Cisco Secure Firewall Threat Defense バージョン 7.6.x リリースノート

最終更新：2026 年 6 月 15 日

Cisco Secure Firewall Threat Defense リリースノート

このドキュメントでは、以下に示す製品のリリース情報を記載しています。

- Cisco Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center（オンプレミス）
- Cisco Cisco Secure Firewall Device Manager

クラウド展開については、『クラウド提供型 Firewall Management Center リリースノート』または「*Security Cloud Control* 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 *7.6* の日付

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
7.6.5	106	2026-02-17	Firewall Management Center	Firewall Management Center
7.6.4	69	2026-01-07	すべて	すべて
7.6.3	113	2025-10-23	Firewall Management Center	Firewall Management Center パブリッククラウドの Firewall Threat Defense Virtual
7.6.2.1	3	2025-09-25	すべて	すべて
7.6.2	329	2025-08-11	すべて	すべて
7.6.1	291	2025-06-02	すべて	すべて

バージョン	ビルド	日付	プラットフォーム：アップグレード	プラットフォーム：再イメージ化
7.6.0	113	2024 年 9 月 16 日	すべて	すべて
	41	2024 年 6 月 27 日	—	利用できなくなりました。

互換性

アップグレードまたは再イメージ化する前に、ターゲットバージョンが展開と互換性があることを確認してください。互換性がないためにアップグレードまたは再イメージ化できない場合は、更新情報について、シスコの担当者またはパートナーにお問い合わせください。互換性については、『*Cisco Secure Firewall Threat Defense* 互換性ガイド』を参照してください。

互換性については、次を参照してください。

- *Cisco Secure Firewall Management Center* 互換性ガイド
- *Cisco Secure Firewall Threat Defense* 互換性ガイド

機能

以前のリリースの機能については、*Cisco Secure Firewall Management Center* の新機能（リリース別）および *Cisco Secure Firewall* デバイスマネージャの新機能（リリース別）を参照してください。

アップグレードの影響

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。望ましくない結果を避けるために、アップグレードの前または後にアクションを実行する必要がある場合、機能がアップグレードに影響を与える可能性もあります。たとえば、設定を変更する必要がある場合などです。

ここでの機能の説明には、必要に応じてアップグレードの影響が含まれています。アップグレードの影響があるバージョンごとの機能の完全なリストについては、アップグレードの影響がある機能 （32 ページ）を参照してください。

メンテナンスリリースの機能

メンテナンスリリース（3 桁）およびパッチ（4 桁）に含まれる機能、拡張機能、および重要な修正は、リリース日、リリースタイプ（短期または長期）、およびその他の要因によっては、今後のリリースをスキップする可能性があります。選択したバージョンの最新のメンテナンスリリースに直接移動することで、アップグレードなどの影響を最小限に抑えます。アップグレードターゲットの選択 （38 ページ）を参照してください。

英語以外の言語でWebインターフェイスを使用している場合は、メンテナンスリリースやパッチで導入される機能が、次のメジャーリリースまで翻訳されない可能性があります。

Snort の機能

Snort 3 は、Firewall Threat Defense をためのデフォルトの検査エンジンです。Firewall Management Center 展開用の Snort 3 機能は、新しい Firewall Device Manager 機能としてリストされていない場合でも、Firewall Device Manager にも適用されます。ただし、Firewall Management Center は Firewall Device Manager よりも多くの設定可能なオプションを提供する場合があることに注意してください。

重要 Snort 2 はバージョン 7.7 以降で廃止されるため、Firewall Threat Defense のアップグレードの妨げとなります。古いデバイスでまだ Snort 2 を使用している場合は、検出とパフォーマンスを向上させるために Snort 3 に切り替えてください。

侵入ルールとキーワード

アップグレードにより、新規および更新された侵入ルールおよびプリプロセッサルール、既存のルールの変更後のステータス、デフォルト侵入ポリシーの変更後の設定をインポートして自動的に有効化が可能です。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。

新しいキーワードの詳細については、Snort リリースノート：https://www.snort.org/downloads を参照してください。

FlexConfig

アップグレードにより、以前はFlexConfigが必要だった機能について、Webインターフェイスまたはスマート CLI のサポートが追加されることがあります。廃止されたコマンドを使用して新しく 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が、ほとんどの場合、既存の FlexConfigs は引き続き動作し、展開も可能です。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。アップグレードではFlexConfigは変換されません。アップグレード後、Web インターフェイスまたは Smart CLI で新しくサポートされた機能を設定します。新しい設定を確認したら、廃止されたFlexConfigを削除できます。

ここでの機能の説明には、必要に応じて、廃止されたFlexConfigに関する情報が含まれています。廃止された FlexConfig 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。

統合とロギング

これらの統合およびロギング機能には、Threat Defense および Management Center のリリースに関連する新機能が含まれている可能性があります。

- Syslog：*Cisco Secure Firewall Threat Defense Syslog Messages*
- Cisco Success Network：Cisco Secure Firewall Management Center から収集された Cisco Success Network テレメトリデータ
- REST API：*Cisco Secure Firewall Management Center REST API クイックスタートガイド* および *Cisco Secure Firewall Threat Defense REST API ガイド*

バージョン 7.6.5 の Firewall Management Center 機能

このリリースに新機能はありません。バージョン 7.6.5 で解決済みのバグ （43 ページ）を参照してください。

バージョン 7.6.4 の Firewall Management Center 機能

表 *2 :* バージョン *7.6.4* の *Firewall Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
以前のメンテナンスリリースからの機能			
以前のメンテナンスリリースからの機能。	機能に依存	機能に依存	バージョン 7.6.4 には、次の機能もあります。 • Cisco Secure Firewall 4200 の DC 電源（7.4.3） • 高可用性 Firewall Threat Defense のためのフェールオーバー。（7.4.3）
パブリックおよびプライベートクラウド			
OpenStack の Firewall Management Center Virtual の高可用性。	7.6.4	任意	Firewall Management Center Virtual OpenStack 対応が高可用性をサポートするようになりました。 プラットフォームの制限：FMCv2 ではサポートされていません

バージョン 7.6.3 の Firewall Management Center 機能

このリリースに新機能はありません。バージョン 7.6.3 で解決済みのバグ （87 ページ）を参照してください。

（注） バージョン 7.6.3 は、特定の脆弱性に対処するためにリリースされました。Firewall Management Center についてはアップグレードまたは新規インストールとして、パブリッククラウドの Firewall Threat Defense Virtual については新規インストールのみとして使用できます。既存の展開については、バージョン 7.6.2.1 は同じ修正を提供します。

バージョン 7.6.2 の Firewall Management Center 機能

このリリースに新機能はありません。バージョン 7.6.2 で解決済みのバグ （88 ページ）を参照してください。

バージョン 7.6.1 の Firewall Management Center 機能

表 *3* : バージョン *7.6.1* の *Firewall Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
以前のメンテナンスリリースからの機能			
以前のメンテナンスリリースからの機能。	機能に依存	機能に依存	バージョン 7.6.1 には次の機能もあります。 • 新しい Cisco AMP クラウド接続方式。アップグレードの影響。（7.0.7） • Cisco AMP クラウド接続のバックアップの廃止。（7.0.7） • すべての RADIUS 応答に Message-Authenticator 属性が必要です。アップグレードの影響。（7.0.7） • 広帯域幅で暗号化されたアプリケーショントラフィックは、侵入インスペクションを不要なものとしてバイパスします。（7.2.10） • 物理インターフェイスとサブインターフェイスのヘルスモニタリングを個別に設定します。（7.4.3） • 親ドメインにログインしているときに、リーフドメイン内のデバイスの正常性ステータスを表示します。（7.4.3） • プロキシを介した Cisco Umbrella の Firewall Management Center との統合。（7.4.3） • デバイス バックアップ ストレージの構成が容易になりました。（7.4.5）
プラットフォームの移行			
移行で Firepower 4100/9300 モデルから Cisco Secure Firewall 3100/4200 を選択する。	7.6.1	任意（Any）	以下のデバイスから、Cisco Secure Firewall 3100/4200 に設定を簡単に移行できるようになりました。 • Firepower 4110、4120、4140、4150 • Firepower 9300：SM-24、SM-36、SM-44
デバイス管理			

機能	最小の Management Center	最小の Threat Defense	詳細
[デバイス（ウィザード）（Device (Wizard)）] に追加された基本初期設定を使用して、登録キーでデバイスを追加する	7.6.1 7.7.0	任意	[デバイス（ウィザード）（Device (Wizard)）] の基本初期設定では、登録キーを使用してデバイスを追加できるようになりました。この機能は、**[追加（Add）]** > **[デバイス（Device）]**画面にも引き続き表示されます。 新規/変更された画面：**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[追加（Add）]** > **[デバイス（ウィザード）（Device (Wizard)）]** 参照：デバイス管理
ルーティング			
BGP AS オーバーライド。	7.6.1 7.7.0	7.6.1 7.7.0	Firewall Threat Defense は、ピアから受信した ASN を独自の BGP ASN で上書きできるようになりました。これにより、Firewall Threat Defense とピアリングする他のルータは、AS_PATH 属性の内容に基づいて、ループを検出しなくても、アドバタイズされたプレフィックスを受け入れることができます。 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）]** > **[ルーティング（Routing）]** > **[BGP IPv4またはIPv6（BGP IPv4 or IPv6）]** > **[ネイバーの追加/編集（Add/Edit Neighbor）]** > **[ASオーバーライド（AS Override）]** 参照：BGP
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
インターネットにアクセスできるデバイスは、インターネットからアップグレードパッケージをダウンロードします。	7.6.1 7.7.0	任意（一部制限あり）	アップグレードパッケージを使用せずにデバイスとシャーシのアップグレードを開始できるようになりました。適切なタイミングで、デバイスがインターネットからパッケージを直接取得します。これにより、時間と Firewall Management Center のディスク容量を節約できます。 インターネットにアクセスできないデバイスでは、引き続き Firewall Management Center または内部サーバーからパッケージを取得できます。デバイスは、インターネットまたは Firewall Management Center の前に、内部サーバー（設定されている場合）を試行することに注意してください。内部サーバーからのダウンロードが失敗した場合、インターネットにアクセスできる新しいデバイスは、インターネット、Firewall Management Center の順に試行しますが、古いデバイスやインターネットにアクセスできないデバイスは、Firewall Management Center のみを試行します。（この文脈での「新しい」とは、Firewall Threat Defense 7.6 以降またはシャーシ 7.4.1 以降を意味します）。 制限事項：Firewall Management Center およびデバイスは、インターネットにアクセスできる必要があります。インターネットにアクセスできるデバイスに、インターネットを試行する前に強制的に Firewall Management Center を試行させる方法はありません。ホットフィックスではサポートされていません。 ダウンロードの場所：https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ 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。

バージョン 7.6.0 の Firewall Management Center の機能

表 *4 :* バージョン *7.6.0* の *Firewall Management Center* 機能

機能	最小の Management Center	最小の Threat Defense	詳細
以前のメンテナンスリリースからの機能			

機能	最小の Management Center	最小の Threat Defense	詳細
以前のメンテナンスリリースからの機能。	機能に依存	機能に依存	バージョン 7.6.0 には次の機能もあります。 • Cisco Security Cloud 地域：インドおよびオーストラリア。（7.0.7） • VMware vSphere/VMware ESXi 8.0 のサポート。（7.2.9） • 非対称トラフィック処理。アップグレードの影響。（7.2.9） • 低解像度の画面用に最適化された Firewall Threat Defense およびシャーシ アップグレード ウィザード。（7.2.10） • Azure 向け Firewall Management Center Virtual 300。（7.4.2） • Azure 向け Firewall Management Center Virtual の高可用性。（7.4.2） • AWS 展開の IMDSv2 サポート。（7.4.3）
プラットフォーム			
Cisco Secure Firewall 1200	7.6.0	7.6.0	Cisco Secure Firewall 1200 が導入されました。これには、次のモデルが含まれます。 • Cisco Secure Firewall 1210CX（1000BASE-T ポート X 8） • Cisco Secure Firewall 1210CP（1000BASE-T ポート X 8、ポート 1/5 ～ 1/8 で Power over Ethernet（PoE）をサポート） • Cisco Secure Firewall 1220CX（1000BASE-T ポート X 8、SFP+ ポート X 2） *Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide*を参照してください。
Cisco Secure Firewall 4200 のネットワークモジュール。	7.6.0	7.6.0	Cisco Secure Firewall 4200 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 400G ネットワークモジュール（FPR-X-NM-2X400G） このモジュールは、ポートごとに 200 Gb、100 Gb、および 40 Gb もサポートするように設計されています。また、ポートごとに全二重イーサネットトラフィックを提供します。400 Gb ネットワークモジュールは、2 つの QSFP-DD トランシーバをサポートしており、200 Gb QSFP56、100 Gb QSFP28、および 40 Gb QSFP+ トランシーバもサポートするように設計されています。 *Cisco Secure Firewall 4200 シリーズ ハードウェア設置ガイド*を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
Firepower 1000 および Cisco Secure Firewall 3100/4200 の前面パネル USB-A ポートを無効にします。	7.6.0	7.6.0	Firepower 1000 および Cisco Secure Firewall 3100/4200 の前面パネル USB-A ポートを無効にできるようになりました。デフォルトでは、ポートは有効になっています。 新規/変更された Firewall Threat Defense CLI コマンド：**system support usb show**、**system support usb port disable**、**system support usb port enable** マルチインスタンスモードの Cisco Secure Firewall 3100/4200 の新規/変更された FXOS CLI コマンド：**show usb-port**、**disable USB port**、**enable usb-port** 参照：*Cisco Secure Firewall Threat Defense コマンドリファレンス*および*Cisco Firepower 4100/9300 FXOS Command Reference*
パブリックおよびプライベートクラウド			
複数の AWS 可用性ゾーンにわたる仮想ファイアウォールクラスタの展開。	7.6.0 fault	7.6.0	AWS リージョン内の複数の可用性ゾーンに Firewall Threat Defense Virtual クラスタを展開できるようになりました。これにより、ディザスタリカバリ中に継続的なトラフィック検査と動的拡張（AWS 自動拡張）が可能になります。 *AWS への Threat Defense Virtual クラスタの展開*を参照してください。
GWLB を使用して、AWS の Firewall Threat Defense Virtual をツーアームモードで展開します。	7.6.0	7.6.0	GWLB を使用して、AWS の Firewall Threat Defense Virtual をツーアームモードで展開できるようになりました。これにより、ネットワークアドレス変換（NAT）を実行しながら、トラフィックインスペクション後にインターネットに向かうトラフィックを直接転送できます。ツーアームモードは、シングルおよびマルチ VPC 環境でサポートされます。 制限事項：クラスタリング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
デバイス管理			

機能	最小の Management Center	最小の Threat Defense	詳細
デバイステンプレート。	7.6.0	7.4.1	デバイステンプレートを使用すると、事前にプロビジョニングされた初期デバイス設定（ゼロタッチプロビジョニング）を使用して、複数のブランチデバイスを展開できます。また、インターフェイス設定が異なる複数のデバイスに設定変更を適用し、既存のデバイスから設定パラメータを複製することもできます。 制約事項：デバイステンプレートを使用して、デバイスをサイト間 VPN トポロジのスポークとして設定できますが、ハブとして設定することはできません。デバイスは、複数のハブアンドスポークサイト間 VPN トポロジの一部にすることができます。 新規/変更された画面：**[デバイス（Devices）] > [テンプレート管理（Template Management）]** サポートされるプラットフォーム：Firepower 1000/2100、Cisco Secure Firewall 1200/3100。Firepower 2100 のサポートは Firewall Threat Defense 7.4.1 ～ 7.4.x のみであることに注意してください。これらのデバイスはバージョン 7.6.0 を実行できません。 参照：テンプレートを使用したデバイス管理
オンプレミス Firewall Management Center からサポートされるシリアル番号登録（ゼロタッチプロビジョニング）。	7.6.0	Management Center がパブリックに到達できる必要がある：7.2.0 削除された制限事項：7.2.4/7.4.0	オンプレミスの Firewall Management Center からシリアル番号を使用してデバイスを登録できるようになりました。テンプレートを使用すると（デバイスに Firewall Threat Defense 7.4.1 以降が必要）、複数のデバイスを一度に登録できます。この機能は、以前はロータッチプロビジョニングと呼ばれていました。 Cisco Security Cloud が必要です。アップグレードされた Firewall Management Center の場合、Cisco Security Cloud を有効にするまで、既存の Security Cloud Control 統合が引き続き機能します。 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（ウィザード）（Device (Wizard)）]** サポートされるプラットフォーム：Firepower 1000/2100、Cisco Secure Firewall 1200/3100。Firepower 2100 のサポートは Firewall Threat Defense 7.4.1 ～ 7.4.x のみであることに注意してください。これらのデバイスはバージョン 7.6.0 を実行できません。 参照：デバイス管理

機能	最小の Management Center	最小の Threat Defense	詳細
ユーザー定義の VRF インターフェイスの場合は AAA。	7.6.0	7.6.0	デバイスの認証、許可、およびアカウンティング（AAA）は、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。デフォルトでは管理インターフェイスを使用します。 デバイスプラットフォームの設定で、VRF インターフェイスを持つセキュリティゾーンまたはインターフェイスグループを、設定済みの外部認証サーバーに関連付けることができるようになりました。 新規/変更された画面：**[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [外部認証（External Authentication）]** 参照：プラットフォームの外部認証用の仮想ルータ認識インターフェイスの有効化
[デバイス管理（Device Management）] ページで [削除（Delete）] は [登録解除（Unregister）] になりました。	7.6.0	任意	**[削除（Delete）]** メニュー選択肢の名前が [登録解除（Unregister）] に変更されました。これにより、デバイス、高可用性ペア、またはクラスタが Firewall Management Center から登録解除されても、高可用性ペアやクラスタが削除されたり、設定が消去されたりはしないことがよりわかりやすく示されるようになりました。デバイス、高可用性ペア、またはクラスタは、再登録されるまでトラフィックを継続して渡します。 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（More）]** 参照：デバイス管理
高可用性/拡張性：Firewall Threat Defense			
Cisco Secure Firewall 4200 のマルチインスタンスモード。	7.6.0	7.6.0	Cisco Secure Firewall 4200 でマルチインスタンスモードがサポートされるようになりました。 参照：Cisco Secure Firewall 3100/4200 のマルチインスタンスモード

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100/4200 の Firewall Management Center でのマルチインスタンスモード変換。	7.6.0	7.6.0	アプリケーションモードのデバイスを Firewall Management Center に登録し、CLI を使用せずにマルチインスタンスモードに変換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）]**、それから 1 つのデバイスを選択し、[その他（More）] (⋮) > [マルチインスタンスに変換（Convert to Multi-Instance）] をクリックします。 • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]**、それから複数のデバイスを選択し、**[一括アクションの選択（Select Bulk Action）]** > **[マルチインスタンスに変換（Convert to Multi-Instance）]** を選択します。 参照：デバイスのマルチインスタンスモードへの変換
Cisco Secure Firewall 3100/4200 の16 ノードクラスタ	7.6.0	7.6.0	Cisco Secure Firewall 3100 および 4200 では、最大ノード数が 8 から 16 に増加しました。 参照：Cisco Secure Firewall 3100/4200 のクラスタリング

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100/4200 クラスタの個別インターフェイスモード。	7.6.0	7.6.0	個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル IP アドレスを持ちます。各インターフェイスのメインクラスタ IP アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。アップストリームスイッチ上でロードバランシングを別途する必要があります。 制限事項：コンテナインスタンス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）] > [クラスタの追加（Add Cluster）] • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [クラスタ（Cluster）] > [インターフェイス/EIGRP/OSPF/OSPFv3/BGP（Interfaces / EIGRP / OSPF / OSPFv3 / BGP）]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）] > [MACアドレスプール（MAC Address Pool）]** 参照：Cisco Secure Firewall 3100/4200 のクラスタリングおよびアドレスプール
ノード参加時のデータノードからの MTU ping テスト	7.6.0	7.6.0	クラスターに参加したノードは、クラスター制御リンク MTU の 2 倍のパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。以前は、制御ノードのみが ping を送信していました。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。 次のコマンドが追加/変更されました。**show cluster history** 参照：「Clustering for the Secure Firewall 3100/4200」、「Clustering for Threat Defense Virtual in a Private Cloud」、「Clustering for Threat Defense Virtual in a Public Cloud」、「Clustering for the Firepower 4100/9300」
Firewall Threat Defense の高可用性は、バックアップから復元した後に自動的に再開されます。	任意	7.6.0	高可用性ペアで障害が発生したユニットを交換する場合、復元が完了してデバイスが再起動した後に、高可用性を手動で再開する必要がなくなりました。ただし引き続き、展開する前に、高可用性が再開されたことを確認することは必要です。 参照：Management Center および管理対象デバイスの復元
SD-WAN			

機能	最小の Management Center	最小の Threat Defense	詳細
SD-WAN ウィザード。	7.6.0	ハブ：7.6.0 スポーク：7.3.0	新しいウィザードを使用すると、中央の本社とリモートのブランチサイト間の VPN トンネルを簡単に設定できます。 新規/変更された画面：**[デバイス（Devices）]**>**[VPN]**>**[サイト間（Site To Site）]**>**[追加（Add）]**>**[SD-WAN トポロジ（SD-WAN Topology）]** 参照：SD-WAN ウィザードを使用した SD-WAN トポロジの設定
アクセス制御：脅威の検出とアプリケーションの識別			
Snort ML：ニューラルネットワークベースのエクスプロイト検出器。	7.6.0	Snort 3 搭載の 7.6.0	新しい Snort 3 インスペクタ snort_ml は、ニューラル ネットワークベースの機械学習（ML）を使用して既知の攻撃と 0-day 攻撃を検出します。複数のプリセットルールは必要ありません。インスペクタは HTTP イベントにサブスクライブし、HTTP URI を検出します。検出された HTTP URI は、エクスプロイト（現在は SQL インジェクションに限定されています）を検出するためにニューラルネットワークによって使用されます。新しいインスペクタは現在、最大検出を除くすべてのデフォルトポリシーで無効になっています。 新しい侵入ルール GID:411 SID:1 は、snort_ml が攻撃を検出するとイベントを生成します。このルールも現在、最大検出を除くすべてのデフォルトポリシーで無効になっています。 *Snort 3 インスペクタリファレンス*を参照してください。
信頼できるトラフィックの EVE ブロック判定をバイパスします。	7.6.0	Snort 3 を搭載するすべて	宛先ネットワークまたは EVE（暗号化された可視性エンジン）プロセス名に基づいて、既知の信頼できるトラフィックの EVE ブロック判定をバイパスできるようになりました。この方法で EVE をバイパスする接続には、新しい [EVE除外（EVE Exempted）] の理由があります。 新規/変更された画面： • アクセス制御ポリシーから例外を追加するには、詳細設定で、[暗号化された可視性エンジン（Encrypted Visibility Engine）] を編集して有効にし、[EVEスコアに基づいてトラフィックをブロック（Block Traffic Based on EVE Score）] と [例外ルールを追加（Add Exception Rule）] を有効にします。 • 統合イベントビューアから例外を追加するには、EVE にブロックされた接続を右クリックし、[EVE 例外の追加（Add EVE Exception）] を選択します。 参照：「Encrypted Visibility Engine」

機能	最小の Management Center	最小の Threat Defense	詳細
機密性の高い、復号できないトラフィックの復号を簡単にバイパスできます。	7.6.0	任意	機密性の高い、復号できないトラフィックの復号を簡単にバイパスできるようになりました。これにより、ユーザーが保護され、パフォーマンスが向上します。 新しい復号ポリシーには、事前定義されたルールが含まれるようになりました。このルールを有効にすると、機密 URL カテゴリ（金融や医療など）、復号できない識別名、および復号できないアプリケーションの復号を自動的にバイパスできます。識別名とアプリケーションは通常、復号不能な TLS/SSL 証明書のピン留めを使用するため、復号できません。 アウトバウンド復号の場合は、ポリシーの作成の一環としてこれらのルールを有効または無効化にします。インバウンド復号の場合、ルールはデフォルトで無効になっています。ポリシーを作成した後、ルール全体を編集、並べ替え、または削除できます。 新規/変更された画面：**[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** > **[復号（Decryption）]** > **[復号ポリシーの作成（Create Decryption Policy）]** 参照：復号ポリシーの作成
QUIC 復号。	7.6.0	Snort 3 搭載の 7.6.0	QUIC プロトコルで実行されているセッションに適用する復号ポリシーを設定できます。QUIC 復号はデフォルトで無効になっています。復号ポリシーごとに QUIC 復号を選択的に有効にし、QUIC トラフィックに適用する復号ルールを作成できます。QUIC 接続を復号することで、システムは侵入、マルウェア、またはその他の問題について接続を検査できます。また、アクセス コントロール ポリシーの特定の基準に基づいて、復号された QUIC 接続のきめ細かい制御とフィルタリングを適用することもできます。 復号ポリシーの [詳細設定（Advanced Settings）] が変更され、QUIC 復号を有効にするオプションが含まれるようになりました。 参照：復号ポリシーの詳細オプション

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Talos に、トラフィックを使用した Advanced Threat Hunting とインテリジェンス収集の実施を許可します。	7.6.0	Snort 3 搭載の 7.6.0	**アップグレードの影響。アップグレードすると、テレメトリが有効になります。** 脅威ハンティングテレメトリを有効にすることで、Talos（シスコの脅威インテリジェンスチーム）が脅威の状況をより包括的に理解する助けになります。この機能により、特別な侵入ルールからのイベントが Talos に送信され、攻撃分析、インテリジェンス収集、およびより優れた保護戦略の策定に役立ちます。この設定は、新規およびアップグレードされた展開ではデフォルトで有効になっています。 新規/変更された画面：[システム（System）]（⚙） > **[設定（Configuration）] > [侵入ポリシー設定（Intrusion Policy Preferences）] > [Talos脅威ハンティングテレメトリ（Talos Threat Hunting Telemetry）]** 参照：侵入ポリシーの設定
アクセス制御：アイデンティティ			

機能	最小の Management Center	最小の Threat Defense	詳細
Microsoft AD のパッシブ ID エージェント。	7.6.0	任意	この機能が導入されます。 パッシブ ID エージェントバージョン 1.1 は 7.6.0 以降と互換性があり、次の機能が追加されています。 • FQDN、IPv4、または IPv6 のいずれかを使用して、パッシブ ID エージェントから Secure Firewall Management Center または Security Cloud Control に接続できます。 • Microsoft Active Directory（AD）から IPv4 と IPv6 の両方のユーザーセッションを Firewall Management Center に送信します。 • トラブルシューティングログを zip ファイルに圧縮できます。 • パッシブ ID エージェント ソフトウェアを起動すると、前提条件のリストが表示されます。 パッシブ ID エージェントのアイデンティティソースは、Microsoft Active Directory（AD）から Firewall Management Center にセッションデータを送信します。パッシブ ID エージェントソフトウェアは、以下でサポートされています。 • Microsoft AD サーバー（Windows Server 2008 以降） • Microsoft AD ドメインコントローラ（Windows Server 2008 以降） • モニタリングするドメインに接続されている任意のクライアント（Windows 8 以降） 参照：パッシブ ID エージェントによるユーザー制御。

機能	最小の Management Center	最小の Threat Defense	詳細
アクティブまたはパッシブ認証用の Microsoft Azure AD レルム。	7.6.0	アクティブ：Snort 3 搭載の 7.6.0 パッシブ：Snort 3 搭載の 7.4.0	アクティブおよびパッシブ認証に Microsoft Azure Active Directory（AD）レルムを使用できるようになりました。 • Azure AD を使用したアクティブ認証：Azure AD をキャプティブポータルとして使用します。 • Cisco ISE を使用したパッシブ認証（バージョン 7.4.0 で導入）：Firewall Management Center は Azure AD からグループを取得し、ISE からログイン ユーザー セッション データを取得します。 SAML（セキュリティアサーションマークアップ言語）を使用して、サービスプロバイダー（認証要求を処理するデバイス）とアイデンティティ プロバイダー（Azure AD）の間に信頼関係を確立します。 **アップグレードの影響**。アップグレード前に Microsoft Azure AD レルムを設定していた場合は、パッシブ認証用に設定された SAML - Azure AD レルムとして表示されます。以前のすべてのユーザーセッションデータは保持されます。 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）] > [SAML - Azure AD]** 新規/変更された CLI コマンド：なし 参照：Microsoft Azure AD（SAML）レルムの作成。
動的属性コネクタの新しいコネクタ。	7.6.0	任意	動的属性コネクタ は、AWS セキュリティグループ、AWS サービスタグ、および Cisco Cyber Vision をサポートするようになりました。 バージョンの制限：オンプレミス動的属性コネクタ 統合の場合、バージョン 3.0 が必要です。 参照先：AWS service groups connector、AWS service tags connector、Cisco Cyber Vision connector
ISE アイデンティティソースの容易な設定。	7.6.0	7.6.0	システムは、外部 RESTful サービス（ERS）オペレータのユーザーログイン情報を使用して、Cisco ISE プライマリ認証ノード（PAN）にログインし、証明書をダウンロードし、アイデンティティソースを設定することができます。 制約事項：ISE-PIC ではサポートされていません。 参照：Cisco ISE のクイック設定
イベントロギングおよび分析			

機能	最小の Management Center	最小の Threat Defense	詳細
接続イベントに含まれる MITRE およびその他のエンリッチメント情報。	7.6.0	Snort 3 搭載の 7.6.0	接続イベントの MITRE およびその他のエンリッチメント情報により、検出された脅威のコンテキスト情報に簡単にアクセスます。これには、Talos および暗号化された可視性エンジン（EVE）からの情報が含まれます。EVE エンリッチメントの場合は、EVE を有効にする必要があります。 接続イベントには、統合イベントビューアと従来のイベントビューアの両方で使用可能な 2 つの新しいフィールドがあります。 • [MITRE ATT&CK]：進行グラフをクリックすると、戦術や手法を含む脅威の詳細の拡張ビューが表示されます。 • [その他のエンリッチメント（Other Enrichment）]：クリックすると、EVE からの情報など、利用可能なその他のエンリッチメント情報が表示されます。 新しい Talos 接続ステータス正常性モジュールは、この機能に必要な Talos を使用して Firewall Management Center の接続をモニターします。必要な特定のインターネットリソースについては、「Internet Access Requirements」を参照してください。 参照：「Connection and Security-Related Connection Event Fields」
統合イベントをイベントタイプで簡単にフィルタ処理します。	7.6.0	任意	統合イベントビューアの [検索（Search）] フィールドの下に、イベントタイプですばやくフィルタ処理できるボタンが追加されました。 参照：統合イベント
ヘルス モニタリング			
アラートなしで正常性データを収集します。	7.6.0	任意	正常性データの収集を続行しながら、ASP ドロップ、CPU、およびメモリ正常性モジュールの正常性アラートや正常性アラートサブタイプを無効にできるようになりました。これにより、正常性アラートのノイズを最小限に抑え、最も重大な問題に集中できます。 新規/変更された画面：正常性ポリシー（[システム（System）]（⚙）> **[正常性（Health）]** > **[ポリシー（Policy）]**）には、ASP ドロップ（Firewall Threat Defense のみ）、CPU、およびメモリの正常性アラートのサブタイプを有効または無効にするチェックボックスが追加されました。 参照：正常性

機能	最小の Management Center	最小の Threat Defense	詳細
デバイス登録時にデフォルトの正常性ポリシーを適用します。	7.6.0	任意	デバイス登録時に適用するデフォルトの正常性ポリシーを選択できるようになりました。[正常性ポリシー（Health Policy）]ページでは、ポリシー名によってどれがデフォルトであるかが示されます。特定のデバイスの登録後に別のポリシーを使用する場合は、そこで変更します。デフォルトのデバイス正常性ポリシーは削除できません。 新規/変更された画面：[システム（System）]（⚙）>**[正常性（Health）]**>**[ポリシー（Policy）]**>[その他（More）]（⋮）>**[デフォルトとして設定（Set as Default）]** 参照：デフォルトの正常性ポリシーの設定
展開とポリシー管理			
アクセス制御のポリシーアナライザとオプティマイザ。	Management Center 7.6.0 以降 Security Cloud Control 7.2.0 以降	任意（Any）	ポリシーアナライザとオプティマイザは、冗長ルールやシャドウルールなどの異常に対するアクセス コントロール ポリシーを評価し、検出された異常を修正するアクションを実行できます。 アクセス コントロール ポリシーアナライザおよびオプティマイザは、バージョン 7.6 以降の Firewall Management Center から直接起動できます。これには Cisco Security Cloud が必要です。バージョン 7.2 ～ 7.4 の Firewall Management Center の場合は、Security Cloud Control を使用します。 新規/変更された画面： • 有効化するには、**[統合（Integration）]**>**[Cisco Security Cloud]**>**[ポリシーアナライザとオプティマイザの有効化（Enable Policy Analyzer & Optimizer）]** をクリックします。 • ポリシーを分析するには、**[ポリシー（Policies）]**>**[アクセス制御（Access Control）]** をクリックしてポリシーを選択し、[ポリシーの分析（Analyze Policies）] をクリックします。 参照：ポリシーアナライザとオプティマイザを使用した異常の特定と修正
アップグレード			

機能	最小の Management Center	最小の Threat Defense	詳細
高可用性 Firewall Management Center のアップグレードプロセスが改善されました。	7.6.0	任意	高可用性 Firewall Management Center のアップグレードが簡単になりました。 • アップグレードパッケージを両方のピアに手動でコピーする必要がなくなりました。セットアップに応じて、サポートサイトから各ピアにパッケージを取得することも、ピア間でパッケージをコピーすることもできます。 • 両方のピアで準備状況チェックを手動で実行する必要がなくなりました。一方で実行すると、両方で実行されます。 • アップグレードを実行するための十分なディスク容量がない場合は、新しい [ディスク容量のクリーンアップ（Clean Up Disk Space）] オプションが役立ちます。 • アップグレードの前に同期を手動で一時停止したり、アップグレード後にスプリットブレインを解決したりする必要がなくなりました。システムはこれを自動的に行います。また、元のアクティブ/スタンバイロールは保持されます。 1 つのピア（スタンバイを推奨）からほとんどのアップグレードプロセスを完了できますが、実際にアップグレードを開始するには、2 番目のピアにログインする必要があります。 新規/変更された画面：[システム（System）]（⚙）>**[製品のアップグレード（Product Upgrades）]** バージョンの制限：この機能は、バージョン 7.6.0 ではなく、バージョン 7.6.0 以降からのアップグレードに適用されます。 参照：Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド

機能	最小の Management Center	最小の Threat Defense	詳細
Firewall Threat Defense およびシャーシアップグレードウィザードからアップグレード後の設定変更レポートを生成およびダウンロードします。	7.6.0	任意	アップグレードワークフローをクリアしていない場合でも、Firewall Threat Defense ウィザードおよびシャーシ アップグレード ウィザードからアップグレード後の設定変更レポートを生成およびダウンロードできるようになりました。 以前は、[高度な展開（Advanced Deploy）]画面を使用してレポートを生成し、メッセージセンターを使用してレポートをダウンロードしていました。このメソッドは引き続き使用できます。これは、複数のデバイスの変更レポートをすばやく生成する場合、またはワークフローをクリアした場合に役立ちます。 新規/変更された画面： • **[デバイス（Devices）] > [Threat Defenseアップグレード（Threat Defense Upgrade）] > [設定の変更（Configuration Changes）]** • **[デバイス（Devices）] > [シャーシアップグレード（Chassis Upgrade）] > [設定の変更（Configuration Changes）]** 参照：Firewall Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
管理			
Cisco AI Assistant for Security。	7.6.0	いずれか	Cisco AI Assistant を使用すると、デバイスやポリシーに関する質問に答えたり、ドキュメントや参考資料を照会したりできるため、ワークフローが合理化され、全体的な効率が向上します。 Cisco Security Cloud が必要です。 参照：Cisco AI Assistant for Security を使用した Threat Defense デバイスの効果的な管理

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Security Cloud が SecureX に置き換わります。	7.6.0	任意	**アップグレードの影響。アップグレード後に Cisco Security Cloud を有効にします。SecureX Firefox 拡張機能を削除します。** オンプレミスの Firewall Management Center を Cisco Security Cloud に登録すると、Cisco AI Assistant for Security、Policy Analyzer & Optimizer、Cisco XDR Automation（SecureX オーケストレーションに代わる）などの最新のサービスにアクセスできます。 Cisco Security Cloud アカウントを使用すると、インベントリを一元的に表示し、ゼロ タッチ プロビジョニング を簡単に実行し、Firewall Management Center 全体で一貫したポリシーを確立し、クラウドにイベントを送信し、脅威ハンティングと調査を強化できます。 新規/変更された画面：**[統合（Integration）] > [Cisco Security Cloud]** 廃止された画面： • **[統合（Integration）] > [SecureX]** • SecureX のリボン。Mozilla Firefox を使用している場合は、Cisco SecureX Ribbon 拡張機能を削除します。 参照：Integrate Management Center with the Cisco Security Cloud
変更管理チケットの引き継ぎ、承認ワークフローのその他の機能。	7.6.0	任意 user	別のユーザーのチケットを引き継ぐことができるようになりました。これは、チケットがポリシーに対する他の更新をブロックしており、ユーザーが使用できない場合に役立ちます。 これらの機能が承認ワークフローに含まれるようになりました：復号ポリシー、DNS ポリシー、ファイルおよびマルウェアポリシー、ネットワーク検出、証明書および証明書グループ、暗号スイートリスト、識別名オブジェクト、シンクホールオブジェクト。 参照：「Change Management」

機能	最小の Management Center	最小の Threat Defense	詳細
使いやすさの改善の報告。	7.6.0	任意	レポートにテーブルを含める場合、列の追加、削除、ソート、移動が簡単になりました。 新規/変更された画面： • **[概要（Overview）] > [レポート（Reporting）] > [レポートテンプレート（Report Templates）] > [レポートテンプレートの作成（Create Report Template）] > [テーブルビューの追加（Add Table View）] > [フィールド（Fields）] > [編集（Edit）]** • 現在のイベントビューに基づいてレポートを作成するには、[レポート（Reporting）] ではなく [レポートの作成（Create Report）] をクリックします。 参照：レポートテンプレート表形式セクションのフィールドの変更
Firewall Management Center の新しいテーマ。	7.6.0	任意	Firewall Management Center に新しい左側のナビゲーションテーマを導入しました。お試しいただくには、右上隅にあるユーザー名をクリックし、[新しいテーマ（New theme）] を選択します。また、クラシックテーマも廃止されました。クラシックテーマを使用していた場合、アップグレードによりライトテーマに切り替わります。 参照：Web インターフェイス表示の変更
シスコのニュースレターおよびその他の製品関連の情報を購読します。	7.6.0	任意	シスコからの販売および製品更新に関する情報、新しいリリース導入のニュースレター、およびその他の製品関連の情報を受信するための電子メールアドレスを提供します。各 Firewall Management Center 内部ユーザーは、独自の電子メールアドレスを持つことができます。 新規/変更された画面：[システム（System）]（⚙） > **[ユーザー（Users）] > [編集（Edit）] > [電子メールアドレス（Email Address）]**。 参照：内部ユーザーの追加または編集
URL フィルタ処理のインターネットアクセス要件を更新しました。	7.6.0	任意	**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。** システムは、URL フィルタリングデータのために *.talos.cisco.com にアクセスする必要があります。regsvc.sco.cisco.com へのアクセスは不要になりました。 この機能に必要なリソースのリスト全体については、「Internet Access Requirements」を参照してください。

機能	最小の Management Center	最小の Threat Defense	詳細
侵入ルール更新のためのインターネットアクセス要件を更新しました。	7.6.0	任意	**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。** 現在、侵入ルールをダウンロードするために、次のリソースへのアクセスが必要です。 • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com talosintelligence.com へのアクセスは不要になりました。
一部の脅威インテリジェンスのダウンロードには Security Services Exchange（SSE）の統合が必要です。	7.6.0	任意	**アップグレードの影響。非エアギャップ SLR 展開で Cisco Security Cloud 統合を有効にします。** Talos クラウドサービス は、侵入ルール、URL フィルタリングデータとルックアップ、および新しいイベントエンリッチメント機能のデータのソースになりました。セキュアなクラウド接続を維持するには、Security Services Exchange（SSE）の統合が必要です。 通常のスマートライセンスを使用している場合、Smart Software Manager（CSSM）で登録すると、SSE統合がセットアップされます。ただし、エアギャップ以外のデプロイメントで特定のライセンス予約を使用している場合、代わりに Cisco Security Cloud（**[統合（Integration）]** > **[Cisco Security Cloud]**）を有効にする必要があります。 データ共有に懸念がある場合は、イベントストレージ、Cisco Success Network、Cisco Support Diagnostics を含むすべての共有オプションを無効化します。ただし、Firewall Management Center は引き続き、選択する地域クラウドに到達できる必要があります。 • 米国：api-sse.cisco.com • EU：api.eu.sse.itd.cisco.com • APJC：api.apj.sse.itd.cisco.com • オーストラリア：api.au.sse.itd.cisco.com • インド：api.in.sse.itd.cisco.com エアギャップ展開では、サポートされていないイベントエンリッチメントを除き、脅威インテリジェンスを手動で更新することに注意してください。
パフォーマンス			

機能	最小の Management Center	最小の Threat Defense	詳細
Cisco Secure Firewall 3100/4200 のハードウェア DTLS 1.2 暗号化アクセラレーション。	7.6.0	Snort 3 搭載の 7.6.0	Cisco Secure Firewall 3100/4200 は、DTLS 1.2 暗号化アクセラレーションと出力最適化をサポートするようになりました。これにより、DTLS 暗号および復号トラフィックのスループットが向上します。これは、新しいデバイスとアップグレードされたデバイスで自動的に有効になります。無効にするには、FlexConfig を使用します。 新規/変更された FlexConfig コマンド：**flow-offload-dtls**、**flow-offload-dtls egress-optimization**、**show flow-offload-dtls** 参照：DTLS 暗号化アクセラレーション
オブジェクトグループの検索パフォーマンスの強化。	7.6.0	任意	オブジェクトグループの検索が高速になり、使用する CPU リソースが少なくなりました。 新しい CLI コマンド：**clear asp table network-object**、**show asp table network-object**、**debug acl ogs** 変更された CLI コメント（拡張出力）：**packet-tracer**、**show access-list**、**show object-group** 参照：オブジェクトグループ検索の構成および *Cisco Secure Firewall Threat Defense* コマンドリファレンス
トラブルシューティング			
CPU とルールプロファイラを使用して Snort 3 のパフォーマンスの問題をトラブルシュートします。	7.6.0	Snort 3 搭載の 7.6.0	新しい CPU とルールプロファイラは、Snort 3 のパフォーマンスの問題のトラブルシュートに役立ちます。以下をモニタリングできるようになりました。 • Snort 3 モジュール/インスペクタがパケットを処理するために要した CPU 時間。 • 各モジュールが消費している CPU リソース（Snort 3 プロセスによって消費された合計 CPU と比較）。 • Snort 3 が CPU を大量に消費している時に、パフォーマンスが不十分なモジュール。 • パフォーマンスが不十分な侵入ルール。 新規/変更された画面：**[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[Snort 3 プロファイリング（Snort 3 Profiling）]** プラットフォームの制限：コンテナインスタンスではサポートされていません。 参照：Advanced Troubleshooting for the Secure Firewall Threat Defense Device

機能	最小の Management Center	最小の Threat Defense	詳細
追加の Firewall Threat Defense のトラブルシューティング syslog を受信し、それらを統合イベントとして表示します。VPN障害対応 syslog が移動されました。	7.6.0	Snort 3 を搭載するすべて	Firewall Threat Defense を設定して、（VPN トラブルシューティング syslog だけではなく）すべてのデバイス トラブルシューティング syslog を Firewall Management Center に送信できるようになりました。 新規/変更された画面： • デバイスのトラブルシューティング syslog を Firewall Management Center に送信するには、Firewall Threat Defense プラットフォーム設定を使用します：**[デバイス（Devices）]** > **[プラットフォーム設定（Platform Settings）]** > **[Syslog]** > **[Cisco Secure Firewall Management Centerへのログイン（Logging to Secure Firewall Management Center）]** の順にクリックします。 • すべてのデバイス トラブルシューティング syslog を表示する方法は、**[デバイス（Devices）]** > **[VPNトラブルシューティング（VPN Troubleshooting）]** が **[デバイス（Devices）]** > **[VPN]** > **[トラブルシューティング（Troubleshooting）]** に置き換えられました。 • 他のイベントとの関連でデバイスのトラブルシューティング syslog を表示するために、**[分析（Analysis）]** > **[統合イベント（Unified Events）]** に [トラブルシュートイベント（Troubleshoot Events）] タイプを追加しました。 参照：Configure Syslog Logging for Threat Defense Devices および View Troubleshooting Syslogs in the Secure Firewall Management Center
接続ベースのトラブルシューティングのアプリケーション検出デバッグログ。	7.6.0	Snort 3 搭載の 7.6.0	接続ベースの障害対応では、アプリケーションディテクタからデバッグログを収集できるようになりました。 新規/変更された CLI コマンド：**debug packet-module appid** は、アプリケーションディテクタのデバッグログのシビラティレベルを有効化して設定します。3（エラー）、4（注意）、または 7（デバッグ）を選択できます。 参照：接続ベースのトラブルシューティングおよび*Cisco Secure Firewall Threat Defense コマンドリファレンス*

