Cisco Secure Firewall Threat Defense バージョン 7.4.x リリースノート

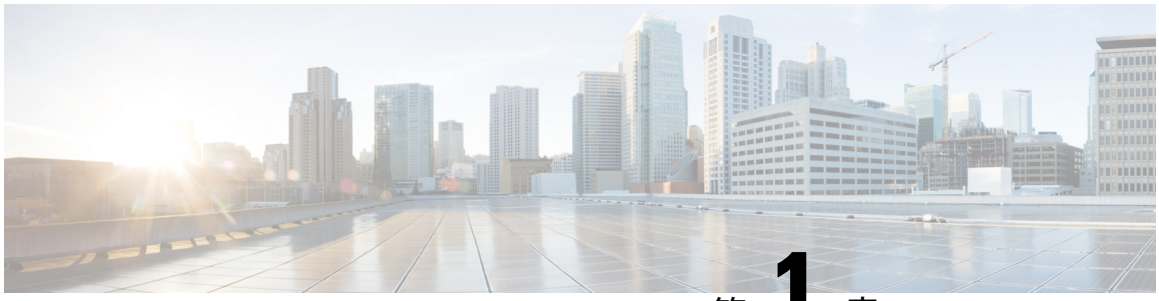
初版：2023 年 9 月 7 日

最終更新：2024 年 4 月 25 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/

© 2023–2024 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

ようこそ

このドキュメントには、Cisco Secure Firewall Threat Defense、Secure Firewall Management Center、およびSecure Firewall Device Manager の バージョン 7.4のリリース情報が含まれています。

Cisco Defense Orchestrator（CDO）の展開については、「Cisco クラウド提供型 Firewall Management Center リリースノート」または「Cisco Defense Orchestrator の新機能」を参照してください。

リリース日

表 *1* : バージョン *7.4* 日付

バージョン	ビルド	日付	プラットフォーム
7.4.1	172	2023 年 12 月 13 日	すべて
7.4.0	81	2023 年 9 月 7 日	Management center Cisco Secure Firewall 4200 シリーズ

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パッチを含む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

Web 分析は、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提供します。ソフトウェアのバージョンと、Management Center または Device Manager を使用しているかどうかに応じて、ブラウザは Google（google.com）または Amplitude（amplitude.com）のいずれかに接続する場合があります。

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。広告ブロッカーは Web 分析をブロックできるため、登録したままにする場合は、Cisco アプライアンスのホスト名/IP アドレスの広告ブロックを無効にしてください。

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。

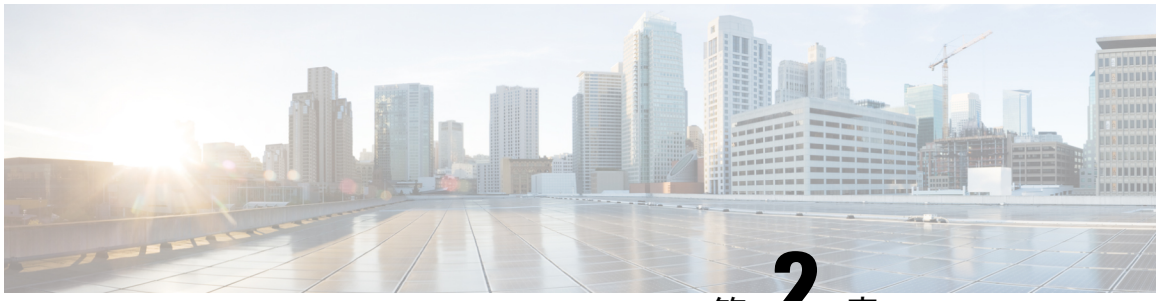
- マニュアル：http://www.cisco.com/go/threatdefense-74-docs
- シスコ サポートおよびダウンロード サイト：https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://www.cisco.com/cisco/support/notifications.html

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 7.4 のシステム要件を記載します。

Management Center プラットフォーム

Management Centerは、一元化されたファイアウォール管理コンソールを提供します。Management Center とのデバイスの互換性については、「Threat Defense 管理 （8 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 7.4 は次の Management Center ハードウェアをサポートします。

- Cisco Secure Firewall Management Center 1700、2700、4700
- Firepower Management Center 1600、2600、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 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 7.4 はパブリッククラウドとプライベートクラウドでの Management Center Virtual 導入をサポートします。

Management Center Virtual では、2、10、または 25 台のデバイスを管理するライセンスを購入できます。一部のプラットフォームでは、300 台のデバイスがサポートされます。2 デバイスライセンスは Management Center ハイアベイラビリティをサポートしていないことに注意してください。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 *7.4 Management Center Virtual* プラットフォーム

プラットフォーム（Platform）	管理対象デバイス		ハイ アベイラビリティ
	2、10、25	300	
パブリック クラウド			
Amazon Web Services（AWS）	対応	対応	対応
Google Cloud Platform（GCP）	対応	—	—
Microsoft Azure	対応	—	対応
Oracle Cloud Infrastrucure（OCI）	対応	対応	対応
プライベート クラウド			
Cisco HyperFlex	対応	—	対応
カーネルベース仮想マシン（KVM）	対応	対応	対応
Microsoft Hyper-V	対応	—	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

クラウド提供型 Firewall Management Center

Cisco クラウド提供型 Firewall Management Center 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。お客様が導入した Management Center は、仮想プラットフォームの場合でも、オンプレミスと呼ばれることが多いことに注意してください。

このドキュメントが公開された時点では、クラウド提供型 Firewall Management Center は Threat Defense バージョン 7.0.3 ～ 7.4.0（7.1 はサポートなし）を実行しているデバイスを管理することができました。最新の互換性情報については、『Cisco クラウド提供型 Firewall Management Center リリースノート』を参照してください。

Threat Defense プラットフォーム

Threat Defense デバイスは、ネットワークトラフィックをモニターし、定義された一連のセキュリティルールに基づいて特定のトラフィックを許可するかブロックするかを決定します。デバイスの管理方法については、「Threat Defense 管理 （8 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 Threat Defense 互換性ガイド を参照してください。

Threat Defense ハードウェア

バージョン 7.4 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 7.4 Threat Defense ハードウェア

プラットフォーム	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 1010E、1010、1120、1140、1150	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Firepower 2110、2120、2130、2140	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Cisco Secure Firewall 3105、3110、3120、3130、3140	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。
Firepower 4112、4115、4125、4145 Firepower 9300 : SM-40、SM-48、SM-56 モジュール	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。 FXOS 2.14.1.131 以降のビルドが必要です。
Cisco Secure Firewall 4215、4225、4245	対応	対応	—	—	—
ISA 3000	対応	対応	対応	対応	バージョン 7.4.1 以降が必要です。 ROMMON の更新が必要な場合があります。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

バージョン 7.4 Threat Defense Virtual 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 *7.4 Threat Defense Virtual* 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	Device Manager + CDO
パブリック クラウド				
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	—	—
プライベート クラウド				
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

Threat Defense 管理

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。

お客様が導入したManagement Center

すべてのデバイスは、お客様が導入した Management Center によるリモート管理に対応しています。FMC では管理対象デバイスと同じまたはそれ以降の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。

ほとんどの場合、旧バージョンのデバイスは Management Center のメジャーバージョンまたはメンテナンスバージョンに直接アップグレードできます。ただし、対象バージョンがデバイスでサポートされていても、直接アップグレードできない旧バージョンのデバイスを管理している場合があります。リリース固有の要件については、を参照してください。アップグレードする最小バージョン （74 ページ）。Threat Defense プラットフォーム （6 ページ） に記載されている特定の Management Center デバイスの組み合わせで、まれに問題が発生することがあります。

表 *5 :* お客様が導入した *Management Center* : デバイスの互換性

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
7.4	7.0
7.3	6.7
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
6.2.1	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	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 Firewall Management Center

クラウド提供型 Firewall Management Center は、次を実行している Threat Defense デバイスを管理できます。

- バージョン 7.2 以降
- 7.0.3 以降のメンテナンスリリース

クラウド提供型 Firewall Management Center は、バージョン 7.1 を実行している Threat Defense デバイス、または任意のバージョンを実行しているクラシックデバイスを管理できません。クラウド管理の登録を解除するか、または無効にしない限り、クラウド管理対象デバイスはバージョン 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。

クラウド管理型のデバイスは、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 以降のお客様が導入した Management Center 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。

Device Manager

Device Manager を使用すると、単一の Threat Defense デバイスをローカルに管理できます。

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。

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は実施していません。また、Management Center How-Tos 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**（⚙）> **[構成（Configuration）]** > **[HTTPS証明書（HTTPS Certificate）]** を選択します。
- 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。

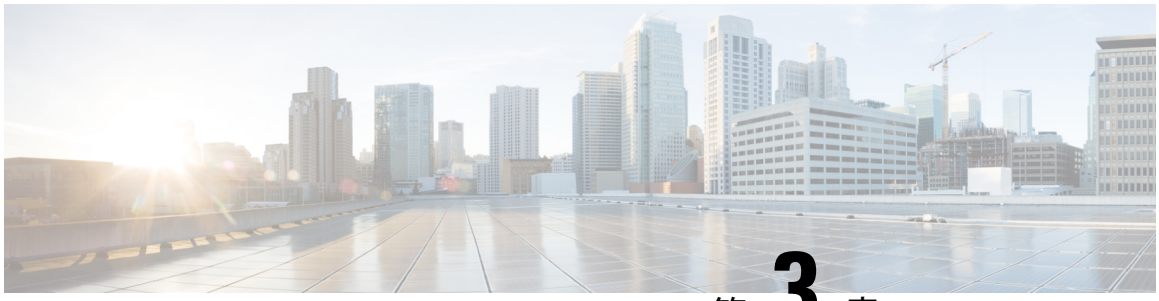
詳しい手順については、オンラインヘルプまたはご使用の製品のコンフィギュレーションガイドを参照してください。

（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7.4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。

アップグレードと展開により、システムでトラフィックが処理されるか、他の操作をしなくても異なる動作が発生する場合、機能がアップグレードに影響を与えます。これは特に、新しい脅威検出およびアプリケーション識別機能で一般的です。または、アップグレードプロセスに特別な要件がある場合もあります。たとえば、アップグレードの前後に非標準のタスクを実行する必要がある場合があります（特定のコンフィギュレーションの編集または削除、ヘルスポリシーの適用、Web インターフェイスでの FlexConfig コマンドのやり直しなど）。

重要 アップグレードでバージョンがスキップされる場合は、リリースノートで機能の履歴情報とアップグレードの影響を確認するか、該当する新機能（リリース別）[英語]ガイドを参照してください。

Management Center 機能

新しい 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、通常は Management Center およびデバイスの両方で最新のリリースが必要です。 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。

バージョン 7.4.1 の Management Center 機能

新機能

表 *6 : Management Center* バージョン *7.4.1* の新機能

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
再導入された機能			
以前のメンテナンスリリースから機能が再導入されました。	7.4.1	機能に依存	バージョン 7.4.1 では、奇数番号のバージョン（7.1、7.3）やバージョン 7.4.0 のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0、7.2）のメンテナンスリリースに含まれていた機能、機能強化、および重要な修正が再導入されています。 アップグレードの影響は、機能によって異なります。 再導入された機能は次のとおりです。 • バージョン 7.3 でサポートされているすべてのデバイスプラットフォーム、および Firepower 1010E（7.2 で最後にサポート）での Threat Defense のサポート。 • Management Center によるインターフェイス同期エラーの検出。 • Web 分析プロバイダーを更新しました。
プラットフォーム（Platform）			
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	7.4.1	7.4.1	Cisco Secure Firewall 3130 および 3140 は次のネットワークモジュールをサポートするようになりました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Firepower 9300 ネットワークモジュール用の光トランシーバ。	7.4.1	7.4.1	Firepower 9300 は、次の光トランシーバをサポートするようになりました。 • QSFP-40/100-SRBD • QSFP-100G-SR1.2 • QSFP-100G-SM-SR 以下のネットワークモジュールでサポート： • FPR9K-NM-4X100G • FPR9K-NM-2X100G • FPR9K-DNM-2X100G 参照： Cisco Firepower 9300 ハードウェア設置ガイド
Cisco Secure Firewall 3100 のパフォーマンスプロファイルのサポート。	7.4.1	7.4.1	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 3100 に適用されるようになりました。以前は、この機能は Firepower 4100/9300、Cisco Secure Firewall 4200、および Threat Defense Virtual でサポートされていました。 参照：「Configure the Performance Profile」
[インターフェイス（Interfaces）]			
Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開します。	7.4.1	7.4.1	Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開できるようになりました。Azure の展開には引き続き少なくとも 2 つのデータインターフェイスが必要ですが、GCP では診断インターフェイスをデータインターフェイスに置き換える必要があり、新しい最小は 3 つです（以前は、Threat Defense Virtual の展開には、1 つの管理インターフェイス、1 つの診断インターフェイス、および少なくとも 2 つのデータインターフェイスが必要でした）。 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center の Web インターフェイスから DHCP リレーの信頼できるインターフェイスを設定します。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、Option 82 がすでに設定されている DHCP パケットを Threat Defense DHCP リレーエージェントが受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合、Threat Defense のデフォルトではそのパケットはドロップされます。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[デバイスの追加/編集（Add/Edit Device）]** > **[DHCP]** > **[DHCP リレー（DHCP Relay）]** 参照：「」「Configure the DHCP Relay Agent」
Device Management			
ユーザー定義の VRF インターフェイスでサポートされるデバイス管理サービス。	7.4.1	いずれか	Threat Defense プラットフォーム設定（NetFlow、SSH アクセス、SNMP ホスト、syslog サーバー）で設定されたデバイス管理サービスが、ユーザー定義の Virtual Routing and Forwarding（VRF）インターフェイスでサポートされるようになりました。 プラットフォームの制限：コンテナインスタンスまたはクラスタ化されたデバイスではサポートされていません。 参照：「Platform Settings」
NAT			
NAT ルールの編集時にネットワークグループを作成します。	7.4.1	いずれか	NAT ルールの編集時に、ネットワークオブジェクトに加えてネットワークグループを作成できるようになりました。 参照：「Customizing NAT Rules for Multiple Devices」
高可用性/拡張性：Threat Defense			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure Firewall 3100 のマルチインスタンスモード。	7.4.1	7.4.1	Secure Firewall 3100 は、単一のデバイス（アプライアンスモード）または複数のコンテナインスタンス（マルチインスタンスモード）として展開できます。マルチインスタンスモードでは、完全に独立したデバイスとして機能する複数のコンテナインスタンスを 1 つのシャーシに展開できます。マルチインスタンスモードでは、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレード対象（シャーシのアップグレード）になることに注意してください。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [Chassis Manager]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [新しいポリシー（New Policy）] > [シャーシプラットフォーム設定（Chassis Platform Settings）]** • **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]** 新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode** プラットフォームの制限：Cisco Secure Firewall 3105 ではサポートされていません。 参照：「Multi-Instance Mode for the Secure Firewall 3100」 および Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
VMware および KVM 向け Threat Defense Virtual の 16 ノードクラスタ	7.4.1	7.4.1	VMware の仮想 Threat Defense と KVM の仮想 Threat Defense に 16 ノードクラスタを構成できるようになりました。 参照：「Clustering for Threat Defense Virtual in a Private Cloud」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバー。	7.4.1	7.4.1	AWS Gateway Load Balancer（GWLB）を使用して AWS のクラスタ化された Threat Defense Virtual デバイスのターゲットフェールオーバーを設定できるようになりました。 プラットフォームの制限：5 台および 10 台のデバイスライセンスでは使用できません。 参照：「Configure Target Failover for Threat Defense Clustering with GWLB in AWS」
Threat Defense 高可用性ペアの設定の不一致を検出します。	7.4.1	7.4.1	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照：「Troubleshoot Configuration Sync Failure」および Cisco Secure Firewall Threat Defense コマンドリファレンス
高可用性：Management Center			
高可用性 Management Center 用の単一のバックアップファイル。	7.4.1	いずれか	高可用性ペアのアクティブ Management Center の設定だけのバックアップを実行すると、いずれかのユニットの復元に使用できる単一のバックアップファイルが作成されるようになりました。 参照：「」「Unified Backup of Management Centers in High Availability」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center の高可用性同期の機能拡張。	7.4.1	いずれか	Management Center の高可用性（HA）には、次の同期機能拡張が含まれています。 • 設定履歴ファイルが大きいと、遅延の大きいネットワークで同期が失敗する可能性があります。これを防ぐために、デバイス設定履歴ファイルは他の設定データと並行して同期されるようになりました。この機能拡張により、同期時間も短縮されます。 • Management Center は、設定履歴ファイルの同期プロセスをモニターし、同期がタイムアウトした場合に正常性アラートを表示するようになりました。 新規/変更された画面：次の画面でこれらのアラートを確認できます。 • [通知（Notifications）] > [メッセージセンター（Message Center）] > [正常性（Health）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [高可用性（High Availability）] > [ステータス （Status）]（[概要（Summary）] の下） 参照：「Viewing Management Center High Availability Status」
SD-WAN			
[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードのアプリケーションモニタリング。	7.4.1	7.4.1	[Cisco SD-WANサマリー（SD-WAN Summary）] ダッシュボードでWANインターフェイスアプリケーションのパフォーマンスをモニターできるようになりました。 新規/変更された画面：**[概要（Overview）] > [Cisco SD-WANサマリー（SD-WAN Summary）] > [アプリケーション モニタリング（Application Monitoring）]** 参照：「WAN Summary Dashboard」
VPN			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPSec フローのオフロード。	7.4.1	7.4.1	**アップグレードの影響。条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。 この機能はアップグレードにより自動的に有効になります。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4100/9300 の暗号デバッグの機能拡張。	7.4.1	7.4.1	バージョン 7.4.0 で導入された暗号デバッグの機能拡張は、Cisco Secure Firewall 3100 および Firepower 4100/9300 に適用されるようになりました。以前は、Cisco Secure Firewall 4200 でのみサポートされていました。 参照：「Troubleshooting Using Crypto Archives」
ルートベース VPN の VTI の詳細を表示します。	7.4.1	いずれか	管理対象デバイスのルートベース VPN の仮想トンネルインターフェイス（VTI）の詳細を表示できるようになりました。ダイナミック VTI の動的に作成されたすべての仮想アクセスインターフェイスの詳細も表示できます。 新規/変更された画面：[デバイス（Device）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit a device）] > [インターフェイス（Interfaces）] > [仮想トンネル（Virtual Tunnels）] タブ。 参照：「About Virtual Tunnel Interfaces」
ルーティング			
FlexConfig を使用して、IS-IS インターフェイスで BFD ルーティングを設定します。	7.4.1	7.4.1	FlexConfig を使用して、物理、サブインターフェイス、および EtherChannel IS-IS インターフェイスで Bidirectional Forwarding Detection（BFD）ルーティングを設定できるようになりました。 参照：「Guidelines for BFD Routing」
アクセス制御：脅威の検出とアプリケーションの識別			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Zero Trust アクセスの機能拡張。	7.4.1	7.4.1（Snort 3）	Management Center には、次の Zero Trust アクセスの機能拡張が含まれています。 • アプリケーションの送信元NAT を設定できます。設定されたネットワークオブジェクトまたはオブジェクトグループは、着信要求のパブリックネットワークの送信元 IP アドレスを、アプリケーション ネットワーク内のルーティング可能な IP アドレスに変換します。 • 診断ツールを使用して、Zero Trust 設定の問題をトラブルシューティングできます。 • エクスペリエンスを向上させるために、Zero Trust アプリケーションポリシーのテレメトリデータを収集するようになりました。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[Zero Trustアプリケーション（Zero Trust Application）]** 新規/変更された CLI コマンド：**show running-config zero-trust**、**show zero-trust statistics** 参照： • アプリケーションの作成 • Zero Trust セッションのモニタリング • Cisco Secure Firewall Threat Defense コマンドリファレンス • Cisco Secure Firewall Management Center から収集される Cisco Success Network テレメトリデータ
CIP 検出。	7.4.1	7.4.1（Snort 3）	セキュリティポリシーで CIP およびイーサネット/IP（ENIP）アプリケーション条件を使用することで、Common Industrial Protocol（CIP）を検出して処理できるようになりました。 参照：「Application Rule Conditions」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
CIP 安全検出。	7.4.1	7.4.1（Snort 3）	CIP Safety は、産業自動化アプリケーションの安全な動作を可能にする CIP 拡張機能です。CIP インスペクタは、CIP トラフィック内の CIP Safety セグメントを検出できるようになりました。CIP Safety セグメントを検出してアクションを実行するには、Management Center のネットワーク分析ポリシーで CIP インスペクタを有効にし、アクセス コントロール ポリシーに割り当てます。 新規/変更された画面：[ポリシー（Policies）]>[アクセス制御（Access Control）]>[ポリシーの編集（Edit a policy）]>[ルールの追加（Add Rule）]>[アプリケーション（Applications）] タブの順に選択し、検索ボックスで CIP Safety を検索します。 参照：Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
Access Control：**Identity**			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
複数の Active Directory レルム（レルムシーケンス）のキャプティブポータル サポート。	7.4.1	7.4.1	**アップグレードの影響。カスタム認証フォームの更新。** LDAP レルム、Microsoft Active Directory レルム、またはレルムシーケンスに対してアクティブ認証を設定できます。さらに、レルムまたはレルムシーケンスを使用してアクティブ認証にフォールバックするパッシブ認証ルールを設定できます。必要に応じて、アクセス制御ルールで同じ ID ポリシーを共有する管理対象デバイス間でセッションを共有できます。 さらに、以前にアクセスしたデバイスとは別の管理対象デバイスを使用してシステムにアクセスするときに、ユーザーに再認証を要求するオプションがあります。 HTTP 応答ページ認証タイプを使用するアップグレード展開では、**`<select name="realm" id="realm"></select>`** をカスタム認証フォームに追加して、ユーザーが選択できる複数のレルムを表示する必要があります。 制限事項：Microsoft Azure Active Directory ではサポートされていません。 新規/変更された画面： • **[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集）> [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** • **[IDポリシー（Identity policy）] >（編集）> [ルールの追加（Add Rule）] > [パッシブ認証（Passive Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** • **[IDポリシー（Identity policy）] >（編集）> [ルールの追加（Add Rule）] > [アクティブ認証（Active Authentication）] > [レルムと設定（Realms & Settings）] > [パッシブ/VPNアイデンティティを確立できない場合にアクティブ認証を使用（Use active authentication if passive or VPN identity cannot be established）]** 参照：「How to Configure the Captive Portal for User Control」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
ファイアウォール全体でキャプティブポータルアクティブ認証セッションを共有します。	7.4.1	7.4.1	以前に接続していたデバイスとは異なる管理対象デバイスに認証セッションが送信されたときに、ユーザーの認証が必要かどうかを決定します。ユーザーがロケーションまたはサイトを変更するたびに認証する必要がある組織の場合は、このオプションを無効にする必要があります。 • (デフォルト) 有効にすると、ユーザーはアクティブな認証アイデンティティルールに関連付けられた管理対象デバイスで認証できます。 • アクティブな認証ルールが展開されている別の管理対象デバイスでユーザーがすでに認証されている場合でも、別の管理対象デバイスでの認証をユーザーに要求する場合は無効にします。 新規/変更された画面：**[ポリシー（Policies）] > [アイデンティティ（Identity）] >（ポリシーの編集） > [アクティブ認証（Active Authentication）] > [ファイアウォール全体でアクティブ認証セッションを共有（Share active authentication sessions across firewalls）]** 参照：「How to Configure the Captive Portal for User Control」
Management Center の Web インターフェイスを使用して、ダウンロード可能なアクセス制御リストを RADIUS アイデンティティソースのシスコ属性値ペア ACL とマージします。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [AAAサーバー（AAA Server）] > [RADIUS サーバーグループ（RADIUS Server Group）] > [RADIUSサーバーグループの追加（Add RADIUS Server Group）] > [ダウンロード可能ACL とシスコAVペアACLの結合（Merge Downloadable ACL with Cisco AV Pair ACL）]** 新しい CLI コマンド： • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl after-avpair** • **sh run aaa-server aaa-server ISE-Server protocol radius merge-dacl before-avpair** 参照：「RADIUS Server Group Options」
イベントロギングおよび分析			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
統合イベントビューアからパケットトレーサを開きます。	7.4.1	いずれか	統合イベントビュー（**[分析（Analysis）] > [統合イベント（Unified Events）]**）からパケットトレーサを開けるようになりました。目的のイベントの横にある省略記号アイコン（[...]）をクリックし、[パケットトレーサで開く（Open in Packet Tracer）] をクリックします。 参照：「Working with the Unified Event Viewer」
ヘルス モニタリング			
Firepower 4100/9300 のシャーシレベルのヘルスアラート。	7.4.1	FXOS 2.14.1 を搭載したすべて	**アップグレードの影響。新しい正常性モジュールを有効にし、アップグレード後にデバイス正常性ポリシーを適用します。** シャーシを読み取り専用デバイスとして Management Center に登録することで、Firepower 4100/9300 のシャーシレベルのヘルスアラートを表示できるようになりました。また、Firewall Threat Defense プラットフォーム障害のヘルスモジュールを有効にして、ヘルスポリシーを適用する必要があります。アラートは、メッセージセンター、ヘルスモニター（左側のペインの [デバイス（Devices）] でシャーシを選択）、およびヘルスイベントビューに表示されます。 マルチインスタンスモードで Cisco Secure Firewall 3100 のシャーシを追加し、正常性アラートを表示することもできます。これらのデバイスの場合は、Management Center を使用してシャーシを管理します。ただし、Firepower 4100/9300 シャーシの場合は、シャーシマネージャまたは FXOS CLI を使用する必要があります。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[シャーシ（Chassis）]** 参照：「Add a Chassis to the Management Center」
展開履歴（ロールバック）ファイルによって使用される過剰なディスク容量に関する正常性アラート。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** Disk Usage 正常性モジュールは、展開履歴（ロールバック）ファイルが Management Center で過剰なディスク容量を使用している場合にアラートを発行するようになりました。 参照：「Disk Usage for Device Configuration History Files Health Alert」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
NTP 同期の問題に関する正常性アラート。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に Management Center の正常性ポリシーを展開します。** 新しい Time Server Status 正常性モジュールは、NTP 同期に関する問題を報告します。 参照：「」「Time Synchronization」および「Health Modules」
Management Center のメモリ使用率の計算、アラート、およびスワップメモリのモニタリングが改善されました。	7.4.1	いずれか	**アップグレードの影響。メモリ使用量アラートのしきい値が引き下げられる可能性があります。** Management Center のメモリ使用量の精度が向上し、デフォルトのアラートしきい値が警告は 88%、重大は 90% に引き下げられました。しきい値が新しいデフォルト値よりも高かった場合、アップグレードによって自動的に下げられます。この変更を有効にするために正常性ポリシーを適用する必要はありません。高メモリプロセスを終了できない場合、システムメモリが極めて少ない状態で Management Center が再起動する可能性があることに注意してください。 新規または既存の Management Center の正常性ダッシュボードに新しいスワップメモリ使用状況メトリックを追加することもできます。[メモリ（Memory）] メトリックグループを選択していることを確認します。 新規/変更された画面： • **システム（⚙） > [正常性（Health）] > [モニタリング（Monitoring）] > [Firewall Management Center][ダッシュボードの追加/編集（Add/Edit Dashboard）][メモリ（Memory）]** • **システム（⚙） > [正常性（Health）] > [ポリシー（Policy）] > [Management Center正常性ポリシー（Management Center Health Policy）] > [メモリ（Memory）]** 参照：「Using Management Center Health Monitor」
展開とポリシー管理			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
変更管理。	7.4.1	いずれか	変更を展開する前の監査追跡や正式な承認など、設定変更に関してより正式なプロセスを実装する必要がある組織の場合は、変更管理を有効にできます。 この機能を有効にするための **システム**（⚙）> **[設定（Configuration）]** > **[変更管理（Change Management）]** ページが追加されました。有効にすると、**システム**（⚙）> **変更管理のワークフロー** ページが表示され、メニューに新しい **[チケット（Ticket）]**（📄）クイックアクセスアイコンが表示されます。 参照：「Change Management」
前回の展開以降の設定変更に関するレポートを表示および生成します。	7.4.1	いずれか	前回の展開以降の設定変更に関する次のレポートを生成、表示、および（zip ファイルとして）ダウンロードできます。 • ポリシー内の追加、変更、または削除、あるいはデバイスに展開されるオブジェクトをプレビューする各デバイスのポリシー変更レポート。 • ポリシー変更レポート生成のステータスに基づいて各デバイスを分類する統合レポート。 これは、Management Center または Threat Defense デバイスのいずれかのアップグレード後に特に役立ち、展開する前にアップグレードによって加えられた変更を確認できます。 新規/変更された画面：**[展開（Deploy）]** > **[高度な展開（Advanced Deploy）]**。 参照：「Download Policy Changes Report for Multiple Devices」
デバイスのロールバックのために保持する展開履歴ファイルの数を設定します。	7.4.1	いずれか	デバイスのロールバックのために保持する展開履歴ファイルの数を最大 10（デフォルト）まで設定できるようになったため、Management Center のディスク容量を節約できます。 新規/変更された画面：[展開（Deploy）] > **[Deployment History]**（🕘）> [展開設定（Deployment Setting）] > [構成バージョン設定（Configuration Version Setting）] 参照：「」「Set the Number of Configuration Versions」
のアップグレード			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
アップグレードの開始ページとパッケージ管理が改善されました。	7.4.1	いずれか	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			新しいアップグレードページでは、アップグレードの選択、ダウンロード、管理、および展開全体への適用が容易になります。これには、Management Center、Threat Defense デバイス、およびすべての古いNGIPSv/ASA FirePOWER デバイスが含まれます。このページには、現在の展開に適用されるすべてのアップグレードパッケージが、特にマークされた推奨リリースとともに一覧表示されます。パッケージを選択してシスコから簡単に直接ダウンロードしたり、パッケージを手動でアップロードおよび削除したりできます。 リスト/直接ダウンロードアップグレードパッケージを取得するには、インターネットアクセスが必要です。インターネットアクセスがない場合は、手動管理に限定されます。適切なメンテナンスリリースのアプライアンスが少なくとも 1 つある（またはパッチを手動でアップロードした）場合を除き、パッチは表示されません。ホットフィックスは手動でアップロードする必要があります。 新規/変更された画面： • **システム**（⚙）> **製品のアップグレード**では、Management Center とすべての管理対象デバイスをアップグレードし、アップグレードパッケージを管理します。 • **システム**（⚙）> **[コンテンツの更新（Content Updates）]**で、侵入ルール、VDB、およびGeoDB を更新できるようになりました。 • **[デバイスの脅威防御のアップグレード**>（**Devices Threat Defense Upgrade**）**]** を選択すると、脅威防御のアップグレードウィザードに直接移動します。 • **システム**（⚙）> **[ユーザー（Users）]** > **[ユーザーロール（User Role）]** > **[ユーザーロールの作成（Create User Role）]** > **[メニューベースの権限（Menu-Based Permissions）]**を使用すると、[製品のアップグレード（Product Upgrades）]（システムソフトウェア）へのアクセスを許可せずに、[コンテンツの更新（Content Updates）]（VDB、GeoDB、侵入ルール ）へのアクセスを許可できます。 廃止された画面/オプション： • **システム**（⚙）> **[更新（Updates）]**は廃止されました。脅威防御アップグレードはすべてウィザードを使用するようになりました。 • 脅威防御アップグレードウィザードの [アップグレードパッケー

