Catalyst 4500 シリーズスイッチ Cisco IOS リリース12.2(54)SGx および 12.2(53)SGx リリースノート

現在のリリース
12.2(53)SG11：2014 年 8 月 18 日

以前のリリース
12.2(54)SG1、12.2(54)SG、12.2(53)SG10、12.2(53)SG9、12.2(53)SG8、12.2(53)SG7、12.2(53)SG6、12.2(53)SG5、12.2(53)SG4、12.2(53)SG3、12.2(53)SG2、12.2(53)SG1、12.2(53)SG、12.2(52)XO、12.2(52)SG、12.2(50)SG8、12.2(50)SG7、12.2(50)SG6、12.2(50)SG5、12.2(50)SG4、12.2(50)SG3、12.2(50)SG2、12.2(50)SG1、12.2(50)SG、12.2(46)SG、12.2(44)SG1、12.2(44)SG、12.2(40)SG

これらのリリース ノートでは、Catalyst 4500 シリーズ スイッチ上の Cisco IOS ソフトウェアの機能、変更点、および警告について説明します。最新のソフトウェアリリースは、Cisco IOS リリース 12.2(54)SG です。

デフォルトイメージである Cisco IOS ソフトウェアリリース 12.2(54)SG のサポートは、次の URL で入手可能な標準の Cisco Systems® サポートポリシーに従います。
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

注 リリースノートは固有で、4 つのプラットフォーム（Catalyst 4500、Catalyst 4900、Catalyst ME 4900、および Catalyst 4900M）ごとに存在しますが、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ガイド、およびシステムメッセージガイドは共通しています。

Catalyst 4500 シリーズ スイッチの詳細については、次の URL を参照してください。

http://www.cisco.com/go/cat4500/docs

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

目次

このマニュアルの内容は、次のとおりです。

Cisco Catalyst 4500 シリーズ向け Cisco IOS ソフトウェア パッケージ

Cisco Catalyst 4500 シリーズ スイッチ向けの新しい Cisco IOS ソフトウェアパッケージは、Cisco IOS ソフトウェアリリース 12.2(25)SG で導入されました。このソフトウェア パッケージは機能の新しい基盤となり、すべての Cisco Catalyst スイッチにおける一貫性を維持します。新しい Cisco IOS ソフトウェア リリース トレインは、12.2SG として指定されています。

以前の Cisco Catalyst 4500 シリーズ スイッチの Cisco Catalyst 4500 シリーズ IOS ソフトウェア イメージ（以前は Basic Layer 3 および Enhanced Layer 3）は、IP Base および Enterprise Services にそれぞれマッピングされます。Cisco IOS ソフトウェアに基づき現在出荷されているすべての Cisco Catalyst 4500 ソフトウェア機能は、一部の例外を除き、リリース 12.2(54)SG の IP Base イメージでサポートされています。

IP Base イメージは、NSF/SSO、BGP、EIGRP、EIGRPv6、OSPF、OSPFv3、IS-IS、Internetwork Packet Exchange（IPX）、AppleTalk、VRF-Lite、およびポリシーベースルーティング（PBR）などの拡張ルーティング機能をサポートしていません。IP Base イメージは、Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、V-10GE、および 6-E での限定ルーティング用の EIGRP スタブをサポートします。

Enterprise Services イメージは、拡張ルーティングなどの Cisco IOS ソフトウェアに基づくすべての Cisco Catalyst 4500 シリーズ ソフトウェア機能をサポートします。Supervisor Engine IV、V、または V-10GE で BGP を有効にする予定のお客様は、BGP が Enterprise Services パッケージに含まれているため、個別の BGP ライセンス（FR-IRC4）を購入する必要がなくなります。12.2(53)SG2 以降では、Supervisor Engine 6L-E で Enterprise Services イメージをサポートしています。

Cisco IOS リリース 12.2（46）SG1 には、新しい LAN Base ソフトウェアと IP アップグレードイメージが含まれています。これらのイメージにより、既存の IP Base イメージおよび Enterprise Services イメージが補完されます。LAN Base イメージは、Supervisor Engine II-Plus-10GE および Supervisor Engine 6L-E からサポートされています。Cisco IOS リリース 12.2(52)XO。LAN Base イメージは主にお客様のアクセスとレイヤ 2 に重点を置いているため、多くの IP Base の機能は必要ありません。後日、これらの機能の一部が必要になった場合は、IP アップグレードイメージを使用できます。

表 1 表 1 には、LAN Base イメージと IP Base イメージのサポート機能の対比が示されています。MIB のサポートについては、次の URL を参照してください。
http://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html

表 1　　LAN Base/IP Base イメージのサポート

機能	LAN ベース	IP Base	エンタープライズサービス
10G アップリンクの使用	12.2(46)SG1	対応	対応
802.1p による優先順位付け	12.2(46)SG1	対応	対応
802.1p/802.1q	12.2(46)SG1	対応	対応
802.1w/802.1s	12.2(46)SG1	対応	対応
802.1X（ゲスト VLAN および VLAN 割り当てあり）	12.2(50)SG	対応	対応
ACL 割り当てを使用した 802.1X および MAB	12.2(50)SG	対応	対応
802.1X（認証失敗 VLAN、クリティカル認証、アカウンティング）	12.2(50)SG	対応	対応
802.1X Wake on LAN	12.2(50)SG	対応	対応
802.1X Web 認証	12.2(50)SG	対応	対応
複数の認証済みマルチホストでの 802.1X	12.2(50)SG	対応	対応
MDA を使用した 802.1X	12.2(50)SG	対応	対応
オープンアクセスを使用した 802.1X	12.2(50)SG	対応	対応
802.3ad LACP	12.2(46)SG1	対応	対応
802.3x：フロー制御	12.2(46)SG1	対応	対応
ACL ロギング	12.2(46)SG1	対応	対応
すべての MIB	12.2(52)SG	対応	対応
自動 QoS	12.2(53)SG	対応	対応
Auto SmartPort	12.2(54)SG	対応	対応
Auto-MDIX	12.2(46)SG1	対応	対応
自動音声 VLAN（AutoQoS の一部）	サポートなし	対応	対応
BOOTP	12.2(46)SG1	対応	対応
ブートアップ GOLD	サポートなし	対応	対応
ブロードキャストの抑制	12.2(46)SG1	対応	対応

表 1　　LAN Base/IP Base イメージのサポート(続き)

機能	LAN ベース	IP Base	エンタープライズサービス
CDP/CDPv2	12.2(46)SG1	対応	対応
コミュニティ PVLAN のサポート	サポートなし	対応	対応
Config File	12.2(46)SG1	対応	対応
コンソールアクセス	12.2(46)SG1	対応	対応
コントロール プレーン ポリシング	12.2(46)SG1	対応	対応
Copy コマンド	12.2(46)SG1	対応	対応
CoS から DSCP へのマップ	対応	対応	対応
debug コマンド	12.2(46)SG1	対応	対応
デバイス管理	12.2(46)SG1	対応	対応
DHCP サーバ	12.2(46)SG1	対応	対応
DHCP スヌーピング	12.2(46)SG1	対応	対応
診断ツール	12.2(46)SG1	対応	対応
ソフトウェアのダウンロード	12.2(46)SG1	対応	対応
DSCP から CoS へのマップ	12.2(46)SG1	対応	対応
DSCP から出力キューへのマッピング	12.2(46)SG1	対応	対応
ダイナミック ARP インスペクション	12.2(46)SG1	対応	対応
EEM と EOT の統合	サポートなし	対応	対応
EIGRP Stub	サポートなし	対応	対応
EnergyWise 1.0	12.2(53)SG	対応	対応
EPoE	12.2(53)SG	対応	対応
イーサネット管理ポート(Fa1 インターフェイス)	12.2(46)SG	対応	対応
イベント ログ	12.2(46)SG1	対応	対応
工場出荷時設定	12.2(46)SG1	対応	対応
ファイル管理	12.2(46)SG1	対応	対応
Flex Link	12.2(53)SG	対応	対応
GLBP	サポートなし	対応	対応
HSRPv1/VRRP	サポートなし	対応	対応

表 1　　LAN Base/IP Base イメージのサポート(続き)

機能	LAN ベース	IP Base	エンタープライズサービス
HSRP v2 IPV4	サポートなし	対応	対応
HSRP v2 IPV6	サポートなし	いいえ	はい
ID 4.0 音声 VLAN 割り当て	12.2(46)SG1	対応	対応
ID 4.1 フィルタ ID と従量制 ACL	12.2(46)SG1	対応	対応
IGMP	12.2(46)SG1	対応	対応
IGMP スヌーピング	12.2(46)SG1	対応	対応
入力ポリシング	12.2(46)SG1	対応	対応
インターフェイスアクセス(Telnet、コンソール/シリアル、Web)	12.2(46)SG1	対応	対応
IP ソース ガード	12.2(46)SG1	対応	対応
IP Multicast:IP マルチキャスト	サポートなし	対応	対応
IPv6 ホット スタンバイ ルータ プロトコル(HSRP)	サポートなし	いいえ	はい
IPv6 MLD スヌーピング V1 および V2	将来的にサポート	対応	対応
IPv6 の再編成	NA	対応	対応
IPv6 ルータ アドバタイズメント(RA)ガード	12.2(54)SG	対応	対応
ISL Trunk	12.2(46)SG1	対応	対応
ISSU	サポートなし	対応	対応
ジャンボ フレーム	12.2(46)SG1	対応	対応
レイヤ 2 デバッグ	12.2(46)SG1	対応	対応
レイヤ 2 PT および QinQ	サポートなし	対応	対応
レイヤ 2 Traceroute	12.2(46)SG1	対応	対応
リンクステート トラッキング	12.2(54)SG	対応	対応
LLDP/LLDP-MED	12.2(52)SG	対応	対応
LLDP の拡張機能(PoE+ レイヤ 2 CoS)	12.2(54)SG	いいえ	はい
ローカル Web 認証	12.2(52)SG	対応	対応
MAB(MAC 認証バイパス)	12.2(50)SG	対応	対応
MAC アドレスのフィルタリング	12.2(50)SG	対応	対応

表 1　　LAN Base/IP Base イメージのサポート(続き)

機能	LAN ベース	IP Base	エンタープライズサービス
MAC ベースのアクセスリスト	12.2(50)SG	対応	対応
管理 IPv6 ポート	12.2(52)SG	対応	対応
MLD スヌーピング	12.2(53)SG	対応	対応
マルチキャスト フィルタ処理	12.2(46)SG1	対応	対応
マルチホップ SXP（CTS）	サポートなし	12.2(52)SG	対応
Network Edge Access Topology（NEAT）	サポートなし	対応	対応
QoS フィルタの数 セキュリティ ACE の数	○（4K エントリ）	対応	対応
VLAN のサポートの数	2048	4096	対応
ルーテッド アクセスの OSPF	サポートなし	対応	対応
PAgP	12.2(46)SG1	対応	対応
パスワード パスワードクリアの防止	12.2(46)SG1	対応	対応
PIM SM/DM	サポートなし	対応	対応
PoE（最大 15.4W まで）	12.2(46)SG1	対応	対応
PoE+ 対応	対応	対応	対応
ポートモニタリング（インターフェイス統計情報）	12.2(46)SG1	対応	対応
ポート セキュリティ	12.2(46)SG1	○（1024 個の MAC のみ）	対応
投稿ステータス	12.2(46)SG1	対応	対応
PVST+	12.2(53)SG	対応	対応
Q-in-Q	サポートなし	対応	対応
RACL（DSCP ベース）	12.2(46)SG1	対応	対応
RADIUS/TACACS+（AAA）	12.2(46)SG1	対応	対応
RMON	12.2(46)SG1	対応	対応
ルーティング、スタティック	12.2(46)SG1	対応	対応
RIP	いいえ	対応	対応
RPR	12.2(46)SG1	対応	対応

表 1　　LAN Base/IP Base イメージのサポート(続き)

機能	LAN ベース	IP Base	エンタープライズサービス
RPVST+	12.2(53)SG	対応	対応
RSPAN	12.2(46)SG1	対応	対応
Service Advertisement Framework（SAF）	サポートなし	いいえ	はい
Smart Call Home	サポートなし	対応	対応
SmartPorts（ロールベースのマクロ）	12.2(53)SG	対応	対応
SNMP（SNMPv3 を含む）	12.2(46)SG1	対応	対応
送信元ポートフィルタリング（プライベート VLAN）	12.2(46)SG1	対応	対応
SPAN（セッションの数）：ポートミラーリング	12.2(46)SG1（2 セッション）	○（8 双方向セッション）	対応
SSHv2/セキュアコピー、FTP、SSL、Syslog、Sys 情報	12.2(46)SG1	対応	対応
ストーム制御	12.2(46)SG1	対応	対応
TDR	サポートなし	対応	対応
タイムプロトコル（SNTP、TimeP）	12.2(46)SG1	対応	対応
タイムプロトコル（SNTP、TimeP）プライマリ（旧称 タイムプロトコル（SNTP、TimeP）マスター）	12.2(52)SG	対応	対応
時間ベースの ACL	12.2(46)SG1	対応	対応
トラフィックミラーリング（SPAN）	12.2(46)SG1	対応	対応
信頼境界（LLDP および CDP ベース）	12.2(46)SG1	対応	対応
UDLD	12.2(46)SG1	対応	対応
VACL および PACL	12.2(46)SG1	対応	対応
VLAN マッピング（VLAN 変換）	12.2(54)SG	対応	対応
音声 VLAN	12.2(46)SG1	対応	対応
VRRP	サポートなし	対応	対応
VTP	12.2(46)SG1	対応	対応
WCCP	サポートなし	対応	対応
XML-PI	12.2(54)SG	対応	対応

発注可能な製品番号:

- S49LB-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(LAN Base イメージ)
- S49LBK9-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(トリプル DES を使用した LAN Base イメージ)
- S49IPB-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(IP Base イメージ)
- S49IPBK9-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(トリプル DES を使用した IP Base イメージ)
- S49ES-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(BGP サポート付き Enterprise Services イメージ)
- S49ESK9-12254SG(=):Cisco Catalyst 4500 シリーズ スイッチ用の Cisco IOS ソフトウェア(3DES および BGP サポート付き Enterprise Services イメージ)
- S45ES-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine IV、V、およびV-10GE 用 の Cisco IOS ソフトウェア(ボーダー ゲートウェイ プロトコル(BGP)をサポートする Enterprise Services イメージ、暗号化なし)
- S45IPBK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア(トリプル DES(3DES)を使用した IP Base イメージ)
- S45IPB-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア(IP Base イメージ、暗号化なし)
- S45ESK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア(3DES および BGP をサポートする Enterprise Services イメージ)
- S45LB-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus-10GE 用の Cisco IOS ソフトウェア(LAN Base イメージ)
- S45LBK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus-10GE 用の Cisco IOS ソフトウェア(3DES を使用した LAN Base イメージ)
- S45IPBU-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus-10GE 用の Cisco IOS ソフトウェア(IP Base アップグレードイメージ)
- S45IPBUK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine II-Plus-10GE 用の Cisco IOS ソフトウェア(3DES を使用した IP Base アップグレードイメージ)
- S45EES-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア(Enterprise Services イメージ)
- S45EESK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア(3DES を使用したEnterprise Services イメージ)
- S45EIPB-12253SG:Cisco Catalyst 4500 Supervisor Engine 6-E および 6L-E 用の Cisco IOS ソフトウェア(IP Base イメージ)
- S45EIPBK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E および 6L-E 用の Cisco IOS ソフトウェア(3DES を使用した IP Base イメージ)
- S45ELB-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア(LAN Base イメージ)
- S45ELBK9-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア(3DES を使用した LAN Base イメージ)
- S45EIPBU-12253SG:Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア(IP Base アップグレードイメージ)

- S45EIPBUK9-12253SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base アップグレードイメージ）
- S45ELB-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（LAN Base、暗号化なし）
- S45ELBK9-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した LAN Base イメージ）
- S45EIPB-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号化なし）
- S45EIPBK9-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）
- S45EIPBU-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（IP アップグレードイメージ、暗号化なし）
- S45EIPBUK9-12252X0：Catalyst 4500 Sup 6L-E 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP アップグレードイメージ）
- S45IPB-12252SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号なし）（cat4500-ipbase-mz）
- S45IPBK9-12252SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45ES-12252SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（BGP をサポートする Enterprise Services イメージ、暗号化なし）（cat4500-entservices-mz）
- S45ESK9-12252SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（3DES および BGP をサポートする Enterprise Services イメージ）（cat4500-entservicesk9-mz）
- S45EIPB-12252SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）
- S45EIPBK9-12252SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45EES-12252SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45EESK9-12252SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45IPB-12250SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号化なし）（cat4500-ipbase-mz）
- S45IPBK9-12250SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45ES-12250SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（BGP をサポートする Enterprise Services イメージ、暗号化なし）（cat4500-entservices-mz）
- S45ESK9-12250SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（3DES および BGP をサポートする Enterprise Services イメージ）（cat4500-entservicesk9-mz）

- S45EIPB-12250SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）
- S45EIPBK9-12250SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）（ccat4500-ipbasek9-mz）
- S45EES-12250SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45EESK9-12250SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45IPB-12246SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号化なし）（cat4500-ipbase-mz）
- S45IPBK9-12246SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45ES-12246SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（BGP をサポートする Enterprise Services イメージ、暗号化なし）（cat4500-entservices-mz）
- S45ESK9-12246SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（3DES および BGP をサポートする Enterprise Services イメージ）（cat4500-entservicesk9-mz）
- S45EIPB-12246SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）
- S45IPBK9-12246SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45EES-12246SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45EESK9-12246SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45IPB-12244SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号化なし）（cat4500-ipbase-mz）
- S45IPBK9-12244SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45ES-12244SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（BGP をサポートする Enterprise Services イメージ、暗号化なし）（cat4500-entservices-mz）
- S45ESK9-12244SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（3DES および BGP をサポートする Enterprise Services イメージ）（cat4500-entservicesk9-mz）
- S45EIPB-12244SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）
- S45IPBK9-12244SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45EES-12244SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）

- S45EESK9-12244SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500-ipbasek9-mz）
- S45IPB-12240SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（IP Base イメージ、暗号化なし）（cat4500-ipbase-mz）
- S45IPBK9-12240SG：Catalyst 4500 シリーズ Supervisor Engine II-Plus、II-Plus-TS、II-Plus-10GE、IV、V、および V-10GE 用の Cisco IOS ソフトウェア（トリプル DES（3DES）を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45ES-12240SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（BGP をサポートする Enterprise Services イメージ、暗号化なし）（cat4500-entservices-mz）
- S45ESK9-12240SG：Catalyst 4500 シリーズ Supervisor Engine IV、V、および V-10GE 用の Cisco IOS ソフトウェア（3DES および BGP をサポートする Enterprise Services イメージ）（cat4500-entservicesk9-mz）
- S45EIPB-12240SG：Cisco Catalyst 4500 シリーズ Supervisor Engine 6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）
- S45IPBK9-12240SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）（cat4500-ipbasek9-mz）
- S45EES-12240SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（Enterprise Services イメージ）（cat4500e-entservices-mz）
- S45EESK9-12240SG：Catalyst 4500 シリーズ Supervisor Engine 6-E 用の Cisco IOS ソフトウェア（3DES イメージを使用した Enterprise Services）（cat4500-entservicesk9-mz）

Catalyst 4500 シリーズ スイッチ Cisco IOS のリリース戦略

Cisco IOS Release 12.2SG トレインでは、Catalyst 4500 シリーズ スーパバイザ エンジンの最新の機能が提供されています。Catalyst 4500 シリーズのスーパバイザエンジンをお使いで、最新のハードウェアサポートおよびソフトウェア機能が必要なお客様は、Cisco IOS リリース 12.2(54)SG に移行する必要があります。

注 Cisco IOS の改良に対する取り組みの中で、Cisco IOS Releases 12.2EW と 12.2SG は、名前が変更されただけで同じリリース トレインです。

Catalyst 4500 シリーズには、3 つのメンテナンストレインがあります。Cisco IOS リリース 12.2(31)SGA トレインは、最も長く使用されているトレインです。現時点では、Cisco IOS リリース 12.2(31)SGA8 が、メンテナンストレインを含むリリースを必要とするお客様に推奨されるリリースです。CiscoIOS リリース 12.2(53)SG は、最新のメンテナンストレインであり、ルーテッドアクセス用の WS-X45-Sup6L-E スーパバイザエンジンおよび OSPF のサポートなどの最新機能が含まれています。

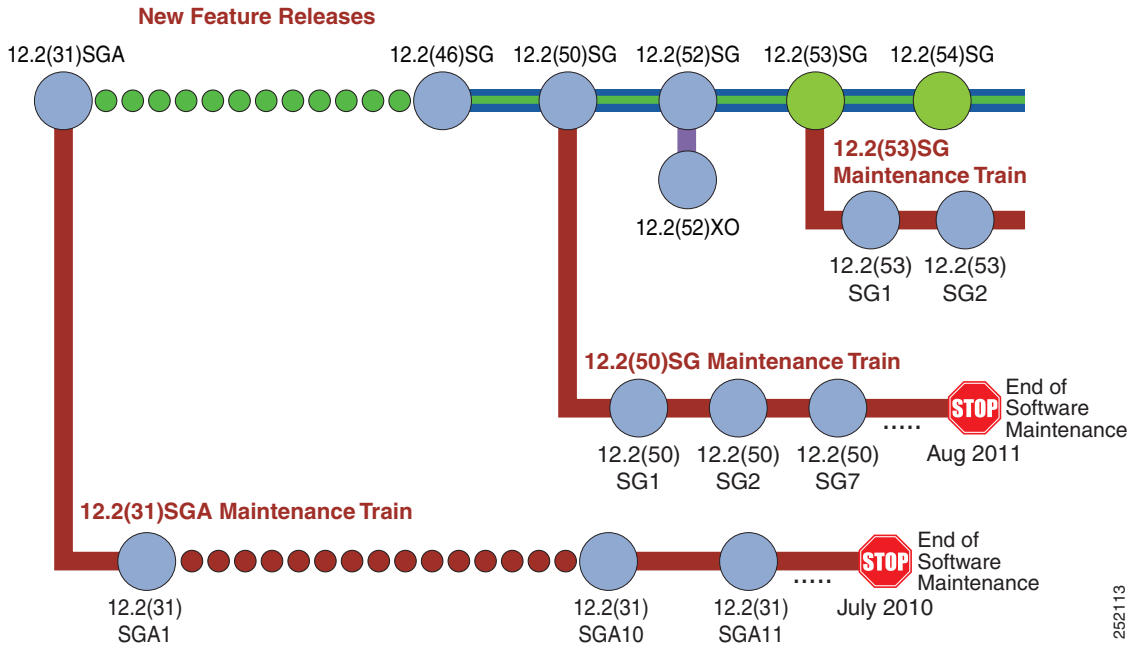
Catalyst 4500 シリーズ スイッチの詳細については、次の URL を参照してください。

http://www.cisco.com/go/cat4500/docs

Cisco IOS ソフトウェア移行ガイド

図 1 は、2 つのアクティブな 12.2(31)SGA と 12.2(50)SG、および新しく導入された 12.2(53)SG 拡張メンテナンストレインを示しています。

図 1　　Catalyst 4500 シリーズ スイッチ用ソフトウェア リリース戦略



移行計画の概要

- 最新の Cisco Catalyst 4500 シリーズのハードウェアおよびソフトウェア機能が必要なお客様は、Cisco IOS ソフトウェアリリース 12.2(54)SG に移行する必要があります。
- Cisco IOS ソフトウェアリリース 12.2(31)SGA および 12.2(50)SG は、継続してメンテナンスリリースを提供します。12.2(31)SGA メンテナンストレインの最新リリースは、12.2(31)SGA10 です。12.2(50)SG メンテナンストレインの最新リリースは、12.2(50)SG4 です。

サポート

Cisco IOS ソフトウェアリリース 12.2(54)SG のサポートは、次の URL で入手可能な標準の Cisco Systems® サポートポリシーに従います。
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

システム要件

ここでは、システム要件について説明します。

Catalyst 4500 シリーズ スイッチでサポートされているハードウェア

表 2 に、Catalyst 4500 シリーズ スイッチでサポートされているハードウェアのリストを示します。

表 2　　サポート対象ハードウェア

製品番号（スペアには「=」を追加）	製品の説明	ソフトウェア リリース
		最小
スーパバイザ エンジン		
WS-X4013+=	Catalyst 4500 シリーズ スイッチ Supervisor Engine II-Plus 注　このエンジンは、3、6、および 7 スロットシャーシでのみサポートされます（10 スロットシャーシではサポートされません）。	12.1(19)EW
WS-X4013+TS	Catalyst 4500 シリーズ スイッチ Supervisor Engine II-Plus-TS 注　このエンジンは、3 スロットシャーシでのみサポートされます。	12.2(20)EWA
WS-X4013+10GE	Catalyst 4500 シリーズ スイッチ Supervisor Engine II-Plus-10GE 注　このエンジンは、3、6、および 7 スロットシャーシでのみサポートされます（10 スロットシャーシではサポートされません）。	12.2(25)SG
WS-X4515=	Catalyst 4500 シリーズ スイッチ Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R シリーズ スイッチ Redundant Supervisor Engine IV	12.1(12c)EW
WS-X4516=	Catalyst 4500 シリーズ スイッチ Supervisor Engine V	12.2(18)EW
WS-X4516/2=	Catalyst 4507R シリーズ スイッチ Redundant Supervisor Engine V	12.2(18)EW
WS-X4516-10GE=	Catalyst 4500 シリーズ スイッチ Supervisor Engine V-10GE	12.2(25)EW
WS-X45-Sup6-E	Catalyst 4500 E シリーズ スイッチ Supervisor Engine 6-E 注　このエンジンは、レガシーシャーシと E シリーズ シャーシでサポートされます。	12.2(40)SG
WS-X45-Sup6L-E	Catalyst 4500 E シリーズ スイッチ Supervisor Engine 6L-E 注　このエンジンは、レガシーシャーシと E シリーズの 3、6、および 7 スロットシャーシでサポートされます。	12.2(52)XO
ギガビット イーサネット スイッチング モジュール		
WS-X4302-GB	2 ポート 1000BASE-X（GBIC）ギガビット イーサネット モジュール	12.1(19)EW
WS-X4306-GB	6 ポート 1000BASE-X（GBIC）ギガビット イーサネット スイッチング モジュール	12.1(8a)EW

表 2　　サポート対象ハードウェア(続き)

製品番号(スペアには「=」を追加)	製品の説明	ソフトウェア リリース
		最小
WS-X4418-GB	18 ポート 1000BASE-X(GBIC)ギガビット イーサネット サーバ スイッチング モジュール	12.1(8a)EW
WS-X4412-2GB-T	12 ポート 1000BASE-T ギガビット イーサネットおよび 2-GBIC ポート スイッチング モジュール 2 個	12.1(8a)EW
WS-X4424-GB-RJ45	24 ポート10/100/1000BASE-T ギガビット イーサネット RJ-45 スイッチング モジュール	12.1(8a)EW
WS-X4448-GB-LX	48 ポート 1000BASE-LX(Small Form-Factor Pluggable)ギガビット イーサネット 光ファイバ インターフェイス スイッチング モジュール	12.1(8a)EW
WS-X4448-GB-RJ45	48 ポート 10/100/1000BASE-T ギガビット イーサネット スイッチング モジュール	12.1(8a)EW
WS-X4448-GB-SFP	48 ポート 1000BASE-X(Small Form-Factor Pluggable)モジュール	12.2(20)EW
WS-X4506-GB-T	6 ポート 有線 10/100/1000BASE-T Catalyst 4500 シリーズ Power over Ethernet(PoE)802.3af または 1000BASE-X SFP	12.2(20)EWA
WS-X4524-GB-RJ45V	24 ポート 10/100/1000BASE-T RJ-45 Catalyst 4500 シリーズ PoE 802.3af	12.2(18)EW
WS-X4548-GB-RJ45	48 ポート 10/100/1000BASE-T ギガビット イーサネット モジュール	12.1(19)EW
WS-X4548-GB-RJ45V	48 ポート 10/100/1000BASE-T RJ-45 Catalyst 4500 シリーズ PoE 802.3af	12.2(18)EW
WS-X4548-RJ45V+	48 ポート 10/100/1000 プレミアム PoE ラインカード	12.2(50)SG
WS-X4624-SFP-E	ノンブロッキング 24 ポート 1000BASEX(小型フォームファクタ着脱可能)モジュール	12.2(44)SG
WS-X4648-RJ45V-E	48 ポート10/100/1000 Mb、2:1 のオーバーサブスクリプション	12.2(40)SG
WS-X4648-RJ45V+E	48 ポート10/100/1000 Mb、2:1 のオーバーサブスクリプション	12.2(40)SG
ファスト イーサネット スイッチング モジュール		
WS-X4124-FX-MT	24 ポート 100BASE-FX ファスト イーサネット MT-RJ マルチモード光ファイバ スイッチング モジュール	12.1(8a)EW
WS-X4148-FX-MT	48 ポート 100BASE-FX ファスト イーサネット MT-RJ マルチモード光ファイバ スイッチング モジュール	12.1(8a)EW
WS-X4148-FE-LX-MT	48 ポート 100BASE-LX10 ファスト イーサネット MT-RJ シングルモード光ファイバ スイッチング モジュール	12.1(13)EW
WS-X4148-FE-BD-LC	48 ポート 100BASE-BX10-D モジュール	12.2(18)EW
WS-X4248-FE-SFP	48 ポート 100BASE-X SFP スイッチング モジュール	12.2(25)SG
WS-U4504-FX-MT	4 ポート 100BASE-FX(MT-RF)アップリンク ドータ カード	12.1(8a)EW
イーサネット/ファスト イーサネット(10/100)スイッチング モジュール		
WS-X4124-RJ45	24 ポート 10/100 RJ-45 モジュール	12.2(20)EW
WS-X4148-RJ	48 ポート 10/100 RJ-45 スイッチング モジュール	12.1(8a)EW
WS-X4148-RJ21	48 ポート 10/100 4xRJ-21(Telco コネクタ)スイッチング モジュール	12.1(8a)EW

表 2　サポート対象ハードウェア(続き)

製品番号(スペアには「=」を追加)	製品の説明	ソフトウェア リリース
		最小
WS-X4148-RJ45V	48 ポート 準規格 PoE 10/100BASE-T スイッチング モジュール	データ サポート用 12.1(8a)EW データおよびインライン パワー サポート用 12.1(11b)EW
WS-X4224-RJ45V	24 ポート 10/100BASE-TX RJ-45 Cisco Catalyst 4500 シリーズ PoE 802.3af	12.2(20)EW
WS-X4232-GB-RJ	32 ポート 10/100 ファスト イーサネット RJ-45 および 2 ポート 1000BASE-X(GBIC) ギガビット イーサネット スイッチング モジュール	12.1(8a)EW
WS-X4248-RJ45V	48 ポート 10/100BASE-T RJ-45 Cisco Catalyst 4500 シリーズ PoE 802.3af	12.2(18)EW
WS-X4248-RJ21V	48 ポート 10/100 ファスト イーサネット RJ-21 Cisco Catalyst 4500 シリーズ PoE 802.3af telco	12.2(18)EW
WS-X4232-RJ-XX	32 ポート 10/100 ファスト イーサネット RJ-45 モジュラ アップリンク スイッチング モジュール	12.1(8a)EW
その他のモジュール		
MEM-C4K-FLD64M	Catalyst 4500 シリーズ スイッチ コンパクトフラッシュ、64 MB オプション	12.1(8a)EW
MEM-C4K-FLD128M	Catalyst 4500 シリーズ スイッチ コンパクトフラッシュ、128 MB オプション	12.1(8a)EW
WS F4531	Catalyst 4500 シリーズ スイッチ Supervisor Engine IV および V の Catalyst 4500 シリーズ スイッチ NetFlow サービスカード	12.1(13)EW
WS-X4590=	Catalyst 4500 シリーズ スイッチ ファブリック冗長モジュール	12.2(18)EW
PWR-C45-1000AC	Catalyst 4500 シリーズ スイッチ シャーシ 4503、4506、および 4507R 用 1000 W AC 電源(データのみ)	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 シリーズ スイッチ 1400 W DC トリプル入力電源装置(データのみ)	12.2(25)EW
PWR-C45-1400DC-P	Catalyst 4500 シリーズ スイッチ PEM 搭載の 1400 W DC 電源装置	12.1(19)EW
PWR-C45-1400AC	Catalyst 4500 シリーズ スイッチ 1400 W AC 電源(データのみ)	12.1(12c)EW
PWR-C45-1300ACV	Catalyst 4500 シリーズ スイッチ シャーシ 4503、4506、および 4507R 用統合音声搭載の 1300 W AC 電源	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 シリーズ スイッチ シャーシ 4503、4506、および 4507R 用統合音声(データおよび PoE)搭載の 2800 W AC 電源	12.1(12c)EW
PWR-C45-4200ACV	Catalyst 4500 シリーズ スイッチ 統合音声(データおよび PoE)搭載の 4200 W AC デュアル電源装置	12.2(25)EWA5
WS-P4502-1PSU	Catalyst 4500 シリーズ スイッチ 補助電源シェルフ(25 スロット)、PWR-4502 x 1 を含む	12.1(19)EW
PWR-4502	Catalyst 4500 シリーズ スイッチ 補助電源シェルフ冗長電源装置	12.1(19)EW
PWR-C45-6000ACV	Catalyst 4500 シリーズ スイッチ 6000 W AC 電源	12.2(53)SG

Catalyst 4500 トランシーバモジュールの互換性情報については、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

表 3 に、Catalyst 4500 シリーズ スイッチの 4 つのシャーシについて簡単に説明します。表に記載されているシャーシのソフトウェア リリース情報については、表 6（18 ページ）を参照してください。

表 3　　Catalyst 4500 シリーズ スイッチのシャーシの説明

製品名（スペアには「=」を追加）	**モジュラ シャーシの説明**
WS-C4503	Catalyst 4503 のシャーシには、次のコンポーネントが含まれています。 • 3 スロット • ファン トレイ • Supervisor Engine 6L-E、Supervisor Engine 6-E、Supervisor Engine V-10GE、Supervisor Engine V、Supervisor Engine IV、Supervisor Engine III、Supervisor Engine II-Plus-10GE、Supervisor Engine II-Plus-TS、Supervisor Engine II-Plus、および Supervisor Engine II をサポート
WS-C4506	Catalyst 4506 のシャーシには、次のコンポーネントが含まれています。 • 6 つのスロット • ファン トレイ • Supervisor Engine 6L-E、Supervisor Engine 6-E、Supervisor Engine V-10GE、Supervisor Engine V、Supervisor Engine IV、Supervisor Engine III、Supervisor Engine II-Plus-10GE、Supervisor Engine II-Plus、および Supervisor Engine II をサポート
WS-C4507R	Catalyst 4507R のシャーシには、次のコンポーネントが含まれています。 • 7 スロット • ファン トレイ • Supervisor Engine 6L-E、Supervisor Engine 6-E、Supervisor Engine V-10GE、Supervisor Engine V、Supervisor Engine IV、Supervisor Engine II-Plus-10GE、および Supervisor Engine II-Plus をサポート
WS-C4510R	Catalyst 4510R のシャーシには、次のコンポーネントが含まれています。 • 10 スロット。スロット 10 では、Catalyst 4500 シリーズの 2 ポート ギガビット イーサネット ラインカード（Supervisor Engine V を搭載した WS-X4302-GB）のみ使用できます。 **注**　Supervisor Engine V-10GE には、このような制限はありません。 • ファン トレイ • Supervisor Engine 6-E、Supervisor Engine V-10GE および Supervisor Engine V をサポート

表 4　Catalyst 4500 シリーズ スイッチでサポートされている DOM

トランシーバ モジュール	ソフトウェアのサポート開始リリース
CWDM- SFP-xx	12.2(20)EWA
DWDM-GBIC-*xx*	12.1(19)EW
DWDM-SFP	12.2(37)SG
DWDM-X2-xx	12.2(50)SG
GLC-BX-D	12.2(20)EWA
GLC-BX-U	12.2(20)EWA
SFP-10G-SR	12.2(54)SG
SFP-10G-LR	12.2(54)SG
SFP-10G-LRM	12.2(54)SG

Catalyst 4500 E シリーズ スイッチでサポートされているハードウェア

従来のラインカードとスーパバイザエンジンに加えて、Cisco IOS ソフトウェアリリース 12.2(54)SG は、CenterFlex テクノロジーを備えた次世代の高性能 E シリーズ Supervisor Engine 6-E と、E シリーズ ラインカードおよびシャーシをサポートしています。Catalyst 4500 シリーズ スイッチでサポートされるプライマリ E シリーズ ハードウェアの一覧（表 5）。

表 5　サポートされている E シリーズのハードウェア

製品番号	説明
WS-C4503-E	Cisco Catalyst 4500 E シリーズ 3 スロット シャーシ • ファン トレイ • 電源装置なし
WS-C4506-E	Cisco Catalyst 4500 E シリーズ 6 スロット シャーシ • ファン トレイ • 電源装置なし
WS-C4507R-E	Cisco Catalyst 4500 E シリーズ 7 スロット シャーシ • ファン トレイ • 電源装置なし • 冗長スーパーバイザエンジンの機能
WS-C4507R+E	Cisco Catalyst 4500 E シリーズ 7 スロット 48 GB 対応シャーシ • ファン トレイ • 電源装置なし • 冗長スーパーバイザエンジンの機能

表 5　　サポートされている E シリーズのハードウェア

製品番号	説明
WS-C4510R-E	Cisco Catalyst 4500 E シリーズ 10 スロット シャーシ • ファン トレイ • 電源装置なし • 冗長スーパーバイザエンジンの機能 • Supervisor Engine 7-E で使用する場合、すべてのポートカードスロットが、6、24、および 48Gbps をサポートします。Supervisor Engine 6-E で使用する場合、スロット 8、9、および 10は 6Gbps に制限されます。
WS-C4510R+E	Cisco Catalyst 4500 E シリーズ 10 スロット 48 GB 対応シャーシ • ファン トレイ • 電源装置なし • 冗長スーパーバイザエンジンの機能 • Supervisor Engine 6-E と組み合わせて使用する場合、Catalyst 4510R+E シャーシのスロット 8、9、および 10 にバックプレーン トラフィック容量が 6Gbps 超えるラインカードは配置できません。
WS-X45-Sup6-E	Cisco Catalyst 4500 E シリーズ Sup 6-E、2x10GE(X2)、TwinGig 搭載
WS-X45-Sup6L-E	Cisco Catalyst 4500 E シリーズ Sup 6L-E
WS-X4624-SFP-E	Cisco Catalyst 4500 E シリーズ 24 ポート 1000BaseX（小型フォーム ファクタ着脱可能）モジュール
WS-X4648-RJ45V-E	Cisco Catalyst 4500 E シリーズ 48 ポート PoE 802.3af 10/100/1000（RJ45）
WS-X4648-RJ45V+E	Cisco Catalyst 4500 E シリーズ 48 ポート Premium PoE 10/100/1000
WS-X4606-X2-E	Cisco Catalyst 4500 E シリーズ 6 ポート 10GbE (X2)、TwinGig 搭載
WS-X4648-RJ45-E	Cisco Catalyst 4500 E シリーズ 48 ポート 10/100/1000（RJ45）

表 6 に、シャーシとスーパバイザエンジンの互換性の概要を示します。
（M = 最小リリース、R = 推奨リリース）

表 6　　シャーシとスーパバイザの互換性

シャーシ	Sup II+	Sup II+TS	Sup II + 10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4506-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4507R-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO

表 6　シャーシとスーパバイザの互換性(続き)

シャーシ	Sup II+	Sup II+TS	Sup II + 10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4507R+E	M: 12.2(54)SG R: 12.2(54)SG		M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG
WS-C4510R-E					M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	
WS-C4510R+E					M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	

Catalyst 4500 シリーズ スイッチでサポートされている機能

表 7 に、Catalyst 4500 シリーズ スイッチの Cisco IOS ソフトウェアの機能を示します。

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット

レイヤ 2 スイッチング機能
ストーム制御
ストーム制御:ポート単位のマルチキャスト抑制(Sup 6-E のみ)
マルチキャスト ストーム制御[1]
IP ソース ガード
スタティック ホスト用 IP ソース ガード
PVRST+
レイヤ 2 プロトコル トンネリング
レイヤ 2 トランスペアレント ブリッジング[2]
ソフトウェアによるレイヤ 2 MAC[3] ラーニング、エージング、およびスイッチング
ユニキャスト MAC アドレスフィルタリング
VMPS[4] クライアント
最大 102 Mpps のレイヤ 2 ハードウェア転送
レイヤ 2 制御ポリシング(Sup 6-E および Sup 6L-E のみ)
レイヤ 2 スイッチポートおよび VLAN トランク
VLAN ごとのスパニングツリープロトコル(IEEE 802.1D)
802.1s および 802.1w
レイヤ 2 の traceroute
単方向イーサネットポート
Per-VLAN Spanning Tree(PVST)および PVST+
Spanning Tree Root Guard

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

Spanning Tree Root Guard および PortFast BPDU フィルタリング
9216 バイトフレームのサポート
PVLAN のポートセキュリティ
プライベート VLAN
プライベート VLAN DHCP スヌーピング
プライベート VLAN 無差別トランク
プライベート VLAN トランク[5]
コミュニティ PVLAN
ISL[6] ベースの VLAN カプセル化（WS-X4418-GB および WS-X4412-2GB-T のブロッキングポートを除く）[7]
IEEE 802.1Q ベースの VLAN カプセル化
マルチプル VLAN アクセスポート
VLAN トランキングプロトコル（VTP）および VTP ドメイン
VTP v3
スイッチあたりの VLAN サポート数：2048（LAN Base の場合）、4096（IP Base の場合）
単方向リンク検出（UDLD）およびアグレッシブ UDLD
サブセカンド UDLD（Fast UDLD）
VLAN インデックスを使用したブリッジ MIB の SNMP V3 サポート
Resilient Ethernet Protocol
イーサネット CFM
イーサネット OAM プロトコル
レイヤ 3 ルーティング、スイッチング、および転送
802.1Q トンネリング（Q-in-Q）[8]
Pragmatic General Multicast
ANCP クライアント[9]
PIM-SSM マッピング
双方向 PIM[10]
自動 RP リスナー
イーサネットポート間の IP および IP マルチキャストルーティングとスイッチング
IP マルチキャスト ロード スプリッティング（S、G、およびネクストホップを使用した Equal Cost Multipath（ECMP; 等コストマルチパス））
スタティック IP ルーティング
クラスレスルーティング[11]
PBR[12]
Dynamic Buffer Limiting
選択的 Dynamic Buffer Limiting
IP プレシデンスに基づく QoS ベースの転送

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

信頼境界
Cisco モジュラ QoS コマンド ライン インターフェイス（Sup 6-E および Sup 6L-E のみ）
自動 QoS
非 IPv4 トラフィックの一致 CoS
ハードウェアでの IPv6 転送（Sup 6-E および Sup 6L-E のみ）
CoS 変換
CEF[13] ロードバランシング
uRPF[14]（Sup 6-E および Sup 6L-E のみ）
48 Mpps でのハードウェアベースの IP CEF ルーティング
最大 128,000 の IP ルート
最大 32,000 の IP ホストエントリ（レイヤ 3 隣接関係）
最大 16,000 の IP マルチキャスト ルート エントリ
STP 変更のためのマルチキャスト フラッディング抑制
IPX、AppleTalk、および IPv6 のソフトウェアルーティング
IGMPv1、IGMPv2、および IGMPv3（フルサポート）
IGMP クエリア
VRF-lite
マルチキャスト VRF-lite[15]
VRF 認識 IP サービス
VRF 対応 TACACS+
ルートリーク[16]
IP アンナンバード
SVI 自動ステート除外
サポートされているプロトコル
IS-IS[17]
DTP[18]
RIP[19] および RIP II
EIGRP[20]
EIGRP IPv6（Sup 6-E および Sup 6L-E のみ）
OSPF[21]
ルーテッド アクセスの OSPF[22]
BGP4[23]
BGP ルートマップ継続
BGP ネイバー ポリシー
MBGP[24]
MSDP[25]
ICMP[26] Router Discovery Protocol

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

PIM[27]：Sparse モードと Dense モード
スタティック ルート
クラスレス ドメイン間ルーティング（CIDR）
DVMRP[28]
SSM
NTP[29]
WCCP バージョン 2 レイヤ 2 リダイレクション
VRRP[30]
SCP[31]
GLBP[32]
EtherChannel の機能
Cisco EtherChannel テクノロジー：10/100/1000 Mbps、10 Gbps
送信元および宛先 IP アドレスに基づく、ルーテッドトラフィックのロードバランシング
MAC アドレスに基づくブリッジドトラフィックのロードシェアリング
すべての EtherChannel の ISL
すべての EtherChannel の IEEE 802.1Q
最大 8 つのイーサネットポートのバンドル
最大 64 のアクティブなイーサネットポートチャネル
EtherChannel を介したトランクポートセキュリティ
リンクステート トラッキング
追加のプロトコルと機能
リンク層検出プロトコル（LLDP）
Link Layer Discovery Protocol Media Endpoint Discovery（LLDP-MED）
LLDP 経由の PoEP
LLDP 経由の DSCP/CoS
ルーテッドジャンボフレームのサポート
SPAN CPU ポートミラーリング
SPAN パケットタイプ フィルタリング
SPAN destination in-packets オプション
SPAN ACL フィルタリング
RSPAN
拡張 VLAN 統計情報
NetFlow バージョン 8
NetFlow 統計情報収集
NetFlow 統計情報エクスポートバージョン 1 およびバージョン 5
NetFlow ブリッジド IP フロー
セカンダリアドレッシング

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

ブートストラッププロトコル（BOOTP）
TACACS+ および RADIUS プロトコルを使用して、認証、許可、およびアカウンティングを行います。
Cisco Discovery Protocol（CDP）
CDP セカンドポートステータス TLV
MAC アドレス テーブル移動更新
FlexLink 双方向高速コンバージェンス
FlexLink VLAN ロードバランシング
Flex Link
Flex Link インターフェイスのプリエンプション
802.1ab リンク層検出プロトコル（LLDP）
802.1ab LLDP Media Discovery（LLDP-MED）
Network Mobility Services Protocol（ネットワーク モビリティ サービス プロトコル）
制御パケットのキャプチャのモード選択（Sup 6-E ではサポート対象外）
スティッキ ポート セキュリティ
トランクポートセキュリティ
音声 VLAN スティッキ ポート セキュリティ
Cisco Group Management Protocol（CGMP）サーバのサポート
HSRP[33] over Ethernet、EtherChannel：10/100/1000 Mbps、10 Gbps
IPv4 用 HSRPv2
IPv6 用 HSRPv2
IGMP スヌーピングバージョン 1、バージョン 2、およびバージョン 3（フルサポート）
IGMP フィルタリング
ポート集約プロトコル（PAgP）
802.3ad LACP
SSH バージョン 1 とバージョン 2[34]
インラインパワーの事前割り当て
show interface capabilities コマンド
ifIndex パーシステンス
UDLR[35]
拡張 SNMP MIB のサポート
SNMP[36] バージョン 1、バージョン 2、およびバージョン 3
SNMP バージョン 3（暗号化あり）
IPv6 マルチキャストリスナー検出スヌーピング（Sup 6-E および 6L-E のみ）
IPv6 PACL（Sup 6-E および 6L-E のみ）
IPv6 RA ガード（Sup 6-E および 6L-E のみ）
IPv6 インターフェイス統計情報（Sup 6-E および 6L-E のみ）

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

DHCP サーバおよびリレーエージェント
DHCP スヌーピング
DHCP クライアント自動設定
DHCP オプション 82 パススルー
IPv6 用の DHCP リレーエージェント [37]
802.1X 複数ドメイン認証および複数許可
ACL 割り当てとリダイレクト URL を使用した 802.1X
ユーザ単位の ACL とフィルタ ID ACL を使用した 802.1X
RADIUS-Provided セッションタイムアウト
RADIUS CoA
MAC の移動と置換
802.1X とゲスト VLAN
802.1X ポートベースの認証
802.1X とポートセキュリティ
802.1X アカウンティング
802.1X と音声 VLAN ID
802.1X プライベート VLAN 割り当て
802.1X プライベートゲスト VLAN
802.1X RADIUS-supplied セッションタイムアウト
802.1X 認証失敗 VLAN
802.1X MAC 認証バイパス
802.1X アクセス不能認証バイパス
802.1X とユーザ ディストリビューション
802.1X 単方向制御ポート
音声割り当てを使用した 802.1X MDA
Cisco TrustSec SGT Exchange Protocol（SXP）IPv4
Flexible Authentication（FlexAuth; フレキシブル認証）シーケンシング
マルチ認証
オープン認証
Web 認証
ローカル Web 認証（EPM syslog および共通セッション ID）
PPPoE 中継エージェント [38]
Cisco NAC [39] レイヤ 2 802.1X
ポート フラッディング ブロッキング
すべてのポートにルータの標準 ACL および拡張 ACL [40] を搭載しても、パフォーマンスの低下なし
Identity 4.1 ACL ポリシーの適用 [41]

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャセット（続き）

Identity 4.1 Network Edge Access Topology
拡張 IPX ACL
VLAN ACL
PACL[42]
時間ベースの ACL
ダウンロード可能 ACL
コントロール プレーン ポリシング
2 レート 3 カラーポリシング（Sup 6-E および Sup 6L-E のみ）
ローカル プロキシ ARP
PVLAN の ダイナミック ARP インスペクション
ダイナミック ARP インスペクション
Dynamic Multi-Protocol Ternary Content Addressable Memory（Sup 6-E および Sup 6L-E のみ）
ポート単位の QoS[43] レート制限およびシェーピング
QoS for IPv6
Per-port Per-VLAN QoS
Per-VLAN CTI
ARP QoS（Sup 6-E および Sup 6L-E のみ）
Cisco IP 電話用インラインパワーのサポート
PoE[44]
Energy Wise
拡張 Power over Ethernet のサポート（Sup 6-E および Sup 6L-E のみ）
電源の冗長性
RPR[45]
SSO[46]
SSO 対応 HSRP
ルーテッドポートの SSO サポート
ノンストップ フォワーディング認識
すべてのスーパバイザエンジンの IP ベースでの EIGRP スタブのノンストップ フォワーディング認識
ノンストップ フォワーディングとステートフル スイッチオーバー
ISSU[47]
MAC アドレス通知
統合モードによる電源復元力
SmartPort マクロ
AutoSmartPort マクロ
強制 10/100 自動ネゴシエーション
802.1s 標準準拠

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャ セット（続き）

IS-IS MIB
OSPF および EIGRP 高速コンバージェンス [48]
TDR
CNA[49]
Auto-MDIX をオフにする CLI[50]
ロギングリダイレクション
サービス認識型リソース割り当て（Sup 6-E および Sup 6L-E のみ）
TwinGig コンバータモジュール（Sup 6-E および 6L-E のみ）
FAT ファイルシステム（Sup 6-E および Sup 6L-E のみ）
高可用性：2 + 2 10GE または 4 + 4 1GE アクティブアップリンク（Sup 6-E のみ）
EEM[51]
ISSU を使用した EEM
PAgP+ を使用した VSS クライアント
IP/SLA[52]
組み込みの管理機能[53]
MAC 通知 MIB
ポートあたり 8 つの設定可能なキュー（Sup 6-E および Sup 6L-E のみ）
X2 リンクデバウンスタイマー
IP SLA
拡張オブジェクトトラッキングのサブ機能： • EOT を使用した HSRP • EOT を使用した VRRP • EOT を使用した GLBP • EOT を使用した IP SLA • EOT を使用した信頼性の高いバックアップ スタティック ルーティング
管理ポート
IPv6 での管理ポート機能
非アクティブ タイマー
OBFL[54]
boot config コマンド
クラッシュダンプの拡張機能
ユニキャスト MAC フィルタリング
Smart Call Home
DHCPv6 イーサネットリモート ID オプション
DHCPv6 リレー：プレフィックス委任に関する永続インターフェイス ID オプションの DHCPv6 リレーエージェントの通知
PIM SSM マッピング

表 7　Catalyst 4500 シリーズおよび E シリーズ スイッチの Cisco IOS ソフトウェア フィーチャセット（続き）

ルーティングプロトコル OSPF/EIGRP/BG による VRF-Lite NSF サポート
PIM Accept Register：不正なマルチキャストサーバ保護 [55]
コンフィギュレーション ロールバック
クラッシュファイル情報のアーカイブ保存
VLAN 単位の学習
XML プログラマチック インターフェイス
VLAN マッピング（VLAN 変換）
GOLD オンライン診断（Sup 6-E および 6L-E のみ）
スタティックホストの IPSG
レイヤ制御パケット
Fa1 インターフェイス（イーサネット管理ポート） [56]

1. Catalyst 4500 シリーズ スイッチ Supervisor Engine V が必要
2. VLAN 内のハードウェアベースのトランスペアレント ブリッジング
3. MAC = Media Access Control
4. VMPS = VLAN マネジメントポリシーサーバ
5. Supervisr Engine 6-E のみ
6. ISL = Inter-Switch Link
7. WS-X4418-GB ではポート 3 ー 18、WS-X4412-2GB ではポート 1 ー 12
8. Catalyst 4500 シリーズ スイッチ Supervisor Engine V
9. Supervisor Engine 6-E ではサポートされていません。
10. Supervisr Engine 6-E のみ
11. クラスレスルーティングがデフォルトで有効になっているため、ip classless コマンドはサポートされていません。
12. PBR = ポリシーベースルーティング
13. CEF = Cisco Express Forwarding
14. uRPF = ユニキャストリバースパス転送
15. Supervisr Engine 6-E のみ
16. グローバル ルーティング テーブルから VRF へのルートリークおよび VRF からグローバル ルーティング テーブルへのルートリーク
17. IS-IS = Intermediate System to Intermediate System
18. DTP = Dynamic Trunking Protocol
19. RIP = Routing Information Protocol
20. EIGRP = Enhanced Interior Gateway Routing Protocol
21. OSPF = Open Shortest Path First
22. Supervisor Engine 6-E および Supervisor Engine 6L-E のみサポート
23. BGP4 = Border Gateway Protocol 4
24. MBGP = Multicast Border Gateway Protocol
25. MSDP = マルチキャスト ソース ディスカバリ プロトコル
26. ICMP = Internet Control Message Protocol
27. PIM = Protocol Independent Multicast
28. DVMRP = ディスタンス ベクター マルチキャスト ルーティング プロトコル
29. NTP = ネットワーク タイム プロトコル
30. VRRP = Virtual Router Redundancy Protocol
31. SCP = Secure Copy Protocol
32. GLBP = Gateway Load Balancing Protocol
33. HSRP = Hot Standby Router Protocol（ホット スタンバイ ルータ プロトコル）

34. SSH = Secure Shell Protocol
35. UDLR = 単方向リンクルーティング
36. SNMP = Simple Network Management Protocol
37. Sup 6-E および 6L-E のみ
38. Supervisor Engine 6-E ではサポートされていません
39. NAC = ネットワーク アドミッション コントロール
40. ACL = アクセス制御リスト
41. フィルタ ID とユーザ単位の ACL
42. PACL = ポートアクセス制御リスト
43. QoS = Quality of Service
44. PoE = Power over Ethernet
45. RPR = スーパバイザエンジンの冗長性
46. SSO = ステートフル スイッチオーバー（ステートフル IGMP スヌーピングおよびステートフル DHCP スヌーピングを含む）
47. ISSU = In Service Software Upgrade プロセス
48. Catalyst 4500 シリーズ スイッチは、Fast Hello、ISPF、および LSA スロットリングをサポートしています。
49. CNA = Cisco Network Assistant。リリース 12.2(25)EW をサポートする最小の CNA リリースは 1.0(2) です。リリース 12.2(20)EWA をサポートする最小の CNA リリースは 1.0(1) です。
50. サポートされているラインカード：WS-X4124-RJ45、WS-X4148-RJ（および WS-X4232-GB-RJ）（ハードウェアリビジョン 3.0 以降）
51. EEM = Embedded Event Manager
52. SSL 3.0 を使用した HTTPS-HTTP、CEF-MIB、組み込み Syslog 管理などが含まれます。
53. SNMP over IPv6、SYSLOG、HTTP over IPv6 が含まれます。
54. OBFL = オンボード障害ロギング。Supverisor Engine 6-E のみ
55. route-map キーワードはサポートされていません。
56. Cisco IOS リリース 12.2(46)SG 以降で使用可能

Supervisor Engine 6-E および 6L-E に固有の機能

Cisco IOS リリース 12.2(54)SGでは、次の機能は Supervisor Engine 6-E および Supervisor Engine 6L-E でのみ使用できます。

- [IPv6]
  - IPv6 アドレッシング アーキテクチャ
  - CDP IPv6 アドレスファミリ
  - IPv4 トランスポートによる AAAA の DNS レゾルバ
  - IPv6 トランスポートによる AAAA の DNS レゾルバ
  - 拡張 ACL
  - ホップバイホップ オプション ヘッダー
  - ICMP レート制限
  - ICMPv6
  - ICMPv6 リダイレクト
  - IPv6 over IEEE 802.1Q
  - ISATAP（ソフトウェアでのみサポート）
  - ループバック
  - MLD スヌーピング（Catalyst 4900M、Catalyst 4948E、Supervisor Engine 6-E、および Catalyst 6L-E のソフトウェアおよびハードウェアでサポート）

  - MLDv1/v2
  - IPv6 の MTU パス検出
  - OSPFv3
  - RIPng
  - EIGRPv6
  - PACL
  - RA ガード
  - IPv6 インターフェイスの統計情報
- FAT ファイルシステム
- PIM（SM、DM、SDM）
- QoS
  - 2 レート 3 カラーポリシング
  - マーキング用のテーブルマップのサポート
  - クラスベースのキューイングアクション（シェーピング/帯域幅/キュー制限/dbl/厳格な優先順位）
- 電圧マージニング CLI
- QoS for IPv6
- ARP QoS

サポートされていない機能

すべての Supervisor Engine（II-Plus ～ 6-E）において、次の機能は、Catalyst 4500 シリーズ スイッチの Cisco IOS リリース 12.2(54)SG ではサポートされていません。

- 次の ACL タイプ:
  - 標準 Xerox Network System（XNS）アクセス リスト
  - 拡張 XNS アクセス リスト
  - DECnet アクセス リスト
  - プロトコル タイプコード アクセス リスト
- IPv6 への ADSL およびダイヤル アクセス
- AppleTalk EIGRP（代わりにネイティブ AppleTalk ルーティングを使用）
- ブリッジ グループ
- CEF アカウンティング
- Cisco IOS ソフトウェア IPX ACL:
  - <1200-1299>　　IPX サマリー アドレス アクセス リスト
- Cisco IOS ソフトウェアベースのトランスペアレント ブリッジング（別名「フォールバック ブリッジング」）
- コネクションレス型（CLNS）ルーティング。CLNS の IS-IS ルーティングを含みます。IS-IS は、IP ルーティングに対してのみサポートされます。
- DLSw（データリンク スイッチング）

