

Cisco Firepower 4100/9300 FXOS 2.4(1) リリースノート

初版：2018年10月25日

最終更新：2021年5月17日

Cisco Firepower 4100/9300 FXOS 2.4(1) リリースノート

このドキュメントには、Cisco Firepower eXtensible Operating System (FXOS) 2.4(1) のリリース情報が記載されています。

このリリースノートは、次のマニュアルのロードマップに示されている他のマニュアルの補足として使用します。

- <http://www.cisco.com/go/firepower9300-docs>
- <http://www.cisco.com/go/firepower4100-docs>



(注) ユーザマニュアルのオンラインバージョンは、初回リリース後に更新されることがあります。その結果、Cisco.com のドキュメントに記載されている情報は、製品に含まれる状況依存ヘルプに記載されている情報よりも優先されます。

はじめに

Cisco Firepower セキュリティ アプライアンスは、ネットワークおよびコンテンツセキュリティソリューションの次世代プラットフォームです。Firepower セキュリティ アプライアンスは Cisco Application Centric Infrastructure (ACI) セキュリティソリューションの一部であり、拡張性、一貫性のある制御、シンプルな管理を実現するために構築された、俊敏でオープン、かつセキュアなプラットフォームを提供します。

Firepower セキュリティ アプライアンスには、次の機能があります。

- モジュラ シャーシベースのセキュリティ システム：高性能で柔軟な入出力構成と、優れた拡張性が提供されます。
- Firepower Chassis Manager：グラフィカルユーザインターフェイスによって、現在のシャーシステータスが効率良く視覚的に表示され、シャーシ機能を簡単に設定できます。

- FXOS CLI : 機能の設定、シャーシステータスのモニタリング、および高度なトラブルシューティング機能へのアクセスを行うコマンドベースのインターフェイスを提供します。
- FXOS REST API : ユーザがシャーシをプログラムによって設定し、管理できます。

新機能

FXOS 2.4.1.268 の新機能

Cisco FXOS 2.4.1.268 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.268 で解決されたバグ \(11 ページ\)](#)」を参照）。

FXOS 2.4.1.266 の新機能

Cisco FXOS 2.4.1.266 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.266 で解決されたバグ \(11 ページ\)](#)」を参照）。

FXOS 2.4.1.252 の新機能

Cisco FXOS 2.4.1.252 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.252 で解決されたバグ \(13 ページ\)](#)」を参照）。

FXOS 2.4.1.249 の新機能

Cisco FXOS 2.4.1.249 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.249 で解決されたバグ \(13 ページ\)](#)」を参照）。

FXOS 2.4.1.244 の新機能

Cisco FXOS 2.4.1.244 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.244 で解決されたバグ \(14 ページ\)](#)」を参照）。

FXOS 2.4.1.238 の新機能

Cisco FXOS 2.4.1.238 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.238 で解決されたバグ](#)」を参照）。

FXOS 2.4.1.234 の新機能

Cisco FXOS 2.4.1.234 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.234 で解決されたバグ](#)」を参照）。

FXOS 2.4.1.222 の新機能

Cisco FXOS 2.4.1.222 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- さまざまな問題を修正します（「[FXOS 2.4.1.222 で解決されたバグ](#)」を参照）。

FXOS 2.4.1.214 の新機能

Cisco FXOS 2.4.1.214 には、以前のリリースに含まれている機能に加えて、次の新機能が導入されています。

- Firepower Threat Defense バージョン 6.3 のサポート。
- Firepower Threat Defense のマルチインスタンス機能（「[Firepower Threat Defense のマルチインスタンス機能](#)」を参照）。



（注） Firepower Threat Defense バージョン 6.3 以降が必要です。

- さまざまな問題を修正します（「[FXOS 2.4.1.214 で解決されたバグ](#)」を参照）。

FXOS 2.4.1.101 の新機能

Cisco FXOS 2.4.1.101 には、次の新機能が導入されています。

- ASA 9.10(1) のサポート。
- ASA 論理デバイスのトランスペアレントモード展開のサポート。

ASA を展開するときに、トランスペアレントまたはルーテッドモードを指定できるようになりました。

新しい/変更された FXOS コマンド：**enter bootstrap-key FIREWALL_MODE、setvalue routed、set value transparent**