機能	最小の Management Center	最小の Threat Defense	詳細
パケットトレーサの改善。	7.6.0	内容に応じて異なる。	パケットトラッカーの改善により、以下が可能になります。 • アイデンティティ トレース データをキャプチャして再生します（Firewall Threat Defense 7.6.0 と Snort 3 が必要）。 • NAT が設定されたデバイスでパケットトレースデータを再生します。 • より現実的なシミュレーションのために、パケットの実際のタイミングを模倣したパケットトレースデータを再生します。 • パケットトレースデータを PCAP ファイルとして保存します。このファイルは、Wireshark などのサードパーティ製ツールを使用して表示できます。 新規/変更されたコマンド： • タイムスタンプオプションを有効にするには、**packet-tracer** コマンドで **honor-timestamp** キーワードを使用します：**packet-tracer input***ifc_name* **pcap***pcap_filename* [**honor-timestamp**] • デバイスで生成されたパケットトレースデータを PCAP ファイルの一部として保存するには、**show packet tracer** コマンドで **export-pcapng** キーワードを使用します：**show packet-tracer pcap trace** [**export-pcapng**] 参照：パケットトレーサ および *Cisco Secure Firewall Threat Defense* コマンドリファレンス
Cisco Success Network と Cisco Support Diagnostic は、デフォルトで有効になっています。	7.6.0	任意	**アップグレードの影響。アップグレードでは、Cisco Success Network と Cisco Support Diagnostics が選択されます。** Cisco Success Network と Cisco Support Diagnostics は、オプトインではなくオプトアウトされるようになりました。以前にオプトアウトしていた場合は、アップグレードによって変更されます。また、Firewall Management Center を Cisco Smart Software Manager（CSSM）に登録するときにオプトアウトすることはできなくなりました。 **[統合（Integration）] > [Cisco Security Cloud] > [Cisco Security Cloud サポート（Cisco Security Cloud Support）]**で引き続きオプトアウトできます。 参照：Integrate Management Center with the Cisco Security Cloud
廃止された機能			

機能	最小の Management Center	最小の Threat Defense	詳細
サポート終了：Firepower 2110、2120、2130、2140。	—	7.6.0	Firepower 2110、2120、2130、または 2140 ではバージョン 7.6 以降は実行できません。 新しい Firewall Management Center は古いデバイスを管理できますが、バージョン 7.6 のドキュメントには、バージョン 7.6 の Firewall Threat Defense でサポートされている機能のみが記載されています。古いデバイスでのみサポートされている機能については、ご使用の Firewall Threat Defense のバージョンに一致する Firewall Management Center のガイドを参照してください。
管理サポートの終了：ASA FirePOWER および NGIPSv。	7.6.0	—	バージョン 7.6 以降の Firewall Management Center では、従来のデバイス（Cisco ASA FirePOWER および NGIPSv）を管理できません。クラシックデバイスはバージョン 7.0 より上にアップグレードすることはできないためです。また、バージョン 7.6 の Firewall Management Center では、バージョン 7.1 までしかさかのぼってデバイスを管理できません。 新規/変更された画面：新規およびアップグレードされた Firewall Management Center では、Classic 固有の設定と画面が削除されます。これには、プラットフォーム設定、NAT、syslog ロギング、ライセンスなどが含まれます。場合によっては、デバイスタイプの選択から始める必要がないため、Firewall Threat Defense の設定を迅速に作成できます。
廃止：Firewall Management Center にローカルに保存されたレポートのバックアップ。	7.6.0	任意	ローカルに保存されたレポートはバックアップされなくなりました。レポートは、安全なリモートロケーションに保存する必要があります。
廃止：デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	7.6.0	7.6.0	Firewall Threat Defense CLI を使用して、管理ネットワークを介してデバイス間でアップグレードパッケージをコピーすることはできなくなりました。Firewall Management Center とそのデバイス間の帯域幅が限られている場合は、内部 Web サーバーからアップグレードパッケージを直接取得するようにデバイスを設定します。 廃止された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	最小の Management Center	最小の Threat Defense	詳細
サポート終了：クラウド提供型 Firewall Management Center でサポートされているすべての Firewall Threat Defense デバイスによる分析専用機能。	いずれか	7.2.0	クラウド提供型 Firewall Management Center とオンプレミスの分析専用 Firewall Management Center を使用してバージョン 7.0.x デバイスを共同管理している場合は、古いデバイスを 7.2 以降にアップグレードするか、それらを交換または削除するまで、Firewall Management Center をバージョン 7.6 にアップグレードできません（アップグレードすると、バージョン 7.6 デバイスを管理可能になります）。 参照： *Cisco Secure Firewall Management Center 互換性ガイド*

バージョン 7.6.x の Firewall Device Manager の機能

表 5 : バージョン *7.6.x* の *Firewall Device Manager* の機能

機能	説明
プラットフォーム機能	
Cisco Secure Firewall 1200	Cisco Secure Firewall 1200 が導入されました。これには、次のモデルが含まれます。 • Cisco Secure Firewall 1210CX（1000BASE-T ポート X 8） • Cisco Secure Firewall 1210CP（1000BASE-T ポート X 8、ポート 1/5 ～ 1/8 で Power over Ethernet（PoE）をサポート） • Cisco Secure Firewall 1220CX（1000BASE-T ポート X 8、SFP+ ポート X 2） *Cisco Secure Firewall 1210CE, 1210CP, and 1220CX Hardware Installation Guide*を参照してください。
OpenStack 向けの Firewall Threat Defense Virtual。	Firewall Threat Defense Virtual は OpenStack をサポートするようになりました。 バージョンの制限：バージョン 7.6.4 が必要です。
Firepower 1000 および Cisco Secure Firewall 3100 の前面パネル USB-A ポートを無効にします。	Firepower 1000 および Cisco Secure Firewall 3100 の前面パネル USB-A ポートを無効にできるようになりました。デフォルトでは、ポートは有効になっています。 新規/変更された CLI コマンド：**system support usb show**、**system support usb port disable**、**system support usb port enable** *Cisco Secure Firewall Threat Defense コマンドリファレンス*を参照してください。

機能	説明
AWS 展開の IMDSv2 サポート。	AWS 向けの Threat Defense は、IMDSv1 よりもセキュリティが向上したインスタンス メタデータ サービス バージョン 2（IMDSv2）をサポートするようになりました。AWS でインスタンス メタデータ サービスを有効にすると、デフォルトは IMDSv2 Optional モードのままですが、IMDSv2 Required を選択することをお勧めします。また、アップグレードされたインスタンスに切り替えることをお勧めします。 Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。
サポート終了：Firepower 2110、2120、2130、2140。	Firepower 2110、2120、2130、または 2140 ではバージョン 7.6 以降は実行できません。
ファイアウォールと IPS の機能	
オブジェクトグループの検索パフォーマンスの強化。	オブジェクトグループの検索が高速になり、使用するリソースが少なくなりました。 新しい CLI コマンド：**clear asp table network-object**、**show asp table network-group** 変更された CLI コメント（拡張出力）：**debug acl logs**、**packet-tracer**、**show access-list**、**show object-group** *Cisco Secure Firewall Threat Defense* コマンドリファレンスを参照してください。
管理およびトラブルシューティングの機能	
URL フィルタ処理のインターネットアクセス要件を更新しました。	**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。** システムは、URL フィルタリングデータのために *.talos.cisco.com にアクセスする必要があります。regsvc.sco.cisco.com へのアクセスは不要になりました。
侵入ルール更新のためのインターネットアクセス要件を更新しました。	**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。** 現在、侵入ルールをダウンロードするために、次のリソースへのアクセスが必要です。 • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com talosintelligence.com へのアクセスは不要になりました。

機能	説明
Firewall Device Manager のカナダフランス語の翻訳。	Firewall Device Manager には、英語、中国語、日本語、および韓国語に加えて、カナダフランス語バージョンが含まれています。ブラウザの言語としてカナダフランス語を選択する必要があります。他のタイプのフランス語を選択しても、フランス語バージョンは表示されません。 参照：Viewing Pages in Languages Other Than English [英語]
すべての RADIUS 応答に Message-Authenticator 属性が必要です。	**アップグレードの影響。Firepower 4100/9300 の場合、Firewall Threat Defense をアップグレードする前に、FXOS の互換性を確認してください。Firewall Threat Defense のアップグレード後、既存のサーバーに対してオプションを有効にします。** すべての RADIUS 応答で Message-Authenticator 属性を要求できるようになりました。この変更により、Firewall Threat Defense VPN ゲートウェイで、RA VPN 用でもデバイス自体へのアクセス用でも、RADIUS サーバーからのすべての応答を安全に検証できるようになります。 新しい RADIUS サーバーでは、[すべてのRADIUS応答にメッセージオーセンティケータを要求（Require Message-Authenticator for all RADIUS Responses）] オプションがデフォルトで有効になっています。既存のサーバーでも有効にすることを推奨します。無効にすると、ファイアウォールが攻撃にさらされる可能性があります。 新しい CLI コマンド：**message-authenticator-required** バージョンの制限：バージョン 7.0.7、7.2.10、7.4.3、7.6.1、または 7.7 以降が必要です。Firepower 4100/9300 の場合、FXOS のアップグレードが必要になる場合があります。最小ビルドについては、『*Cisco Secure Firewall Threat Defense 互換性ガイド*』を参照してください。
パフォーマンス機能	
Cisco Secure Firewall 3100 のハードウェア DTLS 1.2 暗号化アクセラレーション。	Cisco Secure Firewall 3100 は、DTLS 1.2 暗号化アクセラレーションと出力最適化をサポートするようになりました。これにより、DTLS暗号および復号トラフィックのスループットが向上します。これは、新しいデバイスとアップグレードされたデバイスで自動的に有効になります。無効にするには、FlexConfig を使用します。 新規/変更された FlexConfig コマンド：**flow-offload-dtls**、**flow-offload-dtls egress-optimization**、**show flow-offload-dtls** 参照：Advanced Configuration [英語]

アップグレードの影響がある機能

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。望ましくない結果を避けるために、アップグレードの前または後にアクションを実行する必要がある場合、機能がアップグレードに影響を与える可能性もあります。たとえば、設定を変更する必要がある場合などです。

重要 選択したバージョンの最新のメンテナンスリリースに直接移動することで、アップグレードなどの影響を最小限に抑えます。アップグレードターゲットの選択 （38 ページ）を参照してください。

Firewall Management Center のアップグレードの影響がある機能

この表には、Firewall Management Center のアップグレードの影響を受ける可能性のある機能とその説明へのリンクが示されています。最初の列は現在のバージョンで、リンクはその機能が最初に導入されたバージョンを示しています。

表 *6 : Firewall Management Center* のアップグレードの影響がある機能

現在のバージョン	アップグレードの影響がある機能
7.4.x 以前	• Cisco Talos に、トラフィックを使用した Advanced Threat Hunting とインテリジェンス収集の実施を許可します。（7.6.0） • Cisco Security Cloud が SecureX に置き換わります。（7.6.0） • URL フィルタ処理のインターネットアクセス要件を更新しました。（7.6.0） • 侵入ルール更新のためのインターネットアクセス要件を更新しました。（7.6.0） • 一部の脅威インテリジェンスのダウンロードには Security Services Exchange（SSE）の統合が必要です。（7.6.0） • Cisco Success Network と Cisco Support Diagnostic は、デフォルトで有効になっています。（7.6.0）
7.6.0 7.4.0 ～ 7.4.2 7.2.0 ～ 7.2.9 7.1.x	• 新しい Cisco AMP クラウド接続方式。（7.7.0）
7.4.0 以前	• Firewall 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）

現在のバージョン	アップグレードの影響がある機能
7.4.0 7.3.x 7.2.5 以前	• Firewall Management Center 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。（7.2.6） • 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。（7.2.6） • 廃止：メンテナンスリリースのスケジュール済みダウンロード。（7.2.6）
7.4.0 7.3.x 7.2.0 ～ 7.2.5 7.1.x 7.0.5 以前	• Web 分析プロバイダーを更新済み。（7.0.6）
7.3.x 以前	• Firewall Management Center の Web インターフェイスから Firewall Threat Defense デバイスを NetFlow エクスポータとして設定します。（7.4.0）
7.3.0 ～ 7.3.1 7.2.0 ～ 7.2.3 7.1.x 7.0.5 以前	• メモリが少ない Snort 2 デバイス用の小規模 VDB。（7.0.6）
7.2.x 以前	• Firewall Management Center の Web インターフェイスから BGP の BFD を設定。（7.3.0）
7.2.0 ～ 7.2.9 7.1.x 7.0.7 以前	• スマートライセンスのインターネットアクセス要件を更新しました。（7.0.8）
7.2.0 ～ 7.2.3 7.1.0 ～ 7.1.0.2 7.0.4 以前	• CA バンドルの自動更新。（7.0.5）
7.1.x 以前	• Firewall Management Center の Web インターフェイスから VXLAN を設定します。（7.2.0） • Firewall Management Center の Web インターフェイスから EIGRP を設定します。（7.2.0）

Firewall Management Center を使用する Firewall Threat Defense のアップグレードの影響がある機能

この表には、Firewall Management Center を使用する Firewall Threat Defense のアップグレードの影響を受ける可能性のある機能とその説明へのリンクが一覧表示されています。最初の列は現在のバージョンで、リンクはその機能が最初に導入されたバージョンを示しています。

表 *7 : Firewall Management Center* を使用する *Firewall Threat Defense* のアップグレードの影響がある機能

現在のバージョン	アップグレードの影響がある機能
7.6.0 7.4.0 ～ 7.4.2 7.3.x 7.2.9 以前	• すべての RADIUS 応答に Message-Authenticator 属性が必要です。（7.0.7）
7.4.0 ～ 7.4.1 7.3.x 7.2.9 以前	• 非対称トラフィック処理。（7.2.9）
7.4.0 以前	• 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） • 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） • 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）
7.3.x 以前	• 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） • 機密データの検出とマスキング。（7.4.0） • 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）
7.2.x 以前	• Firewall Threat Defense のアップグレード完了後の Snort 3 への自動アップグレードはオプションではなくなりました。（7.3.0） • Cisco Secure Firewall 3100 の統合アップグレードおよびインストール パッケージ。（7.3.0） • Snort 3 デバイスの NetFlow サポート。（7.3.0）
7.2.0 ～ 7.2.3 7.1.0 ～ 7.1.0.2 7.0.4 以前	• CA バンドルの自動更新。（7.0.5）

現在のバージョン	アップグレードの影響がある機能
7.1.x 以前	• GCP 対応 Firewall Threat Defense Virtual の自動スケール。 （7.2.0）

Firewall Device Manager を使用する Firewall Threat Defense のアップグレードの影響がある機能

表 *8 : Firewall Device Manager* を使用する *Firewall Threat Defense* のアップグレードの影響がある機能

ターゲットバージョン	機能
7.6.1 ～ 7.6.x	• すべての RADIUS 応答に Message-Authenticator 属性が必要です。
7.6.0 以降	• URL フィルタ処理のインターネットアクセス要件を更新しました。 • 侵入ルール更新のためのインターネットアクセス要件を更新しました。
7.4.1 以降	• 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。 • 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。 • 機密データの検出とマスキング。 • 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。 • デフォルトの NTP サーバーが更新されました。
7.3.0 以降	• SSL 復号ポリシーでの TLS 1.3 のサポート、および復号できない接続の設定可能な動作。 • Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。 • CA バンドルの自動更新。

アップグレードのガイドライン

これらのリリースノートには、各リリースに固有のアップグレードの警告とガイドラインが含まれています。また、アップグレードの影響を受ける機能とバグも確認する必要があります。

時間とディスク容量の要件に関する一般的な情報、およびトラフィックフローや検査の中断を含む、アップグレード中のシステム動作の詳細については、アップグレードガイドを参照してください：支援が必要な場合 （214 ページ）。

Firewall Management Center のアップグレードガイドライン

表 *9 : Firewall Management Center* のアップグレードガイドライン

現在のバージョン	ガイドライン	詳細
任意	—	現在このバージョンには既知の問題がありますが、アップグレードに影響する未解決の問題と機能は引き続き確認してください。

Firewall Management Center を使用した Firewall Threat Defense のアップグレードガイドライン

表 *10 : Firewall Threat Defense* のアップグレードガイドライン

現在のバージョン	ガイドライン	詳細
7.4.x 以前	サブインターフェイスで VLAN 1 を使用している場合、Firepower 1010 をアップグレードしないでください	組み込みスイッチのあるモデルでは、VLAN 1 を使用してサブインターフェイスを作成できません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。Firepower 1010 をバージョン 7.6 以降にアップグレードし、VLAN 1 をサブインターフェイスに割り当てた場合、まず、サブインターフェイスの VLAN ID を新しい VLAN に変更する必要があります。アップグレード後、存在する場合は、VLAN 1 がサブインターフェイスから削除されます。

Firewall Device Manager を使用した Firewall Threat Defense のアップグレードガイドライン

表 *11 : Firewall Threat Defense* のアップグレードガイドライン

現在のバージョン	ガイドライン	詳細
7.4.x 以前	サブインターフェイスで VLAN 1 を使用している場合、Firepower 1010 をアップグレードしないでください	組み込みスイッチのあるモデルでは、VLAN 1 を使用してサブインターフェイスを作成できません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。Firepower 1010 をバージョン 7.6 以降にアップグレードし、VLAN 1 をサブインターフェイスに割り当てた場合、まず、サブインターフェイスの VLAN ID を新しい VLAN に変更する必要があります。アップグレード後、存在する場合は、VLAN 1 がサブインターフェイスから削除されます。

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

ほとんどの場合、FXOS のメジャーバージョンで最新のビルドを使用することを推奨します。

リリース固有のFXOSアップグレードの警告とガイドライン、およびアップグレードの影響を受ける機能とバグについては、現在のバージョンとターゲットバージョンの間のすべてのリリースノートを参照してください：http://www.cisco.com/go/firepower9300-rns。

アップグレードパス

アップグレードパスとその順序の計画は、大規模な展開、高可用性/クラスタリング、マルチホップアップグレード、およびシャーシ、ホスティング環境、その他のアップグレードを調整する必要がある状況では特に重要です。これらのシナリオと、アップグレードの取り消しおよびアンインストールに関する情報は、アップグレードガイドの「支援が必要な場合（214ページ）」で詳細が説明されています。

アップグレードターゲットの選択

可能な限り最新のバージョン7.6リリースに直接移行することで、アップグレードなどの影響を最小限に抑えます。これは、機能、拡張機能、および重要な修正が、リリース日ではなくバージョン番号で先行する「今後」のリリースをスキップする場合があるためです。たとえば、メジャーバージョンA内で最新の場合、ドットゼロバージョンBにアップグレードすると、機能や修正が廃止される可能性があります。

最新のリリースに移動できない場合、少なくとも現在のバージョンがターゲットバージョンより前の日付でリリースされたことを確認してください。次の表で、現在のバージョンがターゲットバージョンの横に表示されていることを確認します。表示されていない場合は、より新しいターゲットを選択します。

表 *12*：バージョン *7.6.x* より前にリリース済み（日付別）

ターゲットバージョン		現在のバージョン：自分のバージョンがリストされていることを確認してください。				
		7.1 から	**7.2** から	**7.3** から	**7.4** から	**7.6** から
7.6.5 へ	2026-02-17	7.1.0	7.2.0 ～ 7.2.12	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.6	7.6.0 ～ 7.6.4
7.6.4 へ	2026-01-07	7.1.0	7.2.0 ～ 7.2.10	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.4	7.6.0 ～ 7.6.3
7.6.3 へ	2025-10-23	7.1.0	7.2.0 ～ 7.2.10	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.3	7.6.0 ～ 7.6.2
7.6.2 へ	2025-08-11	7.1.0	7.2.0 ～ 7.2.10	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.2	7.6.0 ～ 7.6.1
7.6.1 へ	2025-06-02	7.1.0	7.2.0 ～ 7.2.10	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.2	7.6.0

ターゲットバージョン		現在のバージョン：自分のバージョンがリストされていることを確認してください。				
		7.1 から	**7.2** から	**7.3** から	**7.4** から	**7.6** から
7.6.0 へ	2024 年 9 月 16 日	7.1.0	7.2.0 ～ 7.2.8	7.3.0 ～ 7.3.1	7.4.0 ～ 7.4.2	—

パッチが適用された展開のアップグレード

パッチ/脆弱性（4桁）リリースに含まれる重要な修正は、今後のリリースをスキップすることもできます。これらの重要な修正に依存している場合は、ターゲットバージョンにそれらが含まれていることを確認してください。リリース日の完全なリストについては、*Cisco Secure Firewall Management Center* の新機能（リリース別）または*Cisco Secure Firewall* デバイスマネージャの新機能（リリース別）を参照してください。

サポートされているアップグレードおよびダウングレード

このセクションでは、アップグレードおよびダウングレードの機能について説明します。以下の内容も参照してください。

- アップグレードターゲットの選択については、「アップグレードターゲットの選択 （38 ページ）」を参照してください。
- アップグレードおよびダウングレードの手順（一般ガイドライン、ベストプラクティス、障害対応など）については、現在実行しているバージョンのアップグレードガイド（https://www.cisco.com/go/ftd-upgrade）を参照してください。

サポートされるアップグレード

次の表に、Firewall Management Center および Firewall Threat Defense ソフトウェアでサポートされている直接アップグレードを示します。

（注） パッチ（4桁リリース）を除く任意のリリースに直接アップグレードできます。以前のメジャーリリースまたはメンテナンスリリースからパッチに直接アップグレードすることはできません。パッチを適用したデバイス（4桁目）はパッチを適用していない Firewall Management Center で管理できますが、完全にパッチを適用した展開では拡張テストが実施されます。

表 *13*：サポートされる直接アップグレード

現在のバージョン	対象ソフトウェアバージョン							
	10.x へ	**7.7**	**7.6**	**7.4** *	**7.3**	**7.2**	**7.1**	**7.0**
10.x から	可	—	—	—	—	—	—	—

現在のバージョン	対象ソフトウェアバージョン							
	10.x へ	**7.7**	**7.6**	**7.4 ***	**7.3**	**7.2**	**7.1**	**7.0**
7.7 から	可	可	—	—	—	—	—	—
7.6 から	可	可	可	—	—	—	—	—
7.4 から	可	可	可	可	—	—	—	—
7.3 から	可	可	可	可	可	—	—	—
7.2 から	—	可	可	可	可	可	—	—
7.1 から	—	—	可	可	可	可	可	—
7.0 から	—	—	—	可	可	可	可	可
6.4 から	—	—	—	—	—	—	—	可

* Firewall Threat Defense バージョン 7.4.0 は、Cisco Secure Firewall 4200 でのみ新規インストールとして利用可能です。以前のバージョンに含まれている重要な機能、拡張機能、および重要な修正が削除されています。より新しいリリースにアップグレードします。

Firepower 4100/9300 のアップグレードに対応する FXOS バージョン

Firepower 4100/9300 の場合、この表には、対応する FXOS バージョンがリストされています。シャーシのアップグレードが必要な場合、Firewall Threat Defense のアップグレードはブロックされます。ほとんどの場合、各バージョンで最新のビルドを推奨します。最小ビルドについては、「*Cisco Secure Firewall Threat Defense* 互換性ガイド」を参照してください。

表 *14 : Firepower 4100/9300* のアップグレードに対応する *FXOS* バージョン

ターゲット Firewall Threat Defense バージョン	最小 FXOS バージョン
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1 ～ 7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1

ターゲット Firewall Threat Defense バージョン	最小 FXOS バージョン
6.7	2.9.1
6.6	2.8.1
6.4	2.6.1

サポートされるダウングレード

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、以前のバージョンに戻せることがあります。一般的な情報、特に以前のバージョンに戻ることがサポートされないか推奨されない一般的なシナリオに関する情報については、次のアップグレードガイドを参照してください：https://cisco.com/go/ftd-upgrade。

バグ

以前のリリースのバグについては、該当するバージョンのリリースノートを参照してください。クラウド展開については、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 メンテナンスリリースまたはパッチの未解決のバグのは記載していません。

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。サポート契約がある場合は、Cisco バグ検索ツールを使用して最新のバグリストを取得できます。

バージョン 7.6.0 で未解決のバグ

表の最終更新日：2024 年 9 月 19 日

表 *15*：バージョン *7.6.0* で未解決のバグ

不具合 ID	タイトル
CSCwm40854	MI アプリでの FTD-HA ペア解除の失敗
CSCwk48461	無名のインターフェイス/EtherChannel が存在する場合、Secure Firewall 1200 で 1024 サブインターフェイスを作成できない
CSCwm38714	変更管理：セキュリティゾーンがウィザードにインラインで追加される場合、SD-WAN トポロジの保存でエラーが発生する

不具合 ID	タイトル
CSCwm44162	グローバル デバイス ウィザード ページを介して追加した子ドメインテンプレートが機能しない
CSCwm46752	BGP が有効である場合、Cisco Secure Firewall 3100 L3 クラスタで設定の編集が失敗する
CSCwm44656	デバイスのオンボーディング中にエラーメッセージ「インターフェイス 'management0' にリンクがありません（Interface 'management0' has no link）」が表示される
CSCwk90798	FMC HA ロールスイッチのセカンダリ FMC がイベント設定を取得せず、FTD で脅威ハンティングが失われる
CSCwk36770	FMC - SDWAN：複数のトポロジ間での同じ IKE アイデンティティの問題
CSCwk33511	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
CSCwm47187	SAML CP ルールで使用されているインターフェイスの場合、インターフェイスの nameif を変更した後にポリシー展開が常に失敗する
CSCwm47308	クラスタ中断後に Cisco Secure Firewall クラスタのデータノードでポリシー展開が常に失敗する
CSCwk76563	SDWAN：異なるコミュニティの別のトポロジに同じスポークがあると、ルートの再配布で問題が発生する
CSCwm48550	Cisco Secure Firewall 1200：SMA が次のエラーを報告した：Lina は開始されたが、まだ実行されていない（Lina has started, but is not yet running）
CSCwm51467	[SSLサーバー（SSL Server）] チェックボックスが、[デバイス（Device）] -> [証明書（Certificates）] -> [新しい証明書の追加（Add New Cert）] のデフォルトの新しいテーマにのみ表示されない
CSCwm34180	ポートチャネル/ポートチャネル サブインターフェイスのトラフィックがデバイステンプレート登録で機能しない
CSCwj81646	Snort のリロード時に UDP スループットが大きく変化する
CSCwk98275	最初のスケジュール済みバックアップが完了した後に、次の即時バックアップをトリガーできない

バージョン 7.6.5 で解決済みのバグ

表の最終更新日：2026-03-04

表 *16*：バージョン *7.6.5* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwr96008	Cisco Secure Firewall Management Center ソフトウェアの認証バイパスの脆弱性

バージョン 7.6.4 で解決済みのバグ

表の最終更新日：2026-03-04

表 *17*：バージョン *7.6.4* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwb67583	SSL VPN と HTTP サーバーが同じポートで設定されている場合の ASDM のアクセスに関する問題
CSCwf97953	7.2.0 ビルド 82 から 7.2.5 ビルド 203 にアップグレードした後、FTD が HA に再参加できない
CSCwj69533	FDM 使用時にデフォルトのトンネルグループで認証方式を変更できない
CSCwk22959	問題の概要：デフォルト以外の一部の TLS サーバー構成では
CSCwk75030	6.3 より前の Linux カーネルでの IPv6 実装では、net/ipv6/
CSCwk75032	1.21.3 より前の MIT ケルベロス 5（別名 krb5）では、攻撃者は
CSCwk75033	1.21.3 より前の MIT ケルベロス 5（別名 krb5）では、攻撃者は
CSCwk75035	Apache HTTP サーバー 2.4.59 以前のコアの脆弱性
CSCwk75036	Apache HTTP サーバー 2.4.59 の mod_proxy におけるヌルポインタ参照
CSCwk88981	CCM ID LTS21-RC216-109
CSCwk93503	スタンバイ FMC に VDB の更新をインストールするために、プライマリ FMC で約 400 のタスクが作成された
CSCwm35624	object-group と他のプレーン ACL が含まれる 1 つの AC ルールでブート時間が長くなる
CSCwm49153	Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSH サーバー リソースにおける DoS の脆弱性

不具合 ID	タイトル
CSCwm66841	UI の [センサーリスト（Sensor List）]/[センサー管理（Sensor Management）] ページで、FTDHA バックアップタスクのスイッチロールとバックアップ名に不一致がある
CSCwm71529	cdFMC テナントで hms プロセスが 20GB のメモリを消費している
CSCwm83088	Cisco FXOS および UCS Manager ソフトウェアに蓄積されたクロスサイトスクリプティングの脆弱性
CSCwn06623	OLE2 rijndaelDecrypt でのヒープ バッファ オーバーフローの評価
CSCwn15505	アプリケーションインスタンスが「開始」状態でスタックしている BS/QP での 2.17 の Lina コアの監視
CSCwn55253	FMC GUI で、バックアップに使用されるリモートストレージのユーザー名に "@" が使用できない
CSCwn58226	CVE-2024-46826：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58265	CVE-2024-47707：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58273	CVE-2024-47728：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58285	CVE-2024-47745：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58322	CVE-2024-49888：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58376	CVE-2024-49927：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58383	CVE-2024-49934：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn62998	CVE-2024-49974：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63021	CVE-2024-49996：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63027	CVE-2024-50002：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63035	CVE-2024-50010：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63051	CVE-2024-50038：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63062	CVE-2024-50055：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63065	CVE-2024-50058：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63070	CVE-2024-50067：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63075	CVE-2024-50082：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63084	CVE-2024-50095：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn63112	CVE-2024-50138：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63114	CVE-2024-50142：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63129	CVE-2024-50154：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63157	CVE-2024-50191：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63162	CVE-2024-50194：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63163	CVE-2024-50195：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn69076	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの OSPF DoS 脆弱性
CSCwn69078	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの OSPF DoS 脆弱性
CSCwn69079	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの OSPF メモリ枯渇の脆弱性
CSCwn69963	unicorn zlib ライブラリで報告された CVE に対処
CSCwn73801	Cisco Secure Firewall Threat Defense ソフトウェア TLS と Snort 3 検出エンジンによるサービス妨害の脆弱性
CSCwn78991	FMC レガシー UI で、ACL の過去の時間範囲オブジェクトを作成できる
CSCwn86187	FTD ネイティブ：Radius と同じユーザーを使用すると、LDAP 設定を FTD に展開できない
CSCwn94711	CVE-2021-47036：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94729	CVE-2021-47199：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94753	CVE-2021-47455：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94754	CVE-2021-47469：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94767	CVE-2021-47552：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94794	CVE-2023-52476：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94836	CVE-2023-52679：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94839	CVE-2023-52698：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94850	CVE-2023-52757：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94860	CVE-2023-52845：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn94876	CVE-2024-12084：rsync：ヒープベースのバッファオーバーフローの脆弱性が発見された...
CSCwn94880	CVE-2024-12085：rsync：rsync に欠陥が見つかり...
CSCwn94882	CVE-2024-12086：rsync：rsync に欠陥が見つかった。これにより...
CSCwn94883	CVE-2024-12087：rsync：rsync にパストラバーサルの脆弱性が存在...
CSCwn94884	CVE-2024-12088：rsync：rsync に欠陥が見つかった。次を使用すると...
CSCwn94885	CVE-2024-12747：rsync：rsync に欠陥が見つかった。この脆弱性は...
CSCwn94897	CVE-2024-26663：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94906	CVE-2024-26704：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94911	CVE-2024-26739：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94943	CVE-2024-26928：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94947	CVE-2024-27388：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94968	CVE-2024-35863：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94969	CVE-2024-35864：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94972	CVE-2024-35867：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94974	CVE-2024-35868：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94977	CVE-2024-35896：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94982	CVE-2024-35925：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94988	CVE-2024-35945：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94989	CVE-2024-35998：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94994	CVE-2024-36286：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn94998	CVE-2024-36899：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95001	CVE-2024-36940：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95004	CVE-2024-36954：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95005	CVE-2024-36959：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95016	CVE-2024-38662：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn95033	CVE-2024-42283：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95037	CVE-2024-42285：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95040	CVE-2024-43834：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95041	CVE-2024-43835：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95045	CVE-2024-44934：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95051	CVE-2024-44987：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95067	CVE-2024-46739：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95071	CVE-2024-46743：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95083	CVE-2024-46800：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95084	CVE-2024-46857：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95085	CVE-2024-47678：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95090	CVE-2024-50047：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95126	CVE-2024-50258：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95128	CVE-2024-50262：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95137	CVE-2024-50272：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95159	CVE-2024-50301：linux-kernel：セキュリティ/キー：key_task_permission の slab-out-of-bounds を修正
CSCwn95161	CVE-2024-50302：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95163	CVE-2024-50304：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95170	CVE-2024-53052：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95173	CVE-2024-53057：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95181	CVE-2024-53066：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95183	CVE-2024-53068：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95198	CVE-2024-53096：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95200	CVE-2024-53099：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95213	CVE-2024-53121：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn95215	CVE-2024-53124：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95222	CVE-2024-53135：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95225	CVE-2024-53138：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95228	CVE-2024-53140：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95231	CVE-2024-53142：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95233	CVE-2024-53146：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95238	CVE-2024-53157：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95244	CVE-2024-53173：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95245	CVE-2024-53179：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95259	CVE-2024-55916：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95284	CVE-2024-56601：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95291	CVE-2024-56606：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95294	CVE-2024-56614：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95295	CVE-2024-56615：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95308	CVE-2024-56647：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95316	CVE-2024-56658：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95319	CVE-2024-56662：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95320	CVE-2024-56664：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95323	CVE-2024-56672：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95324	CVE-2024-56688：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95339	CVE-2024-56720：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95345	CVE-2024-56728：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95347	CVE-2024-56739：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95354	CVE-2024-56751：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95358	CVE-2024-56756：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95361	CVE-2024-56763：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn95365	CVE-2024-56770：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95372	CVE-2024-56779：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95453	CVE-2024-57807：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95456	CVE-2024-57890：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95462	CVE-2024-57938：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95464	CVE-2024-57940：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn95466	CVE-2024-8006：libpcap：次によってリモートパケットキャプチャのサポートが無効になる...
CSCwo00332	Firepower がリロード後に SSL トラストポイント設定を削除する
CSCwo14426	拡張 ACL オブジェクトを保存できない：「IPv4 および IPv6 形式のホストとネットワークのみがサポートされています。（Only Host and Network in IPv4 and IPv6 format are supported.）」
CSCwo35938	管理専用マルチキャストルートがないため、IPv6 管理通信が失われる。
CSCwo40957	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IPsec サービス妨害（DoS）の脆弱性
CSCwo44732	ARP が到達不能なネクストホップのパケットをひそかにドロップする
CSCwo48439	スレッド名 Unicorn Admin Handler でのトレースバックとリロード
CSCwo49925	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの IKEv2 DoS 脆弱性
CSCwo49926	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの IKEv2 DoS 脆弱性
CSCwo49932	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアのリモートアクセス SSL VPN 認証サービス妨害（DoS）の脆弱性
CSCwo49934	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアのリモートアクセス SSL VPN メモリ枯渇のサービス妨害（DoS）脆弱性
CSCwo50716	Cisco Secure Firewall Management Center ソフトウェアの SQL インジェクションの脆弱性
CSCwo52298	アクセスルールが API を介して作成されると、FMC UI で重複する ACL が表示される

不具合 ID	タイトル
CSCwo54753	Cisco Secure Firewall Threat Defense ソフトウェアの Snort ディープ インスペクション バイパスの脆弱性
CSCwo55613	CVE-2021-47247：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55647	CVE-2022-23491：python-certifi：証明書はキュレーションされたコレクション...
CSCwo55683	CVE-2022-49043：libxml2：libxml2 の xinclude.c の xmlXIncludeAddNode...
CSCwo55684	CVE-2022-49046：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55707	CVE-2022-49190：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55710	CVE-2022-49215：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55715	CVE-2022-49219：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55868	CVE-2023-52587：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55879	CVE-2023-52612：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55882	CVE-2023-52621：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55883	CVE-2023-52622：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55913	CVE-2023-52879：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55916	CVE-2024-25629：c-ares：c-ares は非同期 DNS の C ライブラリであり...
CSCwo55934	CVE-2024-26659：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55937	CVE-2024-26664：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55942	CVE-2024-26671：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55951	CVE-2024-26679：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55956	CVE-2024-26686：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55957	CVE-2024-26687：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55976	CVE-2024-26763：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55977	CVE-2024-26764：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55983	CVE-2024-26773：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo55992	CVE-2024-26805：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwo55993	CVE-2024-26809：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo56025	CVE-2024-40945：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo56029	CVE-2024-40984：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo56063	CVE-2024-53217：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo56068	CVE-2024-56171：libxml2：2.12.10 および 2.13.x より前の libxml2...
CSCwo56070	CVE-2024-56568：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo56072	CVE-2024-56569：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57066	CVE-2024-57874：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57095	CVE-2024-57977：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57100	CVE-2024-57981：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57103	CVE-2024-58005：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57107	CVE-2024-58017：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57116	CVE-2024-9287：python：CPython に脆弱性が発見された...
CSCwo57126	CVE-2025-21638：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57128	CVE-2025-21669：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57156	CVE-2025-21745：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57161	CVE-2025-21776：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57162	CVE-2025-21779：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57169	CVE-2025-21785：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57171	CVE-2025-21791：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57172	CVE-2025-21814：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo57178	CVE-2025-27113：libxml2：2.12.10 および 2.13.x より前の libxml2...
CSCwo65318	Cisco Secure Firewall Management Center ソフトウェアの SQL インジェクションの脆弱性
CSCwo70286	展開後の libdaq 初期化フェーズでの Snort2|3 トレースバック

不具合 ID	タイトル
CSCwo73885	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwo73886	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアのリモートアクセス SSL VPN 未認証メモリ枯渇のサービス妨害（DoS）脆弱性
CSCwo73888	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの Lua コードインジェクションの脆弱性
CSCwo73889	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアのリモートアクセス SSL VPN Lua インタープリタのサービス妨害（DoS）脆弱性
CSCwo73891	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアのリモートアクセス SSL VPN 認証済みメモリ枯渇のサービス妨害（DoS）脆弱性
CSCwo74009	Cisco FXOS および UCS Manager ソフトウェアのコマンドインジェクションの脆弱性
CSCwo74010	Cisco FXOS および UCS Manager ソフトウェアのコマンドインジェクションの脆弱性
CSCwo74376	CVE-2024-26816：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo74380	CVE-2024-26830：linux-kernel：i40e：信頼できない VF による管理上設定された MAC の削除を許可しない
CSCwo74394	CVE-2024-26851：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo74400	CVE-2024-27437：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo74405	CVE-2024-34158：golang：「//+build」ビルドタグラインで Parse を呼び出す...
CSCwo74407	CVE-2024-45336：golang：次の後に HTTP クライアントが機密ヘッダーを破棄する...
CSCwo74409	CVE-2024-45341：golang：IPv6 アドレスを持つ URI を持つ証明書...
CSCwo78475	FTD でダイナミックオブジェクトを含むポリシーを展開中に、トラフィックが誤った ACP ルールにヒットする
CSCwo87471	CVE-2022-49546：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87475	CVE-2022-49728：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwo87520	CVE-2025-21640：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87522	CVE-2025-21898：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87535	CVE-2025-21920：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87541	CVE-2025-21928：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87551	CVE-2025-21959：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo87578	CVE-2025-32414：libxml2：2.13.8 および 2.14.x より前の libxml2...
CSCwo91748	Lina：ACL 削除後に show access-list を実行すると、スレッド名 SSH でトレースバックが発生する
CSCwo92790	変更の保存後に、すべてのルートマップオブジェクトでルートマップオブジェクトの ACL match 句が上書きされる
CSCwo95496	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの Lua コードインジェクションの脆弱性
CSCwo95633	CVE-2025-21853：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwo95634	CVE-2025-32415：libxml2：2.13.8 および 2.14.x より前の libxml2...
CSCwo95774	コンテキストエクスプローラによって Highcharts の脆弱なバージョンが使用される
CSCwo97439	ACL：AAA 承認コマンドが適用された後に、ASA で「OOB アクセスリストの設定の変更が検出されました（OOB Access-list config change detected）」という誤った警告が表示されることがある
CSCwp05866	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアのマルチコンテキストモード SCP 不正なファイルアクセスの脆弱性
CSCwp09920	ポリシー展開：サイト間 VPN で MD5 を使用すると、手動展開は検証エラーで失敗するが、スケジュール展開は成功する
CSCwp10290	CVE-2024-26870：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwp10292	CVE-2024-26891：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwp10312	CVE-2025-22063：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwp10317	CVE-2025-37785：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwp22451	Cisco Secure Firepower Management Center ソフトウェアの SQL インジェクションの脆弱性

不具合 ID	タイトル
CSCwp29401	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェアの SAML リフレクテッド クロスサイト スクリプティングの脆弱性
CSCwp34291	Cisco Secure Firewall Threat Defense ソフトウェアの Snort ディープ インスペクション バイパスの脆弱性
CSCwp62846	FTD アップグレードを元に戻すと、元に戻された FTD の FMC でオブジェクトのオーバーライドがサイレントで削除される
CSCwp68059	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェアの VPN Web サービス クロスサイト スクリプティングの脆弱性
CSCwp81377	Cisco Secure FTD ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwp98488	PSB: SEC-LOG-NOSENS-FR2 - P12 証明書パスフレーズが FMC ログにプレーンテキストで記録されました
CSCwp99280	複数のシスコ製品の Snort 3 SSL サービス妨害の脆弱性
CSCwq01516	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの IKEv2 DoS 脆弱性
CSCwq01517	Cisco Secure Firepower Management Center ソフトウェアの SQL インジェクションの脆弱性
CSCwq01519	Cisco Secure FTD ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwq01526	Cisco Secure FTD ソフトウェアの認証済み DoS 脆弱性
CSCwq01529	複数のシスコ製品の Snort 3 TBD サービス妨害の脆弱性
CSCwq01530	複数のシスコ製品の Snort 3 TBD サービス妨害の脆弱性
CSCwq02055	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア VPN Web サービス クライアントサイド リクエスト スマグリングの脆弱性
CSCwq18679	CSM/CLI の ASA：最後の ACL 回線に access-list ACL_name 回線 line_nr コメントが存在せず、「Specified remark does not exist」というメッセージが表示される
CSCwq21101	無効なホストヘッダーにより、ASA インターフェイス IP アドレスが表示される

不具合 ID	タイトル
CSCwq23369	Cisco Secure Firewall Threat Defense ソフトウェア Snort 3 Visual Basic for Application サービス妨害の脆弱性
CSCwq23372	Cisco Secure Firewall Threat Defense ソフトウェア Snort 3 Visual Basic for Application 無限ループサービス妨害の脆弱性
CSCwq23373	Cisco Secure Firewall Threat Defense ソフトウェア Snort 3 Visual Basic for Application ヒープ オーバーフロー サービス妨害の脆弱性
CSCwq23374	複数のシスコ製品の Snort 3 TBD サービス妨害の脆弱性
CSCwq23375	Cisco Secure Firewall Management Center ソフトウェアのコマンドインジェクションの脆弱性
CSCwq23377	Cisco Secure Firewall Threat Defense ソフトウェア Snort 3 Visual Basic for Application サービス妨害の脆弱性
CSCwq24081	Cisco Secure Firewall Adaptive Security Appliance ソフトウェア SSH 部分秘密キー認証バイパス脆弱性
CSCwq27947	ucssh プロセスが終了しないループにあるため、高 CPU 使用率および高ディスク使用率の障害が発生する
CSCwq32051	Cisco 適応型セキュリティアプライアンスおよび Firepower Threat Defense ソフトウェアのコマンドインジェクションの脆弱性
CSCwq39942	CVE-2025-32463：sudo：Sudo 1.9.17p1 より前では、ローカルユーザーが次を取得できる。
CSCwq39943	CVE-2025-32462：sudo：1.9.17p1 より前では、ユーザーは意図しないマシンでコマンドを実行できる。
CSCwq40256	暗号マップ ACL が特定のポートを使用している場合、インバウンド IPsec パケットが IPsec オフロードによってドロップされる。
CSCwq50506	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの IKEv2 DoS 脆弱性
CSCwq56017	Cisco Secure Firewall Management Center および Cisco Secure Firewall Threat Defense ソフトウェアのパストラバーサルの脆弱性
CSCwq66716	CVE-2025-27363：free-type：FreeType に境界外書き込みが存在する...
CSCwq73056	CVE-2024-26772：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwq73059	CVE-2024-26804：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwq73060	CVE-2024-26808：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwq73062	CVE-2024-26810：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwq73065	CVE-2024-26843：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwq73656	Cisco Secure Firewall ASA ソフトウェアおよび Secure FTD ソフトウェアの OSPF メモリ破損の脆弱性
CSCwq74738	RAVPN SSL/IKEV2 認証エラー：AAA プロセスの不正なファイバクラス
CSCwq74813	FMC：拡張 ACL オブジェクトに ACE をコピー/切り取り/貼り付けるか、ドラッグアンドドロップすると、既存のルールが削除される
CSCwq75339	複数のシスコ製品での Snort 3 DCERPC の脆弱性
CSCwq75359	複数のシスコ製品での Snort 3 DCERPC の脆弱性
CSCwq78991	レプリケーション中に不完全な ACL ポリシールールを取得するが、ファイアウォールがクラスタに参加する
CSCwq82095	特定の IDP のメッセージが表示され SAML 応答が拒否された
CSCwq82225	'show service policy' で初期関連のドロップに対してドロップカウンタが増加しない
CSCwq84949	Cisco Secure Firewall Threat Defense ソフトウェア SSL 復号ポリシーのサービス妨害の脆弱性
CSCwq85267	Apache HTTP サーバーにおける、有効寿命後のメモリの解放遅延の脆弱性。
CSCwq85285	Apache HTTP サーバーのコアでの HTTP レスポンスの分割により、Content-Type レスポンスヘッダーを操作できる攻撃者が攻撃できる
CSCwq86692	ルートマップ設定をブロックする無効な OSPF プロセスポップアップ
CSCwr13046	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェアの VPN Web サービス クロスサイト スクリプティングの脆弱性
CSCwr18525	CVE-2024-58250：ppp：2.5 より前の ppp の pppd の passprompt プラグイン....
CSCwr18527	CVE-2023-24531：golang：コマンド go env が次を出力していると記載される...
CSCwr18660	CVE-2024-46981：redis：Redis はオープンソースのインメモリデータベースで...
CSCwr18675	CVE-2024-38473：apache-http-server：mod_proxy のエンコーディングの問題...

