Cisco Catalyst 1200 および 1300 シリーズ スイッチ ファームウェア バージョン 4.0.0.91 ～ 4.1.0.76 リリースノート

初版：2024 年 1 月 25 日

解決済みの問題 4.1.0.76

表 *1 :* リリース *V4.1.0.76* で解決された問題。

不具合 ID	説明
CSCwi77502	**症状** 回線レートでトラフィックを転送する場合、長い Cat6A ケーブルを使用すると、まれに C1300-24XT でわずかなパケット損失が発生します。

既知の問題 4.1.0.75

表 *2 :* リリース *V4.1.0.75* で確認された問題

不具合 ID	説明
CSCwi56166	**症状** キー交換で RSA-SHA2-512 および RSA-SHA2-256 ホストキーアルゴリズムを使用すると、デバイスへの SSH 接続に失敗します。 **回避策** なし

解決済みの問題 4.1.0.75

表 *3 :* リリース *V4.1.0.75* で解決された問題。

不具合 ID	説明
CSCwi54956	**症状** C1300-24MGP-4X ポート 17 は、2.5G の速度でパケットを転送できません。
CSCwi54958	**症状** MAC 転送テーブルに同様のエントリが存在する場合、MAC アドレスの再学習が失敗します。
CSCwi54959	**症状** まれに、C1300-48MGP-4X のポート 45、46、47、および 48 が再起動後にリンクアップできないことがあります。

新機能

ここでは、ファームウェアバージョン 4.1.0.72 で導入された新機能と変更について詳しく説明します。

- 新しいハードウェア プラットフォームのサポート：
  - このリリースでは新しい PID が導入されています。それらを次の表に示します。

デバイス PID	説明
C1300-8MGP-2X	Catalyst 1300 シリーズ マネージドスイッチ、4 ポート 2.5GE、4 ポート GE、PoE、2x10G SFP+
C1300-24MGP-4X	Catalyst 1300 シリーズ マネージドスイッチ、8 ポート 2.5GE、16 ポート GE、PoE、4x10G SFP+
C1300-48MGP-4X	Catalyst 1300 シリーズ マネージドスイッチ、16 ポート 2.5GE、32 ポート GE、PoE、4x10G SFP+
C1300-12XT-2X	Catalyst 1300 シリーズ マネージドスイッチ、12 ポート 10GE、2x10G SFP+
C1300-12XS	Catalyst 1300 シリーズ マネージドスイッチ、12 ポート SFP+、2x10GE 共有
C1300-24XT	Catalyst 1300 シリーズ マネージドスイッチ、24 ポート 10GE、4x10G SFP+ 共有

デバイス PID	説明
C1300-24XS	Catalyst 1300 シリーズ マネージドスイッチ、24 ポート SFP+、4x10GE 共有
C1300-16XTS	Catalyst 1300 シリーズ マネージドスイッチ、8 ポート 10GE、8 ポート SFP+
C1300-24XTS	Catalyst 1300 シリーズ マネージドスイッチ、12 ポート 10GE、12 ポート SFP+

- 新しいソフトウェア機能の詳細については、以下を参照してください。
- 既存機能の機能更新の詳細については、以下を参照してください。

新しいソフトウェア機能

すべてのポートで 10G をサポートする 1300 スタッカブルデバイスのサポート

このバージョンでは、すべてのポートで10Gインターフェイスをサポートする Catalyst 1300 スタッカブル マネージド スイッチ シリーズの新しいサブタイプのサポートが追加されました（10G アップリンクポートをサポートする Catalyst 1300 スタッカブルデバイスの既存のサブタイプに加えて）。各サブタイプのデバイスを、他のサブタイプのデバイスと同じスタックにスタックすることはできません。それらを組み合わせてスタックされると、いずれかのサブタイプのユニットがシャットダウンされます。