新規/変更された [Firepower Chassis Manager] 画面：

[Logical Devices] > [Add Device] > [Settings]

新規/変更されたオプション：[Firewall Mode] ドロップダウン リスト

- クラスタ制御リンクのカスタマイズ可能な IP アドレス。

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID (127.2.chassis_id.slot_id) に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック (127.0.0.0/8) およびマルチキャスト (224.0.0.0/4) アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。

新規/変更されたコマンド：**set cluster-control-link network**

新規/変更された画面：

[Logical Devices] > [Add Device] > [Cluster Information]

新規/変更されたオプション：[CCL Subnet IP] フィールド



(注) [CCL Subnet IP] フィールド オプションは、ASA 9.9.2 以降および Firepower Threat Defense 6.3.0 以降でサポートされています

- オン モードでのデータ EtherChannel のサポート。

データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。

新規/変更された画面：

[Interfaces] > [All Interfaces] > [Edit Port Channel] > [Mode]

新規/変更されたコマンド：**set port-channel-mode**

- Firepower 4110 デバイスで ASA を使用して Radware DefensePro (vDP) を有効にできるようになりました。
- Radware DefensePro (vDP) アプリケーションは、シャーシ内クラスタ シナリオのスタンダードアロン コンフィギュレーションに導入できます。
- Firepower 4100 シリーズ デバイスの Cisco Smart Licensing にホスト名データを送信しないオプションが用意されました。
- 一度に複数の障害を確認できるようになりました。
- Firepower シャーシマネージャに、アップロード中のイメージのアップロードの割合が表示されるようになりました。
- さまざまな問題を修正します（「[FXOS 2.4.1.101 で解決されたバグ](#)」を参照）。

Firepower Threat Defense のマルチインスタンス機能



(注) FTD バージョン 6.3 以降が必要です。

単一のセキュリティエンジンまたはモジュールに、それぞれ Firepower Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブアプリケーションインスタンスを展開するだけででした。ネイティブインスタンスも引き続きサポートされています。Firepower 9300 の場合、一部のモジュールでネイティブインスタンスを使用し、他のモジュールではコンテナインスタンスを使用することができます。

柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。コンテナインスタンスを展開する場合、割り当てられた CPU コアの数に指定する必要があります。RAM とディスク容量は、コアの数に従って動的に割り当てられます。このリソース管理を使用すると、各インスタンスのパフォーマンス機能をカスタマイズできます。

2つの個別のシャーシでコンテナインスタンスを使用してハイアベイラビリティを使用することができます。たとえば、10 個のインスタンスを持つシャーシを 2 つ使用する場合は、10 個のハイアベイラビリティペアを作成できます。クラスタリングはサポートされません。



(注) マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。マルチコンテキストモードでは、単一のアプリケーションインスタンスがパーティション化されますが、マルチインスタンス機能では、独立したコンテナインスタンスを使用できます。コンテナインスタンスでは、ハードリソースの分離、個別の構成管理、個別のリロード、個別のソフトウェアアップデート、および Firepower Threat Defense のフル機能のサポートが可能です。マルチ コンテキスト モードでは、共有リソースのおかげで、特定のプラットフォームでより多くのコンテキストをサポートできます。マルチ コンテキスト モードは Firepower Threat Defense では利用できません。

モデルごとの次の最大コンテナ インスタンス数を参照してください。

- Firepower 4110 : 3
- Firepower 4120 : 3
- Firepower 4140 : 7
- Firepower 4150 : 7
- Firepower 9300 SM-24 セキュリティ モジュール : 7
- Firepower 9300 SM-36 セキュリティ モジュール : 11
- Firepower 9300 SM-44 セキュリティ モジュール : 14

新規/変更された [Firepower Chassis Manager] 画面 :

[Overview] > [Devices]

[Interfaces] > [All Interfaces] > [Add New] ドロップダウンメニュー > [Subinterface]

[Interfaces] > [All Interfaces] > [Type]

[Logical Devices] > [Add Device]

[Platform Settings] > [Mac Pool]

[Platform Settings] > [Resource Profiles]