不具合 ID	タイトル
CSCwr58661	Cisco Secure Firewall 適応型セキュリティ アプライアンス ソフトウェアの TCP フラッドにおけるサービス妨害（DoS）の脆弱性
CSCwr96008	Cisco Secure Firewall Management Center ソフトウェアの認証バイパスの脆弱性

表の最終更新日：2026-03-04

表 *18* : バージョン *7.6.4* で解決済みの機能バグ

不具合 ID	タイトル
CSCvm76755	DP-CP arp-in キューと adj-absent キューを分離する必要があります
CSCvu71962	オブジェクト管理の [使用状況の検索（Find-Usage）] のユーザーロール権限
CSCwb07908	スタンバイ FTD/ASA が 0.0.0.0 の送信元 IP で DNS クエリを送信する
CSCwd40371	9300 の日付設定で 2012 年 1 月 1 日が表示される：FMC への 9300 FTD の登録に失敗する
CSCwd54466	新規レルムユーザーが検出されたユーザーに誤ってマッピングされる
CSCwd55939	UTC 開始時刻（DST に基づく）が異なるカレンダー日にある場合、スケジュールされたタスクがまったく実行されない可能性がある
CSCwd83069	100G ポートの自動ネゴシエーションを無効化する機能を追加
CSCwd92327	2k プラットフォームでは、数字で始まるユーザーの外部認証が失敗する
CSCwe39331	Snort3 ルールの推奨事項：ネットワーク検出が設定されていない場合にエラーメッセージを追加する
CSCwe63686	WM FDM @009_check_snort_preproc.sh でアップグレードの準備状況チェックに失敗したが、7.3.1-19 へのアップグレードが成功する
CSCwe89818	FMC での外部認証で、「"strict refs" を使用しているときに文字列（""）を HASH ref として使用できません（Can't use string（""）as a HASH ref while "strict refs" in use）」というエラーがスローされることがある
CSCwf61982	検索関連の EO が多いため、[検索の編集（Edit search）] ページと統合イベントビューアの読み込みが非常に遅くなる
CSCwf72285	DAP：debug dap trace が 3000 行を超えると正常に表示されない
CSCwh04468	Syslog サーバーに送信された接続イベントに「不明（unknown）」な syslog ファシリティがある

不具合 ID	タイトル
CSCwh08441	ENH：FTD で CA 証明書を再生成するコマンドまたはスクリプトを追加
CSCwh53745	ASA：DNS クエリ応答のために着信接続を開始するための予期しないログ
CSCwh78517	92.16.0.125 で設定 @FSM-STAGE:sam:dme:MgmtImporterImport:config のインポートに失敗した
CSCwi03494	順不同イベントにより FTD でトンネルが稼働しているにもかかわらず、S2S トンネルが FMC ダッシュボードで非アクティブと表示される
CSCwi97667	アクティブおよびスタンバイ FMC での VDB/SRU のインストール中に、FMC HA 同期ステータスが失敗と表示される
CSCwi98704	ActionQueueScra が oom-killer を呼び出した
CSCwj17969	rna_ip_os_map が非常に大きくなり、SFDataCorrelator がイベントの処理を停止する可能性がある
CSCwj21985	デバッグ：Eth1/1 が予期せずフラップする
CSCwj23860	cluster exec と show cluster access-list の間でカウンタが一致しない
CSCwj35821	FTD：TCP_PRX PROBE_TOTAL_ACTIVE_CONN のカウンタが無効
CSCwj42875	FTD に通信障害があるにもかかわらず FMC HM が「正常（normal）」と表示する
CSCwj53663	TPK：FXOS は、MI インスタンスの開始失敗時に RM キューをクリーンアップしない
CSCwj61834	IPSecOffload：esp null 暗号化が ipsec プロポーザルで使用されると、トラフィックがドロップされる
CSCwj81031	ASA/FTD に snmpd コアが存在する
CSCwj98648	署名キーを読み取れない（マルチインスタンス展開）
CSCwk09488	RA 認証中に ISE から SGT を処理できなかった場合に誤った syslog が生成される
CSCwk15596	オンプレミスサーバーへの FMC の再登録が失敗する
CSCwk16332	高速の SIP 接続による ASA/FTD のトレースバックとリロード
CSCwk33511	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
CSCwk34786	Victoria-DT CX：1220 CX モデルで 10 ポートチャネルのサポート

不具合 ID	タイトル
CSCwk35638	ダングリング インターフェイスがセキュリティゾーン/インターフェイスグループおよびインターフェイスに存在する
CSCwk37929	スタンドアロン 2110 を 6.6.7-223 から 7.2.8-25 にアップグレードすると、FMC で「インターフェイスが変更されました」というアラートが発生する
CSCwk46737	HA の ASA：スタンバイデバイスの 1 つのコンテキストにおける chunk mem Failed メッセージからの alloc_ch() alloc
CSCwk47035	診断インターフェイスの pre-CMI nameif が MANAGEMENT だと CMI が無効になる
CSCwk62040	マッピングされた送信元で大きな IP 範囲がサービスキーワードとともに使用されている場合、警告を表示する必要がある
CSCwk63011	「show module」コマンド出力のネットワークモジュールのスロットとステータスに関する情報が正しくない
CSCwk70078	障害のシミュレーション後に「show failover statistics」で障害とレコードが表示されない
CSCwk75406	syslog を介した CC-mode 監査の FMC が機能しない
CSCwk75835	FMC から ip アドレスを変更した後でも、スタンバイユニットの古い IP を持つ Sftunnel が存在する。
CSCwk79288	btmp 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
CSCwk82462	コアダンプファイルシステムの変更中にクラスタが無効化される
CSCwk82571	[ユーザーアクティビティ（User Activity）] の FTD スタンバイピアに対して、VPN クライアントアプリケーションのバージョンと OS が表示されない
CSCwk83680	sftunnel AUTH_TIMEOUT を 60 に増やす
CSCwk86404	3100/4200 のマルチインスタンス FTD のログインプロンプトで、ログインバナーが表示されない
CSCwk87599	show conn detail の rx-ring 4294967295（最大値）フィルタで、無効な rx-ring 番号がある接続が表示される
CSCwk87700	FxOS プラットフォーム上の複数の core.svc_sam_statsAG
CSCwk93762	spin_lock_fair_mode_enqueu および nlp_init() でのパニックにより、デバイスのトレースバックとリロードが 3 回発生する

不具合 ID	タイトル
CSCwk94449	fxos tech support に show mgmt-ip-debug を含める
CSCwk95916	正常性ポリシーの下に CPU およびメモリしきい値の調整機能がない
CSCwk97677	7.6.0-1685 のアップグレード後に、TPK-MI FTD インスタンスが検証エラーを取得し、スプリットブレイン HA の ftd が発生する
CSCwm02802	"clear configure interface" によってスタンバイでの HA 解除中に ACK/FHELLO ドロップが発生する
CSCwm03198	sftunnel プロセスがダウンしたため、TPK ネイティブクラスタの移行に失敗する
CSCwm03287	FP4245：NPU アクセラレータで 100Gb インターフェイスの速度が 10Mb に変更される
CSCwm03805	ユーザーページの削除エラー：アクションの削除に失敗しました：未定義の値でメソッド "short" を呼び出すことはできません（Action Delete Failed：Can't call method "short" on an undefined value）
CSCwm05158	「ファームウェアイメージのアップグレードに失敗しました（Failed to upgrade firmware Image）」という障害では、アップグレードに失敗したファームウェアを示す必要がある
CSCwm05960	生成された Crypto チェックサムが設定変更なしで変更される
CSCwm07323	SSH が設定されたリモートストレージでクラスタのクラスタバンドル tar ファイルの作成に失敗する
CSCwm07419	外部 RADIUS 認証に影響を与えるホスト名を使用すると ldap.conf が生成されない
CSCwm10676	DNS が設定されている場合、FMC はオブジェクトを検索できない
CSCwm28962	HA fover_trace.log ファイルに多数のエラーメッセージが含まれると、短時間でログローテーションが発生する
CSCwm31562	NTPD ステータス分析用の FMC 正常性プラグインがローカライズされたデータを使用していない
CSCwm33286	SFDataCorrelator HandleVPNBulkSync db 接続の使用により、HA が「機能低下 - 同期が不完全（Degraded-Synchronization incomplete）」状態になる
CSCwm33529	Firepower デバイスの前面パネルとアップリンクポートの FXOS MTU 処理に改善が必要
CSCwm35144	cdFMC：REALM でプロキシとして使用した場合、ADI プロキシが TPK MI で複数回終了する

不具合 ID	タイトル
CSCwm37363	ポートマネージャと lacp の同期がプログラム的に行われない
CSCwm38027	いずれかのインスタンスが WA4245-760-102 で start-failed 状態になる
CSCwm40744	nlp のデバッグ可能性を強化し、nlp ログを永続化する
CSCwm47187	SAML CP ルールで使用されているインターフェイスの場合、インターフェイスの nameif を変更した後にポリシー展開が常に失敗する
CSCwm48550	Cisco Secure Firewall CSF-1200：SMA が次のエラーを報告した：Lina は開始されたが、まだ実行されていない
CSCwm49213	回帰のために CSCwk63011 で変更が元に戻された後、show mod 機能を修正する必要がある
CSCwm54079	FXOS 用 WA の修正により、MI インスタンスの開始失敗時に RM キューがクリーンアップされない
CSCwm56731	ASA 9.16 SSH クライアントのユーザーコンテキストへのログインが、ecdsa で機能しない
CSCwm58600	FMC：RAVPN ウィザードでセキュア クライアント イメージを選択できない
CSCwm58772	ポリシー展開中に Snort2 インスタンスが OOM で予期せず再起動する
CSCwm61380	FMC が KVM で実行されている場合、Day0 設定が機能しない
CSCwm61693	カーネルで NFS クライアント 4.1 を有効にして、NFS および EFS マウントの問題をデバッグする：stunnel への SIGKILL(9)
CSCwm63670	デバイス設定をコピーする場合、FTD に展開された SGT をプロパゲートする（SGT 設定 UI と LINA が一致しない）
CSCwm63890	VRF のルートリークがある場合、FMC GUI で ECMP 設定を保存できない
CSCwm67644	FMC 使用状況の検索機能でランダムオブジェクトの関連するすべてのアクセス コントロール ポリシーが表示されない
CSCwm68003	アップグレード前にマルチチャネル CLI が無効になっている場合、アップグレード後に再度有効になる
CSCwm69074	ASA PKI：MS 証明書ポリシー拡張が正しく処理されない
CSCwm69085	証明書表示コマンドで ASA がクラッシュする
CSCwm76872	ztna アプリケーションの無効化による Lina のトレースバックとリロード
CSCwm78288	FMC UI で異なるライセンス階層が表示される

不具合 ID	タイトル
CSCwm80580	Snort が 1 分ごとに「正常に終了（exits normally）」を繰り返し、完全に停止する
CSCwm80732	ASA/FTD - TCP プロキシの競合状態によるトレースバックとリロード
CSCwm82566	トンネルが稼働している場合でも、FMC で VPN トンネルのステータスが不明として表示される
CSCwm83033	アップグレード後、FMC で無効な名前の警告が表示されず、保存がグレーアウトされる（Rest API を介して DAP レコードを設定）
CSCwm85795	侵入ポリシー推奨事項にダングリングオブジェクトがあるため、アクセスコントロール ポリシーのエクスポートが失敗する
CSCwm86414	Cisco ASA - フェールオーバー設定の再同期に失敗し、予期しない再起動が発生する
CSCwm87653	未使用のオブジェクトの削除に時間がかかる
CSCwm87669	FMC UI と API の結果との間で未使用オブジェクト数に不一致がある
CSCwm88812	4200/3100/1200 ハードウェアで AppAgent タイマーを変更できる
CSCwm90422	CAT9k スイッチで ASAc の SSH 接続が失敗する
CSCwm90900	GTP インスペクションがエラーによりパケットをドロップする。理由：（IE-Type:CAUSE(2) IE がありません）
CSCwm91406	7.4.2.1 へのアップグレード後に FTD HA スタンバイが繰り返しリロードする
CSCwm92310	リブートまたはトレースバック後にデータインターフェイスの DNS を介して FQDN が解決されない
CSCwm99199	MariaDB のインポート失敗により、FMC-HA 同期が不完全になる
CSCwn04201	user_enforcement SXP データ同期中に SNORT2 が高い CPU 使用率（100%）を示す
CSCwn10173	キーの長さを変更すると、SSH セッションを作成できない
CSCwn12097	DVTI 機能でのメモリリーク
CSCwn13813	ユーザー ID の不一致：ログの追加
CSCwn14458	FMC：ポリシー展開の自動化タスクで [コメント（Comment）] フィールドの検証を有効にする

不具合 ID	タイトル
CSCwn15443	拡張 VPN トラフィックテスト中に snp_vpn_int_api でクラッシュ/アサーションが発生する
CSCwn15787	FMC RAVPN アクティブセッションの終了によって「セッションの終了中にエラーが発生しました（Error while terminating session）」というエラーがスローされる
CSCwn16320	以下の FTD ロギングの syslog サーバーが最初の syslog サーバーの emblem 設定に従ってホスト名情報を送信する
CSCwn22708	LSP から侵入ルールが削除されても、FMC はデータベースからそれらのルールを削除しない
CSCwn23175	パッチが適用されたバージョンのコードを使用した Cisco Secure Firewall 3100 シリーズでのマルチインスタンスの設定
CSCwn23987	9.18 で確認されたポートブロック配分の問題
CSCwn27111	FMC で AC ポリシーレポートが生成されない
CSCwn27583	spin_lock_get_actual_internal での Lina の高い CPU 使用率および/またはトレースバックとリロード
CSCwn27752	無効なセッションエラーが原因で、デプロイメント ポリシー タスクがスタック状態になる
CSCwn27872	「eigrp_interface_ioctl」API で、約 25KB のメモリの大きなチャンクがスタックに割り当てられる
CSCwn28902	FMC がスマートライセンス用に設定されたプロキシを使用しない
CSCwn29609	FMC UI で無視されると表示される場合でも、クラスタ化されたデバイスで拡張 PAT 設定を有効にできる
CSCwn30151	パスワードを変更しようとすると ASA がクラッシュする
CSCwn31151	インターフェイスの説明に改行が含まれていると、展開に失敗する
CSCwn32025	FMC 管理ワークフローの問題：グループから NetworkObject を削除し、同じチケットで削除できない
CSCwn32978	スレッド名 Datapath でのトレースバックとリロード
CSCwn33750	アクセスコントロールルール名の条件を含む相関ルールがスタンバイ FMC で正しく保存されない
CSCwn34741	レルム同期が原因で SMB リモートバックアップが失敗する

不具合 ID	タイトル
CSCwn35495	フェールオーバー時に FXOS でプライマリ FTD インスタンスの MAC アドレスが正しく更新されない
CSCwn36712	スタンバイの 8305 の NAT 迂回がフェールオーバー後に更新されないため、プライマリのスタンバイ FTD が FMC でオフラインと表示される
CSCwn36925	パッチまたはホットフィックスのインストールエラーの後に MI 環境で LSP 展開が失敗する
CSCwn37005	RBD FTD HA の解除は FTD で成功するが FMC で失敗する
CSCwn37490	Firepower Management Center で ACP をコピーできない
CSCwn37993	長期稼働セットアップ：TPK クラスタノードがデバイス管理ページで空のクラスタとして表示される
CSCwn38761	7.7 で、サーバー/サーバーに到達するインターフェイスがダウンしている状態で FQDN オブジェクトが削除された際に、DNS FQDN オブジェクトが未解決にならない
CSCwn39081	SNMP ウォークが IP アドレスではなく IPSEC ピアの ASCII 値になる。
CSCwn39777	syslog 設定の到達不能なホストおよびURL により、デバイス管理ページの読み込みがブロックされる
CSCwn39810	FMC は他の設定を FlexConfig とともに展開するときにユーザーに警告する
CSCwn44527	異なるドメインで同じ名前を持つ侵入ポリシーが IPS ポリシーの破損を引き起こす
CSCwn45194	NTP が外部サーバーから HW ローカルクロックに一時的に切り替わると、FMC は正常性アラートを生成する場合がある
CSCwn46685	HandleUserLoginInfoMsg での SFDataCorrelator のメモリリーク
CSCwn46861	Secure Firewall のマルチインスタンスが sftunnel 証明書を更新しない
CSCwn47308	FPR 1100/2100/3100 のクリティカルな正常性アラート「user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)」
CSCwn49611	キャプチャされたファイルによってディスクマネージャが過負荷になるのを防ぐため、ファイルキャプチャ ディスクマネージャの SILO を削除する
CSCwn50245	FMC で、ポリシーとオブジェクトのサイズが非常に大きくなると、バックエンドサーバーの JVM がメモリ不足になる
CSCwn50760	9.20.3.7 へのアップグレード後の ASA トレースバック

不具合 ID	タイトル
CSCwn54186	アップグレード後に特定のクエリで JBDC クライアントがエラーをスローする
CSCwn55195	展開のプレビュー比較 PDF レポートが生成されない
CSCwn55890	local-base-url に大文字が含まれている場合、SAML DNS LB がローカルホストへのリダイレクトに失敗する
CSCwn57674	解放後に設定されたブロック loc 操作を修正
CSCwn59032	ASA 9.18.4.22（FPR 2130 プラットフォームモード）へのアップグレード後に FCM GUI にアクセスできなくなる
CSCwn59596	FMC での SSH 公開共有キー認証で [完了時にコピー（Copy when complete）] オプションが機能しない
CSCwn60726	スレッド名 vtemplate process でトレースバックおよびリロードする
CSCwn61041	ウォッチドッグを含む bgp * IPv6 ユニキャスト中のトレースバックとリロード
CSCwn61176	FTD 7.2 以降で system support reset-event-bookmarks を実行した後に、EventHandler が再起動しない
CSCwn61232	メモリブロック破損：RAVPN SSL/IKEV2 認証エラー、AAA SHIM の使用可能なファイバの枯渇
CSCwn64025	ASA：他のネイバーから学習した IPv6 EIGRP ルートが、フェイルオーバー後の更新に含まれない
CSCwn64992	[展開（Deploy）] タブでの FMC1600-K9 PDF ダウンロードの失敗
CSCwn69488	ASA/FTD がスレッド名 IP RIB Update でトレースバックおよびリロードする
CSCwn69653	7.7.0-1607 の WM-HA アクティブユニットで Ipv6 TCP syslog が正しく生成されない
CSCwn70473	HA リンクとして使用すると、Finisar の SFF_SFP_10G_25G_CSR_S ポートがバウンスする
CSCwn71946	show blocks old core local を使用すると、予期しないリロードが発生する可能性がある。
CSCwn72938	cdFMC および FMC のスマートライセンス UI に、Malware、IPS、URLFilter、および Apex のライセンス数が重複して表示される

不具合 ID	タイトル
CSCwn76548	パブリッククラウドクラスタの S2S およびリモートアクセス設定をブロックする
CSCwn76740	「アクセスを許可できません。（Unable to authorize access.）」というメッセージが表示され、FMC UI ログインが失敗する
CSCwn78693	FMC：OSPF NSF 認識（ヘルパーモード）をスタンドアロン FTD で設定できない
CSCwn80400	遅延の大きいネットワークでの AnyConnect over TLS によるダウンロード速度の遅延
CSCwn80419	設定可能なオプションとして SVC Rx/Tx キューが必要
CSCwn80643	フロー終了の処理中にセグメンテーション フォールトで Snort3 がクラッシュする
CSCwn80765	CiscoSSH が有効な場合に ASA を搭載した ISA3000 が SSH アクセスを拒否する
CSCwn81118	RTSP パケットが送信キューでスタックして 9k ブロックが枯渇する。
CSCwn81398	FMC が API を介してプレフィックスリストを変更しているときに、入力に重複するエントリがあってもエラーをスローしない
CSCwn81833	FMC ユーザー権限では、[デバイスの変更（Modify Devices）] が選択されていない場合でもユーザーは HA を一時停止できる
CSCwn81995	SNMP インスペクションが有効になっている場合のメモリ破損によるトレースバックとリロード
CSCwn84743	ユーザー EO リビジョンが永続的に蓄積され、最終的にプルーニング機能のジョブ実行能力がオーバーフローする
CSCwn85299	脅威スコア 98 で非常に高い脅威の確実性が表示される
CSCwn85765	xml 処理後に ipv6 ping VRF 名が変更される
CSCwn85913	count(*) で並べ替える際の extdb クエリエラー
CSCwn87164	DHCP リレーエージェントとサーバー側インターフェイスの両方で PC が使用されている場合、検証が行われない
CSCwn87249	Snort3：FMC 接続イベントログに、TCP を使用した DNS クエリの URL が表示されない
CSCwn90900	RA VPN に関連する SNMP OID のポーリングが原因となり、ASA/FTD のメモリ使用率が高くなる

不具合 ID	タイトル
CSCwn91996	PortMgr IPC 通信障害により、WM-DT- FXOS の重大な障害が発生する
CSCwn92066	FTD クラッシュ：SSH 端末セッションが突然終了したときに "more.fxos" プロセスが実行されたままになる
CSCwn92074	さまざまな下位バージョンの vFTD を管理している FMC がイベントハンドラエラーをスローする
CSCwn92248	FPR2100 および FPR1100：ポートチャネルインターフェイスが LACP でフラップする
CSCwn92507	FMC：RAVPN ウィザードおよび FMT ツールに接続イメージがリストされない
CSCwn92894	「show chunkstat top-usage」の出力にすべてのエントリが表示されないことがある
CSCwn93411	snmpd サービスの障害による FXOS のリセットとリロード
CSCwn95939	受信した CRL がキャッシュされた CRL より古い場合に syslog を生成
CSCwn95945	受信した CRL 署名の検証が失敗した場合に syslog を生成
CSCwn96928	ブロックルールが適用されていても URL が許可される
CSCwn96963	FTD が VPN ヘアピンのない VPN ルーティングとして syslog 430002 を生成する
CSCwn97341	MonetDB モニターは、統計パーティション内の欠落した列を検出する必要がある
CSCwn97610	AC ポリシールール名の特殊文字が原因でポリシー展開が失敗する
CSCwn97630	IPv6 パケット処理が原因で DATAPATH で FTD リブートおよびトレースバックが発生する
CSCwn97956	ルール名に特定の特殊文字が含まれている場合、個々のルールのヒットカウントでエラーがスローされる
CSCwn98402	デバッグ可能性：アップグレード後に FP2100 ポートチャネル インターフェイスがフラップする
CSCwn98552	S2S モニタリングの [トンネルの概要（Tunnel Summary）] および [トポロジ（Topology）] ビューに正しいステータスが表示されない
CSCwn98642	動的分析のステータス変更時刻は、動的分析用のファイル送信時にのみ変更される
CSCwn99481	FPR 2100 で、コアファイルは完全に生成されるが、内容に一貫性がない

不具合 ID	タイトル
CSCwn99640	スクリプト 800_post/020_710_fix_users_and_roles.pl での FTD アップグレードの失敗
CSCwo00102	不正なウィンドウサイズ情報を受信したために、Snort3 が無効なシーケンス番号でパケットをトリミングする
CSCwo00225	アップグレード前に設定されている場合、VNI 送信元 MTU がアップグレード後に IPv6 に認識されない
CSCwo01616	サポートされていないモデルで sfipproxy prometheus 設定が試行され、sfipproxy.conf が置き換えられる
CSCwo01653	HTTP 401 UNAUTHORIZED エラーが原因で FMC GUI にログインできない
CSCwo05712	有用性強化：FXOS ディスクエラーをよりわかりやすくする
CSCwo06044	デバイスバックアップからのパフォーマンス モニタリング ファイルの除外
CSCwo08306	ローカルへのコマンド承認のフォールバックが、権限 15 のユーザーに対してのみ機能する。
CSCwo08724	snort 障害中にピアユニットが準備完了状態になる前に、アクティブな HA ユニットが障害状態になる
CSCwo09060	4096 ビットの RSA キーを持つ SSL トラストポイントが、CLI で更新されると ASA で許可されない
CSCwo09618	EEM によるデバッグの有効化が失敗する
CSCwo14706	アップグレード フレームワークで新しい app_bin のバッファ計算が欠落している
CSCwo14737	FTD：LSP のインストール/展開エラー
CSCwo15059	バックアップが失敗し、一般的な「バックアップは予期せず終了しました（Backup died unexpectedly）」というエラー メッセージが表示される場合がある。
CSCwo15715	IKEv2 キー再生成が、IKE キー再生成中のフラグメンテーションによって失敗する
CSCwo15787	SFO のインポートが「UUID が指定されていません（No UUID Provided）」というエラーで失敗する
CSCwo16049	UI バックアップのタイムアウト エラーが原因で、FMC で「長く実行中のバックアップを終了しています（Terminating long running backup）」という誤ったアラートが表示される

不具合 ID	タイトル
CSCwo18838	ASA/FTD がスレッド名「lina_exec_startup_thread」でトレースバックし、リロードすることがある
CSCwo19762	マルチコンテキストモードで mac-address auto を再度有効にすると、クラスタ内のデータノードに再度参加できない
CSCwo19986	FTD TS は重複したデータを収集する
CSCwo20629	フリート アップグレード ワークフローでの無効/不正なデータの処理の改善
CSCwo21105	process_stderr.log：リンク集約ログファイル '/ngfw/var/log/link_aggregation.log' を開けない
CSCwo21830	TS パッケージサイズの削減
CSCwo24772	debug packet-condition が期待どおりに機能しない
CSCwo24856	9K ブロックの枯渇により、ファイアウォールを通過するすべてのトラフィックが遅延する
CSCwo25473	DNS とデフォルトゲートウェイが、データインターフェイス - DNS を介して管理される FTD で削除される
CSCwo25624	無効な AnyConnect イメージと Secure Client プロファイルの参照による展開の失敗
CSCwo25786	REST API を使用すると、ディレクトリ構成なしでレルムを作成できる
CSCwo25834	FMC で統合バックアップに失敗した場合のバックアップステータス通知の強化
CSCwo25854	センサーテーブルのシリアル番号が正しくないため、RMA 後にアップグレードが失敗する
CSCwo26181	FMC での VDB のインストール後、管理対象デバイスに展開された後に SFDataCorrelator が予期せず終了する
CSCwo26258	FPR 4200 シリーズでのリロードまたはアップグレード後における Management0 から Management1 へのデフォルトルートの変更
CSCwo26286	Management1 ゲートウェイの設定は、FPR 4200 シリーズでオプションにする必要がある
CSCwo26725	FMC サイト間監視ダッシュボードがまったく機能しない
CSCwo27260	ユニットがアクティブになるまでに約 13 秒かかる

不具合 ID	タイトル
CSCwo28967	Solar Winds SCP/SFTP を実行しているサーバーに設定すると、FMC リモートストレージテストが失敗することがある
CSCwo31094	NFS が有効になっているディスクアクセスの問題によって、仮想 ASA がトレースバックおよびリロードする
CSCwo31418	ネットワークグループのオーバーライドオブジェクトを含む AC ポリシーにより、デプロイメントが失敗する/ルールが欠落する
CSCwo32845	FPR 4200 シリーズにおけるデュアル管理インターフェイスのリバースパスフィルタの無効化
CSCwo33573	FMC アラート：正常性モジュールのコンパイルエラーを検出
CSCwo33733	LOM が有効な場合に CIMC パスワードの長さが 16 文字に制限されている
CSCwo33815	FMC：プラットフォーム設定から SNMP ホストを削除すると、展開に予想よりも時間がかかる
CSCwo34580	FMC ソフトウェアのアップグレード後に同期を再開した後、FMC HA の定期的な同期の最初のサイクルが失敗することがある
CSCwo34893	リモートストレージサーバーのパスワードが httpsd_error_log にプレーンテキストで表示されている
CSCwo34997	アイデンティティがアタッチされていないときに、アイデンティティポリシーのユーザー/グループを含むルールを変更すると、エラーがスローされない
CSCwo35783	ネイバーとのルートの追加/更新/取り消しに対するデバッグを強化
CSCwo35788	有用性強化：高度なデバッグ用の新しい「show bgp internal」コマンド
CSCwo35810	show bgp update-group a.b.c.d で、有効なネイバーがある場合に「no such neighbor」と表示される
CSCwo36485	vaccess_nameif_action スレッドで ASA/FTD がトレースバックおよびリロードする
CSCwo37055	FMC：FMC の FCM に表示されるメディアタイプが、sfps のスワップ後に CLI と一致しない
CSCwo37500	リモートバックアップが正常に生成されても、設定データベースのバックアップが空になる
CSCwo38855	sftunnel および sfipproxy 構成ファイルの更新がアトミックではない
CSCwo41594	デバッグリセット後の SSL デバッグログの存続

不具合 ID	タイトル
CSCwo42102	show tech-support fprm detail コマンドが長時間スタックする
CSCwo42230	メモリリークが原因でスプリットブレインが発生
CSCwo42501	モジュールの show tech 生成が外部認証で失敗する
CSCwo44267	ASP テーブルリソースが枯渇し、トラフィック転送に影響するため、Firepower がルート制限に達する
CSCwo45497	IKEV2 統計からのカウンタが VPN-Sessiondb のトンネル数と一致しない
CSCwo46142	ポートチャネルメンバーのインターフェイスがフラップによって非アクティブなメンバーになる
CSCwo46533	有効なファイルが検出されない場合、sfipproxy が再起動せず、ユーザー ID などのサービスが失敗することがある
CSCwo47498	FMC で OSPFv3 を無効にしても、FTD インターフェイスからパッシブインターフェイスおよびエリア設定がクリアされない
CSCwo47760	FMC IPsec SA における残りのキー有効期間の秒数から hh:mm:ss への変換が正しくない
CSCwo47929	クラスタノードが部分的に削除され、デバイスが FMC UI でスタンドアロンになる
CSCwo47978	ASA がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwo48157	syslog-ng は、FTD ホスト名を変更すると、想定どおりに FTD ですぐに再起動しない場合がある
CSCwo48607	スタンバイ FMC の 800_post/998_expire_ac_policy.pl でホットフィックスのインストールが失敗することがある
CSCwo49337	FMC：開いているファイルが多すぎるため、ヘルスモニターに「使用可能なデータがありません（No Data Available）」と表示される
CSCwo49366	REST 要求による BGP での EIGRP の再配布が不可能
CSCwo49425	logging recipient-address でロギングメールメッセージのシビラティ（重大度）レベルが上書きされない
CSCwo49658	新しい下位 MR から古い上位 MR にアップグレードした後に、正常性モジュールのコンパイルエラーが発生する
CSCwo49744	DNS とデフォルトゲートウェイが、データインターフェイスを介して管理される FTD で削除される

不具合 ID	タイトル
CSCwo50551	復号ポリシーがオンプレミス FMC から cdFMC への移行に失敗する
CSCwo50885	障害対応パッケージで /mnt/disk0/log フォルダが重複している
CSCwo52139	PingId で SSO を使用して FMC UI からログアウトした後にエラーが発生する
CSCwo54265	ホスト名を介して FMC によって管理されている場合に 7.0.x センサーを 7.0.7 にアップグレードすると、エラーが発生する
CSCwo54996	9344 ブロックのリークによるトラフィック障害
CSCwo55662	FMC REST API は、最初の 1000 個のネットワーク オブジェクト エントリのみを返す
CSCwo56243	AppID NAVL インスタンス化中のウォッチドッグによる Snort3 のトレースバック
CSCwo57098	[新しいセキュリティゾーンオブジェクト（New Security Zone Object）] ウィンドウの [デバイス（Devices）] ドロップダウンで検索が機能しない
CSCwo57740	「${dsk_a} がないか操作できません。ブレードをリブートしています。（${dsk_a} missing or inoperable. Rebooting Blade.）」というエラーにより、不足しているか操作できないディスクが指定されない。
CSCwo57744	チェーン/継承したカスタム IPS ポリシーでオーバーライドが機能しない
CSCwo58033	[クラスター] コンテキストで NAT プールの枯渇が発生すると、CPU 使用率が 100% になる。
CSCwo58191	FTD：snort によって検査されるパケットの大規模な遅延
CSCwo58260	GRE | IPinIP 接続の「built」および「teardown」メッセージを Lina syslog に追加します
CSCwo59534	メモリの破損により lina アサーションとトレースバックが発生する
CSCwo60579	プライマリがダウンしている場合、FTD が HA のセカンダリ Management Center から NTP を介して同期されない
CSCwo60609	ドクタリングルールのタイプがダイナミックであり、インターフェイスがある場合、DNS ドクタリングが正しく機能しない
CSCwo61240	FMC CA を更新した後に、証明書を ArcSight 統合に使用できない
CSCwo61241	checkSystemCPUs 障害により、論理アプリケーションが「Start Failed」でスタックする

不具合 ID	タイトル
CSCwo61788	フェールオーバーおよび状態リンクが有効なサブネットマスクを受け入れない
CSCwo62543	Snort 3 ローカルルールグループ内のルールに対するデフォルトのパスアクションにより、IPS ポリシーで空白のエラーが発生する場合がある
CSCwo63563	FMC と FTD のメジャーバージョンを混在させると、コアごとの CPU 使用率の正常性モジュールが FTD で機能しない
CSCwo65060	FTD HA | ポートチャネルの同じ MAC が原因でネットワーク障害が発生する。
CSCwo65866	プライマリ FTD インスタンスが FCM から無効になっている場合、ネットワーク障害が発生する
CSCwo66872	snmp_logging_thread がコントロールプレーンの CPU を多く使用している
CSCwo67167	FMC の正常性ポリシーとデフォルトの正常性ポリシーに正しい moduleList がない
CSCwo67540	"6" メンバーのシャーシ間クラスタに参加する前に、FPR9K-SM-56 クラスタノードの APP_SYNC タイムアウトが 2 回発生する
CSCwo69015	インベントリ詳細の更新アイコンですべてのモデルのシャーシ情報を更新できない
CSCwo70260	/objects/fqdn フィルタパラメータが機能しない
CSCwo73059	脅威スコアが FTD にキャッシュされている場合、キャプチャされたファイルのステータスは更新されない
CSCwo73901	ルールの一括編集：ゾーン数が 1000 を超える場合、セキュリティゾーン検索で一部のゾーンが検索されない
CSCwo74305	DHCP 設定済み VPN インターフェイスを使用したハブアンドスポーク VTI トポロジでの展開の失敗
CSCwo74496	無関係な BFD ピアがダウンした後、ASA が着信 BFD パケットを処理しないことが原因で BFD がフラップする
CSCwo75483	SNMP エージェントとして使用される HA の FTD マルチインスタンスでシャーシへの SNMP ポーリングが失敗する
CSCwo75810	SNMP 設定が同じ FTD のタイプとバージョン間で一貫して適用されない
CSCso76165	rsync によるデプロイメントの失敗

不具合 ID	タイトル
CSCwo76554	リバース SSL フローおよび TSID（TLS サーバーアイデンティティ）が有効になっている TLS ハンドシェイクが失敗する
CSCwo76644	FMC が正常性アラートを受信：「cgroup_monitor が 5 回終了しました（cgroup_monitor exited 5 time(s)）」
CSCwo77665	「低」に設定されている場合、FMC のポートスキャンイベントで誤った送信元/宛先が表示される
CSCwo78969	ユニットがクラスタに再参加するときのスレッド名 DATAPATH でのトレースバック
CSCwo79004	膨大な数のポリシーが存在する場合に見られる展開の遅延
CSCwo79028	フェイルオーバー後の FQDN 解決が次の DNS ポーリング間隔まで保留される
CSCwo79080	ENH：UDP トラフィックフローで、「show conn detail」の出力に Initiator フィールドと Responder フィールドが必要である。
CSCwo79114	再配置または移動操作に失敗した後にユーザーが保存すると、ルールが失われ、障害が発生する可能性がある
CSCwo79798	リロード後に暗号化チェックサムが変更される
CSCwo80223	代替パス経由で受信したシングルホップ BFD セッションで BFD パケットがドロップされない
CSCwo80682	FMC GUI の [ポリシー（Policy）] > [アラート（Policy）] > [侵入電子メール（Intrusion Emails）] で変更を複数回保存すると、前の変更が削除される
CSCwo82639	ローカルユーザーの詳細がクラスタセットアップのデータノードに複製されない。
CSCwo82658	ASDM：アイデンティティ証明書を追加するときに、キーペアがすでに存在するというエラーが表示される
CSCwo83087	BGP の一般設定の UI に手動ルータ ID が表示されない
CSCwo84467	DATA ノードがまだ一括同期状態のときに BGP が即座に起動する L3 クラスタリング
CSCwo84825	CSF4200 management1/2 インターフェイスが、物理的に切断されているにもかかわらず、Lina で up/up と表示される
CSCwo84910	データノードのデータベースで展開の失敗が更新されない

不具合 ID	タイトル
CSCwo85252	BGP 設定を取得しようとすると、FMC ページがロード状態でスタックする
CSCwo86556	FTD ハブアンドスポーク VPN トポロジ：DHCP が外部 IP に使用される場合、バックアップ VTI が失敗する
CSCwo86835	レルム同期が原因で SMB リモート FMC バックアップが失敗する
CSCwo87219	CPU コア数が最小要件を下回っている場合の起動時の警告
CSCwo87763	ASA/FTD：HA セットアップでのリロード後にプライマリスタンバイユニットがアクティブになる
CSCwo87938	バックアウトの変更により、FIPS モードでクラスタリングを有効にできない
CSCwo88204	sch_dispatch_to_url での Smart Call Home プロセスによって ASA/FTD のトレースバックとリロードが発生する
CSCwo88518	クラスター内のいずれかのノードでコマンドレプリケーションが失敗した場合、クラスターからノードを FMC にキックアウトする
CSCwo88745	参照されたオブジェクトがない場合、ポリシー展開でエントリが書き込まれない
CSCwo89233	アクセスリスト後のコマンド commit noconfirm revert-save でクラスターノードへのコマンド複製が失敗し、追加のデバッグが発生する
CSCwo89802	センサーごとにホスト数を表示する FMC カスタムウィジェットに正しくないセンサー名が表示される
CSCwo90300	セキュリティゾーン内の古いセンサー参照が原因で「ポリシー検証中にエラーが発生しました。内部エラーによりシステムの...（Error during policy validation An internal error is preventing the system... ）」と表示される
CSCwo91049	RADIUS アカウンティング応答メッセージがない場合、シャーシからインスタンスへの接続が遅延または失敗する可能性がある
CSCwo91124	FTD：ユーザーグループの過剰なロギング
CSCwo91436	FPR 4125 マルチインスタンス：Snort およびシステムコアの 高 CPU 使用率（100%）により FMC 重大アラートが発生する
CSCwo91631	FMC が LDAP 経由で AD レルムからユーザーグループをダウンロードできない
CSCwo91965	ASAv が予期せず再起動する

不具合 ID	タイトル
CSCwo92386	HA セカンダリデバイスがアクティブになっている場合、cdFMC がインターフェイスとセキュリティゾーンを表示しない
CSCwo92447	SecureX とのアクティブな統合がないにもかかわらず、FMC に SSE 登録失敗アラームが表示される
CSCwo93174	重複する VTI によって VPN フラップが発生する
CSCwo93444	FTD クラスタ：Snort エンジンの再起動がタイムアウトになったときのログが正しくない
CSCwo94274	FP4100/930 の致命的なエラー：リセットコード 0x0040 でウォッチドッグ前に未完了のチェーンが観察された
CSCwo94483	非 CP スレッドでのトレースバック後に LINA がリロードせずに非アクティブのままになる
CSCwo95586	「脅威設定の変更（Modify Threat Configuration）」権限を持つユーザーは、アクセス コントロール ポリシー（ACP）ルール内で侵入/ファイルポリシーを変更できない
CSCwo96377	セカンダリアドレスは、管理にデータインターフェイスを使用する場合に、FMC 管理対象 FTD に対してのみ設定できるようにする必要がある
CSCwo96854	作成中の UI ロックの問題によって、FMC GUI を介して FTD-HA を編集または解除できない
CSCwo96941	[ヘルスモニター（Health Monitor）]ページのディスク ステータス ウィザードで、ディスク合計が増え続ける
CSCwo98752	クラスタへの再参加を試みる際の、スレッド名 DATAPATH でのトレースバック
CSCwo99544	FTD 外部認証で AD ユーザーの数が多すぎる場合、無効にすると展開が失敗する可能性がある
CSCwp00618	HMS の DB への挿入時にデッドロックが発生し、「アプライアンスに到達できません（Appliance unreachable）」という理由で、デバイスがオフラインで表示される
CSCwp01015	機能 mp_percore での ASA/FTD のトレースバックとリロード
CSCwp02224	プライマリ/スタンバイデバイスの FXOS バージョンをアップグレードすると、FPR フェイルオーバー スプリット ブレインが発生する
CSCwp03910	1 つのドメインがカスタム DNS SI ブロックリストにヒットすると、後続の DNS パケットが単一のフローでドロップされる

不具合 ID	タイトル
CSCwp04235	ASA のトレースバックとリロード
CSCwp06882	Hyper-V で実行している ASA を 9.20.3.9 から 9.20.3.16 にアップグレードした後に CPU 使用率が高くなる
CSCwp07108	アップグレード後の最初の展開中に、脅威検出で Lina がクラッシュする
CSCwp07785	エラー 500：子ドメイン ACP で使用されるグローバルドメイン侵入ポリシーのレポートを生成する際の FMC の内部サーバーエラー
CSCwp08772	ASA：tls-proxy maximum-session コマンドエラー
CSCwp10957	SSL エラーにより、Cisco Smart Software Manager（CSSM）への接続が終了する
CSCwp11382	ASA/FTD：ssl trust-point コマンドがリロード後に削除された
CSCwp11503	Firepower デバイスで RADIUS ダイナミック プロビジョニングが有効になっている場合、ユーザーの作成が失敗する
CSCwp11971	「不正な形式の JSON 文字列（Malformed JSON String）」例外によって FMC GUI がアクセス不能で空白になる
CSCwp11985	FMC アップグレード後に展開が必須となる条件をアップグレードコードに含める必要がある
CSCwp12712	DHCP リレーのクライアント側インターフェイスの設定時に FMC UI が正常に機能しない
CSCwp13016	FTD/ASA SSH：端末モニターにログが表示されない
CSCwp13412	TS 生成に問題がある場合に生成のトラブルシュート用のログファイルが存在しない
CSCwp13540	クライアントレス VPN のファイルパスに日本語テキストを使用したファイルのアップロードに対して、誤った URL が表示される
CSCwp14919	Firepower bandwidth_analyzer.pl スクリプトで、'--size' オプションの適切な入力検証が実行されない
CSCwp15886	Snort2 から Snort3 にアップグレードした後、いくつかの IPS ルールアクションを変更できない
CSCwp16323	FMC 監査の tcp-tls syslog が切り捨てられているか、誤った形式となる
CSCwp16529	「show cluster info load-monitor details」を使用すると、バッファドロップに対して負の値が表示される

不具合 ID	タイトル
CSCwp16546	S2S モニタリング UI で NAT 下にスポークがあると、トンネルステータスに「アクティブデータなし（No Active Data）」と表示される
CSCwp16739	ASA クラッシュ情報ファイルが FP4200 デバイスで生成されない
CSCwp17700	少なくとも 1 つの syslog ホストで EMBLEM 形式が有効になっている場合、Syslog 形式が正しく出力されない。
CSCwp18136	破損した SXP ファイルの読み取り中に ADI でコアダンプが発生する
CSCwp21630	FTD：「プルーニングされたmemcapフロー（Pruned memcap flows）」の発生後に「Blacklist（ブラックリスト）」が理由でトラフィックがドロップされる
CSCwp22214	トラフィックがボックスを通過しているときに、複数のメールドロップと enq の失敗が発生する
CSCwp22237	FMC 上での展開失敗の理由とトランスクリプトの更新
CSCwp22612	Umbrella DNS 設定を削除しようとすると、FTD でポリシー展開が失敗する
CSCwp22743	wpk - 1gsx リンクは wpk で稼働中だが、スイッチ側では接続されていないと表示される
CSCwp24119	FDM で展開タスクが「キュー登録済み（Queued）」状態でスタック状態になる
CSCwp25033	ICMP に到達できないストームにより、2 ユニットの FTD クラスタで CPU が高くなる可能性があります
CSCwp26815	スタンバイ ASA デバイスでの「WebVPNタイマープロセス」による CPU 使用率
CSCwp27718	「NGFW_UPGRADE がマップに存在しません（NGFW_UPGRADE is missing in map）」が原因で FMC の展開がハングして失敗する
CSCwp28229	ファイルダウンロードが 2.1 GB 前後で停止する
CSCwp28801	WA HA：FTD HA のメタデータを取得中にエラーが発生する
CSCwp29273	SAML SSO ユーザー名の大文字と小文字の違いによりログインループが発生する
CSCwp29808	FMC が重複しない IPv6 ホストオブジェクトグループを完全に重複したオブジェクトグループとして報告する
CSCwp32352	インデックス作成が機能しない場合に展開が失敗する

