SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェアバージョン 2.5.8.15 までのリリースノート

はじめに

2021 年 11 月

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.8.15 リリースノート

解決済みの問題 v2_5_8_15

リリースバージョン 2.5.8.15 で解決された問題

不具合 ID	説明
CSCvx47098	**症状** いくつかの SKU のファン速度が正確ではない。
CSCvz30721	**症状** GLC-SX-MMD で Nexans スイッチに接続するために使用される MGBSX1 がコンボポートのみで機能する。
CSCwa17228	**症状** CBD プローブおよびモバイルアプリが、ユーザーパスワードを変更した後、更新されたパスワードでデバイスに接続できない。

はじめに

2021 年 9 月

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.8.12 リリースノート

新機能

このセクションでは、このファームウェアリリースで利用可能な新機能と変更について詳しく説明します。

SG350XG および SG550XG をサポートする最後のバージョン

ファームウェアリリース 2.5.8.12 は、SG350XG および SG550XG SKU をサポートする最後のファームウェアバージョンです（以下の完全なリストを参照）。これらの SKU をファームウェアバージョン 2.6 以降にファームウェアアップグレードすることは禁止され、ブロックされます。これらの SKU のいずれかを含むスタックを、スタック内の他のユニットが異なるタイプであっても、バージョン 2.6 以降にアップグレードすることはできません。

ファームウェアバージョン 2.6 を実行しているスタックに SG350XG または SG550XG SKU が追加された場合、ユニットはシャットダウンし、スタックには参加しません。

以前のバージョン 2.5.7.x からバージョン 2.6 以降へのファームウェアのアップグレードは、すべての SKU で禁止されています。ユーザーは、まずデバイスをバージョン 2.5.8 にアップグレードしてから、（可能であれば）バージョン 2.6 以降にアップグレードする必要があります（SG350XG および SG550X に含まれていない SKU の場合）。

表 *1:* 該当する *SKU*

SKU 名	SKU の説明
SG350XG-24F	SG350XG-24F 24 ポート 10G SFP+ スタッカブル マネージド スイッチ
SG350XG-24T	SG350XG-24T 24 ポート 10GBase-T スタッカブル マネージド スイッチ
SG350XG-48T	SG350XG-48T 48 ポート 10GBase-T スタッカブル マネージド スイッチ
SG350XG-2F10	SG350XG-2F10 12 ポート 10G スタッカブル マネージド スイッチ
SG550XG-8F8T	SG550XG-8F8T 16 ポート 10G スタッカブル マネージド スイッチ
SG550XG-24T	SG550XG-24T 24 ポート 10GBase-T スタッカブル マネージド スイッチ
SG550XG-24T	24 ポート 10GBase-T スタッカブル マネージド スイッチ
SG550XG-48T	48 ポート 10GBase-T スタッカブル マネージド スイッチ

更新された Cisco Trusted Core Bundle

ファームウェアリリース 2.5.8.12 では、2021 年 7 月 5 日付のシスココアバンドルが使用されます。

バージョン 2.5.7.x 以降からバージョン 2.5.5.x 以前へのダウングレード

バージョン 2.5.7.x 以降のスイッチは、AAA ユーザーログイン情報の高度な暗号化をサポートしています。ユーザーログイン情報は、HMAC-SHA-512 ハッシュに基づく PBKDF2 を使用してソルト付与およびハッシュ化されます。この暗号化方式はバージョン 2.5.5.x（およびそれ以前のバージョン）ではサポートされていないため、バージョン 2.5.5.x 以前にダウングレードすると、ユーザーログイン情報を含む構成ファイルを維持管理できなくなります。

そのため、スイッチのセキュリティの維持を目的として、バージョン 2.5.7.x 以降からバージョン 2.5.5.x 以前にダウングレードすると、構成ファイルが消去されます。

ファームウェアをダウングレードする前に、構成ファイルを必ずバックアップしてください。デバイスにもう一度ロードする前に、暗号化された AAA ユーザーログイン情報を含む行を削除します。次に、構成ファイルのコピーをデバイスにダウングレードします。この手順に従うと、デフォルトのログイン情報でログインできるようになります。この時点で、必要なログイン情報を使用してデバイスを更新し、構成を保存します。

ダウングレードに関する注記：PoE チップのバージョン

工場から出荷されたリリース 2.4.5.x 以降のボードは、更新された PoE チップセットである 6920xM バージョン 0x4a02 を使用しています。この新しいチップセットバージョンに加えて、スイッチは以下もサポートします。

- PoE チップセット 6920xM バージョン 0x4b42（2.4.0.x までの SW バージョン 2.2.8.4 を使用して製造されたボードで使用）
- PoE チップセット 6920x バージョン 0x4ac2（SW バージョン 2.1.0.63 ～ 2.2.7.7 を使用して製造されたボードで使用）
  - PoE チップセットのバージョンは、「show power inline」コマンド出力の一部として確認できます。
  - サポートされているチップセットのバージョンが異なるため、次のダウングレードルールが適用されます。
- 非 PoE SKU、および元の PoE チップセット（69208 0x4ac2）を使用する PoE SKU
  - 以前のバージョンと同じダウングレードルールに従います（この SKU によってサポートされる最初の SW バージョンまでのダウングレードが基本的に許可されます）。
- PoE チップセット 0x4b42 をサポートする Sx250 SKU
  - 2.2.7 以前のバージョンへのダウングレードは阻止されます。
- チップセット 0x4a02 をサポートする次の Sx250 SKU：SG250-10P、SG250-26HP/P、SF250-48HP

- 2.4 からのダウングレードは完全に阻止されます。

- チップセット 0x4a02 をサポートする次の Sx250 SKU：SF250-24P、SG250-08HP、SG250-50HP、SG250-50P、SG250X-24P、SG250X-48P
  - バージョン 2.3.5（これらの SKU をサポートする最初の SW バージョン）にのみダウングレードできます。

- チップセット 0x4a02 または 0x4b42 をサポートする Sx350 または Sx550 PoE SKU
  - バージョン 2.2.7 以下へのダウングレードは阻止されます。

既知の問題 V2_5_8

リリースバージョン 2.5.8.12 で確認された問題

不具合 ID	説明
CSCvz45955	**症状** デバイスに失効した証明書が含まれているときに、バージョン 2.5.5.x から 2.5.7.x にアップグレードした場合、show running firmware を実行するとデバイスが再起動する。問題は 2.5.8 リリースで修正されました。 **回避策** 以前のバージョンからバージョン 2.5.8.12 にアップグレードすると、失効エントリが削除されます。その後、ユーザーは新しいバージョンで再設定する必要があります。

解決済みの問題 V2_5_8

リリースバージョン 2.5.8.12 で解決された問題

不具合 ID	説明
CSCvy74466	**症状** イネーブルパスワードを使用してデバイスの特権 EXEC モードにアクセスできない。
CSCvw29853	**症状** 接続済みの Polycom 社製電話機が LLDP 情報を送信すると、デバイスが再起動する場合がある。
CSCvw28120	**症状** 接続済みの電話機 NEC DT800 が LLDP 情報を送信すると、デバイスが再起動する場合がある。

不具合 ID	説明
CSCvy66085	**症状** FDB ハッシュ衝突フラッドに関連した進行中の syslog メッセージによって、コンソールの使用が妨げられる。
CSCvz45993	**症状** いずれかのインターフェイスの説明に「form」という単語が含まれていると、デバイス GUI をロードできない。
CSCvz46007	**症状** JP または CN OLH の一般情報のサブ項目をクリックすると、デバイスが再起動する。
CSCvz46020	**症状** IPv6 トンネルをルートの宛先として設定した後に、デバイスがリロードする。
CSCvz46034	**症状** Web GUI のデバイスフロントパネルが異常な表示になる。

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.7.85 までのリリースノート

2021 年 3 月

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.7.85 リリースノート

新機能

以前のバージョンからのアップグレード時に、複雑度が有効になります（まだ有効に設定されていない場合）。

1.1 パスワードの複雑度

以前のバージョンでは、ユーザーはパスワードの複雑度の設定を有効または無効にすることができました。バージョン 2.5.7 には、セキュリティ強化のため、ユーザーがパスワードの複雑度の設定を無効にするオプションがありません。パスワードの複雑度として、次のデフォルト値と範囲がサポートされています。

- 最小長：範囲 8 ～ 64、デフォルト = 8

- 最小クラス：範囲 1 ～ 4、デフォルト = 3
- 繰り返しなし：範囲 1 ～ 16、デフォルト = 3
- 現在のものではない/ユーザー名ではない/メーカー名ではない：常に有効

1.2 SSL 暗号のサポート

セキュリティ強化のため、次の暗号のサポートが停止されました。

- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_128_GCM_SHA256
- RSA_WITH_AES_128_CCM_8
- RSA_WITH_AES_256_CCM_8

1.3 暗号のサポート

OpenSSL バージョンが 1.1.0b から 1.1.0l（小文字の L）にアップグレードされました。

1.4 デフォルトのユーザー名とパスワード cisco/cisco

バージョン 2.5.5 では、ユーザーは最初のログイン時にデフォルトのログイン情報を変更する必要がありましたが、ログイン情報 cisco/cisco を明示的に設定することができました。バージョン 2.5.7 で、ユーザーは cisco/cisco をログイン情報として設定できなくなりました。これらのログイン情報は、工場出荷時のデフォルトで、サポートされるのは最初のユーザーログインまでです。

1.5 パスワード暗号化

以前のバージョンでは、ユーザーのログイン情報は構成ファイルに保存され、SHA-1 ハッシュアルゴリズムを使用して表示されていました。現在のリリースでは、ユーザーのログイン情報は、HMAC-SHA-512 ハッシュに基づく PBKDF2 を使用してソルト付与およびハッシュ化されます。これにより、ログイン情報のセキュリティが強化され、さまざまな攻撃から保護されます。