- IGRP（代わりに EIGRP を使用）
- isis network point-to-point コマンド
- アクセス コントロールに対する Kerberos のサポート
- LLDP HA
- ロック アンド キー
- IPv6 への NAT-PT
- VRF 単位の NetFlow
- 複数のトラッキング オプションのある PBR
- QoS for IPv6 トラフィック（Supervisor 6 でのみサポート）
- 再帰 ACL
- MPLS ネットワークに展開されたルーティング IPv6
- プライベート VLAN 上での双方向コミュニティ VLAN
- WCCP バージョン 1
- CFM CoS
- EOT を使用した PBR

新機能および変更された機能に関する情報

ここでは、Cisco IOS ソフトウェアを実行している Catalyst 4500 シリーズ スイッチの新規および変更情報について説明します。

リリース 12.2(54)SG1 の新しいハードウェア機能

リリース 12.2(54)SG1 では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- Catalyst 4948E-F：Catalyst 4948E と Catalyst 4948E-F は同じ内部ハードウェアとソフトウェアを共有します。Catalyst 4948E は、ポート側で冷気を吸気し、電源側で熱気を排気します。Catalyst 4948E-F は、電源側で冷気を吸気し、ポート側で熱気を排気します。これは、Catalyst 4948E と Catalyst 4948E-F の唯一の違いです。

リリース 12.2(54)SG1 の新しいソフトウェア機能

リリース 12.2(54)SG には、Catalyst 4500 シリーズ スイッチの新しいソフトウェア機能はありません。

リリース 12.2(54)SG の新しいハードウェア機能

リリース 12.2(54)SG では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- SFP-10G-LRM
- WS-C4507R+E
- WS-C4510R+E
- すべての 10GE インターフェイスでのデジタル オプティカル モニタリング（DOM）のサポート
- CVR-X2-SFP10G（Supervisor Engine II+ から V-10GE でサポートを導入）

リリース 12.2(54)SG の新しいソフトウェア機能

リリース 12.2(54)SG では、Catalyst 4500 シリーズ スイッチに次の新しいソフトウェア機能が用意されています。

- 802.1X とユーザ ディストリビューション（「802.1X ポートベース認証の設定」の章）
- Auto SmartPort（「Auto SmartPort マクロの設定」の章）

- LLDP 経由の DSCP/CoS（「LLDP、LLDP-MED、およびロケーションサービスの設定」の章）
- EEM：Embedded Event Manager 3.2

  詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_12eem.html
- EIGRP Service Advertisement Framework

  詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html
- EnergyWise 2.0

  詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html
- GOLD オンライン診断（「診断の実行」の章、Supervisor Engine 6-E のみ）
- Identity 4.1 ACL ポリシーの拡張機能（「ACL によるネットワークセキュリティの設定」の章）
- Identity 4.1 Network Edge Access Topology（NEAT）（「802.1X ポートベース認証の設定」の章）
- スタティックホストの IPSG（Cisco IOS ライブラリを参照）
- IPv6 PACL（「ACL によるネットワークセキュリティの設定」の章、Supervisor Engine 6-E のみ）
- IPv6 RA ガード（「ACL によるネットワークセキュリティの設定」の章、Supervisor Engine 6-E のみ）
- IPv6 インターフェイス統計情報（「レイヤ 3 イ ンターフェイスの設定」の章、Supervisor Engine 6-E のみ）
- IPv4 および IPv6 用 IS-IS、Supervisor Engine 6-E に拡張（Cisco IOS ライブラリを参照）
- レイヤ制御パケット（Supervisor 6 に拡張）
- リンクステートトラッキング（「EtherChannel およびリンクステートトラッキングの設定」の章）
- MAC の移動と交換（「スイッチの管理」の章）
- VLAN ごとの学習（「スイッチの管理」の章）
- LLDP 経由の PoEP（「LLDP、LLDP-MED、およびロケーションサービスの設定」の章）
- RADIUS CoA（「802.1X ポートベース認証の設定」の章）
- サブセカンド UDLD（「UDLD の設定」の章）
- VLAN 変換（「802.1Q トンネリング、VLAN マッピング、およびレイヤ 2 プロトコルトンネリングの設定」の章、Supervisor Engine 6-E のみ）
- VRF 対応 TACACS+（「VRF-Lite の設定」の章）
- XML プログラマチック インターフェイス（Cisco IOS ライブラリを参照）

  詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_xmlpi_v1.html

リリース 12.2(53)SG6 の新しいハードウェア機能

リリース 12.2(53)SG6 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(53)SG6 の新しいソフトウェア機能

リリース 12.2(53)SG6 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG5 の新しいハードウェア機能

リリース 12.2(53)SG5 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(53)SG5 の新しいソフトウェア機能

リリース 12.2(53)SG5 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG4 の新しいハードウェア機能

リリース 12.2(53)SG4 では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- WS-C4507-R+E
- WS-C4510-R+E

リリース 12.2(53)SG4 の新しいソフトウェア機能

リリース 12.2(53)SG4 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG3 の新しいハードウェア機能

リリース 12.2(53)SG3 では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

注 この一連の光ファイバは、Cisco IOS リリース 12.2(54)SG および Cisco IOS XE Release 3.1.0 SG ではサポートされていません。ただし、Cisco IOS リリース 15.0(2)SG および Cisco IOS XE リリース 3.2.0(SG) では、同じ一連の光ファイバがサポートされています。

- DWDM-SFP-6141
- DWDM-SFP-5736
- DWDM-SFP-5332
- DWDM-SFP-4931
- DWDM-SFP-4532

- DWDM-SFP-4134
- DWDM-SFP-3739
- DWDM-SFP-3346

リリース 12.2(53)SG3 の新しいソフトウェア機能

リリース 12.2(53)SG3 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG2 の新しいハードウェア機能

リリース 12.2(53)SG2 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(53)SG2 の新しいソフトウェア機能

リリース 12.2(53)SG2 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG1 の新しいハードウェア機能

リリース 12.2(53)SG1 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(53)SG1 の新しいソフトウェア機能

リリース 12.2(53)SG1 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(53)SG の新しいハードウェア機能

リリース 12.2(53)SG には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。ただし、12.2(52)XO で導入された Supervisor Engine 6L-E は統合されます。

リリース 12.2(53)SG の新しいソフトウェア機能

リリース 12.2(53)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

- IP マルチキャスト ロード スプリッティング（S、G、およびネクスト ホップを使用した Equal Cost Multipath（ECMP; 等コストマルチパス））
- ルーテッドアクセスの OSPF（Supervisor Engine 6-E および Supervisor Engine 6L-E）

  ルーテッド アクセスの OSPF は、レイヤ 3 ルーティングの機能をアクセスまたはワイヤリング クローゼットに拡張できるようにするために、特に設計されています。

  注 OSPF for Routed Access は、OSPFv2 インスタンスと OSPFv3 インスタンスをそれぞれ 1 つずつと、最大 200 のダイナミックに学習されるルートをサポートします。

ワイヤリング クローゼット（スポーク）が、すべての非ローカルのトラフィックをディストリビューション レイヤに転送するディストリビューション スイッチ（ハブ）に接続された、キャンパス環境の標準的なトポロジ（ハブおよびスポーク）では、ワイヤリング クローゼット スイッチが、完全なルーティング テーブルを保持する必要がありません。OSPF for Routed Access をワイヤリング クローゼットで使用する場合、ディストリビューション スイッチがデフォルトのルートをワイヤリング クローゼット スイッチに送信することで、エリア間ルートおよび外部ルートに到達するベスト プラクティスの設計を使用する必要があります。

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/54sg/configuration/guide/automacr.html

ルーテッドアクセスの OSPF 機能は、次のソフトウェアの制約事項に準拠しています。

- OSPF インスタンスの数を OSPFv2 で 1 つ、OSPFv3 で 1 つに制限します。
- プラットフォームに依存する作業を通じて学習されるダイナミックルートの数を 200 に制限します。

詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html

Cisco IOS Release 12.2(53)SG では、IP ベース イメージはルーテッド アクセスの OSPF をサポートします。ルート制限のない複数の OSPFv2 および OSPFv3 インスタンスが必要な場合は、Enterprise Services イメージが必要です。さらに、VPN Routing and Forwarding Lite（VRF-Lite）機能をイネーブルにするには、Enterprise Services が必要です。

リリース 12.2(52)XO の新しいハードウェア機能

リリース 12.2(52)XO では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- WS-X45-Sup6L-E、Catalyst 4500 E シリーズ スイッチ Supervisor Engine 6L-E
- PWR-C45-6000ACV、Catalyst 4500 シリーズ スイッチ 6000 W AC 電源

注 3、6、7 スロットシャーシ、および IP LAN イメージと IP Base イメージでのみサポート

リリース 12.2(52)XO の新しいソフトウェア機能

注 このリリースの機能は 12.2(52)SG と同等ですが、新しい Sup6L-E スーパバイザのサポートが追加されています。サポートされるスーパバイザエンジンは、Supervisor Engine 6L-E のみです。他のすべてのスーパバイザエンジンでは、代わりに 12.2(52)SG が使用されます。

リリース 12.2(52)XO は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

- EnergyWise
- セキュリティ機能のためのスイッチと IP フォンの相互作用
  - ポート セキュリティ
  - DHCP スヌーピング
  - ダイナミック ARP インスペクション
  - BPDU ガード

- Network Mobility Services Protocol（ネットワーク モビリティ サービス プロトコル）
- Identity ACL ポリシー適用の拡張機能
  - フィルタ ID（Filter-ID）
  - ユーザ単位 ACL
- Smart Call Home*
- IPv6 での管理ポート機能
- ローカル Web 認証の拡張機能
- 音声割り当てを使用した MDA
- IPv4 用 HSRP v2
- HSRPv2 または IPv6
- DHCPv6 の拡張機能
  - DHCPv6 イーサネットリモート ID オプション
  - DHCPv6 リレー:プレフィックス委任に関する永続インターフェイス ID オプションの DHCPv6 リレーエージェントの通知
- PIM SSM マッピング
- ルーティングプロトコル OSPF/EIGRP/BGP による VRF Lite NSF サポート
- サポートされている MIB
  - Cisco Enhanced Image MIB
  - Cisco NHRP Extension MIB
  - CISCO-CALLHOME-MIB.my
  - EnergyWise MIB
  - POE MIB
  - POE ext MIB
  - Entity-Diag-MIB
  - ブリッジ MIB
- タイムプロトコル（SNTP、TimeP）プライマリ
  （旧称 タイムプロトコル（SNTP、TimeP）マスター）

Supervisor Engine 6L-E

- コミュニティ PVLAN のサポート
- EtherType の分類
- QinQ
- PPPoE IA（または中継エージェント）

リリース 12.2(52)SG の新しいハードウェア機能

リリース 12.2(52)SG では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- PWR-C45-6000ACV、Catalyst 4500 シリーズ スイッチ 6000 W AC 電源

リリース 12.2(52)SG の新しいソフトウェア機能

リリース 12.2(52)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

すべてのスーパバイザエンジン

- EnergyWise
- セキュリティ機能のためのスイッチと IP フォンの相互作用
  - ポート セキュリティ
  - DHCP スヌーピング
  - ダイナミック ARP インスペクション
  - BPDU ガード
- Network Mobility Services Protocol（ネットワーク モビリティ サービス プロトコル）
- Identity ACL ポリシー適用の機能拡張
  - フィルタ ID（Filter-ID）
  - ユーザ単位 ACL
- Smart Call Home*
- IPv6 での管理ポート機能
- ローカル WebAuth 拡張
- 音声割り当てを使用した MDA
- IPv4 用 HSRP v2
- HSRP v2 または IPv6
- DHCPv6 の機能拡張
  - DHCPv6 イーサネットリモート ID オプション
  - DHCPv6 リレー：プレフィックス委任に関する永続インターフェイス ID オプションの DHCPv6 リレーエージェントの通知
- SSM Mapping
- PIM Accept Register：不正なマルチキャストサーバ保護（route-map オプションはサポートされていません）
- ルーティングプロトコル OSPF/EIGRP/BGP による VRF Lite NSF サポート
- サポートされている MIB
  - Cisco Enhanced Image MIB
  - Cisco NHRP Extension MIB
  - CISCO-CALLHOME-MIB.my
  - EnergyWise MIB
  - POE MIB
  - POE ext MIB
  - Entity-Diag-MIB
  - ブリッジ MIB

Supervisor Engine 6-E の場合

- コミュニティ PVLAN のサポート
- EtherType の分類
- PBR
- QinQ
- PPPoE IA（または中継エージェント）

リリース 12.2(50)SG3 の新しいハードウェア機能

リリース 12.2(50)SG3 では、Catalyst 4500 シリーズ スイッチに次のハードウェアが用意されています。

- CVR-X2-SFP10G

  スイッチまたはラインカードモジュールの 10 ギガビットイーサネット X2 スロットに適合するホットスワップ可能な入出力（I/O）コンバータモジュール。1 つの 10 ギガビットイーサネット SFP+ トランシーバモジュールをホスト。
- SFP-10G-SR、MMF 用 Cisco 10GBASE-SR SFP+ モジュール

リリース 12.2(50)SG3 の新しいソフトウェア機能

リリース 12.2(50)SG3 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(50)SG2 の新しいハードウェア機能

リリース 12.2(50)SG2 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(50)SG2 の新しいソフトウェア機能

リリース 12.2(50)SG2 には、Catalyst 4500 シリーズ スイッチの新機能はありません。

リリース 12.2(50)SG1 の新しいハードウェア機能

リリース 12.2(50)SG1 には、Catalyst 4500 シリーズ スイッチの新しいハードウェアはありません。

リリース 12.2(50)SG1 の新しいソフトウェア機能

リリース 12.2(50)SG1 は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

- EEM バージョン 2

EEM については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

リリース 12.2(50)SG の新しいハードウェア機能

注 従来のラインカードとスーパバイザエンジンに加えて、Cisco IOS ソフトウェアリリース 12.2(50)SG は、CenterFlex テクノロジーを備えた次世代の高性能 E シリーズ Supervisor Engine 6-E と、E シリーズ ラインカードおよびシャーシをサポートしています。

リリース 12.2(50)SG では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- X2-10GB-ZR 光モジュール
- X2-10GB-DWDM 光モジュール
- 従来のシリーズの 48 ポート 10/100/1000 プレミアム PoE ラインカード

リリース 12.2(50)SG の新しいソフトウェア機能

リリース 12.2(50)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

注 次の章の参照資料は、*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* です。

注 マルチスパニングツリー（MST）の実装が以前のリリースから変更されました。Multiple STP（MSTP）は、IEEE 802.1s 標準に準拠しています。以前の MSTP 実装は、IEEE 802.1s 標準のドラフトに基づいていました。

- IGMP クエリア（「IGMP スヌーピングの設定」の章）
- OSPF および EIGRP の高速コンバージェンスおよび保護（Cisco IOS リリース 12.4 のマニュアルを参照）
- CDP の 2 番目のポートステータス TLV（スイッチでの設定は不要）

注 CDP の 2 番目のポートステータス TLV のリンクアップ/ダウン情報（Cisco IP 電話のホスト移動検出拡張機能によって追加）により、スイッチは以前認証されたデバイスの認証を解除できます。この CDP TLV を生成するには、電話機にファームウェアリリース 8.1(1) 以降をインストールする必要があります。

- ANCP クライアント（E シリーズ Supervisor Engine 6-E ではサポートされていません。「ANCP クライアントの設定」の章）
- boot config コマンド（Cisco IOS リリース 12.2 のマニュアルを参照）
- Crashinfo ファイルのアーカイブ（「コマンドライン インターフェイスの設定」の章）
- ブート構成/クラッシュダンプ（Cisco IOS リリース 12.2 のマニュアルを参照）
- ダウンロード可能な ACL（「ACL によるネットワークセキュリティの設定」の章）
- イーサネット管理ポート（「インターフェイスの設定」の章を参照）

- フレキシブル認証シーケンシング（「802.1X の設定」の章）
- 非アクティブタイマー（「802.1X の設定」の章）
- マルチ認証（「802.1X の設定」の章）
- オープン認証（「802.1X の設定」の章）
- PPPoE 中継エージェント（E シリーズ Supervisor Engine 6-E ではサポートされません。「PPPoE 回線 ID タグの処理」の章）
- VRF 対応 IP サービス（「VRF-Lite の設定」の章）
- VTP バージョン 3（「VLAN、VTP、および VMPS の設定」の章）
- Web 認証（「Web 認証の設定」の章）
- コンフィギュレーション ロールバック
- Cisco TrustSec SGT Exchange Protocol (SXP) IPv4

  詳細については、次の URL を参照してください。

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

Supervisor Engine 6-E の場合

- 双方向 PIM（「IP マルチキャストの設定」の章）
- コントロール プレーン ポリシング（「CPP の設定」の章）
- IPv6 用 DHCP リレーエージェント（Cisco IOS リリース 12.2 メインラインのマニュアルを参照）
- マルチキャスト VRF-Lite（「VRF-Lite の設定」の章）
- オンボード障害ロギング（Cisco IOS リリース 12.2 のマニュアルを参照）
- プライベート VLAN トランク（「プライベート VLAN の設定」の章）
- SVI 自動ステート除外（「レイヤ 3 インターフェイスの設定」の章）
- ユニキャスト MAC フィルタリング（「ACL によるネットワークセキュリティの設定」の章）
- QoS for IPv6（Cisco IOS リリース 12.4T のマニュアルを参照）

リリース 12.2(46)SG の新しいハードウェア機能

注 従来のラインカードとスーパバイザエンジンに加えて、Cisco IOS ソフトウェアリリース 12.2(46)SG は、CenterFlex テクノロジーを備えた次世代の高性能 E シリーズ Supervisor Engine 6-E と、E シリーズ ラインカードおよびシャーシをサポートしています。

リリース 12.2(46)SG では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- 20 W PoE ラインカード

リリース 12.2(46)SG の新しいソフトウェア機能

リリース 12.2(46)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

注　次の章の参照資料は、*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* です。

Supervisor Engine 6-E の場合

- 802.1X 拡張機能（「802.1X の設定」の章を参照）
  - 802.1X ゲスト VLAN
  - 802.1X クリティカル認証
  - Wake On LAN
  - Radius アカウンティング（Radius Accounting）
  - Radius 供給タイムアウト
- ARP QoS（「QoS の設定」の章を参照）
- Per-VLAN CTI（「QoS の設定」の章を参照）
- レイヤ 3 機能に対する Catalyst 4900M スイッチのサポート
- RSPAN（「SPAN および RSPAN の設定」の章を参照）

すべての Supervisor Engine（II-Plus ～ 6-E）

- FlexLink および FlexLink+ と MAC アドレステーブル移動更新（「FlexLink の設定」の章を参照）
- LLDP-MED：ロケーション TLV および MIB（「LLDP および LLDP-MED の設定」の章を参照）
- Auto-MDIX 無効化（「インターフェイスの設定」の章を参照）
- 拡張オブジェクトトラッキング（EOT）（Cisco IOS リリース 12.2 のマニュアルを参照）
  - EOT を使用した HSRP
  - EOT を使用した VRRP
  - EOT を使用した GLBP
  - EOT を使用した IP SLA
  - EOT を使用した信頼性の高いバックアップ スタティック ルーティング
- CFM 802.1ag（「イーサネット CFM および OAM の設定」の章を参照）
- E-OAM 802.3ah（「イーサネット CFM および OAM の設定」の章を参照）

注　マルチスパニングツリー（MST）の実装が以前のリリースから変更されました。マルチ STP（MSTP）は、IEEE 802.1s 標準に準拠しています。以前の MSTP 実装は、IEEE 802.1s 標準のドラフトに基づいていました。

リリース 12.2(44)SG の新しいハードウェア機能

注 従来のラインカードとスーパバイザエンジンに加えて、Cisco IOS ソフトウェアリリース 12.2(44)SG は、CenterFlex テクノロジーを備えた次世代の高性能 E シリーズ Supervisor Engine 6-E と、E シリーズ ラインカードおよびシャーシをサポートしています。

リリース 12.2(44)SG では、Catalyst 4500 シリーズ スイッチに次の新しいハードウェアが用意されています。

- WS-X4624-SFP-E

リリース 12.2(44)SG の新しいソフトウェア機能

リリース 12.2(44)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

注 次の章の参照資料は、*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* です。

Supervisor Engine 6-E の場合

- Supervisor Engine 6-E（SSO/NSF）の高可用性（「SSO での NSF の設定」の章を参照）
- Supervisor Engine 6-E（ISSU）の高可用性（「ISSU の設定」の章を参照）
- 組み込みの管理機能（Cisco IOS リリース 12.4 のマニュアルを参照）
- MAC 通知 MIB（Cisco IOS リリース 12.4 のマニュアルを参照）
- IPv4_BGP、IPv6_BGP（Cisco IOS リリース 12.4 のマニュアルを参照）
- 802.1X ダイナミック VLAN 割り当て（「802.1X の設定」の章を参照）
- 802.1X MAC 認証バイパス（「802.1X の設定」の章を参照）
- VX/PVID を使用した 802.1X（「802.1X の設定」の章を参照）
- 高可用性、2 + 2 10GE または 4 + 4 1GE アクティブアップリンク（「インターフェイスの設定」の章を参照）
- Enhanced Power over Ethernet サポート（「Power over Ethernet の設定」の章を参照）
- ポートごとに 8 つの設定可能なキュー（「QoS の設定」の章を参照）

すべての Supervisor Engine（II-Plus ～ 6-E）

- ISSU を使用した EEM

  詳細については、EEM のホームページを参照してください。
  http://www.cisco.com/en/US/products/ps6815/products_ios_protocol_group_home.html

- ESM

  詳細については、EEM のホームページを参照してください。
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_esm.html

- PagP+ を使用した VSS クライアント

  Catalyst 6500 スイッチで VSS デュアルアクティブを設定すると、Catalyst 4500 シリーズ スイッチは PAgP+ をサポートする VSS デュアルアクティブを検出できます。

- IP SLA（Cisco IOS リリース 12.2 のマニュアルを参照）
- 802.1ab LLDP および 802.1ab LLDP-MED（「LLDP および LLDP-MED の設定」の章を参照）
- X2 リンクデバウンスタイマー（「インターフェイスの設定」の章を参照）
- Resilient Ethernet Protocol（REP）（「REP の設定」の章を参照）

注 マルチスパニングツリー（MST）の実装が以前のリリースから変更されました。マルチ STP（MSTP）は、IEEE 802.1s 標準に準拠しています。以前の MSTP 実装は、IEEE 802.1s 標準のドラフトに基づいていました。

リリース 12.2(40)SG の新しいハードウェア機能

注 従来のラインカードとスーパバイザエンジンに加えて、Cisco IOS ソフトウェアリリース 12.2(40)SG は、CenterFlex テクノロジーを備えた次世代の高性能 E シリーズ Supervisor Engine 6-E と、E シリーズ ラインカードおよびシャーシをサポートしています。

Cisco IOS リリース 12.2(40)SG でサポートされるプライマリ E シリーズ ハードウェアには、次のものが含まれます。

- WS-C4503-E：Cisco Catalyst 4500 E シリーズ 3 スロットシャーシ、ファン、電源なし
- WS-C4506-E：Cisco Catalyst 4500 E シリーズ 6 スロットシャーシ、ファン、電源なし
- WS-C4507R-E：Cisco Catalyst 4500 E シリーズ 7 スロットシャーシ、ファン、電源なし、冗長スーパバイザ対応
- WS-C4510R-E：Cisco Catalyst 4500 E シリーズ 10 スロットシャーシ、ファン、電源なし、冗長スーパバイザ対応
- WS-X45-Sup6-E：Cisco Catalyst 4500 E シリーズ Sup 6-E、2x10GE(X2)、TwinGig 搭載
- WS-X4648-RJ45V-E：Cisco Catalyst 4500 E シリーズ 48 ポート PoE 802.3af 10/100/1000（RJ45）
- WS-X4648-RJ45V+E：Cisco Catalyst 4500 E シリーズ 48 ポート Premium PoE 10/100/1000
- WS-X4606-X2-E：Cisco Catalyst 4500 E シリーズ 6 ポート 10GbE（X2）

リリース 12.2(40)SG の新しいソフトウェア機能

リリース 12.2(40)SG は、Catalyst 4500 シリーズ スイッチに次の Cisco IOS ソフトウェア機能を提供します。

注 次の章の参照資料は、*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide* です。

Supervisor Engine 6-E でのみ使用可能

- ダイナミック マルチプロトコル Ternary Content Addressable Memory（TCAM）（「ACL によるネットワークセキュリティの設定」の章）
- サービス認識型リソース割り当て（Cisco IOS リリース 12.4 のマニュアルを参照）
- Unicast Reverse Path Forwarding（「Unicast Reverse Path Forwarding の設定」の章）

- ハードウェアでの IPv6 転送（Cisco IOS リリース 12.4 のマニュアルを参照）
- Enhanced Interior Gateway Routing Protocol IPv6 のサポート（Cisco IOS リリース 12.4 のマニュアルを参照）
- IPv6 Multicast Listener Discovery Snooping（「MLD スヌーピングの設定」の章）
- TwinGig コンバータモジュール（「インターフェイスの設定」の章）
- 堅牢で柔軟なファイル管理システム（FAT ファイルシステム）（Cisco IOS リリース 12.4 のマニュアルを参照）
- ストーム制御：ポート単位のマルチキャスト抑制（「ストーム制御の設定」の章）
- Cisco モジュラ QoS コマンドライン インターフェイス（「QoS の設定」の章）
- Two-Rate Three-Color ポリシング

Supervisor Engine II-Plus から V-10GE でのみ使用可能

- 制御パケットのキャプチャモードの選択（「ACL によるネットワークセキュリティの設定」の章）
- レイヤ 2 制御ポリシング（「QoS の設定」の章）

すべての Supervisor Engine（II-Plus ～ 6-E）で使用可能

- Gateway Load Balancing Protocol（Cisco IOS リリース 12.4 のマニュアルを参照）
- オプション 82 の拡張機能（「DHCP スヌーピング、IP ソースガード、およびスタティックホストの IPSG の設定」の章）

注 マルチスパニングツリー（MST）の実装が以前のリリースから変更されました。マルチ STP（MSTP）は、IEEE 802.1s 標準に準拠しています。以前の MSTP 実装は、IEEE 802.1s 標準のドラフトに基づいていました。

システム ソフトウェアのアップグレード

多くの場合、スイッチを Cisco IOS ソフトウェアの新しいリリースにアップグレードするときに、ROMMON をアップグレードする必要はありません。ただし、Cisco IOS ソフトウェアの以前のリリースを実行しており、これをアップグレードする計画があるときは、次の表を参照して最低限の Cisco IOS イメージと推奨される ROMMON リリースを確認してください。

注 Supervisor Engine 6-E および Supervisor Engine 6L-E で Cisco IOS リリース 12.2(54)SG を実行するには、ROMMON リリース 12.2(44r)SG5 にアップグレードする必要があります。

注意 ほとんどのスーパバイザ エンジンには、必要な ROMMON リリースがあります。ただし、警告 CSCed25996 により、ROMMON を、推奨されるリリースにアップグレードすることを推奨します。

表 8　スーパバイザ エンジンと最低限の Cisco IOS Release

スーパーバイザ エンジン	Cisco IOS Release の最低要件
IV	12.1（12c）EW または 12.1（14）E
II-Plus	12.1(19)EW

表 8　スーパバイザ エンジンと最低限の Cisco IOS Release（続き）

スーパーバイザ エンジン	Cisco IOS Release の最低要件
II-Plus-10GE	12.2(25)SG
V	12.2(18)EW
II-Plus-TS	12.2(20)EWA
V-10GE	12.2(25)EW
ME-X4924-10GE	12.2(31)SGA
6-E	12.2(40)SG
6L-E	12.2(52)XO

表 9　スーパバイザ エンジンと推奨される ROMMON リリース

スーパーバイザ エンジン	最低限の ROMMON リリース	推奨される ROMMON リリース
IV	12.1（12r）EW	12.2（31r）SGA1
II-Plus	12.1（19r）EW	12.2（31r）SGA1
II-Plus-10GE	12.2（25r）SG	12.2(31r)SGA3
V	12.1（20r）EW1	12.2（31r）SGA1
II-Plus-TS	12.2（20r）EW	12.2（31r）SGA1
V-10GE	12.2（25r）EW	12.2(31r)SGA3
ME-X4924-10GE	12.2（25r）EW	12.2（31r）SGA1
6-E	12.2(44r)SG5	12.2(44r)SG5
6L-E	12.2(44r)SG5	12.2(44r)SG5

表 10　ROMMON リリースと Promupgrade プログラム

ROMMON リリース	Promupgrade プログラム
12.1（11br）EW	cat4000-sup3-promupgrade-121_11br_EW
12.1（12r）EW	cat4000-sup3-promupgrade-121_12r_ew
12.1（19r）EW	cat4000-ios-promupgrade-121_19r_EW
12.1（20r）EW1	cat4000-ios-promupgrade-121_20r_EW1
12.1（20r）EW2	cat4000-ios-promupgrade-121_20r_EW2
12.2（20r）EW	cat4000-ios-promupgrade-122_20r_EW
12.2（20r）EW1	cat4000-ios-promupgrade-122_20r_EW1
12.2（31r）SG3	cat4500-ios-promupgrade-122_31r_SG3
12.2（31r）SGA1	cat4500-ios-promupgrade-122_31r_SGA1
12.2(31r)SGA	cat4500-e-ios-promupgrade-122_31r_SGA3
12.2（40r）SG	cat4500-e-ios-promupgrade-122_40r_SG
12.2（44r）SG1	cat4500-e-ios-promupgrade-122_44r_SG1
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5

ここでは、スイッチ ソフトウェアをアップグレードする方法について説明します。

+E シャーシと ROMMON の識別

+E シャーシは、シャーシの idprom の FRU マイナー値によって識別されます。

スーパバイザエンジン 1（sup1）が ROMMON で、スーパバイザエンジン 2（sup2）が IOS の場合、sup2 のみがシャーシの idprom に含まれる idprom の内容を読み取ることができます。シャーシタイプは、show version コマンドの出力で「+E」と表示されます。逆に、sup1 はシャーシタイプを「E」としてのみ表示できます。

sup1 と sup2 の両方が ROMMON の場合、両方のエンジンがシャーシの idprom を読み取ることができます。シャーシタイプは、show version コマンドの出力で正しく「+E」と表示されます。

sup1 と sup2 の両方が IOS の場合、両方のエンジンがシャーシの idprom を読み取ることができます。シャーシタイプは、**show version** コマンドの出力で正しく「+E」と表示されます。

ROMMON アップグレードに関する注意事項

注意 スーパバイザ エンジンに新バージョンの ROMMON が付属している場合、ダウングレードしないでください。新しい ROMMON には、コンポーネントのハードウェア リビジョンに基づいたボード設定があるため、古い設定では動作しません。

コンソールからのスーパバイザ エンジン ROMMON のアップグレード

注意 システムが起動しなくなる可能性のある操作を避けるため、このセクション全体を読んでからアップグレードを開始してください。

注 この例では、プログラム可能な読み取り専用（PROM）アップグレード バージョン 12.1（20r）EW1 および Cisco IOS Release 12.1（20）EW1 を使用します。その他のリリースでは、ROMMON リリースと Cisco IOS ソフトウェア リリースを、適切なリリースおよびファイル名に置き換えます。

スーパバイザ エンジン ROMMON をアップグレードするには、次の手順に従います。

ステップ 1 シリアル ケーブルを、スーパバイザ エンジンのコンソール ポートに直接接続します。

注 ここでは、コンソールのボー レートが 9600(デフォルト)に設定されているものとします。別のボー レートを使用する場合は、スイッチのコンフィギュレーション レジスタの値を変更します。

ステップ 2 Cisco.com から cat4000-ios-promupgrade-121_20r_EW1 プログラムをダウンロードし、アップグレードするスイッチからアクセスできるディレクトリにある TFTP サーバ上に配置します。

cat4000-ios-promupgrade-121_20r_EW1 プログラムは、Cisco.com の Catalyst 4000 システム イメージをダウンロードした同じ場所から入手できます。

ステップ 3 **dir bootflash:** コマンドを使用して、フラッシュメモリに PROM アップグレードイメージを格納するのに十分なスペースがあることを確認します。領域が不足している場合は、1 つ以上のイメージを削除してから **squeeze bootflash:** コマンドを入力し、領域を再要求します。

Compact Flash カードを使用している場合は、bootflash: を slot0: に置き換えます。

ステップ 4 copy tftp コマンドを使用して、cat4000-ios-promupgrade-121_20r_EW1 プログラムをフラッシュメモリにダウンロードします。

次に、リモート ホスト 172.20.58.78 から PROM アップグレード イメージ cat4000-ios-promupgrade-121_20r_EW1 をダウンロードしてブートフラッシュする例を示します。

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

ステップ 5 reload コマンドを入力してスイッチをリセットし、Ctrl キーを押した状態で C キーを押してブートプロセスを停止してから ROMMON をもう一度入力します。

次に、ROMMON にリセットした後の出力の例を示します。

```
Switch# reload
Proceed with reload? [confirm]

03:57:16:%SYS-5-RELOAD:Reload requested



**********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X4515 System.            *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.1(12r)EW


.
.(output truncated)
```

.

```
 Established physical link 100MB Half Duplex
 Network layer connectivity may take a few seconds
rommon 1 >
```

ステップ 6 次のコマンドを入力して PROM アップグレードプログラムを実行します。
boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

注意 アップグレードの完了に、ユーザによる対処は必要ありません。アップグレードを正常に完了させるために、アップグレード プロセスを中断しないでください。アップグレードが完了するまでは、リセット、電源の再投入、またはスーパバイザ エンジンの OIR を行わないでください。

次に、アップグレードが正常に完了したときの出力とシステム リセットの例を示します。

```
rommon 2 > boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

************************************************************
 *                                                          *
 * Rom Monitor Upgrade Utility For WS-X4515 System        *
 * This upgrades flash Rom Monitor image to the latest     *
 *                                                          *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.         *
 * All rights reserved.                                     *
 *                                                          *
 ************************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!

 Beginning erase of 0x80000 bytes at offset 0x3f80000...  Done!

 Beginning write of prom  (0x4e8ec bytes at offset 0x3f80000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
```

ステップ 7 Cisco IOS ソフトウェアイメージを起動して、show version コマンドを入力し、ROMMON が 12.1(20r)EW1 にアップグレードされていることを確認します。

ステップ 8 delete コマンドを使用してブートフラッシュから PROM アップグレードプログラムを削除し、squeeze コマンドを使用して未使用領域を再要求します。

次に、ブートフラッシュから cat4000-ios-promupgrade-121_20r_EW1 イメージを削除し、未使用領域を再要求する例を示します。

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

ステップ 9 show version コマンドを使用して、ROMMON がアップグレードされたことを確認します。

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L3 Switch Software (cat4500-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC

ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-i9s-mz.121-20.EW1"

cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

Configuration register is 0x2102

Switch#
```

ROMMON がアップグレードされました。

スイッチ上で Cisco IOS ソフトウェアをアップグレードする手順については、「Cisco IOS ソフトウェアのアップグレード」セクション（54 ページ）を参照してください。

Telnet を使用したスーパバイザ エンジン ROMMON のリモートでのアップグレード

注意 システムが起動しなくなる可能性のある操作を避けるため、このセクション全体を読んでからアップグレードを開始してください。

スーパバイザ エンジン ROMMON を Release 12.1(20r)EW1 にアップグレードするには、次の手順に従います。この手順は、コンソール アクセスが利用できないときや ROMMON アップグレードをリモートで実行する必要があるときに使用できます。

注 次の項では、PROM アップグレード バージョン cat4000-ios-promupgrade-121_20r_EW1 を使用します。

ステップ 1 スーパバイザ エンジンへの Telnet セッションを確立します。

注 次の説明では、少なくとも 1 つの IP アドレスが SVI または経路選択済みのポートに割り当てられているものとします。

ステップ 2 Cisco.com から cat4000-ios-promupgrade-121_20r_EW1 プログラムをダウンロードし、アップグレードするスイッチからアクセスできるディレクトリにある TFTP サーバ上に配置します。

cat4000-ios-promupgrade-121_20r_EW1 プログラムは、Cisco.com の Catalyst 4500 システム イメージをダウンロードした同じ場所から入手できます。

ステップ 3 **dir bootflash:** コマンドを使用して、フラッシュメモリに PROM アップグレードイメージを格納するのに十分なスペースがあることを確認します。領域が不足している場合は、1 つ以上のイメージを削除してから **squeeze bootflash:** コマンドを入力し、領域を再要求します。

コンパクトフラッシュ カードを使用している場合は、**bootflash:** を **slot0:** に置き換えます。

ステップ 4 copy tftp コマンドを使用して、cat4000-ios-promupgrade-121_20r_EW1 プログラムをフラッシュメモリに ダウンロードします。

次に、リモート ホスト 172.20.58.78 から PROM アップグレード イメージ cat4000-ios-promupgrade-121_20r_EW1 をダウンロードしてブートフラッシュする例を示します。

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

ステップ 5 no boot system flash bootflash:file_name コマンドを使用して、構成ファイル内のすべての BOOT 変数コマンドをクリアします。この例では、BOOT 変数は、ブートフラッシュからイメージ cat4000-i5s-mz.121-19.EW1.bin を起動するよう設定されています。

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-i5s-mz.121-19.EW1.bin
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#

Use the boot system flash bootflash:file_name command to set the BOOT variable. You will
use two BOOT commands: one to upgrade the ROMMON and a second to load the Cisco IOS
software image after the ROMMON upgrade is complete. Notice the order of the BOOT
variables in the example below. At bootup the first BOOT variable command upgrades the
ROMMON. When the upgrade is complete the supervisor engine will autoboot, and the second
BOOT variable command will load the Cisco IOS software image specified by the second BOOT
command.
```

注 **config-register** は、autoboot に設定する必要があります。

```
In this example, we assume that the console port baud rate is set to 9600 bps and that the
config-register is set to 0x0102.

Use the config-register command to autoboot using image(s) specified by the BOOT variable.
Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after
the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version
12.1(20r)EW1. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 12.1(20)EW1.

config-register to 0x0102.
```

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# boot system flash bootflash:cat4000-i9s-mz.121-20.EW1
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

ステップ 6 起動文字列を確認するには、show bootvar コマンドを使用します。この例の BOOT 変数は、最初に PROM アップグレードを実行してから ROMMON をアップグレードします。その後、アップグレード ソフトウェアがリロードされ、スーパバイザ エンジンにより Cisco IOS イメージがロードされます。

```
Switch# sh bootvar
BOOT variable = bootflash:cat4000-ios-promupgrade-121_20r_EW1,1;bootflash:cat400
0-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

ステップ 7 reload コマンドを実行して、PROM アップグレードプログラムを実行します。このコマンドを実行すると、Telnet セッションの接続が終了します。

注意 ステップ 6 の起動設定を確認してください。アップグレードの完了に、ユーザによる対処は必要ありません。アップグレードを正常に完了させるために、アップグレード プロセスを中断しないでください。アップグレードが完了するまでは、リセット、電源の再投入、またはスーパバイザ エンジンの OIR を行わないでください。

次に、正常に ROMMON アップグレードが完了したときのコンソール ポートの出力とシステム リセットの例を示します。ROMMON アップグレード中は Telnet セッションの接続が切断されるため、この出力は表示されません。このステップの処理には、2 ～ 3分かかることがあります。Telnet セッションは、Cisco IOS ソフトウェア イメージとインターフェイスがロードされてから 2 ～ 3 分後に再接続する必要があります。

```
Switch#reload
Proceed with reload? [confirm]

1d05h: %SYS-5-RELOAD: Reload requested



 ********************************************************
 *                                                      *
 * Welcome to Rom Monitor for WS-X4515 System.          *
 * Copyright (c) 2002 by Cisco Systems, Inc.            *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 2, Board revision 7
 Swamp FPGA revision 28, Dagobah FPGA revision 86

***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
 . . . . .
```

```
 Established physical link 100MB Full Duplex
 Network layer connectivity may take a few seconds


 ******** The system will autoboot now ********


 config-register = 0x0102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1



 ********************************************************
 *                                                      *
 * Rom Monitor Upgrade Utility For  WS-X4515 System     *
 * This upgrades flash Rom Monitor image to the latest  *
 *                                                      *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.      *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!

 Beginning erase of 0x80000 bytes at offset 0x3f80000...  Done!

 Beginning write of prom  (0x4e8ec bytes at offset 0x3f80000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
.
.(output truncated)
.
******** The system will autoboot now ********


 config-register = 0x0102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4000-i9s-mz.121-20.EW1

Rommon reg: 0x56000380

Running IOS...

Decompressing the image
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################## [OK]
```

ステップ 8 no boot system flash bootflash:file_name コマンドを使用して、ROMMON のアップグレードに使用した BOOT コマンドをクリアします。

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

ステップ 9 show version コマンドを使用して、ROMMON がアップグレードされたことを確認します。

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC

ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4000-i9s-mz.121-20.EW1"

cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

Configuration register is 0x0102

Switch#
```

ステップ 10 delete コマンドを使用してブートフラッシュから PROM アップグレードプログラムを削除し、squeeze コマンドを使用して未使用領域を再要求します。

次に、ブートフラッシュから cat4000-ios-promupgrade-121_20r_EW1 イメージ削除し、使用されていないスペースを再要求する例を示します。

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

ステップ 11 show bootvar コマンドを使用して、ROMMON アップグレードプログラムが BOOT 変数から削除されたことを確認します。

```
Switch#sh bootvar
BOOT variable = bootflash:cat4000-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0102
```

ROMMON がアップグレードされました。

スイッチ上で Cisco IOS ソフトウェアをアップグレードする手順については、「Cisco IOS ソフトウェアのアップグレード」セクション（54 ページ）を参照してください。

Cisco IOS ソフトウェアのアップグレード

注意 システムが起動しなくなる可能性のある操作を避けるため、このセクション全体を読んでからアップグレードを開始してください。

続行する前に、次のホスト名の規則に従ってください。

- 大文字小文字の区別を保持することはできません。

  多くのインターネット ソフトウェア アプリケーションでは、大文字と小文字は区別されません。名前は英語と同様に大文字で始めるのが適切であるように思われますが、規則によりコンピュータ名はすべて小文字で表示されます。詳細については、RFC 1178 の『Choosing a Name for Your Computer』を参照してください。
- 名前は文字で始まり、文字または数字で終了する必要があります。
- 内側の文字には、文字、数字、およびハイフンを使用できます。ピリオドとアンダースコアは使用できません。
- 名前は 63 文字以下にする必要があります。ただし、ホスト名は 10 文字以下にすることを推奨します。
- ほとんどのシステムでは、ホスト名と CLI のプロンプトに 30 文字のフィールドが使用されています。コンフィギュレーション モードのプロンプトが長くなると、切り詰められることがあります。

Catalyst 4500 シリーズ スイッチ上の Cisco IOS ソフトウェアをアップグレードするには、次の手順に従います。

ステップ 1 Cisco.com から Cisco IOS Release 12.1(20)EW をダウンロードし、アップグレードするスーパバイザ エンジンからアクセスできるディレクトリにある TFTP サーバに置きます。

ステップ 2 dir bootflash: コマンドを使用して、フラッシュメモリに promupgrade イメージを格納するのに十分な領域があることを確認します。十分な領域がない場合、1 つ以上のイメージを削除してから、squeeze bootflash: コマンドを入力して領域を再要求します。

コンパクトフラッシュ カードを使用している場合は、**bootflash** の代わりに **slot0:** を使用します。

ステップ 3 **copy tftp** コマンドを使用して、ソフトウェアイメージをフラッシュメモリにダウンロードします。

次に、リモートホスト 172.20.58.78 からブートフラッシュに Cisco IOS ソフトウェアイメージ cat4000-is-mz.121-12c.EW をダウンロードする例を示します。

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-is-mz121_12c.EW]?
Destination filename [cat4000-is-mz.121-12c.EW]?
Accessing tftp://172.20.58.78/cat4000-is-mz.121-12c.EW...
Loading cat4000-is-mz.121-12c.EW from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
|!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6923388/13846528 bytes]

6923388 bytes copied in 72.200 secs (96158 bytes/sec)
Switch#
```

ステップ 4　**no boot system flash bootflash:***file_name* コマンドを使用して cat4000-is-mz.121-8a.EW ファイルをクリアし、BOOT 変数に保存します。

次に、BOOT 変数をクリアする例を示します。

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-is-mz.121-8a.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

ステップ 5　boot system flash コマンドを使用して、Cisco IOS ソフトウェアイメージを BOOT 変数に追加します。

次に、cat4000-is-mz.121-12c.EW イメージを BOOT 変数に追加する例を示します。

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-12c.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

ステップ 6　**config-register** コマンドを使用して、コンフィギュレーション レジスタを 0x2102 に設定します。

次に、コンフィギュレーション レジスタの 2 番目に重要ではないビットを設定する例を示します。

```
Switch# configure terminal
Switch(config)# config-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

ステップ 7　reload コマンドを入力してスイッチをリセットし、ソフトウェアをロードします。

注意　アップグレードの完了に、ユーザによる対処は必要ありません。アップグレードを正常に完了させるために、最低でも 5 分間は、アップグレード プロセスを中断することがないよう、リセット、電源の再投入、またはスーパバイザ エンジンの OIR を行わないでください。

次に、アップグレードが正常に完了したときの出力とシステム リセットの例を示します。

```
Switch# reload
Rommon reg: 0x2B004180
```

```
Upgrading FPGA...

Decompressing the image
############### [OK]

 ******************************************************
 *                                                    *
 * WS-X4014 FPGA Upgrade Utility For WS-X4014 Machines *
 *                                                    *
 * Copyright (c) 2002 by Cisco Systems, Inc.          *
 * All rights reserved.                               *
 *                                                    *
 ******************************************************

 Image size = 483.944 KBytes

 Maximum allowed size = 1023.75 KBytes


 Upgrading your FPGA image... DO NOT RESET the system
 unless instructed or upgrade of FPGA will fail !!!

 Beginning erase of 0x100000 bytes at offset 0x3d00000...  Done!

 Beginning write of fpga image  (0x78fb0 bytes at offset 0x3d00000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! FPGA image has been upgraded successfully.
 System will reset itself and reboot in about 15 seconds.
 0



 ********************************************************
 *                                                      *
 * Welcome to Rom Monitor for WS-X4014 System.          *
 * Copyright (c) 2002 by Cisco Systems, Inc.            *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 1, Board revision 5
 Swamp FPGA revision 16, Dagobah FPGA revision 47


 MAC Address  : 00-30-85-XX-XX-XX
 IP Address   : 10.10.10.91
 Netmask      : 255.255.255.0
 Gateway      : 10.10.10.1
 TftpServer   : Not set.
 Main Memory  : 256 MBytes

 ***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
Switch#
```

ステップ 8 show version コマンドを使用して、新しい Cisco IOS リリースがスイッチ上で動作していることを確認します。

制限事項

以降の項では、Catalyst 4500 シリーズ スイッチの Cisco IOS ソフトウェアの現在のリリースに関する制限と制約事項について説明します。

すべてのスーパバイザエンジン

- permit any any ? コマンドを入力すると、Cisco IOS リリース 12.2(54)SG ではサポートされていない octal オプションを確認できます。

  CSCsy31324

- fa1 の SPAN の宛先はサポートされていません。
- 「keepalive」CLIは、スイッチのインターフェイスモードではサポートされていませんが、実行コンフィギュレーションには表示されます。この動作による機能への影響はありません。
- TDR は、オープンまたはショートケーブル状態の 1000BaseT のインターフェイス Gi1/1 ー Gi1/48 でのみサポートされています。TDR の長さの解像度は +/- 10 m です。ケーブルが 10 m 未満の場合、またはケーブルが適切に終端されている場合、TDR の結果には「0」m と表示されます。インターフェイス速度が 1000BaseT ではない場合、「unsupported」という結果ステータスが表示されます。ジャックパネルまたはパッチパネルを使用して延長されたケーブルについては、TDR の結果は信頼できません。
- Fast UDLD には、次のガイドラインが適用されます。
  - Fast UDLD は、デフォルトではディセーブルに設定されています。
  - Fast UDLD をサポートするネットワーク デバイス間のポイントツーポイント リンクでのみ、Fast UDLD を設定します。
  - Fast UDLD は、通常モードでもアグレッシブ モードでも設定できます。
  - Fast UDLD ポートでは、link debounce コマンドを入力しないでください。
  - 互いに接続されたネットワーク デバイス間の少なくとも 2 つのリンクで Fast UDLD を設定します。これにより、誤検出が原因で、Fast UDLD が誤ってリンクを無効にするエラーが発生する可能性が低くなります。
  - 同じネイバー デバイスに対する複数のリンクで同じエラーが同時に発生した場合、Fast UDLD は単一方向リンクを報告しません。
- XML-PI 仕様ファイルのエントリが目的の CLI 出力を返しません。

  show ip route や show access-lists などの特定のコマンドの出力には、非決定的テキストが含まれています。出力は簡単に理解できますが、出力テキストには一貫して出力される文字列が含まれていません。汎用仕様のファイルエントリでは、考えられるすべての出力は解析できません。

  回避策（1）:

  汎用仕様のファイルエントリは使用できない場合がありますが、出力に確実に含まれているテキストを検索することで、目的のテキストを返す仕様ファイルエントリが作成される場合があります。出力に文字列が含まれていることが確実な場合は、解析に使用できます。

たとえば、show ip access-lists SecWiz_Gi3_17_out_ip コマンドの出力は次のようになります。

```
Extended IP access list SecWiz_Gi3_17_out_ip
    10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
    20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
    30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

最初の行は、出力にアクセスリストが含まれていることが確実であるため、簡単に解析できます。

```
<Property name="access list" alias="Name" distance="1.0" length="-1" type="String"
/>
```

残りの行にはすべて、host という用語が含まれています。その結果、その文字列を指定することによって仕様ファイルで必要な値が報告される場合があります。たとえば、次の行

```
<Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

これによって、最初のルールと 2 番目のルールに対して次を生成します。

```
<rule>
    deny
</rule>
```

3 番目のステートメントについては次のとおりです。

```
<rule>
    permit
<rule>
```

回避策（2）:

NETCONF を使用して show running-config コマンドの出力を要求し、目的の文字列の出力を解析します。これは、目的の行に共通点がない場合に便利です。たとえば、次の例に示すように、このアクセスリストのルールには共通の文字列と順序（3 つの permit、次に deny、次に別の permit）が含まれていないため、仕様ファイルのエントリで検索文字列として permit を使用できません。

```
Extended MAC access list MACCOY
    permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
    permit any host 65de.edfe.fefe xns-idp
    permit any any protocol-family rarp-non-ipv4
    deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
    permit any any
```

show running-config コマンドの XML 出力には、必要に応じてプログラムによって解析できる次の内容が含まれています。

```
<mac><access-list><extended><ACLName>MACCOY</ACLName></extended></access-list></mac>
    <X-Interface> permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000
appletalk</X-Interface>
    <X-Interface> permit any host 65de.edfe.fefe xns-idp</X-Interface>
    <X-Interface> permit any any protocol-family rarp-non-ipv4</X-Interface>
    <X-Interface> deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c
dec-spanning</X-Interface>
    <X-Interface> permit any any</X-Interface>
```

- Catalyst 4500 シリーズ スイッチは、Cisco IOS リリース 12.2(46)SG および以前のリリースで使用されているレガシー 802.1X コマンドを引き続きサポートします（つまり、CLI で受け入れられます）が、CLI ヘルプメニューには表示されません。
- 現在の IOS ソフトウェアは、64 文字を超えるファイル名をサポートできません。

- すべてのソフトウェアリリースで、最大 32,768 の IGMP スヌーピング グループ エントリがサポートされています。
- source-interface キーワードを使用する設定で、セカンダリプライベート VLAN に関連付けられた SVI を指定すると、スイッチのリロード時にセカンダリ VLAN に関連する設定が失われる可能性があります。このような状況では、常にプライマリプライベート VLAN を使用します。

Supervisor Engine II+ Plus ー V-10GE の場合

- IP アンナンバード機能では、次の機能がサポートされていません。
  - ダイナミック ルーティング プロトコル
  - HSRP/VRRP
  - スタティック ARP
  - 別の VRF でのアンナンバード インターフェイスとナンバードインターフェイス
- WCCP バージョン 2 では、次はサポートされていません。
  - GRE カプセル化フォワーディング メソッド
  - ハッシュ バケット ベースの割り当てメソッド
  - 出力インターフェイスのリダイレクション（外部へのリダイレクション）
  - リダイレクトリスト ACL
- IPX ソフトウェア ルーティングでは、次はサポートされていません。
  - NHRP（Next Hop Resolution Protocol）
  - NLSP
  - ジャンボ フレーム
- AppleTalk ソフトウェア ルーティングでは、次はサポートされていません。
  - AURP
  - PPP の AppleTalk コントロール プロトコル
  - ジャンボ フレーム
  - EIGRP
- NetFlow 機能には、次の制限が適用されます。
  - NetFlow では、制御パケット、リンクレベルのエラーが発生したパケット、および ARP/RARP パケットは考慮されません。
  - NetFlow のソフトウェアキャッシュは固定されています。ユーザはサイズを変更できません。
  - さまざまなパケット サイズの分布を示す統計分布の行は、表示されません。
- PBR 機能には、次の制限が適用されます。
  - パケットの長さをベースにした一致基準はサポートされていません。
  - IP Precedence、TOS および Qos グループは固定されていません。
  - ACL/ルートマップ統計情報は更新されません。
- IGRP はサポートされていません（代わりに EIGRP を使用）。

- MAC アドレステーブルは、802.1s または 802.1w スパニングツリープロトコルのいずれかが設定されている場合、スーパバイザエンジンを切り替えるとクリアされます。アドレスのクリアとそれに伴うパケットのフラッディングを最小限に抑えるには、エッジポートを spanning-tree portfast に、リンクタイプを spanning-tree link-type point-to-point に設定します。
- NSF および IS-IS IETF モードの実行中に、issu loadversion コマンドを入力してから 5 分以内に issu runversion コマンドを入力すると、ISSU のアップグレード中にパケット損失が発生することがあります。

  回避策：NSF インターバルタイマーを 0 分に設定するか、NSF インターバルタイマーの期限が切れて NSF が再起動するまで issu runversion コマンドの入力を遅らせます。
- スイッチで NSF が有効になっている場合、ルートがルーティングプロトコル間で正しく再配布されない可能性があります。ルートが正しく再配布されるかどうかは、NSF スイッチオーバー後のルーティング プロトコルの収束順序によって決まります。

  回避策：ありません。
- IP クラスフルルーティングはサポートされていません。no ip classless コマンドを使用しないでください。このコマンドはクラスレスルーティングのみをサポートしているため、無効になります。クラスレスルーティングがデフォルトで有効になっているため、ip classless コマンドはサポートされていません。
- Catalyst 4510R スイッチでは、Supervisor Engines II-Plus、III、IV、および II-Plus-10GE はサポートされていません。サポートされていないスーパバイザ エンジンをインストールすると、ソフトウェアで制御できない予期しない動作がハードウェアで発生する可能性があります。サポート対象外のスーパバイザエンジンを冗長スロットに挿入して使用すると、他のスロットに挿入されているサポート対象のスーパバイザエンジンが誤作動する可能性があります。
- Supervisor Engine II-Plus は、以前のリリースの Supervisor Engine III または Supervisor Engine IV でフォーマットされたコンパクトフラッシュ カードを読み取ることができません。
- スタートアップ ファイルの VLAN 設定が VLAN データベース ファイルに格納されている情報と一致しない場合、Catalyst 4500 スーパバイザ エンジンが正しく初期化されません。この現象は、バックアップ設定ファイルが使用された場合に生じることがあります。
- レイヤ 2 LACP チャネルを、スパニングツリー PortFast 機能で設定することはできません。
- ブートローダ イメージを使用するネットブーティングは、サポートされていません。他の方法については、「トラブルシューティング」セクション（468 ページ）を参照してください。
- リリース 12.1(13)EW（以降）を実行した後で、Cisco IOS リリース 12.1(8a)EW1 にダウングレードすることはできません。ダウングレードする必要がある場合、警告 CSCdz59058 について TAC 担当者にお問い合わせください。
- Catalyst 4507R シャーシに冗長スーパバイザエンジンを導入する場合、スタートアップ コンフィギュレーション ファイルの解析中は、存在しないハードウェアには構成ファイルが適用されないという Cisco IOS ソフトウェアの標準的な動作を確認してください。

  たとえば、アクティブなスーパバイザエンジンがスロット 1 にあり、インターフェイス Gi1/1 が設定されている場合、シャーシからアクティブなスーパバイザエンジンを取り外すと、スロット 2 にあるスーパバイザエンジンがアクティブになります。また、スタートアップ コンフィギュレーション ファイルの解析中にインターフェイス Gi1/1 が存在していないことを示すエラーメッセージが表示されます。これは、正常な動作です。以前のアクティブ スーパバイザ エンジンをスロット 1 に再挿入しても、インターフェイス Gi1/1 の設定は残っていません。

  この現象は、両方のスーパバイザエンジンがシャーシに挿入されている場合は発生しません。

  回避策：スタートアップ コンフィギュレーション ファイルを実行コンフィギュレーションにコピーします。

  ```
  Switch# copy startup-config running-config
  ```

- モバイル IP に対してサポートされていないデフォルト CLI が HSRP 設定に表示されます。この CLI はシステムに損害を与えませんが、混乱を避けるために削除することをお勧めします。

  回避策：show standby コマンドを使用して設定を表示し、CLI を削除します。次に、show standby GigabitEthernet1/1 コマンドの出力例を示します。

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- HSRP プリエンプション遅延を一貫して機能させるには、standby delay minimum コマンドを使用する必要があります。遅延を 1 つ以上の hello 間隔に設定して、HSRP が開始状態を終了する前に hello が受信されるようにしてください。

  イメージのリロード後にルータがリブートする場合は、standby delay reload オプションを使用します。

- Cisco 製ルータとサードパーティ製のルータ間で OSPF を実行しようとすると、2 つのインターフェイスが Exstart/Exchange の状態で止まってしまう可能性があります。この問題は、ネイバールータのインターフェイス間で最大伝送単位（MTU）設定が一致しない場合に発生します。より高速に MTU を設定したルータではネイバールータの MTU 設定よりも大きなパケットが送信されるため、ネイバールータはこのパケットを無視します。