新しい/変更された FXOS コマンド :

connect ftd name、connect module telnet、create bootstrap-key PERMIT_EXPERT_MODE、create resource-profile、create subinterface、scope auto-macpool、set cpu-core-count、set deploy-type、set port-type data-sharing、set prefix、set resource-profile-name、set vlan、scope app-instance ftd name、show cgroups container、show interface、show mac-address、show subinterface、show tech-support module app-instance、show version

新規/変更された [Firepower Management Center] 画面 :

[Devices] > [Device Management] > [Edit] アイコン > [Interfaces] タブ

ASA アプリケーション向け FXOS CLI の変更

ASA 論理デバイスの操作時に使用される FXOS CLI コマンドが変更されました。

新しい/変更された FXOS コマンド :

connect asa name、create app-instance asa name、scope app-instance asa name、show app-instance asa name

ソフトウェアのダウンロード

FXOS およびサポートされているアプリケーションのソフトウェアイメージは、次のいずれかの URL からダウンロードできます。

- Firepower 9300 : <https://software.cisco.com/download/type.html?mdfid=286287252>
- Firepower 4100 : <https://software.cisco.com/download/navigator.html?mdfid=286305164>

FXOS の特定のバージョンでサポートされているアプリケーションの詳細については、次の URL の Cisco FXOS 互換性ガイドを参照してください。

<https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html>

特記事項

- ハードウェアバイパス機能を利用している場合は、FXOS 2.4.1.238 にアップグレードする必要があります。2.4.1.238 より前の FXOS リリースでは、障害イベントが発生していてもポートがバイパス状態になる可能性があります。その場合、Firepower Management Center を使用してポートをスタンバイモードに戻す必要があります。
- FXOS 2.4(1) で、FIPS モードで IPSec セキュア チャネルを使用している場合は、IPSec ピア エンティティで RFC 7427 をサポートしている必要があります。

- FXOS 2.4(1) へのアップグレード後にセキュリティ モジュールを再初期化した場合、後で以前の FXOS リリースにダウングレードすると、その非互換のセキュリティ モジュールのディスク パーティションに関するエラー メッセージが表示されることがあります。この問題を解決するには、ダウングレード後にもう一度セキュリティ モジュールを再初期化する必要があります。
- Firepower 4110 または 4120 デバイス上で現在実行中の Firepower Threat Defense アプリケーションのサービス チェーンで Radware DefensePro (vDP) を設定すると、障害アラームが発生してインストールが失敗します。回避策として、Radware DefensePro アプリケーションをインストールする前に、Firepower Threat Defense アプリケーションインスタンスを停止します。この問題と回避策は、Firepower 4110 および 4120 デバイスでの Firepower Threat Defense を使用した、Radware DefensePro サービスチェーンのサポートされているすべてのリリースに適用されることに注意してください。
- ファームウェア アップグレード：最新のファームウェアを使用して Firepower 4100/9300 セキュリティアプライアンスをアップグレードすることを推奨します。ファームウェアの更新と各アップデートに含まれる修正のインストール方法については、<https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html> を参照してください。
- ネットワークまたはセキュリティ モジュールをアップグレードすると、特定の障害が生成され、自動的にクリアされます。これらには、「ホット スワップがサポートされていない」障害または「オンライン状態のときにモジュールが削除された」障害が含まれます。『Cisco Firepower 9300 Hardware Installation Guide』または『Cisco Firepower 4100 Series Hardware Installation Guide』に記載されている、適切な手順に従っている場合は、自動的に障害がクリアされます。追加のアクションは必要ありません。

アダプタ ブートローダのアップグレード

FXOS 2.4(1) には、セキュリティアプライアンスのセキュリティ モジュールアダプタを確認するための追加テストが含まれています。FXOS 2.4.1.101 以降をインストールすると、セキュリティ モジュール アダプタのファームウェアを更新する必要があることを示す重大な障害が次のように表示されることがあります。

「*Critical F1715 2017-05-11T11:43:33.121 339561 セキュリティモジュール 1 のアダプタ 1 は重要なファームウェア アップグレードが必要です。(Critical F1715 2017-05-11T11:43:33.121 339561 Adapter 1 on Security Module 1 requires a critical firmware upgrade.)* このリリースで発表された FXOS リリースノートのアダプタ ブートローダ アップグレードの手順を参照してください。(Please see Adapter Bootloader Upgrade instructions in the FXOS Release Notes posted with this release.)」