関連するログイン情報：

- ローカル データベース パスワード
- Enable password
- 回線パスワード

以前のバージョンから現在のバージョンにアップグレードすると、既存のパスワードはソルトと新しいハッシュ方式を使用して「ダブルハッシュ」されます。アクセスを必要とするユーザーは、以前のバージョンで設定されたのと同じパスワードを引き続き使用します

現在のバージョンから以前のバージョン（バージョン 2.5.5 以前）にダウングレードすると、セキュリティの問題を防ぐためにデバイス設定が消去されます。デバイスをリロードする前に、ユーザーはこの動作を確認するように求められます。

1.6 SNMPv3 の強化

このバージョンでは、認証方式としての md5 と暗号化方式としての DES のサポートが廃止され、SHA-2 ベースの認証方式（HMAC-SHA-224-128、HMAC-SHA-256-192、HMAC-SHA-384-256、HMAC-SHA-512-384）と AES-128 暗号化方式のサポートが追加されました。以前のバージョンからのアップグレードの場合、md5 認証は SHA-1 に置き換えられ、DES 暗号化は AES-128 に置き換えられます。

1.7 自己署名証明書の有効期間

セキュリティを強化するため、デバイスの自己署名証明書のデフォルトの有効期間とサポートされる有効期間が次のように変更されました。

- 有効な範囲：30 日 ～ 1095 日（つまり 3 年）。以前は 30 日 ～ 10 年でした。
- デフォルト：730 日（つまり 2 年）。以前は 1 年でした。

1.8 ポートのセキュリティアクションの更新

以前のリリースでは、違反している MAC がスイッチの他のインターフェイスでセキュア MAC として登録されている場合、port security に対する drop（discard）アクションと trap アクションのみがサポートされていました。これは、インターフェイスに対して「shutdown」オプションが選択されている場合でも当てはまります（「port security discard-shutdown」）。2.5.7 リリースでは、このタイプの違反に対する shutdown アクションもサポートされています。つまり、port security アクションが discard に設定されている場合、違反している MAC アドレスがデバイスの他のインターフェイスのセキュア MAC アドレスであっても、shutdown アクションが適用されます。

1.9 CA マネージャ：証明書の有効期間とデフォルトのシステムクロック

以前のバージョンでは、デバイスにインストールされた CA 証明書は、現在のシステムの日付と時刻が証明書の有効期間内である場合に有効であることが確認されました。システムは、システムクロックのソースをチェックしませんでした。2.5.7 リリースでは、システムがシステムクロックのソースをチェックし、システムクロックが次のいずれかによって設定された場合にのみ、CA 証明書が有効であることが確認されます。

- SNTP
- ユーザー（または Web ブラウザ）による手動

システムクロックが上記のいずれかの方法（デフォルトのシステムクロック）で設定されていない場合、システム TOD が証明書の有効期間内であっても、証明書は無効と見なされます。

1.10 音声 VLAN および Auto Smartport のデフォルト設定の変更

以前のバージョンにおける音声 VLAN と Auto SmartPort のデフォルト設定は次のとおりでした。

- 音声 VLAN のデフォルトの管理状態：auto-triggered
- Auto SmartPort のデフォルトの管理状態：controlled

バージョン 2.5.7 では、これらの機能のデフォルトは次のようになります。

- 音声 VLAN のデフォルトの管理状態：disabled
- Auto SmartPort のデフォルトの管理状態：disabled

新しいデフォルト設定は、工場出荷時にデバイスに適用されます。2.5.5 リリースとの間でアップグレードまたはダウングレードすると、デバイスは両方の設定の既存値を保持します。そのため、構成ファイルの変更が必要になる場合があります（バージョン間のデフォルト設定の違いによる）。

1.11 PnP エージェント：HTTPS トランスポートプロトコル

2.5.7 リリースでは、HTTPS の設定を第 1 選択のトランスポートプロトコルとしてサポートしています。2.5.5 リリースでは、第 1 選択のトランスポートプロトコルとして HTTP のみがサポートされていました。

1.12 PnP エージェント：組み込みバンドルのサポート

以前のバージョンでは、PnP エージェントは CA 証明書バンドル（trustpool）のダウンロードとインストールをサポートしていました。バンドルは、オプション 43 「T パラメータ」または Cisco PnP Connect を使用して、次の URL からダウンロードできます。 http://www.cisco.com/security/pki/trs/ios_core.p7b.

2.5.7 リリースでは、PnP エージェントの一部として含まれている組み込みバンドルへのサポートが追加されました。組み込み証明書は、PnP Connect サーバーへの接続がアクティブでない場合のバックアップとして使用することを目的としています。最新の PnP Connect からダウンロードしたバンドルを使用するようお勧めします。

1.13 PnP エージェント：証明書 CN/SAN 検証のサポート

2.5.7 リリースでは、CA 証明書を使用したサーバー証明書の検証に加えて、デバイスは、サーバーの IP アドレス/ホスト名を証明書の CN（Common Name）および SAN（Subject Alternative Name）フィールドに含まれる情報と比較する方法も使用して証明書を検証します。CN/SAN 検証に失敗すると、PnP サーバーへの接続が終了し、警告レベルの syslog メッセージとトラップが生成されます。

1.14 スタックユニットの命名

このリリースでは、スタックユニットの命名規則が CLI、GUI、およびドキュメントで次のように変更されました。

- スタックマスターユニット = スタックアクティブユニット
- スタック バックアップ ユニット = スタックスタンバイユニット
- スタックスレーブユニット = スタックメンバーユニット

1.15 CBD バージョンのサポート

2.5.7 リリースは、Cisco Network Probe バージョン 2.2.1.x をサポートします。

1.16 ダウングレードに関する注記：PoE チップのバージョン

工場から出荷されたリリース 2.4.5.x 以降のボードは、更新された PoE チップセットである 6920xM バージョン 0x4a02 を使用しています。この新しいチップセットバージョンに加えて、フィールドのデバイスは以下もサポートします。

- PoE チップセット 6920xM バージョン 0x4b42（2.4.0.x までの SW バージョン 2.2.8.4 を使用して製造されたボードで使用）
- PoE チップセット 6920x バージョン 0x4ac2（SW バージョン 2.1.0.63 ～ 2.2.7.7 を使用して製造されたボードで使用）
  - PoE チップセットのバージョンは、「show power inline」コマンド出力の一部として確認できます。
  - サポートされているチップセットのバージョンが異なるため、次のダウングレードルールが適用されます。
- 非 PoE SKU、および元の PoE チップセット（69208 0x4ac2）を使用する PoE SKU
  - 以前のバージョンと同じダウングレードルールに従います（この SKU をサポートする最初の SW バージョンまでのダウングレードが基本的に許可されます）。
- PoE チップセット 0x4b42 をサポートする Sx250 SKU
  - 2.2.7 以前のバージョンへのダウングレードは阻止されます。
- チップセット 0x4a02 をサポートする次の Sx250 SKU：SG250-10P、SG250-26HP/P、SF250-48HP
  - 2.4 からのダウングレードは完全に阻止されます。
- チップセット 0x4a02 をサポートする次の Sx250 SKU：SF250-24P、SG250-08HP、SG250-50HP、SG250-50P、SG250X-24P、SG250X-48P
  - バージョン 2.3.5（これらの SKU をサポートする最初の SW バージョン）にのみダウングレードできます。
- チップセット 0x4a02 または 0x4b42 をサポートする Sx350 または Sx550 PoE SKU
  - バージョン 2.2.7 以下へのダウングレードは阻止されます。

既知の問題

リリースバージョン 2.5.7.85 で確認された問題

不具合 ID	説明
CSCvx52167	**症状** PnP サーバーアドレスが IPv6 リンクローカルアドレスとして設定されていると、PnP サーバーへの接続に失敗する。 **回避策** グローバル IPv6 アドレスまたは IPv4 アドレスを使用します。
CSCvx52220	**症状** ユーザーが無効にしたにもかかわらず、アラートアイコンが点滅し続ける。 **回避策** なし。
CSCvx52223	**症状** 特定のデバイスにおける XG アップリンクでの CIR = 18M 未満の値の出力トラフィックシェーピング。 **回避策** なし

解決済みの問題

リリースバージョン 2.5.7.85 で解決された問題

不具合 ID	説明
CSCuu65557	**症状** 管理セッションがデバイスの IPv6 アドレスを使用するセキュアセッション（HTTPS）である場合、Safari ブラウザを使用してデバイスを管理できない。 **回避策** 別のブラウザ（Internet Explorer など）を使用するか、非セキュアセッション（HTTP）をセットアップします。

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550Xシリーズスイッチソフトウェアバージョン2.5.5.47までのリリースノート

2020 年 5 月

このリリースノートでは、次の表に一覧表示された製品のソフトウェアバージョン 2.5.5.47 で推奨される操作と既知の問題について説明します。

モデル	説明	ポート
SF250-24	24 ポート 10/100 スマート スイッチ	fa1 ～ fa24、gi1 ～ gi4
SF250-24P	24 ポートギガビット PoE スマートスイッチ	fa1 ～ fa48、gi1 ～ gi4
SF250-48	48 ポート 10/100 スマート スイッチ	fa1 ～ fa48、gi1 ～ gi4
SF250-48HP	48 ポート 10/100 PoE スマートスイッチ	fa1 ～ fa48、gi1 ～ gi4
SG250-08	8 ポート ギガビット スマートスイッチ	gi1 ～ gi8
SG250-08HP	8 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi8
SG250-10P	10 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi10
SG250-18	18 ポートギガビットスマートスイッチ	gi1 ～ gi18
SG250-26	26 ポートギガビットスマートスイッチ	gi1 ～ gi26
SG250-26HP	26 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi26
SG250-26P	26 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi26
SG250-50	50 ポートギガビットスマートスイッチ	gi1 ～ gi50

