

Cisco IOS リリース 15.2(7)Ex (Cisco Catalyst 1000 シリーズ スイッチ) リリースノート

初版 : 2019 年 12 月 25 日

最終更新 : 2022 年 3 月 25 日

Cisco IOS リリース 15.2(7)Ex (Cisco Catalyst 1000 シリーズ スイッチ) リリースノート

はじめに

このリリースノートでは、Cisco Catalyst 1000 シリーズ スイッチ上の Cisco IOS リリース 15.2(7)Ex ソフトウェアの機能、変更点、および注意事項について説明します。

サポート対象ハードウェア

Cisco Catalyst 1000 シリーズ スイッチ : モデル番号

次の表に、サポートされるハードウェアモデルを示します。

スイッチ モデル	説明
Cisco Catalyst C1000 8 ポートおよび 16 ポートスイッチのモデルと説明	
C1000-8T-2G-L	10/100/1000 イーサネットポート 8 個、1 ギガビット Small Form-Factor Pluggable (SFP) モジュールアップリンク スロット 2 個または RJ-45 スロット 2 個。
C1000-8T-E-2G-L	外部電源 : 10/100/1000 イーサネットポート 8 個、1 ギガビット SFP モジュールアップリンク スロット 2 個または RJ-45 スロット 2 個。
C1000-8P-2G-L	10/100/1000 Power over Ethernet Plus (PoE+) ポート 8 個 (PoE 電力 67 W)、1 ギガビット SFP モジュールアップリンク スロット 2 個または RJ-45 スロット 2 個

スイッチ モデル	説明
C1000-8P-E-2G-L	外部電源 : 10/100/1000 PoE+ ポート 8 個 (PoE 電力 67 W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個または RJ-45 スロット 2 個。
C1000-8FP-2G-L	10/100/1000 PoE+ ポート 8 個 (PoE 電力 120 W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個または RJ-45 スロット 2 個。
C1000-8FP-E-2G-L	外部電源 : 10/100/1000 PoE+ ポート 8 個 (PoE 電力 120 W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個または RJ-45 スロット 2 個。
C1000-16T-2G-L	10/100/1000 イーサネット ポート 16 個、1 ギガビット Small Form-Factor Pluggable (SFP) モジュール アップリンク スロット 2 個。
C1000-16T-E-2G-L	外部電源 : 10/100/1000 イーサネット ポート 16 個、1 ギガビット SFP モジュール アップリンク スロット 2 個。
C1000-16P-2G-L	10/100/1000 PoE+ ポート 16 個 (PoE 電力 120W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個。
C1000-16P-E-2G-L	外部電源 : 10/100/1000 PoE+ ポート 16 個 (PoE 電力 120 W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個。
C1000-16FP-2G-L	10/100/1000 PoE+ ポート 16 個 (PoE 電力 240 W) 、1 ギガビット SFP モジュール アップリンク スロット 2 個。
Cisco Catalyst C1000 24 ポートおよび 48 ポートスイッチのモデルと説明	
C1000-24T-4G-L	10/100/1000 イーサネット ポート 24 個、1 ギガビット イーサネット SFP モジュール アップリンク スロット 4 個。
C1000-24P-4G-L	10/100/1000 PoE+ ポート (PoE バジェット 195 W) 24 個、1 ギガビット イーサネット SFP アップリンク モジュール スロット 4 個

