



Catalyst 2960-P スイッチ、 Cisco IOS Release 15.0(2)EZ リリース ノート

2013 年 4 月

【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)EZ は Catalyst 2960-P スイッチで動作します。

リリース ノートには、Cisco IOS Release 15.0(2)EZ 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および制約事項が含まれます。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.6) 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.7) 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」 (P.2)
- 「スイッチ ソフトウェアのアップグレード」 (P.6)
- 「インストール上の注意事項」 (P.9)
- 「新しいソフトウェア機能」 (P.9)
- 「主な機能の最小 Cisco IOS Release」 (P.10)
- 「制限事項」 (P.15)
- 「特記事項」 (P.25)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.30)

システム要件

- 「サポート対象ハードウェア」 (P.2)
- 「Device Manager のシステム要件」 (P.5)
- 「クラスタの互換性」 (P.6)
- 「CNA の互換性」 (P.6)

サポート対象ハードウェア

表 1 サポートされている Catalyst 2960、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 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-Plus 24PC-S	10/100BASE-TX PoE ポート× 24 およびデュアルパーパス ポート× 2	Cisco IOS Release 15.0(2)EZ
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-Plus 24LC-S	10/100BASE-TX ポート× 24 (その内 8 ポートが PoE) およびデュアルパーパス ポート× 2	Cisco IOS Release 15.0(2)EZ
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

表 1 サポートされている Catalyst 2960、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 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 Small Form-Factor Pluggable (SFP) モジュール スロット×1 (ファン、RPS ポートはありません))	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-Plus 48PST-S	10/100B SE-TX 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 15.0(2)EZ
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-Plus 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 15.0(2)EZ
Catalyst 2960-24-S	10/100 BASE-TX イーサネット ポート×24 (RPS ポートまたは SFP モジュール スロットはありません)	Cisco IOS Release 12.2(37)EY
Catalyst 2960-Plus 24TC-S	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 (RPS ポートはありません)	Cisco IOS Release 15.0(2)EZ
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-Plus 48TC-S	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 (RPS ポートはありません)	Cisco IOS Release 15.0(2)EZ
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、SFP モジュール スロット×1、ファンまたは RPS ポートはありません)	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-Plus 24PC-L	10/100BASE-TX PoE ポート×24 およびデュアルパーパス ポート×2	Cisco IOS Release 15.0(2)EZ
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 2960G-48TC-L	10/100/1000BASE-T イーサネット ポート×44 およびデュアルパーパス ポート×4	Cisco IOS Release 12.2(25)FX

表 1 サポートされている Catalyst 2960、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 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
Catalyst 2960-Plus 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 15.0(2)EZ
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-Plus 48PST-L	10/100BASE-TX PoE ポート×48、 10/100/1000BASE-T 銅線ポート×2、SFP モジュール スロット×2	Cisco IOS Release 15.0(2)EZ
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 2960-Plus 24LC-L	10/100BASE-TX ポート×24 (その内 8 ポートが PoE) およびデュアルパーパス ポート×2	Cisco IOS Release 15.0(2)EZ
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

表 2 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

表 2 サポートされている他のハードウェア (続き)

スイッチ	説明	サポートする最小 Cisco IOS Release
SFP モジュール (Catalyst 2960)	100BASE-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
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

Device Manager のシステム要件

- 「ハードウェア要件」(P.5)
- 「ソフトウェア要件」(P.5)

ハードウェア要件

表 3 最小ハードウェア要件

プロセッサ速度	DRAM	色数	解像度	フォントサイズ
233 MHz 以上 ¹	512 MB ²	256	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」(P.6)
- 「使用するファイルの決定」(P.7)
- 「ソフトウェア イメージのアーカイブ」(P.7)
- 「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」(P.8)
- 「CLI を使用したスイッチのアップグレード」(P.8)
- 「ソフトウェア障害からの回復」(P.9)

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 4 Cisco IOS ソフトウェア イメージ ファイル

ファイル名	説明
c2960-lanbasek9-tar.150-2.EZ.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.EZ.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。