  回避策：問題は MTU の設定の不一致により生じるため、他の MTU と一致するようにいずれかのルータの MTU を変更する必要があります。

- Supervisor Engine III および Supervisor Engine IV では .1q-in-.1q パケットパススルーを実行できますが、Supervisor Engine II+10GE、Supervisor Engine V、および Supervisor Engine V-10GE では .1q-in-.1q カプセル化のみ実行できます。
- PVST および Catalyst 4500 E シリーズ スイッチの VLAN では、Cisco IOS リリース 12.1(13)EW は最大 3000 のスパニング ツリー ポート インスタンスをサポートしています。これより多くのインスタンスを使用する場合は、PVST ではなく MST を使用してください。
- ISL トランクとして設定できるのは、WS-X4418-GB モジュールのポート 1 およびポート 2 と WS-X4412-2GB-T モジュールのポート 13 およびポート 14 のみです。
- 送信キュー シェーピングまたはコンフィギュレーションの共有により元のパケットが損失しても、引き続き SPAN ポートで SPAN パケットのコピーを送信できます。
- すべてのソフトウェア リリースにおいて、100,000 以上のルータを使用しないでください。
- パフォーマンス上の理由により設定された ACL を使用して、すべてのインターフェイスで no ip unreachables コマンドを使用してください。
- レイヤ 3 パスのロードバランシング メトリックは、Cisco IOS リリース 12.1(8a)EW、12.1(11b)EW、12.1(12c)EW、12.1(13)EW、12.1(19)EW、および 12.1(20)EW ではサポートされていません。（CSCdv10578）
- Dynamic ARP Inspection（DAI）の err-disable 機能のしきい値は、インターフェイスごとに 15 ARP パケット/秒に設定されています。このしきい値は、ネットワーク構成に応じて調整する必要があります。CPU は、持続レートが 1000 pps を超える DHCP パケットは受信しません。
- 制限数の ACL バインディングは、Catalyst 4500 シリーズ スイッチ Supervisor Engine II-Plus の IP ソース ガード機能により動的にインストールされます。IP ソースガード機能を最大限に活用するには、Supervisor Engine IV を使用する必要があります。
- レイヤ 3 ポートに IP アドレスまたは IPv6 アドレスを設定した後、switchport コマンドでレイヤ 3 ポートをレイヤ 2 ポートに変更し、再度レイヤ 3 ポートに戻すと、元の IP/IPv6 アドレスが失われます。
- デフォルトでは、IPv6 はディセーブルになります。IPv6 をルートするには、IPv6 unicast-routing コマンドを入力する必要があります。IPv6 マルチキャストルーティングを使用する予定の場合は、IPv6 multicast-routing コマンドを使用してください。

- デフォルトでは、CEF の IPv6 はディセーブルになります（IPv6 ユニキャスト ルーティングがイネーブルになった後）。IPv6 トラフィックがプロセススイッチングされるのを防ぐには、IPv6 cef コマンドを使用します。
- コミュニティ VLAN のマルチキャスト ソースは、サポートされていません。
- 双方向コミュニティ VLAN は、サポートされていません。
- 音声 VLAN は、コミュニティ VLAN ホスト インターフェイスではサポートされていません。
- プライベート VLAN トランクには、コミュニティ VLAN は含まれません。
- WS-4516 モジュールでプライベート VLAN を使用する場合、手動でエントリをクリアしないと、古い ARP エントリは ARP キャッシュからタイムアウトされません。このイベントによる運用への影響はありません。
- Cisco IOS リリース 12.2(20)EW でフォーマットされた Compact Flash は、Supervisor Engine V-10GE システムと Supervisor V-10GE 以外のシステムの両方のリリース 12.2(25)EW でフォーマットし直す必要があります。その他のリリースでフォーマットされた Compact Flash は、Supervisor Engine V-10GE 以外のシステムでフォーマットし直す必要はありません。
- 冗長システムでは、アクティブ スーパバイザ エンジンの起動中にスタンバイ スーパバイザ エンジンの取り外しや再挿入を行わないでください。これを行うと、オンライン診断テストでエラーが発生する可能性があります。

  回避策：スタンバイ スーパバイザ エンジンの取り外しまたは再挿入はアクティブなスーパバイザエンジンを起動してから行ってください。（CSCsa66509）
- 10 スロットシャーシと組み合わせて使用する場合、Supervisor Engine V は 10 スロット目の Catalyst 4500 シリーズ 2 ポート ギガビット イーサネット ラインカード（WS-X4302-GB）のみサポートします。
- switchport private-vlan mapping trunk コマンドでサポートされる一意のプライベート VLAN ペアの 最大数は 500 です。たとえば、1000 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、1000 のセカンダリ VLAN を 1000 のプライマリ VLAN に 1 対 1 でマッピングしたりすることができます。
- PoE のサポートは、PoE をサポートするラインカードおよび電源装置を使用しているかどうかによって異なります。

  PoE スイッチング モジュール：
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - WS-X4548-GB-RJ45V+

  PoE 対応電源：
  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - PWR-C45-6000ACV

- PVLAN 無差別トランク ポートを設定するための最大マッピング数は、500 プライマリ VLAN から 500 セカンダリ VLAN です。
- NAC LAN ポートの IP 機能では、802.1X アクセス不能認証バイパス機能はサポートされていません。
- line console 0 コンフィギュレーション モードのコンソール速度を変更しても、ROMMON のコンソール速度には影響しません。ROMMON にも同じコンソール速度を適用するには、confreg ROMMON ユーティリティを使用します。
- Supervisor Engine II-Plus では、Cisco IOS リリース 12.2(19)EW より前の Cisco IOS イメージによってフォーマットされた Compact Flash はサポートされません。
- Catalyst 4500 シリーズ スイッチが Cisco Secure Access Control Server（ACS）からの情報を要求すると、サーバが応答しないためメッセージの交換がタイムアウトし、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、スイッチが ACS に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。
- BGP ルータ コンフィギュレーション モードでは、bgp shutdown コマンドはサポートされていません。このコマンドを入力すると、予期しない結果が発生する可能性があります。
- アイドル タイムアウトの後に SSH 接続が切断されると、スプリアス エラー メッセージが表示されます。

  回避策：アイドルタイムアウトを無効にします。（CSCec30214）
- モジュール WS-X4148-RJ45V のインターフェイスで、スイッチとメディア コンバータの両方が 100 Mbps 全二重で動作するように設定されていると、Daiden DN-2800G メディア コンバータのリンクが確立されないことがあります。この現象は、power inline auto コマンドでモジュールのインターフェイスが自動的にデバイスインラインの検出および電源投入を行うよう設定されている場合に発生します。この警告は、すべてのソフトウェア リリースに記載されています。

  回避策：

  1. power inline never コマンドを使用して、スイッチポートでのインラインの電源投入を無効にします。

  2. メディア コンバータで、速度とデュプレックスを 100 Mbps の全二重で動作せずに自動ネゴシエーションするように設定します。（CSCee62109）
- スタティックホストの IPSG は、IPSG と同じポートモードをサポートしますが、トランクポートはサポートしません。
  - レイヤ 2 アクセス ポートおよび PVLAN ホスト ポート（独立ポートまたはコミュニティ ポート）をサポートしています。
  - トランク ポート、レイヤ 3 ポート、または EtherChannel はサポートされません。
- スタティック ホストの IPSG は、アップリンク ポートでは使用しないでください。
- Selective DBL では、タグなし IP パケットとシングルタグ IP パケットのみサポートされています。非 IP パケット（Q-in-Q や IPX など）で Selective DBL に近い機能を実現するには、CoS 値と一致する入力ポリシーマップを適用して、クラスマップの DBL を指定します。
- Selective DBL では、トポロジで Q トンネリングされたレイヤ 2 Q を使用する場合、COS 値と一致するポリシー マップが着信ポートに適用されます。

- DSCP 値のセットが設定されている場合（0 ～ 30、0 ～ 63 など）、qos dbl dscp-based 0-7 コマンドでこれらの DSCP 値のサブセットを指定しても、DSCP の不要な値（8 ～ 63）は削除できません。不要な値は、コマンドの no 形式を使用して削除する必要があります。この場合、no qos dbl dscp-based 8-63 コマンドを使用すると、選択した 0-7 が残ります。
- インターフェイス上でマルチドメイン認証（MDA）を使用したポート セキュリティを使用する場合:
  - 少なくとも 3 つの MAC アドレスがスイッチにアクセスできるようにします。3 つの内 2 つは電話用（データドメインおよび音声ドメインに登録される電話の MAC アドレス）で、1 つは PC 用です。
  - データ VLAN ID と音声 VLAN ID が異なることを確認します。
- スタティック ホストの IP ポート セキュリティ（IPSG）では、次が適用されます。
  - IPSG が各インターフェイス上のスタティックホストを学習するとき、学習するホストが多数ある場合、スイッチ CPU が 100 パーセントになることがあります。ホストが学習されると、CPU 使用率が低くなります。
  - スタティック ホストの IPSG 違反は、違反が発生すると印刷されます。異なるインターフェイスで複数の違反が同時に発生した場合、CLI には最新の違反が表示されます。たとえば、IPSG で 10 ポートが設定され、ポート 3、6、および 9 で違反が発生した場合、印刷される違反メッセージはポート 9 のみになります。
  - いずれかの VLAN が別のポートに関連付けられている場合や VLAN からポートが削除された場合、非アクティブなホスト バインディングがデバイス トラッキング テーブルに表示されます。そのため、ホストをサブネット間で移動すると、そのホストは Inactive としてデバイス トラッキング テーブルに表示されます。
  - 自動ステート機能 SVI は、EtherChannel では動作しません。
- CSCsg08775 の解決策により、GARP ACL エントリはスタティック CAM 領域の一部ではなくなりました。ただし、コントロール プレーン ポリシング（CPP）内のシステム定義 GARP クラスは引き続き存在します。
- Catalyst 4507R および Catalyst 4510R シャーシの設定によっては、利用可能なデータ電力の最大量を超えます。これらの設定には、次の PID の組み合わせがあります。
  - 7 スロット構成
  - シャーシ WS-C4507R-E、WS-C4510R-E
  - デュアルスーパバイザ WS-X45-Sup6-E
  - 1 つ以上の WS-X4448-GB-RJ45 または WS-X4148-FX-MT モデル

  冗長 Supervisor Engine 6-E を使用して、7 スロットおよび 10 スロットのシャーシの 10/100/1000 ポート密度を最大化するためには、WS-X4448-GB-RJ45 ラインカードではなく WS-X4548-GB-RJ45 を取り付けます。WS-X4448-GB-RJ45 ラインカードを使用する必要がある場合は、次の 2 つのオプションがあります。
  - オプション 1

    Catalyst 4507R では 4 つのラインカードスロットのみを使用し、Catalyst 4510R シャーシでは 6 つのラインカードスロットのみを 使用します。
  - オプション 2

    すべてのスロットが必要な場合、使用できるのは WS-X4448-GB-RJ45 ラインカードの 1 モデルのみです。

Supervisor Engine 6-E を使用して、7 および 10 スロットシャーシの 100 BASE-FX ポート密度を最大化するためには、WS-X4148-FX-MT ラインカードではなく FX 光ポートを持つ WS-4248-FE-SFP ラインカードを取り付けます。WS-X4148-FX-MT ラインカードを使用する必要がある場合は、次の 2 つのオプションがあります。

- オプション 1

  Cat4507R シャーシでは 4 つのラインカードスロットのみ、Cat4510R シャーシでは 6 つのラインカードスロットのみを使用できます。

- オプション 2

  すべてのスロットが必要な場合、1 つの WS-X4448-GB-RJ45 ラインカードのみ使用できます。

- 任意の CLI を介して IPv6 がインターフェイス上で有効になっている場合、次のメッセージが表示されることがあります。

```
% Hardware MTU table exhausted
```

  このような場合、ハードウェアでプログラムされている IPv6 の MTU 値は IPv6 インターフェイスの MTU 値とは異なります。この状況は、追加の値を保存する余裕がハードウェア MTU テーブルにない場合に発生します。

  テーブルに空きを作るには、未使用のいくつかの MTU 値を設定解除します。次に、インターフェイスで IPv6 を無効化または再度有効化するか、または MTU 設定を再適用します。

- インターフェイス上のスタティック ホストの IPSG を停止するには、インターフェイス コンフィギュレーションのサブモードで次のコマンドを使用します。

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

  ポート上のスタティック ホストの IPSG をイネーブルにするには、次のコマンドを入力します。

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
```

注意 インターフェイス上で IP デバイストラッキングをグローバルに有効にせずに、または IP デバイストラッキングを最大限に設定せずに、ポート上で ip verify source tracking [port-security] インターフェイス コンフィギュレーション コマンドを設定した場合、スタティックホストの IPSG はそのインターフェイスからのすべての IP トラフィックを拒否します。

注 前述の状況は、PVLAN ホストポート上のスタティックホストの IPSG にも当てはまります。

- Cisco IOS リリース 12.2(40)SG と以前のリリースとの間で ISSU アップグレードを実行する前に、コントロールプレーンから ACL という名前の system-cpp-policy を削除して、ハードウェア コントロール プレーン ポリシングを無効にする必要があります。以前のリリースでは、ACL という名前の system-cpp-policy はコントロールプレーンから切り離すことができません。以前のリリースを実行している場合は、Cisco IOS リリース 12.2(40)SG への ISSU アップグレードを実行する際に、まず Cisco IOS リリース 12.2(31)SGAx の最新のメンテナンスリリースにアップグレードする必要があります。

- Supervisor Engine V-10GE（WS-X4516-10GE）では、新しいアップリンクモードでのスタートアップ コンフィギュレーションをフラッシュメモリにコピーしてシステムに電源を再投入しても、システムは新しいアップリンクモードで起動されません。新しいアップリンク モードでのスタートアップ コンフィギュレーションをフラッシュ メモリにコピーしたら、システムに

電源を再投入する前にコマンド インターフェイスからアップリンク モードを新しいアップリンク モードに変更する必要があります。これにより、新しいアップリンク モードでのシステム起動が保証されます。

- Catalyst 4510R または 4510R-E シャーシで Supervisor Engine V を使用する場合、スロット 10（FlexSlot）で使用できるのは 2 ポート GBIC（WS-X4302-GB）とアクセス ゲートウェイ モジュール（WS-X4604-GWY）のラインカードのみです。アップリンク選択モードが「all」に設定されている場合、Supervisor Engine V-10GE はこれと同様の制限を受けます。アップリンク選択モードが「tengigabitethernet」または「gigabitethernet」に設定されている場合、Supervisor Engine V-10GE は、すべての Catalyst 4500 シリーズのラインカードのスロット 10 への取り付けをサポートします。Supervisor Engine 6-E は、Catalyst 4500 シリーズのすべてのラインカードのスロット 10 への取り付けをサポートします。
- Cisco IOS リリース 12.2(50)SG よりも前のリリースでは、Supervisor Engine V、V-10GE 以前を搭載したスイッチでは、system-cpp-policy のユーザ定義クラスマップのクラスマップ検索統計情報が正しく更新されません。Cisco IOS リリース 12.2(50)SG では、system-cpp-policy のユーザ定義クラスマップの検索統計情報が正しく更新されます。ただし、per-vlan キャプチャモードでは、system-cpp-policy で定義されたシステムの検索統計情報は更新されません。グローバル キャプチャ モードでは、system-cpp-policy にあるすべての（ユーザ定義およびシステム定義の）クラスマップの検索統計情報が適切にアップデートされます。
- MDA またはマルチ認証ホストモードを事前認証オープンアクセスと組み合わせて使用すると、スイッチはユニキャスト EAPOL 応答を無視します。

  回避策:

  - サプリカントにマルチキャスト EAPOL の使用を強制する
  - 認証オープンモードを回避する

  CSCtq33048

Supervisor Engine 6-E および Supervisor Engine 6L-E の場合

- Catalyst 4510R スイッチは Supervisor Engines 6L-E をサポートしていません。サポート対象外のスーパバイザエンジンをインストールすると、ソフトウェアで制御できない予期しない動作がハードウェアで発生する可能性があります。サポート対象外のスーパバイザエンジンを冗長スロットに挿入して使用すると、他のスロットに挿入されているサポート対象のスーパバイザエンジンが誤作動する可能性があります。
- MAC アドレス テーブルは、802.1s または 802.1w スパニングツリー プロトコルのいずれかが設定されている場合、スーパバイザ エンジンを切り替えるとクリアされます。アドレスのクリアとそれに伴うパケットのフラッディングを最小限に抑えるには、エッジ ポートを **spanning-tree portfast** に、リンクタイプを **spanning-tree link-type point-to-point** にそれぞれ設定します。
- IP クラスフルルーティングはサポートされていません。no ip classless コマンドを使用しないでください。このコマンドはクラスレスルーティングのみをサポートしているため、無効になります。クラスレスルーティングがデフォルトで有効になっているため、コマンド **ip classless** はサポートされていません。
- レイヤ 2 LACP チャネルを、スパニングツリー PortFast 機能で設定することはできません。
- ブートローダ イメージを使用するネットブーティングは、サポートされていません。他の方法については、「トラブルシューティング」セクション（468 ページ）を参照してください。
- 冗長スーパーバイザを Catalyst 4507R に展開すると、スタートアップ コンフィギュレーション ファイルが解析されている間は存在しないハードウェアの場合、そのハードウェアのコンフィギュレーション ファイルは適用されません。

たとえば、アクティブなスーパバイザエンジンがスロット 1 にあり、インターフェイス Gi1/1 が設定されている場合、シャーシからアクティブなスーパバイザエンジンを取り外すと、スロット 2 にあるスーパバイザエンジンがアクティブになります。また、スタートアップ コンフィギュレーション ファイルの解析中にインターフェイス Gi1/1 が存在していないことを示すエラーメッセージが表示されます。これは、正常な動作です。以前のアクティブなスーパバイザエンジンをスロット 1 に再挿入しても、インターフェイス Gi1/1 の設定は残っていません。

この現象は、両方のスーパバイザ エンジンが物理的にシャーシに挿入されている場合は発生しません。

回避策 : スタートアップ コンフィギュレーション ファイルを実行コンフィギュレーションにコピーします。

```
Switch# copy startup-config running-config
```

- モバイル IP に対してサポートされていないデフォルト CLI が HSRP 設定に表示されます。この CLI はシステムに害を与えませんが、混乱を避けるために削除することをお勧めします。

  回避策：**show standby** コマンドを使用して設定を表示し、CLI を削除します。次に、show standby GigabitEthernet1/1 コマンドの出力例を示します。

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- HSRP プリエンプション遅延を一貫して機能させるには、**standby delay minimum** コマンドを使用する必要があります。遅延を 1 つ以上の hello 間隔に設定して、HSRP が開始状態を終了する前に hello が受信されるようにしてください。

  イメージのリロード後にルータがリブートする場合は、**standby delay reload** オプションを使用します。

- Cisco 製ルータとサードパーティ製のルータ間で OSPF を実行しようとすると、2 つのインターフェイスが Exstart/Exchange の状態で止まってしまう可能性があります。この問題は、ネイバールータのインターフェイス間で最大伝送単位（MTU）設定が一致しない場合に発生します。より高速に MTU を設定したルータではネイバールータの MTU 設定よりも大きなパケットが送信されるため、ネイバールータはこのパケットを無視します。

  回避策：MTU が一致していることを確認します。

- Supervisor Engine 6-E では、.1q-in-.1q パケットパススルーのみを実行できます。
- PVST および Catalyst 4500 E シリーズ スイッチの VLAN では、Cisco IOS Release 12.1（13）EW は最大 3000 のスパニングツリー ポート インスタンスをサポートしています。これより多くのインスタンスを使用する場合は、PVST ではなく MST を使用してください。
- Supervisor Engine 6-E は FAT ファイルシステムをサポートしているため、次の制限が適用されます。
  - **verify** コマンドと **squeeze** コマンドはサポートされません。
  - **rename** コマンドは FAT ファイル システムでサポートされます。

    Supervisor Engine 6-E では、ブートフラッシュと slot0 に rename コマンドを使用できます。その他すべてのスーパーバイザでは、NVRAM デバイスのみで **rename** コマンドがサポートされます。
  - **fsck** コマンドは、slot0 デバイスでサポートされます。6-E 以外のスーパーバイザ エンジンのファイル システムではサポートされていません。
  - FAT ファイルシステムでは、IOS format bootflash: コマンドはユーザファイルのみを消去します。システム設定は消去しません。
  - FAT ファイルシステムは、ファイル/ディレクトリ名として最大 63 文字をサポートします。パスの最大長は 127 文字です。

  - FAT ファイルシステムでは、ファイル/ディレクトリ名に {、}、#、%、^、およびスペース文字は使用できません。
  - FAT ファイルシステムは、読み取り専用および読み取り/書き込みの Microsoft Windows ファイル属性を受け入れますが、Windows ファイルの隠し属性はサポートしていません。
  - Supervisor Engine 6-E は、Compact Flash（slot0）に FAT ファイルシステムを使用します。Compact Flash が FAT ファイルシステムでフォーマットされていない場合（6-E 以外のスーパバイザエンジンの Compact Flash など）、スイッチはその Compact Flash を認識しません。
- 送信キューシェーピングまたは共有設定により元のパケットが損失しても、引き続き SPAN ポートで SPAN パケットのコピーを送信できます。
- すべてのソフトウェア リリースで、最大 16,000 の IGMP スヌーピング グループ エントリがサポートされています。
- パフォーマンスを最大限に引き上げるには、ACL に設定されているすべてのインターフェイスで **no ip unreachables** コマンドを使用します。
- Dynamic ARP Inspection（DAI）の err-disable 機能のしきい値は、インターフェイスごとに 15 ARP パケット/秒に設定されています。このしきい値は、ネットワーク構成に応じて調整する必要があります。CPU は、持続レートが 1000 pps を超える DHCP パケットは受信しません。
- レイヤ 3 ポートに IP アドレスまたは IPv6 アドレスを設定した後、**switchport** コマンドでレイヤ 3 ポートをレイヤ 2 ポートに変更し、再度これをレイヤ 3 ポートに戻すと、元の IP/IPv6 アドレスが失われます。
- 冗長システムでは、アクティブなスーパバイザエンジンの起動中にスタンバイ スーパバイザエンジンの取り外しまたは再挿入を行わないでください。これを行うと、オンライン診断テストが失敗する可能性があります。

  回避策： スタンバイ スーパバイザ エンジンの取り外しまたは再挿入はアクティブなスーパバイザエンジンを起動してから行ってください。（CSCsa66509）
- **switchport private-vlan mapping trunk** コマンドでサポートされる一意のプライベート VLAN ペアは最大で 500 です。たとえば、500 のセカンダリ VLAN を 1 つのプライマリ VLAN にマッピングしたり、500 のセカンダリ VLAN を 500 のプライマリ VLAN にマッピングしたりできます。
- PoE のサポートは、次のラインカードや電源装置を使用しているかどうかによって異なります。

  PoE スイッチング モジュール：
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - WS-X4648-RJ45V-E
  - WS-X4648-RJ45V+E
  - WS-X4548-GB-RJ45V+

  PoE 対応電源装置：
  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC

  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - PWR-C45-6000ACV
- Catalyst 4500 シリーズ スイッチが Cisco Secure Access Control Server（ACS）からの情報を要求すると、サーバが応答しないためメッセージの交換がタイムアウトします。このとき、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 として正しく設定されていることも確認します。
- スタティック ホストの IP ポート セキュリティ（IPSG）では、次が適用されます。
  - IPSG が各インターフェイス上のスタティックホストを学習するとき、学習するホストが多数ある場合、スイッチ CPU が 100 パーセントになることがあります。ホストが参照されると、CPU 使用率が低くなります。
  - スタティック ホストの IPSG 違反は、違反が発生すると印刷されます。異なるインターフェイスで複数の違反が同時に発生した場合、CLI には最新の違反が表示されます。たとえば、IPSG で 10 ポートが設定され、ポート 3、6、および 9 で違反が発生した場合、印刷される違反メッセージはポート 9 のみになります。
  - いずれかの VLAN が別のポートに関連付けられている場合や VLAN からポートが削除された場合、非アクティブなホスト バインディングがデバイス トラッキング テーブルに表示されます。そのため、ホストをサブネット間で移動すると、そのホストはインアクティブとしてデバイス トラッキング テーブルに表示されます。
  - 自動ステート機能 SVI は、EtherChannel では動作しません。
- CLI を使用して IPv6 がインターフェイスで有効になっている場合、次のメッセージが表示されることがあります。

  ```
  % Hardware MTU table exhausted
  ```

  このような場合、ハードウェアでプログラムされている IPv6 の MTU 値は IPv6 インターフェイスの MTU 値とは異なります。この状況は、追加の値を保存する余裕がハードウェア MTU テーブルにない場合に発生します。

  空きを作るには、未使用のいくつかの MTU 値を設定解除します。次に、インターフェイスで IPv6 を無効または再度有効にするか、または MTU 設定を再適用します。
- インターフェイス上のスタティック ホストの IPSG を停止するには、インターフェイス コンフィギュレーションのサブモードで次のコマンドを使用します。

  ```
  Switch(config-if)# no ip verify source
  Switch(config-if)# no ip device tracking max
  ```

  ポート上のスタティック ホストの IPSG をイネーブルにするには、次のコマンドを入力します。

  ```
  Switch(config)# ip device tracking ****enable IP device tracking globally
  Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
  Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
  ```

注意 インターフェイス上で IP デバイストラッキングをグローバルに有効にせずに、または IP デバイストラッキングを最大限に設定せずに、ポート上で **ip verify source tracking [port-security]** インターフェイス コンフィギュレーション コマンドを設定した場合、スタティックホストの IPSG はそのインターフェイスからのすべての IP トラフィックを拒否します。

注　前述の状況は、PVLAN ホストポート上のスタティックホストの IPSG にも当てはまります。

- uRPF は最大 4 つのパスをサポートします。ハードウェアで RPF VLAN の 1 つとしてプログラムされていない有効な VLAN の 1 つにパケットが着信すると、そのパケットはドロップされます。RPF が設定されていない他のインターフェイスからトラフィックが着信する可能性がある場合は、スイッチングが可能です。
- 入力 ACL と出力 ACL は、uRPF インターフェイスで受信したトラフィックを上書きまたはフィルタリングできません。
- ハードウェアスイッチング中に uRPF ドロップパケットを反映する CLI コマンドはありません。sh ip traffic および show cef int コマンドは、uRPF ドロップを反映しません。
- IPv6 ACL はスイッチポートではサポートされていません。IPv6 パケットは、既知の方法（PACL、VACL、または MACL）を使用してスイッチポートでフィルタリングできません。
- match ip prec | dscp を使用したクラスマップ match ステートメントは IPv4 のみを照合しますが、match prec | dscp を使用して実行した一致は IPv4 パケットと IPv6 パケットの両方を照合します。
- ポリシーマップに IPv6 ACL が含まれており、IPv6 アクセスリストを備えた同じクラスマップ内の一致 CoS で /81 ～ /127 の範囲内にマスクがある場合は、IPv6 QoS ハードウェアスイッチングが無効になります。この状況ではパケットがソフトウェアに転送され、QoS を効率的に無効にします。
- Supervisor Engine 6-E を搭載した Catalyst 4507R-E または 4510R-E シャーシに次のデータ専用 Catalyst 4500 ラインカードを使用すると、電源の容量を超える可能性があります。
  - WS-X4148-FX-MT Cisco Catalyst 4500 ファストイーサネット スイッチングモジュール、48 ポート 100BASE-FX（MT-RJ）
  - WS-X4448-GB-RJ45 Cisco Catalyst 4500 48 ポート 10/100/1000 モジュール（RJ-45）

  Catalyst 4503-E および Catalyst 4506-E に警告はありません。また、定格 1400 W 以上の電源を使用する Catalyst 4507R-E 構成にも警告はありません。

  次の交換用スイッチングモジュールは、Catalyst 4500-E シャーシの電源容量を超えません。

	推奨後継製品	説明
WS-X4148-FX-MT	WS-X4248-FE-SFP	ファストイーサネット、48 ポート 100BASE-X（SFP）
WS-X4448-GB-RJ45	WS-X4548-GB-RJ45	拡張 48 ポート 10/100/1000 モジュール（RJ-45）
WS-X4448-GB-RJ45	WS-X4648-RJ45V-E	E シリーズ 48 ポート 802.3af PoE 10/100/1000（RJ-45）

  Catalyst 4500 シリーズ モジュール インストレーション ガイド [英語] を参照して、すべての Catalyst 4500 ラインカードの電力要件と Catalyst 4500 電源の電力容量を確認してください。
- Supervisor Engine 6-E は、スロット 8-10 で Catalyst 4500 シリーズ ラインカードのみをサポートします。
- 冗長スイッチからラインカードを取り外し、SSO スイッチオーバーを開始してから、ラインカードを再度挿入すると、すべてのインターフェイスがシャットダウンされます。元のラインカードの残りの設定は、保持されます。

  この状況は、ラインカードを取り外す前に、スイッチが SSO に到達した場合にだけ発生します。

- Supervisor Engine 6-E では、アップストリームポートは 1Gモードでのみフロー制御の自動ネゴシエーションをサポートし、10G モードではフロー制御が強制的にオンになります。インターフェイスがフロー制御を自動ネゴシエーションするように設定されており、インターフェイスが 10G モードで動作している場合、システムはフロー制御を強制的にオンにし、自動ネゴシエーションは行いません。
- Supervisor Engine 6-E は、最大 32 ポートで Fast UDLD をサポートします。
- Cisco IOS リリース 12.2(53)SG3（および 12.2(54)SG）では、単一のスーパバイザ、RPR、または固定構成スイッチが自動的にリロードされないようにデフォルトの動作が変更されました。自動リロードを設定するには、diagnostic fpga soft-error recoveraggressive コマンドを入力する必要があります。（CSCth16953）

警告

問題では、Cisco IOS リリースでの予期しない動作について説明します。以前のリリースでオープンになっている問題は、オープンまたは解決済みとして次のリリースに引き継がれます。

注 Release 12.4 におけるすべての警告は、これに対応する 12.1 E リリースにも当てはまります。次の URL にある Cisco IOS リリース 12.4 の警告 [英語] を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124MCAVS.html

注 PSIRTS の最新情報については、次の URL から CCO の『Security Advisories』を参照してください。

http://tools.cisco.com/security/center/publicationListing.x

Cisco IOS リリース 12.2(54)SG1 の未解決の警告

ここでは、Cisco IOS リリース 12.2(54)SG1 の未解決の警告について説明します。

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッ

チには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラーメッセージが表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

この状況は、次の理由で発生する可能性があります。

- パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
- スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクションが必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 より上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブ スーパバイザ エンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルの状態が同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブ スーパバイザ エンジンは、一括同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブ スーパバイザ エンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

  これは、実行中の従来または E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。Cisco IOS リリース 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブ スーパバイザ エンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、再学習が行われ、ホストの MAC がスタンバイ スーパバイザ エンジンに同期されます。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正しい状態です。CSCsz20149

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他のすべての情報は、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。CSCta16492

- Cisco IOS リリース 12.2(53)SG1、12.2(50)SG6、またはそれ以降のリリースを実行し、スイッチでスイッチポート ブロック マルチキャストを設定すると、レイヤ 2 マルチキャストはブロックされません。IPv4 と IPv6 の不明なマルチキャストがブロックされます。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。（CSCta61825）

  回避策：なし。CSCtb30327

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。Catalyst 4900M スイッチ、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  回避策：ありません。CSCte51948

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  CSCsv69853

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  CSCsv90044

- Catalyst 4948E イーサネットスイッチのピアインターフェイスで、errdisabled モードフラップ検出が非常に小さい数（10 秒で 2 フラップなど）に設定されている場合、10GE リンクフラップによってピアインターフェイスが errdisabled 状態になることがあります。

  回避策：Cisco スイッチのデフォルトのリンクフラップ検出値は、10 秒 で 5 フラップです。デフォルト値以上の数値を使用します。CSCtg07677

- VLAN で IGMP スヌーピングを無効にしてから再度有効にすると、show mac address コマンドの出力にはマルチキャストエントリに対する [term] スイッチが表示されません。マルチキャストトラフィックは影響を受けません。

  回避策：SVI で shut を実行し、続いて no shut を実行します。CSCtg72559

- 電話機の背後にある接続済みデータデバイスがマルチ認証ホストモードに設定されたポートから切断されると、デバイスが存在しない場合でも、デバイスの新しいセッションが再起動されます。

  データデバイスが切断されたことを示すために生成された CDP TLV は無視されます。これは、接続されている他のデータクライアント（存在する場合）の切断を回避するために行われます。（CSCta47293 を参照）。

  回避策：次のいずれかのコマンドを入力します。

  - clear authentication session interface
  - authentication timer inactivity

  CSCtg83631

- X2 または SFP が Supervisor Engine V-10GE、Supervisor II+10GE、Supervisor 6-E、または Supervisor 6-LE の非アクティブなアップリンクポートに取り付けられている場合、しきい値違反が 10 分ごとに報告されることがあります。

  回避策：ポートから X2 または SFP を取り外します。CSCth08212

- フォールバック Web 認証とマルチホストがポートに設定され、PACL が存在しない場合、permit ip any any が TCAM にインストールされ、ホストからのすべてのトラフィックが通過できます。

  回避策：ポートで ACL を設定します。CSCte18760

- EPM ロギングを有効にし、クライアントが MAB または Web 認証で認証されると、認証方式に関係なく、EPM syslog メッセージの AUTHTYPE の値は DOT1X になります。

  同様に、show epm sessions コマンドでは、認証方式は常に DOT1X と表示されます。

  回避策：クライアントに使用される認証方式を表示するには、**show authentication sessions** コマンドを入力します。CSCsx42157

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ホストモードマルチドメインが設定され、認証が成功した場合、トラフィックは IP フォンまたはデータデバイスから渡されません。

  回避策：ありません。CSCtj56811

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- スイッチが MAC 認証バイパス（MAB）EAP 用に設定されており、AAA サーバが（EAP 方式として）EAP-TLS を最初に要求すると、MAB は失敗します。

  回避策：

  - スイッチポートを mab eap ではなく mab に設定します。
  - MAA EAP 要求に対して EAP-TLS ではなく EAP-MD5 を最初に提案するように AAA サーバを設定します。CSCti78674

Supervisor Engine 6-E および Supervisor Engine 6L-E に固有の警告

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- X2 SR トランシーバを
  Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：**show policy-map interface** コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。

  ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 からそれ以降のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズフレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 ギガビット イーサネット ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。CSCso71647

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てたときに、この動作が発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを**no switchport trunk native vlan tag** コマンドを入力して無効にします。CSCsz12611

- CX1 または SFP+ を WS-X4908-10GE の OneX コンバータ（CVR-X2-SFP10G）に接続すると、リンクの起動に 1 分かかります。

  回避策：ありません。CSCtc46340

- 大きな PACL がハードウェアに完全にロードされる前に、次のような誤った完了メッセージが表示されることがあります。

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

  回避策：機能に影響はありません。

  ACL がプログラムされるのを待ってから、他の TCAM 関連の変更を実行する必要があります。CSCtd57063

- 宛先アドレス FF02::x のルータアドバタイズメントおよびルータリダイレクトパケットがドロップされた場合、show ipv6 first-hop counters interface コマンドの出力で RA ガードカウンタが増加しません。

  回避策：ありません。CSCtf69108

- ND/NS パケットは、IPv6 ACL がレイヤ 3 インターフェイスに接続されるとドロップされます。

  回避策：次の許可 ACE を ACL に追加します。

  ```
  permit icmp any any nd-ns
   permit icmp any any nd-na
  ```

  CSCtg77035

- サービスポリシーに、明示的なマーキングアクションを含む 56 を超えるクラスが含まれている場合、サービスポリシーをターゲットにアタッチするとスイッチがクラッシュします。以下を参照。

```
policy-map pm
 class c0
   set dscp default
   set cos 0
 class c1
   set dscp 1
   set cos 1
 class c2
   set dscp 2
   set cos 2
... ...
 class c56
   set dscp cs7
   set cos 0
```

回避策：tablemap ベースのマーキングを使用します。CSC99836

Cisco IOS リリース 12.2(54)SG1 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(54)SG1 で解決済みの警告について説明します。

- Catalyst 4500 シリーズ スイッチでは、リンクがダウンすると、ポートセキュリティの VLAN ごとの最大 MAC アドレスが失われることがあります。これは、次のインターフェイス設定に適用されます。

```
switchport port-security maximum <number> vlan access
switchport port-security maximum <number> vlan voice
```

  回避策：ありません。CSCti74791

- VTP アップデートを受信するポートに no vtp が設定されている場合、スイッチはレイヤ 2 制御トラフィック（STP および CDP）を処理しません。

  回避策：12.2(53)SG3、12.2(50)SG8 以降にアップグレードします。CSCth00398

- 多数の PoE ラインカード（WS-X4548-GB-RJ45V、WS-X4548-RJ45V+）を備えた冗長シャーシでスイッチオーバーが発生すると、新しいアクティブ スーパバイザ エンジンの CPU 使用率が 80% を超えます。

注 同じ PoE ラインカードを備えた非冗長シャーシでは、CPU 使用率は 80% に達しません。

この問題は、固定構成シャーシには当てはまりません。

回避策：ありません。CSCti08570

- cat4500e-ipbasek9-mz.122-53.SG1 を実行する Supervisor Engine 6-E またはSupervisor Engine 6L-E では、インターフェイスのフラッピングが原因でリロードが発生することがあります。

  回避策：ありません。CSCtf49878

- 完全に初期化される前のラインカードのハードウェアステータスをソフトウェアが読み取ると、スーパバイザエンジンでソフトウェアによるクラッシュが発生します。

  回避策：ありません。CSCtf82009

- スパニングツリープロセスは、VLAN マッピング変換が設定されている場合、トランクインターフェイスで VLAN を無効にします。

  回避策：コンフィギュレーション インターフェイス モードで spanning-tree bpdufilter enable を設定します。

  CSCtj21636

- 少なくとも 1 つの 1 対 1 変換が設定されている場合、同じ VLAN へのマッピングは許可されません。これは、VLAN 変換を行わずに特定の VLAN でパケットをスイッチングするユーザに影響します。

  回避策：なし

  CSCti22918

- VLAN マッピングが設定されている場合（同じ VLAN と異なる VLAN の 1 対 1 のマッピング）、SVI への ping は失敗します。

  VLAN データベースで VLAN をランダムに追加または削除すると、一部の VLAN で SVI トラフィックが停止します。

  回避策：ありません。CSCtk03191

- バックアップ代表ルータのネイバーがダウンしている間に show ip ospf int コマンドを一時停止すると、show ip ospf int コマンドを入力したときにスイッチがリロードすることがあります。

```
c3560sw2# show ip ospf int
 Vlan804 is up, line protocol is up
   Internet Address 10.0.0.2/24, Area 0
   Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DR, Priority 1
   Designated Router (ID) 10.0.0.2, Interface address 10.0.0.2
  --More--
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
 changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan804, changed
 state to down
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Vlan804 from FULL to DOWN,
 Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
```

  show ip ospf int コマンドで出力される次の行は次のとおりです。

```
Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1
```

  Enter キーまたはスペースキーを押して出力を進めると、デバイスがリロードされて、次のエラーメッセージが表示されます。

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```

  回避策：ありません。CSCtd73256

- show tacacs+ コマンドは、プライベート tacacs+ サーバの統計情報を提供しません。

  回避策：ありません。CSCta96363

- スイッチは、ウォッチドッグ NMI Vector 000 および CRC エラーでクラッシュする可能性があります。以下を参照。

```
"%C4K_SUPERVISOR-2-FPGASOFTERROR: Memory inconsistency detected" have
appeared on the switch followed by link flaps, transceiver (HAMM module, X2,
sfp) insertion/removal on uplinks (base board ports on 4900M)
```

回避策:

  - エラーメッセージが表示されたら、スイッチをリロードします。
  - Cisco Catalyst リリース 12.2(54)SG1、Cisco Catalyst リリース 12.2(53)SG4 以降（使用可能な場合）にアップグレードします。

CSCtk75675

Cisco IOS リリース 12.2(54)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(54)SG の未解決の警告について説明します。

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策: システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策: ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策: 再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

  回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  （CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。

– アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

（CSCsv44866）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

回避策：ありません。CSCsy72343

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

回避策：ありません。

キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。CSCsz20149

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

CSCsz34522

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。CSCta16492

- Cisco IOS リリース 12.2(53)SG1、12.2(50)SG6、またはそれ以降のリリースを実行し、スイッチでスイッチポート ブロック マルチキャストを設定すると、レイヤ 2 マルチキャストはブロックされません。IPv4 と IPv6 の不明なマルチキャストがブロックされます。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。（CSCta61825）

  回避策：なし。CSCtb30327

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。Catalyst 4900M スイッチ、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  回避策：ありません。CSCte51948

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  CSCsv69853

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。
  – 該当ポートに SFP+ を挿入します。
  – 取り外した SFP+ を他のポートに再度挿入します。

  CSCsv90044

- Catalyst 4948E イーサネットスイッチのピアインターフェイスで、errdisabled モードフラップ検出が非常に小さい数（10 秒で 2 フラップなど）に設定されている場合、10GE リンクフラップによってピアインターフェイスが errdisabled 状態になることがあります。

  回避策：Cisco スイッチのデフォルトのリンクフラップ検出値は、10 秒 で 5 フラップです。Use the default value or larger numbers. CSCtg07677

- VLAN で IGMP スヌーピングを無効にしてから再度有効にすると、show mac address コマンドの出力にはマルチキャストエントリに対する [term] スイッチが表示されません。マルチキャストトラフィックは影響を受けません。

  回避策：SVI で shut を実行し、続いて no shut を実行します。CSCtg72559

- 電話機の背後にある接続済みデータデバイスがマルチ認証ホストモードに設定されたポートから切断されると、デバイスが存在しない場合でも、デバイスの新しいセッションが再起動されます。

  データデバイスが切断されたことを示すために生成された CDP TLV は無視されます。これは、接続されている他のデータクライアント（存在する場合）の切断を回避するために行われます。（CSCta47293 を参照）。

  回避策：次のいずれかのコマンドを入力します。

  - show authentication sessions interface
  - authentication timer inactivity

  CSCtg83631

- X2 または SFP が Supervisor Engine V-10GE、Supervisor II+10GE、Supervisor 6-E、または Supervisor 6-LE の非アクティブなアップリンクポートにある場合、しきい値違反が 10 分ごとに報告されることがあります。

  回避策：ポートから X2 または SFP を取り外します。CSCth08212

- フォールバック WebAuth とマルチホストがポートに設定され、PACL が存在しない場合、permit ip any any が TCAM にインストールされ、ホストからのすべてのトラフィックが通過できます。

  回避策：ポートで ACL を設定します。CSCte18760

- EPM ロギングを有効にし、クライアントが MAB または WebAuth で認証されると、認証方式に関係なく、EPM syslog メッセージの AUTHTYPE の値は DOT1X になります。

  同様に、show epm sessions コマンドでは、認証方式は常に DOT1X と表示されます。

  回避策：クライアントに使用される認証方式を表示するには、**show authentication sessions** コマンドを入力します。CSCsx42157

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ホストモードマルチドメインが設定され、認証が成功した場合、トラフィックは IP フォンまたはデータデバイスから渡されません。

  回避策：ありません。CSCtj56811

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- スイッチが MAC 認証バイパス（MAB）EAP 用に設定されており、AAA サーバが（EAP 方式として）EAP-TLS を最初に要求すると、MAB は失敗します。

  回避策：

  - スイッチポートを mab eap ではなく mab に設定します。
  - MAA EAP 要求に対して EAP-TLS ではなく EAP-MD5 を最初に提案するように AAA サーバを設定します。CSCti78674

Supervisor Engine 6-E および Supervisor Engine 6L-E に固有の警告

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。(CSCsk52542)

- X2 SR トランシーバを Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。(CSCsk43618)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。

  ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。(CSCsl72868)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 からそれ以降のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。(CSCsm81875)

- トラフィックおよびポーズフレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 ギガビット イーサネット ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。
  CSCso71647

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てたときに、この動作が発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを**no switchport trunk native vlan tag** コマンドを入力して無効にします。CSCsz12611

- CX1 または SFP+ を WS-X4908-10GEの OneX コンバータ（CVR-X2-SFP10G）に接続すると、リンクの起動に 1 分かかります。

  回避策：ありません。CSCtc46340

- 大きな PACL がハードウェアに完全にロードされる前に、次のような誤った完了メッセージが表示されることがあります。

```
Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-HWPROGSUCCESS: Input Security: pacl - now
fully loaded in hardware *Dec  1 18:44:59.926: %C4K_COMMONHWACLMAN-4-ALLACLINHW: All
configured ACLs now fully loaded in hardware - hardware switching / QoS restored.
```

  回避策：機能に影響はありません。

  ACL がプログラムされるのを待ってから、他の TCAM 関連の変更を実行する必要があります。CSCtd57063

- 宛先アドレス FF02::x のルータアドバタイズメントおよびルータリダイレクトパケットがドロップされた場合、show ipv6 first-hop counters interface コマンドの出力で RA ガードカウンタが増加しません。

  回避策：ありません。CSCtf69108

- ND/NS パケットは、IPv6 ACL がレイヤ 3 インターフェイスに接続されるとドロップされます。

  回避策：次の許可 ACE を ACL に追加します。

```
permit icmp any any nd-ns
 permit icmp any any nd-na
```

  CSCtg77035

- サービスポリシーに、明示的なマーキングアクションを含む 56 を超えるクラスが含まれている場合、サービスポリシーをターゲットにアタッチするとスイッチがクラッシュします。以下を参照。

```
policy-map pm
 class c0
   set dscp default
   set cos 0
 class c1
```

```
   set dscp 1
   set cos 1
 class c2
   set dscp 2
   set cos 2
... ...
 class c56
   set dscp cs7
   set cos 0
```

回避策：tablemap ベースのマーキングを使用します。CSC99836

Cisco IOS リリース 12.2(54)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(54)SG で解決済みの警告について説明します。

- 実行中のスイッチで switchport block multicast を設定する場合 Cisco IOS リリース 12.2(53)SG1 または 12.2(50)SG6 では、レイヤ 2 マルチキャストはブロックされません。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。

  回避策：ありません。CSCta61825

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（認証オープンなし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。CSCta04665

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。CSCsz05888

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で転送すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。CSCsy38640

- Cisco IOS リリース 12.2(54)SG を実行しているスイッチで、アクセス VLAN が削除され、802.1X マルチ認証で設定されたポートで復元されると、アクセス VLAN が復元された後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。CSCso50921

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- AutoQoS が有効になっているインターフェイスでデフォルトのインターフェイス操作を実行すると、エラーメッセージが表示され、AutoQoS 設定が失われます。たとえば、次の一連の操作により設定が失われます。

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

  回避策：default interface コマンドを次のように置き換えます。

```
config# interface interface-number
config-if# switchport
```

  （CSCsq47116）

- VLAN ロード バランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を発行すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no-shut コマンドを入力します。（CSCsq75342）

- IPv6 エントリが CAM でアクティブとなり、CPU が IPv6 パケットを受信します。

  回避策：すべての汎用 QoS ポリシーの設定をシステムから解除します。match any 属性を持つ QoS ポリシーにより、IPv6 エントリがアクティブになります。スイッチが純粋なレイヤ 2 デバイスである場合、汎用プロトコル ファミリの属性を削除して、プロトコル ファミリに絞り込みます。（CSCsq84796）

- IPv6 MLD と関連したコンフィギュレーションがない場合も、IPv6 MLD エントリが、アクティブになります。

  回避策：すべての汎用 QoS ポリシーの設定をシステムから解除します。CSCsq84853

- ポート容量の 99% でトラフィックを送信すると、WS-X4908-10GE で 0.05% の損失が発生します。

  回避策：ありません。CSCsl39767

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更してリセットしてください。CSCsk62457

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- ACL ではなくプレフィックスリストで一致するように PBR ポリシーを設定すると、スイッチで障害が発生します。

  回避策：ACL でのみ一致するようにルートマップを設定します。CSCtg22126

  SFP+ 光モジュール SFP-10G-LRM、SFP-10G-LR、および SFP-10G-SRA の場合、IOS の起動時またはモジュールの交換時に Tx 低電力アラームが表示されます。これは、新しい SFP+ モジュールが検出されたときの最初の誤報です。その後、クリアされます。

  SFP および 10GBASE-CU SFP+ モジュールでは、この問題は発生しません。

  回避策：ありません。CSCtg82213

- サードパーティ製の非 PoE デバイスが WS-4648-RJ45V-E または WS-4648-RJ45V+E に接続されていて、PoE が有効になっている場合、デバイスがリブートしてもリンクは確立されません。デバイスにエラーメッセージが表示されることがあります。

  回避策：PoE を無効にします（インターフェイス コンフィギュレーション モードで power inline never コマンドを入力します）。

  Cisco IOS リリース 12.2(54)SG では、power inline autoneg-advertise コマンドをグローバル コンフィギュレーション モードで入力して、リンクアップを有効にできます。CSCtb78851

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザ エンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。CSCsx64308

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。CSCsu35604

- ACL ではなくプレフィックスリストで一致するように設定された PBR ポリシーがインターフェイスに接続されている場合、スイッチがクラッシュします。

  この問題は、次のいずれかの条件が当てはまる場合に発生します。

  - プレフィックスリストで一致するルートマップが、PBR ポリシーとして入力インターフェイスに接続されている。
  - （インターフェイスにすでに接続されている）PBR のルートマップが、ACL ではなくプレフィックスリストで一致するように設定または変更されている。

  回避策：ACL でのみ一致するように PBR のルートマップを設定します。

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：最大 256 KB のグラフィックを HTML ファイルに埋め込みます（RFC 2397 に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは復元のタイミングには影響しますが、REP 機能には影響しません。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

  回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

  スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

  CSCsy70428

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定する場合、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。CSCsv43819

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。CSCsv42869

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：queue-limit コマンドを入力して、明示的なキューサイズを指定します。CSCso06422

- 認証に 3 回失敗すると、WinXP は 802.1X タイムアウト（デフォルトまたは設定済み）の原因となったスイッチからの EAPOL 要求に応答しなくなります。タイムアウト後、WinXP は認証失敗 VLAN に移行します。

  回避策：タイムアウト後に認証を試行します。CSCte84432

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

この状況は、次の条件を満たしている場合にのみ発生します。

- authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
- デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
- クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

回避策：ありません。

CSCsz63739

- サポートされていない Catalyst 4500 ソフトウェアバージョンを WS-C4507R+E および WS-C4510R+E にロードすると、次のログメッセージが表示され、いずれのポートも起動しません。

```
"%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type"
Or
"%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type"

"%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

回避策：Cisco IOS リリース 12.2(54)SG または 12.2(53)SG4 を WS-C4507R+E および WS-C4510R+E にロードします。CSCtl70275

Cisco IOS リリース 12.2(53)SG11 の未解決の警告

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1
```

```
Service-policy output: p1

  Class-map: c1 (match-all)
    0 packets<--------It stays at '0' despite of traffic being received
    Match: access-group name fnacl21
    police: Per-interface
      Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで802.1Xの設定を解除し、スイッチに接続されているIPフォン（CDPポートのステータスTLVサポート搭載）にホストを再接続すると、ホストのMACアドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストのMACアドレスが新しいアクティブなスーパバイザエンジンのMACアドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで**shutdown**コマンドを入力し、その後に**no shutdown**コマンドを入力します。これにより、ホストのMACが再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- MDAを使用する.1Xがホストモードに設定され、ゲストVLANが有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- Cisco IOSリリース12.2(52)SGを実行している冗長スイッチでは、802.1Xを介してポートが許可された後、show dot1x interface statisticsコマンドを実行すると、スタンバイ スーパバイザ エンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数のOAMモニタリングが設定されたWS-C4900Mシャーシで複数のストリームのCRCエラーが発生した場合、次のCLIを設定すると、OAMはエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドのCall Homeメッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnosticコマンドを入力するときにプロファイル名を指定します。

無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

CSCsz05888

- フラグメントとしてスイッチに入るパケット、またはゼロ以外のフラグメント オフセット フィールドを持つパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップ数が定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  または

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  および

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。

  CSCtq73579

- 期間モードで archive コマンドを使用して SCP 機能を設定すると、スイッチがクラッシュします。

  回避策：ありません。CSCuq36900

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R+E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+E ではなく WS-C4510R-E です。

  回避策：

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられていて、DBL をキューに適用するようにポリシーが設定されている場合、キューにあるフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。（CSCsk52542）

- X2 SR トランシーバを Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  – **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。

  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。(CSCsm81875)

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。(CSCso71647)

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたパケット、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  (CSCso96660)

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合(FlexLink の障害)、代替ポートに移動されません。

  回避策: ありません。(CSCsq99468)

- CFM Inward Facing MEP(IFM)が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします(ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため)。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースのソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R+E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

n はスロット番号です。

スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

回避策：WS-C4510R+E および WS-C4507R+E シャーシで Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降のイメージを使用します。

CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG11 の解決済みの警告

- SSH 経由でログインしようとすると、Cisco IOS リリース 12.2(53)SG10 を実行しているスイッチがクラッシュします。

  回避策：ありません。CSCun08435

- スイッチが Supervisor Engine 2 を搭載した IOS リリース 12.2(53)SG6 を実行しており、電話機と PC が MAB 経由で認証（または許可）され、マルチ認証モードのポートに接続されている場合（認証オープン）、両方のセッションが理由なく 30 秒後に削除されます。

  ```
  AUTH-FEAT-MDA-EVENT (Fa3/6): Deleting all clients in domain DATA
  ```

  回避策：ありません。CSCuo56266

- スイッチが Supervisor Engine II を搭載した IOS リリース 12.2(53)SG6 を実行している場合、データクライアントは認証セッションを受信しますが、ホストモードがポートのマルチ認証で設定されている状態では、音声クライアントのセッションは認証モニタモード（認証オープン）で作成されません。

  回避策：ありません。CSCuo56625

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

Cisco IOS リリース 12.2(53)SG10 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG10 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

– このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  – パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。

  – スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策: ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。(CSCsr00333)

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。

– クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

回避策:「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策:ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインライン電源の供給を停止します。

  回避策:hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策:コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策:ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  または
  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  および
  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策:Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。

  CSCtq73579

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R+E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R + Eではなく WS-C4510R-Eです。

  回避策：

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。(CSCsk52542)

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。(CSCsk43618)

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。(CSCsk72544)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：**show policy-map interface** コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。(CSCsl72868)

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。(CSCso06422)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。(CSCsm81875)

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。(CSCso71647)

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  (CSCso96660)

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合(FlexLink の障害)、代替ポートに移動されません。

  回避策: ありません。(CSCsq99468)

- CFM Inward Facing MEP(IFM)が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします(ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため)。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトラングポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

n はスロット番号です。

スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

回避策：WS-C4510R+E および WS-C4507R +E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG10 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG10 で解決済みの警告について説明します。

- dot1x またはポートセキュリティが設定されているポートでの MAC エージングまたはラーニング中に、次のメッセージが表示されます。

  ```
  %C4K_HWL2MAN-4-ADDRESSNOTLOADABLE message appears
  ```

  回避策：ありません。メッセージは表面的なものです。CSCue77562

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Cisco IOS リリース 12.2(53)SG9 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG9 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

  回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  （CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策: インターフェイスをシャットダウンしてから再度開きます。(CSCso50921)

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策: ISL/dot1q トランクポートを設定します。(CSCsu43445)

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策: 次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  (CSCsv44866)

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策: ありません。(CSCsw14005)

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン(CDP ポートのステータス TLV サポート搭載)にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策: ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

回避策：ありません。

CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で **shut** と入力してから、**no shut** を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  または

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  および

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。

  CSCtq73579

- dot1x またはポートセキュリティが設定されているポートでの MAC エージングまたはラーニング中に、次のメッセージが表示されます。

  ```
  %C4K_HWL2MAN-4-ADDRESSNOTLOADABLE message appears
  ```

  回避策：ありません。メッセージは表面的なものです。CSCue77562

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R+E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

  回避策：

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。(CSCsk52542)

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。(CSCsk43618)

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。(CSCsk72544)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：**show policy-map interface** コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。(CSCsl72868)

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。(CSCso06422)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

  n はスロット番号です。

スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

回避策：WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG9 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG9 で解決済みの警告について説明します。

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- Cisco IOS ソフトウェアの Virtual Route Forwarding（VRF）対応ネットワークアドレス変換（NAT）機能の実装には、IP パケットの変換時の脆弱性があり、認証されていないリモートの攻撃者がサービス妨害（DoS）状態を引き起こすおそれがあります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策がありません。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  注：2013 年 3 月 27 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、7 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。すべてのアドバイザリが Cisco IOS ソフトウェアの脆弱性を扱っています。各 Cisco IOS ソフトウェアのセキュリティアドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2013 年 3 月にバンドルされているすべての Cisco IOS ソフトウェアの脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクについては、次のリンクの Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

  CSCtg47129

Cisco IOS リリース 12.2(53)SG8 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG8 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

– このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  – パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。

  – スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策: ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。(CSCsr00333)

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

回避策：ありません。

キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、**no shut** を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  または
  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  および
  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。
  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。CSCtq73579

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R + E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

  回避策：

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。(CSCsk52542)

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。(CSCsk43618)

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。(CSCsk72544)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：**show policy-map interface** コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。(CSCsl72868)

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。(CSCso06422)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。

- スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

  リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

n はスロット番号です。

スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

回避策：WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG8 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG8 で解決済みの警告について説明します。

- CDP フレームの処理中に、SYS-2-FREEFREE および SYS-6-MTRACEメッセージが表示された後でスイッチがクラッシュすることがあります。

  回避策：no cdp run コマンドを入力して、CDP を無効にします。CSCub45763

Cisco IOS リリース 12.2(53)SG7 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG7 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策: 次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）
- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策: ありません。（CSCsw14005）
- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661
- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策: ありません。CSCsy72343
- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策: ありません。

  CSCsy38640
- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策: ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  または
  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  および
  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。CSCtq73579

- CDP フレームの処理中に、SYS-2-FREEFREE および SYS-6-MTRACEメッセージが表示された後でスイッチがクラッシュすることがあります。

  回避策：no cdp run コマンドを入力して、CDP を無効にします。CSCub45763

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R + E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

  回避策：

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

  n はスロット番号です。

  スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

```
%C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
supervisor detected. Detected the Standby Supervisor bootupFailed
```

アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

回避策：WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG7 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG7 で解決済みの警告について説明します。

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクについては、次のリンクの Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  次の条件が当てはまる場合：

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

  回避策：ありません。CSCtx61557

Cisco IOS リリース 12.2(53)SG6 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG6 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

  回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  （CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策: インターフェイスをシャットダウンしてから再度開きます。(CSCso50921)

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策: ISL/dot1q トランクポートを設定します。(CSCsu43445)

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策: 次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  (CSCsv44866)

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策: ありません。(CSCsw14005)

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン(CDP ポートのステータス TLV サポート搭載)にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策: ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

回避策：ありません。

CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  または

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  および

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。

  CSCtq73579

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。
  CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

次の条件が当てはまる場合:

- スイッチポートは次のように設定されます。

  authentication event server dead action authorize...

  authenticaton event server alive action reinitalize

- 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

  RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

回避策: ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策: トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策: すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策: ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R + E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

  回避策:

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策: ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：**show policy-map interface** コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします(ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため)。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策:スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

  n はスロット番号です。

  スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

  ```
  %C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
  supervisor detected. Detected the Standby Supervisor bootupFailed
  ```

  アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

  2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

  回避策:WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

  CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策:Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策:ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG6 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG6 で解決済みの警告について説明します。

- 認証オープンで MDA またはマルチ認証ホストモードの組み合わせを使用する場合、スイッチはユニキャスト EAPOL 応答を無視します。

  回避策:

