

# Cisco Firepower 4100/9300 FXOS 2.14(1) リリースノート

初版：2023年12月13日

このドキュメントには、Cisco Firepower eXtensible Operating System (FXOS) 2.14.1 のリリース情報が記載されています。

これら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) ユーザー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 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。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。

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。
- シャーシマネージャ：グラフィカル ユーザー 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、シャーシ機能の設定が簡素化されます。
- FXOS CLI：機能の設定、シャーシステータスのモニターリング、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：ユーザー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 2.14.1.143 の新機能

さまざまな問題の修正 ([FXOS 2.14.1.143 で解決されたバグ \(6 ページ\)](#)) の解決済みのバグを参照)

## FXOS 2.14.1 の新機能

Cisco FXOS 2.14.1 には、次の新機能が導入されています。

機能	説明
Secure Firewall Management Center で のシャーシレベルの正 常性アラートのモニタ リング	この機能により、シャーシレベルの正常性アラートについて、Management Center でシャーシをモニタリングできます。Management Center でシャーシレベルの正常性アラートをモニタリングするには、Management Center をシャーシのマネージャとして手動で設定してから、そのシャーシを Management Center に登録する必要があります。  新規/変更された CLI : <b>create device-manager manager_name hostname {hostname   ipv4_address   ipv6_address} nat-id nat_id</b>
統合ファームウェア アップグレード	FXOS ファームウェアアップグレードパッケージが、FXOS アップグレード時のファームウェア自動アップグレード用プラットフォームバンドルに統合されました。FXOS を最新バージョンにアップグレードすると、プラットフォームに応じたファームウェアパッケージが解凍され、スーパーバイザで実行されているファームウェアバージョンのチェックが行われます。ファームウェアバージョンがプラットフォームバンドルに統合されているファームウェアバージョンよりも古い場合、ユーザーが介入することなくファームウェアが自動アップグレードされます。  新規/変更された CLI : 新たに追加された CLI はありません。既存の <b>show firmware monitor</b> コマンドを使ってアップグレードプロセスをモニタリングできます。  含まれるファームウェアパッケージ : ファームウェアパッケージ 1.0.19
Secure Firewall シャー シマネージャシングル サインオン	Chassis Manager は、サードパーティの SAML 2.0 準拠 ID プロバイダー (IdP) で設定された外部ユーザーのシングルサインオン (SSO) をサポートするようになりました。  新規/変更されたページ :  <ul style="list-style-type: none"> <li>• [ログイン (Login) ] &gt; [シングルサインオン (SSO) (Single Sign-On (SSO)) ]</li> <li>• [プラットフォーム設定] (Platform Settings) &gt; [AAA] &gt; [シングルサインオン (SSO) (Single Sign-On (SSO)) ]</li> </ul>

## 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

- 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。
- Firepower 4110 または 4120 デバイス上で現在実行中の 脅威に対する防御 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、脅威に対する防御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 脅威に対する防御 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。

- 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』[英語] または 『Cisco Firepower 4100 Series Hardware Installation Guide』[英語] 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。
- FXOS 2.13 リリース以降、**set maxfailedlogins** コマンドは機能しなくなりました。値は引き続き設定できますが、無効なパスワードを使用して、設定済みの値よりも多くの回数ログインを試行しても、ロックアウトされません。互換性を確保するために、同様のコマンド **set max-login-attempts** を `scope security` で使用できます。このコマンドも一定回数のログイン失敗後のログインを防止しますが、すべてのユーザーに対して値を設定します。これらのコマンドは Firepower 2100 プラットフォームモードでのみ使用でき、他のプラットフォームには影響しません。

## システム要件

- シャーシマネージャにアクセスするには、次のブラウザが必要です。

- 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 2.14.1 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 バージョン 2.2(2) 以降を実行している場合は、Firepower 9300 シリーズまたは Firepower 4100 シリーズのセキュリティアプライアンスを FXOS 2.14.1 に直接アップグレードできます。Firepower 9300 シリーズまたは Firepower 4100 シリーズのセキュリティアプライアンスを FXOS 2.14.0 にアップグレードする前に、FXOS 2.2(2) にアップグレードするか、現在 FXOS 2.2(2) を実行していることを確認してください。

