御 CLI コマンドは、ポリシーに関連しないパケットドロップに関する包括的な情報を表示します。これまでは、いくつかのコマンドを使用してこの情報を表示する必要がありました。
DNS 要求を解決するための複数の DNS サーバーグループ。	クライアントシステムからの DNS 要求を解決するために、複数の DNS グループを設定できます。これらの DNS サーバー グループを使用して、さまざまな DNS ドメインの要求を解決できます。たとえば、インターネットへの接続で使用するために、パブリック DNS サーバーを使用するキャッチオールのデフォルトグループを作成できます。次に、example.com ドメイン内のマシンへの接続など、内部トラフィックに内部 DNS サーバーを使用する別のグループを構成できます。したがって、組織のドメイン名を使用した FQDN への接続は、内部 DNS サーバーを使用して解決されますが、パブリックサーバーへの接続は外部 DNS サーバーを使用します。 新規/変更された画面：**[プラットフォーム設定（Platform Settings）]** > **[DNS]**
使用タイプごとに脅威防御を使用して証明書の検証を設定します。	トラストポイント（脅威防御デバイス）で検証が許可される使用タイプを指定できるようになりました：IPsec クライアント接続、SSL クライアント接続、および SSL サーバー証明書。 新規/変更された画面：証明書登録オブジェクトに [検証の使用（Validation Usage）] オプションを追加しました：**[オブジェクト（Objects）]** > **[オブジェクトマネージャ（Object Manager）]** > **[PKI]** > **[証明書の登録（Cert Enrollment）]**。

機能	説明
展開で管理接続が失われた場合の自動ロールバック。	展開によって Management Center と Threat Defense 間の管理接続がダウンした場合に備えて、設定の自動ロールバックを有効にできるようになりました。以前は、**configure policy rollback** コマンドを使用して手動で設定をロールバックすることしかできませんでした。 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）] > [展開設定（Deployment Settings）] • [展開（Deploy）] > [高度な展開（Advanced Deploy）] > [プレビュー（Preview）] • [展開（Deploy）] > [展開履歴（Deployment History）] > [プレビュー（Preview）]
設定の変更を展開するときに、レポートを生成して電子メールで送信します。	任意の展開タスクのレポートを生成できるようになりました。このレポートには、展開された設定に関する詳細が含まれています。 新規/変更されたページ：**[展開（Deploy）] > [展開履歴（Deployment History）]**[アイコン（icon）]**その他**（⋮）[全般的なレポート（Generate Report）]。
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、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。 バージョン 7.2 以降の Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されてインポートされます。ただし、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）、必ず両方の GeoDB パッケージを取得してインポートしてください。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar 地理位置情報の更新（**システム**（⚙） > [更新（Updates）] > [地理位置情報の更新（Geolocation Updates）]）ページと概要ページ（[ヘルプ（Help）] > [概要（About）]）には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

機能	説明
Webインターフェイスのフランス語オプション。	Management Center の Web インターフェイスをフランス語に切り替えることができるようになりました。 新規/変更された画面：**システム**（⚙）>[設定（Configuration）]>[言語（Language）]
Webインターフェイスの変更：展開とユーザーアクティビティの統合。	バージョン 7.2 では、すべてのケースで以下の Management Center メニューオプションが変更されています。 **[展開（Deploy）]>[展開履歴（Deployment History）]** は次に変更されました。 [展開（Deploy）]>**[展開履歴（Deployment History）]**（右下隅） **[展開（Deploy）]>[展開（Deployment）]** は次に変更されました。 [展開（Deploy）]>[高度な展開（Advanced Deploy）] [分析（Analysis）]>[ユーザー（Users）]>[アクティブなセッション（Active Sessions）] は次に変更されました。 [統合（Integration）]>[ユーザー（Users）]>[アクティブなセッション（Active Sessions）] [分析（Analysis）]>[ユーザー（Users）]>[ユーザー（Users）] は次に変更されました。 [統合（Integration）]>[ユーザー（Users）]>[ユーザー（Users）] [分析（Analysis）]>[ユーザー（Users）]>[ユーザーアクティビティ（User Activity）] は次に変更されました。 [統合（Integration ）]>[ユーザー（Users）]>[ユーザーアクティビティ（User Activity）]

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 7.0.1 以前、またはバージョン 7.1 からアップグレードする場合、バージョン 7.2 では Management Center のメニューオプションが変更されます。 （注） バージョン 7.0.2 またはそれ以降のバージョン 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、メニュー構造はすでに次のようになっています。 [AMP] > [AMP管理（AMP Management）] は次に変更されました。 [統合（Integration）] > [AMP] > [AMP管理（AMP Management）] [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] は次に変更されました。 [統合（Integration）] > [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] [インテリジェンス（Intelligence）] > [ソース（Sources）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [ソース（Sources）] [インテリジェンス（Intelligence）] > [要素（Elements）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [要素（Elements）] [インテリジェンス（Intelligence）] > [設定（Settings）] は次に変更されました。 [統合（Integration）] > [インテリジェンス（Intelligence）] > [設定（Settings）] [インテリジェンス（Intelligence）] > [インシデント（Incidents）] は次に変更さ [統合（Integration）] > [インテリジェンス（Intelligence）] > [インシデント（Incidents）]

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

Management Center REST API

新機能と既存の機能をサポートするために、Management Center REST API サービスと操作が追加されました。詳細については、『Cisco Secure Firewall Management Center REST API Quick Start Guide, Version 7.2』を参照してください。廃止されたサービス/操作については、Management Center バージョン 7.2 で廃止済みの機能 （42 ページ）を参照してください。

シャーシ	• breakoutinterfaces • evaluateoperation • joininterfaces
展開	• downloadreports • emailreports
デバイス	• eigrproutes • devicesettings • changemanagers

機能	説明
統合	• ebssnpshot • umbrellaconnections、testumbrellaconnections
License	• devicelicenses • smartlicenses
オブジェクト	• anyconnectexternalbrowserpackages、anyconnectpackages、anyconnectprofiles • certenrollments • certificatemaps • grouppolicies • hostscanpackages • ipv4addresspools、ipv6addresspools • radiusservergroups • ssoservers • umbrellaprotectionpolicies
ポリシー	• DNS：umbrelladnspolicies、umbrelladnsrules • NAT：autonatrules、manualnatrules • Health：healthpolicies • Remote access VPN：addressassignmentsettings、certificatemapsettings、connectionprofiles、ipsecadvancedsettings、ipseccryptomaps、ldapattributemaps、ravpns • Site-to-site VPN：s2svpnsummaries • Operational（non-policy-specific）：policylocks
検索	• デバイス
Status	• taskstatuses
トラブルシューティング	• task
アップグレード	• upgradesnapshot