モデル	説明	ポート
SG250-50HP	50 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi50
SG250-50HP	50 ポート ギガビット PoE スマート スイッチ	gi1 ～ gi50
SG250X-24	24 ポート ギガビット スマート スイッチ（10G アップリンク付き）	gi1 ～ gi24、te1 ～ te4
SG250X-24P	24 ポートギガビット PoE スマートスイッチ（10G アップリンク付き）	gi1 ～ gi24、te1 ～ te4
SG250X-48	48 ポート ギガビット スマート スイッチ（10G アップリンク付き）	gi1 ～ gi48、te1 ～ te4
SG250X-48P	48 ポートギガビット PoE スマートスイッチ（10G アップリンク付き）	gi1 ～ gi48、te1 ～ te4
SF350-08	8 ポート 10/100 マネージド スイッチ	fa1 ～ fa8
SF350-24	24 ポート 10/100 マネージド スイッチ	fa1 ～ fa24、gi1 ～ gi4
SF350-24MP	24 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa24、gi1 ～ gi4
SF350-24P	24 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa24、gi1 ～ gi4
SF350-48	48 ポート 10/100 マネージド スイッチ	fa1 ～ fa48、gi1 ～ gi4
SF350-48MP	48 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa48、gi1 ～ gi4
SF350-48P	48 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa48、gi1 ～ gi4
SF352-08	8 ポート 10/100 マネージド スイッチ	fa1 ～ fa8、gi1 ～ gi2

モデル	説明	ポート
SF352-08MP	8 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa8、gi1 ～ gi2
SF352-08P	8 ポート 10/100 PoE 対応マネージド スイッチ	fa1 ～ fa8、gi1 ～ gi2
SG350-10	10 ポート ギガビット マネージド スイッチ	gi1 ～ gi10
SG350-10P	10 ポート ギガビット PoE マネージド スイッチ	gi1 ～ gi10
SG350-10FP	10 ポート ギガビット PoE マネージド スイッチ	gi1 ～ gi10
SG350-20	20 ポート ギガビット マネージド スイッチ	gi1 ～ gi10
SG350-28	28 ポート ギガビット マネージド スイッチ	gi1 ～ gi28
SG350-28MP	28 ポート ギガビット PoE 対応マネージド スイッチ	gi1 ～ gi28
SG350-28P	28 ポート ギガビット PoE 対応マネージド スイッチ	gi1 ～ gi28
SG350-28SFP	28 ポート ギガビットマネージド SFP スイッチ	gi1 ～ gi28
SG350-52	52 ポート ギガビット PoE 対応マネージド スイッチ	gi1 ～ gi52
SG350-52MP	52 ポート ギガビット PoE 対応マネージド スイッチ	gi1 ～ gi52
SG350-52P	52 ポート ギガビット PoE 対応マネージド スイッチ	gi1 ～ gi52
SG350X-12PMV	12 ポート 5G PoE スタッカブル マネージド スイッチ	fi1 ～ fi12、xg1 ～ xg4
SG350X-24	24 ポート ギガビット スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG350X-24PV	24 ポート 5G PoE スタッカブル マネージド スイッチ	gi1 ～ gi8、gi13 ～ gi20、fi9 ～ fi12、fi21 ～ fi24、xg1 ～ xg4

モデル	説明	ポート
SG350X-24MP	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG350X-24P	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG350X-24PD	24 ポート 2.5G PoE スタッカブル マネージド スイッチ	gi1 ～ gi10、gi13 ～ gi22、tw11 ～ tw12、tw23 ～ tw24、te1 ～ te4
SG350X-48	48 ポート ギガビット スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SG350X-48MP	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SG350X-48P	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SG350X-48PV	48 ポート 5G PoE スタッカブル マネージド スイッチ	gi1 ～ gi20、gi25 ～ gi44、fi21 ～ fi24、fi45 ～ fi48、xg1 ～ xg4
SG350X-8PMD	8 ポート 2.5G PoE スタッカブル マネージド スイッチ	tw1 ～ tw8、te1 ～ te2
SX350X-08	8 ポート 10 GBase-T スタッカブル マネージド スイッチ	te1 ～ te8
SX350X-12	12 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te12
SX350X-24	24 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te24
SX350X-24F	24 ポート 10G SFP+ スタッカブル マネージド スイッチ	te1 ～ te24
SX350X-52	52 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te52
SG355-10P	10 ポート ギガビット PoE マネージド スイッチ	gi1 ～ gi10

モデル	説明	ポート
SF550X-24	24 ポート 10/100 スタッカブル マネージド スイッチ	fa1 ～ fa24、te1 ～ te4
SF550X-24MP	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	fa1 ～ fa24、te1 ～ te4
SF550X-24P	24 ポート 10/100 PoE スタッカブル マネージド スイッチ	fa1 ～ fa24、te1 ～ te4
SF550X-48	48 ポート 10/100 スタッカブル マネージド スイッチ	fa1 ～ fa48、te1 ～ te4
SF550X-48MP	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	fa1 ～ fa48、te1 ～ te4
SF550X-48P	48 ポート 10/100 PoE スタッカブル マネージド スイッチ	fa1 ～ fa48、te1 ～ te4
SG300-28	24 ポート ギガビット スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG550X-24MP	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG550X-24MMP	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG550X-24P	24 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi24、te1 ～ te4
SG300-28	48 ポート ギガビット スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SG550X-48MP	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SG550X-48P	48 ポート ギガビット PoE スタッカブル マネージド スイッチ	gi1 ～ gi48、te1 ～ te4
SX550X-12F	12 ポート 10G SFP+ スタッカブル マネージド スイッチ	te1 ～ te12

モデル	説明	ポート
SX550X-16FT	16 ポート 10 G スタッカブル マネージド スイッチ	te1 ～ te16
SX550X-24	24 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te24
SX550X-24F	24 ポート 10G SFP+ スタッカブル マネージド スイッチ	te1 ～ te24
SX550X-24FT	24 ポート 10G スタッカブル マネージド スイッチ	te1 ～ te24
SX550X-52	52 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te52
SG350XG-24F	24 ポート 10G SFP+ スタッカブル マネージド スイッチ	te1 ～ te24
SG350XG-24T	24 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te24
SG350XG-2F10	12 ポート 10G スタッカブル マネージド スイッチ	te1 ～ te12
SG350XG-48T	48 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te48
SG550XG-24F	24 ポート 10G SFP+ スタッカブル マネージド スイッチ	te1 ～ te24
SG550XG-24T	24 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te24
SG550XG-48T	48 ポート 10GBase-T スタッカブル マネージド スイッチ	te1 ～ te48
SG550XG-8F8T	16 ポート 10 G スタッカブル マネージド スイッチ	te1 ～ te16

新機能

リリース 2.5.5.47 には、次の更新が含まれています。

FindIT Probe の強化

- 以前のバージョンでは、ユーザーが使用できる唯一の設定は、FindIT Probe を有効または無効にすることでした。プローブが有効になっているスイッチには、プローブ機能用に別の Web ユーザーインターフェイスが備えられています。現在のバージョンには、スイッ

チのプローブがリモートの FindIT Manager に接続できるようにするための設定が追加されています。これらの設定には、Manager のアドレスと転送ポート、FindIT Organization とネットワーク名、Manager のキー ID と秘密が含まれます。

注 スイッチの FindIT Probe には、独自の Web ユーザーインターフェイスがなくなりました。すべての FindIT 管理は、FindIT Network Manager の Web ユーザーインターフェイスを使用して行う必要があります。

CA 証明書管理機能

- FindIT および PnP 機能では、FindIT または PnP サーバーとの HTTPS 通信を確立するために CA 証明書が必要です。CA 証明書管理機能により、これらのアプリケーションとデバイスマネージャは次のことを実行できます。
  - 信頼された CA 証明書をインストールし、不要になった証明書を削除する
  - デバイスの構成ファイルに証明書を静的に追加する
  - 信頼されていない証明書の失効リストを管理する証明書の有効期間は、システムクロックが基準になります。

注 証明書の有効期間は、システムクロックが基準になります。

DHCP オプション 43 に基づく PnP 用の SNTP サーバー

- 以前のバージョンでは、オプション 43 に基づく HTTPS 経由の PnP 接続は、システムクロックが DHCP オプション 43 で指定された SNTP サーバーによって同期されている場合にのみ成功していました。現在、このような PnP 接続は、システムクロックが SNTP サーバーによって同期されている場合、またはスイッチ管理者によって手動で設定されている場合に成功します。

ダウングレードについての注記

リリース 2.4.5.x 以降にリリースされたボードは、更新された PoE チップセット（6920xM バージョン 0x4a02）を使用します。この新しいチップセットバージョンに加えて、デバイスは以下をサポートします。

- PoE チップセット 6920xM バージョン 0x4b42（ソフトウェアバージョン 2.2.8.4 ～ 2.4.0.x を使用して製造されたボードで使用）
- PoE チップセット 6920x バージョン 0x4ac2（ソフトウェアバージョン 2.1.0.63 ～ 2.2.7.7 を使用して製造されたボードで使用）

PoEチップセットのバージョンは、show power inline コマンド出力の一部として表示されます。サポートされるチップセットバージョンが異なるため、次のダウングレードルールが適用されます。