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 4 (P.7) 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) TFTP 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-ip-services-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witch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witch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witch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witch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)EZ の新機能

- Catalyst 2960-P スwitchに搭載された Cisco IOS Release 15.0(2)EZ 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-P スイッチの Cisco IOS Release 15.0(2)EZ のイメージは、FIPS 認証済みです。FIPS 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>
- インストール ノート：
http://www.cisco.com/en/US/products/ps10745/prod_installation_guides_list.html
- 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、スパンニングツリー 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。
- 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-P スイッチの LAN Lite イメージ)。
- 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。
- 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 の LAN Base 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。
- 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 5 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 5 Catalyst 3、2960、2 および 2960-P スイッチ機能と必要な最小 Cisco IOS リリース

機能	必要な最小 Cisco IOS Release	Catalyst スイッチ サポート
クリティカル音声 VLAN	15.0(1)SE	2960、2960-P
サブリカント ポートへのアクセスを制御する NEAT 機能拡張	15.0(1)SE	2960、2960-P
Auto Smartport の改善されたデバイス分類機能	15.0(1)SE	2960、2960-P
EnergyWise Phase 2.5	12.2(58)SE1	2960、2960-P
プロトコル ストーム プロテクション	12.2(58)SE1	2960、2960-P
Smart Install 3.0	12.2(58)SE1	2960、2960-P
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、2960-P
Call Home のサポート	12.2(58)SE1	2960、2960-P
NTP バージョン 4	12.2(58)SE1	2960、2960-P
IPv6 経由の RADIUS、TACACS+、および SSH/SCP	12.2(58)SE1	2960、2960-P
IETF IP-MIB と IP-FORWARD-MIB (RFC4292 および RFC4293) 更新	12.2(58)SE1	2960、2960-P
Auto-QoS の機能拡張	12.2(55)SE	2960、2960-P
グローバル マクロを含む Auto Smartport の拡張機能	12.2(55)SE	2960、2960-P
Smart Install の拡張機能と新機能	12.2(55)SE	2960、2960-P
ポート ACL の改善	12.2(55)SE	2960、2960-P
CDP および LLDP ロケーションの拡張機能	12.2(55)SE	2960、2960-P
VLAN 割り当てを使用した複数認証	12.2(55)SE	2960、2960-P
Cisco TrustSec	12.2(55)SE	2960、2960-P
メモリの整合性検査ルーチン	12.2(55)SE	2960、2960-P
SVI でのスタティック ルーティング サポート	12.2(55)SE	2960、2960-P
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、2960-P
LAN Lite イメージでの DHCP スヌーピング、オプション 82 および LLDP-MED	12.2(55)SE	2960、2960-P
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	2960、2960-P
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	2960、2960-P
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	2960、2960-P
RADIUS 許可の変更 (CoA)。	12.2(52)SE	2960、2960-P
複数の VLAN の配置に対応した 802.1X ユーザ分散。	12.2(52)SE	2960、2960-P
マルチホスト認証を使った、重要な VLAN。	12.2(52)SE	2960、2960-P
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	2960、2960-P
ポートのホスト モードを変更する Network Edge Access Topology (NEAT)。	12.2(52)SE	2960、2960-P

表 5 Catalyst 3、2960、2 および 2960-P スイッチ機能と必要な最小 Cisco IOS リリース (続き)