不具合 ID	タイトル
CSCwp32949	ZTNA ポリシーで ECMP ゾーン メンバー インターフェイスを選択すると展開に失敗する
CSCwp33077	SAML IdP エンティティ ID が 128 文字の上限より増加する
CSCwp33410	dmesg および kern.log ファイルが Tx Queue=0 ログでフラッディングする
CSCwp34610	Windows および MacOS ネイティブ VPN クライアントで IKEv2-EAP 認証が失敗する
CSCwp36133	インターフェイス PAT（接続先インターフェイス）へのフォールスルーの動作が期待どおりに機能しないため、動作を明確にする。
CSCwp37128	estreamer debug コマンドで期待される出力が生成されない
CSCwp37284	ユーザーが [クライアントレス VPN] ページからログアウトをクリックすると、「CSRF Token Mismatch」エラーが表示される。
CSCwp38220	IPv6 コンテンツを含むルールを編集すると内部エラーが表示される
CSCwp38436	FMC での登録後にシャーシのシリアル番号が空になる
CSCwp38565	バックアップ中にリモートストレージへのコピーが失敗すると、一時的な tar ファイルのクリーンアップが行われない
CSCwp39148	タイムスタンプ値が低い user_ip_map.snapshot が存在すると、スナップショットが頻繁に作成される
CSCwp39266	セカンダリがアプリケーション同期をスキップし、ブートストラップ設定の適用後にすぐにアクティブになると、展開後にトラフィックが低下する
CSCwp39319	大規模な CRL の処理中に ASA メモリがリークする。
CSCwp59765	ACP の LDAP ユーザーでレルムが常に非同期と表示される
CSCwp64615	ASA/FTD：'invalid-ip-length' または 'sp-security-failed' の ASP ドロップキャプチャが、一致基準で機能しない。
CSCwp65900	お客様 DU CONSULT、NPS 6：IP またはポートの完全一致のための ACP 検索の切り替え
CSCwp66721	SSL 暗号化でのメモリリークにより、FTD 7.7.0 を実行しているローエンドデバイスで Lina メモリ使用率が高くなる
CSCwp67356	HA 状態が ColdStandby から Active に移行しない
CSCwp80058	FMC 自動展開タスクが繰り返し実行に失敗する

不具合 ID	タイトル
CSCwp80253	URL フィルタリングのダウンロード失敗：talosAgent が FMC で繰り返し終了する
CSCwp83566	SSL - FTD アップグレード後に、アップグレード後の Chrome および Edge で特定のサイトの DND の問題が発生する
CSCwp84206	FMC - CSDAC：マスター UI の過剰な DNS クエリ
CSCwp84585	TCP RST パケットが、設定された地理位置情報ベースのルールに一致しない
CSCwp89969	ファイアウォールの再起動/リブート完了により遅延が発生する
CSCwp90780	.tgz コンテキストファイルを復元すると、割り当てられたインターフェイスが 'system' 設定から削除される
CSCwp91460	snort-unified.log が原因でディスク使用率が高くなる
CSCwp92489	SFDataCorrelator_user_id_mismatch.log によるディスク容量の過剰使用
CSCwp92495	セキュリティゾーンのロードを伴うインターフェイスの追加に 30 秒以上かかる
CSCwp92644	FMC ダイナミックオブジェクトが 1000 個に制限される
CSCwp93368	Azure に展開された FTDv ファイアウォールで LINA トレースバックが観測された：snp_vxlan_encap_and_send_to_remote_peer
CSCwp97402	WA：大規模な snmp 設定がある展開中に、tmatch テーブルでロックの競合が発生するため、トレースバックおよびリロードする
CSCwp97862	フェイルオーバー IPSEC PSK が 78 文字以上の場合、HA が「Could not set failover ipsecpre-shared-key」で中断する
CSCwp97933	FMC GUI のインベントリ詳細に誤ったコンプライアンスモードが表示される
CSCwp98971	FTD トラブルシュートファイルに欠落しているファイルがある
CSCwq01305	FMC ダッシュボードの時間経過に伴う動的分析で「データなし（No Data）」と表示される
CSCwq07197	FMC によって管理される Firepower Chassis Manager 4225 のインターフェイスステータスの可視性に関する問題
CSCwq07441	HA で設定されたインターフェイスのモニタリングが原因で、ASA を実行している FP2110 でメモリリークが観測された

不具合 ID	タイトル
CSCwq07808	イーサネットインターフェイスで速度を変更した後、FP3105 トレースバックとリロードが発生する
CSCwq09614	Snort が SCTP パケットをドロップし、SCTP 接続をブロックすることがある
CSCwq13348	VNI クラスターリンクがデフォルトでパブリック範囲 1.1.1.0/24 の IP アドレスを使用する
CSCwq14900	システムがアイドル状態の場合でも、監査ログにセッション有効期限エントリが繰り返し表示される
CSCwq16926	2 つのプロセスが TD サブネット構造を解放しようとすると、トレースバックとリロードが発生する
CSCwq17612	HA によってリロードがトリガーされると、コンソールに誤った「フェイルオーバーリセット」ログが出力される。
CSCwq20535	大文字と小文字を区別するインターフェイス名が原因で、management-data-interface コマンドが「インターフェイスの有効化に失敗しました（Enable of interface failed）」というエラーで失敗する
CSCwq20891	DAP 後に CoA 処理が停止する
CSCwq21442	3RU MI インスタンスがベースラインまたは作成後にオフラインになる
CSCwq22206	IPSEC-Rekey イベント後に S2S VPN が回復しない
CSCwq23394	FTD が mlx5 ドライバレベルで Azure クラウドでのトラフィックをドロップする場合がある
CSCwq26503	ポリシー展開タスクは無期限にスタック状態になるべきではない
CSCwq26863	FP2110 - ntpd プロセスが常にクラッシュする
CSCwq27217	ASA：脅威検出時にトレースバックとリロードが発生し、その後インターフェイスが不安定になる。
CSCwq28003	以降の展開の失敗を避けるために、展開中の重複メッセージを CD で破棄する
CSCwq29010	Snort3 が ESMTP トラフィックを断続的にブロックし、IPS シグネチャ 124:1:2 をトリガーする
CSCwq29375	ASA/FTD：FP_PUNT の置換中にアサートがトリガーされた（aaa アカウントの一致）
CSCwq29706	SNMP 設定を編集後に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
CSCwq29765	Snort 2 カスタムルールの変換に失敗する。詳細については、/var/sf/htdocs/ips/snort.rej を参照してください。
CSCwq30062	/tmp のディスク容量が不足しているため、ローカル FTD バックアップが失敗する
CSCwq30330	長時間実行されている AQ タスクは FMC でのタイムアウト後に強制終了されるが、FTD の対応するバックアップタスクは引き続き実行される
CSCwq31342	DNS 設定で FPR4200 | FPR3100 マルチインスタンスシャーシの展開が失敗した
CSCwq31988	FPR1010 のすべてのインターフェイスでエラーが発生する | 回線プロトコルがダウンする（スーパーバイザに関連付けられない）
CSCwq32085	crypto_archive を生成した後に FP3100/4200 を再起動すると、「KC ILK issue detected」というエラーがコンソールで発生した
CSCwq35960	OSPF：高可用性セットアップでの高 CPU 使用率、ルートフラップ、Lina トレースバックおよびリロード。
CSCwq36466	expat/xml FW が自身をリブートしたが、クラッシュ情報が生成されない
CSCwq36564	セカンダリ FMC-HA ピア除外リストがネットワーク検出で有効にならない
CSCwq39149	VDB 更新を手動でダウンロードする場合、VDB 更新がページに表示されるようにするには、Web ブラウザを手動で更新する必要がある
CSCwq43365	ダイナミック属性コネクタのステータスに、1 つ以上のサービスが異常であることが示される
CSCwq43711	アイドル SSH セッションが Fin フラグで正常に終了せず、設定されたタイムアウトを超えて存続する
CSCwq44862	syslog/estreamer を介した侵入イベントパケットデータに、大きなパケットのパケットデータが表示されない
CSCwq45017	SmartLicensing は特定の特殊文字を受け入れる必要がある
CSCwq46058	ASA SNMP 応答の問題：奇数の OID に対してのみ応答が送信され、偶数には送信されない
CSCwq47622	'TLS サーバーアイデンティティ検出' を有効にした後、Lina がトレースバックおよびリロードする
CSCwq47694	S2S VPN を設定する場合、アイデンティティの電子メール ID にプラス記号を使用できない

不具合 ID	タイトル
CSCwq48085	FTD HA の形成直後に展開が失敗する
CSCwq48842	FTD：Snort を介した遅延パケットが発生したため、tcp-seq-past-win によってパケットがドロップされた
CSCwq50189	ASAv の展開が失敗した：コンソールが連続してスタック状態になる
CSCwq50373	HA での ASA/FTD：ブートアップ中の snmptranslate プロセスにより、高 CPU および IPC タイムアウトが発生し、スプリットブレインを引き起こす
CSCwq52255	FTD 管理 IP アドレスへの SSH ログインで、/mnt/boot/application/*.de ファイルがないため、FTD CLISH ではなく FXOS シェルにログインする。
CSCwq53328	マルチキャストおよびユニキャストパケットが、ランダムなサブインターフェイスの正しいインスタンスに到達しない。
CSCwq54109	FTD 3130 HA Lina がトレースバックする（ikev2_bin2hex_string）
CSCwq55841	FMC アップグレードが 999_update_onpremfmc_diskcache.sh で無期限に停止する
CSCwq56279	7.6 - Firepower 3100 シリーズ：CSCso00444 の修正が含まれていないバージョンから HA ペアを 7.6 にアップグレードすると、一部のファイアウォールがトレースバックおよびリロードループに入る。
CSCwq57394	FMC が US クラウドに接続できない場合、ダイナミック分析接続のクラウド設定を編集できない
CSCwq60125	着信トラフィックが「リセットしてブロック」ルールにヒットしても、FTD がリセットパケットを送信しない
CSCwq60586	バンドルイメージ存在検証エラーにより、FTD アップグレードが失敗した
CSCwq65955	FPR 4200：HA リンク ARP パケットがドロップされ、内部アップリンク linkChange カウンタが増加する
CSCwq66838	サービスオーケストレーションから複数のハートビート応答の失敗が確認される
CSCwq69599	レガシー UI でユーザーを削除すると、FMC ACP の上位ユーザーが削除される
CSCwq70133	パスワードを変更した後、パスワードの有効期限がリセットされない
CSCwq70511	無効なルールが存在しても、Snort3 ルールの推奨事項では 0 と表示される
CSCwq70773	ASP ルールエンジンの問題を完全およびランタイムで表示

不具合 ID	タイトル
CSCwq71338	非 SSL トラフィックが SSLv2 として誤って分類され、TSID が有効になっている場合にドロップされる
CSCwq72156	特定の条件において、複数の SNMP サーバーのいずれかに SNMP トラップが送信されない
CSCwq73994	ASA：Hyper-V でパフォーマンスと高い CPU 使用率が見られた
CSCwq74204	IKEv1 L2Lvpn がフェーズ 2 で、アップグレード後に "Rejecting IPsec tunnel: no matching crypto map entry" で失敗する。
CSCwq74986	FTD：起動ループでインスタンスがスタック状態になる
CSCwq77569	ClusterPostUpgradeHandler からのアクティビティ ID のリークが原因で SRU アップグレードが失敗する
CSCwq78813	新しい UI でアクセス コントロール ポリシーをロードするときに、断続的に空白の画面が表示される
CSCwq79940	トンネル保護 ipsec ポリシー機能がバックアップ VTI トンネルで動作しない
CSCwq83395	http Opportunistic TLS のプローブがない
CSCwq85986	FP4225：SFP を含むインターフェイス：10/25G_LR_S（または CSR_S）が、ピア側のリブート後に起動しない。
CSCwq86675	Tomcat のキャッシュ内のセッション数の設定が正しくない
CSCwq92373	WA MI：2 つのアプリケーションが次の理由で応答しなくなる：アプリケーションインスタンス ftd. sma のエラーが報告された。再起動ループが原因で、インスタンス xxx が無効になっている。このアプリケーションインスタンスの再インストールを検討してください。
CSCwq92436	NAS：識別子属性の値は常に「sshd」
CSCwq92728	SSH 認証の TACACS+ 要求に ASA クライアント IP がない
CSCwq94584	OPPORTUNISTIC_TLS での HTTP インスペクタのサポート
CSCwq95241	Heimdall PID がないため FP2130 で再起動する
CSCwq95649	200MB を超える Secure Firewall ポスチャイメージファイルをアップロードできない
CSCwq95810	「no http server Basic-auth-client ASDM」で、ASDM から ASA への接続が許可される。
CSCwq95837	オブジェクトの重複の削除で無関係のオブジェクトを削除できる

不具合 ID	タイトル
CSCwq96870	Firepower のシャットダウン時にインターフェイスが起動する
CSCwq98101	FTD HA でインラインセットが設定されている場合、ポリシー展開が失敗する
CSCwq98155	ACP でストレステストが行われると「アクセストークンが無効です（Access token invalid）」というプロンプトが表示される
CSCwq98648	ASAv で RAM 割り当てが少ないと、'asdm image' コマンドで予期しない動作をトリガーする
CSCwr00711	30 文字を超える名前のインターフェイス オブジェクトを削除できない
CSCwr05406	natAddrMapTable での snmpwalk 中に、HA stby ノードでトレースバックする
CSCwr05837	SNMP プロセスが継続的に再起動する
CSCwr06027	FMC はリモート ストレージのホスト名設定で下線文字を受け入れない
CSCwr11851	スタンバイ FMC が ids_event_class_map テーブルの同期に失敗し、誤って分類された侵入イベントを発生させる
CSCwr12965	HA の両方のユニットが同時に暗号化アルゴリズムを変更した
CSCwr14186	"show asp drop" コマンドの使用方法に cmd-invalid-encap asp-drop タイプのコンテキストを追加
CSCwr15697	80 の枯渇による ssl_decrypt_cb のブロック
CSCwr18291	FMC の 4200 インターフェイスイメージがデバイスのインターフェイスの順序と一致しない
CSCwr19123	スタンバイがアクティブに変更されると、FPR HA ESP シーケンス番号の不一致により、アンチリプレイドロップが発生する。
CSCwr21323	ユーザーロールのエスカレーションによる FMC GUI 機能の使用により、GUI セッション中にユーザーがすべての権限を失うことがある
CSCwr21683	デプロイメントによってパフォーマンスプロファイルが変更され、実行中の構成を取得できない
CSCwr22256	FQDN リストが解決済み IP の 200 を超えるエントリを拡張しているときに、トレースバックが発生する
CSCwr22508	アップグレードが成功した後に、デバイスが起動せず、スタック状態になる

不具合 ID	タイトル
CSCwr24365	SRU トリガーのポリシー展開が、FMC HA およびスタンドアロンのアップグレード中、初期/スタンバイ FMC の後に発生する
CSCwr25124	600_schema/103_csm_cfgdbmigration.sh で FMC のアップグレードが失敗する
CSCwr26857	アイドル状態ではないにもかかわらず、1 時間後に SMB TCP 接続が終了したため、ファイルポリシーが動作を停止した
CSCwr27095	以前の tunnel-group に基づいて、AnyConnect ユーザーがプロンプトを誤って取得する
CSCwr28908	ASA：asdm イメージを保存した後にトレースバックとリロードが発生する
CSCwr31782	Cisco Secure Client SAML：IKEv2-IPsec と証明書マッピングを使用すると、外部ブラウザで証明書を要求することがある
CSCwr42577	ASA/FTD がスレッド名「lina」を障害元スレッドに挙げてトレースバックし、リロードすることがある。
CSCwr43586	「Unable to obtain connection lock (connection-lock)」という理由により、自己発信 ICMP TTL 超過メッセージが断続的にドロップする
CSCwr45484	通信が中断された場合、FTD ポリシー展開が FMC で失敗したと誤ってレポートされる
CSCwr48605	パケットで誤ったオプションを受信したため Lina がトレースバックする。
CSCwr49028	SDI プロトコルを使用すると、セキュア クライアント トンネル グループ認証が影響を受ける。
CSCwr49171	Nitrox と KC2 間のインターラケン（ILK）リンク障害により、トラフィックバックプレッシャ/トラフィック障害が発生する
CSCwr50466	ASA/FTD：'show ssl objects' で X509_STORE_CTX に誤った値が表示される。
CSCwr51629	RTSP フローが、"First TCP packet not SYN" というドロップ理由でドロップされる
CSCwr55089	ASA/FTD：スレッド名 DATAPATH でトレースバックおよびリロードが発生する
CSCwr57647	GCP の FMC における 000_start/112_CF_check.sh でのアップグレード失敗
CSCwr59870	Hyper-v で Netvsc ドライバを実行すると、ブートループの問題が発生する

不具合 ID	タイトル
CSCwr62800	ASAv で高いネットワーク遅延が観察された
CSCwr66525	snp_nat_allocate_port でクラスタの形成中に lina コアダンプが生成され WPK ノードがリブートする
CSCwr73236	WA 4245：9.22.2.15 ビルドにアップグレードした後、デバイスが継続的にクラッシュするようになる
CSCwr79344	Lina で ASA/FTD がトレースバックおよびリロードする
CSCwr84332	L2 vaccess_nameif_action スレッドで ASA/FTD がトレースバックおよびリロードする
CSCwr84343	L2 テーブル作成時の ASA/FTD トレースバックとリロードが失敗する
CSCwr88733	「show tech-support fprm」を収集すると、TAR プロセスでコアファイルが生成される
CSCws03807	仮想アクセスの nameif 文字列でのメモリリーク
CSCws06387	SNMP：add_table_to_mib_list() でのメモリ割り当て失敗により、MIB テーブルの登録中に無限ループが発生する可能性がある
CSCws07111	WA：ポートマネージャ：エラー：イーサネット インターフェイスに対して 'no shut' を実行後、ポートマネージャが DIED になる
CSCws21415	Inotify ユーザーのウォッチの制限が、MI FTD を実行している 3100 および 4200 プラットフォームの調整を要求する
CSCws31878	サーバーで行われた新しい変更で、新しいバージョンの FMC によって管理される FTD への外部認証ログインが失敗することがある

バージョン 7.6.3 で解決済みのバグ

表の最終更新日：2025-10-23

表 *19* : バージョン *7.6.3* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーの不正アクセスの脆弱性
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのリモートコード実行の脆弱性

表の最終更新日：2025-10-23

表 *20* : バージョン *7.6.3* で解決済みの機能バグ

不具合 ID	タイトル
CSCso76165	rsync によるデプロイメントの失敗
CSCwq32085	FP3100 は、コンソールに「KC ILK の問題が検出されました（KC ILK issue detected）」というエラーを表示し、crypto_archive を生成した後に再起動する
CSCwq35960	OSPF：高可用性セットアップの両方のユニットで Lina がトレースバックおよびリロードする。
CSCwr22492	ASA/FTD：200 を超えるアドレスに解決する FQDN オブジェクトが原因でトレースバックとリロードが発生する

バージョン 7.6.2.1 で解決済みのバグ

表の最終更新日：2025 年 9 月 25 日

表 *21* : バージョン *7.6.2.1* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーの不正アクセスの脆弱性
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのリモートコード実行の脆弱性

バージョン 7.6.2 で解決済みのバグ

表の最終更新日：2025-08-11

表 *22* : バージョン *7.6.2* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwq03404	クラス属性が使用されている場合、RADIUS から FMC UI への外部認証ログインが失敗することがある
CSCwq10344	FMC のアップグレード後、FMC RADIUS 外部認証アクセスリクエストに 6 つの属性がない

表の最終更新日：2025-08-11

表 *23* : バージョン *7.6.2* で解決済みの機能バグ

不具合 ID	タイトル
CSCwk37929	スタンドアロン 2110 を 6.6.7-223 から 7.2.8-25 にアップグレードすると、FMC で「インターフェイスが変更されました」というアラートが発生する
CSCwn71596	インターフェイスリンクのダウン（Init、mac-link-down）が確認された：ケーブルの取り外し/再接続後に EtherChannel メンバーシップがダウン/ダウン/ダウンの状態になる
CSCwo45449	1 つの Snort3 スレッドが応答しなくなった場合でも、ウォッチドッグがトリガーされることを確認する。
CSCwo71835	FMC の Access-Request に NAS-IP-Address 属性がない
CSCwo98670	FTD MI：アップグレード後に SNMP ポーリングが機能しない
CSCwp14123	Tmatch メモリが、主に ARP-DP によって消費される。
CSCwq21804	FTD：invalid-ip-length が原因で LINA によってインジェクト/トリミングされたパケットがドロップされる
CSCwq37519	スタンバイ FMC が、期限切れ/欠落している証明書を置き換えるためにアクティブな FMC から Talos 証明書をコピーできない場合がある

バージョン 7.6.1 で解決済みのバグ

表の最終更新日：2025 年 6 月 2 日

表 *24* : バージョン *7.6.1* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwf89838	OpenPrinting CUPS は、標準ベースのオープンソース印刷システム
CSCwh71228	GLib に欠陥が見つかった。GVariant の逆シリアル化で検証に失敗する
CSCwh71231	GLib に欠陥が見つかった。GVariant の逆シリアル化に脆弱性があり
CSCwh71232	GLib に欠陥が見つかった。GVariant の逆シリアル化コードは
CSCwh71233	GLib に欠陥が見つかった。GVariant の逆シリアル化コードに脆弱性があり
CSCwh71234	GLib に欠陥が見つかった。GVariant の逆シリアル化に脆弱性があり
CSCwh71515	BusyBox v1.33.2 の CPIO コマンドにある問題により、攻撃者が

不具合 ID	タイトル
CSCwe00713	Libtiff の tiffcrop ユーティリティでメモリリークの欠陥が見つかった。この問題
CSCwe00716	LibTIFF は、整数のオーバーフローに対して脆弱である。この欠陥により、リモート
CSCwe00717	libtiff で脆弱性が見つかった。原因：複数の潜在的な整数の
CSCwi24022	6.5.9 までの Linux カーネルで問題が検出された。競合中
CSCwi24116	Twisted はインターネット アプリケーション用のイベントベースのフレームワーク。Prior t
CSCwi49557	cryptography は、暗号プリミティブを公開するように設計されたパッケージ
CSCwi60427	この欠陥により、悪意のある HTTP サーバーが「スーパークッキー」を設定
CSCwi78200	GnuTLS に脆弱性が見つかった。不正な形式の c への応答時間
CSCwi92930	1.6.0 より前の linux-pam（別名 Linux PAM）で、攻撃者が den を引き起こす
CSCwi92932	Linux カーネル 6.7.1 までの drivers/md/dm-ioctl.c 内の copy_params
CSCwi98274	2005 からの unzip 5.52 に複数の脆弱性が含まれる
CSCwj08155	9.0.2142 より前の Vim で、言語マップの設定エラーが原因でスタックベースのバッファオーバーフローが発生
CSCwj43353	DMA リエントランシーの問題が原因で、use-after-free エラーが見つかった
CSCwj43466	heap-buffer-overflow の脆弱性が LibTIFF、extractI に見つかった
CSCwj45632	静的ルートまたは ACL に関連する展開の失敗が FDM で確認された
CSCwj79229	FMC：外部認証プロファイル「Radius サーバーキー」のプレーンテキストパスワード
CSCwj89224	Linux カーネルにパーティション分割エラーが存在しました CVE-2023-52458
CSCwj89335	Linux カーネルで、次の脆弱性が解決された：e
CSCwj89337	Linux カーネルで、次の脆弱性が解決された。s
CSCwj89412	Linux カーネルで、次の脆弱性が解決された。m
CSCwj89417	Linux カーネルで、次の脆弱性が解決された。d

不具合 ID	タイトル
CSCwj89435	GnuTLS に欠陥が見つかった。Minerva 攻撃は暗号の脆弱性
CSCwj89439	GnuTLS に欠陥が見つかり、アプリケーションがクラッシュする可能性
CSCwk05826	nscd：netgroup キャッシュでのスタックベースのバッファオーバーフロー（Name Servi
CSCwk05827	nscd：notfound 応答の後に null ポインタでクラッシュする
CSCwk05828	nscd：メモリ割り当て失敗時に netgroup キャッシュがデーモンを終了する可能性がある
CSCwk05830	nscd：netgroup キャッシュは NSS コールバックがバッファ内の文字列を使用すると想定
CSCwk08241	FTD が ACL の FQDN を断続的に解決しない
CSCwk12484	復号して再署名/既知のキールールで暗号やバージョンフィルタが設定されないように UI を更新
CSCwk22993	Linux カーネルで、次の脆弱性が解決された。t
CSCwk25751	Linux カーネルで、次の脆弱性が解決された。n
CSCwk25762	Linux カーネルで、次の脆弱性が解決された。i
CSCwk25764	Linux カーネルで、次の脆弱性が解決された。H
CSCwk25765	Linux カーネルで、次の脆弱性が解決された。i
CSCwk44245	Linux カーネルで、次の脆弱性が解決された。i
CSCwk44246	Linux カーネルで、次の脆弱性が解決された。i
CSCwk44247	Linux カーネルで、次の脆弱性が解決された。b
CSCwk57949	linux-kernel CVE-2023-52435 の脆弱性
CSCwk57953	linux-kernel CVE-2023-52463 の脆弱性
CSCwk66255	urllib3 は Python の使いやすい HTTP クライアントライブラリ。※
CSCwk67859	FTD と FXOS：RADIUS プロトコルスプーフィングの脆弱性（Blast-RADIUS）：2024 年 7 月
CSCwk67902	FTD：RADIUS プロトコルスプーフィングの脆弱性（Blast-RADIUS）：2024 年 7 月
CSCwk69454	FDM：Blast-RADIUS CVE-2024-3596

不具合 ID	タイトル
CSCwk71817	FMC：Blast-RADIUS CVE-2024-3596
CSCwk71992	pix-asa（メッセージ オーセンティケータ）に対する BlastRADIUS の脆弱性のフェーズ 1 修正
CSCwk72477	Snort3 で "metadata:impact_flag red" を含むカスタムルールが影響レベル 1 として検出されない
CSCwk75037	Linux カーネルで、次の脆弱性が解決された。x
CSCwm03675	Linux カーネルで、次の脆弱性が解決された。t
CSCwm03678	Linux カーネルで、次の脆弱性が解決された。b
CSCwm05570	7.6.0-68 から 7.7.0-1358 への vFMC アップグレードが失敗 @800_post/890_install_version_mastered_apps.pl
CSCwm12745	Linux カーネルで、次の脆弱性が解決された。a
CSCwm12751	Linux カーネルで（ata: libata-core の場合）、エラー時の null ポインタの逆参照を修正する
CSCwm12757	Linux カーネルで（tcp_metrics の場合）、送信元アドレスの長さを検証する
CSCwm12775	Linux カーネルで、次の脆弱性が解決された。c
CSCwm12910	Jinja は拡張可能なテンプレートエンジン。次の特別なプレースホルダ
CSCwm12911	Jinja は拡張可能なテンプレートエンジン。'xmlattr' フィルタ
CSCwm12913	Vim は、オープンソースのコマンドライン テキスト エディタ。Vim の v9.1.0647 未満
CSCwm29875	Linux カーネルで、次の脆弱性が解決された。n
CSCwm29876	Apache HTTP Server 2.4.5 の mod_rewrite での代替エンコーディングの問題
CSCwm29880	Linux カーネルで、次の脆弱性が解決された。i
CSCwm29882	Linux カーネルで、次の脆弱性が解決された。i
CSCwm29886	Linux カーネルで、次の脆弱性が解決された。n
CSCwm29889	Linux カーネルで、次の脆弱性が解決された。b
CSCwm41195	マルチインスタンス FTD のシャーシを編集しようとすると「要求のタイムアウト。後で再試行してください（Request Timed Out. Retry after sometime）」というメッセージが表示される

不具合 ID	タイトル
CSCwm42979	null ポインタ逆参照の欠陥が hugetlbfs_fill_super で見つかった
CSCwm43160	Linux カーネルで、次の脆弱性が解決された。m
CSCwm43165	Linux カーネルで、次の脆弱性が解決された。n
CSCwm43183	Linux カーネルで、次の脆弱性が解決された。n
CSCwm43186	Linux カーネルで、次の脆弱性が解決された。x
CSCwm43189	Linux カーネルで、次の脆弱性が解決された。f
CSCwm43193	Linux カーネルで、nvme：破棄リクエストの再試行時に特殊なペイロードの二重解放を回避
CSCwm43301	Linux カーネルで発生する可能性のある io_uring デッドロックを修正
CSCwm43304	Linux カーネルで、次の脆弱性が解決された。p
CSCwm43337	Linux カーネルで、次の脆弱性が解決された：e
CSCwm43339	Linux カーネルで、次の脆弱性が解決された。c
CSCwm44719	daq_pkt_msg での FTD Snort3 トレースバック
CSCwm49410	Cross-Origin-Opener-Policy が誤って設定されている
CSCwm50895	EMBLEM 形式の ACL ロギング メッセージにタブ/スペースが追加され、取り込みの問題が発生する
CSCwm57472	Linux カーネルで（filelock の場合）、fcntl/close 競合が検出されたときにロックを確実に削除する
CSCwm57484	Linux カーネルで（mm 内）、ダーティ スロットリング ロジックのオーバーフローを回避する
CSCwm75514	python-cryptography パッケージに欠陥が見つかった。この問題は
CSCwm75518	Linux カーネルで、次の脆弱性が解決された。f
CSCwm75527	Linux カーネルで、次の脆弱性が解決された。n
CSCwm75696	Linux カーネルで（dma の場合）、dmam_free_coherent dmam_free_coherent() のコール順序を修正
CSCwm75706	Linux カーネルで、次の脆弱性が解決された。d
CSCwm75710	Linux カーネルファイルアクセス権限のアクセスチェックエラーを修正
CSCwm75717	Linux カーネルで、次の脆弱性が解決された。m

不具合 ID	タイトル
CSCwm75719	不良なボーレートで ioctl TIOCSSERIAL を呼び出す際の Linux カーネルのゼロ除算エラーを修正
CSCwm77247	デバイスにスペースが残っていないため FTD 復元が失敗する
CSCwm87847	Linux カーネルで、次の脆弱性が解決された。g
CSCwm87858	Linux カーネルで、次の脆弱性が解決された。n
CSCwm87876	Linux カーネルで、次の脆弱性が解決された。s
CSCwm87889	Linux カーネルで、次の脆弱性が解決された。x
CSCwm87897	Linux カーネルで、次の脆弱性が解決された。n
CSCwm87928	Linux カーネルで、次の脆弱性が解決された。v
CSCwm87933	Linux カーネルで、次の脆弱性が解決された。x
CSCwm87951	Linux カーネルで、次の脆弱性が解決された。n
CSCwm88098	Linux カーネルで、次の脆弱性が解決された。m
CSCwm88100	Linux カーネルで、次の脆弱性が解決された。f
CSCwm88105	2.6.3 より前の libexpat で問題が検出された。xmlparse.c は
CSCwm88115	Linux カーネルで、次の脆弱性が解決された：e
CSCwm88121	Linux カーネルで、次の脆弱性が解決された。K
CSCwm88133	Linux カーネルで、次の脆弱性が解決された。P
CSCwm95187	Redis は、ディスク上に永続するオープンソースのメモリ内データベースです。Aut
CSCwm95189	Redis は、ディスク上に永続するオープンソースのメモリ内データベースです。An
CSCwm95191	Linux カーネルで、次の脆弱性が解決された。s
CSCwm95206	Linux カーネルで、次の脆弱性が解決された。a
CSCwm95208	Linux カーネルで、次の脆弱性が解決された。r
CSCwm95213	Linux カーネルで、次の脆弱性が解決された：e
CSCwm95242	CPython に影響する MEDIUM 重大度の脆弱性がある。正規
CSCwm95243	CPython に影響する LOW 重大度の脆弱性がある。特に

不具合 ID	タイトル
CSCwn03652	CVE-2022-48975：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn03738	CVE-2024-47659：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn03740	CVE-2024-47660：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn21134	ユーザーが検証の使用法の種類を選択しない場合、FMC は no-validation-usage をトラストポイントにプッシュしない
CSCwn31143	CVE-2024-38538：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn55478	cdFMC：デバイスの NAT ポリシーと ACL でオブジェクトが再利用されている場合、展開中に NAT 拒否が発生する可能性がある
CSCwn58152	CVE-2023-52498：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58169	CVE-2023-52572：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58186	CVE-2023-52615：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58191	CVE-2024-26595：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58215	CVE-2024-46777：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58237	CVE-2024-47668：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58244	CVE-2024-47679：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58247	CVE-2024-47684：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58253	CVE-2024-47692：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58254	CVE-2024-47693：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58259	CVE-2024-47701：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58263	CVE-2024-47705：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58281	CVE-2024-47737：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58284	CVE-2024-47742：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58297	CVE-2024-49858：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58300	CVE-2024-49860：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58311	CVE-2024-49875：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58314	CVE-2024-49878：linux-kernel：Linux カーネルで、次の脆弱性...

不具合 ID	タイトル
CSCwn58316	CVE-2024-49881：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58318	CVE-2024-49882：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58319	CVE-2024-49883：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58320	CVE-2024-49884：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58323	CVE-2024-49889：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58397	CVE-2024-49948：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58399	CVE-2024-49949：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58404	CVE-2024-49954：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58405	CVE-2024-49955：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn58407	CVE-2024-49959：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn62947	CVE-2024-26958：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63003	CVE-2024-49983：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63018	CVE-2024-49995：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63050	CVE-2024-50036：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63076	CVE-2024-50083：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63104	CVE-2024-50131：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn63126	CVE-2024-50151：linux-kernel：Linux カーネルで、次の脆弱性...
CSCwn72848	Lina インターフェイス フラグメントの db キューサイズが 4294967295 で誤って固定される - Cisco ASA/FTD
CSCwn86912	拡張 ACL オブジェクトの数が数百を超える場合、それらのオブジェクトをロードできない
CSCwn88931	Snort3：アクティブ FTP 経由での FTP ファイル転送を実行中に、マルウェアポリシーがファイルを検出しない
CSCwn90937	Undici は、Node.js 用に新たに作成された HTTP/1.1 クライアント。Undici は
CSCwn90938	Undici は、Node.js 用に新たに作成された HTTP/1.1 クライアント。Undici は

不具合 ID	タイトル
CSCwn90939	Undici は、Node.js 用に新たに作成された HTTP/1.1 クライアント。攻撃者は
CSCwn91730	拡張 ACL オブジェクトの数が数百など非常に多い場合、FMC API の PUT 操作で更新に時間がかかる

表の最終更新日：2025 年 12 月 10 日

表 *25* : バージョン *7.6.1* で解決済みの機能バグ

不具合 ID	タイトル
CSCvi60913	「アドレスプールが使用中です（address-pool in use）」が原因で FTD 展開が失敗する
CSCvx66624	一部の FMC M5 アプライアンスで書き込みキャッシュが無効になる
CSCvz75335	ENH：[ヘルスモニター（Health Monitor）] > [インターフェイス（Interfaces）] で、[内部データ（Internal Data）] インターフェイスの 'no buffer' カウンタをモニターする
CSCwb77894	Firepower 1000/2100 が ROMMON モードにブートすることがある
CSCwc28374	大規模なアクセス コントロール ポリシーの検索機能で検索対象の値が見つからない
CSCwd03720	カスタム IPS ルールが存在し、varset 変数が欠落している場合、デプロイメントがブロックされる
CSCwd08448	FMC が cacert.pem 証明書の有効期限の 60 日前に正常性アラートを提供する
CSCwd80348	FMC はプロキシ設定を使用している Cisco Umbrella をサポートしない
CSCwd86472	S2SVPN リストページに誤ったエクストラネットデバイス名とタイプが表示される
CSCwe28608	SSL ポリシーがない状態で Snort が「SSL によるブロック」を返す。
CSCwe88492	設定時にバナーログインが表示されない
CSCwf04460	Ctrl+C を押して cancel show tech fprm detail コマンドを実行すると、fxos ディレクトリが表示されなくなる。
CSCwf25454	古い anyconnect エントリが原因でルーティングの問題が発生する
CSCwf27687	初期接続の不適切な管理によって Snort3 TCP フローキャッシュエントリが増加する

不具合 ID	タイトル
CSCwf66345	[API] グループ内のオブジェクトの検索が、ルール エディタ ウィンドウでフィルタ処理されない
CSCwf66818	FMC VPN 監視ダッシュボードで、スタンバイ FTD が HA ペアの VPN セッションオーナーとして誤って表示される
CSCwf78497	EIGRP flexconfig 移行 7.2.0 で、デフォルト設定でない no CLI は移行されるべきではない
CSCwh01312	ENH：IPv6 で設定すると、FMC 外部認証が SSH で機能しない
CSCwh11508	FMC で不明な文字を含む問題のある Snort3 ルールの作成を許可すべきではない
CSCwh17965	[表示] FXOS：リロード後に、PC メンバーインターフェイスがダウン状態で関連付けられていない/割り当てられていないと表示される
CSCwh25406	IMS 7.4.1-73 で継続的なトラフィックを実行中に Snort3 のコアダンプが発生する
CSCwh29131	FMC ポリシー分析：冗長性ロジックチェックの破損
CSCwh46732	TSID が有効な場合にリモートデスクトップ（RDP）トラフィックが失敗する
CSCwh71161	ASA|FTD：スレッド名 update_mem_reference でのトレースバックとリロード。
CSCwh73139	ACP ルールを編集しようとすると、同じ名前のルールが存在する
CSCwh82305	ポリシー展開中のスタンバイ FTD における swapcontext の Lina コア
CSCwh85829	新しい UI である [ユーザーアクティブセッション（Users Active Sessions）] の一部のシナリオで、最終確認が誤って更新される
CSCwi21909	FMC：BGP の変更が元に戻された場合、展開プレビューに "missing en-US:BGP" と表示される
CSCwi26712	AnyConnect プロファイルファイルがないため、展開に失敗する
CSCwi27093	ACP にネットワークを追加中に、グループからの無効な IPv4 ネットワークまたはホストリテラルが FMC にエラーとして表示される
CSCwi49884	VTI またはループバック インターフェイスが作成されると、TCP MSS がデフォルト値に戻される
CSCwi52623	DAP エンドポイント基準における誤解を招く証明書属性チェック

不具合 ID	タイトル
CSCwi71076	FTD_HA REST-API の遅延が原因でデバイスのリスト作成に時間がかかる：この現象は HealthMon ページのロード時に確認できる
CSCwi83185	誤ったエラーメッセージタイプが FMC に送信されたため、FMC 展開が失敗する
CSCwj00027	バックアップ失敗メッセージがユーザーの役に立っていない
CSCwj01785	FMC のネットワークリスクレポートに、データソースを選択するオプションがないため、レポートの生成が失敗する可能性がある
CSCwj09874	一部の FMC ページでの 413 エラーを回避するために、Tomcat および Apache の maxHeader サイズを増やす必要がある
CSCwj10923	FTD：制御とイベントが同じサブネット内で設定されている場合、sftunnel の不安定な接続の問題が発生する
CSCwj15125	ASA/FTD が Netflow タイマーインフラに関連するスレッド名「lina」でトレースバックし、リロードすることがある
CSCwj15181	すべての展開での BGP as-override のサポート
CSCwj15382	FTD-HA でマージされていない診断をマージすると、展開が FMC に表示されない
CSCwj22935	Snort の切り替え展開中にリブートが原因で、FTD HA ピア間での Snort バージョンの不一致が発生する
CSCwj28445	アクセス コントロール ポリシーのアプリケーションセクション内で追加の検索機能を許可する
CSCwj28468	外部認証の検証で誤った CLI アクセスユーザーが要求される
CSCwj44464	FXOS-FTD タイムゾーンの不一致により、ACP ルールが展開後に適用されない場合や、展開エラーが発生する場合がある
CSCwj63921	ファイルモジュールのメモリ破損による Snort3 トレースバックおよびリロード
CSCwj69107	FMC SSO 機能がオンになっていても、設定されていない場合、一部のクラウド機能が動作しない場合がある
CSCwj72013	デバイスがクラスタに参加すると、PAT プールを使用した PAT 通信が約 40 秒間失敗する
CSCwj80790	cdFMC およびオンプレミス FMC：デバイス管理/リストに、7.4.1 を実行している FPR-1K のシャーシ URL が表示される

不具合 ID	タイトル
CSCwj98673	シャーシのリブートで無効化されたコンテナを起動できず、Heimdall にアクティビティを記録できない
CSCwj99620	7.4.2 へのアップグレード後、S2S トンネルステータスが空で表示される
CSCwk06689	低速なネットワークでは、sftunnel は接続を STALE とラベル付けし続ける
CSCwk07250	スクリプト 120_check_legacy_private_cloud_for_ampkit.pl の実行中に、FMC のアップグレードが失敗する
CSCwk21915	Snort プラグインが原因でアップグレードの準備状況が失敗する
CSCwk22574	VTI 復号を許可するために SGT フレーム/パケットを削除
CSCwk26266	応答のみが設定されており、リバース ルート インジェクションが有効になっている場合、FTD は VPN ルートを取得できない
CSCwk30049	ASA/FTD がスレッド名「lina」を障害元スレッドに挙げてトレースバックし、リロードすることがある。
CSCwk30965	7.2.6 で AppIdSessionData により Snort3 がクラッシュする
CSCwk35710	EEM スクリプトで「show capture」コマンドが実行されると、FTD/LINA がトレースバックし、リロードすることがある
CSCwk38440	conn_meta null の場合、パケットを Snort に送信しない
CSCwk40335	IP アドレスに関連付けられた FQDN ID が設定された制限の 8 を超えると、アラート/警告をトリガーする
CSCwk40403	WebEx トラフィックが Snort3 でバイパスされない（許可ルール）
CSCwk41396	FMT を介した ASA から FTD への移行により、FMC バックエンド設定でインターフェイスグループが正しく設定されない
CSCwk42266	ゾーンベースの AC ルールにインターフェイスマッピングがない
CSCwk42676	仮想 ASA/FTD がスレッド PTHREAD でトレースバックし、リロードすることがある
CSCwk45975	SSL ポリシーの TLS1.3 復号設定が DND トラフィックに影響する。
CSCwk50179	800_post/890_install_version_masked_apps.pl でアップグレードが失敗する可能性がある
CSCwk50986	オブジェクトグループが保護されたネットワークとして追加されると、UI の [NAT適用除外（NAT Exemptions）] がロードされない

不具合 ID	タイトル
CSCwk52890	HTTP ベースのパスモニタリングが原因で FTD/ASA のメモリ使用率が高くなる
CSCwk55087	ENH：ECMP ゾーンの VTI/物理インターフェイスでの DHCP リレーを FMC でサポート
CSCwk63586	アプリケーション インスタンスが STOP_FAILED でスタックし、エラーメッセージが表示される
CSCwk63733	HA の監視対象のインターフェイスが「待機」状態になり、その後「失敗」になる
CSCwk63811	新しいUI レイアウトからアクティブなセッションを終了すると「セッションの終了中にエラーが発生しました（Error while terminating session）」エラーがスローされる
CSCwk70769	FMC：API インターフェイス設定が、診断インターフェイスの GUI 設定と異なる
CSCwk71866	ASA：同じデバイス上のコンテキスト間のサイト間 VPN が「ipsec-tun-down」によってトラフィックをドロップする
CSCwk75956	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
CSCwk76362	スレッド名 PTHREAD での FTDv のトレースバック
CSCwk76563	SDWAN：異なるコミュニティの別のトポロジに同じスポークがあると、ルートの再配布で問題が発生する
CSCwk76734	fmc 設定と lina 設定の間で 'ip local pool' コマンドが一致しないため、ポリシー展開が失敗する
CSCwk77241	9k ブロックの枯渇（tcpmod proc）によるトラフィック障害が FPR 3100（HA）で確認された
CSCwk78030	ASA/FTD：Threat-Detection によるメモリの枯渇
CSCwk78393	LDAPS SSL エラーのロギングの改善
CSCwk80292	FMC：FMC を介して設定しようとすると、DAP 設定の「ラグ/ハング」が発生する
CSCwk80518	cdFMC の移行中に sfo のインポートが失敗すると、Snort2 'ids_event_msg_map' のクリーンアップが発生しない

不具合 ID	タイトル
CSCwk82337	ポリシーのエクスポートが「エクスポート用のポリシー情報を処理できません（Unable to process the policy information for Export）」というエラーで失敗する
CSCwk82557	FDM を介した 7.4.2 への FTD のアップグレードがブロックされる
CSCwk83804	制御ノードに変更があると、他のクラスタノードでスケジュール済みバックアップが失敗する
CSCwk85012	FMC のアップグレード後に CSDAC コネクタが起動しない
CSCwk86563	SID の評価中に送信元ポートと宛て先ポートがスワップされる
CSCwk86582	「ENDPOINT_TIME_OUT_OF_SYNC」エラーによって SAML 認証が完了しない
CSCwk87457	デバイスのリロード後に ASA/FTD がプロセス名「lina」でトレースバックし、リロードすることがある
CSCwk88182	PTHREAD-8141 spin_lock_fair_mode_enqueue での通常動作時における FTDv50 のトレースバック
CSCwk88225	クリティカルな障害：[FSM:FAILED]：ユーザー設定（FSM:sam:dme:AaaUserEpUpdateUserEp）
CSCwk88571	アップグレード中に FMC 接続が失われると、HA FTD ペアの部分的な設定が失われる
CSCwk88913	リモートサーバーにファイルを正常にコピーするまで、FMC バックアップをローカルで保存する
CSCwk89061	いずれかのポートオブジェクト値が無効でも、検索インデックス処理は失敗すべきではない
CSCwk89836	ASA/FTD がスレッド名「strlen」でトレースバックし、リロードすることがある
CSCwk94382	FTD：Lina が CONFIG_XML_REQUEST に応答せず、展開がスタックすることがある
CSCwk94697	FMC はアイデンティティ証明書のインポートでバイナリ証明書のアップロードを許可する
CSCwk96912	FTD：7.4.1 へのアップグレード後に syslog メッセージ ID 302013 にユーザー名がない
CSCwk97058	FMC：VPN 証明書が機能不全状態の場合、展開前検証でエラーが発生して展開がブロックされる必要がある