スイッチ モデル	説明
C1000-24FP-4G-L	10/100/1000 PoE+ ポート (PoE 電力 370 W) 24 個、1 ギガビット SFP モジュール アプリンク スロット 4 個
C1000-48T-4G-L	10/100/1000 イーサネットポート 48 個、1 ギガビットイーサネット SFP モジュール アプリンク スロット 4 個
C1000-48P-4G-L	10/100/1000 PoE+ ポート (PoE 電力 370W) 48 個、1 ギガビット SFP+モジュール アプリンク スロット 4 個
C1000-48FP-4G-L	10/100/1000 PoE+ ポート (PoE 電力 740 W) 48 個、1 ギガビット SFP モジュール アプリンク スロット 4 個
C1000-24T-4X-L	10/100/1000 イーサネットポート 24 個、10 ギガビットイーサネット Small Form-Factor Pluggable Plus (SFP+) モジュール アプリンク スロット 4 個
C1000-24P-4X-L	10/100/1000 イーサネットポート 24 個、制限付き PoE+ ポート (PoE 電力 195 W) 、10 ギガビットイーサネット SFP+モジュール アプリンク スロット 4 個
C1000-24FP-4X-L	10/100/1000 PoE+ ポート (PoE 電力 370 W) 24 個、10 ギガビット SFP+ モジュール アプリンク スロット 4 個
C1000-48T-4X-L	10/100/1000 イーサネットポート 48 個、10 ギガビットイーサネット SFP+モジュール アプリンク スロット 4 個
C1000-48P-4X-L	10/100/1000 PoE+ ポート (PoE 電力 370 W) 48 個、10 ギガビット SFP+ モジュール アプリンク スロット 4 個
C1000-48FP-4X-L	10/100/1000 PoE+ ポート (PoE 電力 740 W) 48 個、10 ギガビット SFP+ モジュール アプリンク スロット 4 個
Cisco Catalyst C1000 24 ポートおよび 48 ポート FastEthernet スイッチのモデルと説明	

スイッチ モデル	説明
C1000FE-24T-4G-L	24 個の 10/100 ファストイーサネットポート。 2 個の 1 ギガビット SFP モジュールアップリンク スロットまたは 2 個の RJ-45 スロットコンボポート。2 個の 1 ギガビットイーサネット SFP モジュールアップリンク スロット。
C1000FE-24P-4G-L	24 個の 10/100 ファストイーサネットポート (195W の PoE バジェット)。2 個の 1 ギガビット SFP モジュールアップリンク スロットまたは 2 個の RJ-45 スロットコンボポート。2 個の 1 ギガビットイーサネット SFP モジュールアップリンク スロット。
C1000FE-48T-4G-L	48 個の 10/100 ファストイーサネットポート。 2 個の 1 ギガビット SFP モジュールアップリンク スロットまたは 2 個の RJ-45 スロットコンボポート。2 個の 1 ギガビットイーサネット SFP モジュールアップリンク スロット。
C1000FE-48P-4G-L	48 個の 10/100 ファストイーサネットポート (370W の PoE バジェット)。2 個の 1 ギガビット SFP モジュールアップリンク スロットまたは 2 個の RJ-45 スロットコンボポート。2 個の 1 ギガビットイーサネット SFP モジュールアップリンク スロット。

光モジュール

Catalyst 1000 シリーズスイッチは、さまざまなオプティカルモジュールをサポートしています。サポートされるオプティカルモジュールのリストは定期的に更新されます。最新の SFP+ および SFP モジュールの互換性に関する情報については、次の URL の表を参照してください。
<https://tmgmatrix.cisco.com>

スイッチの機能

運用の容易さ

このセクションには、Cisco Catalyst 1000 シリーズスイッチでサポートされている、運用の容易さを実現する機能を示します。

- Cisco Catalyst Smart Operations は、LAN の導入、設定、およびトラブルシューティングを簡素化する包括的な機能セットです。Catalyst Smart Operations は、Auto Smartports、Smart

Configuration、および Smart Troubleshooting で構成され、次のように運用効率を向上させます。

- **Cisco Auto Smartports** : デバイスがスイッチポートに接続されると自動設定を行います。これにより、ネットワーク上でのデバイスの自動検出とプラグアンドプレイが実現します。
- **Cisco Smart Troubleshooting** : 汎用オンライン診断 (GOLD) や オンボード障害ロギング (OBFL) など、スイッチ内で使用できるデバッグ診断コマンドとシステムヘルスチェックを豊富に提供します。
- **Auto Configuration** : エンドポイントデバイスのタイプに基づいてエンドポイントに提供するネットワークアクセスのレベルを決定します。
- インターフェイステンプレートは、複数のコマンドを同時に設定してターゲット (インターフェイスなど) に関連付けるメカニズムを提供します。インターフェイステンプレートは、特定のポートに適用できる設定またはポリシーのコンテナです。