機能	必要な最小 Cisco IOS Release	Catalyst スイッチ サポート
VLAN ID ベース MAC 認証	12.2(52)SE	2960、2960-P
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	2960、2960-P
SNMPv3 を使った 3DES および AES。	12.2(52)SE	2960、2960-P
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	2960、2960-P
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	2960、2960-P
LLPD-MED へのサポート強化	12.2(52)SE	2960、2960-P
LLPD-MED MIB および CISCO-ADMISSION-POLICY-MIB。	12.2(52)SE	2960、2960-P
IPv6 QoS トラスト機能。	12.2(52)SE	2960、2960-P
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	2960、2960-P
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	2960、2960-P
802.1x スイッチ サブ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	2960、2960-P
オープン アクセスを使用した 802.1x	12.2(50)SE	2960、2960-P
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	2960、2960-P
柔軟な認証シーケンス	12.2(50)SE	2960、2960-P
マルチユーザ認証	12.2(50)SE	2960、2960-P
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	2960、2960-P
ワイヤード ロケーション サービス	12.2(50)SE	2960、2960-P
CPU 使用率しきい値トラップ	12.2(50)SE	2960、2960-P
Cisco IOS Configuration Engine (旧称 Cisco IOS CNS エージェント)	12.2(50)SE	2960、2960-P
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	2960、2960-P
RADIUS サーバのロード バランシング	12.2(50)SE	2960、2960-P
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	2960、2960-P
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	2960、2960-P
制限付き VLAN を使用した 802.1x 認証	12.2(50)SE	2960、2960-P
IP ソース ガード	12.2(50)SE	2960、2960-P
ダイナミック ARP インスペクション	12.2(50)SE	2960、2960-P
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	2960、2960-P

表 5 Catalyst 3、2960、2 および 2960-P スイッチ機能と必要な最小 Cisco IOS リリース (続き)

機能	必要な最小 Cisco IOS Release	Catalyst スイッチ サポート
汎用メッセージ認証サポート	12.2(46)SE	2960、2960-P
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	2960、2960-P
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	2960、2960-P
DHCP サーバ ポート ベースのアドレス割り当て	12.2(46)SE	2960、2960-P
IPv6 デフォルト ルータの初期設定 (DRP)	12.2(46)SE	2960、2960-P
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、2960-P
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、2960-P
ACL および RADIUS Filter-Id 属性を使った IEEE 802.1x 認証。	12.2(46)SE	2960、2960-P
IEEE 802.1x 準備状態チェック	12.2(44)SE	2960、2960-P
DHCP ベースの自動設定とイメージアップデート	12.2(44)SE	2960、2960-P
設定可能なスモール フレーム着信しきい値	12.2(44)SE	2960、2960-P
IPv6 経由の HTTP および HTTP のサポート	12.2(44)SE	2960、2960-P
IPv6 トランスポート経由の SNMP 設定	12.2(44)SE	2960、2960-P
IPv6 ステートレス自動設定	12.2(44)SE	2960、2960-P
Flex Link マルチキャスト高速コンバージェンス	12.2(44)SE	2960、2960-P
設定の交換およびロールバック	12.2(40)SE	2960、2960-P
リンク層検出プロトコル メディア拡張 (LLDP-MED)	12.2(40)SE	2960、2960-P
Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6	12.2(40)SE	2960、2960-P
自動 Quality of Service (QoS) Voice over IP (VoIP)	12.2(40)SE	2960、2960-P
MLD スヌーピング	12.2(40)SE	2960、2960-P
IPv6 ホスト	12.2(40)SE	2960、2960-P
IP Phone 検出機能拡張	12.2(37)SE	2960、2960-P
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	2960、2960-P
VLAN 認識ポート セキュリティ オプション	12.2(37)SE	2960、2960-P
VLAN Flex Link ロード バランシング	12.2(37)SE	2960、2960-P
Web 認証	12.2(35)SE	2960、2960-P
MAC 非アクティブ エージング	12.2(35)SE	2960、2960-P
DHCP Option 82 が設定可能なリモート ID および回線 ID	12.2(25)SEE	2960、2960-P
IPv6 ACL	12.2(25)SED	2960、2960-P
IPv6 Multicast Listener Discovery (MLD) スヌーピング	12.2(25)SED	2960、2960-P
ポートでの QoS 階層型ポリシー マップ	12.2(25)SED	2960、2960-P
NAC レイヤ 2 IEEE 802.1x 検証	12.2(25)SED	2960、2960-P
NAC レイヤ 2 IP 検証	12.2(25)SED	2960、2960-P

表 5 Catalyst 3、2960、2 および 2960-P スイッチ機能と必要な最小 Cisco IOS リリース (続き)

