Cisco IOS Release 15.0(2)SE 以降対応 Catalyst 3750、3560、3560-C、2960、2960-S、および 2960-C スイッチ リリース ノート

2013 年 1 月 14 日

【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。

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。

Cisco IOS Release 15.0(2)SE 以降は、Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、および Cisco EtherSwitch サービス モジュールで動作します。

（注） すべての Catalyst 3750 および 3560 スイッチが、このリリースを実行できるわけではありません。次のモデルは、Cisco IOS Release 12.2(58)SE1 以降ではサポートされ*ません*：WS-C3560-24TS、WS-C3560-24PS、WS-C3560-48PS、WS-C3560-48TS、WS-C3750-24PS、WS-C3750-24TS、WS-C3750-48PS、WS-C3750-48TS、WS-3750G-24T、WS-C3750G-12S、WS-C3750G-24TS、WS-C3750G-16TD。上記のモデルの継続的なメンテナンスのリビルドには、Cisco IOS Release 12.2(55)SE 以降（SE1、SE2 など）を使用します。

Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュールは、Cisco StackWise テクノロジーを利用したスタック構成をサポートします。Catalyst 3560 スイッチおよび 2960 スイッチは、スイッチのスタック構成をサポートしません。Catalyst 2960-S はスタック構成をサポートします。特に明記しない限り、*スイッチ*という用語は、スタンドアロン スイッチおよびスイッチ スタックを指します。

これらのリリース ノートには、IOS Release 15.0(2)SE に関する重要な情報と、このリリースに適用される制限事項、制約事項、警告が含まれます。これらのリリース ノートが次のスイッチで正しいことを確認してください。

- 新しいスイッチを設置する場合は、スイッチの背面パネルにある Cisco IOS リリースのラベルを参照してください。
- スイッチの電源が入っている場合、**show version** 特権 EXEC コマンドを使用します。「ソフトウェアのバージョンとフィーチャ セットの確認」（P.9）を参照してください。
- 新しいリリースにアップグレードするには、ソフトウェア バージョンのソフトウェア アップグレード ファイル名を参照してください。「使用するファイルの決定」（P.9）を参照してください。

スイッチ ソフトウェアは、次のサイトからダウンロードできます（ログイン パスワードを持つ Cisco.com の登録ユーザ）。
http://www.cisco.com/cisco/web/download/index.html

内容

システム要件

サポート対象ハードウェア

表 1　サポートされる Catalyst 3750 および Cisco EtherSwitch サービス モジュール

スイッチ	説明	サポートする最小 Cisco IOS リリース
Catalyst 3750G-24WS-S25	10/100/1000 PoE[1] ポート× 24 および SFP[2] モジュール スロット× 2、および最大 25 個のアクセス ポイントをサポートする統合ワイヤレス LAN コントローラ。	Cisco IOS Release 12.2(25)FZ または Cisco IOS Release 12.2(35)SE
Catalyst 3750G-24WS-S50	10/100/1000 PoE ポート× 24 および SFP モジュール スロット× 2、および最大 50 個のアクセス ポイントをサポートする統合ワイヤレス LAN コントローラ。	Cisco IOS Release 12.2(25)FZ または Cisco IOS Release 12.2(35)SE
Catalyst 3750-24FS	100BASE-FX ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(25)SEB
Catalyst 3750G-24PS	10/100/1000 PoE ポート× 24 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-24TS-1U	10/100/1000 イーサネット ポート× 24 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48PS	10/100/1000 PoE ポート× 48 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3750G-48TS	10/100/1000 イーサネット ポート× 48 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3750V2-24PS	10/100 PoE ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-24TS	10/100 ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48PS	10/100 PoE ポート× 48 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-48TS	10/100 ポート× 48 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3750V2-24FS	SFP モジュール スロット× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(55)EY
NME-16ES-1G[3]	10/100 ポート× 16、10/100/1000 イーサネット ポート×1、StackWise コネクタ ポートなし、シングル幅	Cisco IOS Release 12.2(25)SEC
NME-16ES-1G-P[4]	10/100 PoE ポート× 16、10/100/1000 イーサネット ポート×1、StackWise コネクタ ポートなし、シングル幅	Cisco IOS Release 12.2(25)EZ
NME-X-23ES-1G[4]	10/100 ポート× 23、10/100/1000 PoE ×1、StackWise コネクタ ポートなし、拡張シングル幅	Cisco IOS Release 12.2(25)SEC
NME-X-23ES-1G-P[4]	10/100 PoE ポート× 23、10/100/1000 PoE ポート×1、StackWise コネクタ ポートなし、拡張シングル幅	Cisco IOS Release 12.2(25)EZ

表 1　サポートされる Catalyst 3750 および Cisco EtherSwitch サービス モジュール （続き）

スイッチ	説明	サポートする最小 Cisco IOS リリース
NME-XD-24ES-1S-P[4]	10/100 PoE ポート× 24、SFP モジュール ポート× 1、StackWise コネクタ ポート× 2、拡張倍幅	Cisco IOS Release 12.2(25)EZ
NME-XD-48ES-2S-P[4]	10/100 PoE ポート× 48、SFP モジュール ポート× 2、StackWise コネクタ ポートなし、拡張倍幅	Cisco IOS Release 12.2(25)EZ

1. PoE = Power over Ethernet
2. SFP = Small Form-Factor Pluggable
3. Cisco EtherSwitch サービス モジュール

表 2　サポートされている Catalyst 3560 スイッチ

スイッチ	説明	サポートする最小 Cisco IOS Release
Catalyst 3560-8PC	10/100 PoE ポート× 8 および両用ポート× 1[1]（10/100/1000BASE-T 銅線ポート× 1 および SFP モジュール スロット× 1）	Cisco IOS Release 12.2(35)SE
Catalyst 3560G-24PS	10/100 PoE ポート× 24 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-24TS	10/100/1000 イーサネット ポート× 24 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48PS	10/100/1000 PoE ポート× 48 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3560G-48TS	10/100/1000 イーサネット ポート× 48 および SFP モジュール スロット× 4	Cisco IOS Release 12.2(20)SE3
Catalyst 3560-12PC コンパクト スイッチ	イーサネット 10/100 ポート（PoE 搭載）× 12、デュアルパーパス 10/100/1000 または SFP アップリンク× 1	Cisco IOS Release 12.2(50)SE
Catalyst 3560V2-24PS	10/100 PoE ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS	10/100 ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48PS	10/100 PoE ポート× 48 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-48TS	10/100 ポート× 48 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1
Catalyst 3560V2-24TS-SD	10/100 ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE1

1. 各アップリンク ポートはデュアル フロント エンド（RJ-45 コネクタおよび SFP モジュール スロット）を持つ単一のインターフェイスと見なされます。デュアル フロント エンドは冗長インターフェイスではなく、ペアの 1 個のポートだけがアクティブになります。

表 3　サポートされる Catalyst 2960 および 2960-S スイッチ

スイッチ	説明	サポートする最小 Cisco IOS Release
Catalyst 2960-48PST-S	10/100 PoE ポート× 48、10/100/1000 ポート× 2、および SFP モジュール スロット× 2	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-24PC-S	10/100 PoE ポート× 24 およびデュアルパーパス ポート× 2 （10/100/1000BASE-T 銅線ポート× 2 および SFP モジュール スロット× 2）	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-24LC-S	10/100 ポート× 24（8 ポートが PoE）およびデュアルパーパス ポート× 2 （10/100/1000BASE-T 銅線ポート× 2 および SFP モジュール スロット× 2）	Cisco IOS Release 12.2(50)SE2
Catalyst 2960-8TC-S	10/100 ポート× 8 およびデュアルパーパス ポート[3]× 1（10/100/1000BASE-T 銅線ポート× 1 および SFP モジュール スロット× 1）	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48TT-S	10/100 ポート× 48 および 10/100/1000 ポート× 1	Cisco IOS Release 12.2(46)SE
Catalyst 2960-48PST-L	10/100 PoE ポート× 48、10/100/1000 ポート× 1、および SFP モジュール スロット× 2	Cisco IOS Release 12.2(46)SE
Catalyst 2960-24-S	10/100 BASE-TX イーサネット ポート× 24	Cisco IOS Release 12.2(37)EY
Catalyst 2960-24TC-S	10/100BASE-T イーサネット ポート× 24 およびデュアルパーパス ポート× 2（10/100/1000BASE-T 銅線ポート× 2 および SFP モジュール スロット× 2）	Cisco IOS Release 12.2(37)EY
Catalyst 2960-48TC-S	10/100BASE-T イーサネット ポート× 48 およびデュアルパーパス ポート× 2（10/100/1000BASE-T 銅線ポート× 2 および SFP モジュール スロット× 2）	Cisco IOS Release 12.2(37)EY
Catalyst 2960PD-8TT-L	10/100 ポート× 8 および電力を受け取る 10/100/1000 ポート× 1	Cisco IOS Release 12.2(44)SE
Catalyst 2960-8TC-L	10/100 イーサネット ポート× 8 およびデュアルパーパス ポート× 1（10/100/1000BASE-T 銅線ポート× 1 および SFP モジュール スロット× 1）	Cisco IOS Release 12.2(35)SE
Catalyst 2960G-8TC-L	10/100/1000 イーサネット ポート× 7 およびデュアルパーパス ポート× 1（10/100/1000BASE-T 銅線ポート× 1 および SFP モジュール スロット× 1）	Cisco IOS Release 12.2(35)SE
Catalyst 2960-24LT-L	10/100 ポート× 24（8 ポートが PoE）および 10/100/1000 ポート× 2	Cisco IOS Release 12.2(44)SE
Catalyst 2960-48TC-L	10/100BASE-TX イーサネット ポート× 48 およびデュアルパーパス ポート× 2	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24TC-L	10/100BASE-TX イーサネット ポート× 24 およびデュアルパーパス ポート× 2	Cisco IOS Release 12.2(25)FX
Catalyst 2960-24PC-L	10/100 Power over Ethernet（PoE）ポート× 24 およびデュアルパーパス ポート× 2 （10/100/1000BASE-T 銅線ポート× 2 および Small Form-Factor Pluggable [SFP] モジュール スロット× 2）	Cisco IOS Release 12.2(44)SE

表 3　サポートされる Catalyst 2960 および 2960-S スイッチ （続き）

スイッチ	説明	サポートする最小 Cisco IOS Release
Catalyst 2960-24TT-L	10/100BASE-T イーサネット ポート× 24 および 10/100/1000BASE-T イーサネット ポート× 2	Cisco IOS Release 12.2(25)FX
Catalyst 2960-48TT-L	10/100BASE-T イーサネット ポート× 48 および 10/100/1000BASE-T イーサネット ポート× 2	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-24TC-L	デュアルパーパス ポート× 4 を含む 10/100/1000BASE-T イーサネット ポート× 24（10/100/1000BASE-T 銅線ポート× 4 および SFP モジュール スロット× 4）	Cisco IOS Release 12.2(25)FX
Catalyst 2960G-48TC-L	デュアルパーパス ポート× 4 を含む 10/100/1000BASE-T イーサネット ポート× 48（10/100/1000BASE-T 銅線ポート× 4 および SFP モジュール スロット× 4）	Cisco IOS Release 12.2(25)SEE
Catalyst 2960S-48FPD-L[1]	10/100/1000 Power over Ethernet Plus（PoE+）ポート× 48（PoE 電力 740 W）および SFP+[2] モジュール スロット× 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPD-L[1]	10/100/1000 PoE+ ポート（PoE 電力 370 W）X 48 および SFP+ モジュール スロット X 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PD-L[1]	10/100/1000 PoE+ ポート（PoE 電力 370 W）X 24 および SFP+ モジュール スロット X 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TD-L[1]	10/100/1000 ポート X 48 および SFP+ モジュール スロット X 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TD-L[1]	10/100/1000 ポート X 24 および SFP+ モジュール スロット X 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48FPS-L[1]	10/100/1000 PoE+ ポート（PoE 電力 740 W）X 48 および SFP モジュール スロット X 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48LPS-L[1]	10/100/1000 PoE+ ポート（PoE 電力 370 W）X 48 および SFP モジュール スロット X 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24PS-L[1]	10/100/1000 PoE+ ポート（PoE 電力 370 W）X 24 および SFP モジュール スロット X 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-L[1]	10/100/1000 ポート X 48 および SFP モジュール スロット X 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-L[1]	10/100/1000 ポート X 24 および SFP モジュール スロット X 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-F48FPS-L[1]	10/100 PoE+ ポート（PoE 電力 740 W）× 48 および SFP モジュール スロット× 4	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48LPS-L[1]	10/100 PoE+ ポート（PoE 電力 370 W）× 48 および SFP モジュール スロット× 4	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F48TS-L[1]	10/100 ポート× 48 および SFP モジュール スロット× 4	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24PS-L[1]	10/100 PoE+ ポート（PoE 電力 370 W）× 24 および SFP モジュール スロット× 2	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-L[1]	10/100 ポート× 24 および SFP モジュール スロット× 2	Cisco IOS Release 15.0(2)SE

表 3　サポートされる Catalyst 2960 および 2960-S スイッチ （続き）

スイッチ	説明	サポートする最小 Cisco IOS Release
Catalyst 2960S-F48TS-S	10/100 ポート × 48 および SFP モジュール スロット × 2	Cisco IOS Release 15.0(2)SE
Catalyst 2960S-F24TS-S	10/100 ポート × 24 および SFP モジュール スロット × 2	Cisco IOS Release 15.0(2)SE

1.Cisco FlexStack テクノロジーをサポートしています。

2.SFP+ = 10 ギガビット ファイバ アップリンク。

表 4　サポートされている他のハードウェア

スイッチ	説明	サポートする最小 Cisco IOS Release
Cisco CGS 2520 スイッチ	Cisco 2520 Connected Grid スイッチ（CGS 2520）は、エネルギー業界や電力業界での過酷な環境向けに設計された堅牢なスイッチです。 http://www.cisco.com/en/US/partner/products/ps10978/products_installation_and_configuration_guides_list.html	Cisco IOS Release 12.2(53)EX
SFP モジュール（Catalyst 3750 および 3560）	1000BASE-CWDM[1]、- LX、- SX、T、- ZX 100BASE-FX（MMF）[2] 8 個の追加 DWDM SFP 光モジュールをサポートします。サポートされる SFP および部品番号のリストについては、次のデータ シートを参照してください。 http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.html	Cisco IOS Release 12.2(18)SE Cisco IOS Release 12.2(20)SE
SFP モジュール（Catalyst 2960）	1000BASE-BX、CWDM、- LX/LH、- ZX、- ZX 100BASE-BX、FX、- LX サポートされる SFP および部品番号の完全なリストについては、次の SFP モジュールの互換性情報を参照してください。 http://www.cisco.com/en/US/partner/products/hw/modules/ps5455/products_device_support_tables_list.html	Cisco IOS Release 12.2(25)FX
XENPAK モジュール[3]	XENPAK-10-GB-ER、XENPAK-10-GB-LR および XENPAK-10-GB-SR	Cisco IOS Release 12.2(18)SE
冗長電源システム	Cisco RPS 675 冗長電源システム Cisco RPS 300 冗長電源システム（Catalyst 2960 スイッチでのみサポート） Cisco 冗長電源システム 2300	すべてのソフトウェア リリースでサポート すべてのソフトウェア リリースでサポート Cisco IOS Release 12.2(35)SE 以降

1. CWDM：Coarse Wavelength-Division Multiplexer
2. MMF：Multimode Fiber
3. XENPAK モジュールは、Catalyst 3750G-16TD スイッチでのみサポートされます。

Device Manager のシステム要件

ハードウェア要件

表 5　　最小ハードウェア要件

プロセッサ速度	DRAM	色の数	解像度	フォント サイズ
233 MHz 以上[1]	512 MB[2]	256	1024 x 768	小

1. 1 GHz を推奨します。
2. 1 GB DRAM を推奨します。

ソフトウェア要件

- Windows 2000、XP、Vista、Windows Server 2003。
- JavaScript が有効になっている Internet Explorer 6.0、7.0、Firefox 1.5、2.0 以降。

デバイス マネージャは、セッションを開始するときにブラウザのバージョンを確認し、プラグインを必要としません。

クラスタの互換性

デバイス マネージャからスイッチ クラスタを作成したり管理したりすることはできません。スイッチ クラスタの作成と管理には、コマンドライン インターフェイス（CLI）または Network Assistant アプリケーションを使用します。

スイッチ クラスタの作成またはスイッチをクラスタに追加する場合は、次のガイドラインに従ってください。

- スイッチ クラスタを作成する場合は、クラスタ内で最もハイエンドなスイッチをコマンド スイッチとして設定することを推奨します。
- Network Assistant を使用してクラスタを管理する場合は、最新のソフトウェアを使用するスイッチをコマンド スイッチとする必要があります。
- スタンバイ コマンド スイッチはコマンド スイッチと同じタイプである必要があります。たとえば、コマンド スイッチが Catalyst 3750 スイッチの場合、すべてのスタンバイ コマンド スイッチは、Catalyst 3750 スイッチにする必要があります。

クラスタリングについての詳細は、『*Getting Started with Cisco Network Assistant*』、『*Release Notes for Cisco Network Assistant*』（発注はできませんが Cisco.com で入手可能です）、ソフトウェア コンフィギュレーション ガイド、コマンド リファレンス、および Cisco EtherSwitch サービス モジュールの機能のマニュアルを参照してください。

CNA の互換性

Cisco IOS 12.2(50)SE 以降は、Cisco Network Assistant (CNA) 5.0 以降とのみ互換性があります。次の URL から Cisco Network Assistant をダウンロードできます。
http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

Cisco Network Assistant の詳細情報については、Cisco.com の『*Release Notes for Cisco Network Assistant*』を参照してください。

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。サブディレクトリには、Web 管理に必要なファイルが格納されます。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。バージョンは 2 行目に表示されます。

（注） Catalyst 3750 スイッチおよび 3560 スイッチ、Cisco EtherSwitch サービス モジュールについては、**show version** の出力はスイッチで稼働しているソフトウェア イメージを常に表示しますが、この表示の最後に表示されるモデル名は、工場出荷時の設定（IP ベース イメージまたは IP サービス イメージ）であり、ソフトウェア イメージ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。

使用するファイルの決定

このリリース ノートのアップグレード手順では、結合された tar ファイルを使用してアップグレードを行う方法について説明します。このファイルには Cisco IOS イメージ ファイルと、組み込みデバイス マネージャに必要なファイルが含まれます。デバイス マネージャを使用してスイッチをアップグレードするためには、この結合された tar ファイルを使用する必要があります。コマンドライン インターフェイス（CLI）を使ってスイッチをアップグレードするには、tar ファイルおよび **archive download-sw** 特権 EXEC コマンドを使用します。

表 6　Cisco IOS ソフトウェア イメージ ファイル

ファイル名	説明
c3750-ipbasek9-tar.150-2.SE.tar	Catalyst 3750 IP ベース暗号化イメージ ファイルおよびデバイス マネージャ ファイル。このイメージには、Kerberos、SSH[1]、レイヤ 2+ および基本的なレイヤ 3 ルーティング機能が含まれています。このイメージは、Cisco EtherSwitch サービス モジュールでも動作します。
c3750-ipservicesk9-tar.150-2.SE.tar	Catalyst 3750 IP サービス暗号化イメージ ファイルおよびデバイス マネージャ ファイル。このイメージには、Kerberos、SSH、レイヤ 2+ および完全なレイヤ 3 機能が含まれています。このイメージは、Cisco EtherSwitch サービス モジュールでも動作します。
c3560-ipbasek9-tar.150-2.SE.tar	Catalyst 3560 IP ベース暗号化イメージ ファイルおよびデバイス マネージャ ファイル。このイメージには、Kerberos、SSH、レイヤ 2+ および基本的なレイヤ 3 ルーティング機能が含まれています。
c3560-ipservicesk9-tar.150-2.SE.tar	Catalyst 3560 IP サービス暗号化イメージ ファイルおよびデバイス マネージャ ファイル。このイメージには、Kerberos、SSH、レイヤ 2+ および完全なレイヤ 3 機能が含まれています。
c3560c405ex-universalk9npe-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 3560-C イメージは、MACsec の暗号化をサポートしていません。
c3560c405ex-universalk9-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 3560-C イメージ。
c3560c405-universalk9npe-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 3560 イメージは、MACsec の暗号化をサポートしていません。
c3560c405-universalk9-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 3560-C イメージ。
c2960-lanbasek9-tar.150-2.SE.tar	Catalyst 2960 暗号化イメージ ファイルおよびデバイス マネージャ ファイル。このイメージには Kerberos および SSH 機能が含まれています。
c2960-lanlitek9-tar.150-2.SE.tar	Catalyst 2960 LAN Lite 暗号化イメージ ファイルおよびデバイス マネージャ ファイル。
c2960s-universalk9-tar.150-2.SE.tar	デバイス マネージャを備えた LAN Base および LAN Lite 暗号化イメージ
c2960c405ex-universalk9-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 2960-C イメージ。
c2960c405-universalk9-tar.150-2.SE.tar	サポートされているすべてのユニバーサル イメージの機能、および Web ベースのデバイス マネージャを備えた Catalyst 2960-C イメージ。
c2960sm-lanbasek9-tar.150-2.SE.tar	Web ベースのデバイス マネージャを備えた Catalyst 2960-SM LAN Base イメージ。

