Catalyst 2960-S、2960-SF、2960-C、2960-Plus、および 3560-C スイッチ、Cisco IOS Release 15.2(1)E に関するリリース ノート

2013 年 8 年 28 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 15.2(1)E 以降は、Catalyst 2960-S、2960-SF、2960-C、2960-Plus、および 3560-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。

Catalyst 2960-S はスイッチ スタックをサポートします。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 スイッチを指し、スイッチ スタックを指しません。

これらのリリース ノートには、IOS Release 15.2(1)E 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.5）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.6）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

目次

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 2960-S、および 2960-P スイッチ

スイッチ	説明	サポートする最小 Cisco IOS Release
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）× 48 および SFP+ モジュール スロット × 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）× 24 および SFP+ モジュール スロット × 2	Cisco IOS Release 12.2(53)SE1

表 1　サポートされる Catalyst 2960-S、および 2960-P 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-48TD-L[1]	10/100/1000 ポート × 48 および SFP+ モジュール スロット × 2	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TD-L[1]	10/100/1000 ポート × 24 および SFP+ モジュール スロット × 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）× 48 および SFP モジュール スロット × 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）× 48 および SFP モジュール スロット × 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）× 24 および SFP モジュール スロット × 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-48TS-L[1]	10/100/1000 ポート × 48 および SFP モジュール スロット × 4	Cisco IOS Release 12.2(53)SE1
Catalyst 2960S-24TS-L[1]	10/100/1000 ポート × 24 および SFP モジュール スロット × 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
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
Catalyst C2960P-48PST-L	PoE 対応 10/100 ポート × 48、1000BASE-T× 2、SFP アップリンク × 2、LAN Base イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24PC-L	PoE 対応 10/100 ポート × 24、1000BASE-T× 2 または SFP アップリンク × 2、LAN Base イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24LC-L	10/100 ポート × 24、PoE 対応ポート × 8、1000BASE-T× 2 または SFP アップリンク × 2、LAN Base イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48TC-L	10/100 ポート × 48、1000BASE-T× 2 または SFP アップリンク × 2、LAN Base イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24TC-L	10/100 ポート × 24、1000BASE-T× 2 または SFP アップリンク × 2、LAN Base イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48PST-S	PoE 対応 10/100 ポート × 48、1000BASE-T× 2、SFP アップリンク × 2、LAN Lite イメージ	Cisco IOS Release 15.0(2)EZ

表 1　サポートされる Catalyst 2960-S、および 2960-P スイッチ （続き）

スイッチ	説明	サポートする最小 Cisco IOS Release
Catalyst C2960P-24PC-S	PoE 対応 10/100 ポート × 24、1000BASE-T× 2 または SFP アップリンク × 2、LAN Lite イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24LC-S	10/100 ポート × 24、PoE 対応ポート × 8、1000BASE-T× 2 または SFP アップリンク × 2、LAN Lite イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-48TC-S	10/100 ポート × 48、1000BASE-T× 2 または SFP アップリンク × 2、LAN Lite イメージ	Cisco IOS Release 15.0(2)EZ
Catalyst C2960P-24TC-S	10/100 ポート × 24、1000BASE-T× 2 または SFP アップリンク × 2、LAN Lite イメージ	Cisco IOS Release 15.0(2)EZ

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。

Device Manager のシステム要件

- 「ハードウェア要件」（P.4）
- 「ソフトウェア要件」（P.4）

ハードウェア要件

表 2　最小ハードウェア要件

プロセッサの速度	DRAM	色数	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 2960-C 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 2960-C 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。

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 3　　Cisco IOS ソフトウェア イメージ ファイル

ファイル名	説明
c3560c405ex-universalk9npe-tar.152-1.E.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.152-1.E.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.152-1.E.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。
c3560c405-universalk9-tar.152-1.E.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。
c2960s-universalk9-tar.152-1.E.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.152-1.E.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.152-1.E.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。

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 3（P.6）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。