ネットワーク セキュリティ

Cisco Catalyst 1000 シリーズスイッチは、ネットワークへのアクセスを制限して脅威を軽減するための幅広いセキュリティ機能を提供します。

- Cisco IOS リリース 15.2(7)E3 以降のリリースでは、SSH はネットワークに接続するためにデフォルトで有効になっており、Telnet はデフォルトで無効になっています。
- **ポートセキュリティ** : MAC アドレスに基づいてアクセスポートまたはトランクポートへのアクセスを保護します。学習される MAC アドレスの数を制限して、MAC アドレスのフラッドを阻止します。
- **動的ホスト制御プロトコル (DHCP) スヌーピング** : 信頼できないホストと DHCP サーバの間の信頼できない DHCP メッセージをフィルタリングします。
- **ダイナミック ARP インспекション (DAI)** : 不正な Address Resolution Protocol (ARP) 要求や応答を同じ VLAN 上の他のポートにリレーしないことにより、デバイスに対する悪意のある攻撃を回避します。
- **フレキシブル認証** : 802.1X、MAC 認証バイパス、Web 認証など、複数の認証機構を使用できます。
- **オープンモード** : 802.1X を運用する使いやすい環境を構築します。
- **RADIUS 認可変更 (CoA)** : 非同期ポリシー管理を可能にします。
- **標準および拡張アクセスコントロールリスト (ACL)** : ルーティングインターフェイス上に、コントロールプレーンおよびデータプレーンのトラフィックを対象とするセキュリティポリシーを定義します。IPv6 ACL を適用して IPv6 トラフィックをフィルタリングできます。

- ポートベースのACL：レイヤ2インターフェイスで個々のスイッチポートにセキュリティポリシーを適用できます。
- セキュアシェル (SSH) プロトコルおよび簡易ネットワーク管理プロトコルバージョン3 (SNMPv3) は、TelnetおよびSNMPセッション時の管理者トラフィックを暗号化してネットワークセキュリティを提供します。SSHプロトコル、Kerberos、およびSNMPv3暗号化バージョンでは、米国の輸出規制の関係で、特別な暗号化ソフトウェアが必要です。
- スイッチドポートアナライザ (SPAN) ポートでの双方向データサポート：Cisco Intrusion Detection を実現します。
- TACACS+ および RADIUS 認証：デバイスの集中管理を可能にし、不正なユーザーが構成を変更することを制限します。
- MAC アドレス通知：ネットワークに追加された (またはネットワークから削除された) ユーザーを管理者に通知します。
- コンソールアクセスへのマルチレベルのセキュリティ：不正なユーザーがデバイス構成を変更することを阻止します。
- ブリッジプロトコルデータユニット (BPDU) ガード：BPDU が受信されると、不測のトポロジループを回避するために、スパンニングツリー PortFast 対応インターフェイスをシャットダウンします。
- Internet Group Management Protocol (IGMP) フィルタリング：非加入者を除外することでマルチキャスト認証を実現し、同時に使用できるマルチキャストストリーム数をポート単位で制限します。
- 802.1x モニタモード：有線のユーザーまたはデバイスに影響を与えることなく、有線インフラストラクチャ全体で、監査モードで認証を有効にすることができます。これにより、IT管理者は、デバイスの再設定が必要な場合や、802.1x サプリカントがない場合に、アクセスおよびシステムメッセージのロギングを許可することで、802.1x の移行をスムーズに管理できます。

展開機能と制御機能

このセクションには、展開機能と制御機能を示します。

- オートネゴシエーション：すべてのポートで半二重または全二重伝送モードが自動的に選択され、帯域幅が最適化されます。
- Dynamic Host Configuration Protocol (DHCP)：ブートサーバによって複数のスイッチのDHCPを自動的に設定できるため、スイッチを容易に展開できます。
- ダイナミック トランキンング プロトコル (DTP)：全スイッチポートでダイナミックリンクを容易に設定できます。
- ポート集約プロトコル (PAgP)：Cisco Fast EtherChannel グループと Gigabit グループの作成を自動化します。