1. SSH = Secure Shell（セキュア シェル）

ソフトウェア イメージのアーカイブ

スイッチ ソフトウェアをアップグレードする前に、現在の Cisco IOS リリースと、アップグレード後の Cisco IOS リリースのコピーをアーカイブしておく必要があります。ネットワーク内のすべてのデバイスを新しい Cisco IOS イメージにアップグレードし、新しい Cisco IOS イメージがネットワークで正常に機能することを確認するまで、アーカイブされたイメージは保持しておく必要があります。

シスコは、Cisco.com から定期的に古いバージョンの Cisco IOS を削除します。詳細については、次の「*製品速報 2863*」を参照してください。
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

copy flash: tftp: 特権 EXEC コマンドを使用して、フラッシュ メモリ上の bin ソフトウェア イメージ ファイルをホスト上の適切な TFTP ディレクトリにコピーすることができます。

（注） フラッシュ メモリ上にあるファイルはすべて TFTP サーバにコピーできますが、tar ファイル内のすべての HTML ファイルをコピーするには時間がかかります。tar ファイルを Cisco.com からダウンロードして、これをネットワーク内の内部ホストにアーカイブすることをお勧めします。

tftp-server グローバル コンフィギュレーション コマンドを使用することで、スイッチを TFTP サーバとして設定し、あるスイッチから別のスイッチに外部 TFTP サーバを使用せずにファイルをコピーすることもできます。**tftp-server** コマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*』の「Basic File Transfer Services Commands」の項を参照してください。
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

デバイス マネージャまたは Network Assistant を使用したスイッチのアップグレード

デバイス マネージャまたは Network Assistant を使用してスイッチ ソフトウェアをアップグレードできます。詳細については、[Help] をクリックしてください。

（注） スイッチをアップグレードするためにデバイス マネージャを使用する場合、アップグレード プロセスが開始された後でブラウザ セッションを使用したり終了したりしないでください。アップグレード プロセスが完了するまで待機してください。

CLI を使用したスイッチのアップグレード

この手順は、スイッチに結合された tar ファイルのコピーに使用します。TFTP サーバからスイッチへファイルをコピーして、ファイルを抽出します。イメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

ソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1 表 6（P.10）を使用してダウンロードするファイルを指定します。

ステップ 2 ソフトウェア イメージ ファイルをダウンロードします。

a. 登録ユーザは、次の URL にアクセスして、ログインします。
http://www.cisco.com/cisco/web/download/index.html

b. [Switches] > [LAN Switches - Access] に移動します。

c. スイッチ モデルに移動します。

d. [IOS Software] をクリックして最新の IOS リリースを選択します。

ステップ 1 で指定したイメージをダウンロードします。

注意 Cisco IOS Release 12.1(19)EA1c 以前のリリースを実行している Catalyst 3750 スイッチをアップグレードする場合、このリリースにはブートローダのアップグレードが含まれます。新しいソフトウェアが初めてロードされるときには、ブートローダのアップグレードに最大 1 分必要です。ブートローダのアップグレード中には、スイッチの電源のオフ / オンを行わないでください。

ステップ 3 イメージをワーク ステーション上の適切な TFTP ディレクトリにコピーし、TFTP サーバが正しく設定されていることを確認します。

詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Appendix B」を参照してください。

ステップ 4 コンソール ポートまたは Telnet セッションを介して、スイッチにログインします。

ステップ 5 （任意）TPTP サーバに次の特権 EXEC コマンドを入力して、IP 接続を確認します。

```
Switch# ping tftp-server-address
```

IP アドレスとデフォルト ゲートウェイのスイッチへの割り当てに関する詳細については、このリリースに対応するソフトウェア コンフィギュレーション ガイドを参照してください。

ステップ 6 TFTP サーバからスイッチにイメージ ファイルをダウンロードします。スイッチに現在含まれるソフトウェアと同じバージョンをインストールする場合は、次の特権 EXEC コマンドを入力して、現在のイメージを上書きします。

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

/overwrite オプションを指定すると、フラッシュ メモリ内のソフトウェア イメージがダウンロードされたイメージによって上書きされます。

/reload オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。

allow-feature-upgrade オプションを使用すると、異なる機能セットを備えたイメージをインストールできます（たとえば、IP ベース イメージから IP サービス イメージへのアップグレードなど）。