- 非 PoE デバイス、および元の PoE チップセット（69208 0x4ac2）を使用する PoE デバイスは、以前のバージョンと同じダウングレードルールに従います。ダウングレードは、デバイスがサポートする最初のソフトウェアバージョンに基づいてサポートされます。
- PoE チップセット 0x4b42 をサポートする Sx250 デバイスの場合、ソフトウェアバージョン 2.2.7 以前へのダウングレードは阻止されます。
- チップセット 0x4a02 をサポートする SG250-10P、SG250-26HP/P、SF250-48HP デバイスの場合、ソフトウェアリリース 2.4 からのダウングレードは阻止されます。
- チップセット 0x4a02 をサポートする SF250-24P、SG250-08HP、SG250-50HP、SG250-50P、SG250X-24P、および SG250X-48P デバイスの場合、バージョン 2.3.5（上記のデバイスをサポートする最初のソフトウェアバージョン）にのみダウングレードできます。
- チップセット 0x4a02 または 0x4b42 をサポートする Sx350 または Sx550 PoE デバイスの場合、ソフトウェアバージョン 2.2.7 以前のダウングレードは阻止されます。

既知の問題

リリースバージョン 2.5.5.47 で確認された問題

不具合 ID	説明
CSCvu16265	**症状** 証明書チェーンを含む P12 証明書を FindIT 経由でインストールしようとすると、HTTP 経由の PnP が失敗する。 **回避策** 問題は次の FindIT マネージャドロップで修正されます。現在のバージョンの場合、FindIT にインストールされている自己署名証明書を使用するか、DHCP オプション 43 を使用して証明書バンドルをダウンロードします。
CSCvu16276	**症状** バックアップユニットへのスタックスイッチオーバーの後、システムが FindIT Manager に自動的に再接続しない。 **回避策** プローブを無効にしてから再度有効にするか、マネージャへの接続を無効にしてから再度有効にして、マネージャへの接続を再開します。またはスタックをリロードします。

不具合 ID	説明
CSCvp69075	**症状** タイムゾーン設定を変更する際に、構成ファイルのタイムスタンプが更新されない。 **回避策** この問題は、構成ファイルのコンテンツや動作に機能的な影響を与えるものではなく、次のバージョンで修正されます。
CSCvu16298	**症状** デバイスの再起動後、デバイスの LED が無効になっているのに、ポートの PoE LED がオフにならない。 **回避策** なし

解決済みの問題

リリースバージョン 2.5.5.47 で解決された問題

不具合 ID	説明
CSCvn74799	**症状** まれに、10G インターフェイスへの特定の NIC 接続により、数日おきにリンクフラップが発生することがある。このようなリンクパートナーとのネゴシエーションの調整を可能にするコマンドが追加されました。コマンドシンタックスは「ports negotiation tuning」です。こうしたリンクフラップが 10G インターフェイスで発生する状況でのみ、このコマンドを使用するようお勧めします。詳細については、CLI ガイドを参照してください。
CSCvo49699	**症状** LAG 内の特定のリンクがフラップすると、デバイスが再起動することがある（再起動メッセージ「PSET-FILLEGAL_IFINDEX:PSETG_add_port_to_set: Illegal ifIndex 0」）。
CSCvq71611	**症状** 一部の Avaya製 IP フォンによる LLDP アドバタイズメントにより、デバイスが再起動する場合がある（再起動メッセージ「Msg:%AUTOSMARTPORT-F- DEV_CALC_FAILED: XDP device type calculation failed: interface gi1/0/40 - capability 3」）。

不具合 ID	説明
CSCvp64740	**症状** HTTP または HTTPS タイムアウト時に、Web GUI によってユーザーがログインページに自動的にリダイレクトされない。自動リダイレクトは、HTTP または HTTPS タイムアウトの後にいずれかの Web ページを参照すると機能します。
CSCvr01301	**症状** スイッチが VLAN の PVST/RPVS+ BPDU の通過を停止し、結果として STP ループが発生する場合がある。
CSCvp40307	**症状** シスコ プラグアンドプレイ接続：IPv4 と IPv6 両方の DNS レコードを受信すると、サーバーの IPv4 アドレスの検出に失敗する。デフォルトの IPv6 ルートがないことを確認します。
CSCvp64778	**症状** トランクポートが VLAN のメンバーではない場合でも、ポートの RPVST ステータスは、この VLAN が現在もアクティブであることを示す。これは表示の問題であり、機能への実際の影響はありません。
CSCvs51601	**症状** http（s）セッションがタイムアウトした後、Web GUI がログインページに自動的に戻らない。任意の Web ページを参照すると、ログインページに戻ります。

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.0.90 リリースノート

2019 年 11 月

SF250、SG250、SF350、SG350/350X/350XG、SF550X、SG550X/550XG、SX350X、SX550X シリーズ スイッチ ソフトウェア バージョン 2.5.0.90 リリースノート

新機能

このセクションでは、リリース 2.5.0.92 の新機能と変更について詳しく説明します。

- ボードが複数のセンサーをサポートしている場合でも、show system コマンドの出力には、スタック内のユニットごとに 1 つのセンサーの温度が表示されるようになりました。この

出力には、最高温度を検出したセンサーからの情報が表示されます。以前のバージョンでは、このコマンドの出力には、スタック内の各ユニットの指定されたセンサーの温度が表示されていました。更新された機能により、スイッチの温度に関する潜在的な問題を検出する能力が向上します。すべてのセンサーの温度測定値を表示するには、show system sensor コマンドを使用します。このコマンドは、センサーの位置やアラートのしきい値など、各センサーに関するその他の詳細も表示します。

リリース 2.5.0.90 では、以下の解決済みセクション記載のバグが修正されています。

リリース 2.5.0.83 では、バグ CSCvo48821 および CSCvp12473 が修正されています。

リリース 2.5.0.82 では、バグ CSCvp95489 が修正されています。

リリース 2.5.0.79 には、次の更新が含まれています。

- mGig 5G インターフェイスのサポート：このリリースには、マルチギガビット（mGig）RJ45 銅製ポートを含む SG350X12PMV、SG350X-24PV、および SG350X-48PV スイッチモデルのサポートが追加されています。これらのスイッチにより、100M/1G/2.5/5Gbps の速度をサポートする 5G インターフェイスのサポートが追加されます。mGig ポートのネゴシエーションは 2.5G/5Gbase-T IEEE 802.3bz-2016 に基づいており、NBASE-T 最終仕様（バージョン 2.3）に完全に準拠しています。mGig ポートの位置は、スイッチモデルによって異なります。以前のバージョンと同様に、mGig をサポートするインターフェイスは、その最大ポート速度にちなんで名付けられました。5G の最大速度をサポートするインターフェイスは、「FiveGigabitEthernet1/0/1」または略して「fi 1/0/1」と呼ばれます。以前のリリースの 2.5G インターフェイスと同様に、5G インターフェイスの番号付けは 1G インターフェイスから連続して行われます。たとえば、5G ポートが 7 番目と 8 番目のポートに物理的に配置されている場合、「tw 1/0/7」および「tw1/0/8」という名前が付けられます。
- 強化されたセキュリティ：デバイス管理のセキュリティを強化するために、このリリースでは次の機能が導入されています。
  - デフォルトのユーザー名 cisco とデフォルトのパスワード cisco でログインしてデバイスへの初期接続を完了すると、システムはユーザー名とパスワードを変更するように要求します。以前のリリースでは、変更するよう求められるのはパスワードのみで、パスワード変更プロセスのスキップを選択することが可能でした。
  - 注：以前のリリースのスタートアップ コンフィギュレーションにレベル 15 のログイン情報が含まれていない場合、以前のリリースからこのリリースにアップグレードするときに、デフォルトのログイン情報の置き換えも適用されます。
  - パスワードの複雑度を無効にすると、ログイン情報としてユーザー名 cisco とパスワード cisco を設定することができるようになります。これらのログイン情報をスタートアップ時に保存した場合、ログイン情報の変更を求めるプロンプトは表示されません。
  - ログイン情報 cisco/cisco は、デバイス構成ファイルに記載されます。以前のリリースでは、デフォルトログイン情報 cisco/cisco は構成ファイルに記載されませんでした。
  - 最後の権限レベル 15 のデフォルトのユーザー名とパスワードを消去または削除することはできません。この機能により、デフォルトログイン情報 cisco/cisco に（おそら

く意図せずに）戻すことを防ぐことができます。以前のリリースでは、最後のレベル15ユーザーを削除することができました。削除すると、ログイン情報cisco/ciscoがアクティブになりました。

- デバイス設定を削除するか、デバイスを再起動して工場出荷時のデフォルトに戻すと、デフォルトのログイン情報が復元されます。この場合、ログイン情報を再度変更する必要があります。

- ランタイムディフェンス機能には、システムをハッキングから保護するオペレーティングシステム、コンパイラ、およびプロセッサ機能が含まれます。このデバイスは、次の関連機能をサポートしています。
  - X-SPACE：コードがデータセグメントなどの不正なメモリ領域にある場合、コードの実行を防ぐことにより、許可されていないアプリケーションの実行を防止します。
  - ASLR：オペレーティングシステム（Linux）がアプリケーションとプロセスの実行に使用するアドレスをランダム化します。プロセスが実行されるたびに、オペレーティングシステムは異なるアドレスをプロセスに使用するため、ハッカーが自分のコードの実行権限を得ることが難しくなります。
  - BOSC：バッファオーバーフロー（メモリが不足しているメモリへのアクセスを試行するコード）からの保護を追加します。

- 次の PnP 機能のサポートが、既存の PnP エージェントの動作に追加されました。
  - このバージョンは、シスコプラグアンドプレイ接続をサポートしています。この接続方式により、HTTPS 経由で実行される完全に設定済みの PnP サーバー検出が可能です。スイッチは、FQDN「devicehelper.cisco.com」を使用してリダイレクションサービスに接続し、そこから PnP サーバー情報を取得します。
  - DHCPおよびシスコプラグアンドプレイ接続方式を使用した第1選択としての証明書処理（SSL クライアント）/HTTPS。
  - イメージと構成ファイルのダウンロードは、PnPサーバーによって追加され、スイッチによって検証される MD5 チェックサムによって保護されます。