  - サプリカントにマルチキャスト EAPOL の使用を強制する
  - 認証オープンモードを回避します。CSCtq33048

- rep preempt segment コマンドを入力すると、MAC がフラッシュしないことがあります。

  回避策:rep preempt segment コマンドを再入力します。

  CSCtr89862

- ポリシーベースルーティング(ルートマップ)の変更後にスイッチがクラッシュします。

  回避策:ルートマップのデフォルトのネクストホップを変更する前に、インターフェイスでポリシーが設定されていることを確認します。CSCtr31759

- IPv4 アドレスが設定されていない場合、IPv6 SNMP で次の問題が発生します。

  - トラップは IPv6 を介して送信されません。
  - スイッチの IPv6 アドレスに送信された SNMP GET がトレースバックをトリガーします。

  回避策:次のタスクを実行します。

  1. no snmp-server コマンドを使用して SNMP エンジンを無効にします。
  2. ループバック インターフェイスで IPv4 アドレスと IPv6 アドレスを設定します。
  3. SNMP エンジンを有効にします。

  CSCsw76894

- IPv4 アドレスを割り当てる前に SNMP を有効にすると、SNMP は要求をリッスンしません。

  回避策:次のタスクを実行します。

  1. no snmp-server コマンドを使用して SNMP エンジンを無効にします。
  2. ループバック インターフェイスで IP アドレスと IPv6 アドレスを設定します。
  3. SNMP エンジンを有効にします。

  CSCsw92921

- FlexLink ロードバランシングを使用する場合、バックアップ インターフェイスをソースとする MAC アドレスは、ダイナミック MAC アドレステーブルにプログラムされません。送信元アドレスの学習は、これらの MAC アドレスからのすべてのトラフィックに対してトリガーされ、CPU 使用率が高くなる可能性があります。

  回避策:バックアップ FlexLink インターフェイスの送信元アドレスにスタティック MAC アドレスを設定します。CSCtr40070

- ラウンドトリップ時間(RTT)遅延が 5 ミリ秒以上のネットワークでは、IP SLA イーサネット ジッター プローブが NoConnection/Busy/Timeout 状態でスタックします。

  ```
  uPE1#sh ip sla stat | inc Timeout
  Latest RTT: NoConnection/Busy/Timeout
  ```

  この問題は、低遅延(5 ミリ秒未満)の環境では発生しない可能性があります。

回避策:

- なし(イーサネット ジッター プローブに関して)
- IP sla ethernet echo プローブを使用して RTT 統計情報を収集することを検討してください。CSCtb96522

- LLDP ネイバーエントリごとに 10 を超える MA(管理アドレス)TLV を受信すると、システムがクラッシュする可能性があります。

  回避策: ピアで LLDP MA TLV 送信を無効にします。CSCtj22354

- 無効なインデックスを使用して rttMonHistory オブジェクトをクエリすると、スイッチがクラッシュします。

  回避策: get ではなく getnext を使用して、MIB OID の有効なインデックスをリストします。CSCtr52740

- TCL ポリシーを登録すると、スイッチがハングすることがあります。

  回避策: ありません。CSCto72927

- メンバーリンクまたはポートチャネルのフラップが発生した後、フラッディングされたマルチキャストトラフィックがポートチャネル インターフェイスを介して送信されません。

  回避策:

  - no vlan vlan_id および vlan vlan_id コマンドを使用して、影響を受ける VLAN を削除および追加します。
  - shutdown コマンドと no shutdown コマンドを使用して、影響を受けるポートチャネルをフラップします。CSCtr17251

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策: 次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  (CSCsv69853)

Cisco IOS リリース 12.2(53)SG5 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG5 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策: 次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）
- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策: 次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）
- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策: ありません。（CSCsw14005）
- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：「deny ip any any」に加えて、デフォルト ACL にエントリを追加します。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  または
  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```
  および
  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14" (where n is a slot number)
  ```

  回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

  CSCtl70275

- ポートがプライベート VLAN 用に設定され、ゲスト VLAN で許可されている場合、コンソールにトレースバックが表示されます。

  回避策：ありません。

  CSCtq73579

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。
  CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

次の条件が当てはまる場合:

- スイッチポートは次のように設定されます。

  authentication event server dead action authorize...

  authenticaton event server alive action reinitalize

- 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

  RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

回避策: ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策: トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策: すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策: ありません。（CSCso93282）

  Supervisor Engine II+10GE が 4510R + E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

  Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

  回避策:

  - Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
  - 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

  CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策: ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします(ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため)。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策:スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
  14
  ```

  n はスロット番号です。

  スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

  ```
  %C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
  supervisor detected. Detected the Standby Supervisor bootupFailed
  ```

  アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

  2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

  回避策:WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

  CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策:Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策:ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG5 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG5 で解決済みの警告について説明します。

- 余分なスペースを含むプロキシ ACL ACE を指定すると、認証されたホストや許可されたホストに対してプロキシ ACL がプログラムされません。

  回避策:

  - プロキシ ACL ACE を指定するときは、余分なスペースを含めないでください。
  - プロキシ ACL ではなく、ダウンロード可能な ACL またはフィルタ ID ACL を使用します。CSCtk67010

- 出力ポリシーマップが「単一の」アクティブポートに適用されている場合、マルチキャスト制御パケット（HSRP および OSPF）の IP ToS フィールドは変更できません。

  回避策：ありません。CSCtg60011

- Catalyst 4500 シリーズ スイッチに接続されたインターフェイスは、アクティブ スーパバイザ エンジンが存在しない場合でもリンクされたままになります。

  この状況は、非冗長スイッチのラインカードにピアスイッチが接続されている場合に、アクティブ スーパバイザ エンジンをリロードすると発生します。一部のラインカードの一部のインターフェイスはリンクされたままです。遠端スイッチは、プロトコルタイムアウトに依存してスイッチのリロードを検出する必要があります。

  この状況は、WS-X4648-RJ45-E および WS-X4548-RJ45-VE ラインカードでのみ発生します。

  回避策：hw module module n コマンドを使用してラインカードをリセットし、スイッチをリロードします。CSCtl11764

- 2 線式または 4 線式ケーブル（1、2、3、6）を使用して 4648-RJ45-E/+E ラインカードポートに接続すると、一部の非受電デバイスがリンクアップしません。

  回避策:

  - 4 ペア線を使用します。
  - power inline never コマンドを入力します。
  - speed auto 10 100 コマンドを入力します。CSCtn43537

- IP デバイストラッキングを使用してスイッチに再接続すると、Windows Vista、Windows 2008、または Windows 2007 デバイスが重複アドレスメッセージを登録します。

  回避策：Windows デバイスで Gratuitous ARP を無効にします。CSCtn27420

- ゲスト VLAN のポートに接続された 802.1X サプリカントが初期認証に失敗します。

  回避策:

  - 802.1X を再試行するようにサプリカントを設定します。
  - ポートに接続するか、ポートとの接続を切断します。CSCtl89361

- Web 認証用に AAA アカウンティングパケットが生成されると、スイッチがクラッシュします。

  回避策：AAA アカウンティングを無効にします。CSCtl77241

- IP SLA プローブが設定され、72 週間アクティブになっているときに、プローブ統計情報のために rttmon mib をポーリングすると、ルータがリロードされます。

  問題は、その後 72 週間は観察されません。

  回避策：ありません。CSCsl70722

- デバイスがスイッチの複数のポートに接続されていて、no ip routing が設定されていない場合、ARP エントリが誤った VLAN に表示されます（pv vlan がエントリに表示されます）。

  回避策：ip routing を設定します。CSCtj20399

- スイッチが Web 認証で 802.X を使用しているときに、http セッションを開くと、https ではなく http を使用したログイン画面が表示されます。

  これは、次のように設定されたカスタムバナーを使用する場合にのみ発生します。

  ```
  ip auth-proxy auth-proxy-banner http ^C Custom Banner here ^C
  ```

  回避策：カスタムバナーを削除します。CSCtb77378

- フォールバック設定を削除する前にクライアントの認証方式を Web 認証に変更すると、Web 認証がトリガーされます。

  回避策：

  - no dot1x pae authenticator/dot1x pae authenticator コマンドを使用して802.1Xを再設定します。
  - スイッチをリロードします。CSCtd43793

- dot1q トランクのネイティブ VLAN がデフォルト（VLAN 1）でない場合、LLDP パケットは（.1q）タグ付きで送信されます。

  LLDP IEEE 標準規格では、タグなしでフレームを送信する必要があります。この問題により、一部のピアデバイスがタグ付き LLDP フレームを拒否することがあります。

  回避策：トランクにデフォルトのネイティブ VLAN を使用します。CSCtn29321

- 冗長電源がオフの場合、スーパバイザエンジンの LED がオレンジ色の場合でも、ciscoEnvMonAlarmContacts から 00 が返されます。

  回避策：デバイス設定に snmp-server enable traps envmon を含めると、電源がオフになるか、または障害が発生したときに ciscoEnvMonSuppStatusChangeNotification が生成されます。CSCtl72109

- ip cef accounting non-recursive が設定されていて、BGP ルートが提供されている場合、スイッチがクラッシュする可能性があります。

  回避策：IP cef アカウンティングを無効にします。CSCtn68186

- 次の条件が当てはまる場合、ポートチャネルは正しく確立されません。

  - vlan dot1q tag native が設定されている。
  - ネイティブ VLAN がトランクで許可されていないか、ピアがタグ付きチャネルプロトコルのパケットを受け入れていない。

  回避策：ありません。CSCtj90471

- 電源装置は取り外されたものとしてリストされますが、正常に機能し続けます。この動作は、次のシステムメッセージで示されます。

  ```
  %C4K_IOSMODPORTMAN-4-POWERSUPPLYREMOVED: Power supply 1 has been removed
  %C4K_CHASSIS-3-INSUFFICIENTPOWERSUPPLIESDETECTED: Insufficient power supplies present
  for specified configuration
  %C4K_CHASSIS-2-INSUFFICIENTPOWERDETECTED: Insufficient power available for the
  ```

  回避策：ありません。CSCtn38000

- それぞれが異なる VLAN リストを持つ複数の REP リングが使用されている場合、MAC ラーニングが絶えず行われるため、CPU 使用率が高くなります。

  回避策：問題が発生した REP リングに STCN をエクスポートする他の REP リング内のポートを含め、REP リングトポロジ内のすべてのトランクポートに同じ VLAN リストが設定されていることを確認します。CSCto67625

- アンナンバード インターフェイスでロードバランシングされた DHCP リレーを介して更新する DHCP クライアントは、更新 ACK が失われるため、リースを更新できない場合があります。

  回避策：DHCP ロードバランシングを使用しないでください。CSCth00482

- スイッチが複数認証ホストモードに設定されており、そのスイッチのインターフェイスが 802.1X に対して設定されている場合、そのインターフェイスは単方向ポート制御を許可せず、Wake-on-LAN の機能を中断します。

  回避策：別のホストモードを使用します。CSCti92970

- 内部テスト中に、破損した SSH パケットによるメモリリークが SSH プロセスで検出されました。

  回避策：信頼できるホストからの SSH 接続のみを許可します。CSCth87458

- プロキシ ACL ACE を指定する際に、間に余分なスペースを追加すると、認証されたホストや許可されたホストに対してプロキシ ACL がプログラムされません。

  回避策

  - プロキシ ACL ACE を指定するときは、余分なスペースを含めないでください。
  - プロキシ ACL の代わりに DACL またはフィルタ ID ACL を使用します。CSCtk67010

- マルチ認証モードでは、Cisco IP 電話の背後にある PC を切断しても、データセッションは削除されません。

  これは想定されている動作です。マルチ認証モードでは、電話機に接続されているデータクライアントと、ハブを介してスイッチに接続されているデータクライアントを区別できません。

  回避策：ありません。CSCtd70009

- no set extcommunity cost を使用してルートマップ内の set extcommunity cost を削除し、show run と入力すると、スイッチがクラッシュします。

  回避策：ルートマップ全体を削除して、再作成します。CSCsr23563

- SSH および Telnet が設定されたスイッチでは、バナーを設定してからルータに SSH 接続すると、バナーが正しく表示されません。

  ```
  pqiu@apt-cse-613% ssh cisco@10.66.79.211
  "$(hostname) via line $(line) $(line-desc)"
  ```

  バナーの設定方法を次に示します。

  ```
  banner login ^CC
  $(hostname) via line $(line) $(line-desc)
  ^C
  !
  ```

  ルータに Telnet 接続すると、次のようにバナーが正しく表示されます。

  ```
  "SV-9-5 via line 67"
  ```

  回避策：ありません。CSCei24145

- REP リングトポロジでリロードされたスイッチを起動すると、すぐに代替ポートがトラフィックを転送し、ループが発生します。ループは、代替ポートで shut および no shut を入力するまで続きます。

  回避策：代替インターフェイスで shut と no shut を入力します。CSCtn03533

- 直接接続されたネットワークから到達可能な RP アドレスにスタティックルートが設定されている場合、スイッチが PIM レジスタを RP に送信しません。

  回避策：重複する IP アドレスを設定しないでください。CSCtj96095

Cisco IOS リリース 12.2(53)SG4 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG4 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets<--------It stays at '0' despite of traffic being received
      Match: access-group name fnacl21
      police: Per-interface
        Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

– このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  – パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。

  – スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策: ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。(CSCsr00333)

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで802.1Xの設定を解除し、スイッチに接続されているIPフォン（CDPポートのステータスTLVサポート搭載）にホストを再接続すると、ホストのMACアドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストのMACアドレスが新しいアクティブなスーパバイザエンジンのMACアドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで**shutdown**コマンドを入力し、その後に**no shutdown**コマンドを入力します。これにより、ホストのMACが再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLANトランクポートのプライマリVLANに接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDAを使用する.1Xがホストモードに設定され、ゲストVLANが有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対してshow adjacency x.x.x.x internalコマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは0のままです。

  回避策：ありません。

  CSCsu35604

- Cisco IOSリリース12.2(52)SGを実行している冗長スイッチでは、802.1Xを介してポートが許可された後、show dot1x interface statisticsコマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数のOAMモニタリングが設定されたWS-C4900Mシャーシで複数のストリームのCRCエラーが発生した場合、次のCLIを設定すると、OAMはエラーフレーム秒数の値を正しく報告しません。

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドのCall Homeメッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
```

```
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- ファイルのサイズが 0 Kb の場合、スイッチは DHCP スヌーピングファイルへの FTP に失敗することがあります。

  回避策：ファイルを作成するときに、いくつかの文字を入力し、ftp コマンドを削除してから再入力します。以下を参照。

  ```
  Switch(config)# no ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.$
  Switch(config)# ip dhcp snooping database ftp://griff:ddd@192.168.1.4/test1.log
  ```

  CSCsk38763

- 次のメッセージは、サポートされているバージョンの Catalyst 4500 ソフトウェアを WS-C4507R+E および WS-C4510R+E にロードし、いずれのポートも起動しない場合に表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  または

```
%C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
WS-C4507R-E, but chassis' serial eeprom chassis type is Unknown chassis type
```

および

```
%C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type
14" (where n is a slot number)
```

回避策：Cisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG 以降をロードします。

CSCtl70275

- 余分なスペースを含むプロキシ ACL ACE を指定した場合、認証されたホストや許可されたホストに対してプロキシ ACL がプログラムされません。

  回避策：

  - プロキシ ACL ACE を指定するときは、余分なスペースを含めないでください。
  - プロキシ ACL の代わりにダウンロード可能な ACL またはフィルタ ID ACL を使用します。

  CSCtk67010l

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。
  CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

```
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
```

次の条件が当てはまる場合:

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

回避策: ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

回避策: トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

回避策: すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

回避策: ありません。（CSCso93282）

Supervisor Engine II+10GE が非実稼働 4510R+E シャーシで起動しようとすると、次のエラーメッセージが表示されます。

```
" ERROR!
Sup II+10GE 10GE (X2), 1000BaseX (SFP) not supported in WS-C4510R-E chassis, system
can not boot
Rebooting in 10 seconds...
10  09  08  07  06  05  04  03  02  01  "
```

Supervisor Engine II+10GE は、10 スロットシャーシではサポートされません。したがって、正しいメッセージが表示されますが、表示されるシャーシタイプは WS-C4510R+Eではなく WS-C4510R-Eです。

回避策:

- Supervisor Engine II+10GE を 7 スロットシャーシに配置します。
- 10 スロットシャーシでサポートされているスーパバイザエンジンを配置します。シャーシタイプの識別の不一致は、単に表面的なものです。

CSCtl80173

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策: ありません。(CSCsk66449)

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent(キューの輻輳のため、ドロップに応答して返信待機しないフロー)として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策: 問題となっているキューがデフォルト以外の場合(キューイングアクションがポリシーマップの class-default クラスで設定されていない場合)、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。(CSCsk62457)

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策: ありません。(CSCsk52542)

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策: X2 を再挿入します。(CSCsk43618)

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

回避策：ありません。

（CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(53)SG4、12.54(SG)、または 15.0(1)SG より前のリリースソフトウェアイメージを冗長 WS-C4510R+E または WS-C4507R +E シャーシにロードすると、アクティブ スーパバイザ エンジンに次のログメッセージが表示されます。

  ```
  %C4K_CHASSIS-3-CHASSISTYPEMISMATCHINSPROM: Supervisor's FPGA register chassis type is
  WS-C4510R-E, but chassis' serial eeprom chassis type is Unknown chassis type
  ```

  アクティブ スーパバイザ エンジンは、シャーシの各ラインカードスロットについて次のログメッセージも表示します。

  ```
  %C4K_CHASSIS-2-MUXBUFFERTYPENOTSUPPORTED: Mux Buffer in slot <n> of unsupported type 14
  ```

  n はスロット番号です。

  スタンバイ スーパバイザ エンジンが起動すると、アクティブ スーパバイザ エンジンは次のメッセージを表示してリブートします。

  ```
  %C4K_REDUNDANCY-2-POSTFAIL_RESET: Power-On Self Test (POST) failure on ACTIVE
  supervisor detected. Detected the Standby Supervisor bootupFailed
  ```

  アクティブ スーパバイザ エンジンが稼働している間は、スイッチでトラフィックを処理できません。

  2 つのスーパバイザエンジンが交互に連続してリブートする場合があります。

  回避策：WS-C4510R+E および WS-C4507R+E シャーシでCisco IOS リリース 12.2(53)SG4、12.2(54)SG、15.0(1)SG以降のイメージを使用します。

  CSCtl84092

- Cisco IOS リリース 12.2(53)SG3 以前の LAN Base イメージを WS-C4510R+E または WS-C4507R+E シャーシにロードすると、システムがハングし、エラーメッセージは表示されません。

  Cisco IOS リリース 12.2(53)SG3 および以前のリリースは、WS-C4510R+E および WS-4507R+E シャーシではサポートされず、ロード時に有効なエラーメッセージが表示されます。

  回避策：Cisco IOS リリース 12.2(53)SG4 以降から LAN Base イメージをロードします。

  CSCtl89329

- Supervisor Engine 6-E または Supervisor Engine 6L-E が 4507R+E または 4510R+E シャーシに挿入されている場合、ROMMON はシャーシを 4507R-E または 4510R-E として誤って報告します。

  回避策：ありません。CSCtl74638

Cisco IOS リリース 12.2(53)SG4 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG4 で解決済みの警告について説明します。

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。

  CSCsw42967

- CX1 または SFP+ を WS-X4908-10GE の OneX コンバータ（CVR-X2-SFP10G）に接続すると、リンクの起動に 1 分かかります。

  回避策：ありません。

  CSCtc46340

- Cisco IOS リリース 12.2(53)SG3 または IOS-XE 3.1.0 SG を実行しているスイッチで大きなカスタム Web 認証ログインページを使用しており、複数のユーザがカスタム HTML ページにアクセスしようとすると、スイッチがリロードされることがあります。

  回避策：デフォルトの内部 Web 認証ページを使用するようにカスタマイズされた HTML ページの設定解除し、設定変更後にスイッチをリロードします。CSCti81874

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

Cisco IOS リリース 12.2(53)SG3 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG3 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

  （SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

- このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策: 再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策: 12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

回避策: ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

この状況は、次の理由で発生する可能性があります。

- パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
- スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。

  - ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策: ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。(CSCsr00333)

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策: ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。(CSCsv54529)

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策: ありません。(CSCsw14005)

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン(CDP ポートのステータス TLV サポート搭載)にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策: ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策: ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策: ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策: ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策: ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

  ```
  Switch# call-home send alert-group diagnostic module 2
  Sending diagnostic info call-home message ...
  Please wait. This may take some time ...
  Switch#
  *Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
  message failed to send (ERR 18, The alert group is not subscribed)
  ```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- WS-X4548-GB-RJ45V は、冗長スーパバイザエンジンへのスイッチオーバーを実行し、ウォッチドッグタイマーを期限切れにした後、インターフェイス 1 ー 8 へのインラインパワーの供給を停止します。

  回避策：hw-module reset コマンドを入力して、ラインカードをリロードします。

  CSCti17849

- コールまたはパケットのドロップが定期的に増加し、スイッチで使用可能な空きメモリが常に減少している場合は、show memory debug leak コマンドを使用できます。ただし、このコマンドは CPU 使用率が高いため、ライブネットワークで使用すると、コールまたはデータセッションが切断される可能性があります。

  show memory debug relay lowmem コマンドは、メモリが非常に少ない状況でも機能しますが、CPU の負荷が非常に高いためにスイッチがクラッシュする可能性があります。また、完了までに 20 ー 90 分かかります。

  回避策：コールまたはパケットドロップが続く場合は、これらのコマンドを自分で入力せずに、TAC にお問い合わせください。CSCsi48986

- Cisco IOS リリース 12.2(53)SG3 または IOS-XE 3.1.0 SG を実行しているスイッチで大きなカスタム WebAuth ログインページを使用しており、複数のユーザがカスタム HTML ページにアクセスしようとすると、スイッチがリロードされることがあります。

  回避策：デフォルトの内部 WebAuth ページを使用するようにカスタマイズされた HTML ページの設定解除し、設定変更後にスイッチをリロードします。CSCti81874

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  次の条件が当てはまる場合：

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

  回避策：ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- CX1 または SFP+ を WS-X4908-10GEの OneX コンバータ（CVR-X2-SFP10G）に接続すると、リンクの起動に 1 分かかります。

  回避策：ありません。

  CSCtc46340

Cisco IOS リリース 12.2(53)SG3 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG3 で解決済みの警告について説明します。

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。CSCsv42869

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイル（最大 256 KB）に埋め込みます（RFC 2397 に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  CSCsu37834

- スタンバイ スーパバイザ エンジン WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

  回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

  スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。CSCsy70428

- Cisco IOS リリース 12.2(53)SG1、12.2(50)SG6、またはそれ以降のリリースを実行し、スイッチでスイッチポート ブロック マルチキャストを設定すると、レイヤ 2 マルチキャストはブロックされません。IPv4 と IPv6 の不明なマルチキャストがブロックされます。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。CSCta61825

  回避策：ありません。CSCtb30327

- ACL ではなくプレフィックスリストで一致するように設定された PBR ポリシーがインターフェイスに接続されている場合、スイッチがクラッシュします。

この問題は、次のいずれかの条件が当てはまる場合に発生します。

- プレフィックスリストで一致するルートマップは、PBR ポリシーとして入力インターフェイスに付加されます。
- （インターフェイスにすでに接続されている）PBR のルートマップが、ACL ではなくプレフィックスリストで一致するように設定または変更されている。

回避策：ACL でのみ一致するように PBR のルートマップを設定します。CSCtg22126

- SSH 設定では、access-class vty-login in を使用する場合、VRF のインターフェイスで Telnet を実行できません。SSH はまだ使用可能ですが、有効になっていません。記載されているように、vrf-also キーワードが access-class で使用されていない場合、VRF のインターフェイスへの SSH 接続は機能しません。

  Cisco IOS リリース 12.2(53)SG3 にアップグレードした後は、SSH 設定の任意の access-class の後に vrf-also キーワードが続くようにします。

  回避策：ありません。CSCsv86113

Cisco IOS リリース 12.2(53)SG2 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG2 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	< 未使用のキュー >	control-packet
	11	< 未使用のキュー >	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。

– CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

（CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  – ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。

  – アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。

b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。

c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

（CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。

  – 該当ポートに SFP+ を挿入します。

  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  – Internet Explorer 8

  – Mozilla Firefox

  – Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

  回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

CSCsy70428

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

CSCsz05888

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

回避策：ありません。

キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

回避策：ありません。

CSCsz06719（現時点では、4500 + 4900）

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

回避策：ポート で shut と入力してから、no shut を入力します。

CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- Cisco IOS リリース 12.2(53)SG1、12.2(50)SG6、またはそれ以降のリリースを実行し、スイッチでスイッチポート ブロック マルチキャストを設定すると、レイヤ 2 マルチキャストはブロックされません。IPv4 と IPv6 の不明なマルチキャストがブロックされます。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。（CSCta61825）

  CSCtb30327

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- ACL ではなくプレフィックスリストで一致するように設定された PBR ポリシーがインターフェイスに接続されている場合、スイッチがクラッシュします。

  この問題は、次のいずれかの条件が当てはまる場合に発生します。

  - プレフィックスリストで一致するルートマップは、PBR ポリシーとして入力インターフェイスに付加されます。
  - （インターフェイスにすでに接続されている）PBR のルートマップが、ACL ではなくプレフィックスリストで一致するように設定または変更されている。

  回避策：ACL でのみ一致するように PBR のルートマップを設定します。

  CSCtg22126

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  次の条件が当てはまる場合:

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート(たとえば、デバイスが接続されていないハブ)が、関連付けられた MAC アドレスのないアクセス不能認証バイパス(IAB)VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

  回避策:ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策:トランクポートのネイティブ VLAN のデフォルト設定(VLAN 1)を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策:すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策:ありません。(CSCso93282)

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策:ありません。(CSCsk66449)

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent(キューの輻輳のため、ドロップに応答して返信待機しないフロー)として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策:問題となっているキューがデフォルト以外の場合(キューイングアクションがポリシーマップの class-default クラスで設定されていない場合)、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。(CSCsk62457)

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。(CSCsk52542)

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。(CSCsk43618)

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。(CSCsk72544)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。(CSCsl72868)

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。(CSCso06422)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

  リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- CX1 または SFP+ を WS-X4908-10GE の OneX コンバータ（CVR-X2-SFP10G）に接続すると、リンクの起動に 1 分かかります。

  回避策: ありません。

  CSCtc46340

Cisco IOS リリース 12.2(53)SG2 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG2 で解決済みの警告について説明します。

- Cisco IOS リリース 12.2(52)SGA を実行している Catalyst 4510R シャーシの WS-X45-SUP6-E は、7 つ以上の WS-X4248-RJ45V がシャーシにインストールされている場合、起動に失敗することがあります。

  これは、Cisco IOS リリース 12.2(52)SG でのみ発生します。

  回避策：Cisco IOS リリース 12.2(50)SG3 にダウングレードします。

  CSCta99577

- マルチ認証が有効な 802.1X ポートは、正常に認証された電話機の MAC アドレスの学習を開始しない場合があります。

  回避策：authentication host-mode multi-domain コマンドを使用して、（マルチ認証モードではなく）マルチドメインモードでポートを設定します。

  CSCtb28114

- HSRP や OSPF などのプロトコルにサブセカンドタイマーを使用すると、ブートフラッシュへの書き込みによって CPU 使用率が高くなり、プロトコルのフラッピングが発生する可能性があります。

  回避策：大きなファイルをコピーするなど、IOS では長時間のブートフラッシュ操作はしないでください。

  CSCsw84727

- PBR ポリシーは、Cisco IOS リリース 12.2(53)SG または 12.2(52)SG を実行している Supervisor Engine 6 では適用されません。パケットは、ポリシーベースのルーティングではなく、通常のルーティングテーブルを介して転送されます。

  これは、共有度の高いパスの副次的影響です。

  回避策：ありません。

  CSCtc90702

- Cisco IOS リリース 12.2(52)SG、12.2(52)XO、12.2(53)SG、または 12.2(53)SG1 にアップグレード後、フラッシュデバイス名がデフォルトの名前 flash: とは異なる場合、コンソールに継続的に次のメッセージが表示されることがあります。

  ```
  %Error copying flash:/eem_pnt_2 (Invalid path)
  ```

  回避策：フラッシュデバイスの名前をデフォルトの名前 flash: に変更します。

  CSCte05909

- MAC ラーニングは、ゲスト VLAN、Wake-on-LAN、およびポートセキュリティでは機能しません。インターフェイスでこれらの機能を同時に有効にすると、MAC ラーニングは機能せず、どのパケットも転送されません。

  回避策：ありません。

  インターフェイスで Wake-on-LAN を無効にする必要があります。

  CSCtc58982

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- PVLAN 独立ポートが、マルチキャスト送信元として機能するルータに接続され、IGMP スヌーピングを有効にすると、独立ポートに接続されたルータは PIM ネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 802.1X ポートをゲスト VLAN に対して有効にした後、RADIUS サーバに接続されているポートをシャットダウンして、サーバが停止し、EAPOL パケットがそのポートで送信されると、サーバは到達不能ですが、アクセス VLAN で許可されます。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCsz63355

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行している冗長 Catalyst 4500 シリーズスイッチでは、インターフェイスネイバーから FastEthernet1 インターフェイス（管理インターフェイス）への ping が SSO スイッチオーバーの直後に失敗することがあります。

  回避策：ネイバースイッチの ARP テーブルをクリアします。

  CSCsy86030

- 明示的なホストトラッキングが有効になっているスイッチが IGMPv3 を実行している場合、IGMPv3 レポートの送信を停止したポートは、タイムアウトするまで IGMPv3 テーブルに表示されます。

  回避策：影響を受ける VLAN で明示的なホストトラッキングを無効にします。

  CSCsz28612

- Supervisor Engine V-10GE では、リロードまたは電源オフ/オンのたびに、システムクロックが最大 59 秒失われる（減少する）ことがあります。

  Cisco IOS リリース 12.2(31)SGA9、12.2(50)SG6、および 12.2(53)SG1 までのすべてのソフトウェアリリースが影響を受けます。

  回避策：スイッチを再起動後、clock set コマンドを使用してシステムクロックを調整します。

  CSCtc65375

- Cisco IOS リリース 12.2(53)SG を実行しているスイッチに、次のメッセージが表示されます。

  %C4K_EBM-4-HOSTFLAPPING：Ethernet OAM（EOAM）を使用して、レイヤ3（IPv4 および IPv6）パケットループ中にマスターループバックポートと送信元ポート間で発生

  このメッセージはパフォーマンスに影響しません。

  回避策：ありません。

  CSCtc26043

- EnergyWise が有効になっており、energywise level level recurrence importance importance at minute hour day_of_month month day_of_week 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、スイッチで繰り返しイベントを設定しています。時刻が夏時間から標準時間に変更されると、スイッチで以下の状態が発生する可能性があります。
  - PoE デバイスに電力を供給する場合に再起動する
  - PoE デバイスの電源を間違った時刻にオンまたはオフにする
  - 障害発生

  これは、次の年の時刻変更が現在の年の時刻変更後に発生した場合に発生します。

  時刻変更が発生する前に、次の回避策のいずれかを使用します。
  - EnergyWise 設定から繰り返しイベントを削除し、1 週間は繰り返しイベントを使用せず、時刻変更が発生してから 1 週間後に再設定します。
  - energywise level level recurrence importance importance time-range time-range-name インターフェイス コンフィギュレーション コマンドを使用して、イベントを再スケジュールします。
  - power inline auto 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、PoE ポートの電源をオンにします。

  CSCtc91312
- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannel が定義されていると、リブート後に FlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）
- ルータにグループの（*、G）エントリがある場合、非 RPF パケットが CPU にヒットするのをブロックする fastdrop エントリは作成されません。

  回避策：非 RPF パケットが非 RPF ポートに入るのをブロックする ACL を作成します。

  CSCta93522
- Supervisor Engine 6-E では、リロードまたは電源オフ/オンのたびに、システムクロックが最大 59 秒失われる（減少する）ことがあります。

  Cisco IOS リリース 12.2(31)SGA9、12.2(50)SG6、および 12.2(53)SG1 までのすべてのソフトウェアリリースが影響を受けます。

  回避策：スイッチを再起動後、clock set コマンドを使用してシステムクロックを調整します。

  CSCtc65375
- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。
  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- IOS リリース 12.2(53)SG1 または 12.2(50)SG6 を実行している 4500-E および 4900M スイッチは、特定の VLAN の唯一の QoS サービスポリシーが VLAN レベルである場合にクラッシュする可能性があります。

  この問題は、次の 3 つの条件を満たしている場合に発生します。

  - ソフトウェア生成またはソフトウェアスイッチド パケットが、VLAN（V）のメンバーであるインターフェイス（P）を出る。
  - パケットの優先順位が高くない。PAK_PRIORITY が設定されていない。
  - 出力方向の 3 つのターゲット（ポート P、VLAN V、およびポート VLAN PV）のうち、qos ポリシーマップが出力方向の VLAN V にのみ付加される。

  回避策:

  - VLAN 専用ポリシーマップにマーキングアクションのみがある場合は、VLAN 専用ポリシーマップを VLAN 内のすべてのポートのポート VLAN ポリシーマップに置き換えます。
  - VLAN 専用ポリシーマップにポリシングアクションがある場合は、VLAN 出力ポリシーマップを保持し、その VLAN のすべてのポートにキューイングアクション専用出力ポリシーマップを付加します。

  ポートレベルのポリシーマップは次のように表示されます。

  ```
  policy-map p1
      class class-default
          bandwidth percent 100
  ```

  CSCte12571

- Supervisor Engine II+10G E または Supervisor Engine V-10GE を実行している場合、X2-10GB-LRM リンクは起動時にダウンします。

  この問題は、Cisco IOS リリース 12.2(46)SG 以降のイメージで発生します。

  CSCtf26763

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンが危険温度になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策: show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの危険温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

Cisco IOS リリース 12.2(53)SG1 の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG1 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	< 未使用のキュー >	control-packet
	11	< 未使用のキュー >	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

  回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  （CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずに CTS SXP 接続が設定され、ボックスにデフォルトの SXP 送信元 IP アドレスが設定されていない場合、異なる SXP 接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

回避策：次のいずれかの操作を実行します。

- ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
- アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

（CSCsv44866）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- RADIUS サーバとクライアントを接続するポートが異なる VLAN に配置されている場合、ip radius source-interface コマンドを入力して 2 つの SSO スイッチオーバーを実行すると、認証されたセッションが失われます。

  回避策：クライアントを再認証します。

  CSCsx94066

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

回避策: フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

CSCsy37181

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

CSCsy70428

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

CSCsz05888

- アクセスリストがハードウェアリソースが極端に枯渇している状態でインターフェイスに接続されている場合、後でハードウェアリソースが使用可能になっても、ACL がハードウェアに自動的にロードされないことがあります。

新しいアクセスリストに使用できる TCAM エントリはありません。

回避策：スイッチ上の他の分類ポリシーを削除または短縮して、ハードウェア TCAM リソースを解放した後で、ACL を手動で削除して再適用します。

CSCsy85006

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

回避策：ありません。

キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

CSCsz20149

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

回避策：ありません。

CSCsz06719（現時点では、4500 + 4900）

- 802.1X ポートをゲスト VLAN に対して有効にした後、RADIUS サーバに接続されているポートをシャットダウンして、サーバが停止し、EAPOL パケットがそのポートで送信されると、サーバは到達不能ですが、アクセス VLAN で許可されます。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCsz63355

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行している冗長 Catalyst 4500 シリーズスイッチでは、インターフェイスネイバーから FastEthernet1 インターフェイス（管理インターフェイス）への ping が SSO スイッチオーバーの直後に失敗することがあります。

  回避策：ネイバースイッチの ARP テーブルをクリアします。

  CSCsy86030

- 明示的なホストトラッキングが有効になっているスイッチが IGMPv3 を実行している場合、IGMPv3 レポートの送信を停止したポートは、タイムアウトするまで IGMPv3 テーブルに表示されます。

  回避策：影響を受ける VLAN で明示的なホストトラッキングを無効にします。

  CSCsz28612

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- マルチ認証が有効な 802.1X ポートは、正常に認証された電話機の MAC アドレスの学習を開始しない場合があります。

  回避策：authentication host-mode multi-domain コマンドを使用して、（マルチ認証モードではなく）マルチドメインモードでポートを設定します。

  CSCtb28114

- Supervisor Engine V-10GE では、リロードまたは電源オフ/オンのたびに、システムクロックが最大 59 秒失われる（減少する）ことがあります。

  Cisco IOS リリース 12.2(31)SGA9、12.2(50)SG6、および 12.2(53)SG1 までのすべてのソフトウェアリリースが影響を受けます。

  回避策：スイッチを再起動後、clock set コマンドを使用してシステムクロックを調整します。

  CSCtc65375

- Cisco IOS リリース 12.2(53)SG1、12.2(50)SG6、またはそれ以降のリリースを実行し、スイッチでスイッチポート ブロック マルチキャストを設定すると、レイヤ 2 マルチキャストはブロックされません。IPv4 と IPv6 の不明なマルチキャストがブロックされます。

  Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 より前では、switchport block multicast コマンドは IP マルチキャスト、レイヤ 2 マルチキャスト、およびブロードキャスト トラフィックをブロックします。（CSCta61825）

  CSCtb30327

- Cisco IOS リリース 12.2(53)SG　を実行しているスイッチに、次のメッセージが表示されます。

  %C4K_EBM-4-HOSTFLAPPING：Ethernet OAM（EOAM）を使用して、レイヤ3（IPv4 および IPv6）パケットループ中にマスターループバックポートと送信元ポート間で発生

  このメッセージはパフォーマンスに影響しません。

  回避策：ありません。

  CSCtc26043

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

- EnergyWise が有効になっており、energywise level level recurrence importance importance at minute hour day_of_month month day_of_week 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、スイッチで繰り返しイベントを設定します。時刻が夏時間から標準時間に変更されると、スイッチで以下の状態が発生する可能性があります。

  - PoE デバイスに電力を供給するために再起動する
  - PoE デバイスの電源を間違った時刻にオンまたはオフにする
  - 障害発生

  これは、次の年の時刻変更が現在の年の時刻変更後に発生した場合に発生します。

  時刻変更が発生する前に、次の回避策のいずれかを使用します。

  - EnergyWise 設定から定期的なイベントを削除し、1 週間は定期的なイベントを使用せず、時刻変更が発生してから 1 週間後に再設定します。

  - energywise level level recurrence importance importance time-range time-range-name インターフェイス コンフィギュレーション コマンドを使用して、イベントを再スケジュールします。
  - power inline auto 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、PoE ポートの電源をオンにします。

  CSCtc91312

- Cisco IOS リリース 12.2(52)SG、12.2(52)XO、12.2(53)SG、または 12.2(53)SG1 にアップグレード後、フラッシュデバイス名がデフォルトの名前 flash: とは異なる場合、コンソールに継続的に次のメッセージが表示されることがあります。

  ```
  %Error copying flash:/eem_pnt_2 (Invalid path)
  ```

  回避策：フラッシュデバイスの名前をデフォルトの名前 flash: に変更します。

  CSCte05909

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

  回避策：ip cef accounting non-recursive コマンドを無効にします。

  （CSCtn68186）

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

  回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。
  CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

  Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

  シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

  このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

  CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  次の条件が当てはまる場合：

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

  回避策：ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- Cisco IOS リリース 12.2(52)SGA を実行している Catalyst 4510R シャーシの WS-X45-SUP6-E は、7 つ以上の WS-X4248-RJ45V がシャーシにインストールされている場合、起動に失敗することがあります。

  これは、Cisco IOS リリース 12.2(52)SG でのみ発生します。

  回避策：Cisco IOS リリース 12.2(50)SG3 にダウングレードします。

  CSCta99577

- ルータにグループの（*、G）エントリがある場合、非 RPF パケットが CPU にヒットするのをブロックする fastdrop エントリは作成されません。

回避策:非 RPF パケットが非 RPF ポートに入るのをブロックする ACL を作成します。

CSCta93522

- Supervisor Engine 6-E では、リロードまたは電源オフ/オンのたびに、システムクロックが最大 59 秒失われる(減少する)ことがあります。

  Cisco IOS リリース 12.2(31)SGA9、12.2(50)SG6、および 12.2(53)SG1 までのすべてのソフトウェアリリースが影響を受けます。

  回避策:スイッチを再起動後、clock set コマンドを使用してシステムクロックを調整します。

  CSCtc65375

- CX1 または SFP+ を WS-X4908-10GE の OneX コンバータ(CVR-X2-SFP10G)に接続すると、リンクの起動に 1 分かかります。

  回避策:ありません。

  CSCtc46340

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています(ICMP タイプまたは ICMP コード)。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策:ありません。

  CSCtc13297

Cisco IOS リリース 12.2(53)SG1 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG1 で解決済みの警告について説明します。

- 不明なマルチキャストトラフィックをブロックするために switchport block multicast をポートに設定すると、ブロードキャスト トラフィックもブロックされます。したがって、ポートは不明なマルチキャストまたはブロードキャスト トラフィックを受信しません。

  すべてのブロードキャスト トラフィック(ARP 要求や DHCP ディスカバリなど)は、ポートで受信されません。そのため、このようなブロードキャストを使用するプロトコルは動作を停止します。

  回避策:なし

  CSCta61825

- Cisco IOS リリース 12.2(50)SG1 を実行している Supervisor Engine 6-E または 6L-E を搭載したスイッチでは、次のいずれかを行うと EIGRP 隣接関係が切断されます。

  - VRF でマルチキャストルーティングを有効にせずに、VRF の VLAN インターフェイスで ip pim sparse-mode を有効にします。

– VRF でマルチキャストルーティングを有効にし、STP しきい値を無限に設定します。

回避策：スタティックネイバーを使用します。

CSCsz61756

- Supervisor Engine 6L-E およびいずれかのラインカード（WS-X4648-RJ45V-E/+E、WS-X4624-SFP、WS-X4606-10GE）を使用する冗長 SSO モードのスイッチでは、ラインカードが無効になり、次のメッセージが表示されることがあります。

```
%C4K_LINECARD-3-LINECARDWATCHDOGTIMEOUT: Module 2 linecard watchdog has expired.
%C4K_IOSMODPORTMAN-6-MODULEOFFLINE: Module 2 is offline
%C4K_IOSMODPORTMAN-6-MODULEOFFLINE: STANDBY:Module 2 is offline
```

show module コマンドは、ラインカードに障害があることを示します。

回避策：障害が発生したモジュールで hw-module reset を入力し、障害が発生したモジュールを再装着します。

CSCsz96231

- 非常にまれな状況において、Supervisor Engine 6-E および 6L-E がトラフィックの転送を停止することがあります。

この警告は、レジスタ値が破損し、その後レイヤ 3 機能を有効にした場合に発生します。

回避策：なし（CSCsz48273）

- サービスポリシーがポートチャネルにアタッチされ、そのサービスポリシーが CPU 生成パケットと一致するように設定されている場合、CPU 生成パケットの分類統計情報は増加しません。

回避策：アクセスリストを設定して、CPU 生成パケットを許可し、ACL をクラスマップに適用します。

CSCsy43967

- ポリシーマップを編集してポリサー設定を追加する場合に、do show policy-map interface または do show policy-map control-plane コマンドを入力すると、システムがリロードされます。

回避策：ポリシーマップ コンフィギュレーション モードではなく、EXEC モードで show policy-map interface および show policy-map control-plane コマンドを入力します。

CSCsy43261

- ポリシーマップがインターフェイスに適用されていて、そのインターフェイスが非アクティブ（つまり、ポートが TwinGig モードではなく 10GE モードで実行されている）の場合、show policy-map interface コマンドを入力すると、Supervisor Engines 6-E または 6L-E が Vector 0xD00 でクラッシュすることがあります。

回避策：ポートがアクティブであることを確認してから、ポリシーマップを適用するか、show policy-map コマンドを入力します。

以前に非アクティブだったインターフェイスをアクティブにするコマンドは次のとおりです。

hw-module module [module number] port-group [group number] select [gigabitethernet]

CSCtb90328

- 時間ベースの実行スケジュールを使用して PoE ポートで EnergyWise 電力制御を設定すると、夏時間を調整せずに時刻入力が実行されます。

回避策：新しい時刻設定を使用してすべてのエントリを手動で再入力します。

CSCsy27389

- 多数の ARP エントリ（47k）が存在する状態で、ARP テーブルをクリアすると、システムがリロードし、次のメッセージが表示されてスイッチがクラッシュします。

```
ROM by abort at PC 0x0
```

回避策：ありません。

必要に応じて、Cisco IOS リリース 12.2(50)SG3 にダウングレードします。

CSCta49512

- Cisco IOS リリース 12.2(46)SG を実行している Supervisor Engine 6-E または 6L-E で RSPAN を設定すると、モニタ対象トラフィックが宛先ポートに送信されるときに CPU 使用率が高くなります。

  回避策：RSPAN を無効にします。

  CSCsu81046

- Supervisor 6-E/6L-E で多数の ACL を設定し、統計情報を有効にすると、スイッチの CPU 使用率が高くなることがあります。

  デフォルトでは、特定のアプリケーション（IP ソースガードや QoS など）によって ACL 統計情報が有効になります。このような機能を設定すると、CPU 使用率が高くなります。

  CPU 使用率の高さは、show proc cpu コマンドで確認できます。また、show platform health コマンドの出力は、CPU 使用率が高いプロセスが「K5AclCamStatsMan hw」であることを示しています。

  この問題は、Cisco IOS リリース 12.2(40)SG 以降のリリースで発生する可能性があります。

  この問題は、Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 で解決されています。

  回避策：ACL、IPSG、および QoS 設定のサイズを小さくします。統計情報が ACL に対して明示的に有効になっている場合は、CLI で無効にします。

  ACL と IPSG が原因で CPU 使用率が高くなっている場合は、新しいソフトウェアにアップグレードします。

  QoS 設定が原因で CPU 使用率が高くなっている場合は、IOS イメージをアップグレードし、no qos statistics classification コマンドを入力します。

  CSCta54369

- スイッチが VTP バージョン 3 に移行した後に VTP プルーニングを有効にすると、トランクで VLAN プルーニングは行われません。

  回避策：VTP バージョンを 3 からバージョン 2 または 1 に変更してから、バージョン 3 に戻します。

  CSCsy66803

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行しているスイッチで、PVLAN コミュニティ VLAN が設定された 802.1X ポートが AAA サーバから新しい PVLAN 割り当てを受信する場合、このインターフェイスの設定をリセットすると、スイッチがリロードされることがあります。

  回避策：ありません。

  CSCsz38442

- vlan-port の状態が FlexLink ポートで変更されると、次の 2 つのメッセージがコンソールに表示されます。

  ```
  A syslog warning message "%SM-4-BADEVENT: Event 'forward' is invalid for the current
  state 'present': pm_vp .."

  A traceback error message
  ```

  この問題は、次の2 つのシナリオで FlexLink ポートでのみ発生します。

  - バックアップ インターフェイスのポートモードをトランクモードに変更する前に、FlexLink VLAN ロードバランシングを設定している。
  - FlexLink が per vlan-port error disable 状態から回復する。

  回避策：なし

syslog とトレースバック機能には影響しません。FlexLink の状態は正しい状態になり、トラフィック転送には影響しません。

CSCta05317

- Per vlan-port error disable 機能（dhcp-rate-limit および arp-inspection）は、FlexLink では機能しません（VLAN ロードバランシングなし）。アクティブリンクで違反が発生した場合、対応する vlan-port は error disabled になりません。

  既存の per-port error disable（違反が発生した場合、ポート全体が error disabled になる）は、引き続き FlexLink で機能します。

  回避策：VLAN ロードバランシングで FlexLink を使用します。

  VLAN ロードバランシングを使用しない場合は、アクティブインターフェイスで switchport backup interface perfer vlan コマンドを入力します。vlan z はシステム上の未使用の VLAN に設定されます。

  CSCta76320

- VLAN/SVI 上の多数のパケットがソフトウェアによって処理されると、スイッチの CPU 使用率が高い状態が長時間にわたって観察されることがあります。

  回避策：ありません。機能は影響を受けません。

  CSCsy32312

- Cisco IOS リリース 12.2(52)SG を実行しているスイッチが MPLS パケットを受信すると、SA ミスとホストラーニングにより CPU 使用率が高くなります。

  回避策：

  - mac address-table dynamic group protocols ip other コマンドを入力します。
  - スタティック MAC アドレスを設定します。

  CSCta09651

Cisco IOS リリース 12.2(53)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(53)SG の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet

	QueueID	以前の QueueName	新しい QueueName
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）
- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）
- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）
- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）
- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）
- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

（CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。

  – 該当ポートに SFP+ を挿入します。

  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  – Internet Explorer 8

  – Mozilla Firefox

  – Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- RADIUS サーバとクライアントを接続するポートが異なる VLAN に配置されている場合、ip radius source-interface コマンドを入力して 2 つの SSO スイッチオーバーを実行すると、認証されたセッションが失われます。

  回避策：クライアントを再認証します。

  CSCsx94066

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

  回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

  スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

  CSCsy70428

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan 3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- アクセスリストがハードウェアリソース極端に枯渇している状態でインターフェイスに接続されている場合、後でハードウェアリソースが使用可能になっても、ACL がハードウェアに自動的にロードされないことがあります。

  新しいアクセスリストに使用できる TCAM エントリはありません。

  回避策：スイッチ上の他の分類ポリシーを削除または短縮して、ハードウェア TCAM リソースを解放した後で、ACL を手動で削除して再適用します。

  CSCsy85006

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行しているスイッチで、PVLAN コミュニティ VLAN が設定された 802.1X ポートが AAA サーバから新しい PVLAN 割り当てを受信する場合、このインターフェイスの設定をリセットすると、スイッチがリロードされることがあります。

  回避策：ありません。

  CSCsz38442

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- 802.1X ポートをゲスト VLAN に対して有効にした後、RADIUS サーバに接続されているポートをシャットダウンして、サーバが停止し、EAPOL パケットがそのポートで送信されると、サーバは到達不能ですが、アクセス VLAN で許可されます。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCsz63355

- 時間ベースの実行スケジュールを使用して PoE ポートで EnergyWise 電力制御を設定すると、夏時間を調整せずに時刻入力が実行されます。

  回避策：新しい時刻設定を使用してすべてのエントリを手動で再入力します。

  CSCsy27389

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行している冗長 Catalyst 4500 シリーズスイッチでは、インターフェイスネイバーから FastEthernet1 インターフェイス（管理インターフェイス）への ping が SSO スイッチオーバーの直後に失敗することがあります。

  回避策：ネイバースイッチの ARP テーブルをクリアします。

  CSCsy86030

- 明示的なホストトラッキングが有効になっているスイッチが IGMPv3 を実行している場合、IGMPv3 レポートの送信を停止したポートは、タイムアウトするまで IGMPv3 テーブルに表示されます。

  回避策：影響を受ける VLAN で明示的なホストトラッキングを無効にします。

  CSCsz28612

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。

  音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- ホストがデータ VLAN で認証されると、VLAN の STP ステートがブロックされます。

  ポートで認証オープンを設定し、ホストがそのポートで認証されている場合、オープン認証（オープン認証なし）を設定解除すると、認証済みポートで STP ステートがブロックされます。

  接続されたホストは認証されるため、トラフィックを送信でき、STP ステートは転送になります。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCta04665

- Supervisor Engine II+ ～ V-10GE のレイヤ 2 ポート（つまり、スイッチポート）で、lauto qos voice trust コマンドを使用すると、他のパラメータに加えて、qos trust cos 設定が自動生成されます。ただし、no switchport コマンドを使用してポートをレイヤ 2 からレイヤ 3 に変換すると、qos trust dscp コマンドが生成されます。

  回避策：インターフェイスモードをレイヤ 2 からレイヤ 3 に変更する場合は、cos trust dscp コマンドを入力して、インターフェイスの信頼状態を手動で変更します。

  CSCta16492

- vlan-portの状態が Flex Link ポートで変更されると、次の2 つのメッセージがコンソールに表示されます。

```
A syslog warning message "%SM-4-BADEVENT: Event 'forward' is invalid for the current
state 'present': pm_vp .."

A traceback error message
```

この問題は、次の2 つのシナリオで Flex Link ポートでのみ発生します。

- バックアップ インターフェイスのポートモードをトランクモードに変更する前に、Flex Link VLAN ロードバランシングを設定します。
- Flex Link は、VLANポートごとのエラー無効状態から回復します。

回避策：なし

syslog とトレースバック機能には影響しません。Flex Link の状態は正しい状態になり、トラフィック転送には影響しません。

CSCta05317

- Per vlan-port error disable 機能（dhcp-rate-limit および arp-inspection）は、FlexLink では機能しません（VLAN ロードバランシングなし）。アクティブリンクで違反が発生した場合、対応する VLAN ポートはエラー無効になりません。

既存の per-port error disable（違反が発生した場合、ポート全体が error disabled にる）は、引き続き Flex Link で機能します。

回避策：VLAN ロードバランシングで Flex Link を使用します。

VLAN ロードバランシングを使用しない場合は、アクティブインターフェイスで switchport backup interface perfer vlan コマンドを入力します。vlan z はシステム上の未使用の VLAN に設定されます。

CSCta76320

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

この状況、次の条件が満たされた場合にのみ発生します。

- authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
- デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
- クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

回避策：ありません。

CSCsz63739

- EnergyWise が有効になっており、energywise level level recurrence importance importance at minute hour day_of_month month day_of_week 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、スイッチで繰り返しイベントを設定します。時刻が夏時間から標準時間に変更されると、スイッチで以下の状態が発生する可能性があります。
  - PoE デバイスに電力を供給するために再起動する
  - PoE デバイスの電源を間違った時刻にオンまたはオフにする
  - 障害発生

これは、次の年の時刻変更が現在の年の時刻変更後に発生した場合に発生します。

時刻変更が発生する前に、次の回避策のいずれかを使用します。

- EnergyWise 設定から定期的なイベントを削除し、1 週間は定期的なイベントを使用せず、時刻変更が発生してから 1 週間後に再設定します。
- energywise level level recurrence importance importance time-range time-range-name インターフェイス コンフィギュレーション コマンドを使用して、イベントを再スケジュールします。
- power inline auto 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、PoE ポートの電源をオンにします。

CSCtc91312

- Cisco IOS リリース 12.2(52)SG、12.2(52)XO、12.2(53)SG、または 12.2(53)SG1 にアップグレード後、フラッシュデバイス名がデフォルトの名前 flash: とは異なる場合、コンソールに継続的に次のメッセージが表示されることがあります。

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

回避策：フラッシュデバイスの名前をデフォルトの名前 flash: に変更します。

CSCte05909

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

- ip cef accounting non-recursive コマンドがすでに設定されている場合、BGP ルートのロード中にスイッチがクラッシュすることがあります。

回避策：ip cef accounting non-recursive コマンドを無効にします。

（CSCtn68186）

- broadcast キーワードを指定して AAA アカウンティングを使用すると、スイッチで予期しない動作が発生したり、クラッシュしたりすることがあります。

回避策：broadcast キーワードを指定して AAA アカウンティングを使用しないでください。
CSCts56125

- Cisco IOS ソフトウェアには、リモートのアプリケーションまたはデバイスが認証、許可、およびアカウンティング（AAA）許可を使用した場合に、許可レベルを超えることができる脆弱性が存在します。この脆弱性では、HTTP または HTTPS サーバが Cisco IOS デバイス上でイネーブルになっている必要があります。

Cisco IOS ソフトウェアを実行していない製品は脆弱性の影響を受けません。

シスコはこれらの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

HTTP サーバは、このアドバイザリに記載されている脆弱性に対する回避策として無効になっている可能性があります。

このアドバイザリは、次のリンク先で確認できます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

Cisco のセキュリティ脆弱性ポリシーに関する追加情報については、次の URL を参照してください。

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

CSCtr91106

- セッションが RADIUS サーバから DHCP 情報を受信する DHCP サーバとして動作しているスイッチでは、クラッシュや DHCP 関連のエラーが発生することがあります。

  回避策：ありません。CSCtj48387

- Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの Multicast Source Discovery Protocol（MSDP）の実装の脆弱性により、リモートの非認証攻撃者に対して影響を受けるデバイスのリロードを認めることがあります。この脆弱性を悪用しようとする試みが繰り返された結果、DoS 状態が発生する可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。このアドバイザリは、次のリンク先で確認できます。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  注 2012 年 3 月 28 日、Cisco IOS ソフトウェアのセキュリティアドバイザリにおいて、9 つの Cisco セキュリティアドバイザリを含むバンドル資料を公開しました。各アドバイザリには、アドバイザリに記載されている脆弱性を修正する Cisco IOS ソフトウェアリリース、および 2012 年 3 月にバンドルされているすべての脆弱性を修正する Cisco IOS ソフトウェアリリースが記載されています。

  個々の公開リンクは、次のリンクの Cisco Event Response: Semiannual Cisco IOS XE Software Security Advisory Bundled Publication [英語] を参照してください。

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  CSCtr28857

- 次のメッセージを表示した後、スイッチがクラッシュします。

  ```
  %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (Unknown
  MAC) on Interface Gi5/39 AuditSessionID AC156241000000670001BC9.
  ```

  次の条件が当てはまる場合：

  - スイッチポートは次のように設定されます。

    authentication event server dead action authorize...

    authenticaton event server alive action reinitalize

  - 以前に RADIUS サーバがダウンして、トラフィックのないポート（たとえば、デバイスが接続されていないハブ）が、関連付けられた MAC アドレスのないアクセス不能認証バイパス（IAB）VLAN に許可されました。

    RADIUS サーバが再び使用可能になると、IAB 許可ポートが別の状態に移行します。

  回避策：ありません。CSCtx61557

- トランクポートが VLAN 1 以外のネイティブ VLAN で設定されている場合、REP パケットはその VLAN で送信されません。

  回避策：トランクポートのネイティブ VLAN のデフォルト設定（VLAN 1）を保持します。CSCud05521

- TCAM リソースが最初に使い果たされてから解放されても、CPU の使用率は高いままです。

  回避策：すべてのインターフェイスで ACL を再設定します。CSCuf93866

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- Cisco IOS リリース 12.2(52)SG を実行しているスイッチが MPLS パケットを受信すると、SA ミスとホストラーニングにより CPU 使用率が高くなります。

  回避策：

  - mac address-table dynamic group protocols ip other コマンドを入力します。
  - スタティック MAC アドレスを設定します。

  CSCta09651

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策: トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策: flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策: スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- VLAN/SVI 上の多数のパケットがソフトウェアによって処理されると、スイッチの CPU 使用率が高い状態が長時間にわたって観察されることがあります。

回避策：ありません。機能は影響を受けません。

CSCsy32312

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- HSRP や OSPF などのプロトコルにサブセカンドタイマーを使用すると、ブートフラッシュへの書き込みによって CPU 使用率が高くなり、プロトコルのフラッピングが発生する可能性があります。

  回避策：大きなファイルをコピーするなど、IOS では長時間のブートフラッシュ操作はしないでください。

  CSCsw84727

Cisco IOS リリース 12.2(53)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(53)SG で解決済みの警告について説明します。

- プライマリおよびセカンダリプライベート VLAN を伝送する通常のトランクでポートセキュリティが設定されている場合、その設定は次の状況で実行コンフィギュレーションから削除できます。