//location には、TFTP サーバの IP アドレスを指定します。

/directory/image-name.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

次の例では、198.30.20.19 の TFTP サーバからイメージをダウンロードし、スイッチでイメージを上書きする方法を示します。

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c3750-ipservices-tar.122-50.SE.tar
```

TFTP サーバからスイッチにイメージ ファイルをダウンロードして、**/overwrite** オプションを **/leave-old-sw** オプションと置き換えることで、現在のイメージを維持することもできます。

ソフトウェア障害からの回復

リカバリ手順については、このリリースに対応するソフトウェア コンフィギュレーション ガイドの「Troubleshooting」の章を参照してください。

インストール上の注意事項

スイッチに IP 情報を割り当てるには、次の方法を使用してください。

- スイッチのスタートアップ ガイドに説明されている Express Setup プログラム。
- スイッチのハードウェア インストレーション ガイドに説明されている CLI ベースのセットアップ プログラム。
- スイッチのソフトウェア コンフィギュレーション ガイドに説明されている DHCP ベースの自動設定。
- スイッチのソフトウェア コンフィギュレーション ガイドに説明されているように手動で IP アドレスを割り当てます。

新しいソフトウェア機能

Cisco IOS Release 15.0(2)SE 1 の新機能

- Catalyst 2960-S、3750、3560、2960-C405、2960-C405ex、3560-C405、3560-C405ex スイッチに搭載された Cisco IOS Release 15.0(2)SE1 は、FIPS 140-2 の認証を受け、Common Criteria および米国政府ネットワーク デバイス セキュリティ要件バージョン 1.0（pp_nd_v1.0、2010 年 12 月 10 日発行）に準拠しています。

  （注） Catalyst 2960-S、3750、3560、2960-C405、2960-C405ex、3560-C405、3560-C405ex スイッチの Cisco IOS Release 15.0(2)SE1 のイメージは、FIPS 認証済みです。FPIS 認定イメージの使用に関する詳細については、ソフトウェア コンフィギュレーション ガイドの「Assigning the Switch IP Address and Default Gateway」の章の「Boot Loader Upgrade and Image Verification for the FIPS Mode of Operation」の項を参照してください。

  FIPS 140-2 は、暗号化に焦点を当てた認証であり、多くの政府およびエンタープライズの顧客により義務付けられています。これは、スイッチで実行される暗号化および復号化処理が、これらの処理を保護するために、承認された FIPS 暗号化強度および管理方法に準拠していることを保証します。詳細については、以下を参照してください。

  - セキュリティ ポリシーのドキュメント：
    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2011.htm#1657
  - インストレーション ノート：
    http://www.cisco.com/en/US/products/ps10745/prod_installation_guides_list.html

  Common Criteria はコンピュータ セキュリティ証明書向け国際基準（ISO/IEC 15408）です。この規格は一連の要件、テスト、評価方法から成り、評価のターゲットが特定の保護プロファイルまたはカスタム セキュリティ ターゲットに準拠していることを保証します。詳細については、次のセキュリティ ターゲットの資料を参照してください。
  http://www.niap-ccevs.org/st/vid10488/

- Resilient Ethernet Protocol（REP）に対するサポート。REP はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、リング トポロジにおけるコンバージェンス時間の改善を実現します。Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring Resilient Ethernet Protocol*」の章を参照してください。（Catalyst 3560-C スイッチ）

Cisco IOS Release 15.0(2)SE の新機能

- Universal Power over Ethernet（UPoE）機能に対するサポート。IEEE802.3at 標準に基づく RJ-45 イーサネット ケーブルのシグナル ペアおよびスペア ペアの両方を経由して最大 60 W（2X 30W）の電力を供給します。自動的に UPoE 対応電源デバイスを検出し、CDP や LLDP などのレイヤ 2 電力ネゴシエーション プロトコルを使用して、最大 60 W の電力をネゴシエートします。また、CDP/LLDP ネゴシエーションなしでポートに 60 W の電力を供給します（必須の UPoE TLV をサポートしていないデバイス用）。（Catalyst 2960-C および 3560- C スイッチ）

  UPoE の詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの 15 ページから 13 ページにある 15 章「Configuring Interface Characteristics」の「Universal Power over Ethernet」の項を参照してください。

- IPv6 Ready Logo Phase-2 コア プロトコル テスト スイートに準拠する IOS IPv6 ホスト モードに対するサポート （Catalyst 2960、2960-C、2960-S の各スイッチの LAN Lite イメージ、Catalyst 3750、3750v2、3560、3560v2、3650-C 各スイッチの IP ベース イメージ）。

- **class class-default** ポリシーマップ コンフィギュレーション コマンドを使用して、Catalyst 2960-S スイッチにデフォルト クラスを設定するオプション。詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring QoS*」の章を参照してください。（Catalyst 2960-S スイッチ）

- OSPFv3 高速コンバージェンスに対するサポート。OSPFv3 のリンクステート アドバタイズメント（LSA）および Shortest Path First（SPF）スロットリング機能は、ネットワークが不安定な間、OSPFv3 でのリンクステート アドバタイズメント アップデートを低速化するためのダイナミック方式を提供します。また、この機能は、LSA のレート制限をミリ秒単位で指定することにより、OSPFv3 コンバージェンス時間の短縮を可能にします。詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring IPv6 Unicast Routing*」の章を参照してください。（Catalyst 3750 スイッチおよび Catalyst 3560 スイッチ）

- OSPFv2 LSA のレート制限に関する CLI オプションでの変更。**all** キーワードは、**timers throttle lsa** グローバル コンフィギュレーション コマンドから削除されました。（Catalyst 3560-C、3560v2、および 3750 v2 スイッチ）

- IPsec による OSPFv3 認証に対するサポート。改変されずにパケットがスイッチに再送信されるよう、IPsec セキュア ソケット API を使用して OSPF for IPv6（OSPFv3）パケットを認証できるようになりました。詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring IPv6 Unicast Routing*」の章を参照してください。（Catalyst 3560、3560-C、3560v2、3750、および 3750v2 スイッチ）

- IPv6 でのホップ セキュリティ（FHS）に対するサポート。サポート対象の機能は次のとおりです：IPv6 スヌーピング、IPv6 FHS バインディング、ネイバー探索プロトコル（NDP）アドレス グリーニング、IPv6 データ アドレス グリーニング、IPv6 Dynamic Host Configuration Protocol（DHCP）アドレス グリーニング、IPv6 デバイス トラッキング、ネイバー探索（ND）インスペクション、IPv6 ポート ベースのアクセス リスト、IPv6 DHCP ガード、IPv6 ルータ アドバタイズメント（RA）ガード、IPv6 ソース ガード。詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring IPv6 Host Functions*」の章を参照してください。（Catalyst 2960-C、2960-S および 3560- C スイッチ）

- Smart Install 管理に使用する VLAN を設定するためのサポート。**vstack startup-vlan** コマンドが追加されました。詳細については、Cisco.com のコマンド リファレンスを参照してください。

- 設定可能な MAC 認証バイパス (MAB) に対するサポート。クライアントの MAC アドレスが想定される標準の形式とは異なっている場合や、RADIUS の設定によりユーザ名とパスワードが異なっている場合に、MAB 認証をどのように実行するかを設定できます。詳細については、Cisco.com のソフトウェア コンフィギュレーション ガイドの「*Configuring IEEE 802.1x Port-Based Authentication*」の章を参照してください。

- Universal PoE（UPoE）のネゴシエートに対するサポート。詳細については、「Catalyst 3560 および 2960 ソフトウェア コンフィギュレーション ガイドの更新内容」（P.59）を参照してください。（Catalyst 2960-C スイッチおよび 3560-C スイッチ）
- Media Access Control Security（MACsec）に対するサポート。スイッチは、スイッチとホスト デバイス間の暗号化に、ダウンリンク ポートとアップリンク ポートで MACsec Key Agreement（MKA）による 802.1AE 暗号化をサポートします。詳細については、ソフトウェア コンフィギュレーション ガイドの「*Configuring MACsec Encryption*」の章を参照してください。（Catalyst 3560-C）
- IKEv2 プロトコルおよび IPSecv3 プロトコルに対するサポート。（Catalyst 3750、3750v2、3560、3560v2 の各スイッチの場合 IP ベース イメージ）
- スイッチのレイヤ 2 インターフェイス上のポート ACL に対するサポート。（Catalyst 2960-C、2960-S の各スイッチの LAN ベース イメージ、Catalyst 3560-C スイッチの IP ベース イメージ）
- Switch Virtual Interface (SVI) 上のルータ ACL に対するサポート。SVI は、VLAN へのレイヤ 3 インターフェイス、物理レイヤ 3 インターフェイス、レイヤ 3 EtherChannel インターフェイスのいずれかにすることができます。（Catalyst 2960-C、2960-S の各スイッチの LAN ベース イメージ、Catalyst 3560-C スイッチの IP ベース イメージ）
- ルータに直接接続されていないネットワークにパケット データを送信できるように、ルーティング テーブルでのスタティック IPv6 ルートの設定をサポートします。（Catalyst 2960、2960-C、2960-S の各スイッチの場合 LAN ベース イメージ）
- Cisco TrustSec SXP バージョン 2、syslog メッセージに対するサポートと、SNMP サポートは LAN ベース ライセンスまで拡張されました。（Catalyst 3560-C スイッチの IP ベース イメージ）
- Etherchannel でのポート セキュリティに対するサポート。詳細については、ソフトウェア コンフィギュレーション ガイドの「*Configuring Port-Based Traffic Control*」の章を参照してください。
- Etherchannel での IP ソース ガードに対するサポート。詳細については、ソフトウェア コンフィギュレーション ガイドの「*Configuring DHCP and IP Source Guard*」の章を参照してください。
- Cisco CGS 2520 スイッチでの Precision Time Protocol（PTP）と温度ならびに電圧のモニタリングに対するサポート。

主な機能の最小 Cisco IOS Release

表 7 には、Catalyst 3750、3560、2960-S、および 2960 の各スイッチと Cisco EtherSwitch サービス モジュールの主要な機能をサポートするために必要なソフトウェアの最小リリースが示されています。

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
Cisco TrustSec SXP バージョン 2、Syslog メッセージおよび SNMP サポート	15.0(2)SE	3560-C、2960-S、2960-C
クリティカル音声 VLAN	15.0(1)SE	3750、3560、2960-S、2960
サプリカント ポートへのアクセスを制御する NEAT 機能拡張	15.0(1)SE	3750、3560、2960-S、2960
Cisco TrustSec SXP バージョン 2、Syslog メッセージおよび SNMP サポート	15.0(1)SE	3750 および 3560

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
Auto Smartport の改善されたデバイス分類機能	15.0(1)SE	3750、3560、2960-S、2960
デバイス センサー	15.0(1)SE	3750、3560
Cisco IOS IP SLA ビデオ動作を使用した組み込み型トラフィック シミュレータ	12.2(58)SE1	3750、3560
Cisco Mediatrace サポート	12.2(58)SE1	3750、3560
Cisco Performance Monitor	12.2(58)SE1	3750、3560
EnergyWise Phase 2.5	12.2(58)SE1	3750、3560、2960-S、2960
Smart ロギング	12.2(58)SE1	3750、3560
プロトコル ストーム プロテクション	12.2(58)SE1	3750、3560、2960-S、2960
VACL ロギング	12.2(58)SE1	3750、3560
Smart Install 3.0	12.2(58)SE1	3750、3560、2960-S、2960
Digital Media Player 上で Auto QoS をイネーブルにする Auto SmartPort の拡張機能。	12.2(58)SE1	3750、3560、2960-S、2960
メモリの整合性検査ルーチン	12.2(58)SE1	2960-S
Call Home のサポート	12.2(58)SE1	3750、3560、2960-S、2960
NTP バージョン 4	12.2(58)SE1	3750、3560、2960-S、2960
DHCPv6 バルクリース クエリーおよび DHCPv6 リレー送信元設定	12.2(58)SE1	3750、3560
OSPFv2 および OSPFv3（IP サービス イメージ）の NSF IETF モード	12.2(58)SE1	3750、3560
IPv6 経由の RADIUS、TACACS+、および SSH/SCP	12.2(58)SE1	3750、3560、2960-S、2960
IPv4 の VRRP	12.2(58)SE1	3750、3560
IETF IP-MIB と IP-FORWARD-MIB（RFC4292 および RFC4293）更新	12.2(58)SE1	3750、3560、2960-S、2960
Auto-QoS の機能拡張	12.2(55)SE	3750、3560、2975、2960、2960-S
グローバル マクロを含む Auto Smartport の拡張機能	12.2(55)SE	3750、3560、2975、2960、2960-S
Smart Install の拡張機能と新機能	12.2(55)SE	3750、3560、2975、2960、2960-S
ポート ACL の改善	12.2(55)SE	3750、3560、2975、2960、2960-S
CDP および LLDP ロケーションの拡張機能	12.2(55)SE	3750、3560、2975、2960、2960-S
VLAN 割り当てを使用した複数認証	12.2(55)SE	3750、3560、2975、2960、2960-S
Cisco TrustSec	12.2(55)SE	3750 および 3560
メモリの整合性検査ルーチン	12.2(55)SE	3750、3560、2975、2960
SVI でのスタティック ルーティング サポート	12.2(55)SE	2975、2960、および 2960-S

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
ポートからホストが切断されるときにセッションを終了する MAC 置換。	12.2(55)SE	3750、3560、2975、2960、2960-S
LAN Lite イメージでの DHCP スヌーピング、オプション 82 および LLPD-MED	12.2(55)SE	2960 および 2960-S
ネットワークの 1 箇所（ディレクタ）からの管理を可能にする Smart Install。	12.2(52)SE	3750、3560、2975、2960
スタティック ホストでの IP ソース ガードのサポート。	12.2(52)SE	3750、3560、2975、2960
AutoSmartPort 機能拡張（マクロ永続性、LLDP に基づくトリガー、MAC アドレスおよび OUI ベースのトリガー、リモート マクロ）。	12.2(52)SE	3750、3560、2975、2960
RADIUS 許可の変更（CoA）。	12.2(52)SE	3750、3560、2975、2960
複数の VLAN の配置に対応した 802.1X ユーザ分散。	12.2(52)SE	3750、3560、2975、2960
マルチホスト認証を使った、重要な VLAN。	12.2(52)SE	3750、3560、2975、2960
ユーザ定義ページの作成を許可するカスタマイズ可能な Web 認証機能強化。	12.2(52)SE	3750、3560、2975、2960
ポートのホスト モードを変更する Network Edge Access Topology（NEAT）。	12.2(52)SE	3750、3560、2975、2960
VLAN ID ベース MAC 認証	12.2(52)SE	3750、3560、2975、2960
ホストが同じスイッチ内のポート間を移動できるようにする MAC 移動。	12.2(52)SE	3750、3560、2975、2960
SNMPv3 を使った 3DES および AES。	12.2(52)SE	3750、3560、2975、2960
DHCPDISCOVER パケットの Option 12 フィールドにホスト名の入力をサポート。	12.2(52)SE	3750、3560、2975、2960
circuit-id サブオプションに対する DHCP スヌーピング拡張機能。	12.2(52)SE	3750、3560、2975、2960
LLPD-MED へのサポート強化	12.2(52)SE	3750、3560、2975、2960
LLPD-MED MIB および CISCO-ADMISSION-POLICY-MIB。	12.2(52)SE	3750、3560、2975、2960
IPv6 QoS トラスト機能。	12.2(52)SE	3750、3560
ビデオ アプリケーション向けネットワーク インフラストラクチャでインテリジェント サービスを可能にする Cisco Medianet。	12.2(52)SE	3750、3560
ネイバー探索、ID、MAC アドレス テーブルの EEM 3.2 イベント検出器。	12.2(52)SE	3750、3560
EnergyWise エージェントを実行している EnergyWise 対応のシスコ デバイスとシスコ以外のエンド ポイントを管理する Cisco EnergyWise Phase 2。	12.2(53)SE1	3750、3560、2960
802.1x スイッチ サプリカント機能を持つ Network Edge Access Topology（NEAT）、CISP を使ったホスト認証、および自動イネーブル化	12.2(50)SE	3750、3560、2960
オープン アクセスを使用した 802.1x	12.2(50)SE	3750、3560、2960
ダウンロード可能な ACL とリダイレクト URL を使用した 802.1x 認証	12.2(50)SE	3750、3560、2960

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
柔軟な認証シーケンス	12.2(50)SE	3750、3560、2960
マルチユーザ認証	12.2(50)SE	3750、3560、2960
PoE デバイス経由の電力消費量を管理する Cisco EnergyWise Phase 1。	12.2(50)SE	3750、3560、2960
ワイヤード ロケーション サービス	12.2(50)SE	3750、3560、2960
CPU 使用率しきい値トラップ	12.2(50)SE	3750、3560、2960
Cisco IOS Configuration Engine（旧称 Cisco IOS CNS エージェント）	12.2(50)SE	3750、3560、2960
LLDP-MED ネットワーク ポリシー プロファイル時間、長さ、値（TLV）	12.2(50)SE	3750、3560、2960
RADIUS サーバのロード バランシング	12.2(50)SE	3750、3560、2960
Auto Smartport のシスコのデフォルト マクロとユーザ定義マクロ	12.2(50)SE	3750、3560、2960
CONFIG_COPY MIB、CISCO-AUTH-FRAMEWORK-MIB、CISCO-MAC-AUTH-BYPASS MIB、LLDP MIB での SCP 属性のサポート。	12.2(50)SE	3750、3560、2960
Connectionless Network Service（CLNS）ネットワーク用 Intermediate System-to-Intermediate System（IS-IS）ルーティング	12.2(50)SE	3750、3560
組み込みイベント マネージャ バージョン 2.4 に対するサポート。	12.2(50)SE	3750、3560
IP サービス イメージおよび IP ベース イメージでの IPv6 機能：ACL、DCHP サーバ/クライアント/リレー デバイス用 DHCPv6、EIGRPv6、HSRPv6、OSPFv3、RIP、スタティック ルート	12.2(50)SE	3750、3560
スタックのトラブルシューティング機能の拡張	12.2(50)SE	3750
制限付き VLAN を使用した 802.1x 認証	12.2(50)SE	2960
IP ソース ガード	12.2(50)SE	2960
ダイナミック ARP インスペクション	12.2(50)SE	2960
SSH プロトコルを使用した汎用メッセージ認証サポートおよび RFC 4256 への準拠	12.2(46)SE	3750、3560、2960
汎用メッセージ認証サポート	12.2(46)SE	3750、3560、2960
VLAN の MAC アドレス ラーニングをディセーブルにします。	12.2(46)SE	3750、3560、2960
PAgP と仮想スイッチとの相互交流およびデュアルアクティブ検出	12.2(46)SE	3750、3560、2960
DHCP サーバ ポート ベースのアドレス割り当て	12.2(46)SE	3750、3560、2960
IPv6 デフォルト ルータの初期設定（DRP）	12.2(46)SE	3750、3560、2960
音声対応 IEEE 802.1x および MAC 認証バイパス（MAB）セキュリティ違反	12.2(46)SE	3750、3560
ローカル Web 認証バナー	12.2(46)SE	3750、3560
CISCO-NAC-NAD および CISCO-PAE MIB に対するサポート	12.2(46)SE	3750、3560
SVI ラインステート計算からの VLAN ポートの除外	12.2(46)SE	3750、3560
EOT および IP SLA EOT スタティック ルートのサポート	12.2(46)SE	3750、3560
HSRP バージョン 2（HSRPv2）のサポート	12.2(46)SE	3750、3560

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
IPv6 対応 HSRP（拡張 IP サービス イメージ）	12.2(46)SE	3750、3560
IPv6 のリレー、クライアント、サーバ アドレス割り当て、プレフィックス委任に対応した DHCP（拡張 IP サービス イメージ）	12.2(46)SE	3750、3560
組み込みイベント マネージャ（EEM）（IP サービス イメージのみ）	12.2(46)SE	3750、3560
マルチドメイン認証 (MDA) のダイナミック音声仮想 LAN（VLAN）（LAN ベース イメージのみ）	12.2(46)SE	2960
PoE ポート単位でのリアルタイム電力消費のモニタリング	12.2(46)SE	2960
ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。	12.2(46)SE	2960
IEEE 802.1x 準備状態チェック	12.2(44)SE	3750、3560、2960
DHCP ベースの自動設定とイメージ アップデート	12.2(44)SE	3750、3560、2960
設定可能なスモール フレーム着信しきい値	12.2(44)SE	3750、3560、2960
IPV6 経由の HTTP および HTTP のサポート	12.2(44)SE	3750、3560、2960
IPv6 トランスポート経由の SNMP 設定	12.2(44)SE	3750、3560、2960
IPv6 ステートレス自動設定	12.2(44)SE	3750、3560、2960
Flex Link マルチキャスト高速コンバージェンス	12.2(44)SE	3750、3560、2960
デジタル オプティカル モニタリング（DOM）	12.2(44)SE	3750、3560
Source Specific Multicast（SSM）マッピング	12.2(44)SE	3750、3560
マルチキャスト トラフィックの /31 ビット マスクのサポート	12.2(44)SE	3750、3560
設定の交換およびロールバック	12.2(40)SE	3750、3560、2960
リンク層検出プロトコル メディア拡張（LLDP-MED）	12.2(40)SE	3750、3560、2960
Enhanced Interior Gateway Routing Protocol（EIGRP）IPv6	12.2(40)SE	3750、3560
自動 Quality of Service（QoS）Voice over IP（VoIP）	12.2(40)SE	3750、3560、2960
MDA 対応ポートのダイナミック音声仮想 LAN（VLAN）	12.2(40)SE	3750、3560
インターネット グループ管理プロトコル（IGMP）ヘルパー	12.2(40)SE	3750、3560
IP サービス レベル契約（IP SLA）	12.2(40)SE	3750、3560
IP SLA EOT	12.2(40)SE	3750、3560
マルチキャスト VPN ルーティングおよび転送（VRF）Lite	12.2(40)SE	3750、3560
SSM PIM プロトコル	12.2(40)SE	3750、3560
HSRP、uRPF、ARP、SNMP、IP SLA、TFTP、FTP、syslog、traceroute、ping に対する VRF 認識サポート	12.2(40)SE	3750、3560
MLD スヌーピング	12.2(40)SE	2960
IPv6 ホスト	12.2(40)SE	2960
IP Phone 検出機能拡張	12.2(37)SE	3750、3560、2960
リンク層検出プロトコル（LLDP）および LLDP Media Endpoint Discovery（LLDP-MED）	12.2(37)SE	3750、3560、2960
PIM スタブ ルーティング	12.2(37)SE	3750、3560
PVLAN ホストでのポート セキュリティ	12.2(37)SE	3750、3560

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
VLAN 認識ポート セキュリティ オプション	12.2(37)SE	3750、3560、2960
マルチキャスト用自動ランデブー ポイント（Auto-RP）	12.2(37)SE	3750、3560
VLAN Flex Link ロード バランシング	12.2(37)SE	3750、3560、2960
Web Cache Communication Protocol（WCCP）	12.2(37)SE	3750、3560
マルチドメイン認証（MDA）	12.2(35)SE	3750、3560
Web 認証	12.2(35)SE	3750、3560、2960
MAC 非アクティブ エージング	12.2(35)SE	3750、3560、2960
Express Setup による IPv6 のサポート	12.2(35)SE	3750、3560
総合オンライン診断の設定	12.2(35)SE	3560
Stack MAC Persistent Timer および Archive Download の機能拡張	12.2(35)SE	3750
HSRP の拡張オブジェクト トラッキング	12.2(35)SE	3750、3560
OSPF および EIGRP ノンストップ フォワーディング機能（IP サービス イメージのみ）	12.2(35)SE	3750
インバウンド レイヤ 3 管理トラフィック用の IPv6 ルータ ACL	12.2(35)SE	3750、3560
スーパーバイザ エンジンのハードウェア機能をテストする総合オンライン診断の設定	12.2(25)SEE	3750
DHCP Option 82 が設定可能なリモート ID および回線 ID	12.2(25)SEE	3750、3560、2960
IP ベース イメージでの EIGRP スタブ ルーティング	12.2(25)SEE	3750、3560
ユニキャスト トラフィックの /31 ビット マスクのサポート	12.2(25)SEE	3750、3560
SDM テンプレートへのアクセス	12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール
IPv6 ACL	12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール
IPv6 Multicast Listener Discovery（MLD）スヌーピング	12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール
ポートでの QoS 階層型ポリシー マップ	12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール
NAC レイヤ 2 IEEE 802.1x 検証	12.2(25)SED	3750、3560、2960 Cisco EtherSwitch サービス モジュール
NAC レイヤ 2 IP 検証	12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
IEEE 802.1x アクセス不能認証バイパス	12.2(25)SED 12.2(25)SEE	3750、3560 Cisco EtherSwitch サービス モジュール 2960
制限付き VLAN を使用した IEEE 802.1x	12.2(25)SED	3750、3560、2960 Cisco EtherSwitch サービス モジュール
PoE ポートに接続された装置の電力バジェット	12.2(25)SEC	3750、3560 Cisco EtherSwitch サービス モジュール
IEEE 802.1s 標準に基づく Multiple Spanning Tree（MST）	12.2(25)SEC 12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール 2960
Unique Device Identifier（UDI）	12.2(25)SEC 12.2(25)SED	3750、3560 Cisco EtherSwitch サービス モジュール 2960
VRF Lite	12.2(25)SEC	3750、3560 Cisco EtherSwitch サービス モジュール
Wake-on-LAN 機能を使用した IEEE 802.1x	12.2(25)SEC 12.2(25)SED	3750、3560 2960、Cisco EtherSwitch サービス モジュール
ノンストップ フォワーディング（NSF）認識	12.2(25)SEC	3750、3560 Cisco EtherSwitch サービス モジュール
コンフィギュレーション ロギング	12.2(25)SEC 12.2(25)SED	3750、3560 2960、Cisco EtherSwitch サービス モジュール
Secure Copy Protocol（SCP）	12.2(25)SEC 12.2(25)SED	3750、3560 2960、Cisco EtherSwitch サービス モジュール
スタック間 EtherChannel	12.2(25)SEC	3750 Cisco EtherSwitch サービス モジュール
ダイナミック ARP インスペクション用に設定されたインターフェイスのプライベート VLAN	12.2(25)SEB	3750、3560
プライベート VLAN の IP ソース ガード	12.2(25)SEB	3750、3560
IEEE 802.1x の制限付き VLAN	12.2(25)SED	3750、3560、2960
IGMP Leave タイマー	12.2(25)SEB 12.2(25)SED	3750、3560、2960

表 7　Catalyst 3750、3560、3560-C、2960、2960-S、2960-C スイッチ、Cisco EtherSwitch サービス モジュール機能と必要な最小 Cisco IOS リリース （続き）

機能	必要な最小 Cisco IOS リリース	Catalyst スイッチ サポート
IGMP スヌーピング クエリア	12.2(25)SEA 12.2(25)FX	3750、3560、2960
高度な IP サービス	12.2(25)SEA	3750、3560
DSCP 透過性	12.2(25)SE 12.2(25)FX	3750、3560、2960
SVI での VLAN ベース QoS[1] および階層型ポリシー マップ[2]	12.2(25)SE	3750、3560
デバイス マネージャ	12.2(25)SE 12.2(25)FX	3750、3560、2960
IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリング	12.2(25)SE	3750、3560
レイヤ 2 ポイントツーポイント トンネリングとレイヤ 2 のポイントツーポイント トンネリングのバイパス	12.2(25)SE	3750、3560
セキュア HTTP 通信の SSL バージョン 3.0（暗号化イメージのみ）	12.2(25)SE 12.2(25)FX	3750、3560、2960
ダイナミック ARP インスペクション用に設定されたインターフェイスでのプライベート VLAN ポート（IP サービス イメージのみ）	12.2(25)SE	3750、3560
プライベート VLAN での IP ソース ガード（IP サービス イメージのみ）	12.2(25)SE	3750、3560
Cisco インテリジェント電力管理	12.2(25)SE	3750、3560
IEEE 802.1x アカウンティングおよび MIB（IEEE 8021-PAE-MIB および CISCO-PAE-MIB）	12.2(20)SE 12.2(25)FX	3750、3560、2960
ダイナミック ARP インスペクション	12.2(20)SE	3750、3560
Flex Link	12.2(20)SE 12.2(25)FX	3750、3560、2960
ソフトウェア アップグレード（デバイス マネージャ、または Network Assistant のみ）	12.2(20)SE 12.2(25)FX	3750、3560、2960
IP ソース ガード	12.2(20)SE	3750、3560
プライベート VLAN（IP サービス イメージのみ）	12.2(20)SE	3750、3560
SFP モジュール診断管理インターフェイス	12.2(20)SE 12.2(25)FX	3750、3560、2960
スイッチ スタックのオフライン設定	12.2(20)SE	3750
スタック リング アクティビティ統計情報	12.2(20)SE	3750
SmartPort マクロ	12.2(18)SE 12.2(25)FX	3750、3560、2960
総合オンライン診断（GOLD）	12.2(25)SEE	3750
Flex Link の優先スイッチオーバー	12.2(25)SEE	3750、3560、2960

1. QoS = Quality of Service
2. SVI = Switched Virtual Interface

制限事項

スイッチでの作業を開始する前にこの項を検討する必要があります。修正対象外の制限事項が記載されており、回避策がない場合もあります。記載どおりに動作しない機能や、スイッチ ハードウェアまたはソフトウェアに加えた最新の変更に影響を受ける機能があります。

Cisco IOS 制限事項

特に記載のない限り、以下の制限事項は、Catalyst 3750、3560、および 2960 スイッチおよび Cisco EtherSwitch サービス モジュールに適用されます。

設定

- 以前取得した DHCP IP アドレスのリース期限が切れるときに固定 IP アドレスが削除される可能性があります。

  この問題は、次の条件で発生します。

  - スイッチが設定なしで起動されたとき（フラッシュ メモリ内に config.text ファイルがない）。
  - スイッチへのアドレスを提供するように設定されている DHCP サーバにスイッチが接続されているとき（ダイナミック IP アドレスが VLAN 1 に割り当てられます）。

  - VLAN 1 に割り当てられたダイナミック アドレスのリース期限が切れる前に IP アドレスが VLAN 1 に設定されているとき。

  これは、スタティック IP アドレスを再設定することで回避できます。（CSCea71176 および CSCdz11708）

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）**show interface** 特権 EXEC コマンドを IEEE 802.1Q を実行するポートに対して入力すると、IEEE 802.1Q を実行するポートから矛盾する統計情報が報告される場合があります。

  これは、Cisco IOS Release 12.1(20)EA1 にアップグレードすることで回避できます。（CSCec35100）

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）非ルーテッド ポートからルーテッド ポートへ（またはその逆）ポートを変更する場合、適用される Auto QoS 設定が、**show running interface** または **show mls qos interface** ユーザ EXEC コマンドを使用して確認する際に変更または更新されません。

  回避策は以下のとおりです。

  1. インターフェイス上で Auto QoS をディセーブルにします。
  2. ルーテッド ポートから非ルーテッド ポート、またはその逆にルーテッド ポートを変更します。
  3. インターフェイス上で Auto QoS を再度イネーブルにします。（CSCec44169）

- プリアンブルを早期に送信するサードパーティ製デバイスに接続されている場合に、100 Mb/s 全二重または 100 Mb/s 半二重で動作するスイッチ ポートでライン プロトコルがアップまたはダウンになる場合があります。この問題は、スイッチがフレームを受信している場合のみに発生します。

  これは、10 Mb/s および半二重用にポートを設定するか、ハブまたは影響を受けないデバイスをスイッチに接続することで回避できます。（CSCed39091）

- DHCP スヌーピング バインディング データベースは、次の状況のいずれかの場合、フラッシュ メモリまたはリモート ファイルに書き込まれません。

  - （Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュール）Network Time Protocol（NTP）が設定されていますが、NTP クロックが同期していません。**show NTP status** 特権 EXEC コマンドを入力して、NTP サーバとピアへのネットワーク接続が正常に動作していることを確認することにより、クロックの状態を検査できます。
  - （Catalyst 3750 または 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）DHCP スヌーピング データベース ファイルはファイル システムから手動で削除されます。データベースの URL の設定により、DHCP スヌーピング データベースをイネーブルにすると、データベース ファイルが作成されます。ファイルがファイル システムから手動で削除されると、DHCP スヌーピング データベースによって、別のデータベース ファイルが作成されません。データベース ファイルを作成するには、DHCP スヌーピング データベースをディセーブルにしてから再度イネーブルにする必要があります。
  - （Catalyst 3750 または 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）設定された DHCP スヌーピング データベースの URL が、元の URL がアクセス可能ではなかったために置き換えられました。新しい URL が、古い URL のタイムアウト後に反映されない場合があります。

  必要な回避策はありません。これは故意の動作です。（CSCed50819）

- （Catalyst 3750 または 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）ダイナミック ARP インスペクションがスイッチまたはスイッチ スタックでイネーブルの場合、2016 バイトよりも大きい ARP および RARP パケットは、スイッチまたはスイッチ スタックによりドロップされます。これはハードウェアの制限です。

  ただし、ダイナミック ARP インスペクションがイネーブルでなく、ジャンボ MTU が設定されている場合、ARP パケットおよび RARP パケットはハードウェアで正しくブリッジングされます。（CSCed79734）

- （Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュール）スイッチの障害後にダイナミック ARP インスペクション ログ エントリが失われる可能性があります。障害が発生したスイッチ上で、ログ バッファに引き続き残っている（システム メッセージとして出力されていない）ログ エントリが失われます。

  show ip arp inspection log 特権 EXEC コマンドを入力すると、ログ エントリは、スタック内のすべてのスイッチからコマンドを入力したスイッチに移動します。

  回避策はありません。（CSCed95822）

- ポート セキュリティが制限モードのインターフェイス上でイネーブルに設定され、**switchport block unicast interface** コマンドがそのインターフェイスに入力された場合、MAC アドレスは、ブロックする必要がある場合に誤って転送されます。

  これは、その特定のインターフェイスで **no switchport block unicast** インターフェイス コンフィギュレーション コマンドを入力することで回避できます。（CSCee93822）

- SSL クライアント セッション後に暗号キーが生成されるとトレース バック エラーが発生します。

  回避策はありません。これは表面的なエラーであり、スイッチの機能には影響しません。（CSCef59331）

- （Cisco EtherSwitch サービス モジュール）スイッチ CLI を使用してコンソール ボー レートを変更できません。Cisco EtherSwitch サービス モジュールのコンソールは、3 個のボー レート（9600 b/s、19200 b/s および 38400 b/s）のみをサポートし、ブートローダ プロンプトで設定する必要があります。スイッチは、ボー レートを変更するために CLI コマンドを拒否します。

  ボー レートを変更するには、ブートローダ プロンプトで Cisco EtherSwitch サービス モジュールをリロードします。次にボー レートを変更し、Cisco EtherSwitch サービス モジュールのコンソールに接続されているルータの TTY 回線速度を変更できます。

  回避策はありません。（CSCeh50152）

- EtherChannel インターフェイスのポート チャネルのタイプがレイヤ 2 からレイヤ 3 またはその逆へ変更される場合、スイッチは次のようなトレース バックを表示する可能性があります。

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  （CSCsh12472 [Catalyst 3750 スイッチおよび 3560 スイッチ]）

- 遠端エラー オプション機能が GLC-GE-100FX SFP モジュールでサポートされていません。

  これは、アグレッシブ UDLD を設定することで回避策されます。（CSCsh70244）。

- ciscoFlashMIBTrap メッセージがスイッチの起動中に表示されます。これは、スイッチの機能には影響しません。（CSCsj46992）

- クライアントが設定のダウンロードを試みる時間を指定するため、**boot host retry timeout** グローバル コンフィギュレーション コマンドを入力してタイムアウト値を入力しないと、デフォルト値はクライアントが無限に試行することを意味するゼロとなります。ただし、クライアントは、設定のダウンロードを試行しません。

  これは、**boot host retry timeout** *timeout-value* コマンドを入力するときにタイムアウト値に常にゼロ以外の値を入力することで回避できます。（CSCsk65142）

- コンフィギュレーション ファイルがスイッチから削除され、スイッチがリブートされると、VLAN 1 と管理ポート（ファスト イーサネット 0）のポート ステータスは、`up` と報告される場合と `down` と報告される場合があり、矛盾が生じます。このステータスはリブート クエリーに応答した時点によって異なります。

