Cisco Business 250 - 350 シリーズ スイッチ リリースノート ファームウェアバージョン 3.2.0.89

はじめに

2022 年 10 月

このリリースノートでは、Cisco Business 250 および 350 シリーズ スイッチのソフトウェアバージョン 3.2.0.89 で推奨される操作と既知の問題について説明します。

警告 ファームウェア アップグレードをインストールする前に、Readme ノートをお読みください。ファームウェアのアップグレードプロセスは完了までに約 15 分かかる場合があることに注意してください。この間、スイッチはアクティビティを何も示さない場合があります。アップグレードプロセスの一環として、スイッチが数回再起動する場合があります。アップグレードプロセスを中断すると、スイッチが回復不能な損傷を受け、使用できなくなる可能性があります。

解決済みの問題

表 *1 :* リリース *V3.2.0.89* で解決された問題

ケース	説明
CSCwd29685	**症状** 特定のスタートアップ コンフィギュレーション ファイルを表示すると致命的なエラー「%SYSLOG-F-OSFATAL: caught segmentation fault exception at address 0xfffe947e9000」が発生する。
CSCwc68648	**症状** Rapid PVST モードで ARP の問題が発生する。
CSCwc31999	**症状** CBS350-48P-4X-EU：SSH セッションがタイムアウトしない。

ケース	説明
CSCwc32010	**症状** しばらくすると、コンソール、SSH、およびGUIを使用したデバイスの管理に失敗する。
CSCwa69564	**症状** CBS350で、GUIで作成されたアクセスコントロールリストエントリ（ACE）をCLIで削除できない。

今回のリリースでの新機能

このセクションでは、このリリースの新機能と変更について、以前のリリースと比較して詳しく説明します。

以前のバージョンへのダウングレード

バージョン3.2.xxからバージョン3.1.1.7以前にダウングレードしようとすると、ダウングレード操作の一環としてデバイスのスタートアップコンフィギュレーションが削除されることに注意してください。バージョン3.2.0.84より前のイメージから起動しようとすると、この動作についての警告が表示されます。ダウングレードを実行する前にデバイスコンフィギュレーション ファイルをバックアップし、保存したコンフィギュレーション ファイルをダウングレードの完了後にデバイスにロードすることを強くお勧めします。

PoE – CDP および LLDP 電力ネゴシエーションの無効化

以前のバージョンでは、ポートでCDPまたはLLDPが有効になっている場合は、ポートに接続されたPDとの電力ネゴシエーションに常にそのCDPまたはLLDPが使用されていました。状況によっては、ポートで他のCDPおよびLLDPの動作を維持しながら、CDPおよびLLDP電力ネゴシエーションを無効にすることが望ましい場合があります。

バージョン3.2.0.84では、ポートでCDPおよびLLDP電力ネゴシエーションを無効にできるCLIコマンドが追加されました。コマンドシンタックスは **power inline negotiation** {**none | all**}です。GUIインターフェイスを使用したコマンドはサポートされていません。

PoE – 期限切れモードの動作の拡張

以前のバージョンでは、電力ネゴシエーション（CDPまたはLLDP）が期限切れになった場合、ネゴシエーションが期限切れになる前に最後に受信したネゴシエーションパケットに従って、ポートは動作を継続していました。ネゴシエーションを再開するには、PoEをオフにしてから再度オンにするか、ケーブルを取り外してから再度取り付けるしかありませんでした。バージョン3.2.0.84では、ネゴシエーションが期限切れになった後に新しいネゴシエーションパケットを受信した場合にも、電力ネゴシエーションが再開されます。この場合、ポートは期限切れモードから復帰し、新しいパケットに基づいてネゴシエーションを再開します。

パスワード履歴（Password History）

パスワード履歴機能のサポートがバージョン 3.2.0.84 で追加されました。パスワード履歴機能を使用すると、スイッチ管理者は以前に使用したパスワードの使用を制限できるため、パスワードのセキュリティレベルが向上します。この機能がデバイスで有効になっていると、新しいパスワードが以前に設定されたパスワードのいずれかと同じ場合、新しいパスワードの設定は拒否されます。管理者は、チェック対象とする以前に使用したパスワードの数を設定します。

パスワード変更時のパスワード再認証

パスワード再認証要件の目的は、バイパスした人物によるパスワードの変更を防止することです。バージョン3.2.0.84では、ログインユーザー（コンソール、Telnet、SSH、またはGUI）が自分のローカルデータベース関連のパスワードを変更しようとすると、現在のパスワードを**クリアテキスト形式で**入力するよう求められます。別のユーザーのパスワードを変更する場合や、回線パスワードまたはイネーブルパスワードの変更を要求する場合は、再認証は必要ありません。

ユーザーが設定したパスワードと既知の値の比較

バージョン 3.2.0.84 では、ユーザーが設定したパスワードが既知の値と比較され、既知の値と一致する場合、パスワードは拒否されます。次のいずれかが発生した場合、パスワードは拒否されます。