不具合 ID	タイトル
CSCwk97812	RAVPN 証明書グループマップが FMC で変更されると削除される
CSCwm00154	FTD：プロセス sftunnel が予期せず終了し、コアファイルが生成される
CSCwm01544	data-path スレッドでの Lina のトレースバックとリロード
CSCwm01901	/var/log/messages ファイルでの「vpn:vpn [INFO] device」メッセージの過剰なロギング
CSCwm02801	HA が不安定になって展開が失敗する
CSCwm03142	マルチインスタンスセットアップの共有インターフェイスで IPv6 ネイバー探索が失敗する
CSCwm03227	/ngfw/var/cisco/deploy/tmp_bundle/db/ パスに複数の DB フォルダがあるため、FTD のアップグレードが失敗する
CSCwm03772	CLI "ssl server-max-version" は、Flex Config 経由で展開できない
CSCwm03898	FMC GUI からのパケットキャプチャで、FTD デバイスのパフォーマンスへの悪影響についてユーザーに警告されない
CSCwm05155	Snort AppID が SSH トラフィックを誤って「不明（Unknown）」と識別する
CSCwm05221	IDS パッシブモードでの非対称トラフィックで Snort3 ファイルの検出が失敗する
CSCwm05226	S2S VPN ダッシュボードで、VPN トポロジのステータスに「アクティブなデータがありません（No Active Data）」と表示される
CSCwm05520	FTD クラスタが inline-set で展開されている場合、クラスタの syn cookie 復号を無効にする
CSCwm05949	ロード状態が続いて PolicyRPC コールが保留中のままになる
CSCwm06059	ネイティブモード（FTD）の TPK で configure manager コマンドが出力なしでハングする
CSCwm06393	ポートチャネルメンバーシップまたはメンバーステータスの変更により、定期的な OSPF/EIGRP 隣接関係フラップが発生することがある
CSCwm07389	リブートのたびに ASA syslog で CGroups エラーが発生する
CSCwm08889	マウントされたストレージポイントが原因で、df コマンドがスタック状態になることがある
CSCwm09571	DVTI：DVTI 設定の変更時にインターフェイスの shut および no shut に関する情報/警告メッセージが表示される

不具合 ID	タイトル
CSCwm09680	syslog サーバーの DNS ルックアップの失敗によってログスパムが発生し、ネットワークが遅延する可能性がある
CSCwm11171	ローカルファイルシステムのみのオプションを使用するように df コマンドを変更する
CSCwm12434	大きな undo/ibdata ログファイルで準備状況チェックが実装される必要がある
CSCwm12920	Azure の表示名にサポートされていない文字を使用すると、アクセス コントロール ポリシーでエラーが発生する
CSCwm13137	相関で接続期間が検出されない
CSCwm13141	show コマンドを実行しようとすると、FTD CLISH/CLI がロックされる
CSCwm13199	NAT 未変換での予期しない動作により、SIP トラフィックが影響を受ける。
CSCwm14509	GTP インスペクション中に、23、24、25 の IE タイプに対する無効な長さによる誤ったドロップが発生する
CSCwm14561	ASA/FTD がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwm27687	中国語の説明を使用してカスタムワークフローを作成すると、「カスタムワークフロー」の GUI にエラー 500 が表示される
CSCwm28007	ユーザーが WebVPN のブックマークをクリックすると、ブラウザが空白のページにリダイレクトする
CSCwm29469	FMC GUI に、FTD の SSH ルールが 50 個のみ表示されるという制限がある（[プラットフォーム設定（Platform Settings）] > [SSH]）
CSCwm29929	QoS ポリシーに 50 を超えるルールがある場合、FMC GUI の QoS ポリシーエディタでページネーション機能が失われる
CSCwm29941	ベースポリシーから継承した場合、プレフィルタポリシーが子 ACP に適用されない
CSCwm30731	ASA の OSPF ルーティングテーブルがネイバーと正しく同期されない
CSCwm30786	SFTunnel 接続チェック要求のタイムアウトの増加
CSCwm30825	遅い SFTunnel 接続をマーキングするための接続ステータスファイルを追加

不具合 ID	タイトル
CSCwm31353	FTD ログには、破損している証明書名またはファイルが含まれている必要がある
CSCwm33229	SAML の強制再認証において、接続の再試行時にユーザーにログイン情報の再入力が強制されない
CSCwm33552	FMC のシステム構成設定で、アクセスリストの有効な IP 範囲形式が受け入れられない
CSCwm33613	SAML アサーション属性の複数のグループポリシーを受け取ると、デフォルトのグループポリシーが適用される
CSCwm33619	FTD Vault プロセスが 1 分ごとに終了する：「プロセス vaultApp（23597）が正常に終了しました：256（Process vaultApp（23597）exited normally：256）」
CSCwm34333	FTD：マルチインスタンスの docker0 インターフェイスがプライベートネットワーク 172.17.0.0/16 と重複する
CSCwm34786	プラットフォーム設定ポリシーが UI で非表示になっている
CSCwm35035	設定したアルゴリズムとは関係なく、FTD による SAML 認証要求が常に Sha1 によって署名される
CSCwm35051	ホスト名/IP アドレスフィールドは、数字で終わるドメインを受け入れない
CSCwm35251	FMC4700 に早期のファン速度アラートが表示される
CSCwm35730	LINA がスレッド名 Datapath with NAT config でトレースバックすることがある
CSCwm35751	FPR3100：インターフェイスが半二重に移行することがあり、速度が 100mbps にハードコードされる
CSCwm36631	FTD のセカンダリユニットが一括同期状態でスタックする。
CSCwm36646	FMC のアップグレード後、スタンバイ FTDv は FTD HA のパフォーマンス階層を失う
CSCwm37043	MI セットアップで Snort3 エラーのクラッシュハンドラ通知が送信されない
CSCwm37455	ASA/FTD が無効なネットマスクを持つローカル IP プールを許可する
CSCwm37690	FMC でポリシーを保存すると、[NATルール：前（NAT Rules Before）] が削除される

不具合 ID	タイトル
CSCwm38299	CDO から cdFMC への REST コールが、null または空の応答でランダムに失敗する
CSCwm38513	[既存のものを置換する（Replace existing）] オプションを使用してポリシーをインポートすると、オブジェクトが重複する
CSCwm38635	TACACS+ トラフィックは、XTLS モジュールの TLS サーバーアイデンティティによってドロップされる
CSCwm40278	展開後に S2S VPN 設定が予期せず削除される
CSCwm40721	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
CSCwm41381	マルウェアおよびファイルポリシーが設定されていると、ファイルのダウンロードが断続的に失敗する
CSCwm41404	アクティブな HA FMC での FTD ウィザードで、もう一方のマネージャを "analytics FMC" として参照するエラーメッセージが表示される
CSCwm41847	PDTS の書き込み/読み取りブロックをキャプチャして根本原因 CSCwm36314 の解決をサポートするための有用性
CSCwm42000	FTD/ASA が DATAPATH スレッドでトレースバックし、リロードすることがある
CSCwm42745	IKE_AUTH がない場合、ダイナミックサイト間トンネルが IN-NEG 状態でスタックする
CSCwm44162	グローバル デバイス ウィザード ページを介して追加した子ドメインテンプレートが機能しない
CSCwm44412	FTD インラインセットが挿入/書き換えのリバースフラグを無視する
CSCwm47235	policy_deployment.db が破損しているか使用できない場合、FTD アップグレードが 901_reapply_sensor_policy.pl で失敗する可能性がある
CSCwm47769	REST API POST を介した設定のコピー中に他のデバイスの ID 属性により、元の設定が削除される可能性がある
CSCwm47775	ブロック割り当ておよびラウンドロビンが有効になっている NAT ポリシーを変更すると、FMC の展開に失敗する
CSCwm48218	FMC：保存ボタンがグレー表示されているため、インターフェイス設定を保存できない
CSCwm48621	ENH：物理インターフェイスおよびサブインターフェイスの HM を個別に有効/無効にするオプションを提供

不具合 ID	タイトル
CSCwm49154	展開時に FXOS 障害 F1738 が発生し、エラー CSP_OP_ERROR が表示される。CSP 署名確認エラー
CSCwm49458	アップグレード後の展開で DNS 設定が削除される
CSCwm49721	メモリ破損が検出されたことによる ASA のトレースバックとリロード
CSCwm49782	sma 2nd cruz ハートビートのロギングを強化
CSCwm49940	ha-mode graceful-restart が詳細プレビューにない
CSCwm50591	ASA/FTD：VTI とサブインターフェイスで IPsec オフロードが有効になっていると、インバウンド IPsec パケットがドロップされる
CSCwm50936	両端の Innolight QSFP で 100GB インターフェイスがフラップする
CSCwm51467	[SSLサーバー（SSL Server）] チェックボックスが、[デバイス（Device）] -> [証明書（Certificates）] -> [新しい証明書の追加（Add New Cert）] のデフォルトの新しいテーマにのみ表示されない
CSCwm51747	FXOS のアップグレード後に公開キー認証を使用した SSH アクセスが失敗する
CSCwm51923	展開のトランスクリプトに「管理アクセスの有効化：false（Enable management access: false）」と表示される
CSCwm52264	「パスワード暗号キーが設定されていません。（The password encryption key has not been set.）」という障害を除去またはクリアできない
CSCwm52430	39% 600_schema/103_csm_cfgdbmigration.sh で FMC のアップグレードが失敗する
CSCwm52931	ASA/FTD がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwm52973	TPK Low End FPR3100：インターフェイス速度を 1g から 100mbps/100mps から 1g に変更するとリンクがダウンする
CSCwm55634	バージョン 7.4.x 以降、FMC 正常性ポリシーに [インポートとエクスポート（Import and Export）] ボタンがない
CSCwm56864	show run access-list コマンドが警告を返す
CSCwm57511	extdb Omniquery の実行に関する問題
CSCwm58260	TLS 証明書の発行者と共通名は同じだが署名アルゴリズムと公開キーが異なる場合に Snort3 がクラッシュする

不具合 ID	タイトル
CSCwm58948	FMC で AzureAD ユーザー/グループのダウンロードが失敗する：SQL 変数が多すぎます（too many SQL variable）
CSCwm60536	クラスタリングデータユニットでSQLNet トラフィックが断続的にドロップされる。
CSCwm61282	ASA/FTD：RA VPN トンネルによってメモリリークが発生し、トレースバックとリロードが行われる
CSCwm61417	複数の SSE コンシューマが有効になっている場合、EventHandler がブロックする可能性がある
CSCwm63024	FMC の DAP 証明書シリアル番号チェックフィールドは 16 進形式ではなく自由形式にする必要がある
CSCwm63648	FTD センサーを元に戻して再アップグレードすると、UI に [ウェイトの設定（Set Weight）] オプションが表示されない
CSCwm63868	FTD：FTD HA フェールオーバーイベント後に BGP の advertised-routes にルートがない
CSCwm64553	Po メンバーインターフェイスがフラップした後に互換性のないメンバーに関する警告メッセージが表示され、Po に再参加できない
CSCwm65693	FMC の GUI で表示される Snort 3 ルールに不一致がある
CSCwm65773	sftuunel が UP の場合、インベントリの更新で誤ったメッセージ「デバイスに到達できません（Device is not reachable）」が表示される
CSCwm66653	FMC で DHCP リレーエージェントおよびサーバーが UI に表示されず、変更が許可されない
CSCwm66731	RAVPN ポリシーで LDAP 属性マップを編集する際に、編集アクションがスタック状態になる
CSCwm68211	スレッド snmp_inspect での ASA のトレースバックとリロード
CSCwm69907	FMC で RADIUS 設定ファイルが FTD に送信/同期されない
CSCwm70040	FMC 移行後に外部 LDAP ユーザーを介して FMC にログインできない
CSCwm70490	長期稼働セットアップで VDB のアップグレードが失敗する
CSCwm70835	APCF ファイル使用中のスタックオーバーフローによる ASA のトレースバックとリロード
CSCwm71265	PDP の gtpv1 エンドマーカーメッセージを処理しているときに、ASA がスレッド DATAPATH でトレースバックし、リロードする

不具合 ID	タイトル
CSCwm71730	古いドメイン ID 参照によりオブジェクトのグローバル検索が機能しない
CSCwm72176	FTD スタートアップ後に何らかの理由で mysql/mariadb が再起動されると、FTD Lina プロセスが停止する
CSCwm72757	Snort3 が ESMTP トラフィックを断続的にブロックし、IPS シグネチャ 124:3:2 および 124:1:2 をトリガーする
CSCwm74289	NAT トラップのレートの制限が必要
CSCwm75352	スケジュールされたタスクは、間隔が 24 時間に設定されている場合は実行されないが、1 日に設定されると実行される
CSCwm77055	FMC/FTD：VNI インターフェイスを使用するクラウド上の既存の FTDv 展開でポリシー展開が失敗する
CSCwm77673	ポリシー展開が 5/8%（ポリシーとオブジェクトの収集）のときにハングする
CSCwm78241	cdFMC の FTD-HA ペアで、スタンバイノードに古いインターフェイスステータスの正常性アラートがある
CSCwm78351	キャプチャコードの無条件実行により、マルチコンテキストクラスタのセットアップで CPU 使用率が高くなる可能性がある
CSCwm79807	DCEControlMessageReconfigure を呼び出す際に SFDataCorrelator でコアダンプが発生する
CSCwm79920	外部認証（Radius）ユーザーは、初回ログイン時に大文字と小文字の不一致により FTD にログインできない
CSCwm80082	[ENH] OpenStack の FTDv で FDM を有効にしようとすると FDM がサポートされていないことをユーザーに通知する
CSCwm80085	FMC が侵入ポリシー推奨事項の再生成時に古い推奨事項をクリアしない
CSCwm82683	peers ディレクトリを開けない場合、登録のクリーンアップを実行しないようにする必要がある
CSCwm83580	FMC リモートストレージエラー：初期化されていない値 $^WARNING_BITS がビット単位の xor（^）で使用されている
CSCwm85228	フェールオーバーに参加するときに、ASA/FTD がスレッド名「IKEv2 Daemon」でトレースバックし、リロードすることがある
CSCwm85497	セカンダリ FMC は、アップグレードが完了しているにもかかわらず FTD がアップグレード中であることを示す

不具合 ID	タイトル
CSCwm86416	ENH：FMC API：Threat Defense アップグレードオプションは、障害対応ファイルの自動生成をスキップする
CSCwm87310	デフォルトの next-hop を指定した PBR は、ネクスト ホップなしでは許可されない
CSCwm87409	FMC が SNMPv3 トラップで engineID に誤った値を送信する
CSCwm89523	「no capture /all」によってバックエンドでキャプチャを完全に無効にできず、データパス CPU の使用率が高くなる
CSCwm89747	「エラー：dhcpd が内部で有効になっていません（Error-no dhcpd enable inside）」という理由で、展開に失敗する
CSCwm90905	GTP インスペクションがエラー ERROR-DROP:MsgType:32 でパケットをドロップする
CSCwm92397	「IP RIB Update」スレッドを指す LINA コアがある
CSCwm93119	FMCv は、特定の KVM ハイパーバイザ ソフトウェア バージョンと互換性がない
CSCwm94752	選択したネットワークオブジェクトがあっても、アイデンティティ マッピング フィルタが空白で表示される
CSCwm95116	両方の FMC ADI のミュートが解除されるため、FTD で ADI がクラッシュする
CSCwm95328	1 ページ目以外の UI ページでルールをコピーして貼り付けると、ポリシーの UI が 1 ページ目に戻る
CSCwm96280	リセットボタンを押した後に FTD デバイスが rommon モードでスタックする
CSCwm96652	クラスタがユニットに対して誤った NAT を割り当てており、トラフィックがユニットに適切に転送されない
CSCwm97054	高速の SIP 接続による ASA/FTD のトレースバックとリロード
CSCwm98278	FIN の ACK を受信した後に TCP 接続がハーフクローズとしてフラグ付けされない。
CSCwn00475	priority-queue によるメモリブロック 80 および 9344 のリーク
CSCwn01281	セッション作成応答の原因タイプが 18 の場合、GTP インスペクションで GTP データパケットが許可されない

不具合 ID	タイトル
CSCwn03446	クラスタインターフェイスでキャプチャが有効になっている場合、設定されたルールとともに常に CCL IP が含まれる
CSCwn03796	AMPkit ポータルに登録した後の Unity スタイルの登録
CSCwn03835	ASA/FTD がスレッド名「SSH Ctxt Thread」でトレースバックし、リロードすることがある
CSCwn05183	ポリシー展開に失敗した後に、FTD HA アクティブ ノード インターフェイスがダウンする
CSCwn06641	FTD syslog-over-TLS によって許可される CC モードの曲線が多すぎる
CSCwn07008	SLA モニターで名前付きインターフェイスを使用すると、cdFMC の移行が失敗する
CSCwn08085	ほとんどの UI テーマの相関ポリシー エディタで、[利用可能なルール（Available Rules）] モーダルに垂直スクロールバーがない
CSCwn08887	ZeroMQ 送信エラー後、vFTD の FMC UI で接続イベントが表示されない
CSCwn09870	FlexConfig オブジェクト Policy_Based_Routing および Policy_Based_Routing_Clear により、展開に失敗する
CSCwn10538	FTD の ADI がクラッシュ後に停止しない
CSCwn11728	FPR9K-SM-56 モジュールが断続的にロックアップし、トラフィックに影響を与える。
CSCwn13187	9.20.2.21 からターゲットバージョン 9.20.3.4 への ASA のアップグレードが失敗する
CSCwn13238	[生成（Generate）] オプションを使用し、後で適用すると、侵入ルールの推奨事項が適用されない
CSCwn13672	暗号化後の追加の Route-Lookup を回避するために VTI トンネル送信元インターフェイスに ESP をバインドする
CSCwn14130	拡張 PAT の有効化後にトレースバックとリロードを行う FTD クラスタ
CSCwn14355	ハブアンドスポークトポロジの更新後に検証エラーが発生する
CSCwn14447	ASA/FTD がスレッド名「ldap_client_thread」でトレースバックし、リロードすることがある
CSCwn15104	swapcontext 機能のトレースバックによる FTD のリロード
CSCwn17121	ASA/FTD がスレッド名「cli_xml_request_process」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
CSCwn18734	cdFMC：デバイス移行後の展開の検証でセキュリティゾーンにインターフェイスがないことが示される
CSCwn19190	メモリフラグメンテーションにより、lina で大きなページを使用できなくなる
CSCwn19498	クラスタアプリケーションの同期フェーズ中に既存のクラスタセットアップにデータノードを追加できない
CSCwn19690	重大な正常性アラート、モジュール SMART_LICENSE のスマート ライセンス エージェントが実行されていない
CSCwn19706	管理者ユーザーは、外部サーバーへの認証のときにローカルパスワードの変更を求められる
CSCwn19739	HA が、コールドスタンバイから障害状態に移行する間にデータインターフェイスを起動する
CSCwn19761	CloudConfig に多数の古いリビジョンが含まれていると、FMC のパフォーマンスに影響する
CSCwn20024	ASA 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
CSCwn20642	RA VPN ユーザー アクティビティ レポートでの VPN バイト数の不一致
CSCwn22036	FTD：Management0/0 のステータスがダウンになり、アップグレード後にラインプロトコルがアップ状態になる
CSCwn22456	GTPv2 IE タイプ 157（シグナリング優先順位表示）が不明な IE タイプとしてドロップされる
CSCwn23031	ワークフローモードが有効になっている場合、IPS ポリシーは削除できない
CSCwn23362	FTD：Snort AppID が NetBIOS-ssn トラフィックを誤って「不明（Unknown）」として分類する
CSCwn23992	ポート 443 で FMC にアクセスすると、UMS を含むプッシュメッセージが破損する
CSCwn24577	「no pim」または「no igmp」設定を含めると、ASA のブートプロセスがフリーズすることがある
CSCwn26165	Radius パケットが原因となり、FTD/ASA が展開中/Radius の変更中にトレースバックし、リロードすることがある
CSCwn27819	ジャンボフレームパケットがフラグメント化されている

不具合 ID	タイトル
CSCwn29465	ユーザーが [パケットキャプチャ（Packet-Capture）] ページにアクセスしようとすると、一般的なエラーがスローされる
CSCwn29611	Radius ユーザーの ssh ログインが失敗し、エラー「ユーザー名が有効なサービスタイプで定義されていません（username is not defined with a service type that is valid）」が表示される
CSCwn31166	エスケープ解除中に範囲外の例外が発生し、JS 正規化で Snort3 がクラッシュする
CSCwn31240	webvpn dtls フローオフロードが有効な場合のトレースバックとリロード
CSCwn31588	MI：FPR42xx で 14 ー 70 の CPU コアを使用して RP を割り当てると、インスタンスがスプリットブレイン状態になる
CSCwn31653	FTD がスレッド名「FPRLI_FPR4K-SM-32」でトレースバックし、リロードすることがある
CSCwn34259	9.20.3.7 へのアップグレード後に監視対象のインターフェイスが待機状態になることがある
CSCwn34659	DNS 応答で TC ビットセットを受信した後でも、ファイアウォールが TCP 要求を開始しない
CSCwn34707	複数の Unicorn Admin Handler プロセスが、すべてのコントロールプレーンの CPU を消費する。
CSCwn35470	サービスアビリティ：FQDN パケットベースのデバッグとキャプチャトレースのサポート
CSCwn38431	カスタム属性のダイナミック スプリット トンネリングにドメインを含めようとすると内部エラーが発生する
CSCwn39159	新しい UI を使用したアクセスポリシーページでポートオブジェクトに未定義の値が表示される
CSCwn39762	インスタンスコアのサイズを変更すると、55recalculate_arc.pl で展開が失敗する
CSCwn39780	FTD 展開のレジリエンス：クリティカルでない/存在しないコマンドをスキップして展開の失敗を回避。
CSCwn39826	HA は、copy/config-sync/rollback の進行中にフェールオーバー要求を受け入れないようにする必要がある
CSCwn39896	SAML SSO テスト設定と SSO ログインが、設定が正常に完了した後も機能しない

不具合 ID	タイトル
CSCwn40485	MI：データ共有インターフェイスで有効になっている場合、トラフィックがセカンダリ FTD に到達できない
CSCwn40572	MI：仮想 MAC が設定されている場合、Vlan 情報が FXOS レベルで適用されない
CSCwn42949	分散セカンダリフロー接続を処理する非オーナーユニットでのフォワーダーフローの導入
CSCwn44326	GeoDB の定期的な更新をルールの更新と同じ時間帯にスケジュールすると、インストールが失敗することがある
CSCwn44335	FXOS：Download コマンドが HTTP および HTTPS GET 要求に対して追加の「/」を生成する
CSCwn45049	Coverity システム SA の警告、2024 年 9 月 9 日、Coverity の不具合 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN トンネルの子 SA の再ネゴシエーションが失敗する
CSCwn46426	ASA 21xx：「sh environment temperature」に誤った温度値が表示される
CSCwn46794	Snort 2 ルールを変換およびダウンロードすると、FMC UI が応答しなくなる
CSCwn46855	LINA で Netflow が設定されたランダムトレースバックが確認されることがある
CSCwn47353	復号ポリシー作成ウィザードで、復号の除外に関する誤解を招く情報メッセージが表示される
CSCwn49391	FTD HA のアップグレード後に頻繁にトレースバックが発生する
CSCwn50961	SVTI で仮想トンネルインターフェイスの送信がデフォルトで有効になっている
CSCwn51845	ASA 9.20.3.4 を実行しているクラスタメンバーでトレースバックが確認される
CSCwn54561	ポリシー展開サブグループのメモリ割り当ての変更
CSCwn54837	イベント処理中に VDB のアプリケーション名の変更が反映されない
CSCwn54966	Snort3：ACK での TCP ミッドストリーム トラフィックが Snort によって正規化され、ストリームプリプロセッサによってブロックされる
CSCwn57518	FMC：OSPF 設定画面を FMC の英語 UI で開けない

不具合 ID	タイトル
CSCwn57940	デバイスがあるドメインから別のドメインに移動されると、展開のプレビューが失敗する
CSCwn58715	ヘルスモニタリング UI の高可用性ウィジェットで、プライマリデバイスに誤ったデバイス情報が表示される
CSCwn59632	RabbitMQ がダウンしている場合、FMC への FTD 登録がハングする
CSCwn61640	膨大な数のルールで syslog または SNMP にイベントを送信する場合、スタートアップ中に EventHandler でコアダンプが発生する
CSCwn63839	BVI との arp permit-nonconnected の設定時にスレッド名 Lina でトレースバックする
CSCwn73318	FMC ヘルスモニター（HM）グラフに表示される Snort およびシステムの CPU コアの数が正しくない
CSCwn73351	アジア/バンコクのタイムゾーンオプションが、firepower1k で実行している ASA に表示されない
CSCwn73371	FMC HA の同期状態が低下しているという誤ったアラートが発生する
CSCwn75536	FMC を 7.4.2.1 にアップグレードした後、cfgdb のダンプ中に FMC のバックアップが失敗する
CSCwn75667	設定時にバナー motd が表示されない
CSCwn75744	FMC のアップグレード後、SI オブジェクト数が多いために展開が失敗する
CSCwn76079	SSH は管理コンテキストで動作するものの、ssh key-exchange を変更するとユーザーコンテキストで動作しない
CSCwn76475	[すべてのSyslogメッセージの有効化（Enable All Syslog Messages）] を使用すると、イベントリストが展開されない
CSCwn79553	到達不能な LDAP/AD を照会すると、FTD の外部認証で遅延またはタイムアウトが発生することがある
CSCwn80762	コミュニティリストが変更されても、FMC でコミュニティリストのオーバーライドが削除されない
CSCwn83268	16 個を超えるディレクトリを含むレルムは、LDAP 対応の RA-VPN に展開できない
CSCwn84557	「spin_lock_fair_mode_enqueue」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
CSCwn89243	接続先のみのオブジェクトが拡張された場合、アイデンティティ NAT はしきい値の超過によるエラーをスローすべきではない
CSCwn93319	ASA/FTD がスレッド名「DATAPATH」でトレースバックし、リロードすることがある
CSCwn95451	FMC HA ページの最後の同期時刻に、英語以外の言語で「利用可能なデータがありません（Data unavailable）」と表示される
CSCwn96064	不明に分類されたファイルで、ステータスと脅威スコアの受信に時間がかかる
CSCwn96929	ASA：スレッド名 SSH でのトレースバックとリロード
CSCwo00444	FPR3100 プラットフォームでの暗号ハードウェアのオフロードに影響する Nitrox Engine（Crypto Accelerator）の問題
CSCwo00702	コミュニティリストは、リストの最後の項目が削除されるまでエラーをスローしない必要がある
CSCwo01557	メモリ破損による DATAPATH スレッドでの ASA のトレースバックとリロード
CSCwo06959	マルウェア クラウド ルックアップのタイムアウトにより、マルウェアブロックが発生しない
CSCwo07139	フローデータがクリアされても、Snort3 ストリームインスペクタのフロースタッシュがクリアされない
CSCwo08042	Unicorn Proxy スレッドでのトレースバックにより、ASAv が予期せずリロードする
CSCwo09195	FQDN を無効化した後の展開中のトレースバックとリロード。
CSCwo13863	Don’t Fragment ビットが設定され、IPv4 フラグメントをフラグメントとして処理しなかったため、Snort3 がクラッシュする
CSCwo14722	/ngfw/var/cisco/deploy/pkg/var/cisco/packages 内の古いファイルをプルーニングする
CSCwo16016	MA が有効になっている場合、レガシー Radius サーバーのユーザーがスタンバイ FMC ドメインにログインできる
CSCwo18883	FMC は、BGP に使用される prefix-list のオーバーライドを削除し、デフォルト値を自動的にインストールする
CSCwo21767	カスタム設定に対してポートスキャンアラートが生成されない

不具合 ID	タイトル
CSCwo25271	auth-daemon が再起動すると空のスナップショットが送信され、ユーザーがログアウトされる
CSCwo25478	競合状態による auth-daemon プロセスの再起動
CSCwo31467	TLS：Outlook は TLS 1.2 のみをサポートし、1.3 はサポートしないが、FMC はデフォルトで TLS 1.3 を使用する
CSCwo32943	アクティブ FMC：FMC HA の同期状態が低下しているという誤ったアラートが発生する
CSCwo34220	ランダムな QoS ポリシーが無効化され、後続の展開で追加される
CSCwo35585	アップグレード中の AMP 関連の正常性アラートとアラートメッセージの誤字
CSCwo41250	メモリ不足状態時のスレッド DATAPATH-1-23988 でのトレースバックとリロード
CSCwo42139	VDB アップグレードによる Snort3 トレースバックと展開の失敗
CSCwo45848	SecGW：データノードが cluster_ccp_make_rpc_call failed to clnt_call エラーでクラスタに参加できない
CSCwo53892	FMC で FTD 正常性メトリックに「使用可能なデータがありません（No data available）」と表示される
CSCwo63951	Talos との通信に使用される FMC クライアント側の証明書が正しく自動更新されない
CSCwo71052	リロード後に FPR1010 Ethernet1/1 トランクポートで VLAN トラフィックが渡されない
CSCwo76436	ピアスイッチのリロード時に、インターフェイス MAC 用の 3100 マーベル 4.3.14 CPSS パッチがスタック状態になる
CSCwo77662	RADIUS ユーザーのパスワードに特定の特殊文字またはスペースが含まれていると、FMC でログインが失敗する
CSCwo77937	ミニダンプ コア ファイルが MI モードで生成されない
CSCwo91053	fover_trace.log がローテーションされず、巨大なサイズに増加する
CSCwp03056	モデルの移行中に VNI インターフェイスでプロキシが無効になっていても、プロキシが有効な状態で VNI インターフェイスを設定できないというエラーが表示される

不具合 ID	タイトル
CSCwp06890	Finisar の SFF_SFP_10G_25G_CSR_S V03 モジュール同士の接続時にポートがバウンスする

バージョン 7.6.0 で解決済みのバグ

表の最終更新日：2025 年 10 月 14 日

表 *26* : バージョン *7.6.0* で解決済みのセキュリティバグ

不具合 ID	タイトル
CSCwb67583	SSL VPN と HTTP サーバーが同じポートで設定されている場合の ASDM のアクセスに関する問題
CSCwc28334	Cisco ASA および FTD ソフトウェアの RSA 秘密キーリークの脆弱性
CSCwc31953	根本原因を問わない RSA 秘密キーのリークの防止。
CSCwd30856	per-user-override が設定されている場合、vpn-filter のないユーザーが追加のアクセス権を取得できることがある
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
CSCwd50155	CVE-2022-42252 に関する FMC の評価
CSCwd62859	Cisco ASA および FTD AnyConnect の SSL/TLS VPN におけるサービス拒否攻撃に対する脆弱性
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
CSCwd77581	Cisco ASA および FTD の ICMPv6 メッセージ処理のサービス妨害（DoS）の脆弱性
CSCwd95043	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwd96845	Cisco ASA および FTD における AnyConnect アクセス制御リストのバイパスの脆弱性
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
CSCwd98316	Cisco ASA および FTD ソフトウェアの VPN パケット検証の脆弱性
CSCwe15280	複数のシスコ製品で確認された Snort 3 アクセス コントロール ポリシー バイパスの脆弱性

不具合 ID	タイトル
CSCwe20918	Cisco ASA および FTD ソフトウェアにおけるリモート アクセス SSL VPN の複数証明書認証のバイパス
CSCwe22176	CCM レイヤ（シーケンス 43）での WR6、WR8、LTS18、および LTS21 コミット ID の更新。
CSCwe44099	Cisco 適応型セキュリティ仮想アプライアンスと Secure FTD 仮想 SSL VPN における DoS の脆弱性
CSCwe45093	per-user-override が設定されている場合、vpn-filter のないユーザーが追加のアクセス権を取得できることがある（IKEv2 RAVPN）
CSCwe48399	パブリック API 関数 BIO_new_NDEF は str に使用されるヘルパー関数
CSCwe51443	OpenSSL の脆弱性の ASA 評価 CVE-2022-0778
CSCwe59809	CCM seq 45：WR6、WR8、LTS18、および LTS21。
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
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
CSCwe66360	フローによってメモリが解放されないため、Snort3 がメモリ不足になり、プロセスが予期せず終了する
CSCwe74328	AnyConnect - hostscan が有効な場合、モバイルデバイスは接続できない
CSCwe86964	Consul および Consul Enterprise で、次のサービスを持つ認証済みユーザーが許可される：
CSCwe87591	Cisco FTD ソフトウェア SSL/TLS URL カテゴリおよび Snort 3 検出エンジンのバイパスおよび DOS 脆弱性
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
CSCwe88928	ヘルスモニタリングに管理対象外デバイスが表示される
CSCwe90609	Cisco ASA ソフトウェアと FTD ソフトウェアの SNMP におけるサービス妨害攻撃に対する脆弱性
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
CSCwe93537	threat-detectionで個々の IPv6 エントリをクリアできない
CSCwe93558	Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSH におけるリモート コマンド インジェクションの脆弱性

不具合 ID	タイトル
CSCwe93561	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwe95729	Cisco ASA および FTD SAML 認証バイパスの脆弱性
CSCwe98687	Cisco Firepower 2100 シリーズ用 Cisco FTD ソフトウェアにおけるインスペクションルールのサービス妨害（DoS）の脆弱性
CSCwf08387	7.2.4 ビルドを使用する SSP_CLUSTER の LINA プロンプトで、LSP バージョンが最新に更新されていない
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
CSCwf17389	ASA は RA VPN 認証用にリプレイされた SAML アサーションを受け入れる
CSCwf22005	ASA/FTD：パケットトレーサは、正しい判定を生成するにもかかわらず、誤った ACL ルールを表示する場合がある
CSCwf22483	シャーシへの SSH により、設定で許可されていない IP の 3 ウェイハンドシェイクが可能
CSCwf23262	Cisco ASA および FTD における AnyConnect アクセス制御リストのバイパスの脆弱性
CSCwf34069	Cisco ASA および FTD のリモートアクセス SSL VPN 認証における標的型サービス妨害（DoS）の脆弱性
CSCwf34070	Cisco ASA および FTD のリモートアクセス SSL VPN 認証における標的型サービス妨害（DoS）の脆弱性
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
CSCwf35233	シスコの適応型セキュリティ アプライアンス ソフトウェアと Firepower Threat Defense の DoS
CSCwf36419	ASA/FTD：スレッド名 'PTHREAD' でのトレースバックおよびリロード
CSCwf40594	Wyoming/SFCN ASA：show crypto ssl objects CLI で DBRG の値が正しく表示されない
CSCwf47924	Cisco ASA および FTD VPN Web クライアントサービスのクライアント側要求のスマグリングの脆弱性
CSCwf62729	Cisco ASA/FTD Firepower 2100 SSL/TLS におけるサービス妨害攻撃に対する脆弱性

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
CSCwf85757	Cisco ASA ソフトウェアおよび FTD ソフトウェアの SAML アサーションのハイジャックの脆弱性
CSCwf89265	CDFMC：ディザスタリカバリの実行後に古いバージョンにロールバックする VDB バージョン
CSCwf93293	複数のシスコ製品で確認された Snort レートフィルタ バイパスの脆弱性
CSCwh00692	トレースバック @<capture_file_show+605 at ../infrastructure/capture/capture_file_finesse.c:282>
CSCwh10931	「show webvpn saml idp」CLI コマンドを呼び出したときの ASA/FTD のトレースバックとリロード
CSCwh14067	Cisco FTD の TCP/IP トラフィックにおける Snort 2/3 のサービス妨害（DoS）の脆弱性
CSCwh14352	Lina CiscoSSL の 1.1.1v および FOM 7.3a へのアップグレード
CSCwh20307	NAT または ACL ルールを削除した後に FMC が展開に失敗する
CSCwh22565	Snort 3 HTTP 侵入防御システムルールのバイパスの脆弱性
CSCwh23100	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh29276	ASA：シングルモードからマルチモードへの切り替え時のトレースバックとリロード
CSCwh39258	HA がアクティブにフェールオーバーした後、外部認証が機能しないことがある
CSCwh41094	Cisco FTD の TCP/IP トラフィックにおける Snort 2/3 のサービス妨害（DoS）の脆弱性
CSCwh45108	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN の不正アクセスの脆弱性
CSCwh52710	VMware 用 FMC での open-vm-tools/VMware Tools の評価 -- CVE-2023-20900 および VMSA-2023-0019
CSCwh68482	Firepower 2100 シリーズ向け Cisco Firepower Threat Defense ソフトウェアの TLS におけるサービス妨害（DoS）の脆弱性
CSCwe00713	Libtiff の tiffcrop ユーティリティでメモリリークの欠陥が見つかった。この問題

不具合 ID	タイトル
CSCwi05240	ASA：HA 同期 ACL-DAP 中にスタンバイデバイスをトレースバックする
CSCwi05435	[ENH] FMC が、展開された SRU のデバイスレコードではなく FTD デバイスの現在の SRU バージョンをプルする
CSCwi12284	Cisco ASA webvpn XSS の脆弱性
CSCwi15595	ACL 設定変更中の ASA のトレースバックとリロード
CSCwi19145	アップグレード中に FTD/ASA が PKI でトレースバックし、リロードすることがある
CSCwi20114	Cisco ASA ソフトウェアと FTD ソフトウェアの SNMP におけるサービス妨害攻撃に対する脆弱性
CSCwi21625	FailSafe 管理者パスワードがシステムコンテキストの有効化パスワードと正しく同期されない
CSCwi22693	ACP ルールを再配置した後に変更を破棄すると、そのルールが削除される
CSCwi29934	Cisco FXOS ソフトウェアの Link Layer Discovery Protocol におけるサービス妨害（DoS）の脆弱性
CSCwi32063	ASA/FTD：SSL VPN の第 2 要素フィールドが非表示になる
CSCwi38962	Cisco Firepower Threat Defense ソフトウェアにおける地理位置情報 ACL のバイパスの脆弱性
CSCwi42291	Cisco Firepower Threat Defense ソフトウェアにおける TCP Snort 3 検出エンジンのバイパスの脆弱性
CSCwi42295	ASA を 9.18.2 以降のバージョンにアップグレードした後 に RADIUS トラフィックが通過しない
CSCwi46163	Apache Tomcat 11 以降の不適切な入力検証の脆弱性
CSCwi56048	インターフェイス フラグメント キューがフラグメント データベース サイズの 3 分の 2 でスタックすることがある
CSCwi56499	カットスループロキシ機能を使用すると、未認証のトラフィックが大量に発生して CP CPU がスパイクする
CSCwi57783	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアにおけるアクセスコントロールルールのバイパスの脆弱性
CSCwi59525	cdFMC によって管理される 7.2.6 KP2110 上の複数の lina コア

不具合 ID	タイトル
CSCwi60430	CVE-2023-51385（シビラティ（重大度）中）9.6 より前の OpenSSH の ssh で OS コマンドインジェクションが発生することがある
CSCwi61058	Cisco Firepower Management Center のクロスサイト スクリプティングの脆弱性
CSCwi62683	特定の OpenSSH 拡張機能を備えた SSH トランスポートプロトコル（CVE-2023-48795）
CSCwi64429	MonetDB のメモリ使用量が時間の経過とともに徐々に増加する
CSCwi65260	送信元オブジェクトグループと宛先オブジェクトグループに同じ内部オブジェクトグループが含まれていると、宛先エントリの変更が失敗する
CSCwi78063	Cisco FTD ソフトウェアおよび FMC ソフトウェアのコードインジェクションの脆弱性
CSCwi78370	41xx/93xx：CiscoSSH（シャーシマネージャ FXOS）を更新して CVE-2023-48795 に対処する
CSCwi78593	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCwi78596	Cisco Firepower Management Center の SQL インジェクションの脆弱性
CSCwi81503	アプリケーションの HTTP/HTTPS 検出は、より早く失敗する必要がある
CSCwi90040	Cisco ASA および FTD ソフトウェアのコマンドインジェクションの脆弱性
CSCwi96521	FTD でアクセスグループを適用中に、エラーを回避するために access-group の設定クリアをプッシュする
CSCwi96562	Cisco ASA および FTD の FXOS CLI ルート権限エスカレーションの脆弱性
CSCwi98274	2005 からの unzip 5.52 に複数の脆弱性が含まれる
CSCwi98284	Cisco ASA および FTD ソフトウェアの永続的なローカルコード実行の脆弱性
CSCwj03056	API 応答からの FMC ユーザー名の列挙
CSCwj03348	vFMC25 OCI から vFMC300 OCI への移行が失敗し、「Y から a への移行は許可されません（Migration from Y to a is not allowed）」と表示される
CSCwj06006	Cisco Secure Firewall Management Center ソフトウェアの XPATH インジェクションの脆弱性
CSCwj06675	Cisco ASA および FTD ソフトウェアの永続的なローカルコード実行の脆弱性

不具合 ID	タイトル
CSCwj08083	2.11.7 より前と 2.1 より前の 2.12.x の libxml2 で問題が見つかった
CSCwj08667	SSL セッション確立中の ASA/FTD のトレースバックとリロード
CSCwj09110	ASA のアップグレード後にクライアントレスポータルを介したファイルのアップロードが期待どおりに機能しない
CSCwj10955	Cisco ASA および FTD ソフトウェアの Web サービスにおけるサービス妨害（DoS）の脆弱性
CSCwj11119	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCwj12173	ポリシー キャッシュ クリーンアップ スレッドは、ログアウトされたセッションのために開き続けているキャッシュをクリーンアップする必要がある
CSCwj14624	バックアップは 4115 でメモリ割り当てエラーで終了する
CSCwj15792	Cisco ASA および FTD ソフトウェアのダイナミック アクセス ポリシーにおけるサービス妨害（DoS）の脆弱性
CSCwj16125	無効な hostscan イメージをテストまたはロードする際のトレースバックとリロード
CSCwj19125	Cisco ASA および FTD における NSG アクセス制御リストのバイパスの脆弱性
CSCwj20804	Cisco ASA および FTD ソフトウェアの VPN Web サーバーにおける限定的な情報漏洩の脆弱性
CSCwj33129	FTD がリーフドメインに移動された場合、VPN 設定がリーフドメインに同期されない
CSCwj33187	予期しない clear configure access-list による内部キャッシュ access-group リストのメンテナンスの問題
CSCwj45822	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN におけるブルートフォースサービス妨害（DoS）の脆弱性
CSCwj48754	大規模なネットワーク マップ ホストで再起動すると、SFDataCorrelator のメモリ使用率が高くなる
CSCwj49745	Cisco ASA および FTD の VPN Web クライアントサービスにおけるクロスサイト スクリプティングの脆弱性
CSCwj58955	FMC に登録されている TPK 3110 シャーシがドメインの下にある場合、そのシャーシに変更を加えることはできない

不具合 ID	タイトル
CSCwj59315	http-proxy が原因で 7.4.1 ベースライン後の FDM でスマートライセンスの登録が失敗する
CSCwj63974	webvpn 内部 lua ライブラリのメモリマネージャの改善
CSCwj68540	Cisco Secure Firewall Management Center ソフトウェアのコマンドインジェクションの脆弱性
CSCwj72683	ASA：ログインの成功後に WebVPN ポータルのブックマークに到達できない
CSCwj77284	Cisco Firepower Management Center ソフトウェアのクロスサイト スクリプティングに対する脆弱性
CSCwj91570	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN におけるブルートフォースサービス妨害（DoS）の脆弱性
CSCwj92223	Cisco 適応型セキュリティアプライアンスおよび Firepower Threat Defense の TLS におけるサービス妨害（DoS）の脆弱性
CSCwj99043	Cisco ASA および FTD ソフトウェアの IKEv2 におけるサービス妨害（DoS）の脆弱性
CSCwj99068	Cisco ASA および FTD ソフトウェアの IKEv2 VPN におけるサービス妨害（DoS）の脆弱性
CSCwk05564	FDM クラウドサービスの米国リージョンのみ
CSCwk07982	Firepower 1000、2100、3100、および 4200 シリーズ用 Cisco FTD ソフトウェアの静的クレデンシャルの脆弱性
CSCwk08241	FTD が ACL の FQDN を断続的に解決しない
CSCwk12738	Cisco 適応型セキュリティ仮想アプライアンスと Secure FTD 仮想 SSL VPN における DoS の脆弱性
CSCwk21540	FTD HA のセットアップで RAVPN セッションを確立できない
CSCwk25117	ENH：LINA で連続して発生する AAA 障害をブロックするためのアプリケーションサポートを追加
CSCwk37414	アップグレード中に FMC 接続がダウンした場合、クラウドリージョンのドロップダウンにリージョンが表示されないことがある
CSCwk44165	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア リモートアクセス SSL VPN のサービス妨害（DoS）脆弱性

不具合 ID	タイトル
CSCwk48975	パケットトレーサの出力で data-plane access-group のドロップに「control-plane」が誤って追加される
CSCwk53369	Cisco ASA および FTD ソフトウェアのリモートアクセス VPN におけるサービス妨害（DoS）の脆弱性
CSCwk62296	SSP OpenSSH regreSSHion の脆弱性に対処
CSCwk62297	OpenSSH regreSSHion の脆弱性に対する SSP の評価
CSCwk67859	FTD と FXOS：RADIUS プロトコルスプーフィングの脆弱性（Blast-RADIUS）：2024 年 7 月
CSCwk69742	FTD：チェックサムの不一致によってポリシーの展開が失敗する。
CSCwk71992	pix-asa（メッセージ オーセンティケータ）に対する BlastRADIUS の脆弱性のフェーズ 1 修正
CSCwk74813	Cisco 適応型セキュリティアプライアンスおよび Firepower Threat Defense の TLS におけるサービス妨害（DoS）の脆弱性
CSCwk74997	CVE-ID では、FMC で IPS イベントを検索できない
CSCwk75035	Apache HTTP サーバー 2.4.59 以前のコアの脆弱性
CSCwk75832	AppID のリロードと Snort の再起動が同時に発生すると、Snort3 がリロードされる
CSCwk85702	Cisco Secure Firewall Management Center ソフトウェアの HTML インジェクションの脆弱性
CSCwm08231	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアのネットワークアドレス変換 DNS インスペクションのサービス妨害（DoS）の脆弱性
CSCwm08232	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアのネットワークアドレス変換 DNS インスペクションのサービス妨害（DoS）の脆弱性
CSCwm08235	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアの DHCP サービス妨害（DoS）の脆弱性
CSCwm35624	object-group と他のプレーン ACL が含まれる 1 つの AC ルールでブート時間が長くなる
CSCwm49153	Cisco 適応型セキュリティ アプライアンス ソフトウェアの SSH サーバーリソースにおける DoS の脆弱性