  ```
  Would you like to enter the initial configuration dialog?
  ```

  - リブート後に VLAN 1 のライン プロトコルのステータスが応答前にコンソールに表示されるまで待機すると、VLAN 1 のライン ステータスは常に `down` と表示されます。これは正常な状態です。
  - VLAN 1 のライン ステータスがコンソールに表示される前にクエリーに応答すると、問題（`up` を報告する VLAN 1）が発生します。

  これは、クエリーに応答する前に、このステータスの報告後、VLAN 1 インターフェイスのライン ステータスがコンソールに表示されるまで約 1 分間待機することで回避できます。（CSCsl02680）（Catalyst 3750 スイッチおよび 3560 スイッチ）

- 起動後に、以下の条件で T-start エラー メッセージが表示されます。
  - 同じスイッチ上の 2 つのリンク ポートがクロス ケーブルで接続している。
  - スイッチが Cisco IOS 12.2(50)SE3 以降を実行している。

  これは、ストレート ケーブルで 2 個のポートを接続することで回避できます。（CSCsr41271）（Catalyst 3750V2 スイッチおよび Catalyst 3560V2 PoE スイッチおよび Cisco EtherSwitch サービス モジュールのみ）

- **show tech-support** 特権 EXEC コマンドを **remote command** {**all** | *stack-member-number*} 特権 EXEC コマンドを入力してから入力すると、完全な出力が表示されません。

  これは、**session** *stack-member-number* 特権 EXEC コマンドを使用することで回避できます。（CSCsz38090）

- 許可およびアカウンティングがスイッチ上でイネーブルになっていて、interface range コマンドを使用してインターフェイス範囲の設定を変更すると、この変更により CPU 使用率が高くなり、認証エラーが発生する可能性があります。

  これは、許可およびアカウンティングをディセーブルにするか、一度に 1 つのインターフェイスの設定変更を入力することで回避できます。（CSCsg80238、CSCti76748）

- Identity Services Engine（ISE）は、Catalyst 2000 シリーズ スイッチでは使用できません。
- **device-sensor accounting** グローバル コンフィギュレーション コマンドは、Catalyst 2000 シリーズ スイッチでは使用できません。

Ethernet

- （Cisco EtherSwitch サービス モジュール）Intel Pro1000 NIC の一部の古いモデルと 10/100/1000 スイッチ ポート インターフェイス間でがリンク接続が失われることがあります。接続の喪失は、Cisco EtherSwitch サービス モジュールの NIC とギガビット イーサネット ポート間で発生します。

  回避策は以下のとおりです。

  - NIC ベンダーに連絡し、カードの最新のドライバを入手します。

  - 10/100 Mb/s の代わりに 1000 Mb/s のインターフェイスを設定します。
  - ここに記載されていないインターフェイスに NIC を接続します。（CSCea77032）

  詳細については、次の URL にアクセスして、Bug Toolkit で *CSCea77032* を入力してください。
  http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl

- （Cisco EtherSwitch サービス モジュール）Cisco EtherSwitch サービス モジュールがリロードされるか、内部リンクがリセットされると、設定によって、PoE デバイスへの電力の供給で、最大 45 秒の遅延が発生する可能性があります。ルータに接続された Cisco EtherSwitch サービス モジュール上のギガビット イーサネット インターフェイスがアクセス モードまたはトランク モードのスイッチ ポートとして設定されている場合、内部リンクは STP フォワーディング ステートに到達するまで機能しません。したがって、ホスト ルータからの PoE も、内部ギガビット イーサネット リンクが STP フォワーディング ステートに到達するまで使用できません。これは、STP コンバージェンス時間が原因です。この問題は、ルーテッド ポートでは発生しません。

  Cisco EtherSwitch サービス モジュールがアクセス モードの場合は、内部ギガビット イーサネット インターフェイスで **spanning-tree portfast** インターフェイス コンフィギュレーション コマンドを使用することで回避できます。このサービス モジュールがトランク モードの場合、回避策はありません。

- EtherChannel ポートのトラフィックが、完全にロードバランシングされていません。EtherChannel ポートの出力トラフィックは、MAC または IP アドレスなどのロード バランス設定およびトラフィック特性のメンバー ポートに配信されます。複数のトラフィック ストリームが ASIC で計算されたハッシュの結果に基づいて同じメンバー ポートにマッピングされる場合があります。

  この場合、不均等なトラフィック分散が EtherChannel ポートで発生されます。

  ロード バランシングの配布方法を変更したり、EtherChannel のポート数を変更したりすると、この問題を解決できます。次のいずれかの回避策を使用して、EtherChannel ロード バランシングを改善します。

  - 任意の source-ip および dest-ip トラフィックの場合は、ロード バランス方式を **src-dst-ip** として設定します。
  - 増分 source-ip トラフィックの場合は、ロード バランス方式を **src-ip** として設定します。
  - 増分 dest-ip トラフィックの場合は、ロード バランス方式を **dst-ip** として設定します。
  - EtherChannel のポート数を 2 の倍数と等しくなる（つまり、2、4、または 8）ように設定します。

  たとえば、ロード バランスを 150 種類の増分宛先 IP アドレスを持つ **dst-ip** として設定し、EtherChannel のポート数を 2、4、8 のいずれかに設定している場合、負荷分散が最適です。（CSCeh81991）

EtherSwitch モジュール

- 2 つの EtherSwitch サービス モジュールに直接接続された 2 つのファスト イーサネット インターフェイスが 100 Mb/s と全二重の両方として、かつ自動速度とデュプレックス設定として設定されている場合、デュプレックスの不一致が発生します。これは、Cisco EtherSwitch サービス モジュールの PHY で予期される動作です。

  回避策はありません。（CSCeh35595）

フォールバック ブリッジング

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）ブリッジ グループにスタティック MAC アドレスが設定されている VLAN が含まれている場合、この MAC アドレスの宛先を持つブリッジ グループのすべての非 IP トラフィックはブリッジ グループのすべてのポートに送信されます。

  これは、ブリッジ グループから VLAN を削除するか、VLAN からスタティック MAC アドレスを削除することで回避できます。（CSCdw81955）

- （Catalyst 3750 または 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）セキュア アドレスがポートで認識済みあるいは設定済みで、このポートの VLAN がブリッジ グループの一部である場合、既知のユニキャスト（セキュア）アドレスがブリッジ グループ内にブラッディングされます。セキュア アドレスを宛先とする非 IP トラフィックがブリッジ グループ内にフラッディングされます。

  これは、フォールバック ブリッジングをディセーブルにするか、フォールバック ブリッジングに属するすべての VLAN 上のすべてのポートでポート セキュリティをディセーブルにすることで回避できます。ブリッジ グループからインターフェイスを削除したり、ブリッジ グループを削除したりするには、**no bridge-group** *bridge-group* インターフェイス コンフィギュレーション コマンドを使用します。フォールバック ブリッジングに属するすべての VLAN 上のすべてのポートでポート セキュリティをディセーブルにするには、**no switchport port-security** インターフェイス コンフィギュレーション コマンドを使用します。（CSCdz80499）

HSRP

- アクティブ スイッチで HSRP の冗長性を使用するスイッチ クラスタに障害が発生した場合、新しいアクティブ スイッチに完全なクラスタ メンバーのリストが含まれていない場合があります。

  これは、スタンバイ クラスタ メンバーのポートがスパニングツリー ブロッキング ステートになっていないことで回避できます。これらのポートがブロッキング ステートになっていないことを確認するには、ソフトウェア コンフィギュレーション ガイドの「Configuring STP」の章を参照してください。（CSCec76893）

IP

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）ARP のタイム アウト値が 15 秒で ARP 要求がタイムアウトになると、スイッチは隣接テーブル エントリを作成しません。

  これは、ARP タイムアウト値を 120 秒より小さい値に設定しないことで回避できます。（CSCea21674）

- 受信した DHCP 要求のレートが長期間にわたって 1 分間に 2,000 パケットを超えると、コンソールを使用している場合に応答時間が遅くなることがあります。

  これは、DoS 攻撃の発生を防ぐために DHCP トラフィックのレート制限を使用することで回避できます。（CSCeb59166）

IP テレフォニー

- IEEE 802.1x がイネーブルになっているポートのアクセス VLAN を変更した後、IP Phone のアドレスが削除されます。ラーニングが IEEE 802.1x 対応ポートに制限されているため、アドレスが再ラーニングされるまで約 30 秒かかります。

  回避策は不要です。（CSCea85312）

- （Catalyst 3750 スイッチまたは 3560 PoE 対応スイッチおよび Cisco EtherSwitch サービス モジュール）スイッチは、IEEE 分類機能を使用して、電源を投入する前の受電デバイスの最大消費電力を認識します。スイッチは、ポートに設定された最大ワット数が IEEE クラスの最大値以下の場合にのみ電力を供給します。これにより、スイッチの供給電力がオーバーサブスクライブしないようになります。シスコ先行標準の受電デバイスには、このような機能はありません。

  先行標準受電デバイスのネットワークの場合、最大ワット数をデフォルト値（15.4 W）のままにしておくことで回避できます。ポートの最大ワット数を、CDP メッセージを通じて電力消費として受電デバイスが報告する値以上に設定することもできます。IEEE クラス 0、3、または 4 デバイスのネットワークの場合、デフォルトの 15.4 W（15,400 ミリワット）未満でポートに最大ワット数を設定しないでください。（CSCee80668）

- 内部リンクがダウンしているため、スイッチ ポートが電話機に電力を供給できない場合は、スイッチ ポートに接続された大量の IEEE 電話によって生成される電話機検出イベントにより、大量の CPU 時間が消費されるおそれがあります。

  問題が解決しない場合、IP Phone に電力は供給していないが接続しているすべてのファスト イーサネット ポート上で **power inline never** インターフェイス コンフィギュレーション コマンドを入力すると回避できます。（CSCef84975、Cisco EtherSwitch サービス モジュールのみ）

- 一部のアクセス ポイント デバイスが、IEEE 802.3af Class 1 デバイスとして誤って検出されます。これらのアクセス ポイントはシスコ先行標準デバイスとして検出される必要があります。**show power inline** ユーザ EXEC コマンドにより、IEEE クラス 1 デバイスとしてのアクセス ポイントが示されます。

  これは、AC 壁面アダプタを使用して、アクセス ポイントに給電することで回避できます。（CSCin69533）

- Cisco 7905 IP Phone は、壁面コンセントに接続されると、errdisable となります。

  これは、PoE をイネーブルにし、PoE errdisable ステートから回復するようにスイッチを設定することで回避できます。（CSCsf32300）

MAC アドレッシング

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）MAC アドレスがルーテッド ポートの内部 VLAN でフィルタ用に設定されている場合、MAC アドレスからルーテッド ポートへの着信パケットがドロップされません。（CSCeb67937）

管理

CiscoWorks は Catalyst 3750-24FS スイッチではサポートされません。

マルチキャスト

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。Distance Vector Multicast Routing Protocol（DVMRP）トンネル インターフェイスのみがマルチキャスト ルーティングでサポートされます。

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）VLAN でブリッジングされるグループに対する Reverse Path Forwarding（RPF）以外の IP マルチキャスト トラフィックは、ポートが VLAN グループのメンバーでなくても、別の VLAN グループに属している場合、VLAN トランク ポートにリークされます。不要なトラフィックがトランク ポートで送信されるため、ポートの帯域幅が減少します。

非 RPF トラフィックが特定のトポロジで連続しているため、この問題に対する回避策はありません。トランク ポートが少なくとも 1 つの VLAN グループのメンバーである限り、この問題は、非 RPF トラフィックで発生します。（CSCdu25219）

- マルチキャスト ルート数および Internet Group Management Protocol（IGMP）グループが **show sdm prefer** グローバル コンフィギュレーション コマンドで指定された最大数より大きい場合は、不明なグループで受信されたトラフィックが受信した VLAN でフラッディングされます。このフラッディングは、**show ip igmp snooping multicast-table** 特権 EXEC コマンドから出力が示されても発生します。

  これは、マルチキャスト ルートの数と IGMP スヌーピング グループの数をサポートされている最大値よりも小さくすることで回避できます。（CSCdy09008）

- IGMP フィルタリングは、ハードウェアから転送されるパケットに適用されます。これはソフトウェアから転送されるパケットには適用されません。したがって、マルチキャスト ルーティングがイネーブルになっていると、最初のいくつかのパケットがポートから送信されます。これは、送信元のポートがあるグループを拒否するように IGMP フィルタリングが設定されていても発生します。

  回避策はありません。（CSCdy82818）

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）VLAN グループへのアクセスを拒否するルータ Access Control List（ACL）で **ip access-group** インターフェイス コンフィギュレーション コマンドを使用すると、VLAN で受信されたグループへのマルチキャスト データは、VLAN の IGMP グループ メンバーシップに関係なく、VLAN で常にフラッディングされます。これにより、VLAN で直接接続されたクライアントがある場合、このクライアントに対する到達可能性が提供されます。

  これは、VLAN インターフェイスへのアクセスを拒否するルータ ACL セットを適用しないことで回避できます。他の方法でセキュリティを適用します。たとえば、グループのルータ ACL を使用する代わりに、VLAN に VLAN マップを適用します。（CSCdz86110）

- （Catalyst 3750 スイッチ スタック）**ip mroute** グローバル コンフィギュレーション コマンドを入力した直後にスタック マスターに電源が再投入された場合、スタック マスター変更後にこの設定変更が失われる可能性がわずかにあります。これは、電力が供給される前に、すべてのスタック メンバーに実行コンフィギュレーションを伝播する時間がスタック マスターになかったために発生します。この問題は、他のコンフィギュレーション コマンドに影響を与える可能性もあります。

  回避策はありません。（CSCea71255）

- （Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュール）トンネル インターフェイスの IP Protocol Independent Multicast（PIM）をイネーブルにすると、スイッチは `Multicast is not supported on tunnel interfaces` というエラー メッセージを誤って表示します。IP PIM はトンネル インターフェイスではサポートされません。

  回避策はありません。（CSCeb75366）

- IGMP レポート パケットに 2 個のマルチキャスト グループ レコードがある場合、スイッチはパケットの次のレコードの順に応じて、インターフェイスを削除または追加します。
  - ALLOW_NEW_SOURCE レコードが BLOCK_OLD_SOURCE レコードの前にある場合、このスイッチで、ポートがグループから削除されます。
  - BLOCK_OLD_SOURCE レコードが ALLOW_NEW_SOURCE レコードの前にある場合、このスイッチで、ポートがグループに追加されます。

  回避策はありません。（CSCec20128）

- IGMP スヌーピングがディセーブルで、**switchport block multicast** インターフェイス コンフィギュレーション コマンドを入力すると、IP マルチキャスト トラフィックはブロックされません。

  switchport block multicast インターフェイス コンフィギュレーション コマンドは、非 IP マルチキャスト トラフィックのみに適用できます。

  回避策はありません。（CSCee16865）

- 不完全なマルチキャスト トラフィックは次のいずれかの条件の下で確認できます。
  - IP マルチキャスト ルーティングをディセーブルにするか、インターフェイスでグローバルに再度イネーブルにする。
  - スイッチの mroute テーブルが一時的にリソース不足になり、後で回復する。

  これは、インターフェイスで **clear ip mroute** 特権 EXEC コマンドを入力することで回避できます。（CSCef42436）

  ip igmp join-group *group-address* インターフェイス コンフィギュレーション コマンドを入力して、マルチキャスト グループに加入するスイッチを設定後、スイッチはクライアントから参加パケットを受信せず、クライアントに接続されているスイッチ ポートが IGMP スヌーピング転送テーブルから削除されます。

  次のいずれかの回避策を使用します。
  - SVI で **no ip igmp join-group** *group-address* インターフェイス コンフィギュレーション コマンドを使用してマルチキャスト グループ内のメンバーシップをキャンセルします。
  - **no ip igmp snooping vlan** *vlan-id* を使用して、VLAN インターフェイスで IGMP スヌーピングをディセーブルにします。（CSCeh90425）

電力

- ネットワークに接続された非 PoE デバイスが IEEE 802.3af 準拠の受電デバイスであると誤って検出され、Cisco EtherSwitch サービス モジュールから電力が供給された可能性があります。

  回避策はありません。PoE デバイスに接続されていない Cisco EtherSwitch サービス モジュール ポート上で **power inline never** インターフェイス コンフィギュレーション コマンドを使用する必要があります。（CSCee71979）

- **show power inline** 特権 EXEC コマンドを入力すると、出力はルータにすべての Cisco EtherSwitch サービス モジュールが使用する総電力を示します。表示される残りの電力はルータにすべての Cisco EtherSwitch サービス モジュールのスイッチング ポートへの割り当てに使用できます。

  特定の EtherSwitch サービス モジュールが使用する総電力を表示するには、ルータに対して **show power inline** コマンドを入力します。この出力は次のように表示されます。

```
Router# show power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS           0       360.000   121.000         PS1 GOOD   PS2 ABSENT
Interface   Config   Device    Powered    PowerAllocated
---------   ------   ------    -------    --------------
Gi4/0       auto     Unknown   On         121.000 Watts
```

  これは、システム上の使用電力の合計と利用可能な残りの電力を正しく示しているため、問題ではありません。（CSCeg74337）

- 内部リンクで **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると、PoE 操作を中断できます。内部リンクがシャットダウン状態の間に新しい IP Phone が追加され、内部リンクが 5 分以内に起動された場合、その IP Phone にはインライン パワーが与えられません。

  これは、内部リンクが起動されてからサービス モジュール ポートに接続した新しい IP Phone のファスト イーサネット インターフェイス上で **shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力することで回避できます。（CSCeh45465）

QoS

- バッファ サイズまたはしきい値レベルが **mls qos queue-set output-set output** グローバル コンフィギュレーション コマンドによって非常に低く設定されている場合、一部のスイッチがディセーブルになります。バッファ サイズとしきい値レベルの比率は、キューをディセーブルにすることを避けるため、10 より大きくする必要があります。

  これは、互換性のあるバッファ サイズとしきい値レベルを選択することで回避できます。（CSCea76893）

- Auto QoS がスイッチでイネーブルの場合、プライオリティ キューイングはイネーブルになりません。代わりに、スイッチはキューイング メカニズムとして Shaped Round Robin（SRR）を使用します。Auto QoS 機能は、フィーチャ セットおよびハードウェアの制限に基づいて各プラットフォームで設計され、各プラットフォームでサポートされるキューイング メカニズムが異なる可能性があります。回避策はありません。（CSCee22591）

- クラス マップに大量の入力インターフェイス VLAN を設定するときは、次のようなトレース バック メッセージが表示されることがあります。

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  スイッチ機能には影響しません。

  回避策はありません。（CSCtg32101）

RADIUS

- RADIUS 認可変更（COA）の再認可はクリティカル認証 VLAN ではサポートされません。

  回避策はありません。（CSCta05071）

ルーティング

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）スイッチは、ユニキャスト ルーテッド トラフィックのトンネル インターフェイスをサポートしません。Distance Vector Multicast Routing Protocol（DVMRP）トンネル インターフェイスのみがマルチキャスト ルーティングでサポートされます。

- （Catalyst 3750 または 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）Differentiated Services Code Point（DSCP）句付きの ACL を含むルート マップは、レイヤ 3 インターフェイスに適用できません。スイッチはこの設定を拒否し、ルート マップがサポートされていないことを示すメッセージが表示されます。

  回避策はありません。（CSCea52915）

- 多数のスイッチ仮想インターフェイス（SVI）、ルート、または両方を、フル装備のメンバー スイッチ スタックに備えた Catalyst 3750 または Cisco EtherSwitch サービス モジュールのスイッチ スタックで、スイッチ スタックをリロードするか、スタックにスイッチを追加するとこのメッセージが表示される場合があります。

