Cisco Firepower 4100/9300 FXOS 2.7(1) リリースノート

初版：2019 年 11 月 12 日

最終更新：2021 年 5 月 17 日

Cisco Firepower 4100/9300 FXOS 2.7(1) リリースノート

このドキュメントには、Cisco Firepower eXtensible Operating System（FXOS）2.7(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。

最新情報

FXOS 2.7.1.131 の新機能

さまざまな問題を修正します（「FXOS 2.7.1.131 で解決されたバグ （10 ページ）」を参照）。

FXOS 2.7.1.122 の新機能

さまざまな問題を修正します（「FXOS 2.7.1.122 で解決されたバグ （12 ページ）」を参照）。

FXOS 2.7.1.106 の新機能

さまざまな問題を修正します（「FXOS 2.7.1.106 で解決されたバグ （12 ページ）」を参照）。

FXOS 2.7.1.98 の新機能

さまざまな問題を修正します（「FXOS 2.7.1.98 で解決されたバグ （13 ページ）」を参照）。

FXOS 2.7.1.92 の新機能

Cisco FXOS 2.7.1.92 には、次の新機能が導入されています。

表 *1 : FXOS 2.7.1.92* の新機能

機能	説明
ASA 9.13(1) のサポート	ASA 9.13.1 の詳細については、『Release Notes for the Cisco ASA Series, 9.13(x)』を参照してください。 バージョンの互換性の詳細については、『Cisco Firepower 4100/9300 FXOS Compatibility』を参照してください。
Firepower Threat Defense 6.5 のサポート	FTD 6.5 の詳細については、『Cisco Firepower Release Notes, Version 6.5.0』を参照してください。 バージョンの互換性の詳細については、『Cisco Firepower 4100/9300 FXOS Compatibility』を参照してください。

機能	説明
Firepower Device Manager を使用した FTD のサポート	ネイティブ FTD インスタンスを表示し、FDM 管理を指定できるようになりました。コンテナ インスタンスはサポートされていません。 新しい/変更されたコマンド： `scope ssa > enter logical-device > create mgmt-bootstrap >` **enter bootstrap-key MANAGEMENT_TYPE、set value LOCALLY_MANAGED** 。 新規/変更された [Firepower Chassis Manager] 画面： **Logical Devices > Add Device > Settings > Management type of application instance** 注：FTD 6.5.0 以降が必要です。
ハードウェアバイパス OIR のサポート	ハードウェア バイパス ネットワーク モジュールの活性挿抜（OIR）を実行できるようになりました。
複数のコンテナインスタンスの TLS 暗号化アクセラレーション	Firepower 4100/9300 シャーシ上の複数のコンテナインスタンス（最大 16 個）で TLS 暗号化アクセラレーションがサポートされるようになりました。以前は、モジュール/セキュリティエンジンごとに 1 つのコンテナインスタンスに対してのみ TLS 暗号化アクセラレーションを有効にすることができました。 新しいインスタンスでは、この機能がデフォルトで有効になっています。ただし、アップグレードによって既存のインスタンスのアクセラレーションが有効になることはありません。代わりに、**create hw-crypto** および **scope hw-crypto** CLI コマンドを使用します。詳細については、『Cisco Firepower 4100/9300 FXOS Command Reference』を参照してください。
ASA Security Service Exchange（SSE）テレメトリ	ネットワークで Cisco Success Network を有効にすると、デバイスの使用状況に関する情報と統計情報がシスコに提供され、テクニカルサポートの最適化に使用されます。ASA デバイスで収集されるテレメトリ データには、CPU、メモリ、ディスク、または帯域幅の使用状況、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。
500 VLAN のサポート（不測事態がない場合）	以前は、親インターフェイスの数とその他の導入の決定事項に応じて、250 から 500 の VLAN がサポートされていました。すべてのケースで 500 の VLAN を使用できるようになりました。
HTTP/HTTPS を使用したイメージのダウンロードのサポート	FXOS CLI および RestAPI 経由で HTTP/HTTPS を使用して FXOS イメージをダウンロードできるようになりました。
LLDP 構成に対する Chassis Manager のサポート	Firepower Chassis Manager インターフェイスを使用して LLDP を有効または無効にするオプションが追加されました。

機能	説明
新しい IPSec 暗号とアルゴリズム	次の IKE 暗号および ESP 暗号とアルゴリズムが追加されました。 • 暗号：aes192。既存の暗号には、aes128、aes256、aes128gcm16 などがあります。 • 疑似乱数関数（PRF）（IKE のみ）：prfsha384、prfsha512、prfsha256。既存の PRF：prfsha1。 • 整合性アルゴリズム：sha256、sha384、sha512、sha1_160。既存のアルゴリズム：sha1。 • Diffie-Hellman グループ：curve25519、ecp256、ecp384、ecp521、modp3072、modp4096。既存のグループ：modp2048。
SSH 認証の機能拡張	次の SSH サーバ暗号化アルゴリズムが追加されました。 • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com 次の SSH サーバ キー交換方式が追加されました。 • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
キーリングの ECDSA キー	キーリングに ECDSA キーを使用できるようになりました。以前は、RSA キーだけがサポートされていました。