2 つのサブタイプの機能セットは、次の点を除いて同じです。

- 次の機能は、すべてのポートで10Gインターフェイスをサポートするデバイスのサブタイプでのみサポートされます。
  - 管理用の物理 OOB ポート：IPv4 をサポート
  - IPv6 手動トンネル
  - 自動 6to4 トンネル
  - IPv6 の ISATAP ルーティング
- 2 つのサブタイプは、テーブルサイズ（主にハードウェアリソースに依存する機能について）が異なります。
- スタッキング インターフェイス
  - 10G インターフェイスをサポートするデバイスでは、最大 8 つのスタッキング インターフェイスがサポートされます。任意のインターフェイスをスタッキングインターフェイスとして定義できます。
  - 10G アップリンクポートをサポートするデバイスでは、最大4つのスタッキング インターフェイスがサポートされます。10G アップリンク インターフェイスのみをスタッキング インターフェイスとして定義できます。

PNP エージェントのサポート

スイッチのプラグアンドプレイ（PNP）エージェントは、PNP サーバーと通信します。これにより、設定ファイルとイメージファイルをスイッチに一元的にインストールできます。このため、さまざまな展開シナリオや展開場所でスイッチのゼロタッチインストールを実行できます。PNP 動作により、ネットワーク デバイスの展開/設置に関連するコストを削減するとともに時間を短縮し、セキュリティを損なわずにより簡単に展開できます。

Cisco Business ダッシュボード（CBD）のサポート

Cisco Business ダッシュボード（CBD）は、Cisco Business ダッシュボードマネージャを使用して、シスコネットワークをモニターおよび管理するために役立ちます。Cisco Business ダッシュボードマネージャは、ネットワークを自動的に検出し、シスコのスイッチ、ルータ、ワイヤレスアクセスポイントなど、サポートされているすべてのシスコデバイスを設定およびモニターすることを可能にするアドオンです。

Cisco Business ダッシュボードマネージャは、2 つの個別のコンポーネントまたはアプリケーション（Cisco Business ダッシュボードプローブと呼ばれる 1 つ以上のプローブと、Cisco Business ダッシュボードマネージャと呼ばれる 1 つのマネージャ）から構成される分散アプリケーションです。Cisco Business ダッシュボードプローブのインスタンスは、ネットワークの各サイトにインストールされ、ネットワークを検出し各シスコデバイスと直接通信します。

認証局（CA）証明書マネージャ

Cisco Business ダッシュボードプローブ（CBD）およびプラグアンドプレイ（PNP）機能では、CBD 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 証明書マネージャ機能により、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
- デバイス設定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

HTTPS リダイレクト

スイッチのシステムセキュリティ強化の一環として、管理 GUI にアクセスするユーザーは、サポートされている場合は常に HTTPS を使用する必要があります。HTTPS を確実に使用させるために、デバイスで HTTPS が有効になっている場合、すべての HTTP 要求が HTTPS にリダイレクトされます。

ポート位置情報（ビーコン）

場合によっては、ポート LED を物理外部（デバイスの前面パネル）インジケータとして使用して、デバイス上の単一または複数のインターフェイスを物理的に識別する必要があります。このような状況の例としては、システム管理者が遠隔地におり、オンサイトの設置者またはサポートエンジニアに指示する必要がある場合があります。ポート位置情報/ビーコン機能は、システム管理者が 1 つ以上の指定されたインターフェイス（物理インターフェイスまたは LAG）のインターフェイス LED をアクティブにできるようにすることで、この問題に対処します。