```
%SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
Pool: I/O Free: 77124  Cause: Memory fragmentation
Alternate Pool: None Free: 0  Cause: No Alternate pool
```

このエラー メッセージは、一時メモリ不足があるが通常は自動的に復旧することを意味します。**show cef line** ユーザ EXEC コマンドを入力し、ラインカード ステートが `up` および `sync` であることを確認することにより、スイッチ スタックが復旧していることを確認することができます。

問題が自動的に修正されため、回避策は不要です。（CSCea71611）

- （Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュール）スパニングツリー ループは、次の条件をすべて満たす場合に発生する可能性があります。
  - ポート セキュリティは、違反モードを保護に設定している場合にイネーブルになっている。
  - セキュア アドレスの最大数が、ポートに接続されているスイッチの数よりも小さくなっている。
  - MAC アドレスが保護されていないスイッチを介するネットワークに物理ループがあり、そのループの BPDU によりセキュア違反が発生する。

  これは、リストの条件のいずれかを変更することで回避できます。（CSCed53633）

Smart Install

- スタック内のスイッチをアップグレードするときに、スタック内のすべてのスイッチが同時に起動しないと、ディレクタがスタックに適切なイメージと設定を送信できません。スタック内のスイッチは、誤ったイメージや設定を受け取る可能性があります。

  これは、**vstack download config** および **vstack download image** コマンドを入力して、スタック内のスイッチのアップグレードにオンデマンド アップグレードを使用することで回避できます。（CSCta64962）

- Smart Install ディレクタを Cisco IOS Release 12.2(55)SE にアップグレードする一方で、ディレクタ設定をアップグレードしないと、ディレクタはクライアント スイッチをアップグレードできません。

  Cisco IOS Release 12.2(55)SE にディレクタをアップグレードするときに、すべての組み込み、カスタム、デフォルトの各グループを含むように設定を変更することでも回避できます。保存されたイメージのイメージ リスト ファイル名の代わりに tar イメージ名を設定する必要もあります。（CSCte07949）

- バックアップ リポジトリが Windows サーバで、バックアップ ファイルがサーバにすでに存在する場合、Smart Install 設定のバックアップに失敗する可能性があります。

  これは、別のサーバの TFTP ユーティリティを Windows サーバの代わりに使用するか、再びバックアップする前に既存のバックアップ ファイルを手動で削除することで回避できます。（CSCte53737）

- Smart Install ネットワークで、ディレクタがクライアントと DHCP サーバの間で接続され、サーバにイメージと設定用にオプションが設定されている場合、クライアントは、自動アップグレード中に DHCP サーバから送信されるイメージ ファイルとコンフィギュレーション ファイルを受信しません。代わりにファイルがディレクタによって上書きされ、クライアントはディレクタが送信するイメージと設定を受信します。

  次のいずれかの回避策を使用します。

  - クライアントが、DHCP サーバ オプションで設定されたイメージ ファイルとコンフィギュレーション ファイルを使用してアップグレードする必要がある場合、アップグレード中に Smart Install ネットワークからクライアントを除外する必要があります。

  - Smart Install を使用するネットワークでは、DHCP サーバでのイメージと設定用にオプションを設定しないでください。Smart Install を使用してアップグレードするクライアントの場合、製品特定のイメージ ファイルとコンフィギュレーション ファイルをディレクタに指定する必要があります。（CSCte99366）

- バックアップ機能をイネーブルにした Smart Install ネットワーク（デフォルト）では、ディレクタは、ゼロ タッチ交換中に、クライアントにバックアップ コンフィギュレーション ファイルを送信します。ただし、クライアントがスタック内のスイッチの場合、クライアントは、バックアップ コンフィギュレーション ファイルを受信する代わりに、シード ファイルを受信します。

  バックアップ設定を使用してスタックにスイッチを設定する必要がある場合、**vstack download config** 特権 EXEC コマンドを使用して、ディレクタがクライアントでオンデマンド アップグレードを行うことで回避できます。

  - バックアップ設定がリモート リポジトリに保存される場合は、リポジトリの場所を入力します。
  - バックアップ ファイルがディレクタのフラッシュ メモリに格納されている場合、**vstack download config** コマンドを入力する前に、手動でファイルの権限を設定する必要があります。（CSCtf18775）

- Smart Install ネットワークのディレクタがアクセス ポイントと DHCP サーバの間にある場合、アクセス ポイントがサポートされていない場合でもアップグレードするため、アクセス ポイントは Smart Install 機能を使用しようとします。ディレクタにアクセス ポイントに対してイメージ ファイルとコンフィギュレーション ファイルがない場合に失敗します。

  回避策はありません。（CSCtg98656）

- Smart Install ディレクタが、Smart Install 対応ではない（つまり、Cisco IOS Release 12.2(52)SE 以降を実行している）クライアント スイッチをアップグレードしている場合、ディレクタはクライアント スイッチに設定されているパスワードを入力する必要があります。クライアント スイッチに設定されたパスワードがない場合、クライアント上で実行されるソフトウェア リリースに応じて、予期せぬ結果が発生します。

  - ディレクタ CLI に [NONE] オプションを選択すると、Cisco IOS Release 12.2(25)SE から 12.2(46)SE までを実行しているクライアント スイッチでアップグレードが許可され、正常に終了にしている必要があります。一方 Cisco IOS Release 12.2(50)SE から 12.2(50)SEx までを実行するクライアントで失敗します。
  - ディレクタ CLI に任意のパスワードを入力すると、Cisco IOS Release 12.2(25)SE から 12.2(46)SE までを実行しているクライアント スイッチでアップグレードが許可されていないが、正常に終了にしている必要があります。一方 Cisco IOS Release 12.2(50)SE から 12.2(50)SEx までを実行するクライアントで失敗します。

  回避策はありません。（CSCth35152）

SPAN および RSPAN

- （Cisco EtherSwitch サービス モジュール）パスを指定されたユニキャスト トラフィックの出力 SPAN コピーには、ローカルとリモートの両方の SPAN セッションに関する不正な宛先 MAC アドレスが含まれることがあります。この制限事項はブリッジド パケットには適用されません。ローカル SPAN の場合、**replicate** オプションを使用することで回避できます。リモート SPAN セッションの場合、対応策はありません。

  これはハードウェアの制限で、Cisco EtherSwitch サービス モジュール（CSCdy72835）にのみ適用されます。

- （Cisco EtherSwitch サービス モジュール）出力 SPAN ルーテッド パケット（ユニキャストとマルチキャストの両方）に間違った送信元 MAC アドレスが示されます。リモート SPAN パケットの場合、送信元 MAC アドレスは出力 VLAN の MAC アドレスである必要がありますが、代わりにパケットに RSPAN VLAN の MAC アドレスが表示されます。宛先ポートでネイティブ カプセル化を使用したローカル SPAN パケットの場合、パケットには VLAN 1 の MAC アドレスが表示されます。カプセル化レプリケーション オプションが使用されている場合、この問題はローカル **encapsulation replicate** では現れません。この制限事項はブリッジド パケットには適用されません。回避方法として、**monitor session** グローバル コンフィギュレーション コマンドの **encapsulate replicate** キーワードを使用します。これ以外の場合、回避策はありません。

  これはハードウェアの制限で、Cisco EtherSwitch サービス モジュール（CSCdy81521）にのみ適用されます。

- （Cisco EtherSwitch サービス モジュール）トラフィックが非常に混んでいる間に 2 つの RSPAN 送信元セッションが設定されると、片方の RSPAN セッションのパケットの VLAN ID が別の RSPAN セッションのパケットの VLAN ID を上書きします。上書きされると、この RSPAN VLAN 対象のパケットが誤って別の RSPAN VLAN に送信されます。この問題により RSPAN 宛先セッションは影響を受けません。回避策は RSPAN 送信元セッションを 1 つだけ設定することです。

  これはハードウェアの制限で、Cisco EtherSwitch サービス モジュール（CSCea72326）にのみ適用されます。

- （Catalyst 3750 スイッチまたは 3560 スイッチおよび Cisco EtherSwitch サービス モジュール）出力 SPAN のデータ レートは、フォール バック ブリッジングまたはマルチキャスト ルーティングがイネーブルの場合にパフォーマンスが低下する可能性があります。低下量は、プロセッサの負荷によって異なります。通常、スイッチは最大 40,000 pps（64 バイトのパケット）で SPAN を出力できます。モニタ対象トラフィックの合計がこの制限よりも小さければ、低下しません。ただし、モニタ対象トラフィックが制限を超えると、ソース ストリームの一部だけがスパニングされます。その場合、`Decreased egress SPAN rate` というコンソール メッセージが表示されます。いずれの場合も、通常のトラフィックは影響を受けません。パフォーマンス低下は、元のソース ストリームからスパニング出力される量のみに限定されます。フォール バック ブリッジングおよびマルチキャスト ルーティングがディセーブルの場合、出力 SPAN は低下しません。

  回避策はありません。可能な場合は、フォール バック ブリッジングおよびマルチキャスト ルーティングをディセーブルにします。可能であれば、同じトラフィックを監視するための入力 SPAN を使用します。（CSCeb01216）

- Catalyst 3750 スイッチ、Catalyst 3560 スイッチ、または Cisco EtherSwitch サービス モジュールでは、IP オプションを持つ一部の IGMP レポートおよびクエリー パケットが入力スパニングされない場合があります。この問題の影響を受けやすいパケットは、4 バイトの IP オプション（IP ヘッダー長が 24 バイト）を含む IGMP パケットです。このようなパケットの例では、ルータ アラート IP オプションを持つ IGMP レポートおよびクエリーとなります。このようなパケットの入力スパニングは正確ではなく、トラフィック レートによって異なる場合があります。通常、スパニングされるのはごく少数であるか、いずれのパケットもスパニングされません。

  回避策はありません。（CSCeb23352）

- SPAN 送信元から受信された Cisco Discovery Protocol（CDP）、VLAN Trunking Protocol（VTP）、および Port Aggregation Protocol（PAgP）パケットはローカル SPAN セッションの宛先インターフェイスに送信されません。これは、ローカル SPAN について **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} グローバル コンフィギュレーション コマンドを使用することで回避できます。（CSCed24036）

スパニングツリー プロトコル

- CSCtl60247

  Multiple Spanning Tree（MST）を実行しているスイッチまたはスイッチ スタックが Rapid Spanning Tree Protocol（RSTP）を実行しているスイッチに接続されている場合、MST スイッチがルート ブリッジとして機能し、RST のスイッチに接続する境界ポートで、各 VLAN Spanning Tree（PVST）のシミュレーション モードを実行します。これらのスイッチを接続しているすべてのトランク ポートで許可された VLAN を VLAN 1 以外の VLAN に変更し、RSTP スイッチのルート ポートがシャット ダウンされた後でイネーブルにされている場合、ルート ポートに接続する境界ポートは、PVST+ のスロー移行を通過せずに転送ステートにただちに移行します。

  回避策はありません。

スタック（Catalyst 3750 または Cisco EtherSwitch サービス モジュールのスイッチ スタックのみ）

- 複数の VLAN の追加後ただちにスタック マスターがリロードされると、新しいスタック マスターが失敗する可能性があります。これは、スタック マスターをリロードする前に VLAN を追加してから数分間待つことで回避できます。（CSCea26207）
- コンソール速度がスタックで変更された場合、コンフィギュレーション ファイルは更新されますが、ボー レートは更新されません。スイッチがリロードされると、コンフィギュレーション ファイルが解析され、コンソール速度が正しい値に設定される前に、無意味な文字が起動時にコンソールに表示されることがあります。コンソール速度を変更した後に、手動による起動がイネーブルであるか、またはスタートアップ コンフィギュレーションが削除されると、スイッチの再起動後にコンソールにアクセスできません。

  回避策はありません。（CSCec36644）
- スイッチがギガビットの入力インターフェイスから 100 Mb/s の出力インターフェイスにトラフィックを転送する場合は、出力インターフェイスがギガビット イーサネット スイッチにある場合よりもファスト イーサネット スイッチにある場合に、オーバーサブスクリプションにより、入力インターフェイスがより多くのパケットをドロップする可能性があります。

  回避策はありません。（CSCed00328）
- スタックがスタックから削除され、設定が保存されていないか、別のスイッチがスタックに同時に保存されない場合、最初のメンバー スイッチの設定が失われる可能性があります。

  これは、スタック内のスイッチを削除または交換する前にスタック設定を保存することで回避できます。（CSCed15939）
- **switchport** および **no switchport** インターフェイス コンフィギュレーション コマンドが Catalyst 3750 スイッチのポートまたは Cisco EtherSwitch サービス モジュールで 20,000 回を超えて入力されると、すべての使用可能なメモリが使用され、スイッチは停止します。

  回避策はありません。（CSCed54150）
- プライベート VLAN ドメインで、デフォルトのプライベート VLAN IP ゲートウェイのみがスティッキ ARP をイネーブルにします。プライベート VLAN をイネーブルにする中間レイヤ 2 スイッチがスティッキ ARP をディセーブルにします。スタック マスターの再選択が Catalyst 3750 または Cisco EtherSwitch サービス モジュールのデフォルト IP ゲートウェイの 1 個で発生すると、メッセージ `IP-3-STCKYARPOVR` が他のデフォルト IP ゲートウェイのコンソールに表示されます。スティッキ ARP がディセーブルになっていないため、スタック マスターの再選択による MAC アドレスの更新は完了できません。

  これは、**clear arp** 特権 EXEC コマンドを入力して、MAC アドレスの更新を完了することで回避できます。（CSCed62409）

- Catalyst 3750 スイッチまたは Cisco EtherSwitch サービス モジュールがスイッチ スタックにリロードされ、Cisco Express Forwarding（CEF）テーブルがスイッチにダウンロードされている間、パケット損失が最大 1 分発生する可能性があります。これはリロードされているスイッチを経由するトラフィックだけに影響します。

  回避策はありません。（CSCed70894）

- 矛盾したプライベート VLAN の設定は、新しいスタック マスターが IP ベース イメージを実行し、古いスタック マスターが IP サービス イメージを実行している場合にスイッチ スタックで発生する可能性があります。

  プライベート VLAN は、スタック マスターが IP サービス イメージまたは IP ベース イメージを実行しているかどうかによって、スイッチ スタック上でイネーブルまたはディセーブルになります。

  - スタック マスターが IP サービス イメージを実行している場合、すべてのスタック メンバーでプライベート VLAN をイネーブルにします。
  - スタック マスターが IP ベース イメージを実行している場合は、すべてのスタック メンバーでプライベート VLAN をディセーブルにします。

  これは、以前のスタック マスターが IP サービス イメージを実行し、新しいスタック マスターが IP ベース イメージを実行している場合に、スタック マスターの再選択後に発生します。スタック メンバーをプライベート VLAN に設定されますが、スタックを結合した新しいスイッチでプライベート VLAN をディセーブルにします。

  回避策は以下のとおりです。これらの 1 つのみが必要です。

  - IP サービス イメージから IP ベース イメージにマスター スイッチが変更された（またはその逆）後に、スタックをリロードします。
  - IP サービス イメージから IP ベース イメージにマスター スイッチが変更される前に、既存のスタック マスターから、プライベート VLAN の設定を削除します。（CSCee06802）

- ポート設定情報は、Catalyst 3750 スイッチで、**switchport** モードから **no switchport** モードに変更される際に失われません。

  これはオフライン設定（プロビジョニング）機能の動作と考えられます。回避策はありません。（CSCee12431）

- Cisco EtherSwitch サービス モジュールのセッションの補助ポート経由でルータに接続されている場合、サービス モジュール セッションは、サービス モジュールのルータ インターフェイス上で、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを入力すると失敗します。

  回避策は以下のとおりです。

  - ルータをリロードします。
  - ルータにコンソール ポート経由で接続し、サービス モジュールへのセッションを開きます。（CSCeh01250）（Cisco EtherSwitch サービス モジュール）

- Catalyst 3750 スイッチのスタック内の 1 つのスイッチが、起動可能イメージを検索するために他のスイッチよりも多くの時間が必要な場合は、スタック マスター選択のウィンドウが欠落している可能性があります。ただし、スイッチは、スタック マスター選択に割り当てられていない場合でも、メンバーとしてスタックに加わります。

  これは、親ディレクトリまたは最初のディレクトリへブート可能イメージをコピーすることで回避できます。（CSCei69329）

- ルート ブリッジへのパス コストが、スタック ルート上のポートと、非スタック ルート上のポートで等しい場合、BLK ポートは、指定ブリッジ プライオリティが変更されるとスタックで正しく選択されません。この問題は、PVST、Rapid-PVST+、および MST モードで稼働するスイッチで出現します。

これは、転送ポートにより低いパス コストを割り当てることで回避できます。（CSCsd95246）

- 3750 スイッチのスタックがクロススタック EtherChannel に設定され、EtherChannel の物理ポートの 1 つにリンクアップまたはリンク ダウン イベントが発生した場合、スタックは EtherChannel 間で重複したパケットを送信している可能性があります。問題は、条件を変更し、アクティブな物理ポートの新しい設定にロード バランス アルゴリズムを採用するために、スイッチ スタックが EtherChannel を調整している間の非常に短い期間中に発生します。

  これはリンク フラップ中に常に発生するわけではなく、数ミリ秒以上は持続しません。この問題は、モードを ON または LACP に設定したクロススタック EtherChannel で発生する可能性があります。

  回避策はありません。手動操作は必要ではありません。問題は、スタックのすべてのスイッチとしてリンク フラップが新しいロードバランス設定と同期化した後で短時間に自動的に修正されます。（CSCse75508）

- 入力されたスタック マスターの実行コンフィギュレーションにスイッチのコンフィギュレーションをコピーするため、新しいメンバー スイッチがコマンドの 30 秒以内にスイッチ スタックに加入すると、新しいメンバーは最新の実行コンフィギュレーションを取得せず、正しく機能しない可能性があります。

  これは、新しいメンバー スイッチをリブートすることで回避できます。**remote command all show run** 特権 EXEC コマンドを使用して、スタック メンバーの実行コンフィギュレーションを比較します。（CSCsf31301）

- エラー メッセージ `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` は、次の条件でスイッチ スタックに発生する可能性があります。

  - IEEE 802.1 がイネーブルになっている。
  - サプリカントが少なくとも 1 つのポートで認証されている。
  - 新しいメンバーがスイッチ スタックに加入している。

  次のいずれかの回避策を使用します。

  - **shutdown** および no shutdown インターフェイス コンフィギュレーション コマンドを入力してポートをリセットします。
  - VLAN を削除し、再設定します。（CSCsi26444）

- Catalyst 3750 スイッチおよび Catalyst 3750-E スイッチが混在するスタックでは、スタックがリロードすると、Catalyst 3750-E は、スイッチ プライオリティがより高く設定されていてもスタック マスターにならない可能性があります。

  これは、フラッシュを検査することで回避できます。これは多くのファイルが含まれている場合は、不要なものを削除します。フラッシュ内の lost and found ディレクトリを点検し、多くのファイルが含まれている場合は削除します。番号を調べるにはファイルは **fsck flash:** コマンドを使用します。（CSCsi69447）

- 次の手順を実行すると、スタック メンバー スイッチがレイヤ 2 プロトコル トンネル ポートをポート チャネルにバンドルできない場合があります。

  1. マスター スイッチにレイヤ 2 プロトコル トンネル ポートを設定します。
  2. メンバー スイッチにレイヤ 2 プロトコル トンネル ポートを設定します。
  3. マスター スイッチのレイヤ 2 プロトコル トンネル ポートにポート チャネルを追加します。
  4. メンバー スイッチのレイヤ 2 プロトコル トンネル ポートにポート チャネルを追加します。

  この手順のシーケンスの後に、メンバー ポートは一時停止状態のままになることがあります。

  これは、レイヤ 2 プロトコル トンネルと同時に、ポート チャネルとしてメンバー スイッチにポートを設定することで回避できます。次に例を示します。