機能	説明
ユーザパスワードの改善	次のようなパスワードセキュリティの改善が追加されました。 • ローカルユーザおよびリモートユーザのパスワードには最大 127 文字を使用できます。古い制限は 80 文字でした。 • デフォルトでは、強力なパスワード チェックが有効になっています。 • 管理者パスワードの設定を求めるプロンプトが表示されます。 • パスワードの有効期限切れ。 • パスワード再利用の制限。 • **set change-during-interval** コマンドを削除し、**set change-interval**、**set no-change-interval**、および **set history-count** コマンドの **disabled** オプションを追加しました。
アプライアンス コンポーネントの安全な消去	**erase secure** FXOS CLI コマンドを使用して、指定したアプライアンス コンポーネントを安全に消去できるようになりました。
さまざまな問題の修正	詳細については、FXOS 2.7.1.92 で解決されたバグ （13 ページ）を参照してください。

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

- CSCvq34340 を軽減するために、FTD デバイスをバージョン 6.5.0.2 にアップグレードすると、出力最適化機能が有効か無効かにかかわらず、出力最適化処理がオフになります。詳細については、『Cisco Firepower Release Notes, Version 6.5.0.x』を参照してください。
- FXOS 2.4(1) 以降で、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 2.6(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。

（注） 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ます。

- 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 2.7(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.*）」

こ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。この手順はトラフィックの中断につながる可能性があるため、ビジネスへの影響を避けるためにメンテナンス期間中に実行する必要があります。

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, 2.7(1)』または『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.7(1)』の「Accessing the FXOS CLI」のトピックを参照してください。
2. 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*
3. 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)
```

4. **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
```