Device Manager バージョン 7.2 の新機能

機能	説明
ファイアウォールと IPS の機能	
オブジェクトグループ検索は、アクセス制御のためにデフォルトで有効になっています。	CLI 構成コマンド **object-group-search access-control** は現在、デフォルトで有効になっています。FlexConfig を使用してコマンドを構成している場合は、FlexConfig オブジェクトを削除できます。この機能を無効にする必要がある場合は、FlexConfig を使用して **no object-group-search access-control** コマンドを実装します。
ルールのヒットカウントは再起動後も存続します。	デバイスを再起動しても、アクセス制御ルールのヒットカウントがゼロにリセットされなくなりました。カウンタを能動的にクリアした場合にのみ、ヒットカウントがリセットされます。さらに、カウントは HA ペアまたはクラスタ内の各ユニットによって個別に維持されます。**show rule hits** コマンドを使用して、HA ペアまたはクラスタ全体の累積カウンタを表示したり、ノードごとのカウントを表示したりできます。 次の Threat Defense CLI コマンドを変更しました：**show rule hits**。
VPN 機能	
IPsec フローがオフロードされます。	Cisco Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティ アソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールド プログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
インターフェイス機能	
Cisco Secure Firewall 3130 および 3140 のブレークアウトポートのサポート。	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成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）]** > **[インターフェイス（Interfaces）]**
インターフェイスでの Cisco TrustSec の有効化または無効化。	名前付きか名前なしかにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。 インターフェイス構成ダイアログボックスに [Propagate Security Group Tag] 属性を追加し、さまざまなインターフェイス API に **ctsEnabled** 属性を追加しました。
ライセンシング機能	

機能	説明
ISA 3000 の永久ライセンス予約のサポート。	ISA 3000 は、承認されたお客様向けのユニバーサル永久ライセンスの予約をサポートす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	
完全な展開を強制する機能。	変更を展開すると、システムは通常、最後の正常な展開以降に加えられた変更のみを展開します。ただし、問題が発生した場合は、デバイスの構成を完全に更新するフル展開を強制するように選択できます。展開ダイアログボックスに [Apply Full Deployment] オプションを追加しました。
Threat Defense REST API バージョン 6.3（v6）。	ソフトウェアバージョン 7.2 の Threat Defense REST API はバージョン 6.3 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。6.3 の URL バージョンパス要素は、6.0、6.1 および 6.2 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、Device Manager 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 7.2 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 *7.2.0* 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
Secure Firewall 3100 の NetMod。	Cisco Secure Firewall 3100 向けに次の NetMod が導入されました。 • 6 ポート 1 G SFP Fail-to-Wire ネットワークモジュール、SX（マルチモード）（FPR3K-XNM-6X1SXF） • 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-6X10SRF） • 6 ポート 10 G SFP Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X10LRF） • 6 ポート 25 G SFP Fail-to-Wire ネットワークモジュール、SR（マルチモード）（FPR3K-XNM-X25SRF） • 6 ポート 25 G Fail-to-Wire ネットワークモジュール、LR（シングルモード）（FPR3K-XNM-6X25LRF） • 8 ポート 1 G 銅ケーブル Fail-to-Wire ネットワークモジュール（銅ケーブル）（FPR3K-XNM-8X1GF） Management Center を導入すると、これらの NetMod がハードウェアバイパスをサポートします。
Alibaba 向け Management Center Virtual および Threat Defense Virtual。	Alibaba 向けの Secure Firewall Management Center Virtual および Secure Firewall Threat Defense が導入されました。Management Center を使用して、Alibaba 向け Threat Defense Virtual を管理する必要があります。デバイスマネージャーはサポートされていません。 Alibaba インフラストラクチャの根本的な問題により、Threat Defense Virtual のインスタンスタイプ ecs.g5ne.4xLarge は、特に 1 秒あたりの接続数（CPS）に関してパフォーマンスが低いことに注意してください。2xlarge または 4xlarge を推奨します。
デバイスマネージャが GCP 向け Threat Defense Virtual をサポート。	デバイスネージャを使用して、GCP 対応 Threat Defense Virtual を構成できるようになりました。

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。

- Management Center：**[ヘルプ（Help）]** > **[概要（About）]**を選択します。
- Device Manager ：**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

Management Center バージョン 7.2 で廃止済みの機能

表 *11 : Management Center* バージョン *7.2.0* で廃止済みの機能

機能	アップグレードの影響	説明
EIGRP FlexConfig オブジェクト。	なし。ただし、アップグレード後に構成をやり直す必要があります。	Management Center の Web インターフェイスから EIGRP ルーティングを設定できるようになりました。Management Center バージョン 7.2 の新機能 （13 ページ） を参照してください。 次の FlexConfig オブジェクトは不要になりました：Eigrp_Configure、Eigrp_Interface_Configure、Eigrp_Unconfigure、Eigrp_Unconfigure_all。 および、次の関連するテキストオブジェクトが廃止されました：eigrpAS、eigrpNetworks、eigrpDisableAutoSummary、eigrpRouterId、eigrpStubReceiveOnly、eigrpStubRedistributed、eigrpStubConnected、eigrpStubStatic、eigrpStubSummary、eigrpIntfList、eigrpAS、eigrpAuthKey、eigrpAuthKeyId、eigrpHelloInterval、eigrpHoldTime、eigrpDisableSplitHorizon。 システムでは、アップグレード後に展開できますが、EIGRP 構成をやり直すように警告されます。このプロセスを支援するために、コマンドライン移行ツールが用意されています。詳細については、コンフィギュレーションガイドの FlexConfig ポリシーの移行 を参照してください。