```
Switch(config)# interface fastethernet1/0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# channel-group 1 mode on
```
(CSCsk96058) (Catalyst 3750 switches)

- スタックの起動後、ポートが認証済みステートの場合でも、IEEE 802.1x をイネーブルにしているポートのスパニングツリー ステートがブロックされている可能性があります。これは、PortFast 機能がイネーブルの音声ポートで発生する可能性があります。

  ブロック ステートのポートに **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、続けて **no shutdown** コマンドを入力することで回避できます。（CSCsl64124）

- スイッチ スタックが 802.1x シングル ホスト モード認証を実行していて、インターフェイスに適用されるフィルタ ID またはユーザ単位ポリシー マップがある場合は、ポリシーはマスター スイッチオーバーが発生すると削除されます。**show ip access-list** 特権 EXEC コマンドの出力は、これらの ACL が含まれていたとしても、ポリシーは適用されません。

  これは、**shutdown** インターフェイス コンフィギュレーション コマンドを入力し、続けて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力することで回避できます。（CSCsx70643）（Catalyst 3750 switch）

- スイッチ スタックが HSRP アクティブ ステートになっていて、マスターの切り替えが発生すると、HSRP 仮想 IP アドレスを使用してスタック接続を確認できません。

  回避策はありません。（CSCth00938）（Catalyst 3750 スイッチおよび 2960-S スイッチ）

トランキング

- スイッチは、混合カプセル化（IEEE 802.1Q およびスイッチ間リンク [ISL]）で受信されるフレームを FCS エラー付きフレームとして処理し、エラー カウンタを増やし、ポート LED がオレンジで点滅します。これは、ISL を認識しないデバイスが ISL カプセル化パケットを受信し、IEEE 802.1Q トランク インターフェイスにフレームを転送したときに発生します。

  回避策はありません。（CSCdz33708）

- IP Phone が設定された IP オプションが、トランク ポートでリークされることがあります。たとえば、トランク ポートは、VLAN X の IP マルチキャスト グループのメンバーですが、VLAN Y のメンバーではありません。VLAN Y がマルチキャスト グループに割り当てられたマルチキャスト ルート エントリの出力インターフェイスと VLAN Y のインターフェイスが同じマルチキャスト グループに属する場合、VLAN Y のインターフェイス以外の入力 VLAN インターフェイスで受信した IP オプションのトラフィックは、ポートに VLAN Y のグループ メンバーシップがなくてもトランク ポートが VLAN Y で転送しているため、VLAN Y のトランク ポートで送信されます。

  回避策はありません。（CSCdz42909）。

- Catalyst 3750 スイッチ スタックが指定ブリッジに接続され、スイッチ スタックのルート ポートが代替ルート ポートと別のスイッチにある場合、指定ブリッジの指定ポートのポート プライオリティを変更すると、Catalyst 3750 スイッチ スタックのルート ポート選択の効果はありません。

  回避策はありません。（CSCea40988）

- IEEE 802.1Q タギングが設定されたトランク ポートまたはアクセス ポートの場合、矛盾する統計情報が **show interfaces counters** 特権 EXEC コマンド出力で表示される可能性があります。ポート LED がオレンジで点滅していても、64 ～ 66 バイトの有効な IEEE 802.1Q フレームが正しく転送され、このフレームはインターフェイス統計情報に含まれません。

  回避策はありません。（CSCec35100）。

VLAN

- VLAN の数とトランク ポートの数を掛けたものが 13,000 の推奨限度を超える場合、スイッチに失敗することがあります。

  これは、VLAN またはトランクの数を削減することで回避できます。（CSCeb31087）

- （Catalyst 3750 スイッチまたは 3560 スイッチ）プライベート VLAN を設定するときに CPUHOG メッセージが表示されることがあります。プライベート VLAN の設定に影響される 1 つ以上のポートでポート セキュリティをイネーブルにします。

  回避策はありません。（CSCed71422）

- （Catalyst 3750）VLAN 単位の Quality of Service（QoS）を適用すると、VLAN Switched Virtual Interface（SVI）へのポート単位のポリサーのポリシー マップは、使用中の下位レベル（子）のポリシー マップを別のポリシー マップで再使用することはできません。

  これは、別のポリシー マップに使用するものと同じ設定で、下位レベルのポリシー マップに別のポリシー マップ名を定義することで回避できます。（CSCef47377）

- ダイナミック ARP インスペクションを VLAN に設定し、VLAN ポートの ARP トラフィックが設定済みレート制限内である場合、ポートは errdisable ステートになる可能性があります。

  これは、バースト間隔を 1 秒より長く設定すると回避できます。（CSCse06827、Catalyst 3750 スイッチのみ）

- ライン レートのトラフィックがダイナミック ポートを通過していて、ポート範囲について **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力した場合、VLAN が正しく割り当てられない可能性があります。ヌル ID のある 1 つ以上の VLAN は、代わりに MAC アドレス テーブルに表示されます。

  これは、各ポートで **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを個別に入力することで回避できます。（CSCsi26392）

- 多数の VLAN がスイッチに設定されている場合、多くのリンクが同時にフラッピングしていると高い CPU 使用率が発生します。

  これは、多くのリンクがフラッピングしている場合に CPU 使用率を抑えるために不要な VLAN を排除することで回避できます。（CSCtl04815）

デバイス マネージャの制限

- セキュリティ証明書を受け入れるようにプロンプトが表示され、[No] をクリックすると、画面だけが表示され、デバイス マネージャは起動されません。

  これは、証明書を受け入れるようにプロンプトが表示され、[Yes] をクリックすることで回避できます。（CSCef45718）

特記事項

スイッチ スタックに関する注意事項

- スイッチ スタックへのスイッチの追加または取り外しの際には、必ずスイッチの電源をオフにしてください。
- Catalyst 3560 スイッチは、スイッチのスタック構成をサポートしません。ただし、**show processes** 特権 EXEC コマンドは、まだスタック関連プロセスを示します。これは、次のスイッチがスタッキングをサポートする他のスイッチと共通するコードを共有するためです。
- Cisco IOS Release 12.2(25)SEB を実行している Catalyst 3750 スイッチは、Cisco IOS Release 12.2(25)EZ を実行している Cisco EtherSwitch サービス モジュールと互換性があります。Catalyst 3750 スイッチと Cisco EtherSwitch サービスモジュールは、同じスイッチ スタックに共存できます。このようなスイッチ スタックでは、Catalyst 3750 スイッチと Cisco EtherSwitch サービスモジュールのいずれもスタック マスターになれます。

Catalyst 2960-S コントロール プレーンの保護

Catalyst 2960-S スイッチは、内部的に最大 16 個の異なるコントロール プレーン キューをサポートします。各キューは、特定のプロトコル パケット処理専用であり、プライオリティ レベルが割り当てられます。たとえば、STP、ルーテッド パケット、ログに記録されたパケットが、3 種類のコントロール プレーン キューに送信されます。このキューでは、STP に最も高い優先度を持たせ、対応する順にプライオリティが与えられます。各キューは、そのプライオリティに基づいて、ある程度の処理時間割り当てられます。低レベル機能と高レベル機能間の処理時間の比率は 1 対 2 に割り当てられます。したがって、コントロール プレーンのロジックは CPU 使用率を動的に調整し、高度な管理機能を処理すると同時にバント トラフィック（最大 CPU 処理容量まで）を処理します。CLI のような基本コントロール プレーン機能は、パケットのロギングまたはフォワーディングなどの機能によって過負荷にはなりません。

Cisco IOS に関する注意事項

- サーバが応答しないため、Cisco Secure Access Control Server（ACS）およびメッセージ交換時からのスイッチ要求がタイムアウトになった場合、次のようなメッセージが表示されます。

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  このメッセージが表示された場合は、スイッチと ACS 間がネットワーク接続されていることを確認します。また、スイッチが ACS の AAA クライアントとして正しく設定されていることも確認します。

- スイッチに Voice over IP（VoIP）に対して Auto QoS が設定されたインターフェイスが実装されていて、スイッチ ソフトウェアを Cisco IOS Release 12.2(40)SE（以降）にアップグレードする場合に、別のインターフェイスで **auto qos voip cisco-phone** インターフェイス コンフィギュレーション コマンドを入力すると、次のメッセージが表示される場合があります。

  ```
  AutoQoS Error: ciscophone input service policy was not properly applied
  policy map AutoQoS-Police-CiscoPhone not configured
  ```

  この場合、削除するこの設定のすべてのインターフェイスで、**no auto qos voip cisco-phone** インターフェイス コマンドを入力します。次に、設定を再適用するこれらの各インターフェイスで、**auto qos voip cisco-phone** コマンドを入力します。

デバイス マネージャに関する注意事項

- デバイス マネージャからスイッチ クラスタを作成したり管理したりすることはできません。スイッチ クラスタの作成と管理には、CLI または Cisco Network Assistant を使用します。
- スイッチがデバイス マネージャのローカライズ バージョンを実行している場合、スイッチは英文字のみで設定およびステータスを表示します。スイッチの入力エントリは英文字のみできます。
- Internet Explorer のデバイス マネージャ セッションでは、日本語、簡体字中国語のポップアップ メッセージは、文字化けしたテキストとして表示されることがあります。これらのメッセージは、オペレーティング システムが日本語または中国語である場合、正しく表示されます。
- デバイス マネージャの凡例に 1000BASE-BX SFP モジュールが誤って組み込まれています。
- Microsoft Internet Explorer からデバイス マネージャを表示するために必要な時間を高速化するこのブラウザ設定を推奨します。

  Microsoft Internet Explorer から次の手順を実行します。

  1. [Tools] > [Internet Options] を選択します。
  2. [Temporary Internet files] エリアで [Settings] をクリックします。
  3. [Settings] ウィンドウで、[Automatically] を選択します。
  4. [OK] をクリックします。
  5. [OK] をクリックして [Internet Options] ウィンドウを終了します。
- HTTP サーバ インターフェイスは、デバイス マネージャを表示できるようにイネーブルにする必要があります。デフォルトでは、HTTP サーバがスイッチでイネーブルになっています。HTTP サーバがイネーブルか、またはディセーブルかを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

  認証（enable パスワード）のデフォルト方式を使用*しない*場合、スイッチで使用する認証方式の HTTP インターフェイスを設定する必要があります。

HTTP サーバ インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip http authentication** {**aaa** | **enable** | **local**}	ユーザが使用する認証のタイプに対して HTTP サーバ インターフェイスを設定します。 • **aaa**：認証、許可、アカウンティング機能をイネーブルにします。**aaa** キーワードを表示させるには、**aaa new-model** インターフェイス コンフィギュレーション コマンドを入力します。 • **enable**：HTTP サーバのユーザ認証のデフォルト方式である enable パスワードが使用されます。 • **local**：シスコ製ルータまたはアクセス サーバで定義されているとおりにローカル ユーザ データベースが使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。

デバイス マネージャでは、HTTP プロトコル（デフォルトはポート 80）および認証（enable パスワード）のデフォルト方式を使用して、スイッチとイーサネット ポートのいずれかを使用して通信し、標準 Web ブラウザからスイッチ管理を許可します。

HTTP ポートを変更すると、ブラウザの [Location] または [Address] フィールドに IP アドレスを入力するときに新しいポート番号を組み込む必要があります（http://10.1.126.45:184 など。ここで 184 は新しい HTTP のポート番号を意味します）。接続先ポート番号を記録しておく必要があります。スイッチの IP 情報を変更する場合は注意してください。

- Internet Explorer バージョン 5.5 を使用して、アドレスの最後に非標準ポートを付けた URL（*www.cisco.com:84* など）を選択した場合、URL プレフィックスとして *http://* を入力する必要があります。入力しないと、デバイス マネージャを起動できません。

未解決の不具合

特に記載のない限り、これらの警告は、Catalyst 3750、3560、2960-S および 2960 スイッチ、および Cisco EtherSwitch サービス モジュールに適用されます。

- CSCtg35226（Catalyst 3750 スイッチ）

  Cisco Network Assistant は、スタックの一部として Catalyst 3750G-48PS スイッチがあるスタック内のすべてのスイッチに対するライト ブルーのカラー LED ポートを表示します。

  回避策はありません。

- CSCtj97806（Catalyst 3750 スイッチおよび 3560 スイッチ）

  Mediatrace は次の状態では発信側の統計情報を報告しません。

  - 応答側がマスター スイッチとして Catalyst 3750 との混在スイッチ スタックである
  - 発信側からの応答側の入力インターフェイスがメンバー スイッチにある

  これは、Mediatrace の入出力の接続がスタック マスターにあることを確認するか、Catalyst 3750-E または 3750-X をスタック マスターとして設定してからスイッチ スタックをリロードすることで回避できます。

- CSCtl32991（Catalyst 3560、3560v2、3750、および 3750v2 スイッチ）

  スイッチを宛先とするユニキャスト EIGRP パケットが、最高のプライオリティのルーティング プロトコル キューへの代わりにホスト キューに送信されます。

（注） これは、パケットが別の宛先にスイッチ経由でルーティングされる場合は発生しません。

  回避策はありません。

- CSCto70539（Catalyst 2960-S）

  Catalyst 2960-S スイッチのイーサネット管理ポートは、ポートが 100 Mb/s および全二重に設定されていると正常に機能しない場合があります。

  これは、自動速度および自動二重に接続されたデバイスとイーサネット管理ポートを設定することで回避できます。

- CSCtq35006

  スイッチ スタックで、メンバー スイッチに接続された IP Phone にクリティカル音声 VLAN 機能を使用して許可された MAC アドレスがある場合、マスターの切り替えが発生すると、音声トラフィックがドロップされます。IP Phone のドロップ エントリが MAC アドレス テーブル管理

（MATM）テーブルに表示されます。これは、クリティカル音声 VLAN トラフィックを再認証する前に、スイッチが最初に音声トラフィックをドロップするために発生します。クリティカル音声 VLAN 認証が発生するときにドロップされたエントリが削除されます。

回避策はありません。ドロップされたエントリは、IP Phone が再認証されるときに削除されます。

- CSCtq39377

  Auto SmartPort がイネーブルで、SmartPort マクロでセキュア ポートに適用される場合はポート セキュリティ違反が無視されることがあります。この動作は、IOS センサー（Auto SmartPort の一部）がホスト モードを複数認証（マルチホスト モード）に設定し、ホスト アクセス テーブルで 802.1x をイネーブルにするために発生します。マルチホスト モードでは、別のポートで、同じ VLAN に同じ MAC アドレスがある場合は許可されません。そのため、パケットは違反を作成するポート セキュリティ モジュールに到達しません。

  これは、IOS センサー（Auto-SmartPort）機能を全体的にディセーブルにする **no macro auto monitor** グローバル コンフィギュレーション コマンドを入力することで回避できます。

- CSCtq81500

  IP Phone が音声 VLAN で Multidomain Authentication（MDA）を実行しているスイッチ ポートで認証されている場合、スイッチは、有効なパスワードが設定されていない電話機を再認証する継続的な試行の後で CPU 使用率が高くなる可能性があります。再認証は、次の条件で発生します。

  - 認証タイマーの期限切れ
  - **dot1x re-authenticate interface** *interface-id* 特権 EXEC コマンドの入力

  問題を解決するための回避策は以下のとおりです。

  - **shutdown** インターフェイス コマンドを入力し、続いて **no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。
  - **dot1x initialize interface** *interface-id* 特権 EXEC コマンドを入力してインターフェイスを初期化します。
  - 電話のパスワードを修正します。

  状況を回避するには次の操作を実行します。

  - 音声ドメインの定期再認証を使用しません。
  - 手動で認証をクリアした場合、**dot1x re-authenticate interface** コマンドの代わりに **clear authentication session** 特権 EXEC コマンドを使用します。

- CSCtr07908

  前のダウンロードが中断または失敗した場合に発生するフラッシュ メモリに *update* ディレクトリが存在する場合、画像アーカイブ ダウンロード プロセスが機能しません。

  これは、**archive download-sw** 特権 EXEC コマンドを実行する前に、フラッシュ メモリから update ディレクトリを削除することで回避できます。

- CSCud21309（Catalyst 2960-C、2960-S、および 3560-C スイッチ）

  Address Resolution Protocol（ARP）パケットは、dot1x がイネーブルの場合、プライベート VLAN の独立ポートでリークします。

  既知の回避策はありません。

- CSCtr16643（Catalyst 2960-S）

  同じ VLAN の TCP パケットが 1 つのスイッチから別のスイッチに送信される場合、ACL の拒否ログは ACL が Switch Virtual Interface（SVI）に適用されても表示されます。

  メッセージを停止するためには、SVI またはルーテッド ポートで **ip unreachables** インターフェイス コンフィギュレーション コマンドを入力して、IP 到達不能を設定することで回避できます。

- CSCtr82236（Catalyst 3750 スイッチおよび 3850v2 スイッチ）

  RMON 統計情報収集用に設定されたスイッチ スタックのメンバーがマスター スイッチで起動しない場合、RMON 収集設定がスタックの実行設定から欠落しています。この状況が発生しないようにするには、RMON 統計情報の収集用に設定されたすべてのスタック スイッチが、他のスタック メンバーとマスター スイッチを同時に起動する必要があります。

  回避策はありません。

- CSCtr83551

  マルチキャスト パケット損失は、受信者が IGMPv3 ブロッキング ソースに基づいてグループを残しておく場合に発生します。

  回避策はありません。

- CSCtr87645

  ASP は、スイッチに接続されたデバイスの種類を決定するデバイスの分類子を使用するようになりました。その結果、ASP がデバイスの検出に使用されるプロトコル タイプを制御できなくなりました。そのため、プロトコル検出制御は推奨されません。**macro auto global control detection** コマンドを入力すると、プロトコルは実行コンフィギュレーションに表示されません。ただし、**filter-spec** コマンドは出力に表示されます。

  回避策はありません。非推奨コマンドを表示するには、**show running config deprecated** グローバルおよびインターフェイス コンフィギュレーション コマンドを入力します。

- CSCtt11621

  dot1x default インターフェイス コンフィギュレーション コマンドが入力されると、ホストのアクセス コントロールがディセーブルになり、**authentication host-mode**、**authentication timer reauthenticate**、および **authentication port-control** コマンドの値はデフォルト値にリセットされます。

  これは、**dot1x default** コマンドを使用することは避け、802.1x ポート パラメータを個別にリセットすることで回避できます。または、**dot1x default** コマンドを入力して、誤って変更された値を再設定することでも回避できます。

- CSCtt31681（Cisco IOS LANLite イメージを実行している Catalyst 2960 イメージ）

  IPv6 アドレッシングがスイッチに設定されていても、スイッチは着信 IPv6 Telnet/SSH の接続を受け入れません。

- CSCtw42349

  この問題はサプリカント デバイスがメイン デバイス経由でスイッチに接続されている、認証、ポート セキュリティと IP ソース ガード（IPSG）でインターフェイスがイネーブルになった場合に発生します。メインおよびサプリカント デバイスはスティッキ MAC アドレスに設定されます。これにより、ポートがシャット ダウンすると、サプリカントから発信されたトラフィックはドロップされます。

  これはポート上のポート セキュリティはディセーブルにすることで回避できます。

- CSCtx69656

  スイッチのブート後に、接続されたデバイスはスイッチから Gratuitous ARP（GARP）パケットを受信しません。

これは、次のいずれかの操作を実行することで回避できます。

- 接続されたデバイスの ARP キャッシュを解消する
- デバイスが接続されているポート上で **switchport nonegotiate** コマンドを使用する
- スイッチから接続されているデバイスに ping を実行する

- CSCty74328（Catalyst 2960、2960-S、および 3750v2 スイッチ）

  スイッチ スタックで、スタック マスターがシステム メモリ低下が原因で突然停止します。この問題は、次の条件に適合する場合に発生します。

  - 複数の 802.1x クライアントが大規模（最大 500 ユーザ）な MDA ホスト モードで認証されている
  - 認証されたクライアントが AAA サーバからダイナミックな ACL をダウンロードする
  - AAA の定期アカウンティングがシステムでイネーブルになっている

  回避策はありません。

- CSCtz13824（Catalyst 2960-G スイッチおよび 3750-G スイッチ）

  QoS はスイッチ上の 4 つ以上のポートに適用できません。

  回避策はありません。

- CSCtz87828（Catalyst 2960-S、3750、および 3750v2 スイッチ）

  クロススタック EtherChannel を使用し、リンクの 1 つがダウンまたはアップすると、このポート チャネルから学習した MAC アドレスがテーブルから早く削除されるか期限切れになることがあります。

  これは、単一スイッチの Etherchannel を使用するか、リンクが追加されたか、チャネルから削除された後、動的に学習された MAC アドレスを消去することで回避できます。

- CSCtz96168（Catalyst 3560、3560v2、3750、および 3750v2 スイッチ）

  IPv6 パケットは、同じプライベート VLAN の 2 つの独立ポート間を通過します。

  回避策はありません。

- CSCtz98066（Catalyst 2960-S、3750、および 3750v2 スイッチ）

  スイッチ スタック内のマスター スイッチがリロードするか、電源を失い、メンバー スイッチ（スイッチ A）としてスタックに再加入すると、スイッチ A から宛先へのトラフィックが時折失われる可能性があります。

  これは、スタティック ARP エントリを追加したり、スイッチ A から宛先の接続を確認したりすることで回避できます。

- CSCtz99447

  システムの Web 認証リソースの制限により、スイッチのローカル Web 認証と HTTP サービスが応答しません。リソース制限は、通常、正しく終了しなかった HTTP セッションまたは TCP セッションによって起こります。

  つぎは考えられる回避策ですが、問題を解決することは保証されていません。

  - **ip admission max-login-attempts** 特権 EXEC コマンドを入力して、ユーザ 1 人あたりに許可されている最大ログイン試行回数を増やします。
  - Web 認証モジュールが Web クライアントからの HTTP セッションを認証しようとしてこのセッションを代行受信している場合、別のブラウザを使用してみてください。
  - HTTP トランスポートを使用するバックグラウンド プロセスを排除します。

- CSCua25981

  Auto Smartport 対応のインターフェイスは、スイッチが Auto SmartPort に接続され、2 番目のホップ スイッチが DHCP がイネーブルになっている IP Phone に接続されている場合、errdisable 状態になります。

  これは、**no macro auto processing** コマンドをインターフェイス コンフィギュレーション モードで使用し、スイッチ間リンクで処理するマクロをディセーブルにすることで回避できます。

- CSCua54137

  スイッチがフローティング スタティック ルートからスタティック ルートに戻ると、パケットは失われます。

  これはスタティック ARP を設定することで回避できます。

- CSCua54224

  過剰なトラフィック負荷の状態により、ループ ガードの保護機能が自動的にアクティブになり、ほぼ即時に非アクティブになる場合があります。これらの状態は、**shutdown** および **shutdown** インターフェイス コンフィギュレーション コマンドの入力または 40 個より多いポートでのインターフェイスのリンク フラップが原因の可能性があります。次のログ メッセージが表示されます。