- Link Aggregation Control Protocol (LACP) : IEEE 802.3ad 準拠のデバイスでイーサネットチャネリングを作成できます。
- Link Aggregation Control Protocol (LACP) : IEEE 802.3ad 準拠のデバイスでイーサネットチャネリングを作成できます。
- Unidirectional Link Detection Protocol (UDLD) およびアグレッシブ UDLD : 誤った配線による単方向リンクを可能にします。また、インターフェイスでポート障害を検出して無効にすることもできます。
- IPv4 向けインターネットグループ管理プロトコル (IGMP) v1、v2、v3 スヌーピング。MLD v1 および v2 スヌーピング : マルチキャストストリームへのクライアントの参加と離脱を迅速に処理し、広帯域を必要とするビデオトラフィックを要求者に限定して配信できます。
- 音声 VLAN : 独立した VLAN で音声トラフィックを維持することによってテレフォニーの導入を簡素化し、管理とトラブルシューティングを容易にします。
- レイヤ2 traceroute : 送信元から宛先までのパケットの物理パスを識別することにより、トラブルシューティングが容易になります。
- Trivial File Transfer Protocol (TFTP) : 中央ロケーションからダウンロードすることにより、ソフトウェアアップグレードの管理コストが削減されます。
- Network Timing Protocol (NTP) : イントラネットのすべてのスイッチに対して、正確で一貫したタイムスタンプが提供されます。
- ユニキャスト、ブロードキャスト、およびマルチキャストトラフィックのストーム制御 : LAN でのパケットフラディングによるネットワークの中断を防ぎます。
- IEEE 802.1s/w 高速スパニングツリープロトコル (RSTP) およびマルチスパニングツリープロトコル (MSTP) : スパニングツリータイマーから独立した高速のスパニングツリーコンバージェンスを実現します。また、レイヤ2 ロードバランシングと分散処理の利点も得られます。
- スイッチポートの自動回復機能 (error-disable) : ネットワークエラーで無効になったリンクについて再アクティブ化を自動的に試行します。

QoS

このセクションには、Quality of Service (QoS) 機能を記載しています。

- マルチレイヤスイッチング (MLS) QoS : すべてのインターフェイスにきめ細かいポリシーとクラスを設定する機能を提供します。これらのポリシーには、ポリサー、マーカー、および分類子が含まれます。
- ポートごとに最大4つの出力キューをサポート : 非厳格プライオリティキューに2つのしきい値マーカーを使用したきめ細かいフローの分離を行います。
- 厳密に優先順位付けされたキューイング : 優先順位が最も高いパケットが、他のトラフィックよりも先に処理されるようにします。

- Shaped Round Robin (SRR) スケジューリング：パケットフローの優先順位付けを確立します。

Cisco IOS リリース 15.2(7)E1 のソフトウェア機能

新しいソフトウェア機能

機能名	説明
IPv6 RA ガード	ネットワークデバイスプラットフォームに到着した不要または不正なルータアドバタイズメント (RA) ガードメッセージを、ネットワーク管理者がブロックまたは拒否できるようにします。
拡張 PAgP を使用したデュアルアクティブ検出	デバイスが PAgP EtherChannel 経由で仮想スイッチングシステム (VSS) に接続されている場合、デュアルアクティブ検出用のこの EtherChannel 上で拡張 PAgP を使用して、自動的に VSS クライアントになります。
サンプリングされた Flow (sFlow)	スイッチやルータを含むデータネットワーク内のリアルタイムトラフィックをモニタできます。sFlow では、トラフィックをモニタするためにスイッチ上の sFlow エージェントソフトウェアでサンプリングメカニズムを使用して、サンプルデータを中央のデータコレクタに転送します。
EtherChannel 向けの IP ソースガードのサポート	EtherChannel インターフェイスで IP ソースガードを設定できます。
シングル IP 管理	1G および 10G SFP/SFP+ アップリンクポートをサポートする Cisco Catalyst 1000 シリーズスイッチは、シングル IP 管理に含めることができます。SFP/SFP+ ポートを使用して、さまざまなロケーションに配置されたボックスに光ケーブルで接続し、小型ボックスが異なるフロアやビルに配置されたグループを構成することができます。

機能名	説明
SSH ファイル転送プロトコル	デバイスは SSH File Transfer Protocol (SFTP) をサポートしています。SFTP クライアント機能は SSH コンポーネントの一部として提供され、対応するデバイスで常に有効になっています。したがって、適切な権限を持つ SFTP サーバのユーザは、デバイスとの間でファイルをコピーできます。

Cisco IOS リリース 15.2(7)E2 のソフトウェア機能

新しいソフトウェア機能

機能名	説明
Dying Gasp	Dying Gasp は、リセットまたは電源障害によりデバイスがダウンしようとしているときに生成される信号またはアラートです。システムは、電源障害が発生した後、管理者またはユーザーに通知する Dying Gasp メッセージを送信するために十分な残存電力を保持します。