機能	アップグレードの影響	説明
VXLAN FlexConfig オブジェクト。	なし。ただし、アップグレード後に構成をやり直す必要があります。	Management Center の Web インターフェイスから VXLAN インターフェイスを設定できるようになりました。Management Center バージョン 7.2 の新機能 （13 ページ） を参照してください。 次の FlexConfig オブジェクトは不要になりました：VxLAN_Clear_Nve、VxLAN_Clear_Nve_Only、VxLAN_Configure_Port_And_Nve、VxLAN_Make_Nve_Only、VxLAN_Make_Vni。 これらの関連するテキストオブジェクト：vxlan_Port_And_Nve、vxlan_Nve_Only、vxlan_Vni。 以前のバージョンで FlexConfig を使用して VXLAN インターフェイスを設定した場合、それらは引き続き機能します。実際、この場合は FlexConfig が優先されます。Web インターフェイスで VXLAN 設定をやり直す場合は、FlexConfig 設定を削除します。
アップグレード前の自動トラブルシューティング。	管理センターのアップグレードは高速化され、使用するディスク容量も少なくなりましたが、アップグレード前のトラブルシューティング ファイルは含まれません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センターのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]** を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。
REST API で SecureX との統合を設定。	なし。	SecureX 統合の改善の一環として（Management Center バージョン 7.2 の新機能 （13 ページ） を参照）、REST API を使用して SecureX との統合を設定できなくなりました。管理センターの Web インターフェイスを使用する必要があります。

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。

⚠

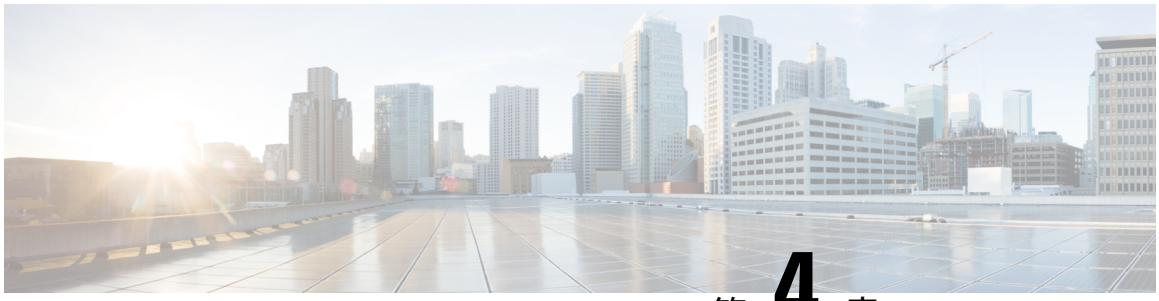
注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

FlexConfig について

いくつかの Threat Defense 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 7.2 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 （65 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 （45 ページ）
- アップグレードする最小バージョン （46 ページ）
- バージョン 7.2 のアップグレードガイドライン （47 ページ）
- FXOS のアップグレードガイドライン （49 ページ）
- 応答しないアップグレード （50 ページ）
- アップグレードを元に戻す （51 ページ）
- トラフィック フローとインスペクション （51 ページ）
- 時間とディスク容量のテスト （56 ページ）

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-72-docs）を参照してください。

表 *12*：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 7.2 に直接アップグレードできます。

バージョン 7.2 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。

表 13 : バージョン 7.2 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
Management Center	6.6
Threat Defense （GCP 対応 Threat Defense Virtual を除く）	6.6 Firepower 4100/9300 には FXOS 2.12.0.31 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 2.12 リリースノートを参照してください。
GCP 向け Threat Defense Virtual	7.2 GCP 向け Threat Defense Virtual は、バージョン 7.2 を飛び越してアップグレードできません。つまり、バージョン 7.1 以前からバージョン 7.2 以降にアップグレードすることはできません。「GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない（48 ページ）」を参照してください。

バージョン 7.2 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 14 : Management Center を使用した Threat Defense のアップグレードガイドラインバージョン 7.2

✓	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 （46 ページ）	任意（Any）	任意（Any）	7.2
	FXOS のアップグレードガイドライン （49 ページ）	Firepower 4100/9300	任意（Any）	7.2
	GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない （48 ページ）	GCP 用 Threat Defense Virtual	6.7.0 ～ 7.1.x	7.2 以降
	高可用性 Management Center の Cisco Secure Malware Analytics に再接続する （48 ページ）	Management Center	6.4.0 ～ 6.7.x	7.0 以上

✓	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：Firepower 1010 スイッチポートでの無効な VLAN ID （49 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 以降

表 *15 : Device Manager* を使用した *Threat Defense* のアップグレードガイドラインバージョン *7.2*

✓	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 （46 ページ）	任意（Any）	任意（Any）	7.2
	FXOS のアップグレードガイドライン （49 ページ）	Firepower 4100/9300	任意（Any）	7.2
	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 （49 ページ）	Firepower 1010	6.4.0 ～ 6.6.x	6.7 以降

GCP 向け Threat Defense Virtual はバージョン 7.2.0 を飛び越してアップグレードできない

展開対象：GCP 向け Threat Defense Virtual

アップグレード元：バージョン 6.7.0 ～ 7.1.x

直接アップグレード先：バージョン 7.2.0 以降

自動スケーリングのサポートに必要なインターフェースの変更により、GCP 向け Threat Defense Virtual のアップグレードはバージョン 7.2.0 を飛び越すことができません。つまり、バージョン 7.1.x 以前からバージョン 7.2.0 より後にアップグレードすることはできません。新しいインスタンスを展開し、デバイス固有の設定をやり直す必要があります。

高可用性 Management Center 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 management center 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、Threat Defense 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。

FXOS のアップグレードガイドライン

Firepower 4100/9300 の場合、Threat Defense 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。Threat Defense 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することもできます。

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。

Threat Defense 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 7.2 を実行するために必要な FXOS の最小バージョンは、FXOS 2.12.0.31 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 （51 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 Management Center

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 Threat Defense 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。

- Management Center：[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。
- Device Manager ：[システムアップグレード（System Upgrade）] パネルを使用します。

Threat Defense CLI を使用することもできます。

（注） デフォルトでは、Threat Defense 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

Threat Defense のメジャーアップグレードまたはメンテナンス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、復元が可能な場合があります。 復元すると、ソフトウェアは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）。パッチ適用後に復元すると、パッチも必然的に削除されます。

パッチまたはホットフィックスでは、復元はサポートされていません。 復元の手順については、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。

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 *16 :* 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。

導入	トラフィックの挙動	メソッド
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。

Management Center を使用した Threat Defense 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 *17:* 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。