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

### インストール上の注意事項

- FXOS 2.14.1 以降、FXOS ファームウェアは FXOS ソフトウェアイメージにバンドルされています。FXOS のアップグレード時に、システムによりファームウェアが最新バージョンに自動アップグレードされます（該当する場合）。ファームウェアをアップグレードした場合、システムが 2 回再起動するため、FXOS のアップグレードにかかる合計時間は長くなります。

次の表に、ファームウェアアップグレードありの場合となしの場合それぞれのアップグレードにかかる時間を示します。

ファームウェアアップグレードを伴う FXOS アップグレード	所要時間 (分)
統合された FW の変更による FXOS アップグレードの開始	-
FXOS アップグレードによってトリガーされる 1 回目のリポート	およそ 9
FXOS アップグレード後の CLI (FW アップグレード前)	およそ 8
FW アップグレードによってトリガーされる 2 回目のリポート	およそ 1 ~ 20*
FXOS アップグレードおよび FW アップグレード後の CLI	およそ 8

ファームウェアアップグレードを伴う FXOS アップグレード	所要時間 (分)
ブレードがオンラインになる	およそ 13
アプリケーションがオンラインになる	およそ 10
合計	およそ 49 ~ 70 分

ファームウェア アップグレードを伴わない FXOS アップグレード	所要時間 (分)
統合されたファームウェアの変更による FXOS アップグレードの開始	-
FXOS アップグレードによってトリガーされるリポート	およそ 9
FXOS アップグレード後の CLI (ファームウェア アップグレード前)	およそ 8
ブレードがオンラインになる	およそ 13
アプリケーションがオンラインになる	およそ 10
合計	およそ 40 分

- 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。

## 解決済みのバグと未解決のバグ

このリリースで解決済みのバグと未解決のバグには、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、[Cisco.com](#) を参照してください。

Cisco Bug Search Tool の詳細については、[Bug Search Tool Help & FAQ \[英語\]](#) を参照してください。

### FXOS 2.14.1.143 で解決されたバグ

次の表に、FXOS 2.14.1.143 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。

ID	見出し
<a href="#">CSCwh19613</a>	SAML シナリオで Cisco ASA がクラッシュする。
<a href="#">CSCwi62683</a>	FXOS アドレス CVE-2023-48795 で CiscoSSH 1.13.46 にアップグレード。
<a href="#">CSCwi66007</a>	エントロピーの混合により NPU ビルドが中断される。
<a href="#">CSCwi76630</a>	FP2100/FP1000 : リロード後に Cisco ASA スマートライセンスが失われる。
<a href="#">CSCwj09999</a>	管理インターフェイスで FP 3100 MTU を変更し、リポートすると変更が維持されない (デフォルトの MTU に戻る)。
<a href="#">CSCwf61280</a>	SAML SSO ログインを介して FTD イメージをダウンロードできない。
<a href="#">CSCwh22888</a>	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。
<a href="#">CSCwh53276</a>	SSP MIO で CiscoSSL 1.1.1v.7.3.338-fips にアップグレード。
<a href="#">CSCwh68167</a>	SSP MIO に Jent ライブラリを追加。
<a href="#">CSCwi17589</a>	SSP MIO に Jent を導入。
<a href="#">CSCwi27924</a>	CiscoSSL でのエントロピーの混合の使用。
<a href="#">CSCwi36311</a>	SMA で SIGTERM に代えてキルツリー機能を使用。
<a href="#">CSCwe11124</a>	ENH : ファームウェア バンドル パッケージを FXOS MIO 更新パッケージに結合。
<a href="#">CSCwh33196</a>	SSP MIO : 署名イメージで swims トークンをサポート。
<a href="#">CSCwf62228</a>	9300/4100 プラットフォームでタイムゾーンが正しく機能しない。

## 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、『[Navigating the Cisco Firepower 4100/9300 FXOS Documentation](#)』 [英語] 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、FXOS ソフトウェアのインストールと設定、技術的問題の解決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](mailto: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](#) [英語] 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](#) [英語] 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](#) [英語] 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](#) [英語] 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。

## 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。