Cisco IOS リリース 15.2(7)E3 のソフトウェア機能

新しいソフトウェア機能

機能名	説明
パスワードマスキングの有効化	シークレットマスキング機能を有効にするために、新しいキーワード masked-secret が username コマンドに追加されました。シークレットの入力はコンソールでマスクされ、デフォルトでタイプ9に変換されます。
アップグレードおよびダウングレード履歴の表示	コマンド show archive sw-upgrade history は、デバイスで実行されたアップグレードとダウングレードを表示します。 tar ファイルまたはバイナリファイルの TFTP による手動アップグレードは表示されないことに注意してください。

Cisco IOS リリース 15.2(7)E4 のソフトウェア機能

新しいソフトウェア機能

なし。

Cisco IOS リリース 15.2(7)E5 のソフトウェア機能

新しいソフトウェア機能

なし。

Cisco IOS リリース 15.2(7)E6 のソフトウェア機能

新しいソフトウェア機能

なし。

互換性マトリクス

次の表に、ソフトウェア互換性情報を示します。

Catalyst 1000 スイッチ	Cisco Identity Services Engine	Cisco Configuration Professional for Catalyst
Cisco IOS リリース 15.2(7)E1	2.7	1.7.1
Cisco IOS リリース 15.2(7)E3	3.0	1.8.0

Device Manager のシステム要件

次の表に、Cisco Configuration Professional for Catalyst を実行する PC のシステム要件（Web ブラウザのバージョンを含む）を示します。

最小ハードウェア要件

プロセッサ速度	DRAM	色数	解像度	フォントサイズ
233 MHz 以上 ¹	512 MB ²	256	1280 x 800	小

¹ 1 GHz を推奨

² 1 GB DRAM を推奨

ソフトウェア要件

オペレーティング システム

- Windows 10 以降
- Mac OS X 10.11 以降

ブラウザ

- Google Chrome : バージョン 38 以降 (Windows および Mac)
- Microsoft Edge
- Mozilla Firefox : バージョン 42 以降 (Windows および Mac)
- Safari : バージョン 9 以降 (Mac)

スイッチ ソフトウェアのアップグレード

ソフトウェアのバージョンとフィーチャセットの確認

Cisco IOS イメージは、Cisco IOS リリース番号で指定されたディレクトリ内に bin ファイルとして保存されます。Web 管理に必要なファイルはサブディレクトリに格納されます。イメージはシステムボードのフラッシュデバイス (flash:) に格納されます。

show version 特権 EXEC コマンドを使用すると、スイッチで稼働しているソフトウェアバージョンを参照できます。



(注) **show version** の出力にはスイッチで稼働しているソフトウェアイメージが常に表示されますが、最後に表示されるモデル名は工場出荷時の設定であり、ソフトウェアライセンスをアップグレードしても変更されません。

また、**dir filesystem:** 特権 EXEC コマンドを使用して、フラッシュメモリに保存している可能性のある他のソフトウェアイメージのディレクトリ名を表示できます。

ソフトウェア イメージ

サポートサービスの契約をお持ちでソフトウェアライセンスを注文した場合やスイッチを注文した場合は、ユニバーサル ソフトウェア イメージと特定のソフトウェアライセンスが提供されます。

表 1: Cisco Catalyst 1000 のソフトウェアイメージ

イメージ	ファイル名
ユニバーサルイメージ	c1000-universalk9-mz.152-7.E1.bin

イメージ	ファイル名
ユニバーサルイメージ	c1000-universalk9-tar.152-7.E1.tar

Web UI

ソフトウェアのアップグレード後に Web UI が正しくロードまたは動作しない場合は、次の手順を実行します。

1. HTTP サーバユーザの認証方法をローカルに指定します。
Device(config)# **ip http authentication local**
2. ユーザ名とパスワードを権限 15 で設定します。
Device(config)# **username user privilege 15 password password**
3. ブラウザのキャッシュをクリアし、Web UI を再起動します。
4. 権限 15 のユーザ名とパスワードを入力してログインします。

スケーリングのガイドライン

機能のスケーリングのガイドラインについては、Cisco Catalyst 1000 シリーズ スイッチのデータシート

(<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1000-series-switches/nb-06-cat1k-ser-switch-ds-cte-en.html>) を参照してください。