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
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。

シングルユニットのクラスタでは、ヒットレスアップグレードはサポートされないことに注意してください。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。

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 *18 :* 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

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
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。

Device Manager を使用した Threat Defense 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、management center 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 （50 ページ） を参照してください。

表 *19*: 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、management center 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。
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。

条件	詳細
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 management center（/Volume または /var 内）に必要な容量も報告します。Threat Defense 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 Device Manager 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 *20 :* ディスク容量の確認

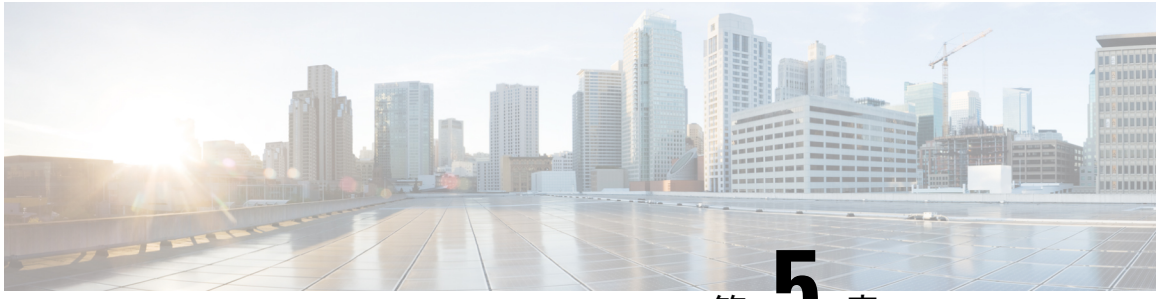
プラットフォーム	コマンド
Management Center	**[システム（System）]**>**[モニタリング（Monitoring）]**>**[統計（Statistics）]**を選択し、management center を選択します。[Disk Usage] で、[By Partition] の詳細を展開します。
Threat Defense with management center	**[System]** > **[Monitoring]** > **[Statistics]**を選択し、確認するデバイスを選択します。[Disk Usage] で、[By Partition]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

バージョン 7.2.0 の時間とディスク容量

表 *21 :* バージョン *7.2.0* 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	Management Center の必要容量	アップグレード時間	リブート時間
Management Center	バージョン 6.6.0 ～ 6.7.0	/var 内で 16.7 GB	/ 内で 51 MB	—	30 分	9 分
	バージョン 7.0 以降	/Volume 内で 19.1 GB	/ 内で 45 MB			
Management Center Virtual：VMware	バージョン 6.6.0 ～ 6.7.0	/var 内で 16.7 GB	/ 内で 50 MB で	—	30 分	5 分
	バージョン 7.0 以降	/Volume 内で 19.2 GB	/ 内で 45 MB			
Firepower 1000 シリーズ		—	/ngfw 内で 7.6 GB	930 MB	15 分	13 分
Firepower 2100 シリーズ		—	/ngfw 内で 7.7 GB	1.0 GB	13 分	13 分
Secure Firewall 3100 シリーズ		—	使用できません	1.2 GB	使用できません	使用できません
Firepower 4100 シリーズ		—	/ngfw 内で 7.8 GB	880 MB	12 分	9 分
Firepower 4100 シリーズ コンテナ インスタンス		—	/ngfw 内で 7.9 GB	880 MB	12 分	8 分
Firepower 9300		—	/ngfw 内で 11.2 GB	880 MB	11 分	12 分

プラットフォーム		ボリュームの容量	必要容量	Management Center の必要容量	アップグレード時間	リブート時間
ISA 3000	バージョン 6.6.0	/home 内で 9.3 GB	/ngfw 内で 270 KB	1.0 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 ～ 7.1.0	/ngfw/var 内で 9.3 GB	/ngfw/bin 内で 270 KB			
Threat Defense Virtual：VMware	バージョン 6.6.0	/home 内で 4.6 GB	/ngfw 内で 350 KB	1.0 GB	11 分	8 分
	バージョン 6.7.0	/ngfw/Volume 内で 4.4 GB	/ngfw 内で 350 KB			
	バージョン 7.0.0 ～ 7.1.0	/ngfw/var 内で 5.4 GB	/ngfw/bin 内で 250 KB			



第 5 章

ソフトウェアのインストール

バージョン7.2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 （61 ページ）
- 設置ガイド （64 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。management center の展開では、デバイスを経由せずに management center 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、management center 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 *22 : 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
management center を再イメージ化します。	手動で登録解除します。
management center のモデルを移行します。	ソースの management center をシャットダウンする前に、手動で登録を解除します。
management center で Threat Defense を再イメージ化します。	management center 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。
Device Manager で Threat Defense を再イメージ化します。	手動で登録解除します。
management center からデバイスマネージャーに Threat Defense を切り替えます。	management center 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 management center に Threat Defense 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。

management center 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、management center 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 *23*：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
management center を再イメージ化します。	管理からデバイスを削除します。
Threat Defense 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 management center に Threat Defense 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 Threat Defense 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 Threat Defense 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。

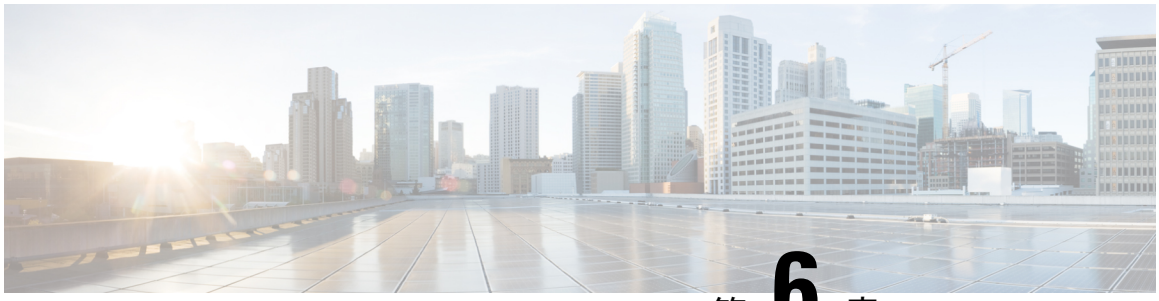
表 *24*：完全な再イメージ化のシナリオ

モデル	詳細
Firepower 1000 シリーズ 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	Threat Defense 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、Threat Defense 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。Threat Defense 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 Threat Defense 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 *25*：設置ガイド

