

Cisco IOS XE 17.15.x (Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォーム) リリースノート

最終更新：2025 年 2 月 4 日

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジ プラットフォームについて

Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォームは、サービスの高速化、マルチレイヤセキュリティ、クラウドネイティブの俊敏性、エッジでのインテリジェンスを実現し、クラウドへの移行を促進するために設計された、クラス最高レベルの 5G 対応クラウドエッジプラットフォームです。

Cisco IOS XE SD-WAN ソフトウェアを搭載した Cisco Catalyst 8200 および Catalyst 8300 シリーズエッジプラットフォームを利用すれば、クラウド対応のセキュアな Cisco SD-WAN ソリューションをブランチに導入できます。Cisco Catalyst 8200 および Catalyst 8300 シリーズエッジプラットフォームは、高性能の統合 SD-WAN サービスに加えて、クラウドまたはオンプレミスのいずれでもセキュリティサービスおよびネットワークサービスを提供できる柔軟性を備えています。また、高密度の WAN ポートと冗長電源にも対応しています。Cisco Catalyst 8200 および Catalyst 8300 シリーズエッジプラットフォームには、モジュール密度の高いものから低いものまで各種インターフェイスオプションが用意されています。インターフェイスは、既存のさまざまな WAN、LAN、音声、コンピューティング モジュールと下位互換性があります。Catalyst 8500 シリーズプラットフォームは、Cisco IOS XE、完全にプログラム可能なソフトウェアアーキテクチャ、API をベースに大規模な自動化を促進し、ワークロードをクラウドに移行しながらゼロタッチ IT を実現します。また、Cisco Catalyst 8200 および Catalyst 8300 シリーズエッジプラットフォームは、Trustworthy ソリューション 2.0 インフラストラクチャも搭載しているため、整合性をチェックして脅威を修復することで、脅威や脆弱性からプラットフォームを保護します。

Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォームは、中規模～大規模の企業のブランチオフィスで統合 SD-WAN サービスを利用し、高い WAN IPSec パフォーマンスを実現するのに適しています。

Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォームの機能と仕様の詳細については、『Cisco Catalyst 8500 シリーズ エッジプラットフォーム データシート』を参照してください。



(注) このドキュメントのセクションは、特定のモデルへの参照が明示的に行われない限り、Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォームのすべてのモデルに適用されます。



(注) Cisco IOS XE 17.15.1a は、Cisco IOS XE 17.15.x リリースシリーズの Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジ プラットフォームの最初のリリースです。

製品に関する Field Notice

シスコでは、シスコ製品に関する重要な問題についてカスタマーとパートナーに通知するために、Field Notice を発行しています。通常それらの問題については、アップグレード、回避策、またはその他のユーザーアクションが必要になります。詳細については、<https://www.cisco.com/c/en/us/support/web/field-notice-overview.html> を参照してください。

シスコでは、ソフトウェアまたはハードウェアプラットフォームが影響を受けるかどうかを判定するために、フィールド通知を確認することを推奨します。Field Notice には <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories> からアクセスできます。

ハードウェアおよびソフトウェアの新機能および変更された機能

このリリースでは新しいハードウェア機能はありません。

Feature Navigator

Cisco Feature Navigator (CFN) を使用して、Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジプラットフォームのソフトウェア機能、プラットフォーム、およびソフトウェアイメージのサポートに関する情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfng.cisco.com/> に進みます。



Note CFN にアクセスするために cisco.com のアカウントは必要ありません。

ハードウェアの新機能および変更された機能

このリリースでは新しいハードウェア機能はありません。

Cisco IOS XE 17.15.1a のソフトウェアの新機能および変更された機能

表 1: Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジ プラットフォームのソフトウェア機能

機能	説明
HTTP または HTTPS ファイル転送の絶対パス	HTTP または HTTPS を使用したファイル転送機能では、 copy コマンドを使用してリモートサーバーからローカルデバイスにファイルをコピーできます。