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 15.2(1)E の新機能

- （Catalyst スイッチ 2960-C LAN ベース、3560-C LAN Base）IPv6 のファーストホップ セキュリティ機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外するルータ アドバタイズメント ガードをサポートします。
- （Catalyst スイッチ 2960-C LAN ベース、3560-C LAN ベース）またファーストホップ セキュリティ機能は、バインディング インテグリティ ガードをサポートします。バインディング インテグリティ ガードは、不正なユーザがアドレスの盗難またはスプーフィングができないようにバインディング テーブルを使用します。
- （Catalyst スイッチ 2960-Plus）IPv6 のファーストホップ セキュリティ機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外するルータ アドバタイズメント ガードをサポートします。
- （Catalyst スイッチ 2960-S、2960-SF および 2960-C、3560-C LAN Base）IPv6 QoS のサポート。
- （LAN Base）ciscoDynamicArpInspectionMIB のサポート。
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）Smart Install Upgrade フォールバック、設定のみ導入、イメージのみ導入をサポート。
- （Catalyst スイッチ 2960-S、2960-SF、および 3560-C LAN Base）ホップごとの EH ACL スロットリングおよびフィルタリングのサポート。
- （Catalyst スイッチ 2960-S、2960-SF、および 2960-C LAN Lite、3560-C LAN Base）GLC-T SFP+ ポートのサポート。
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 3560-C LAN Base）SFP+ ポートでの GLC-GE-100FX のサポート（Wall-E ではサポートされません）。
- （Catalyst スイッチ 2960-S、2960-SF、および 2960-C LAN Lite、2960-Plus、3560-C LAN Base）スクリプト ベースのゼロ タッチ プロビジョニングのサポート。
- （Catalyst スイッチ 2960-S および 2960-SF LAN Base）DWDM SFP+ のサポート。
- （Catalyst スイッチ 2960-S および 2960-SF LAN Base）SFP+ ZR のサポート。
- （Catalyst スイッチ 2960-S、2960-SF、および 2960-C LAN Lite）SFP 光トランシーバのデジタル オプティカル モニタリング（DOM）MIB では、リアルタイムの動作パラメータを監視できます。それぞれの DOM 対応光トランシーバは、特定のインターフェイスで温度、電圧、レーザー バイアス電流および Optical Tx および Rx Power などの動作パラメータを監視するために設定された 5 台のセンサーがあります。
- （Catalyst スイッチ 3560-C IP Base）MSP およびメタデータのサポート。
- （Catalyst スイッチ 3560-C IP ベース）IPv4 を介した手動設定トンネルのサポート。
- （Catalyst スイッチ 3560-C IP Base）IPv6 EIGRP スタブ ルーティングのサポート。
- （Catalyst スイッチ 3560-C IP Base）IPv6 PIM スタブ ルーティングのサポート。
- （Catalyst スイッチ 2960-S および 2960-SF LAN Base）SXP ループ検出のサポート。
- （Catalyst スイッチ 2960-S、2960-SF、2960-C、3560-C IP Base、および 2960-Plus LAN Base）デバイス センサーの DHCP グリーニングのサポート。
- （Catalyst スイッチ 3560-C IP Base）スイッチ内の PMK パスワードの暗号化のサポート。
- （LAN ベース）CISCO-EMBEDDED-EVENT-MGR-MIB のサポート。

- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）SNMP-COMMUNITY-MIB のサポート。
- IPv6 対応機能：
  - （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）ICMP RFCs 4291、4443、3484, 2526、4861、4862、5095、4007、3513 を更新しました。
  - （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）UDP MIB（RFC 4113）および TCP MIB（RFC 4022）のサポート。
- （Catalyst スイッチ 3560-C IP Base）EIGRP 機能：
  - EIGRP IPv6 NSF/GR
  - EIGRP MIB
  - EIGRP IPv6 MIBs
  - ルート タグの機能拡張
  - EIGRP ネイバーがダウン状態になったときに SNMP トラップを生成します。
  - EIGRP での IPX のディセーブル化
  - EIGRP 追加パス
  - EIGRP ワイド メトリックのサポート
- （Catalyst スイッチ 3560-C IP Base）OSPF 機能：
  - OSPFv3 BFD
  - OSPFv3 グレースフル シャットダウン
  - OSPFv2 NSSA
  - OSPFv3 NSSA オプション
  - OSPFv3 外部パス プリファレンス
  - OSPFv3 ルータの最大メトリック ルータ LSA
  - OSPFv3 再送信の制限
  - OSPFv3 プレフィックス抑制のサポート
  - OSPFv3 Area Filter/DC Ignore のサポート
  - OSPFv3 MIB、OSPF MIB
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）TFTP の IPv6 のサポート。
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）IPv6 経由の DNS のサポート。
- （Catalyst スイッチ 3560-C IP Base）HSRP-aware PIM のサポート。
- （LAN Base）IPv6 ネイバー探索拡張機能：
  - 非送信請求 NA のグローバル IPv6 エントリを作成するための機能拡張
  - IPv6 ND キャッシュの失効
  - NUD で使用される NS タイマーの幾何バック オフを設定するためのオプション
- （Catalyst スイッチ 3560-C IP サービス）BGP 機能：
  - 4 バイト BGP ASN 数のサポート