- PnPエージェントとDHCP自動設定機能およびイメージ機能を同時に有効にできるようになり、両方の機能がデフォルトで有効になっています。スイッチがPnPエージェント関連オプション（オプション43）およびDHCP自動更新関連オプション（オプション57または125）を含むDHCP応答を受信した場合、スイッチはPnPエージェントオプション情報を無視します。

- デフォルトでは、VLANマッピング トンネリング エッジ ポートは、次の宛先MACアドレスを持つ入力L2 PDUをドロップします。
  - 01:80:C2:00:00:00-01:80:C2:00:00:FF
  - 01:00:0C:00:00:00-01:00:0C:FF:FF:FF
  - 01:00:0C:CD:CD:D0

以前のバージョンでは、これらの宛先 MAC アドレスを持つフレームを転送できませんでした。このバージョンでは、特定のポートを定義して、CDP、LLDP、STP、または VPT のいずれかのプロトコルで PDU を転送できます（PDU を転送する前に、PDU の VLAN タグを指定する必要があります）。この機能により、プロバイダーネットワーク経由で前述のようなタグなしフレームを転送できます。このようなパケットに特定のCoS値を割り当て、しきい値レートを設定することも可能です。

- STP、RSTP、MSTP に加えて、デバイスは PVST+ と RPVST+ をサポートします。PVST+ および /RPVST+ は、VLAN ごとに 802.1Q STP の個別のインスタンスで実行されます。Rapid PVST は、VLAN ごとに 802.1Q RSTP の個別のインスタンスで実行されるプロトコルです。デバイスは、最大 126 の PVST/RPVST インスタンスをサポートします。
- トランクポート VLAN メンバーシップのコマンドラインシンタックスが強化され、追加および削除に加えて、許可された VLAN リストを指定するオプションがサポートされるようになりました。構成ファイルも強化され、削除された VLAN リストの代わりに許可された VLAN リストが表示されるようになりました。設定は、アップグレード時またはダウングレード時に自動的に移行されます。

既知の問題

リリースバージョン 2.5.0.92 で確認された問題

不具合 ID	説明
CSCvq63060	**症状** セキュアなSSHファイルの（スイッチからSSH/SCPサーバーへの）コピーが、SSH接続（スイッチはSSHサーバー）でサポートされない。 **回避策** コンソール、Telnet、またはWeb接続を使用して、スイッチからSCPサーバーへのセキュアなSSHファイルのコピーを実行します。
CSCvs51601	**症状** http（s）セッションがタイムアウトした後、Web GUIがログインページに自動的に戻らない。 **回避策** 別のWebページを参照するか、既存のページで[Edit]または[Apply]などのコントロールを選択するか、ブラウザのメニューバーにデバイスのURLを再入力すると、ログインページにリダイレクトされます。

リリースバージョン 2.5.0.92 で確認された問題

不具合 ID	説明
CSCvr54104	**症状** 接続されたルータがゲートウェイアドレスのスイッチ ICMP リダイレクトメッセージを送信すると、FindiT Probe GUI がサブネットで機能しないことがある。この問題は、RV325 ルータの接続時に発生しました。 **回避策** ICMP リダイレクトメッセージをデバイスに送信しないようにルータを設定します。ネットワークでリダイレクトメッセージが必要な場合は、デバイスのインターフェイスで ACL を使用してリダイレクトメッセージをブロックします。

リリースバージョン 2.5.0.79 で確認された問題

不具合 ID	説明
CSCvp64751	**症状** マスターユニットとバックアップユニットを含むスタックをバージョン2.2.5（またはそれ以前）にダウングレードした後に、バージョン 2.5 にアップグレードすることができない。 **回避策** オプション1（ダウングレードを開始する前に使用）：バージョン 2.5 のスタートアップ コンフィギュレーションを削除してから、バージョン 2.2.5 にダウングレードします。 オプション2（ダウングレードがすでに実行されているものの、2.5 へのアップグレードはまだ実行されていない場合に使用）：ダウングレード後、バックアップユニットを切断してから、バックアップユニットのスタートアップ コンフィギュレーションを削除します。マスターユニットとバックアップユニットを再起動し、バックアップユニットをマスターユニットに再接続します。
CSCvp64768	**症状** PVST/RPVST が有効になっているときに、トリガーされるべきではないループバック検出がトリガーされる。 **回避策** PVST/RPVST によるループバック検出を有効にしないでください。

不具合 ID	説明
CSCvp64778	**症状** トランクポートが VLAN のメンバーではない場合でも、ポートの RPVST ステータスは、この VLAN がアクティブであることを示す。 **回避策** 表示の問題であり、機能への実際の影響はありません。

リリースバージョン 2.5.0.78 で確認された問題

不具合 ID	説明
CSCvp40302	**症状** PVST/RPVST が有効になっているときに、トリガーされるべきではないループバック検出がトリガーされる。 **回避策** PVST/RPVST によるループバック検出を有効にしないでください。
CSCvp40307	**症状** シスコ プラグアンドプレイ接続：IPv4 と IPv6 両方の DNS レコードを受信すると、サーバーの IPv4 アドレスの検出に失敗する。 **回避策** DNS サーバーで IPv4 レコードのみを設定します。
CSCvp40311	**症状** cable-diagnostics tdr を実行すると、10G ポートにいつも「short cable」と表示される。 **回避策** なし。
CSCvp40317	**症状** 特定の NIC（PD デバイスではない）に接続された PSE ポートに「Short」状態のステータスが表示される。 **回避策** なし。

リリースバージョン 2.5.0.71 で確認された問題

不具合 ID	説明
CSCvn31532	**症状** FindIT Network Probe を使用していくつかのデバイスで同時にイメージをアップグレードすると、イメージのアップグレードに失敗する場合がある。 **回避策** 各スイッチでのダウンロードが終了したことを確認してから、次のスイッチをアップグレードしてください。
CSCvn31587	**症状** デバイスでHTTPSが無効になっていると、ログインページからFindIT Network Probe アプリケーションに接続できない。 FindIT Network Probe が有効になっているスイッチに関連した問題です。ログインページから通常の [Switch Management] にアクセスし、ページの上部にある [FindIT] リンクをクリックすることで、引き続きプローブに接続できます。 **回避策** HTTPS をイネーブルにします。 （注） このバグは、ソフトウェアバージョン 2.5.0.92 で解決されました。
CSCvn31596	**症状** FindIT Network Manager が、HTTPS が無効になっているスイッチとの相互起動に失敗する。 **回避策** HTTPS をイネーブルにします。
CSCvn31554	**症状** デバイスの IP アドレスを DHCP から静的 IP アドレスに変更したときに、スイッチによって送信されるBonjourブロードキャストに古いIPアドレス情報が含まれる場合がある。FindIT Network Probe では、短いネットマスク（20 ビット未満）を含む新しいデバイス IP アドレスは更新されません。 **回避策** IP アドレスを変更したデバイスを再起動します。

リリースバージョン 2.4.0.94 および 2.4.0.91 で確認された問題

不具合 ID	説明
CSCvj32368	**症状** show green-ethernet コマンドの使用中に、ショートリーチ設定の結果としての [Power Savings] の % が正確に表示されない。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.5.0.92 で解決されました。
CSCvj32379	**症状** 一部の SKU で、show fan system CLI コマンドを発行すると、ファンの RPM（分あたり回転数）が「0」と表示される。ファンの機能への影響はありません。 **回避策** なし
CSCvj32418	**症状** まれなシナリオ（特定の IPv6 ルートを 700 追加する場合）で、リソーステーブルがいっぱいでない場合でも、ハードウェアルーティングが無効になる。 **回避策** IPv6 ルートを減らすか、別の IPv6 ルートを設定します。問題が解決しない場合は、必要のないいくつかのルートを減らし、ハードウェアベースのルーティングを再度アクティブにします。
CSCvj32432	**症状** ハイブリッドスタックモードの Sx550x が、2,000 のレイヤ 2 マルチキャストエントリをサポートしている（4,000 をサポートする必要がある）。 **回避策** 可能であればネイティブモードを使用します。 （注） このバグは、ソフトウェアバージョン 2.4.5.71 で解決されました。

不具合 ID	説明
CSCvj32442	**症状** show inventory コマンドにより、MFEFX1、MFELX1、MFEBX1、MFEBBX1、MFEBSX1、MFELH1、MFELX1、MGBT1 の各 SFP の誤った形式の PID と vid＝“information not available” という誤った情報が表示される。この問題は表示に影響しますが、機能への影響はありません。 **回避策** なし。
CSCvj32448	**症状** ：一部の SFP ポートに SFP MGBLX1 と 40km 光ファイバケーブルを接続すると、ファイバリンクがフラップする場合がある。リンクフラップ防止機能により、最終的にリンクがダウンすることがある。 **回避策** なし。
CSCvj32452	**症状** 2.4.0.x では、TCP または UDP ポート範囲オプションが IPv6 ACL でサポートされていないため、ACE 設定で特定のポートを使用する必要がある。 **回避策** 2.4.0.x にアップグレードすると、範囲設定を含む ACE が ACL から削除されるため、IPv6 ACL の特定のポートを再設定する必要があります。

リリースバージョン 2.3.5.63 で確認された問題

不具合 ID	説明
CSCvf88706	**症状** 追加のユニットを 3 ユニットの既存のスタックに接続したときに、ユニット 1 の PoE 情報が CLI または GUI に表示されない。 **回避策** スタックを再起動します。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。