- パスワードに、既知の辞書に載っている単語と、以前の侵害コーパスから取得したパスワードが含まれている。
- パスワードに、繰り返し（この制限は以前のバージョンでサポート済み）または3つ以上の連続した（または逆の）文字か数字が含まれている。
- パスワードが CBS という語、ユーザー名（この制限は以前のバージョンでサポート済み）、またはciscoという語（この制限は以前のバージョンでサポート済み）と等しいか、パスワードにそれらが含まれている。

（注） 次のような他の文字に置き換えられる文字も上記のセクションの制限に含まれます。「s」の代わりの「$」、「a」の代わりの「@」、「o」の代わりの「0」、「l」の代わりの「1」、「i」の代わりの「!」、「e」の代わりの「3」。

パスワードのランダム生成

バージョン 3.2.0.84 では、手動でパスワードを入力する代わりに、ランダムに生成されたパスワードを選択できます。ランダムに生成されたパスワードは、人間のユーザーが作成したパスワードよりも安全であると考えられるため、侵害が困難です。ユーザーがパスワードを作成または編集する際に、ソフトウェアによってランダムに生成されたパスワードを要求するオプションが表示されます。ユーザーは、提案されたパスワードを受け入れるか拒否するかを選択できます。拒否する場合は、パスワードを再設定する必要があります。デバイスは、ランダム

に生成されたパスワードをデータベースパスワード、イネーブル データベース パスワード、および回線パスワード用に提供できます。

パスワード エージング

ユーザーが設定した一定期間後にパスワードを変更するという要件は、以前のバージョンですでにサポートされています。ただし、バージョン 3.2.0.84 では、次の機能が追加または変更されました。

- パスワードエージングのデフォルト設定は無効になっています（以前のバージョンでは、デフォルトで有効になっていました）。機能のステータスは、以前のバージョンからのアップグレード時または以前のバージョンへのダウングレード時にも保持されます。
- パスワードエージングは、レベル 15 のユーザーだけでなく、すべてのユーザーレベル（1～15）に適用されます。また、すべてのパスワードタイプ（ローカル、イネーブル、および回線）にも適用されます。
- 警告期間が追加されました。パスワードの有効期限が切れる 10 日前にデバイスにログインすると、パスワードが 10 日後に期限切れになるという警告が表示されます。これにより、有効期限が切れる前でもパスワードを変更でき、その後パスワードが変更されない場合、デバイスへのアクセスは拒否されます。
- 有効期限日が過ぎると、ログインしているユーザーはパスワードの変更が強制されます。パスワードが正常に変更されない限り、アクセスは許可されません。

ログイン遅延とログイン攻撃の防止

デバイスのアドレスがわかっている場合、悪意のあるユーザーが辞書攻撃を試みる可能性があります。辞書攻撃とは、数千、時には数百万ものログイン情報でログインを試行する自動化されたプロセスです。このような攻撃を防ぐために、バージョン 3.2.0.84 では、ログイン試行に失敗した後の遅延を設定できます。この遅延は、悪意のある接続の試行を遅らせるのに役立ちます。

試行に失敗した後の待機時間

辞書攻撃に対処するために、バージョン 3.2.0.84 では、失敗した試行が指定の回数に達した後に続く待機モード時間を定義して、特定の時間範囲内で許可されるログイン試行回数を制限することもできます。待機モード時間の間、デバイスは追加の接続要求を受け入れません。ただし、ユーザーが事前に設定した管理アクセスリストによって承認されている接続要求は除きます。このリストは、こうした攻撃を受けているときでも既知のユーザーにアクセスを許可するために必要です。

SSL 暗号化

サポートされる SSL 暗号のリストがバージョン 3.2.0.84 で更新されました。次の暗号方式がサポートされています。

- TLSv1.2：
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256（secp256r1）

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256（secp256r1）
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA（secp256r1）
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384（secp256r1）
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384（secp256r1）
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256（secp256r1）
- TLS_RSA_WITH_AES_128_CBC_SHA（rsa 3072）
- TLS_RSA_WITH_AES_256_CBC_SHA（rsa 3072）
- TLS_RSA_WITH_AES_256_CBC_SHA256（rsa 3072）
- TLS_RSA_WITH_AES_256_GCM_SHA384（rsa 3072）

- TLSv1.3 – このバージョンで新たに追加：
  - TLS_AES_128_GCM_SHA256
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_256_GCM_SHA384

OpenSSL バージョン

OpenSSL バージョンがバージョン 3.2.0.84 から OpenSSL バージョン 1.1.1n にアップグレードされました。

OpenSSH の機能強化

- 次の SHA2 公開キーアルゴリズムのサポートが追加されました。
  - rsa-sha2-512
  - rsa-sha2-256
- 次の MAC（メッセージ認証コード）方式のサポートが追加されました。
  - hmac-sha2-256
  - hmac-sha2-512
- SSH キー交換方式に次の変更が導入されました。
  - Diffie-hellman-group-exchange-sha1 – この方式は、バージョン 3.2.0.84 ではサポートされなくなりました。
  - Diffie-hellman-group16-sha512 – この方式のサポートがバージョン 3.2.0.84 で追加されました。

