

# Cisco IOS XE 17.14.x (Cisco Catalyst 8200 およびCatalyst 8300 シリーズ エッジプラットフォーム フォーム) リリースノート

---

初版 : 2024 年 4 月 29 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](http://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たい限り、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 17.14.1a は、Cisco IOS XE 17.14.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](https://www.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 17.14.1a 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
設定グループの機能拡張	<p>このリリースでは、Cisco SD-WAN Manager で次のサポートが導入されています。</p> <ul style="list-style-type: none"> <li>• トランスポートプロファイル</li> <li>• 管理プロファイル</li> <li>• サービス プロファイル</li> <li>• CLI プロファイル</li> <li>• ポリシー オブジェクト プロファイル</li> </ul>
セキュアサービスエッジの設定	<p>セキュアサービスエッジは、インターネットベースの脅威から保護するために、シームレスで透過的な、セキュアなダイレクトインターネットアクセス (DIA) を提供するクラウドソリューションです。このソリューションは、Cisco SD-WAN Manager を使用してポリシーグループで設定できます。</p>
SD ルーティングデバイスでの TLS トラフィックの復号のための SSL/TLS プロキシの設定	<p>SSL/TLS プロキシ機能を使用すると、自律デバイスをトランスペアレント SSL/TLS プロキシとして設定できます。このようなプロキシデバイスは、着信および発信 TLS トラフィックを復号して、Unified Threat Defense (UTD) によるインスペクションを有効にし、エンドツーエンドの暗号化によって隠されているリスクを特定できます。</p>
SD ルーティングデバイスの VPN ソリューションの設定のサポート	<p>このリリースでは、次の VPN ソリューションへのサポートが導入されています。</p> <ul style="list-style-type: none"> <li>• FlexVPN</li> <li>• GETVPN</li> <li>• DMVPN</li> <li>• L3VPN</li> </ul> <p>これらの VPN ソリューションは、Cisco SD-WAN Manager の <b>[Configuration] &gt; [Configuration Groups] &gt; [CLI Add-on Profile]</b> オプションを使用して設定できます。</p>

機能	説明
SD ルーティングデバイスの YANG 設定モデルのサポート	<p>このリリースでは、次の YANG 設定モデルのサポートが導入されています。</p> <ul style="list-style-type: none"> <li>• BGP</li> <li>• MPLS</li> <li>• RSVP</li> <li>• SNMP</li> <li>• AAA</li> <li>• QoS</li> <li>• ACL</li> <li>• DHCP</li> </ul>
SDルーティングデバイスでのモデル化されていないコマンドの表示	SDルーティングデバイスを展開すると、Cisco SD-WAN Manager でモデル化されていないコマンドを表示できます。デバイスが再起動すると、モデル化されていないコマンドのリストが再生成されます。
拡張 IS-IS 高速フラッディング	IS-IS 高速フラッディング機能は、レシーバの機能に基づいて LSP レートを動的に調整することで、LSP 伝送を最適化し、ネットワークコンバージェンスを高速化します。Cisco IOS XE 17.14.1a 以降では、 <b>router isis lsp-fast-flooding</b> コマンドを使用して IS-IS 高速フラッディングを設定できます。LSP 伝送は、同じ router isis コマンド内で <b>max-lsp-tx</b> 、 <b>psnp-interval</b> 、および <b>per-interface</b> などの引数を使用してさらにカスタマイズしたり、 <b>isis remote-psnp-delay</b> コマンドを使用して拡張したりすることができます。この機能はデフォルトでディセーブルになり、イネーブルにするには手動で設定する必要があります。
show reload-history コマンドの機能拡張	Cisco IOS XE 17.14.1a 以降、 <b>show reload-history</b> コマンドは <b>show reload history</b> に変更されています。コマンドの出力が更新され、クラッシュデータ、Cisco High Availability (HA) ステータス、およびソフトウェアバージョンが含まれるようになりました。