この機能は、CLI を介してのみサポートされます。

err-disable 状態を示すインターフェイス LED の点滅

インターフェイスが err-disable 状態に移行すると、インターフェイス LED がオレンジ色で点滅して、その状態であることを示します。

追加トランシーバのサポート

このバージョンでは、次の SFP/SFP+ トランシーバのサポートが追加されました。

- GLC-EX-SMD
- GLC-ZX-SMD
- CWDM-SFP-1470
- CWDM-SFP-1530
- CWDM-SFP-1610
- SFP-H10GB-ACU7M
- SFP-10G-AOC2M

既存の機能の変更

ここでは、以前のバージョンですでにサポートされていた機能の重要な変更について詳しく説明します。

自動監視 VLAN（ASV）

このバージョンでは、次の 2 つの変更が ASV に導入されました。

- ASV VLAN の ID を変更（CLI コマンド「surveillance-vlan vlan-id」）すると、確認メッセージが表示されます。ユーザーは、変更が必要であることを確認する必要があります。
- ASV を有効にすると、グローバル ブリッジ マルチキャスト フィルタリング設定が自動的に有効になります（以前のバージョンで自動的に有効になっていた IGMP スヌーピングと IGMP スヌーピング クエリアに加えて）。
- 一部の SKU では、ASV エントリは、アクセスモードのポートでも TCAM エントリを消費します（TCAM エントリの使用状況は、コマンド「show system tcam usage」を使用すると表示されます）。以前のバージョンでは、ASV エントリは、インターフェイスが一般モードの場合にのみエントリを消費しました。
- ASV で分類されたトラフィックの CoS アクションが「再マーキング」（remark）に変更されました。これは、パケットの VPT フィールド値が CLI コマンド「surveillance-vlan cos」で定義された値に変更されることを意味します（以前のバージョンでは、CoS アクションは「割り当て」（assign）でした。これは、パケットが、定義された CoS キューに割り当てられるものの、VPT フィールドの値は変更されないことを意味します）。

（注） 再マーキングアクションは TCAM エントリを消費します。これらのエントリは、**show system tcam utilization** コマンドを使用して表示される TCAM エントリに追加されます。

半二重のサポート

上記の表に示されているスイッチの 10G ポートでは、半二重モードはサポートされません。

パスワードの複雑度

次の要件に関して、より寛容な解釈が実装されています。

- 3 つ以上の連続する文字または数字は使用できません。
- 新しいパスワードでは既知のパスワードを使用できません。このリリース（4.1.0.72）では、新しいパスワードの先頭部分のみが既知のパスワードと比較され、中間部分はチェックされません。さらに、この比較には、逆順や、「s」の「$」への、「a」の「@」への、「o」の「0」への、「l」の「1」への、「i」の「!」への、および「e」の「3」への文字の置き換えは含まれません。

チップ保護

「show platform hardware Integrity」コマンドの出力に、観測およびインプリントされた DB ハッシュ値が追加されました。

起動時間の変化

このリリース（4.1.0.72）の起動時間は、以前のリリース（4.0.0.94）と比較して約 27 秒長くなりました。起動時間の増加は、CBD 機能へのサポートの追加によるものです。

既知の問題

リリース V4.1.0.72 で確認された問題。

不具合 ID	説明
CSCwi00331	**症状** 「show dying-gasp packets」コマンドにより、IPv6 syslog および SNMP サーバーに関連する情報が表示されません。 **回避策** なし
CSCwi00359	**症状** スタッキングケーブルを取り外して再接続すると、スタックインターフェイス LED が点灯しないことがあります。 **回避策** なし

不具合 ID	説明
CSCwi00366	**症状** デバイスに設定されているDNSサーバーに既存のホストが到達できない場合、スイッチが、静的DNSエントリを使用してCBDダッシュボードに接続できません。 **回避策** DNS サーバーが到達可能であることを確認するか、静的 DNS エントリが使用されている場合にDNSサーバー設定を削除します。
CSCwi00368	**症状** 光ファイバケーブルを取り外してすぐに再接続すると、1G 光ファイバインターフェイスがリンクアップに失敗することがあります。 **回避策** インターフェイスで shutdown/no shutdown コマンドを使用するか、光ファイバケーブルを SFP といっしょに取り外してから再挿入します。
CSCwi00373	**症状** STP モードが PVST で、STP が無効になっている場合、ループバック検出が失敗します。 **回避策** STP モードを RSTP に変更してから、PVST/RPVST に戻します。
CSCwi00382	**症状** 実際の不整合タイプが「ポートタイプ」であっても、GUI の [PVST Interface Settings] ページに不整合タイプが「PVID」と表示されます。 **回避策** GUI の [PVST Inconsistent Ports] ページには不整合タイプが正しく表示されます。
CSCwi00552	**症状** 不整合タイプが「Port PVID」の場合に、GUI の [PVST Interface settings] ページに空の不整合タイプが表示されます。 **回避策** GUI の [PVST Inconsistent Ports] ページには不整合タイプが正しく表示されます。