セキュリティ関連ロギング

バージョン 3.2.0.84 では、セキュリティに関連するデバイス構成または設定の変更に対して追加のアラート（syslog および SNMP トラップ）を提供することにより、デバイスのセキュリティが強化されました。次のアラートが追加されました。

- デバイスのアクティブまたは非アクティブなイメージファイルの変更（すでにサポートされているアラートに加えて追加のアラートが導入されました）。
- ユーザーまたは SNTP によるシステムクロックまたはシステムクロック設定の変更。これには、時刻自体、時刻源、ゾーン、および夏時間情報の変更が含まれます。
- デバッグモードへのアクセス。
- 認証ポリシーと認証情報の変更。これには次のものが含まれます。
  - ユーザーアカウント（ローカル、イネーブル、および回線）とパスワードの変更
  - 認証または許可方式リストの変更
  - パスワードの複雑度の設定の変更
  - RADIUS または TACACS+ クライアントアドレスまたはキー設定の変更
  - RADIUS サーバーの NAS シークレットの変更
  - SNMP 認証構成の変更
  - 管理 ACL の変更
  - ACL、クラスマップ、およびポリシーマップ設定の変更
- 双方向の暗号化 SSH または TLS 接続のセットアップとシャットダウンをログに記録します。この動作は、ユーザーが有効化または無効化できます。デフォルトでは無効です。

HTTP Strict Transport Security（HSTS）のサポート

HTTP Strict-Transport-Security（HSTS）レスポンスヘッダーは、サイトへの今後の接続に HTTPS のみを使用する必要があることをブラウザに通知します。これにより、セキュリティが強化され、MITM 攻撃のリスクが低下します。バージョン 3.2.0.84 では、デバイスが TLS 暗号化接続の要求に応答するときは常に、「Strict-Transport-Security」ヘッダーを含めて、デバイス Web サーバーへの今後のすべての要求にも暗号化接続を使用する必要があることをクライアントに通知します。HTTP クライアントとして、デバイスはサーバーから受信した「Strict-Transport-Security」ヘッダーを受け入れます。

（注） HSTS は、ブラウザからデバイスへの最初の接続が HTTPS 経由の場合にのみ関係します。Web 管理に HTTP を使用することを選択したユーザーは保護されません。デバイス管理に接続するときは、常にセキュアな接続を使用することをお勧めします。

FPGA のアップグレード

バージョン 3.2.0.84 では、一般的なイメージの更新の一環として FPGA バージョンのアップグレードをサポートします。

Cisco Business ダッシュボード

バージョン 3.2.0.84 では、Cisco Business ダッシュボード（CBD）のサポートが次のように強化されました。

- CBS プローブのバージョンがバージョン 2.4.1.20220225 にアップグレードされました。
- CBD 接続ステータスと理由のサポートが追加されました。

（注） MCU のバージョン 0xF0 へのアップグレードには、スタンドアロンスイッチの場合、約 5 分かかります。スイッチのスタックでは、スタックメンバーの検出に時間が必要になるため、アップグレードにはさらに数分かかります。

解決済みの問題

表 *2 :* リリース *V3.2.0.84* で解決された問題

ケース	説明
CSCvx89372	**症状** ヘルプテキストが [Destination/Source MAC Wildcard Mask] で、フィールド形式に関する情報が提供されていなかった。このヘルプテキストは [See Online Help for format] に変更済み。
CSCwc39418	**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。
CSCvw65642	**症状** GUI でセッションタイムアウトを設定した場合に、この設定がスタートアップコンフィギュレーションに保存されず、再起動後に適用されないことがある。
CSCwa91538	**症状** ACL を削除して VLAN インターフェイスに再適用した場合に、ハードウェアリソースに関するメッセージが表示されて操作が失敗し、バックアップユニットが再起動することがある。

ケース	説明
CSCvz42028	**症状** PVST モードでのコマンド「show spanning-tree active vlan <#>」の出力に、指定した VLAN に属していないアクセスポートが表示されることがある。
CSCwc39424	**症状** 約 2 時間後に、SNTP がホスト名で設定された SNTP サーバーのポーリングを停止する。
CSCwc39428	**症状** 2.5 および 10G インターフェイスの LDP MAC-PHY TLV 値が正しくない。
CSCwc39431	**症状** スタンバイユニットへのスタックスイッチオーバーの後、プローブが CBD ダッシュボードに自動的に再接続しない。
CSCvu81808	**症状** GUI で編集すると、ACE が削除されることがある。
CSCwc39432	**症状** インターフェイスが自動ネゴシエーションに設定されているにもかかわらず、MAC/PHY コンフィギュレーション/ステータス TLV の自動ネゴシエーションが無効を示している。
CSCwc39434	**症状** GUI から「タブ」文字を含む CA 証明書をインポートすると、「署名者」CA が 2 回表示される。
CSCwc39437	**症状** GUI での PoE 設定および統計情報ページの表示が非常に遅い。
CSCwc39514	**症状** DHCPv6 クライアントを VLAN インターフェイスから物理インターフェイスに切り替えると、デバイスがクラッシュすることがある。
CSCwc39515	**症状** VLAN 1 のデフォルト IP との競合が原因で OOB インターフェイスがアドレスを拒否した場合に、コマンド renew dhcp oob が失敗する。
CSCwc39531	**症状** GUI でデバイスのログイン情報を追加または変更した場合に、CBD モバイルアプリを介したログインに失敗する。