  セカンダリ VLAN を削除した後、ポートで shut、no shut の順に入力します。

  回避策：

  - VLAN の削除後に shut、no shut を入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
  - MAC アドレスをエージアウトするポートセキュリティ エージング タイムを設定してから、shut、no shut の順に入力します。その後、スイッチのリロード後にのみ、ポートのポートセキュリティを再設定できます。

  CSCsz73895

- port-security vp err disable を設定した後、ポートで shut、no shut の順に入力すると、違反が発生します。

  回避策：

  - ポートを回復するには、shut、no shut と入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
  - shut、no shut ではなく、clear errdisable interface vlan と入力します。

  - MAC アドレスをエージアウトするポートセキュリティ エージング タイムを設定してから、shut、no shut の順に入力します。スイッチをリロードしてから、ポートセキュリティを再設定します。

CSCsy80415

- Cisco IOS ソフトウェアには、攻撃者がリモートから巧妙に細工された暗号化パケットを送信して Cisco IOS デバイスをリロードさせる可能性がある脆弱性が存在します。シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

- CSCsq24002
- 影響を受けるバージョンの Cisco IOS ソフトウェアを実行しているシスコデバイスは、IP トンネルおよび Cisco Express Forwarding 用に設定されている場合、サービス妨害（DoS）攻撃に対して脆弱です。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  CSCsx70889

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

Cisco IOS リリース 12.2(52)XO の未解決の警告

ここでは、Cisco IOS リリース 12.2(52)XO の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1
```

```
Service-policy output: p1

  Class-map: c1 (match-all)
    0 packets<--------It stays at '0' despite of traffic being received
    Match: access-group name fnacl21
    police: Per-interface
      Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは Informational（情報提供）メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）
- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。
  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）
- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）
- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。
  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）
- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）
- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。
  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）
- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。
  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。

c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

（CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。

  – 該当ポートに SFP+ を挿入します。

  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  – Internet Explorer 8

  – Mozilla Firefox

  – Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策：ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策：ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策：ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策：ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策：ありません。

  CSCsx64308

- RADIUS サーバとクライアントを接続するポートが異なる VLAN に配置されている場合、ip radius source-interface コマンドを入力して 2 つの SSO スイッチオーバーを実行すると、認証されたセッションが失われます。

  回避策：クライアントを再認証します。

  CSCsx94066

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

  ```
  ethernet oam link-monitor frame-seconds window
  ethernet oam link-monitor frame-seconds threshold low
  ```

  回避策：フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

  CSCsy37181

- スイッチが VTP バージョン 3 に移行した後に VTP プルーニングを有効にすると、トランクで VLAN プルーニングは行われません。

  回避策：VTP バージョンを 3 からバージョン 2 または 1 に変更してから、バージョン 3 に戻します。

  CSCsy66803

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

  回避策：アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

  スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

  CSCsy70428

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

  回避策：diagnostic コマンドを入力するときにプロファイル名を指定します。

  無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

  CSCsz05888

- アクセスリストがハードウェアリソース極端に枯渇している状態でインターフェイスに接続されている場合、後でハードウェアリソースが使用可能になっても、ACL がハードウェアに自動的にロードされないことがあります。

  新しいアクセスリストに使用できる TCAM エントリはありません。

  回避策：スイッチ上の他の分類ポリシーを削除または短縮して、ハードウェア TCAM リソースを解放した後で、ACL を手動で削除して再適用します。

  CSCsy85006

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

  回避策：ありません。

  キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

  CSCsz20149

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行しているスイッチで、PVLAN コミュニティ VLAN が設定された 802.1X ポートが AAA サーバから新しい PVLAN 割り当てを受信する場合、このインターフェイスの設定をリセットすると、スイッチがリロードされることがあります。

  回避策：ありません。

  CSCsz38442

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- 802.1X ポートをゲスト VLAN に対して有効にした後、RADIUS サーバに接続されているポートをシャットダウンして、サーバが停止し、EAPOL パケットがそのポートで送信されると、サーバは到達不能ですが、アクセス VLAN で許可されます。

  回避策：ポート で shut と入力してから、no shut を入力します。

  CSCsz63355

- 時間ベースの実行スケジュールを使用して PoE ポートで EnergyWise 電力制御を設定すると、夏時間を調整せずに時刻入力が実行されます。

  回避策：新しい時刻設定を使用してすべてのエントリを手動で再入力します。

  CSCsy27389

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行している冗長 Catalyst 4500 シリーズスイッチでは、インターフェイスネイバーから FastEthernet1 インターフェイス（管理インターフェイス）への ping が SSO スイッチオーバーの直後に失敗することがあります。

  回避策：ネイバースイッチの ARP テーブルをクリアします。

  CSCsy86030

- 明示的なホストトラッキングが有効になっているスイッチが IGMPv3 を実行している場合、IGMPv3 レポートの送信を停止したポートは、タイムアウトするまで IGMPv3 テーブルに表示されます。この動作は、Cisco IOS リリース 12.2(50)SG では発生していませんでした。

  回避策：影響を受ける VLAN で明示的なホストトラッキングを無効にします。

  CSCsz28612

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。具体的には、音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- プライマリおよびセカンダリプライベート VLAN を伝送する通常のトランクでポートセキュリティが設定されている場合、その設定は次の状況で running-config から消去できます。

  セカンダリ VLAN を削除した後、ポートで shut/no shut と入力します。（CSCsz73895）

  回避策：

  - VLAN の削除後に shut/no shut を入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
  - MAC アドレスをエージアウトするポートセキュリティ エージング タイムを設定してから、shut/no shut と入力します。その後、スイッチのリロード後にのみ、ポートのポートセキュリティを再設定できます。

  CSCsz73895

port-security vp err disable を設定した後、ポートで shut/no shut と入力すると、違反が発生します。(CSCsz80415)

回避策:

- ポートを回復するには、shut/no shut と入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
- shut/no shut と入力する代わりに、clear errdisable interface name vlan [range] を設定します。
- MAC アドレスをエージアウトするポートセキュリティ エージングタイムを設定してから、shut、no shut の順に入力します。次に、スイッチのリロード後にポートのポートセキュリティを再設定します。

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL(IP アクセスリスト)が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策: ありません。

  CSCsz63739

- EnergyWise が有効になっており、energywise level level recurrence importance importance at minute hour day_of_month month day_of_week 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、スイッチで繰り返しイベントを設定します。時刻が夏時間から標準時間に変更されると、スイッチで以下の状態が発生する可能性があります。
  - PoE デバイスに電力を供給するために再起動する
  - PoE デバイスの電源を間違った時刻にオンまたはオフにする
  - 障害発生

  これは、次の年の時刻変更が現在の年の時刻変更後に発生した場合に発生します。

  時刻変更が発生する前に、次の回避策のいずれかを使用します。

  - EnergyWise 設定から定期的なイベントを削除し、1 週間は定期的なイベントを使用せず、時刻変更が発生してから 1 週間後に再設定します。
  - energywise level level recurrence importance importance time-range time-range-name インターフェイス コンフィギュレーション コマンドを使用して、イベントを再スケジュールします。
  - power inline auto 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、PoE ポートの電源をオンにします。

  CSCtc91312

- Cisco IOS リリース 12.2(52)SG、12.2(52)XO、12.2(53)SG、または 12.2(53)SG1 にアップグレード後、フラッシュデバイス名がデフォルトの名前 flash: とは異なる場合、コンソールに継続的に次のメッセージが表示されることがあります。

  ```
  %Error copying flash:/eem_pnt_2 (Invalid path)
  ```

  回避策: フラッシュデバイスの名前をデフォルトの名前 flash: に変更します。

  CSCte05909

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

- ルートブリッジとして機能する SSW（Catalyst 3750 シリーズ スイッチ）に接続された ASW（Catalyst 4500 シリーズ スイッチ）に NEAT を設定し、ASW と SSW 間に冗長リンクを設定すると、次のようになります。
  - STP が安定しない。
  - SVI（ネットワーク）に到達できない。設定の STP フラップおよび CISP の動作が原因で ASW に SVI が存在する場合、ASW の SVI MAC 設定が正しくありません。

  回避策：すべての VLAN のルートブリッジとして ASW またはその他のスイッチアップストリームを設定します。CSCtg71030

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- Cisco IOS リリース 12.2(52)SG を実行しているスイッチが MPLS パケットを受信すると、SA ミスとホストラーニングにより CPU 使用率が高くなります。

  回避策：
  - mac address-table dynamic group protocols ip other コマンドを入力します。
  - スタティック MAC アドレスを設定します。

  CSCta09651

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- HSRP や OSPF などのプロトコルにサブセカンドタイマーを使用すると、ブートフラッシュへの書き込みによって CPU 使用率が高くなり、プロトコルのフラッピングが発生する可能性があります。

  回避策：大きなファイルをコピーするなど、IOS では長時間のブートフラッシュ操作はしないでください。

  CSCsw84727

Cisco IOS リリース 12.2(52)XO の解決済みの警告

ここでは、Cisco IOS リリース 12.2(52)XO で解決済みの警告について説明します。

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行している Supervisor Engine WS-X45-SUP6-E を備えたスイッチで、トラフィックが 802.1Q トランクポートおよび非ネイティブ VLAN で送信される場合、DSCP 46 でローカルに生成されたトラフィックが送信される前に DSCP 0 に再マーキングされます。

  この動作は、スイッチを通過するトラフィックでは発生しません。

  回避策：ありません。

  CSCsu01848

- 通常の操作時には、ログに次のメッセージが表示されます。

  ```
  001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
  001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
  ```

  回避策：なし

  CSCsv17545

- コントロール プレーン ポリシングでは、コントロールプレーンクラス（ macro global apply system-cpp コマンドで自動生成されるクラスで、定義済み ACL を使用してトラフィックを照合）により、それぞれのパケットとバイトカウントの両方が増加します。したがって、両方のカウンタはゼロ以外です。

  対照的に、データプレーンクラス（ユーザ作成の ACL によって手動で設定されるクラス）では、バイトカウンタは期待どおりに増加しますが、パケットカウントは 0 のままです。

  回避策：ありません。

  CSCsw16557

- Catalyst 4500 では、隔離されたプライベート VLAN トランクインターフェイスがフラップすると、ポート単位の VLAN 単位の入力および出力ポリシーはポートに適用されなくなります。

  影響を受ける Cisco IOS リリースは、12.2(31)SGA08、12.2(37)SG、12.2(40)SG、12.2(44)SG、12.2(46)SG、12.2(50)SG、および 12.2(50)SG1 です。

  回避策：

  従来のシリーズの Supervisor Engine の場合は、ポートで QoS を無効にして設定します。

  たとえば、Gig 2/1 を独立プライベート VLAN トランクポートとして設定するには、次の手順を実行します。

  ```
  Switch# conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  Switch(config)# interface gigabitEthernet 2/1
  Switch(config-if)# no qos
  Switch(config-if)# qos
  Switch(config-if)# end
  Switch#
  ```

次の EEM スクリプトを設定して、この回避策を自動化できます。QoS は、ポートがフラップするたびに無効になり、再度有効になります。

```
logging event link-status global

event manager applet linkup-reqos
 event syslog pattern "changed state to up"
 action 1 cli command "enable"
 action 2 cli command "conf t"
 action 3 cli command "interface gigabitEthernet 2/1"
 action 4 cli command "no qos"
 action 5 cli command "qos"
```

Supervisor Engine 6-E または Catalyst 4900M スイッチで、影響を受ける VLAN の QoS サービスポリシーを削除して再適用します。

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# vlan-range 10
Switch(config-if-vlan-range)# no service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# no service policy input secVlanInPolicy
Switch(config-if-vlan-range)# service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# service policy input secVlanInPolicy
Switch(config-if-vlan-range)# end
Switch#
```

CSCsw19087

- 次のコマンドを入力すると、スタンバイ スーパバイザ エンジンがクラッシュします。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

この問題は、冗長 Catalyst 4500 シリーズ スイッチで Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行していて、次のスーパバイザエンジンのいずれかを使用している場合に発生します。II Plus、II Plus+10GE、IV、V、または V-10GE。

回避策：各インターフェイスを個別に設定します。

上記の tx-queue 設定コンテキストを終了するには、exit または end コマンドを明示的に入力します。exit コマンドの短縮形（ex）は機能しません。多くのコマンドをコピーして貼り付けるのではなく、exit コマンドと end コマンドを 1 行ずつ入力します。

CSCsx44995

- 1000BASE-SX の自動ネゴシエーションを有効にすると、Intel 1000Base ファイバ NIC をリロードまたは再接続した後に、一部のポートが正しく起動しない場合があります。

  次のラインカードが影響を受けます。

  - WS-X4302-GB
  - WS-X4306-GB
  - WS-X4418-GB
  - WS-X4448-GB-SFP
  - WS-X4506-GB-T

SFP、HAMM モジュールを使用する TenGigabit ポート、および WS-C4948 SFP アップリンクを備えた E シリーズ ラインカードでは、この問題は発生しません。

回避策：次のいずれかの操作を実行します。

- shut、no shut コマンドの順に入力します。
- ケーブルを再接続します。

CSCsx74970

- 単一の SSH ウィンドウ（セッション）で cbQoSPoliceStatsTable および cbQoSREDClassStatsTable に対して SNMP（getmany）クエリを実行すると、CPU 使用率が 99% に達します。18の SSH セッションから cbQoSPoliceStatsTable および cbQoSREDClassStatsTable をクエリすると、CPU-HOG エラーメッセージが表示されます。

  回避策：クエリを停止するしかありません。

  CSCsw89720

- 1 つ以上のポートがシングルホストモード、MAB、および authentication control-direction in に設定された Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているスーパバイザエンジンでは、ポートがシングルホストモード用に設定されていて、unidirectional control in コマンドを入力した場合、ホストは MAB によって認証されません（Wake-on-LAN）。

  回避策：authentication control-direction in コマンドを無効にします。

  authentication control-direction in が必要な場合は、マルチ認証またはマルチドメイン認証（MDA）用にポートを設定します。

  CSCsx98360

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行している冗長スイッチで、802.1X VVID およびポートセキュリティがポートに設定されている場合、802.1X 非対応の Cisco IP 電話からの CDP MAC は、スタンバイ スーパバイザ エンジンのポートセキュリティテーブルに追加されない場合があります。

  回避策：ありません。

  この問題は、Cisco IOS リリース 12.2(50)SG2 および 12.2(52)SG で修正されています。

  CSCsw29489

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行しているスイッチで、802.1X VVID とポートセキュリティがポートに設定されている場合、LLDP 機能を備えた 802.1X 非対応の Cisco IP 電話とその背後にある PC を挿入すると、セキュリティ違反が発生することがあります。

  回避策：CallManager から LLDP（スイッチ上）と電話機をオフにします。

  この問題は、12.2(50)SG2 および 12.2(52)SG で修正されています。

  CSCsy21167

- CPU のキャッシュ内のパリティエラーにより、IOS がクラッシュし、次のようなクラッシュダンプファイルが表示されます。

```
Switch# show platform crashdump

VECTOR 0

*** CRASH DUMP ***
02/09/2009 10:10:30
Last crash: 02/09/2009 10:10:30

Build: 12.2(20090206:234053) IPBASE
buildversion addr: 13115584
```

```
MCSR: 40000000 <--- non-zero value!
.
```

重要なデータは「VECTOR 0」であり、MCSR 値は 40000000、20000000、または 10000000 です。

回避策：show platform cpu cache コマンドを入力して IOS アルゴリズムを起動し、CPU のキャッシュ内のパリティエラーを検出して回復します。実行中のシステムで正常に検出され、修正された CPU キャッシュのパリティエラー数の実行カウントを取得します。

```
Switch# show platform cpu cache
L1 Instruction Cache: ENABLED
L1 Data Cache: ENABLED
L2 Cache: ENABLED
Machine Check Interrupts: 5
L1 Instruction Cache Parity Errors: 3
L1 Instruction Cache Parity Errors (CPU30): 1
L1 Data Cache Parity Errors: 1
```

CSCsx15372

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 署名を、そのイメージの CCO にポストされた署名と比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  （CSCsu37068）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策：ありません。

  （CSCsw32519）

- channel-group x または channel-protocol モードで、fa1 管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。

  （CSCsv91302）

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行している従来のシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。

  CSCsy29140

- Cisco IOS リリース 12.2(46)SG および 12.2(50)SGA を、Supervisor Engines II+、II+10GE、IV、V、または V-10GE を搭載した Catalyst 4500 シリーズ スイッチで実行している場合、次のコマンドを入力するとスタンバイ スーパバイザ エンジンで障害が発生します。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

  回避策：すべてのインターフェイスを個別に設定します。

  スタンバイ スーパバイザ エンジンのリブートを回避するには、インターフェイス範囲で作業しているときに、exit または end コマンドを明示的に実行して tx-queue コンフィギュレーション コンテキストを終了します。exit コマンドの短縮形 ex は機能しません。これらのコマンドは、1 行ずつ入力する必要があります。コピー/ペーストは機能しません。

  CSCsx44995

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、12.2(40)SG で初めて確認されました。

回避策：AutoQoS によって生成された設定を手動で適用します。AutoQoS は使用しないでください。CSCsv03316

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの QoS ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- 通常、ログには次のメッセージが頻繁に表示されますが、パフォーマンスへの影響はありません。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

  回避策：ありません。（CSCsv17545）

- スーパバイザに障害が発生すると、exception crashinfo ファイルが作成されますが、スイッチを RPR モードで設定すると、そのようなコピーが有効になっていても、ブートフラッシュや slot0 にはコピーされません。手動でコピーまたは検査することもできます。

  exception crashinfo ファイル機能は、RPR モードではサポートされていません。

  回避策：ありません。（CSCsr66481）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- 12.2(50)SG または 12.2(50)SG1 を実行している Catalyst 4500 スイッチで、スイッチポートで 802.1X VVID とポートセキュリティが同時に設定されている場合、802.1x 非対応の Cisco IP 電話を背後の PC とともに挿入すると、セキュリティ違反が発生することがあります。

  回避策：ありません。CSCsv63638

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。

- AAA サーバ が CiscoSecure ACS 2.4 を実行している。
- callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

回避策:ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。(CSCei62358)

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策:インターフェイスをシャットダウンしてから再度開きます。(CSCsr58573)

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、12.2(40)SG で初めて確認されました。

  回避策:AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

- 通常、ログには次のメッセージが頻繁に表示されますが、パフォーマンスへの影響はありません。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

  回避策:ありません。(CSCsv17545)

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策:ありません。

  (CSCsv91302)

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策:ありません。

  (CSCsw32519)

- 次のコマンドを入力すると、スタンバイ スーパバイザ エンジンがクラッシュします。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

この問題は、冗長 Catalyst 4500 シリーズ スイッチで Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行していて、次のスーパバイザエンジンのいずれかを使用している場合に発生します。II Plus、II Plus+10GE、IV、V、または V-10GE。

回避策: 各インターフェイスを個別に設定します。

上記の tx-queue 設定コンテキストを終了するには、exit または end コマンドを明示的に入力します。exit コマンドの短縮形（ex）は機能しません。多くのコマンドをコピーして貼り付けるのではなく、exit コマンドと end コマンドを 1 行ずつ入力します。

CSCsx44995

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。

  CSCsy29140

- Cisco IOS ソフトウェアには、攻撃者がリモートから巧妙に細工された暗号化パケットを送信して Cisco IOS デバイスをリロードさせる可能性がある脆弱性が存在します。シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

- CSCsq24002

Cisco IOS リリース 12.2(52)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(52)SG の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet

	QueueID	以前の QueueName	新しい QueueName
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

（CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

回避策：Shut down, and then reopen the interface.

（CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。

- IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
- PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

（CSCsu39009）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。
  – 該当ポートに SFP+ を挿入します。
  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  – Internet Explorer 8
  – Mozilla Firefox
  – Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策: ありません。CSCsy72343

- MDA を使用する .1X がホストモードに設定され、ゲスト VLAN が有効になっている場合、トラフィックジェネレータからのトラフィックを高速で送信すると、誤ってセキュリティ違反のフラグが付きます。

  回避策: ありません。

  CSCsy38640

- 隣接関係に対して show adjacency x.x.x.x internal コマンドを入力すると、パケットカウンタは正しく増加しますが、バイトカウンタは 0 のままです。

  回避策: ありません。

  CSCsu35604

- 2 つのスイッチを接続する REP セグメント内のリンクで障害が発生すると、3 回の試行のうち 1 回でコンバージェンスタイミングが 300ms を超えます。

  回避策: ありません。

  CSCsw42967

- 各ノードで VLAN が設定されている 16 ノードの閉じた REP セグメントでリンクに障害が発生すると、特にマルチキャストトラフィックでコンバージェンス時間が 250ms を超えます。

  回避策: ありません。

  これは REP 機能には影響しませんが、復元のタイミングには影響します。REP セグメントに障害が発生すると、トラフィックの復元時間が 200ms を超えることがあります。

  CSCsx55704

- Cisco IOS リリース 12.2(52)SG を実行している冗長スイッチでは、802.1X を介してポートが許可された後、show dot1x interface statistics コマンドを実行すると、スタンバイ スーパバイザエンジンで空の値が表示されることがあります。

  統計情報は、アクティブなスーパバイザで正しく表示されます。

  回避策: ありません。

  CSCsx64308

- RADIUS サーバとクライアントを接続するポートが異なる VLAN に配置されている場合、ip radius source-interface コマンドを入力して 2 つの SSO スイッチオーバーを実行すると、認証されたセッションが失われます。

  回避策: クライアントを再認証します。

  CSCsx94066

- フレームエラー秒数の OAM モニタリングが設定された WS-C4900M シャーシで複数のストリームの CRC エラーが発生した場合、次の CLI を設定すると、OAM はエラーフレーム秒数の値を正しく報告しません。

```
ethernet oam link-monitor frame-seconds window
ethernet oam link-monitor frame-seconds threshold low
```

回避策: フレームエラーが予想されるフレームエラー秒数に分割されるように、下限しきい値に低い値を設定します。

CSCsy37181

- スイッチが VTP バージョン 3 に移行した後に VTP プルーニングを有効にすると、トランクで VLAN プルーニングは行われません。

回避策: VTP バージョンを 3 からバージョン 2 または 1 に変更してから、バージョン 3 に戻します。

CSCsy66803

- スタンバイスーパバイザ WS-X45-SUP6-E 上の 10Gig アップリンクは、アクティブ スーパバイザ エンジンの OIR を介して古いスタンバイエンジンがアクティブになった後（OIR が 5 秒以内に完了した場合）、トラフィックの送受信を停止します。

回避策: アクティブおよびスタンバイ スーパバイザ エンジンをリロードします。

スーパバイザエンジンの OIR を実行している間は、エンジンを完全に取り外してから再挿入する必要があります。

CSCsy70428

- プロファイル名を指定せずにオンデマンドの Call Home メッセージ送信を要求し、指定されたモジュールから不明な診断結果が返される場合、次のエラーメッセージが表示されます。

```
Switch# call-home send alert-group diagnostic module 2
Sending diagnostic info call-home message ...
Please wait. This may take some time ...
Switch#
*Jan  3 01:54:24.471: %CALL_HOME-3-ONDEMAND_MESSAGE_FAILED: call-home on-demand
message failed to send (ERR 18, The alert group is not subscribed)
```

回避策: diagnostic コマンドを入力するときにプロファイル名を指定します。

無効なモジュールのオンデマンド送信を要求しないようにすることができます。まず、show module コマンドを入力して、有効なモジュールまたは存在するモジュールを確認します。

CSCsz05888

- アクセスリストがハードウェアリソース極端に枯渇している状態でインターフェイスに接続されている場合、後でハードウェアリソースが使用可能になっても、ACL がハードウェアに自動的にロードされないことがあります。

新しいアクセスリストに使用できる TCAM エントリはありません。

回避策: スイッチ上の他の分類ポリシーを削除または短縮して、ハードウェア TCAM リソースを解放した後で、ACL を手動で削除して再適用します。

CSCsy85006

- サービスポリシーを出力方向のポートに適用すると同時に、出力方向のポートの VLAN 範囲にサービスポリシーを適用すると、**show policy-map interface** コマンドの出力内のクラスマップのヒットカウンタが誤った値を示します。

回避策: ありません。

キュー送信カウンタとポリシング統計情報（存在する場合）は正確です。

CSCsz20149

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行しているスイッチで、PVLAN コミュニティ VLAN が設定された 802.1X ポートが AAA サーバから新しい PVLAN 割り当てを受信する場合、このインターフェイスの設定をリセットすると、スイッチがリロードされることがあります。

  回避策：ありません。

  CSCsz38442

- フラグメントとして、またはゼロ以外のフラグメント オフセット フィールドを持つスイッチに入るパケットは、PBR の対象になりません。

  回避策：ありません。

  CSCsz06719（現時点では、4500 + 4900）

- 1X ポートをゲスト VLAN に対して有効にした後、RADIUS サーバに接続されているポートをシャットダウンして、サーバが停止し、EAPOL パケットがそのポートで送信されると、サーバは到達不能ですが、アクセス VLAN で許可されます。

  回避策：ポート で **shut** と入力してから、**no shut** を入力します。

  CSCsz63355

- 時間ベースの実行スケジュールを使用して PoE ポートで EnergyWise 電力制御を設定すると、夏時間を調整せずに時刻入力が実行されます。

  回避策：新しい時刻設定を使用してすべてのエントリを手動で再入力します。

  CSCsy27389

- Cisco IOS リリース 12.2(50)SG または 12.2(52)SG を実行している冗長 Catalyst 4500 シリーズスイッチでは、インターフェイスネイバーから FastEthernet1 インターフェイス（管理インターフェイス）への ping が SSO スイッチオーバーの直後に失敗することがあります。

  回避策：ネイバースイッチの ARP テーブルをクリアします。

  CSCsy86030

- 明示的なホストトラッキングが有効になっているスイッチが IGMPv3 を実行している場合、IGMPv3 レポートの送信を停止したポートは、タイムアウトするまで IGMPv3 テーブルに表示されます。この動作は、Cisco IOS リリース 12.2(50)SG では発生していませんでした。

  回避策：影響を受ける VLAN で明示的なホストトラッキングを無効にします。

  CSCsz28612

- Wireless Control System（WCS）で、lldp-med 対応電話機の背後にある PC の一部のデバイス情報が誤って表示されます。具体的には、WCS は PC のデバイス情報に電話機のシリアル番号、モデル番号、およびソフトウェアバージョンを表示します。PC に関するその他の情報はすべて、WCS 上に正しく表示されます。

  これは、スイッチが Network Mobility Service Protocol（NMSP）を実行している場合にのみ発生します。電話機で CDP が有効になっている場合は発生しません。

  回避策：VLAN ID または名前を使用して、IP フォンと WCS 上の電話の背後にある PC を区別します。具体的には、音声 VLAN で IP フォンが検出され、シリアル番号、モデル番号、およびソフトウェアバージョンの情報が正しく表示されます。ただし、電話の背後にある PC がデータ VLAN で検出され、表示されたデバイス情報が誤っているため、無視する必要があります。

  CSCsz34522

- プライマリおよびセカンダリプライベート VLAN を伝送する通常のトランクでポートセキュリティが設定されている場合、その設定は次の状況で running-config から消去できます。

  セカンダリ VLAN を削除した後、ポートで shut、no shut の順に入力します。(CSCsz73895)

  回避策:

  - VLAN の削除後に shut、no shut を入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
  - MAC アドレスをエージアウトするポートセキュリティ エージングタイムを設定してから、shut、no shut の順に入力します。その後、スイッチのリロード後にのみ、ポートのポートセキュリティを再設定できます。

  port-security vp err disable を設定した後、ポートで shut/no shut to入力すると、違反が発生します。(CSCsz80415)

  回避策:

  - ポートを回復するには、shut/no shut と入力する代わりに、ポートセキュリティ違反のエラー回復を設定します。
  - shut/no shut と入力する代わりに、clear errdisable interface name vlan [range] を設定します。
  - MAC アドレスをエージアウトするポートセキュリティ エージングタイムを設定してから、shut、no shut の順に入力します。次に、スイッチのリロード後にポートのポートセキュリティを再設定します。

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL(IP アクセスリスト)が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策: ありません。

  CSCsz63739

- EnergyWise が有効になっており、energywise level level recurrence importance importance at minute hour day_of_month month day_of_week 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、スイッチで繰り返しイベントを設定します。時刻が夏時間から標準時間に変更されると、スイッチで以下の状態が発生する可能性があります。

  - PoE デバイスに電力を供給するために再起動する
  - PoE デバイスの電源を間違った時刻にオンまたはオフにする
  - 障害発生

  これは、次の年の時刻変更が現在の年の時刻変更後に発生した場合に発生します。

  時刻変更が発生する前に、次の回避策のいずれかを使用します。

  - EnergyWise 設定から定期的なイベントを削除し、1 週間は定期的なイベントを使用せず、時刻変更が発生してから 1 週間後に再設定します。
  - energywise level level recurrence importance importance time-range time-range-name インターフェイス コンフィギュレーション コマンドを使用して、イベントを再スケジュールします。

– power inline auto 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、PoE ポートの電源をオンにします。

CSCtc91312

- Cisco IOS リリース 12.2(52)SG、12.2(52)XO、12.2(53)SG、または 12.2(53)SG1 にアップグレード後、フラッシュデバイス名がデフォルトの名前 flash: とは異なる場合、コンソールに継続的に次のメッセージが表示されることがあります。

```
%Error copying flash:/eem_pnt_2 (Invalid path)
```

回避策：フラッシュデバイスの名前をデフォルトの名前 flash: に変更します。

CSCte05909

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

回避策：ありません。（CSCso68331）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine 6-E で vlan dot1q tag native をグローバルに設定すると、MST 制御パケットはネイティブ VLAN の出力でタグ付けされます。これは 802.1s と矛盾します。Cisco 7600 シリーズ ルータは、MST プロポーザルアグリーメントをドロップします（ネイティブ VLAN MST 制御パケットがタグ付けされていないことを想定しているため）。これにより、スパニングツリーの収束中に 30 秒間のトラフィック損失が発生します。

  回避策：スイッチのトランクポートでネイティブ VLAN タギングを **no switchport trunk native vlan tag** コマンドを入力して無効にします。

  CSCsz12611

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- HSRP や OSPF などのプロトコルにサブセカンドタイマーを使用すると、ブートフラッシュへの書き込みによって CPU 使用率が高くなり、プロトコルのフラッピングが発生する可能性があります。

  回避策：大きなファイルをコピーするなど、IOS では長時間のブートフラッシュ操作はしないでください。

  CSCsw84727

Cisco IOS リリース 12.2(52)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(52)SG で解決済みの警告について説明します。

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行している Supervisor Engine WS-X45-SUP6-E を備えたスイッチで、トラフィックが 802.1Q トランクポートおよび非ネイティブ VLAN で送信される場合、DSCP 46 でローカルに生成されたトラフィックが送信される前に DSCP 0 に再マーキングされます。

  この動作は、スイッチを通過するトラフィックでは発生しません。

  回避策：ありません。

  CSCsu01848

- 通常の操作時には、ログに次のメッセージが表示されます。

  ```
  001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
  001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
  ```

  回避策：なし

  CSCsv17545

- コントロール プレーン ポリシングでは、コントロールプレーンクラス macro global apply system-cpp コマンドで自動生成されるクラスで、定義済み ACL を使用してトラフィックを照合）により、それぞれのパケット数とバイト数の両方が増えます。したがって、両方のカウンタはゼロ以外です。

  対照的に、データプレーンクラス（ユーザ作成の ACL によって手動で設定されるクラス）では、バイトカウンタは期待どおりに増加しますが、パケットカウントは 0 のままです。

  回避策：ありません。

  CSCsw16557

- Catalyst 4500 シリーズ スイッチでは、隔離されたプライベートVLANトランクインターフェイスがフラップすると、ポート単位のVLAN単位の入力ポリサーはポートに適用されなくなります。

  影響を受ける Cisco IOS リリースは、12.2(31)SGA08、12.2(37)SG、12.2(40)SG、12.2(44)SG、12.2(46)SG、12.2(50)SG、および 12.2(50)SG1 です。

  回避策：

  クラシックシリーズの Supervisor Engine の場合は、ポートで QoS を無効にして設定します。

  たとえば、Gig 2/1 を独立プライベート VLAN トランクポートとして設定するには、次の手順を実行します。

  ```
  Switch# conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  Switch(config)# interface gigabitEthernet 2/1
  Switch(config-if)# no qos
  Switch(config-if)# qos
  Switch(config-if)# end
  Switch#
  ```

次の EEM スクリプトを設定して、この回避策を自動化できます。QoS は、ポートがフラップするたびに無効になり、再度有効になります。

```
logging event link-status global

event manager applet linkup-reqos
 event syslog pattern "changed state to up"
 action 1 cli command "enable"
 action 2 cli command "conf t"
 action 3 cli command "interface gigabitEthernet 2/1"
 action 4 cli command "no qos"
 action 5 cli command "qos"
```

Supervisor Engine 6-E または Catalyst 4900M スイッチで、影響を受ける VLAN の QoS サービスポリシーを削除して再適用します。

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# vlan-range 10
Switch(config-if-vlan-range)# no service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# no service policy input secVlanInPolicy
Switch(config-if-vlan-range)# service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# service policy input secVlanInPolicy
Switch(config-if-vlan-range)# end
Switch#
```

CSCsw19087

- 次のコマンドを入力すると、スタンバイ スーパバイザ エンジンがクラッシュします。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

この問題は、冗長 Catalyst 4500 シリーズ スイッチで Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行していて、次のスーパバイザエンジンのいずれかを使用している場合に発生します。II Plus、II Plus+10GE、IV、V、または V-10GE。

回避策:各インターフェイスを個別に設定します。

上記の tx-queue 設定コンテキストを終了するには、exit または end コマンドを明示的に入力します。exit コマンドの短縮形(ex)は機能しません。多くのコマンドをコピーして貼り付けるのではなく、exit コマンドと end コマンドを 1 行ずつ入力します。

CSCsx44995

- 1000BASE-SX の自動ネゴシエーションを有効にすると、Intel 1000Base ファイバ NIC をリロードまたは再接続した後に、一部のポートが正しく起動しない場合があります。

  次のラインカードが影響を受けます。

  - WS-X4302-GB
  - WS-X4306-GB
  - WS-X4418-GB
  - WS-X4448-GB-SFP
  - WS-X4506-GB-T

SFP、HAMM モジュールを使用する TenGigabit ポート、および WS-C4948 SFP アップリンクを備えた E シリーズ ラインカードでは、この問題は発生しません。

回避策：次のいずれかの操作を実行します。

- shut、no shut コマンドの順に入力します。
- ケーブルを再接続します。

CSCsx74970

- 単一の SSH ウィンドウ（セッション）で cbQosPoliceStatsTable および cbQosREDClassStatsTable に対して SNMP（getmany）クエリを実行すると、CPU 使用率が 99% に達します。18の SSH セッションから cbQosPoliceStatsTable および cbQosREDClassStatsTable をクエリすると、CPU-HOG エラーメッセージが表示されます。

  回避策：クエリの停止しかありません。

  CSCsw89720

- 1 つ以上のポートがシングルホストモード、MAB、および認証制御方向に設定された Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているスーパバイザエンジンでは、ポートがシングルホストモード用に設定されていて、unidirectional control in コマンドを入力した場合、ホストは MAB によって認証されません（Wake-on-LAN）。

  回避策：authentication control-direction in コマンドを無効にします。

  authentication control-direction in が必要な場合は、マルチ認証またはマルチドメイン認証（MDA）用にポートを設定します。

  CSCsx98360

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行している冗長スイッチで、802.1X VVID およびポートセキュリティがポートに設定されている場合、802.1X 非対応の Cisco IP 電話からの CDP MAC は、スタンバイ スーパバイザ エンジンのポートセキュリティテーブルに追加されない場合があります。

  回避策：ありません。

  この問題は、Cisco IOS リリース 12.2(50)SG2 および 12.2(52)SG で修正されています。

  CSCsw29489

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行しているスイッチで、802.1X VVID とポートセキュリティがポートに設定されている場合、LLDP 機能を備えた 802.1X 非対応の Cisco IP 電話とその背後にある PC を挿入すると、セキュリティ違反が発生することがあります。

  回避策：LLDP（スイッチ上）と電話機をオフにします（CallManager から実行）。

  この問題は、12.2(50)SG2 および 12.2(52)SG で修正されています。

  CSCsy21167

- CPU のキャッシュ内のパリティエラーにより、IOS がクラッシュし、次のようなクラッシュダンプファイルが表示されます。

```
Switch# show platform crashdump

VECTOR 0

*** CRASH DUMP ***
02/09/2009 10:10:30
Last crash: 02/09/2009 10:10:30

Build: 12.2(20090206:234053) IPBASE
buildversion addr: 13115584
```

```
MCSR: 40000000 <--- non-zero value!
.
```

重要なデータは「VECTOR 0」であり、MCSR 値は 40000000、20000000、または 10000000 です。

回避策：show platform cpu cache コマンドを入力して IOS アルゴリズムを起動し、CPU のキャッシュ内のパリティエラーを検出して回復します。実行中のシステムで正常に検出され、修正された CPU キャッシュのパリティエラー数の実行カウントを取得します。

```
Switch# show platform cpu cache
L1 Instruction Cache: ENABLED
L1 Data Cache: ENABLED
L2 Cache: ENABLED
Machine Check Interrupts: 5
L1 Instruction Cache Parity Errors: 3
L1 Instruction Cache Parity Errors (CPU30): 1
L1 Data Cache Parity Errors: 1
```

CSCsx15372

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- PVLAN 独立トランクがスイッチで設定され、ネイティブ VLAN が独立トランクポートに割り当てられていない場合は、sw private-vlan trunk native vlan コマンドを使用してネイティブ VLAN を割り当てる必要があります。

  回避策：PVLAN 独立トランクのネイティブ VLAN を設定します。（CSCsv38137）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- スイッチが snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
```

```
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  （CSCsu37068）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策：ありません。

  （CSCsw32519）

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。

  （CSCsv91302）

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。

  CSCsy29140

- Cisco IOS リリース 12.2(46)SG および 12.2(50)SGA を Supervisor Engines II+, II+10GE, IV, V or V-10GECatalyst 4500 series switch with s, 次のコマンドを入力するとスタンバイ スーパバイザ エンジンで障害が発生します。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

回避策：すべてのインターフェイスを個別に設定します。

スタンバイ スーパバイザ エンジンのリブートを回避するには、インターフェイス範囲で作業しているときに、exit または end コマンドを明示的に実行して tx-queue コンフィギュレーション コンテキストを終了します。exit コマンドの短縮形 ex は機能しません。これらのコマンドは、1 行ずつ入力する必要があります。コピー/ペーストは機能しません。

CSCsx44995

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

この問題は、12.2(40)SG で初めて確認されました。

回避策：AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

（CSCsh72408）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

（CSCsq74229）

- 通常、ログには次のメッセージが頻繁に表示されますが、パフォーマンスへの影響はありません。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

回避策：ありません。（CSCsv17545）

- スーパバイザに障害が発生すると、例外 crashinfo ファイルが作成されますが、スイッチを RPR モードで設定すると、そのようなコピーが有効になっていても、ブートフラッシュや slot0 にはコピーされません。手動でコピーまたは検査することもできます。

例外 crashinfo ファイル機能は、RPRモードではサポートされていません。

回避策：ありません。（CSCsr66481）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

（CSCsq71546）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- 12.2(50)SG または 12.2(50)SG1 を実行している Catalyst 4500 スイッチで、スイッチポートで 802.1X VVID とポートセキュリティが同時に設定されている場合、802.1x 非対応の Cisco IP 電話を背後の PC とともに挿入すると、セキュリティ違反が発生することがあります。

  回避策：ありません。CSCsv63638

- 冗長 WS-X45-Sup6-E または WS-X4516-10G で、スーパバイザエンジンの 10GE アップリンクが次のピアスーパバイザエンジンまたはラインカードの 10GE ポートのいずれかに直接接続されている場合、およびこのピアエンジンが Cisco IOS リリース 12.2(50)SG2 または以前のリリースを実行している場合、SSO スイッチオーバー後にリンクフラップが報告されます。
  - WS-X4516-10G
  - WS-C4948-10GE
  - WS-C4900M
  - WS-X4904-10GE

  回避策：
  - 影響を受ける 10GE ピアポートでリンクデバウンスを有効にします。
  - 現在の IOSリ ビジョンでリンクデバウンスが使用できない場合は、Cisco IOS リリース 12.2(52)SG にアップグレードします。リンクデバウンスの設定は必要ありません。

  CSCsy48647

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- ping が、ポスチャ検証の前に実行されません。

  回避策：permit icmp コマンドを使用して、インターフェイスに ID ポリシーを再適用します。（CSCsu03507）

- PVLAN 独立トランクがスイッチで設定され、ネイティブ VLAN が独立トランクポートに割り当てられていない場合は、sw private-vlan trunk native vlan コマンドを使用してネイティブ VLAN を割り当てる必要があります。

  回避策：PVLAN 独立トランクのネイティブ VLAN を設定します。（CSCsv38137）

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。
  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策：ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策: インターフェイスをシャットダウンしてから再度開きます。(CSCsr58573)

- ping が、ポスチャ検証の前に実行されません。

  回避策: permit icmp コマンドを使用して、インターフェイスにアイデンティティポリシーを再適用します。CSCsu03507

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、12.2(40)SG で初めて確認されました。

  回避策: AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

- 通常、ログには次のメッセージが頻繁に表示されますが、パフォーマンスへの影響はありません。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

  回避策: ありません。(CSCsv17545)

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策: ありません。

  (CSCsv91302)

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策: ありません。

  (CSCsw32519)

- 次のコマンドを入力すると、スタンバイ スーパバイザ エンジンがクラッシュします。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

  この問題は、冗長 Catalyst 4500 シリーズ スイッチで Cisco IOS リリース 12.2(46)SG または 12.2(50)SG を実行していて、次のスーパバイザエンジンのいずれかを使用している場合に発生します。II Plus、II Plus+10GE、IV、V、または V-10GE。

  回避策: 各インターフェイスを個別に設定します。

上記の tx-queue 設定コンテキストを終了するには、exit または end コマンドを明示的に入力します。exit コマンドの短縮形（ex）は機能しません。多くのコマンドをコピーして貼り付けるのではなく、exit コマンドと end コマンドを 1 行ずつ入力します。

CSCsx44995

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。

  CSCsy29140

- インターフェイスで無差別 TCP モードを使用する WCCPv2 サービスグループを使用する場合、スイッチはグループ内の WAAS デバイスの 1 つに GRE トラフィックをリダイレクトします。

  回避策：WCCP リダイレクションを削除します。

  WAAS デバイスがこの予期しない GRE トラフィックをドロップする場合、無差別モードの WCCP サービスグループはインターフェイスで使用できません。逆に、WAAS デバイスがスイッチにトラフィックを返す場合、スイッチは通常、元の宛先にトラフィックをルーティングします。

  CSCsx56922

- Cisco IOS ソフトウェアには、攻撃者がリモートから巧妙に細工された暗号化パケットを送信して Cisco IOS デバイスをリロードさせる可能性がある脆弱性が存在します。シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

- CSCsq24002

- Catalyst 4900M でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、12.2(46)SG、12.2(50)SG ～ SG5 を実行しているスイッチで発生する可能性があります。

  この問題は、12.2(52)SG 以降のリリースおよび 12.2(50)SG6 以降のリリースで解決されています。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- Cisco IOS 12.2(52)SG を実行しているスイッチで、ポートセキュリティ、DAI、DHCP スヌーピング、または BPDU ガードによってトリガーされた違反が原因で 802.1X が設定されたポートが per vp errdisable モードになると、ポートの 802.1X セッションはリンクダウンしているにもかかわらず、クリアされません。

回避策：ありません。

他の per vp errdisable 機能を使用して 802.1X を設定しないでください。

CSCsx74871

- スタンバイ WS-X45-SUP6-E スーパバイザエンジン上の 10 ギガビット イーサネット アップリンクは、SSO を介してアクティブになった後も引き続きパケットを受信しますが、トラフィックの送信を停止します。

  スタンバイ スーパバイザ エンジンをリセットしても、インターフェイスの設定を変更しても、アップリンクは復元できません。

  回避策：別の SSO スイッチオーバーを強制的に実行します。

  場合によっては、さらにスイッチオーバーを実行する必要があります。

  CSCsx52834

- AutoQoS は、ポートチャネルのメンバーポートでは設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、Cisco IOS リリース 12.2(40)SG で初めて確認されました。

  回避策：AutoQoS によって生成された設定を手動で適用します。

  CSCsv03316

- 2 つの WS-X4503+ スーパバイザエンジンが冗長構成でインストールされ、IOS HTTP サーバで default interface コマンドを入力すると、WS-X4503+ スーパバイザエンジンがリブートします。

  回避策：WS-X4503+ スーパバイザエンジンで default interface コマンドを入力します。

  CSCsy46543

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 以前のリリースから Cisco IOS リリース 12.2(52)SG（以降）への ISSU アップグレード中、または Cisco IOS リリース 12.2(52)SG（以降）から以前のリリースへのダウングレード中に、古いリリースの PM ISSU クライアントによって、次の無害なメッセージ（およびトレースバック）が表示されます。このメッセージは無視してください。

```
*Aug  7 14:28:27.167: %PM_ISSU-3-CAPABILITY: STANDBY:Port Manager ISSU client
rejecting capability 2
-Traceback= 10A55FEC 10A56738 104806A0 101498B8 115D5FC8 115D6044 101418FC
  10141A24 10141C50 10480A60 104782AC 108E5B84 108E4700 108E3D28 108E143C
  108DBBB8
```

  回避策：ありません。CSCsr85652

Cisco IOS リリース 12.2(50)SG8 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG8 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

  （SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

- このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	< 未使用のキュー >	control-packet
	11	< 未使用のキュー >	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

この状況は、次の理由で発生する可能性があります。

- パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
- スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策: ありません。このメッセージは情報メッセージです。(CSCsi60913)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

回避策：次のいずれかの操作を実行します。

- スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
- あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
- 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

（CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策:SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  (CSCsv90044)

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

  この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

  回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  (CSCsu36320)

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。(CSCsu37068)

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策:グラフィックを HTML ファイルに 256 KB まで埋め込みます(RFC 2397に準拠)。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  (CSCsu37834)

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで802.1Xの設定を解除し、スイッチに接続されているIPフォン（CDPポートのステータスTLVサポート搭載）にホストを再接続すると、ホストのMACアドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストのMACアドレスが新しいアクティブなスーパバイザエンジンのMACアドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで**shutdown**コマンドを入力し、その後に**no shutdown**コマンドを入力します。これにより、ホストのMACが再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOSリリース12.2(50)SG以降を実行しているデュアル スーパバイザ エンジンを搭載したスイッチでは、CDPポートステータスTLVをサポートするCisco IP電話がdot1xポートに接続され、PCが電話機の背後に接続されます。PCが電話機の背後から切断された後、ポートでdot1xを無効にし、PCを電話機に再接続すると、ホストのMACアドレスがスタンバイ スーパバイザ エンジンに同期されなくなります。この状態でスーパバイザ スイッチオーバーが実行されると、ホストのMACアドレスが新しいアクティブスーパバイザのMACアドレステーブルに存在しないため、ホストの接続が失われる可能性があります。

  回避策：インターフェイスでshutdown、no shutdownの順に入力します。これにより、再学習が行われ、ホストのMACがスタンバイ スーパバイザ エンジンに同期されます。

  CSCsw91661

- クラスマップヒットカウンタは、プライベートVLANトランクポートのプライマリVLANに接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは適切に適用されます。

  回避策：ありません。

  CSCsy72343

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any anyコマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-hostコマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルトACL（IPアクセスリスト）が、deny ip any anyを指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any anyを指定している。

  回避策：ありません。

  CSCsz63739

- link debounceコマンドでtimeが指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、およびSupervisor Engine 6L-Eのデフォルトは10 mSです。他のすべてのスーパバイザエンジンのデフォルトは100 mSです。

回避策：ありません。

デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

CSCte51948

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

Cisco IOS Release 12.2(40)SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

Cisco IOS リリース 12.2(50)SG8 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG8 で解決済みの警告について説明します。

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- Cisco IOS リリース 12.2(50)SG7 および 12.2(50)SG6で は、インターフェイス Fa1の [speed] full / [duplex] full 設定でローカルスイッチ（Catalyst 4900M または Supervisor Engine 6-E）をリロードすると、ブートアップ後に両側のリンクがダウンします。

  回避策：100/Full を設定解除し、shut/no shut を実行してから、ローカルスイッチで 100/Full を再設定します。

  CSCtf76196

- ACL ではなくプレフィックスリストで一致するように PBR ポリシーを設定すると、スイッチは失敗します。

  回避策：ACL でのみ一致するようにルートマップを設定します。

  CSCtg22126

Cisco IOS リリース 12.2(50)SG7 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG7 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet

	QueueID	以前の QueueName	新しい QueueName
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

回避策：Shut down, and then reopen the interface.

（CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

回避策：次のいずれかの操作を実行します。

- ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
- アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

（CSCsv44866）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
```

```
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOS リリース 12.2(50)SG 以降を実行しているデュアル スーパバイザ エンジンを搭載したスイッチでは、CDP ポートステータス TLV をサポートする Cisco IP 電話が dot1x ポートに接続され、PC が電話機の背後に接続されます。PC が電話機の背後から切断された後、ポートで dot1x を無効にし、PC を電話機に再接続すると、ホストの MAC アドレスがスタンバイ スーパバイザ エンジンに同期されなくなります。この状態でスーパバイザ スイッチオーバーが実行

されると、ホストの MAC アドレスが新しいアクティブスーパバイザの MAC アドレステーブルに存在しないため、ホストの接続が失われる可能性があります。

回避策：shutdown と入力してから、インターフェイスをno shutdownにします。これにより、再学習が行われ、ホストの MAC がスタンバイ スーパバイザ エンジンに同期されます。

CSCsw91661

- クラスマップヒットカウンタは、プライベート VLAN トランクポートのプライマリ VLAN にアタッチされている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは適切に適用されます。

  回避策：ありません。

  CSCsy72343

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策：ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

- ACL ではなくプレフィックスリストで一致するように PBR ポリシーを設定すると、スイッチは失敗します。

  回避策：ACL でのみ一致するようにルートマップを設定します。

  CSCtg22126

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策: 関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策: トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策: flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SG7 および 12.2(50)SG6で は、インターフェイス Fa1の [speed] full / [duplex] full 設定でローカルスイッチ（Catalyst 4900M または Supervisor Engine 6-E）をリロードすると、ブートアップ後に両側のリンクがダウンします。

  回避策: 100/Full を設定解除し、shut/no shut を実行してから、ローカルスイッチで 100/Full を再設定します。

  CSCtf76196

Cisco IOS リリース 12.2(50)SG7 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG7 で解決済みの警告について説明します。

- IOS リリース 12.2(53)SG1 または 12.2(50)SG6 を実行している 4500-E および 4900M スイッチは、特定の VLAN の唯一の QoS サービスポリシーが VLAN レベルである場合にクラッシュする可能性があります。

  この問題は、次の 3 つの条件を満たしている場合に発生します。

  - ソフトウェア生成またはソフトウェアスイッチド パケットが、VLAN（V）のメンバーであるインターフェイス（P）を出る。
  - パケットの優先順位は高くなく、PAK_PRIORITY が設定されていない。
  - 出力方向の 3 つのターゲット（ポート P、VLAN V、およびポート VLAN PV）のうち、qos ポリシーマップは出力方向の VLAN V にのみ付加される。

  回避策:

  - VLAN 専用ポリシーマップにマーキングアクションのみがある場合は、VLAN 専用ポリシーマップを VLAN 内のすべてのポートのポート VLAN ポリシーマップに置き換えます。
  - VLAN 専用ポリシーマップにポリシングアクションがある場合、VLAN 出力ポリシーマップを保持し、その VLAN のすべてのポートにキューイングアクション専用出力ポリシーマップを付加します。

  ポートレベルのポリシーマップは次のように表示されます。

  ```
  policy-map p1
      class class-default
          bandwidth percent 100
  ```

  CSCte12571

- Supervisor Engine II+10G E または Supervisor Engine V-10GE を実行している場合、X2-10GB-LRM リンクは起動時にダウンします。

  この問題は、Cisco IOS リリース 12.2(46)SG 以降のイメージで発生します。

  CSCtf26763

- PBR ポリシーは、Cisco IOS リリース 12.2(53)SG または 12.2(52)SG を実行している Supervisor Engine 6 では適用されません。パケットは、ポリシーベースのルーティングではなく、通常のルーティングテーブルを介して転送されます。

  これは、共有度の高いパスの副次的影響です。

  回避策: ありません。

  CSCtc90702

- Cisco IOS リリース 12.2(50)SG、12.2(52)SG、および 12.2(53)SG では、12.2(50)SG にアップグレードした後、一部の GBIC が互換性がないと見なされる場合があります。次のメッセージが表示される場合があります。

  ```
  %C4K_TRANSCEIVERMAN-3-INCOMPATIBLE: Port Gi5/10: New transceiver (speed
   10Gbps) is incompatible with this module
   The Gbic is unusable in the switch configuration with the 12.2(50)SG IOS.
  ```

  回避策: 次のいずれかの操作を実行します。

  - 別の GBIC を使用します。
  - Cisco IOS リリース 12.2(46)SG にダウングレードします。
  - Cisco IOS リリース 12.2(53)SG2 または 12.2(50)SG7 にアップグレードします。

  CSCtd40838

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- PVLAN トランクポートでは、学習した MAC アドレスが無条件にエージアウトし、フレーム配信の初期フェーズだけでなく、MAC エージング間隔ごとに定期的にフラッディングが発生します。この動作では、switchport block unicast コマンドを使用しますが、通信ができなくなるためリスクを伴います。

  回避策：ありません。ただし、PVLAN トランクポートでは switchport block unicast コマンドは入力できません。

  CSCtd49056

- ポートセキュリティが設定されているか、または独立トランクポートにスタティック MAC アドレスが設定されている場合、ポートの隣接関係はセカンダリ VLAN ではなくプライマリ VLAN で解決されます。

  回避策：ありません。

  CSCtc79119

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- Cisco IOS リリース 12.2(50)SG 以降を実行している Catalyst 4500 シリーズ スイッチでは、clear port-security dynamic interface fastethernet1 コマンドを入力すると、スイッチがリロードされます。

  インターフェイスにポートセキュリティが設定されていない場合は、このコマンドを入力しないでください。

  fa1 ではこのコマンドを入力しないでください。

  回避策：ありません。CSCtb16586

- Supervisor Engine 6-E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

Cisco IOS リリース 12.2(50)SG6 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG6 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。

- IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
- PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

（CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。
- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

  この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

  回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  (CSCsu36320)

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。(CSCsu37068)

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策:グラフィックを HTML ファイルに 256 KB まで埋め込みます(RFC 2397に準拠)。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  (CSCsu37834)

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策:ありません。(CSCsw14005)

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン(CDP ポートのステータス TLV サポート搭載)にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

回避策: インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOS リリース 12.2(50)SG 以降を実行しているデュアル スーパバイザ エンジンを搭載したスイッチでは、CDP ポートステータス TLV をサポートする Cisco IP 電話が dot1x ポートに接続され、PC が電話機の背後に接続されます。PC が電話機の背後から切断された後、ポートで dot1x を無効にし、PC を電話機に再接続すると、ホストの MAC アドレスがスタンバイ スーパバイザ エンジンに同期されなくなります。この状態でスーパバイザ スイッチオーバーが実行されると、ホストの MAC アドレスが新しいアクティブスーパバイザの MAC アドレステーブルに存在しないため、ホストの接続が失われる可能性があります。

  回避策: shutdown と入力してから、インターフェイスをno shutdownにします。これにより、再学習が行われ、ホストの MAC がスタンバイ スーパバイザ エンジンに同期されます。

  CSCsw91661

- クラスマップヒットカウンタは、プライベート VLAN トランクポートのプライマリ VLAN にアタッチされている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは適切に適用されます。

  回避策: ありません。

  CSCsy72343

- Cisco IOS リリース 12.2(50)SG 以降を実行している Catalyst 4500 シリーズ スイッチでは、clear port-security dynamic interface fastethernet1 コマンドを入力すると、スイッチがリロードされます。

  インターフェイスにポートセキュリティが設定されていない場合は、このコマンドを入力しないでください。

  fa1 ではこのコマンドを入力しないでください。

  回避策: ありません。CSCtb16586

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策: ありません。

  CSCsz63739

- link debounce コマンドで time が指定されていない場合、デフォルト値はスーパバイザエンジンによって異なります。C4900M、Supervisor Engine 6-E、および Supervisor Engine 6L-E のデフォルトは 10 mS です。他のすべてのスーパバイザエンジンのデフォルトは 100 mS です。

  回避策: ありません。

  デフォルト値は異なりますが、時間範囲内の任意の値を設定できます。

  CSCte51948

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

- **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
- スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

- PVLAN トランクポートでは、学習した MAC アドレスが無条件にエージアウトし、フレーム配信の初期フェーズだけでなく、MACエージング間隔ごとに定期的にフラッディングが発生します。この動作では、switchport block unicast コマンドを使用しますが、通信ができなくなるためリスクを伴います。

  回避策：ありません。ただし、PVLAN トランクポートでは switchport block unicast コマンドは入力できません。

  CSCtd49056

- ポートセキュリティが設定されているか、または独立トランクポートにスタティック MAC アドレスが設定されている場合、ポートの隣接関係はセカンダリ VLAN ではなくプライマリ VLAN で解決されます。

  回避策：ありません。

  CSCtc79119

Cisco IOS リリース 12.2(50)SG6 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG6 で解決済みの警告について説明します。

- システムで多数のレイヤ 3 ルートを使用して Supervisor Engine 6 を実行している場合、最小限の永続的な ARP アクティビティが存在すると、CPU 使用率が高くなることがあります。

  show processes cpu コマンドは、Cat4k Mgmt LoPri が大量の CPU を消費することを示します。show platform health コマンドは、K5L3FlcMan FwdEntry、K5L3Unciast IFE Review、および K5L3UnicastRpf IFE Review プロセスがターゲット使用率を超えて実行されていることを示します。

  大量の不完全な ARP エントリは、デバイスやウイルスのスキャンの結果生じる可能性があることに注意してください。

  回避策:

  - レイヤ 3 ルートの数を減らします。
  - 高い CPU 使用率をトリガーする ARP アクティビティを防止します。

  CSCta77487

- Supervisor 6-E/6L-E で多数の ACL を設定し、統計情報を有効にすると、スイッチの CPU 使用率が高くなることがあります。

  デフォルトでは、特定のアプリケーション（IP ソースガード および QoS）によって ACL 統計情報が統計になります。このような機能を設定すると、CPU 使用率が高くなります。

  CPU 使用率の高さは、show proc cpu コマンドで確認できます。また、show platform health コマンドの出力は、CPU 使用率が高いプロセスが「K5AclCamStatsMan hw」であることを示しています。