制限事項と制約事項

- GLC-TE を使用するアップリンクポートでは、10/100Mbps の速度はサポートされません。
- アップリンクポートまたはダウンリンクポートは、オレンジ色の物理的な発光ダイオード (LED) をサポートしていません。すべてのポート関連の LED を確認するには、**show hardware led** コマンドを使用します。
- トラフィックレートが変化しても、アップリンクおよびダウンリンクの LED は点滅しません。
- マルチシャーン EtherChannel (MEC) はサポートされていません。
- ファストイーサネットポートは、シングル IP 管理をサポートしません。
- ファストイーサネットポートにケーブルが接続されていない場合、**show cable-diagnostics tdr interface** コマンドの出力で、ペアのステータスが *Open* ではなく *Normal* として表示されます。ペアのステータスは、ケーブルが破損した場合にのみ、*Open* と報告されます。
- タイムドメイン反射率計 (TDR) では、ケーブル全体の長さが 10m を超える場合にのみ、障害ステータスに正しい長さが与えられます。ペアの極性、速度、ペアのステータスな

ど、ケーブル診断結果の他のすべてのフィールドには、任意の長さのケーブルの正しい結果が表示されます。一端が終端されている場合、TDRは正しい長さを報告しないことがあります。

- プロトコルに依存しないマルチキャスト (PIM) はサポートされていません。

不具合

注意事項では、Cisco IOS リリースでの予期しない動作について説明します。以前のリリースでオープンになっている警告は、オープンまたは解決済みとして次のリリースに引き継がれます。

Cisco バグ検索ツール

Cisco [バグ検索ツール](#) (BST) を使用すると、パートナーとお客様は製品、リリース、キーワードに基づいてソフトウェアバグを検索し、バグ詳細、製品、バージョンなどの主要データを集約することができます。BST は、ネットワーク リスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。このツールでは、クレデンシャルに基づいてバグをフィルタし、検索入力に関する外部および内部のバグビューを提供することもできます。

問題の詳細を表示するには、ID をクリックします。

未解決の注意事項

表 2: Cisco IOS リリース 15.2(7)E1 の未解決の注意事項

問題 ID 番号	説明
CSCvs21192	Catalyst 1000 : マルチキャストアドレスが無効な IP に設定され、クエリポートのフラップ後にトラフィックに影響します。
CSCvs23382	Catalyst 1000 : STP フラップで作成されたマルチキャストの古いエン트리。

Cisco IOS リリース 15.2(7)E2 の未解決の注意事項

Cisco IOS リリース 15.2(7)E2 には未解決の注意事項はありません。

Cisco IOS リリース 15.2(7)E3 の未解決の注意事項

問題 ID 番号	説明
CSCvv60364	Cisco Catalyst 1000 シリーズ スイッチ FE : ソークテスト時にランダムダウンリンクポートで見られるリンクフラップ。

Cisco IOS リリース 15.2(7)E4 の未解決の警告

問題 ID 番号	説明
CSCvv86851	TACACS グループサーバで Cisco IOS リリース 15.2(7)E3 および Cisco IOS XE リリース 3.11.3E の server-private ip key passw コマンドがある場合、TACACS は機能しません。

Cisco IOS リリース 15.2(7)E4 の未解決の警告

問題 ID 番号	説明
CSCvx42435	Cisco Catalyst 1000 シリーズ スイッチ : DHCPv6 リレーが実行されず、送信要求パケットが転送されません。

Cisco IOS リリース 15.2(7)E5 の未解決の警告

問題 ID 番号	説明
CSCvz53228	C1000 が mroute ポートにグループ退会メッセージを送信しません

Cisco IOS リリース 15.2(7)E6 の未解決の注意事項

表 3: 未解決の警告

不具合 ID	タイトル
CSCwa92718	MAC-move は、認証ポートから学習した MAC を静的として FDB にインストールしません。
CSCwb19078	Catalyst 1000 : MAB がインターフェイスで設定されている場合、スイッチに接続された特定のクライアントで通信の喪失が発生します。