ケース	説明
CSCwb57285	**症状** 優先順位が低く、LLDP がネゴシエートされていない Class0-4 PoE PD が、Class4 PD の接続時に再起動することがある。
CSCvz97713	**症状** CBS250-8P-E-2G：リンクフラップが発生し、PoE で「拒否カウンタ」が増加する。

既知の問題

リリース V3.2.0.84 で確認された問題

不具合 ID	説明
CSCwc39517	**症状** 短時間の停電の後、スイッチが応答しなくなることがある。この症状が発生する SKU は CBS350-24XTS のみである。 **回避策** なし
CSCwc39527	**症状** 一部のプラットフォームで、レガシー PoE PD が 802.3AF ではなく 802.3AT として検出される。 **回避策** なし
CSCwc39529	**症状** SFP GLC-BX、GLC-BX-D、または MGBLX1-V2-1G トランシーバを取り付けると、I2C 関連のメッセージが生成されることがある。 **回避策** 機能上の問題はありません。SFP は数秒で初期化されます。
CSCwc44155	**症状** Web ページの [File operations] が無効になるため、CBD を有効にする前にダッシュボードデータを USB にバックアップする。 **回避策** Web ページ [File operations] の機能は復元できませんが、関連する CLI 機能は引き続き動作します。

不具合 ID	説明
CSCwc39519	**症状** アクティブユニットのスイッチオーバーが発生すると、ログイン攻撃の防止策（ログイン試行に失敗した回数、期間、および待機モード）がリセットされる。 **回避策** なし。
CSCwc39521	**症状** VLAN1 を静的 IP アドレス 192.168.1.254 に設定し、他のデバイスにすぐに ping を実行すると、ping が失敗する。 **回避策** IP 設定コマンドをコピーして貼り付けるのではなく、手動で IP アドレスを設定します。
CSCwc39522	デバイスソフトウェアが 3.2.0.x から 3.1.1.7 以前のバージョンにダウングレードされた場合、ユーザーがブラウザクッキーを削除しない限り、デバイス GUI 管理にアクセスできない。 **回避策** デバイスに接続する前にブラウザクッキーを削除します。
CSCwc39527	**症状** 一部のプラットフォームで、レガシー PoE PD が 802.3AF ではなく 802.3AT として検出される。 **回避策** なし。
CSCwc39529	**症状** SFP GLC-BX、GLC-BX-D、または MGBLX1-V2-1G トランシーバを取り付けると、I2C 関連のメッセージが生成される。 **回避策** 機能上の問題はありませんが、show inventory コマンドおよび show interface status コマンドを使用してトランシーバのステータスを確認することをお勧めします。

不具合 ID	説明
CSCwc39530	**症状** 以前のバージョンからバージョン 3.1.1.7 にアップグレードした後、構成ファイルに証明書失効構成がない。 **回避策** なし

はじめに

2021 年 9 月

このリリースノートでは、Cisco Business 250 および 350 シリーズ スイッチのソフトウェアバージョン 3.1.1.7 で推奨される操作と既知の問題について説明します。

今回のリリースでの新機能

このセクションでは、このリリースの新機能と変更について、以前のリリースと比較して詳しく説明します。

1.1 OOB をサポートするデバイスのデフォルトの IP 設定

以前のバージョンでは、ネイティブモードで OOB をサポートするデバイスのデフォルトの管理インターフェイスは、デフォルトの VLAN ではなく OOB ポートに適用されていました。ハイブリッドモードでは、デフォルトの IP 管理インターフェイスは VLAN 1 に適用され、OOB は無効になります。このバージョン以降、OOB をサポートするネイティブモードのデバイスでも、デフォルトの管理インターフェイスは VLAN 1 に適用されます。新しい動作では、OOB インターフェイスはネイティブモードではデフォルトで DHCP が有効になり、デフォルトの IP 設定をサポートしません。ハイブリッドモードでは、以前のバージョンと同様に OOB が無効になります。

次の表は、バージョン 3.1.1.7 で適用された変更の前後における VLAN 1 および OOB のデフォルトの IP 設定をまとめたものです。

	Cisco Business ファームウェアバージョン 3.1 以前		**Cisco Business ファームウェアバージョン 3.1.1.7**	
	OOB インターフェース	VLAN 1 インターフェイス	OOB インターフェース	VLAN 1 インターフェイス
IP 設定	デフォルト IP + DHCP		DHCP 有効	デフォルト IP + DHCP
インターフェイスの CLI 設定	なし	なし	「IP address dhcp」	なし

	Cisco Business ファームウェアバージョン 3.1 以前		Cisco Business ファームウェアバージョン 3.1.1.7	
その他	Bonjour 有効	なし	なし	Bonjour 有効