不具合 ID	説明
CSCvf88738	**症状** 特定の ACL に「disable-port」オプション付きの拒否 ACE が含まれている場合、トラフィック下のポートからその ACL をバインド解除すると、ポートが一時停止（シャットダウン）する。 **回避策** ポートを shutdown にした後、no shutdown にして回復します。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCvf88746	**症状** スイッチを新しいファームウェアバージョンにアップグレードした後、スイッチを再起動すると、スイッチへの SNA 接続が切断される。 **回避策** ブラウザを更新してスイッチに再接続します。
CSCvf88761	**症状** IPv6 ルーティングを有効にしてから IPv6 6to4 トンネルを設定すると、トンネルステータスが「not present」になる。 **回避策** IPv6 ルーティングを一旦無効にした後に有効にするか、トンネルを設定してから IPv6 ルーティングを有効にします。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCvf88777	**症状** あるスイッチ（SSH クライアント）から別のスイッチ（SSH サーバー）に接続すると、SSH 接続が遅くなる。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。

不具合 ID	説明
CSCvf88810	**症状** 非コンボ SFP ポートが 100M SFP モジュールをサポートしない。 **回避策** なし。

リリースバージョン 2.3.0.130 で確認された問題

CSCve55065	**症状** 6to4 トンネルトラフィックは、トンネル発信ポートがトランクポートであるか、general タグ付きの場合、ラインレートで転送されない。 **回避策** トンネルの発信ポートをアクセスポートまたはノースイッチポートとして設定します。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCve55069	**症状** ：Apple Safari ブラウザを使用している場合、Web GUI の一部の機能（再起動ボタン、ログアウト、[Locate Device] の [Stop] ボタン）が応答しない。 **回避策** Google Chrome、Mozilla Firefox、または Microsoft Edge ブラウザを使用します。
CSCve55070	**症状** PoE ポートが PD ではないネイバーに接続されている場合、無効な署名カウンタの数字が増え続ける。 **回避策** この動作は、PD 以外のデバイスがポートに接続されている場合の検出プロセスによる想定内の動作です。

CSCve55072	**症状** PoE 操作の時間範囲を定義したときに、時間範囲にアクティブ時間として00:00を含めなかった場合、表示期間中に消費があったとしても、時間、日、および週の PoE 消費値が 0 と表示される（分には正しい値が表示される）。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCve55074	**症状** スタック内のユニットのユニット ID 設定がセット ID から自動ユニットIDに変更された場合、リロード後にデバイスがスタックに参加しないことがある。 **回避策** すでにスタック内にあるユニットのユニットID設定を変更しないでください。問題が発生した場合は、動作しなくなったユニットを電源から切断して再接続し、スタックに再度追加します。 （注） このバグは、ソフトウェアバージョン 2.3.5.63 で解決されました。
CSCve55078	**症状** XGデバイスのアップリンクインターフェイスでの出力トラフィックシェーピングによって、（80 Kbpsよりも低いレートを設定した場合でも）トラフィックが 80 Kbps に制限される。 **回避策** 80 Kbps よりも高い出力シェーピング値を使用します。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCve55081/CSCve55217	**症状** 一部のデバイスおよび特定のポートでは、ケーブルが接続されていない場合やケーブルの長さが非常に短い場合に、「test cable-diagnostics tdr」コマンドを使用してケーブルテストを実行すると、予期しない結果になることがある。 **回避策** なし。

CSCve55082	**症状** Cisco 28/29xx ターミナルサーバーがスレーブユニットに接続されており、回線で「exec」が設定されている場合、（マスターから）rebootコマンドを発行すると、スレーブユニットの再起動が一時停止することがある。 **回避策** この問題を防止するには、スタックを再起動する前に、ターミナルサーバーの回線で「no exec」を設定します。
CSCve55087	**症状** バックアップからマスターにユニットを切り替えた後、USB インターフェイスが、挿入されたフラッシュスティック（ディスクオンキー）を認識しない。 **回避策** ユニットをリロードします。 （注） このバグは、ソフトウェアバージョン 2.3.5.63 で解決されました。
CSCve55090	**症状** SNA：複数のインターフェイスのデュプレックスと速度設定を同時に設定する場合、更新された設定を表示するには Web ページを更新する必要がある。 **回避策** Web ページを更新します。
CSCve55094	**症状** キュー統計：統計は出力の統計だが、パケットサイズは入力のパケットサイズに基づいて計算される。 **回避策** なし。
CSCve55102	**症状** PoE：まれに、PD に接続されたポートの電圧表示が実際の電圧よりも低くなる。 **回避策** なし。

CSCve55112	**症状** 構成の移行：Sx200/Sx300/Sx500 PoE デバイスから Sx250/Sx350/Sx550 非 PoE デバイスに構成ファイルを変換する際、「ldp med enable network-policy poepse inventory」 コマンドに PoE パラメータが含められ、接続先デバイスへのファイルのロードに失敗する。 **回避策** PoE 関連の項目を手動で削除します。
CSCve55117	**症状** 構成移行ツール：サイズの大きなファイル（10,000 行以上）を変換すると、ブラウザの応答が遅くなったり、クラッシュしたりすることがある。 **回避策** なし。
CSCve55188	**症状** 夜間などに SNA を長時間開いたままにすると、RAM を正常に解放しないため、RAM 不足が原因で Web ブラウザがハングアップすることがある。 **回避策** なし。
CSCve55203	**症状** SNA：ファームウェアをアップグレードする複数のデバイスを選択し、ダウンロード後にデバイスを再起動するオプションを選択すると、すべてのデバイスで操作が完了する前に、成功を示すメッセージが表示される。 **回避策** なし。
CSCve55206	**症状** 48 ポート未満の XG デバイスでは、「show queue statistics」 コマンドによるキュー統計に、パケット数とバイト数に関する間違った情報が表示される場合がある。 **回避策** なし。

CSCve60999	**症状** （元のマスターからバックアップへの）マスタースイッチオーバーの後、またはユニットが切断されてからスタックに再接続されたときに、ユニットがスタックに再参加しないことがある。 **回避策** 動作しなくなったユニットを電源から切断して再接続し、スタックに再度追加します。 （注） このバグは、ソフトウェアバージョン 2.3.5.63 で解決されました。

リリースバージョン 2.2.8.04 で確認された問題

不具合 ID	説明
CSCvc73697	**症状** 学習済みの音声 VLAN が 1024 を超えると、既存の VLAN がフラッシュされる。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン2.3.0.130で解決されました。

リリースバージョン 2.2.5.68 で確認された問題

不具合 ID	説明
CSCva97565	**症状** CLI ガイドのシステム管理の章にコマンド「delete sna storage file-name」が記載されていない。このコマンドを使用すると、特定のユーザー（「file-name」パラメータで指定）用に保存された SNA 設定を削除できます。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.5.68 で解決されました。

不具合 ID	説明
CSCva97578	**症状** SNA：まれに、SNA の表示を何時間も操作しないと、SNA のトポロジー表示が同期されなくなる。 **回避策** SNA の表示を更新します。
CSCva97583	**症状** SNA：デバイスで 802.1x/RADIUS 設定が（CLI または Web を介して）事前設定済みである場合、DAC を使用した表示/設定に失敗することがある。 **回避策** DAC 機能を使用する前に、すべての手動による DAC 関連設定（802.1x/RADIUS）をデバイスから削除します。 （注） このバグは、ソフトウェアバージョン 2.3.0.130 で解決されました。
CSCva97586	**症状** RSPAN：ミラーリング操作ともう一つの操作（通常の転送など）によってトラフィックが宛先ポートに同時に転送されるときに、RSPAN 宛先ポートにミラーリングされないトラフィックがある。 **回避策** なし。
CSCva97588	**症状** SNA：Win10 Edge を使用して IPv6 アドレスでデバイスにログインすると、ネットワークトポロジを表示できない。 **回避策** IPv4 アドレスまたは他のブラウザを使用して接続します。 （注） このバグは、ソフトウェアバージョン 2.3.0.130 で解決されました。

不具合 ID	説明
CSCva97591	**症状** SNA：デバイス間で時間が異なる場合、異なるクロック時間のデバイス用に選択されたインターフェイスを使用して「Connection Explorer」で統計を選択すると、誤ったグラフが表示される。 **回避策** すべてのデバイスに（SNTP などにより）同期されたクロックがあることを確認します。
CSCva97601	**症状** SNA デバイスからバージョン V2.1 以前のデバイスにファームウェアと構成ファイルをアップグレードできない。 **回避策** 2.2 よりも前のバージョンへのファームウェアのダウンロードはサポートされていません。
CSCva97603	**症状** ：VLAN の最後の物理インターフェイスが L3 モードに設定された後に L2 モードに再度設定された場合、VLAN ステータスがダウンのままになる。 **回避策** 物理インターフェイスで shutdown/no shutdown を実行します。 （注） このバグは、ソフトウェアバージョン 2.4.0.91 で解決されました。
CSCva97605	**症状** XMODEM を使用して、バージョン 2.2.0.x を実行しているボードをバージョン 2.2.5.x にアップグレードできない。 **回避策** バージョン 2.2.0.x からバージョン 2.2.5.x へのアップグレードには TFTP を使用します。