  - 不正な形式の属性エラー処理に対する BGP サポート
  - Cisco-BGP-MIBv2 に対する BGP サポート
  - グレースフル シャットダウンに対する BGP サポート
  - Add-Path に対する BGP サポート
  - VRF ダイナミック ルート リークに対する BGP サポート（VRF Lite）
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）Netconf XML PI **show output** のサポート。
- （Catalyst スイッチ 2960-S、2960-SF、2960-C LAN Lite、および 2960-Plus、3560-C LAN Base）TCP キープアライブ タイマーのサポート。

主な機能の最小 Cisco IOS Release

表 4 には、Catalyst 2960-S、2960-C および 3560-C 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 4　Catalyst 2960-S、2960-C および 3560-C スイッチと必要な Cisco IOS の最小リリース

機能	必要な最小 Cisco IOS Release	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	2960-S
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	2960-S
Auto Smartport の改善されたデバイス分類機能	15.0(1)SE	2960-S
EnergyWise Phase 2.5	12.2(58)SE1	2960-S
プロトコル ストーム プロテクション	12.2(58)SE1	2960-S
Smart Install 3.0	12.2(58)SE1	2960-S
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	2960-S
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	2960-S
NTP バージョン 4	12.2(58)SE1	2960-S
IPv6 経由の RADIUS、TACACS+、および SSH/SCP	12.2(58)SE1	2960-S
IETF IP-MIB と IP-FORWARD-MIB（RFC4292 および RFC4293）更新	12.2(58)SE1	2960-S
Auto-QoS の機能拡張	12.2(55)SE	2960-S
グローバル マクロを含む Auto Smartport の拡張機能	12.2(55)SE	2960-S
Smart Install の拡張機能と新機能	12.2(55)SE	2960-S
ポート ACL の改善	12.2(55)SE	2960-S
CDP および LLDP ロケーションの拡張機能	12.2(55)SE	2960-S
VLAN 割り当てを使用した複数認証	12.2(55)SE	2960-S
SVI でのスタティック ルーティング サポート	12.2(55)SE	2960-S

表 4　Catalyst 2960-S、2960-C および 3560-C スイッチと必要な Cisco IOS の最小リリース （続き）

機能	必要な最小 Cisco IOS Release	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	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-S

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」（P.12）
- 「デバイス マネージャの制限」（P.18）

Cisco IOS 制限事項

特に明記しない限り、Catalyst 2960-S、2960-SF、2960-C、2960-Plus、および 3560-C スイッチには、次の制限事項が適用されます。

- 「設定」（P.12）
- 「イーサネット」（P.13）
- 「HSRP」（P.14）
- 「HSRP」（P.14）
- 「IP」（P.14）
- 「IP テレフォニー」（P.14）
- 「電源」（P.15）
- 「QoS」（P.15）
- 「Smart Install」（P.16）
- 「SPAN および RSPAN」（P.17）
- 「スパニングツリー プロトコル」（P.17）
- 「トランキング」（P.18）
- 「VLAN」（P.18）

設定

- 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）

- 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）

- 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）

- 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）

イーサネット

- 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）

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

- 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）

- 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）

- 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）

- 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）

電源

- 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）

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）

- 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

- スイッチに RSPAN 機能が設定されている場合は、RSPAN 送信元ポートから受信した Cisco Discovery Protocol（CDP）パケットには RSPAN VLAN ID のタグが付けられ、RSPAN VLAN を伝送するトランク ポートに転送されます。このような場合、2 ホップ以上離れたスイッチは、RSPAN 送信元ポートに接続されているスイッチを CDP ネイバーとして誤ってリストします。

  これはハードウェアの制限です。これは、スイッチに接続されたデバイス上で RSPAN VLAN を伝送するすべてのインターフェイスの CDP をディセーブルにすることで回避できます。（CSCeb32326）

- SPAN 送信元から受信された CDP、VLAN トランキング プロトコル（VTP）、およびポート集約プロトコル（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。

トランキング

- 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）。

- 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）

- 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 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