機能	説明
Cisco Umbrella スコープログイン情報	Cisco IOS XE 17.15.1a 以降、この機能により、Umbrella SIG と Umbrella DNS の両方に新しい単一の Cisco Umbrella ログイン情報を定義および設定できます。
拡張 NAT 管理	Cisco IOS XE 17.15.1a 以降、拡張 NAT 管理機能により、ネットワークオペレータは CPU 使用率を基に ip nat translation max-entries cpu コマンドを使用して NAT 変換を制限することで、システムパフォーマンスを保護できます。また、この機能により ip nat settings redundancy optimized-data-sync コマンドを使用して、冗長システムでの NAT 同期の合理化を有効にすることもできます。
IPv6 データプレーンを介したセグメントルーティングの機能拡張	Cisco IOS XE 17.15.1a 以降、IPv6 データプレーンを介したセグメントルーティングでは、次の機能がサポートされます。 • IS-IS マイクロループ回避 • IS-IS ループフリー代替高速再ルーティング • トポロジに依存しない IS-IS ループフリー代替高速ルーティング • OAM トラフィック エンジニアリング
柔軟なギガビットイーサネットおよびファイバチャネルサービス	Cisco Coarse Wavelength-Division Multiplexing (CWDM) Small Form-Factor Pluggable (SFP) ソリューションにより、スケーラブルなギガビットイーサネットおよびファイバチャネルサービスを効率的に導入できます。これらのホットスワップ可能なトランシーバによって電気信号がシングルモード光ファイバインターフェイスに変換され、標準 SC コネクタを使用して CWDM パッシブ光システムに接続できるようになります。

機能	説明
SD-Routing ライセンス管理	このリリースでは、SD-Routing デバイスのライセンス管理サポートが導入されています。サポートされるライセンスワークフローには、ライセンスの割り当てや設定、ライセンスの使用、およびライセンス使用状況レポートが含まれます。これらのワークフローは、デバイスに応じて Cisco Catalyst SD-WAN Manager またはデバイス上で実行されます。
カスタム VRF を使用した Cisco SD-Routing デバイスでの複数の WAN インターフェイスの設定	1つ以上の WAN インターフェイスをホストするカスタム VRF を作成できるようになりました。この機能を拡張して、各 VRF が複数の WAN インターフェイスをホストする、複数のカスタム VRF を作成できます。これらの WAN インターフェイスは、Cisco Catalyst SD-WAN Manager への制御接続を確立するためのトランスポート インターフェイスとして機能するようになりました。複数の WAN インターフェイスを使用することで、制御接続とトランスポートトラフィックのルーティングにおける復元力が確保されます。
SD-Routing アラームのモニタリング	Cisco IOS XE 17.15.1a 以降、ネットワーク管理者は Cisco Catalyst SD-WAN Manager で SD-Routing デバイスのアラームをモニターできます。この機能により、SD-Routing デバイスで、制御コンポーネントやルータによって生成されたさまざまなアラームを記録および保存できます。詳細については、「 Cisco SD-Routing Command Reference Guide 」を参照してください。
SD-Routing デバイスの Network-Wide Path Insight	Network-Wide Path Insight (NWPI) は、ネットワーク管理者が Cisco SD-Routing の展開をモニターし、ネットワークとアプリケーションの問題を特定してネットワークを最適化できるツールです。

機能	説明
SD-Routing デバイスへの DMVPN の設定	Cisco DMVPN（ダイナミックマルチポイント VPN）は、すべてのデバイスを静的に設定することなく、複数のサイトで VPN ネットワークを構築するためのルーティング技術です。この技術では、トンネリングプロトコルと暗号化されたセキュリティ対策を使用して、サイト間に仮想接続（トンネル）を作成します。これらのトンネルは必要に応じて動的に作成されるため、効率的でコスト効果も高くなります。
SD-Routing デバイスへのフローレベル Flexible NetFlow サポートの有効化	フローレベルの Flexible NetFlow（FNF）機能を使用すると、NetFlow トラフィックをモニターし、アプリケーションレベルの統計情報を含むキャプチャされたすべてのフローレベルの FNF データを表示できます。
SD-Routing デバイスのシームレスなソフトウェアアップグレード	この機能では、シスコの既存のルーティングデバイスを Cisco SD-WAN インフラストラクチャにシームレスにアップグレードしてオンボーディングする方法について説明します。