上記のメッセージを受信した場合は、次の手順を使用してアダプタのブートイメージを更新します。

1. Firepower セキュリティ アプライアンスの FXOS CLI に接続します。手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.4(1)』[英語] または『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.4(1)』[英語] の「Accessing the FXOS CLI」のトピックを参照してください。

- ブートイメージを更新するアダプタのアダプタ モードを入力します。

```
fxos-chassis# scope adapter 1/security_module_number/adapter_number
```

- 使用可能なアダプタ イメージを表示し、fxos-m83-8p40-cruzboot.4.0.1.62.bin がインストール可能であることを確認するには、**show image** を入力します。

```
fxos-chassis /chassis/server/adapter # show image
Name Type Version
```

```
-----
fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)
```

```
fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
```

- update boot-loader** と入力して、アダプタのブートイメージをバージョン 4.0.1.62 に更新します。

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may
cause adapter to become UNUSABLE!
After upgrade has completed, blade will be power cycled automatically
fxos-chassis /chassis/server/adapter* # commit-buffer
```

- 更新ステータスをモニタするには、**show boot-update status** と入力します。

```
fxos-chassis /chassis/server/adapter # show boot-update status
State: Updating
fxos-chassis /chassis/server/adapter # show boot-update status
State: Ready
```

- 更新が成功したことを確認するには、**show version detail** と入力します。



(注) **show version detail** の出力は、次の例とは異なる場合があります。ただし、Bootloader-Update-Status が「Ready」であり、Bootloader-Vers が 4.0(1.62) であることを確認します。

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
Running-Vers: 5.2(1.2)
Package-Vers: 2.2(2.17)
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.2(1.2)
Backup-Vers: 5.0(1.2)
Bootloader-Vers: 4.0(1.62)
```

システム要件

Firepower Chassis Manager には、次のブラウザを使用してアクセスできます。

- Mozilla Firefox : バージョン 42 以降
- Google Chrome : バージョン 47 以降

- Microsoft Internet Explorer : バージョン 11 以降

Mozilla Firefox バージョン 42、Google Chrome バージョン 47、および Internet Explorer バージョン 11 を使用して FXOS 2.4(1) をテストしました。これらのブラウザの他のバージョンも正常に動作することが想定されます。ただし、ブラウザに関連する問題が発生した場合は、テストされたバージョンのいずれかに戻すことをお勧めします。

アップグレード手順

現在 FXOS 2.0(1) 以降のビルドを実行している場合は、Firepower 9300 または Firepower 4100 シリーズセキュリティ アプライアンスを FXOS 2.4(1.214) にアップグレードできます。

アップグレード手順については、『[Cisco Firepower 4100/9300 Upgrade Guide](#)』を参照してください。

インストール上の注意事項

- FXOS 2.4(1) へのアップグレードには最大 45 分かかる場合があります。適切なアップグレード活動の計画を行ってください。
- スタンドアロン論理デバイスを実行中の Firepower 9300 または Firepower 4100 シリーズセキュリティ アプライアンスをアップグレードしている場合、またはシャーシ内クラスタを実行中の Firepower 9300 セキュリティ アプライアンスをアップグレードしている場合、アップグレード中にデバイスを介してトラフィックは通過しません。
- シャーシ間クラスタに属する Firepower 9300 または Firepower 4100 シリーズセキュリティ アプライアンスをアップグレードしている場合、アップグレード中にアップグレードされたデバイスを介してトラフィックは通過しません。ただし、クラスタ内の他のデバイスではトラフィックは通過し続けます。
- FXOS イメージのダウングレードは公式にはサポートされていません。シスコがサポートする唯一の FXOS のイメージバージョンのダウングレード方法は、デバイスの完全な再イメージ化を実行することです。

未解決のバグおよび解決されたバグ

このリリースで未解決のバグおよび解決済みのバグには、Cisco Bug Search Tool を使用してアクセスできます。この Web ベース ツールから、この製品やその他のシスコハードウェアおよびソフトウェア製品でのバグと脆弱性に関する情報を保守するシスコ バグ トラッキング システムにアクセスできます。