  ```
  %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port GigabitEthernet1/0/1 on MST0.
  %SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port GigabitEthernet1/0/1 on
  MST0.
  ```

  回避策はありません。

- CSCua58659（Catalyst 2960-S スイッチ）

  power inline consumption default 15400 グローバル コマンドで、PoE+ ポート 15.4 W の電力消費の制限に失敗します。

  これは、インターフェイス コンフィギュレーション モードで **power inline consumption 15400** コマンドを使用することで回避できます。

- CSCua59800（Catalyst 2960-S スイッチ）

  Flex Link が Catalyst 2960-S スイッチ スタックに設定されて、スタック内のスイッチが（接続の問題が原因で）相互に接続解除された場合、バックアップ ポートのスイッチは、ダミーのマルチキャスト メッセージを（MAC アドレスが MAC アドレス テーブルになくても）ピア スイッチに送信します。

  これは、スイッチ スタックをリロードすることで回避できます。

- CSCua67288（Catalyst 3750-X スイッチ）

  QoS がポートでディセーブルになっている場合、IP フラグメントの発生により、キュー 1 でパケットがドロップされることがあります。

  これは、QoS をイネーブルにし、バッファしきい値を調整することで回避できます。

- CSCua74302（LAN ベース イメージを実行しているスイッチ）

  Switch Virtual Interface（SVI）の発信トラフィックに適用される ACL が機能しません。

  回避策はありません。

- CSCua87594（Catalyst 3560-G、3560v2、3750-G、3750、および 3750v2 スイッチ）

  ピア スイッチがシスコ製スイッチのブロッキング ポートで（プロポーザル ビットをオンに設定して）下位のブリッジ プロトコル データ ユニット（BPDU）を送信すると、シスコ製スイッチは、より上位の BPDU で応答する前に、このような 3 個の BPDU を待機します。つまり、5 秒よりも長いコンバージェンス時間が発生します。問題は、次の条件で発生します。

  - シスコ製スイッチがルート スイッチとして設定されていません。

  - シスコ製スイッチは Multiple Spanning-Tree Protocol（MSTP）を使用し、ピア スイッチは Rapid Spanning Tree Protocol（RSTP）または Rapid Per-VLAN Spanning-Tree plus（Rapid PVST+）を使用します。

  回避策はありません。

- CSCub14238

  Cisco IOS Release 15.0(2)SE を実行しているスイッチで、ポート ベースのアドレス割り当てが設定されたときに問題が発生しました。クライアント ID が ASCII ストリングとして設定された場合、または加入者 ID がクライアント ID として使用された場合、DHCP クライアントはサーバから IP アドレスを受信しませんでした。

  この問題は修正されました。特に対処の必要はありません。

- CSCub14641

  モニタ セッションのソース インターフェイスを設定し、保存した場合、設定はリブート後には保存されません。

  回避策はありません。

- CSCub24886（Catalyst 2960-S スイッチ）

  スタック メンバーの双方向ポートが不正な状態を返します。

  回避策はありません。

- CSCub26534（Catalyst 2960-S スイッチ）

  ソフトウェア アップグレード中にステータス メッセージが表示されないことがあります。ただし、アップグレードはバックグラウンドで実行され、新しいソフトウェアが正常にインストールされます。

  回避策はありません。

- CSCub20474（Catalyst 3560、C3560v2、C3750、および C3750v2 スイッチ）

  スイッチ スタックでは、マルチキャスト トラフィックはマスター スイッチがリロードされるとき最大 60 秒間失われる可能性があります。プラットフォームはマルチキャスト無停止フォワーディング（NSF）をサポートしないためスイッチオーバー後のトラフィックの再コンバージェンスまでの時間は変わることがあります。

  回避策はありません。

- CSCub63066（Catalyst 3560-C、3560-G、3560v2、3750-G、および 3750v2 スイッチ）

  システム リソース割り当てに失敗した時にスイッチが以前割り当てられたメモリを解放しないため、ルーティング エントリがテーブルで更新されるとメモリが失われます。

  回避策はありません。

- CSCub86631（Catalyst 3750v2 スイッチのみ）

  no logging event link-status interface range コマンドをメンバー スイッチで設定して保存し、そのスタック メンバーまたはスタック全体をリブートすると、設定はリブート後に利用できなくなります。

  これは、コマンドを再設定することで回避できます。

解決済みの警告

- 「Cisco IOS Release 15.0(2)SE1 で解決済みの警告」（P.49）
- 「Cisco IOS Release 15.0(2)SE で解決済みの警告」（P.52）

Cisco IOS Release 15.0(2)SE1 で解決済みの警告

- CSCee32792

  SNMP v3 を使用している場合、スイッチで snmp_free_variable_element が発生すると、スイッチが突然リロードされます。

  回避策はありません。

- CSCth03648

  2 個のトラップが 2 つの独立したプロセスによって生成されるとき、他のプロセスが最初のプロセスで使用される変数を更新する間に 1 つのプロセスが停止された場合、スイッチで障害が発生します。

  これは、すべての SNMP トラップをディセーブルにすることで回避できます。

- CSCth59458

  冗長電源装置（RSP）のスイッチオーバーが一括設定の同期中に発生した場合、回線設定の一部が失われることがあります。

  これは、回線設定を再適用することで回避できます。

- CSCti95154（Catalyst 2960、2960-S、3560、および 3750 スイッチ）

  Cisco IOS Release 12.2(52)SE 以降では、デバイス トラッキング テーブルが 1 つの IP アドレスのみを 1 つの MAC アドレスにマッピングできます。この制限は削除され、複数の IP アドレスが 1 つの MAC アドレスにマッピングできるようになりました。

- CSCtl12389

  show ip dhcp pool コマンドは、多数のリースされたアドレスを表示します。

  これは、**ip dhcp remember** オフにしてスイッチをリロードすることで回避できます。

- CSCtq64716

  RADIUS または TACACS サーバを定義した場合でも、ブート プロセス中に次の警告メッセージが表示される場合があります。

  ```
  %RADIUS-4-NOSERVNAME:
  ```

  または

  ```
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```

  回避策はありません。

- CSCtq75383（Cisco IOS LANLite イメージを実行している Catalyst 2960 スイッチ）

  traceroute コマンドは次のエラー メッセージを返します。

  ```
  % VRF  is not accessible.
  ```

  回避策はありません。

- CSCtr37757

  Secure Copy 機能（**copy:** *source-filename* **scp**: *destination-filename* コマンド）が機能しません。

  回避策はありません。

- CSCtw33903

  この問題は、インターフェイスに接続されたデバイスについて、Enterprise Policy Manager（EPM）がクローズ モードで承認され、ポリシーが設定されていないかダウンロードされていない場合に発生します。ポート ACL が設定されていない場合、認証デフォルトのアクセス コントロール リスト（ACL）がスイッチに適用されます。別のデバイスがこのデバイスに接続されている場合、制限付き VLAN（**authentication event** インターフェイス コンフィギュレーション コマンド）がポートでイネーブルになっています。Application Control Engine（ACE）は、接続デバイスから発信されるトラフィックを許可するように設定されておらず、IP パケットはドロップされます。

  これは、インターフェイスに接続されたデバイスに対して特定の IP 範囲の IP トラフィックを許可するようにポート ACL を設定することで回避できます。

- CSCtw89960（Catalyst 3560-C スイッチ）

  Catalyst 3750 スイッチまたは Catalyst 3560 がローカル接続ホストを備えたレイヤ 3 スイッチとして設定されている場合、スイッチはローカル接続されたホスト向けの大きな IPv6 トラフィック負荷をドロップします。

  これは、IPv4 VRF を全体的に設定しないことで回避できます。

- CSCtx69656（Catalyst 3560-C、2960-C、および 2960-S スイッチ）

  Catalyst 2960 スイッチが Cisco IOS Release 12.2(50)SE5 以降で起動すると、トランク ポートによって Catalyst 2960 スイッチに接続された Catalyst 3750 スイッチは、Catalyst 2960 スイッチから Generic Attribute Registration Protocol（GARP）データ パケットを受信できません。

  これは、次の操作を実行することで回避できます。

  - Cisco IOS Release 12.2(25)SEE または 12.2(53)SE2 で Catalyst 2960 スイッチを実行します。

  - 接続先デバイスの Address Resolution Protocol（ARP）を解消します。

  - Dynamic Trunking Protocol（DTP）ネゴシエーション パケットがレイヤ 2 インターフェイスに送信されないことを指定するように **switchport noneg** コマンドを入力します。

  - Catalyst 2960 スイッチから接続先デバイスに対して ping を実行します。

  - Switch Virtual Interface（SVI）のタイミングを制御するために **line-proto-delay** コマンドを使用します。

- CSCtz13824（Catalyst 3750-G、3560-G、および 2960-G スイッチ）

  ユーザは、スイッチの別の ASIC で、4 つ以上のポート インターフェイスに Quality of Service（QoS）ポリシー マップを適用できません。これは、複数の ASIC を持つ Catalyst 2960G、3560G、および 3750G スイッチに共通の問題です。

  既知の回避策はありません。

- CSCtz91389（Catalyst 3750-G、3560-G、および 3750-V2、3560-V2 スイッチ）

  ip rsvp snoopingp コマンドがレイヤ 2 環境でイネーブルの場合、スイッチはメタデータ パケット転送を停止します。

  既知の回避策はありません。

- CSCtz96168（Catalyst 3750-G、3560-G、および 3750-V2、3560-V2 スイッチ）

  IPv6 パケットは、同じプライベート VLAN の 2 つの独立ポート間で転送されます。

  既知の回避策はありません。

- CSCty10239

  ipl=5 の場合、Catalyst 2960 スイッチが 20 バイトの malloc 失敗メッセージを受信すると、トレースバックが割り込みレベルが原因で発生します。

  既知の回避策はありません。

- CSCty81591（Catalyst 2960-S スイッチ）

  プラットフォーム アサート失敗メッセージがスイッチに表示されます。スタティック MAC アドレス テーブルの削除後にトレースバックが発生します。

  これは、ダイナミック MAC アドレス テーブルを設定し、SD を割り当てる API の戻り値が正しく検査されていることを確認することで回避できます。

- CSCtz98066（Catalyst 2960-S スイッチ）

  マスター スイッチ（スイッチ A）がリロードされるか、電源を失い、メンバー スイッチとしてスタックに再加入すると、新しく加入したメンバーがネクスト ホップ ルータまたはスイッチに対する Address Resolution Protocol（ARP）エントリを確立できないため、スイッチ A を終了するすべてのトラフィック ストリームがドロップされます。トラフィックは引き続きスイッチに送信されますが、デバッグにより、スイッチ A がネクスト ホップについて GARP または ARP を送信しないことが確認されます。

  これはスタティック ARP を追加することで回避できます。ARP を応答するよう強制するようにスイッチ A から宛先を ping します。

- CSCua64859

  組み込みマクロまたはユーザ定義マクロを持たないデバイスが CDP、Link Layer Discovery Protocol（LLDP）、または DHCP をサポートしているかどうかに関係なく、CISCO_LAST_RESORT_AUTO_SMARTPORT マクロがこのデバイスに適用されます。デバイスが、組み込みマクロまたはユーザ定義マクロにデバイスを一致させるディスカバリ プロトコルを実行していないことを確認するために、スイッチは CISCO_LAST_RESORT_AUTO_SMARTPORT マクロを適用する前に約 120 秒間待機します。このマクロは、PC、ラップトップ、プリンタなどのデバイスに適用されます。MAC Operationally Unique Identifier（OUI）ベースのトリガーを設定したり、このデバイスのマクロにこれらのトリガーをマップしたりする必要はありません。

- CSCub93357

  インターフェイスが **switchport port-security maximum 1 vlan** コマンドで設定されると、次のエラー メッセージが表示されます。

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
  address XXXX.XXXX.XXXX on port <interface>
  ```

  回避策はありません。

- CSCuc03555

  フラッシュの手動によるフォーマット時にフラッシュ メモリが破損します。

  これは、スイッチをリロードすることで回避できます。（これでフラッシュ メモリが消去されるため、TFTP、USB ドライブ、またはシリアル ケーブルを使用してソフトウェア イメージをリロードする必要があることに注意してください）。

- CSCuc04407（Catalyst 3560 スイッチ）

  VLAN ベースの QoS は WS-C3560CG スイッチ上のインターフェイスでは使用できません。

  回避策はありません。

- CSCuc17720

  Performance Monitor のキャッシュが（**show performance monitor cache** コマンドを使用して）表示され、**q** キーワードを入力してコマンド出力表示を停止しようとすると、出力が停止する前に著しく長い遅延があります。

  これは、すべてのコマンド出力が中断なしで表示されるように、**term len 0** 特権 EXEC コマンドを入力することで回避できます。

- CSCuc36990（Catalyst 3560 スイッチ）

  Cisco TrustSec Media Access Control Security（MACsec）は、アップリンク ポートに設定できません。MACsec インターフェイス コマンドは、**sap pmk** *key* **modelist no-encap** コマンドを入力する場合を除き、スイッチで受け入れられません。この問題は、インターフェイス範囲 GigabitEthernet0/9 から GigabitEthernet0/10 のスイッチ モデル WS-C3560CG に出現します。

  Cisco TrustSec MACsec をインターフェイス範囲 GigabitEthernet0/1 から GigabitEthernet0/8 の RJ-45 ギガビット イーサネット ポートに設定することで回避できます。ギガビット イーサネット光リンクでの Cisco TrustSec MACsec の設定に対する回避策はありません。

- CSCuc53848（Catalyst 3560 スイッチ）

  device-sensor accounting グローバル コンフィギュレーション コマンドが使用できなくなります。

  回避策はありません。

Cisco IOS Release 15.0(2)SE で解決済みの警告

- CSCtk12589（Catalyst 2960-S スイッチ）

  Catalyst 2960S シリーズ スイッチを起動すると、書き込みメッセージについて多数の Yeti2S88gMdioWr: Unknown ステータスがコンソールに表示される場合があります。エラー メッセージによって起動時間が大幅に増えることがありますが、スイッチは Cisco IOS ブート後に完全に機能します。

  これは、リカバリを迅速に行うため、スイッチの電源を再投入することで回避できます。これはソフトウェアの問題であり、スイッチの交換は不要です。

- CSCtl41917（Catalyst 2960-S スイッチ）

  スイッチオーバーがスイッチ スタックで発生した場合、ホスト セッション情報は失われます。

  これは、すべてのクライアントを再認証することで回避できます。

- CSCtl48226

  show epm session summary コマンドまたは **show epm** コマンドが SSH または Telnet セッションから入力され、別のコマンドがコンソールから入力されると、スイッチが突然リセットされ、クラッシュ情報を生成する場合があります。

  これは、両方のコマンドを同じセッション、つまり SSH/telnet またはコンソールから入力することで回避できます。

- CSCtl60151

  スイッチは、CPU 過負荷が発生した後に、どのプロセスが CPU を過負荷にしているかに関係なくリロードされることがあります。

  回避策はありません。

- CSCto09117

  スイッチは、同じイメージが現在ロードされ、実行されている場合でも、TFTP サーバから実行中の IOS イメージをダウンロードし、再起動します。

  回避策はありません。

- CSCto57723

  Cisco IOS ソフトウェアおよび Cisco XE ソフトウェアには、認証されていないリモートの攻撃者がサービス拒否（DoS）状態を引き起こす可能性のある脆弱性が存在します。攻撃者は、DHCP バージョン 6（DHCPv6）サーバ機能が有効な該当デバイスに対して巧妙に細工されたリクエストを送信することで、この脆弱性を不正利用できる可能性があります。その結果、再起動が発生します。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-dhcpv6

- CSCtq38500（Catalyst 2960-S スイッチ）

  インターフェイスが **mls qos** コマンドによって設定されている場合、トラフィックは範囲オプションを使用するポート ベースの QoS ACL と一致しません。

  これは、単一ポート eq キーワードを使用してスイッチを設定することで回避できます。あるいは、acl-range オプションを使用する同じポリシー マップのクラス デフォルト設定で信頼状態を設定することもできます。

- CSCtq51049（Catalyst 2960-S、2960SM、3750、および 3750v2 スイッチ）

  スイッチ スタックで、ACL が VTY 回線に適用されるとメンバー スイッチとのコンソール セッションを確立できません。

  これは、ACL を line vty 0 4 と line vty 5 15 に適用する際に次の手順を使用することで回避できます。

  1. **vty** ACL を作成し、127 ネットワークを許可します。
  2. **vrf-also** キーワードを設定された access-class inbound に付加します。

  次の例を参照してください。