特に明記しない限り、Catalyst 2960-S、2960-SF、2960-C、2960-Plus、および 3560-C スイッチには、次の警告が含まれます。

- 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。

- 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。

- 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。

- CSCug54690

  IPv6 アクセスリスト カウンタは、IPv6 ACL に一致するクラス マップに関連付けられたポリシーマップが物理インターフェイスに適用されて、一致したトラフィックが送信される場合は増加しません。

  回避策はありません。

- CSCug69823

  設定した直後に EnergyWise SNMP プロキシ設定を削除した場合、システムがクラッシュします。

  これは、EnergyWise SNMP プロキシを設定した後、しばらくの間待機してそれから設定を削除することでクラッシュを回避できます。

- CSCug74567（Catalyst 2960-S および 2960-SF スイッチ）

  スタック マスターのリロードで、フィルタ ID のサプリカントが接続不能になります。

これは、フィルタ ID の代わりに dACL を使用することで回避できます。フィルタ ID のサプリカントは、新しいセッションが確立されるまで接続が失われます。

- CSCuj00841（Catalyst 3560-CG スイッチ）

  Cisco TrustSec 機能が利用できません。

  回避策はありません。

解決済みの警告

Cisco IOS Release 15.2(1)E で解決済みの警告

- 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。

- 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アクセス コントロール リスト（ACL）が機能しません。

  回避策はありません。

- CSCuc51915

  Preboot Execution Environment（PXE）がイネーブルになっているホストは、IP ソース ガードがスイッチに設定されている場合は正常に起動できません。

  回避策はありません。

- CSCud47137（Catalyst 2960-S スイッチ）

  マスター スイッチに障害が発生すると、LACP がイネーブルにされた EtherChannel 内のスタック メンバー リンクが回復できません。

  これは、スイッチを再起動してリンク障害をリカバリすることで回避できます。

- CSCue09838（Catalyst 2960-S スイッチ）

  VLAN は情報を、Telnet セッションを介して **show tech-suppot details** コマンドから収集するときに、VLAN がダウンします。

  これは、スイッチをリロードすることで回避できます。

- CSCuf13634

  インターフェイス ステータスは、（**speed nonegotiate** 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場合）リンク ネゴシエーションがディセーブルでも、ポートがアップ状態でデュプレックスと速度が自動に設定されていることを表示します。

  これは、**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 コマンドを使用してインターフェイスを再起動することで回避できます。

- CSCuf77683

show snmp mib ifmib ifindex コマンドを入力するか、SNMP が ipMIB オブジェクトをクエリーする場合に、内部 VLAN が表示されます。

これは、表示された VLAN が内部であるかどうか確認し、次にこれらを非表示にすることで回避できます。

- CSCug17582

  AAA が設定されている場合、**enable** コマンドを入力すると次のメッセージが表示されます。

  ```
  Password required, but none set
  ```

  これは、**aaa authentication enable default enable** 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します。

- CSCug43533

  マクロがデバイスの分類に使用される場合、CISCO_LAST_RESORT_EVENT マクロが、スイッチで理由なくトリガーされます。

  回避策はありません。

- CSCug51225（Catalyst 2960-S および 2960-C スイッチ）

  新しいメンバーがスイッチ スタックに追加されると、トポロジ変更通知（TCN）フラッディングがネットワークでトリガーされます。

  回避策はありません。

- CSCug67745（Catalyst 3560-C スイッチ）

  マルチキャスト モードでは、Web キャッシュ通信プロトコル（WCCP）ISY パケットがキャッシュ エンジンで受信されません。

  これは、ユニキャスト モードを使用することで回避できます。

- CSCuh04978（Catalyst 2960-S スイッチ）

  ポートで動的に学習された MAC アドレスは連続的な着信トラフィックであっても削除されます。この結果、削除された MAC アドレス宛のパケットでユニキャスト フラッディングが発生します。

  これは、MAC アドレス エントリを静的に設定するか、または（**no macro auto monitor** グローバル コンフィギュレーション コマンドを使用して）デバイス分類子をディセーブルにすることで回避できます。

- CSCuh12528

  （**ip dhcp conflict resolution** グローバル コンフィギュレーション コマンドを使用して）DHCP アドレス競合解決が有効な状態で、**clear ip dhcp conflict** コマンドが入力すると、スイッチは動作を停止します。

  回避策はありません。

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 2960-S、2960-SF、2960-C、2960-Plus、および 3560-C 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。

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 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の一覧も示されています。
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。

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/