ROMMON の互換性マトリクス

次の表は、Cisco IOS XE 17.15.x リリースでサポートされる ROMMON リリースをリスト表示しています。

表 2: Cisco Catalyst 8200 および Catalyst 8300 シリーズ エッジ プラットフォームでサポートされる最小および推奨 ROMMON リリース

プラットフォーム	Cisco IOS XE リリース	IOS XE でサポートされる最小 ROMMON リリース	IOS XE でサポートされる推奨 ROMMON リリース
Catalyst 8300 シリーズ エッジ プラットフォーム			
C8300-1N1S-4T2X 6T	17.15.1a	17.3(4.2r)	17.6(6r)
C8300-2N2S-4T2X 6T	17.15.1a	17.3(4.1r)	17.7(1r)
Catalyst 8200 シリーズ エッジ プラットフォーム			
C8200-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)
C8200L-1N-4T	17.15.1a	17.6(8.1r)	17.6(8.1r)



(注) Cisco Catalyst 8200 および 8200L シリーズ エッジ プラットフォームでは、ROMMON のバージョンが 17.6(8.1r) 未満の場合、次のいずれかの方法を使用してデバイスを IOS XE 17.15.1a にアップグレードできます。

- バンドルモードでは、デバイスを手動で Cisco IOS XE 17.12.4 にアップグレードします。これにより、ROMMON が 17.6(8.1r) に自動アップグレードされます。その後、デバイスを 17.15.1a にアップグレードするか、または
- バンドルモードで、ROMMON を 17.6(8.1r) に手動でアップグレードします。次に、デバイスを 17.15.1a にアップグレードできます。
- インストールモードでは、デバイスを IOS XE 17.15.1a にアップグレードできます。ROMMON は、デバイスの起動時に推奨バージョンに自動的にアップグレードされます。

Cisco Catalyst 8300 シリーズ エッジ プラットフォームでは、ROMMON のバージョンがサポートされている最小バージョン未満の場合に、デバイスを Cisco IOS XE 17.12.4 に手動でアップグレードします。これにより、ROMMON が推奨バージョンに自動アップグレードされます。次に、デバイスを 17.15.1a にアップグレードできます。

ROMmon のアップグレード

デバイスの ROMmon バージョンをアップグレードするには、次の手順を実行します。

1. **show rom-monitor r0** コマンドを使用して、ROMmon の既存のバージョンを確認します。新しいデバイスに Cisco IOS XE ソフトウェアをインストールする場合は、この手順をスキップします。
2. アップグレードする予定のデバイスに推奨される ROMmon ソフトウェアのバージョンを特定するには、「[ROMMON の互換性マトリクス](#)」を確認します。
3. <https://software.cisco.com/#> に移動して、ROMmon パッケージファイルをダウンロードします。
4. ROMmon ファイルを次のフラッシュドライブにコピーします。
copy ftp://username:password@IP addressROMmon package file flash:
5. 次のコマンドを使用して、ROMmon パッケージをアップグレードします。
upgrade rom-monitor filename bootflash:ROMmon package name all
6. **reload** コマンドを実行して、ROMmon アップグレードプロセスを完了します。
7. **show rom-monitor r0** コマンドを実行して、ROMmon ソフトウェアがアップグレードされていることを確認します。