```
ip access-list standard vty-acl
   permit 127.0.0.0 0.0.0.255

line vty 0 4
   access-class vty-acl in vrf-also
   privilege level 15
   length 0
   transport input ssh
line vty 5 15
   access-class vty-acl in vrf-also
   privilege level 15
   transport input ssh
```

- CSCtq86186（Catalyst 2960-S）

  スイッチ スタックでは、**show interface** コマンドによって出力ドロップに不正な値が示されます。

  これは、**show platform port-asic stats drops** コマンドを使用して、正しい値が表示されるようにすることで回避できます。

- CSCtr07908

  アーカイブのダウンロード機能は、フラッシュに「update」ディレクトリが含まれると機能しません。この状況は、前述のダウンロードが失敗したか中断され、「update」ディレクトリがフラッシュにまだ残っている場合に発生する可能性があります。

  これは、アーカイブのダウンロードを開始する前に、フラッシュの「update」ディレクトリを削除することで回避できます。

- CSCtr19734（Catalyst 2960-S、3750、および 3759v2 スイッチ）

  null0 にセットされるネクスト ホップを持つスタティック ルートは、マスター スイッチがスイッチ スタックの設定内で変更されたときに削除されます。この状況は、スイッチがスタックされ、スタティック ルートが **network 0.0.0.0** コマンドによってアドバタイズされるときに発生します。

  これは、**ip summary-address eigrp** *as-number ip-address mask* コマンドを使用して、ネクスト ホップがあるインターフェイスの IP サマリー集約アドレスを設定することで回避できます。

- CSCty88456

  Supervisor Engine 7L-E を搭載する Catalyst 4500E シリーズ スイッチには、デバイスのリロードの原因となる特別に作成されたパケットを処理する際に DoS の脆弱性が含まれます。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  これらの脆弱性に対しては回避策がありません。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-ecc

- CSCtr32202（Catalyst 2960-S スイッチ）

  スイッチ スタックの各スイッチのポートがアップリンク ポート チャネルを形成するために同時にバンドルされると、Multicast VLAN Registration（MVR）ストリームはポート チャネルにアクティブ メンバーを持つスイッチにのみ送信されます。

  これは、Internet Group Management Protocol（IGMP）スヌーピングを使用することで回避できます。

- CSCtr44361（Catalyst 2960-S、3750、および 3750v2 スイッチ）

  デバイスがスイッチのスタックで 1 つのポートから別のポートに移動された場合、移動イベントに対して生成された SNMP データが正しくありません。

  これは、コア ネットワークへのアップリンクがマスター スイッチに設定されている（1/0/x ポートなど）ことを確認することで回避できます。

- CSCtr55645

  OSPFv3 ネイバーは、スイッチ ハンドルが既知の IPv6 マルチキャスト アドレスを宛先とする IPv6 トラフィックを処理する方法のためフラップする場合があります。

  回避策はありません。

- CSCts36715

  Web プロキシ認証用に設定されたデバイス経由でネットワークに接続しているユーザで、Web 認証障害が発生する可能性があります。

  回避策はありません。**clear tcp tcb** コマンドを使用して HTTP Proxy Server プロセスを解放します。

- CSCtt11621

  ポートで **dot1x default** コマンドを使用して、ポート アクセス コントロールをディセーブルにし、**authentication host-mode** コマンドおよび **authentication timer reauthenticate** コマンドの値をデフォルト値にリセットします。

  これは、**dot1x default** コマンドを使用せずにさまざまな dot1x パラメータを個別に設定することで回避できます。または **dot1x default** コマンドを入力した後に変更されたパラメータを再設定することもできます。

- CSCtt19547（Catalyst 3560、3560v2、3750、および C3750v2）

  スイッチは、VPN ルーティング/転送（VRF）インスタンスに関連付けられた Switch Virtual Interface（SVI）のレイヤ 2 ポート チャネルから受信したレイヤ 3 マルチキャスト トラフィックをドロップします。

  これは、入力物理インターフェイス、SVI、またはポート チャネルをフラップすることで回避できます。

- CSCtt98094（Catalyst 2960-S スイッチ）

  スイッチ スタックの設定では、メンバー スイッチのリロード後、スレーブ スイッチで **mls qos cos 7** などの値が指定された、マルチレイヤ スイッチング（MLS）サービス クラス（CoS）コンフィギュレーション コマンドは機能しなくなりました。この状況は、タグなし IP パケットおよびレイヤ 2 パケットに影響します。

  これは、インターフェイスにサービス ポリシーを設定したときに、インターフェイスのデフォルト CoS レベルも設定することで回避できます。インターフェイス コンフィギュレーション モードで **mls qos trust cos** コマンドを使用できます。

- CSCtw98934（Catalyst 2960-C スイッチおよび 2960-S スイッチ）

  スイッチがダウンリンク ポートでジャンボ フレーム（9000 バイトより大きい）を受信するとフレーム チェック シーケンス（FCS）のエラーが発生します。

  回避策はありません。

- CSCtx33436

  switchport port-security maximum 1 **vlan access** コマンドを使用して、パーソナル コンピュータと接続している IP Phone がポート セキュリティを備えたアクセス ポートに接続されるとセキュリティ違反がインターフェイスで発生します。このタイプのメッセージは、コンソールに表示されます。

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  XXXX.XXXX.XXXX on port FastEthernet0/1.
  ```

  次に設定例を示します。

  ```
  interface gigabitethernet 3/0/47
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 3
  switchport port-security maximum 2
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  ```

  これは、**switchport port-security maximum** 1 **vlan access** の行を削除することで回避されます。

- CSCtx96491

  bpduguard がインターフェイスで設定されている場合でも、認証された IP Phone のスイッチ ポートが、dot1x のセキュリティで設定され、認証されたポートにループするとき、スイッチがループバックを正しく検出しません。この状況により、CPU 使用率が 100 % となり、スイッチのパフォーマンスが低下する可能性があります。

  これは、**authentication open** コマンドを使用してインターフェイスを設定するか、スイッチに **authentication mac-move permit** を設定することで回避できます。

Cisco IOS Release 15.0(1)SE1 で解決済みの警告

- CSCth62705

  EtherChannel を設定し、既存のドメインに別の EnergyWise ドメインを使用した新しいドメイン メンバーまたは EnergyWise 対応エンドポイントを追加すると、スイッチの CPU 使用率が高くなります。

  これは、CPU 使用率が高くなるポート チャネルをディセーブルにすることで回避できます。

- CSCtq75612

  FlexStack 設定で 2 つのスイッチを結合し、マスター スイッチのパスワードを設定した場合、スイッチからログアウトし、再びログインすると、**show run** コマンドに変更が反映されていません。

  回避策はありません。

- CSCtr28857

  Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr31957

  ipc_check_qtime_process() がプロセッサ間通信（IPC）メッセージ テーブルからのメッセージを処理すると、メッセージの受信が中断することがあります。この場合、割り込みハンドラがそのメッセージをメッセージ キャッシュに戻すため、メッセージは無効となり、スイッチは、メッセージへのアクセスを引き続き試行するためクラッシュします。

  回避策はありません。

- CSCtr49064

  Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアにおけるセキュア シェル（SSH）サーバの実装には、SSH バージョン 2（SSHv2）機能にサービス拒否（DoS）の脆弱性が存在します。非認証のリモート攻撃者は、細工されたユーザ名を使用したリバース SSH ログインの試行によってこの脆弱性を悪用する可能性があります。この脆弱性の不正利用に成功した場合、攻撃者はデバイスの再起動を引き起こすことによって DoS 状態を発生させる可能性があります。繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

  Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの SSH サーバは任意に選択するサービスですが、Cisco IOS デバイスを管理するためのセキュリティのベスト プラクティスとして使用することを推奨します。SSHv2 接続の受け入れが設定されていないデバイスは、この脆弱性の影響を受けません。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ssh

- CSCtr75161

  Access Control List（ACL）ポリシーを使用してスイッチ上に Web 認証を設定し、ポート ACL も設定すると、ポート ACL は Web ACL にフォールバックする際にホストに適用されます。

  回避策はありません。Cisco IOS Release 12.2(55)SE にダウングレードすると機能を維持できます。

- CSCtr79386 - （Catalyst スイッチ 3750）

  Dynamic Host Configuration Protocol（DHCP）スヌーピングをイネーブルにすると、着信トラフィックは I/O を使い果たし、スイッチがクラッシュします。

  これは DHCP スヌーピングをディセーブルにすることで回避できます。

- CSCtr91106

  Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、アカウンティング（AAA）許可を使用した場合に、許可レベルを超えることのできる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts36715

  Web サーバへのクライアント接続に失敗した場合は、その後の試行で HTTP プロキシ サーバのプロセスが停止して、新しい HTTP プロキシ サーバが作成されます。これらのプロセスを表示するには、**show processes** コマンドを入力します。プロセス数が **ip admission http proxy** インターフェイス コンフィギュレーション コマンドで指定された制限に達すると、後続のすべての Web 認証が失敗します。

  これは、スイッチをリロードすることで回避できます。

- CSCts52797（Catalyst スイッチ 2960）

  64 MB の DRAM を搭載した Catalyst 2960 は、スイッチを 12.2(58)SE 以降にアップグレードした後、コンソールにメモリ不足を示す可能性があります。

  これは、このリリースが必要な場合はスイッチの異なる機能で使用されるメモリを制限することで回避できます。1 つのスイッチで使用中のトランク ポートと VLAN の数を最小限に抑えることで、メモリの使用量を減らすことができます。

- CSCts88664

  Web 認証中に、ユーザが自分の資格情報を入力してすぐにログインした場合、スイッチがクラッシュしてリブートします。

  これは、ユーザ クレデンシャルを入力してから 4 ～ 5 秒の一時停止後にログインすることで回避できます。

- CSCtt16051

  Smart Install 機能がイネーブルの場合、Cisco IOS ソフトウェアには、非認証のリモート攻撃者に対して影響を受けるデバイスのリロードを認める可能性のある Smart Install 機能の脆弱性が含まれます。この脆弱性は、影響を受けるデバイスが TCP ポート 4786 で Smart Install の不正な形式のメッセージを処理するときに起こります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性を軽減する回避策はありません。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-smartinstall

- CSCtt18020

  ルータが突然リロードされます。この問題は、SSH を使用してルータにログインする場合に発生します。

  Telnet を使用してルータにログインすることで回避できます。

- CSCtu09846

  ユーザが中央 Web 認証を使用してリダイレクトするとスイッチがクラッシュします。

  これは、中央 Web 認証をディセーブルにすることで回避できます。

Cisco IOS Release 15.0(1)SE で解決済みの警告

- CSCti30313（Catalyst 2960 スイッチおよび 2960-S スイッチ）

  show sd からの出力

  m prefer lanbase-routing 特権 EXEC コマンドで一部不正な値が表示されます。正しい値は次のとおりです。

```
number of IPv4 unicast routes:                    4.25K should be: 0.75K
    number of directly-connected IPv4 hosts:        4K  should be: 0.75K
    number of indirect IPv4 routes:                 0.256    should be 16
```

  回避策はありません。

- CSCtj83964（Catalyst 3750 スイッチおよび 3560 スイッチ）

  プロトコル独立マルチキャスト（PIM）と Source Specific Multicast（SSM）を実行しているスイッチで、スイッチのリロード後にマルチキャスト トラフィックが正しいポートに送信されない場合があります。

  これは、**clear ip route** 特権 EXEC コマンドを入力するか、リロード後に PIM および SSM を再設定することで回避できます。

- CSCtl51859

  IPv6 MLD スヌーピング機能がスイッチで全体的にイネーブルになっていると、ネイバー探索は、スイッチに接続された IPv6 ホストで失敗します。

  これは、スイッチで IPv6 MLD スヌーピングをディセーブルにすることで回避できます。

- CSCtl81217（Catalyst 3750 および 3560）

  IP アドレスを割り当てるために、スイッチが DHCP サーバを使用していて、スイッチのインターフェイスで RIP をイネーブルにしている場合にスイッチがリロードされると、インターフェイスで一部の RIP 設定（特に RIP 認証モードおよび RIP 認証キー チェーン）が失われます。IP アドレスがインターフェイスに静的に設定されている場合は発生しません。問題が発生するのは、IP アドレスが DHCP サーバによって割り当てられる前に RIP を設定している場合のみです。

  回避策はありませんが、組み込みイベント マネージャ（EEM）スクリプトを使用して、インターフェイスに次のインターフェイス コンフィギュレーション コマンドを追加することができます。

  ip rip authentication mode

  ip rip key-chain

- CSCto10165

  Cisco IOS ソフトウェアを実行している Cisco Catalyst スイッチの Smart Install 機能には、認証されていない攻撃者が該当デバイスに対してリモートからコードを実行できる可能性のある脆弱性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

Smart Install 機能を無効にする以外に、この脆弱性を軽減する回避策はありません。

このアドバイザリは、
http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml で公開されています。

- CSCtq01926

  ポートに **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力して、そのポートがダイナミック VLAN となるように設定した場合、スイッチはポートでの ARP 要求を処理するときにリロードすることがあります。

  これは、これらのポートにスタティック VLAN を設定することで回避できます。

- CSCtq86035（Catalyst 2960-S）

  USB タイプ A ポートのスイッチに USB フラッシュ デバイス（サム ドライブや USB キー）を挿入するとスイッチがリロードされる場合があります。

  これは、USB フラッシュ デバイスを USB タイプ A ポートに挿入しないことで回避できます。

マニュアルの更新

Catalyst 3560 および 2960 ソフトウェア コンフィギュレーション ガイドの更新内容

「Configuring Interface Characteristics」の章に追加された情報

「Configuring Interface Characteristics」の章に次の新しい項が追加されました。

Universal Power over Ethernet Support

Cisco Universal Power over Ethernet（UPoE）は、標準のイーサネット ケーブル配線インフラストラクチャ（クラス E またはそれ以上）により最大 60 W の電力を供給するように、IEEE 802.3 PoE 標準を拡張するシスコ独自のテクノロジーです。UPOE 電力ネゴシエーションは Cisco Discovery Protocol（CDP）および Link Layer Discovery Protocol（LLDP）を独自の Type-Length-Value（TLV）要素の導入先に使用します。UPoE は受電デバイス（PD）と給電装置（PSE）の両方がこれらの追加 TLV をサポートしている場合にだけ使用できます。

Catalyst 2960-C スイッチおよび 3560-C スイッチには PD と PSE の両方の機能があります。これらのスイッチは一度に 1 つのアップリンク インターフェイスでの UPoE をサポートし、親 PSE から最大 60 W の電力をネゴシエートします。ダウンリンク インターフェイスでは、スイッチは IEEE 802.3af PoE の給電のみが可能です。

注意事項と制約事項

- CDP は、スイッチでデフォルトでイネーブルであるため、UPoE のネゴシエーションをイネーブルにするには、特別な設定は必要ではありません。CDP の代わりに LLDP を使用する場合は、CDP をディセーブルにし、LLDP をグローバル コンフィギュレーション モードでイネーブルにして、次に親スイッチのインターフェイスに **shutdown/no shutdown** コマンド シーケンスを入力します。
- 一般的に、両方のアップリンクが PoE 対応 PSE に接続されている場合、スイッチは UPOE 電力をネゴシエートできません。例外は、アップリンクの 1 つが PSE データ専用インターフェイスに接続されている場合、または最初のアップリンクが UPOE 電力をネゴシエートした場合です。最初のアップリンクが UPOE 電力をネゴシエートすると、2 番目のアップリンクはデータ専用インターフェイスのように動作します。
- 表 8 に、スイッチが UPoE 対応の PSE に接続された場合に有効な設定を示します。

表 8　UPoE 対応 PSE に接続している Catalyst 2960-C スイッチおよび 3560-C スイッチ

受電デバイスのアップリンク 1	受電デバイスのアップリンク 2
UPOE	データ専用
データ専用	UPOE

- 表 9 に、スイッチが UPoE をネゴシエートした場合にパススルー PoE で使用可能な電力量を示します。

表 9　パススルー PoE で使用可能な電力

スイッチ	パススルー電力
Catalyst 2960-C	30.8 W
Catalyst 3560-C	22.4 W

関連資料

HTML 形式のユーザ マニュアルには最新のマニュアル更新が含まれており、Cisco.com で入手可能な完全版 PDF よりも最新である可能性があります。

次のマニュアルには、Catalyst 3750、3560、2975、2960-S および 2960 スイッチ、および Cisco EtherSwitch サービス モジュールに関する詳細情報が記載されており、Cisco.com から入手できます。

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/hw/switches/ps5528/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps10081/tsd_products_support_series_home.html

http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

次のマニュアルには、Catalyst 3750 スイッチおよび Cisco EtherSwitch サービス モジュールに関する詳細情報が記載されています。

- *『Catalyst 3750 Switch Software Configuration Guide』*

- 『*Catalyst 3750 Switch Command Reference*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*』
- 『*Catalyst 3750 Switch Hardware Installation Guide*』
- 『*Catalyst 3750 Getting Started Guide*』
- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Catalyst 3750 Switch*』

次のマニュアルには、Catalyst 3750G Integrated Wireless LAN Controller Switch および Integrated Wireless LAN Controller に関する詳細情報が記載されています。Cisco.com から入手できます。

- 『*Catalyst 3750 Integrated Wireless LAN Controller Switch Getting Started Guide*』
- 『*Release Notes for Cisco Wireless LAN Controller and Lightweight Access Point, Release 4.0.x.0*』
- 『*Cisco Wireless LAN Controller Configuration Guide, Release 4.0*』
- 『*Cisco W*ireless *LAN Controller Command Reference, Release 4.0*』

次のマニュアルには、Catalyst 3560 スイッチに関する詳細情報が記載されています。

- 『*Catalyst 3560 Switch Software Configuration Guide*』
- 『*Catalyst 3560 Switch Command Reference*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*』
- 『*Catalyst 3560 Switch Hardware Installation Guide*』
- 『*Catalyst 3560 Switch Getting Started Guide*』
- 『*Regulatory Compliance and Safety Information for the Catalyst 3560 Switch*』

次のマニュアルには、Catalyst 2960 および 2960-S スイッチに関する詳細情報が記載されており、Cisco.com から入手できます。

- 『*Catalyst 2960 and 2960-S Switch Software Configuration Guide*』
- 『*Catalyst 2960 and 2960-S Switch Command Reference*』
- 『*Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*』
- 『*Catalyst 2960-S Switch Hardware Installation Guide*』
- 『*Catalyst 2960-S Switch Getting Started Guide*』
- 『*Catalyst 2960 Switch Hardware Installation Guide*』
- 『*Catalyst 2960 Switch Getting Started Guide*』
- 『*Catalyst 2960 Switch Getting Started Guide*』（英国、簡体字中国語、フランス語、ドイツ語、イタリア語、日本語、およびスペイン語で入手可能）
- 『*Regulatory Compliance and Safety Information for the Catalyst 2960 and 2960-S Switch*』

関連製品のその他の情報については、次の資料を参照してください。

- 『*Smart Install Configuration Guide*』
- 『*Auto Smartports Configuration Guide*』
- 『*Cisco EnergyWise Configuration Guide*』
- 『*Getting Started with Cisco Network Assistant*』
- 『*Release Notes for Cisco Network Assistant*』
- 『*Cisco RPS 300 Redundant Power System Hardware Installation Guide*』
- 『*Cisco RPS 675 Redundant Power System Hardware Installation Guide*』

- Network Admission Control（NAC）の詳細については、『*Network Admission Control Software Configuration Guide*』を参照してください。
- Cisco SFP、SFP+、および GBIC モジュールに関する情報は、Cisco.com の次のページで入手可能です。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP の互換性マトリクスに関するマニュアルは、次の Cisco.com サイトにあります。
  http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルも一覧表示されています。
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/