  この問題は、Cisco IOS リリース 12.2(40)SG 以降のリリースで発生する可能性があります。

  この問題は、Cisco IOS リリース 12.2(53)SG1 および 12.2(50)SG6 で解決されています。

  回避策: ACL、IPSG、および QoS 設定のサイズを小さくします。統計情報が ACL に対して明示的に有効になっている場合は、CLI で無効にします。

  ACL と IPSG が原因で CPU 使用率が高くなっている場合は、新しいソフトウェアにアップグレードします。

  QoS 設定が原因で CPU 使用率が高くなっている場合は、IOS イメージをアップグレードし、no qos statistics classification コマンドを入力します。

  CSCta54369

- 多数の ARP エントリ（47k）が存在する状態で、ARP テーブルをクリアすると、システムがリロードし、次のメッセージが表示されてスイッチがクラッシュします。

  ```
  ROM by abort at PC 0x0
  ```

  回避策: ありません。

  必要に応じて、Cisco IOS リリース 12.2(50)SG3 にダウングレードします。

  CSCta49512

- HSRP や OSPF などのプロトコルにサブセカンドタイマーを使用すると、ブートフラッシュへの書き込みによって CPU 使用率が高くなり、プロトコルのフラッピングが発生する可能性があります。

  回避策: 大きなファイルをコピーするなど、IOS では長時間のブートフラッシュ操作はしないでください。

  CSCsw84727

- no ip sticky arp コマンドがグローバルに設定されている場合でも、PVLAN SVI で学習された ARP エントリがエージアウトになりません。

  通常の SVI で学習された ARP エントリは影響を受けません。

  回避策：clear ip arp コマンドを使用して、それらの ARP エントリをクリアします。

  CSCtb37718

- ポートセキュリティと ARP インスペクションを同時に設定すると、スイッチに接続されているホストからの最初の ARP パケットが ARP インスペクションをバイパスし、誤ってブリッジアウトされる可能性があります。

  回避策：ポートセキュリティを無効にします。

  CSCtb40187

- QoS のサービスポリシーが設定されたスイッチでポリシーマップを変更せずにポリシーマップ コンフィギュレーション モードを終了すると、EtherChannel インターフェイスで出力サービスポリシーを設定するとリンクフラップが発生します。

  回避策：各 EtherChannel が独自のポリシーを持つように、異なる名前で同一のポリシーマップを設定します。このアクションにより、このリンクフラップの影響は限られた数の EtherChannel に限定されます。

  CSCsz82795

- サービスポリシーがポートチャネルにアタッチされ、そのサービスポリシーが CPU 生成パケットと一致するように設定されている場合、CPU 生成パケットの分類統計情報は増加しません。

  回避策：アクセスリストを設定して、CPU 生成パケットを許可し、ACL をクラスマップに適用します。

  CSCsy43967

- VLAN/SVI 上の多数のパケットがソフトウェアによって処理される場合、CPU に到達するパケットの数が多い間は、高い CPU 使用率が確認されることがあります。

  回避策：ありません。通常の機能は影響を受けません。

  CSCsy32312

Cisco IOS リリース 12.2(50)SG5 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG5 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

```
%CHKPT-4-INVALID: Invalid checkpoint client ID (189)
```

回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

（CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

（CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。
  – 該当ポートに SFP+ を挿入します。
  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

  この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  （CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  – Internet Explorer 8
  – Mozilla Firefox
  – Safari

  （CSCsu37834）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOS リリース 12.2(50)SG 以降を実行しているデュアル スーパバイザ エンジンを搭載したスイッチでは、CDP ポートステータス TLV をサポートする Cisco IP 電話が dot1x ポートに接続され、PC が電話機の背後に接続されます。PC が電話機の背後から切断された後、ポートで dot1x を無効にし、PC を電話機に再接続すると、ホストの MAC アドレスがスタンバイ スーパバイザ エンジンに同期されなくなります。この状態でスーパバイザ スイッチオーバーが実行されると、ホストの MAC アドレスが新しいアクティブスーパバイザの MAC アドレステーブルに存在しないため、ホストの接続が失われる可能性があります。

  回避策：shutdown と入力してから、インターフェイスをno shutdownにします。これにより、再学習が行われ、ホストの MAC がスタンバイ スーパバイザ エンジンに同期されます。

  CSCsw91661

- クラスマップヒットカウンタは、プライベート VLAN トランクポートのプライマリ VLAN にアタッチされている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは適切に適用されます。

  回避策：ありません。

  CSCsy72343

- Cisco IOS リリース 12.2(50)SG 以降を実行している Catalyst 4500 シリーズ スイッチでは、clear port-security dynamic interface fastethernet1 コマンドを入力すると、スイッチがリロードされます。

  インターフェイスにポートセキュリティが設定されていない場合は、このコマンドを入力しないでください。

  fa1 ではこのコマンドを入力しないでください。

  回避策：ありません。CSCtb16586

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

この状況、次の条件が満たされた場合にのみ発生します。

- authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
- デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
- クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

回避策：ありません。

CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
  reset.
  ```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

  WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは不要です。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（Engineering Failure Analysis）のためにラインカードを送信する必要もありません。

  （CSCsx32444）

- VLAN/SVI 上の多数のパケットがソフトウェアによって処理される場合、CPU に到達するパケットの数が多い間は、高い CPU 使用率が確認されることがあります。

  回避策：ありません。通常の機能は影響を受けません。

  CSCsy32312

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

次の条件では、RACL が正しく機能しなくなる可能性があります。

- ACL は、インターフェイスの出力方向に適用されます。
- IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

回避策：ありません。

CSCtc13297

Cisco IOS リリース 12.2(50)SG5 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG5 で解決済みの警告について説明します。

- 非常にまれな状況では、WS-X45-SUP6-E、WS-X45-SUP6L-E がトラフィックの転送をサイレントに停止することがあります。

  この警告は、レジスタ値が破損し、その後レイヤ 3 機能を有効にした場合に発生します。

  回避策：なし（CSCsz48273）

Cisco IOS リリース 12.2(50)SG4 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG4 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if

	QueueID	以前の QueueName	新しい QueueName
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。

– 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

（CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  – ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。

  – アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。

  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。

  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

- 該当ポートに任意のコマンドを入力します。
- 該当ポートに SFP+ を挿入します。
- 取り外した SFP+ を他のポートに再度挿入します。

(CSCsv90044)

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

(CSCsu36320)

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

回避策:verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。(CSCsu37068)

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

回避策:グラフィックを HTML ファイルに 256 KB まで埋め込みます(RFC 2397に準拠)。

次のブラウザは RFC 2397 をサポートしています。

- Internet Explorer 8
- Mozilla Firefox
- Safari

(CSCsu37834)

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- ポートで802.1Xの設定を解除し、スイッチに接続されているIPフォン（CDPポートのステータスTLVサポート搭載）にホストを再接続すると、ホストのMACアドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストのMACアドレスが新しいアクティブなスーパバイザエンジンのMACアドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで**shutdown**コマンドを入力し、その後に**no shutdown**コマンドを入力します。これにより、ホストのMACが再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOSリリース12.2(50)SG以降を実行しているデュアル スーパバイザ エンジンを搭載したスイッチでは、CDPポートステータスTLVをサポートするCisco IP電話がdot1xポートに接続され、PCが電話機の背後に接続されます。PCが電話機の背後から切断された後、ポートでdot1xを無効にし、PCを電話機に再接続すると、ホストのMACアドレスがスタンバイ スーパバイザ エンジンに同期されなくなります。この状態でスーパバイザ スイッチオーバーが実行されると、ホストのMACアドレスが新しいアクティブスーパバイザのMACアドレステーブルに存在しないため、ホストの接続が失われる可能性があります。

  回避策：shutdownと入力してから、インターフェイスをno shutdownにします。これにより、再学習が行われ、ホストのMACがスタンバイ スーパバイザ エンジンに同期されます。

  CSCsw91661

- クラスマップヒットカウンタは、プライベートVLANトランクポートのプライマリVLANにアタッチされている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは適切に適用されます。

  回避策：ありません。

  CSCsy72343

- Cisco IOSリリース12.2(50)SG以降を実行しているCatalyst 4500シリーズ スイッチでは、clear port-security dynamic interface fastethernet1コマンドを入力すると、スイッチがリロードされます。

  インターフェイスにポートセキュリティが設定されていない場合は、このコマンドを入力しないでください。

  fa1ではこのコマンドを入力しないでください。

  回避策：ありません。CSCtb16586

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any anyコマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-hostコマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルトACL（IPアクセスリスト）が、deny ip any anyを指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any anyを指定している。

  回避策：ありません。

  CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

- **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
- スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
  reset.
  ```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

  WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは実行しません。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（エンジニアリング障害分析）のためにラインカードを送信する必要もありません。

  （CSCsx32444）

- VLAN/SVI 上の多数のパケットがソフトウェアによって処理される場合、CPU に到達するパケットの数が多い間は、高い CPU 使用率が確認されることがあります。

  回避策：ありません。通常の機能は影響を受けません。

  CSCsy32312

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

  ```
  IPv6 access list a1
      permit icmp any any nd-ns sequence 10
      deny ipv6 any any sequence 20
  ```

```
IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

回避策：ありません。

CSCtc13297

Cisco IOS リリース 12.2(50)SG4 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG4 で解決済みの警告について説明します。

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策：ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- ping が、ポスチャ検証の前に実行されません。

  回避策：permit icmp コマンドを使用して、インターフェイスに ID ポリシーを再適用します。（CSCsu03507）

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、12.2(40)SG で初めて確認されました。

  回避策：AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

- 通常、ログには次のメッセージが頻繁に記録されます。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

  パフォーマンスへの影響はありません。

  回避策：ありません。（CSCsv17545）

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策: ありません。(CSCsv91302)

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策: ありません。(CSCsw32519)

- Cisco IOS リリース 12.2(46)SG および 12.2(50)SGA を Supervisor Engines II+, II+10GE, IV, V or V-10GECatalyst 4500 series switch with s, 次のコマンドを入力するとスタンバイ スーパバイザ エンジンで障害が発生します。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

  回避策: すべてのインターフェイスを個別に設定します。

  スタンバイ スーパバイザ エンジンのリブートを回避するには、インターフェイス範囲で作業しているときに、exit または end コマンドを明示的に実行して tx-queue コンフィギュレーション コンテキストを終了します。exit コマンドの短縮形 ex は機能しません。これらのコマンドは、1 行ずつ入力する必要があります。コピー/ペーストは機能しません。

  CSCsx44995

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN(authentication control-direction in コマンドを使用)およびマルチドメイン認証(MDA)(authentication host-mode multi-domain コマンドを使用)に対して設定されているポートでは出力トラフィックは許可されません。

  回避策: ありません。(CSCsy29140)

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

  この動作は、ピアデバイスがリモート障害を送信するときに、Cisco IOS リリース 12.2(50)SG から 12.2(50)SG3 で確認されています。

  回避策: 両端で自動ネゴシエーションを無効にします。

  (CSCta02425)

- HTTP(S) の認証プロキシ、Web 認証、または同意機能が設定された Cisco IOS ソフトウェアには、認証されていないセッションが認証プロキシサーバや同意 Web ページをバイパスする可能性がある脆弱性が含まれています。

この脆弱性を軽減する回避策はありません。

このアドバイザリは次のリンクに掲載されています。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

CSCsy15227

- Cisco IOS ソフトウェアには、攻撃者がリモートから巧妙に細工された暗号化パケットを送信して Cisco IOS デバイスをリロードさせる可能性がある脆弱性が存在します。シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tls

- CSCsq24002

- 影響を受けるバージョンの Cisco IOS ソフトウェアを実行しているシスコデバイスは、IP トンネルおよび Cisco Express Forwarding 用に設定されている場合、サービス妨害（DoS）攻撃に対して脆弱です。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  CSCsx70889

- AutoQoS は、ポートチャネルのメンバーポートでは設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、Cisco IOS リリース 12.2(40)SG で初めて確認されました。

  回避策：AutoQoS によって生成された設定を手動で適用します。

  CSCsv03316

- 2 つの WS-X4503+ スーパバイザエンジンが冗長構成でインストールされ、IOS HTTP サーバで default interface コマンドを入力すると、WS-X4503+スーパバイザエンジンがリブートします。

  回避策：WS-X4503+ スーパバイザエンジンで default interface コマンドを入力します。

  CSCsy46543

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
reset.
```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

  WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは実行しません。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（エンジニアリング障害分析）のためにラインカードを送信する必要もありません。

  （CSCsx32444）

- Cisco IOS 12.2(50)SG2 から ISSU を介して冗長 SUP6-E スイッチをダウングレードすると、スーパバイザアップリンクはトラフィックの伝送を停止します。すべてのリンクはアップのままです。

回避策：シェルフをリロードします。

注 以前のリリースを使用した SSO スイッチオーバーでは、トラフィックが復元される可能性がありますが、一時的なものです。

（CSCsz17726）

Cisco IOS リリース 12.2(50)SG3 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG3 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

  （SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはス

イッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策:

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)
- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)
- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: **no shutdown** コマンドを入力します。(CSCsg27395)
- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)
- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策: ありません。このメッセージは情報メッセージです。(CSCsi60913)
- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)
- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)
- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

- **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
- CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

（CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

```
%PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
```

回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

この問題は、VRF が設定されたインターフェイスでのみ発生します。

回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

回避策：Shut down, and then reopen the interface.

（CSCso50921）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

回避策：ありません。（CSCsr95941）

- ping が、ポスチャ検証の前に実行されません。

回避策：permit icmp コマンドを使用して、インターフェイスにID ポリシーを再適用します。（CSCsu03507）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

  （CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  - 該当ポートに任意のコマンドを入力します。
  - 該当ポートに SFP+ を挿入します。
  - 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

  この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

  （CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策：ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策：ありません。（CSCsw32519）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。（CSCsv91302）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。CSCsy29140

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

回避策：ありません。

CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

  回避策：ありません。（CSCso68331）

- AutoQoS は、ポートチャネルのメンバーポートでは設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

  この問題は、Cisco IOS リリース 12.2(40)SG で初めて確認されました。

  回避策：AutoQoS によって生成された設定を手動で適用します。

  CSCsv03316

- Cisco IOS リリース 12.2(46)SG および 12.2(50)SGA を Supervisor Engines II+, II+10GE, IV, V or V-10GECatalyst 4500 series switch with s, 次のコマンドを入力するとスタンバイ スーパバイザ エンジンで障害が発生します。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

  回避策：すべてのインターフェイスを個別に設定します。

  スタンバイ スーパバイザ エンジンのリブートを回避するには、インターフェイス範囲で作業しているときに、exit または end コマンドを明示的に実行して tx-queue コンフィギュレーション コンテキストを終了します。exit コマンドの短縮形 ex は機能しません。これらのコマンドは、1 行ずつ入力する必要があります。コピー/ペーストは機能しません。

  CSCsx44995

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

この問題は、12.2(40)SG で初めて確認されました。

回避策：AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

  回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策: 関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策: トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策: flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策: ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策: ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

回避策：ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SGI の実行中に、まれに、PoE ラインカードが正常に機能している場合でも、次の syslog エラーメッセージが表示されます。

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
reset.
```

このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は示していません。

これは、Catalyst 4500-E シャーシ（WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカード）のみに影響します。

回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは不要です。RMA を実行したり、EFA のラインカードを送信したりする必要はありません。

（CSCsx32444）

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

```
%C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
reset.
```

このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは実行しません。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（エンジニアリング障害分析）のためにラインカードを送信する必要もありません。

（CSCsx32444）

- 通常、ログには次のメッセージが頻繁に記録されます。

```
001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
```

パフォーマンスへの影響はありません。

回避策：ありません。（CSCsv17545）

- Cisco IOS 12.2(50)SG2 から ISSU を介して冗長 SUP6-E スイッチをダウングレードすると、スーパバイザアップリンクはトラフィックの伝送を停止します。すべてのリンクはアップのままです。

回避策：シェルフをリロードします。

注 以前のリリースを使用した SSO スイッチオーバーでは、トラフィックが復元される可能性がありますが、一時的なものです。

（CSCsz17726）

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

  この動作は、ピアデバイスがリモート障害を送信するときに、Cisco IOS リリース 12.2(50)SG から 12.2(50)SG3 で確認されています。

  回避策：両端で自動ネゴシエーションを無効にします。

  （CSCta02425）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

Cisco IOS リリース 12.2(50)SG3 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG3 で解決済みの警告について説明します。

- Supervisor Engine 6-E を搭載した Catalyst 4500 E シリーズ スイッチは、TwinGig コンバータのインストールまたは削除時、あるいは TwinGig コンバータをインストールした状態での起動時にクラッシュすることがあります。

  TwinGig コンバータは、E シリーズ スーパバイザおよびラインカードでのみサポートされます。このバグは、コンバータがインストールされていないシステムには影響しません。

  回避策：ありません。

  スイッチが正常に起動し、インストールされているすべての TwinGig コンバータが検出されると、コンバータを挿入しない限りクラッシュする可能性は低くなります。CSCsz49331

Cisco IOS リリース 12.2(50)SG2 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG2 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

  Service-policy output: p1

    Class-map: c1 (match-all)
      0 packets<--------It stays at '0' despite of traffic being received
      Match: access-group name fnacl21
      police: Per-interface
        Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

– このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  この状況は、次の理由で発生する可能性があります。

  – パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。

  – スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: no shutdown コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策: ありません。このメッセージは情報メッセージです。(CSCsi60913)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- ping が、ポスチャ検証の前に実行されません。

  回避策：permit icmp コマンドを使用して、インターフェイスにID ポリシーを再適用します。（CSCsu03507）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。

- アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

（CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

（CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

- 該当ポートに任意のコマンドを入力します。
- 該当ポートに SFP+ を挿入します。
- 取り外した SFP+ を他のポートに再度挿入します。

（CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
```

```
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策：ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策：ありません。（CSCsw32519）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。（CSCsv91302）

- ポートで 802.1X の設定を解除し、スイッチに接続されている IP フォン（CDP ポートのステータス TLV サポート搭載）にホストを再接続すると、ホストの MAC アドレスはスタンバイ スーパバイザ エンジンに同期されません。

  この状態の間にスイッチがスーパバイザのスイッチオーバーを実行すると、ホストの MAC アドレスが新しいアクティブなスーパバイザエンジンの MAC アドレステーブルに存在しないため、ホストで接続が切断される可能性があります。

  回避策：インターフェイスで **shutdown** コマンドを入力し、その後に **no shutdown** コマンドを入力します。これにより、ホストの MAC が再度学習され、スタンバイ スーパバイザ エンジンに同期されるようになります。CSCsw91661

- Cisco IOS リリース 12.2(50)SG 以降のリリースを実行しているクラシックシリーズのスーパバイザおよび Supervisor Engine 6-E では、ポートが許可される前は、Wake-on-LAN（authentication control-direction in コマンドを使用）およびマルチドメイン認証（MDA）（authentication host-mode multi-domain コマンドを使用）に対して設定されているポートでは出力トラフィックは許可されません。

  回避策：ありません。CSCsy29140

- クラスマップヒットカウンタは、PVLAN トランクポートのプライマリ VLAN に接続されている出力ポリシーマップでは増加しません。ただし、トラフィックは適切に分類され、ポリシーで設定されたアクションは正しく適用されます。

  回避策：ありません。CSCsy72343

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

```
Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
software error occurred. Null0 linked to wrong hwidb Null0
```

回避策:ありません。(CSCso68331)

- AutoQoS は、ポートチャネルのメンバーポートでは設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

この問題は、Cisco IOS リリース 12.2(40)SG で初めて確認されました。

回避策:AutoQoS によって生成された設定を手動で適用します。

CSCsv03316

- Cisco IOS リリース 12.2(46)SG および 12.2(50)SGA を Supervisor Engines II+, II+10GE, IV, V or V-10GECatalyst 4500 series switch with s, 次のコマンドを入力するとスタンバイ スーパバイザ エンジンで障害が発生します。

```
interface range GigabitEthernet8/2 - 48
   switchport voice vlan 505
   qos vlan-based
   tx-queue 3
     priority high
   ip dhcp snooping limit rate 100
```

回避策:すべてのインターフェイスを個別に設定します。

スタンバイ スーパバイザ エンジンのリブートを回避するには、インターフェイス範囲で作業しているときに、exit または end コマンドを明示的に実行して tx-queue コンフィギュレーション コンテキストを終了します。exit コマンドの短縮形 ex は機能しません。これらのコマンドは、1 行ずつ入力する必要があります。コピー/ペーストは機能しません。

CSCsx44995

- ポートチャネルのメンバーポートでは AutoQoS を設定できません。

```
Switch# sh runn int fa 3/1
 channel-group 2 mode on  -- Port in etherchannel
Switch# conf t
Switch(config)# int fa 3/1
Switch(config-if)# auto qos voip trust
AutoQoS Error: AutoQoS can not be configured on member port(s) of a port-channel
```

この問題は、12.2(40)SG で初めて確認されました。

回避策:AutoQoS によって生成された設定を手動で適用します。Auto QoS は使用しないでください。CSCsv03316

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  （CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策: 関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  （CSCso96660）

- VLAN ロードバランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策: トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策: flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策: ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策: ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策: ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SGI の実行中に、まれに、PoE ラインカードが正常に機能している場合でも、次の syslog エラーメッセージが表示されることがあります。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
  reset.
  ```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は示していません。

  これは、Catalyst 4500-E シャーシ（WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカード）のみに影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは不要です。RMA を実行したり、EFA のラインカードを送信したりする必要はありません。

  （CSCsx32444）

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be
  reset.
  ```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

  WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは実行しません。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（エンジニアリング障害分析）のためにラインカードを送信する必要もありません。

  （CSCsx32444）

- 通常、ログには次のメッセージが頻繁に記録されます。

  ```
  001298: .Oct  8 01:38:50.968: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2947 dPErr: 1 mPErr: 0 valid: 1
  001299: .Oct  8 01:51:20.100: %C4K_SWITCHINGENGINEMAN-4-TCAMINTERRUPT: flCam0
  aPErr interrupt. errAddr: 0x2B59 dPErr: 1 mPErr: 0 valid: 1
  ```

  パフォーマンスへの影響はありません。

  回避策：ありません。（CSCsv17545）

- Cisco IOS 12.2(50)SG2 から ISSU を介して冗長 SUP6-E スイッチをダウングレードすると、スーパバイザアップリンクはトラフィックの伝送を停止します。すべてのリンクはアップのままです。

  回避策：シェルフをリロードします。

  注　以前のリリースを使用した SSO スイッチオーバーでは、トラフィックが復元される可能性がありますが、一時的なものです。

  （CSCsz17726）

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

  この動作は、ピアデバイスがリモート障害を送信するときに、Cisco IOS リリース 12.2(50)SG から 12.2(50)SG3 で確認されています。

  回避策: 両端で自動ネゴシエーションを無効にします。

  （CSCta02425）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

Cisco IOS リリース 12.2(50)SG2 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG2 で解決済みの警告について説明します。

- ARP テーブルで MAC エントリが SNAP であることが示されると、SNAP ホスト宛てのトラフィックのパケットがドロップされることがあります。

  回避策：

  1. ホストのスタティック ARPA エントリを設定します。

  2. 修正を含む将来の IOS リリースにアップグレードします。

  CSCsu90780

- SPAN が有効で、コリジョンによって生成されたエラーパケットなどの不正な形式のパケットを SPAN 送信元ポートが受信している場合、ポートはパケットの受信を停止したり、パケットを繰り返し再生して他のポートへのフラッディングを起こしたりすることがあります。

この問題は、WS-C4948 および WS-X4548-GB を含むプラットフォーム、および次のようなラインカードで確認されています。

- WS-X4418-GB（ポート 3 ～ 18）
- WS-X4506-GB-T（RJ45 ポート）
- WS-X4424-GB-RJ45
- WS-X4448-GB-RJ45
- WS-X4548-GB-RJ45
- WS-X4524-GB-RJ45V
- WS-X4548-GB-RJ45V

回避策：次のコマンドを使用して、SPAN セッションが正常なパケットのみを渡すようにパケットフィルタリングを有効にします。

```
monitor session 1 filter packet-type good rx
```

CSCsv07168

- Cisco IOS リリース 12.21(31)SGA または 12.2(46)SG を実行している Catalyst 4948-10GE シャーシでは、IP DSCP 値に基づくデフォルトの送信キューの選択が正しくありません。たとえば、CS1 と CS5 の両方のトラフィックは、送信キュー 1 と 3 ではなく、送信キュー 1 を通過します。

  回避策：次のように、グローバル QoS を有効または無効にします。

```
switch# conf t
switch(conf)# qos
switch(conf)# no qos
```

CSCsv29945

- 複数の REP セグメントを設定する場合、1 つのセグメントでプリエンプションを実行すると、すべての REP セグメントがダウンします。

  回避策：ありません。CSCsv91297

- Catalyst 4500 シリーズ スイッチでは、隔離されたプライベート VLAN トランクインターフェイスがフラップすると、ポート単位の VLAN 単位の入力ポリサーはポートに適用されなくなります。

  影響を受ける Cisco IOS リリースには、12.2(31)SGA08、12.2(37)SG、12.2(40)SG、12.2(46)SG、および 12.2(50)SG が含まれます。

  回避策：次のように QoS を無効にして設定します。

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no qos
Switch(config)# qos
Switch(config)# end
Switch#
```

CSCsw19087

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行している Catalyst 4500 冗長スイッチでは、スイッチポートで 802.1X VVID とポートセキュリティを同時に設定すると、802.1X 非対応の Cisco IP 電話からの CDP MAC は、スタンバイ スーパバイザ エンジンのポートセキュリティテーブルには追加されない場合があります。

  回避策：ありません。CSCsw29489

- 特定の条件下で、2 つのスーパバイザエンジン（Sup II+、Sup IV、または Sup V）を搭載した Catalyst 4500R シャーシでは、ピアスーパバイザエンジンからのキープアライブメッセージが 162 秒間失われると、フェールオーバー（スーパバイザ スイッチオーバー）が発生することがあります。

  問題が発生している間、次のメッセージが表示されます。

  ```
  %C4K_REDUNDANCY-4-KEEPALIVE_WARNING: STANDBY:Keepalive messages from peer Supervisor
  are missing for 162 seconds
  %C4K_REDUNDANCY-3-PEER_RELOAD: STANDBY:The peer Supervisor is being reset because
  keepalive message(s) not received.
  ```

  回避策：ありません。（CSCsw64001）

- show idprom interface FastEthernet 1 コマンドを入力すると、クラッシュが発生します。

  回避策：ありません。CSCsw77413

- スタンバイ スーパバイザ エンジン WS-X45-SUP6-E 上の 10GE アップリンクが、SSO スイッチオーバーによってアクティブになった後、トラフィックの送信を停止します。ただし、パケットはアップリンクで引き続き受信されます。

  ピアスイッチからのトラフィックは影響を受けるスイッチによって受信されますが、ピアスイッチは影響を受けるスイッチからのトラフィックを受信しません。そのため、CDP などのプロトコルで混乱が生じる可能性があります。影響を受けるスイッチは、予想される CDP 隣接関係を報告しますが、ピアスイッチは報告しません。これにより、ピアスイッチの問題が誤診断される可能性があります。

  スタンバイ スーパバイザ エンジンをリセットしたり、インターフェイスの設定を変更したりしても、10GE アップリンクは復元できません。

  回避策：別の SSO スイッチオーバーを強制します。

  まれに、2 回目のスイッチオーバーで問題が再発することがあります。その場合、追加のスイッチオーバーが必要になります。

  CSCsx52834

- ポートが次のように設定されている場合、ホストは MAB を介して認証されません。シングルホストモード（authentication host-mode single-host コマンドを使用）および Wake-on-LAN（authentication control-direction in コマンドを使用）。

  回避策：no authentication control-direction in コマンドを使用して Wake-on-LAN を無効にします。

  CSCsx98360

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行している Catalyst 4500 シリーズ スイッチで、スイッチポートで 802.1X VVID とポートセキュリティが同時に設定されている場合、LLDP 機能を備えた 802.1X 非対応の Cisco IP 電話を背後にある PC とともに挿入すると、セキュリティ違反が発生することがあります。IP フォンが LLDP パケットを送信する前に、電話機の背後にある PC がポートで許可されると、違反がトリガーされます。

  回避策：CallManager からスイッチと Cisco IP 電話の LLDP をオフにします。

  CSCsy21167

- ラインカード WS-X4648-RJ45V-E または WS-X4648-RJ45V+E は、スイッチのブートアップ時またはラインカードのリセット時に PoE 電源を提供しません。非 PoE リンクは引き続き機能します。

  回避策：hw-module reset コマンドを使用してラインカードをリロードします。

  CSCsy74921

- コントロール プレーン ポリシングを使用する場合、コントロールプレーンクラス（macro global apply system-cpp コマンドによって自動的に作成され、定義済み ACL を使用してトラフィックを照合するクラス）がパケット数とバイト数を増加させます。これは、両方のカウンタがゼロ以外であることを意味します。

  対照的に、データプレーンクラス（ユーザが記述した ACL によって手動で設定）はバイトカウンタを増加させますが、パケット数は増加しません（0 のまま）。

  回避策：ありません。

  CSCsw16557

Cisco IOS リリース 12.2(50)SG1 の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG1 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- ごくまれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6 / 1 コマンドの出力に、一致しているパケットが表示されないことがあります。

```
Switch# show policy-map int fa6/1

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

  （SCef01798）

- SSO スイッチオーバーの後、shutdown コマンドを入力してから UDLD disable ステートになっているポート上で no shutdown コマンドを入力すると、スイッチ コンソールに「PM-4-PORT_INCONSISTENT」エラー メッセージが表示される場合があります。これはス

イッチには影響しません。ポートは UDLD disable ステートのままです。shutdown コマンドを再入力してから同じポート上で no shutdown コマンドを入力すると、エラー メッセージが表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書を検索します。
  - 永続的な自己署名証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンで個別に生成され、証明書は異なります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- 12.2(31)SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェアリリースの場合と同様に動作しないことがあります。次の表に、この変更が反映されています。

  これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

	QueueID	以前の QueueName	新しい QueueName
	5	control-packet	control-packet
	6	rpf-failure	control-packet
	7	adj-same-if	control-packet
	8	<未使用のキュー>	control-packet
	11	<未使用のキュー>	adj-same-if
	13	acl input log	rfp-failure
	14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを入力します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

この状況は、次の理由で発生する可能性があります。

- パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
- スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバードポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation コマンドを入力しても、ポリサーによって 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に a- が追加されます。

  これはパフォーマンスには影響しません。

  回避策: no shutdown コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されることがあります。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策: ありません。このメッセージは情報メッセージです。(CSCsi60913)

- ISSU アップグレードを実行し、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- 3000 以上の VLAN ID でトラフィックを送信すると、障害により発生するコンバージェンスタイミングが 225 ms を超えます。

  回避策: ありません。(CSCsm30320)

- スイッチのリロード後に、番号付けされていない IP 設定が失われます。

  回避策: 次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  (CSCsq63051)

- SSO モード時に、同じチャネル番号を持つアクティブなスーパバイザエンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後にポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定すると、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- PVLAN 独立トランクがスイッチで設定され、ネイティブ VLAN が独立トランクポートに割り当てられていない場合は、sw private-vlan trunk native vlan コマンドを使用してネイティブ VLAN を割り当てる必要があります。

  回避策：PVLAN 独立トランクのネイティブ VLAN を設定します。（CSCsv38137）

- Cisco IOS リリース 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、復元後も、スパニングツリーは disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  回避策：Shut down, and then reopen the interface.

  （CSCso50921）

- Cisco IOS リリース 12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN を削除しても Unauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチは snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、スイッチはこのコマンドを拒否します。

  回避策：ありません。（CSCsr95941）

- ping が、ポスチャ検証の前に実行されません。

  回避策：permit icmp コマンドを使用して、インターフェイスにID ポリシーを再適用します。（CSCsu03507）

- PVLAN 独立ポートが、マルチキャストソースとして機能するルータに接続され、IGMPスヌーピングを有効にすると、独立ポートに接続されたルータはPIMネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。

- PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

（CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを入力すると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：debug management expression evaluator コマンドを無効にします。（CSCsu67323）

- 802.1X を単方向制御ポートとして設定すると、出力トラフィックが許可されない場合があります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスを設定すると、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずにCTS SXP接続が設定され、ボックスにデフォルトのSXP送信元 IP アドレスが設定されていない場合、異なるSXP接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブなスーパバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブなスーパバイザエンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

回避策：次のいずれかの操作を実行します。

– ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
– アクティブなスーパバイザエンジンでコマンドを削除してから入力し直します。スタンバイ スーパバイザ エンジンがこの変更を取得します。

（CSCsv44866）

- 冗長シャーシで issu loadversion コマンドを入力すると、「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが発生する場合があります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードを CFM サポートモードから CFM 非サポートモードに変更すると、CFM は自動的に無効になります。モードをサポートモードにリセットすると、インターフェイスの実行コンフィギュレーションで確認されるように、CFM の状態は Disabled のままになります。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion を実行すると、一括同期の失敗が発生します。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次のタスクを実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。
  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。
  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。
  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、「duplicate seeprom」エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。
  – 該当ポートに SFP+ を挿入します。
  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを入力すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507# verify bootflash:cat4500-entservices-mz.122-37.SG1
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この問題は、Cisco IOS リリース 12.2(40)SG 以降を実行している場合に発生することがあります。

回避策 : verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力が表示されません。

  回避策 : verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策 : グラフィックを HTML ファイルに 256 KB まで埋め込みます（RFC 2397に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策 : ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策 : ありません。（CSCsw32519）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

```
%SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
106617F8
```

これは、実行中のクラシックまたはEシリーズのCatalyst 4500スーパバイザエンジンに適用されます。
Cisco IOS Release 12.2(50)SG

回避策：ありません。（CSCsw14005）

- channel-group x または channel-protocol モードで、fa1管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、fa1 管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。（CSCsv91302）

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM をグローバルに有効にし、さらに入力インターフェイス上で有効にすると、インターフェイスで受信した CFM パケットはハードウェア コントロール プレーン ポリシングでポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

- コントロール プレーン ポリシングを使用する場合、コントロールプレーンクラス（macro global apply system-cpp コマンドによって自動的に作成され、定義済み ACL を使用してトラフィックを照合するクラス）がパケット数とバイト数を増加させます。これは、両方のカウンタがゼロ以外であることを意味します。

  代わりに、データプレーンクラス（ユーザが記述した ACL によって手動で設定）はバイトカウンタを増加させますが、パケット数は増加しません（0 のまま）。

  回避策：ありません。CSCsw16557

Supervisor Engine 6-E に固有の警告

- Cisco IOS リリース 12.2(40)SG を実行しているシステムは、ソフトウェア QoS ルックアップの .1Q パケットの処理をサポートしていません。

  回避策：ありません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth や shape などのキューイングパラメータをいくつか変更して再設定して、問題を解決してください。（CSCsk62457）

- E シリーズ スイッチでファントレイの障害が発生するか、またはスーパバイザエンジンの温度が重大な状態になると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を見つけます。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、ファントレイの障害を示しています。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザエンジンの臨界温度が障害のしきい値を超えたことを示しています。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG を実行している WS-X4706-10GE で使用すると、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生することがあります。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが接続されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキングアクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の CoS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された CoS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 で説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。(CSCsk72544)

- インターフェイス上で信頼境界機能が有効になっている場合に、現在の動作状態を確認するコマンドはありません。

  回避策:ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを確認できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの CoS/DSCP フィールドは強制的にゼロになります。これは、そのインターフェイスの 1 つの Qos ポリシーが分類のために CoS/DSCP 値を使用しているためで、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。

  (CSCsh72408)

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策:show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。(CSCsi71036)

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策:ありません。ただし、**show policy-map** *name* を入力すると、無条件のマーキング アクションが表示されます。(CSCsi94144)

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。Cisco IOS を起動すると、シャーシタイプは正しく表示されます。

  回避策:ありません。(CSCsl72868)

- ポリシーマップで class-default クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策:DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。このコマンドは、サイズの範囲を指定します。(CSCso06422)

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から後続のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブなスーパーバイザ エンジンが IOS を実行しており、スタンバイ スーパーバイザ エンジンが ROMMON で実行され、スタンバイ スーパーバイザ エンジンの ROMMON がバージョン 0.34 からそれ以降のバージョンにアップグレードされると発生します。アップグレード処理により、スタンバイ スーパーバイザ エンジンのアップリンクがダウンしますが、アクティブなスーパーバイザエンジンはこれを認識しません。

  回避策:通常の操作を再開するには、次のいずれかの操作を実行します。

  - **redundancy reload shelf** コマンドで、両方のスーパーバイザエンジンをリロードします。
  - スタンバイ スーパーバイザ エンジンをシャーシから一時的に短時間取り出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。(CSCsm81875)

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズフレームがスイッチポートに送信され、フロー制御の受信設定が 10 Gb ポートに切り替えられたときに発生します。

回避策: トラフィックが存在しない場合は、フロー制御の受信設定を変更します。(CSCso71647)

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策: 関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  (CSCsq71546)

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力で内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策: ありません。

  (CSCso96660)

- VLAN ロードバランシング(VLB)を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートがあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策: トポロジ内の任意の REP ポート(VLB が設定されているのと同じセグメント)で shut を入力してから no shut コマンドを入力します。(CSCsq75342)

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannelが定義されていれば、リブート後にFlexLink の設定が適用されないことがあります。

  回避策: flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。(CSCsq13477)

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合(FlexLink の障害)、代替ポートに移動されません。

  回避策: ありません。(CSCsq99468)

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策: ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。(CSCsq77181)

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策: ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  (CSCsq74229)

- CFM Inward Facing MEP(IFM)が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、**show ethernet cfm maintenance-points local** コマンドによって IFM CC ステータスが inactive と表示されます。VLAN を割り当てても、CC-status は Inactive のままになります。

  この動作は、IFM を設定する前に VLAN を最初に割り当てておらず、後で同じ VLAN を割り当てた場合にのみ発生します。

  回避策: ポート上の IFM の設定を解除し、再設定します。

- Cisco IOS リリース 12.2(50)SGI の実行中に、まれに、PoE ラインカードが正常に機能している場合でも、次の syslog エラーメッセージが表示されることがあります。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
  ```

このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は示していません。

これは、Catalyst 4500-E シャーシ（WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカード）のみに影響します。

回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは不要です。RMA を実行したり、EFA のラインカードを送信したりする必要はありません。

（CSCsx32444）

- Cisco IOS リリース 12.2(50)SG または 12.2(50)SG1 を実行し、WS-X4648-GB-RJ45V または WS-X4648-GB-RJ45V+ ラインカードを使用している場合、PoE ラインカードが正しく機能している場合でも、まれに次の syslog エラーメッセージが表示されます。

  ```
  %C4K_ETHPOE-3-POEMICROCONTROLLERWARNING: Switching module in slot [x] needs to be reset.
  ```

  このログメッセージは情報提供のみを目的としています。ラインカードの潜在的な問題は反映されません。

  WS-X4648-GB-RJ45V および WS-X4648-GB-RJ45V+ ラインカードにのみ影響します。

  回避策：警告メッセージを無視します。ラインカードまたはポートをリセットするアクションは実行しません。RMA（Return to Manufacturing for Analysis）を実行する必要も、EFA（エンジニアリング障害分析）のためにラインカードを送信する必要もありません。

  （CSCsx32444）

- ポートが次のように設定されている場合、ホストは MAB を介して認証されません。シングルホストモード（authentication host-mode single-host コマンドを使用）および Wake-on-LAN（authentication control-direction in コマンドを使用）。

  回避策：authentication control-direction in コマンドを使用して Wake-on-LAN を無効にします。

  CSCsx98360

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

  この動作は、ピアデバイスがリモート障害を送信するときに、Cisco IOS リリース 12.2(50)SG から 12.2(50)SG3 で確認されています。

  回避策：両端で自動ネゴシエーションを無効にします。

  （CSCta02425）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

- ACL は、インターフェイスの出力方向に適用されます。
- IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

回避策：ありません。

CSCtc13297

Cisco IOS リリース 12.2(50)SG1 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG1 で解決済みの警告について説明します。

- スイッチが予期せずリロードされることがあります。コンソールまたは crashinfo ファイルに、次のメッセージが表示されることがあります。

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
  ```

  回避策：NetFlow が設定されているすべてのサブインターフェイスで、次のいずれかのコマンドを使用して NetFlow を無効にします。

  ```
  no ip flow ingress
  no ip flow egress
  no ip route-cache flow
  ```

  （CSCsq75944）

- IP フォンを介してホストに接続されたポートでポートセキュリティが設定されていて、ホストが切断されている場合、IP フォンとスイッチが CDP の 2 番目のポートの TLV 切断機能をサポートしている場合でも、ホストの MAC アドレスはポートセキュリティ MAC アドレステーブルから削除されません。

  回避策：ポートセキュリティ MAC アドレステーブルからホストの MAC アドレスを削除するには、ポートのポートセキュリティを設定解除して再設定します。（CSCsr74097）

Cisco IOS リリース 12.2(50)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(50)SG の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- まれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 のパケット一致カウンタに、一致するパケットが表示されないことがあります。

```
clearwater# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、UDLD err-disable ステートになっているポート上で shutdown コマンドを入力してから no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD err-disable ステートのままです。同じポート上で shutdown コマンドを再入力してから no shutdown コマンドを入力すると、エラーメッセージは表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書の存在を確認します。
  - このような証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンでそれぞれ個別に生成されます。そのため、証明書は異なったものになります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- Cisco IOS 12.2（31）SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェア リリースの場合と同様に動作しないことがあります。

これは、12.2(31)SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2(31)SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

QueueID	以前の QueueName	新しい QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<未使用のキュー>	control-packet
11	<未使用のキュー>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

回避策:12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを使用します。

  回避策:ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  これは、次の理由で発生する場合があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - これは、スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを実行した場合も同様です。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策:

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバード ポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィックパフォーマンスを測定する場合、qos account layer2 encapsulation を設定していても、ポリサーにより 802.1Q タグを構成する 4 バイトが除外されます。

  回避策:ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に「a-」が追加されます。

  これはパフォーマンスには影響しません。

  回避策:no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG 以降のイメージへの ISSU アップグレード中に、次のエラーメッセージが表示されます。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- 3000 以上の VLAN ID でトラフィックが送信されると、障害により発生するコンバージェンス タイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- リロード後に、IP アンナンバード コンフィギュレーションが失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- SSO モード時に、同じチャネル番号を持つアクティブ スーパバイザ エンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイ ポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後、ポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- インターフェイスで ip source binding を静的に設定し、そのインターフェイスが存在するラインカードを削除しても、エントリは実行コンフィギュレーションから削除されません。

  回避策：ラインカードを削除する前に、ラインカードのいずれかのインターフェイスで静的に設定された ip source binding エントリを削除します。（CSCsv54529）

- EtherChannel（少なくとも 2 つのインターフェイス）に OFM を設定する場合、チャネルに参加した最初のメンバーをシャットダウンまたは削除すると、CFM ネイバーが失われます。

  回避策：EXEC モードで clear ethernet cfm errors コマンドを使用してエラーをクリアします。（CSCsv43819）

- PVLAN 独立トランクがスイッチで設定され、ネイティブ VLAN が独立トランクポートに割り当てられていない場合は、sw private-vlan trunk native vlan コマンドを使用してネイティブ VLAN を割り当てる必要があります。

  回避策：PVLAN 独立トランクのネイティブ VLAN を設定します。（CSCsv38137）

- ip multicast helper-map コマンドを設定すると、スタンバイ スーパバイザ エンジンで障害が発生します。

  この問題は、VRF が設定されたインターフェイスでのみ発生します。

  回避策：ありません。（CSCsr69187）

- 12.2(50)SG を実行している Catalyst 4500 スイッチで、アクセス VLAN が削除され、802.1x マルチ認証で設定されたポートで復元されると、アクセス VLAN の復元後も、スパニングツリーは Disabled 状態のままなので、許可された 802.1X クライアントはトラフィックを通過させることができません。

  この問題は、802.1X クライアントがマルチ認証ポートで許可されている場合に発生します。アクセス VLAN が削除されてから復元されると、クライアントは再認証されますが、アクセス VLAN のスパニングツリーの状態は Disabled のままになります。

  回避策：インターフェイスをシャットダウンしてから再度開きます。

  （CSCso50921）

- Cisco IOS リリース12.2(50)SG を実行しているスイッチでは、マルチ認証ホストモードの PVLAN で許可されたサプリカントは、PVLAN が削除されても Uauthorized 状態に移行しません。

  この問題は、ポートに PVLAN および 802.1X マルチ認証が設定されている場合にのみ発生します。

  回避策：インターフェイスをシャットダウンしてから再度開きます。（CSCsr58573）

- インターフェイスを削除して再作成すると、タッキングプロセスはそのステートトラックを追跡できません。

  回避策：新しく作成されたインターフェイスでトラッキングを再設定します。（CSCsr66876）

- スイッチが snmp mib target list vrf コマンドを受け入れません。VRF が DUT に存在する場合でも、このコマンドは拒否されます。

  回避策：ありません。（CSCsr95941）

- ping が、ポスチャ検証の前に実行されません。

  回避策：permit icmp コマンドを使用して、インターフェイスにID ポリシーを再適用します。（CSCsu03507）

- PVLAN 独立ポートが、マルチキャスト送信元として機能するルータに接続され、IGMP スヌーピングを有効にすると、独立ポートに接続されたルータは PIM ネイバーとして表示されます。

  回避策：次のいずれかの操作を実行します。

  - ルータを PVLAN 独立ポートに接続しないでください。
  - IGMP スヌーピングを無効にします（グローバルまたは VLAN のいずれか）。
  - PVLAN 独立ポートに接続されたルータをマルチキャスト送信元として使用しないでください。

  （CSCsu39009）

- 802.1X マルチドメイン認証（MDA）およびゲスト VLAN が設定されたスイッチポートがハブ経由で非 802.1X サプリカント PC に接続されている場合、ポートはゲスト VLAN にフォールバックします。その後、ゲスト VLAN でスタックし、ハブに接続されている別の 802.1X サプリカント PC からのすべての EAPOL トラフィックを無視します。

  回避策：ありません。（CSCsu42775）

- VTP データベースは無差別トランクポートを通じて伝達されません。無差別トランクのみが設定されている場合、VTP ドメイン内の他のスイッチで VLAN の更新は表示されません。

  回避策：VTP データベース伝播の場合、ISL/dot1q トランクポートを設定します。（CSCsu43445）

- SNMP で expExpressionTable の行を削除し、同時に expExpressionEntryStatus を 6 に設定すると、スイッチがクラッシュします。

- debug management expression evaluator コマンドを有効にすると、SNMP を介して expExpressionTable 行を破棄した後にスイッチがリロードすることがあります。

  回避策：上記の debug コマンドを削除します。（CSCsu67323）

- dot1x でポートセキュリティを設定すると、Cisco IOS リリース 12.2(50)SG へのアップグレード中に ISSU runversion を実行した後、ポートセキュリティ MAC アドレステーブルのセキュアダイナミック MAC アドレスが同期しません。

  回避策：なし（CSCsu67388）

- 802.1X が単方向制御ポートとして設定されている場合、出力トラフィックが許可されないことがあります。

  回避策：次のいずれかの操作を実行します。

  - 802.1X ポートで spanning-tree portfast、authentication control-direction の順に入力します。
  - 802.1X ポートで shut、no shut の順に入力します。

  （CSCsv05205）

- 2 つのスイッチに 2 つの MST インスタンスが設定されている場合、MST 情報が 2 番目のスイッチのスタンバイに正しく同期されません。

  回避策：ありません。（CSCsv07019）

- 特定の Cisco Trusted Security（CTS）SXP 接続設定では、各 SXP 接続に最適な送信元 IP が一貫して選択されない場合があります。

  複数のレイヤ 3 インターフェイスを持つスイッチで、送信元 IP アドレスを指定せずに CTS SXP 接続が設定され、ボックスにデフォルトの SXP 送信元 IP アドレスが設定されていない場合、異なる SXP 接続が接続ごとに異なる送信元 IP アドレスを取得することがあります。

  回避策：次のいずれかの操作を実行します。

  - スイッチにアクティブなレイヤ 3 インターフェイスが 1 つだけ存在することを確認します。
  - あいまいさをなくすために、各 SXP 接続設定で IP アドレスの送信元を指定します。
  - 送信元 IP アドレスのない SXP 接続がこの送信元 IP アドレスを使用するように、デフォルトの SXP 送信元 IP アドレスを設定します。

  （CSCsv28348）

- IP ルータオプションは、IGMP バージョン 2 では動作しない可能性があります。

  回避策：ありません。（CSCsv42869）

- スタンバイ スーパバイザ エンジンの起動中に IGMP スヌーピングが設定されたポートを含むラインカードを取り外すと、アクティブ スーパバイザ エンジンは、一括同期の一部としてこの設定をスタンバイ スーパバイザ エンジンに同期しません。ラインカードを再度取り付けると、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンの設定が一致しなくなります。

  回避策：次のいずれかの操作を実行します。

  - ラインカードを取り付けた状態で、スタンバイスイッチを再度リロードします。
  - コマンドを削除および追加して、アクティブに戻します。スタンバイがこの変更を取得します。

  （CSCsv44866）

- issu loadversion コマンドを入力すると、冗長シャーシで「Bad parent VLAN ID」エラーメッセージを伴うトレースバックが表示されることがあります。

  回避策：ありません。（CSCsv59929）

- スイッチポートのモードが CFM サポートモードから CFM 非サポートモードに変更されると、CFM は自動的に無効になります。モードがサポートモードに戻ると、CFM の状態は Disabled のままになります。この問題は、インターフェイスの実行コンフィギュレーションで確認できます。たとえば、Cisco IOS リリース 12.2(44)SG から 12.2(46)SG への ISSU runversion では、一括同期の失敗が表示されます。

  CFM は、デフォルトのスイッチポートモードでサポートされます。CFM は、PVLAN アクセスモード（無差別、隔離、およびコミュニティホストポート）および dot1q-tunnel モードではサポートされていません。他のすべてのスイッチポートモードでサポートされます。

  回避策：ethernet cfm enable コマンドを使用して、インターフェイスで CFM を有効にします。（CSCsv67507）

- VLAN ロードバランシングが進行中で、異なるブロッキングポートを反映するように VLAN ロードバランシングを再設定する場合、手動プリエンプションは発生しません。

  回避策：次の手順を実行して、異なる設定で VLAN ロードバランシングを再設定します。

  a. 目的の REP ポートで VLAN ロードバランシング設定を再設定します。

  b. セグメント内の 1 つの REP ポートで shut コマンドを使用すると、そのセグメントで障害が発生します。

  c. 同じポートで no-shut を使用して、1 つの ALT ポートで通常の REP トポロジを復元します。

  d. プライマリエッジポートで手動プリエンプションを呼び出して、新しい設定で VLAN ロードバランシングを取得します。

  （CSCsv69853）

- X2 スロットの OneX コンバータから SFP+ を取り外すと、システムがこのアクションを認識するまでに約 45 秒かかります。この間、すべてのコマンドで SFP+ がまだ存在していることが示されます。別のポートに SFP+ を再挿入するか、同じポートに別の SFP+ を挿入すると、Duplicate Seeprom エラーメッセージが表示されることがあります。

  回避策：SFP+ が取り外されたことを示すログメッセージが表示されたら、次のいずれかを実行します。

  – 該当ポートに任意のコマンドを入力します。

  – 該当ポートに SFP+ を挿入します。

  – 取り外した SFP+ を他のポートに再度挿入します。

  （CSCsv90044）

- ブートフラッシュ内のイメージで verify コマンドを発行すると、次のシステムメッセージが表示されることがあります。

```
Catalyst-4507#verify bootflash:cat4500-entservices-mz.122-37.SG1
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Verifying file integrity of bootflash:cat4500-entservices-mz.122-37.SG1
Embedded hash not found in file bootflash:cat4500-entservices-mz.122-37.SG1.
File system hash verification successful.
Catalyst-4507#
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

```
01:09:25: %SIGNATURE-4-NOT_PRESENT: %WARNING: Signature not found in file
bootflash:cat4500-entservices-mz.122-37.SG1.
```

この症状は、12.2(40)SG 以降を実行している場合に発生することがあります。

回避策：<CmdBold>verify /md5<noCmdBold> コマンドを使用して、イメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。

（CSCsu36320）

- Supervisor Engine 6-E および Catalyst 4900M では、ブートフラッシュイメージで /md5 パラメータを指定せずに verify コマンドを入力すると、出力は表示されません。

  回避策：verify / md5 コマンドを使用してイメージの整合性を確認します。結果の MD5 シグニチャを、そのイメージの CCO にポストされたシグニチャと比較します。（CSCsu37068）

- HTML ページで参照されているグラフィックは、Web 認証中にユーザのブラウザに表示されない場合があります。

  回避策：グラフィックを HTML ファイル（最大 256 KB）に埋め込みます（RFC 2397 に準拠）。

  次のブラウザは RFC 2397 をサポートしています。

  - Internet Explorer 8
  - Mozilla Firefox
  - Safari

  （CSCsu37834）

- 権限レベル 15 のユーザが、callback または callback-dialstring 属性を使用してログオンすると、ルータがクラッシュすることがあります。

  この問題は、Cisco IOS リリース 12.2(50)SG を実行しているすべての Catalyst 4500 または 4900 シャーシで発生します。この問題は、次の条件を満たしている場合に発生します。

  - ルータが AAA 認証および認可を使用して設定されている。
  - AAA サーバ が CiscoSecure ACS 2.4 を実行している。
  - callback または callback-dialstring 属性が、ユーザの AAA サーバで設定されている。

  回避策：ユーザの callback または callback-dialstring 属性を設定しないでください。TACACS+ プロファイルで callback-dialstring 属性を使用する場合は、NULL 値が設定されていないことを確認します。（CSCei62358）

- Cisco IOS リリース 12.2(50)SG と 12.2(44)SG または 12.2(46)SG 間で ISSU のアップグレードまたはダウングレードを試みると、スイッチにトレースバックが表示されます。

  回避策：ありません。（CSCsw32519）

- ポスチャ検証が成功した後、global RADIUS コマンドと IP device tracking コマンドの設定を解除すると、次の無害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。

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

  これは、実行中のクラシックまたは E シリーズの Catalyst 4500 スーパバイザエンジンに適用されます。
  Cisco IOS Release 12.2(50)SG

  回避策：ありません。（CSCsw14005）

- channel-group x または channel-protocol モードで、fa1 管理インターフェイスに対して lacp または pagp コマンドを入力すると、アクティブ スーパバイザ エンジンがリロードされます。

  ポートチャネル機能は、管理インターフェイスではサポートされていません。

  これは、設定エラーです。

  回避策：ありません。（CSCsv91302）

- セキュアポートで認証されたクライアントまたはホストにダイナミック ポリシー インストールを使用する場合、permit ip any any コマンドがクライアントのダイナミックポリシーとして指定されている場合でも、クライアントからのトラフィックは許可されません。

  この状況、次の条件が満たされた場合にのみ発生します。

  - authentication host-mode multi-host コマンドを使用して、ポートでマルチホストモードを設定している。
  - デフォルト ACL（IP アクセスリスト）が、deny ip any any を指定するインターフェイスで設定されている。
  - クライアントのダイナミックポリシー許可で、permit ip any any を指定している。

  回避策：ありません。

  CSCsz63739

Supervisor Engine 6-E ではサポートされていません。

- CFM を入力インターフェイス上およびグローバルにイネーブルにすると、インターフェイスで受信した CFM パケットが HW コントロール プレーン ポリシング（HW Control Plane Policing）でポリシングされません。

  回避策：ありません。（CSCso93282）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

- コントロール プレーン ポリシングを使用する場合、コントロールプレーンクラス（**macro global apply system-cpp** コマンドによって自動的に作成され、定義済み ACL を使用してトラフィックを照合するクラス）がパケット数とバイト数を増加させます。これは、両方のカウンタがゼロ以外であることを意味します。

  代わりに、データプレーンクラス（ユーザが記述した ACL によって手動で設定）はバイトカウンタを増加させますが、パケット数は増加しません（0 のまま）。

  回避策：ありません。CSCsw16557

Supervisor Engine 6-E に固有の問題

- 必要な QoS 操作を適用するためのソフトウェア QoS が .1Q パケットと正しく一致しません。

  回避策：ありません。

  Cisco IOS Release 12.2（40）SG リリースでは、ソフトウェア QoS ルックアップを行う 1Q パケット処理はサポートされていません。（CSCsk66449）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth/shape fixes the issue などのキューイング パラメータをいくつか変更して再設定してください。（CSCsk62457）

- E シリーズ スイッチでファン トレイの障害またはスーパバイザでの危険温度のいずれかが発生すると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を特定します。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、原因はファントレイの障害です。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザの危険温度が障害のしきい値を超えたことが原因です。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。さらに、物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG で、カードまたは X2 を挿入すると、リロード後または電源の再投入後に CTC エラーが発生します。

  回避策：X2 を再挿入します。（CSCsk43618）

- 出力 QoS ポリシーが設定されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキング アクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の COS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された COS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 に説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能がイネーブルになっている場合、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを特定できます。

信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの COS/DSCP フィールドが強制的にゼロになります。

インターフェイス上に存在する QoS ポリシーは、この COS/DSCP の値を分類に使用します。そのため、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。（CSCsh72408）

- シングルレートポリサーに burst が明示的に設定されていない場合、show policy-map コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、show policy-map name を入力すると、無条件のマーキングアクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシ タイプが「Unknown」と表示されます。IOS を起動した後、シャーシ タイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- ポリシーマップで「class-default」クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。サイズの範囲は、queue-limit コマンドにより表示されます。（CSCso06422）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から最新のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、ACTIVE スーパバイザ エンジンが IOS で、STANDBY スーパバイザ エンジンが ROMMON でそれぞれ実行され、STANDBY の ROMMON がバージョン 0.34 または最新バージョンにアップグレードされたときに、冗長スイッチで発生します。アップグレード処理により STANDBY スーパバイザ エンジンのアップリンクがダウンしますが、ACTIVE スーパバイザ エンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - redundancy reload shelf コマンドで、両方のスーパバイザをリロードします。
  - STANDBY スーパバイザ エンジンをしばらくの間シャーシから抜き出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズ フレームがスイッチ ポートに送信され、フロー制御の受信設定が 10G ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力でシステム内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策：ありません。

  （CSCso96660）

- VLAN ロード バランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートのあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

  回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no-shut コマンドを入力します。（CSCsq75342）

- FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannel が定義されていると、リブート後に FlexLink の設定が適用されないことがあります。

  回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

  回避策：ありません。（CSCsq99468）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

  回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、show ethernet cfm maintenance-points local コマンドによって IFM CC ステータスが Inactive と表示されます。VLAN を割り当てても、CC ステータスは Inactive のままです。

  この問題は、VLAN を割り当てずに IFM を設定した後で、同じ VLAN を割り当てたときにのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

- Catalyst 4900M スイッチでは、WS-X4908-10GE カードを CVR-X2-SFP TwinGig コンバータとともに使用すると、ギガポートはリモート障害を送信するピアデバイスにリンクアップされません。show int status | inc gi x/y コマンドは、notconnect を示します。

  同様の動作は、Supervisor Engine 6-E アップリンクおよび WS-X4706-10GE ラインカードでも確認されています。

この動作は、ピアデバイスがリモート障害を送信するときに、Cisco IOS リリース 12.2(50)SG から 12.2(50)SG3 で確認されています。

回避策: 両端で自動ネゴシエーションを無効にします。

（CSCta02425）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

Cisco IOS リリース 12.2(50)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(50)SG で解決済みの警告について説明します。

- マルチドメイン認証（MDA）で設定されたポート上でデータ デバイスが（dot1x または MAB を介して）承認された後、アクセス VLAN を変更すると、デバイスがポートに接続されていない場合でも、このデバイスのトラフィックが失われます。ポートに接続されている音声デバイスのトラフィックには影響しません。

  回避策：ポート上のアクセス VLAN を変更後、インターフェイス上で shutdown コマンドを入力してから no shutdown コマンドを入力します。（CSCsk45969）

- IPv4 ルートが RTR2 から IPv6 ピアリングを介して RTR3 にアドバタイズされると、RTR2 の IPv6 アドレスの最初の 32 ビットが IPv4 アドレスに変換されます。この IPv4 アドレスは、RTR3 に対するネクストホップ アドレスとしてアドバタイズされます。このアドレスが Martian アドレスになると、RTR3 は BGP 更新メッセージを無視するため、IPv4 ルートが認識されません。

  RTR3 でインバウンドルートマップを設定して RTR2 がアドバタイズしたネクストホップを上書きしても、BGP 更新メッセージは無視されるため、この問題は回避できません。

  回避策：RTR2 でアウトバウンドルートマップを設定し、暗示的にプロトコルで取得するのではなく、明示的に IPv4 ネクストホップアドレスを設定します。（CSCsk65139）

- CFM では、サービスインスタンス/MEP に関連付けられた VLAN が、ステータスが down になっているインターフェイス上で Inward Facing MEP（IFM）が設定された後に割り当てられると、show ethernet CFM maintenance local コマンドの出力でも IFM CC ステータスは inactive のままになります。また、CFM リモート ネイバーは表示されません。

このような動作は、IFM を設定した後に VLAN が割り当てられたときにのみ見られます。

回避策：no ethernet cfm mep level mpid vlan コマンドで設定を解除してから、VLAN が割り当てられた後にポート上で ethernet cfm mep level mpid vlan コマンドを実行して IFM を再設定します。IFM の C ステータスが Active であることを show ethernet cfm maintenance-points local コマンドで確認します。（CSCsm85460）

- PC が、MDA、MAC 認証バイパス（MAB）およびポート セキュリティで設定したポートに接続された 802.1X 対応電話を経由してトラフィックを送信し続けた場合、ポートで電話が完全に認証される前にポートが PC からのトラフィックを観察すると、802.1X セキュリティの競合が発生することがあります。

  回避策：電話の背後にある PC を接続する前に、電話を認証します。（CSCsq92724）

- CFM をグローバルにディセーブルし、CFM 設定を使用してスイッチをリロードした後、CFM をグローバルにイネーブルにすると、CFM が非アクティブになり、CFM ネイバーが損失します。

  回避策：次のいずれかの操作を実行します。

  – CFM 設定を再適用します。スイッチのすべてのインターフェイスで設定した MEP を削除して再度追加します。

  – CFM サービス VLAN の割り当てを解除します。その後、再度割り当てます。

  （CSCsq90598）

- netflow aggregation for origin-as が設定されている場合、show ip cache verbose flow コマンドで、AS パス情報が表示されません。

  回避策：ありません。（CSCsq63572）

- ポリサー、シェイプ、またはシェイプ値がポリシーのリンク帯域幅のパーセンテージとして指定され、ポリシーが適用されているインターフェイスが、speed 10/100/1000 コマンドで特定の速度に強制される場合、適用されたポリサー、シェイプ、または帯域幅の値は、強制された新しい速度に対応しない場合があります。

  サービスポリシーは、パーセンテージのポリサー、シェイプ、またはシェイプ値で設定し、リンク速度は強制的に特定の値にする必要があります。次に例を示します。