不具合 ID	説明
CSCwi00728	**症状** CPU 使用率が自動的に更新されません（GUI の [Status and Statistics] > [CPU Utilization] ページ）。 **回避策** ページを手動で更新します。
CSCwi00748	**症状** 「show lldp local tlvs-overloading」コマンドの出力：「Left」フィールド（TLV のバイト数）に、ローカル TLV でまだ使用可能なバイト数ではなく、オーバーロードされたバイト数が表示されます。 **回避策** MTU 値（1500）から「total」フィールドに表示される値を減算することで、TLV に使用可能なバイト数を計算します。
CSCwi00760	**症状** 次のシナリオで、デバイスコンソールと GUI が約 3 分間応答しません。 • デバイスに設定されている 1 つ以上の DNS サーバーに到達できない。 • この状態で、ユーザーが、デフォルトの SNTP サーバーを削除してから追加する。 **回避策** すべてのインターフェイスで IPv6 を無効にします。
CSCwi00762	**症状** 1G コンボインターフェイスのポート LED が、ポートが err-disable 状態の場合にオレンジ色で点滅しません。 **回避策** インターフェイスがダウン状態に移行すると、これらのポートの LED は消灯します。この場合、CLI または GUI 表示を使用して、このポートが err-disable になっているかどうか（または、切断または手動設定によりダウンしているかどうか）を確認します。

不具合 ID	説明
CSCwi00765	**症状** ボードの再起動時に「Invalid perpetual restart detected, restarting board」という syslog メッセージが表示されることがあります。 **回避策** デバイスの機能に影響はありません（ボードの再起動と無停止型 PoE のサポートは影響を受けません）。
CSCwi00769	**症状** リングトポロジを使用した 6 つ以上のメンバーのスタックで、自動ユニット ID を使用する場合、スタックリンクが Te1-2 と Te3-4 の組み合わせであると、一部のメンバーが常時再起動する可能性があります。この問題が発生した場合、スタック全体を再起動するだけで回復でき、次回の再起動には再発しません。 **回避策** TE1-2 または TE3-4 を使用してスタックネイバーを接続します。ただし、それらを混在させないでください。または、次のいずれかを実行します。 • 固定ユニット ID を使用します。 • チェーントポロジにします。 • スタックをもう一度再起動します。
CSCwi00776	**症状** 「MST インスタンス VLAN マッピング」の VLAN にないポートを、このインスタンスの MST 計算に含めないでください。 **回避策** なし

解決済みの問題

リリース V4.1.0.72 で解決された問題。

不具合 ID	説明
CSCwf56969	**症状** C1200 C1300：DBS-210 での PoE の問題。

不具合 ID	説明
CSCwh21119/CSCwh06683	**症状** STP モードが PVST/RPVST に設定されている場合、802.1x MAC ベースの認証が失敗します。
CSCwh58899	**症状** ファームウェア 4.0.0.93 を実行しているスイッチが、Uboot の [Basic Menu] で [load golden image to factory reset] オプションを実行（CTRL+Shift+6 キーを押し、[Basic Menu] > [1. load golden image to factory reset] を選択）した後に起動に失敗する可能性があります。
CSCwe81251	**症状** ユーザーが CLI を使用して、1 行で 512 文字を超えるログインバナーを設定すると、ウェルカムバナー（GUI で設定された）が消去されます。
CSCwe81247	**症状** GUI で PoE クラスを表示（[Port Management] > [PoE] > [Setting] ページ）すると、クラス 0 PD に関して正しく表示されません。
CSCwe81236	no ipv6 nd hop-limit コマンドを設定すると、エラーメッセージが表示され、設定が受け入れられません。
CSCwi00805	IfTable->ifEntry->ifindex に snmp "ipNetToMediaIfIndex" ifindex 値が存在しません。

はじめに

リリース 4.0.0.93 は、次の製品シリーズをサポートしています。

- Catalyst 1200 シリーズ スマートスイッチ
- Catalyst 1300 シリーズ マネージドスイッチ
- Catalyst 1300 シリーズ スタッカブル マネージド スイッチ

このリリース（4.0.0.93）は、バージョン4.0.0.91 で見つかったバグを修正するメンテナンスリリースです。リリース 4.0.0.91 に新機能は追加されません。