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			ジの追加（Add Upgrade Package）]ボタンは、新しいアップグレードページへの[アップグレードパッケージの管理（Manage Upgrade Packages）]リンクに置き換えられました。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
推奨リリースの通知。	7.4.1	いずれか	新しい推奨リリースが利用可能になると、Management Center から通知されるようになりました。今すぐアップグレードしない場合は、後でシステムに通知するか、次の推奨リリースまでリマインダを延期できます。新しいアップグレードページには、推奨リリースも示されます。 参照： Cisco Secure Firewall Management Center の新機能（リリース別）
アップグレード：Threat Defense			
Threat Defense のアップグレードウィザードからの復元の有効化。	7.4.1	いずれか	脅威防御アップグレードウィザードからの復元を有効化できます。 その他のバージョンの制限：Threat Defense をバージョン 7.1 以降にアップグレードする必要があります。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。	7.4.1	いずれか	Threat Defense アップグレードウィザードの最終ページで、アップグレードの進行状況をモニターできるようになりました。この機能は、[デバイス管理（Device Management）]ページの[アップグレード（Upgrade）]タブおよび Management Center の既存のモニタリング機能に追加されます。新しいアップグレードフローを開始していない限り、**[デバイス（Devices）]** > **[Threat Defenseアップグレード（Threat Defense Upgrade）]**によってこのウィザードの最後のページに戻り、現在の（または最後に完了した）デバイスのアップグレードの詳細なステータスを確認できます。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
FXOS アップグレードに含まれるファームウェアのアップグレード。	7.4.1	いずれか	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。マルチインスタンスモードの Cisco Secure Firewall 3100（バージョン 7.4.1 の新機能）には、FXOS とファームウェアのアップグレードもバンドルされています。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアの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。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
アップグレード：Management Center			
Management Center の新しいアップグレード ウィザード。	7.4.1	いずれか	新しいアップグレード開始ページとウィザードにより、Management Center のアップグレードを簡単に実行できます。**システム**（⚙）**>[製品のアップグレード（Product Upgrades）]**を使用して、Management Center で適切なアップグレードパッケージを入手したら、[アップグレード（Upgrade）] をクリックして開始します。 その他のバージョンの制限：バージョン 7.4.1 以降からの Management Center のアップグレードでのみサポートされます。 Management Center を任意のバージョンにアップグレードするには、Management Center で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。：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド。バージョン 7.4.0 を実行している場合は、バージョン 7.3.x のガイドを使用できます。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center のアップグレード後に設定変更レポートを自動的に生成します。	7.4.1	いずれか	Management Center のメジャーおよびメンテナンスアップグレード後に、設定変更に関するレポートを自動的に生成できます。このレポートは、展開しようとしている変更を理解するのに役立ちます。レポートが生成されたら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。 その他のバージョンの制限：バージョン 7.4.1 以降の Management Center のアップグレードでのみサポートされます。バージョン 7.4.1 以前のバージョンへのアップグレードはサポートされていません。 新規/変更された画面：**システム**（⚙）**>[設定（Configuration）]>[設定のアップグレード（Upgrade Configuration）]>[アップグレード後のレポートの有効化（Enable Post-Upgrade Report）]** 参照：「Upgrade Configuration」
同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。	7.4.1	いずれか	ホットフィックス リリース ノートに特に記載されていない、または Cisco TAC から指示されていない限り、高可用性 Management Center にホットフィックスをインストールするために同期を一時停止する必要はありません。 参照：Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
管理（Administration）			
Management Center ハードウェアのハードドライブを消去します。	7.4.1	いずれか	Management Center CLI を使用してリブートし、ハードドライブデータを完全に消去できます。消去が完了したら、新しいソフトウェアイメージをインストールできます。 新規/変更された CLI コマンド： **secure erase** 参照：「Secure Firewall Management Center Command Line Reference」
ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。	7.4.1	いずれか	**アップグレードの影響。システムは新しいリソースに接続します。** Management Center では、ソフトウェア アップグレード パッケージの直接ダウンロードの場所が sourcefire.com から amazonaws.com に変更されています。 参照：「」「 Internet Access Requirements」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
スケジュール済みタスクでは、パッチおよびVDB 更新のみダウンロードされます。	7.4.1	いずれか	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Management Center に直接ダウンロードするには、**システム**（⚙）> **[製品のアップグレード（Product Upgrades）]**を使用します。 参照：「」「Software Update Automation」
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			
アクセス制御オブジェクトの最適化を有効または無効にします。	7.4.1	いずれか	Management Center の Web インターフェイスからアクセス制御オブジェクトの最適化を有効化または無効化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）]**>**[アクセス コントロールの設定（Access Control Preferences）]**>**[オブジェクトの最適化（Object Optimization）]** 参照：「Access Control Preferences」および「Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations」。
クラスタ制御リンク ping ツール。	7.4.1	いずれか	ping を実行して、すべてのクラスタノードがクラスタ制御リンクを介して相互に到達できることを確認できます。ノードがクラスタに参加できない主な原因の 1 つは、クラスタ制御リンクの設定が正しくないことです。たとえば、クラスタ制御リンクの MTU が、接続しているスイッチの MTU よりも大きい値に設定されている可能性があります。 新規/変更された画面：**[デバイス（Devices）]**>**[デバイス管理（Device Management）]**> **その他**（⋮）>**[クラスタのライブステータス（Cluster Live Status）]** 参照：「」「Perform a Ping on the Cluster Control Link」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
トラブルシューティングファイルの生成とダウンロードは、[デバイス（Device）] および [クラスタ（Cluster）] ページから実行できます。	7.4.1	7.4.1	[デバイス（Device）] ページの各デバイス、および [クラスタ（Cluster）] ページのすべてのクラスタノードのトラブルシューティングファイルを生成およびダウンロードできます。クラスタの場合、すべてのファイルを単一の圧縮ファイルとしてダウンロードできます。クラスタノードのクラスタのクラスタログを含めることもできます。または、**[デバイス（Devices）] > [デバイス管理（Device Management）] > その他**（⋮）> [トラブルシューティング ファイル（Troubleshoot Files）] メニューからファイル生成をトリガーできます。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [全般（General）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]** 参照：「Generate Troubleshooting Files」
クラスタへの参加に失敗した場合のノードでのトラブルシューティングファイルの自動生成。	7.4.1	7.4.1	ノードがクラスタに参加できない場合、そのノードのトラブルシューティング ファイルが自動的に生成されます。[タスク（Tasks）] または [クラスタ（Cluster）] ページからファイルをダウンロードできます。 参照：「Troubleshooting the Cluster」
デバイスまたはデバイスクラスタの CLI 出力を表示します。	7.4.1	いずれか	デバイスまたはクラスタのトラブルシューティングに役立つ一連の定義済み CLI 出力を表示できます。また、任意の **show** コマンドを入力して、出力を確認できます。 新規/変更された画面：**[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [全般（General）]** 参照：「View CLI Output」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Snort 3 はメモリ使用量が過剰になると再起動し、HA フェールオーバーがトリガーされることがあります。	7.4.1	7.4.1（Snort 3）	操作の継続性を向上させるために、Snort によるメモリ使用が過剰な場合、高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスのメモリ使用が過剰な場合に Snort 3 が再起動されるようになったためです。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、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）。 この機能は、デフォルトでイネーブルにされています。CLI を使用して無効にしたり、メモリしきい値を設定したりできます。 プラットフォームの制限：クラスタ化されたデバイスではサポートされていません。 新規/変更された CLI コマンド：**configure snort3 memory-monitor**、**show snort3 memory-monitor-status** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Snort 3 コアダンプの頻度を設定します。	7.4.1	7.4.1（Snort 3）	Snort 3 コアダンプの頻度を設定できるようになりました。Snort がクラッシュするたびにコアダンプを生成する代わりに、次回 Snort がクラッシュしたときにのみコアダンプを生成できます。または、過去 1 日あるいは 1 週間以内にクラッシュが発生していない場合に生成します。 Snort 3 コアダンプは、スタンドアロンデバイスではデフォルトで無効になっています。高可用性およびクラスタ化されたデバイスの場合、デフォルトの頻度が毎回ではなく 1 日に 1 回になりました。 新規/変更された CLI コマンド：**configure coredump snort3**、**show coredump** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Secure Firewall 3100/4200 でドロップされたパケットをキャプチャします。	7.4.1	7.4.1	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100/4200 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの [**drop** { **disable** | **mac-filter** }]。 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
データプレーン障害後の迅速なリカバリ。	7.4.1	7.4.1	データプレーンプロセスがクラッシュした場合、デバイスをリブートする代わりに、データプレーンプロセスのみリロードするようになりました。データプレーンプロセスのリロードに加えて、Snortおよび他のいくつかのプロセスもリロードされます。 ただし、ブートアップ中にデータプレーンプロセスがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードプロセスループの発生を回避できます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 プラットフォームの制限：マルチインスタンスモードではサポートされていません。 参照：Cisco Secure Firewall Threat Defense コマンドリファレンス および『Cisco Secure Firewall ASA シリーズ コマンド リファレンス』

廃止された機能

表 *7: Management Center* バージョン *7.4.1* で廃止済みの機能

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
廃止：イベント正常性アラートの頻繁なドレイン。	7.4.1	7.4.1	[ディスク使用量（Disk Usage）] 正常性モジュールは、イベントの頻繁なドレインでアラートを生成しなくなりました。Management Center のアップグレード後も、正常性ポリシーを管理対象デバイスに展開する（アラートの表示を停止する）か、デバイスをバージョン 7.4.1 以降にアップグレードする（アラートの送信を停止する）まで、アラートが表示され続ける場合があります。 参照：「Disk Usage and Drain of Events Health Monitor Alerts」

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
廃止：FlexConfig を使用した DHCP リレーの信頼できるインターフェイス。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** Management Center の Web インターフェイスを使用して、DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。このように設定すると既存の FlexConfig が上書きされますが、削除する必要があります。 参照：「Configure the DHCP Relay Agent」
廃止：ダウンロード可能なアクセス制御リストと、FlexConfig を使用した RADIUS アイデンティティソースのシスコ属性値ペア ACL のマージ。	7.4.1	いずれか	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** この機能は、Management Center の Web インターフェイスでサポートされるようになりました。

バージョン 7.4.0 の Management Center 機能

（注） バージョン 7.4.0 は、Cisco Secure Firewall Management Center および Cisco Secure Firewall 4200 でのみ使用できます。バージョン 7.4.0 Management Center は他のデバイスモデルの古いバージョンを管理できますが、Threat Defense 7.4.0 を必要とする機能には Cisco Secure Firewall 4200 を使用する必要があります。他のすべてのデバイスプラットフォームのサポートは、バージョン 7.4.1 で再開されます。

新機能

表 *8 : Management Center* バージョン *7.4.0* の新機能

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
以前のメンテナンスリリースから機能が再導入されました。	7.4.0	機能に依存	バージョン 7.4.0 では、奇数番号のバージョン（7.1、7.3）のメンテナンスリリースに含まれなかったが、偶数番号のバージョン（7.0.x、7.2.x）のメンテナンスリリースに含まれていた機能、機能拡張および重要な修正が再度サポートされます。 再導入された機能は次のとおりです。 • アクセス制御のパフォーマンスの向上（オブジェクトの最適化）。
プラットフォーム			
Management Center 1700、2700、4700。	7.4.0	いずれか	最大 300 台のデバイス管理が可能な Cisco Secure Firewall Management Center 1700、2700、および 4700 が導入されました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center 1700、2700、および 4700 スタートアップガイド
Microsoft Hyper-V 向けの Management Center Virtual。	7.4.0	いずれか	最大 25 台のデバイスを管理できる Microsoft Hyper-V 向けの Cisco Secure Firewall Management Center Virtual を導入しました。Management Center の高可用性がサポートされています。 参照： Cisco Secure Firewall Management Center Virtual 入門ガイド
Cisco Secure Firewall 4200。	7.4.0	7.4.0	Cisco Secure Firewall 4215、4225、および 4245 を導入しました。Management Center を使用してこれらのデバイスを管理する必要があります。デバイスマネージャはサポートしていません。 これらのデバイスは、以下の新しいネットワークモジュールをサポートしています。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR4K-XNM-2X100G） • 4 ポート 200G QSFP+ ネットワークモジュール（FPR4K-XNM-4X200G） 参照： Cisco Secure Firewall 4215、4225、4245 ハードウェア設置ガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure Firewall 4200 のパフォーマンスプロファイルのサポート。	7.4.0	7.4.0	プラットフォーム設定ポリシーで使用可能なパフォーマンスプロファイル設定が、Cisco Secure Firewall 4200 に適用されるようになりました。以前は、この機能は Firepower 4100/9300 および Threat Defense Virtual でのみサポートされていました。 参照：「Configure the Performance Profile」
プラットフォームの移行			
Firepower 1000/2100 から Cisco Secure Firewall 3100 への移行。	7.4.0	いずれか（Any）	Firepower 1000/2100 から Cisco Secure Firewall 3100 に設定を簡単に移行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）]** > **[移行（Migrate）]** プラットフォームの制限：Firepower 1010 または 1010E からの移行はサポートされていません。 参照：「About Secure Firewall Threat Defense Model Migration」
Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS への移行。	7.4.0	いずれか	Firepower Management Center 4600 から Cisco Secure Firewall Management Center for AWS（300 台のデバイスライセンスあり）への移行。 参照： Cisco Secure Firewall Management Center モデル移行ガイド
Firepower Management Center 1600/2600/4600 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0	いずれか	Firepower Management Center 1600/2600/4600 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。 参照： Cisco Secure Firewall Management Center モデル移行ガイド

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Firepower Management Center 1000/2500/4500 から Cisco Secure Firewall Management Center 1700/2700/4700 への移行。	7.4.0	7.0.0	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			Firepower Management Center 1000/2500/4500 を Cisco Secure Firewall Management Center 1700/2700/4700 に移行できます。移行するには、古い Management Center をバージョン 7.0 からバージョン 7.4 に一時的にアップグレードする必要があります。 **重要** バージョン 7.4 は、移行プロセス中に 1000/2500/4500 でのみサポートされます。Management Center のアップグレードとデバイスの移行までの間隔は最小限に抑える必要があります。 移行プロセスを要約すると、次のようになります。 **1.** アップグレードと移行の準備をします。リリースノート、アップグレードガイド、および移行ガイドに記載されているすべての前提条件を読み、理解し、条件を満たしてください。 アップグレードする前に、古い Management Center の「移行準備ができている」こと、つまり、新たに展開されていて、完全にバックアップされていること、すべてのアプライアンスが正常な状態であることなどが特に重要です。新しい Management Center も設定する必要があります。 **2.** 古い Management Center とそのすべての管理対象デバイスを少なくともバージョン 7.0.0 にアップグレードします（バージョン 7.0.5 を推奨）。 すでに最小バージョンを実行している場合は、この手順をスキップできます。 **3.** 古い Management Center をバージョン 7.4 にアップグレードします。 アップグレードパッケージを解凍し（ただし、展開はしない）、Management Center にアップロードします。Special Release からダウンロードします。 **4.** モデル移行ガイドの説明に従って、Management Center を移行します。 **5.** 移行が成功したことを確認します。 移行しても期待どおりに機能せず、元に戻す場合、1000/2500/4500 の一般的な操作ではバージョン 7.4 がサポートされていないことに注意してください。古い Management Center をサポートされているバージョンに戻すには、バージョン 7.0 に再イメージ化し、バッ

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			クアップから復元して、デバイスを再登録する必要があります。 参照： • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • Cisco Secure Firewall Management Center モデル移行ガイド 移行プロセスの任意の時点で質問がある場合、またはサポートが必要な場合は、Cisco TAC にお問い合わせください。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Firepower Management Center 1000/2500/4500 から クラウド提供型 Firewall Management Center へのデバイスの移行。	7.4.0	7.0.3	

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			Firepower Management Center 1000/2500/4500 からクラウド提供型 Firewall Management Centerにデバイスを移行できます。 デバイスを移行するには、オンプレミス Management Center をバージョン 7.0.3（7.0.5 を推奨）からバージョン 7.4 に一時的にアップグレードする必要があります。バージョン 7.0 の Management Center ではクラウドへのデバイスの移行がサポートされていないため、この一時的なアップグレードが必要です。さらに、バージョン 7.0.3 以降（7.0.5 を推奨）を実行しているスタンドアロンおよび高可用性 Threat Defense デバイスのみが移行の対象となります。クラスタの移行は現時点ではサポートされていません。 **重要** バージョン 7.4 は、移行プロセス中に 1000/2500/4500 でのみサポートされます。Management Center のアップグレードとデバイスの移行までの間隔は最小限に抑える必要があります。 移行プロセスを要約すると、次のようになります。 **1.** アップグレードと移行の準備をします。リリースノート、アップグレードガイド、および移行ガイドに記載されているすべての前提条件を読み、理解し、条件を満たしてください。 アップグレードする前に、古い Management Center の「移行準備ができている」こと、つまり、移行するデバイスのみ管理していること、設定の影響（VPN の影響など）を評価していること、新たに展開されていて、完全にバックアップされていること、すべてのアプライアンスが正常な状態であることなどが特に重要です。 また、クラウドテナントのプロビジョニング、ライセンス付与、および準備もする必要があります。これには、セキュリティイベントロギングの方法を含める必要があります。サポートされていないバージョンが実行されるため、分析のためにオンプレミス Management Center を保持することはできません。 **2.** オンプレミス Management Center とそのすべての管理対象デバイスを少なくともバージョン 7.0.3 にアップグレードします（バージョン 7.0.5 を推奨）。 すでに最小バージョンを実行している場合は、この手順をスキップできます。 **3.** オンプレミス Management Center をバージョン 7.4 にアップグレードします。