プラットフォーム	ガイド
Management Center	
FMC 1600、2600、4600	Cisco Firepower Management Center 1600、2600、4600 スタートアップガイド
Management Center Virtual	Cisco Secure Firewall Management Center Virtual 入門ガイド
Threat Defense	
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
Threat Defense Virtual	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 7.2 で未解決のバグ （65 ページ）
- 解決済みのバグ バージョン 7.2 （66 ページ）

バージョン 7.2 で未解決のバグ

バージョン 7.2.0 で未解決のバグ

表 *26* : バージョン *7.2.0* で未解決のバグ

不具合 ID	タイトル
CSCwb43433	ジャンボフレームのパフォーマンスが Firepower 2100 シリーズで最大 45% 低下
CSCwb78233	7.1.0 からのアップグレード後に 7.2.0 1984 Nutanix vFMC にアクセスできない
CSCwb80789	以前に復号されたサイトへの TLS 1.3 の接続が失敗することがある
CSCwb87724	削除されたユニットが既存のクラスタに再参加したものの、コントロールとその他の削除された vFTD クラスタにリストされない

不具合 ID	タイトル
CSCwb88887	snp_fp_vxlan_encap_and_grp_send_common：adj. bp->l3_type = 8, inner_sip メッセージが見つかりませんでした
CSCwb89905	JF とともに vFTD をインストールしたものの、有効にして vFTD を再起動する JF に関する情報が FMC に引き続き表示される
CSCwb90105	Nutanix 用の FTDv における 7.2 へのアップグレードが再起動後にスタックする
CSCwb94573	3140 - プラットフォーム障害 - コード：F1374 - 重大度：クリティカル
CSCwb96990	初期のデータが原因で xtls がプローブの応答を待たない場合がある
CSCwb97486	FPR3100：25G 光ファイバが一部の 1/10G 対応光ファイバポートのみでリンクをアップと表示する場合がある
CSCwb99960	onPremFMC に CDO 管理対象デバイスのみが登録されている場合、マルウェアイベントページにライセンス警告が表示される

解決済みのバグ バージョン 7.2

バージョン 7.2.0 で解決済みのバグ

表 *27*：バージョン *7.2.0* で解決済みのバグ

不具合 ID	タイトル
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
CSCvz67001	リモート SSH ストレージターゲットへの FMC イベントバックアップが失敗する
CSCvy46482	S2S VPN で暗号 ACL が使用されているときに作成される冗長 service-object グループ
CSCwb22359	誤った再起動とイベントのログ記録の増加を防ぐことを目的としたポートマネージャ/LACP の改善
CSCwb64551	FMC バックアップの失敗：Monetdb バックアップ失敗コード 102
CSCwa00038	/mnt/disk0 パーティションがいっぱいになってブレードが再起動されるとディスクが破損する

不具合 ID	タイトル
CSCwa40223	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCwa45656	管理対象デバイスで SLR ライセンスアプリケーションが失敗する
CSCwa34110	FMC は南半球の DST 設定をサポートする必要がある
CSCwa32956	展開の競合状態により、接続イベントが Firepower Management Center に送信されない
CSCvz40765	FMC CPU グラフに表示される Snort コアとシステムコアの数が間違っている
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
CSCwa12688	再試行が無効なため、Radius 外部認証オブジェクトを FTD にインストールできない
CSCwb40001	SNMP コマンド実行時の長い遅延
CSCwa95694	ASA-SFR モジュールで SSL ポリシーが有効になっていると Snort コアが断続的に生成される
CSCwa08262	マッピングされたグループポリシーを持つ AnyConnect ユーザーは、トンネルグループの下にあるデフォルト GP から属性を取得します
CSCvz27235	複数のシスコ製品の Snort Modbus におけるサービス妨害の脆弱性
CSCvz14377	MySQL DB と EO から管理者とその他のユーザーが失われる
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
CSCvz68336	複数のインラインペアでの単一接続が原因で SSL 復号化が機能しない
CSCvx75683	「show cluster info trace」の出力が「タグが存在しません」というメッセージにより負担がかかっています
CSCwa79604	タスクリストのジョブが無限に実行される
CSCwa43497	AnyConnect-SSL の ICMP PMTU を送信するときにデータパスのデッドロックが発生する
CSCvx59252	FXOS は管理インターフェイスのログファイルをローテーションしていません
CSCwa15093	アクセス ポリシー コントロール クリア ヒット カウントで「エラー 403：禁止（Error 403: Forbidden）」がスローされる

不具合 ID	タイトル
CSCwa06608	セカンダリでフェールオーバーをアクティブにすると WM 1010 HA フェールオーバーが成功しない
CSCvz41761	FMC では、$ 文字を使用した EIGRP 認証秘密鍵の作成は許可されない
CSCwb46481	FMC のアップグレード後に SNMPv3 が機能しない
CSCvq29993	FPR2100 のみ：サイズが 80、256、1550 のメモリブロックで永続的なブロックリークとブラックホールトラフィックが発生
CSCwa70323	AnyConnect VPN のカスタム属性の一部として、1,024 文字を超える余分なドメインをプッシュできない
CSCwb46340	アップグレード中に Elektra のアップグレードに失敗した
CSCvz77050	ポリシー展開の失敗が成功と報告されることがある
CSCvz61456	明確な理由がなく ASA アプリケーションのソフトウェアアップグレードが失敗することがある
CSCwb16561	FMC GUI が侵入ポリシーをロードしない
CSCwa74984	FMC のアップグレード後に [FMCアクセスの詳細（FMC Access Details）] -> [設定（Configuration）] タブを開けない
CSCvy89713	FMC のアップグレード後に FMC プロセス dbsrv16 の CPU 使用率が高くなる
CSCvz73583	VDB と GEODB をダウンロードするときに、FTD がプロキシサーバーに認証情報を送信しない
CSCvz02027	パケットで利用できない場合は URL からホストを更新し、null ホストの http リクエストのクラウドルックアップを停止する
CSCwa84862	FMC の標準アクセスリストオブジェクトを削除または変更できない
CSCvz03524	sha1 ではなく sha256 リクエストが原因で PKI の「OCSP 失効チェック」が失敗する
CSCwa85340	ネストされた大きいオブジェクトを含むアクセスポリシーで PDF を生成できない
CSCwa27488	「テーブルではありません（is not a table）」というエラーでインポートが失敗する
CSCwa89689	snort3 で「早期アプリケーション検出」を有効にすると、FTD によって削除された TLS でサーバー hello が実行される
CSCwb50405	暗号ハッシュ関数での ASA/FTD のトレースバック