（注） 以前のバージョンと現在のバージョンの間でアップグレードまたはダウングレードを行う場合、デバイスが工場出荷時のデフォルトに設定されていない限り、既存の構成を維持することを目的とします。アップグレードまたはダウングレード操作の前後の構成を書き留め、構成を確認してください。

（注） 新しいバージョンにアップグレードするときは、スタッキングモードを変更しないでください。新しい設定は、予想とは異なる場合があります。モードの変更が必要な場合は、最初にモードを変更してからスタックをアップグレードします。

1.2 更新された Cisco Trusted Core Bundle

3.1.1.7 ファームウェアは Cisco コアバンドルを使用します。

1.3 新しい PoE ドライバ

新しい PoE ドライバのバージョンは 0.2.0.17 です。

解決済みの問題

表 *3 :* リリース *V3.1.1.7* で解決された問題

ケース	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。

ケース	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** 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。
CSCvz59935	**症状** SG350X-48MP と CBS350-48XT-4 の間のファイバリンクがフラップしてから中断される。
CSCvw84846	**症状** しばらくすると、PoE が一部のインターフェイスで電力供給を停止する。
CSCvw86418	**症状** デバイスで設定されている CA 証明書の名前にスペースが含まれている場合（「my cert」など）、CBD プローブから接続できない。
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。

既知の問題

リリース V3.1.1.7 で確認された問題

不具合 ID	説明
CSCvz58788	**症状** 以前のバージョンからバージョン 3.1.1.7 にアップグレードした後、構成ファイルに証明書失効構成がない。 **回避策** なし。

不具合 ID	説明
CSCvz62516	CBD プローブおよびモバイルアプリが、デバイスの Web GUI で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。CLI または CBD プローブでユーザーパスワードを変更した場合、問題は発生しない。 **回避策** デバイスの Web GUI からログアウトし、新しいパスワードでログインします。
CSCvz64701	CBS350-48P-4G：ワイヤレスアクセスポイントと電話の両方が接続されている場合、ポートの電源が再投入されることがある。 **回避策** なし。
CSCvz67634	CBS350-24P-4X：PoE が適切にリセットされず、PD デバイスの電力が失われてフラップが発生する。 **回避策** なし。

Cisco Business 250 および 350 シリーズ スイッチリリースノート - ソフトウェアバージョン 3.1.0.57

2021 年 2 月

このリリースノートでは、Cisco Business 250 および 350 シリーズ スイッチのソフトウェアバージョン 3.1.0.57 で推奨される操作と既知の問題について説明します。

このリリースの最新情報

1.1 機能強化

次のリストに、このリリースで導入された変更と機能強化を示します。

- CBS350 SKU での RIPv2 サポート
- CA 証明書は、システムクロックがユーザー、RTC、または SNTP によって設定されている場合にのみ有効です。
- CBS350 スタック構成 SKU にハイブリッドスタックのサポートが追加されました。
- スタック構成ユニットの役割の名前が、アクティブユニット、スタンバイユニット、メンバーユニットに変更されました。

- CBD プローブバージョン 2.2.1.x

解決済みの問題

表 *4 :* リリース *V3.1.0.57* で解決された問題

ケース	説明
CSCvs26294	**症状** ポートセキュリティにより、他のインターフェイスで保護されている MAC のシャットダウンアクションがサポートされるようになりました。
CSCvx48537	**症状** md5 認証方式と DES 暗号化方式を廃止し、暗号化方式として SHA-2 認証と AES-128 に置き換えることによって、SNMPv3 のセキュリティを強化しました。
CSCvx48588	**症状** 音声 VLAN および Autosmart ポートのデフォルト設定が無効に変更されました。
CSCvx48591	**症状** PNP エージェントの組み込みバンドルのサポートが追加されました。
CSCvx48594	**症状** セキュリティを強化するために、PNP サーバー証明書の CN/SAN 検証が追加されました。
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。
CSCvu81809	**症状** ポートチャネルとそのメンバーポートについて ACL を適用または削除すると、トラフィックが中断される。
CSCvu81810	**症状** GUI で時間範囲を MAC ACL に関連付けることができない。
CSCvu81807	**症状** permit ip source 10.10.10.1 service telnet gi1 を設定した後、管理アクセスリスト Telnet_Only を表示すると、ポートが表示されない。

既知の問題

表 *5 :* リリース *V3.1.0.57* で確認された問題

ケース	説明
CSCvx44260	**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。
CSCvx44267	**症状** 100Mbps 半二重を OOB ポートで設定できない。 **回避策** 別の速度設定を使用して OOB に接続します。
CSCvx44269	**症状** 一部の Mgig インターフェイスでは、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（3 メートル未満）場合に、ケーブルテスト（VCT）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。
CSCvx44271	**症状** ユーザーがアラートアイコン点滅を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。
CSCvx44276	**症状** 特定のデバイスの XG アップリンク インターフェイスで、値が 18M 未満の出力トラフィックシェーピング（CIR）により、トラフィックが設定値未満にシェーピングされることがある。 **回避策** なし。