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
			アップグレードパッケージを解凍し（ただし、展開はしない）、Management Center にアップロードします。Special Release からダウンロードします。 4. オンプレミス Management Center を CDO にオンボードします。 5. 移行ガイドの説明に従って、すべてのデバイスをオンプレミス Management Center から クラウド提供型 Firewall Management Center に移行します。 移行するデバイスを選択する場合は、[オンプレミスFMCからFTDを削除する（Delete FTD from On-Prem FMC）] を選択してください。変更をコミットするか、14 日が経過するまで、デバイスは完全には削除されないことに注意してください。 6. 移行が成功したことを確認します。 移行しても期待どおりに機能しない場合は、14 日以内に戻すことができます。戻さない場合は自動的にコミットされます。ただし、バージョン 7.4 は一般的な操作ではサポートされていないことに注意してください。オンプレミス Management Center をサポートされているバージョンに戻すには、再移行したデバイスを削除し、バージョン 7.0.x に再イメージ化し、バックアップから復元して、デバイスを再登録する必要があります。 参照： • Cisco Secure Firewall Threat Defense リリースノート • Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 • オンプレミス Management Center 管理対象 Cisco Secure Firewall Threat DefenseFirepower Threat Defense のクラウド提供型 Firewall Management Center への移行 移行プロセスの任意の時点で質問がある場合、またはサポートが必要な場合は、Cisco TAC にお問い合わせください。
Device Management			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
シリアル番号を使用して Firepower 1000/2100 および Cisco Secure Firewall 3100を Management Centerに登録するロータッチプロビジョニング。	7.4.0	Management Center がパブリックに到達可能：7.2.0 Management Center がパブリックに到達できない：7.2.4	ロータッチプロビジョニングを使用すると、Firepower 1000/2100 および Cisco Secure Firewall 3100 デバイスで初期セットアップを実行することなく、シリアル番号でデバイスを Management Center に登録できます。Management Center は、この機能のために SecureX および Cisco Defense Orchestrator と統合されています。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（Device）]** > **[シリアル番号（Serial Number）]** その他のバージョンの制限：この機能は、Management Center がパブリックに到達できない場合、バージョン 7.3.x または 7.4.0 Threat Defense デバイスではサポートされません。バージョン 7.4.1 でサポートが再開されています。 参照：「Add a Device to the Management Center Using the Serial Number (Low-Touch Provisioning)」
[インターフェイス（Interfaces）]			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
マージされた管理インターフェイスと診断インターフェイス。	7.4.0	7.4.0	**アップグレードの影響。アップグレード後にインターフェイスをマージします。** 7.4以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 プラットフォーム設定の場合、これは次のことを意味します。 • 診断インターフェイスで、HTTP、ICMP、または SMTP を有効にすることはできなくなりました。 • SNMP については、診断インターフェイスではなく管理インターフェイスでホストを許可できます。 • Syslog サーバーについては、診断インターフェイスではなく管理インターフェイスでアクセスできます。 • Syslog サーバーまたは SNMP ホストのプラットフォーム設定で診断インターフェイスが名前で指定されている場合、マージされたデバイスとマージされていないデバイスに別々のプラットフォーム設定ポリシーを使用する必要があります。 • インターフェイスを指定しない場合、DNS ルックアップは管理専用ルーティングテーブルにフォールバックしなくなりました。 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）]** 新規/変更されたコマンド： **show management-interface convergence** 参照：「Merge the Management and Diagnostic Interfaces」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
VXLAN VTEP IPv6 のサポート。	7.4.0	7.4.0	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 は、Threat Defense Virtual クラスタ制御リンクまたは Geneve カプセル化ではサポートされていません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [VTEP] > [VTEPの追加（Add VTEP）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Devices）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** 参照：「Configure Geneve Interfaces」
BGP および管理トラフィックのループバック インターフェイスのサポート。	7.4.0	7.4.0	AAA、BGP、DNS、HTTP、ICMP、IPsec フローオフロード、NetFlow、SNMP、SSH、および syslog にループバック インターフェイス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）] > [デバイスの編集（Edit Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [ループバック インターフェイス（Loopback Interface）] 参照：「Configure Loopback Interfaces」
ループバックおよび管理タイプのインターフェイス グループ オブジェクト。	7.4.0	7.4.0	管理専用インターフェイスまたはループバック インターフェイスのみを含むインターフェイス グループ オブジェクトを作成でき、作成したグループを DNS サーバー、HTTP アクセス、SSH などの管理機能に使用できます。ループバックグループは、ループバック インターフェイスを利用できるすべての機能で使用できますが、DNS では管理インターフェイスはサポートされていない点に注意してください。 新規/変更された画面：**[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [インターフェイス（Interface）] > [追加（Add）] > [インターフェイスグループ（Interface Group）]** 参照：「Interface」
高可用性/拡張性			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
データインターフェイスを使用して、Threat Defense ハイアベイラビリティペアを管理します。	7.4.0	7.4.0	Threat Defense ハイアベイラビリティでは、Management Center との通信に通常のデータインターフェイスを使用できるようになりました。以前は、スタンドアロンデバイスのみがこの機能をサポートしていました。 参照：「Using the Threat Defense Data Interface for Management」
Threat Defense の高可用性のための「誤フェールオーバー」の削減。	7.4.0	7.4.0	参照：「」「Heartbeat Module Redundancy」
SD-WAN			
WAN サマリーダッシュボード。	7.4.0	7.2.0	WAN サマリーダッシュボードには、WAN デバイスとデバイスのインターフェイスのスナップショットが表示されます。また、WAN ネットワーク、デバイス正常性に関する情報、インターフェイス接続、アプリケーション スループット、および VPN 接続に関するインサイトが表示されます。WAN リンクを監視し、予防的かつ迅速な回復措置を実行できます。 新規/変更された画面：[概要（Overview）] > [WANサマリー（WAN Summary）] 参照：「WAN Summary Dashboard」
HTTP パスのモニタリングを使用したポリシーベースのルーティング。	7.4.0	7.2.0	ポリシーベースルーティング（PBR）は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集された評価指標（RTT、ジッター、パケット損失、およびMOS）を使用できるようになりました。インターフェイスの HTTP ベースのアプリケーション モニタリング オプションは、デフォルトで有効になっています。モニタリング対象のアプリケーションが搭載され、パスを決定するためのインターフェイスの順序付けを行う一致 ACL を使用して、PBR ポリシーを設定できます。 新規/変更された画面：[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[インターフェイスの編集（Edit interface）] > [パスモニタリング（Path Monitoring）] > [HTTPベースのアプリケーションモニタリングの有効化（Enable HTTP based Application Monitoring）] チェックボックス。 プラットフォームの制限：クラスタ化されたデバイスではサポートされていません。 参照：「Configure Path Monitoring Settings」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
ユーザー ID と SGT を使用したポリシーベースのルーティング。	7.4.0	7.4.0	ユーザーとユーザーグループ、および PBR ポリシーの SGT に基づいてネットワークトラフィックを分類できるようになりました。PBR ポリシーの拡張 ACL を定義するときに、ID および SGT オブジェクトを選択できます。 新規/変更された画面：[オブジェクト（Objects）]>[オブジェクト管理（Object Management）] > [アクセスリスト（Access List）] > [拡張（Extended）] > [拡張アクセスリストの追加/編集（Add/Edit Extended Access List）] > [拡張アクセスリストエントリの追加/編集（Add/Edit Extended Access List Entry）] > [ユーザー（Users）] および [セキュリティグループタグ（Security Group Tag）] 参照：「Configure Extended ACL Objects」
VPN			
Cisco Secure Firewall 4200 向け VTI ループバックインターフェイスの IPSec フローのオフロード。	7.4.0	7.4.0	Cisco Secure Firewall 4200 では、VTI ループバックインターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされます。以前は、この機能は Secure Firewall 3100 の物理インターフェイスでサポートされていました。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。 その他の要件：FPGA ファームウェア 6.2 以降 参照：「IPSec Flow Offload」
Cisco Secure Firewall 4200 の暗号デバッグの機能拡張。	7.4.0	7.4.0	暗号デバッグの機能拡張は次のとおりです。 • 暗号アーカイブは、テキスト形式とバイナリ形式で使用できるようになりました。 • 追加の SSL カウンタをデバッグに使用できます。 • スタックした暗号化ルールは、デバイスを再起動せずに ASP テーブルから削除できます。 新規/変更された CLI コマンド： **show counters** 参照：「Troubleshooting Using Crypto Archives」
VPN：リモートアクセス			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Secure Client のメッセージ、アイコン、画像、接続/切断スクリプトをカスタマイズします。	7.4.0	7.1.0	Secure Client をカスタマイズして、それらのカスタマイズを VPN ヘッドエンドに展開できるようになりました。サポートされている Secure Client のカスタマイズは次のとおりです。 • GUI テキストとメッセージ • アイコンとイメージ • スクリプト • バイナリ • Customized Installer Transforms • Localized Installer Transforms エンドユーザーが Secure Client から接続すると、Threat Defense によりそれらのカスタマイズがエンドポイントに配布されます。 新規/変更された画面： • [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [Secure Clientのカスタマイズ（Secure Client Customization）] • [デバイス（Device）] > [リモートアクセス（Remote Access）] > [VPNポリシーの編集（Edit VPN policy）] > [詳細設定（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customization）] 参照：「Customize Cisco Secure Client」
VPN：サイト間			
VPN ノードの IKE および IPsec セッションの詳細を簡単に表示できます。	7.4.0	いずれか	サイト間 VPN ダッシュボードで、VPN ノードの IKE および IPsec セッションの詳細を使いやすい形式で表示できます。 新規/変更された画面：[概要（Overview）] > [サイト間VPN（Site to Site VPN）] の順に選択し、[トンネルステータス（Tunnel Status）] ウィジェットの下で、トポロジにカーソルを合わせて [表示（View）] をクリックし、[CLIの詳細（CLI Details）] タブをクリックします。 参照：「Monitoring the Site-to-Site VPNs 」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
接続イベントのサイト間 VPN 情報	7.4.0	7.4.0（Snort 3）	接続イベントに、[ピアの暗号化（Encrypt Peer）]、[ピアの復号（Decrypt Peer）]、[VPNアクション（VPN Action）] の 3 つの新しいフィールドが含まれるようになりました。ポリシーベースおよびルートベースのサイト間 VPN トラフィックの場合、これらのフィールドにより、接続が暗号化または復号化（またはその両方）されたかどうか、および実行ユーザーが示されます。 新規/変更された画面：**[分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [イベントのテーブルビュー（Table View of Events）]** 参照：「Site to Site VPN Connection Event Monitoring」
NAT 変換からサイト間 VPN トラフィックを簡単に免除します。	7.4.0	いずれか	サイト間 VPN トラフィックを NAT 変換から簡単に免除できるようになりました。 新規/変更された画面： • エンドポイントの NAT 免除の有効化：**[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [サイト間VPNの追加/編集（Add/Edit Site to Site VPN）] > [エンドポイントの追加/編集（Add/Edit Endpoint）] > [ネットワークアドレス変換からVPNトラフィックを免除する（Exempt VPN traffic from network address translation）]** • NAT ポリシーのないデバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [NAT免除（NAT Exemptions）]** • 単一デバイスの NAT 免除ルールの表示：**[デバイス（Devices）] > [NAT] > [Threat Defense NATポリシー（Threat Defense NAT Policy）] > [NAT免除（NAT Exemptions）]** 参照：「NAT Exemption」
ルーティング			
IPv6 ネットワークで BGP のグレースフルリスタートを構成します。	7.4.0	7.3.0	管理対象デバイスのバージョン 7.3 以降の IPv6 ネットワークに対しては、BGP グレースフルリスタートを設定できます。 新規/変更された画面：[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] > [BGP] > [IPv6] > [ネイバー（Neighbor）] > [ネイバーの追加/編集（Add/Edit Neighbor）]。 参照：「Configure BGP Neighbor Settings」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
動的 VTI による仮想ルーティング。	7.4.0	7.4.0	ルートベースのサイト間VPNにダイナミック VTI を使用して仮想ルータを設定できるようになりました。 新規/変更された画面：[使用可能なインターフェイス（Available Interfaces）] の下の [デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] > [仮想ルータのプロパティ（Virtual Router Properties）] > [ダイナミックVTIインターフェイス（Dynamic VTI interfaces）]。 プラットフォームの制限：ネイティブモードのスタンドアロンまたは高可用性デバイスでのみサポートされます。コンテナインスタンスやクラスタ化されたデバイスではサポートされていません。 参照：「About Virtual Routers and Dynamic VTI」
アクセス制御：脅威の検出とアプリケーションの識別			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
クライアントレスの Zero Trust アクセス。	7.4.0	7.4.0（Snort 3）	Zero Trust アクセスが導入され、外部の SAML ID プロバイダー（IdP）ポリシーを使用して、ネットワークの内部（オンプレミス）または外部（リモート）から保護された Web ベースのリソース、アプリケーション、またはデータへのアクセスを認証および承認できます。 設定では、ゼロトラストアプリケーションポリシー、アプリケーショングループ、およびアプリケーションを指定します。 新規/変更された画面： • **[ポリシー（Policies）] > [Zero Trustアプリケーション（Zero Trust Application）]** • **[分析（Analysis）] > [接続（Connections）] > [イベント（Events）]** • **[概要（Overview）] > [ダッシュボード（Dashboard）] > [Zero Trust]** 新規/変更された CLI コマンド： • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics** 参照：「Zero Trust Access」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
暗号化された可視性エンジン機能の拡張。	7.4.0	7.4.0（Snort 3）	暗号化された可視性エンジン（EVE）で、次のことができるようになりました。 • 脅威スコアに基づいて暗号化トラフィック内の悪意のある通信をブロックする。 • EVE で検出されたプロセスに基づいてクライアント アプリケーションを判断する。 • 検出のために、フラグメント化された Client Hello パケットを再構成する。 新規/変更された画面：アクセス コントロール ポリシーの詳細設定を使用して EVE を有効にし、これらの設定を行います。 参照：「Encrypted Visibility Engine」
特定のネットワークとポートをエレファントフローのバイパスまたはスロットリングから免除します。	7.4.0	7.4.0（Snort 3）	エレファントフローのバイパスまたはスロットリングから特定のネットワークとポートを免除できるようになりました。 新規/変更された画面： • アクセス コントロール ポリシーの詳細設定でエレファントフロー検出を構成するときに、[エレファントフローの修復（Elephant Flow Remediation）] オプションを有効にすると、[ルールの追加（Add Rule）] をクリックして、バイパスまたはスロットリングから免除するトラフィックを指定できるようになりました。 • システムがバイパスまたはスロットリングから免除されているエレファントフローを検出すると、[エレファントフローが免除されました（Elephant Flow Exempted）] という理由でフロー中接続イベントを生成します。 プラットフォームの制限：Firepower 2100 シリーズではサポートされていません。 参照：「Elephant Flow Detection」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
カスタム アプリケーションディテクタを使用した最初のパケットアプリケーションの識別。	7.4.0	7.4.0（Snort 3）	新しい Lua ディテクタ API が導入され、TCP セッションの最初のパケットの IP アドレス、ポート、およびプロトコルがアプリケーションプロトコル（サービス AppID）、クライアントアプリケーション（クライアント AppID）、および Web アプリケーション（ペイロード AppID）にマッピングされます。この新しい Lua API addHostFirstPktApp は、パフォーマンスの向上、再検査、およびトラフィック内の攻撃の早期検出に使用されます。この機能を使用するには、カスタムアプリケーション ディテクタの高度なディテクタで検出基準を指定して、Lua ディテクタをアップロードする必要があります。 参照：「Custom Application Detectors」
機密データの検出とマスキング。	7.4.0	7.4.0（Snort 3）	**アップグレードの影響。デフォルトポリシーの新しいルールが有効になります。** 社会保障番号、クレジットカード番号、E メールなどの機密データは、インターネットに意図的に、または誤って漏洩される可能性があります。機密データの検出は、機密データの漏洩の可能性を検出してイベントを生成するために使用され、大量の個人識別情報（PII）データが転送された場合にのみイベントを生成します。機密データの検出では、組み込みパターンを使用して、イベントの出力で PII をマスクできます。 データマスキングの無効化はサポートされていません。 参照：「Custom Rules in Snort 3」
JavaScript インスペクションの改善。	7.4.0	7.4.0（Snort 3）	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。 参照：「HTTP Inspect Inspector」および Cisco Secure Firewall Management Center Snort 3 コンフィギュレーション ガイド [英語]
ファイルおよびマルウェアイベントに含まれる MITRE 情報。	7.4.0	7.4.0	ファイルおよびマルウェアイベントに MITRE 情報（ローカルマルウェア分析結果）が含まれるようになりました。以前は、この情報は侵入イベントについてのみ利用可能でした。MITRE 情報は、クラシックイベントビューと統合イベントビューの両方で表示できます。MITRE 列は、両方のイベントビューでデフォルトで非表示になっていることに注意してください。 参照：「Local Malware Analysis」および「File and Malware Event Fields」
Access Control：**Identity**			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Cisco Secure 動的属性コネクタによる動的オブジェクト管理の機能強化。	7.4.0	いずれか（Any）	次を使用した動的オブジェクト管理がサポートされるようになりました。 • Management Center の Cisco Secure 動的属性コネクタ。 • スタンドアロン アプリケーションとしての Cisco Secure 動的属性コネクタ 2.1。 参照：「Cisco Secure Dynamic Attributes Connector」および Cisco Secure Dynamic Attributes Connector コンフィギュレーション ガイド、バージョン2.1 [英語]
ユーザー ID ソースとしての Microsoft Azure AD。	7.4.0	7.4.0	Microsoft Azure Active Directory（Azure AD）レルムと ISE を使用すると、ユーザーを認証したりユーザー制御のためにユーザーセッションを取得したりできます。 新規/変更された画面： • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（Realms）] > [レルムを追加（Add Realm）] > [Azure AD（Azure AD）] • [統合（Integration）] > [その他の統合（Other Integrations）] > [レルム（ Realms）] > [アクション（Actions）]（ユーザーのダウンロード、コピー、編集、削除など） サポートされている ISE バージョン：3.0 パッチ 5 以降、3.1（任意のパッチレベル）、3.2（任意のパッチレベル） 参照：「Create a Microsoft Azure Active Directory Realm」
イベントロギングおよび分析			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして設定できます。	7.4.0	いずれか（Any）	**アップグレードの影響。アップグレード後に、関連する FlexConfig をすべてやり直します。** NetFlow は、パケットフローの統計情報を提供するシスコアプリケーションの 1 つです。Management Center の Web インターフェイスを使用して、Threat Defense デバイスを NetFlow エクスポータとして設定できるようになりました。既存の NetFlow FlexConfig があり、Web インターフェイスで設定をやり直す場合は、廃止された FlexConfig を削除するまで展開できません。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [Threat Defense設定ポリシー（Threat Defense Settings policy）] > [NetFlow]** 参照：「Configure NetFlow」
ログに記録された暗号化接続での「不明な」SSL アクションに関する詳細。	7.4.0	7.4.0	イベントレポートおよび復号ルールマッチングの有用性が向上しました。 • 暗号化された接続の SSL ハンドシェイクが完了していないかどうかを示す新しい**SSL ステータス**。ログに記録された接続の SSL ハンドシェイクが完了していない場合、接続イベントの [SSL ステータス（SSL Status）] 列に「不明（不完全なハンドシェイク）（Unknown (Incomplete Handshake)）」と表示されます。 • 証明書のサブジェクト代替名（SAN）は、強化された復号ルールマッチングの認証局（CA）名を照合するときに使用されるようになりました。 新規/変更された画面： • [分析（Analysis）] > [接続（Connections）] > [イベント（Events）] > [SSL ステータス（SSL Status）] • [分析（Analysis）] > [接続（Connections）] > [セキュリティ関連イベント（Security-Related Events）] > [SSL ステータス（SSL Status）] 参照：「Connection and Security-Related Connection Event Fields」
ヘルス モニタリング			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
OpenConfig を使用して、テレメトリを外部サーバーにストリーミング。	7.4.0	7.4.0	OpenConfigを使用して、メトリックとヘルスモニタリング情報をThreat Defenseデバイスから外部サーバー（gNMIコレクタ）に送信できるようになりました。TLSにより暗号化された接続を開始するようにThreat Defenseまたはコレクタを設定できます。 新規/変更された画面：**システム**（⚙）>**[ヘルス（Health）]**>**[ポリシー（Policy）]**>**[Firewall Threat Defenseポリシー（Firewall Threat Defense Policies）]**>**[設定（Settings）]**>**[OpenConfigストリーミングテレメトリ（OpenConfig Streaming Telemetry）]** 参照：「Send Vendor-Neutral Telemetry Streams Using OpenConfig」
新しいASPドロップメトリック。	7.4.0	7.4.0	新規または既存のデバイス正常性ダッシュボードに、600を超える新しいASP（高速セキュリティパス）ドロップメトリックを追加できます。[ASPドロップ（ASP Drops）]メトリックグループを選択していることを確認します。 新規/変更された画面：**システム**（⚙）>**[正常性（Health）]**>**[モニター（Monitor）]**>**[デバイス（Device）]** 参照：「show asp drop Command Usage」
管理（Administration）			
詳細な Management Center の監査ログを syslog に送信します。	7.4.0	いずれか	構成データの形式とホストを指定することにより、構成変更を監査ログデータの一部としてsyslogにストリーミングできます。Management Centerは、監査構成ログのバックアップと復元をサポートしています。 新規/変更された画面：**システム**（⚙）>[設定（Configuration）]>[監査ログ（Audit Log）]>[設定変更の送信（Send Configuration Changes）]。 参照：「Stream Audit Logs to Syslog」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
アクセスコントロールポリシーとルールを変更するための詳細なアクセス許可。	7.4.0	いずれか	カスタムユーザーロールを定義して、アクセスコントロールポリシーおよびルールの侵入設定と、その他のアクセスコントロールポリシーおよびルールを区別できます。これらのアクセス許可を使用すると、ネットワーク管理チームと侵入管理チームの責任を分離できます。 ユーザーロールを定義するときに、**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[アクセスコントロールポリシー（Access Control Policy）]** > **[アクセスコントロールポリシーの変更（Modify Access Control Policy）]** > **[脅威設定の変更（Modify Threat Configuration）]**オプションを選択して、侵入ポリシー、変数セット、およびルール内のファイルポリシー、ネットワーク分析および侵入ポリシーの詳細オプションの設定、アクセス コントロール ポリシーのセキュリティ インテリジェンス ポリシーの構成、およびポリシーのデフォルトアクションの侵入アクションを選択できるようにします。[残りのアクセスコントロールポリシー設定の変更（Modify Remaining Access Control Policy Configuration）] を使用して、ポリシーの他のすべての側面を編集する機能を制御できます。アクセス コントロール ポリシーの変更権限を含む既存の事前定義されたユーザーロールは、引き続きすべてのサブ権限をサポートします。詳細な権限を適用する場合は、独自のカスタムロールを作成する必要があります。 参照：「Create Custom User Roles」
国コードの地理位置情報パッケージのみをダウンロードします。	7.4.0	いずれか	IP アドレスを国や大陸にマッピングする地理位置情報データベース（GeoDB）の国コードパッケージのみをダウンロードするようにシステムを設定できるようになりました。追加のロケーションの詳細や接続情報を含むコンテキストデータを含む大規模な IP パッケージは、オプションになりました。デフォルトでは、両方のパッケージがダウンロードされます。 新規/変更された画面：**システム**（⚙） > **[更新（Updates）]** > **[地理位置情報の更新（Geolocation Updates）]** > **[IPパッケージの設定（IP Package Configuration）]** 参照：「」「Update the Geolocation Database」
証明書の失効を確認する際の IPv6 URL のサポート。	7.4.0	7.4.0	以前は、Threat Defense は IPv4 OCSP URL のみをサポートしていました。現在、Threat Defense は IPv4 と IPv6 の両方の OCSP URL をサポートしています。 参照：「Requiring Valid HTTPS Client Certificates」および「Certificate Enrollment Object Revocation Options」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
デフォルトの NTP サーバーが更新されました。	7.4.0	いずれか	新しい Management Center の展開では、デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。Management Center を使用して、独自のデバイスに時刻を提供することを推奨します。**システム**（⚙）>**[設定（Configuration）]**>**[時刻の同期（Time Synchronization）]**で Management Center の NTP サーバーを更新できます。 参照：「Internet Access Requirements」
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			

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
ユーザービリティの拡張。	7.4.0	いずれか	次の作業に進んでください。 • **システム**（⚙）> **[スマートライセンス（Smart Licenses）]** から Threat Defense クラスタのスマートライセンスを管理します。以前は、[デバイス管理（Device Management）] ページを使用する必要がありました。 参照：デバイスクラスタのライセンス • メッセージセンター通知のレポートをダウンロードします。メッセージセンターで、[通知を表示（Show Notifications）] スライダの横にある新しい [レポートのダウンロード（Download Report）] アイコンをクリックします。 参照：システムメッセージの管理 • すべての登録済みデバイスのレポートをダウンロードします。**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** に移動し、ページの右上にある新しい [デバイスリストレポートのダウンロード（Download Device List Report）] リンクをクリックします。 参照：管理対象デバイスリストのダウンロード • ネットワークおよびポートオブジェクトを複製します。オブジェクトマネージャ（**[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]**）で、ポートまたはネットワークオブジェクトの横にある新しい [クローン（Clone）] アイコンをクリックします。その後、新しいオブジェクトのプロパティを変更し、新しい名前で保存できます。 参照：ネットワークオブジェクトの作成およびポートオブジェクトの作成 • カスタム ヘルス モニタリング ダッシュボードを簡単に作成し、既存のダッシュボードを簡単に編集できます。 参照：「Correlating Device Metrics」

機能	Management Center の最小バージョン	Threat Defense の最小バージョン要件	詳細（Details）
Secure Firewall 4200 のパケットキャプチャでキャプチャするトラフィックの方向を指定します。	7.4.0	7.4.0	Secure Firewall 4200 では、 コマンドで新しい**direction**キーワード**capture**を使用できます。 新規/変更された CLI コマンド：**capture***capture_name***switchinterface***interface_name* [**direction** { **both** | **egress** | **ingress** }] 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Snort 3 が無応答になると再起動し、HA フェールオーバーがトリガーされる可能性があります。	7.4.0	7.4.0（Snort 3）	操作の継続性を向上させるために、応答しない Snort が高可用性フェールオーバーをトリガーできるようになりました。これは、プロセスが応答しなくなった場合に Snort 3 が再起動されるようになったために発生します。Snort プロセスを再起動すると、デバイスでのトラフィックフローと検査が一時的に中断され、高可用性展開ではフェールオーバーがトリガーされる可能性があります（スタンドアロン展開では、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）。 この機能は、デフォルトでイネーブルにされています。CLI を使用してフェールオーバーを無効にするか、Snort を再起動する条件として時間や無応答スレッド数を設定できます。 新規/変更された CLI コマンド： **configure snort3-watchdog** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
Management Center REST API			
Management Center REST API。	7.4.0	機能に依存	Management Center REST API の変更については、API クイックスタートガイドの「What's New in Version 7.4」を参照してください。

廃止された機能

表 *9 : Management Center* バージョン *7.4.0* で廃止済みの機能

機能	Management Center では廃止	Threat Defense では廃止	詳細（Details）
廃止：FlexConfig を使用した NetFlow。	7.4.0	いずれか	Management Center の Web インターフェイスから、Threat Defense デバイスを NetFlow エクスポータとして設定できるようになりました。この設定をすると、廃止された FlexConfig を削除するまで展開できません。 参照：「Configure NetFlow」

Device Manager の機能

この表では、Threat Defense バージョン 7.4 で使用可能な新機能と廃止された機能について説明します。

（注） バージョン 7.4 の機能に対する Device Manager のサポートは、バージョン 7.4.1 から始まります。これは、Device Manager をサポートするプラットフォームではバージョン 7.4.0 を使用できないためです。

バージョンごとの Snort 拡張機能の詳細については、Management Center が Device Manager よりも多くの設定可能オプションを提供する可能性があることに注意してくださいManagement Center の新機能リストを参照してください。Snort は、Device Manager または Management Center のどちらを使用しているか関係なく、Threat Defense の主要な検査エンジンです。

表 *10 : Device Manager* バージョン *7.4.1* の新機能と廃止された機能

機能	説明
プラットフォーム機能	
Firepower 1010E のサポートが再開されています。。	バージョン 7.2.3 で導入され、バージョン 7.3 で一時的に廃止された Firepower 1010E のサポートが再開されています。 参照：「Cabling for the Firepower 1010」

機能	説明
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	Cisco Secure Firewall 3130 および 3140 向けに次のネットワークモジュールが導入されました。 • 2 ポート 100G QSFP+ ネットワークモジュール（FPR3K-XNM-2X100G） 参照： Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド
VPN 機能	
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPSec フローのオフロード。	**アップグレードの影響。 条件を満たす接続のオフロードが開始されます。** Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPsec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。この機能はアップグレードにより自動的に有効になります。 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	

機能	説明
マージされた管理インターフェイスと診断インターフェイス。	**アップグレードの影響。アップグレード後にインターフェイスをマージします。** 7.4 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。 7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。 マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。 新規/変更された画面： • **[Devices]** > **[Interfaces]** > **[Management]** インターフェイス • （インターフェイスに移動）**[System Settings]** > **[Management Interface]** • **[Devices]** > **[Interfaces]** > **[Merge Interface action needed]** > **[Management Interface Merge]** 新規/変更されたコマンド： **show management-interface convergence**
Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開します。	Azure と GCP の Threat Defense Virtual で診断インターフェイスを使用しないで展開できるようになりました。Azure の展開には引き続き少なくとも 2 つのデータインターフェイスが必要ですが、GCP では診断インターフェイスをデータインターフェイスに置き換える必要があり、新しい最小は3つです（以前は、Threat Defense Virtual の展開には、1 つの管理インターフェイス、1 つの診断インターフェイス、および少なくとも 2 つのデータインターフェイスが必要でした）。 制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