不具合 ID	タイトル
CSCvz08588	検出されたアイデンティティ レルム ユーザーに対するユーザーに認識されないアラーム
CSCug96057	同じカテゴリのデバイスが複数のカテゴリ名で分類される
CSCwb11939	ASA/FTD MAC の変更が、INSPECT がオンになっているフラグメント化されたパケットの処理で見られる
CSCvz09109	ヘッダーのみが設定されているにもかかわらず、クラスタ CCL インターフェイスのキャプチャでフルパケットが表示される
CSCwb20940	FMC：検出モードでの SSL/Snort3/NAP の組み合わせの検証チェックを追加
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
CSCwa55868	snort2 による QP vFTD ポリシーの展開が未定義のパッケージ変数で失敗した
CSCvz78331	再イメージ化後に SNMP ポーリングが失敗する
CSCwa70482	MAC ポップアップの ASDM によって hostscan/CSD pkg が削除される
CSCvz62517	SRU のインストールでは完了時にファイルを検証する必要がある
CSCwa41918	SSL インスペクションで、証明書を削除するときに予期しない動作が発生する場合がある
CSCvz29656	index.cgi のメモリ使用率が高くなる FMC 接続イベント検索
CSCvz78548	[デバイス（Devices）] --> [証明書（Certificates）] ページを読み込めない
CSCwa79676	HA 印刷の FPR1010 で複数のインターフェイスのブロードキャスト ストーム アラートが発生する
CSCwa81395	巧妙に細工されたリクエスト本文がバッファオーバーフローを引き起こす可能性がある
CSCwa81143	アプリケーション ポリシー フィルタを保存できない[保存（Save）] タブがスタックして継続的に読み込まれる
CSCvy75131	削除したセンサー/インターフェイスがセキュリティゾーンから削除されないことがある
CSCvz73957	FTD が EventHandler コアで syslog ID 430002 および 430003 の生成を停止する
CSCvy24921	SNMPv3：構成が変更されるたびに SNMP EngineID が変更される

不具合 ID	タイトル
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
CSCwa97423	展開をロールバックすると、操作の順序が原因で短時間トラフィックがドロップされる
CSCvz89106	複数のシスコ製品のサーバー名識別におけるデータ漏洩の脆弱性
CSCwa11088	ページの更新/読み込み前に編集しようとすると、制御ルールの順序が自動的に変更される
CSCvz62261	ASDM の使用時にユーザーアクセスを制限できない
CSCwb19387	ASA SNMP ポーリングが失敗し、「現在この要求を受け入れることができません。後で再試行してください。（Unable to honour this request now. Please try again later.）」と表示される
CSCwa98983	KP-HA での 7.1.0.1-25 のアップグレードが 800_post/901_reapply_sensor_policy.pl で失敗した
CSCwa83078	snort3：復号されていない再開されたセッションが失敗することがある
CSCwb42846	Snort インスタンスで CPU 使用率が 100% になりスタックする
CSCwb59218	DAP エンドポイント基準を「無効」として保存できない
CSCvx90486	ifXTable の snmpwalk がデータインターフェイスを返さないことがある
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
CSCvz13564	Firepower 2100 FTD：アップグレード後に ssh-access-list 設定が失われる
CSCwa35179	FTD AC VPN 証明書がリロードで失われる
CSCwb84225	ASDM および ASA REST API の評価版 OpenJDK CVE
CSCwa38996	snmpd.log leading で大量のメッセージが繰り返されてログサイズが大きくなる
CSCvy80380	FPR4150-ASA シャーシのディスク使用率によって /var/tmp が増加している
CSCwb01126	FDM 7.1.0 の RA VPN ページで設定すると、DNS サーバーの設定が失われる
CSCwa68004	FMC 7.0 FlexConfig が代替のないトランスペアレント FTD の mac-address-table age-time をブロックした

不具合 ID	タイトル
CSCwb29126	FMC のレルム AD プライマリドメイン設定でアンダースコア（_）を使用できない
CSCwa99370	ASDM:DAP 設定に AAA 属性タイプがない（Radius/LDAP）
CSCwa89560	ルールの検索後に NAT ルールを修正するとルールの順序が変わる
CSCvy33501	FDM フェールオーバーペア：新しく設定された sVTI IPSEC SA がスタンバイと同期されない。FDM は HA が同期していないことを示しています
CSCwa75077	プレフィルタルールに時間範囲オブジェクトが誤って入力される
CSCwb07319	権限付与タグに無効な文字が含まれている
CSCwa91070	バックアッププロセスの oom-k をトリガーする Cgroup
CSCwa45369	コマンドを実行すると、新しいゾンビプロセスが発生するように見える
CSCwb44048	FMC ヘルス モニタリング ダッシュボードのイベントレートが非常に高い値を示している
CSCvz72467	Cisco FXOS および NX-OS ソフトウェアの Cisco Discovery Protocol サービスのサービス拒否
CSCwb37999	カスタマイズされた変数名が原因で Snort3 検証が失敗する
CSCvz73315	FMC で接続イベントが表示されず、SFDataC が to_import dir からのイベントを処理しない
CSCwb21704	FDM：検出モードにおける SSL/Snort3/NAP の組み合わせの検証チェックを追加
CSCwb32841	NAT (any,any) ステートメントは、フェールオーバー インターフェイスの状態を示し、結果としてスプリット ブレイン イベントが発生する
CSCvz79930	Snort3.dmp および crashinfo ファイルがディスクマネージャによって管理されない
CSCwa51867	FDM IKEv2 S2S PSK が正しく展開されない（非対称 PSK から対称 PSK への変更）
CSCwa39683	SSL デバッグが有効になっている場合、ssl_policy log_error メッセージによってログファイルがあふれる
CSCwa25033	セグメンテーション違反を引き起こす予期しない HTTP/2 データフレーム
CSCwa39680	SSL 復号のデバッグを有効にすると、Snort がパケット処理を停止する（Snort2）