- (注) Cisco Bug Search Tool にログインしてこのツールを使用するには、Cisco.com アカウントが必要です。アカウントがない場合は、[アカウントを登録](#)できます。

Cisco Bug Search Tool の詳細については、[Bug Search Tool \(BST\) ヘルプおよび FAQ](#) を参照してください。

未解決のバグ

次の表に、このリリースノートの発行時点で未解決のバグを示します。

表 1: FXOS 2.4(1)に影響を与える未解決のバグ

ID	説明
CSCUw31077	インターフェイスに適用されたフィルタを検証する必要がある
CSCUx63101	メモリ アレイのすべてのメモリは、操作可能なカラムで unknown と表示される
CSCUx77947	データが高レートで送信されたときに pcap ファイルサイズが正しく更新されない
CSCUx98517	VDP の非修飾データ ポートは、シャーシマネージャから許可する必要がある
CSCUz93180	検証に失敗した場合、AAA LDAP 設定で情報が保持されない
CSCvc03494	Radware vDP を APSolute Vision に追加することはできない。回避策として、デバイス ドライバを手動でダウンロードして、それをビジョンにインストールする必要がある。
CSCvc44522	管理コントローラ サーバ 1/1 のログ容量が非常に少なくなっていることを示す警告
CSCvd90177	FXOS 2.2.1.57 を使用して QP-D で MIO リロードを実行した後に、ブレードが障害状態になった
CSCvj96380	スイッチバイパスの有効化が失敗した場合、SAM カプラーによって強制的に FTW バイパスが行われます
CSCvk46399	MIO の再起動後に svc_sam_bladeAG_log コアが表示されます
CSCvk61563	KP ASA で、再起動後に /root/.ssh が作成されません
CSCvm66013	再起動中に MIO がハングしました。カーネルパニックの問題が検出されました
CSCvm84592	キャプチャセッションの [Edit Session] が実行されると、フィルタ設定が失われます
CSCvo64240	警告アラーム「Service profile ssp-sprof-2 is not associated」を確認できません。
CSCvo68997	FXOS ip ブロックを回復済み sam.configure にできません

FXOS 2.4.1.273 で解決されたバグ

次の表に、FXOS 2.4.1.273 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 2: FXOS 2.4.1.273 で解決されたバグ

不具合 ID 番号	説明
CSCvt31171	Firepower 4100/9300 シリーズ アプライアンス向け Cisco FXOS ソフトウェアのセキュアブートバイパスの脆弱性
CSCvt31177	FP 1000/2100 シリーズアプライアンス向け Cisco ASA および FTD ソフトウェアのセキュアブートバイパスの脆弱性
CSCvt31178	FP 1000/2100 シリーズ アプライアンス向け Cisco ASA および FTD ソフトウェアのセキュアブートバイパスの脆弱性
CSCvv96092	Cisco FXOS および NX-OS ソフトウェアの UDLD DoS と任意のコード実行の脆弱性
CSCvw38984	Cisco FXOS および NX-OS ソフトウェアの UDLD DoS と任意のコード実行の脆弱性
CSCvx13861	Firepower 9300/4100 Supervisor での QuoVadis ルート CA のデコミッション
CSCvx88998	2.3.1.213 で「System does not allow 16 TPs (システムは 16 TP を許可しません)」
CSCvx90804	MIO SSD が誤ったファームウェアバージョンにアップグレードされた
CSCvo14325	ファームウェア アップグレードがグレースフルの場合に MIO がリブートすることを確認
CSCvv05277	FXOS での SSD のファームウェア アップグレードのサポートが必要

FXOS 2.4.1.268 で解決されたバグ

次の表に、FXOS 2.4.1.268 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 3: FXOS 2.4.1.268 で解決されたバグ

ID	説明
CSCvu27487	FXOS ASA の競合状態が原因でクラスタへの参加が失敗し、ネットワークが停止する

FXOS 2.4.1.266 で解決されたバグ

次の表に、FXOS 2.4.1.266 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 4: FXOS 2.4.1.266 で解決されたバグ