機能	説明
Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 に対するインラインセット。	Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 デバイスでインラインセットを設定できます。[インターフェイス（Interface）] ページに [インラインセット（inline sets）] タブを追加しました。
ライセンシング機能	
ライセンス名の変更およびキャリアライセンスのサポート。	ライセンス名が次のように変更されました。 • Threat は IPS に変更 • Malware は Malware Defense に変更 • Base は Essentials に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。これらの機能を設定するには、FlexConfig を使用します。 参照：「Licensing the System」
管理およびトラブルシューティングの機能	
デフォルトの NTP サーバーが更新されました。	**アップグレードの影響。システムは新しいリソースに接続します。** デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。別の NTP サーバーを使用するには、[デバイス（Device）] を選択し、[システム設定（System Settings）] パネルで [タイムサービス（Time Services）] をクリックします。

機能	説明
HTTPS 管理ユーザーアクセス用の SAML サーバー。	HTTPS 管理アクセスに外部認証を提供するように SAML サーバーを設定できます。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーを使用する場合は、ログインに共通アクセスカード（CAC）を使用できます。 SAML アイデンティティ ソース オブジェクトの設定を更新し、該当オブジェクトを受け入れるように**[システム設定（System Settings）] > [管理アクセス（Management Access）]** ページを更新しました。
Threat Defense 高可用性ペアの設定の不一致を検出します。	CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。 新規/変更された CLI コマンド：**show failover config-sync error**、**show failover config-sync stats** 参照：Cisco Secure Firewall Threat Defense コマンドリファレンス
Cisco Secure Firewall 3100 でドロップされたパケットをキャプチャします。	MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100 は、これらのドロップされたパケットをキャプチャできるようになりました。 新規/変更された CLI コマンド：**capture** コマンドの **[drop** { **disable** | **mac-filter** }]。 参照：Cisco Secure Firewall Threat Defense コマンドリファレンス

機能	説明
FXOS アップグレードに含まれるファームウェアのアップグレード。	**シャーシ/FXOSアップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 以降への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアの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。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	Firepower 1000/2100 または Firepower 4100/9300 のデータプレーンプロセスがクラッシュすると、デバイスを再起動する代わりにプロセスがリロードされます。データプレーンをリロードすると、Snort を含む他のプロセスも再起動します。ブートアップ中にデータプレーンがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードループが回避されます。 この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。 新規/変更された ASA CLI コマンド：**data-plane quick-reload**、**show data-plane quick-reload status** 新規/変更された Threat Defense CLI コマンド：**show data-plane quick-reload status** サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300 参照：Cisco Secure Firewall Threat Defense コマンドリファレンスおよびCisco Secure Firewall ASA シリーズ コマンド リファレンス

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。

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。

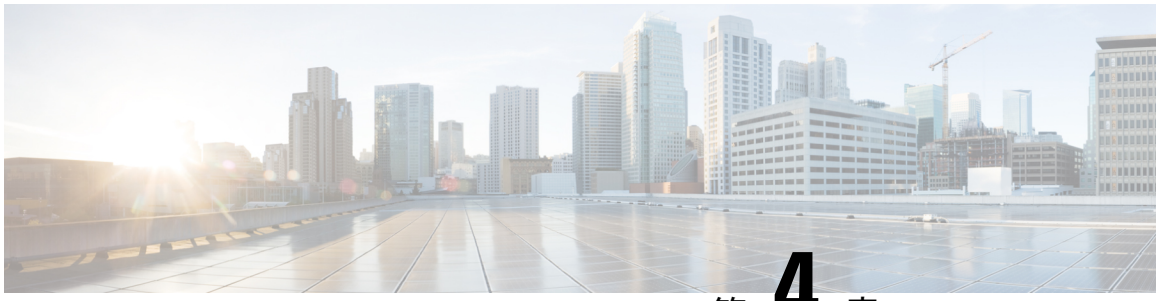
注意 ほとんどの場合、既存の FlexConfig 設定はアップグレード後も引き続き機能し、展開ができます。ただし、廃止されたコマンドを使用すると、展開の問題が発生する場合があります。

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

アップグレードガイドライン

このドキュメントには、バージョン 7.4 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、

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-74-docs）を参照してください。

表 *11* : 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。

計画フェーズ	次を含む
バックアップ	設定およびイベントをバックアップします。 Firepower 4100/9300 および 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 のファームウェアをアップグレードします。 Firepower 4100/9300 および 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。 Management Center で変更管理ワークフローを確認します。 設定を展開します。 準備状況チェックを実行します。 ディスク容量を確認します。 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

アップグレードする最小バージョン

次のように、メンテナンスリリースを含む バージョン 7.4 に直接アップグレードできます。

表 *12 :* バージョン *7.4* 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	7.0

プラットフォーム	最小バージョン
脅威防御 （GCP 対応 Threat Defense Virtual を除く）	7.0 Firepower 4100/9300 には FXOS 2.14.1.131 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 2.14 リリースノート を参照してください。
GCP 向け Threat Defense Virtual	7.2 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ないため、新しいインスタンスを展開する必要があります。

バージョン 7.4 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 *13 : 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 *7.4*

✓	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
常にチェック				
	アップグレードする最小バージョン （74 ページ）	任意（Any）	任意（Any）	任意（Any）
	Cisco Secure Firewall Management Center の新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	任意（Any）	任意（Any）	任意（Any）
	未解決のバグおよび解決されたバグ （93 ページ）：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	任意（Any）	任意（Any）	任意（Any）

✓	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
	クラウド提供型 Firewall Management Center のアップグレードガイドライン （78 ページ）	Threat Defense	任意（Any）	任意（Any）
	Firepower 4100/9300 シャーシのアップグレードガイドライン （78 ページ）	Firepower 4100/9300 Secure Firewall 3100/4200	任意（Any）	任意（Any）
特定の展開に対するその他のガイドライン				
	大規模構成向けの拡張された、バージョン 7.4.0 へのアップグレード後の展開 （77 ページ）	Management Center	6.6.0 +	7.4.0 のみ

表 *14 : 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 *7.4*

✓	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
常にチェック				
	アップグレードする最小バージョン （74 ページ）	任意（Any）	任意（Any）	任意（Any）
	Cisco Secure Firewall デバイスマネージャの新機能（リリース別）：アップグレードに影響を与える新機能および廃止された機能が記載されています。現在のバージョンと対象バージョンの間にあるすべてのバージョンを確認してください。	任意（Any）	任意（Any）	任意（Any）
	未解決のバグおよび解決されたバグ （93 ページ）：アップグレードに影響を与えるバグが記載されています。現在のバージョンと対象バージョン間にあるすべてのバージョンのリリースノートを確認してください。	任意（Any）	任意（Any）	任意（Any）

✓	ガイドライン	プラットフォーム	アップグレード元	直接アップグレード先
	Firepower 4100/9300 シャーシのアップグレードガイドライン（78 ページ）	Firepower 4100/9300	任意（Any）	任意（Any）

特定の展開に対するその他のガイドライン
このリリースに固有の Device Manager に関する追加のアップグレードガイドラインはありません。

大規模構成向けの拡張された、バージョン7.4.0へのアップグレード後の展開

展開：Management Center

アップグレード元：オブジェクト最適化が無効になっている展開。

直接アップグレード先：バージョン 7.4.0 のみ

アクセス コントロール オブジェクトの最適化により、ネットワークが重複するアクセス コントロール ルールがある場合、パフォーマンスが向上し、デバイス リソースの消費が少なくなります。最適化は、Management Center で機能が有効になった後の最初の展開時に管理対象デバイスで行われます（アップグレードで有効になった場合も含む）。ルールの数が多い場合、システムがポリシーを評価してオブジェクトの最適化を実行するのに数分から 1 時間かかることがあります。この間、デバイスの CPU 使用率も高くなることがあります。機能が無効になった後の最初の展開でも同様のことが発生します（アップグレードによって無効になった場合も含む）。この機能が有効または無効になった後は、メンテナンス時間帯やトラフィックの少ない時間帯など、影響が最小限になる時間に展開することを強く推奨します。

計画するには、次の表を使用します。

表 *15*：オブジェクト最適化を使用した *Management Center* のアップグレードの計画

バージョン（Version）	デフォルト/設定の再イメージ	Upgrading	有効化/無効化
7.0.5 以前	サポートされていません（無効）。	—	—
7.0.6以降のメンテナンスリリース	ディセーブル。	現在の設定が保持されます。	Cisco TAC にお問い合わせください。
7.1.0 ～ 7.2.3	サポートされていません（無効）。	無効。	—

バージョン（Version）	デフォルト/設定の再イメージ	Upgrading	有効化/無効化
7.2.4 ～ 7.2.5	イネーブル。	有効。	Cisco TAC にお問い合わせください。
7.3.x	サポートされていません（無効）。	無効。	—
7.4.0	イネーブル。	有効。	Cisco TAC にお問い合わせください。
7.4.1 以降	イネーブル。	現在の設定が保持されます。	ユーザー設定可能。

クラウド提供型 Firewall Management Center のアップグレードガイドライン

クラウド提供型 Firewall Management Center はアップグレード対象外です。機能の更新はシスコが行います。クラウド提供型 Firewall Management Center を使用して Threat Defense をアップグレードするには、クラウド提供型 Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイドを参照してください。

Firepower 4100/9300 シャーシ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シャーシのアップグレード（FXOS とファームウェア）も必要です。メンテナンスリリースとパッチで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、最新のビルドにアップグレードして、解決済みの問題を活用することもできます。

表 *16 : Firepower 4100/9300* シャーシのアップグレードガイドライン

ガイドライン	詳細
FXOS のアップグレード。	Firepower 4100/9300 で Threat Defense バージョン 7.4 を実行するには、FXOS 2.14.1.131 以降が必要です。 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。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。

ガイドライン	詳細
ファームウェアのアップグレード。	FXOS 2.14.1 以降のアップグレードにはファームウェアが含まれます。以前の FXOS バージョンにアップグレードする場合は、Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイドを参照してください。
アップグレードの時間。	シャーシのアップグレードには最長 45 分かかり、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、シャーシ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 （79 ページ）を参照してください。

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。

- マネージャにかかわらず、メジャーおよびメンテナンスアップグレードの Threat Defense への復元がサポートされています。
- Management Center を使用した Threat Defense のパッチのアンインストールがサポートされています。Management Center パッチをアンインストールすることもできます。

これが機能せず、以前のバージョンに戻す必要がある場合、イメージを再作成する必要があります。ガイドライン、制限、および手順については、現在実行しているバージョンの Management Center/デバイスマネージャ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（ソフトウェアおよびオペレーティングシステム）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。

シャーシ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。ファームウェアのアップグレードを含むバージョン 2.14.1 以降への FXOS アップグレードの場合、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。対象には、 のバージョン 7.4.1 以降のシャーシアップグレードが含まれます。

高可用性またはクラスタ展開の場合でも、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 *17:* 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

Threat Defense の導入	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。

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 *18*：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。

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 *19*：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。

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

アップグレードまでの時間

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。次の表に、アップグレード時間に影響を与える可能性のあるいくつかの事項を示します。

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、アップグレードガイド（https://www.cisco.com/go/ftd-upgrade）でトラブルシューティング情報を見つけることができます。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。

表 *20*：アップグレード時間の考慮事項

考慮事項	詳細（Details）
バージョン	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	通常、ローエンドモデルではアップグレード時間が長くなります。
仮想アプライアンス	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します。

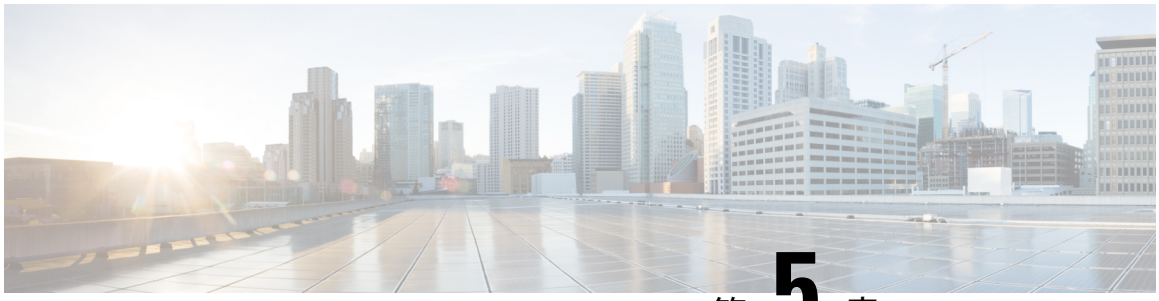
考慮事項	詳細（**Details**）
高可用性とクラスタリング	高可用性の構成またはクラスタ化された構成では、動作の継続性を保持するため、複数のデバイスは 1 つずつアップグレードされます。アップグレード中は、各デバイスはメンテナンスモードで動作します。そのため、デバイスペアまたはクラスタ全体のアップグレードには、スタンドアロンデバイスのアップグレードよりも長い時間がかかります。
設定	アップグレード時間は、構成の複雑さ、イベントデータベースのサイズ、それらがアップグレードから影響を受けるかどうか、どのような影響を受けるかによって長くなります。たとえば、多くのアクセス制御ルールを使用している場合、アップグレードではそ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、さらに長い時間がかかります。
コンポーネント	オペレーティングシステムまたは仮想ホスティングのアップグレード、アップグレードパッケージの転送、準備状況チェック、VDB と侵入ルール（SRU/LSP）の更新、設定の展開、およびその他の関連タスクを実行するために、追加の時間が必要になる場合があります。

アップグレードするディスク容量

アップグレードするには、アップグレードパッケージがアプライアンスにある必要があります。Management Center を使用するデバイスのアップグレードの場合は、Management Center（/Volume または /var のいずれか）にもデバイス アップグレード パッケージ用の十分な容量が必要です。または、内部サーバーを使用して保存することもできます。準備状況チェックでは、アップグレードを実行するのに十分なディスク容量があるかどうかが示されます。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 *21* : 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**（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]** を選択し、Management Center を選択します。 [ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
Management Center による脅威防御	**システム**（⚙） > **[モニタリング（Monitoring）]** > **[統計（Statistics）]** を選択し、確認するデバイスを選択します。 [ディスク使用率（Disk Usage）] で、[By Partition] の詳細を展開します。
Device Manager を使用した Threat Defense	**show disk** CLI コマンドを使用します。



第 5 章

ソフトウェアのインストール

バージョン 7.4 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たくない場合は、ソフトウェアを新しく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。

- 設置に関するガイドライン （87 ページ）
- 設置ガイド （91 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。

Cisco Secure Firewall 3100 バージョン 7.3 以降への再イメージ化

再イメージ化の影響。

バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。

- バージョン 7.1 ～ 7.2 インストールパッケージ：isco-ftd-fp3k.*version*.SPA
- バージョン 7.1 ～ 7.2 アップグレードパッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar
- バージョン 7.3 以降の統合パッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar

Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。

Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。

- Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。

  該当するアップグレードガイドを参照してください。

- Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。

  『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「*Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100*」、次に「*ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100*」を参照してください。

- ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。

  『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「*ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100*」を参照してください。

- Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。

  『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「*Reimage the System with a New Software Version*」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。
Threat Defense を Management Center から Device Manager へ切り替えます。	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。

Management Center からのデバイスの削除

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 : Management Center* 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。
Threat Defense を Management Center から Device Manager へ切り替えます。	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。

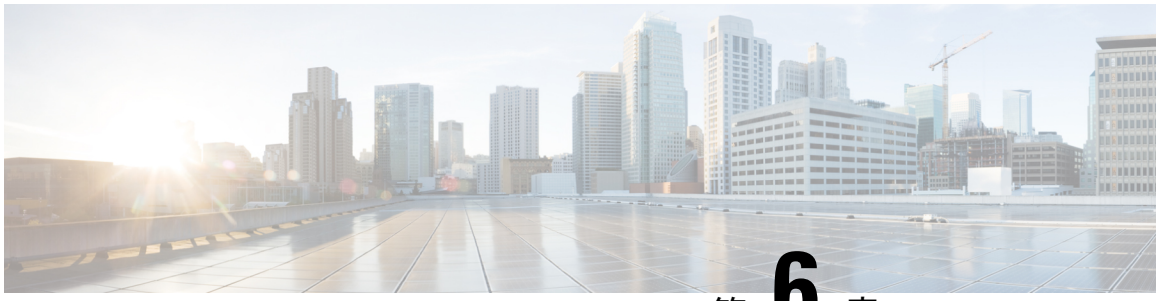
表 *24 :* 完全な再イメージ化のシナリオ

モデル	詳細
Firepower 1000 シリーズ Firepower 2100 シリーズ Secure Firewall 3100 シリーズ Cisco Secure Firewall 4200 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。 Secure Firewall 3100/4200 の場合は、再イメージ化によってデバイスがアプライアンスモードになります。マルチインスタンスモードを使用していた場合は、再度有効にする必要があります。
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	
Cisco Secure Firewall Management Center 1700、2700、4700	Cisco Secure Firewall Management Center 1700、2700、および 4700 スタートアップガイド
FMC 1600、2600、4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide ド
Management Center Virtual	Cisco Secure Firewall Management Center Virtual 入門ガイド
Threat Defense	
Firepower 1000/2100 シリーズ Secure Firewall 3100/4200 シリーズ	Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides：イメージ管理に関する章 Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide
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

このドキュメントには、バージョン 7.4 デバイスならびにお客様が導入した Management Center の未解決のバグと解決済みのバグの一覧が記載されています。

クラウド提供型 Firewall Management Center のバグについては、Cisco クラウド提供型 Firewall Management Center リリースノート を参照してください。

重要 バグリストは一度自動生成されると、その後は更新されない場合があります。更新された場合、「表の最終更新日」は、リストがその日付で完全に正確になったことを意味するのではありません。一部に変更が加えられただけです。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。大部分の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。

未解決のバグ

バージョン 7.4.1 で未解決のバグ

表の最終更新日：2023 年 12 月 14 日

表 *26* : バージョン *7.4.1* で未解決のバグ

不具合 ID	タイトル
CSCwd87510	フローのエクスポート先が交換された場合、またはポート値が変更された場合に展開が失敗する
CSCwe37049	9.20/WA GCM と CBC のパフォーマンスの調査

不具合 ID	タイトル
CSCwh74666	アプリケーションが見つからないため、レガシー ACP UI がロード中にスタックすることがある
CSCwh79546	別のチケットで作成された新しいオブジェクトで参照されているオブジェクトを削除した場合にエラーメッセージが表示されない
CSCwi02997	AI アシスタントのチャットウィンドウにネットワークエラーが表示される
CSCwi24816	WM での 「サービス要素はオブジェクト ネットワーク サービスにすでに存在します（The service element already exists in object network-service）」メッセージフラッド 4 CMI の有効化/無効化
CSCwi31008	展開中にデバイスがダウンし、起動しない場合、FMC で展開がスタックする
CSCwi38929	更新された nmap 7.94 バージョンの OS フィンガープリント マッピングの更新
CSCwi44265	メモリ/ストレスが低いため、ブロックの二重解放とリロードが発生する
CSCwi46679	FMC ダッシュボードに製品の更新に関する情報がロードされない

バージョン 7.4.0 で未解決のバグ

表の最終更新日：2023 年 9 月 11 日

表 *27* : バージョン *7.4.0* で未解決のバグ

不具合 ID	タイトル
CSCwd87510	フローのエクスポート先が交換された場合、またはポート値が変更された場合に展開が失敗する
CSCwe36422	Zero Trust ポリシーの IDP SAML 欠落フィルタにより、すべてのグループに IDP データが欠落していると表示される
CSCwf93776	[新規ユーザー（New User）] アクティビティページに特殊なアイデンティティレルムのイベントが表示されない
CSCwh00002	サブスクリプションを無効にするか、ISE 構成を変更した後、Azure AD セッションが削除されない
CSCwh04354	プロキシを使用してレルムをインポートできない
CSCwh38213	CSDAC 動的属性フィルタの編集で内部エラーがスローされる
CSCwh41164	OSPFv3 BFD セッションが 7 を超えて起動しない

不具合 ID	タイトル
CSCwh45488	FTD から cdFMC への移行中に、ユーザー ID を使用した PBR 設定が移行されない
CSCwh46657	Zero Trust ポリシーの更新時に [保存（Save）] ボタンが無効になる
CSCwh49918	Management Center のアップグレード時に新しい SRU がすぐにインストールされない
CSCwh50221	4200 シリーズ：LACP がアクティブモードの場合、クラスタのポートチャネルがダウンしたままになることがある
CSCwh50259	ファイルが存在しない場合に統合ファイルを開けないときに、EventHandler で警告がログに記録されない

解決済みのバグ

バージョン 7.4.1 で解決済みのバグ

表の最終更新日：2023 年 12 月 13 日

表 *28* : バージョン *7.4.1* で解決済みのバグ

不具合 ID	タイトル
CSCvc06888	FMC は FTD の名前付きインターフェイスのみをモニターする必要がある
CSCvq48086	syslog サーバーに送信中に、ASA によって syslog イベントが他の syslog イベントに連結される
CSCvj22491	FMC が SSM への接続に失敗し、「サーバーへのメッセージの送信に失敗しました（Failed to send the message to the server）」というエラーが表示される
CSCvx44261	SNMPv3：FXOS SNMPv3 設定で特殊文字を使用すると認証エラーが発生する
CSCvy31169	展開の失敗：コンテナをロードできない
CSCvy50598	インターフェイスの停止時に BGP テーブルが接続ルートを削除しない
CSCvz03407	IPTables.conf ファイルが消え、バックアップと復元が失敗する
CSCvz22945	エラー：削除済みの IDB が使用中のキューで見つかりました：メッセージが誤解を招く

不具合 ID	タイトル
CSCvz34289	場合によっては、軽量プロキシへの移行が Do Not Decrypt フローで機能しない
CSCvz36903	クラスタのキープアライブパケットに新しいブロックを割り当てている間に ASA でトレースバックとリロードが発生する
CSCvz71215	FMC が誤った順序で SLA モニターコマンドをプッシュしているため、展開が失敗する
CSCvz71596	「アクティブとスタンバイのインターフェイスの数が一致していません」という警告の syslog がトリガーされるはずである
CSCwa36535	構成サイズが大きいため、スタンバイユニットがフェールオーバーの参加に失敗
CSCwa53186	インライン TAP を使用した FTD が誤った MAC アドレスでフレームを書き換え、接続の問題が発生する
CSCwa59907	LINA は、スレッド名「snmp_client_callback_thread」でトレースバックを観察した
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
CSCwa72528	証明書からのユーザー名機能が SER オプションで機能しない
CSCwa72929	プライバシーアルゴリズムの AES192 または AES256 を使用した場合、SNMPv3 ポーリングが失敗することがある
CSCwa74063	NLP への管理アクセスが有効になった後、NLP ルールのインストールの回避策が無効になる
CSCwa82791	ENH：「Blocks free curr」が低くなった場合の InternalData インターフェイスでの RX キューのスナップショットのサポート
CSCwa82850	ASA フェールオーバーで、参加ノードを「スタンバイ準備完了」と宣言する前にコンテキストの不一致が検出されない
CSCwa97917	電源再投入後に ISA3000 がブートループの状態になる
CSCwb00871	ENH：拡張時またはストレス時のウォッチドッグを減らすために log_handler_file の遅延を削減
CSCwb04000	ASA/FTD：VTI にルーティングされるパケットに DF ビットが設定されている
CSCwb17963	動的レート制限メカニズムを識別できず、syslog サーバーで 1 秒あたりのメッセージ制限に従っていない

不具合 ID	タイトル
CSCwb31551	インバウンドパケットに SGT ヘッダーが含まれている場合、FPR2100 が 5 タプルごとに適切に配布できない
CSCwb53172	FTD：IKEv2 トンネルが 24 時間ごとにフラップし、暗号アーカイブが生成される
CSCwb53328	Smart Call Home プロセス sch_dispatch_to_url によって ASA/FTD のトレースバックとリロードが引き起こされる
CSCwb66382	ASAv：9344 ジャンボフレームを有効にした後にブロックが自動的に作成されず、OSPF MD5 が壊れる
CSCwb73248	タイマーインフラ/ネットフロータイマーで FW のトレースバックが発生する
CSCwb74571	ゾーンメンバーを使用する ASA ルーテッドモードで PBR が機能しない
CSCwb79062	FMC GUI に未使用のネットワークオブジェクトの正しい数が表示されない
CSCwb79812	RIP が接続されているすべての Anyconnect ユーザーをアドバタイズしており、再配布用のルートマップと一致しない
CSCwb83691	FMC から開始されたキャプチャが原因で ASA/FTD のトレースバックとリロードが発生する
CSCwb87498	EIGRP ルート更新処理中の Lina のトレースバックとリロード。
CSCwb89963	スレッド名：「Datapath」 での ASA トレースバックとリロード
CSCwb90532	NAT 関連の機能 nat_policy_find_location で ASA/FTD のトレースバックとリロードが発生する
CSCwb92320	Flex の移行後にネットワークオブジェクトが表示されず、EIGRP の [設定（Setup）] でインターフェイスの変更を保存できない
CSCwb92709	インターフェイスがコンテキストから削除されると、「snmpwalk」を使用してインターフェイスを監視できない
CSCwb93932	接続レプリケーションの競合状態に起因する ASA/FTD フェールオーバーペアのトレースバックとリロード
CSCwb94190	フォワーディング リファレンス関数と FIPS が有効になっている ACL を適用すると、ASA がグレースフルシャットダウンする
CSCwb94312	SSH 設定を ASA バージョン 9.16 以降に適用できない

不具合 ID	タイトル
CSCwb95784	レジスタの読み取り中に障害/遅延が発生した場合に、最後の 20 rmu 要求応答パケットをキャッシュおよびダンプする
CSCwb95850	アプリケーションディテクタが無効になっているため、lua ファイルが見つからずに Snort がダウンする（PM 側）
CSCwb97251	ASA/FTD がスレッド名「ssh」でトレースバックし、リロードすることがある
CSCwc02488	ASA/FTD がスレッド名「None」でトレースバックし、リロードすることがある
CSCwc03069	インターフェイスの internal data0/0 は cli からは up/up になるが、SNMP ポーリングからは up/down になる
CSCwc03507	CPU ホグの証拠がほとんどないにもかかわらず、内部データインターフェイスでのバッファドロップがない
CSCwc05375	AnyConnect SAML - 外部ブラウザ内でクライアント証明書プロンプトが正しく表示されない
CSCwc07262	スタンバイ ASA が、9.16(3) へのアップグレード後、設定の複製中にブートループになる。
CSCwc08646	SSH クライアントからログインすると、パスワードのないユーザーがパスワードの変更を求められる
CSCwc09414	ASA/FTD がスレッド名「ci/console」でトレースバックし、リロードすることがある
CSCwc10145	FTDv クラスタユニットがクラスタに再参加せず、エラーメッセージ「NLP SSL リスニングソケットを開けませんでした」が表示される
CSCwc10241	アップグレードまたはデバイスのリブート後の一時的な HA スプリットブレイン
CSCwc10483	ASA/FTD がスレッド名「appAgent_subscribe_nd_thread」でトレースバックする
CSCwc11511	FTD: 7.0.2 へのアップグレード後の SNMP エラー
CSCwc11597	SFR が 6.7.0.3 にアップグレードされると、ASA のトレースバックが発生する
CSCwc11663	CSM または CLI を使用して DNS インスペクションポリシーを変更すると、ASA のトレースバックとリロードが発生する