```
Policy-map p1
    class-map c1
       police rate percent 10
```

  回避策：speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー、シェイプ、またはシェイプ値を絶対値で指定します。次に例を示します。

```
Policy-map p1
   class-map c1
     police rate 10 mbps
```

  （CSCsk56877）

- スイッチの起動時には、「Module M linecard watchdog has expired」というメッセージが表示されます。

  ハードウェアの電源投入方法によって、ラインカードの起動時にメッセージが表示されることがあります。

  回避策：ラインカードをリセットします。（CSCsq21215）

- システムをリロードした後、デフォルト以外の速度を持つインターフェイス上のパーセンテージ ベースの入力ポリサーが動作しません。

  回避策：インターフェイス上のサービスポリシーを削除して再適用します。

  （CSCsq79073）

- ポリシーでポリサー値またはシェイプ値がリンク帯域幅に対するパーセンテージとして指定されており、これらの値が割り当てられたインターフェイスが speed 10/100/1000 コマンドを使用して特定の速度になるよう強制されている場合、適用されたポリサー値またはシェイプ値が、強制された新しい速度に対応する場合があります。

  例:

  ```
  Policy-map p1
         class-map c1
            police rate percent 10
  ```

  回避策:speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー値またはシェイプ値を絶対値で指定します。

  例:

  ```
  Policy-map p1
        class-map c1
          police rate 10 mbps
  ```

  (CSCsk56877)

- パーセントベースの操作を含むポリシーマップがチャネルメンバーポートと別のスタンドアロンポート間で共有されると、チャネルがバンドル解除および再バンドルされ、スタンドアロンポートが レイヤ 2 からレイヤ 3 またはレイヤ 3 からレイヤ 2 に変更されます。

  回避策:ありません。(CSCso54096)

- 自動 QoS が有効になっているインターフェイスでデフォルトのインターフェイス操作を実行すると、エラーメッセージが表示され、自動 QoS 設定が失われます。たとえば、次の一連の操作により設定が失われます。

  ```
  config-if# auto qos voip cisco-phone
  config# default interface interface-name
  ```

  回避策:default interface コマンドを次のように置き換えます。

  ```
  config# interface interface-number
  config-if# switchport
  ```

  (CSCsq47116)

- REP および VLAN ロード バランシングが設定されたブロック VLAN セットを変更した後、手動プリエンプションが許可されません。

  回避策:物理的にケーブルを引き抜くかインターフェイスをシャットダウンすることで、意図的に 2 つのスイッチ間のリンクを失敗させます。その後、リンクを元の状態に戻します。この後、遅延したプリエンプションが続きます。(CSCsm91997)

- SSO モードで service-policies メンバーを port-channel メンバーに追加、削除、または変更すると、次のトレースバックがアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンの両方に表示されます。

  ```
  03:50:00: %SM-4-BADEVENT: STANDBY:Event 'bundle_sync' is invalid for the current state
  'COLLECTING_DISTRIBUTING': lacp_mux Gi7/7 - mux
  -Traceback= 10B97B80 10B98294 10189F78 1038FE0C 103944FC 1055E420 1055C4B8 10A2C28C
  10A2AE88 10A2A4B0 10A27A18 10A225E8 1059E824 10595AAC
  ```

  回避策:ありません。(CSCso23786)

- IPv6 エントリが CAM でアクティブとなり、CPU が IPv6 パケットを受信します。

  回避策:すべての汎用 QOS ポリシーの設定をシステムから解除します。match any 属性を持つ QoS ポリシーにより、IPv6 エントリがアクティブになります。スイッチが純粋なレイヤ 2 デバイスである場合、汎用プロトコル ファミリの属性を削除して、プロトコル ファミリに絞り込みます。

  (CSCsq84796)

- スイッチで実行されているソフトウェアのバージョンを Cisco IOS リリース 12.2(46)SG に変更した場合、または 12.2(46)SG から変更した場合、ifindex の永続性が機能しません。show snmp mib ifmib ifindex コマンドを実行すると、インターフェイス名が正しく表示されないことがあります。

回避策:

デュアル SUP アップグレード(ISSU):12.2(46)SG とその他のリリース間

何も変更せずに ISSU プロセスを実行します。アップグレード中は、次の項目に従ってください。

1. write memory または同等のコマンドを使用して、構成ファイルを NVRAM に明示的に保存しないでください。issu commitversion コマンドは、設定を NVRAM に保存し、NVRAM に保存されている ifIndices を復元します。
2. アップグレードプロセス中に issu abortversion コマンドを入力しないでください。

シングル スーパバイザ アップグレード:Cisco IOS リリース 12.2(44)SG1 以前から 12.2(46)SG へのアップグレード、および 12.2(46)SG から 12.2(44)SG1 以前へのダウングレード

前の項で説明したソフトウェアバージョンの場合、ソフトウェアバージョンが version-a から version-b に変更され、スイッチが現在 version-a を実行していることを確認します。

次の操作を行ってください。

1. version-a の実行中に、ifIndices を含むファイルを del nvram:ifIndex-table.gz コマンドを使用して削除します。

注 ステップ 1 の後に、write nvram または同様のコマンドを使用して構成ファイルの保存を開始しないでください。

2. リロード後に version-b を実行するようにスイッチをリロードします。
3. スイッチが version-b を実行している間に、write memory コマンドを使用して設定を保存し、ifIndices を含むファイルを再生成します。

シングル スーパバイザ アップグレード:Cisco IOS リリース 12.2(46)SG から 12.2(50)SG 以降へのアップグレード

1. 12.2(46)SG の実行中に、ブートフラッシュ内のファイルに設定を保存します。

```
Switch# copy running-config bootflash:oldconfig
```

2. NVRAM に保存されている設定を削除します。

```
Switch# erase nvram:
```

3. ifIndices を含むファイルを削除します。

```
Switch# del nvram:ifIndex-table.gz
```

4. スイッチをリロードし、リロード後に、Cisco IOS リリース 12.2(44)SG1 または以前のリリースを実行できるようにします。
5. スイッチが Cisco IOS リリース 12.2(44)SG1 を実行している間に、次の手順を実行して ifIndices を再生成します。
   - ifIndex 永続化機能を有効にします。
   - write memory コマンドを入力して、生成された ifIndices を NVRAM に保存します。
6. Cisco IOS リリース 12.2(50)SG または以降のリリースにアップグレードします。スイッチがリリース 12.2(50)SG 以降を実行している場合は、ステップ 1 で保存した設定を、copy bootflash:oldconfig running-config コマンドを使用して、ブートフラッシュからロードします。

7. write memory コマンドを使用して、設定を NVRAM に保存します。

（CSCsv85746）

- Catalyst 4500 シリーズ スイッチを Supervisor Engine 6-E とともに使用し、インターフェイスに出力サービスポリシーが設定されている場合、同じ出力サービスポリシーが適用されている別のインターフェイスで shut/no shut を入力すると、キューがフル状態のために出力がドロップされます。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、および 12.2(46)SG で発生します。

  この問題は、12.2(50)SG で解決されています。

  回避策：qos autoqos マクロを使用しないでください。

  ポリシーマップが複数のターゲットで共有されている場合は、パーセンテージベースのアクションを使用しないでください。ポリシング、シェーピング、および帯域幅アクションでは、絶対値を使用する必要があります。そのためには、スイッチでサポートされる 4 つのインターフェイス速度（10M、100M、1G、および 10G）ごとに異なるポリシーマップが必要です。そのため、パーセンテージベースのアクションで単一のポリシーマップを有効にするのではなく、4 つの異なるポリシーマップを作成する必要があります。これは、サービスポリシーの方向に関係なく、すべての共有ポリシーマップに適用されます。

  （CSCsr12142）

- Cisco IOS ソフトウェアの複数の機能には、攻撃者が該当デバイスにサービス妨害（DoS）状態を引き起こす可能性のある脆弱性が存在します。特別に細工された TCP パケットのシーケンスにより、脆弱なデバイスがリロードされる可能性があります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  このアドバイザリの回避策セクションで、いくつかの緩和戦略について説明します。

  このアドバイザリは、次の URL に掲載されています。
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

  CSCsr29468

- 症状：Cisco IOS ソフトウェア内の複数の機能が、巧妙に細工された UDP パケットの脆弱性の影響を受けます。影響を受ける機能のいずれかが有効になっている場合、攻撃が成功すると、着信インターフェイスで入力キューがブロックされます。デバイス宛ての巧妙に細工された UDP パケットのみがインターフェイスをブロックする可能性があり、中継トラフィックはインターフェイスをブロックしません。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  この脆弱性を軽減する回避策は、アドバイザリの回避策セクションに記載されています。このアドバイザリは次のリンクに掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

  CSCsk64158

- 症状：SSLVPN サービスが新しい SSLVPN 接続を受け入れなくなります。

  条件：SSLVPN サービス用の新しい TCP 接続の処理に脆弱性があるため、SSLVPN 用に設定されたデバイスが新しい SSLVPN 接続の受け入れを停止する場合があります。「debug ip tcp transactions」が有効になっており、この脆弱性がトリガーされると、接続キューの制限に達したデバッグメッセージが表示されます。この脆弱性は、2 つの個別の Cisco Bug ID（CSCso04657 と CSCsg00102）で文書化されており、どちらも完全な修正のために必要です。

  CSCso04657

- IPv6 MLD と関連したコンフィギュレーションがない場合も、IPv6 MLD エントリが、アクティブになります。

  回避策：すべての汎用 QOS ポリシーの設定をシステムから解除します。（CSCsq84853）

- Cisco IOS Release 12.2（47）SG を実行している Catalyst 4500 シリーズ スイッチでは、AAA サーバに接続するスイッチ ポートをアクセス VLAN 上で SVI をイネーブルにしたレイヤ 2 インターフェイスとして設定している場合、802.1X をイネーブルにした電話が MDA ポートで認証しようとすると、ポート セキュリティとスパニングツリー PortFast で設定したすべての MDA ポートで 802.1X セキュリティ違反が発生する場合があります。

  回避策：

  a. ポートのポート セキュリティをディセーブルにするか、スイッチを標準レイヤ 3 ポートで AAA サーバに接続します。

  b. spanning-tree portfast をディセーブルにします。

  （CSCsq62342）

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- 冗長スイッチが SSO モードであるか、または ISSU アップグレード/ダウングレード中の場合に、スタンバイスーパバイザが IOS ソフトウェアリリース 12.2(44)SG または 12.2(46)SG を実行している場合、サービスポリシーが付加されたインターフェイスで auto qos voip trust コマンドを入力すると、スタンバイ スーパバイザ エンジンがリブートします。

  回避策：インターフェイスからすべてのサービスポリシーを削除してから、auto qos voip trust コマンドを入力します。

  CSCsq37471

- 複数のシスコ製品は、Transmission Control Protocol（TCP）接続の状態が操作されるサービス妨害（DoS）の脆弱性の影響を受けます。攻撃者は TCP 接続の状態を操作することにより、TCP 接続を強制的に長時間、あるいは無限に存続させる可能性があります。十分な数の TCP 接続が強制的に長時間または無限に存続させられると、攻撃されたシステムのリソースが消費され、新しい TCP 接続が受け入れられなくなる可能性があります。場合によっては、正常なシステム動作を回復するためにシステムのリブートが必要になることもあります。攻撃者がこれらの脆弱性をエクスプロイトするには、脆弱なシステム上で TCP 3 ウェイハンドシェイクを完了できる必要があります。

  これらの脆弱性に加えて、Cisco Nexus 5000 デバイスには、システムクラッシュを引き起こす可能性がある TCP DoS 脆弱性があります。この新たな脆弱性は、TCP 状態操作の脆弱性をテストした結果として発見されました。

  シスコは、Cisco Web サイトからダウンロードできる、これらの脆弱性に対処する無償のソフトウェアアップデートをリリースしました。これらの脆弱性を軽減する回避策はあります。

  このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24

  CSCsv04836

Cisco IOS Release 12.2(46)SG でオープンになっている警告

ここでは、Cisco IOS Release 12.2(46)SG でオープンになっている警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- まれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 のパケット照合カウンタに、一致するパケットが表示されないことがあります。

```
clearwater# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、UDLD err-disable ステートになっているポート上で shutdown コマンドを入力してから no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD err-disable ステートのままです。同じポート上で shutdown コマンドを再入力してから no shutdown コマンドを入力すると、エラーメッセージは表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書の存在を確認します。
  - このような証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。

– このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンでそれぞれ個別に生成されます。そのため、証明書は異なったものになります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

回避策：再接続します。（CSCsb11964）

- Cisco IOS 12.2（31）SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェア リリースの場合と同様に動作しないことがあります。

  これは、12.2（31）SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

QueueID	以前の QueueName	新しい QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<未使用のキュー>	control-packet
11	<未使用のキュー>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを使用します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  これは、次の理由で発生する場合があります。

  – パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。

  – これは、スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを実行した場合も同様です。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

回避策:

- Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバード ポートに送信する必要のあるパケットを投入しないでください。
- ホスト側で正しいデフォルト ゲートウェイを設定してください。(CSCse75660)

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィック パフォーマンスを測定する場合、qos account layer2 encapsulation を設定している場合でも、ポリサーにより 802.1Q タグを構成する 4 バイトが qos account layer2 encapsulation を設定していても、ポリサーにより 802.1Q タグを構成する 4 バイトが除外されます。

  回避策: ありません。(CSCsg58526)

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に「a-」が追加されます。

  これはパフォーマンスには影響しません。

  回避策: no shutdown コマンドを入力します。(CSCsg27395)

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策: 新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。(CSCse34693)

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG以降のイメージへのISSUアップグレード中に、次のエラーメッセージが表示されます。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策: ありません。このメッセージは情報メッセージです。(CSCsi60913)

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策: ありません。これは通知メッセージです。(CSCsi60898)

- Cisco IP Phone にサプリカントが付属している場合、MDA で設定し、電話およびサプリカントに接続された DUT ポートをリロードするときに、ポートがトラフィックを送信しません。電話は unknown ステートになります。

  電話がスタンド アロン デバイスの場合、この問題は見られません。

  回避策: Cisco IP 電話の電源を再投入します。(CSCsk81297)

- マルチドメイン認証(MDA)で設定されたポート上でデータ デバイスが(dot1x または MAB を介して)承認された後、アクセス VLAN を変更すると、デバイスがポートに接続されていない場合でも、このデバイスのトラフィックが失われます。ポートに接続されている音声デバイスのトラフィックには影響しません。

  回避策: ポート上のアクセス VLAN を変更後、インターフェイス上で shutdown コマンドを入力してから no shutdown コマンドを入力します。(CSCsk45969)

- 3000 以上の VLAN ID でトラフィックが送信されると、障害により発生するコンバージェンス タイミングが 225 ms を超えます。

回避策：ありません。（CSCsm30320）

- REP および VLAN ロードバランシングが設定されている一連のブロック VLAN を変更した後、手動プリエンプションが許可されません。

  回避策：物理的にケーブルを引き抜くかインターフェイスをシャットダウンすることで、2 つのスイッチ間のリンクを失敗させます。その後、リンクを元の状態に戻します。この後、遅延したプリエンプションが続きます。（CSCsm91997）

- PC が、MDA、MAC 認証バイパス（MAB）およびポート セキュリティで設定したポートに接続された 802.1X 対応電話を経由してトラフィックを送信し続けた場合、ポートで電話が完全に認証される前にポートが PC からのトラフィックを観察すると、802.1X セキュリティの競合が発生することがあります。

  回避策：電話の背後にある PC を接続する前に、電話を認証します。（CSCsq92724）

- リロード後に、IP アンナンバード コンフィギュレーションが失われます。

  回避策：次のいずれかの操作を実行します。

  - リロード後、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
  - **ip unnumbered** コマンドのターゲットとして、ループバック インターフェイスを使用します。
  - CLI 設定を変更して、起動時にルータ ポートが最初に作成されるようにします。

  （CSCsq63051）

- CFM をグローバルにディセーブルし、CFM 設定を使用してスイッチをリロードした後、CFM をグローバルにイネーブルにすると、CFM が非アクティブになり、CFM ネイバーが損失します。

  回避策：次のいずれかの操作を実行します。

  - CFM 設定を再適用します。スイッチのすべてのインターフェイスで設定した MEP を削除して再度追加します。
  - CFM サービス VLAN の割り当てを解除します。その後、再度割り当てます。

  （CSCsq90598）

- SSO モード時に、同じチャネル番号を持つアクティブ スーパバイザ エンジンでポートチャネルの作成、削除、再作成を行うと、スタンバイ ポートチャネルのステートが同期しなくなります。スイッチ オーバーした後に、次のメッセージが表示されます。

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  回避策：ポートチャネルがフラップし始めたら、ポートチャネルで **shut** および **no shut** を入力します。最初のスイッチオーバー後、ポートチャネルを削除してから、新しいチャネルを作成します。（CSCsr00333）

- ISSU 対応の冗長スーパバイザエンジンの場合、Cisco IOS リリース 12.2(44)SG 以前から 12.2(46)SG 以降にアップグレードすると、ifindex の永続性が機能しません。The show snmp mib ifmib ifindex コマンドでインターフェイス名が正しく表示されないことがあります。

  回避策：ISSU 実行中に issu commitversion を使用して設定を更新します。これは通常のプロセスです。write nvram を使用して設定を明示的に保存しないでください。（CSCsv85746）

- スイッチで実行されているソフトウェアのバージョンを Cisco IOS リリース 12.2(46)SG に変更した場合、または 12.2(46)SG から変更した場合、ifindex の永続性が機能しません。show snmp mib ifmib ifindex コマンドを実行すると、インターフェイス名が正しく表示されないことがあります。

回避策：

デュアル SUP アップグレード（ISSU）：12.2(46)SG とその他のリリース間

何も変更せずに ISSU プロセスを実行します。アップグレード中は、次の項目に従ってください。

1. write memory または同等のコマンドを使用して、構成ファイルを NVRAM に明示的に保存しないでください。issu commitversion コマンドは、設定を NVRAM に保存し、NVRAM に保存されている ifIndices を復元します。
2. アップグレードプロセス中に issu abortversion コマンドを入力しないでください。

シングル スーパバイザ アップグレード：Cisco IOS リリース 12.2(44)SG1 以前から 12.2(46)SG へのアップグレード、および 12.2(46)SG から 12.2(44)SG1 以前へのダウングレード

前の項で説明したソフトウェアバージョンの場合、ソフトウェアバージョンがバージョン a からバージョン b に変更され、スイッチが現在バージョン a を実行していることを確認します。

次の操作を行ってください。

1. バージョン a の実行中に、ifIndices を含むファイルを del nvram:ifIndex-table.gz コマンドを使用して削除します。

注 ステップ 1 の後に、write nvram または同様のコマンドを使用して構成ファイルの保存を開始しないでください。

2. リロード後に version-b を実行するようにスイッチをリロードします。
3. スイッチが version-b を実行している間に、write memory コマンドを使用して設定を保存し、ifIndicesを 含むファイルを再生成します。

シングル スーパバイザ アップグレード：Cisco IOS リリース 12.2(46)SG から 12.2(50)SG 以降へのアップグレード

1. 12.2(46)SG の実行中に、ブートフラッシュ内のファイルに設定を保存します。

```
Switch# copy running-config bootflash:oldconfig
```

2. NVRAM に保存されている設定を削除します。

```
Switch# erase nvram:
```

3. ifIndices を含むファイルを削除します。

```
Switch# del nvram:ifIndex-table.gz
```

4. スイッチをリロードし、リロード後に、Cisco IOS リリース 12.2(44)SG1 または以前のリリースを実行できるようにします。
5. スイッチが Cisco IOS リリース 12.2(44)SG1 を実行している間に、次の手順を実行して ifIndices を再生成します。

– ifIndex 永続化機能を有効にします。
– write memory コマンドを入力して、生成された ifIndices を NVRAM に保存します。

6. Cisco IOS リリース 12.2(50)SG または以降のリリースにアップグレードします。スイッチがリリース 12.2(50)SG 以降を実行している場合は、ステップ 1 で保存した設定を、copy bootflash:oldconfig running-config コマンドを使用して、ブートフラッシュからロードします。
7. write memory コマンドを使用して、設定を NVRAM に保存します。

（CSCsv85746）

Supervisor Engine 6-E ではサポートされていません。

- CFM を入力インターフェイス上およびグローバルにイネーブルにすると、インターフェイスで受信した CFM パケットが HW コントロール プレーン ポリシング（HW Control Plane Policing）でポリシングされません。

  回避策：ありません。（CSCso93282）

- netflow aggregation for origin-as が設定されている場合、show ip cache verbose flow コマンドで、AS パス情報が表示されません。

  回避策：ありません。（CSCsq63572）

- ISSU のアップグレードまたは v122_31_sg_throttle から v122_46_sg_throttle へのダウングレード中に、次のエラーメッセージがアクティブ スーパバイザ エンジンのコンソールに表示されます。

  ```
  Mar 6 03:28:29.140 EST: %COMMON_FIB-3-FIBHWIDBINCONS: An internal
  software error occurred. Null0 linked to wrong hwidb Null0
  ```

  回避策：ありません。（CSCso68331）

- コントロール プレーン ポリシングを使用する場合、コントロールプレーンクラス（**macro global apply system-cpp** コマンドによって自動的に作成され、定義済み ACL を使用してトラフィックを照合するクラス）がパケット数とバイト数を増加させます。これは、両方のカウンタがゼロ以外であることを意味します。

  代わりに、データプレーンクラス（ユーザが記述した ACL によって手動で設定）はバイトカウンタを増加させますが、パケット数は増加しません（0 のまま）。

  回避策：ありません。CSCsw16557

Supervisor Engine 6-E に固有の問題

- 必要な QoS 操作を適用するためのソフトウェア QoS が .1Q パケットと正しく一致しません。

  回避策：ありません。

  Cisco IOS Release 12.2（40）SG リリースでは、ソフトウェア QoS ルックアップを行う 1Q パケット処理はサポートされていません。（CSCsk66449）

- ポリサー、シェイプ、またはシェイプ値がポリシーのリンク帯域幅のパーセンテージとして指定され、ポリシーが適用されているインターフェイスが、speed 10/100/1000 コマンドで特定の速度に強制される場合、適用されたポリサー、シェイプ、または帯域幅の値は、強制された新しい速度に対応しない場合があります。

  サービス ポリシーは、パーセンテージのポリサー、シェイプ、またはシェイプ値で設定し、リンク速度は強制的に特定の値にする必要があります。次に例を示します。

  ```
  Policy-map p1
      class-map c1
         police rate percent 10
  ```

  回避策：speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー、シェイプ、またはシェイプ値を絶対値で指定します。次に例を示します。

  ```
  Policy-map p1
     class-map c1
       police rate 10 mbps
  ```

  （CSCsk56877）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth/shape fixes the issue などのキューイング パラメータをいくつか変更して再設定してください。（CSCsk62457）

- E シリーズ スイッチでファン トレイの障害またはスーパバイザでの危険温度のいずれかが発生すると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を特定します。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、原因はファン トレイの障害です。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザの臨界温度が障害のしきい値を超えたことが原因です。

  （CSCsk48632）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。さらに、物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG で、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生します。

  回避策：X2 を再挿入します。（CSCsk43618）

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- 出力 QoS ポリシーが設定されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキング アクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の COS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された COS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

この問題の根本的原因の一部は、CSCsk66449 に説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能がイネーブルになっている場合、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを特定できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの COS/DSCP フィールドが強制的にゼロになります。

  インターフェイス上に存在する QoS ポリシーは、この COS/DSCP の値を分類に使用します。そのため、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。（CSCsh72408）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- cisco-phone マクロで設定したポート上で default interface コマンドを 2 回実行すると、バック トレースが表示されます。

  回避策：default interface コマンドを入力せずに、コンフィギュレーション行を一行ずつ削除します。（CSCsj23103）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、show policy-map name を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシタイプが「Unknown」と表示されます。IOS を起動した後、シャーシ タイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- WS-X4648-RJ45V-E（PoE）および WS-X4648-RJ45V+E（ポートあたり 30 W の Premium PoE）ラインカード上で QoS ポリシーをキューイングアクション（共有またはシェーピング）で設定すると、SSO スイッチオーバー後に共有およびシェーピングのパーセンテージエラーが 3 パーセントに増加します。

  回避策：次のいずれかの操作を実行します。

  - インターフェイスからサービスポリシーを削除し、[no] service-policy {input|output} コマンドを使用して設定を再適用します。
  - shutdown コマンドを入力してから no shutdown コマンドを入力します。

  （CSCsm45156）

- ポリシーマップで「class-default」クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。サイズの範囲は、queue-limit コマンドにより表示されます。（CSCso06422）

- IPv4 ルートが RTR2 から IPv6 ピアリングを介して RTR3 にアドバタイズされると、RTR2 の IPv6 アドレスの最初の 32 ビットが IPv4 アドレスに変換されます。この IPv4 アドレスは、RTR3 に対するネクストホップ アドレスとしてアドバタイズされます。このアドレスが Martian アドレスになると、RTR3 は BGP 更新メッセージを無視するため、IPv4 ルートが認識されません。

  RTR3 でインバウンド ルートマップを設定して RTR2 がアドバタイズしたネクストホップを上書きしても、BGP 更新メッセージは無視されるため、この問題を回避することはできません。

  回避策：RTR2 でアウトバウンドルートマップを設定し、暗示的にプロトコルで取得するのではなく、明示的に IPv4 ネクストホップを設定します。（CSCsk65139）

- IPv6 EIGRP に割り当てられたリンク帯域幅を、ipv6 bandwidth-percent eigrp as-number percent コマンドを使用して変更しようとすると、スーパバイザエンジンがリロードします。冗長性をイネーブルにすると、STANDBY スーパバイザ エンジンが ACTIVE になり、リロードされたスーパバイザ エンジンが STANDBY に設定されます。

  回避策：ありません。（CSCso30051）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 からそれ以降のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、アクティブ スーパバイザ エンジンが IOS を実行しており、スタンバイ スーパバイザ エンジンが ROMMON モードになっていて、スタンバイ スーパバイザ エンジンの ROMMON がバージョン 0.34 から以降のバージョンにアップグレードされると冗長スイッチで発生します。アップグレードプロセスにより、スタンバイ スーパバイザ エンジンのアップリンクがダウンしますが、アクティブ スーパバイザ エンジンはそのダウンを検出しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - redundancy reload shelf コマンドで、両方のスーパバイザをリロードします。
  - STANDBY スーパバイザ エンジンをしばらくの間シャーシから抜き出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- スイッチの起動時には、「Module M linecard watchdog has expired」というメッセージが表示されます。

  ハードウェアの電源投入方法によって、ラインカードの起動時にメッセージが表示されることがあります。

  回避策：ラインカードをリセットします。（CSCsq21215）

- トラフィックおよびポーズ フレームでフロー制御の設定を変更すると、トラフィックの一部が失われます。

  この問題は、ポーズ フレームがスイッチ ポートに送信され、フロー制御の受信設定が 10G ポートに切り替えられたときに発生します。

  回避策：トラフィックが存在しない場合は、フロー制御の受信設定を変更します。（CSCso71647）

- IGMP スヌーピング エントリが、すべての IGMP スヌーピングをディセーブルにした後もアクティブです。

  回避策：関連するすべての VLAN 上で IGMP スヌーピングを無効にしてから、IGMP スヌーピングをグローバルに無効にします。

  （CSCsq71546）

- Cisco IOS Release 12.2(47)SG を実行している Catalyst 4500 シリーズ スイッチでは、AAA サーバに接続するスイッチ ポートをアクセス VLAN 上で SVI をイネーブルにしたレイヤ 2 インターフェイスとして設定している場合、802.1X をイネーブルにした電話が MDA ポートで認証しようとすると、ポート セキュリティとスパニングツリー PortFast で設定したすべての MDA ポートで 802.1X セキュリティ違反が発生する場合があります。

  回避策:

  a. ポートのポート セキュリティをディセーブルにするか、スイッチを標準レイヤ 3 ポートで AAA サーバに接続します。

  b. spanning-tree portfast をディセーブルにします。

  (CSCsq62342)

- システムをリロードした後、デフォルト以外の速度を持つインターフェイス上のパーセンテージ ベースの入力ポリサーが動作しません。

  回避策:インターフェイス上のサービスポリシーを削除して再適用します。

  (CSCsq79073)

- スイッチ上のソフトウェアを介してパケットが切り替えられると、そのパケット上での入力 QoS のマーキングアクションが適用されません。

  この問題は、スイッチを介して論理的に切り替えられたものの、スイッチ自体によってシステム生成された出力でシステム内部制御されているパケットにのみ見られます。これは、DAI、IGMP スヌーピング、DHCP スヌーピング、および MLD スヌーピングなどの特定のスヌーピング機能の場合に発生します。また、ソフトウェアで処理する必要のある IP オプションおよび拡張ヘッダーを持つ IPv4/v6 パケットの場合にも発生します。

  回避策:ありません。

  (CSCso96660)

- ポリシーでポリサー値またはシェイプ値がリンク帯域幅に対するパーセンテージとして指定されており、これらの値が割り当てられたインターフェイスが speed 10/100/1000 コマンドを使用して特定の速度になるよう強制されている場合、適用されたポリサー値またはシェイプ値が、強制された新しい速度に対応する場合があります。

  例:

```
Policy-map p1
       class-map c1
          police rate percent 10
```

  回避策:speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー値またはシェイプ値を絶対値で指定します。

  例:

```
Policy-map p1
      class-map c1
        police rate 10 mbps
```

  (CSCsk56877)

- パーセントベースの操作を含むポリシーマップがチャネルメンバーポートと別のスタンドアロンポート間で共有されると、チャネルがバンドル解除および再バンドルされ、スタンドアロンポートが レイヤ 2 からレイヤ 3 またはレイヤ 3 からレイヤ 2 に変更されます。

  回避策:ありません。(CSCso54096)

- SSO モードで service-policies メンバーを port-channel メンバーに追加、削除、または変更すると、次のトレースバックがアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンの両方に表示されます。

```
03:50:00: %SM-4-BADEVENT: STANDBY:Event 'bundle_sync' is invalid for the current state
'COLLECTING_DISTRIBUTING': lacp_mux Gi7/7 - mux
-Traceback= 10B97B80 10B98294 10189F78 1038FE0C 103944FC 1055E420 1055C4B8 10A2C28C
10A2AE88 10A2A4B0 10A27A18 10A225E8 1059E824 10595AAC
```

回避策：ありません。（CSCso23786）

- IPv6 MLD と関連したコンフィギュレーションがない場合も、IPv6 MLD エントリが、アクティブになります。

回避策：すべての汎用 QOS ポリシーの設定をシステムから解除します。（CSCsq84853）

- IPv6 エントリが CAM でアクティブとなり、CPU が IPv6 パケットを受信します。

回避策：すべての汎用 QOS ポリシーの設定をシステムから解除します。match any 属性を持つ QoS ポリシーにより、IPv6 エントリがアクティブになります。スイッチが純粋なレイヤ 2 デバイスである場合、汎用プロトコル ファミリの属性を削除して、プロトコル ファミリに絞り込みます。

（CSCsq84796）

- VLAN ロード バランシング（VLB）を設定した REP が、最初は正常に動作します。セカンダリ ALT ポートとして動作しているポートのあるスイッチで force-switchover を入力すると、トポロジでループが発生します。

回避策：トポロジ内の任意の REP ポート（VLB が設定されているのと同じセグメント）で shut を入力してから no-shut コマンドを入力します。（CSCsq75342）

- Cisco IOS リリース 12.2(46)SG では、FlexLink が EtherChannel のペアに適用されている場合、FlexLink の設定後にバックアップ EtherChannel が定義されていると、リブート後に FlexLink の設定が適用されないことがあります。

回避策：flexlink コマンドを適用する前に、バックアップ EtherChannel を定義します。（CSCsq13477）

- Cisco IOS リリース 12.2(46)SG では、EtherChannel が FlexLink ペアのメンバーである場合、EtherChannel に設定されたスタティック MAC アドレスは、EtherChannel に障害が発生した場合（FlexLink の障害）、代替ポートに移動されません。

回避策：ありません。（CSCsq99468）

- 自動 QoS が有効になっているインターフェイスでデフォルトのインターフェイス操作を実行すると、エラーメッセージが表示され、自動 QoS 設定が失われます。たとえば、次の一連の操作により設定が失われます。

```
config-if# auto qos voip cisco-phone
config# default interface interface-name
```

回避策：default interface コマンドを次のように置き換えます。

```
config# interface interface-number
config-if# switchport
```

（CSCsq47116）

- リンク上でアクティビティがない状態が 15 秒続くと、IPv6 ICMP ネイバーステートが REACH から STALE に変わります。

回避策：ネイバーのグローバルアドレスとリンクローカルアドレスを ping し、到達可能性を確認して修復します。（CSCsq77181）

- IPv6 EIGRP ルートがポート チャネルから認識されません。

  回避策：ポートチャネルと関連付けられた物理ポートの設定を解除し、それらを再設定します。

  （CSCsq74229）

- CFM Inward Facing MEP（IFM）が、DOWN のスイッチポートに割り当てられていない VLAN で設定されている場合、show ethernet cfm maintenance-points local コマンドによって IFM CC ステータスが Inactive と表示されます。VLAN を割り当てても、CC ステータスは Inactive のままです。

  この問題は、VLAN を割り当てずに IFM を設定した後で、同じ VLAN を割り当てたときにのみ発生します。

  回避策：ポート上の IFM の設定を解除し、再設定します。

- CFM では、サービスインスタンス/MEP に関連付けられた VLAN が、ステータスが down になっているインターフェイス上で Inward Facing MEP（IFM）が設定された後に割り当てられると、show ethernet CFM maintenance local コマンドの出力でも IFM CC ステータスは inactive のままになります。また、CFM リモート ネイバーは表示されません。

  このような動作は、IFM を設定した後に VLAN が割り当てられたときにのみ見られます。

  回避策：no ethernet cfm mep level mpid vlan コマンドで設定を解除してから、VLAN が割り当てられた後にポート上で ethernet cfm mep level mpid vlan コマンドを実行して IFM を再設定します。IFM の C ステータスが Activ eであることを show ethernet cfm maintenance-points local コマンドで確認します。（CSCsm85460）

- Catalyst 4500 シリーズ スイッチを Supervisor Engine 6-E とともに使用し、インターフェイスに出力サービスポリシーが設定されている場合、同じ出力サービスポリシーが適用されている別のインターフェイスで shut/no shut を入力すると、キューがフル状態のために出力がドロップされます。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、および 12.2(46)SG で発生します。

  この問題は、12.2(50)SG で解決されています。

  回避策：qos autoqos マクロを使用しないでください。

  ポリシーマップが複数のターゲットで共有されている場合は、パーセンテージベースのアクションを使用しないでください。ポリシング、シェーピング、および帯域幅アクションでは、絶対値を使用する必要があります。そのためには、スイッチでサポートされる 4 つのインターフェイス速度（10M、100M、1G、および 10G）ごとに異なるポリシーマップが必要です。そのため、パーセンテージベースのアクションで単一のポリシーマップを有効にするのではなく、4 つの異なるポリシーマップを作成する必要があります。これは、サービスポリシーの方向に関係なく、すべての共有ポリシーマップに適用されます。

  （CSCsr12142）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
```

```
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

回避策：ありません。

CSCtc13297

Cisco IOS Release 12.2(46)SG で解決済みの警告

ここでは、Cisco IOS Release 12.2(46)SG で解決済みの警告について説明します。

- SSO モードでアクティブ スーパバイザ エンジン上で bgp dampening route-map bgp_damp コマンドを入力すると、次のシステムログがスタンバイ スーパバイザ エンジンのコンソールに表示されます。

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  この時点で、アクティブ スーパバイザ エンジン上で bgp dampening コマンドに戻ると、新しいコマンドがスタンバイ スーパバイザ エンジンと同期されなくなります。

  回避策：no bgp dampening コマンドを入力してから、bgp dampening コマンドを入力します。（CSCse12485）

- REP 管理 VLAN と RSPAN 宛先 VLAN が一致しません。特定の VLAN を REP 管理 VLAN または RSPAN 宛先 VLAN として設定できます。

  回避策：REP 管理 VLAN と RSPAN 宛先 VLAN が異なっていることを確認します。（CSCso12495）

- VLAN ロードバランシングがアクティブになっている場合、セグメントの障害やスーバーバイザエンジンの取り外しにより、REP セグメントでループが発生する場合があります。

  回避策：ありません。（CSCsm61748）

- すべての機能の組み合わせがハードウェアにより同時にサポートされるわけではありません。サポート可能な機能の組み合わせが設定されている場合、パケットはソフトウェアで処理され、次のログメッセージが生成されます。

  ```
  %C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
  SignatureInconsistent - packets will be handled in software, QoS is disabled.
  ```

  この問題は、CoS ビット上で一致する QoS ポリシーを、アドレスの下位 48 ビットを部分的にマスクする IPv6 送信元アドレスと一致する IPv6 ACL コンフィギュレーションと組み合わせると発生する場合があります（この動作は、IPv6 マルチキャストルーティングが有効になっている場合、/81 ～ /127 の範囲の IPv6 サブネットを使用することでも発生します）。

  回避策：競合する機能の組み合わせを設定しないでください。現在、上記の COS ビット上で一致する QoS ポリシーと送信元アドレスの下位 48 ビットを部分的にマスクする IPv6 設定の競合は、機能の組み合わせの競合としてのみ認識されています。QoS ポリシーにより CoS ビット上での一致が要求される場合、/80 以上のサブネットを使用して IPv6 ネットワークを設計してください。（CSCsk79791）

- ip icmp unreachable コマンドが、レイヤ 3 インターフェイス上の IPv4 と IPv6 の両方のパケットに対する ICMP の到着不能メッセージの生成に影響する場合があります。さらに、IPv6 アドレスを持つレイヤ 3 インターフェイス上のレイヤ 3 の拒否 ACL では、ICMP の到着不能メッセージを生成せずに、拒否されたトラフィックを CPU にコピーしない場合があります。

  最初の問題は、IPv4 および IPv6 の両方のアドレスが設定されるデュアルレイヤ 3 のインターフェイスで発生します。2 番目の問題は、スイッチのすべてのレイヤ 3 のインターフェイスが IPv6 アドレスのみで設定されている場合に発生します。

  回避策：IPv4 および IPv6 の両方のアドレスが設定されているデュアルレイヤ 3 のインターフェイスを使用しないでください。

  スイッチを IPv6 レイヤ 3 のインターフェイス専用ルータとして使用しないでください。IPv4 アドレスが設定された SVI ごとに、少なくとも 1 つのレイヤ 3 インターフェイスがあることを確認してください。（CSCsk77234）

- インターフェイス コンフィギュレーションをレイヤ 3/ルータポートからレイヤ 2/スイッチポートに切り替えてからレイヤ 3/ルータポートに戻すと、ルータインターフェイスの IOS 設定が設定されていない場合でも、元のルータインターフェイスに接続された IPv6 ACL が TCAM ハードウェアで正常に削除されないことがあります。

  回避策：レイヤ 3 インターフェイスをルータポートからスイッチポートに切り替える前に、ルータインターフェイスの IPv6 ACL の設定を解除します。これにより、IPv6 ACL が IOS 実行コンフィギュレーションと TCAM ハードウェアの両方で正常にクリーンアップされます。（CSCsk60775）

- モジュールにより危険温度またはシャットダウン温度のアラームが報告された場合でも、E シリーズ スーパバイザおよびラインカードの LED は緑に点灯したままです。LED はオレンジまたは赤に点灯するはずです。

  これは、危険温度またはシャットダウン温度のアラームを報告する E シリーズのすべてのラインカードで発生します。実際の温度とアラームのステータスが show environment temperature コマンドの出力に表示されます。

  回避策：LED の色に関してはありません。ただし、アラームが発生または解除されると、コンソール ログ メッセージと SNMP トラップが入力されます。また、温度アラームの現在のステータスが show environment temperature コマンドの出力に表示されます。（CSCsk57143）

- デフォルト以外のデュプレックス設定が FastEthernet インターフェイスに適用されていて、Cisco IOS リリース 12.2(31)SGA から 12.2(40)SG にアップグレードすると、FastEthernet 設定のデュプレックス設定は失われます。インターフェイスがデフォルトのデュプレックス設定に戻り、デュプレックス設定が show running コマンドの出力に表示されなくなります。

  回避策：実行コンフィギュレーションにデフォルト以外のデュプレックス設定がある場合、アップグレードする前にそれらの設定を控えておき、アップグレード完了後に再適用します。（CSCsk83670）

- ポリシーマップで、プライオリティ キューイング クラス設定の前に bandwidth remaining percent <> コマンドを設定したキューイングクラスがある場合、リロード時に bandwidth remaining percent <> コマンドのアクションが適用されません。

  回避策：ポリシーマップを再適用します。（CSCsk75793）

- ポートは、ポートチャネルのメンバーになるか、または AutoQoS を適用することができますが、両方はできません。これらの機能は相互排他的です。

  現在、ポートチャネルのメンバーであるポートに AutoQoS が適用されている場合、アプリケーションは拒否され、エラーメッセージが表示されます。ただし、その逆は正しくありません。AutoQoS が最初に適用され、ポートがポートチャネルに参加する場合、コマンドは受け入れられます。

ポート g2/1 を使用する次の例は、回避すべき使用のタイプを示しています。

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

この例では、ポート（g2/1）に AutoQoS を適用し、その後ポートをポートチャネル（10）のメンバーにします。

回避策：AutoQoS が有効になっているポートをポートチャネルのメンバーにしないでください。（CSCsi95018）

- デュアルレートポリサーに対して exceed burst が明示的に設定されていない場合、show policy-map コマンドを実行するとバースト値として 0 が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の exceed burst 値を調べます。（CSCsj44237）

- 冗長 WS-X45-SUP6-E スーパバイザ エンジンを搭載したスイッチおよび RJ-45 を使用するよう設定された WS-X4506-GB-T インターフェイスを搭載したスイッチでは、SSO スイッチオーバーの後、インターフェイス上の QoS 設定が無効になります。さらに、メディア タイプを SFP に変更した後、再度 RJ-45 に戻すと、QoS 設定が失われる可能性があります。

  QoS 設定は実行コンフィギュレーションには表示されますが、インターフェイス上では維持されません。

  回避策：QoS 設定をインターフェイスに再適用します。（CSCsm58839）

- 最初にインターフェイスで IPv6 を有効にせずに ipv6 mtu mtu-value コマンドを使用してインターフェイス上で IPv6 MTU を設定すると、起動時にスイッチが無期限に停止する場合があります。

  回避策：インターフェイス上で IPv6 MTU を設定する前に、インターフェイス上で IPv6 を有効にする必要があります。IPv6 を有効にするには、ipv6 enable コマンドを使用します。

  この問題が発生した場合は、次のコマンドを使用してスイッチを復旧してください。

1. ROMMON プロンプトで confreg コマンドを入力して、スタートアップ コンフィギュレーションを無視します。
2. reset コマンドを入力して、スイッチをリブートします。
3. copy startup-config running-config コマンドを入力して、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
4. ipv6 enable コマンドを入力して、インターフェイスで IPv6 を有効にします。
5. ipv6 mtu mtu-value コマンドを入力して、インターフェイス上で IPv6 MTU を設定します。
6. ccopy running-config startup-config コマンドを入力して、回復コンフィギュレーションを保存します。
7. スイッチで reload コマンドを入力して、ROMMON に戻ります。
8. ROMMON から confreg コマンドを入力して、スタートアップ コンフィギュレーションを処理します。
9. スイッチをリセットして、通常の操作を再開します。（CSCso42867）

- Catalyst 4500 スーパバイザ エンジンのアップリンク ポートに直接接続されているスイッチでは、エンジンがリロードされるときにリンク ダウンが認識されません。そのため、UDLD がイネーブルの場合、リンク パートナーにより err-disable ステートが入力されます。

  回避策：リロードする前に、スーパバイザ アップリンク ポートをシャットダウンします。（CSCsl34390）

- 2 つのスイッチが 2 つ以上のリンクを介してバックツーバックで接続されており、パケットの発信元がローカルにある場合、ソース IP アドレスが発信インターフェイスの IP アドレスと一致しないことがあります。ユニキャスト RPF 機能がイネーブルになっているこのようなパケットを受信するスイッチが、着信パケットをドロップする可能性があります。

  回避策：ありません。（CSCsh99124）

Cisco IOS リリース 12.2(44)SG1 の未解決の警告

ここでは、Cisco IOS リリース 12.2(44)SG1 の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザ エンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- まれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 のパケット照合カウンタに、一致するパケットが表示されないことがあります。

```
clearwater# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、UDLD err-disable ステートになっているポート上で shutdown コマンドを入力してから no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD err-disable ステートのままです。同じポート上で shutdown コマンドを再入力してから no shutdown コマンドを入力すると、エラーメッセージは表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書の存在を確認します。
  - このような証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンでそれぞれ個別に生成されます。そのため、証明書は異なったものになります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- Cisco IOS 12.2（31）SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェア リリースの場合と同様に動作しないことがあります。

  これは、12.2（31）SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

QueueID	以前の QueueName	新しい QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<未使用のキュー>	control-packet
11	<未使用のキュー>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  （CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを使用します。

回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  これは、次の理由で発生する場合があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - これは、スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合も同様です。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバード ポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- SSO モードでアクティブ スーパバイザ エンジン上で bgp dampening route-map bgp_damp コマンドを設定すると、次のシステムログがスタンバイ スーパバイザ エンジンのコンソールに表示されます。

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  この時点で、アクティブ スーパバイザ エンジン上で bgp dampening コマンドに戻ると、新しいコマンドがスタンバイ スーパバイザ エンジンと同期されなくなります。

  回避策：no bgp dampening コマンドを入力してから、bgp dampening コマンドを入力します。（CSCse12485）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィック パフォーマンスを測定する場合、qos account layer2 encapsulation を設定している場合でも、ポリサーにより 802.1Q タグを構成する 4 バイトが qos account layer2 encapsulation を設定していても、ポリサーにより 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に「a-」が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG以降のイメージへのISSUアップグレード中に、次のエラーメッセージが表示されます。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- Cisco IP 電話がサプリカントに接続している場合、MDA で設定し、電話およびサプリカントに接続された DUT ポートをリロードすると、そのポートがトラフィックを渡しません。電話は unknown ステートになります。

  電話がスタンドアロンデバイスの場合、この問題は確認されません。

  回避策：Cisco IP 電話の電源を再投入します。（CSCsk81297）

- マルチドメイン認証（MDA）で設定されたポート上でデータ デバイスが（dot1x または MAB を介して）承認された後、アクセス VLAN を変更すると、デバイスがポートに接続されていない場合でも、このデバイスのトラフィックが失われます。ポートに接続されている音声デバイスのトラフィックには影響しません。

  回避策：ポート上のアクセス VLAN を変更後、インターフェイス上で shutdoown コマンドを入力してから no shutdown コマンドを入力します。（CSCsk45969）

- REP 管理 VLAN と RSPAN 宛先 VLAN が一致しません。特定の VLAN を REP 管理 VLAN または RSPAN 宛先 VLAN として設定できます。

  回避策：REP 管理 VLAN と RSPAN 宛先 VLAN が異なっていることを確認します。（CSCso12495）

- 3000 以上の VLAN ID でトラフィックが送信されると、障害により発生するコンバージェンス タイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- REP で、異なる VLAN ブロッキングを反映するように VLAN ロードバランシングの設定を変更すると、手動プリエンプションは発生しません。

  回避策：物理的にケーブルを引き抜くかインターフェイスをシャットダウンすることで、意図的に 2 つのスイッチ間のリンクを失敗させます。その後、リンクを元の状態に戻します。この後、遅延したプリエンプションが続きます。（CSCsm91997）

- VLAN ロード バランシングでは、セグメントの障害やスーバーバイザ エンジンの取り外しにより、REP セグメントでループが発生する場合があります。

  回避策：ありません。（CSCsm61748）

Supervisor Engine 6-E に固有の問題

- 必要な QoS 操作を適用するためのソフトウェア QoS が .1Q パケットと正しく一致しません。

  回避策：なし。

  Cisco IOS Release 12.2（40）SG リリースでは、ソフトウェア QoS ルックアップを行う 1Q パケット処理はサポートされていません。（CSCsk66449）

- すべての機能の組み合わせがハードウェアにより同時にサポートされるわけではありません。サポートされていない機能の組み合わせが設定されている場合、パケットはソフトウェアで処理され、次の内容を示すログ メッセージが生成されます。

  ```
  %C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
  SignatureInconsistent - packets will be handled in software, QoS is disabled.
  ```

このような問題は、cos ビット上で一致する QoS ポリシーを、アドレスの下位 48 ビットを部分的にマスクする IPv6 送信元アドレスと一致する IPv6 ACL コンフィギュレーションと組み合わせようとすると発生する場合があります(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場合、/81 ～ /127 の範囲の IPv6 サブネットを使用することでもこのような問題が発生します)。

回避策:競合する機能の組み合わせを設定しないでください。現在、上記の COS ビット上で一致する QoS ポリシーと送信元アドレスの下位 48 ビットを部分的にマスクする IPv6 設定の競合は、機能の組み合わせの競合としてのみ認識されています。QoS ポリシーにより COS ビット上での一致が要求される場合、/80 以上のサブネットを使用して IPv6 ネットワークを構築してください。(CSCsk79791)

- ポリサー、シェイプ、またはシェイプ値がポリシーのリンク帯域幅のパーセンテージとして指定され、ポリシーが適用されているインターフェイスが、speed 10/100/1000 コマンドで特定の速度に強制される場合、適用されたポリサー、シェイプ、または帯域幅の値は、強制された新しい速度に対応する場合があります。

  サービス ポリシーは、パーセンテージのポリサー、シェイプ、またはシェイプ値で設定し、リンク速度は強制的に特定の値にする必要があります。次に例を示します。

```
Policy-map p1
    class-map c1
       police rate percent 10
```

  回避策:speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー、シェイプ、またはシェイプ値を絶対値で指定します。次に例を示します。

```
Policy-map p1
   class-map c1
     police rate 10 mbps
```

  (CSCsk56877)

- ip icmp unreachable コマンドが、レイヤ 3 インターフェイス上の IPv4 と IPv6 の両方のパケットに対する ICMP の到着不能メッセージの生成に影響する場合があります。さらに、IPv6 アドレスを持つレイヤ 3 インターフェイス上のレイヤ 3 の拒否 ACL では、ICMP の到着不能メッセージを生成せずに、拒否されたトラフィックを CPU にコピーしない場合があります。

  最初の問題は、IPv4 および IPv6 の両方のアドレスが設定されるデュアル レイヤ 3 のインターフェイスで発生します。2 番目の問題は、スイッチ上のすべてのレイヤ 3 のインターフェイスが IPv6 アドレスのみで設定されている場合に発生します。

  回避策:IPv4 および IPv6 の両方のアドレスが設定されているデュアルレイヤ 3 のインターフェイスを使用しないでください。

  スイッチを IPv6 レイヤ 3 のインターフェイス専用ルータとして使用しないでください。IPv4 アドレスの設定された SVI ごとに、少なくとも 1 つのレイヤ 3 インターフェイスがあることを確認してください。(CSCsk77234)

- インターフェイス コンフィギュレーションをレイヤ 3/ルータポートからレイヤ 2/スイッチポートに切り替えてからレイヤ 3/ルータポートに戻すと、ルータインターフェイスの IOS 設定が設定されていない場合でも、元のルータインターフェイスに接続された IPv6 ACL が TCAM ハードウェアで正常にフラッシュされないことがあります。

  回避策:レイヤ 3 インターフェイスをルータポートからスイッチポートに切り替える前に、ルータインターフェイスの IPv6 ACL の設定を解除します。これにより、IPv6 ACL が IOS 実行コンフィギュレーションと TCAM ハードウェアの両方で正常にクリーンアップされます。(CSCsk60775)

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

デフォルトのキューでこの問題が発生した場合、bandwidth/shape fixes the issue などのキューイング パラメータをいくつか変更して再設定してください。（CSCsk62457）

- E シリーズ スイッチでファン トレイの障害またはスーパバイザでの危険温度のいずれかが発生すると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を特定します。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、原因はファン トレイの障害です。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザの臨界温度が障害のしきい値を超えたことが原因です。

  （CSCsk48632）

- モジュールにより危険温度またはシャットダウン温度のアラームが報告された場合でも、E シリーズ スーパバイザおよびラインカードの LED は緑に点灯したままです。LED はオレンジまたは赤に点灯するはずです。

  これは、危険温度またはシャットダウン温度のアラームを報告する E シリーズのすべてのラインカードで発生します。実際の温度とアラームのステータスが show environment temperature コマンドの出力に表示されます。

  回避策：LED の色に関してはありません。ただし、アラームが発生または解除されると、コンソール ログ メッセージと SNMP トラップが入力されます。また、温度アラームの現在のステータスが show environment temperature コマンドの出力に表示されます。（CSCsk57143）

- 2 つのスイッチが 2 つ以上のリンクを介してバックツーバックで接続されており、パケットの発信元がローカルにある場合、ソース IP アドレスが発信インターフェイスの IP アドレスと一致しないことがあります。ユニキャスト RPF 機能がイネーブルになっているこのようなパケットを受信するスイッチが、着信パケットをドロップする可能性があります。

  回避策：ありません。（CSCsh99124）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。さらに、物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- デフォルト以外のデュプレックス設定が FastEthernet インターフェイスに適用されていて、Cisco IOS リリース 12.2(31)SGA から 12.2(40)SG にアップグレードすると、FastEthernet 設定のデュプレックス設定は失われます。インターフェイスがデフォルトのデュプレックス設定に戻り、デュプレックス設定が show running コマンドの出力に表示されなくなります。

回避策：実行コンフィギュレーションにデフォルト以外のデュプレックス設定がある場合、アップグレードする前にそれらの設定を控えておき、アップグレード完了後に再適用します。（CSCsk83670）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG で、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生します。

  回避策：X2 を再挿入します。（CSCsk43618）

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- ポリシーマップで、プライオリティ キューイング クラス設定の前に bandwidth remaining percent <> コマンドを設定したキューイングクラスがある場合、リロード時に bandwidth remaining percent <> コマンドのアクションが適用されません。

  回避策：ポリシーマップを再適用します。（CSCsk75793）

- 出力 QoS ポリシーが設定されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキング アクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の COS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された COS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 に説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能がイネーブルになっている場合、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを特定できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの COS/DSCP フィールドが強制的にゼロになります。

  インターフェイス上に存在する QoS ポリシーは、この COS/DSCP の値を分類に使用します。そのため、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。（CSCsh72408）

- ポートは、ポートチャネルのメンバーになるか、または AutoQoS を適用することができますが、両方はできません。これらの機能は相互排他的です。

  現在、ポートチャネルのメンバーであるポートに AutoQoS が適用されている場合、アプリケーションは拒否され、エラーメッセージが表示されます。ただし、その逆は正しくありません。AutoQoS が最初に適用され、ポートがポートチャネルに参加する場合、コマンドは受け入れられます。

  ポート g2/1 を使用する次の例は、回避すべき使用のタイプを示しています。