機能	説明
IP エンドポイントの遅延測定および活性モニタリング	この機能を使用すると、エンドツーエンドの遅延を測定し、指定した IPv4 または IPv6 エンドポイントのいずれかに対する活性をモニターできます。Cisco IOS XE 17.14.1a 以降では、 <b>performance-Measurement endpoint</b> コマンドおよび <b>performance-Measurement delay-profile endpoint</b> コマンドを使用してこの機能を設定できます。
MAP-T カスタマーエッジ (CE) のサポート	MAP-T カスタマーエッジ (CE) 機能は、IPv4 パケットを IPv6 パケットに、またはその逆に変換するために使用されます。Cisco IOS XE 17.14.1a 以降、MAP-T は CE デバイス上の既存の NAT44 プールベースの変換を使用してプライベート IPv4 アドレスをパブリック IPv4 アドレスに変換し、次に既存の NAT64 変換を使用して IPv4 ヘッダーを IPv6 ヘッダーに置き換えます。
電力使用量統計情報	この機能を使用すると、コンポーネントの名前と、デバイスの総電力使用量を含む電力消費量を表示できます。Cisco IOS XE 17.14.1a 以降では、 <b>show power usage</b> コマンドを使用して、デバイスの各コンポーネントの電力消費量とデバイスの総電力消費量を表示できます。
GET VPN を使用した Suite B 暗号のサポート	Cisco IOS XE 17.14.1a 以降、この機能拡張により、次のプラットフォームおよび対応するモデルで GET VPN を使用した Suite B 暗号のサポートが導入されます。  Cisco Catalyst 8300 シリーズ エッジプラットフォーム： <ul style="list-style-type: none"> <li>• C8300-1N1S-6T</li> <li>• C8300-1N1S-4T2X</li> <li>• C8300-2N2S-6T</li> <li>• C8300-2N2S-4T2X</li> </ul> Cisco Catalyst 8200 シリーズ エッジプラットフォーム： <ul style="list-style-type: none"> <li>• C8200-1N-4T</li> <li>• C8200L-1N-4T</li> </ul>

機能	説明
電圧と電流のメトリック	電源入力モジュール (PEM) センサーは、デバイスが安全で効率的なパラメータの範囲内で動作するように、電圧、電流、場合によっては温度など、電源のさまざまな側面のモニタリングを行うデバイス内の重要なコンポーネントです。Cisco IOS XE 17.14.1a 以降では、 <b>show environment</b> コマンドを使用して、デバイスの PEM センサーの読み取り値を mV (ミリボルト) および mA (ミリアンペア) 単位で表示できます。
トランスポート側での EtherChannel のロードバランシングのサポート	この機能は、 <b>port-channel load-balance-hash-algo</b> SD-WAN コマンドを使用して、Cisco IOS XE Catalyst SD-WAN デバイスのトランスポート側で EtherChannel のロードバランシングを設定する機能を追加します。
<b>CUBE の機能</b>	
TLS 1.3 を使用した Secure SIP のサポート	Cisco IOS XE 17.14.1a 以降、クライアントとサーバー間の通信のセキュリティは、 <b>Transport Layer Security (TLS) バージョン 1.3 および関連する暗号スイートのサポート</b> により強化されています。
<b>ライセンス機能</b>	
自律モードでの Tier 1 および 250 Mbps スループット設定の 500 Mbps 集約	このリリース以降、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能な場合、総スループットのロットリングが有効になります。アップストリームおよびダウンストリーム方向で、500 Mbps の制限内のトラフィックの分散が許可されます。以前のリリースでは、双方向スループットロットリングは T1 および 250 Mbps に適用され、スループットは各方向で 250 Mbps に制限されていました。

## ROMMON の互換性マトリクス

次の表は、Cisco IOS XE 17.14.x リリースでサポートされている 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それぞれ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 でサポートされている最小 ROMMON リリース	IOS XE でサポートされる推奨 ROMMON リリース
<b>Catalyst 8300 シリーズ エッジ プラットフォーム</b>			
C8300-1N1S-4T2X 6T	17.14.1a	17.3(1r)	17.6(6r)
C8300-2N2S-4T2X 6T	17.14.1a	17.3(1.2r)	17.6(6.1r)
<b>Catalyst 8200 シリーズ エッジ プラットフォーム</b>			
C8200-1N-4T	17.14.1a	17.4(1r)	17.6(6r)
C8200L-1N-4T	17.14.1a	17.5(1.1r)	17.6(6r)