ID	説明
CSCvi48404	License Manager による Firepower シャーシのリロード
CSCvj85155	4100 および 9300 Chassis Manager でログイン前のバナーが削除される
CSCvn11962	FXOS で、4 つの NTP サーバを追加すると、1 つの NTP サーバが「到達不能または無効な NTP サーバ (Unreachable Or Invalid NTP Server)」としてランダムに表示される
CSCvq12258	FXOS のアップグレード中にストレージコントローラのファームウェアバージョンがアップグレードされない
CSCvr01651	シャーシの再起動後にデータインターフェイスが遅延して起動します。
CSCvr04845	最大数の https ip-blocks が設定された FXOS シャーシのリロード後に DME がクラッシュします。
CSCvr15083	Cisco FXOS、IOS XR、および NX-OS ソフトウェアの Cisco Discovery Protocol における DoS 脆弱性
CSCvr24920	FPR-4110 : feature-mgr プロセスで FXOS CLI がクラッシュする
CSCvr37151	Cisco FXOS および NX-OS CDP の任意のコードの実行と DoS の脆弱性
CSCvr40573	FPR-4100 : fwm hap がリセットされて FXOS CLI がクラッシュする
CSCvs23575	M5 ブレードでのメモリーリークが原因で BladeAG がリロードされる
CSCvs34851	継続的なリンクフラッピングにより、snm_log コアファイルが生成される
CSCvs90447	FXOS 8x1G FTW の継続的なリンクフラッピング
CSCvs92044	ポートチャネルメンバーインターフェイスのフラップによる FXOS L3 出力オブジェクトのリソースリーク
CSCvt06091	FXOS が show interface から WSP-Q40GLR4L トランシーバをタイプ QSFP-40G-LR4 として表示する

ID	説明
CSCvt34160	FPR9K-NM-4X40G で WSP-Q40GLR4L トランシーバを使用すると、再起動後に「リンクが接続されていない (Link not connected)」というエラーが発生する
CSCvt39897	FP4120 svc_sam_dcosAG がクラッシュタイプ 139 でクラッシュする

FXOS 2.4.1.252 で解決されたバグ

次の表に、FXOS 2.4.1.252 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 5: FXOS 2.4.1.252 で解決されたバグ

ID	説明
CSCvs39368	Firepower 9300/4100 のメモリリークが原因で DME のプロセスがクラッシュします。

FXOS 2.4.1.249 で解決されたバグ

次の表に、FXOS 2.4.1.249 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 6: FXOS 2.4.1.249 で解決されたバグ

ID	説明
CSCvh68895	FPR9300 に余分な「ローカルディスク3」が表示される
CSCvk70849	パスワードが 32 文字を超えている場合に、「ログインできません。認証に失敗しました (Unable to Login. Authentication failed)」というエラーで、FCM GUI 認証が失敗する
CSCvm76266	スレッド名 : cli_xml_server での Lina のトレースバック
CSCvm87556	92.5(1.232) のアップグレード中にファームウェアの自動インストール状態のエラーが発生する
CSCvm96265	有効な HTTP オプションが無効になります
CSCvn24594	NTPD を開始する前に、ブレード sysclock の NTPDATE update をスーパーバイザから追加する
CSCvn45138	シャーシマネージャの UI からブートストラップを変更した後に FTD の登録が解除される
CSCvo40340	FPR4100 : ファン OIR 後にシリアル、モデル、およびベンダーが黒で表示される

ID	説明
CSCvo79145	k9.2.4.1.222.SPA から k9.2.6.1.118.SPA へのアップグレード時に FTD が起動しない (ディスククォータの問題)
CSCvp35769	[ciam] Apache HTTP Server の URL 正規化に関する DoS 攻撃の脆弱性
CSCvq17910	アプリケーションの再起動またはクラスタの再参加時にシャーシでマルチキャスト MAC がプログラミングされない
CSCvq19641	TCP_SACK に対する Firepower 4K/9K スーパーバイザの評価
CSCvq33916	FP 4100 とスイッチとの間 (40Gb BiDi から 40/100Gb BiDi への場合) のリンクダウン

FXOS 2.4.1.244 で解決されたバグ

次の表に、FXOS 2.4.1.244 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 7: FXOS 2.4.1.244 で解決されたバグ