Cisco Business 250 および 350 シリーズ スイッチリリースノート - ソフトウェアバージョン 3.0.0.69

2020 年 9 月

このリリースノートでは、次のモデルを含む Cisco Business 250 および 350 シリーズ スイッチのソフトウェアバージョン 3.0.0.69 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	製品ラベル
CBS250-8T-E-2G	8 ポート ギガビット スマート スイッチ
CBS250-8PP-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-8P-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-8FP-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-16T-2G	16 ポート ギガビット スマート スイッチ
CBS250-16P-2G	16 ポートギガビット PoE スマートスイッチ
CBS250-24T-4G	24 ポート ギガビット スマート スイッチ
CBS250-24PP-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-24P-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-24FP-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-48T-4G	48 ポート ギガビット スマート スイッチ
CBS250-48PP-4G	48 ポートギガビット PoE スマートスイッチ
CBS250-48P-4G	48 ポートギガビット PoE スマートスイッチ
CBS250-24T-4X	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）
CBS250-24P-4X	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）
CBS250-24FP-4X	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）
CBS250-48T-4X	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）

モデル	製品ラベル
CBS250-48P-4X	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）
CBS350-8T-E-2G	8 ポート ギガビット マネージド スイッチ
CBS350-8P-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8P-E-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8FP-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8FP-E-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-16T-2G	16 ポート ギガビット マネージド スイッチ
CBS350-16T-E-2G	16 ポート ギガビット マネージド スイッチ
CBS350-16P-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-16P-E-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-16FP-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24T-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24P-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24FP-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-48T-4G	48 ポート ギガビット マネージド スイッチ
CBS350-48P-4G	48 ポートギガビット PoE マネージドスイッチ
CBS350-48FP-4G	48 ポートギガビット PoE マネージドスイッチ
CBS350-24T-4X	24 ポート ギガビット スタッカブル マネージド スイッチ（10G アップリンク付き）
CBS350-24P-4X	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（10G アップリンク付き）
CBS350-24FP-4X	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（10G アップリンク付き）
CBS350-48T-4X	48 ポート ギガビット スタッカブル マネージド スイッチ（10G アップリンク付き）
CBS350-48P-4X	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（10G アップリンク付き）

モデル	製品ラベル
CBS350-48FP-4X	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（10G アップリンク付き）

今回のリリースでの新機能

1.1 ブラウザと OS のサポート

デバイスの Web UI は、次のブラウザと OS システムをサポートしています。

- サポートされている OS：MS Windows 7（32 および 64 ビット）、MS Windows 10（32 および 64 ビット）、MAC OS（サポート対象外：MS Windows 8、8.1、XP および Vista、Linux）
- サポートされているブラウザ：Chrome、Firefox、Microsoft Edge（Microsoft Internet Explorer はサポート対象外）（Windows と MAC OS の両方）。 Safari（MAC OS のみ）。

1.2 Web GUI スタイル

CBS 3.0 では、PISA に準拠した新しい GUI スタイルを使用します。

1.3 パスワードの複雑度

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

1.4 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

1.5 SSL 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。

1.6 コンソールのサポート

このリリースノートに記載されているCBS350およびCBS250スイッチモデルでは、RJ45とミニUSBの両方のコンソールがサポートされています。ミニUSBが優先されます。

1.7 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

1.8 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。

1.9 リアルタイムクロック

このリリースのSKUには、デバイスがシャットダウンされて電源に接続されていない場合でも正確な時刻を維持する、自己完結型リアルタイムクロック（RTC）コンポーネントが内蔵されています。この内部クロックは製造中に初期化され、ソフトウェアクロックの（手動やSNTPなどによる）設定時に、デバイスの時刻機能によって更新されます。

スタック構成では、すべてのユニットがマスターユニットのRTCと同期します。スタックの動作の詳細については、機能仕様を参照してください。CBSの今後のリリースには、RTCをサポートしないSKUが含まれる可能性があることに注意してください。この場合、別のユニット（マスターではない）がシステム時刻源として使用されます。

RTCは、「信頼できる」時刻源を必要とする機能（時間範囲の設定、IP DHCPスヌーピングデータベースの更新、スケジュール設定による再起動）に対して「信頼できる」と見なされます。

1.10 PNPエージェントの機能強化

CBS 3.0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。Tesla 2.5.5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。

1.11 スタックユニット ID の表示

このリリースのスタック構成 SKU は、専用のスタック構成 LED をサポートしていません。したがって、これらのユニットではシステム LED を次のように使用してスタックユニット ID を示します。

- アクティブユニット：システム LED は緑色に点灯したままになります（デバイスがブートアップフェーズにある場合、ハードウェア障害がある場合、またはデバイスが電源に接続されていない場合を除く）。
- メンバーユニットの場合：ブートアップフェーズとマスターユニットへの接続が完了した後、20 秒ごとにシステム LED がメンバーユニットのユニット ID に従って緑色に点滅します。
  - ユニット 1（アクティブではない場合）：システム LED が 1 回点滅します。
  - ユニット 2（アクティブではない場合）：システム LED が 2 回点滅します。
- ユニット 3：システム LED が 3 回点滅します。
- ユニット 4：システム LED が 4 回点滅します。