Cisco IOS XE 17.15.1a の解決済みおよび未解決のバグ

Cisco IOS XE 17.15.1a で解決済みのバグ

ID	見出し
CSCwj51700	QFP の使用率が高い状態で ip nat settings pap limit ... bpa 機能を再設定/設定すると、CPP がクラッシュする。
CSCwk03686	負の値によるセグメンテーション違反が原因でクラッシュする。
CSCwk42634	%PMAN-0-PROCFAILCRIT: R0/0: pvp : クリティカルプロセス vip_confid_startup_sh has に失敗した (rc 6)。
CSCwk33173	EzPM アプリケーションパフォーマンス プロファイルにより TCP フローが長時間アイドル状態になり、メモリリークとクラッシュが発生する。
CSCwk16333	FNF フローの追加が原因で、デバイスの FTMD が繰り返しクラッシュする。
CSCwj96852	1 つの TLOC で受信した外部の NAT トラフィックの内部へのリターントラフィックが、他の TLOC から転送される。
CSCwj95633	SAIE アプリケーション - IOS XE ルータに表示するデータがない。
CSCwk39131	show sdwan ftm next-hop chain all を発行すると、デバイスがクラッシュする。
CSCwk37351	IOS XE ルータ : PVDM OIR 中に予期しないリブートが発生する。
CSCwk22225	ログイン情報機能テンプレートの更新を受信すると、FTMD がクラッシュする。
CSCwj48909	exp_sig_auto_tunnel スイートの実行中にトラッカーモジュールでコアダンプが確認された。
CSCwk23723	WRED 階層型 QoS での平均キュー計算が正しくない。
CSCwk45165	デバイスで fman_fp メモリリークが発生する。
CSCwj16153	Rx 側がダウンしても、シングルモードファイバの 10G 前面パネルポートがダウンしない。
CSCwj84949	FLEXVPN ハブアンドスポークのセットアップで IPsec トンネルが機能していないため、トラフィックが暗号化されない。
CSCwj90614	confd_cli の CPU 使用率が高い。
CSCwi81026	拡張環境での IPSec キー再生成中に BFD セッションがフラッピングする。

ID	見出し
CSCWk39268	sdn-network-infra-iwan の「hash sha256」が 17.11 より大きいため更新できない。
CSCWj76662	「ftmd」プロセスが原因でメモリ使用率が高くなる。
CSCWj92560	STCAPP コマンドがリロード後にデバイスから削除された。
CSCWk31715	NAT 設定を削除した後も、IP アドレスがルーティングテーブルに表示されたままになる。
CSCWk42253	コントローラモードのルータで HTTP 接続が 404 エラーにより失敗すると、予期しないリブートが発生する。
CSCWj42448	セルラーコントローラプロファイルが設定されている場合、APN パスワードがプレーンテキストで表示される。
CSCWk12524	ezManage モバイルアプリサービスによりデバイスがリロードされた。
CSCWk44078	GETVPN/新しい KEK RSA キーへの移行では、GM の再登録がトリガーされない。
CSCWi99454	FNF の test_tunnel_name_change_CSCvt57024 ケースが、pm5 のセッションが動作していないために失敗した。
CSCWk22942	一方のピアがもう一方のピアを介して PAT される場合、同じ送信元/宛先を持つ 2 つの IPSec SA を構築できない。
CSCWj96092	ICMP トラッカータイプのエコーからタイムスタンプへの変更により、トラッカーが失敗する。
CSCWj99827	「vdaemon」プロセスのクラッシュにより、デバイスが予期せずリロードする。
CSCWj23674	PPPOA に対応するダイヤラインターフェイスの最大 MTU が 1492 になる。
CSCWj02401	フローの大量処理中に admin tech を生成すると、ルータがリロードされる。
CSCWj40223	CISCO-SDWAN-APP-ROUTE-MIB で appRouteStatisticsTable シーケンスの順序が誤っているか、OS が誤った順序を返す。
CSCWk19725	show sdwan app-fwd フローに FNF キャッシュ制限が追加される。
CSCWj86794	NWPI トレースの処理中にデバイスがクラッシュする。
CSCWj67591	シャーシのアクティブ化が、新しい UUID を使用した 2 回目の再試行後にのみ有効になる。
CSCWj32347	DIA エンドポイントトラッカーが ECMP ルートで機能しない。