不具合 ID	タイトル
CSCvz24238	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCwa31373	ルールをコピーすると、FMC 6.6.5 で重複する ACP ルールが生成される
CSCwa43311	サイズが大きい（1G）ファイルをダウンロードすると、Snort がパケットをブロックしてドロップする
CSCwa32286	CCM レイヤ（スプリント 125、シーケンス 21）での WR6、WR8 および LTS18 コミット ID の更新
CSCwb24039	ルーティングでの ASA のトレースバックとリロード
CSCwa46963	セキュリティ：CVE-2021-44228 → Log4j 2 における脆弱性
CSCwb06543	LACP プロセスの予期しない再起動イベントを診断するためにログレベルを上げる
CSCwb43018	ifc と ip が HA LU または CMD インターフェイスに属していることを確認するために SNP API を導入
CSCvz76652	URL フィルタリング（Beaker サービス）のプロキシ URI URL には、エンコードされたユーザー/パスワード文字列が含まれる
CSCvz51570	FDM：HA ユニットと FDM UI/CLI 間の管理インターフェイス名の不一致
CSCvz66236	特定のルールに Type:Both を設定した後の「-1」のしきい値誤動作
CSCwb59488	メモリ割り当てでの ASA/FTD のトレースバックが失敗した
CSCwa42350	「利用可能なリソースがモジュールで更新されていません（Available resources not updated by module）」という内部エラーが原因で ASA のインストール/アップグレードが失敗する
CSCvz32593	無効な状態の QP4110 と QW4115 で CD App Sync エラーが発生し、アクティブなデバイスで Rsync が有効になっていない
CSCwa76621	FTD 1120 で HM プロセス OOM が強制終了される
CSCvy67765	送信元インターフェイスが up/up で動作しているにもかかわらず、FTD VTI が TUNNEL_SRC_IS_UP を false と報告する
CSCvz02076	Snort のリロードがタイムアウトして再起動する
CSCwa32628	競合状態により、AddFileToPendingHash() で SFDataCorrelator がクラッシュする
CSCwa07390	FMC のみの設定：SI フィードのダウンロードしたファイルが予想されるチェックサムと一致しない

不具合 ID	タイトル
CSCwa97910	接続イベントレポートに同じデバイスが 2 回表示される
CSCwb48686	ASAV が Dell PowerEdge R650 の REDHAT KVM で起動しない
CSCwa27822	6.7 または 7.0 への FTD のメジャーアップグレード後、Lina プロセスが開始状態のままになる
CSCwb11325	100_ftd_onbox_data_import.pl 中の nullPointerException により、7.0.0 から 7.1.0 へのアップグレードが失敗する
CSCwb32721	syslog ID 725021 および 725022 が有効な ID としてリストされない
CSCwa35596	AnyConnect HostScan クラスファイルの同期の失敗により、スタンバイ FMC に登録済みデバイスが表示されないことがある
CSCwa26353	Snort3：LSP の更新後にポリシーがダーティにならない（カスタム侵入ポリシーのみが使用されている場合）
CSCvz70539	ロギングレートが高い場合、OOM が原因で Loggerd プロセスが強制終了される
CSCvr97157	ENH：FDM によって管理される FTD で展開が失敗したときの動作を改善
CSCwb28047	FMC：「例外：stoiで受信スレッドが終了しました（Receiving thread exited with an exception: sto）」が原因で pxGrid がフラッピングする
CSCwa21016	Cisco Firepower Threat Defense ソフトウェアの DNS 適用で確認されたサービス拒否攻撃に対する脆弱性
CSCwb16663	AC ポリシーの [詳細（Advanced）] タブで NAP を設定できない
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
CSCvt76856	Smart Satellite Server への接続で証明書を使用している場合、その証明書を復元することはできない
CSCwa77396	FMC で監視アラートを作成できない
CSCvy50797	プラットフォームの設定に SSL の DH グループ 1 が含まれている場合、ポリシーの展開が失敗することがある
CSCvz91266	FXOS 偽造されたリクエスト uri-path により mod_proxy がそのリクエストを送信元サーバーに転送する可能性がある
CSCwa86210	PM が mysqld を無効にすると、完全にシャットダウンするまでに予想以上に時間がかかることがある

不具合 ID	タイトル
CSCwa72641	「早期アプリケーション検出」が有効になっていると、TLS v1.2 の自己署名 URL の URL が正しく抽出されない
CSCwa85138	トランザクションコミット診断に関する複数の問題が発生
CSCwa48169	netsnmp_handler_check_cache 関数での ASA/FTD のトレースバックとリロード
CSCvx24470	FTD/FDM：RA VPN のカスタム ポートが設定されている場合、展開のたびに RA VPN セッションが切断される
CSCvz96440	FMC で NGIPS デバイスのアーカイブが作成されないようにする必要がある
CSCwa04171	FMC がレルムの AAA コマンドを不必要に生成および削除している
CSCwa31488	フェールオーバー インターフェイスとして Etherchannel を使用して FDM 高可用性を作成できない
CSCvy65200	特定のクエリの DNSQuery フィールドにランダムな文字が表示される
CSCwb31699	プライマリはリロード後にアクティブな役割を果たします
CSCwb19648	crasLocalAddress の SNMP クエリで SSL/DTLS トンネルに割り当てられた IP が返されない
CSCvz70688	default-information originate が最初に設定されると、設定に対する stub コマンドが許可されない
CSCwa03732	展開が展開中のスナップショット生成フェーズでハングする
CSCvz69699	内部データベースの接続リークが原因で FMC UI にアクセスできなくなることがある
CSCwa69279	FMC：IKEv2 プロトコルのみが有効になっている group-policy に AnyConnect MTU を設定できない
CSCwa62167	CIAM：Apache-http-server CVE-2021-44790 および CVE-2021-44224
CSCwa48849	再開されたセッションでの SSL の予期しない動作
CSCwa52215	ファームウェアをアップロードすると、データポートチャネルがフラッピングする
CSCvy99218	更新に失敗した場合、VDB バージョンが更新されてはいけない
CSCwa50145	FPR8000 センサーの UI ログインにより、基本的な権限を持つシェルユーザーが作成される