このバージョンには、重要な修正が含まれています。そのため、以前のバージョンを実行しているデバイスをバージョン 4.0.0.93 にアップグレードすることを強くお勧めします。

バージョン 4.0.0.93 から以前のバージョンへのダウングレードはブロックされます。

バージョン 4.0.0.93 で実装されたダウングレード防止により、以前のバージョンからアップグレードする場合は、アクティブなイメージと非アクティブなイメージの両方がアップグレードされます。

⚠

注意 バージョン 4.0.0.93 に適用されたダウングレード防止により、バージョン 4.0.0.93 を実行しているユニットを、以前のバージョンを実行しているスタックに追加すると、バージョンの非互換性が原因で新しいユニットがシャットダウンされます。

この問題を解決するには、4.0.0.93 を実行しているユニットをスタックから切断し、リロードします。次に、既存のスタックをバージョン4.0.0.93にアップグレードしてから、新しいユニットをスタックに追加します。

そのため、新しいユニットを追加する前に、この動作を防ぐために現在のスタックをバージョン 4.0.0.93 にアップグレードすることをお勧めします。

今回のリリースでの新機能

ここでは、このリリースの新機能と変更について詳しく説明します。

リリース 4.0.0.93 は、どのキャパシティでも、リリース 4.0.0.91 を超える追加の機能をサポートしていません。

既知の問題

リリース V4.0.0.93 で確認された問題。

不具合 ID	説明
CSCwh21119	**症状** PVST コマンドが追加されると、MAC 認証が失敗します。 **回避策** PVST/RPVST 以外の STP モードを使用します。

不具合 ID	説明
CSCwh58899	**症状** ファームウェア 4.0.0.93 を実行している C1200/1300 スイッチが、Uboot の [Basic Menu] で [load golden image to factory reset] オプションを実行（CTRL+Shift+6 キーを押し、[Basic Menu] > [1. load golden image to factory reset] を選択）した後に起動に失敗する可能性があります。 （注） [Load golden image to factory reset] オプションはほとんど使用されないため、この問題はユーザーにほとんど影響しません。 スイッチの設定を工場出荷時のデフォルトにリセットするには、リセットボタン、CLI、GUI、またはスタートアップメニューを使用して設定します。 4.1.0.x で修正される予定です。 **回避策** [Load golden image to factory reset] オプションを使用してスイッチをリセットした後にスイッチがこの状態になった場合は、シスコサポートに連絡して支援を依頼してください。 **推奨するアクション**： スイッチのファームウェアバージョンが 4.0.0.93 の場合は、スイッチを工場出荷時の状態にリセットするために [Load golden image to factory reset] オプションを使用しないでください。

解決済みの問題

リリース V4.0.0.93 で解決された問題。

不具合 ID	説明
CSCwh02042	**症状** 非常に低い確率（1/4096）で、起動プロセスがハングし、「hw error」というエラーメッセージがコンソールに表示されます。

Cisco Catalyst 1200 および 1300 シリーズ スイッチ：ファームウェア バージョン 4.0.0.91 リリースノート

2023 年 8 月

このリリースノートでは、Cisco Catalyst 1200 および 1300 シリーズ スイッチのソフトウェア バージョン 4.0.0.91 で推奨される操作と既知の問題について説明します。

新機能

ここでは、このリリースの新機能と変更について詳しく説明します。

ハードウェアコンポーネントの変更

リセットボタン機能

リセットボタン機能は、次のように更新されました。

- システム LED は、通常のデバイスリロードと工場出荷時のデフォルトへのリセットで点滅の仕方が異なります。
  - 通常のデバイスリロード（リセットボタンを押してから 6 ～ 10 秒以内に離す）：システム LED は、それを示すためにゆっくり点滅します。
  - デバイスの工場出荷時のデフォルトへのリセット（リセットボタンを押してから 16 ～ 20 秒以内に離す）：システム LED は、それを示すために素早く点滅します。
- PoE をサポートする SKU でシステム LED を押して 1 ～ 2 秒以内に離すと、次のように状態が示されます。
  - 接続された PD に電力を供給しているポートでは、ポート LED がオレンジ色で 5 秒間点灯します。
  - 接続された PD に電力を供給していないポートでは、ポート LED では 5 秒間何も示されません（LED は消灯します）。