リリースバージョン 2.2.0.63 で確認された問題

不具合 ID	説明
CSCuy97777	**症状** リロード後、ポートチャネルの実際のスパニングツリーコストが実行コンフィギュレーションと異なる。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCuy97791	**症状** STP コストパスが等しい場合、優先順位の値が高かったとしても、ポートチャネルが常にルートポートとして選択される。 **回避策** STP は引き続き適切に機能し、ループは形成されません。必要に応じて、コスト設定を使用してルートポートを変更します。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCuy97837	**症状** ダッシュボードで、適切なポートのインターフェイスカウンタと rmon 統計がクリアされていても、ポートの rx トラフィックエラーが赤色で表示される。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCuz01765	**症状** Cisco IP Phone 7960 の一部のリビジョンで、スイッチ 60W ポートの電源を入れることができない。 **回避策** この問題は、電話機のピン間のショートが原因で発生します。電話機を AF/AT ポートに接続するか、CAT 3 ケーブル（2 ペア）を使用して電話機を 60W ポートに接続します。

不具合 ID	説明
CSCuy97915	**症状** GUI を使用して、XG ポートの設定を「disable negotiation」に変更しながら、同時に速度を設定することができない。 **回避策** ネゴシエーションを無効にして [Apply] をクリックしてから、その後に速度を変更して [Apply] をクリックします。
CSCuy97943	**症状** スタックユニットタイプが固定から自動に変更されると、マスターユニットがリロードされる場合がある。 **回避策** スタックユニットが2回リロードされた場合にのみ発生します。マスターのリロード後にスタックが安定します。 （注） このバグは、ソフトウェアバージョン2.2.5で解決されました。
CSCuy97946	**症状** 宛先がトンネルインターフェイスに設定されていると、DHCPv6リレーが機能しない。 **回避策** IPv6グローバル宛先アドレスをDHCPv6宛先として使用します。
CSCuy97999	**症状** Web ベース認証とデバイス DHCP サーバーを使用しているときに、ステーションが認証されない。 **回避策** リースが完全に期限切れになった後、IP アドレスが期限切れになるまで待ちます。

不具合 ID	説明
CSCuz45730	**症状** 60W PoE と Cisco PD スイッチのネゴシエート中、Cisco PoE-PSE スイッチが 60W を供給できず、30W のみを供給する場合がある。 **回避策** PSE スイッチが起動する前に、PD スイッチを PSE スイッチに接続します。または、問題が発生したときに PD スイッチを切断してから再接続します。または、静的 60W を使用します。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。

リリースバージョン 2.1.0 で確認された問題

不具合 ID	説明
CSCux77649	**症状** スイッチを Cisco Catalyst コンパクト UPOE PD デバイスに接続すると、LLDP が AT/AF ポートの電源とネゴシエートしない場合がある。 **回避策** CDP を使用してネゴシエートします。 （注） このバグは、ソフトウェアバージョン 2.2.0 で解決されました。
CSCux77651	**症状** 入力インターフェイスにポリサーを適用し、複数の優先順位を持つトラフィックを送信すると、低速の出力ポートで優先順位の高いトラフィックがドロップされる場合がある。 **回避策** なし。

不具合 ID	説明
CSCux77654	**症状** ACE にパラメータとして TCP/UDP ポート範囲が含まれている場合、出力 ACL をインターフェイスに適用できない。 **回避策** 関連するインターフェイスで、必要な TCP/UDP ポートを ACL の個々のポートとして適用するか、入力 ACL として一定の範囲を適用します。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCux77675	**症状** 集約ポリサーの QoS 統計で、プロファイル内およびプロファイル外の両方のカウンタが常に 0 の値を表示する。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCux89410	**症状** メンバーシップタイプが GUI を介して禁止に設定されている場合、PVID がインターフェイスで有効にならない。インターフェイス機能は影響を受けません。ポートは、関連する VLAN のトラフィックを引き続きブロックします。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.0 で解決されました。
CSCux89413	**症状** Auto SmartMacro：インターフェイスに接続されているデバイスを電話/デスクトップからスイッチに置き換えた後、インターフェイスが BPDU guard erri-disable の状態に設定されることがある。 **回避策** インターフェイスの持続的な設定を無効にします。または、問題が発生した後に、インターフェイスからデスクトップ/電話機のマクロを削除し、ポートを再度アクティブにしてから、スイッチをインターフェイスに接続します。

不具合 ID	説明
CSCux89418	**症状** PD としての Sx350P を PSE としての Sx300P/Sx500P に接続した場合、AC 電源を切断すると Sx350P が再起動する。再起動後は、Sx350P の電源が入り、想定どおりに機能します。 **回避策** なし。
CSCux89582	**症状** 銅製 SFP（MGBT1/GLC-T SFP）をケーブルなしで接続すると、インターフェイスが一時停止（ダウン）する。この問題は、Sx350/Sx250 のアップリンク GE ポート（gi3 や gi4 など）または XG ネットワークポートに挿入するときに発生します。 **回避策** インターフェイスの停止を防ぐため、SFP をポートに挿入する前にケーブルを SFP に挿入します。ポートがすでに一時停止状態になっている場合、ケーブルを SFP に挿入してから一時停止状態のポートをアクティブにすると、ポートはアップ状態に移行します。 （注） このバグは、ソフトウェアバージョン 2.5.0.90 で解決されました。
CSCux89585	**症状** ポートで CDP と LLDP の両方が有効になっている場合、いずれかを無効にすると、残っている方のプロトコル PoE ネゴシエーションに失敗することがある。 **回避策** CDP と LLDP の両方の電力ネゴシエーションを同時に有効にしないでください。問題が発生した場合は、ケーブルを取り外してから PD に再接続します。 （注） このバグは、ソフトウェアバージョン 2.3.0.130 で解決されました。
CSCux89597	**症状** ポート制限モードで、全タイプのポート（AF、AT、および60W PoE）のデフォルト管理電力制限値が 30W になる。 **回避策** 必要に応じて、60Wの制限を手動で設定します。

不具合 ID	説明
CSCux89611	**症状** LLDP を介した 60W PoE の電力ネゴシエーションが完了するまでに最大 1 分かかる場合がある。 **回避策** なし。
CSCux89626	**症状** 60W PD をスイッチに接続すると、スイッチの電力表示が 60W を超える場合がある。このバグは表示の問題です。実際の PD 消費電力は 60W です。 **回避策** なし。

リリースバージョン 2.0.0 で確認された問題

不具合 ID	説明
CSCuq03628	**症状** トンネルインターフェイスが一旦無効になってから再度有効になったときにのみ、ISATAP クライアントが RS パケットを送信する。 **回避策** トンネルのエンドポイントが両方とも SG350XG/SG550XG である限り、トンネルは機能します。混合デバイスアプリケーションでは、トンネルインターフェイスを手動で無効にしてから有効にします。
CSCur86883	**症状** Web ベースの設定インターフェイスを使用してキューのスケジューリングを設定する場合、システムに 4 つ以上のユニットのスタックが含まれていると、応答時間が長くなることがある。 **回避策** 約 1 分後に、Web ベースの設定インターフェイスが再び応答するようになり、設定が有効になります。応答時間を短縮するには、コマンド ライン インターフェイス（CLI）コマンドを使用します。

不具合 ID	説明
CSCuu60952	**症状** 設定インターフェイスを使用してACEアクションを（たとえば拒否からシャットダウンに）変更すると、ACEがACLから削除される場合がある。 **回避策** ACE を再設定するか、CLI を使用して ACE を削除してから新しいアクションで設定します。
CSCuu60958	**症状** Web ベースの設定インターフェイスを使用して MAC ACE を設定すると、新しいACEの作成が失敗し、存在しないにもかかわらず、「Entry Already Exists」というエラーメッセージが表示されることがある。 **回避策** ACE を再度設定すると受け入れられます。または CLI を使用して ACE を設定します。
CSCuu60983	**症状** デバイスでVRRPが有効になっている場合、オプション82を使用したDCHPリレーに失敗する。 **回避策** デバイスでVRRPが有効になっている場合は、オプション82を有効にせずにDHCPリレーを使用します。
CSCuu60986	**症状** ユーザーインターフェイスを使用してLAGでフロー制御を有効にすると、リンクがアップになってもポートLEDが点灯しない。 **回避策** このバグはLED表示の問題です。機能は想定どおりに動作します。必要に応じて、コマンドラインインターフェイスを使用してフロー制御を有効にします。 （注） このバグは、ソフトウェアバージョン2.2.0で解決されました。

不具合 ID	説明
CSCuu60989 CSCuu61046	**症状** ポートが VLAN の静的メンバーであり、スイッチポートモード（非アクティブモードを含む）である場合、ポートで 802.1X ゲスト VLAN または音声 VLAN を有効にすることが禁止される。 **回避策** スイッチポートモードを使用するポート VLAN メンバーシップを変更して、ポートが目的の VLAN の静的メンバーにならないようにします。 （注） スイッチポートモードが [Trunk] の場合、ポートはデフォルトですべての VLAN のメンバーになります。802.1X ゲスト VLAN または音声 VLAN を設定する前に、目的の VLAN またはすべての VLAN のメンバーシップを削除します。 このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCuu61008	**症状** 承諾済みの自動音声 VLAN は、その音声 VLAN が無効になった後でも、プライマリ VLAN として定義できない。 **回避策** なし。
CSCuu61061	**症状** ポートでショートリーチが有効になっていると、Cat6a ケーブルを使用したケーブル長テストに失敗する。 **回避策** インターフェイスでケーブル長テストを実行するときは、ショートリーチを無効にします。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。

不具合 ID	説明
CSCuu61080	**症状** DHCP ルーターオプション（オプション 3）が、このプールにオプションが設定されていない場合でも、スイッチ DHCP サーバーによって送信される。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.0 で解決されました。
CSCuu61084	**症状** [IPv6 Routes] に常時「0」の計測値が表示される。 **回避策** なし。 （注） このバグは、ソフトウェアバージョン 2.2.5 で解決されました。
CSCuu61088	**症状** show qos interface コマンドにより、存在しないインターフェイスの情報が表示される。 **回避策** このバグは表示のみの問題です。
CSCuu61100	**症状** デバイスインターフェイスが管理上シャットダウンされている場合でも、リンクパートナーはリンクがアップであることを示す。 **回避策** このバグは表示の問題です。リンクは実際にはダウンしており、トラフィックは転送されません。
CSCuu61125	**症状** VLAN 1 の show VLAN コマンドにより、存在しないインターフェイス（ポートおよびスタックユニット）が表示される。 **回避策** このバグは表示のみの問題です。