不具合 ID	タイトル
CSCwm49410	Cross-Origin-Opener-Policy が誤って設定されている
CSCwm50890	GWT および TID ページで参照されている Highcharts の未使用の脆弱なバージョン
CSCwm91176	Cisco ASA/FTD Firepower 3100/4200 シリーズの TLS 1.3 暗号サービス妨害（DoS）の脆弱性
CSCwm95070	FP 2100 シリーズ用 Cisco Secure Firewall ASA および Secure FTD ソフトウェアの IPv6 over IPsec サービス妨害（DoS）の脆弱性
CSCwn13597	VPN のお客様の FQDN がインターネットで予期せず検出可能となる
CSCwn15505	アプリケーションインスタンスが「開始」状態でスタックしている BS/QP での 2.17 の Lina コアの監視
CSCwn19639	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアにおけるアクセスコントロールルールのバイパスの脆弱性
CSCwn21584	Cisco Secure Firewall 適応型セキュリティアプライアンスおよび Secure Firewall Threat Defense ソフトウェアにおける Web サービスのサービス妨害（DoS）の脆弱性
CSCwn69963	unicorn zlib ライブラリで報告された CVE に対処
CSCwn73399	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwn90958	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwn91612	Cisco Secure Firewall Adaptive Security Appliance および Cisco Secure Firewall Threat Defense ソフトウェアの認証済みコマンドインジェクションの脆弱性
CSCwo00332	Firepower がリロード後に SSL トラストポイント設定を削除する
CSCwo00880	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのサービス妨害（DoS）脆弱性
CSCwo15021	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15022	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性

不具合 ID	タイトル
CSCwo15023	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15024	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア IKEv2 サービス妨害の脆弱性
CSCwo15027	Cisco Secure Firewall Adaptive Security Appliance および Secure Firewall Threat Defense ソフトウェア リモートアクセス SSL VPN のサービス妨害（DoS）脆弱性
CSCwo18850	Cisco Secure Firewall Adaptive Security Appliance、Secure Firewall Threat Defense ソフトウェア HTTPサーバー リモートでのコード実行の脆弱性
CSCwo35938	管理専用マルチキャストルートがないため、IPv6 管理通信が失われる。
CSCwo44732	ARP が到達不能なネクストホップのパケットをひそかにドロップする
CSCwo48439	スレッド名 Unicorn Admin Handler でのトレースバックとリロード
CSCwo91748	Lina：ACL 削除後に show access-list を実行すると、スレッド名 SSH でトレースバックが発生する
CSCwo97439	ACL：AAA 承認コマンドが適用された後に、ASA で「OOB アクセスリストの設定の変更が検出されました（OOB Access-list config change detected）」という誤った警告が表示されることがある
CSCwq18679	CSM/CLI の ASA：最後の ACL 回線に access-list ACL_name 回線 line_nr コメントが存在せず、「Specified remark does not exist」というメッセージが表示される
CSCwq21101	無効なホストヘッダーにより、ASA インターフェイス IP アドレスが表示される
CSCwq40256	暗号マップ ACL が特定のポートを使用している場合、インバウンド IPsec パケットが IPsec オフロードによってドロップされる。
CSCwq78991	レプリケーション中に不完全な ACL ポリシールールを取得するが、ファイアウォールがクラスタに参加する
CSCwq79815	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーの不正アクセスの脆弱性
CSCwq79831	Cisco Secure Firewall Adaptive Security Appliance ソフトウェアおよび Secure Firewall Threat Defense ソフトウェア VPN Web サーバーのリモートコード実行の脆弱性
CSCwq82095	特定の IDP のメッセージが表示され SAML 応答が拒否された

不具合 ID	タイトル
CSCwq82225	'show service policy' で初期関連のドロップに対してドロップカウンタが増加しない

表の最終更新日：2025 年 10 月 14 日

表 *27* : バージョン *7.6.0* で解決済みの機能バグ

不具合 ID	タイトル
CSCvj85665	ENH：アプライアンスのホスト名または IP アドレスは、FX-OS syslog に含まれている必要がある
CSCvm76755	DP-CP arp-in キューと adj-absent キューを分離する必要があります
CSCvn25053	FMC：vmsDBEngine を含む重要なプロセスを起動できない
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
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
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
CSCvx37329	Firewall Threat Defense で syslog メッセージ 852001 および 852002 を削除
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
CSCvx69675	アダプタホストと仮想インターフェイスのダウンに関する FXOS の重大な障害
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
CSCvx74133	アプリケーションインスタンスがオンラインではなく開始済みと表示される
CSCvz03407	IPTables.conf ファイルが消え、バックアップと復元が失敗する
CSCvz07712	展開が internal_errors で失敗する - 新しい ID を取得できない
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
CSCvz56980	API コールを使用する場合に処理不能な URL カテゴリオブジェクトが取得される
CSCvz66351	FTD シャーシのシリアル番号が FMC デバイスインベントリの詳細で「N/A（該当なし）」になっている
CSCvz68713	ASAv5 の PLR ライセンス予約は ASAv10 を要求している
CSCvz70310	ASA が SNMP の NAT ルールの作成に失敗し、「NAT がポートを予約できない」というエラーが表示されることがある。
CSCvz81888	asa-9.14.3 から asa-9.15.1/9.16.1.28 にアップグレードした後、NTP が *（同期済み）ステータスに変更されない
CSCvz85153	show access-control-config で NAP/IPS ポリシー名が表示されない
CSCwa34287	ASA：FPR11xx：アップグレード後のリロードの後に NTP 同期が失われる
CSCwa35200	AnyConnect SSL の一部の syslog が、ユーザーコンテキストではなく管理コンテキストで生成される
CSCwa76822	syslog-ng 宛先のスロットリングフロー制御が調整される
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
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
CSCwa95060	FTD デバイスでの「SFDataCorrelator：パーサー [エラー] シンタックスエラー（SFDataCorrelator:Parser [ERROR] Syntax error）」
CSCwa99932	クラッシュおよび再起動後に ASA/FTD がスタックする
CSCwb07908	スタンバイ FTD/ASA が 0.0.0.0 の送信元 IP で DNS クエリを送信する
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
CSCwb44245	SNORT3：tls1.3 インスペクションが有効になっている場合に、ポート 80 でプロキシトラフィックの問題が発生する
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
CSCwb55243	snort3 crashinfo がすべてのフレームの収集に失敗することがある
CSCwb67073	FMC：NAT ルールのコピー/切り取り/貼り付けができない
CSCwb77894	Firepower 1000/2100 が ROMMON モードにブートすることがある

不具合 ID	タイトル
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
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）
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
CSCwc44419	ASA/FTD がスレッド名 fover_health_monitoring_thread でトレースバックし、リロードすることがある
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
CSCwc76419	不要なファンエラーログを thermal ファイルから削除する必要がある
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
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
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
CSCwd02864	logging/syslog は、SNMP トラップとログ履歴の影響を受ける
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
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
CSCwd07098	25G CU SFP が Brentwood 8x25G netmod で機能しない
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
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

不具合 ID	タイトル
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
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
CSCwd10880	FPR 1100/2100/3100 のクリティカルな正常性アラート「user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)」
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
CSCwd22413	ASA/FTD：スレッド名 EIGRP-IPv4 でトレースバックし、リロードする
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
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
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
CSCwd39442	ssl ポリシーエラー：サーバー証明書の内部キャッシュステータスを取得できない
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
CSCwd43666	/opt/cisco/config/var/log/ASAconsole.log の logrotate がない理由を分析する
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
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
CSCwd47278	TLS1.3 セッションでの 256/1550 ブロックリーク
CSCwd50218	ASA の復元で vlan 設定が適用されない
CSCwd53635	AWS：Geneve トンネルインターフェイスで SSL 復号が失敗する

不具合 ID	タイトル
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
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
CSCwd56431	FTD プロダクションビルドでアサートを無効にする
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
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
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
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 AC クライアントの一致の失敗
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
CSCwd67100	データパスプロセスでの ASA のトレースバックとリロード
CSCwd67101	FPR1150：ease secure all を実行すると、実行形式エラーが表示され、リロードするまでデバイスがハングする
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
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
CSCwd70490	LACPDU が受信されない場合、ポートチャネル メンバー ポート ステータス フラグとメンバーシップステータスはダウンである
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
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
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

不具合 ID	タイトル
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
CSCwd78123	fips モードで dh グループ 31 で IPSec/Ikev2 VPN セッションを起動するときに、ASA/FTD がトレースバックおよびリロードする
CSCwd78624	ASA が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
CSCwd78915	設定エラーが原因で展開が失敗し続ける -- service-policy policy_map
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
CSCwd81123	プロセス smConlogger の FXOS での CPU 使用率が高い
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
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
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。
CSCwd85073	Snort3 ストリームコアで init_tcp_packet_analysis が検出される
CSCwd85178	AWS ASAv PAYG ライセンスが GovCloud リージョンで機能しない。
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
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
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

不具合 ID	タイトル
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
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
CSCwd89811	"timeout conn" 秒後に Azure ASAv クラスタリングでトラフィックが失敗する
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
CSCwd90894	ASA：アップグレード後、SSH を介してインターフェイスに接続できない
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
CSCwd92327	2k プラットフォームでは、数字で始まるユーザーの外部認証が失敗する
CSCwd92804	FPR2100 で FAN LED がオレンジに点滅する
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
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
CSCwd95415	snort ハートビート障害により、スタンバイデバイスが障害状態になる
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
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	FPR41xx/9300：ブレードがリブート信号をキャプチャまたはログに記録しない
CSCwd99592	HealthMon ページにおけるサイドバーのロードの最適化

不具合 ID	タイトル
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
CSCwe01977	DHCPv6 が設定された状態でリロードすると、ASA/FTD がトレースバックしてリロードされることがある
CSCwe02012	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
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
CSCwe03991	tmatch コンパイルプロセス中に FTD/ASA がトレースバックおよびリロードする
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
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。
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
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
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
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
CSCwe10670	アイデンティティ ネットワーク フィルタが FTD から削除されない
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
CSCwe11754	内部クラスタリングエラーが原因で、ノードがランダムにクラスタに参加できない
CSCwe11902	FTD：HA トレースバックとリロード

不具合 ID	タイトル
CSCwe12407	SSL ハンドルのリークによる高 Lina メモリ使用量である
CSCwe12645	ノードがリブートされて管理インターフェイスがシャットダウンされると、セカンダリの状態が準備完了と失敗の間で反転する
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
CSCwe13781	FTD/ASA での IKEv2 マルチ DVTI ハブのサポート
CSCwe13965	VTI/DVTI インターフェイスでのインターフェイス統計情報とトンネル稼働時間の表示のサポート
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 IP SLA 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
CSCwe15477	アプリケーション管理インターフェイスがダウンしており、管理接続障害が発生している可能性がある
CSCwe16905	cdFMC：VPN セッションマネージャロールを持つユーザーが cdFMC にアクセスできない
CSCwe18216	ログに Null 接続エラーが表示される
CSCwe18462	ASA/FTD：GTP インスペクションロギングの改善
CSCwe18467	ASA/FTD：GTP インスペクションエンジンの有用性
CSCwe18472	[FTD Multi-Instance][SNMP] - CPU OID が、関連する CPU の不完全なリストを返す
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
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
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

不具合 ID	タイトル
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
CSCwe21884	「kill」コマンドのラッパーが作成されて、呼び出し元がログに記録される
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
CSCwe22152	SNMPD コアが snmp_sess_close および notifyTable_register_notifications に存在する
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
CSCwe22431	[SXP-UserIP ミュートリーダー] FMC HA の参加で FW IP_SGT マッピングがフラッシュされ、登録済みセンサーで再ストリーミングされる
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
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
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
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
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
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

不具合 ID	タイトル
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
CSCwe28912	FTD HA のアップグレード後にプライマリユニットですべての HA 設定が失われる
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
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
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
CSCwe30359	Snort での膨大なルール評価によるトラフィックのドロップ
CSCwe30687	mp_counter_alloc での dvti メモリリーク
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
CSCwe32058	Geneve キャプチャの確認中に ASA/FTD がスレッド名「ci/console」でトレースバックおよびリロードすることがある
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
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
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。

不具合 ID	タイトル
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
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用に使用すると SSH が動作を停止する
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
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
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
CSCwe42986	クラシックイベントおよび統合イベントは SMC に到達できないケースを処理する必要がある
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
CSCwe44672	Syslog ASA-6-611101 が 1 つの SSH 接続に対して 2 回生成される
CSCwe45569	management-access が有効になっているために 7.0 から 7.2.x への FTD アップグレードでトレースバック/リロードが発生する
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
CSCwe47485	FTD：コマンド実行が LINA プロンプトをロックしているため CLISH が遅くなる
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
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
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。
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
CSCwe54999	ASAv および FTDv 用の ESXi 8 でのより低い CPU インスタンスによるプロトコルダウン

不具合 ID	タイトル
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
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
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
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
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
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。
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
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
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。
CSCwe63686	WM FDM @009_check_snort_preproc.sh でアップグレードの準備状況チェックに失敗したが、7.3.1-19 へのアップグレードが成功する
CSCwe63759	クラスタ強化の修正
CSCwe64404	ASA/FTD がトレースバックおよびリロードすることがある

不具合 ID	タイトル
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
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
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
CSCwe68917	Snort3 が SMTPS トラフィックを ACP ルールに一致させられない
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。
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 での FTD のトレースバックおよびリロード
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
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

不具合 ID	タイトル
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
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
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
CSCwe78474	FPR4100/9300 では、ファームウェアがバージョン 1.0.19 に正常にアップグレードされると、package-vers が 0.0 と表示される
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
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
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
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
CSCwe81291	設定のバックアップが復元されると、HA が無効の状態で FTD ユニットが起動する
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
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

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
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
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
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
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
CSCwe87134	ASA/FTD：SCTP トラフィックのレートが高いため、トレースバックとリロードが発生する
CSCwe87831	FMC UI の応答が非常に遅い：FMC ntpd サーバーのアクセス可能性をモニタリングする正常性モジュールを追加する
CSCwe88492	設定時にバナーログインが表示されない
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
CSCwe89256	Firepower Chassis Manager に ECDSA 証明書でアクセスできない
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
CSCwe90168	証明書認証の使用時に FMC GUI にアクセスできない
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
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
CSCwe91008	cd_pdts.so で Snort3 が頻繁にクラッシュする
CSCwe92324	FPR31xx：SNMP ポーリングにおいて、FanTray が実際に動作しているにもかかわらず、誤ってダウン状態で報告される

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
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
CSCwe93202	FXOS REST API：タイプ「ecdsa」のキーリングを作成できない
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
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
CSCwe93925	既存の VLAN ID を異なるインターフェイスで再利用/再割り当てすると、FTD への展開が失敗する
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
CSCwe95110	接続イベントで、パッシブ インターフェイス トラフィックの OVERSUBSCRIPTION フロー メッセージが正しく表示されない
CSCwe95462	正常性アラートに 8 個を超えるフィールドが含まれていると、ヘルスモニタリングでコアダンプが発生する
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
CSCwe95786	lina:tcp プロキシでトレースバックとリロードが発生する
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
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
CSCwe97939	ASA/FTD クラスタ：「cluster replication delay」を変更して、最大値を 15 秒から 50 秒に増やす
CSCwe98146	特定のトラフィック条件下で Snort3 のコアダンプが発生する

不具合 ID	タイトル
CSCwe98319	ASAConfig を複数回再起動すると、再起動ごとに 16K メモリがリークし、ZMQ のメモリ不足が発生する
CSCwe98559	Snort3：RNA 統計情報に必要なカウンタがない
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。
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
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
CSCwf01064	9.18.2 以降、TCP ping が全く機能しない
CSCwf02363	nss_passwd_lookup からのコール後に SslServiceDetector で Snort3 がクラッシュする
CSCwf03490	portmanager.sh が継続的に bash 警告をログファイルに出力する
CSCwf04460	Ctrl+C を押して cancel show tech fprm detail コマンドを実行すると、fxos ディレクトリが表示されなくなる。
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
CSCwf04983	3100 ユニットが、エラー「設定済みのオブジェクト（sys/switch-A/slot-2）が見つかりません（configured object（sys/switch-A/slot-2）not found）」でクラスタに参加できない
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。
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	Firepower 4100 および 9300 のハートビートタイムアウトを 6 秒に設定
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
CSCwf10494	ユーザーが [デバイス管理（Device Mgmt）] ページから [パケットトレーサ（Packet Tracer）] に移動した場合に、選択したデバイスが正しくない
CSCwf10910	FTD：7.3.0 を実行している ZMQ でのトレースバック
CSCwf11877	TPK 3110：7.2.4-144 へのアップグレード後のファームウェアバージョンの不一致
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
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
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）
CSCwf14126	プロセス名 Lina を示す ASA のトレースバックとリロード
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
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
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。
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
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。

不具合 ID	タイトル
CSCwf17314	/internal_rest_api/accesscontrol/rapplicationsavailable が原因で、FMC の展開ログのローテーションが速くなる
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）
CSCwf17858	インターフェイスの正常性チェックに失敗したため、ノードが TPK クラスタから離脱している
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
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
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
CSCwf21640	相関ルールの [セキュリティインテリジェンスカテゴリ（Security Intelligence Category）] オプションに DNS および URL の値がない
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
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
CSCwf23868	同期がスキップされている場合に設定状態を更新する
CSCwf24773	crashhandler がテストモードの Snort で実行されている
CSCwf25454	古い anyconnect エントリが原因でルーティングの問題が発生する
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
CSCwf26599	NAT ページでデータを読み込み中にエラーが発生する：未使用のポートオブジェクトが使用されている場合
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

不具合 ID	タイトル
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
CSCwf27458	AC ポリシーの変更が、編集時にインスタンスページに反映されない
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
CSCwf30542	CHP オブジェクトのクリーンアップ中に Snort3 がクラッシュする
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。
CSCwf30824	CIMC IPMI ハングの問題の自動リカバリとして CIMC リセットを追加
CSCwf31050	FMC で複数のアプライアンスの高い CPU 使用率が誤って表示される
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
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	[IMS_7_4_0] - 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
CSCwf34500	FTD：GRE トラフィックが CPU コア間で負荷分散されていない
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
CSCwf35500	FXOS/SSP：システムでの DIMM の修正可能なエラーイベントの可視性が向上する
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
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。
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
CSCwf38782	syslog メッセージ ASA-3-202010 の変更

不具合 ID	タイトル
CSCwf39108	asp load-balance per-packet auto が使用されていると、ファイアウォールリングがスタックしてパケット損失が発生する可能性がある
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
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
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
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
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 でトレースバックとリロードが発生する
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 でトレースバックとリロードが発生する
CSCwf44621	スレッド DATAPATH-6-21369 でトレースバックとリロードが発生し、syslog メッセージ ID 202010 の生成に関連する
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
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	FTD から Priority-queue コマンドを削除する || Priority-queue コマンドによりサイレント出力パケットドロップが発生する
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
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
CSCwf51512	内部リンクのダウンおよび NPU の切断による 2100 のリロード

不具合 ID	タイトル
CSCwf51635	予期しない TLS クライアントキー交換による Snort3 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
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
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
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
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
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
CSCwf57856	MTS バッファキューのリークが原因の FXOS のトレースバックとリロード
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
CSCwf59529	アイデンティティポリシーのアクティブ認証で Snort3 リダイレクトホスト名にすべての FQDN オブジェクトが一覧表示されない
CSCwf59571	FTD/Lina：特定の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
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
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
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

不具合 ID	タイトル
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
CSCwf63256	Firepower がトレースバックとともに予期せずリロードする
CSCwf63589	FTD snmpd プロセスのトレースバックと再起動
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
CSCwf66307	インターフェイスステータスを除外する除外ポリシーが、しばらくすると FMC で削除される
CSCwf66333	インターフェイス ステータス モジュールの FTD 除外ポリシーで [すべてのインターフェイス（All interfaces）] を選択しても機能しない
CSCwf69633	FTD が ABORT_HA_DEPLOYMENT が原因で HA に参加できず、ユニットが無効状態になった
CSCwf69880	SNMP スレッドに起因するファイアウォールのトレースバックとリロード
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
CSCwf70275	FTD：クライアント hello のサイズが TCP MSS バイトを超える場合、TLS サーバーアイデンティティが機能しない
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
CSCwf72285	DAP：debug dap trace が 3000 行を超えると正常に表示されない
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
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
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
CSCwf75694	ASA：無効な TEID=0 が原因で GTP インスペクションが「PDP コンテキスト削除応答」メッセージをドロップする

不具合 ID	タイトル
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。
CSCwf77795	FMC QoS ダッシュボードに、一致した QoS ルールが表示されない
CSCwf77994	FTD デバイスシステムコアの瞬間的な高使用率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
CSCwf78950	FMC プロセス ssp_snmp_trap_fwdr のメモリ使用率が高い
CSCwf79279	ns_reload 中に複数の network-service オブジェクトをロード中に Azure vFTD ノードのトレースバックが発生する
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
CSCwf80183	トラフィックフロー中に navl で Snort3 コアが表示される
CSCwf81058	FTD：[有効（Enabled）] と表示される Firepower 3100 の動的フローオフロード
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。
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
CSCwf84318	スレッド DATAPATH での ASA/FTD のトレースバックとリロード
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

不具合 ID	タイトル
CSCwf87348	state-link がフラッピングされると、HA 状態がフェールオーバーの理由なしでスタンバイ準備完了から一括同期に変更される
CSCwf88124	FPR 1010：トランクモードのスイッチポートが、電力損失またはリブートの後に VLAN トラフィックを通過させない場合がある
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
CSCwf89959	ASA：ISA3000 が entPhySensorValue OID SNMP ポーリングに応答しない
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
CSCwf92308	トレースバック：CdFMC：ネットワークオブジェクト（network/host/range/fqdn）オーバーライドの編集により内部エラーがスローされる
CSCwf92371	HA セカンダリユニットがリブート後に無効化：プロセスマネージャが LSP の保護に失敗する
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 を含む一部の Vault シークレットでファイルが欠落する
CSCwf94450	メモリ破損により、FTD Lina でスレッド名 DATAPATH のトレースバックが発生する
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
CSCwf95288	FPR1k スイッチポートで CDP トラフィックが渡される
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
CSCwf99303	アップグレード後に、管理 UI にカスタム CA 署名付き証明書ではなく自己署名証明書が表示される
CSCwf99434	新しいイメージファイルを FPR2130 に転送できず、トレースバックが観測された
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

不具合 ID	タイトル
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
CSCwh03373	GWLB で展開された FTDv で TLS サーバーアイデンティティ検出を有効にしない
CSCwh04185	アクティブな応答で Snort がクラッシュする
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
CSCwh09113	HA の FPR1010 が「edsa_rcv: out_drop」エラーで GARP/ARP との送受信に失敗する
CSCwh09968	ASA/FTD：NAT の変更によるトレースバックとリロード
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
CSCwh11677	128 文字を超える saml idp 名を使用できない
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
CSCwh11960	Max Detect on Detection により、一部の ping トラフィックがブロックされる
CSCwh12120	VTI トラフィックのネクストホップに不適切な終了インターフェイスが選択される
CSCwh13312	通知デーモンのハートビートアクションの無効化
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

不具合 ID	タイトル
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
CSCwh15223	DAQ/Snort が不正な L3 ヘッダーを送信する場合の Lina トレースバックおよびリロード
CSCwh15636	100G Netmod を実行している複数インスタンスでの ARP 学習の問題
CSCwh15649	出力 VRF に接続先へのルートがない場合、unexpected-packet ドロップの理由によるパケットドロップが発生する
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
CSCwh16759	マルチコンテキスト環境のプライマリアクティブ ASA ユニットで SNMP が機能しない
CSCwh17052	API を使用してオブジェクト/カテゴリ名を作成する際に文字列長の検証が行われていない
CSCwh17576	FTD 側から稼働している場合でも、FMC でのサイト間 VPN トンネルのステータスがダウンしていると表示される
CSCwh17965	[表示] FXOS：リロード後に、PC メンバーインターフェイスがダウン状態で関連付けられていない/割り当てられていないと表示される
CSCwh18967	FXOS FPRM のトラブルシューティングに「show env tech」を含める
CSCwh19352	1 ACK がドロップされた場合でも comm アラームが発生し、ユニットがスイッチオーバーする
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
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
CSCwh21381	LinaConfigTool と xml サーバー間のメッセージ交換に関するロギングの改善
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

不具合 ID	タイトル
CSCwh22888	FXOS：DIMM で修正可能なエラーが複数回発生すると、ブレードが強制的に縮退状態になる措置を削除
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
CSCwh23863	SYSLOG UDP：いずれかの syslog サーバーで userVRF の syslog メッセージが取得されない
CSCwh24321	FXOS：Alperton 100G NetMod が適切に認識されない
CSCwh24932	FP3110 上の ASA ソフトウェアが show inventory 出力で誤ったシリアル番号を表示する
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
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。
CSCwh27886	シャーシマネージャで、特定の場合に HTTP 500 内部サーバーエラーが表示される
CSCwh28144	特定の OID 1.3.6.1.2.1.25 が応答しない
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
CSCwh30257	ファイル API のメモリ破損が原因で Snort3 がクラッシュする
CSCwh30346	ASA/FTD：各 NLP NAT ルールの 1 秒のフェールオーバー遅延
CSCwh30676	クラスタのセットアップで、管理インターフェイスで設定された systemIP への ping が失敗する
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
CSCwh31502	HA での startup-config から backup-config.cfg への Lina コピー操作の機能拡張
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

不具合 ID	タイトル
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
CSCwh34836	侵入ポリシーの編集および保存中に UI で例外が発生する
CSCwh36005	「1 errors seen during populateGlobalSnapshot」が原因でポリシーの展開に失敗する
CSCwh37268	Fover_trace ログが繰り返し表示される
CSCwh37655	Snort2：プロセスのシャットダウン中にマルウェアシードファイルの書き込みがスキップされる
CSCwh37733	FTD が MAC アドレス 0000.000.000 で UDP500 パケットに応答する
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
CSCwh40294	SNMP 設定中のパニックイベントによる ASA のトレースバック
CSCwh40635	FTD のリブートまたは lina のリロード後に管理インターフェイスを介した syslog が loggerd を通過しない
CSCwh40968	最大セグメントの制限に達したため、大きなファイルのダウンロードに失敗する
CSCwh41127	ASA/FTD：スタンドアロン ASA の「overlaps with inside standby interface address」NAT64 エラー
CSCwh41606	問題のある展開での大量のロギングにより、重要なログがロールオーバーされる
CSCwh42077	Cisco_Firepower_GEODB_FMC_Update* が diskmanager に含まれていない
CSCwh42142	NTP 時間の問題（以前の展開が将来のタイムスタンプで完了）により、ポリシー適用がスタックする
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
CSCwh43230	強力な暗号化ライセンスが HA の ASA ファイアウォールに適用されない。
CSCwh43945	ssl パケットのデバッグが有効になっている場合、FTD/ASA のトレースバックとリロードが発生することがある

不具合 ID	タイトル
CSCwh44215	ENH：TSID プローブを EVE 検査から除外する
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
CSCwh47053	ASA/FTD がスレッド名「dns_cache_time」でトレースバックし、リロードすることがある
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 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
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
CSCwh51438	10G-T-X モジュールのサポートを追加
CSCwh51872	「asa_log_client が 1 回終了（asa_log_client exited 1 time(s)）」というメッセージが複数回表示される
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）
CSCwh53143	ASA：IPSec トンネルを介した管理アクセスが機能しない
CSCwh53377	TLS1.3 が使用されている場合、FMC は FTD デバイスに対して発行された証明書を検証しない
CSCwh53745	ASA：DNS クエリ応答のために着信接続を開始するための予期しないログ
CSCwh54029	FMC HA：FTD が切断されると、セカンダリ FMC で冗長 FTD 登録タスクが失敗する。
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
CSCwh55178	callhome test コマンドでのメモリリークの処理

不具合 ID	タイトル
CSCwh55543	FMC 4600 v7.2.4 EVE ダッシュボードウィジェットが破損したデータを表示する
CSCwh56290	リブート後に FPR2100 プラットフォームで設定された将来の日付が反映されない（クロックを手動で設定）
CSCwh57976	SSL インスペクションでのサポートされている署名アルゴリズム処理における CPU 使用率の改善
CSCwh58190	csm_snapshot_error で FMC 展開に失敗する
CSCwh58467	ASA が「warmstart」SNMP トラップを送信しない
CSCwh58490	アップグレード後に内部エラーが原因で FMC 展開に失敗する
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
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
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
CSCwh60971	32k オブジェクト ID の制限に達していないにもかかわらず、NAT プールが正常に機能しない。
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
CSCwh62731	6.6.5 から 7.2.5 への FTD のアップグレードで OGS が削除され、ブート時にルールが拡張される
CSCwh63211	snp_nat_xlate_verify_magic.part で Lina のコアダンプが発生し、ソフトトレースが生成される
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
CSCwh65128	LINA show tech-support が sf_troubleshoot.pl（トラブルシューティング ファイル）の一部として生成されない

不具合 ID	タイトル
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、トレースバックが発生することがある
CSCwh68068	VRF が設定されていると Firepower WCCP router-id がランダムに変わる
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
CSCwh69156	snort3 のトレースバック時に FTD-HA がフェールオーバーしないことがある
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
CSCwh69843	WM DT：トランスペアレントモードの ASA が、すべてのノードに等しい IPv6 ルータ アドバタイズメント パケットを送信しない
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	ウォッチドッグ時間がデフォルトの 15 秒を超えているため、ASA/FTD がトレースバックし、リロードすることがある
CSCwh70874	FTD：ポリシー展開が進行せず、中止されるため失敗する
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
CSCwh71008	CSF 4200：PSU ファン速度がクリティカル
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
CSCwh71161	ASA|FTD：スレッド名 update_mem_reference でのトレースバックとリロード。
CSCwh71358	Firepower 3105 デバイスで FDM を介して VRF を作成できない
CSCwh71589	Coverity 886745：verify_generic_signature で OVERRUN が発生する
CSCwh71665	CPU プロファイリング中に match_partial_keyword で ASA がトレースバックする

不具合 ID	タイトル
CSCwh72370	FTD：glibc アロケータでの効果的ではないメモリ解放アルゴリズムが原因で、Mariadb を使用すると OOM が発生する可能性がある
CSCwh73727	Snort3 で IP プロトコル 51 がドロップされる
CSCwh74219	FMC 7.2.4.1 から 7.2.5 へのアップグレードが 600_schema/000_install_fmc.sh で失敗する
CSCwh74870	DAQ 未処理カウンタの予期しない高い値
CSCwh75829	FMC プライマリディスクの劣化エラー
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
CSCwh78064	FTD：重要なアップグレードスクリプトは、アップグレードの再試行によってバイパスされるべきではない
CSCwh78118	プロセス fsm_send_config_info_initiator で ASA/FTD のトレースバックとリロードが発生する
CSCwh79095	Snort がゼロバイトを含む過剰な数の snort-unified ログファイルを生成する
CSCwh81366	[マルチインスタンス] 2 番目のハードドライブ（FPR-MSP-SSD）が使用されていない
CSCwh82305	FTD でポリシー展開中に swapcontext で Lina のコアダンプが発生する
CSCwh82766	FTD バックアップを内部でバッチ処理により一括生成できるようにする
CSCwh82962	ファイアウォールで使用するために、ins（シーケンス内）および oos（シーケンス外）パケットを正しく更新する必要がある
CSCwh83021	ASA/FTD HA ペアの EIGRP ルートがフェールオーバー後にフラッシュされる
CSCwh83254	ASA/FTD：スレッド名 CP Crypto Result Processing でのトレースバックとリロード
CSCwh83301	プロセス Telegraf による高 CPU 使用率アラート
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
CSCwh83517	VRF シナリオで検出されたルート変更が原因で VTI トンネルがダウンする
CSCwh83854	2000 を超える GID の値がないため、相関ルールを設定できない

不具合 ID	タイトル
CSCwh84376	FPR4200/FPR3100-HA/クラスタで、デバイスのリブート時に crashinfo/corefile.lina が確認された
CSCwh84610	FMC GUI から RA VPN ユーザーを切断すると失敗する
CSCwh84647	バックアップ復元：デバイスがローカルで管理されている場合にサイレントエラーが発生する
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
CSCwh87058	FTD：内部証明書の生成により、証明書と秘密キーの不一致が発生する
CSCwh88378	WA MI：Management1/2 の nameif がルーテッドインスタンスで設定されていない場合、FMC からの HA 展開がブロックされる
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
CSCwh91419	FTD のインストールが FPR-2K のエラーメッセージが表示されて失敗する。「アプリケーションインスタンス FTD のエラー。（Error in App Instance FTD.）使用可能なメモリがブレードによって更新されていません（Available memory not updated by blade）」。
CSCwh91574	FTD：スレッド名 cli_xml_request_process でのトレースバック
CSCwh91976	WA MI：統合が有効になっていても、シャーシからのトラップ（リンクアップ/ダウン）が NMS で表示されない
CSCwh92156	ファイアウォールが誤解を招く SCP ファイルのコピーの失敗理由を表示する
CSCwh92345	ソフトウェアのアップグレード後に crypto_archive ファイルが生成される。
CSCwh92541	ランダムな FTD Snort3 トレースバック
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
CSCwh93710	ASA、ASDM、および FTD で [最後のヒット（Last Hit）] のタイムスタンプが最新の値に更新されない
CSCwh95003	バックアップの失敗後に Init プロセスの CPU 使用率が 100% に急増する
CSCwh95010	スレッド名 Lina で予期しないトレースバックが発生し、デバイスがリブートされる

不具合 ID	タイトル
CSCwh95025	GTP 接続が特定の状況下で clear conn を発行してもクリアされない。
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
CSCwh95443	データパスが占有され、クラスタリングユニットがクラスタから除外される
CSCwh96055	データインターフェイスがゲートウェイとして使用されている場合、管理 DNS サーバーに到達できないことがある
CSCwh98733	ASA：多くのトラフィックフローと syslog メッセージのテスト中にトレースバックとリロードが発生する
CSCwh99398	ASA/FTD がスレッド名「DATAPATH-34-17852」でトレースバックし、リロードすることがある
CSCwi01085	PTHREAD-3587 での FTD VMware のトレースバック
CSCwi01323	show interface がゼロ以外であるにもかかわらず、MIO の SNMP OID ifOutDiscards が常にゼロになる
CSCwi01381	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
CSCwi01895	ハートビートエラーによるファイル転送中の接続ドロップ
CSCwi01981	30 日間のアップグレードの revert-info の自動削除は、通信障害に対して耐性がない
CSCwi02039	FMC clean_revert_backup スクリプトがログを作成せずにサイレントで失敗する
CSCwi02134	FTD が同じフローイベントに対して複数の複製された NetFlow レコードを送信する
CSCwi02599	FTD の CDO への移行時に、SSX イベントが古いテナントに送信され続ける
CSCwi02754	SNMP が有効になっているスタンバイユニットでの FTD 1120 のトレースバックおよびリロード。
CSCwi02919	snmp-server host が指定されていると SNMP が応答しない
CSCwi03407	トリガーポイントなしの FP2140 でのトレースバック
CSCwi03528	クロス IFC アクセス：PING を以前の非クロス IFC 動作に戻す
CSCwi04021	日次変更調整レポートが同じ期間のレポートをランダムに生成する

不具合 ID	タイトル
CSCwi04351	スクリプト 999_finish/999_zz_install_bundle.sh で FTD アップグレードが失敗する
CSCwi05618	「CD App Sync エラーによりスタンバイで SSP 設定を適用できませんでした（CD App Sync error is Failed to apply SSP config on standby）」によって FTD HA 同期が失敗する
CSCwi06690	AnyConnect 証明書認証/承認を使用した場合の証明書エンコーディングの問題
CSCwi06797	スレッド DATAPATH での ASA/FTD のトレースバックとリロード
CSCwi07068	SFDataCorrelator は毎分「MySQL 接続を強制終了します（Killing MySQL connection）」とログに記録し、パフォーマンスの問題が発生する
CSCwi08374	DCCSM の問題が原因で発生する「登録のブロック（Registration Blocking）」エラーで、FMC バックアップが失敗する
CSCwi11049	Cisco Secure Access：FWaaS を介してトラフィック損失が不定期に発生する
CSCwi11520	FTD OSPFV3 IPV6 ルーティング：FTD がサポートされていない拡張 LSA 要求をネイバールータに送信する
CSCwi12772	スレッド名 DATAPATH-8-17824 での ASA クラスタのトレースバック
CSCwi13134	FP3140 でハードウェアバイパスが期待どおりに機能しない
CSCwi13223	VTI インターフェイスの送信元が空になる
CSCwi13510	Config-url が設定ファイルとしてディレクトリを受け入れる
CSCwi14132	FMC/cdFMC での API レート制限の増加
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
CSCwi15409	ASA/FTD：スレッド名「Unicorn Proxy Thread」でトレースバックし、リロードすることがある
CSCwi15787	any->any で NAT 免除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
CSCwi16034	FMC は、データベース完全性チェックエラーに関する電子メールによる正常性通知を生成しない
CSCwi16571	Snort3 を使用した capture-traffic Clish コマンドで適切なキャプチャ結果が生成されない

不具合 ID	タイトル
CSCwi18581	SSH スレッドに起因するファイアウォールのトレースバックとリロード
CSCwi18663	FMC-4600：プレフィルタポリシーに none と表示される
CSCwi19015	ASA/FTD がスレッド名「DATAPATH-13-6022」でトレースバックし、リロードすることがある
CSCwi19485	フェールオープン snort-down は、FMC から有効化されて展開されているにもかかわらず、インラインペアでオフになる
CSCwi19849	フェーズ 2 の廃止された暗号を使用した VPN load-balancing クラスタ暗号化
CSCwi20045	ウォッチドッグ（watchdog_time＝0）に起因して、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
CSCwi20848	RAVPN OID ポーリングによる SNMP が原因で ASA/FTD のメモリ使用率が高くなる
CSCwi20955	TAP モードを有効にすると、FTD が展開中に data-path でトレースバックすることがある
CSCwi22296	ASA：大規模な設定が原因で論理デバイスがフェイルセーフモードでブートすることがある
CSCwi23545	HA CP クライアントの統計で、実際の Tx/Rx および信頼できる Tx/Rx が表示されない
CSCwi24368	テーブル内の以前のエントリが原因で、プライマリ FMC でスタンバイマネージャの追加が失敗する
CSCwi24370	古い HA トランザクションを失敗状態に移行し、後続の HA トランザクションを作成する必要がある
CSCwi24461	ポートマネージャ用に生成されたコアでデバイス/ポートチャネルがダウンする
CSCwi24814	FIPS モードで、TLS 設定が有効になっている外部認証では、CLI ログインが機能しない（FMC および FTD）
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
CSCwi26064	ASA：1 つのコンテキストで route-map を変更すると他のコンテキストに影響する
CSCwi26895	ASA SNMP OID cpmCPUTotalPhysicalIndex が CPU インデックス値ではなくゼロの値を返す

不具合 ID	タイトル
CSCwi27338	TCP 443 の古い asp エントリがデフォルトポートの変更後もスタンバイのままになる
CSCwi27402	FTD：WM ファームウェアを 1023.0207 に更新
CSCwi28645	読み取り専用カスタムロールに割り当てられたユーザーは、Snort2 の侵入ポリシーのコンテンツを表示できない
CSCwi29041	/var/log/messages でのログスパム：'map_id' 列の範囲外の値
CSCwi29538	失敗した「FlexConfig ポリシー」スクリプトを使用した EIGRP の移行の失敗でデータベース破損が生成される
CSCwi30843	永続的ではない除外期間が選択されている場合、[ポリシーの除外（Exclude Policy）] ページでデータを取得するとエラーが発生する
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
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
CSCwi31480	アラート：デコミッションの失敗、理由：確認後に内部エラーが FCM または CLI からクリアされない
CSCwi31558	File-extracts.logs が diskmanager で認識されないため、ディスク使用量が増加する
CSCwi31766	PSU ファンが、正常に動作しているときに show environment の出力でクリティカルと表示される
CSCwi31966	FTD ADI デバッグで SAML 認証セッションの誤った server_group および/または realm_id が表示されることがある
CSCwi32759	最初の属性が欠落している場合、Username-from-certificate のセカンダリ属性が抽出されない
CSCwi33710	cli_firstboot がブートストラップ設定のマルチインスタンスをインストールすると、ipv6 テーブルフラッシュの例外が発生する
CSCwi34125	ASA：Snmpwalk で OID ceSensorExtThresholdValue に「そのようなインスタンスはありません（No such Instance）」と表示される
CSCwi34719	Radius で外部認証を使用して FTD デバイスに SSH 接続できない
CSCwi34730	TLS Web サイト復号化が ERR_HTTP2_PROTOCOL_ERROR で中断する
CSCwi35267	TLS1.3：コア復号ポイントが tls_trk_try_switch_to_bypass_aux() になる

不具合 ID	タイトル
CSCwi36311	SMA で SIGTERM ではなくキルツリー機能を使用
CSCwi36843	操作中にサブインターフェイスの管理状態が変更された理由に関連する詳細なロギング
CSCwi38061	ファイル記述子の制限を超えていることによる ASA/FTD のトレースバックおよびリロード
CSCwi38425	グローバルに設定されたヘルスモニターアラートが、リーフドメインに割り当てられたデバイスからのアラートを送信しない
CSCwi38440	アラート電子メールの内容でホスト名が IP アドレスに置き換えられる
CSCwi38449	アラートに表示されるモジュール名が変更され、FMC で設定されているモジュール名とは異なる名前になる
CSCwi38662	FMC で FTD HA が部分的に作成されるべきではない
CSCwi38708	FDM 展開の失敗
CSCwi38957	FDM から FMC へのポリシー適用が失敗する
CSCwi40193	最適ではないルックアップ時の DCE/RPC/FTP トラフィックのヘアピニング
CSCwi40302	"no username admin" が設定された新しい AWS FTDv デバイスで展開が失敗する
CSCwi40487	SNORT クラッシュ後の FTD HA 障害
CSCwi40536	ASA/FTD：show tech を実行しており、メモリ使用率が高い状態だとトレースバックとリロードが発生する
CSCwi40674	UI でグループポリシーを編集すると、Cisco Umbrella プロファイルなどが正しくクリアされない
CSCwi41666	大きなファイルをクリーンアップするための MonetDB スタートアップの機能拡張
CSCwi42962	GeoDB 国コードパッケージの更新を FMC にインストールしても、更新が FTD に自動的にプッシュされない
CSCwi42992	ASA/FTD がスレッド名 IKEv2 Daemon でトレースバックし、リロードすることがある
CSCwi43240	ネットワーク検出ポリシー参照が FMC データベースにない場合、展開が失敗する
CSCwi43492	スレッド名 DATAPATH での ASA のトレースバックとリロード

不具合 ID	タイトル
CSCwi43782	ヘッダー長が IE タイプ 152 で無効なため、GTP インスペクションが IE 152 のパケットをドロップする
CSCwi44007	NAT64 で、大きなオブジェクト範囲では FMC 検証が失敗し、オブジェクトネットワークでは成功する
CSCwi44148	ISE-PIC 接続の誤ったヘルスモニターアラート
CSCwi44208	メモリ/負荷が低いため SNMP でトレースバックが発生する
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
CSCwi44488	Cisco ASA/FTD：プロセス「lina」で、ikev2_find_child_sa_by_local_spi が原因でトレースバックとリロードが行われる
CSCwi44912	ISA3000 のトレースバックとリロードによるブートループ
CSCwi44953	マイナーパッチのアップグレード中は sru_install をスキップし、必要な場合にのみインストールする必要がある
CSCwi45054	FMC 展開のプレビューでは、FTD 展開の前後で異なる情報が表示される
CSCwi45408	Monetdb に 14GB の不明な BAT データがあり、「/Volume で管理対象外ディスクの高使用率（High unmanaged disk usage on /Volume）」が発生している
CSCwi45630	fqdn トラフィックによる Snort3 のトレースバック
CSCwi45878	ASA/FTD：SAML を使用した DNS ロードバランシングが VPN ロードバランシングで機能しない
CSCwi46010	ASA/FTD：クラスタが PAT IP 宛ての無効なパケットに対して誤って syslog 202010 を生成する
CSCwi46023	FTD が二重タグ付き BPDU をドロップする。
CSCwi46641	インターフェイスのステータスを変更すると、FTDv がスレッド名「PTHREAD-3744」でトレースバックし、リロードすることがある
CSCwi46676	API：/operational/commands が Swagger の記載どおりに機能しない
CSCwi47029	FMC 内で「最新の Cisco Firepower 地理位置情報データベースの更新をダウンロードします （Download Latest Cisco Firepower Geolocation Database Update）」で「更新ファイルが破損しています（Update file is corrupted）」と表示される
CSCwi48699	ASA がスレッド名 pix_flash_config_thread でトレースバックし、リロードする