Type-C USB インターフェイス

このデバイスは、デバイスの前面パネルにある Type-C USB インターフェイスをサポートしています。これにより、RJ45 インターフェイスの他に追加のコンソールインターフェイスが提供されます。Type-C USB ベースのコンソールには、次の特性があります。

- このコンソールは、OS の初期化ステージ以降でのみアクティブになります。
- アクティブになっている場合、Type-C USB コンソールが RJ45 コンソールよりも優先されます。
- Type-C USB コンソールは、ボーレート設定に依存しません。

トラステッド プラットフォーム モジュール（TPM）サポート

すべての SKU が、TPM コンポーネントをサポートしています。TPM は、チップガードやブート整合性の可視性などのセキュリティ関連機能に関して、ハードウェアレベルの保護と動作を提供します。このデバイスは、TPM 2.0 仕様をサポートしています。

Bluetooth 管理インターフェイス

現在のバージョンでは、Bluetooth管理インターフェイスのサポートが追加されており、Bluetoothを介したIP接続が可能です。このデバイスのBluetoothを介した管理は、Telnet、SSH、またはHTTP/HTTPS GUIインターフェイスを使用して行われます。

Bluetoothのサポートは、Bluetooth（BT）ドングルをデバイスのUSBポートに接続することによって実現されます。デバイスは、サポートされているBTドングルがデバイスのUSBポートに挿入されたことを自動的に検出し、Bluetoothホストのサポートを提供します。このデバイスは、次のBluetoothドングルをサポートしています。

1. BTD-400 Bluetooth 4.0 アダプタ（Kinivo 社製）
2. Bluetooth 4.0 USB アダプタ（ASUS 社製）
3. Bluetooth 4.0 USB アダプタ（Insignia 社製）
4. Philips 4.0 Bluetooth アダプタ
5. Lenovo LX1815 Bluetooth 5.0 USB アダプタ
6. Lenovo LX1812 Bluetooth 4.0 USB アダプタ

持続性 PoE

永続的なPoE機能（Always-On PoEとも呼ばれます）は、スイッチのステータスに対するPoE動作の依存性を最小限に抑えます。この機能が導入される前は、ソフトウェア関連の再起動などのスイッチ操作で中断が発生すると、デバイスが回復を完了するまで、PoE動作も中断されました。永続的なPoE機能を使用すると、reloadコマンドによって実行されるようなウォームリブートでは、現在の状態でのPoEの動作が中断されることはありません。これにより、スイッチに接続されたPDが継続して動作できます。

自動監視 VLAN（ASV）

多くの場合、カメラや監視機器などの監視デバイス間のネットワーク通信には、より高い優先順位を与える必要があり、組織内の監視インフラストラクチャを構成するさまざまなデバイスが相互に到達可能であることが重要です。

通常、ネットワーク管理者は、すべての監視デバイスが同じVLANに接続されていることを確認し、この優先度の高いトラフィックを許可するようにこのVLANとそのインターフェイスを設定する必要があります。

自動監視VLAN（ASV）機能は、ネットワーク上の監視デバイスを検出してVLANに割り当て、それらのトラフィックの優先順位を設定することにより、このセットアップを自動化します。

MSTP の機能拡張

このリリースでは、次のMSTP関連の機能拡張が追加されました。

- Catalyst 1300 製品ラインは 16 のインスタンスをサポートしています。
- MSTP インスタンス ID の範囲は 0 ～ 4094 です。

MSTPインスタンスIDに0 ～ 4094の範囲のサポートを許可するには、ユーザーがMSTPインスタンスを作成し、インスタンスIDを割り当てる必要があります。インスタンスIDが作成さ

れると、ユーザーは、作成されたインスタンスにVLANをマッピングできます（以前のリリースでは、VLANをインスタンスにマッピングする前にインスタンスを作成する必要はありませんでした）。

