

Cisco Firepower 4100/9300 FXOS 2.16 リリースノート

最終更新：2026年4月21日

このドキュメントには、Cisco Firepower eXtensible Operating System (FXOS) 2.16.0 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。
- Firewall Chassis Manager：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 2.16.1.147 の新機能

さまざまな問題の修正 (FXOS 2.16.1.147 で解決済みのバグ (5 ページ) の解決済みのバグを参照)

FXOS 2.16.0.136 の新機能

さまざまな問題の修正 (FXOS 2.16.0.136 で解決済みのバグ (11 ページ) の解決済みのバグを参照)

FXOS 2.16.0 の新機能

Cisco FXOS 2.16.0 には、次の新機能が導入されています。

機能	説明
スマートトランスポートを使用するスマートライセンス	<p>スマートトランスポートは、スマートライセンスが Cisco Smart Software Manager (CSSM) サーバーとの通信に使用する新しいトランスポートメカニズムです。スマートトランスポートは、ダイレクト URL を使用してスマートライセンスメッセージを CSSM サーバーに送信します。Firepower 9300 シャーシでは、トランスポートタイプはデフォルトでスマートトランスポートに設定されています。FXOS CLI から Call Home に変更できます。</p> <p>新規および変更されたコマンド : scope transport、set transport、set transport smart、set transport-url、set transport callhome、show license transport</p> <p>変更されたページ : [システム (System)]>[ライセンス (Licensing)]>[サーバーの設定 (Server Configuration)]</p>

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。
- 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

- Firewall Chassis Manager 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 2.16.0 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 2.16.0 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 2.16.0 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 回目のリブート	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 回目のリブート	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
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
Total	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ブート	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
Total	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、[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 Help & FAQ \[英語\]](#) を参照してください。

FXOS 2.16.1.147 で解決済みのバグ

次の表に、FXOS 2.16.1.147 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
CSCWk82557	FDM を介した Threat Defense 7.4.2 へのアップグレードがブロックされる
CSCwo75483	SNMP エージェントとして使用される HA の Threat Defense 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
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
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
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

ID	見出し
CSCwo83389	FXOS の複数の場所での RSA キーの長さの違い
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
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
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、通信がセカンダリ Threat Defense に到達できない
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
CSCwb02701	FXOS がサーバーとの NTP 同期を再試行しない
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。
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
CSCwo91436	Cisco Secure Firewall 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
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
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。
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
CSCwm54190	Firepower 1010 および Cisco Secure Firewall 1200 : ASA アプリケーションインスタンスが起動失敗状態 START_FAILED でスタックし、CPU リソースを使用できない
CSCwq92373	Cisco Secure Firewall 4200 MI で、2つのアプリケーションが次の理由で [応答不可 (Not Responding)] 状態になった : アプリケーション インスタンス fd でエラーが発生した。SMA が次のエラーを報告した : 再起動ループによってインスタンス 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。
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
CSCwi48918	パートナーが低速レートを要求した場合でも、FXOS が高速な LACP PDU を送信する

ID	見出し
CSCWq60586	バンドルイメージ存在検証エラーにより、Threat Defense のアップグレードが失敗した
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
CSCWq36466	expat/xml FW が自身をリポートしたが、クラッシュ情報が生成されない
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
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
CSCWq26863	FP2110 - ntpd プロセスが常にクラッシュする
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
CSCwd40371	9300 の日付設定で 2012 年 1 月 1 日が示されているため、Management Center への 9300 Threat Defense の登録が失敗する
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
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
CSCWj98673	シャーシのリポ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
CSCwd92327	Firepower 2100 プラットフォームで、数字で始まるユーザーの外部認証が失敗する
CSCWp89969	ファイアウォールの再起動/リポート完了により遅延が発生する
CSCwo42102	show tech-support fprm detail コマンドが長時間スタックする
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
CSCwo86422	CCL を介した一方向通信により分割クラスターが発生する
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
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
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。