ID	説明
CSCvn77125	FXOS : copy コマンドでワイルドカードを使用して複数のファイルを転送できる必要がある
CSCvo85861	リンクステートの伝達が FTD CLI に表示されない
CSCvo90987	カスタマー ユニット上の bcm_usd.log ファイルに関するリンクダウン/リンクフラップの問題をデバッグするための機能拡張
CSCvp10674	vDP をインストールして FXOS をバージョン 2.4.1 にアップグレードした後、FTD がオンラインにならない場合があります。
CSCvp15176	Firepower デバイスにインストールされたアプリケーションが通信障害を報告し、それ自体をアクティブ/マスターとみなす場合がある
CSCvp21561	Cruz カーネルパッチと Cruz カーネルバージョン間の互換性がないために Cruz アダプタがクラッシュする
CSCvp40260	STP および FC フレームが SUP CPU に送信されない
CSCvp56801	4100 上にインスタンスが 1 つしかない場合に 'show tech-support module 1 app-instance <appname> <identifier>' が失敗する
CSCvp83437	ローカルアカウントによるシリアルコンソールログインが成功しても、すぐにログインプロンプトに戻る

FXOS 2.4.1.238 で解決されたバグ

次の表に、FXOS 2.4.1.238 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 8: FXOS 2.4.1.238 で解決されたバグ

ID	説明
CSCvk47441	FXOS 4100/9300 : FXOS OOB 管理ルーティング テーブルで icmp リダイレクトが永続的にスタックする
CSCvk60985	マシンチェックイベントがログに記録されました。ハードウェアの問題が考えられます。FXOS ブレード : mcelog のサポート
CSCvm72541	ポートチャンネルのステータスが down の場合、interfaceMapping メッセージの速度が 0 になる
CSCvn46577	FXOS への SSH セッションの一部が、絶対/セッション タイムアウトによってタイムアウトしない
CSCvn98401	/opt/cisco/platform/logs/corruptConfigs 内に多くの 0 バイトファイルがあり、LACP の問題が発生して不安定になる
CSCvo29067	FXOS のアップグレードがハングし、DME コアファイルの生成を開始しました
CSCvo31071	ユニットがクラスタに再参加すると、トラフィックがドロップされます。
CSCvo56910	コンテキストに割り当てられた ASA サブインターフェイスが、断続的にフェールオーバー後に応答を停止します
CSCvo58998	FXOS Cruz アダプタが、論理デバイスによって送信されたデータを検証しないため、オフロードされたパケットがドロップされます。
CSCvo64091	SSP : 「Required external ports not available」のため、クラスタ スレーブ FTD プロビジョニングが失敗する
CSCvo75349	メモリの破損による FXOS ブレード CRUZ FW コアダンプ
CSCvo87116	AppAG recv_q で MTS メッセージがスタックしました
CSCvp09791	FXOS/FTD マルチインスタンス展開のマルチキャスト トラフィックの停止

FXOS 2.4.1.234 で解決されたバグ

次の表に、FXOS 2.4.1.234 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 9: FXOS 2.4.1.234 で解決されたバグ

ID	説明
CSCvn31390	コンピューティング プロセッサ PortSmash サイドチャンネル情報開示の脆弱性

ID	説明
CSCvn42582	リブート後にFXOSの「エクスポートをトリガーするリマインダ」が無効から有効に変更される
CSCvn48162	NTP通信エラーにより、iptablesでエントリの重複が発生し、HBエラーが発生する可能性がある
CSCvn56156	分類子テーブルのエントリが破損しているため、FXOSプラットフォームでサイレントパケットのドロップが発生することがある
CSCvn77641	SSPの障害が発生したワイヤポートは回復できない
CSCvn78014	グレースフルシャットダウンがデータポートで動作していない
CSCvn90677	FTDのインストール時に、ディスクパーティションのサイズを設定すると、何も表示せず失敗することがある
CSCvn90701	FTDのインストール中に発生したエラーはログに記録されない
CSCvn93793	SSD障害が発生した場合、フェールオーバーは発生しません
CSCvo10712	cspCfgXmlが破損している場合、SMAは1分ごとに新しいファイルを作成する
CSCvo28623	アップグレードに失敗した後にssp_admin_status.shが残ったメタデータjsonファイルを検出する
CSCvo28634	MIOがアプリケーションインスタンスに誤ったステータスを報告する
CSCvo30356	アップグレード後にポートチャネルが中断状態になっています。
CSCvo44029	FTDがまだ稼働しているときに、ワイヤポートペアがバイパス状態に入れません