## Cisco IOS XE 17.14.1a の解決済みおよび未解決のバグ

### Cisco IOS XE 17.14.1a で解決済みのバグ

ID	見出し
<a href="#">CSCwh94906</a>	デバイスのワイヤレス LAN コントローラ (WLC) で、Network Mobility Services Protocol (NMSP) に関連付けられたセグメンテーション障害が原因でクラッシュが発生する。
<a href="#">CSCwi03502</a>	「at#enadis=0」の後に「at#reboot」をデバイスに送信する CLI コマンドが作成される (これは Multi-PDN の設定時に必要)。
<a href="#">CSCwi49846</a>	SIG GRE トンネル設定が削除されると fcmd がクラッシュする。
<a href="#">CSCwi55725</a>	SDR CLI 設定グループの問題。
<a href="#">CSCwi61369</a>	SIGABRT が原因で cEdge デバイスが予期せずリロードされる可能性がある。
<a href="#">CSCwi35716</a>	AAR バックアップの優先カラーが 17.12.1 から期待どおりに機能しない。
<a href="#">CSCwi76516</a>	esim セルラー設定テンプレートの展開が失敗する。
<a href="#">CSCwi53306</a>	ZBFW HSL ログに不明な appID がある。
<a href="#">CSCwf08658</a>	非平衡状態にあり、対称 NAT がある場合、エッジデバイスにより BFD セッションがフラップする。
<a href="#">CSCwf84567</a>	Cisco SD-WAN コントローラへの再接続後に予期しないリロードが発生する。



ID	見出し
CSCwi14178	デバイスへの接続に失敗しました：x.x.x.x ポート：830 ユーザー：vmanage-admin エラー：接続に失敗しました。
CSCwj25493	rp_0_0 でクリティカルプロセス linux_iosd_image 障害が発生し、cEdge が 2 回クラッシュする。
CSCwi40603	Crypto IKMP プロセスでのメモリーク。
CSCwh36635	17.13 デバイス：confd/SMP がクラッシュする。コアファイルのデコードに失敗した。
CSCwi35177	多数の IPSec インターフェイスに関連付けられたインターフェイスの継続的なフラッピングが原因でデバイスがクラッシュする。
CSCwi60266	エンタープライズ証明書を持つ cEdge デバイスが、アップグレード後にコントローラとの制御接続を確立できない。
CSCwi67983	DNS クエリが失敗すると、Cisco Catalyst SD-WAN cEdge/トラッカーの状態ログが欠落する。
CSCwi53951	ユニキャスト MAC を持つパケットが、デバイスのリブート後にポートチャンネル L2 sub-intf でドロップされる。
CSCwb25507	CWMP：NBAR プロトコルパックバージョンのベンダー固有パラメータを追加。
CSCwi53549	cedge ルータが次の理由でクラッシュする：fp_0_0 でのクリティカルプロセス fman_fp_image 障害 (rc=134)。
CSCwi82548	IKEv2 クラスタロードバランサでクラッシュする。
CSCwi51381	ciscoSdwanBfdStateChange の TrapOID が MIB ファイルと異なる。
CSCwh09033	C-NIM-8T モジュールを使用してデバイスを起動できない。
CSCwi78365	アップグレード時にインストールされた証明書がトリミングされる。
CSCwi85293	ロードバランシングを使用する IKEv2 IPv6 クラスタでは、Front VRF (FVRF) が使用されている場合、クラスタ内のセカンダリノードがクラスタへの接続を確立できない。
CSCwi86698	SD ルーティングデバイスでシステム IP としてマルチキャストアドレスを使用する場合、エラーメッセージが表示されない。
CSCwi93784	(SWI ケース 01257768) 17.12.1a および 17.12.2 IOS を搭載した P-LTE-MNA では、FW アップグレードが正しく機能しない。

ID	見出し
<a href="#">CSCwj06622</a>	speedtest が原因で、コントローラ管理型 SD-WAN の IOS-XE でセグメンテーション障害とコアファイルが表示される。
<a href="#">CSCwi16111</a>	IPv6 TCP adjust-mss 設定を削除して再設定した後、正しく機能しない。
<a href="#">CSCwi62230</a>	SIG トンネルの場合、IG STATE に空白の値が表示される。
<a href="#">CSCwj27545</a>	ftmd が原因で cEdge デバイスがクラッシュする。
<a href="#">CSCwj70773</a>	最大数が制限されたポートチャネルインターフェイスを作成できない