パスワードエージングの機能拡張

パスワードエージングにより、管理者は、事前定義された期間の経過後にパスワードを強制的に変更できます。現在のバージョンでは、次の機能拡張が追加されました。

- レベル 15 のユーザのみがパスワードを変更できます。レベル 1 のユーザーには、（予期される）パスワードの有効期限に関する通知が表示されますが、パスワードを変更する権限はありません。
- 有効期限までの期間（パスワードの有効期限までの10日間）：ログイン時に（レベル15）ユーザーにパスワードを変更するオプションが表示されます。ユーザーは、このオプションを拒否する（その場合、ログインできます）か、提案を受け入れる（その場合、パスワードをすぐに変更できます）ことが可能です（以前のバージョンでは、ユーザーは、ログインしてから、関連する設定モードを開始する必要がありました）。

構成証明の証明書およびキーペア（AIK）のサポート

証明書およびキーペアは、さまざまなデバイス情報を検証し、セキュリティ関連情報（チップガードやブート整合性の可視性など）を表示するコマンドの出力に署名するために使用されます。

現在のバージョンでは、追加の証明書およびキーペアのサポートが追加されました。これは、構成証明の証明書およびキーペア（「構成証明アイデンティティキー」（AIK）とも呼ばれます）です。AIK 証明書を使用した操作はトラステッド プラットフォーム モジュール（TPM）内に限定されるため、構成証明の証明書およびキーは SUDI の証明書およびキーよりも安全であると見なされます。これにより、署名された情報の有効性の信頼度が高まります。

ブート整合性の可視性（BIV）

ブート整合性の可視性（BIV）機能によって、プラットフォームのソフトウェアの整合性情報が可視化され、実用可能になります。ソフトウェアの整合性ではブート整合性の測定値が明らかになり、それを使用してプラットフォームが信頼できるコードを起動および実行しているかどうかを評価できます。Catalyst 1200 および 1300 製品ラインの BIV は、TPM コンポーネントの機能を利用します。

ブートプロセス中に、ソフトウェアは、ブートステージに関連するさまざまなイメージのハッシュレコードを作成します。測定値の整合性を確保するために、測定値は、TPM と呼ばれるハードウェアで保護されたコンポーネントに保存され、PCR（プラットフォーム設定レジスタ）に拡張されます。ユーザーは、これらのレコードを取得（CLI コマンドを使用します）し、シスコが保持している既知の適正な値（KGV）のレコードと比較できます。値が一致しない場合、デバイスは、シスコによって認定されていない、または未承認パーティによって改ざんされているソフトウェアイメージを実行している可能性があります。

CLI コマンドを使用すると、ブートローダおよびイメージ全体のハッシュ測定値と PCR 見積を表示できます。必要に応じて、SUDI キーまたは構成証明キーを使用してこの情報に署名することもできます。

（注） BIV機能は、ユーザーが操作したり、変更を受け入れなくても、そのままで機能しますが、エンドユーザーがこれを確認する必要がある場合にユーザーを支援するオプションがまもなく提供される予定です。

チップガードの機能拡張

現在のバージョンでは、次の機能拡張が追加されました。

- チップガード情報を表示する CLI コマンドのサポート。
- コマンド出力に署名するための構成証明の証明書およびキーのサポート。

デバッグアクセス用のランダムトークン

- 特定のデバッグインターフェイス（Linux シェルなど）は機密性が高かったり、デバイスの動作を中断させる可能性があったりするため、昇格されたアクセス制御および検証が必要です。
- 現在のバージョンでは、そのようなデバッグインターフェイスにアクセスしようとするたびにランダムなチャレンジを生成し、そのチャレンジに基づいてパスワードの入力を求めるプロンプトを表示することによって、拡張された要件に対応します。
- このインターフェイスにアクセスするには、シスコが管理する専用のキーでチャレンジに署名する必要があります。

Dying Gasp

Dying Gasp機能は、ハードウェア障害（電源の切断または中断）によってデバイスで予期しない電力損失が発生していることをモニターシステムに警告するメカニズムを提供します。

電源喪失イベントが発生すると、ハードウェアコンデンサがデバイスのシャットダウンを短時間遅らせます。この間に、デバイスは Dying Gasp メッセージを送信します。メッセージは、SNMP サーバー（通知として）または syslog サーバーに送信できます。