FXOS 2.4.1.222 で解決されたバグ

次の表に、FXOS 2.4.1.222 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 10: FXOS 2.4.1.222 で解決されたバグ

ID	説明
CSCvm53282	FTD: ICMPリダイレクトによって追加されたルーティングテーブルが、ルーティングテーブルのキャッシュ内で永続的にスタックする
CSCvn23221	ecpumgrアサーションパニックによりcruzASICがクラッシュする
CSCvn36413	特定のバージョン管理形式/命名に関するアップグレード-リカバリのコーナーケース

FXOS 2.4.1.214 で解決されたバグ

次の表に、FXOS 2.4.1.214 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 11: FXOS 2.4.1.214 で解決されたバグ

ID	説明
CSCvg72548	Maverick のフロントおよびバックプレーンのパケットキャプチャでダブルVLAN ヘッダーが確認された
CSCvj06276	FXOS : snmpwalk によって正しいディスク使用率の値 (/dev/sdaX) を取得できない
CSCvk09976	同じインターフェイスの物理ポートとアプリケーションポートの両方に同じフィルタが適用されている場合、パケットがキャプチャされません
CSCvm21278	CVE-2018-5391 (FragmentSmack) の ssp の評価
CSCvm33545	システムのクロックの誤差が原因で、ndmain によってサービスダウンステータスが報告される
CSCvm73853	FXOS 2.2.2.26 で実行されているライセンス マネージャで Firepower シャーシがリロードされる
CSCvn02840	2.2.2 から 2.4.1 にアップグレードする際に sdExternalPortLink のポートタイプが不明です
CSCvn08869	FCM : イメージバージョンの取得が [Logical Devices] ページでハングします
CSCvn11768	アプリケーションインスタンスが参照している場合、アプリケーション CSP を削除できない
CSCvn17585	FXOS : dcosAG クラッシュによる予期しないリロード

FXOS 2.4.1.101 で解決されたバグ

次の表に、FXOS 2.4.1.101 で解決された、以前にリリースされた、またはお客様が発見したバグを示します。

表 12: FXOS 2.4.1.101 で解決されたバグ

ID	説明
CSCuy21573	シャーシ マネージャ : 更新ページでのソートが破損している
CSCvf38144	FXOS ホスト名には、デフォルトで「-A」が付加される
CSCvf70180	FCM は、1つのドメインだけではなく ASDM に DNS 検索ドメインリストを送信している
CSCvg57022	シャーシ マネージャ : ログイン詳細情報のタイムゾーンが正しくない

ID	説明
CSCvg57037	シャーシマネージャ：パスワードの「Set:Yes」または No が誤った場所に表示される（日本語版）
CSCvg62443	シャーシマネージャ UI ([論理デバイス (Logical Devices)] ページ) に、FTD デバイスの正しい IP が表示されない
CSCvg67730	ディスク容量が少ないため、不完全なブレードのテクニカルサポートを回避するようにブレード コア ファイルにキャップを配置する
CSCvg71168	asa は、障害が発生したセキュリティ モジュールでも開始される
CSCvg72559	IPv6 フィルタを使用したパケット キャプチャの有効化に失敗した

関連資料

Firepower 9300 または 4100 シリーズ セキュリティ アプライアンスおよび FXOS の詳細については、[Cisco FXOS ドキュメント一覧](#)を参照してください。

オンラインリソース

シスコは、ドキュメント、ソフトウェア、ツールのダウンロードのほか、バグを照会したり、サービス リクエストをオープンしたりするためのオンライン リソースを提供しています。これらのリソースは、Firepower ソフトウェアをインストールして設定したり、技術的問題を解決したりするために使用してください。

- シスコ サポート & ダウンロード サイト：<https://www.cisco.com/c/en/us/support/index.html>
- Cisco Bug Search Tool：<https://tools.cisco.com/bugsearch/>
- シスコ通知サービス：<https://www.cisco.com/cisco/support/notifications.html>

シスコ サポート & ダウンロード サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。

シスコへのお問い合わせ

上記のオンライン リソースでは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](#)

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービス リクエストを送信するには、[シスコサポート](#)にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