不具合 ID	タイトル
CSCwc12322	FPR3100 プラットフォームでのデジタル署名された ASDM イメージ検証エラーである
CSCwc13017	../inspect/proxy.h:439 で FTD/ASA のトレースバックとリロードが発生する
CSCwc13994	ASA：バックアップ後にインターフェイス設定で新しい構成を削除せずに復元する
CSCwc18312	EEM スクリプト内で実行される「show nat pool cluster」コマンドにより、トレースバックとリロードが発生する
CSCwc18524	コマンド「show environment」で ASA/FTD 電圧情報が不足している
CSCwc23356	ASA/FTD がスレッド名「DATAPATH-20-7695」でトレースバックおよびリロードすることがある
CSCwc23695	ASA/FTD がユーザー証明書の SAN フィールドから UPN を解析できない
CSCwc24422	クライアントのマシン証明書に空のサブジェクトがある場合、AC SSLVPN で証明書の認証と DAP に失敗する
CSCwc24906	スレッド ID 1637 で ASA/FTD のトレースバックとリロードが発生する
CSCwc26648	ASA/FTD がスレッド名 Lina または Datatath でトレースバックおよびリロードする
CSCwc27846	アップグレードとリロードの後の HA 同期中にトレースバックおよびリロードする。
CSCwc28532	インラインセットインターフェイスの内部フロー処理によってフラグメント化された GRE トラフィックが原因で、9344 ブロックでリークが発生する
CSCwc28684	FTD コンテナインスタンスがリロードされると MI がハングし、応答しない
CSCwc28806	プロセス名 Lina で ASA がトレースバックし、リロードする
CSCwc28854	複数のコンテキストでフェールオーバーが設定されている場合の不適切な IF-MIB 応答である
CSCwc28928	ASA：VTY セッションで SLA デバッグが表示されない
CSCwc32246	オブジェクトサブネット 0.0.0.0 0.0.0.0 が使用されている場合、NAT64 はすべての IPv6 アドレスを 0.0.0.0/0 に変換する
CSCwc35583	作成された各 u2 ファイルで Snort がファイル記述子をリークする

不具合 ID	タイトル
CSCwc36905	「slib_malloc.c でヒープ メモリが破損」した結果、ASA がトレースバックしリロードする
CSCwc37256	アップグレード後に SSL AnyConnect アクセスがブロックされる
CSCwc40352	Lina NetFlow から許可されたイベントが Stealthwatch に送信され、後で Snort によってブロックされる
CSCwc40381	ASA：カットスループロキシが有効になっている場合の HTTPS トラフィック認証の問題
CSCwc44289	FTD：IPv4 <> IPv6 NAT 変換を実行するときのトレースバックとリロード
CSCwc45108	ASA/FTD：9344 サイズのブロックリークを引き起こす GTP インスペクション
CSCwc45397	ASA HA：プライマリの復元で、バックアップ後に行われた新しいインターフェイス設定が削除されない
CSCwc45575	nopassword キーワードを持つユーザー名を使用した ssh の場合、ASA/FTD がトレースバックおよびリロードする
CSCwc48375	インバウンド IPSEC SA が非アクティブのままスタックする：「show crypto ipsec sa」の 1 つのアウトバウンド SPI に対して多数のインバウンド SPI がある
CSCwc49095	フラグメントが結合されて PDTS に送信される場合、ASA/FTD 2100 プラットフォームがトレースバックおよびリロードする
CSCwc50887	FTD：CCL リンク経由でリダイレクトされる UDP フローの NAT IPv4 <> IPv6 でのトレースバックとリロード
CSCwc50891	MPLS タギングが FTD によって削除される
CSCwc51326	FXOS ベースの Firepower プラットフォームで、RX リングウォーターマークの値が高いにもかかわらず、「バッファなし」ドロップを示す
CSCwc52351	「any」およびグローバル IP/範囲がブロードキャスト IP に一致する NAT が原因で起こる ASA/FTD クラスタスプリットブレイン
CSCwc53280	ASA パーサーが OSPF プロセスの下で不完全なネットワークステートメントを受け取り、show run に表示される
CSCwc54217	FPR2140 でフェールオーバーに関する syslog が出力されない
CSCwc54984	IKEv2キー の再生成：Create_Child_SA 応答の直後に受信した新しい SPI に対して無効な SPI を応答する

不具合 ID	タイトル
CSCwc60037	ASA が IPSEC エラーでキーの再生成に失敗する: アウトバウンド ハードウェア コンテキストの割り当てに失敗する
CSCwc61912	ASA/FTD OSPFv3 が IPv6 のメッセージタイプ 8 LSA を生成しない
CSCwc66757	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwc67031	NAT-T が有効なピンホール接続を備えた vti ハブがループし、snort ビジードロップを引き起こしている
CSCwc67886	ASA/FTD がスレッド名「lina_inotify_file_monitor_thread」でトレースバックおよびリロードすることがある
CSCwc70962	FTD/ASA の「書き込みスタンバイ」により ECDSA 暗号が有効になり、AC SSLv3 ハンドシェイクが失敗する
CSCwc72155	ASA/FTD が関数「snp_cluster_trans_allocb」でトレースバックおよびリロードする
CSCwc72284	TACACS アカウンティングに、クライアントの誤った IPv6 アドレスが含まれる
CSCwc73224	スタンバイデバイスの Call Home 設定がリロード後に失われる
CSCwc74103	ASA/FTD がスレッド名「DATAPATH-11-32591」でトレースバックおよびリロードすることがある
CSCwc74858	FTD：スレッド名 DATAPATH でのトレースバック
CSCwc77680	FTD は、スレッド名「DATAPATH-0-4948」でトレースバックおよびリロードする場合がある
CSCwc77892	起動後の ASA syslog の CGroups エラー
CSCwc78781	ACL 変更が PBR 設定にリンクされている間に ASA/FTD トレースバックとリロードが発生することがある
CSCwc79366	展開中に、デバイスが構成要求の処理中にスタックする
CSCwc80234	アクティブとスタンバイ間の「inspect snmp」設定が異なる
CSCwc81184	ASA/FTD が SNMP プロセス障害によりトレースバックおよびリロードする
CSCwc81945	インターフェイス NAT を備えた GCP クラスタで、データユニットのトラフィックが「LU allocate xlate failed」でドロップされる

不具合 ID	タイトル
CSCwc81960	アクセスリストでオブジェクトグループを使用すると、ルート マップで「match ip address」を設定できない
CSCwc82188	FMC UI または CLISH から長いコマンドを適用した場合、FTD がトレースバックおよびリロードする
CSCwc83346	ASA/FTD がスレッド名 IKE Daemon でトレースバックおよびリロードする
CSCwc88897	DNS インスペクションポリシー変更後の Cisco Umbrella のヌルポインタが原因で ASA がトレースバックおよびリロードする
CSCwc90091	ユーザー統計がある ASA 9.12(4)47 が、「policy-server xxxx global」の可視性に影響する
CSCwc93166	ユーザーコンテキストで write standby を使用すると、セカンダリファイアウォールのライセンスステータスが無効な状態のままになる
CSCwc94085	6.6.5 からのアップグレード後、FIPS が有効になっている DTLSv1.2 を確立できない
CSCwc94501	ctm_n5 リセットにより ASA/FTD のメモリリークとトレースバックが発生する
CSCwc94547	「debug menu fxos_parser 4」発行時に Lina がトレースバックおよびリロードする
CSCwc95290	vpn-context に ESP ルールがないため、IPSec トラフィックがドロップすることがある
CSCwc96805	スレッド unicorn の tcp インターセプト統計によりトレースバックおよびリロードする
CSCwc99242	リロード後に ISA3000 LACP チャネルメンバー SFP ポートが中断状態になる
CSCwd00386	「snp_clear_acl_log_flow_all」が原因で設定をクリアすると、ASA/FTD がトレースバックおよびリロードすることがある
CSCwd00778	SNMP ポーリングによる ifAdminStatus の出力が異常
CSCwd02864	logging/syslog は、SNMP トラップとログ履歴の影響を受ける
CSCwd03793	FTD トレースバックとリロード
CSCwd03810	アップグレード後に ASA カスタムログインページが webvpn 経由で機能しない

不具合 ID	タイトル
CSCwd04135	検出モード NAP でファイル検査を使用すると、Snort3 が 4MB 後にパケットを予期せずドロップする
CSCwd04436	別のレルムを変更して保存すると、ユーザー/グループのダウンロードが失敗することがある
CSCwd04494	Firepower 3110 の同じポートチャネルにオンボードインターフェイスと netmod インターフェイスを追加できない
CSCwd05756	syslog コンポーネントによる Lina の FTD トレースバック
CSCwd06005	ノード離脱中に ASA/FTD クラスタがトレースバックおよびリロードする
CSCwd07098	25G CU SFP が Brentwood 8x25G netmod で機能しない
CSCwd08098	FMC の cacert.pem が期限切れになり、すべてのデバイスが無効として表示される
CSCwd10822	ディスク障害が原因で他のユニットの検査エンジンに障害が発生したため、フェールオーバーがトリガーされる
CSCwd11303	ikev2 プロセスで ASA がトレースバックを生成し、リロードすることがある
CSCwd11855	ASA/FTD がスレッド名「ikev2_fo_event」でトレースバックおよびリロードすることがある
CSCwd14972	ASA/FTD がスレッド名 pix_flash_config_thread でトレースバックおよびリロードする
CSCwd16294	GTP インスペクションで、オプションの IE ヘッダー長が短すぎると、パケットがドロップされる
CSCwd16689	ASA/FTD がブロックデータの破損によりトレースバックする
CSCwd20627	ASA/FTD：NAT 設定の展開の失敗
CSCwd22349	ASA：「定期認証証明書」が有効になっている AnyConnect 証明書ベースの認証に接続できない
CSCwd22907	SNMP 通知スレッドでの ASA/FTD の高い CPU 使用率
CSCwd23913	プレフィックスリストを使用して BGP ネイバーを追加した後に、HA の FTD が複数回トレースバックする。
CSCwd25201	SNMP トラップサーバーが設定されていない場合に、ASA/FTD の SNMP トラップがキューに入れられる

不具合 ID	タイトル
CSCwd25256	ASA/FTD トランザクションコミットにより、ルールの不一致とトラフィック損失が発生する可能性がある
CSCwd26867	リブートがトリガーされたら、デバイスがアクティブ状態に移行しない必要がある
CSCwd28037	TPK：トラフィック中に nameif が発生しないとデバイスがトレースバックされ、Lina コアが生成される
CSCwd31181	Lina がトレースバックおよびリロードする：VPN 親チャネル（SAL）に無効な基盤となるチャネルがある
CSCwd31806	ASAv show crashinfo の出力が継続的にループする
CSCwd31960	カスタム NAT が設定されている場合、VPN 経由の管理アクセスが機能しない
CSCwd33811	DATA_NODE がクラスタに参加していないため、クラスタの登録に失敗する
CSCwd33962	3130 HA assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCwd34079	FTD：プロセス名 Lina でトレースバックおよびリロードする
CSCwd38583	ASA/FTD：コマンド「no snmp-server enable oid mempool」がデフォルトで有効になっているか、アップグレード時に強制される
CSCwd38805	Syslog 106016 がデフォルトでレート制限されていない
CSCwd40260	有用性の強化：ペイロードを解析できない場合、ASA/FTD によってサイレントにドロップされる
CSCwd41083	ASA が DNS インスペクションによりトレースバックおよびリロードする
CSCwd41553	PIM トンネルインターフェイスのダウン状態により、PIM レジスタパケットがランデブーポイント（RP）に送信されない
CSCwd43622	92.14.0 でネイティブ論理デバイスを削除した後、ブレードが 600 秒以上オンラインのままになる
CSCwd45451	FMC：FMC の IP/ホスト名が変更されたときに FTD のホスト名/IP を変更するスクリプト
CSCwd49402	FTDv クラスタの仮想 IP に ping を実行できない
CSCwd54360	FP2100：HA の FXOS 側の変更に、予期しない lacp プロセス終了の問題に対するレジリエンスがない

不具合 ID	タイトル
CSCwd66822	FDM FPR2k ネットワーク モジュール インターフェイスが、7.1.0 アップデート後にグレー表示される
CSCwd68745	QEMU KVM コンソールが [カーネルを起動中（Booting the kernel）] ページでスタックする
CSCwd73020	ブートアップ警告の修正：カウンタ ID 'TLS13_DOWNSTREAM_CLIENT_CERTIFICATE_VERIFY' が長すぎる
CSCwd79150	クラスタデバイスのデバイス API healthStatus がデバイスリストのヘルスステータスと一致しない
CSCwd85073	Snort3 ストリームコアで init_tcp_packet_analysis が検出される
CSCwd89095	リロード後に Stratix5950 および ISA3000 LACP チャネルメンバー SFP ポートが一時停止になる
CSCwd98070	ビルドアウト FMC 2700（FMC HA アクティブ）に新しいデバイスを登録できない
CSCwe04043	FTD-HA アップグレードが失敗する
CSCwe10872	PPPoE 設定の編集中に内部エラーが発生する
CSCwe12705	multimode-tmatch_df_hijack_walk トレースバックが、FO に接続したスイッチインターフェイスでのシャットダウン/シャットダウン解除中に観測される
CSCwe15924	MariaDB レプリケーションが良好な状態ではないのに回復されたため、FMC-HA 同期が 1 時間以上失われる
CSCwe21301	7.3.0 から 7.4.0 にアップグレード後、Azure FMC にアクセスできない
CSCwe25025	8x10Gb netmod がオンラインにならない
CSCwe25342	ASA/FTD：snmp-server が設定されていない場合の SNMP 関連のメモリリーク動作
CSCwe25412	Azure D5v2 FTDv がトラフィックを送信できない：アンダーランと DPDK バッファの枯渇が確認される
CSCwe28912	FPR 4115：FTD HA アップグレード後にプライマリユニットのすべての HA 設定が失われる
CSCwe30359	展開中に数分間トラフィックがドロップする
CSCwe33282	FTD：HTTPD プロセスが実行されていなかったため、アップグレードが失敗する

不具合 ID	タイトル
CSCwe34664	ユーザーが名前を変更すると、インターフェイスがインターフェイスグループから削除される（API）
CSCwe37941	v1_message* および abp* ファイルと SXP ブックマークが、デバイス登録の user_enforcement で消去されない
CSCwe38601	FMC 検索エラー：「データ検索サービスのロード中にエラーが発生しました。再度実行してください（Error Loading Data Search Service Please Try Again）」
CSCwe38640	syslog ファシリティが CONSOLE の場合の EventHandler 警告である
CSCwe41766	バンドルされている FXOS バージョンが新旧のバージョンで同じ場合、アップグレード後に FTD が期待どおりに再起動しないことがある
CSCwe42061	FTD インターフェイスで BVI を削除すると、他の BVI でパケットドロップが発生する
CSCwe42236	FMC：ドメインの作成がエラー「Index 'netmap_num' for table 'domain_control_info'」で失敗する
CSCwe44571	FMC：地理位置情報サイズが原因でアップグレードが失敗する
CSCwe45569	management-access が有効になっているために 7.0 から 7.2.x 以降への FTD アップグレードがクラッシュする
CSCwe48997	同じ IDP を持つ異なる SAML サーバーで 2 つの RA-VPN プロファイルを作成できない
CSCwe55308	MessageService のメモリリーク
CSCwe58635	準備状況チェックに失敗 [ERROR] 致命的なエラー：エンタープライズ オブジェクトの整合性チェックが 7 つのエラーで失敗しました
CSCwe58700	ASA/FTD：クラスタイベントメッセージ「正常性チェックで左側のクラスタを制御していることが検出されました（Health check detected that control left cluster）」の改訂
CSCwe59889	API を介した ID サービスエンジンの作成で「404 クライアントエラー：見つかりませんでした（404 Client Error: Not Found）」が返される
CSCwe63759	クラスタ強化の修正
CSCwe65492	KP がデコードできない無効なコアファイルを生成する 7.2.4-64
CSCwe65516	SSH を有効にした後、show xlate に内部インターフェイス（nlp_int_tap）の xlate エントリが表示されない

不具合 ID	タイトル
CSCwe67180	キャッシュファイルの破損が原因で、FTD HA アプリケーション同期に失敗する
CSCwe68840	FMC でのレート制限に関するsyslog ID の範囲（805,003 ～ 852,002）を追加
CSCwe69824	FMC GUI の検証チェックで問題が発生し、新しい NAT オブジェクトの追加時にエラーがスローされる
CSCwe70378	接続がスタンバイ FTD に複製されない
CSCwe71220	スレッド名：CP Processing で FTD がクラッシュする
CSCwe73933	プライバシーアルゴリズムの AES192 または AES256 を使用した場合、SNMPv3 ポーリングが失敗することがある
CSCwe75267	FTD HA ペアを強制的に解除できない
CSCwe78674	ユーザーグループのダウンロードが使用可能なデータよりも少ないデータを取得するか、「サイズ制限を超えました（Size limit exceeded）」というエラーで失敗する
CSCwe80273	[FMCデバイス検索（FMC Device Search）] ページでグループから FTD が削除され、グループ化されていない状態に戻される
CSCwe82704	マルチインスタンス HA でデータ/データ共有として設定された PortChannel サブインターフェイスが「待機」状態になる
CSCwe83255	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe84079	asa_snmp.log がローテーションされず、ファイルサイズが大きくなる
CSCwe84695	FMC/FTD ダイナミック VPN。ドロップダウンリストからデフォルトの事前共有キーを選択できます。
CSCwe85156	FTD：アップグレードしてダウン状態になると、10Gbps/Full インターフェイスが 1Gbps/Auto に変更される
CSCwe87134	Lina コアが高トラフィックのテスト中に作成される
CSCwe88802	FTD の準備とアップグレードが ProgressReport として例外ログで渡され、属性「KB_UNIT」がない
CSCwe90168	証明書認証の使用時に FMC GUI にアクセスできない
CSCwe92723	ポリシーの展開中に 7.0.1 でフェーズ 2 NAP の遅延が確認される

不具合 ID	タイトル
CSCwe93137	KP：マルチモード：HA ノードの切断と再参加中に ASA トレースバックが確認される
CSCwe97277	VPN トラフィックの実行中にヒットレスアップグレードを実行すると、ASA のトレースバックとリロードが観察される
CSCwe98435	ID ポリシー（キャプティブポータル）および SSL ポリシー（dp-tcp-proxy）CLI を使用した選択的ポリシー展開
CSCwf00804	EventHandler の偶発的なバンドルレコードの破損：SFDataCorrelator で「逆シリアル化のエラー（Error deserializing）」がログに記録される
CSCwf05295	FP1000 シリーズで実行されている FTD が、「Client Hello」メッセージの後の TLS フローのパケットをドロップすることがある。
CSCwf08790	デバイスに空き領域がないため、 FMC でのリモートバックアップの復元が失敗する
CSCwf13674	展開によって、特定の RAVPN ユーザーマッピングが削除される可能性がある
CSCwf14031	アプリケーションディテクタが無効になっているため、Lua ファイルが見つからずに Snort がダウンする（VDBM 側）
CSCwf14411	トラフィックで誤った宛先ゾーンを取得すると、トラフィックが誤った AC ルールに一致する
CSCwf15863	非常に限定的な「vpn-idle-timeout」値により、SSL セッションの切断と再接続が継続的に発生する。
CSCwf16559	[センサーリストのアップグレード（Upgrade Sensor List）]ページを表示中に getReadinessStatusTaskList pjb 要求が頻繁に発生する
CSCwf16679	HA 有用性強化：現在のアプリケーション同期の HA NLP クライアント統計と HA CTL NLP カウンタを維持
CSCwf17042	ASDM が、バックアップ復元時にクラス インスペクション オプションでカスタムの policy-map をデフォルトマップに置き換える。
CSCwf19621	侵入ポリシーの名前またはインスペクションモードを編集できない
CSCwf21204	ユーザーが設定バックアップのみを収集している場合、MonetDB に対して DBCheck を実行できない
CSCwf22045	MySQL、または TCP の高トラフィックが Snort3 によってブロックされ、ドロップ理由として snort-block が表示される

不具合 ID	タイトル
CSCwf22637	ネットワーク オブジェクト グループのオーバーライドが表示されない、または FMC GUI から編集できない
CSCwf24818	LOM アクセスがあった場合、FMC の移行後に管理者ユーザーのパスワードを変更できない
CSCwf25402	FMC：CSV ファイルからの SSL 証明書ピンニングのインポートにより、FTD でのポリシーの展開に失敗することがある
CSCwf25563	新しい AC ポリシーの作成中にデバイスリストのロードに時間がかかる
CSCwf25642	大規模な MariaDB Undo ログに起因する高いディスク使用率とパフォーマンスの問題
CSCwf26350	ポリシーのインポートが失敗した場合、従属する IPS がユーザーに通知されない
CSCwf27337	KP：FTD の再インストール時に 2 番目の（MSP）ディスクがクリーンアップ/再フォーマットされる
CSCwf31050	[IMS_7_5_MAIN] 複数のアプライアンスの CPU 使用率が高い
CSCwf35573	TLS サーバーのアイデンティティプローブのタイムアウトが長すぎると、トラフィックが影響を受ける可能性がある
CSCwf36563	FTD のアップグレード後にインターフェイス設定が欠落している
CSCwf36621	access-list：異なるタイプのアクセスリストを混在させることができない。
CSCwf39163	ASAv：snmpwalk 実行中の ICMP ping パケットにより Azure 環境で高遅延が発生する
CSCwf39821	FTD：ピアでのエラー ngfwManager restart により、CD App Sync エラーで高可用性ユニットがヒットする
CSCwf41187	WINSCP および SFTP ディテクタが期待どおりに機能しない
CSCwf41433	SSH 認証の TACACS+ 要求に ASA/FTD クライアント IP がない
CSCwf42012	FPR 3100/4200 の ERSPAN インターフェイスでのトラフィックの不適切なロードバランシング
CSCwf42097	バンドルされている FXOS アップグレードで PSEQ（Power-Sequencer）ファームウェアをアップグレードできない場合がある
CSCwf42234	アップグレード後に S2S ダッシュボードの SVTI トンネルの詳細が表示されない

不具合 ID	タイトル
CSCwf43537	FTD クラスタのアップグレード中にスレッド名 cli_xml_request_process で Lina がクラッシュする
CSCwf43850	Firepower での ipsec セッションの ECMP + NAT のサポートの要求
CSCwf44537	nat_remove_policy_from_np で 99.20.1.16 lina がクラッシュする
CSCwf45091	SMTPS ホストで証明書が交換される場合、Snort3 で SMTP_RESPONSE_OVERFLOW（IPS ルール 124:3）が一致する
CSCwf47227	priority-queue コマンドにより、すべてのポートチャネルインターフェイスでサイレント出力パケットがドロップされる
CSCwf49486	store_*list_history.pl タスクが終了することなく 5 分ごとに作成され、FMC の速度が低下する
CSCwf50497	DNS キャッシュエントリの枯渇によりトレースバックが発生する
CSCwf52810	ASA SNMP ポーリングが機能せず、show コマンドで「Unable to honour this request now」と表示される
CSCwf54510	スレッド名 DHCPRA Monitor での ASA トレースバックおよびリロード
CSCwf55236	すべての IP ポリシーから除外されている場合でも、カスタムルールグループを削除できない
CSCwf56386	vFTD がメモリ不足になり、障害状態になる
CSCwf56811	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード
CSCwf59643	FTD：スタンバイユニットでの fover インターフェイスフラップにより HA アプリケーション同期が失敗する
CSCwf60590	トランスペアレントモードの FTD で「show route all summary」を実行すると、CLISH の動作が遅くなる。
CSCwf62820	フェールオーバー：アクセスリスト変更中のスタンバイユニットのトレースバックとリロード
CSCwf63358	FTD Diskmanager.log が破損し、hm_du モジュールから高いディスク使用率の誤ったアラートが表示される
CSCwf63872	フェールオーバー スイッチオーバー後に FTD が OSPF 隣接関係を形成するのに想定以上に時間がかかる
CSCwf64590	HB ミスが原因でユニットがクラスタからランダムにキックアウトされる | ASA 9.16.3.220

不具合 ID	タイトル
CSCwf68335	vFMC：スケジュールされた展開が失敗する
CSCwf69313	接続トラッカーの相関イベントの（<、<=、=、または !=）ルールに、無関係な接続のデータが表示される
CSCwf69880	FP3110 7.2.4：Firepower 3110 デバイスの予期しない再起動
CSCwf69901	FTD：OSPF 再配布プロセス実行中のトレースバックとリロード
CSCwf71602	ダウンまたはアイドル時に FMC から FTD S2S VPN アラートが生成されない
CSCwf72434	最大数に関するシステム制限ルールに達したときに意味のあるログを追加
CSCwf73773	最後の 20 の rmu 要求応答パケットのダンプに失敗する
CSCwf75214	リロード後にキー文字列がバックスラッシュ「\」で終わる場合、ASA は IKEv2 リモート PSK を削除する
CSCwf75695	複数のクラスタイベントが同時に発生すると、重複する FTD クラスタが作成される
CSCwf76945	アップグレード後もパケットデータがドロップされる
CSCwf77994	diskmanager/Pruner を実行している FTD デバイスシステムコアに関する誤った重大な高 CPU アラートが表示される
CSCwf78321	ASA：クライアントレス WebVPN によるチェックヒープのトレースバックとリロード
CSCwf79372	HA ブレーク後、1 つのデバイスがアップグレード用に選択されている場合、選択されたリストに両方のデバイスが表示される
CSCwf80163	Critical Alert Smart Agent が Smart Licensing Cloud に登録されていない
CSCwf80183	トラフィックフロー中に navl で Snort3 コアが表示される
CSCwf82279	/opt/cisco/platform/logs/messages への ssp-multi-instance-mode メッセージの過剰なロギング
CSCwf82447	アイデンティティ NAT ルールを編集すると、「ルートルックアップの実行」がサイレントに無効になる
CSCwf82742	FTD：管理インターフェイスで SNMP が機能しない
CSCwf82970	TLS サーバー ID 検出機能を有効にした後、Snort2 エンジンがクラッシュする
CSCwf84200	IP フロー統計の実行中の Snort コア