機能	必要な最小 Cisco IOS Release	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	2960、2960-P
制限付き VLAN を使用した IEEE 802.1x	12.2(25)SED	2960、2960-P
PoE ポートに接続された装置の電力バジェット	12.2(25)SEC	2960、2960-P
IEEE 802.1s 標準に基づく Multiple Spanning Tree (MST)	12.2(25)SEC 12.2(25)SED	2960、2960-P
Unique Device Identifier (UDI)	12.2(25)SEC 12.2(25)SED	2960、2960-P
Wake-on-LAN 機能を使用した IEEE 802.1x	12.2(25)SEC 12.2(25)SED	2960、2960-P
コンフィギュレーション ロギング	12.2(25)SEC 12.2(25)SED	2960、2960-P
Secure Copy Protocol (SCP)	12.2(25)SEC 12.2(25)SED	2960、2960-P
スタック間 EtherChannel	12.2(25)SEC	2960、2960-P
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	2960、2960-P
プライベート VLAN の IP ソース ガード	12.2(25)SEB	2960、2960-P
IEEE 802.1x の制限付き VLAN	12.2(25)SED	2960、2960-P
IGMP Leave タイマー	12.2(25)SEB 12.2(25)SED	2960、2960-P
IGMP スヌーピング クェリア	12.2(25)SEA 12.2(25)FX	2960、2960-P
DSCP 透過性	12.2(25)SE 12.2(25)FX	2960、2960-P
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	2960、2960-P
デバイス マネージャ	12.2(25)SE 12.2(25)FX	2960、2960-P
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	2960、2960-P
Cisco インテリジェント電力管理	12.2(25)SE	2960、2960-P
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	2960、2960-P
ダイナミック ARP インスペクション	12.2(20)SE	2960、2960-P
Flex Link	12.2(20)SE 12.2(25)FX	2960、2960-P
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	2960、2960-P

表 5 Catalyst 3、2960、2 および 2960-P スイッチ機能と必要な最小 Cisco IOS リリース (続き)

機能	必要な最小 Cisco IOS Release	Catalyst スイッチ サポート
IP ソース ガード	12.2(20)SE	2960、2960-P
プライベート VLAN (IP サービス イメージのみ)	12.2(20)SE	2960、2960-P
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	2960、2960-P
SmartPort マクロ	12.2(18)SE 12.2(25)FX	2960、2960-P
Flex Link の優先スイッチオーバー	12.2(25)SEE	2960、2960-P

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」 (P.15)
- 「デバイス マネージャの制限」 (P.25)

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」 (P.16)
- 「イーサネット」 (P.17)
- 「EtherSwitch モジュール」 (P.18)
- 「HSRP」 (P.18)
- 「IP」 (P.18)
- 「IP テレフォニー」 (P.18)
- 「マルチキャスト」 (P.19)
- 「電力」 (P.20)
- 「QoS」 (P.20)
- 「RADIUS」 (P.22)
- 「Smart Install」 (P.22)
- 「SPAN および RSPAN」 (P.23)
- 「スパニングツリー プロトコル」 (P.24)
- 「トランッキング」 (P.24)

- 「VLAN」 (P.25)

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。（CSCe71176 および CSCdz11708）

- プリアンプ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）

- (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 ポー 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 個のポー 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、ポー レートを変更するために CLI コマンドを拒否します。

ポー 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。次にポー 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）

- 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）

- **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。

イーサネット

- (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)

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ンニングツリー 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)

- 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)

マルチキャスト

- 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せん。

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)

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があります。(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。

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。

- 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、RSTP 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

- 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 エントリの出カ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

- 「Cisco IOS に関する注意事項」(P.25)
- 「Cisco IOS に関する注意事項」(P.25)
- 「デバイス マネージャに関する注意事項」(P.26)

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witch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ため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}	<p>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。</p> <ul style="list-style-type: none"> • aaa : 認証、許可、アカウント機能を一時的に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おりローカル ユーザ データベースが使用されます。

	コマンド	目的
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。

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、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 2960 および 2960-P 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-P Switch Software Configuration Guide*』
- 『*Catalyst 2960 and 2960-P Switch Command Reference*』
- 『*Catalyst 2960 Switch Hardware Installation Guide*』
- 『*Catalyst 2960 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。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

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/>