（注） 注：今後のリリースで追加される SKU は、専用のスタック構成 LED をサポートする可能性があります。

1.12 オンラインヘルプ（OLH）と言語ファイル

バージョン 3.0.0.69 には、OLH ファイルに対する複数の修正が含まれています。また、このバージョンでは中国語と日本語の言語ファイルがサポートされています。

1.13 CBD プローブバージョン 2.2.0.20200801

バージョン 3.0.0.69 では、CBD プローブはバージョン 2.2.0.20200801 にアップグレードされました。

解決済みの問題

表 *6 :* リリース *V3.0.0.69* で解決された問題

ケース	説明
CSCvv70507	**症状** まれに、再起動後にデバイスのアクティブイメージが破損し、正しくロードされないことがある。

Cisco Business 250 および 350 シリーズ スイッチリリースノート - ソフトウェアバージョン 3.0.0.61

2020 年 8 月

このリリースノートでは、次のモデルを含む Cisco Business 250 および 350 シリーズ スイッチのソフトウェアバージョン 3.0.0.61 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	製品ラベル
CBS250-8T-E-2G	8 ポート ギガビット スマート スイッチ
CBS250-8PP-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-8P-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-8FP-E-2G	8 ポート ギガビット PoE スマート スイッチ
CBS250-16T-2G	16 ポート ギガビット スマート スイッチ
CBS250-16P-2G	16 ポートギガビット PoE スマートスイッチ
CBS250-24T-4G	24 ポート ギガビット スマート スイッチ
CBS250-24PP-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-24P-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-24FP-4G	24 ポートギガビット PoE スマートスイッチ
CBS250-48T-4G	48 ポート ギガビット スマート スイッチ
CBS250-48PP-4G	48 ポートギガビット PoE スマートスイッチ
CBS250-48P-4G	48 ポートギガビット PoE スマートスイッチ
CBS250-24T-4X	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）
CBS250-24P-4X	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）
CBS250-24FP-4X	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）
CBS250-48T-4X	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）

モデル	製品ラベル
CBS250-48P-4X	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）
CBS350-8T-E-2G	8 ポート ギガビット マネージド スイッチ
CBS350-8P-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8P-E-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8FP-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-8FP-E-2G	8 ポートギガビット PoE マネージドスイッチ
CBS350-16T-2G	16 ポート ギガビット マネージド スイッチ
CBS350-16T-E-2G	16 ポート ギガビット マネージド スイッチ
CBS350-16P-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-16P-E-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-16FP-2G	16 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24T-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24P-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-24FP-4G	24 ポート ギガビット PoE 対応マネージド スイッチ
CBS350-48T-4G	48 ポート ギガビット マネージド スイッチ
CBS350-48P-4G	48 ポートギガビット PoE マネージドスイッチ
CBS350-48FP-4G	48 ポートギガビット PoE マネージドスイッチ
CBS350-24T-4X	24 ポート ギガビット スタッカブル マネージド スイッチ（10G アップリンク付き）
CBS350-24P-4X	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（10G アップリンク付き）
CBS350-24FP-4X	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（10G アップリンク付き）
CBS350-48T-4X	48 ポート ギガビット スタッカブル マネージド スイッチ（10G アップリンク付き）
CBS350-48P-4X	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（10G アップリンク付き）

モデル	製品ラベル
CBS350-48FP-4X	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（10G アップリンク付き）

今回のリリースでの新機能

1.1 ブラウザと OS のサポート

デバイスの Web UI は、次のブラウザと OS システムをサポートしています。

- サポートされている OS：MS Windows 7（32 および 64 ビット）、MS Windows 10（32 および 64 ビット）、MAC OS（サポート対象外：MS Windows 8、8.1、XP および Vista、Linux）
- サポートされているブラウザ：Chrome、Firefox、Microsoft Edge（Microsoft Internet Explorer はサポート対象外）（Windows と MAC OS の両方）。 Safari（MAC OS のみ）。

1.2 Web GUI スタイル

CBS 3.0 では、PISA に準拠した新しい GUI スタイルを使用します。

1.3 パスワードの複雑度

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

1.4 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

1.5 SSL 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。

1.6 コンソールのサポート

コンソールのサポートに次の変更が導入されました。

- このリリースのSKUは、RJ45とミニUSBの両方のコンソールをサポートしています。ミニ USB が優先されます。
- CBS250 SKU はコンソールインターフェイスをサポートします（Tesla 製品ラインでは、250 SKU はコンソールインターフェイスをサポートしていませんでした）。

（注） コンソールのサポートは、このリリースの SKU にのみ関連します。今後のリリースの SKU は単一の RJ45 インターフェイスをサポートし、250 製品ラインの SKU はコンソールをサポートしません。

1.7 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

1.8 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。

1.9 リアルタイムクロック

このリリースの SKU には、デバイスがシャットダウンされて電源に接続されていない場合でも正確な時刻を維持する、自己完結型リアルタイムクロック（RTC）コンポーネントが内蔵されています。この内部クロックは製造中に初期化され、ソフトウェアクロックの（手動やSNTPなどによる）設定時に、デバイスの時刻機能によって更新されます。