ID	見出し
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
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
CSCwq74986	FTD : 起動ループでインスタンスがスタック状態になる
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
CSCwm49782	sma 2nd cruz ハートビートのロギングを強化
CSCwb77894	Firepower 1000/2100 が ROMMON モードにブートすることがある
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
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
CSCwo57740	「 <code>{dsk_a}</code> がいないか操作できません。ブレードをリブートしています。 (<code>{dsk_a}</code> 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。
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
CSCwk62297	OpenSSH regreSSHion の脆弱性に対する SSP の評価
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
CSCwk67859	Threat Defense および FXOS : RADIUS プロトコルのスプーフィング脆弱性 (Blast-RADIUS) : 2024 年 7 月
CSCwq65955	Cisco Secure Firewall 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
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。
CSCwh19613	SAML シナリオで Cisco ASA がクラッシュする
CSCwi13062	show tech-support fprm detail を実行すると、コンソールにデバッグメッセージが表示される

ID	見出し
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
CSCwk88225	クリティカルな障害：[FSM:FAILED]：ユーザー設定 (FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwm50936	両端の Innolight QSFP で 100GB インターフェイスがフラップする
CSCwm34333	Threat Defense：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
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
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)」
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
CSCwn00093	ASA が snp_fp_shared_ingress でトレースバックしてリロードし、LINA コアを生成する場合がある
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
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
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
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
CSCwm96280	リセットボタンを押した後に Threat Defense デバイスが rommon モードでスタックする
CSCwq85986	Cisco Secure Firewall 4225 での、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。
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
CSCwm30872	入力に対する不十分な検証による脆弱性
CSCwn92248	Firepower 1100/2100：ポートチャネルインターフェイスが LACP でフラップする

ID	見出し
CSCwn46426	2100 プラットフォームの sh environment temperature に誤った温度値が表示される
CSCwq23394	Threat Defense が、mlx5 ドライバレベルで Azure クラウドでの通信をドロップする可能性がある
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
CSCwm30886	入力に対する不十分な検証による脆弱性
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
CSCwq31988	Firepower 1010 のすべてのインターフェイスでエラーが発生し、回線プロトコルがダウンしている（スーパーバイザに関連付けられていない）
CSCws07111	Cisco Secure Firewall 4200 : 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
CSCwn93411	snmpd サービスの障害による FXOS のリセットとリロード
CSCwi59271	FXOS での "End of script output before headers" syslog を抑制する
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
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
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
CSCwm35751	Cisco Secure Firewall 3100 で、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
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
CSCwp06890	接続すると、Finisar ポートの SFP_SFP_10G_25G_CSR_S V03 モジュールがバウンスします。
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
CSCwn59032	FPR 2130 プラットフォームモードで Cisco ASA 9.18.4.22 にアップグレードした後、Cisco Secure Firewall Chassis Manager GUI にアクセスできなくなった

ID	見出し
CSCwq95241	Heimdall PID がいないため FP2130 で再起動する
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。
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
CSCwe00713	Libtiff の tiffcrop ユーティリティでメモリーリークの欠陥が見つかった。この問題

FXOS 2.16.0.136 で解決済みのバグ

次の表に、FXOS 2.16.0.136 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
CSCwb77894	Firepower 1000/2100 が ROMMON モードにブートすることがある
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
CSCwm96280	リセットボタンを押した後に Threat Defense デバイスが rommon モードでスタックする
CSCwj98673	シャーシのレポ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
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
CSCwn21204	管理インターフェイスの SNMPv3 が断続的に応答せず、SNMP コアファイルが頻繁に生成される
CSCwm49154	マルチインスタンス展開での FXOS 障害 F1738。エラー : CSP_OP_ERROR。CSP 署名確認エラー
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
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
CSCwn46426	ASA 21xx : 「sh environment temperature」に誤った温度値が表示される

ID	見出し
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
CSCwm52973	Secure Firewall 3100 : 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
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
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
CSCwm49782	sma 2nd cruz ハートビートのロギングを強化
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
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、通信がセカンダリ Threat Defense に到達できない
CSCwm34333	Threat Defense : 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と重複する。

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 バグ検索ツール : <https://bst.cloudapps.cisco.com/bugsearch/search>
- 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
- 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 \[英語\]](#) 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。

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。