5. 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
```

6. 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

Firepowerr 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 2.7(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を使用する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 2.7(1) 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 2.7(1) への単一シャーシのアップグレードには最大 45 ~ 60 分かかる場合があります。アップグレード時間は、ハードウェア、ソフトウェア、および展開の複雑度によって異なる場合があることに注意してください。適切なアップグレードの計画を行ってください。

  FXOS CLI で **scope system > show firmware monitor** を使用して、アップグレードの進行状況をモニタします。

- 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 *2 : FXOS 2.7(1)* に影響を与える未解決のバグ

ID	説明
CSCvq30293	FTD のバージョンのダウングレード後にブートストラップ設定が更新されません。
CSCvq47804	FTD のシャットダウン後に FXOS セキュリティモジュールの電源が投入されない
CSCvq87570	「hostname Transmission sts」スクリプトは、例外ホスト名 null が原因で失敗します。
CSCvr08375	ASA テレメトリ：登録ステージの前に、登録を確認するために別の FSM ステージを追加し、GET KEY を呼び出す
CSCvr18121	スロット 1 の認識後に show server status で「全体のステータス：ディスクに障害が発生しました（Overall status : Disc failed）」と表示される
CSCvr20219	6.4.0.4 から 6.5 へのアップグレード後に表示される、FXOS UI と FMC でのバージョンの不一致。

FXOS 2.7.1.143 で解決されたバグ

次の表に、FXOS 2.7.1.143 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 2.7.1.143* で解決されたバグ

ID	説明
CSCvu78537	FXOS マルチインスタンス fault F0479 仮想インターフェイスのリンクの状態はダウンしている
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
CSCvy23422	2.8.1.143 へのアップグレード後の QW:4112:FXOS トレースバックとリロード
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
CSCvu01873	CSP/SPA インストールファイル名のチェックで有効な文字が許可されない
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 2.7.1.131 で解決されたバグ

次の表に、FXOS 2.7.1.131 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 2.7.1.131* で解決されたバグ

ID	説明
CSCvj00997	「show open-network-ports」で FPR4100 シリーズの適切な情報が表示されていません
CSCvn78002	FPR4100/9300 スマートライセンスの失敗：エラー：ライセンスの内部エラー（68）
CSCvr68885	FXOS fault F0479 仮想インターフェイスのリンクの状態はダウンしています。
CSCvr74901	FXOS 論理デバイスブートストラップの AppAG エンコーディング

ID	説明
CSCvr79926	FXOS クラッシュ（cruz のトレースバック）
CSCvr88163	ファームウェアのアップグレードのために再起動がトリガーされた後に FPR9300 がハングする
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
CSCvs41966	リンクステートの伝達によりポートがダウンしている場合の FXOS でのインターフェイスステータスの不整合
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
CSCvt06743	FTW ウォッチドッグのキック遅延により、インラインセットがダウン/バイパス失敗する可能性がある
CSCvt17448	OSPF マルチキャスト MAC が l2-table から削除され、OSPF が失敗する
CSCvt17947	Firepower プラットフォームでのフェールオーバーと OSPF に専用の Rx リングが必要 - Cruz fix
CSCvt20235	Firepower 4100 シリーズのすべての FTW インターフェイスが同時にリンクフラップするが、まれにしか発生しない
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	FP 4120 svc_sam_dcosAG がクラッシュタイプ 139 でクラッシュする
CSCvt70832	fxos メモリ使用量への fpr4100 snmp ポーリングが CLI の出力と比較して誤った値を示す
CSCvt78809	VNIC の設定エラーが原因でインスタンスの起動に失敗した
CSCvt90558	9300/4100：シャーシソフトウェアのアップグレード後にポートチャネルがダウンする。

ID	説明
CSCvu11868	FPR9K-NM-4X40G で QSFP-40G-LR4 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
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
CSCvu76107	ASA アプリケーション インスタンスが監査ログまたはトリガーなしで再起動する
CSCvu78537	FXOS マルチインスタンス fault F0479 仮想インターフェイスのリンクの状態はダウンしている
CSCvu85589	Firepower 9300 FPR-NM-4X100G または FPR-NM-2X100G インターフェイスがポートチャネルメンバのトラフィックをブラックホール化する場合がある
CSCvu94706	FXOS が動的に外部マシンの Mac アドレスを学習すると停止する

FXOS 2.7.1.122 で解決されたバグ

次の表に、FXOS 2.7.1.122 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 2.7.1.122* で解決されたバグ

ID	説明
CSCvs23575	M5 ブレードでのメモリリークが原因で BladeAG がリロードされる

FXOS 2.7.1.106 で解決されたバグ

次の表に、FXOS 2.7.1.106 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 2.7.1.106* 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
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

ID	説明
CSCvq93572	外部認証を使用して FTD にユーザを追加することができません。
CSCvr02367	[ciam] Apache HTTP Server の mod_rewrite 設定のオープンなリダイレクトの脆弱性。
CSCvr82740	mgmt bootstrap PASSWORD を appAG ログに含めることができません。
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 2.7.1.98 で解決されたバグ

次の表に、FXOS 2.7.1.98 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 2.7.1.98* で解決されたバグ

ID	説明
CSCvp69229	OpenSSL 0 バイトレコードパディング Oracle の情報漏えいの脆弱性。
CSCvq31946	SFP（1G 光）の自動ネゴシエーションを無効化する機能。
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。
CSCvr24920	FPR-4110：feature-mgr プロセスで FXOS CLI がクラッシュする
CSCvr40573	FPR-4100：fwm hap がリセットされて FXOS CLI がクラッシュする

FXOS 2.7.1.92 で解決されたバグ

次の表に、FXOS 2.7.1.92 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 2.7.1.92* で解決されたバグ

ID	説明
CSCvd90177	FXOS 2.2.1.57 を使用して 4150 でのスーパーバイザのリロード後、セキュリティ モジュールが障害状態になりました。

ID	説明
CSCvj93832	ブレード上で「init 6」を使用した x86 電源の再投入後に、SM40/48/56 x86 cpu が起動しません
CSCvk26697	bcm_usd_log コア ファイルが 92.4.1.2889 イメージで検出されました。
CSCvn57429	Ftd アプリケーション インスタンスが INSTALL_ERROR で失敗したインストールでスタックします。アプリケーション内部スクリプト エラー。
CSCvo03589	アプリケーション エージェントのハートビートが、MI のシナリオで失われる可能性がある
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。
CSCvo55237	1 つのセキュリティ モジュールが稼働している場合でも、[global upgrade] ボタンがグレー表示されます。
CSCvo55809	2.6.1.112 + ASA 9.12.0.125 でのインストール状態で ASA アプリケーションがスタックします。
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。
CSCvo60117	割り当て済みとしてシャーシ マネージャに表示されている場合でも、インターフェイスが MI インスタンスに関連付けられていません。
CSCvo74625	管理ゲートウェイがデータインターフェイスとして設定されている場合、6.4.0 - IPv6 ルーティングが WM および KP で機能しない
CSCvo83802	再起動後にクラスタ ノードの管理接続が失われました。
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。
CSCvp44939	ASA アプリケーションが 2.6.1.157+9.12.1.111 でのインストール中にエラー「SMA_blade_reboot_inprogress」でスタックします。

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。