スタック構成では、すべてのユニットがマスターユニットの RTC と同期します。スタックの動作の詳細については、機能仕様を参照してください。CBS の今後のリリースには、RTC を

サポートしないSKUが含まれる可能性があることに注意してください。この場合、別のユニット（マスターではない）がシステム時刻源として使用されます。

RTC は、「信頼できる」時刻源を必要とする機能（時間範囲の設定、IP DHCP スヌーピングデータベースの更新、スケジュール設定による再起動）に対して「信頼できる」と見なされます。

1.10 PNP エージェントの機能強化

CBS 3.0 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。Tesla 2.5.5 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。

1.11 スタックユニット ID の表示

このリリースのスタック構成 SKU は、専用のスタック構成 LED をサポートしていません。したがって、これらのユニットではシステム LED を次のように使用してスタックユニット ID を示します。

- アクティブユニット：システム LED は緑色に点灯したままになります（デバイスがブートアップフェーズにある場合、ハードウェア障害がある場合、またはデバイスが電源に接続されていない場合を除く）。
- メンバーユニットの場合：ブートアップフェーズとマスターユニットへの接続が完了した後、20 秒ごとにシステム LED がメンバーユニットのユニット ID に従って緑色に点滅します。
  - ユニット 1（アクティブではない場合）：システム LED が 1 回点滅します。
  - ユニット 2（アクティブではない場合）：システム LED が 2 回点滅します。
- ユニット 3：システム LED が 3 回点滅します。
- ユニット 4：システム LED が 4 回点滅します。

（注） 注：今後のリリースで追加される SKU は、専用のスタック構成 LED をサポートする可能性があります。

既知の問題

表 *7:* リリース ***V3.0.0.61*** で確認された問題

ケース	説明
CSCvu81820	**症状** SKU SG252X-4 からファンを取り外した後でも、ファンのステータスが OK を示す。 **回避策** なし。
CSCvu81812	**症状** 非コンボポートで 100M SFP がサポートされない。 **回避策** なし。
CSCvu81814	**症状** PD 以外がスイッチの PoE ポートに接続すると、PoE 不足カウンタが増加し、ステータスが障害を示す。 **回避策** ポートレベルで PoE を無効にします。
CSCvu81816	**症状** PVST/RPVST が有効になっているとき、ループバック検出はトリガーされるべきではない。 **回避策** なし。
CSCvu81808	**症状** GUI で ACE を数回編集すると、ACE が誤って削除される。 **回避策** なし。
CSCvu81809	**症状** ポートチャネルとそのメンバーポートについて ACL を適用または削除すると、トラフィックが中断される。 **回避策** なし。

ケース	説明
CSCvu81810	**症状** GUI で時間範囲を MAC ACL に関連付けることができない。 **回避策** なし。
CSCvu81811	**症状** GUI：DUT でスパニングツリーを PVST として設定するのに 45 秒かかる。 **回避策** なし。
CSCvu81807	**症状** permit ip source 10.10.10.1 service telnet gi1 を設定した後、管理アクセスリスト Telnet を表示すると、ポートが表示されない。 **回避策** なし。
CSCvu81818	**症状** CBS250-48T-4X のファンの RPM が、ファンを取り外した後も常に 4075 を示す。 **回避策** なし。
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。

ケース	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** 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。
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** これは単に表示の問題です。
CSCuu61008	**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** なし。
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、認証されないステーションの IP アドレスが、ステーションによって DHCP リリースが送信された後に期限切れにならない。 **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。

ケース	説明
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）が同時に実行されることによってトラフィックが宛先ポートに複製されるときに、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。
CSCve55081/CSCve55217	**症状** 指定されたデバイスの特定のポートでは、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、コマンド「test cable-diagnostics tdr」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。
CSCve55094	**症状** キュー統計：統計自体は出力の統計だが、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。
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** 設定するIPv6ルートを少なくするか、異なる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。
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と一緒にループバック検出を有効にしないでください。

ケース	説明
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。
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。
CSCvu16282	**症状** Cisco Business ダッシュボードプローブが、プライマリスタックのスイッチオーバー後にマネージャに自動的に接続できない。 **回避策** スタックをリロードします。
CSCvu16298	**症状** 「ポートの LED の無効化」を保存して再起動した後も、PoE LED が点灯する。 **回避策** なし。
CSCvu24619	**症状** Cisco Business ダッシュボードプローブの状態が数秒以内に無効と有効の間で切り替わると、スタック内のバックアップユニットが再起動することがある。 **回避策** 10 秒以上待ってから、Cisco Business ダッシュボードプローブの状態を切り替えます。

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
サポート	
CBS250 製品ページ	http://www.cisco.com/c/en/us/products/switches/business-250-series-smart-switches/index.html
CBS350 製品ページ	https://www.cisco.com/c/en/us/products/switches/business-350-series-managed-switches/index.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。

© 2022 Cisco Systems, Inc. All rights reserved.