不具合 ID	説明
CSCuu65516	**症状** ：（ネットワークの問題などにより）言語ファイルのダウンロードに失敗した場合、インターネットブラウザに「incomplete/error information」が表示されることがある。 **回避策** ブラウザクッキーを削除して、もう一度お試しください。デバイスは、Telnet を使用して引き続き管理できます。
CSCuu65557	**症状** 管理セッションがデバイスの IPv6 アドレスを使用するセキュアセッション（HTTPS）である場合、Safari ブラウザを使用してデバイスを管理できない。 **回避策** 別のブラウザ（Internet Explorer など）を使用するか、非セキュアセッション（HTTP）をセットアップします。
CSCuu65577	**症状** Web ベースの設定インターフェイスを使用して RIP の新しいキーチェーンを設定する場合は、accept-lifetime を含めます。accept-lifetime を含めないと、設定は有効になりません。 **回避策** CLI を使用してキーチェーンを入力するか、ユーザーインターフェイスで accept-lifetime と send-lifetime の両方を入力します。
CSCuu65593	**症状** 光ファイバー専用ポートではネゴシエーションは常に有効だが、show コマンドによりネゴシエーションが無効と表示される。リンクパートナーのネゴシエーションが無効になっている場合、リンクが起動しないことがある。 **回避策** リンクパートナーのネゴシエーションが有効になっていることを確認します。
CSCuu65595	**症状** IPv6 インターフェイスの MLD スヌーピングモードが、モードを (S, G) に設定しても、常に (*, G) になる。 **回避策** なし。

解決済みの問題

リリースバージョン 2.5.0.92 で解決された問題

不具合 ID	説明
CSCvr54104	**症状** Cisco Small Business スイッチに関する情報漏えいの脆弱性
CSCvo48821	**症状** 特定の OID に対する SNMP Get により例外が発生する。
CSCvp12473	**症状** SG550XG と SG250X 間の 10G リンクでの断続的な接続。

リリースバージョン 2.5.0.90 で解決された問題

不具合 ID	説明
CSCux89582 S	**症状** 銅製 SFP（MGBT1/GLC-T SFP）をケーブルなしで接続すると、インターフェイスが一時停止（ダウン）する。この問題は、Sx350/Sx250 のアップリンク GE ポート（gi3 や gi4 など）または XG ネットワークポートに挿入するときに発生します。
CSCvo26128	**症状** IPv6 DHCP リレーエントリをクリアすると、デバイスが再起動することがある。
CSCvo48776	**症状** ケーブルなしで MGBT1 SFP を使用すると、リンクフラッピングによってポートが中断される。この問題は、制限付きで部分的に修正されました。RPS が SG550XG シリーズに接続されている場合、リンクは引き続き中断されます。こうした状況では、SFP を必ずケーブルとともに挿入してください。
CSCvp64736	**症状** トラフィックの異常や持続的なリンクフラッピングによる UDLD の動作が原因で、スタック内のスレーブユニットがリロードされる場合がある。
CSCvq51790	**症状** ポート 49/50 の LED が、管理上の shutdown で点灯し、管理上の no shutdown で消灯する。

不具合 ID	説明
CSCvq62235	症状 FHS（ファースト ホップ セキュリティ）機能と LAG を使用すると、致命的なエラーが発生したときにスタックが再起動する（再起動の syslog - SYSLOGF-OSFATAL: SW3P_pcl_vll_FHS_verify_reservations_of_all_units: Reservations for unit does not match the needed amount）。
CSCvq31960	症状 TCP SACK（選択的 ACK）の脆弱性に対してデバイスが脆弱である。
CSCvq02158	症状 不要なソフトウェアコンポーネント tcpdump がデバイスで検出された。
CSCvq02165	症状 不要なソフトウェアコンポーネント GNU デバッガ（gdbserver）がデバイスで検出された。
CSCvp35677、CSCvp35688、CSCvo26471、CSCvo28159	症状 「Cisco Small Business スイッチに関する CSRF の脆弱性。」
CSCvq02187	症状 スイッチにハードコードされたパスワードハッシュが含まれている。

リリースバージョン 2.5.0.82 で解決された問題

不具合 ID	説明
CSCvp95489	症状 SG550X-48MP：2.5.0.7x に更新すると、ハードウェアバージョン 2 で再起動ループが発生する。

リリースバージョン 2.5.0.78 で解決された問題

不具合 ID	説明
CSCvn80396	症状 デフォルトの IPv4 アドレスを使用しているときに、sFlow が IPv6 で動作しない。

不具合 ID	説明
CSCvn31587	**症状** デバイスでHTTPSが無効になっていると、ログインページからFindIT Network Probeアプリケーションに接続できません。FindIT Network Probe が有効になっているスイッチに関連した問題です。ログインページから通常の [Switch Management] にアクセスし、ページの上部にある [FindIT] リンクをクリックすることで、引き続きプローブに接続できます。
CSCvj32368	**症状** show green-ethernet コマンドの使用中に、ショートリーチ設定の結果としての [Power Savings] の % が正確に表示されない。
CSCvp40263	**症状** 空きアドレスがない場合、DHCP サーバーが最初に拒否したアドレスの提供を続ける。
CSCvp40272	**症状** IP ルーティングを無効にすると、デフォルトの ARP タイムアウトが 60000 秒のままになる（そのような場合は 300 秒にする必要がある）。
CSCvm76475	**症状** 一部の MIB（ifOutDiscards 1.3.6.1.2.1.2.2.1.19）が Cisco Prime で NULL 値を返す。
CSCvn49346	**症状** DOS：pacific OID の SNMP ウォーキングにより、デバイスが再起動する。
CSCvi71623	**症状** Pacific Avaya 製電話機の LLDP によりスイッチがクラッシュする。

リリースバージョン 2.5.0.71 で解決された問題

不具合 ID	説明
CSCvj32448	**症状** 一部の SFP ポートに SFP MGBLX1 と 40km 光ファイバケーブルを接続すると、ファイバリンクがフラップする場合がある。リンクフラップ防止機能により、最終的にリンクがダウンすることがある。

不具合 ID	説明
CSCvj32432	**症状** ハイブリッドスタックモードの Sx550x が、2,000 のレイヤ 2 マルチキャストエントリをサポートしている（4,000 をサポートする必要がある）。
CSCvg69635/CSCvb96602	**症状** OOB インターフェイスがネットワークに接続されているときにデバイスが再起動し、「%2SWPORTF-Failed2ConvertPort: SW2C_port_get_customer - failed to validate ifIndex -1 relativeIf -1」というエラーメッセージが表示されることがある。
CSCvj23510	**症状** ポートのネイティブ VLAN が VLAN 1 ではなく、ポートがすべての VLAN のメンバーではない場合、トランクモードポートの VLAN メンバーシップは削除され、設定がダウンロードされてから、スタートアップコンフィギュレーションにコピーされる。
CSCvk06454	**症状** デバイスが TLS_RSA_WITH_SEED_CBC_SHA という弱い暗号スイートをサポートしている。
CSCvm20300	**症状** 要求された DNS 応答と受信した IP タイプ（IPv6/IPv4）が相互に関連しない特定の DNS 応答を受信すると、デバイスがリロードされる場合がある。
CSCvk75871	**症状** 複数の CLI コマンドを SSH 経由でコンソールにコピーして貼り付けると、デバイス管理がスタックする。
CSCvi65951	**症状** MAC テーブル タイムアウト カウンタがエージングタイムの 2 倍に達すると、ポートチャネル（LAG）でパケットフラッドが発生する。

Cisco Business のオンラインサポート

最新のサポート情報については、次に示すページを参照してください。

Cisco Business	
Cisco Business のホームページ	http://www.cisco.com/go/ciscobusiness

Cisco Business	
サポート	
Cisco Business 350 シリーズ マネージドスイッチ	http://www.cisco.com/c/en/us/support/switches/350-series-managed-switches/tsd-products-support-series-home.html
Cisco Small Business 350X シリーズ スタッカブル マネージド スイッチ	http://www.cisco.com/c/en/us/support/switches/350x-series-stackable-managed-switches/tsd-products-support-series-home.html
Cisco Small Business 550X シリーズ スタッカブル マネージド スイッチ	http://www.cisco.com/c/en/us/support/switches/550x-series-stackable-managed-switches/tsd-products-support-series-home.html
Cisco Business サポートコミュニティ	http://www.cisco.com/go/cbcommunity
Cisco Business のサポートおよび関連リソース	http://www.cisco.com/go/smallbizhelp
Cisco Business の電話によるサポート	http://www.cisco.com/go/cbphone
Cisco Business のチャットサポート	http://www.cisco.com/go/cbchat
Cisco Business ファームウェアのダウンロード	http://www.cisco.com/go/smallbizfirmware リンクを選択して、シスコ製品のファームウェアをダウンロードできます。ログインは不要です。
Cisco Business のオープンソースのリクエスト	アプリケーションの無料/オープン ソース ライセンス（GNU Lesser/一般公的使用許諾など）により使用資格が与えられているソース コードのコピーを受け取るには、次の宛先にリクエストを送信してください。 external-opensource-requests@cisco.com リクエストには、製品のオープンソースマニュアルに記載されているシスコ製品の名前、バージョン、および 18 桁の参照番号（例：7XEEX17D99-3X49X08 1）を明記してください。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。