Cisco Firepower 4100/9300 FXOS リリースノート、2.14(2)

最終更新：2026 年 2 月 4 日

このドキュメントには、Cisco Firepower eXtensible Operating System（FXOS）2.14.2 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 2.14.2.138 の新機能

さまざまな問題の修正（FXOS 2.14.2.138 で解決済みのバグ （5 ページ）の解決済みのバグを参照）

FXOS 2.14.2.137 の新機能

さまざまな問題の修正（FXOS 2.14.2.137 で解決済みのバグ （5 ページ）の解決済みのバグを参照）

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 2.14.2 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る

  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*

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）
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 2.14.2.138 で解決済みのバグ

次の表に、FXOS 2.14.2.138 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
CSCwq21442	3RU MI クラスターインスタンスが、ベースラインまたは作成後にオフラインになる

FXOS 2.14.2.137 で解決済みのバグ

次の表に、FXOS 2.14.2.137 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
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
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。
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
CSCwi13134	Cisco Secure Firewall 3140 でハードウェアバイパスが期待どおりに機能しない
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起動することがある
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
CSCwi46641	インターフェイスのステータスを変更すると、Threat Defense Virtual 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
CSCwi55629	ASA/Threat Defense：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

ID	見出し
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）
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
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
CSCwi90399	ASA/Threat Defense システムクロックが 2023 年にリセットされる
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
CSCwj08015	FTW が Warwick 上の NM3 で動作しなくなった
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
CSCwj09999	管理インターフェイスで Cisco Secure Firewall 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）
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
CSCwj29599	ファームウェアのアップグレードが原因で、追加の再起動によりデバイスマネージャのブートストラップが中断される可能性がある
CSCwj30962	Cisco Secure Firewall 3140 3 MI インスタンスでアップグレードが失敗した
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
CSCwj38928	Cisco Secure Firewall 3100 シリーズデバイスで長い遅延が観察された
CSCwj49958	エラー「Failed to compute a hash value」が発生し、Crypto IPSEC ネゴシエーションが失敗する
CSCwj54717	外部認証の 14 文字を超える Radius 秘密鍵が展開されない（Cisco Secure Firewall 3100）
CSCwj56615	nghttp2 を使用した Wireshark パッケージの構築
CSCwj57435	古い logrotate ファイルをクリーンアップ
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
CSCwj77877	MI インスタンスを無効化/有効化すると「State Failed」になる
CSCwj79895	ENH ログ Firepower 4110（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
CSCwk41007	Cisco Cisco ASA/Threat Defense がトレースバックし、リロードすることがある

ID	見出し
CSCwk42676	仮想 Cisco Cisco ASA/Threat Defense 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
CSCwk48628	Threat Defense/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
CSCwk56467	Cisco Secure Firewall 3100 でロードすると、メモリデータの破損が検出され、継続的にブートされる
CSCwk62296	SSP OpenSSH regreSSHion の脆弱性に対処
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）
CSCwk71227	LDAP を使用して Firepower 2100 で実行されている Threat Defense 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
CSCwk75406	syslog を介した CC-mode 監査の Management Center が機能しない
CSCwk82557	デバイスマネージャを介した Threat Defense の 7.4.2 へのアップグレードがブロックされる
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
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
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
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
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
CSCwm40531	Threat Defense/ASA：Nexus 9K スイッチに接続されている場合、FP3100 の 1SXF インターフェイスがリンクダウン状態のままになる
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
CSCwm50936	両端の Innolight QSFP で 100GB インターフェイスがフラップする
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
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。

ID	見出し
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
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
CSCwn22610	コア生成を含む fs-daemon のハプリセット
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
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
CSCwn46426	ASA 21xx：「sh environment temperature」に誤った温度値が表示される
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
CSCwn86002	クイックコア機能に切り替えてもコア破損が引き続き発生する
CSCwn92248	Threat Defense Firepower 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
CSCwn98402	デバッグ可能性：アップグレード後に Firepower 2100 ポートチャネルインターフェイスがフラップする
CSCwo42102	show tech-support fprm detail コマンドが長時間スタックする
CSCwo64788	FPR9K-SM-56 クラスター：アプリケーション インストール ループで FTD がスタック状態になり、エラー「pooled address is unknown」が発生する
CSCwo65866	プライマリ Threat Defense インスタンスがシャーシマネージャから無効化されている場合のネットワーク障害
CSCwo71052	リロード後に Firepower 1010 Ethernet1/1 トランクポートが Vlan 通信を通過させない
CSCwo73467	ピアスイッチのリロードによって、またはアップグレード後にインターフェイス mac のスタックの問題が発生する
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
CSCwo94274	Firepower 4100/9300 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
CSCwp18885	「Kernel Panic」により Firepower 9300/4100 でトレースバックおよびリロードが発生する場合がある