不具合 ID	タイトル
CSCwi49770	スレッド名 Datapath での ASA/FTD のトレースバックとリロード
CSCwi49797	オブジェクトとネットワークを使用したイベント検索では、オブジェクトに一致するイベントのみが表示される
CSCwi49829	Threat Defense サービスポリシー：[タイムアウト時に接続をリセット（Reset Connection Upon Timeout）] が機能しない
CSCwi49884	VTI またはループバック インターフェイスが作成されると、TCP MSS がデフォルト値に戻される
CSCwi50343	FPR-4112 で 7.2.2 を実行するスタンドアロン FTD において、SNMP モジュールでトレースバックが発生する
CSCwi51611	FTD 7.4.1 Snort は、低いトラフィック レートでも 100% の使用率を示す
CSCwi51941	アップグレードパッケージがすでにデバイスにコピーされている場合、741 から 76 への無人モード FTD アップグレードが失敗する
CSCwi52008	競合状態での Snort3 のトレースバックと再起動
CSCwi53150	access-list がすでに参照されている場合に、サービスの object-group protocol タイプの不一致エラーが表示される
CSCwi53431	100 を超える environment-data とデータユニットを同期できない
CSCwi53949	TcpReassembler::scan_data_post_ack での Snort3 のトレースバック
CSCwi53987	SSL プロトコル設定で FDM GUI 証明書の設定が変更されたり、TLSv1.1 が無効になったりしない
CSCwi54171	ポリシーを変更/作成したユーザーが削除された場合、復号ポリシーページは空になる
CSCwi55009	セキュリティ分析ユーザーが [パケットキャプチャ（Packet Capture）] ページにアクセスしようとすると、エラーがスローされる
CSCwi55629	ASA/FTD：アップグレード後も Firepower 1010 デバイスでポートチャネルがダウンしたままになる
CSCwi55842	7.4：ポリシーの保存が進行中の場合、展開は一部のデバイスでのみエラーを示す可能性がある
CSCwi56667	フェールオーバーグループの変更後に、スタンバイのスレッド名「fover_parse」で ASA のトレースバックとリロードが発生する
CSCwi56733	FMC で PBR を設定しようとすると内部エラーが発生する

不具合 ID	タイトル
CSCwi57476	FXOS logrotate ユーティリティへのインターフェイス idb ロギングログローテーション
CSCwi57670	RAVPN SAML：FTD/ASA がアサーションの解析に失敗すると、外部ブラウザで誤解を招くメッセージが表示される
CSCwi58187	NAT 警告のしきい値の上限（131838 IP）が正しくない
CSCwi58754	「ファイアウォールプリプロセッサによってブロックされた」という理由で SMB トラフィックがブロックされる
CSCwi59453	アップグレード後にブートストラップが失敗する：HA の再開時に展開がすでに存在するという理由が表示される
CSCwi59831	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
CSCwi59871	eventdb での大きなログ先行書き込みによってディスク使用率が高くなる
CSCwi59969	ZTNA：FMC が誤った sp-acs-url パラメータをプッシュする："?" が 0x3F としてエンコードされる
CSCwi60151	ZTNA：FMC がローカルドメインを持つ IdP を受け入れない
CSCwi60285	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
CSCwi61135	SSH セッションでデバッグを有効にできない
CSCwi62796	SSL/DTLS のトラフィックの処理に関連する ASA/FTD のトレースバックとリロード
CSCwi62985	ビジー状態の FMC で SFDataCorrelator のタイムアウトスレッドのデッドロック検出でコアダンプが生成される
CSCwi63057	Threat Defense アップグレードウィザードで、クラスタ/HA が無効として誤って表示される場合がある
CSCwi63113	トレースバックとリロードにつながる SNMP での Null ポインタの逆参照
CSCwi63743	ASA/FTD がスレッド名「appAgent_monitor_nd_thread」と RIP: _lina_assert でトレースバックし、リロードすることがある。
CSCwi64772	UMS で Geodb のインストール通知がスタック状態であるか、一部のタスクで通知が作成されない
CSCwi64829	機能 HA に関するトレースバックとリロード
CSCwi65116	DHCPv6：スレッド名 DHCPv6 CLIENT での ASA のトレースバック。

不具合 ID	タイトル
CSCwi65428	IAB 設定のフロー速度メトリックが正しくない。
CSCwi66461	Victoria CE でポートチャネルを作成しているときに（速度に互換性がなく一時停止したという）警告メッセージが表示される
CSCwi66570	[変数セット（Variable Sets）] の名前を変更した後に「デフォルト変数（Default Variables）」情報がレポートに含まれない
CSCwi66676	ASA/FTD がスレッド名「webvpn_task」でトレースバックおよびリロードすることがある
CSCwi67291	FMC 7.6 へのアップグレード後に FMC でイベント（接続/マルウェア/その他）を表示できない
CSCwi67510	FMC：VLAN インターフェイスでパケットトレーサに「インターフェイスはサポートされていません（Interface not supported）」エラーが表示される
CSCwi67629	準備状況チェックが開始されると、デバイスのステータスが「アップグレードパッケージが存在しません（missing the upgrade package）」に変更される場合がある
CSCwi67638	Azure IDP SAML 属性を含む FMC の設定済み DAP ルールが一致しない
CSCwi67998	同じインスタンスの再展開後に、TPK MI シャーシでポリシーの展開に失敗する
CSCwi68320	prometheus ディレクトリが欠落しているために、FMC ハードウェア移行中にエラーが発生する
CSCwi68604	eddsa が kex hostkey として使用されている場合に ASA への ssh アクセスでエラーログが生成される
CSCwi68625	IP を設定する前に SNMP ホストを設定すると、snmpd が繰り返し再起動する
CSCwi68833	ASA/FTD：フェールオーバーに起因するメモリリークにより、同期されていない Cisco Umbrella のフローが原因で dnscrypt キーキャッシュが解放されない
CSCwi68970	下線 "_" を含む DAP ポリシーを作成すると、リモートアクセス VPN ポリシーに適用済みとして表示されない
CSCwi69091	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
CSCwi69260	FMC の 7.2.x へのアップグレードでは、FTD のインターフェイスから FlexConfig 提供の EIGRP 認証が削除される

不具合 ID	タイトル
CSCwi70371	VTI がループバックから送信される場合の断続的なパケット損失
CSCwi70492	ファイアウォールが疑似スタンバイモードで App Sync エラー状態になり、アクティブユニットからの IP を使用する
CSCwi70940	FMC バックアップの復元時に restore.log に標準エラー（stderr）が挿入されない
CSCwi71786	使用可能なアップグレードパッケージのダウンロードに失敗する
CSCwi71998	SSL ポリシーの decrypt all が使用されている場合、「Stream: TCP normalization error in NO_TIMESTAMP」が表示される
CSCwi72054	7.2.x のアップグレード後にカスタム DNS サーバー グループ オブジェクトを削除できない
CSCwi72158	HA ペアのデバイスは、[Threat Defenseのアップグレード（Threat Defense Upgrade）] ページでスタンドアロンとして表示される
CSCwi72294	FTD：LSP パッケージ検証ロジックを改善または最適化し、実行速度を向上させる
CSCwi74214	アクティブ HA からスタンバイ HA に移行するときに、ASA/FTD がスレッド名 IKEv2 Daemon でトレースバックし、リロードする
CSCwi75111	CLI を介した MTU 値の設定が適用されない
CSCwi75198	スタンバイ FTD で定期的にトレースバックとリロードが発生する
CSCwi76002	tmatch のための解放メカニズムがないことによるメモリの枯渇
CSCwi76361	トランスペアレント ファイアウォール MAC フィルタで STP-UplinkFast dst MAC のフレームが一貫してキャプチャされない
CSCwi76630	FP2100/FP1000：リロード後に Cisco ASA スマートライセンスが失われる
CSCwi77415	設定の問題に起因して、ASAv デバイスで ASDM の接続が失われるという問題が確認される
CSCwi78064	CloudAgent スマートエージェント例外：スマート エージェント マネージャでは、NTP が FDM で実行されている必要がある
CSCwi78941	FDM 展開が「一部のインターフェイスがデバイスに追加されたか、デバイスから削除されました（Some interfaces have been added to or removed from the device）」というエラーで失敗する
CSCwi79037	IKEv2 クライアントサービスが有効にならず、XML プロファイルがダウンロードされない

不具合 ID	タイトル
CSCwi79042	NAT ポリシーを追加した後、データパスで FTD/Lina が HA ペアのトレースバックとリロードを実行する
CSCwi79120	一部の SSH セッションがタイムアウトしないため、SSH とコンソールが FXOS CLI に接続できない
CSCwi79289	FMC：PM 機能へのロギングの追加
CSCwi79393	セキュリティインテリジェンスから Cisco Umbrella DNS ポリシーを削除すると、ポリシーの展開が失敗する
CSCwi79538	ネットワークオブジェクトのオーバーライドに対する FMC API コールが、アクティブ FW とスタンバイ FW で異なる結果を返す
CSCwi79703	FXOS 経由で設定された場合、FTD 上のタイムゾーン形式が正しくない
CSCwi80453	ピアアプリケーション同期または設定同期中のアクティブノードのリロードにより、早期フェールオーバー、設定同期の失敗、および予期しないリブートが発生する
CSCwi80979	Snort がパケット情報を削除し、そのパケットに 0 バイトのデータを挿入する
CSCwi81771	メモリキャッシュの問題が原因で、不明なファイルの判定を ThreatGrid に送信できない
CSCwi81772	同じ FMC バージョンで AC ポリシーをエクスポートおよびインポートできない（Snort2 または Snort3 IPS 破損関連のバグ。古いエントリが存在する）
CSCwi82866	WAL サイズに基づいて MonetDB を再起動する MonetDB モニタートリガーが有効に機能しない
CSCwi83890	AC ポリシー用に生成されたレポートファイルが空になる
CSCwi84314	複数の SSH で「show run」を実行すると ASA CLI がハングする
CSCwi84417	トラフィックが期限切れ後に時間範囲オブジェクトを含む ALLOW ルールと誤って一致する
CSCwi85277	「デバイスに展開されていない変更が存在するため、アップグレードに失敗しました（Upgrade failed because of undeployed changes present on the device）」というエラーで、アップグレードが失敗する
CSCwi85628	Rsync チャンクチェックサムの遅延による展開の失敗
CSCwi85689	TLS サーバー識別：「show asp table socket」の出力に複数の TLS_TRK エントリが表示される

不具合 ID	タイトル
CSCwi86036	Radius キーに特殊文字が含まれていると、アップグレード後に外部 Radius 認証が失敗する
CSCwi86187	[VPNモニタリング（VPN Monitoring）] ページで VTI トンネルの誤ったポートチャネル関連付け情報が表示される
CSCwi86198	IDS 用に設定された FTD で SFDataCorrelator が繰り返し終了する
CSCwi87382	SSH セッションでデバッグを実行しているときに、プライマリユニットでトレースバックとリロードが発生する
CSCwi89167	同時署名検証が原因で VDB/SRU の自動ダウンロードが失敗する
CSCwi89447	レルム同期のたびにアクセス コントロール ポリシーの変更が示される
CSCwi90399	FTD/ASA システムクロックが 2023 年にリセットされる
CSCwi90571	クライアントレス SSL VPN 経由での Web サイトへのアクセスが失敗する
CSCwi90751	FTD/ASA：snmpwalk を使用した SNMP クエリですべての「nameif」インターフェイスが表示されない
CSCwi90998	環境 FXOS DME MIB（.1.3.6.1.4.1.9.9.826.2）の ASA SNMP ポーリングが失敗する
CSCwi91166	ストリームでブロックの理由を追加する必要がある
CSCwi91384	ドメインをまたがる ASA から FMC への S2S の移行
CSCwi91588	Snort シャットダウン時のディスカバリフィルタでのヒープ解放後使用
CSCwi91602	LSP インストール後、デプロイメントは通知でタイムアウトせず（ただし、開始されていない）、数時間実行中になる
CSCwi92702	アップグレード後、[FMCヘルスモニタリング（FMC Health Monitoring）] ページの [すべて実行（Run All）] 機能がグレー表示される
CSCwi94356	スレッド名 cli_xml_request_process での Lina のトレースバックとリロード
CSCwi95228	リブート後に「crypto ikev2 limit queue sa_init」がリセットされる
CSCwi95708	FTD：syslog メッセージにホスト名がない
CSCwi95796	FTD SNMP OID 1.3.6.1.4.1.9.9.109.1.1.1.1.7 で SysProc Average に対して常に 0% が返される
CSCwi95871	ソフトウェアのアップグレード後に非管理コンテキストへの SSH/SNMP 接続が失敗する

不具合 ID	タイトル
CSCwi95994	ファイアウォールで FIPS CC が有効になっていると、Chromium ベースのブラウザで SSL 接続の競合が発生する。
CSCwi97836	nlp_int_tap でキャプチャを設定してコンテキストを削除した後の ASA のトレースバックとリロード
CSCwi97839	vni_idb_get_mode での FTD のトレースバックアサートとリロード
CSCwi97948	アップグレード後、または "shutdown"/"no shutdown" コマンドの後に、EIGRP 帯域幅が変更される
CSCwi98147	証明書の更新により、LTP フローの途中で Tomcat が再起動する
CSCwi99429	ポリシー展開の失敗のロールバックにより、FTD デバイスが再設定されない
CSCwj00659	FMC：電子メールアラートで複数の電子メールアドレスが機能しない
CSCwj00956	Snort プロセスが大量の syslog-ng メッセージを送信し、syslog-ng が停止する
CSCwj01197	FMCv300 のブートアップで VMXNET3 ドライバが自動的にロードされない
CSCwj01346	展開ごとにロギングリスト MANAGER_VPN_EVENT_LIST が削除され、再適用される
CSCwj01418	ユーザーが送信元ネットワークを変更した場合のポート値が、パッチ API 応答に含まれない
CSCwj01569	インターフェイスエラーが原因で、スタンドアロン FDM でポリシー展開が失敗する
CSCwj02259	バックアップ失敗は、GUI に正しい状態で表示される必要がある
CSCwj02505	同じ engineID を 2 回入力したときの ASA Checkheaps のトレースバック
CSCwj02708	FDM でのバックアップ生成が、「レガシーデータをバックアップできません（Unable to backup Legacy data）」というエラーで失敗する
CSCwj03112	monetdb の pmtool による再起動で、monetdb の Volume ディレクトリ内のファイルが多すぎるため、monetdb の起動に失敗する
CSCwj03253	MonetDB テーブルパーティションの作成が失敗すると、SFDataCorrelator により膨大な数の to_import ファイルが作成される
CSCwj03285	FMC：ディスク使用量に関するヘルスモニターアラートが適切に発行されていない

不具合 ID	タイトル
CSCwj03764	ISP2 がダウンしている場合のスポークデュアル ISP における ISP1 フラッピングに関連する VTI トンネル。
CSCwj03876	Snort 3 IPS ルールを削除しても監査ログが生成されない
CSCwj03937	ENH：FTDに「ユーザーアイデンティティ証明書に CRL が見つかりません（No CRL found in User identity Certificate）」を示すデバッグメッセージを追加
CSCwj04154	FTD 管理インターフェイス DHCP サーバーが起動に失敗し、接続に問題が発生したり、障害が表示されたりすることがある
CSCwj05151	GTP スピンロックアサーションに起因して、ASA/FTD がスレッド名 DATAPATH でトレースバックし、リロードすることがある
CSCwj05464	FMC サーバー証明書に最初の 20 個のオブジェクトのみが表示される
CSCwj05484	ASA の 9.16 から 9.18 へのアップグレードにより、余分なスラッシュ「\」が追加されて AAA ldap 属性値が変更される
CSCwj07837	ロギングイベントリスト名のサイズ超過による展開の失敗
CSCwj08015	FTW が Warwick 上の NM3 で動作しなくなった
CSCwj08203	FMC：FireAMP が生成するログが多すぎる
CSCwj08302	FTD：HostScan のスキャン結果がバージョン 7.4.1 で処理されない
CSCwj08980	ノードから開始されたときに ICMP 応答が送信者ノードにランダムに到達しない。
CSCwj09373	BBManager テキストベース検索：lucene
CSCwj09938	一度追加した抑制設定を Snort3 ルールから削除できない
CSCwj09999	管理インターフェイスで FP 3100 MTU を変更し、リブートすると変更が維持されない（デフォルトの MTU に戻る）
CSCwj10451	プライマリデバイスのリブート中にセカンダリデバイスがリロードされる。
CSCwj11331	Web コンテンツファイルが application/octet-stream である必要があるときにテキスト/プレーンとして表示される
CSCwj12168	期限切れなしのマシンユーザーがさまざまな場所でログアウトされない
CSCwj13910	IPSEC オフロードが有効になっているときに Crypto IPSEC SA の出力に SA エラーが表示されない

不具合 ID	タイトル
CSCwj14242	アプリケーションが TOR として誤って識別され、Snort3 によってブロックされる
CSCwj14589	FTD で空の connector.toml ファイルが原因で、FMC-SSE クラウド設定の SSE 登録失敗アラートが発生する
CSCwj14798	TSS_Daemon プロセスが毎分終了する
CSCwj14832	SAML：認証が成功した後、シングルサインオン AnyConnect トークンの検証エラーが表示される
CSCwj15125	ASA/FTD が Netflow タイマーインフラに関連するスレッド名「lina」でトレースバックし、リロードすることがある
CSCwj16279	「@」文字を含むユーザー名が、asa ログインでは機能するものの「connect fxos」では失敗する
CSCwj16521	FMC UI でポリシーが読み込み状態でスタックする
CSCwj17447	ASA/FTD がスレッド名「DATAPATH-6-26174」でトレースバックし、リロードすることがある
CSCwj17677	PM の再起動をブロックするか、リブートになる可能性をユーザーに警告する必要がある
CSCwj17852	FMC：[継承設定（Inheritance Settings）] の [基本ポリシーの選択（Select Base Policy）]メニューが、Light または Dusk UI を使用してスクロール中に非表示になる
CSCwj19252	次の展開が 2 時間後の場合、FMC でオブジェクトの最適化が無効になる
CSCwj19653	FTD：fqdn オブジェクトを含む NAT に起因するトレースバックとリロード
CSCwj20067	ASA：スタティック インターフェイス NAT が設定されていると警告メッセージが表示されない
CSCwj20118	EIGRP 設定のプッシュ後に FTDv がリロードし、バックトレースが生成される
CSCwj21880	インターフェイスオブジェクトの最適化が有効になっている FTD が、ゾーン名を変更した後にトラフィックをブロックする
CSCwj21985	デバッグ：Eth1/1 が予期せずフラップする
CSCwj22086	ファイアウォールモードで不一致が起きると、アクティブユニットが無効状態になる

不具合 ID	タイトル
CSCwj22235	mps_hash_memory が null ハッシュテーブルを指しているために Lina のトレースバックとリロードが発生する
CSCwj22990	ASA をアップグレードすると、「Slot 1: ATA Compact Flash memory」に異なる値が表示される
CSCwj24517	LSP 展開がマルチインスタンス FP 41xx/93xx で失敗する
CSCwj25629	FPR9K で「show tech-support module detail」を実行するとエラーが発生する
CSCwj25975	FTD/ASA：「会社名（Company Name）」属性間にコンマを使用した CSR の生成が期待どおりに機能しない
CSCwj26204	復元された FMC バックアップデバイスは、FMC と接続していないにもかかわらず、「通常（normal）」および「正常（healthy）」と表示される
CSCwj26595	FMC では、外部認証オブジェクトにバイナリ証明書をロードできる
CSCwj26627	スナップショット障害が原因でポリシー展開エラーが発生した場合、FMC にユーザーフレンドリでないエラーが表示される
CSCwj27112	REST API '/devices/devicerecords' が（RA VPN）ポリシーオブジェクト ID と一致しない値を返す
CSCwj28049	[アイデンティティマッピングフィルタ（Identity Mapping Filter）] フィールドが、新しく作成されたネットワークオブジェクトで更新される
CSCwj28437	Snort3：大量の無効なシーケンス番号と無効な ACK により、アップグレード後に TCP トラフィック障害が発生する
CSCwj29599	ファームウェアのアップグレードが原因で、追加のリブートにより FDM のブートストラップが中断される可能性がある
CSCwj30825	アクティブデバイスの登録解除後の SFDataCorrelator のメモリリーク
CSCwj30962	3140 3 MI インスタンスのアップグレードが失敗する
CSCwj30980	CTS SXP フローの ID の使用状況をキャプチャすることを目的としたデバッグと show コマンドの追加。
CSCwj31382	FMC の監査ログに誤った IP アドレスが記録される
CSCwj31816	RSA-PSS 署名アルゴリズムが原因で、FTD で TLS Secure Client セッションを確立できない

不具合 ID	タイトル
CSCwj31904	アップグレード後、FDM の展開が失敗する：「Snort 検出エンジンによるトラフィック処理の待機中にタイムアウトしました（Timeout waiting for snort detection engines to process traffic）」
CSCwj31918	HA 同期中に "logger_msg_dispatch" でセグメンテーション違反が発生する
CSCwj32035	クライアントレス VPN ユーザーが HTTP Basic 認証でページに到達できない
CSCwj32736	ngfw 管理インターフェイスで SNMP を設定した後に IP を設定すると、SNMP ウォークが機能しない。
CSCwj32823	FMC のアップグレード後、変更がなくても FMC から "strong-encryption-disable" がプッシュされる
CSCwj33487	DTLS トラフィックの処理中に ASA/FTD がトレースバックし、リロードすることがある
CSCwj33580	複数の暗号/プロポーザルによるフラグメンテーションとスロットリングが原因で IKEv2 トンネルがフラップする
CSCwj33891	ポートブロック割り当てのリリース中に NAT プロセスが原因で ASA/FTD クラスタのメモリが枯渇する
CSCwj34204	コアファイルのディスククォータはプラットフォームに基づいた見直しが必要
CSCwj34235	FTD のステートフル署名評価 で Snort3 のコアダンプが発生する
CSCwj34374	FMC がプロキシサーバーの背後にある場合、SecureX/Cisco Security Cloud の登録が失敗する
CSCwj34881	送信元 IP アドレスでフィルタ処理された access-policy のカウンタを表示するコマンドの結果が正しくない
CSCwj34975	複数のコンテキスト インターフェイスがトラフィックを渡せない
CSCwj35701	Dns ガードがタイミング条件により接続を早期に終了する
CSCwj35902	URL フィルタリングおよび Cisco-Intelligence-Feed ダウンロードの失敗
CSCwj38871	スレッド名 SSH での ASA のトレースバック
CSCwj38928	FPR31xx で高遅延が確認される
CSCwj39107	膨大な数の古いサービスアイデンティティをプルーニングすると、SFDataCorrelator のメモリ使用量が増加する
CSCwj39184	FDM：7.3.1 で /ngfw/var/sf/fwcfg/zones.conf が空になっている

不具合 ID	タイトル
CSCwj39212	膨大な数の期限切れのユーザーアイデンティティを処理すると、SFDataCorrelator のメモリ使用量が増加する
CSCwj39296	新しく登録された FTD について、FTD コンプライアンスモードが FMC に正確に表示されない
CSCwj40124	PBR 設定の OOM が原因で FMC 7.3 展開が失敗する
CSCwj40597	FTD：マルチインスタンスまたはスタンドアロンでバックアップが失敗し、「バックアップが予期せず終了しました（Backup died unexpectedly）」というエラーが発生する
CSCwj40665	SFDataCorrelator での追加メモリトラッキング
CSCwj40761	ASA/FTD がスレッド名 **CTM KC FPGA stats handler** でトレースバックすることがある
CSCwj41427	FMC でオーバーライドの保存に時間がかかるため、FTD-HA の作成が失敗する
CSCwj41916	FTD-HA アップグレードの開始に失敗：アクティブとスタンバイの間で設定が同期していない
CSCwj43069	FMC で手動アドレスエントリとして ::/0 を指定した IPv6 ルールが期待どおりに機能しない。
CSCwj43345	一部の OID の SNMP ポーリングによって CPU が占有され、ICMP パケットで高遅延が確認される可能性がある
CSCwj43902	FTDv：AWS GW に接続されているインターフェイスで DHCP の接続の問題が発生しているか、そのインターフェイスがアイドル状態になっている可能性がある。
CSCwj44398	FTD のルート RIP で route-map を設定すると、FTD のリロード後にルートの更新が機能しない
CSCwj45351	アップグレードされた FMC に LDAP 属性マップを追加できない
CSCwj45439	内部証明書のインポートエラー：「証明書ベース EO の検証に失敗：サポートされていないキータイプ（Failed to validate Cert Based EO：Unsupported Key Type）」
CSCwj48308	モデルの移行後 UMS に古い正常性アラートが表示される
CSCwj48704	ASDM からファイルシステムにアクセスするときの ASA のトレースバックとリロード
CSCwj48801	FPR42xx で高遅延が確認される

不具合 ID	タイトル
CSCwj49958	「ハッシュ値の計算に失敗しました（Failed to compute a hash value）」というエラーで Crypto IPSEC ネゴシエーションが失敗する
CSCwj50024	インドおよびオーストラリア向けの新しい Cloud SSX リージョンのサポートを追加
CSCwj50064	SSE 接続イベントで、FirewallRuleList フィールドが適切な形式で送信されない
CSCwj50406	デバイスフラッピングで設定されたすべての IPV6 BGP ルート
CSCwj50557	頻繁にポリシーが展開されると、Snort が snort-unified ログファイルを過剰に作成する
CSCwj51115	7.x バージョンにアップグレードした後に、FMC バックアップの Solar Winds リモートサーバーへのコピーが失敗する
CSCwj52326	ホールド時間に関連する BGP 設定が正常に展開されない
CSCwj53324	オブジェクトルックアップで、オブジェクト管理下で参照されたポリシーが自動的に表示されない
CSCwj53725	ASA スタンバイで 'no failover' および 'failover' を適用中にトレースバックが確認された
CSCwj54042	インターフェイス/サブインターフェイス設定の変更で、暗号化 IKEv2 ポリシーシーケンスの順序が変更される
CSCwj54644	FMC は、48 文字を超えるパスフレーズを使用して PKCS12 証明書をアップロードできない
CSCwj54717	外部認証の 14 文字を超える Radius 秘密鍵が展開されない（FPR3100）
CSCwj55036	ASA/FTD：async crypto コマンドでの遅延により、トレースバックとその後のリロードが発生する。
CSCwj55081	FPR3K のリブート時に FPR3K の管理データインターフェイスを介した FMC への接続が失われる
CSCwj56099	ASA：failsafe-exit コマンドを実行するとインターフェイスが DISABLED 状態になる
CSCwj56595	UI から開始した後に準備状況/アップグレードのプロセス作成が遅延する
CSCwj56639	FDM1010E 7.4.1 を SA に登録できず、「権限付与タグが無効です（Invalid entitlement tag）」メッセージが表示される

不具合 ID	タイトル
CSCwj56662	他の言語では、FMC HA ウィザードで「高可用性ステータスを取得できません（Unable to retrieve high availability status）」というエラーが表示される
CSCwj56668	FMC で ISE 一括ダウンロードのアラートエラーが誤検出される
CSCwj57435	古い logrotate ファイルをクリーンアップ
CSCwj58431	FMC REST API が 'deploymentStatus' 属性を送信しない
CSCwj58442	オンプレミス FMC の FTD HA ステータスが破損しており、セカンダリがプライマリとレポートされる
CSCwj59861	SCP/SSH プロセスに起因して、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
CSCwj59981	FMC は RADIUS サーバーに接続するときに最大 30 文字の共有秘密鍵のみを受け入れる
CSCwj60265	ASA/FTD がスレッド名「DATAPATH-1-16803」でトレースバックし、リロードすることがある
CSCwj61086	クラスターの中断またはインラインセットの削除後の展開中に svc_sam_dme プロセスで CPU 使用率が高くなる
CSCwj61885	アップグレードイメージを検証する際のファイル記述子のリーク
CSCwj62056	cEdge URLF 機能が URL をカテゴリでブロックしない
CSCwj62723	SSH 設定の有効化中に Firepower 2100 デバイスのコンソールにエラーメッセージが大量に表示される
CSCwj62959	フェールオーバー MAC アドレスを持つサブインターフェイスの親を変更すると、展開が失敗してロールバックする
CSCwj62984	Snort3：stream_tcp の重複処理によって MSSQL クエリトラフィックが破損し、SQL HY000 が発生する
CSCwj63048	展開中の内部エラー：Lina タイムアウトが原因で FDM で {0} が確認される
CSCwj63975	正常性モジュールを無効にしても、その正常性モジュールの UMS メッセージは削除されない
CSCwj65587	Snmpwalk がエラーメッセージ #"snmp/error: truncating integer value > 32 bits" をスローする

不具合 ID	タイトル
CSCwj65811	TLS サーバーアイデンティティ検出がオンになっている場合、FMC が「ポリシーの SSL ルール ID が見つかりません（Unable to find SSL rule id for policy）」でフラッディングする
CSCwj66285	Radius 外部認証オブジェクトのタイムアウトは、FTD では 5 秒に設定されているが、FMC では 30 秒に設定されている
CSCwj66339	OGO がカスタム オブジェクト グループのコンテンツの順序を変更し、静的 NAT で障害を発生させる
CSCwj66537	PDF トークナイザーを制限なく処理するため、Snort3 がクラッシュする
CSCwj67600	1010 v7.2.5 をオンボーディングすると、cdFMC v20240307 で自動展開が失敗する
CSCwj67707	ECDSA 証明書が FMC ISE 統合でサポートされていない
CSCwj67787	VPN の送受信バイト数が大きいため、新しいユーザーアクティビティページがロードされない
CSCwj68096	9.18.3.56 にアップグレードすると、CSP でホストされている ASAv のコンソールアクセスがスタックする
CSCwj68277	LDAP 設定の証明書チェックの制限が厳しすぎる
CSCwj68286	名前にピリオドが含まれているトポロジ名を検索すると、FMC GUI でエラーが発生する
CSCwj68604	ユーザーロールの説明が長すぎると、アップグレード後に Tomcat および VmsBackendServer が停止する
CSCwj68783	コマンド同期プロセスが特殊文字を含む設定を送信しているため、FTD/ASA-HA 設定が同期しない
CSCwj69145	FTD："show asp inspect-dp snort" の出力で CPU 使用率が高いことが示される
CSCwj69632	4110 の Firepower Chassis Manager 証明書のデフォルトのハッシュアルゴリズムは SHA1
CSCwj69780	SNMP ホストグループのコンテンツの変更により、管理インターフェイスで SNMP プロセスが終了する
CSCwj71064	ファイアウォールプリプロセッサによってブロックまたはブラックリストに登録されたという理由で Snort が接続をドロップする
CSCwj71443	FMC での「FDM キーリングの証明書が無効です。理由：期限切れ（FDM Keyring's certificate is invalid, reason: expired）」正常性アラート

不具合 ID	タイトル
CSCwj72013	デバイスがクラスタに参加すると、PAT プールを使用した PAT 通信が約 40 秒間失敗する
CSCwj72022	特定のプラットフォーム設定を適用すると、アップグレード後にデプロイメント時間が 30 ～ 45 秒増加する
CSCwj72369	同期コールがスタック状態になり、ブートループが発生する
CSCwj72560	選択したデバイスにデバイステンプレートが適用されている場合、パケットトレーサページに「登録が完了するまでお待ちください（Wait for registration to complete）」というエラーが表示される
CSCwj72615	サイト間モニタリングで VPN ステータスが更新されない
CSCwj72721	route-map match 句で BGP コミュニティが追加または削除されると、展開が失敗してロールバックされる
CSCwj73053	ASA がスレッド名「DATAPATH-21-16432」でトレースバックし、リロードすることがある
CSCwj73061	CPUTotal1min の SNMP OID がポーリング時に snort cpu コアのエントリを除外する
CSCwj73171	Snort3：小さなサイズのパケットが最大セグメント制限を超え、Snort ブロックが発生する
CSCwj74323	VPN の PKI/Crypto を含む ASAv のメモリリーク
CSCwj74716	tpk_mi の 7.4.1.1 から 7.6.0 000_start/000_00_run_cli_kick_start.sh へのアップグレードが失敗する。
CSCwj77061	SHOW_XML_REQUEST のタイムアウトにより、FTD HA ノードでのポリシー展開に失敗する
CSCwj77504	ハードウェア FMC モデルを FMC2600 から FMC4700 に移行した後のユーザーグループマップの欠落
CSCwj77700	idfw_proc スレッドでの FTD LINA のトレースバックとリロード
CSCwj77877	MI インスタンスを無効化/有効化すると「状態が失敗（State Failed）」になる
CSCwj79736	FMC が CDO 管理対象 FTD からイベントを受信すると、eStreamer メモリリークが発生する
CSCwj79895	ENH ログ FP4110（FXOS 2.10.1.179）デバイスの再起動後にセキュリティモジュールが応答しなくなる

不具合 ID	タイトル
CSCwj81031	ASA/FTD に snmpd コアが存在する
CSCwj81115	RNAStop および monetdb 出力キューがいっぱいになった後の再設定での SFDataCorrelator のデッドロック
CSCwj81743	FTD：fqdn オブジェクトを含む NAT に起因するトレースバックとリロード
CSCwj82285	ASA/FTD がスレッド名「sdi_work」でトレースバックし、リロードすることがある
CSCwj82736	セグメント化またはフラグメント化されたクライアント Hello パケットを順不同で受信した場合、TLS ハンドシェイクが失敗する
CSCwj82903	FDM HA の展開が「ApplicationException：データベースにエクスポートできません（ApplicationException：Unable to export to database）」エラーで失敗する
CSCwj83185	FTD/ASA：メモリトラッキングを有効にした後のスタンバイ FTD のトレースバックとリロード
CSCwj83533	ファンは想定どおりに動作しているものの、ファン LED がオフ状態になっている。
CSCwj83634	「reg_fover_nlp_sessions: failover ioctl C_FOREG failed」というメッセージが表示される
CSCwj84168	SFDataCorrelator で、期限切れのサービスとクライアント アプリケーションを繰り返し消去するログスパムが発生する
CSCwj85106	FMC をアップグレードすると、FTDv のパフォーマンス階層が失われる
CSCwj85232	アップグレードを元に戻した後に FTD が FTD-HA に参加できない
CSCwj85333	Web ブラウザでハイブリッド化された kyber 暗号が有効になっている場合、FPR は TLS1.3 接続をドロップすることがある
CSCwj86116	NetFlow の設定が原因で LINA CPU の使用率が高くなる
CSCwj86320	誤った「Hello」メッセージ MAC により、スタンバイユニットのインターフェイスが FTD のアップグレード後に「待機」ステータスになる
CSCwj87257	無効な正常性アラートメッセージ：FTD 上のクラシックライセンス期限切れモニターによる「スタック上のライセンスの不一致（License mismatch on stack）」
CSCwj87373	ログ間隔属性が設定されていない場合の FMC REST API 内部サーバーエラー

不具合 ID	タイトル
CSCwj87501	ASA/FTD がスレッド名「fover_FSM_thread」でトレースバックし、リロードすることがある
CSCwj87770	FPR2100-ASA が SAN フィールドで FXOS IP アドレスなしで CSR を生成できない
CSCwj88400	FTD が appAgent メッセージの応答の処理中にプロセス名 lina でトレースバックし、リロードすることがある
CSCwj88562	[7.6.0] RADIUS 認証がカスタム秘密鍵で機能しない
CSCwj88765	言語が変更されると、FMC ヘルスモニタリングで不完全なメッセージが送信される
CSCwj88843	EoRevisionStore テーブルのエントリが大きいため、HA 同期で mysqldump プロセスに失敗する
CSCwj89033	syslog UI で次のページに移動中に内部エラー画面が表示される
CSCwj89228	Snort のメモリマップファイルが原因で FTD/mnt ディスク使用率が 100% になる
CSCwj89264	FTD HA：netsnmp_oid_compare_ll でのトレースバックとリロード
CSCwj90826	Chrome v124 以降で、既知のキーを使用した Snort2 SSL 復号が失敗する
CSCwj91341	フェールセーフモードのデフォルト値は、一部のプラットフォームでは実現できないため、プラットフォーム/モードごとに調整が必要
CSCwj91420	flow-ip-profiling の収集中に Snort3 がクラッシュする
CSCwj92784	RAVPN：ID テーブルの枯渇により SGT-IP マッピングの作成に失敗する
CSCwj92973	CdFMC：インポート中に RAVPN を使用したデバイス移行が失敗する
CSCwj93300	FMC：クラシックテーマのレガシー UI でのルール変更に関するコメントの要求が機能しない
CSCwj93718	FXOS で「nslookup」コマンドを実行できない
CSCwj93860	LINA クラッシュ後の FDM HA での CD アプリケーション同期エラー
CSCwj95322	ファイルの統計チェックを無効化
CSCwj95590	ユーザーが WebVPN のブックマークをクリックすると、ブラウザがログオンページにリダイレクトする
CSCwj96572	ASA でロギングクラスを無効にした後も syslog が送信される

不具合 ID	タイトル
CSCwj97444	cdFMC：AC ルールがポリシープレビューで削除済みと表示される
CSCwj97492	7.2.4 から 7.2.5 にパッチ適用した後、アクセスルール名にルール名ではなく「無効な ID（invalid ID）」と表示される
CSCwj98451	アップグレード後に FMC がスマートライセンスから登録解除される
CSCwj98573	アイデンティティポリシーを変更しようとしたときに、不明なエラー[9999]が発生する
CSCwj98580	侵入イベントと相関イベント間の分類の不一致
CSCwj98648	署名キーを読み取れない（マルチインスタンス展開）
CSCwj98673	シャーシのリブートで無効化されたコンテナを起動できず、Heimdall にアクティビティを記録できない
CSCwj99362	Firepower で「show inventory」の出力に Name: "power supply 0" と表示される
CSCwj99941	M6 ハードウェアモデルでは、わずか 1 週間前のヘルスモニタリングデータもほとんど保存されない
CSCwk00401	CdFMC：登録フェーズでの FTD 移行の失敗
CSCwk00604	ASA が IKEv2-EAP と Windows ネイティブ VPN クライアントとの AAA 認証を開始できない
CSCwk00628	FMC 7.4.x および FTD バージョン 7.4 未満の Snort 2 で、キャプティブポータルが不正なリクエストを返す
CSCwk02213	OSPF/EIGRP ネットワークと SVI ネットワークの重複に関する検証が不完全または無効
CSCwk02332	Snort2：SSL 復号に失敗し、一部の Web サイトが Chrome v124 以降でロードされない
CSCwk02804	WebVPN 接続が CLOSEWAIT 状態でスタックする
CSCwk02928	ASA/FTD がスレッド名 PTHREAD でトレースバックし、リロードすることがある
CSCwk04216	レルムのダウンロードタスクが失敗し、ADI プロセスが現在利用できないというメッセージが表示される
CSCwk04246	ユーザー/グループをダウンロードできず、ADI からの応答を取得できない
CSCwk04290	FPR 21xx：通常の動作中にプロセス名 lina-mps でトレースバックする

不具合 ID	タイトル
CSCwk04492	複数の ssh セッションで「show run」を実行すると ASA CLI がハングする
CSCwk04754	フィルタ処理された ACP ルールを一括アクションで無効にしても、グレー表示されない
CSCwk04893	FTD は、SGT/IP マッピングの更新を伝達するために使用されるファイルを圧縮しない
CSCwk04908	FTD：DNS サーバーが空のまま設定されているため、FMC に登録できない
CSCwk05800	snmp-server host-group でのネットワークの重複により ASA/FTD の SNMP ポーリングが失敗する
CSCwk05851	IP アドレスが NAME に一致する場合、「set ip next-hop」行がリロード時に設定から削除される
CSCwk06216	展開後にセキュリティゾーンとのインターフェイスマッピングが失われる
CSCwk06264	FMC REST API || コード値がない ICMP オブジェクトにより、GET コールおよび JSON 解析が中断される
CSCwk06573	有用性：ルーティングインフラのデバッグを改善し、新しいエラー状態を追加
CSCwk07563	強制的に展開すると、デバイスでエクスポートキャッシュが再生成されない
CSCwk07934	FXOS と Lina 間のクロックスキューにより、SAML アサーション処理が失敗する
CSCwk08064	ADI セッション処理の遅延が 7.2.x へのアップグレード後に再度発生する
CSCwk08476	「show bgp summary」メモリリークによる FTD/ASA のトレースバックとリロード
CSCwk08576	サービスワーカーのデバッグメニュー設定を出力するコマンド
CSCwk09488	RA 認証中に ISE から SGT を処理できなかった場合に誤った syslog が生成される
CSCwk09559	FMC：カスタムユーザーロール VPN では、[変更（Modify）]がオフになっている場合でも、ユーザーはサイト間 VPN を変更できる
CSCwk09612	クロックスキュー：FXOS クロックが Lina NTP 時間の約 1 ～ 10 秒から分岐する

不具合 ID	タイトル
CSCwk10884	l2_table とサブインターフェイスの MAC アドレスが一致しないため接続に失敗する
CSCwk11254	侵入イベントパケットビューで、一部のローカル侵入ルールに関して「ルールを使用不可（Rule Unavailable）」と表示される場合がある
CSCwk11381	LDAP 属性マップを使用して承認サーバーを展開すると、展開に失敗する
CSCwk11983	「flow-export delay flow-create」の設定が原因で LINA CPU の使用率が高くなる
CSCwk11989	複数の ssh セッションから object-group への重複オブジェクト/グループオブジェクトの受け入れ
CSCwk12337	ケルベロスを使用したキャプティブポータル認証の場合、FMC/FTD で RC4 暗号を無効にできない
CSCwk12470	致命的なエラー：スクリプト 800_post/100_ftd_onbox_data_import.sh の実行中にエラーが発生する
CSCwk12497	HA 切断操作によるアクティブユニットでのトレースバックとリロード。
CSCwk12673	1 バイトのキープアライブを受信すると、TCP セッションが中断される
CSCwk12698	管理コンテキストの管理インターフェイスの SNMP ポーリングですべてのコンテキストの全インターフェイスを表示できない
CSCwk13812	アップグレード後に ASA/FTD が拡張コミュニティ属性を誤って転送する。
CSCwk14300	FMC 管理 IP が変更された後も、TS ファイル名に古い IP が表示される
CSCwk14657	RAVPN セッションにおける weblaunch の portal-access-rule のサポートを元に戻す
CSCwk14685	FTD：管理インターフェイスが稼働しているにもかかわらずダウン状態と表示される
CSCwk14909	multi-ctx モードでの TCM cfgd を使用したフェールオーバーの後に、「rule-transaction-in-progress」でトラフィックがドロップする
CSCwk16332	高速の SIP 接続による ASA/FTD のトレースバックとリロード
CSCwk17536	ASA/FTD：プロセス Unified2File_Read に起因するメモリ不足でリロードが発生する
CSCwk17637	FTD HA での Snort のトレースバックによってトリガーされたフェールオーバーの後に、ステートリンクが Hello メッセージの送信を停止する

不具合 ID	タイトル
CSCwk17854	FTD が、AAAA クエリで 1 つの DNS サーバーから拒否エラーを受信した後、タイプ A クエリを送信しない
CSCwk20882	SA の確立/キー再生成後に ESP シーケンス番号 0 が送信される
CSCwk21533	サブドメインの [FMCユーザー（FMC Users）] ページがロードされない
CSCwk21561	CCL MTU の設定時の警告メッセージを追加
CSCwk21562	FTD 外部認証用の Radius サーバーの設定が FTD に展開されない。
CSCwk22034	Snmpwalk で 10G 以上の値の誤ったインターフェイス速度が表示される
CSCwk22574	VTI 復号を許可するために SGT フレーム/パケットを削除
CSCwk22814	FMC：CCL MTU の設定時の警告メッセージを追加
CSCwk24176	FTD/ASA：デバイスを通過する VPN トラフィックがトレースバックとリロードをトリガーすることがある。
CSCwk24380	パケットトレーサの [デバイスの選択（Select Device）] ドロップダウンにデバイスが表示されない
CSCwk24440	filebackup.tar の内容が非常に大きい場合、リモートストレージでバックアップが失敗することがある
CSCwk24597	Snort が多くのゼロ長 snort-unified ファイルを書き込むと、EventHandler が FMC にイベントを送信しないことがある
CSCwk24684	qemu が show users CLI コマンドにリストされている
CSCwk26594	一時バックアップファイルはリモートストレージに保存せず、他の形式のファイルを解析しないようにする必要がある
CSCwk26968	バックアップ機能がマルチコンテキストモードで DAP の設定を保存/復元しない。
CSCwk27175	ASA/FTD：設定のロードにかかる時間が大幅に増加する
CSCwk27628	CDO：シャーシの CDO へのオンボーディングがホスト名が原因で失敗する
CSCwk27639	FMC 7.2.5：フリートアップグレードで、6.6.5 の FTD HA に関する誤ったデータが表示される
CSCwk27830	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
CSCwk27965	（IDS）Post-ACK モードでの不正なストリーム TCP 状態による無限再帰クラッシュに対するセーフティネット
CSCwk28058	FTD メモリの枯渇によってトレースバックとリロードが発生する
CSCwk28296	一方のデバイスチャネルがブロックされると、SFDataCorrelator はもう一方のチャネルでイベントの受信を停止する
CSCwk29771	FTD 7.4.1.x は Radius 要求パケットで NAS-IP-Address:0.0.0.0 をネットワーク インターフェイスとして送信する
CSCwk30049	ASA/FTD がスレッド名「lina」を障害元スレッドに挙げてトレースバックし、リロードすることがある。
CSCwk31371	NAT_HARDEN：マッピングされた ifc が any として設定されていると CGNAT が中断する
CSCwk32340	展開が "SNAPSHOT_PG_TIMESTAMP_ERROR" で失敗した場合に、破損したポリシーをログで特定できるようにする
CSCwk32501	256/1550 ブロックの枯渇プロセス fover_thread
CSCwk33070	FMC：feed_data_manager.log での "java.lang.OutOfMemoryError: Java heap space" エラー
CSCwk33511	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
CSCwk33577	OS バージョンが一致しないため、クラスタを作成するときにデータノードを追加するデバイスがリストされない
CSCwk33634	TLS Client Hello パケットが Snort によってドロップされる
CSCwk33842	FMC 管理ワークフローの問題：グループから NetworkObject を削除し、同じチケットで削除できない
CSCwk33876	標準アクセスリストオブジェクトは、先頭に空白を使用して記述できてしまう
CSCwk34786	Victoria-DT CX：1220 CX モデルで 10 ポートチャネルのサポート
CSCwk34888	メインインターフェイスが除外されていても、サブインターフェイスに対して正常性アラートが生成される
CSCwk34905	ISE サービスがダウンしている FMC での ISE 接続ステータスの正常性アラート
CSCwk35710	EEM スクリプトで「show capture」コマンドが実行されると、FTD/LINA がトレースバックし、リロードすることがある