不具合 ID	タイトル
CSCwf86519	ピアの 1 つがエクストラネットの場合、ステータスがアップであっても、FMC で VPN ステータスが不明と表示される
CSCwf86557	復号エンジン/SSL 接続がハングし、PKI インターフェイスエラーが表示される
CSCwf87070	WM RM：SFP ポート 9 のステータスが SFP 10|11|12 のポートの状態の後に表示される
CSCwf88030	FMC が論理デバイスの管理インターフェイスで「shutdown」コマンドをプッシュする
CSCwf88124	トランクモードのスイッチポートが、電力損失後に VLAN トラフィックを通過させない
CSCwf89959	ASA：ISA3000 が entPhySensorValue OID SNMP ポーリングに応答しない
CSCwf91282	含まれているローカル/カスタムルールに空白のルールメッセージフィールドがあるため、.SFO の FMC へのインポートに失敗する
CSCwf92135	ASA：スレッド名「fover_FSM_thread」および「ha_ntfy_prog_process_timer」でのトレースバックとリロード
CSCwf92646	EC521 の SHA384 を使用した ECDSA 自己署名証明書
CSCwf92661	ASA|FTD：空きバッファの破損によるトレースバックとリロード
CSCwf92726	Vault トークンが破損している場合、アップグレード後に LDAP のファイルが見つからない
CSCwf94194	FMC：同じインターフェイスを同じ ECMP ゾーンに追加できない
CSCwf94450	FTD Lina トレースバックスレッド名：二重解放による DATAPATH-3-11917
CSCwf94677	両方の HA ユニットが同時にリロードされた後、「failover standby config-lock」設定が失われる
CSCwf95147	OSPFv3 トラフィックがトランスペアレントモードで一元化される
CSCwf96938	FMC：UDP ポート 6081 を使用した ACP ルールが後続の展開後に削除される
CSCwh01673	Snort3 URL DB ファイルで FTD/ngfw ディスク容量がいっぱいになる
CSCwh02457	AWS 上の ASAv を 9.18.2 以降の任意のバージョンにアップグレードした後、Radius 認証が機能しない
CSCwh02561	ポリシー展開後にポートチャネル インターフェイスの速度が 10G から 1G に変更される

不具合 ID	タイトル
CSCwh04365	メモリヘッダー検証によるプロセス名 lina での ASA トレースバックとリロード- webvpn 側の修正
CSCwh04395	マルチコンテキスト セットアップで ASDM アプリケーションがランダムに終了または中断し、アラートメッセージが表示される
CSCwh04730	メモリバッファが破損している場合に ASA/FTD HA checkheaps がクラッシュする
CSCwh05863	デフォルト以外のポートが 80 で始まる場合、ASA で OCSP 要求の HTTP ヘッダーのホストフィールドのポートが省略される
CSCwh06452	OID.1.3.6.1.2.1.2.2 を使用した SNMP 応答のインターフェイス速度の不一致
CSCwh08481	FreeB および VPN 機能を使用した Lina プロセスでの ASA トレースバック
CSCwh08683	FTDv/AWS：Lina と FTD クラスタ間の NTP クロックオフセット
CSCwh09968	ASA/FTD：NAT の変更と使用中の DVTI によるトレースバックとリロード
CSCwh10087	コアファイル名に空白が含まれているため、core-compressor が失敗する
CSCwh11411	展開中に Snort でトラフィックがブラックリストに登録される
CSCwh11764	ASA/FTD が、スレッド名「RAND_DRBG_bytes」および n5 プラットフォーム上の CTM 機能でトレースバックおよびリロードすることがある
CSCwh13625	暗号化された可視性エンジン（EVE）FMC ダッシュボードタブとウィジェットの名前が 7.1 から 7.2 以降へのアップグレード後に変更されない
CSCwh13821	キャプチャバッファサイズを変更すると、ASA/FTD がトレースバックおよびリロードすることがある
CSCwh14467	AnyConnect/Secure Client イメージのファイルサイズが 100MB を超えると、FMC にアップロードできない
CSCwh14863	FTD 7.0.4 クラスタで、tcp-not-syn が原因で Oracle の sqlnet パケットがドロップされる
CSCwh15109	SRU のインストールが 602_log_package.pl スクリプトでスタックし、展開が失敗する
CSCwh15223	DAQ/Snort で不正な形式の L3 ヘッダーが送信されると、snp_fp_tcp_normalizer() で Lina がクラッシュする
CSCwh16301	クラスタ全体の出力において ASA クラスタのみのヒットカウント統計が正しくない

不具合 ID	タイトル
CSCwh18967	FXOS FPRM のトラブルシューティングに「show env tech」を含める
CSCwh19475	フローが断続的に不明な app-id トラフィックの Snort によってホワイトリストに登録される
CSCwh19897	ASA/FTD クラスタ：同じ 5 タプルを使用した 2 つの異なる接続での TCP ランダム化シーケンス番号の再利用
CSCwh21141	FMC プレビュー展開に誤った情報が表示される
CSCwh21360	741：HA および AppAgent：瞬間的なスプリットブレイン状況を回避するための長期的なソリューション
CSCwh21420	MIO ブレードのハートビート障害による ASA の予期しない HA フェールオーバー
CSCwh21474	access-list の再設定時の ASA トレースバック
CSCwh22348	テーブルの破損「rua_event_xxxxx」が原因で sfdatacorrelator がクラッシュする
CSCwh23567	リロード時にスタンバイで PAC キーファイルが欠落している
CSCwh24826	FMC のアップグレードが 1039_fmc_rabbitmq_enable でスタックする
CSCwh24901	FMC から削除されるイベント（未処理イベントではない）の頻繁なドレイン
CSCwh25351	FTD VMware：ファイルシステムの破損が原因で /dev/sda8 パーティションでディスク使用率が高くなる
CSCwh25928	FMC ユーザーロールに権限がないため、7.2.4 へのアップグレード後に Tomcat が継続的に再起動することがある
CSCwh26526	大規模なクエリに関連する SQL パケットが、理由 snort-block で Snort3 によってドロップされる
CSCwh27230	インターフェイスがインラインモードの場合、アイドルタイムアウト後に接続がクリアされない。
CSCwh28007	AC ポリシールールの編集中に、ルールの順序番号の位置がずれる
CSCwh28144	特定の OID 1.3.6.1.2.1.25 が応答しない
CSCwh28185	データベースクエリがブロックされると、dl_task.pl タスクが 1 時間ごとに作成され続ける
CSCwh28206	IP と SGT のマッピングによるフェールオーバー後、ファイアウォールでパケットがブロックされる

不具合 ID	タイトル
CSCwh28218	プレフィルタルール名が変更されたときに Syslog が更新されない
CSCwh29092	スクリプト 800_post/100_ftd_onbox_data_import.sh の実行時に FTD（FDM）が失敗する
CSCwh30111	FTD：アップグレードによって永続的な VPN トンネルのヘルスモニターアラームがトリガーされる
CSCwh30891	SNMPV3 設定の追加時に ASA/FTD がスレッド名「ssh」でトレースバックおよびリロードすることがある
CSCwh31495	FTD：CPU コアによって NAT ルールが削除されたことによるトレースバックとリロード
CSCwh32118	HTTP セッションが CLOSE_WAIT でスタックしているため、ASDM 管理セッションのクォータに達している
CSCwh34344	「ファイアウォールセッションの削除」後に FTD で接続終了イベントが生成されない
CSCwh36167	DAP：FMC で Lua スクリプトに &#13 文字が追加される
CSCwh37475	FlexConfig ロールバック中の msie-proxy コマンドの削除
CSCwh37733	FTD が MAC アドレス 0000.000.000 で UDP500 パケットに応答する
CSCwb37737	FMC7.2.x EIGRP flexconfig 移行がインターフェイス設定の不一致による内部エラーで失敗する
CSCwh38492	MySQL の復元が完了後、FMC の復元が Vault クリアステージでスタックする
CSCwh38708	ASA の「pager line 25」コマンドが一部の端末アプリケーションで期待どおりに機能しない
CSCwh40106	プレフィルタアクションが分析の場合、KP でホストされている FTD で復号された ESP パケットが誤ってドロップされる
CSCwh41127	ASA/FTD：スタンドアロン ASA の「overlaps with inside standby interface address」NAT64 エラー
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* が diskmanager に含まれていない
CSCwh42412	FTD：インラインセットインターフェイスの内部フロー処理によってフラグメント化された GRE トラフィックが原因で、9344 ブロックでリークが発生する
CSCwh44479	設定アーカイブの作成に失敗し、展開プレビューでエラーがスローされる

不具合 ID	タイトル
CSCwh45450	2100：ポートチャネルのメンバーとしてインターフェイスを削除後、FTD にインターフェイスが表示されない
CSCwh47395	拡張アクセスリストオブジェクトで IP 範囲の設定が許可されない
CSCwh47701	ASA で、物理データおよび管理専用インターフェイスに対して同じ BGP ダイナミック ルーティング プロセスが許可される
CSCwh48844	FTD：Mate version 0.0 is not compatible でフェールオーバー/ハイアベイラビリティが無効になる
CSCwh49244	「show aaa-server」コマンドで、常に平均ラウンドトリップ時間 0 ミリ秒が表示される
CSCwh49483	show inventory all の実行中に ASA/FTD がトレースバックおよびリロードすることがある
CSCwh52420	AMP クラウドルックアップが頻繁にタイムアウトする
CSCwh52526	ユーザーセッションが 1 時間以上アクティブな場合の FMC SSO タイムアウト（アイドルタイムアウト）
CSCwh53116	イベントビューアのカスタムビューにイニシエータの国と大陸が表示されない
CSCwh53143	ASA：IPSec トンネルを介した管理アクセスが機能しない
CSCwh54228	FMC：query_engine.log が予想よりも急速に増加し、ディスク使用率が高くなる
CSCwh54477	FMC に 11xx/21xx/31xx デバイスの「パスワード暗号化キーが設定されていません（The password encryption key has not been set）」というアラートが表示される
CSCwh56218	ASA：CCL リンク障害/回復後の 6 ノードクラスタ同期中のトレースバックとリロード
CSCwh56945	RNA_DB_InsertServiceInfo で SFDataCorrelator が繰り返しクラッシュする
CSCwh58999	クラシックライセンスを持つデバイスを、バージョン 7.2.X を実行している FMC に登録できない
CSCwh59199	IPSec VPN を使用した ASA/FTD のトレースバックとリロード（場合によってはアップグレードを含む）
CSCwh59222	SNORT3：FTD： TSID 高 CPU、SSL が有効な場合、DAQ ポーリングで十分なパケットがプルされない

不具合 ID	タイトル
CSCwh59557	インターフェイスの過負荷が原因で、送信元 NAT ルールで誤った変換が実行される
CSCwh60604	DAP データを処理中に ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwh60608	VPN ロードバランシングクラスタの IP アドレス/ホスト名がパブリックインターフェイスと同じサブネット上にない
CSCwh60631	MPLS トンネルの再アセンブルでフラグメント化された UDP パケットが失敗する
CSCwh61690	ボックストラフィックを介したマルチキャストにより、1GBps トラフィックで CPU 使用率が高くなる
CSCwh62080	ブロックと SSL キャッシュの FTD トラブルシューティングに必要な追加のコマンド出力
CSCwh62473	FMC HA：スタンバイ FMC にログインすると、スタックトレースが常に存在する
CSCwh63588	ホストグループ設定を追加後、FTD SNMPv3 ホスト設定が iptables から削除される
CSCwh63663	レルム AD プライマリドメイン設定で .k12 ドメインを使用できない
CSCwh64508	Web UI の処理中に FTDv 変数が取得されないときに発生する回帰の修正
CSCwh66359	CLI でロギングタイムスタンプを有効にした後に、ASDM がログのタイムスタンプを認識できない
CSCwh66636	「match ip address test」を設定および設定解除すると、クラッシュすることがある
CSCwh66991	アップグレード中に SSHD が再起動すると、/new-root がデフォルトのルートパーティションになる
CSCwh68856	TLS1.3 を無効にする設定
CSCwh68878	Diskmanager プロセスが予期せず終了する
CSCwh69209	プレフィルタで FMC のトンネルルールにトンネルエンドポイントを追加できない
CSCwh69346	ASA：CLI を使用して設定を復元する際のトレースバックとリロード
CSCwh69815	アップグレード後に FTDv スループットが 100Kbps に変更される

不具合 ID	タイトル
CSCwh70323	syslog サーバーに送信される一部の syslog メッセージのタイムスタンプエントリが欠落している
CSCwh70481	ルータから送信されたコミュニティストリングが ASA と一致しない
CSCwh70628	kp 741-1146 でスピンロックとウォッチドッグがクラッシュする：ctm_ipsec_get_sa_lock+112
CSCwh70905	セカンダリが IPv6 を使用して内部でフェールオーバー通信を失ったが、内部の次のテストに合格する
CSCwh71050	FXOS：NTP エントリの重複により、エラーメッセージが表示される：到達不能または無効な NTP サーバー
CSCwh71358	Firepower 3105 デバイスで FDM を介して VRF を作成できない
CSCwh73727	Snort3 で IP プロトコル 51 がドロップされる
CSCwh74870	DAQ 未処理カウンタの予期しない高い値
CSCwh76959	アクセスリストに加えられた変更が FMC で保存されない
CSCwh77348	ASA：クラスタ設定で「show nat pool detail」コマンドを実行すると、トレースバックとリロードが発生する
CSCwh77527	リモートストレージの設定中に、サポートの有無を FMC がユーザーに報告する必要がある
CSCwh83328	SNMP が FMC からの正確なホスト名のポーリングに失敗する
CSCwh84833	すでに無効になっている場合に、すべての HA 同期で URL フィルタリングの無効化が試行される
CSCwh85824	eStreamer JSON 解析エラーとメモリリーク
CSCwh89289	実行ごとに timerange と nap conf の内容が異なるため、展開中に Snort がリロードされる
CSCwh90693	登録が成功した直後に、FTD でスタンバイ FMC が登録解除される
CSCwh90813	期限切れの証明書に起因する FDM アップグレードの失敗
CSCwh93649	ciscossh スタックを使用した SCP 経由のファイルコピーが「該当するファイルまたはディレクトリがありません（no such file or directory）」というエラーで失敗する
CSCwh95175	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある

不具合 ID	タイトル
CSCwh98733	CPOC：CPS テストで 4245 ASA がクラッシュする
CSCwi03528	クロス IFC アクセス：PING を以前の非クロス IFC 動作に戻す
CSCwi06007	FMC で syslog ポート設定の検証が欠落している
CSCwi14896	ルールのプロファイリングの有効化または無効化中にノードがクラスタからキックアウトされる
CSCwi24880	「ip verify reverse-path」が設定されている場合、ASA が IPSEC トラフィックを誤ってドロップする
CSCwi31091	プレフィックスリストを使用した OSPF 再配布ルートマップがアップグレード後に機能しない

バージョン 7.4.0 で解決済みのバグ

表の最終更新日：2023 年 9 月 7 日

表 *29*：バージョン *7.4.0* で解決済みのバグ

不具合 ID	タイトル
CSCvq20057	Cisco Secure Firewall（Firepower）バックアップのログ記録を改善し、リモートストレージを使用するときに gzip を再試行する
CSCvq25866	$SYS_FW_ENABLED_INSPECT_PROTOCOL_LIST の Flex 構成プレビューでエラーがスローされる
CSCvt25221	QoS ポリシー展開時のスレッド名 cli_xml_server での FTD トレースバック
CSCvu24703	FTD - フローオフロードはレート制限機能（QoS）と共存できる必要がある
CSCvu28887	ネットワークオブジェクトのフィルタリングが機能せず、「データのロードエラー（Error Loading Data）」が発生する
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
CSCvx04003	CP への ARP スロットリング欠如のミス表示により、オーバーサブスクリプションになる
CSCvx52042	6.6.1 へのアップグレードが 800_post/1025_vrf_policy_upgrade.pl で失敗する
CSCvx68173	いくつかの snort インスタンスが 100% でスタックすることが観察された

不具合 ID	タイトル
CSCvx71936	FXOS：障害「パスワード暗号化キーが設定されていません（The password encryption key has not been set.）」が FPR1000 および FPR2100 デバイスで表示された
CSCvx75441	ファイルリストのプレビュー：類似した内容がほとんどない 2 つのリストを削除すると、FMC-UI でスタックトレースがスローされる
CSCvy11606	データのロード中にエラーが発生しました。STDACE BB の一部を解決できませんでした
CSCvy26676	「警告：更新が失敗したか、進行中です（Warning:Update failed/in-progress）」。正常に更新された後の外観
CSCvy95809	snort2 を実行している SFR で Crashinfo スクリプトが呼び出され、デバイスが 7.0 へのアップグレードに失敗する
CSCvz07004	SNORT2：SSL ルールに DND アクションがある場合でも、FTD はフルプロキシを実行している
CSCvz08312	ENH：CAC 認証ユーザーの削除と手動による変更の再設定は行われません。
CSCvz42065	IPS ポリシーは、アクセスコントロールポリシーで参照されている場合にインポートする必要がある
CSCwa04262	Cisco ASA ソフトウェアの SSL VPN クライアント側リクエストの、「/」URI を介したスマグリングの脆弱性
CSCwa22766	FMC4500/4600 に仮想ライセンスが表示される
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）
CSCwa72481	複数のインターフェイスを持つ FMC の API キーが破損した
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
CSCwa93215	DNS ルックアップでプライマリで HA フェールオーバーを実行すると、プライマリノードが VPN クラスタから切断される
CSCwb02955	オブジェクトが破損している場合に FMC アップグレードが失敗しないように /800_post/1027_ldap_external_auth_fix.pl を変更する
CSCwb08189	Microsoft 更新トラフィックが Snort バージョン 3 マルウェアインスペクションでブロックされる
CSCwb20926	FDM：未使用の IKEv1 ポリシーが原因でアップグレード後のポリシー展開が失敗する

不具合 ID	タイトル
CSCwb44848	ASA/FTD がプロセス名 lina でトレースバックおよびリロードする
CSCwb51821	ngfw ディレクトリの下にある大きなバックアップ統合ファイルによる Firepower Azure デバイスのディスク使用エラーである
CSCwb67464	ブートストラップが完了していないときにデバイスが再起動すると、FDM ブートストラップがスキップされる可能性がある
CSCwb84677	FMC バックアップは、monetdb バックアップの失敗が原因でリターンコード 102 で失敗することがある
CSCwb92583	大量のモニター対象外のディスク領域を使用してアップグレードすると、アップグレードが失敗し、デバイスがハングすることがある
CSCwb94431	発信インターフェイスリストが Null の場合、その他のドロップではなく MFIB RPF 失敗カウンタが増加する
CSCwb95453	ASA：管理コンテキストによって生成されるすべてのログのタイムスタンプが同じである
CSCwc03332	FP2100 の FTD が、リブートプロセス中に HA アクティブユニットとして引き継ぐことができる
CSCwc13477	FMC | インターフェイスの更新に失敗しました。送信元インターフェイスが見つかりませんでした
CSCwc23844	空きメモリが 30% を超えているにもかかわらず、ASAv の CPU およびスタックメモリの割り当てエラーが高い
CSCwc28660	Snort3：FTD 経由のトラフィックで NFSv3 マウントが失敗することがある
CSCwc30573	ライトテーマで設定されたアップグレードテストの実行中に、[展開/タスク（Deployment/Tasks）] ボタンが FMC_UI に表示されない
CSCwc32245	FMC：NAT ルールの指数関数的な拡張を防ぐための検証チェックである
CSCwc44608	IPS の選択的な展開により、FTD 構成ファイルが正しく書き込まれないため、障害が発生する可能性がある
CSCwc45298	FMC にイベントを送信するようにルールが設定されていない場合でも、FMC で接続イベントが表示される
CSCwc49655	FTPS が ssl3_get_record を取得：KK および DR ルール接続中の不正なレコードの種類
CSCwc49936	FMC 7.2.0|7.3.0 [統合（Integration）] > [ID ソース（Identity Sources）] ページがロードされず、回転し続ける

不具合 ID	タイトル
CSCwc50519	hm_du.pm からの過度のロギングは、syslog-ng プロセスの再起動につながる可能性がある
CSCwc51588	SMB/SSH を介した FMC バックアップ/復元の生成に失敗する
CSCwc52357	Estreamer ページが ASDM でロードに失敗する
CSCwc59953	Snort3 が TLS 1.3 でクラッシュする
CSCwc61828	複数のクラッシュハンドラの問題を修正
CSCwc62215	Snort 検証に失敗したため FTD が HA を同期できない
CSCwc64923	ASA/FTD がスレッド名「lina」IP ルーティング「ndbshr」でトレースバックおよびリロードすることがある
CSCwc65814	sybase 関連のモジュールが削除されてしまう
CSCwc65907	snort3 がクラッシュハンドラでハングするため、snort クラッシュ中に停止時間が長くなる可能性がある
CSCwc67687	ASA HA フェールオーバーによって HTTP サーバーの再起動の失敗と ASDM の停止がトリガーされる
CSCwc74099	アプライアンスの再起動/リロード後に FPR2140 ASA クロックタイムゾーンが UTC に戻る
CSCwc74271	SSO が無効になっている場合、Auth-Daemon プロセスが継続的に再起動される
CSCwc74841	FeedBurner がアクティブでなくなったため、FMC RSS フィードが壊れた - 「フィードを解析できない」
CSCwc75082	25G-SR の場合、FC-FEC ではなく RS-FEC（IEEE CL108）をデフォルトにする必要がある
CSCwc76849	完全なシャーシの再起動を実行すると、リンク状態の伝達が機能しなくなる
CSCwc77519	FPR1000 ASA/FTD：リロード後にプライマリがアクティブロールになる
CSCwc78296	アップグレード中に、データベースのシャットダウンや起動が正しく行われないことがある
CSCwc78689	AD 参加パスワードが空でない限り、レルム設定を保存できない
CSCwc79520	Snort プロセスは ssl_debug_log_config でトレースバックし、コアファイルを生成する可能性がある

不具合 ID	タイトル
CSCwc81219	snort3 を使用すると、侵入イベントが FMC に断続的に表示されなくなる
CSCwc82205	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwc83037	CCM レイヤ（シーケンス 36）での WR6、WR8、LTS18、および LTS21 コミット ID の更新
CSCwc87963	ASAv 「ライセンス情報を取得できません。後でもう一度お試しください（Unable to retrieve license info. Please try again later）」
CSCwc89661	「NPU との通信が失われました（Communication with NPU lost）」エラーの調査に必要な診断データが FTD で見つからない
CSCwc89924	内部データ「no buffer」インターフェイスカウンタをポーリングするための FXOS ASA/FTD の SNMP OID
CSCwc93964	ASA が、メモリトラッキング中に Unicorn スレッドで WebVPN トレースバックを使用する
CSCwc96016	クロスドメインでのキャプティブポータルのサポートである
CSCwc96780	FMC モジュール固有の正常性除外はすべての正常性チェックを無効にする
CSCwd00583	SNMP の「コミュニティ文字列の確認」の文字列が FMC のアップグレード後に自動入力されない
CSCwd04210	ASA：ASDM セッションが CLOSE_WAIT でスタックし、その結果 MGMT が不足する
CSCwd05814	PDTS バッファがいっぱいになると、Daq からの PDTS 書き込みが失敗することがあり、最終的にブロックが枯渇する
CSCwd07059	FTD を 7.2.0 から 7.2.0.1 にアップグレードした後、複数の snort3 がクラッシュする
CSCwd07278	TCM がオフのとき、ユニットがクラスタに参加するときの ASA/FTD tmatch コンパイルチェック
CSCwd09870	外部ブラウザとラウンドロビン DNS を使用した AnyConnect SAML が断続的に失敗する
CSCwd09967	スタックトレースで展開が失敗する：無効なタイプである（LocalIdentitySource）
CSCwd10497	センサーバックアップの復元の実行後に ngfw.rules ファイルに FTD センサールールがない

不具合 ID	タイトル
CSCwd10880	2100/3100 デバイスでの重要な正常性アラート「ユーザー設定（FSM.sam.dme.AaaUserEpUpdateUserEp）」である
CSCwd11005	fqdns_old.conf ファイルが見つからないため、FTD HA アプリケーションの同期が失敗する
CSCwd13083	FMC - 脅威のライセンス検証が正しくないため、展開を開始できない
CSCwd13917	FMC のファイルイベントからのダウンロード中、FMC で CPU 使用率が高く、20 分間後にダウンロードが失敗する
CSCwd14688	Syslog ファイルが急速に生成/削除されるため、FTD アップグレードが失敗する
CSCwd14732	管理 IP の変更後に FTD をポート 8305 にバインドできない
CSCwd15197	ASA/FTD：2 つ以上のインターフェイスで PAT ルールでラウンドロビンを使用すると、IP スティッキ性が失われる
CSCwd16017	NAT ルールに関連付けられている場合、オブジェクト編集は遅い
CSCwd16517	GTP ドロップが、バッファと syslog に常に記録されない
CSCwd16902	ファイルイベントは、不明の処理が正しいファイルに対してアクションを「マルウェアブロック」として表示する
CSCwd16906	ASA/FTD がポリシー展開後にスレッド名「lina」でトレースバックし、リロードすることがある
CSCwd17940	NDClient からの誤解を招くステータス更新が原因で、HA はフェールオーバーしなかった
CSCwd18744	「他のユニットの hwidb インデックスのセットが異なります（Other unit has different set of hwidb index）」という理由により、FPR1K FTD が HA の形成に失敗する
CSCwd19053	ASA/FTD が、配布リストを使用して多数のネットワークオブジェクトの展開をトレースバックすることがある
CSCwd20900	HTTP ブロック応答ページとインタラクティブブロック応答ページが Snort3 によって表示されない
CSCwd22413	EIGRPv6 - LINA で「mem_lock：アサーション mem_refcount' が失敗しました（mem_lock: Assertion mem_refcount' failed）」でクラッシュした
CSCwd23188	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある

不具合 ID	タイトル
CSCwd27186	FTD 設定に access-group コマンドがないため、すべてのトラフィックがブロックされる
CSCwd28236	アクティブ IP とスタンバイ IP の両方を使用しているスタンバイユニットが、nat「any」により重複 IP の問題の原因となる
CSCwd29835	ログローテーションでファイルの循環に失敗し、ファイルサイズが大きくなる
CSCwd30298	FTD：FTPS データチャネル接続が FTD によって送信された TLS サーバー ID および検出プローブの影響を受ける
CSCwd30774	FMC HA - 同期タスクが失敗すると、tmp/Sync 内のファイルがセカンダリに残される
CSCwd32892	FMC スマートカード認証の 7.2.1 へのアップグレード後に cac.conf が失われた
CSCwd33054	DHCP リレーが DHCP オファーパケットをループバックしているため、FTD/ASA で dhcprelay が失敗する
CSCwd33479	重複 SMB セッション ID パケットが snort3 クラッシュを引き起こしている
CSCwd34662	CCM レイヤ（シーケンス 39）での LTS18 および LTS21 コミット ID の更新
CSCwd35726	Cisco FXOS ソフトウェアにおける任意ファイルの書き込みの脆弱性
CSCwd36246	展開履歴ページでのジョブのフィルタリングは、上位 50 件のジョブにのみ基準を適用する
CSCwd37135	ASA/FTD がスレッド名 fover_fail_check でトレースバックおよびリロードする
CSCwd38196	Definitive DND ルールが一致している場合でもプロキシが使用される
CSCwd38526	FMC は、復号化ポリシーを使用したテストモードでの NAP の展開を許可できる
CSCwd39506	SSL ポリシー DND のデフォルトルールがサポートされていない暗号スイートでエラーになり、SKE エラーが表示される
CSCwd40141	Snort2 ローカル侵入ルールの Firepower Management Center GUI ビューがない
CSCwd40955	SSL ポリシーの大きなネットワークオブジェクトが原因で、ポリシー展開中の検証時間が非常に長くなる

不具合 ID	タイトル
CSCwd41224	FMC HA WebUI で FTDv 変数階層に割り当てられた FTDv が取得されない：変数
CSCwd41466	信頼できるドメインを持つフォレストからユーザーを再ダウンロードすると、未解決になるまたは同期が取れなくなることがある
CSCwd41806	policy_apply.pl プロセスの OOM（メモリ不足）で展開が失敗した
CSCwd41986	インターフェイス名を小文字から大文字に更新すると、Packet Tracer インターフェイスが UI に表示されない
CSCwd42072	SRU のインストールエラー
CSCwd42347	同じシーケンス番号を持つプレフィックスリストの変更を展開すると、FMC にアラートや警告が表示されない
CSCwd42410	予期された SNMP 出力が「show run | in fxos snmp」に見つからない
CSCwd42620	説明にエスケープされた値を含むオブジェクトを展開すると、以降のすべての展開が失敗する可能性がある
CSCwd43666	/opt/cisco/config/var/log/ASAconsole.log の logrotate がない理由を分析する
CSCwd43745	FTDv クラスタヘルスモニターが「クラスタのライブステータスを取得中にエラーが発生しました（Error fetching live status of the cluster）」で失敗する
CSCwd44326	オブジェクト NAT 編集が失敗する
CSCwd45048	92.14.0 で FCM WebUI のログイン前バナーに余分な文字が表示される
CSCwd46061	FPR 2100：1G SFP を備えた 10G インターフェイスがリロード後にダウンする
CSCwd46182	定期的な同期の失敗がユーザーに報告されない
CSCwd46741	fxos ログローテーションでファイルの循環に失敗し、ファイルサイズが大きくなる
CSCwd46780	ASA/FTD：スレッド名 appAgent_reply_processor_thread でトレースバックおよびリロードする
CSCwd47340	FXOS：svc_sam_envAG プロセスのメモリリークである
CSCwd47442	800_post/1027_ldap_external_auth_fix.pl アップグレードエラー -- 欠落している認証オブジェクトを参照する
CSCwd47481	CCM レイヤ（シーケンス 40）での WR6、WR8、LTS18、および LTS21 コミット ID の更新

不具合 ID	タイトル
CSCwd48633	ASA：Webvpn ポータルが使用されている場合にトレースバックおよびリロードする
CSCwd48776	展開後にポートチャネル インターフェイスがダウンした
CSCwd49636	正常性イベントが処理されないため、FMC UI が複数のデバイスの無効化/オフラインを示す
CSCwd49685	SSL MEMCAP がないため、snort 検出エンジンを待機するタイムアウトが原因で展開が失敗する
CSCwd49758	膨大な数のポリシーが原因で FMC で発生する事前展開が失敗する
CSCwd50131	アップグレードで mysql ファイルがクリーンアップされず、「/ngfw でのアンマネージドディスクの使用率が高い（High unmanaged disk usage on /ngfw）」というアラートが表示される
CSCwd50218	ASA の復元で vlan 設定が適用されない
CSCwd51757	接続レート OID の SNMP GET を使用してポーリング結果を取得できない
CSCwd51964	サービスアプリケーションの空のパターンをチェックするために、luaディテクタ API に検証を追加する
CSCwd52995	FMC で展開プレビューウィンドウが開かない
CSCwd53135	ASA/FTD：しきい値を超えるフローのオブジェクトグループ検索 Syslog
CSCwd53340	snort が 4085 ～ 4096 バイトのサイズのメッセージを送信すると、FTD PDTS LINA RX キューがスタックすることがある
CSCwd53635	AWS：Geneve トンネルインターフェイスで SSL 復号が失敗する
CSCwd53863	POLICY_SNAPSHOT のデータサイズが大きいため、Sybase から MariaDB へのデータ移行に時間がかかる
CSCwd54439	FMC は、Snort2 から Snort3 ルールへの変換の失敗に関する無関係なエラーメッセージを表示する
CSCwd55642	7.0.0 以降へのアップグレード後に、古い CPU コアの正常性イベントが FMC UI に表示される
CSCwd55673	log_handler_file ウォッチドッグのクラッシュフィックスの修正が必要である
CSCwd55853	アップグレード後のローカルプールの重複エラーによって展開が失敗する
CSCwd56254	FTD で実行すると、「show tech-support」の生成内容に「show inventory」が含まれない

不具合 ID	タイトル
CSCwd56296	FTD Lina がスレッド名「IP Init Thread」でトレースバックおよびリロードする
CSCwd56774	「show asp drop」の紛らわしいドロップ理由
CSCwd56995	application/octet-stream と text/plain を使用した Web コンテンツへのクライアントレスアクセス
CSCwd57698	ina_duart_write での再帰パニック
CSCwd57927	アップグレード後に FMC UI が使用できなくなり、「システムプロセスが開始しました（System processes are starting）」というメッセージが表示されることがある
CSCwd58188	インラインペアの状態が、ハードウェアバイパスからスタンバイモードに自動回復できない。
CSCwd58337	ポリシー展開サブグループに、より多くの cgroup メモリを割り当てる
CSCwd58417	cfg ファイルが見つからないため、HA の定期的な同期が失敗する
CSCwd58430	AC ポリシーの保存に時間がかかる場合があり、10 分以上かかる場合がある
CSCwd59736	ASA/FTD：アップグレード中の SNMP グループ設定によりトレースバックおよびリロードする
CSCwd61016	ASA：EEM が設定されている場合、リブート時に「Sync Config」ステータスでスタンバイがスタックすることがある
CSCwd61082	FMC UI が S2S VPN モニタリングページに不正確なデータを表示する
CSCwd62025	FTDv：フェールオーバー インターフェイスのインターフェイス設定が原因でポリシー展開が失敗する
CSCwd62138	DCD が有効になっている場合に ASA 接続がアイドル状態でスタックする
CSCwd62915	ASCII 以外の文字を使用したクロスドメインユーザーは解決されない
CSCwd63580	FPR2100：アプライアンスモードの ASA でのフェールオーバー コンバージェンス時間の増加
CSCwd63722	AWS GWLB の背後にある FTDv シングルアームプロキシは、すべて 0 チェックサムの geneve-invalid-udp-checksum が原因でドロップする
CSCwd63961	属性値が大きすぎることによる、DAP ルールとの AC クライアントの一致の失敗

不具合 ID	タイトル
CSCwd64480	ASA のコンテキストのカスケード接続を介したパケットが、ソフトウェアアップグレード後にゲートウェイコンテキストでドロップされる
CSCwd64919	FXOS は PoE ログをローテーションしていない
CSCwd66709	HA の FP4125 2.10.1.166 FTD アプリケーションが応答なし状態になった
CSCwd66815	サポートのための Lina の変更 - FQDN ベースのトラフィックを処理する際に、Snort3 が daq-pdts でトレースバックする
CSCwd68088	ASA|FTD：RFC 推奨事項に基づいて異なる TLS diffie-hellman 素数を導入する
CSCwd69236	FMC 接続イベントが最新のイベントを表示しなくなる
CSCwd69454	セカンダリユニットのポートチャネルインターフェイスは、リロード後に待機状態になる
CSCwd70117	管理対象デバイスのインターフェイスの説明フィールドの改行を FMC で処理できない
CSCwd71254	ASA/FTD が idfw fqdn ハッシュルックアップでトレースバックおよびリロードすることがある
CSCwd71274	S2S VPN ダッシュボードに、KP-HA スイッチロール後に KP-HA と WA-HA 間の IPv4 SVTI トンネルがダウンと表示される
CSCwd72680	FXOS：FTD アクセス コントロール ポリシー展開中の高い CPU 使用率によってトリガーされる FP2100 FTW タイムアウト
CSCwd72915	FMC 7.1.0.1 は、展開中に S2S VPN 構成に廃止された MD5 ハッシュが含まれているという警告をスローしない
CSCwd73981	FMC：更新ページの読み込みに 5 分以上かかる
CSCwd74116	DSID リークによる DH 計算エラーのため、S2S トンネルが機能しない
CSCwd74839	ユニットがクラスタに再参加するときの 30 秒以上のデータ損失
CSCwd75738	事前定義された FlexConfig テキストオブジェクトがインポート/エクスポート機能によってエクスポートされない
CSCwd75782	FMC 外部認証テストエラー「暗号化方式は設定されていますが、証明書はアップロードされていません（Encryption method is configured but you did not upload a certificate）」。
CSCwd76622	Snort3 を使用した FTD では、同じ IP トラフィックスケーリングを使用して、snort ファイルでメモリ破損 BT が発生する場合がある

不具合 ID	タイトル
CSCwd76634	FMC のインポートに時間がかかりすぎる
CSCwd76930	ラベルの FPR3110 ファンの SN が show inventory cli 出力と異なる
CSCwd77300	7.3.0 および 7.4.0 で VDB インストールを使用して Mercury ライブラリをリロードすると、Snort がクラッシュする
CSCwd78624	HA が設定された ASA は、複数の入出力エラーメッセージでトレースバックおよびリロードすることがある
CSCwd79388	FMC を 7.0.3 から 7.1.0 にアップグレードした後、侵入イベントを MariaDB から MonetDB に移行できない
CSCwd80284	インポート/エクスポートがバックエンドエラーで失敗する
CSCwd80343	7.0.4 を実行している MI FTD でディスク使用率が高い
CSCwd80741	Snort は、Early Application Detection が有効になっている Bomgar アプリケーションパケットをドロップする
CSCwd81538	peer_proxy_tx_q の 9344 ブロック枯渇による FTD トラフィック障害
CSCwd81897	appid ディテクタのリロード後に今後のフロー接続を処理しているときに Snort3 のクラッシュが時々発生する
CSCwd82235	LINA がスレッド名 update_cpu_usage 下の FPR-1010 でトレースバックする
CSCwd82801	Snort は大量のパケットイベントを出力する - IPS イベントビューに「パケット情報がありません（No Packet Information）」と表示される場合がある
CSCwd83441	ポートチャネルにバンドルされている物理FTDインターフェイスのステータスが FMC に表示される必要がある
CSCwd83990	FTD - Snort はトラフィックに対して間違った NAP ID を照合する
CSCwd84046	Microsoft SCEP 登録で ASA ID 証明書の取得に失敗する - PKCS7 を確認できない
CSCwd84133	ASA/FTD がスレッド名「telnet/ci」でトレースバックおよびリロードすることがある
CSCwd84153	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwd84868	フローオフロードが使用されていない場合に、いくつかの devcmd 障害と checkheaps トレースバックが発生する。

不具合 ID	タイトル
CSCwd84942	Snort メモリ使用アラートは、cgroups ではなく Snort インスタンスの perfstats から値を読み取る必要がある
CSCwd85178	AWS ASAv PAYG ライセンスが GovCloud リージョンで機能しない。
CSCwd85609	6.6.x を実行している FTD は新しい HM（6.7 以降）で切断されているように表示されるが、チェックは実行され、更新されている
CSCwd85927	webvpn ユーザーが 36k 要素で DAP アクセスリストに一致する場合、トレースバックおよびリロードする
CSCwd86313	ダイナミック アクセス ポリシーを保存できない
CSCwd86457	ポリシーで更新されていないオブジェクトの数 >>> セキュリティ インテリジェンス >>> ブロックリストである
CSCwd86535	ASA/FTD：Netflow タイマーインフラでのトレースバックとリロード
CSCwd86783	userappid.conf から NAVL GUID を無効にしても機能しない
CSCwd86929	カットスループロキシが HTTPS トラフィックで機能しない
CSCwd87129	FMC のアクセスポリシーでエラーが表示される：「ポリシーの検証中にエラーが発生しました（Error during policy validation）」
CSCwd87438	syslog のロギングメカニズムの強化
CSCwd88585	ASA/FTD NAT プールクラスタの割り当てとユニット間の予約の不一致である
CSCwd88641	デバイスモデルと snort エンジンに基づいて VDB パッケージをプッシュするための展開の変更である
CSCwd89848	シャーシとブレード間のハートビート損失による ASA/FTD の障害
CSCwd90112	netmap クエリに関連する MariaDB のクラッシュである（セグメンテーション違反）
CSCwd90846	改善されたネクストホップ検証が原因で FDM でのソフトウェアアップグレードが失敗する
CSCwd91013	FMC | csm_snapshot_error で展開失敗
CSCwd91421	ASA/FTD が logging_cfg 処理でトレースバックおよびリロードすることがある
CSCwd91932	時間範囲オブジェクト取得 API のページングとカウント値が正しくない
CSCwd92804	FPR2100 で FAN LED がオレンジに点滅する

不具合 ID	タイトル
CSCwd93316	FMC のアップグレード後に展開すると、インスペクションの中断に関する警告が表示されない
CSCwd93376	クライアントレス VPN ユーザーが、WebVPN ポータルから大きなファイルをダウンロードできない
CSCwd93792	多数の MAC アドレスが検出されたホストに関連する SFDataCorrelator パフォーマンスの低下である
CSCwd94096	ASA が別の認証および承認サーバーを使用している場合、Anyconnect ユーザーが接続できない
CSCwd94183	ssp_ntp.log ログローテーションの問題により、マルチインスタンスでの FXOS 更新のサポート後にブレードが起動しない
CSCwd94670	FDM 7.3 で RA VPN グループポリシーを変更できない
CSCwd95436	セカンダリの再起動時のプライマリ ASA のトレースバックである
CSCwd95908	ASA/FTD がトレースバックおよびリロードする、スレッド名：rtcli async executor process
CSCwd96041	7.x へのアップグレード後、プロキシ経由の FMC SecureX が動作を停止する
CSCwd96493	起動時に FPR1010 で数秒間リンクアップが見られる
CSCwd96500	FTD：FPR3100 で WebVPN キープアウトまたは証明書マップを設定できない
CSCwd96755	バックアップの実行時に ASA が予期せずリロードされる
CSCwd96766	41xx：ブレードが再起動信号をキャプチャまたはログに記録しない
CSCwd96790	すべての管理対象デバイスの構成スナップショットが原因で FMC バックアップファイルのサイズが大きくなる
CSCwd97020	ASA/FTD：外部 IDP SAML 認証が「Bad Request」というメッセージで失敗する
CSCwe00757	サマリー ステータス ダッシュボードは、ログイン時にロードするのに 3 分以上かかる
CSCwe00828	Web サイトが https にリダイレクトされると、インタラクティブ ブロック アクションが機能しない
CSCwe00864	クラスタの参加に失敗すると、ライセンスコマンドがクラスタデータユニットで失われる

不具合 ID	タイトル
CSCwe03529	PAT プールの展開中の FTD トレースバックとリロード
CSCwe03631	「logging history <mode>」でレート制限を指定する必要がある
CSCwe04437	トラブルシューティングの top.log.gz のコレクションは、競合状態が原因で破損している可能性がある
CSCwe04746	データフローがないスタンバイ HA データインターフェイスで予期しない「No Traffic」正常性アラートが表示される
CSCwe05913	FTD トレースバック/リロード - Icmp エラーパケット処理に snp_nat_xlate_identity が含まれる
CSCwe06562	FPR1K/FPR2K：サブインターフェイスの数が多いトランスペアレントモードでのフェールオーバー時間の増加
CSCwe06724	一部のテーブルでデータベーステーブルの最適化が機能しない
CSCwe06826	正常なデータベースバックアップに対して電子メールアラートが誤って送信される
CSCwe06828	SendUserReloadSGTAndEndpointsEvent からの応答がない場合、FMC HA 同期が永久にハングする可能性がある
CSCwe07103	FMC：「rule_comments」に対する多数の EO 警告が原因で、DB 整合性チェックでアップグレードが失敗する
CSCwe07722	クラスタデータユニットが、ASP の理由「VPN reclassify failure」で非 VPN トラフィックをドロップする。
CSCwe07928	クラウド配信の FMC では、SAL/CDO にも送信せずにイベントを syslog に送信する方法はない
CSCwe08729	FPR1120：HA でのスイッチオーバー後に接続がティアダウンされる
CSCwe08908	Threat Grid 統合設定が FMC HA 同期の一部として同期されない
CSCwe09074	CRL チェックに失敗すると、トラストポイントの [なし（None）] オプションが機能しない
CSCwe09121	「snort3.validation.lua:5：「change」の近くに「=」が必要です（snort3.validation.lua:5: '=' expected near 'change'）」によって FTD 展開が失敗する
CSCwe09811	ポリシー展開の NAT ステートメントの追加/削除/編集中に FTD がトレースバックおよびリロードする
CSCwe10290	FTD が WSA からの GRE トラフィックをドロップする

不具合 ID	タイトル
CSCwe10548	設定が欠落している認証方式として LDAP を使用した ASA バインディングである
CSCwe11119	ASA：SNMP パケットの処理中にトレースバックおよびリロードする
CSCwe11727	1 つのデバイスにバージョンがない場合、すべてのデバイスで構成アーカイブのパージが失敗した
CSCwe12407	SSL ハンドルのリークによる高 Lina メモリ使用量である
CSCwe13627	FMC が VPN トラブルシューティングのログを取得できない
CSCwe14174	FTD - メモリ割り当てに不適切な値を提供する「show memory top-usage」である
CSCwe14417	FTD：宛先に到達可能になっても IPSLA プリエンプションが機能しない
CSCwe14514	キャプチャ設定の削除中のスタンバイユニットの ASA/FTD トレースバックとリロードである
CSCwe14590	FMC 展開プレビューに差分ではなく完全な設定が表示されている
CSCwe15111	FMC が、API PUT 要求を介して BGP のデフォルト発信設定を取得していない
CSCwe16554	フラグメント化された Client Hello の後、特定の条件下で TLS セッションがドロップされた
CSCwe16620	FMC ヘルスモニターがインターフェイス ステータス モジュールのアラートを報告しない
CSCwe16730	展開の失敗：「show-xml-response file コンテンツの印刷中にエラーが発生しました（Error while printing show-xml-response file contents）」という XML 応答が大きすぎる
CSCwe17858	CLOUD_SERVICE をサポートするための FMC HA 情報が FTD に確実に同期されない
CSCwe18090	FMC 展開の失敗：「検証に失敗しました。これは slav*/ha スタンバイデバイスであり、展開を拒否します（Validation failed: This is a slav*/ha standby device, rejecting deployment）」。
CSCwe18216	ログに Null 接続エラーが表示される
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OID が、関連する CPU の不完全なリストを返す

不具合 ID	タイトル
CSCwe18974	ASA/FTD がスレッド名「CTM Daemon」でトレースバックおよびリロードすることがある
CSCwe19051	保存されたファイルが /ngfw/Volume/root1/ にあるために、FTD の「アンマネージドディスクの使用率が高い」アラートがトリガーされる
CSCwe19830	ポリシーの展開に失敗する「error executing /*!40101 SET character_set_client = @saved_cs_client */; *」
CSCwe20043	ASA5516 の FTD でジャンボフレームが有効になっている場合、256 バイトのメモリブロックが開始時に枯渇する
CSCwe20714	プライマリデバイスがアクティブな場合にトラフィックがドロップする
CSCwe21037	Snort メモリ使用アラートは、top.log の値と一致する必要がある
CSCwe21187	UDP タイムアウトが期限切れになるまで、ASP ドロップ理由 no-mcast-intrf により、ASA/FTD がマルチキャストパケットをドロップすることがある
CSCwe21280	マルチキャスト接続の確立またはティアダウン syslog メッセージが生成されない場合がある
CSCwe21831	VPN ログ設定のログレベルが情報である場合に、FTD プラットフォーム設定に警告が追加される
CSCwe21959	Snort3：D 状態のプロセスの結果、jemalloc メモリマネージャで OOM が発生する
CSCwe22254	マルウェア分析を無効にすると、/dev/shm/snort のディスク使用率が高くなる
CSCwe22302	wtmp ファイルがログローテーションされないため、パーティション「/opt/cisco/config」がいっぱいになる
CSCwe22386	予期しないファイアウォールがトレースバックでリロードされる
CSCwe22492	ホストのテーブルビューの UI 読み込みが遅い
CSCwe22980	データベースの整合性チェックが完了するまでに数分かかる
CSCwe23039	NTP ポーリング頻度を 5 分から 1 秒に変更すると、役に立たない大きなログファイルが生成される
CSCwe23801	FPR2100：KP プラットフォームで複数の Snort3 および Snort2 コアが生成され、センサーがダウンする
CSCwe24532	/opt/cisco/platform/logs/ の下の nvram.out ログローテーションファイルの複数のインスタンス

不具合 ID	タイトル
CSCwe25187	FMC 外部認証で「内部エラー」が発生する
CSCwe25391	ユニバーサルアドレスが空の文字列であるために、rpc サービスディテクタが snort トレースバックを引き起こす
CSCwe26342	スレッド名 asacli/0 を示す ASA トレースバックとリロード
CSCwe26612	フェールオーバー スイッチオーバー後に FTD が OSPF 隣接関係を形成するのに想定以上に時間がかかる
CSCwe28094	VPN トンネルの作成時に「すべてのカウンタをクリア（clear counters all）」を実行した後、ASA/FTD がトレースバックおよびリロードすることがある
CSCwe28362	ルールのコピーと貼り付けが失敗し、ID ポリシーに空白のエラーメッセージが表示される
CSCwe28407	icmp_thread での LINA トレースバック
CSCwe28726	作成されたコンテキストを削除すると、コマンド「app-agent heartbeat」が削除される
CSCwe29179	CLUSTER：フロー所有者からの CLU 追加フロー要求よりも前に、ICMP 応答がディレクタに到着する
CSCwe29498	net::ERR_TOO_MANY_RETRIES エラーが発生して、light-modal-ac-rule-xx.css のロードに失敗することがある
CSCwe29529	FTD MI が BVI に接続された VLAN 上の PVID を調整しない
CSCwe29583	ASA/FTD が lua_getinfo のスレッド名「None」でトレースバックおよびリロードすることがある
CSCwe29850	ASA/FTD Show chunkstat top コマンドの実装である
CSCwe29952	1 時間のデッドロックタイムアウト後のスタックデータベースクエリによる SFDataCorrelator コアである
CSCwe30228	cf_reinject_hide フラグが原因で、ASA/FTD が関数「snp_fp_l2_capture_internal」でトレースバックすることがある
CSCwe30867	ローエンドプラットフォームで ntp ログから hwclock を設定するための回避策
CSCwe32448	FMC GUI イベントビューアで時間枠設定を変更すると、SecureX と統合された FMC で機能しない場合がある

不具合 ID	タイトル
CSCwe33130	重大度がマイナーのセンサー ID 79 の IERR が原因で、応答しないモジュール/ブレードをスーパーバイザがリブートしない
CSCwe34871	アクティブな認証セッションが VPN ダッシュボードに表示される
CSCwe36176	ASA/FTD：多数の（サブ）インターフェイスと HTTP サーバーが有効になっていると、フェールオーバーの遅延が大きくなる
CSCwe37132	TLS サーバー ID によって、特定のクライアントが破損した Client Hello を生成することがある
CSCwe37453	共有管理インターフェイスを使用して、管理者およびユーザーコンテキストでスタンバイユニットからゲートウェイに到達できない
CSCwe38029	スタンバイユニットで複数のトレースバックが観察される。
CSCwe39425	2100：電源スイッチの切り替えにより、異常なシャットダウンが発生し、「PowerCycleRequest」がリセットされる
CSCwe39431	FMC アップグレード：FTD ごとの sftunnel.json ファイルの生成は、重複した名前をチェックしない
CSCwe39546	FMC：使用できないリモートホストにバックアップすると、アプライアンスを再起動できなくなる
CSCwe40463	ピアからの削除がない場合、同時 IKE SA 処理中に古い IKEv2 SA が形成される
CSCwe41336	データインターフェイスを管理として使用して 7.2.3 ベータ版をアップグレードした後、FDM WM-HA ssh が機能しない
CSCwe41898	ASA：FTD アクセス コントロール ポリシー展開中の高い CPU 使用率によってトリガーされる FP2100 FTW タイムアウトである
CSCwe43965	ルールを ACP からプレフィルタに移動するルール名の 30 文字の制限を削除する
CSCwe44311	FP2100：再帰的なメッセージ -<date>.1.gz rotated filenames を回避するために LINA asa.log ファイルを更新する
CSCwe44620	NAT の説明に疑問符があると、FTD クラスタのデータメンバーで設定の不一致が発生する
CSCwe44672	Syslog ASA-6-611101 が 1 つの SSH 接続に対して 2 回生成される
CSCwe44766	IMS：FTD アクセス コントロール ポリシー展開中の高い CPU 使用率によってトリガーされる FP2100 FTW タイムアウトである