ID	見出し
CSCwp83345	クラスター：マルチブレードシャーシで、特定の VLAN 宛てのブロードキャスト通信が送信されない
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
CSCwe92324	Cisco Secure Firewall 3100： SNMP ポーリングにおいて、実際には動作しているにもかかわらず、FanTray のステータスが誤ってダウンと報告される
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
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
CSCwh21382	FXOS：Add Time モジュールのトラブルシュートが tech_support_brief に生成された
CSCwh91976	Cisco Secure Firewall 4200 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
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
CSCwi14659	zeromq：詳細なロギングによりお客様のログが大量に生成されている
CSCwi36311	SMA で SIGTERM に代わりに kill tree 機能が使用される
CSCwi53987	SSL プロトコル設定でデバイスマネージャ GUI 証明書の設定が変更されたり、TLSv1.1 が無効化されたりしない
CSCwi55599	Cisco Secure Firewall 3100/4200 KC：有用性：PCIE リンクトレーニングがダウングレード状態になっている（QDMA モニター）
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
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
CSCwi67998	同じインスタンスの再展開後に、Cisco Secure Firewall 3100 MI シャーシでポリシーの展開に失敗する
CSCwi68581	300_os/001_verify_bundle.sh での 35 秒および 10 秒スリープタイムアウトの処理方法を改善する必要がある
CSCwi83821	"erase configuration" コマンドの実行後に表示される CLI メッセージを変更
CSCwi84615	一部の stdout ログが logrotate によってローテーションされない
CSCwj25629	FPR9K で「show tech-support module detail」を実行するとエラーが発生する

ID	見出し
CSCwj30576	14 文字以上の場合、Firepower 2100 RADIUS 共有秘密が更新されないため、新規フィールドが必要になる
CSCwj48801	Cisco Secure Firewall 4200 で長い遅延が観察された
CSCwj55081	リブート時に Cisco Secure Firewall 3100 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
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。
CSCwk14596	エラーメッセージ「can't read」を解消するための pidof パッチ
CSCwk14685	Threat Defense：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
CSCwk59458	Firepower 2100：デバッグログプロセスがハングし、スタック書き込み操作からの回復が妨げられる
CSCwk75035	Apache HTTP サーバー 2.4.59 以前のコアの脆弱性
CSCwk88225	クリティカルな障害：[FSM:FAILED]：ユーザー設定（FSM:sam:dme:AaaUserEpUpdateUserEp）
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
CSCwm10964	Cisco Secure Firewall 3100/4100 における 10/25g モジュールの CTLE ピーク値の更新
CSCwm49782	sma 2nd cruz ハートビートのロギングを強化
CSCwm51874	FXOS：通知デーモンメッセージが大量に届いてメッセージが40分ごとにローテーションする
CSCwm52264	障害「The password encryption key has not been set.」を削除またはクリアできない
CSCwm52973	Low End Cisco 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
CSCwm58723	Wind River から pam radius モジュールの新しいバージョンの統合を完了する
CSCwn21204	snmp バインド障害を特定するために、SAM ログにさらにロギング機能を追加する有用性
CSCwn44335	FXOS：ダウンロードコマンドが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

ID	見出し
CSCwn47308	FPR 1100/2100 および Cisco Secure Firewall 3100 のクリティカルな正常性アラート「user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)」
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
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
CSCwo26258	Cisco Secure Firewall 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
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
CSCwo83389	FXOS の複数の場所での RSA キーの長さの違い
CSCwo95140	Cisco Secure Firewall 1200 DT： RMU のログが Portmgr.out ファイルにダンプされる
CSCwp83219	ピアがリロード/フラップすると、Cisco Secure Firewall 3100（aldrin/aldrin2、CPSS 4.3.5）Intf Tx MAC のスタックの問題が発生する
CSCwc57341	インラインペアの FTW バイパス動作モードが間違って「Phy バイパス」になっている
CSCwc75659	Cisco Secure Firewall 3100/4200 管理サブインターフェイスが機能していない
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
CSCwe45584	Firepower 2130：FPRM の tech_support_brief に間違ったスペルがある
CSCwh36976	Firepower モジュール「show tech-support」で、ASA|LINA の非 ASCII 文字によりトレースバックが発生する可能性がある
CSCwh99647	ブートアップ中に、「Proxy thread creation successful」がエラーとして syslog メッセージに表示される
CSCwi21894	「zmq_poll return 1」ログが FTD コンソールに表示される
CSCwi93080	Threat Defense：メッセージファイルに「Ipc」からの大量のログが含まれる
CSCwj76075	python パッケージ pymonetdb をバージョン 1.8.2に更新する必要がある
CSCwd34920	過去 5 日間以上のデータを含めるために topout.log を保持する必要がある
CSCwq19936	シャーシマネージャ用の compile_email.py から acme 参照を削除

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。それらのリソースは、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。