不具合 ID	タイトル
CSCwk36144	42xx プラットフォームのファンの RPM しきい値を更新
CSCwk36312	「更新ブロックの枯渇」で CPU 使用率が高くなり、二次的な影響（Bgp フラップ、トラフィックドロップ）が生じる
CSCwk37371	7.4.x へのアップグレード後に SGT INLINE-TAG を追加
CSCwk37701	FTD バックアップの復元後に FTD が cdFMC との接続を失う
CSCwk38851	パッチ/ホットフィックスのインストール中に、FMC はポリシーバックアップを作成すべきではない
CSCwk39514	FMC を介して HostScan パッケージを変更すると、エンドポイントアセスメント機能が有効にならない
CSCwk40335	IP アドレスに関連付けられた FQDN ID が設定された制限の 8 を超えると、アラート/警告をトリガーする
CSCwk40726	AC ポリシーデータを取得する FMC REST API コールがタイムアウトし、ルールクエリが大きい場合に AC ポリシー GUI の動作が遅くなる
CSCwk41007	ASA/FTD がトレースバックおよびリロードすることがある
CSCwk41806	OOM によって強制終了しないように LINA を保護する必要がある
CSCwk42112	正常性ポリシーに加えられた変更が保存されない
CSCwk42676	仮想 ASA/FTD がスレッド PTHREAD でトレースバックし、リロードすることがある
CSCwk44366	cdFMC がインターフェイスで configure-geneve-encapsulation を実行できない
CSCwk45257	DVTI でバックアップ VTI に「ピアへの仮想トンネルインターフェイス IP の送信（Send Virtual Tunnel Interface IP to the peers）」フラグが正しく設定されない
CSCwk45975	SSL ポリシーの TLS1.3 復号設定が DND トラフィックに影響する。
CSCwk46737	HA の ASA：スタンバイデバイスの 1 つのコンテキストにおける chunk mem Failed メッセージからの alloc_ch() alloc
CSCwk47035	診断インターフェイスの pre-CMI nameif が MANAGEMENT だと CMI が無効になる
CSCwk48628	FTD/FxOS：設定をアップグレード/削除すると、App-instance が「Operational State: Starting」になる

不具合 ID	タイトル
CSCwk52448	オンプレミスから cdFMC に移行された 21xx 11xx FTD-HA ペアの 7.0.x バージョンに変更を展開できない
CSCwk52890	HTTP ベースのパスモニタリングが原因で FTD/ASA のメモリ使用率が高くなる
CSCwk53048	スタンバイ HA FMC がスタンドアロンモードに移行：作成された /var/tmp/compliance.rules が無効
CSCwk53257	ftdallinterfaces の API コールが不正確な "self" 要素を返す
CSCwk53312	「クラスタ/HA ペアは対象外（cluster/HA pair is not eligible）」というステータスのクラスタはアップグレードできない
CSCwk54033	管理インターフェイスでプロキシが有効になっている場合、FMC でプライベート AMP に接続できない
CSCwk54077	空のネットワークオブジェクトにより、cdFMC の移行が失敗する
CSCwk56388	GRE トラフィックがフェールオーバー後にドロップされる
CSCwk59009	HA ペアで IPv6 SSL Anyconnect アクセスがブロックされる
CSCwk59520	スタートアッププロセスで新しいログをインストゥルメント化して詳細情報を収集
CSCwk61157	dhcp_daemon スレッドでの FTD LINA のトレースバックとリロード
CSCwk61479	onPrem から cdFMC への移行中に、特定のオブジェクトで CSM と EO の間に不整合が発生する
CSCwk62366	FMC からテレメトリデータを取得中に例外が発生する
CSCwk62381	SCP の使用中に ssh/クライアントが null ポインタにヒットするために、ASA がトレースバックし、リロードすることがある
CSCwk63011	「show module」コマンド出力のネットワークモジュールのスロットとステータスに関する情報が正しくない
CSCwk63586	アプリケーション インスタンスが STOP_FAILED でスタックし、エラーメッセージが表示される
CSCwk63733	HA の監視対象のインターフェイスが「待機」状態になり、その後「失敗」になる
CSCwk64418	SHA-1 認証を使用すると、NTP が同期しない
CSCwk64643	ファイアウォールがネゴシエーション中にフェールオーバープロンプトで state active と表示される

不具合 ID	タイトル
CSCwk64709	/mnt/pss に空き領域が不足しているため、FXOS のアップグレードが失敗する（isan.log がほとんどの領域を消費する）
CSCwk67346	DAP ポリシーが属性 TRUE/FALSE で機能しない
CSCwk70078	障害のシミュレーション後に「show failover statistics」で障害とレコードが表示されない
CSCwk70673	FIPS が有効な場合、トラストプールでの証明書の検証が失敗する
CSCwk71227	LDAP を使用して FPR 2K で実行されている FTD が、ldap.conf を更新するときにバックスラッシュをスキップする
CSCwk71866	ASA：同じデバイス上のコンテキスト間のサイト間 VPN が「ipsec-tun-down」によってトラフィックをドロップする
CSCwk75406	syslog を介した CC-mode 監査の FMC が機能しない
CSCwk75956	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
CSCwk76362	スレッド名 PTHREAD での FTDv のトレースバック
CSCwk77241	9k ブロックの枯渇（tcpmod proc）によるトラフィック障害が FPR 3100（HA）で確認された
CSCwk78030	ASA/FTD：Threat-Detection によるメモリの枯渇
CSCwk78075	FTD が、スタック状態の進行中の展開を失敗としてマークせず、後続の展開に失敗する
CSCwk78242	LDAP の空のユーザー属性により、部分的なユーザー/グループがダウンロードされる
CSCwk79222	FMC で表示される正常性アラート：Beaker3 経由の URL/LSP
CSCwk79288	btmp 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
CSCwk81274	FMC：アップグレード後に電子メールアラートを受信しない
CSCwk82557	FDM を介した 7.4.2 への FTD のアップグレードがブロックされる
CSCwk82571	[ユーザーアクティビティ（User Activity）] の FTD スタンバイピアに対して、VPN クライアントアプリケーションのバージョンと OS が表示されない
CSCwk82591	TPK シャーシで MI FTD を作成できない

不具合 ID	タイトル
CSCwk85351	FTD HA ポートレットが、FTD HA 対応デバイスのモニタリングページに表示されない
CSCwk86033	cdFMC への移行後の VPN オブジェクトによるデータベースの破損
CSCwk86582	「ENDPOINT_TIME_OUT_OF_SYNC」エラーによって SAML 認証が完了しない
CSCwk87081	tmp_cisco が大量のブートボリューム スペースを消費し、FMC でファイル記述子のリークを引き起こす
CSCwk87457	デバイスのリロード後に ASA/FTD がプロセス名「lina」でトレースバックし、リロードすることがある
CSCwk87599	show conn detail の rx-ring 4294967295（最大値）フィルタで、無効な rx-ring 番号がある接続が表示される
CSCwk87700	FxOS プラットフォーム上の複数の core.svc_sam_statsAG
CSCwk88182	PTHREAD-8141 spin_lock_fair_mode_enqueue での通常動作時における FTDv50 のトレースバック
CSCwk88201	FPR 9.20 のアップグレード後にサードパーティとの S2S VPN が切断される
CSCwk88225	クリティカルな障害：[FSM:FAILED]：ユーザー設定（FSM:sam:dme:AaaUserEpUpdateUserEp）
CSCwk89127	Backup_info テーブルがプルーニングされないため、DB クエリが遅くなる
CSCwk89836	ASA/FTD がスレッド名「strlen」でトレースバックし、リロードすることがある
CSCwk90663	同じバックアッププロファイルでの外部ストレージの設定が 2 回目に失敗する
CSCwk93762	spin_lock_fair_mode_enqueu および nlp_init() でのパニックにより、デバイスのトレースバックとリロードが 3 回発生する
CSCwk94382	FTD：Lina が CONFIG_XML_REQUEST に応答せず、展開がスタックすることがある
CSCwk96912	FTD：7.4.1 へのアップグレード後に syslog メッセージ ID 302013 にユーザー名がない
CSCwk98990	多数の統計ファイルにより、イベントが遅延する可能性がある
CSCwm01544	data-path スレッドでの Lina のトレースバックとリロード

不具合 ID	タイトル
CSCwm02801	HA が不安定になって展開が失敗する
CSCwm03142	マルチインスタンスセットアップの共有インターフェイスでIPv6ネイバー探索/マルチキャスト通信が影響を受ける
CSCwm03287	FP4245：NPU アクセラレータで 100Gb インターフェイスの速度が 10Mb に変更される
CSCwm04021	プロセス名 lina での ASA/FTD のトレースバックとリロード
CSCwm04085	NAT 警告「NAT ルールが IP アドレスのしきい値 131,838 を超えています...（The NAT rule exceeds the threshold limit of 131,838 IP addresses..）」をドキュメントに記載
CSCwm04650	メモリ使用率が増加して Lina でトレースバックが発生する。
CSCwm05520	FTD クラスタが inline-set で展開されている場合、クラスタの syn cookie 復号を無効にする
CSCwm05960	生成された Crypto チェックサムが設定変更なしで変更される
CSCwm06393	ポートチャネルメンバーシップまたはメンバーステータスの変更により、定期的な OSPF/EIGRP 隣接関係フラップが発生することがある
CSCwm07389	リブートのたびに ASA syslog で CGroups エラーが発生する
CSCwm07419	外部 RADIUS 認証に影響を与えるホスト名を使用すると ldap.conf が生成されない
CSCwm11515	アップグレード後に SNMP トラップ OID が変更される
CSCwm13141	show コマンドを実行しようとすると、FTD CLISH/CLI がロックされる
CSCwm13199	NAT 未変換での予期しない動作により、SIP トラフィックが影響を受ける。
CSCwm14509	GTP インスペクション中に、23、24、25 の IE タイプに対する無効な長さによる誤ったドロップが発生する
CSCwm14561	ASA/FTD がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwm14729	CSF 3100 シリーズが停電後にリブートせず、手動での電源の再投入が必要になる
CSCwm27588	FMC アップグレード中に認証オブジェクト名のスペース文字を削除するよう修正すると、アップグレードが失敗する可能性がある

不具合 ID	タイトル
CSCwm28007	ユーザーが WebVPN のブックマークをクリックすると、ブラウザが空白のページにリダイレクトする
CSCwm28962	HA fover_trace.log ファイルに多数のエラーメッセージが含まれると、短時間でログローテーションが発生する
CSCwm29768	ロギングが有効になっていないルールで接続がログに記録される
CSCwm30035	cdFMC：DAP が設定された FTD の展開に失敗する
CSCwm30731	ASA の OSPF ルーティングテーブルがネイバーと正しく同期されない
CSCwm33229	SAML の強制再認証において、接続の再試行時にユーザーにログイン情報の再入力が強制されない
CSCwm33529	Firepower デバイスの前面パネルとアップリンクポートの FXOS MTU 処理に改善が必要
CSCwm33613	SAML アサーション属性の複数のグループポリシーを受け取ると、デフォルトのグループポリシーが適用される
CSCwm34333	FTD：マルチインスタンスの docker0 インターフェイスがプライベートネットワーク 172.17.0.0/16 と重複する
CSCwm35035	設定したアルゴリズムとは関係なく、FTD による SAML 認証要求が常に Sha1 によって署名される
CSCwm35730	LINA がスレッド名 Datapath with NAT config でトレースバックすることがある
CSCwm35751	FPR3100：インターフェイスが半二重に移行することがあり、速度が 100mbps にハードコードされる
CSCwm36631	FTD のセカンダリユニットが一括同期状態でスタックする。
CSCwm37363	ポートマネージャと lacp の同期がプログラム的に行われない
CSCwm37455	ASA/FTD が無効なネットマスクを持つローカル IP プールを許可する
CSCwm41847	PDTS の書き込み/読み取りブロックをキャプチャして根本原因 CSCwm36314 の解決をサポートするための有用性
CSCwm42000	FTD/ASA が DATAPATH スレッドでトレースバックし、リロードすることがある
CSCwm42745	IKE_AUTH がない場合、ダイナミックサイト間トンネルが IN-NEG 状態でスタックする
CSCwm44412	FTD インラインセットが挿入/書き換えのリバースフラグを無視する

不具合 ID	タイトル
CSCwm44744	オンプレミス FMC から cdFMC へのインポート/エクスポートがブロックされない
CSCwm45164	cdFMC：トンネルタイプが DB に存在しないため、VTI インターフェイスを変更できない
CSCwm49154	展開時に FXOS 障害 F1738 が発生し、エラー CSP_OP_ERROR が表示される。CSP 署名確認エラー
CSCwm49213	回帰のために CSCwk63011 で変更が元に戻された後、show mod 機能を修正する必要がある
CSCwm49721	メモリ破損が検出されたことによる ASA のトレースバックとリロード
CSCwm49782	sma 2nd cruz ハートビートのロギングを強化
CSCwm50591	ASA/FTD：VTI とサブインターフェイスで IPsec オフロードが有効になっていると、インバウンド IPsec パケットがドロップされる
CSCwm50936	両端の Innolight QSFP で 100GB インターフェイスがフラップする
CSCwm51399	オンラインではない場合に、CDO インベントリにデバイスステータスがオンラインと表示される
CSCwm51747	FXOS のアップグレード後に公開キー認証を使用した SSH アクセスが失敗する
CSCwm52264	「パスワード暗号キーが設定されていません。（The password encryption key has not been set.）」という障害を除去またはクリアできない
CSCwm52931	ASA/FTD がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwm52973	TPK Low End FPR3100：インターフェイス速度を 1g から 100mbps/100mps から 1g に変更するとリンクがダウンする
CSCwm56864	show run access-list コマンドが警告を返す
CSCwm58772	ポリシー展開中に Snort2 インスタンスが OOM で予期せず再起動する
CSCwm60536	クラスタリングデータユニットで SQLNet トラフィックが断続的にドロップされる。
CSCwm61282	ASA/FTD：RA VPN トンネルによってメモリリークが発生し、トレースバックとリロードが行われる
CSCwm61693	カーネルで NFS クライアント 4.1 を有効にして、NFS および EFS マウントの問題をデバッグする：stunnel への SIGKILL(9)

不具合 ID	タイトル
CSCwm63868	FTD：FTD HA フェールオーバーイベント後に BGP の advertised-routes にルートがない
CSCwm64553	Po メンバーインターフェイスがフラップした後に互換性のないメンバーに関する警告メッセージが表示され、Po に再参加できない
CSCwm65714	RAID が EZ_BIOSUPDATE-7.2.99.99-6 で正しくアップグレードされない
CSCwm68211	スレッド snmp_inspect での ASA のトレースバックとリロード
CSCwm70835	APCF ファイル使用中のスタックオーバーフローによる ASA のトレースバックとリロード
CSCwm71265	PDP の gtpv1 エンドマーカーメッセージを処理しているときに、ASA がスレッド DATAPATH でトレースバックし、リロードする
CSCwm74289	NAT トラップのレートの制限が必要
CSCwm76872	ztna アプリケーションの無効化による Lina のトレースバックとリロード
CSCwm78351	キャプチャコードの無条件実行により、マルチコンテキストクラスタのセットアップで CPU 使用率が高くなる可能性がある
CSCwm85228	フェールオーバーに参加するときに、ASA/FTD がスレッド名「IKEv2 Daemon」でトレースバックし、リロードすることがある
CSCwm86414	Cisco ASA - フェールオーバー設定の再同期に失敗し、予期しない再起動が発生する
CSCwm88812	4200/3100/1200 ハードウェアで AppAgent タイマーを変更できる
CSCwm89523	「no capture /all」によってバックエンドでキャプチャを完全に無効にできず、データパス CPU の使用率が高くなる
CSCwm90900	GTP インスペクションがエラーによりパケットをドロップする。理由：（IE-Type:CAUSE(2) IE がありません）
CSCwm90905	GTP インスペクションがエラー ERROR-DROP:MsgType:32 でパケットをドロップする
CSCwm91406	7.4.2.1 へのアップグレード後に FTD HA スタンバイが繰り返しリロードする
CSCwm92310	リブートまたはトレースバック後にデータインターフェイスの DNS を介して FQDN が解決されない
CSCwm92397	「IP RIB Update」スレッドを指す LINA コアがある

不具合 ID	タイトル
CSCwm96280	リセットボタンを押した後にFTDデバイスがrommonモードでスタックする
CSCwm96652	クラスタがユニットに対して誤った NAT を割り当てており、トラフィックがユニットに適切に転送されない
CSCwm97054	高速の SIP 接続による ASA/FTD のトレースバックとリロード
CSCwm98278	FIN の ACK を受信した後に TCP 接続がハーフクローズとしてフラグ付けされない。
CSCwm99183	cdFMC：SFOExport ファイルが tmp フォルダでクリアされないため、ディスク使用率が高くなる
CSCwn00475	priority-queue によるメモリブロック 80 および 9344 のリーク
CSCwn01281	セッション作成応答の原因タイプが 18 の場合、GTP インスペクションで GTP データパケットが許可されない
CSCwn03446	クラスタインターフェイスでキャプチャが有効になっている場合、設定されたルールとともに常に CCL IP が含まれる
CSCwn03835	ASA/FTDがスレッド名「SSH Ctxt Thread」でトレースバックし、リロードすることがある
CSCwn11728	FPR9K-SM-56 モジュールが断続的にロックアップし、トラフィックに影響を与える。
CSCwn13187	9.20.2.21 からターゲットバージョン 9.20.3.4 への ASA のアップグレードが失敗する
CSCwn13672	暗号化後の追加の Route-Lookup を回避するために VTI トンネル送信元インターフェイスに ESP をバインドする
CSCwn14130	拡張 PAT の有効化後にトレースバックとリロードを行う FTD クラスタ
CSCwn14447	ASA/FTDがスレッド名「ldap_client_thread」でトレースバックし、リロードすることがある
CSCwn15104	swapcontext 機能のトレースバックによる FTD のリロード
CSCwn15443	拡張 VPN トラフィックテスト中に snp_vpn_int_api でクラッシュ/アサーションが発生する
CSCwn16320	以下の FTD ロギングの syslog サーバーが最初の syslog サーバーの emblem 設定に従ってホスト名情報を送信する

不具合 ID	タイトル
CSCwn17121	ASA/FTD がスレッド名「cli_xml_request_process」でトレースバックし、リロードすることがある。
CSCwn18728	cdFMC へのデバイス移行で、ポリシーベースルーティングが誤ってインポートされる
CSCwn19190	メモリフラグメンテーションにより、lina で大きなページを使用できなくなる
CSCwn19706	管理者ユーザーは、外部サーバーへの認証のときにローカルパスワードの変更を求められる
CSCwn19739	HA が、コールドスタンバイから障害状態に移行する間にデータインターフェイスを起動する
CSCwn20024	ASA 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
CSCwn20642	RA VPN ユーザー アクティビティ レポートでの VPN バイト数の不一致
CSCwn22036	FTD：Management0/0 のステータスがダウンになり、アップグレード後にラインプロトコルがアップ状態になる
CSCwn22456	GTPv2 IE タイプ 157（シグナリング優先順位表示）が不明な IE タイプとしてドロップされる
CSCwn22565	頻繁なルート更新によってルートが削除され、障害が発生する
CSCwn24577	「no pim」または「no igmp」設定を含めると、ASA のブートプロセスがフリーズすることがある
CSCwn26165	Radius パケットが原因となり、FTD/ASA が展開中/Radius の変更中にトレースバックし、リロードすることがある
CSCwn27583	spin_lock_get_actual_internal での Lina の高い CPU 使用率および/またはトレースバックとリロード
CSCwn27819	ジャンボフレームパケットがフラグメント化されている
CSCwn27872	「eigrp_interface_ioctl」API で、約 25KB のメモリの大きなチャンクがスタックに割り当てられる
CSCwn29611	Radius ユーザーの ssh ログインが失敗し、エラー「ユーザー名が有効なサービスタイプで定義されていません（username is not defined with a service type that is valid）」が表示される
CSCwn31240	webvpn dtls フローオフロードが有効な場合のトレースバックとリロード

不具合 ID	タイトル
CSCwn31588	MI：FPR42xx で 14 ー 70 の CPU コアを使用して RP を割り当てると、インスタンスがスプリットブレイン状態になる
CSCwn31653	FTD がスレッド名「FPRLI_FPR4K-SM-32」でトレースバックし、リロードすることがある
CSCwn32978	スレッド名 Datapath でのトレースバックとリロード
CSCwn34259	9.20.3.7 へのアップグレード後に監視対象のインターフェイスが待機状態になることがある
CSCwn34659	DNS 応答で TC ビットセットを受信した後でも、ファイアウォールが TCP 要求を開始しない
CSCwn34707	複数の Unicorn Admin Handler プロセスが、すべてのコントロールプレーンの CPU を消費する。
CSCwn35495	フェールオーバー時に FXOS でプライマリ FTD インスタンスの MAC アドレスが正しく更新されない
CSCwn36712	スタンバイの 8305 の NAT 迂回がフェールオーバー後に更新されないため、プライマリのスタンバイ FTD が FMC でオフラインと表示される
CSCwn38761	7.7 で、サーバー/サーバーに到達するインターフェイスがダウンしている状態で FQDN オブジェクトが削除された際に、DNS FQDN オブジェクトが未解決にならない
CSCwn39081	SNMP ウォークが IP アドレスではなく IPSEC ピアの ASCII 値になる。
CSCwn39780	FTD 展開のレジリエンス：クリティカルでない/存在しないコマンドをスキップして展開の失敗を回避。
CSCwn39826	HA は、copy/config-sync/rollback の進行中にフェールオーバー要求を受け入れないようにする必要がある
CSCwn40485	MI：データ共有インターフェイスで有効になっている場合、トラフィックがセカンダリ FTD に到達できない
CSCwn40572	MI：仮想 MAC が設定されている場合、Vlan 情報が FXOS レベルで適用されない
CSCwn42949	分散セカンダリフロー接続を処理する非オーナーユニットでのフォワーダーフローの導入
CSCwn44335	FXOS：Download コマンドが HTTP および HTTPS GET 要求に対して追加の「/」を生成する

不具合 ID	タイトル
CSCwn45049	Coverity システム SA の警告、2024 年 9 月 9 日、Coverity の不具合 922530 922529 922528 922630 921809 921808
CSCwn45510	S2S VPN トンネルの子 SA の再ネゴシエーションが失敗する
CSCwn46426	ASA 21xx：「sh environment temperature」に誤った温度値が表示される
CSCwn46855	LINA で Netflow が設定されたランダムトレースバックが確認されることがある
CSCwn47308	FPR 1100/2100/3100 のクリティカルな正常性アラート「user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)」
CSCwn49391	FTD HA のアップグレード後に頻繁にトレースバックが発生する
CSCwn50760	9.20.3.7 へのアップグレード後の ASA トレースバック
CSCwn51845	ASA 9.20.3.4 を実行しているクラスタメンバーでトレースバックが確認される
CSCwn57674	解放後に設定されたブロック loc 操作を修正
CSCwn59032	ASA 9.18.4.22（FPR 2130 プラットフォームモード）へのアップグレード後に FCM GUI にアクセスできなくなる
CSCwn60726	スレッド名 vtemplate process でトレースバックおよびリロードする
CSCwn63839	BVI との arp permit-nonconnected の設定時にスレッド名 Lina でトレースバックする
CSCwn64025	ASA：他のネイバーから学習した IPv6 EIGRP ルートが、フェイルオーバー後の更新に含まれない
CSCwn65415	ASA：ネクストホップの ARP エントリなしで接続が作成された場合、floating-conn で UDP 接続が閉じられない
CSCwn71596	インターフェイスリンクのダウン（Init、mac-link-down）が確認された：ケーブルの取り外し/再接続後に EtherChannel メンバーシップがダウン/ダウン/ダウンの状態になる
CSCwn71946	show blocks old core local を使用すると、予期しないリロードが発生する可能性がある。
CSCwn73351	アジア/バンコクのタイムゾーンオプションが、firepower1k で実行している ASA に表示されない
CSCwn75667	設定時にバナー motd が表示されない

不具合 ID	タイトル
CSCwn76079	SSH は管理コンテキストで動作するものの、ssh key-exchange を変更するとユーザーコンテキストで動作しない
CSCwn79553	到達不能な LDAP/AD を照会すると、FTD の外部認証で遅延またはタイムアウトが発生することがある
CSCwn80419	設定可能なオプションとして SVC Rx/Tx キューが必要
CSCwn80765	CiscoSSH が有効な場合に ASA を搭載した ISA3000 が SSH アクセスを拒否する
CSCwn81118	RTSP パケットが送信キューでスタックして 9k ブロックが枯渇する。
CSCwn81995	SNMP インスペクションが有効になっている場合のメモリ破損によるトレースバックとリロード
CSCwn84557	「spin_lock_fair_mode_enqueue」による Lina のトレースバックとリロード
CSCwn90900	RA VPN に関連する SNMP OID のポーリングが原因となり、ASA/FTD のメモリ使用率が高くなる
CSCwn91996	WM-DT-7.7.0-40：デバイスコンソールでスイッチの設定の失敗とスイッチの Mac エラーが確認される
CSCwn92248	FTD FP2100 ポートチャネル インターフェイスが LACP でフラップする
CSCwn92894	「show chunkstat top-usage」の出力にすべてのエントリが表示されないことがある
CSCwn93319	ASA/FTD がスレッド名「DATAPATH」でトレースバックし、リロードすることがある
CSCwn95939	受信した CRL がキャッシュされた CRL より古い場合に syslog を生成
CSCwn95945	受信した CRL 署名の検証が失敗した場合に syslog を生成
CSCwn96929	ASA：スレッド名 SSH でのトレースバックとリロード
CSCwn96963	FTD が VPN ヘアピンのない VPN ルーティングとして syslog 430002 を生成する
CSCwn97630	IPv6 パケット処理が原因で DATAPATH で FTD リブートおよびトレースバックが発生する
CSCwn98402	デバッグ可能性：アップグレード後に FP2100 ポートチャネル インターフェイスがフラップする
CSCwo00102	不正なウィンドウサイズ情報を受信したために、Snort3 が無効なシーケンス番号でパケットをトリミングする

不具合 ID	タイトル
CSCwo00225	アップグレード前に設定されている場合、VNI送信元MTUがアップグレード後に IPv6 に認識されない
CSCwo00444	FPR3100プラットフォームでの暗号ハードウェアのオフロードに影響する Nitrox Engine（Crypto Accelerator）の問題
CSCwo00702	コミュニティリストは、リストの最後の項目が削除されるまでエラーをスローしない必要がある
CSCwo01557	メモリ破損による DATAPATH スレッドでの ASA のトレースバックとリロード
CSCwo05712	有用性強化：FXOS ディスクエラーをよりわかりやすくする
CSCwo08042	Unicorn Proxy スレッドでのトレースバックにより、ASAv が予期せずリロードする
CSCwo08306	ローカルへのコマンド承認のフォールバックが、権限 15 のユーザーに対してのみ機能する。
CSCwo08724	snort 障害中にピアユニットが準備完了状態になる前に、アクティブな HA ユニットが障害状態になる
CSCwo09060	4096 ビットの RSA キーを持つ SSL トラストポイントが、CLI で更新されると ASA で許可されない
CSCwo09195	FQDN を無効化した後の展開中のトレースバックとリロード。
CSCwo09618	EEM によるデバッグの有効化が失敗する
CSCwo15715	IKEv2 キー再生成が、IKE キー再生成中のフラグメンテーションによって失敗する
CSCwo18838	ASA/FTD がスレッド名「lina_exec_startup_thread」でトレースバックし、リロードすることがある
CSCwo19762	マルチコンテキストモードで mac-address auto を再度有効にすると、クラスタ内のデータノードに再度参加できない
CSCwo21767	カスタム設定に対してポートスキャンアラートが生成されない
CSCwo24772	debug packet-condition が期待どおりに機能しない
CSCwo24856	FPR 2140 HA 7.4.2.1（Snort 2）：9K ブロックの枯渇により、ファイアウォールを通過するすべてのトラフィックが遅延する
CSCwo26258	FPR 4200 シリーズでのリロードまたはアップグレード後における Management0 から Management1 へのデフォルトルートの変更

不具合 ID	タイトル
CSCwo27260	ユニットがアクティブになるまでに約 13 秒かかる
CSCwo31094	NFS が有効になっているディスクアクセスの問題によって、仮想 ASA がトレースバックおよびリロードする
CSCwo33815	FMC：プラットフォーム設定から SNMP ホストを削除すると、展開に予想よりも時間がかかる
CSCwo35783	ネイバーとのルートの追加/更新/取り消しに対するデバッグを強化
CSCwo35788	有用性強化：高度なデバッグ用の新しい「show bgp internal」コマンド
CSCwo41250	メモリ不足状態時のスレッド DATAPATH-1-23988 でのトレースバックとリロード
CSCwo42102	show tech-support fprm detail コマンドが長時間スタックする
CSCwo42230	メモリリークが原因でスプリットブレインが発生
CSCwo45848	SecGW：データノードが cluster_ccp_make_rpc_call failed to clnt_call エラーでクラスタに参加できない
CSCwo46142	ポートチャネルメンバーのインターフェイスがフラップによって非アクティブなメンバーになる
CSCwo47978	ASA がスレッド名「fover_parse」でトレースバックし、リロードすることがある
CSCwo49425	logging recipient-address でロギングメールメッセージのシビラティ（重大度）レベルが上書きされない
CSCwo49744	DNS とデフォルトゲートウェイが、データインターフェイスを介して管理される FTD で削除される
CSCwo50417	Warwick Avenue：MGMT 1/2 インターフェイスがダウン状態の場合、LLDP ネイバーが検出されない
CSCwo54996	9344 ブロックのリークによるトラフィック障害
CSCwo57740	「${dsk_a} がないか操作できません。ブレードをリブートしています。（${dsk_a} missing or inoperable. Rebooting Blade.）」というエラーにより、不足しているか操作できないディスクが指定されない。
CSCwo58033	[クラスター] コンテキストで NAT プールの枯渇が発生すると、CPU 使用率が 100% になる。
CSCwo58191	FTD：snort によって検査されるパケットの大規模な遅延

不具合 ID	タイトル
CSCwo58260	GRE | IPinIP 接続の「built」および「teardown」メッセージを Lina syslog に追加します
CSCwo59534	メモリの破損により lina アサーションとトレースバックが発生する
CSCwo60609	ドクタリングルールのタイプがダイナミックであり、インターフェイスがある場合、DNS ドクタリングが正しく機能しない
CSCwo61241	checkSystemCPUs 障害により、論理アプリケーションが「Start Failed」でスタックする
CSCwo65060	FTD HA | ポートチャネルの同じ MAC が原因でネットワーク障害が発生する。
CSCwo65891	変更チケットを検証できない：
CSCwo66872	snmp_logging_thread がコントロールプレーンの CPU を多く使用している
CSCwo69637	「管理者（Admin）」ユーザーによる FMC SSL ポリシー詳細設定の変更が「読み取り専用（Read-only）」ユーザーに表示されない
CSCwo71052	リロード後に FPR1010 Ethernet1/1 トランクポートで Vlan トラフィックが渡されない
CSCwo74496	無関係な BFD ピアがダウンした後、ASA が着信 BFD パケットを処理しないことが原因で BFD がフラップする
CSCwo75483	SNMP エージェントとして使用される HA の FTD マルチインスタンスでシャーシへの SNMP ポーリングが失敗する
CSCwo75810	SNMP 設定が同じ FTD のタイプとバージョン間で一貫して適用されない
CSCso76165	rsync によるデプロイメントの失敗
CSCwo76436	ピアスイッチのリロード時に、インターフェイス MAC 用の 3100 マーベル 4.3.14 CPSS パッチがスタック状態になる
CSCwo77665	「低」に設定されている場合、FMC のポートスキャンイベントで誤った送信元/宛先が表示される
CSCwo78969	ユニットがクラスタに再参加するときのスレッド名 DATAPATH でのトレースバック
CSCwo79028	フェイルオーバー後の FQDN 解決が次の DNS ポーリング間隔まで保留される
CSCwo79798	リロード後に暗号化チェックサムが変更される

不具合 ID	タイトル
CSCwo80223	代替パス経由で受信したシングルホップ BFD セッションで BFD パケットがドロップされない
CSCwo82639	ローカルユーザーの詳細がクラスタセットアップのデータノードに複製されない。
CSCwo82658	ASDM：アイデンティティ証明書を追加するときに、キーペアがすでに存在するというエラーが表示される
CSCwo83389	FXOS の複数の場所での RSA キーの長さの違い
CSCwo84467	DATA ノードがまだ一括同期状態のときに BGP が即座に起動する L3 クラスタリング
CSCwo86422	CCL を介した一方向通信により分割クラスタが発生する
CSCwo87938	バックアウトの変更により、FIPS モードでクラスタリングを有効にできない
CSCwo88204	sch_dispatch_to_url での Smart Call Home プロセスによって ASA/FTD のトレースバックとリロードが発生する
CSCwo88518	クラスター内のいずれかのノードでコマンドレプリケーションが失敗した場合、クラスターからノードを FMC にキックアウトする
CSCwo89233	アクセスリスト後のコマンド commit noconfirm revert-save でクラスターノードへのコマンド複製が失敗し、追加のデバッグが発生する
CSCwo91436	FPR 4125 マルチインスタンス：Snort およびシステムコアの 高 CPU 使用率（100%）により FMC 重大アラートが発生する
CSCwo91965	ASAv が予期せず再起動する
CSCwo94483	非 CP スレッドでのトレースバック後に LINA がリロードせずに非アクティブのままになる
CSCwo98752	クラスタへの再参加を試みる際の、スレッド名 DATAPATH でのトレースバック
CSCwp01015	機能 mp_percore での ASA/FTD のトレースバックとリロード
CSCwp04235	ASA のトレースバックとリロード
CSCwp06882	Hyper-V で実行している ASA を 9.20.3.9 から 9.20.3.16 にアップグレードした後に CPU 使用率が高くなる
CSCwp06890	接続すると、Finisar ポートの SFF_SFP_10G_25G_CSR_S V03 モジュールがバウンスします。

不具合 ID	タイトル
CSCwp08772	ASA：tls-proxy maximum-session コマンドエラー
CSCwp10957	SSL エラーにより、Cisco Smart Software Manager（CSSM）への接続が終了する
CSCwp11382	ASA/FTD：ssl trust-point コマンドがリロード後に削除された
CSCwp13016	FTD/ASA SSH：端末モニターにログが表示されない
CSCwp13540	クライアントレス VPN のファイルパスに日本語テキストを使用したファイルのアップロードに対して、誤った URL が表示される
CSCwp14123	Tmatch メモリが、主に ARP-DP によって消費される。
CSCwp16529	「show cluster info load-monitor details」を使用すると、バッファドロップに対して負の値が表示される
CSCwp16739	ASA クラッシュ情報ファイルが FP4200 デバイスで生成されない
CSCwp17700	少なくとも 1 つの syslog ホストで EMBLEM 形式が有効になっている場合、Syslog 形式が正しく出力されない。
CSCwp22214	トラフィックがボックスを通過しているときに、複数のメールドロップと enq の失敗が発生する
CSCwp22612	Umbrella DNS 設定を削除しようとすると、FTD でポリシー展開が失敗する
CSCwp22743	wpk - 1gsx リンクは wpk で稼働中だが、スイッチ側では接続されていないと表示される
CSCwp25033	ICMP に到達できないストームにより、2 ユニットの FTD クラスタで CPU が高くなる可能性があります
CSCwp26815	スタンバイ ASA デバイスでの「WebVPNタイマープロセス」による CPU 使用率
CSCwp33077	SAML IdP エンティティ ID が 128 文字の上限より増加する
CSCwp33410	dmesg および kern.log ファイルが Tx Queue=0 ログでフラッディングする
CSCwp34610	Windows および MacOS ネイティブ VPN クライアントで IKEv2-EAP 認証が失敗する
CSCwp36133	インターフェイス PAT（接続先インターフェイス）へのフォールスルーの動作が期待どおりに機能しないため、動作を明確にする。
CSCwp37284	ユーザーが [クライアントレス VPN] ページからログアウトをクリックすると、「CSRF Token Mismatch」エラーが表示される。

不具合 ID	タイトル
CSCwp39319	大規模な CRL の処理中に ASA メモリがリークする。
CSCwp66721	SSL 暗号化でのメモリリークにより、FTD 7.7.0 を実行しているローエンドデバイスで Lina メモリ使用率が高くなる
CSCwp67356	HA 状態が ColdStandby から Active に移行しない
CSCwp89969	ファイアウォールの再起動/リブート完了により遅延が発生する
CSCwp90780	.tgz コンテキストファイルを復元すると、割り当てられたインターフェイスが 'system' 設定から削除される
CSCwp93368	Azure に展開された FTDv ファイアウォールで LINA トレースバックが観測された：snp_vxlan_encap_and_send_to_remote_peer
CSCwp97402	WA：大規模な snmp 設定がある展開中に、tmatch テーブルでロックの競合が発生するため、トレースバックおよびリロードする
CSCwp97862	フェイルオーバー IPSEC PSK が 78 文字以上の場合、HA が「Could not set failover ipsecpre-shared-key」で中断する
CSCwq07441	HA で設定されたインターフェイスのモニタリングが原因で、ASA を実行している FP2110 でメモリリークが観測された
CSCwq07808	イーサネットインターフェイスで速度を変更した後、FP3105 トレースバックとリロードが発生する
CSCwq09614	Snort が SCTP パケットをドロップし、SCTP 接続をブロックすることがある
CSCwq16926	2 つのプロセスが TD サブネット構造を解放しようとすると、トレースバックとリロードが発生する
CSCwq17612	HA によってリロードがトリガーされると、コンソールに誤った「フェイルオーバーリセット」ログが出力される。
CSCwq22206	キー再生成中に 'IKEv2 negotiation aborted due to ERROR: Platform errors' により、VPN が失われた
CSCwq23394	FTD が mlx5 ドライバレベルで Azure クラウドでのトラフィックをドロップする場合がある
CSCwq26863	FP2110 - ntpd プロセスが常にクラッシュする
CSCwq27217	ASA：脅威検出時にトレースバックとリロードが発生し、その後インターフェイスが不安定になる。

不具合 ID	タイトル
CSCwq29375	ASA/FTD：FP_PUNT の置換中にアサートがトリガーされた（aaa アカウントの一致）
CSCwq29706	SNMP 設定を編集後にトレースバックとリロードが発生する。
CSCwq32085	FP3100 は、コンソールに「KC ILK の問題が検出されました（KC ILK issue detected）」というエラーを表示し、crypto_archive を生成した後に再起動する
CSCwq35960	OSPF：高可用性セットアップの両方のユニットで Lina がトレースバックおよびリロードする。
CSCwq36466	expat/xml FW が自身をリブートしたが、クラッシュ情報が生成されない
CSCwq43711	アイドル SSH セッションが Fin フラグで正常に終了せず、設定されたタイムアウトを超えて存続する
CSCwq46058	ASA SNMP 応答の問題：奇数の OID に対してのみ応答が送信され、偶数には送信されない
CSCwq46143	SSE-ASAc 同期中に復元された修正を再コミットする
CSCwq47622	'TLS サーバーアイデンティティ検出' を有効にした後、Lina がトレースバックおよびリロードする
CSCwq50189	ASAv の展開が失敗した：コンソールが連続してスタック状態になる
CSCwq50373	HA での ASA/FTD：ブートアップ中の snmptranslate プロセスにより、高 CPU および IPC タイムアウトが発生し、スプリットブレインを引き起こす
CSCwq52255	FTD 管理 IP アドレスへの SSH ログインで、/mnt/boot/application/*.de ファイルがないため、FTD CLISH ではなく FXOS シェルにログインする。
CSCwq54109	FTD 3130 HA Lina がトレースバックする（ikev2_bin2hex_string）
CSCwq60586	バンドルイメージ存在検証エラーにより、FTD アップグレードが失敗した
CSCwq65955	HA リンク ARP パケットがドロップされ、内部アップリンク linkChange カウンタが増加する
CSCwq70133	パスワードを変更した後、パスワードの有効期限がリセットされない
CSCwq70773	ASP ルールエンジンの問題を完全およびランタイムで表示
CSCwq72156	特定の条件において、複数の SNMP サーバーのいずれかに SNMP トラップが送信されない
CSCwq73994	ASA：Hyper-V でパフォーマンスと高い CPU 使用率が見られた

不具合 ID	タイトル
CSCwq74204	IKEv1 L2Lvpn がフェーズ 2 で、アップグレード後に "Rejecting IPsec tunnel: no matching crypto map entry" で失敗する。
CSCwq74738	RAVPN SSL/IKEV2 認証エラー：AAA プロセスの不正なファイバクラス
CSCwq74986	FTD：起動ループでインスタンスがスタック状態になる
CSCwq81480	FTD MI：アップグレード後に SNMP ポーリングが機能しない
CSCwq92728	SSH 認証の TACACS+ 要求に ASA クライアント IP がない
CSCwq95810	「no http server Basic-auth-client ASDM」で、ASDM から ASA への接続が許可される。
CSCwq96870	Firepower のシャットダウン時にインターフェイスが起動する
CSCwq98101	FTD HA でインラインセットが設定されている場合、ポリシー展開が失敗する
CSCwq98648	ASAv で RAM 割り当てが少ないと、'asdm image' コマンドで予期しない動作をトリガーする
CSCwr05406	natAddrMapTable での snmpwalk 中に、HA stby ノードでトレースバックする
CSCwr12965	HA の両方のユニットが同時に暗号化アルゴリズムを変更した
CSCwr14186	"show asp drop" コマンドの使用方法に cmd-invalid-encap asp-drop タイプのコンテキストを追加
CSCwr15697	80 の枯渇による ssl_decrypt_cb のブロック
CSCwr19123	スタンバイがアクティブに変更されると、FPR HA ESP シーケンス番号の不一致により、アンチリプレイドロップが発生する。
CSCwr22256	FQDN リストが解決済み IP の 200 を超えるエントリを拡張しているときに、トレースバックが発生する
CSCwr22492	ASA/FTD：200 を超えるアドレスに解決する FQDN オブジェクトが原因でトレースバックとリロードが発生する
CSCwr28908	ASA：asdm イメージを保存した後にトレースバックとリロードが発生する
CSCwr31782	Cisco Secure Client SAML：IKEv2-IPsec と証明書マッピングを使用すると、外部ブラウザで証明書を要求することがある
CSCwr49028	SDI プロトコルを使用すると、セキュア クライアント トンネル グループ認証が影響を受ける。

不具合 ID	タイトル
CSCwr50466	ASA/FTD：'show ssl objects' で X509_STORE_CTX に誤った値が表示される。
CSCwr55089	ASA/FTD：スレッド名 DATAPATH でトレースバックおよびリロードが発生する

支援が必要な場合

アップグレード ガイド

Firewall Management Center 展開では、Firewall Management Center は管理対象デバイスと同じまたは新しいメンテナンス（3桁）リリースを実行する必要があります。最初に Firewall Management Center をアップグレードし、次にデバイスをアップグレードします。ターゲットバージョンではなく、現在実行しているバージョンのアップグレードガイドを使用してください。

表 *28*：アップグレード ガイド

プラットフォーム	アップグレード ガイド	リンク
Firewall Management Center	現在実行中の Firewall Management Center バージョン。	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense with Firewall Management Center	現在実行中の Firewall Management Center バージョン。	https://cisco.com/go/ftd-fmc-upgrade
デバイスマネージャを使用した Firewall Threat Defense	現在実行中の Firewall Threat Defense バージョン。	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense with クラウド提供型 Firewall Management Center	クラウド提供型 Firewall Management Center。	https://cisco.com/go/ftd-cdfmc-upgrade

インストールガイド

アップグレードできない場合、またはアップグレードしない場合は、メジャーリリースおよびメンテナンスリリースを新規インストールできます。これは再イメージ化とも呼ばれます。パッチに再イメージ化することはできません。適切なメジャーリリースまたはメンテナンスリリースをインストールしてからパッチを適用してください。FXOS デバイスで以前の Firewall Threat Defense バージョンに再イメージ化する場合は、オペレーティングシステムとソフトウェアがバンドルされているデバイスでも、完全な再イメージ化を実行します。

表 *29* : インストールガイド

プラットフォーム	インストール ガイド	リンク
Firewall Management Center ハードウェア	ご使用の Firewall Management Center ハードウェアモデルのスタートアップガイド。	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Firewall Management Center Virtual スタートアップガイド。	https://cisco.com/go/fmcv-quick
Firewall Threat Defense ハードウェア	ご使用のデバイスモデルのスタートアップガイドまたは再イメージ化ガイド。	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	ご使用の Firewall Threat Defense Virtual バージョンのスタートアップガイド。	https://cisco.com/go/ftdv-quick
Firepower 4100/9300 用 FXOS	FXOS バージョンのコンフィギュレーション ガイドの「*Image Management*」の章。	https://cisco.com/go/firepower9300-config
Firepower 1000 および Secure Firewall 3100/4200 用 FXOS	トラブルシューティング ガイドの「*Reimage Procedures*」の章。	*Cisco FXOS* 障害対応ガイド（*Firepower Threat Defense* 向け）

その他の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：https://cisco.com/go/threatdefense-76-docs
- シスコ サポートおよびダウンロード サイト：https://cisco.com/c/ja_jp/support/index.html
- Cisco Bug Search Tool：https://tools.cisco.com/bugsearch/
- シスコ通知サービス：https://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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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。