不具合 ID	タイトル
CSCwe45211	FDM によって管理される FTD で完全な展開をトリガーする前に、ユーザーに警告する必要がある
CSCwe45222	データの Dce2Smb2FileTracker 処理で Snort3 のクラッシュが見られる
CSCwe45779	有効な隣接関係がないためにフローティング接続がデフォルト値でない場合、ASA/FTD は BVI へのトラフィックをドロップする
CSCwe45879	存在しない bulkcsv ファイルのロードの失敗に関するエラーが頻繁に表示される
CSCwe48378	ファイルキャッシュのスラッシングによるディスク I/O の増加を防ぐために、FMC drop_cache トリガーを削除する
CSCwe48432	内部エラーのため、アクセス コントロール ポリシーの変更を保存できない
CSCwe50946	管理インターフェイスのリンクステータスが FXOS と ASA の間で同期されない
CSCwe50993	SFR モジュールの SNMP がダウンし、復旧しない
CSCwe51286	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe51296	REST API を介して RAVPN からグループポリシーを削除できない
CSCwe51443	OpenSSL の脆弱性の ASA 評価 CVE-2022-0778
CSCwe52120	tx chksum-offload が有効になっている場合、SSL 復号された接続が egress interface a pppoe で失敗する。
CSCwe52499	NGIPSv syslog-tls.conf.tt は、CC モードのときにフィルタを削除する必要がある
CSCwe53089	サブドメインに属するユーザーがパケットトレーサを収集できない
CSCwe54529	FPR2140 の FTD：TCP 正規化による Lina のトレースバックとリロード
CSCwe54567	マネージャが FTD から単独で登録解除され、show manager に「設定されたマネージャがありません（No manager configured）」と表示される
CSCwe56452	BGP IPv6 設定：ネイバーとのルートマップの関連付けが展開されない
CSCwe57218	FMC：FTD クラスタロールのステータスが正しくないため、FTD をアップグレードできない
CSCwe58207	logging history が有効になっている場合、ASA/FTD でメモリリークが発生する

不具合 ID	タイトル
CSCwe58576	FTD：SSL エラーが原因で、ノードが「正常性チェックで左側のクラスタを制御していることが検出されました（Health check detected that control left cluster）」でクラスタに参加しない
CSCwe58881	FMC のアップグレード後、設定されたクラウドリージョンに関係なく、SecureX リボンが米国のクラウドリージョンにリダイレクトされる
CSCwe58980	/var/sf/QueryPoolData がウェアハウスディレクトリでいっぱいになる
CSCwe59380	FTD：VRF ルーティングに依存する接続で「timeout floating-conn」が期待どおりに動作しない
CSCwe59664	ホットフィックスが適用された Windows OS を検出するために FMC GUI で作成された DAP ポリシーが期待どおりに機能しない
CSCwe59737	p3_tree_lookup のウォッチドッグタイムアウトを指すトレースバックが原因で ASA/FTD がリブートする
CSCwe59919	スレッド名「NetSnmp Event mib process」での FTD トレースバックとリロード
CSCwe60267	キーリングレポートが更新されたにもかかわらず、FXOS 障害 F0853 および F0855 が表示される
CSCwe61599	FTD 2100：バッファの破損から保護するために daq-ioq mempool を更新
CSCwe61703	カスタム AnyConnect 属性（dynamic-split-tunnel）をグループポリシーから削除できない
CSCwe61928	FTD がデフォルトゲートウェイを使用して RP に到達している場合、リロード後に PIM 登録パケットが RP に送信されない
CSCwe61969	ASA マルチコンテキストの「management-only」インターフェイス属性が作成中に同期されない
CSCwe62361	ハートビートが失われ、「NPU との通信が失われた」ために ASA がリブートする
CSCwe62703	複数のセッションが開かれている場合、新しい context サブコマンドが HA スタンバイで複製されない。
CSCwe62927	DCCSM セッション認証の失敗により、FMC 全体で複数の問題が発生する
CSCwe62971	Umbrella DNS コネクタ設定を削除しようとすると、ポリシー展開が失敗する
CSCwe62997	snp_tracer_format_route での ASA/FTD トレースバックである

不具合 ID	タイトル
CSCwe63067	tcp インターセプト統計により、ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe63232	ASA/FTD：クラスタ内のフローオフロード状態が同じであることを確認する
CSCwe63266	無効なファームウェア MF-111-234949 の障害/エラーが必要
CSCwe63316	プリアクティブ FMC でスタンバイマネージャを設定するための FTD の登録タスクがトリガーされない
CSCwe63493	バックアップ後、複数の復元プロセスが起動しない。バックアップまたは復元中にエラーは表示されない。
CSCwe64043	リロード時に Cisco ASA および FTD ACL がインストールされない
CSCwe64281	FMC を 7.3 にアップグレード後、スナップショットの生成で展開に失敗する
CSCwe64404	認証サーバーの IP を変更した後、ASA/FTD がトレースバックおよびリロードすることがある
CSCwe64542	TID python プロセスが CPU 100% でスタックする
CSCwe64557	ASA：サポートされていないプラットフォームで SFR モジュール設定を防止する
CSCwe64563	作成されたコンテキストを削除すると、コマンド「neighbor xxxx ha-mode graceful-restart」が削除された
CSCwe65245	SNMP ポーリング レートが非常に高い場合、FP2100 シリーズ デバイスが過剰なメモリを使用することがある
CSCwe65634	ASA：ACL DAP の同期中にスタンバイデバイスがトレースバックおよびリロードすることがある
CSCwe66132	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe67751	SIP IPv6 パケットの最後のフラグメントの MF は 1 であり、より多くのパケットが予想されることを示している
CSCwe67816	isakmp キャプチャを削除するときに、ASA/FTD がトレースバックおよびリロードする
CSCwe68159	フェールオーバーの fover_trace.log ファイルがフラッディングし、すぐに上書きされる

不具合 ID	タイトル
CSCwe68917	Snort3 が SMTPS トラフィックを ACP ルールに一致させられない
CSCwe69388	FMC は、AnyConnect カスタム属性の遅延キーワードを大文字ではなく小文字でプッシュする必要がある
CSCwe70202	異なる「相手装置動作モード」が誤って認識されたため、フェールオーバーが複数回無効になる可能性がある。
CSCwe70558	FTD：CLISH プロンプトでコマンドを実行できない
CSCwe70665	CSCwd84942 に修正を加えても、Snort の高メモリアラートが引き続き表示される
CSCwe70721	展開前の検証エラーが原因で展開がブロックされた - 無効なエンドポイントである
CSCwe71284	ASA/FTD がスレッド名「DATAPATH-3-21853」でトレースバックおよびリロードする場合がある
CSCwe71672	ルート構成を無効にする選択的展開である
CSCwe71673	プレフィルタ設定を削除する選択的展開である
CSCwe71674	グループポリシーを削除する選択的展開である
CSCwe72330	静的ルーティングを追加した後のデータパススレッドでの FTD LINA のトレースバックとリロード
CSCwe72535	外部認証を使用して FTD にログインできない
CSCwe73116	クロスインターフェイスアクセス：VPN を介した管理アクセスインターフェイスへの ICMP ping が機能しない
CSCwe73240	Snort が大量のパケットログを送信すると FMC がスペース不足になる
CSCwe74059	logrotate によって 9.16 ASA または 7.0 FTD のファイルが圧縮されない
CSCwe74089	ASA/FTD がスレッド名「DATAPATH-1-1656」でトレースバックおよびリロードすることがある
CSCwe74290	/var/log/messages に SFDataCorrelator スパムが見られる
CSCwe74328	AnyConnect - hostscan が有効な場合、モバイルデバイスは接続できない
CSCwe74899	RMA デバイスでのバックアップ復元後、セカンダリ/スタンバイで CD App Sync エラーでアプリ構成の適用に失敗する
CSCwe74916	リンクステートの伝達により、 Inline-set でインターフェイスが DOWN を維持する

不具合 ID	タイトル
CSCwe75018	Snort2 ルールの推奨事項により、無効なルールの数が大幅に増加する
CSCwe75055	（FMC モデルの移行）FMC のヘルスモニタリングでエラーが報告される
CSCwe75124	アップグレードされた FMC は、ホットフィックスが適用された FTD をライト登録済みとしてマークしなかった - FMC HA 同期に失敗した
CSCwe75207	ネットワークマップの更新率が高いと、イベント処理で大きな遅延とバックログが発生する可能性がある
CSCwe76036	ndclientd エラーメッセージ「ローカルディスクがいっぱいです（Local Disk is full）」が表示され、いっぱいになっているマウントの詳細を提供する必要がある
CSCwe76722	ASA/FTD：カスタム VRF を使用すると、from-the-box ping が失敗する
CSCwe77123	ASA/FTD：VPN ピア間に遅延がある場合の、IPSEC VPN を介した FPR2100 での TCP スループットの低下
CSCwe77896	Azure AD レルムのドキュメントの改善
CSCwe78977	ASA/FTD がスレッド名「pix_flash_config_thread」でトレースバックおよびリロードすることがある
CSCwe79051	EIGRP/BGP 変更の展開により、ポリシーの適用中に一時的な障害が発生することがある
CSCwe79072	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe79954	同じ LDAP サーバーがプライマリとバックアップとして追加されている場合、LDAP 外部認証設定を FTD に展開できない
CSCwe80063	ポートチャネルのサブインターフェイスのデフォルト DLY 値が親 PortChannel と一致しない
CSCwe81684	ASA：「management-only」の解析でスタンバイ障害がパーサー/フェールオーバーサブシステムに報告されない
CSCwe82107	[FSM:STAGE:FAILED] という正常性アラート：外部 AAA サーバー設定
CSCwe82631	FMC で 30 を超える VLAN インターフェイスを作成できない
CSCwe83061	アクティブプライマリ FMC からの FMC のアップグレードが「インストール失敗：不完全なピア検出（Installation failed: Peer Discovery incomplete）」で失敗する
CSCwe83069	Snort3 メモリ使用率の値を修正する

不具合 ID	タイトル
CSCwe83478	プルーニングターゲットは、プルーニングされたスレッドから割り当てられたメモリを考慮する必要がある
CSCwe85432	SIP インスペクションが有効になっていると、スレッド DATAPATH-14-11344 で ASA/FTD がトレースバックし、リロードする
CSCwe86029	FTP/SCP プロトコルを使用している場合、FMC の再イメージ化中に FMC システム復元認証エラーが発生する
CSCwe86225	スレッド名 cli_xml_server in tm_job_add を示す ASA/FTD のトレースバックとリロード
CSCwe86350	7.2 にアップグレード後、スケジュールされたアクティビティへの電子メールアラートが機能しない
CSCwe88496	Snort 2 カスタムルールの変換に失敗しました。詳細については、/var/sf/htdocs/ips/snort.rej を参照してください。
CSCwe88772	プロセス名 cli_xml_request_process での ASA のトレースバックとリロード
CSCwe89030	証明書のサブジェクト DN からのシリアル番号属性をユーザー名として使用する必要がある
CSCwe89305	「R から N への移行は許可されていません（migration from R to N is not allowed）」というエラーで vFMC300 から FMC2600 への移行が失敗する
CSCwe89731	サービスダウンの通知デーモン誤アラームである
CSCwe89985	CVIM コンソールが [カーネルを起動中（Booting the kernel）] ページでスタックする
CSCwe90095	証明書からのユーザー名（Username-from-certificate）機能は、電子メール属性を抽出できない
CSCwe90202	ASA：動的設定変更の「management-only」の解析時にスタンバイ障害が発生する
CSCwe90334	unified_events-2.log にインスタンス ID がない
CSCwe90596	FMC でエレファントフロー検出が無効になり、ランダム展開後に FTD で有効になる
CSCwe90720	ha_msg の破損による解析スレッドでの ASA のトレースバックとリロード
CSCwe91958	接続イベントに基づく相関イベントにセキュリティ インテリジェンス カテゴリのコンテンツが含まれない

不具合 ID	タイトル
CSCwe92905	ngfwManager プロセスが継続的に再起動し、ZMQ Out of Memory のトレースバックが発生する
CSCwe93061	efd.lua ファイルの内容が空の場合、FTD から「show elephant-flow status」の出力が返されない
CSCwe93162	FP1140 7.0.4 の展開がエラー「HASH 参照としての未定義の値を使用できません（Can't use an undefined value as a HASH reference）」で失敗し続ける
CSCwe93176	FMC のアップグレード後に ngfw.rules（assignment_data テーブル）に Snort2 ルールが割り当てられていない
CSCwe93202	FXOS REST API：タイプ「ecdsa」のキーリングを作成できない
CSCwe93489	threat-detection がプレフィックス付き IPv6 の例外オブジェクトを認識しない
CSCwe93532	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe93537	threat-detectionで個々の IPv6 エントリをクリアできない
CSCwe93566	FDM GUI のデフォルトの TLS 1.1（廃止）サポートをオフにする必要がある
CSCwe93736	コマンドを受理しても ASA がタイムゾーンを更新しない
CSCwe94287	複数の DHCP サーバーが設定されている場合、FTD DHCP リレーが NACK をドロップする
CSCwe94789	バイパスドメインフィールドの Cisco Umbrella DNS ネゲートが FMC から生成されない
CSCwe95757	ASA/FTD がスレッド名「lina」でトレースバックし、リロードすることがある
CSCwe96023	ASA/FTD：6.6.5 から 7.0.1 へのアップグレード直後の SNMP 関連のトレースバックとリロード
CSCwe96068	ASA：CLU RX/TX キューでの大量のアンダーラン/オーバーランに対する設定可能な CLU
CSCwe96857	実名フィールドのワイド文字が原因で、FMC エラーでユーザーページが表示される
CSCwe97325	期限日の形式が原因で FDM が自己署名証明書を作成できない
CSCwe98430	7.2.4 FMC から 6.7 FTD への AC ポリシーの展開が失敗する

不具合 ID	タイトル
CSCwe99040	tcpmod_proxy_continue_bp プロセスでのスレッドデータパスのトレースバックとリロード
CSCwe99550	asa log infraでファイル固有のロギングを一時停止/再開するノブを追加。
CSCwe99945	DOC：Cisco Firepower 2100 GLC-T および GLC-TE SFP サポートの紛らわしいドキュメント
CSCwf00417	FTD：SSL エラーを生成しているクライアントで TLS サーバー ID を使用して TLS1.2 Web サイトを処理できない
CSCwf00483	孤立した SFTop10Cacher プロセスが見つかる
CSCwf00865	一方のスポークで IPSec フローがオフロードされ、もう一方でオフロードされていない場合、FTD/ASA ハブアンドスポーク（U ターン）VPN が失敗する
CSCwf01051	QP-MI HA 7.0.3 から 7.2.4-126 の後にスタンバイが無効状態になる、APPLY_APP_CONFIG_APPLICATION_FAILURE
CSCwf01064	9.18.2 以降、TCP ping が全く機能しない
CSCwf01954	FTD：ADI.conf - s2s VPN 正常性ポリシーを適用した後でも、send_s2s_vpn_events が 0 に設定される
CSCwf02363	nss_passwd_lookup からのコール後に SslServiceDetector で Snort3 がクラッシュする
CSCwf03011	FMC を 7.3 バージョン以降にアップグレードする前に sfsnort スキーマに存在していた対称トリガーがプルーニングされる
CSCwf04831	ASA/FTD がスレッド名「ci/console」でトレースバックし、リロードすることがある
CSCwf04870	ASA：「Ping<ifc_name> xxxx」が 9.18.x 以降、期待どおりに機能しない
CSCwf06318	FMC HA を一時停止せずに準備状況チェックを実行できるようにする必要がある
CSCwf06377	BS および QP のハートビートタイムアウトを 6 秒に設定
CSCwf07030	アップグレード デバイス リスト ページで、25 の FTD が登録されているページを完全にロードするのに 15 分以上かかる
CSCwf07791	ASA で SNMP PDU および SNMP VAR チャンクが不足している
CSCwf08043	フラグメント化されたパケットによる Lina のトレースバックとリロード

不具合 ID	タイトル
CSCwf08515	FPR3100：ASA/FTD の高トラフィックがすべてのデータインターフェイスに影響し、「demux drops」のカウンタが高い値を示す
CSCwf10422	成功しても「セキュリティ インテリジェンス フィードのダウンロードに失敗しました（Security Intelligence feed download failed）」と表示される
CSCwf10486	カンマで区切られた複数のネットワークが ISE 統合ネットワークフィルタで処理されない
CSCwf10910	FTD：7.3.0 を実行している ZMQ でのトレースバック
CSCwf12005	ASA が user-agent と host なしで OCSP 要求を送信する
CSCwf12408	ASA：9.16.4 へのアップグレード後、最初のリブート時にすべてのタイプ 8 パスワードが失われる
CSCwf12521	FMC GUI の侵入ポリシーページをロードできない
CSCwf12985	FTDv：dpdk プールの枯渇と rx_buff_alloc_failure による VMware 展開でのトラフィック障害
CSCwf14126	プロセス名 Lina を示す ASA のトレースバックとリロード
CSCwf14257	ピア送信の不正なハッシュエラーが原因で、バックアップから復元された FTD コンテナを FMC に登録できない
CSCwf14735	Nat/Pat に関連する、プロセス名 lina での ASA のトレースバックとリロード
CSCwf14811	TCP ノーマライザには、パケットドロップなどのアクションを示す統計が必要
CSCwf15858	大量の認証プロファイルを送信するユーザーに対して SSL を介した LDAP 認証が機能しない
CSCwf15902	Hyper-V の ASAv が管理インターフェイスでパケットをドロップする
CSCwf16108	スペースを含む FMC 7.3.1 でバックアップピア IP を有効にすると、VPN IPSec プロファイルが削除される
CSCwf17406	70 日以上経過した Snort 統計ファイルを削除できない
CSCwf17814	ASA/FTD がスレッド名「19」でトレースバックし、リロードすることがある（空きブロックチェックサムエラー）
CSCwf19562	/var/log/tid_process.log に書き込まれる lamplighter ログの変更
CSCwf19853	eventdb テーブルの列がないため、DBCheck で致命的なエラーが発生する

不具合 ID	タイトル
CSCwf20215	管理者ユーザーを CLI シェルアクセスフィルタから除外する必要がある
CSCwf20338	ASA がスレッド名「DHCPv6 Relay」でトレースバックおよびリロードすることがある
CSCwf20958	Health.log ファイルの logrotate と最大サイズが設定されていない
CSCwf21106	ASA/FTD：SNMP およびインターフェイスの変更中の、スレッド名 snmp_master_callback_thread でのトレースバック
CSCwf22005	ASA packet-tracer が常に最初の ACL ルールを表示するが、正しい ACL と一致する
CSCwf22568	FTD HA の作成に失敗し、FMC でデバイスが一貫性のない状態で表示される
CSCwf22854	[マルウェアの概要（Malware Summary）] ページから「\u」を含むファイル名のファイルをクリーンリストに追加できない
CSCwf23564	パススルーデバイスとして GRE TUNNEL および FTD を介した MD5 認証を使用すると、BGP を確立できない
CSCwf24124	FMC で SFDataCorrelator プロセスが頻繁にクラッシュする
CSCwf24773	crashhandler がテストモードの Snort で実行されている
CSCwf25144	[FMCバックアップ管理（FMC Backup Management）] ページに FTD センサーの「バックアップの検証」が表示されている
CSCwf26264	リモートストレージに到達できない場合、FMC バックアップの復元ページのロードに約 5 分かかる
CSCwf26407	FP2130：ポートチャネルのメンバーの関連付けを解除できず、展開に失敗し、FTD/FMC でメンバーが失われる
CSCwf26534	ASA/FTD：SIP-SDP ヘッダーの接続情報が、destination static Anyで変換されないままになる
CSCwf26939	FTD がエラー「IPv4 宛先の実際のオブジェクトアドレス範囲が広すぎます（IPv4 dst real obj address range is huge）」で NAT ルールの作成に失敗することがある
CSCwf28488	emblem が設定され、 buffer logging が debug に設定されている場合に一貫性のないログメッセージが表示される
CSCwf28592	一部の特定のシナリオで、オブジェクトオプティマイザによってデバイスに誤ったルールが展開される可能性がある

不具合 ID	タイトル
CSCwf30716	マルチコンテキストの ASA で、MIO HB のリカバリ後でもスタンバイデバイスが失敗状態で表示される。
CSCwf30727	validation-usage ssl-server を使用しない場合、ASA と Umbrella の統合が機能しない。
CSCwf31701	スレッド名 **CP Crypto Result Processing** での ASA トレースバックとリロード
CSCwf31820	グローバル VRF またはユーザー VRF 間のルーティング時にファイアウォールがパケットをドロップすることがある
CSCwf32890	スタンバイ FMC SSH 接続が頻繁に切断される
CSCwf33574	アップグレード後に ASA access-list エントリのハッシュが同じになる
CSCwf33904	仮想 FDM のアップグレードが失敗する：UpgradeOnStandby 実行後に HA configStatus='OUT_OF_SYNC となる
CSCwf34152	SFTunnel の確立の失敗により、FMC が新しい FTD の展開または登録に失敗する
CSCwf34450	重複するカスタムアプリケーションが存在する場合、結果として Snort の再起動後に Snort3 がクラッシュする
CSCwf34500	FTD：GRE トラフィックが CPU コア間で負荷分散される
CSCwf35173	running_config.conf ファイルの設定ミスが原因で SFTunnel が適切に確立されない
CSCwf35207	ASA：ASA で ACL を更新中にトレースバックとリロードが発生する
CSCwf35346	SXP のダウンロード中に ISE からエラーが報告された場合、FMC はエラーを適切に処理する必要がある
CSCwf37160	証明書グループマップが設定されている場合、AnyConnect Ikev2 ログインに失敗する
CSCwf39968	[オブジェクト管理（Object Management）] ページの FMC UI 関連の問題
CSCwf42144	プロセス名「Lina」を示す ASA/FTD のトレースバックが発生することがある
CSCwf43247	NMAP 修復スキャンタスクがアクションキューテーブルで保留状態のままになり、クリアされない
CSCwf43288	クラスタ構成のセットアップで、スレッド名「ssh/client」でのトレースバックが発生する

不具合 ID	タイトル
CSCwf43391	FMC のネットワーク オブジェクト グループに追加されたネットワークの検証チェックの追加
CSCwf44915	古い LSP パッケージがプルーニングされないため、ディスク使用率が高くなる
CSCwf47487	tar で読み取り中に CSM 監査ログファイルが変更されたために、CSM のバックアップが失敗する
CSCwf48599	廃止された暗号を使用した VPN ロードバランシング クラスタ暗号化
CSCwf49573	ASA/FTD：「show memory webvpn all objects」を発行する際のトレースバックとリロード
CSCwf51824	ユーザーが FXOS SNMP の「sys/svc-ext/snmp-svc のプロパティコミュニティが範囲外（property community of sys/svc-ext/snmp-svc is out of range）」を理解できない
CSCwf51933	アップグレード後にドット付きの FTD ユーザー名が AAA-RADIUS 外部認証ログインに失敗する
CSCwf54418	重複検出後に形成された古い IKEv2 SA のクリアにかかる時間の短縮
CSCwf56291	7.2.4 にアップグレードする前に ca_purge ツールを使用した場合、FMC 設定アーカイブの保持がデフォルトに戻る
CSCwf57850	FMC のアップグレード後、TelemetryApp プロセスが毎分終了し続ける
CSCwf58876	KP2140-HA、リロードされたプライマリユニットがピアユニットを検出できない
CSCwf59571	FTD/Lina：ローエンドプラットフォームでの Msglyr プールメモリの減少により ZMQ が OUT OF MEMORY を発行する。
CSCwf60311	9.16.4.19 へのアップグレード後にスレッド名 DATAPATH-53-18309 で ASA でトレースバックが発生する
CSCwf60584	ヘルスモニタリングでトランスペアレントモード FTD のルート統計情報が収集されない
CSCwf62103	FTD への展開を許可する前に、FMC が QoS ポリシールールを適切に検証する必要がある
CSCwf62885	AWS GWLB の背後にある FTDv シングルアームプロキシが、geneve-invalid-udp-checksum が原因でドロップする
CSCwf66271	デバイス除外ポリシーの下にインターフェイスを一覧表示できない

不具合 ID	タイトル
CSCwf71606	リロード時に Cisco ASA および FTD ACL がインストールされない
CSCwf71812	FTD Lina エンジンが、アサーションが原因でデータパスでトレースバックすることがある
CSCwf72510	HA の両方のデバイスが FMC にイベントを送信しないようにする
CSCwf73189	NAT 障害により、FTD が WSA からの GRE トラフィックをドロップする
CSCwf76970	セカンダリユニットがアクティブな場合、HA の中断中に警告を含める
CSCwf77191	ASA アプライアンスモード - 「connect fxos [admin]」で「ERROR: failed to open connection」が返される。
CSCwf78950	FMC 1600 プロセス ssp_snmp_trap_fwdr のメモリ使用率が高い
CSCwf81058	FTD：[有効（Enabled）] と表示される Firepower 3100 の動的フローオフロード
CSCwf81320	FMC 7.2.4 で RAVPN の IPv6 DNS サーバーを設定および展開できない
CSCwf82247	ルートの同じプレフィックス/メトリックが別の VRF で設定されている場合、ポリシーの展開が失敗する。
CSCwf84588	SFTunnel 通信のために TLS 1.1 が永続的に無効化される
CSCwf85307	[Snort 3] IPS ポリシーのオーバーライドが連鎖侵入ポリシーで機能しない
CSCwf86860	FMC GUI	ルールで検索を実行し、最後のページに移動すると、ACP ページが空白になりハングする
CSCwf87761	ポリシーをコピーすると、すべてのデバイスがダーティとしてマークされる
CSCwf88552	ASA/FTD：NAT L7 インスペクションの書き換えによるトレースバックとリロード
CSCwh12009	共有ルールレイヤの削除後に EOStore 失敗エラーが出力される
CSCwh13551	アップグレード時に暗号化された可視性エンジン（EVE）ダッシュボードタブとウィジェットが FMC GUI に追加されない
CSCwh14731	認証オブジェクト名に空白を含めることができない
CSCwh21337	FTD：展開ロールバック中の LSP パッケージコードの問題
CSCwh28779	名前が 40 文字を超えているため、7.x へのアップグレード後に侵入ポリシーを保存できない

不具合 ID	タイトル
CSCwh30276	侵入ポリシーのルール更新フィルタに一貫性のない結果が表示される

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。