不具合 ID	タイトル
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
CSCwa85220	デバイスの登録中に DCCSM ブリッジで承認が失敗する
CSCwa21061	FTD のアップグレードが 800_post/100_ftd_onbox_data_import.sh で失敗する
CSCwa98853	エラー F0854：FDM Keyring の RSA 係数が無効です（FDM Keyring's RSA modulus is invalid）
CSCvv59757	すでに実行されている場合、FMC イベントレポートの生成が失敗する
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
CSCvz85234	FMC から syslog への監査ログの送信でファシリティ ALERT、AUDIT、CLOCK、KERN が機能しない
CSCvz84733	inline-set を通過する LACP パケットが確認なくドロップされる
CSCvx89451	ISA3000：shutdown コマンドがシステムをシャットダウンする代わりに再起動する
CSCvz43325	HA を解除した後、アクティブな FMC がセンサーの登録を解除しない
CSCwa55974	FMC は、新しいデルタを適用する前に以前の設定セッションを中止する必要がある
CSCwa77083	ネットワーク検出ルールでセキュリティゾーンが設定されている場合、ホスト情報が欠落する
CSCwa42596	SNMPv3 設定を使用した ASA は、snmpd コアで予期しないリロードを観察する
CSCwb84638	外部イベントの再起動時にログイベントをキャプチャするためのポートマネージャ/LACP の改善
CSCwa31139	FMC が FTD フェールオーバー インターフェイスとの IP のオーバーラップをチェックしない
CSCwa08084	FMC ハードウェアアプライアンスの復元がエラー「不明な障害状態（Unknown Failure Condition）」で終了する
CSCwb08828	FP1010 スイッチポートアクセス VLAN インターフェイスが up/up ステータスでもトラフィックを渡さない
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

不具合 ID	タイトル
CSCvv82681	RTC の不安定なクロックレジスタ読み取りにより、コンソールで「ウォッチドッグ：バグ：ソフトロックアップ - CPU#0がスタック（watchdog: BUG: soft lockup - CPU#0 stuck）」エラーが発生する
CSCwa67145	AD でグループの 1 つが削除されると、レルムのダウンロードが実行されない
CSCvu82743	Snort のリロード後に Snort ジェネレータ ID 3 のルールが無効になる
CSCwa17918	OSPF のデフォルトルートを常にアドバタイズするオプションをオフにできない
CSCvp15884	FMC SI 正常性アラート：SI URL リストとフィード - 失敗の誤検出
CSCwa55418	アップグレード前に AnyConnect パッケージを使用して展開すると、複数の DB フォルダ current-policy-bundle が生成される
CSCvz35787	中間フローについて、FTD で誤解を招く OVER_SUBSCRIBED フローフラグが付けられる
CSCwa53088	snort 2 ssl-debug ファイルが書き込まれない場合がある
CSCwa29956	FTD のアップグレード後に「デバイスでインターフェイスの設定が変更されました」というメッセージが表示される場合がある
CSCwa60574	snp_ha_trans_alloc_msg_muxbuf_space 関数で ASA のトレースバックとリロードが発生する
CSCwb38669	FPR1150 で 7.1.0.90（2.11.1.154）にアップグレードした後、LACP ポリシー名が Null に設定される
CSCwb08644	Scaled S2S+AC-DTLS+SNMP の長時間テストからの IKEv2 における ASA/FTD のトレースバックとリロード
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
CSCwb09219	ASA/FTD：「署名者証明書が見つかりません」が原因で、アップグレード後に OCSP が機能しない場合がある
CSCwa85297	マルチインスタンス内部ポートチャネル VLAN が正しくプログラムされず、トラフィックが失われる
CSCvz25197	複数のシスコ製品の Snort Modbus におけるサービス妨害の脆弱性
CSCug44895	PAS から返されるカーソルの数が多くなると、アップロードが失敗する

不具合 ID	タイトル
CSCwa67209	FTD のアップグレード後、FMC で 1 Gbps SFP ファイバーメンバーのポートチャネルの自動ネゴシエーションが無効になることがある
CSCwb24101	Loggerd syslog に（FirstPacketSecond よりかなり前などの）誤った不適切なタイムスタンプが含まれている
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
CSCwa78082	FMC 侵入イベント検索の結果が一貫していない
CSCwa80040	6.4.0.4 から 7.0.1 へのアップグレード後に FMC NFS の設定が失敗する
CSCvz52430	設定されている 5 台の DNS サーバーが原因で FDM UI にアクセスできず、503 サービスを利用できない
CSCwb07981	トレースバック：スタンバイ FTD が再起動し、スレッド名 cli_xml_server でクラッシュ情報と lina コアを生成する
CSCwb02316	MAC アドレス設定中のエラー「「1」ではノンストップフォワーディングはサポートされません（Non stop forwarding not supported on '1'）」
CSCwa92883	ドメイン スナップショット エラーによりフェーズ 2 で展開が失敗した
CSCvz61463	アップグレード後に radware vdp コアで FP9k SM-44 6.7.0.2 の CPU 使用率が高くなる
CSCwa55142	通常の DND ではなく、追加の DND ボトムルールがある場合の SNORT3/SSL/Definitive DND 判定
CSCvy88460	6.7.0 へのアップグレード後に Radius 認証オブジェクトを追加できない
CSCvz72771	ASA/FTD が、スタックトレースの「c_assert_cond_terminate」でトレースバックおよびリロードする場合がある
CSCwb07908	スタンバイ FTD/ASA が 0.0.0.0 の送信元 IP で DNS クエリを送信する
CSCwa13721	SSL 設定でカスタム暗号が選択されている場合、FDM で管理する FTD のアップグレードが失敗する
CSCvj08826	FMC ibdata1 ファイルのサイズが大きくなることがある
CSCwa14524	SSL がアクティブ化された pdts_sftls_daq_acquire の Snort コア
CSCwb43629	ライセンスとルールで HA 管理対象デバイスに対して誤って生成されたテレメトリデータがカウントされる
CSCwa31508	QW-4145 デバイスで継続的に展開に失敗する
CSCwa79905	FMC NAT ポリシーのレポート生成で 51*x ごとにルールが記録されない

不具合 ID	タイトル
CSCwa90660	FMC レルムのユーザー/グループのダウンロードでタスクが開始されない
CSCwb56718	ポリシーの展開がエラー「ルールの更新は実行中ですが、進行中の更新はありません。（Rule update is running but there are no updates in progress.）」で失敗する

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。

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。