この機能は、1300製品ライン（スタンドアロンおよびスタッキング）でのみサポートされています。1200 製品ラインではサポートされていません。

ゴールデンイメージのサポート

- 現在のバージョンでは、ゴールデンイメージのサポートが追加されました。
- ゴールデンイメージは実稼働レベルのイメージであるため、広範なテストサイクルが実施されています。
- 現在のソフトウェアが破損しており、ロードされない場合、デバイスは、ゴールデンイメージをフォールバックイメージとして自動的にロードします。これにより、そのようなユニットの RMA の必要がなくなる可能性があります。ゴールデンイメージをロードすると、デバイス設定が消去される可能性があります。
- ゴールデンイメージは、製造プロセスの一部としてデバイスのフラッシュに書き込まれます。ユーザーには、ゴールデンイメージのバージョンを更新するオプションはありませ

ん。場合によっては（セキュアブートキーの失効など）、通常のイメージ更新の一部としてゴールデンイメージが更新されます。

デバイスを工場出荷時のデフォルトにリセットする CLI コマンド

CLI コマンドを使用すると、スイッチを再起動するだけでなく、スイッチを工場出荷時のデフォルトにリセットすることもできます。詳細については、スタンドアロンおよびスタッカブルスイッチの詳細なコマンドに関する CLI ガイドを参照してください。

SSL および SSH のサポート

現在のリリースでは、以下の変更が導入されました。

- TLS 1.2 のセキュアなクライアントが開始する再ネゴシエーションが無効になっています。
- サポートされている OpenSSL バージョン：1.1.1q
- サポートされている OpenSSH バージョン：バージョン 7.3p1（以前のバージョンへの変更なし）

既知の問題

リリース V4.0.0.91 で確認された問題。

不具合 ID	説明
CSCwe81236	**症状** no ipv6 nd hop-limit コマンドを設定すると、エラーメッセージが表示され、設定が受け入れられません。 **回避策** インターフェイス上の IPv6 を無効にします。
CSCwe81238	**症状** STP モードが PVST/RPVST に設定されている場合、自動監視 VLAN（ASV）は一般モードのポートでアクティブになりません。 **回避策** インターフェイスで ASV をアクティブにするには、ASV VLAN を無効にしてから再度有効にするか、STP モードを STP/RSTP に変更してから PVST/RPVST に戻します。
CSCwe81247	**症状** ポートがクラスモードに設定されている場合、GUI で PoE クラスを表示（[Port Management] > [PoE] > [Setting]）すると、クラス 0 PD に関して正しく表示されません。 **回避策** CLI を使用してクラス情報を確認します。

不具合 ID	説明
CSCwe81251	**症状** ユーザーが CLI を使用して、1 行で 512 文字を超えるログインバナーを設定すると、ウェルカムバナー（GUI で設定された）が消去されます。 **回避策** なし
CSCwe81253	**症状** 認証またはログインのデフォルト方式のリストが更新されると、Syslog メッセージが重複します。 **回避策** なし
CSCwe81254	**症状** DHCP プール名に特殊文字（一重引用符、二重引用符、バックスラッシュなど）が含まれており、ユーザーが [IPv4 Configuration] > [DHCP Server] > [Network Pools] GUI ページで [Details] ボタンをクリックすると、エラーメッセージがコンソールに表示されます。 **回避策** 機能に影響はなく、回避策はありません。
CSCwe84307	**症状** C1200/C1300：非 PoE デバイスが接続されている場合、PoE ポートが障害ステータスになります。 **回避策** **power inline never** コマンドを PoE インターフェイスに適用して、ポートの PoE を無効にします。
CSCwf56969	**症状** C1200 C1300：DBS-210 での PoE の問題 **回避策** 回避策はありません。
CSCwe81260	**症状** 先行標準の PD が、POE バジェット不足により、電源拒否状態を終了できません。 **回避策** 問題のあるポートで POE を無効にしてから有効にします。

不具合 ID	説明
CSCwe81261	**症状** 負荷が通常状態まで低下した後でも、POE ポートが過負荷状態から回復できないことがあります。 **回避策** 問題のあるポートで POE を無効にしてから有効にします。