## Cisco IOS CG 17.14.1a で未解決のバグ

ID	見出し
<a href="#">CSCwh86922</a>	EVC（イーサネット仮想回線）をディセーブルにしても、デバイス上のインターフェイスの元の MAC フィルタテーブルエントリが復元されない。
<a href="#">CSCwj48421</a>	%CRYPTO-4-RECVD_PKT_INV_SPI : decaps : 受信した IPsec パケットに無効な SPI がある。
<a href="#">CSCwj07584</a>	複数のインターフェイスで同じ HSRP 仮想 MAC アドレスを使用すると、デバイスでのデータ処理に問題が発生する可能性がある。
<a href="#">CSCwj02246</a>	インターフェイスで <b>no shutdown</b> コマンドを実行した後、デバイスの SFP EN（イネーブル）LED が点灯しない。
<a href="#">CSCwi29637</a>	デバイスの SFP インターフェイスはシャットダウンされるが、接続されたデバイスの対応するインターフェイスはアクティブなままとなる。
<a href="#">CSCwj09284</a>	SSL が原因で WLC が予期せず再起動する。
<a href="#">CSCwi98707</a>	音声ポートでの PCM キャプチャの収集中に、デバイスの NIM モジュールがリロードされる。
<a href="#">CSCwj40589</a>	DNS を使用するエンドポイントトラッカーは、DNS サーバーに到達できなくなると、ダウンメッセージの記録に失敗する。
<a href="#">CSCwj26085</a>	システム統合テスト（SIT）中に、Unified Threat Defense（UTD）が有効になっている場合、Cisco Catalyst SD-WAN コントローラおよび Cisco Catalyst SD-WAN マネージャの Transport Layer Security（TLS）の制御接続が試行中の状態になることが観察される。
<a href="#">CSCwj45177</a>	<b>show sdwan certificate validation</b> コマンドを実行しようとする、 「dmidecode: command not found」というエラーが表示される。

ID	見出し
<a href="#">CSCwj34578</a>	デバイスが NAT64 用に設定されており、Carrier Supporting Carrier (CsC) のカスタマーエッジ (CE) デバイスとしても機能している場合、NAT46 変換パケットがドロップされる。
<a href="#">CSCwi81026</a>	拡張環境での IPsec キーの再生成中に SDWAN BFD セッションがフラッピングする。
<a href="#">CSCwa67621</a>	fp_0_0でのクリティカルプロセス cpp_ha_top_level_serverの障害 (rc=69)。デバイスで重大な問題が発生しました。cpp_ha_top_level_serverという名前のプロセスが転送プロセッサ fp_0_0 で失敗し、リターンコードは 69 でした。
<a href="#">CSCwi59854</a>	特定のアプリケーション名を指定して <b>show sdwan policy service-path</b> コマンドを実行すると、一貫性のない結果が生成される。
<a href="#">CSCwj42448</a>	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。
<a href="#">CSCwj02661</a>	UTD 署名の更新に失敗し、デバイスが更新を記録していない。
<a href="#">CSCwj43905</a>	QFP-Ucode-Radium エラーによる予期しない再起動。
<a href="#">CSCwj02628</a>	コード 17.12.2 で実行されている cEdge デバイスの速度テストが機能しない。
<a href="#">CSCwi59834</a>	PDU1 の entSensorThresholdValue OID がデバイスにない。
<a href="#">CSCwi77159</a>	CISCO-SDWAN-APP-ROUTE-MIB の一部のオブジェクトが実装されない。
<a href="#">CSCwj40223</a>	CISCO-SDWAN-APP-ROUTE-MIB で、appRouteStatisticsTable 内のエントリのシーケンスが正しくないか、オペレーティングシステムが誤った順序でシーケンスを返す。
<a href="#">CSCwj30334</a>	使用済みブロックでマージしようとする、CVLA ucode がクラッシュする。
<a href="#">CSCwj34010</a>	[SITLite] : エッジデバイスのインターフェイスに TLOC 拡張 FIA がいないため、誤った制御が発生する。
<a href="#">CSCwj27108</a>	Cisco Catalyst SD-WAN Manager が、デフォルトルート間でトラフィックを均等に分散していない。
<a href="#">CSCwj49941</a>	一部の正規表現パターンで、dns-snoop-agent の TCAM エントリがすべてゼロである。
<a href="#">CSCwj31354</a>	サービスのタイムスタンプが原因でテンプレートのプッシュに失敗する。
<a href="#">CSCwj32347</a>	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
<a href="#">CSCwj13681</a>	デバイスは 64 個の FQDN パターンのみを保存できるが、設定では 64 個を超えるパターンが受け入れられる。

## 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](#) 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、[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 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。

### シスコバグ検索ツール

[Cisco 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 Cisco 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

シスコのテクニカルドキュメント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](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。