ID	見出し
CSCwj41728	CLI で http リンクを使用して TE エージェントをインストールできない

Cisco IOS CG 17.15.1a で未解決のバグ

ID	見出し
CSCwi76516	esim セルラー設定テンプレートの展開が失敗する。
CSCwk75733	カスタムアプリケーションが正しくプログラムされていない可能性がある。
CSCwk89256	デバイステンプレートのプッシュ後に IOS-XE 設定で速度の不一致が発生する。
CSCwm07994	スレッドのスタックによりルータがクラッシュする。
CSCwk85704	match traffic-category アドオンの CLI をプッシュできない。
CSCwj01917	アップグレード後にセルラーインターフェイス IP ADDRESS NEGOTIATED で不一致が発生する。
CSCwm01269	速度テストで、セカンダリルータの TLOC 拡張の方が良い結果が出る。
CSCwj76689	.bin をアップグレードするとデバイス設定が失われる。
CSCwk86355	「lost connection」というメッセージでファイル転送に失敗する。
CSCwk49806	プロセス NHRP のクラッシュにより、ルータが予期せずリブートした。
CSCwk81360	NAT スタティック変換の設定中にルータが予期せずリブートすることがある。
CSCwk62954	複数の「match address local interface <int>」が暗号プロファイルでプッシュされない。
CSCwk63722	PKI サーバーを有効化するとスタートアップ設定に失敗する。
CSCwk97092	EVC で shut/no shut を実行すると MKA セッションが起動しない。
CSCwm07564	data-policy local-tloc-list によって RTP メディアストリームが中断される。
CSCwk54544	ルールの順序が変更されると ZBFW TCAM が誤ってプログラミングされる。
CSCwk74298	アプリケーション通信エラーによりテンプレートのプッシュと一部の show コマンドでデバイスが拒否された。
CSCwk98578	GETVPN IPv6 クリプトマップがインターフェイス設定に表示されない。

ID	見出し
CSCWj42448	セルラーコントローラプロファイルが設定されている場合、APNパスワードがプレーンテキストで表示される。
CSCWk70630	デバイス証明書をインポートできない。
CSCWk97930	リンクローカルを送信元の IPv6 パケットが転送されると、クラッシュが発生する。
CSCWm13223	不正な形式の DMVPN-5-NHRP_RES_REPLY_IGNORE syslog により、IOSd でデバイスがクラッシュする。
CSCWk79454	デフォルトルートが削除されても、エンドポイントトラッカーが失敗しない。
CSCWk90014	ポート割り当ての失敗により、NAT/DIA トラフィックがドロップされる。
CSCWi87546	QFP CPP が rw_lock の待機中にスタックしたためにデバイスが予期せずリブートし、ロック ID 0 が解放される。
CSCWk61238	ステートフル IPSec が設定されている場合、リロード後に RRI スタティックでルートが入力されない。
CSCWm12851	デバイスで GETVPN のデフォルトのキー再生成アルゴリズムとして 3DES が使用される。
CSCWk95044	パケット複製リンクがフェールオーバーすると、SPA.smu.bin がドロップされる。
CSCWj87028	デバイスで DRE Opt の使用時にカスタムアプリの出力トラフィックが「unknown」と表示される。
CSCWk20995	サブインターフェイスを使用する PPPoE セッションがリブート後にスタックする。
CSCWm08545	集中型ポリシーポリサーが、サイトや vpn のリスト単位ではなく同じサイト上の PC 単位で機能する。
CSCWf62943	ディスク容量が原因でイメージの拡張が失敗した場合、システムイメージファイルが packages.conf に設定されない。
CSCWm00309	一連の操作を変更後、パケットが正しいデータポリシーに到達しない。

関連資料

- [Catalyst 8200 シリーズ エッジ プラットフォーム ハードウェア 設置ガイド](#)
- [Catalyst 8300 シリーズ エッジ プラットフォーム ハードウェア 設置ガイド](#)

- シスコ エンタープライズ ルーティング プラットフォーム向けポリシーを使用したスマートライセンス管理
- Cisco Catalyst 8300 および 8200 シリーズ エッジ プラットフォーム ソフトウェア コンフィギュレーションガイド

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。
- 重要な技術によって求めるビジネス成果を得るには、[Cisco Services](#) [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、[Cisco Support](#) [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 DevNet](#) [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](#) [英語] 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](#) [英語] にアクセスしてください。

シスコバグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、[トラブルシュート](#)および[アラート](#)を参照してください。

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。