Cisco IOS リリース 15.2(7)E3 で解決済みの注意事項

表 4: 解決済みの不具合

問題 ID 番号	説明
CSCvt16192	Cisco Catalyst 1000 シリーズ SKU のスイッチライセンスを削除します。
CSCvt16716	IPv6 ソースガード機能は、Cisco IOS リリース 15.2(7)E では機能しません。
CSCvu10399	Cisco IOS および IOS XE ソフトウェアにおける情報漏えいの脆弱性。
CSCvu22034	エンドポイントが接続されていなくても、アイドルタイムアウトはセッションをクリアしません。

問題 ID 番号	説明
CSCvq41676	マルチキャストパケットが、Cisco Catalyst 1000 シリーズスイッチの 2 メンバースタックで 2 回複製されます。
CSCvv00134	VTY telnet がプラットフォーム要求に基づいて SSH を無効、有効にします。

Cisco IOS リリース 15.2(7)E3k で解決済みの注意事項

表 5: 解決済みの不具合

問題 ID 番号	説明
CSCvv99161	Cisco Catalyst 1000 シリーズスイッチの FIPS 対応。

Cisco IOS リリース 15.2(7)E4 で解決済みの警告

表 6: 解決済みの不具合

問題 ID 番号	説明
CSCvw95683	Cisco Catalyst 1000 シリーズスイッチでは、ランダムなクラッシュ/ハング/サイレントリロードが発生することがあります。
CSCvv93417	メンバースイッチが有線 dot1x で失敗します。プライマリスイッチは、同じ設定を使用して dot1x を渡します。
CSCvw18208	Cisco Catalyst 1000 シリーズスイッチのメンバーが、プライマリスイッチとは異なるバージョンで起動します。
CSCvv23128	設定された load-interval コマンドと show interface に表示される値の不一致。
CSCvv75698	スイッチがトレースとエラーログでハングします。
CSCvv86851	TACACS グループサーバで Cisco IOS リリース 15.2(7)E3 および Cisco IOS XE リリース 3.11.3E の server-private ip key passw コマンドがある場合、TACACS は機能しません。
CSCvx03576	特定の SVI を介した Cisco Catalyst 1000 シリーズスイッチのトラフィックは、ネットワークループ後に失敗することがあります。

Cisco IOS リリース 15.2(7)E5 で解決済みの警告

表 7: 解決済みの不具合

問題 ID 番号	説明
CSCvu61737	インターフェイスをデフォルトに設定後にメンバースイッチで設定が非表示になります。
CSCvx76066	「HTTP コア」が原因でスイッチがクラッシュします。
CSCvy03539	C1000 : リロード後に no cdp enable が no cdp tlv app に変更されます。
CSCvy40917	ユーザ名 <username> の特権コマンドは、パスワードを指定しないと受け入れられません。
CSCvz05103	C1000 シリーズ スイッチのインターフェイスから DACL が削除されていません。
CSCvx37117	C1000 スタックスイッチ 2 のトラフィックは、異なる ASIC 上のインターフェイス間を流れません。
CSCvx66699	Cisco IOS および IOS XE Software TrustSec CLI パーサーにおけるサービス妨害の脆弱性

Cisco IOS リリース 15.2(7)E6 で解決済みの警告

表 8: 解決済みの不具合

不具合 ID	タイトル
CSCvz63002	Catalyst 1000 では、DSCP を使用している ACE で class-map が照合される際に、QoS が正しく機能しません。
CSCvz30562	no ip igmp snooping コマンドが設定されているにもかかわらず、Catalyst 1000 は IGMP メンバシップレポートをフラッディングしません。
CSCvx17595	Catalyst 1000 : スタックメンバーの電源をオフまたはオンにした後に、 switchport autostate exclude および no power efficient-ethernet コマンドが追加されます。
CSCvz53228	Catalyst 1000 が mroute ポートにグループ退会メッセージを送信しません

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、次の URL にある Cisco TAC Web サイトを参照してください。

<https://www.cisco.com/en/US/support/index.html>

[Product Support] 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、[Troubleshoot and Alerts] を参照してください。

関連資料

Cisco IOS XE 16 に関する情報は、次の URL から入手できます。 <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html>

Cisco Validated Designs ドキュメントは、次の URL から入手できます。 <https://www.cisco.com/go/designzone>

選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

<http://www.cisco.com/go/mibs>

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](#) 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](#) 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。

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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)

© 2021-2022 Cisco Systems, Inc. All rights reserved.