```
conf t
int g2/1
auto qos voice trust
channel-group 10 mode auto
```

この例では、ポート（g2/1）に AutoQoS を適用し、その後ポートをポートチャネル（10）のメンバーにします。

回避策：AutoQoS が有効になっているポートをポートチャネルのメンバーにしないでください。（CSCsi95018）

- デュアルレートポリサーに対して exceed burst が明示的に設定されていない場合、show policy-map コマンドを実行するとバースト値として「0」が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の exceed burst 値を調べます。（CSCsj44237）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- cisco-phone マクロで設定したポート上で default interface を 2 回実行すると、バックトレースが表示されます。

  回避策：default interface コマンドを入力せずに、コンフィギュレーション行を一行ずつ削除します。（CSCsj23103）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、show policy-map name を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシ タイプが「Unknown」と表示されます。IOS を起動した後、シャーシ タイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- WS-X4648-RJ45V-E（PoE）および WS-X4648-RJ45V+E（ポートあたり 30 W の Premium PoE）ラインカード上で QoS ポリシーをキューイング アクション（分散またはシェーピング）で設定すると、SSO スイッチ オーバー後に分散およびシェーピングのパーセンテージ エラーが 3 パーセントに増大します。

  回避策：次のいずれかの操作を実行します。

  - インターフェイスからサービスポリシーを削除し、[no] service-policy {input|output} コマンドを使用して設定を再適用します。
  - shutdown コマンドおよび no shutdown コマンドを入力します。

  （CSCsm45156）

- 冗長 WS-X45-SUP6-E スーパバイザ エンジンを搭載したスイッチおよび RJ-45 を使用するよう設定された WS-X4506-GB-T インターフェイスを搭載したスイッチでは、SSO スイッチオーバーの後、インターフェイス上の QoS 設定が無効になります。さらに、メディア タイプを SFP に変更した後、再度 RJ-45 に戻すと、QoS 設定が失われる可能性があります。

  QoS 設定は実行コンフィギュレーションには表示されますが、インターフェイス上では維持されません。

  回避策：QoS 設定をインターフェイスに再適用します。（CSCsm58839）

- ポリシーマップで「class-default」クラスマップの DBL アクションを指定すると、デフォルトキューのサイズによっては動作しないことがあります。

回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。サイズの範囲は、queue-limit コマンドにより表示されます。（CSCso06422）

- IPv4 ルートが RTR2 から IPv6 ピアリングを介して RTR3 にアドバタイズされると、RTR2 の IPv6 アドレスの最初の 32 ビットが IPv4 アドレスに変換されます。この IPv4 アドレスは、RTR3 に対するネクストホップ アドレスとしてアドバタイズされます。このアドレスが Martian アドレスになると、RTR3 は BGP 更新メッセージを無視するため、IPv4 ルートが認識されません。

  RTR3 でインバウンド ルートマップを設定して RTR2 がアドバタイズしたネクストホップを上書きしても、BGP 更新メッセージは無視されるため、この問題を回避することはできません。

  回避策：RTR2 でアウトバウンドルートマップを設定し、暗示的にプロトコルで取得するのではなく、明示的に IPv4 ネクストホップを設定します。（CSCsk65139）

- IPv6 EIGRP に割り当てられたリンク帯域幅を、ipv6 bandwidth-percent eigrp as-number percent コマンドを使用して変更しようとすると、スーパバイザエンジンがリロードします。冗長性をイネーブルにすると、STANDBY スーパバイザ エンジンが ACTIVE になり、リロードされたスーパバイザ エンジンが STANDBY に設定されます。

  回避策：ありません。（CSCso30051）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から最新のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、ACTIVE スーパバイザ エンジンが IOS で、STANDBY スーパバイザ エンジンが ROMMON でそれぞれ実行され、STANDBY の ROMMON がバージョン 0.34 または最新バージョンにアップグレードされたときに、冗長スイッチで発生します。アップグレード処理により STANDBY スーパバイザ エンジンのアップリンクがダウンしますが、ACTIVE スーパバイザ エンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - redundancy reload shelf コマンドで、両方のスーパバイザをリロードします。
  - STANDBY スーパバイザ エンジンをしばらくの間シャーシから抜き出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- 最初にインターフェイスで IPv6 をイネーブルにせずに ipv6 mtu mtu-value コマンドを使用してインターフェイス上で IPv6 MTU を設定すると、起動時にスイッチが無期限に停止する場合があります。

  回避策：インターフェイス上で IPv6 MTU を設定する前に、インターフェイス上で IPv6 を有効にする必要があります。IPv6 をイネーブルにするには、ipv6 enable コマンドを使用します。

  この問題が発生した場合は、次のコマンドを入力してスイッチを復旧してください。

---

1. rommon プロンプトで confreg コマンドを使用して、スタートアップ コンフィギュレーションを無視します。
2. reset コマンドを使用して、スイッチをリブートします。
3. copy startup-config running-config コマンドを使用して、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
4. ipv6 enable コマンドを使用して、インターフェイス上で IPv6 を有効にします。
5. ipv6 mtu mtu-value コマンドを使用して、インターフェイス上で IPv6 MTU を設定します。

6. ccopy running-config startup-config コマンドを使用して、回復コンフィギュレーションを保存します。
7. スイッチで reload コマンドを使用して、ROMMON に戻ります。
8. ROMMON から、confreg コマンドを使用して、スタートアップ コンフィギュレーションを処理します。
9. スイッチをリセットして、通常の操作を再開します。(CSCso42867)

- Catalyst 4500 シリーズ スイッチを Supervisor Engine 6-E とともに使用し、インターフェイスに出力サービスポリシーが設定されている場合、同じ出力サービスポリシーが適用されている別のインターフェイスで shut/no shut を入力すると、キューがフル状態のために出力がドロップされます。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、および 12.2(46)SG で発生します。

  この問題は、12.2(50)SG で解決されています。

  回避策:qos autoqos マクロを使用しないでください。

  ポリシーマップが複数のターゲットで共有されている場合は、パーセンテージベースのアクションを使用しないでください。ポリシング、シェーピング、および帯域幅アクションでは、絶対値を使用する必要があります。そのためには、スイッチでサポートされる 4 つのインターフェイス速度(10M、100M、1G、および 10G)ごとに異なるポリシーマップが必要です。そのため、パーセンテージベースのアクションで単一のポリシーマップを有効にするのではなく、4 つの異なるポリシーマップを作成する必要があります。これは、サービスポリシーの方向に関係なく、すべての共有ポリシーマップに適用されます。

  (CSCsr12142)

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策:Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。(CSCsy80664)

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています(ICMP タイプまたは ICMP コード)。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策:ありません。

  CSCtc13297

Cisco IOS リリース 12.2(44)SG1 の解決済みの警告

ここでは、Cisco IOS リリース 12.2(44)SG1 で解決済みの警告について説明します。

- EIGRP パッシブインターフェイスとして設定されたインターフェイスでリンクアップまたはリンクダウンイベントが発生すると、スイッチが予期せずリロードされることがあります。この場合、通常はコンソール上に「Vector 300」メッセージが表示されます。

  回避策：EIGRP パッシブインターフェイスの設定を削除します。

  すべてのスーパバイザで Cisco IOS リリース 12.2(44)SG1 または 12.2(46)SG にアップグレードすると、問題が解消されます。

  この障害は、従来のスーパバイザのみをサポートする 12.2(31)SGA ソフトウェアトレインには存在しません。（CSCsk04287）

- 一方または両方の 220V 接続を備えたデュアル 4200W AC 電源を備えた Catalyst 4500 シリーズスイッチでは、次のメッセージが表示されることがあります。

```
Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the
chassis are receiving different voltage inputs

Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the
chassis are of different types (AC/DC) or wattage
```

  PoE デバイスが接続されているポートでは、次のように表示されることもあります。

```
%ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi2/33: inline power denied
```

  影響を受ける電源が一時的にシャットダウンし、電源の冗長性が失われます。データおよびシャーシの電力が減少し、ラインカードがシャットダウンすることがあります。また、PoE の電力が減少し、PD がシャットダウンしてリセットされます。

注 両方のユニットに 110V の入力がある場合、影響はありません。（出力電流は、両方の 110V の入力接続により低くなります。CCO の Power Supply Calculator（http://tools.cisco.com/cpc/launch.jsp）を参照してください）。

回避策：ありません。（CSCso67729）

Cisco IOS リリース 12.2(44)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(44)SG の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- まれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 のパケット照合カウンタに、一致するパケットが表示されないことがあります。

```
clearwater# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。（SCef01798）

- SSO スイッチオーバーの後、UDLD err-disable ステートになっているポート上で shutdown コマンドを入力してから no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD err-disable ステートのままです。同じポート上で shutdown コマンドを再入力してから no shutdown コマンドを入力すると、エラーメッセージは表示されなくなります。

  回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書の存在を確認します。
  - このような証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンでそれぞれ個別に生成されます。そのため、証明書は異なったものになります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- Cisco IOS 12.2（31）SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェア リリースの場合と同様に動作しないことがあります。

  これは、12.2（31）SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

QueueID	以前の QueueName	新しい QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<未使用のキュー>	control-packet
11	<未使用のキュー>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを使用します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  これは、次の理由で発生する場合があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - これは、スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合も同様です。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバード ポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- SSO モードでアクティブ スーパバイザ エンジン上で bgp dampening route-map bgp_damp コマンドを設定すると、次のシステムログがスタンバイ スーパバイザ エンジンのコンソールに表示されます。

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF

00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

  この時点で、アクティブ スーパバイザ エンジン上で bgp dampening コマンドに戻ると、新しいコマンドがスタンバイ スーパバイザ エンジンと同期されなくなります。

  回避策：no bgp dampening コマンドを入力してから、bgp dampening コマンドを入力します。（CSCse12485）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィック パフォーマンスを測定する場合、qos account layer2 encapsulation を設定している場合でも、ポリサーにより 802.1Q タグを構成する 4 バイトが qos account layer2 encapsulation を設定していても、ポリサーにより 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に「a-」が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG以降のイメージへのISSUアップグレード中に、次のエラーメッセージが表示されます。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

- Cisco IP Phone にサプリカントが付属している場合、MDA で設定し、電話およびサプリカントに接続された DUT ポートをリロードするときに、ポートがトラフィックを送信しません。電話は unknown ステートになります。

  電話がスタンド アロン デバイスの場合、この問題は見られません。

  回避策：Cisco IP 電話の電源を再投入します。（CSCsk81297）

- マルチドメイン認証（MDA）で設定されたポート上でデータ デバイスが（dot1x または MAB を介して）承認された後、アクセス VLAN を変更すると、デバイスがポートに接続されていない場合でも、このデバイスのトラフィックが失われます。ポートに接続されている音声デバイスのトラフィックには影響しません。

  回避策：ポート上のアクセス VLAN を変更後、インターフェイス上で shutdown コマンドを入力してから no shutdown コマンドを入力します。（CSCsk45969）

- REP 管理 VLAN と RSPAN 宛先 VLAN が一致しません。特定の VLAN を REP 管理 VLAN または RSPAN 宛先 VLAN として設定できます。

  回避策：REP 管理 VLAN と RSPAN 宛先 VLAN が異なっていることを確認します。（CSCso12495）

- 3000 以上の VLAN ID でトラフィックが送信されると、障害により発生するコンバージェンス タイミングが 225 ms を超えます。

  回避策：ありません。（CSCsm30320）

- REP で、異なる VLAN ブロッキングを反映するように VLAN ロードバランシングの設定を変更すると、手動プリエンプションは発生しません。

  回避策：物理的にケーブルを引き抜くかインターフェイスをシャットダウンすることで、意図的に 2 つのスイッチ間のリンクを失敗させます。その後、リンクを元の状態に戻します。この後、遅延したプリエンプションが続きます。（CSCsm91997）

- VLAN ロード バランシングでは、セグメントの障害やスーパーバイザ エンジンの取り外しにより、REP セグメントでループが発生する場合があります。

  回避策：ありません。（CSCsm61748）

Supervisor Engine 6-E に固有の問題

- 必要な QoS 操作を適用するためのソフトウェア QoS が .1Q パケットと正しく一致しません。

  回避策：なし。

  Cisco IOS Release 12.2（40）SG リリースでは、ソフトウェア QoS ルックアップを行う 1Q パケット処理はサポートされていません。（CSCsk66449）

- すべての機能の組み合わせがハードウェアにより同時にサポートされるわけではありません。サポートされていない機能の組み合わせが設定されている場合、パケットはソフトウェアで処理され、次の内容を示すログ メッセージが生成されます。

  ```
  %C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
  SignatureInconsistent - packets will be handled in software, QoS is disabled.
  ```

  このような問題は、cos ビット上で一致する QoS ポリシーを、アドレスの下位 48 ビットを部分的にマスクする IPv6 送信元アドレスと一致する IPv6 ACL コンフィギュレーションと組み合わせようとすると発生する場合があります（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場合、/81 ～ /127 の範囲の IPv6 サブネットを使用することでもこのような問題が発生します）。

  回避策：競合する機能の組み合わせを設定しないでください。現在、上記の COS ビット上で一致する QoS ポリシーと送信元アドレスの下位 48 ビットを部分的にマスクする IPv6 設定の競合は、機能の組み合わせの競合としてのみ認識されています。QoS ポリシーにより COS ビット上での一致が要求される場合、/80 以上のサブネットを使用して IPv6 ネットワークを構築してください。（CSCsk79791）

- ポリサー、シェイプ、またはシェイプ値がポリシーのリンク帯域幅のパーセンテージとして指定され、ポリシーが適用されているインターフェイスが、speed 10/100/1000 コマンドで特定の速度に強制される場合、適用されたポリサー、シェイプ、または帯域幅の値は、強制された新しい速度に対応する場合があります。

  サービス ポリシーは、パーセンテージのポリサー、シェイプ、またはシェイプ値で設定し、リンク速度は強制的に特定の値にする必要があります。次に例を示します。

  ```
  Policy-map p1
      class-map c1
         police rate percent 10
  ```

  回避策：speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー、シェイプ、またはシェイプ値を絶対値で指定します。次に例を示します。

  ```
  Policy-map p1
     class-map c1
       police rate 10 mbps
  ```

  （CSCsk56877）

- ip icmp unreachable コマンドが、レイヤ 3 インターフェイス上の IPv4 と IPv6 の両方のパケットに対する ICMP の到着不能メッセージの生成に影響する場合があります。さらに、IPv6 アドレスを持つレイヤ 3 インターフェイス上のレイヤ 3 の拒否 ACL では、ICMP の到着不能メッセージを生成せずに、拒否されたトラフィックを CPU にコピーしない場合があります。

  最初の問題は、IPv4 および IPv6 の両方のアドレスが設定されるデュアル レイヤ 3 のインターフェイスで発生します。2 番目の問題は、スイッチ上のすべてのレイヤ 3 のインターフェイスが IPv6 アドレスのみで設定されている場合に発生します。

  回避策：IPv4 および IPv6 の両方のアドレスが設定されているデュアルレイヤ 3 のインターフェイスを使用しないでください。

  スイッチを IPv6 レイヤ 3 のインターフェイス専用ルータとして使用しないでください。IPv4 アドレスの設定された SVI ごとに、少なくとも 1 つのレイヤ 3 インターフェイスがあることを確認してください。（CSCsk77234）

- インターフェイス コンフィギュレーションをレイヤ 3/ルータポートからレイヤ 2/スイッチポートに切り替えてからレイヤ 3/ルータポートに戻すと、ルータインターフェイスの IOS 設定が設定されていない場合でも、元のルータインターフェイスにアタッチされた IPv6 ACL が TCAM ハードウェアで正常にフラッシュされないことがあります。

  回避策：レイヤ 3 インターフェイスをルータポートからスイッチポートに切り替える前に、ルータインターフェイスの IPv6 ACL の設定を解除します。これにより、IPv6 ACL が IOS 実行コンフィギュレーションと TCAM ハードウェアの両方で正常にクリーンアップされます。（CSCsk60775）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth/shape fixes the issue などのキューイング パラメータをいくつか変更して再設定してください。（CSCsk62457）

- E シリーズ スイッチでファン トレイの障害またはスーパバイザでの危険温度のいずれかが発生すると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を特定します。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、原因はファン トレイの障害です。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザの臨界温度が障害のしきい値を超えたことが原因です。

  （CSCsk48632）

- モジュールにより危険温度またはシャットダウン温度のアラームが報告された場合でも、E シリーズ スーパバイザおよびラインカードの LED は緑に点灯したままです。LED はオレンジまたは赤に点灯するはずです。

これは、危険温度またはシャットダウン温度のアラームを報告する E シリーズのすべてのラインカードで発生します。実際の温度とアラームのステータスが show environment temperature コマンドの出力に表示されます。

回避策：LED の色に関してはありません。ただし、アラームが発生または解除されると、コンソール ログ メッセージと SNMP トラップが入力されます。また、温度アラームの現在のステータスが show environment temperature コマンドの出力に表示されます。（CSCsk57143）

- 2 つのスイッチが 2 つ以上のリンクを介してバックツーバックで接続されており、パケットの発信元がローカルにある場合、ソース IP アドレスが発信インターフェイスの IP アドレスと一致しないことがあります。ユニキャスト RPF 機能がイネーブルになっているこのようなパケットを受信するスイッチが、着信パケットをドロップする可能性があります。

  回避策：ありません。（CSCsh99124）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。さらに、物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- デフォルト以外のデュプレックス設定が FastEthernet インターフェイスに適用されていて、Cisco IOS リリース 12.2(31)SGA から 12.2(40)SG にアップグレードすると、FastEthernet 設定のデュプレックス設定は失われます。インターフェイスがデフォルトのデュプレックス設定に戻り、デュプレックス設定が show running コマンドの出力に表示されなくなります。

  回避策：実行コンフィギュレーションにデフォルト以外のデュプレックス設定がある場合、アップグレードする前にそれらの設定を控えておき、アップグレード完了後に再適用します。（CSCsk83670）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG で、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生します。

  回避策：X2 を再挿入します。（CSCsk43618）

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- ポリシーマップで、プライオリティ キューイング クラス設定の前に bandwidth remaining percent <> コマンドを設定したキューイングクラスがある場合、リロード時に bandwidth remaining percent <> コマンドのアクションが適用されません。

  回避策：ポリシーマップを再適用します。（CSCsk75793）

- 出力 QoS ポリシーが設定されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキング アクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の COS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された COS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 に説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能がイネーブルになっている場合、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを特定できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの COS/DSCP フィールドが強制的にゼロになります。

  インターフェイス上に存在する QoS ポリシーは、この COS/DSCP の値を分類に使用します。そのため、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。（CSCsh72408）

- ポートは、ポートチャネルのメンバーになるか、または AutoQoS を適用することができますが、両方はできません。これらの機能は相互排他的です。

  現在、ポートチャネルのメンバーであるポートに AutoQoS が適用されている場合、アプリケーションは拒否され、エラーメッセージが表示されます。ただし、その逆は正しくありません。AutoQoS が最初に適用され、ポートがポートチャネルに参加する場合、コマンドは受け入れられます。

  ポート g2/1 を使用する次の例は、回避すべき使用のタイプを示しています。

  ```
  conf t
  int g2/1
  auto qos voice trust
  channel-group 10 mode auto
  ```

  この例では、ポート（g2/1）に AutoQoS を適用し、その後ポートをポートチャネル（10）のメンバーにします。

  回避策：AutoQoS が有効になっているポートをポートチャネルのメンバーにしないでください。（CSCsi95018）

- デュアルレートポリサーに対して exceed burst が明示的に設定されていない場合、show policy-map コマンドを実行するとバースト値として「0」が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の exceed burst 値を調べます。（CSCsj44237）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力して、プログラムされている実際の *burst* 値を調べます。（CSCsi71036）

- cisco-phone マクロで設定したポート上で default interface を 2 回実行すると、バック トレースが表示されます。

  回避策：default interface コマンドを入力せずに、コンフィギュレーション行を一行ずつ削除します。（CSCsj23103）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキングアクションが表示されません。

  回避策：ありません。ただし、show policy-map name を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシ タイプが「Unknown」と表示されます。IOS を起動した後、シャーシ タイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- WS-X4648-RJ45V-E（PoE）および WS-X4648-RJ45V+E（ポートあたり 30 W の Premium PoE）ラインカード上で QoS ポリシーをキューイング アクション（分散またはシェーピング）で設定すると、SSO スイッチ オーバー後に分散およびシェーピングのパーセンテージ エラーが 3 パーセントに増大します。

  回避策：次のいずれかの操作を実行します。

  - インターフェイスからサービスポリシーを削除し、[no] service-policy {input|output} コマンドを使用して設定を再適用します。
  - shutdown を入力してから no shutdown を入力します。

  （CSCsm45156）

- 冗長 WS-X45-SUP6-E スーパバイザ エンジンを搭載したスイッチおよび RJ-45 を使用するよう設定された WS-X4506-GB-T インターフェイスを搭載したスイッチでは、SSO スイッチオーバーの後、インターフェイス上の QoS 設定が無効になります。さらに、メディア タイプを SFP に変更した後、再度 RJ-45 に戻すと、QoS 設定が失われる可能性があります。

  QoS 設定は実行コンフィギュレーションには表示されますが、インターフェイス上では維持されません。

  回避策：QoS 設定をインターフェイスに再適用します。（CSCsm58839）

- ポリシーマップで「class-default」クラスマップの DBL アクションを指定すると、デフォルト キューのサイズによっては動作しないことがあります。

  回避策：DBL アクションがデフォルトキューで動作することを確認するには、queue-limit コマンドを使用して明示的にキューサイズを指定します。サイズの範囲は、queue-limit コマンドにより表示されます。（CSCso06422）

- IPv4 ルートが RTR2 から IPv6 ピアリングを介して RTR3 にアドバタイズされると、RTR2 の IPv6 アドレスの最初の 32 ビットが IPv4 アドレスに変換されます。この IPv4 アドレスは、RTR3 に対するネクストホップ アドレスとしてアドバタイズされます。このアドレスが Martian アドレスになると、RTR3 は BGP 更新メッセージを無視するため、IPv4 ルートが認識されません。

  RTR3 でインバウンド ルートマップを設定して RTR2 がアドバタイズしたネクストホップを上書きしても、BGP 更新メッセージは無視されるため、この問題を回避することはできません。

  回避策：RTR2 でアウトバウンドルートマップを設定して、暗示的にプロトコルで取得するのではなく、明示的に IPv4 ネクストホップを設定します。（CSCsk65139）

- IPv6 EIGRP に割り当てられたリンク帯域幅を、ipv6 bandwidth-percent eigrp as-number percent コマンドを使用して変更しようとすると、スーパバイザエンジンがリロードします。冗長性をイネーブルにすると、STANDBY スーパバイザ エンジンが ACTIVE になり、リロードされたスーパバイザ エンジンが STANDBY に設定されます。

  回避策：ありません。（CSCso30051）

- WS-X45-SUP6-E スーパバイザの ROMMON をバージョン 0.34 から最新のバージョンにアップグレードすると、アップリンクがダウンします。

  この動作は、ACTIVE スーパバイザ エンジンが IOS で、STANDBY スーパバイザ エンジンが ROMMON でそれぞれ実行され、STANDBY の ROMMON がバージョン 0.34 または最新バージョンにアップグレードされたときに、冗長スイッチで発生します。アップグレード処理により STANDBY スーパバイザ エンジンのアップリンクがダウンしますが、ACTIVE スーパバイザ エンジンはこれを認識しません。

  回避策：通常の操作を再開するには、次のいずれかの操作を実行します。

  - redundancy reload shelf コマンドで、両方のスーパバイザをリロードします。

  - STANDBY スーパバイザ エンジンをしばらくの間シャーシから抜き出して、電源を再投入します。

    リンクフラップの問題に対する回避策はありません。（CSCsm81875）

- 最初にインターフェイスで IPv6 をイネーブルにせずに ipv6 mtu mtu-value コマンドを使用してインターフェイス上で IPv6 MTU を設定すると、起動時にスイッチが無期限に停止する場合があります。

  回避策：インターフェイス上で IPv6 MTU を設定する前に、インターフェイス上で IPv6 を有効にする必要があります。IPv6 をイネーブルにするには、ipv6 enable コマンドを使用します。

  この問題が発生した場合は、次のコマンドを入力してスイッチを復旧してください。

---

1. rommon プロンプトで confreg コマンドを使用して、スタートアップ コンフィギュレーションを無視します。
2. reset コマンドを使用して、スイッチをリブートします。
3. copy startup-config running-config コマンドを使用して、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。
4. ipv6 enable コマンドを使用して、インターフェイス上で IPv6 を有効にします。
5. ipv6 mtu mtu-value コマンドを使用して、インターフェイス上で IPv6 MTU を設定します。
6. ccopy running-config startup-config コマンドを使用して、回復コンフィギュレーションを保存します。
7. スイッチで reload コマンドを使用して、Rommon に戻ります。
8. rommon から、confreg コマンドを使用して、スタートアップ コンフィギュレーションを処理します。
9. スイッチをリセットして、通常の操作を再開します。（CSCso42867）

- Catalyst 4500 シリーズ スイッチを Supervisor Engine 6-E とともに使用し、インターフェイスに出力サービスポリシーが設定されている場合、同じ出力サービスポリシーが適用されている別のインターフェイスで shut/no shut を入力すると、キューがフル状態のために出力がドロップされます。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、および 12.2(46)SG で発生します。

  この問題は、12.2(50)SG で解決されています。

  回避策：qos autoqos マクロを使用しないでください。

  ポリシーマップが複数のターゲットで共有されている場合は、パーセンテージベースのアクションを使用しないでください。ポリシング、シェーピング、および帯域幅アクションでは、絶対値を使用する必要があります。そのためには、スイッチでサポートされる 4 つのインターフェイス速度（10M、100M、1G、および 10G）ごとに異なるポリシーマップが必要です。そのため、パーセンテージベースのアクションで単一のポリシーマップを有効にするのではなく、4 つの異なるポリシーマップを作成する必要があります。これは、サービスポリシーの方向に関係なく、すべての共有ポリシーマップに適用されます。

  （CSCsr12142）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

Cisco IOS リリース 12.2(44)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(44)SG で解決済みの警告について説明します。

- EtherChannel のメンバーである物理ポートからサービスポリシーが削除されると、LACP または PAGP プロトコルベースの EtherChannel がダウンします。ポートチャネルメンバーは再びバンドルされますが、相手側とのプロトコルパケットの交換に失敗したため、中断状態のままになります。

  回避策：EtherChannel メンバーから削除する前に、チャネルからサービスポリシーを削除します。その後、サービスポリシーをチャネルに戻します。（CSCsk70568）

- キューイングポリシーマップで bandwidth percentage アクションを使用する場合、実際の帯域幅共有は、設定されたポリシーマップとは異なります。

  キューイング QoS ポリシーでは、明示的にユーザ指定された帯域幅共有が指定されている 0 個以上のキューイングクラスが存在する可能性があります。このようなユーザ指定の帯域幅共有を持たないキューイングクラスは 0 個以上存在できます。システムは、未割り当ての帯域幅共有を取得し、後者の一連のクラスに均等に割り当てます。

  パーセントベースの帯域幅割り当てを使用する場合、共有が 1% 未満になると、それらのクラスに対応するキューは、新しい帯域幅共有ではハードウェアで更新されません。それらのキューは、予想される帯域幅の共有を超えています。

  回避策：未割り当ての帯域幅のパーセンテージが、明示的な bandwidth percentage コマンドが指定されていないキューの数以上であることを確認します。これには、デフォルトキューとプライオリティキューを含める必要があります。（CSCsk77757）

- ポートチャネル メンバー ポートのサービスポリシーが変更されると、一部のクラスのトラフィックがドロップされることがあります。

  回避策：次の手順を実行します。

a. このポリシーマップが接続されているインターフェイスをポートチャネルから設定解除します。

b. ポリシーマップを変更します。

c. ポートチャネルでインターフェイスを設定します。

- レイヤ 2 ポートで AutoQoS を設定し、ポートをレイヤ 3 に変更してから、そのポートで AutoQoS を削除すると、AutoQoS が適用されたときと削除されたときの間で不一致が生じるため、このプロセスではポート上の QoS サービスポリシーがクリーンアップされません。

  同様に、レイヤ 3 ポートで AutoQoS を設定し、ポートをレイヤ 2 に変更してから、そのポートで AutoQoS を削除した場合、このプロセスではポート上の QoS サービスポリシーが正常に削除されません。

  次のようなシーケンスでは、ポート g2/1 で問題が発生します。

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
no auto qos voice trust
```

  回避策：ポートの設定を AutoQoS が適用されたときの設定に戻します。ポートがレイヤ 2 ポートであるときに AutoQoS が有効になっていた場合は、AutoQoS を削除する前にレイヤ 2 に戻す必要があります。同様に、AutoQoS が最初に適用されたときにポートがレイヤ 3 に設定されていた場合、AutoQoS を削除する前にレイヤ 3 に戻す必要があります。

  問題のシーケンスを参照すると、最初にレイヤ 2 ポートに AutoQoS を適用し、レイヤ 3 に変更してから、レイヤ 2 に戻して、AutoQoS を削除します。

```
conf t
int g2/1
switchport
auto qos voice trust
no switchport
switchport
no auto qos voice trust
```

  （CSCsk95871）

- ポート単位の VLAN 単位 QoS ポリシーで設定されたトランクポートにキューイングポリシーが適用されている場合、ポートレベルのキューイングポリシーは VLAN 単位ポリシーの一部として処理され、ブートアップ時に拒否されます。

  キューイングポリシーは、出力方向の物理インターフェイスでのみサポートされます。

  回避策：ブートアップ後、物理インターフェイスにキューイングポリシーを再接続します。（CSCsk87548）

- PVQoS ポリシーのあるポート チャネルを削除すると、スイッチはクラッシュします。

  回避策：ポートチャネルを削除する前に、次の手順を実行します。

  1. 存在する場合は PVQoS ポリシーを削除します。

  2. no vlan-range コマンドを使用して、ポートチャネル上の VLAN 設定を削除します。

  （CSCsk91916）

- cbQoSPoliceCfgTable mib オブジェクトは、police bps byte コマンドによって入力されません。

  回避策：ありません。（CSCsk45940）

- exceed-action drop を使用してクラスマップを設定した場合、exceed-action transmit を使用して同じクラスマップを再設定すると、同じクラスマップの設定が競合します。

回避策：exceed-action などのクラスマップアクションを変更する場合は、ポリシーマップサブモードで no class c1 コマンドを使用してクラスマップを削除する必要があります。次に、更新された変更を含む新しいクラスマップを適用します。

（CSCsk70826）

- SSL パケットの処理中に Cisco IOS デバイスがクラッシュすることがあります。これは、SSL ベースのセッションの終了時に発生する可能性があります。問題のパケットは不正な形式ではなく、通常はパケット交換の一部として受信されます。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  影響を受けるサービスを無効にする以外に、この脆弱性のエクスプロイトを軽減する回避策はありません。

  このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl

  （CSCsj85065）

- Cisco IOS ソフトウェア マルチプロトコルラベルスイッチング（MPLS）転送インフラストラクチャ（MFI）は、特別に細工されたパケットからのサービス妨害（DoS）攻撃に対して脆弱です。MFI のみがこの脆弱性の影響を受けます。MFI に置き換えられた古いラベル転送情報ベース（LFIB）の実装は影響を受けません。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。

  このアドバイザリは、次の URL に掲載されています。

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi

  （CSCsk93241）

Cisco IOS リリース 12.2(40)SG の未解決の警告

ここでは、Cisco IOS リリース 12.2(40)SG の未解決の警告について説明します。

- SSO モードで動作している冗長シャーシで access-list N permit host hostname コマンドを入力すると、次の syslog メッセージが表示されることがあります。このコマンドは冗長スーパバイザエンジンとは同期されないため、キープアライブ警告が表示されます。

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

回避策：access-list N permit host hostname コマンドを使用する場合は、ホスト名ではなく、ホストの IP アドレスを指定します。（CSCef67489）

- まれに、MAC ACL ベースのポリサーを使用している場合、show policy-map interface fa6/1 のパケット照合カウンタに、一致するパケットが表示されないことがあります。

```
clearwater# show policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

回避策：システムを介して送信される MAC アドレスが学習されていることを確認します。

（SCef01798）

- SSO スイッチオーバーの後、UDLD err-disable ステートになっているポート上で shutdown コマンドを入力してから no shutdown コマンドを入力すると、スイッチコンソールに「PM-4-PORT_INCONSISTENT」エラーメッセージが表示される場合があります。これはスイッチには影響しません。ポートは UDLD err-disable ステートのままです。同じポート上で shutdown コマンドを再入力してから no shutdown コマンドを入力すると、エラーメッセージは表示されなくなります。

回避策：ありません。（CSCeg48586）

- ip http secure-server コマンドを入力すると（またはスタートアップ コンフィギュレーションから読み込まれると）、デバイスは起動時に永続的な自己署名証明書の存在を確認します。
  - このような証明書が存在せず、デバイスのホスト名と default_domain が設定されている場合、永続的な自己署名証明書が生成されます。
  - このような証明書が存在する場合、証明書の FQDN が現在のデバイスのホスト名および default_domain と比較されます。これらのいずれかが証明書の FQDN と異なる場合は、既存の永続的な自己署名証明書が更新された FQDN を含む新しい証明書に置き換えられます。既存のキーペアが新しい証明書で使用されることに注意してください。

  冗長性をサポートするスイッチでは、自己署名証明書がアクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンでそれぞれ個別に生成されます。そのため、証明書は異なったものになります。スイッチオーバーの後、古い証明書を保持している HTTP クライアントは HTTPS サーバに接続できなくなります。

  回避策：再接続します。（CSCsb11964）

- Cisco IOS 12.2（31）SG 以降のリリースにアップグレードした後、SPAN 送信元として設定し、スタートアップ コンフィギュレーション ファイルに保存した CPU キューの一部が、以前のソフトウェア リリースの場合と同様に動作しないことがあります。

  これは、12.2（31）SG より前のリリースで SPAN 送信元として設定され、スタートアップ コンフィギュレーションに保存された、次のいずれかのキューがあるスイッチにのみ影響します。12.2（31）SG にアップグレードした後は、SPAN 宛先が同じトラフィックを取得することはありません。

QueueID	以前の QueueName	新しい QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet

QueueID	以前の QueueName	新しい QueueName
8	<未使用のキュー>	control-packet
11	<未使用のキュー>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

回避策：12.2(31)SG 以降のリリースにアップグレードした後、以前の SPAN 送信元の設定を削除して、新しいキューの名前/ID で再設定します。次に例を示します。

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

（CSCsc94802）

- ハードウェアの消耗により無効になっている IP CEF を有効にするには、ip cef distributed コマンドを使用します。

  回避策：ありません。（CSCsc11726）

- 発信インターフェイスが Catalyst 4500 シリーズ スイッチの IP アンナンバード ポートにある場合、IP リダイレクトが送信されないことがあります。

  これは、次の理由で発生する場合があります。

  - パケットは、Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に、IP アンナンバード発信ポートに IP リダイレクト送信されなければなりません。
  - これは、スイッチ管理者が IP アンナンバードが有効になっている発信インターフェイスで shutdown コマンドと no shutdown コマンドを入力した場合も同様です。スイッチはリダイレクト送信が必要なパケットを受信し、宛先 MAC アドレスは、すでに ARP テーブルに存在します。

  回避策：

  - Catalyst 4500 シリーズ スイッチを起動してから 3 分以内に IP リダイレクトを IP アンナンバード ポートに送信する必要のあるパケットを投入しないでください。
  - ホスト側で正しいデフォルト ゲートウェイを設定してください。（CSCse75660）

- SSO モードでアクティブ スーパバイザ エンジン上で bgp dampening route-map bgp_damp コマンドを設定すると、次のシステムログがスタンバイ スーパバイザ エンジンのコンソールに表示されます。

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  この時点で、アクティブ スーパバイザ エンジン上で bgp dampening コマンドに戻ると、新しいコマンドがスタンバイ スーパバイザ エンジンと同期されなくなります。

  回避策：no bgp dampening コマンドを入力してから、bgp dampening コマンドを入力します。（CSCse12485）

- IEEE 802.1Q のタグの付いた非 IP トラフィックをポリシングしてトラフィック パフォーマンスを測定する場合、qos account layer2 encapsulation を設定している場合でも、ポリサーにより 802.1Q タグを構成する 4 バイトが qos account layer2 encapsulation を設定していても、ポリサーにより 802.1Q タグを構成する 4 バイトが除外されます。

  回避策：ありません。（CSCsg58526）

- インターフェイスをシャットダウンしてハードコードされたデュプレックスと速度の設定が削除されると、show interface status コマンドの出力のデュプレックスと速度に「a-」が追加されます。

  これはパフォーマンスには影響しません。

  回避策：no shutdown コマンドを入力します。（CSCsg27395）

- 任意のポートからトランシーバを迅速に抜き取って同じシャーシの別のポートに取り付けると、重複した seeprom メッセージが表示され、ポートでトラフィックを処理できないことがあります。

  回避策：新しいポートからトランシーバを抜き取って、古いポートに取り付けます。古いポートで SFP が認識されたら、これをゆっくり抜き取って新しいポートに挿入します。（CSCse34693）

- Cisco IOS リリース 12.2(31)SGA または 12.2(31)SGA1 から Cisco IOS リリース 12.2(37)SG以降のイメージへのISSUアップグレード中に、次のエラーメッセージが表示されます。

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  回避策：ありません。このメッセージは情報メッセージです。（CSCsi60913）

- ISSU アップグレードを実行し、アクティブ スーパバイザ エンジンとスタンバイ スーパバイザ エンジンのバージョンが異なる場合、スタンバイ スーパバイザ エンジンのコンソールに次のメッセージが表示されます。

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  回避策：ありません。これは通知メッセージです。（CSCsi60898）

Supervisor Engine 6-E に固有の問題

- 必要な QoS 操作を適用するためのソフトウェア QoS が .1Q パケットと正しく一致しません。

  回避策：なし。

  Cisco IOS Release 12.2（40）SG リリースでは、ソフトウェア QoS ルックアップを行う 1Q パケット処理はサポートされていません。（CSCsk66449）

- EtherChannel のメンバーである物理ポートからサービスポリシーが削除されると、LACP または PAGP プロトコルベースの EtherChannel がダウンします。ポートチャネルメンバーは再びバンドルされますが、相手側とのプロトコルパケットの交換に失敗したため、中断状態のままになります。

  回避策：EtherChannel メンバーからサービスポリシーを削除する前に、チャネルから削除します。その後、サービスポリシーをチャネルに戻します。（CSCsk70568）

- キューイングポリシーマップで bandwidth percentage アクションを使用する場合、実際の帯域幅共有は、設定されたポリシーマップとは異なります。

  キューイング QoS ポリシーでは、明示的にユーザ指定された帯域幅共有が指定されている 0 個以上のキューイングクラスが存在する可能性があります。このようなユーザ指定の帯域幅共有を持たないキューイングクラスは 0 個以上存在できます。システムは、未割り当ての帯域幅共有を取得し、後者の一連のクラスに均等に割り当てます。

  パーセントベースの帯域幅割り当てを使用する場合、共有が 1%未満になると、それらのクラスに対応するキューは、新しい帯域幅共有のハードウェアでは更新されません。それらのキューは、予想される帯域幅の共有を超えています。

  回避策：未割り当ての帯域幅のパーセンテージが、明示的な bandwidth percentage コマンドが指定されていないキューの数以上であることを確認します。これには、デフォルトキューとプライオリティキューを含める必要があります。（CSCsk77757）

- すべての機能の組み合わせがハードウェアにより同時にサポートされるわけではありません。サポートされていない機能の組み合わせが設定されている場合、パケットはソフトウェアで処理され、次の内容を示すログ メッセージが生成されます。

```
%C4K_HWACLMAN-4-ACLHWLABELERR: Path (in :50, 1006) label allocation failure:
SignatureInconsistent - packets will be handled in software, QoS is disabled.
```

このような問題は、cos ビット上で一致する QoS ポリシーを、アドレスの下位 48 ビットを部分的にマスクする IPv6 送信元アドレスと一致する IPv6 ACL コンフィギュレーションと組み合わせようとすると発生する場合があります(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場合、/81 ～ /127 の範囲の IPv6 サブネットを使用することでもこのような問題が発生します)。

回避策:競合する機能の組み合わせを設定しないでください。現在、上記の COS ビット上で一致する QoS ポリシーと送信元アドレスの下位 48 ビットを部分的にマスクする IPv6 設定の競合は、機能の組み合わせの競合としてのみ認識されています。QoS ポリシーにより COS ビット上での一致が要求される場合、/80 以上のサブネットを使用して IPv6 ネットワークを構築してください。(CSCsk79791)

- ポリサー、シェイプ、またはシェイプ値がポリシーのリンク帯域幅のパーセンテージとして指定され、ポリシーが適用されているインターフェイスが、speed 10/100/1000 コマンドで特定の速度に強制される場合、適用されたポリサー、シェイプ、またはシェイプの値は、強制された新しい速度に対応する場合があります。

サービス ポリシーは、パーセンテージのポリサー、シェイプ、またはシェイプ値で設定し、リンク速度は強制的に特定の値にする必要があります。次に例を示します。

```
Policy-map p1
    class-map c1
       police rate percent 10
```

回避策:speed auto 10/100/1000 コマンドを使用するか、またはパーセンテージの値ではなく、ポリサー、シェイプ、またはシェイプ値を絶対値で指定します。次に例を示します。

```
Policy-map p1
   class-map c1
     police rate 10 mbps
```

(CSCsk56877)

- ip icmp unreachable コマンドが、レイヤ 3 インターフェイス上の IPv4 と IPv6 の両方のパケットに対する ICMP の到着不能メッセージの生成に影響する場合があります。さらに、IPv6 アドレスを持つレイヤ 3 インターフェイス上のレイヤ 3 の拒否 ACL では、ICMP の到着不能メッセージを生成せずに、拒否されたトラフィックを CPU にコピーしない場合があります。

最初の問題は、IPv4 および IPv6 の両方のアドレスが設定されるデュアル レイヤ 3 のインターフェイスで発生します。2 番目の問題は、スイッチ上のすべてのレイヤ 3 のインターフェイスが IPv6 アドレスのみで設定されている場合に発生します。

回避策:IPv4 および IPv6 の両方のアドレスが設定されているデュアルレイヤ 3 のインターフェイスを使用しないでください。

スイッチを IPv6 レイヤ 3 のインターフェイス専用ルータとして使用しないでください。IPv4 アドレスの設定された SVI ごとに、少なくとも 1 つのレイヤ 3 インターフェイスがあることを確認してください。(CSCsk77234)

- インターフェイス コンフィギュレーションをレイヤ 3/ルータポートからレイヤ 2/スイッチポートに切り替えてからレイヤ 3/ルータポートに戻すと、ルータインターフェイスの IOS 設定が設定されていない場合でも、元のルータインターフェイスにアタッチされた IPv6 ACL が TCAM ハードウェアで正常にフラッシュされないことがあります。

回避策：レイヤ 3 インターフェイスをルータポートからスイッチポートに切り替える前に、ルータインターフェイスの IPv6 ACL の設定を解除します。これにより、IPv6 ACL が IOS 実行コンフィギュレーションと TCAM ハードウェアの両方で正常にクリーンアップされます。（CSCsk60775）

- 状況によっては、DBL がサービスポリシーから削除された後であっても、DBL により 1 つ以上のフローが引き続きドロップされることがあります。

  出力サービスポリシーがインターフェイスに割り当てられている場合、ポリシーで DBL をキューに適用するよう設定すると、キューに置かれたフローが DBL アルゴリズムの対象となります。1 つ以上のフローが belligerent（キューの輻輳のため、ドロップに応答して返信待機しないフロー）として分類されると、これらのフローはキューで DBL が無効になった後でも belligerent に分類されたままになります。

  このような状態が続く場合、問題となっている転送キューは長時間輻輳します。この輻輳は、belligerent のままになっているフローが原因で発生します。

  回避策：問題となっているキューがデフォルト以外の場合（キューイングアクションがポリシーマップの class-default クラスで設定されていない場合）、サービスポリシーを取り外してから再度取り付けます。

  デフォルトのキューでこの問題が発生した場合、bandwidth/shape fixes the issue などのキューイング パラメータをいくつか変更して再設定してください。（CSCsk62457）

- E シリーズ スイッチでファン トレイの障害またはスーパバイザでの危険温度のいずれかが発生すると、シャーシの電源が切断されます。show crashdump コマンドの出力に、電源切断の原因が表示されません。

  回避策：show log コマンドを使用して、電源切断の原因を特定します。

  - ログに LogGalInsufficientFansDetected メッセージがある場合、原因はファン トレイの障害です。
  - ログに LogRkiosModuleShutdownTemp メッセージがある場合、スーパバイザの臨界温度が障害のしきい値を超えたことが原因です。

  （CSCsk48632）

- モジュールにより危険温度またはシャットダウン温度のアラームが報告された場合でも、E シリーズ スーパバイザおよびラインカードの LED は緑に点灯したままです。LED はオレンジまたは赤に点灯するはずです。

  これは、危険温度またはシャットダウン温度のアラームを報告する E シリーズのすべてのラインカードで発生します。実際の温度とアラームのステータスが show environment temperature コマンドの出力に表示されます。

  回避策：LED の色に関してはありません。ただし、アラームの発生またはクリア時には、コンソールログメッセージと SNMP トラップが発行されます。また、温度アラームの現在のステータスが show environment temperature コマンドの出力に表示されます。（CSCsk57143）

- キューイングポリシーマップが切り離されてすぐに接続された場合、デフォルト以外のトラフィッククラスのパケットはほとんどドロップされません。

  このシナリオでは、ハードウェアが新しい設定（[デタッチ（Detach）] > [アタッチ（Attach）]）でプログラムされるまで、デフォルト以外のキューは非アクティブです。したがって、それらのキューがアクティブになるまで、デフォルト以外のキューに一致するトラフィックはドロップされます。

  回避策：なし。（CSCsk85379）

- ポートチャネル メンバー ポートのサービスポリシーが変更されると、一部のクラスのトラフィックがドロップされることがあります。

  回避策：次の手順を実行します。

a. このポリシーマップがアタッチされているインターフェイスをポートチャネルから設定解除します。
b. ポリシーマップを変更します。
c. ポートチャネルでインターフェイスを設定します。

（CSCsk77119）

- 2 つのスイッチが 2 つ以上のリンクを介してバックツーバックで接続されており、パケットの発信元がローカルにある場合、ソース IP アドレスが発信インターフェイスの IP アドレスと一致しないことがあります。ユニキャスト RPF 機能がイネーブルになっているこのようなパケットを受信するスイッチが、着信パケットをドロップする可能性があります。

  回避策：ありません。（CSCsh99124）

- Supervisor Engine 6-E を搭載した Catalyst 4500 シリーズ スイッチは、システム全体で最大 32 の MTU 値をサポートします。

  Cisco IOS Release 12.2（40）SG を実行しているスイッチ上では、モジュールがリセットされると、ラインカードで設定されているすべての MTU 値がデフォルトに設定されます。さらに、物理的に移動されたモジュールの MTU 値は維持されません。

  回避策：ありません。（CSCsk52542）

- デフォルト以外のデュプレックス設定が FastEthernet インターフェイスに適用されていて、Cisco IOS リリース 12.2(31)SGA から 12.2(40)SG にアップグレードすると、FastEthernet 設定のデュプレックス設定は失われます。インターフェイスがデフォルトのデュプレックス設定に戻り、デュプレックス設定が show running コマンドの出力に表示されなくなります。

  回避策：実行コンフィギュレーションにデフォルト以外のデュプレックス設定がある場合、アップグレードする前にそれらの設定を控えておき、アップグレード完了後に再適用します。（CSCsk83670）

- まれに、実行中の WS-X4706-10GE で X2 SR トランシーバを使用する場合 Cisco IOS リリース 12.2(40)SG で、カードまたは X2 の挿入時にリロード後または電源の再投入後に CTC エラーが発生します。

  回避策：X2 を再挿入します。（CSCsk43618）

- system class-maps system-cpp-dhcp-cs、system-cpp-dhcp-sc、および system-cpp-dhcp-ss として識別された DHCP トラフィックに適用されたコントロール プレーン ポリシングが、有効にならないことがあります。

  回避策：ありません。（CSCsk67395）

- ポリシーマップで、プライオリティ キューイング クラス設定の前に bandwidth remaining percent <> コマンドを設定したキューイングクラスがある場合、リロード時に bandwidth remaining percent <> コマンドのアクションが適用されません。

  回避策：ポリシーマップを再適用します。（CSCsk75793）

- 出力 QoS ポリシーが設定されたインターフェイス上で CPU により .1X パケットが転送されると、パケットが一致せず、QoS マーキング アクションが行われずに終了します。

  パケットがその CPU に送信されると、他のインターフェイスに送信される場合があります。その場合、.1X パケットの元の COS 値をソフトウェア QoS（CSCsk66449 による）によって一致させることはできません。パケットは、生成された COS 値（ここで説明した MLDv1 パケットの場合は 7）と一緒に送信されます。

  回避策：ありません。

  この問題の根本的原因の一部は、CSCsk66449 に説明しています。ここでは、ソフトウェア QoS によって .1X パケットを一致させることができないことを示しています。（CSCsk72544）

- インターフェイス上で信頼境界機能がイネーブルになっている場合、現在の動作状態を確認するコマンドはありません。

  回避策：ありません。信頼境界ステートを明示的に確認することはできません。ただし、間接的にこのステートを特定できます。

  信頼境界機能は、パケットの COS/DSCP 値が信頼できるかどうかを確認します。インターフェイスが信頼ステートになっていない場合、受信したパケットの COS/DSCP フィールドが強制的にゼロになります。

  インターフェイス上に存在する QoS ポリシーは、この COS/DSCP の値を分類に使用します。そのため、パケットの分類がパケット値に基づいて行われる場合は、インターフェイスが信頼ステートになっていることがわかります。（CSCsh72408）

- ポートは、ポートチャネルのメンバーになるか、または AutoQoS を適用することができますが、両方はできません。これらの機能は相互排他的です。

  現在、ポートチャネルのメンバーであるポートに AutoQoS が適用されている場合、アプリケーションは拒否され、エラーメッセージが表示されます。ただし、その逆は正しくありません。AutoQoS が最初に適用され、ポートがポートチャネルに参加する場合、コマンドは受け入れられます。

  ポート g2/1 を使用する次の例は、回避すべき使用のタイプを示しています。

  ```
  conf t
  int g2/1
  auto qos voice trust
  channel-group 10 mode auto
  ```

  この例では、ポート（g2/1）に AutoQoS を適用し、その後ポートをポートチャネル（10）のメンバーにします。

  回避策：AutoQoS が有効になっているポートをポートチャネルのメンバーにしないでください。（CSCsi95018）

- レイヤ 2 ポートで AutoQoS を設定し、ポートをレイヤ 3 に変更してから、そのポートで AutoQoS を削除すると、AutoQoS の適用時と削除時の間で不一致が生じるため、プロセスによってポート上の QoS サービスポリシーがクリーンアップされません。

  同様に、レイヤ 3 ポートで AutoQoS を設定し、ポートをレイヤ 2 に変更してから、そのポートで AutoQoS を削除した場合、このプロセスではポート上の QoS サービスポリシーが正常に削除されません。

  次のようなシーケンスでは、ポート g2/1 で問題が発生します。

  ```
  conf t
  int g2/1
  switchport
  auto qos voice trust
  no switchport
  no auto qos voice trust
  ```

  回避策：ポートの設定を AutoQoS が適用されたときの設定に戻します。ポートがレイヤ 2 ポートであるときに AutoQoS が有効になっていた場合は、AutoQoS を削除する前にレイヤ 2 に戻す必要があります。同様に、AutoQoS が最初に適用されたときにポートがレイヤ 3 に設定されていた場合、AutoQoS を削除する前にレイヤ 3 に戻す必要があります。

  問題のシーケンスを参照すると、最初にレイヤ 2 ポートに AutoQoS を適用し、レイヤ 3 に変更してから、レイヤ 2 に戻して、AutoQoS を削除します。

  ```
  conf t
  int g2/1
  switchport
  auto qos voice trust
  no switchport
  ```

```
switchport
no auto qos voice trust
```

（CSCsk95871）

- exceed-action drop を使用してクラスマップを設定した場合、exceed-action transmit を使用して同じクラスマップを再設定すると、同じクラスマップの設定が競合します。

  回避策：exceed-action などのクラスマップアクションを変更する場合は、ポリシーマップサブモードで no class c1 コマンドを使用してクラスマップを削除する必要があります。次に、更新された変更を含む新しいクラスマップを適用します。

  （CSCsk70826）

- ルーテッドポートに割り当てられた VLAN にポリシーを適用すると、内部 VLAN がポリシングされます。

  回避策：ルーテッドポートに内部的に割り当てられた VLAN は作成しないでください。（CSCsh60244）

- デュアルレートポリサーに対して exceed burst が明示的に設定されていない場合、show policy-map コマンドを実行するとバースト値として「0」が表示されます。

  回避策：show policy-map interface コマンドを入力します。（CSCsj44237）

- シングルレートポリサーに *burst* が明示的に設定されていない場合、**show policy-map** コマンドで不正な burst 値が表示されます。

  回避策：show policy-map interface コマンドを入力します。（CSCsi71036）

- ポート単位の VLAN 単位 QoS ポリシーで設定されたトランクポートにキューイングポリシーが適用されている場合、ポートレベルのキューイングポリシーは VLAN 単位ポリシーの一部として処理され、起動時に拒否されます。

  キューイングポリシーは、出力方向の物理インターフェイスでのみサポートされます。

  回避策：ブートアップ後、物理インターフェイスにキューイングポリシーを再接続します。（CSCsk87548）

- PVQoS ポリシーのあるポート チャネルを削除すると、スイッチはクラッシュします。

  回避策：ポート チャネルを削除する前に、次の作業を実行します。

  1. 存在する場合は PVQoS ポリシーを削除します。

  2. no vlan-range コマンドを使用して、ポートチャネル上の VLAN 設定を削除します。

  （CSCsk91916）

- cbQosPoliceCfgTable mib オブジェクトは、police bps byte コマンドによって入力されません。

  回避策：ありません。（CSCsk45940）

- cisco-phone マクロで設定したポート上で default interface を 2 回実行すると、バック トレースが表示されます。

  回避策：default interface コマンドを入力せずに、コンフィギュレーション行を一行ずつ削除します。（CSCsj23103）

- show policy-map vlan vlan コマンドを入力すると、VLAN で設定されている無条件のマーキング アクションが表示されません。

  回避策：ありません。ただし、show policy-map name を入力すると、無条件のマーキング アクションが表示されます。（CSCsi94144）

- ROMMON を実行している Catalyst 4503-E シャーシの Supervisor Engine II-Plus-TS では、シャーシ タイプが「Unknown」と表示されます。IOS を起動した後、シャーシ タイプは正しく表示されます。

  回避策：ありません。（CSCsl72868）

- Catalyst 4500 シリーズ スイッチを Supervisor Engine 6-E とともに使用し、インターフェイスに出力サービスポリシーが設定されている場合、同じ出力サービスポリシーが適用されている別のインターフェイスで shut/no shut を入力すると、キューがフル状態のために出力がドロップされます。

  この問題は、Cisco IOS リリース 12.2(40)SG、12.2(44)SG、および 12.2(46)SG で発生します。

  この問題は、12.2(50)SG で解決されています。

  回避策：qos autoqos マクロを使用しないでください。

  ポリシーマップが複数のターゲットで共有されている場合は、パーセンテージベースのアクションを使用しないでください。ポリシング、シェーピング、および帯域幅アクションでは、絶対値を使用する必要があります。そのためには、スイッチでサポートされる 4 つのインターフェイス速度（10M、100M、1G、および 10G）ごとに異なるポリシーマップが必要です。そのため、パーセンテージベースのアクションで単一のポリシーマップを有効にするのではなく、4 つの異なるポリシーマップを作成する必要があります。これは、サービスポリシーの方向に関係なく、すべての共有ポリシーマップに適用されます。

  （CSCsr12142）

- Supervisor Engine-6E でネストされたポリシーマップ機能を使用しようとすると、スイッチがリブートする可能性があります。

  回避策：Cisco IOS リリース 12.2(40)SG および 12.2(44)SG では、ネストされたポリシーマップ機能を使用しないでください。（CSCsy80664）

- ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

  次の条件では、RACL が正しく機能しなくなる可能性があります。

  - ACL は、インターフェイスの出力方向に適用されます。
  - IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

  このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
    permit icmp any any nd-ns sequence 10
    deny ipv6 any any sequence 20

IPv6 access list a2
   permit icmp 2020::/96 any nd-ns sequence 10
    deny ipv6 any any sequence 20
```

  回避策：ありません。

  CSCtc13297

Cisco IOS リリース 12.2(40)SG の解決済みの警告

ここでは、Cisco IOS リリース 12.2(40)SG で解決済みの警告について説明します。

- コンソールから scp コピーを開始し、タイムアウトが発生するまでの遅延が十分にある場合、コンソールは切断されます。

  回避策：

  - 別のコピープロトコルを使用します。
  - より長い SSH タイムアウトを設定します。

  （CSCsc94317）

- dot1x（RADIUS 割り当て VLAN）、ポートセキュリティおよび音声 VLAN が、電話機と PC が接続されているポートで有効になっており、PC が RADIUS 割り当て VLAN で認証されると、スイッチオーバー時に PC からの最初のパケットがセキュリティ違反をトリガーします。

  回避策：ポートで shut/no shut と入力して、PC を正しく認証します。（CSCsi31362）

- ISSU runversion または冗長スイッチオーバー中に、スイッチがレイヤ 3 パケットの転送を数秒間停止します。

  トラフィック損失は、トラフィックが通過するインターフェイスが HSRP で設定され、現在 HSRP アクティブ状態である場合にのみ発生します。

  回避策：ありません。（CSCsi40980）

- Cisco IOS リリース 12.2(31)SGA および後続のメンテナンスリリースからリリース 12.2(37)SG1 にアップグレードしようとすると、「issu commitversion」の実行時に次の無害なメッセージが表示されます。

```
At ACTIVE:
ISSU_PROCESS-3-SYSTEM: Failed to set Standby ISSU state to the local ISSU state.

At STANDBY:
ISSU_PROCESS-3-SYSTEM: STANDBY:System not in [Init (Commit Version)] or [Init (Commit
Version)] for transitioning to [*]

where "*" can be "Init", "Load Version", etc.
```

  回避策：ありません。これらは情報メッセージです。（CSCsj89384）

- IOS のアップグレード後に SNMPv3 が動作しないことがあります。

  回避策：snmp-server user コマンドを使用してユーザログイン情報を再適用します。

- シスコのマルチキャスト バーチャル プライベート ネットワーク（MVPN）実装の脆弱性は、悪意のあるユーザが特別な細工をしたメッセージを送信することで、コアルータで追加のマルチキャストステートを作成したり、他のマルチプロトコル ラベル スイッチング（MPLS）ベースのバーチャル プライベート ネットワーク（VPN）からマルチキャストトラフィックを受信したりできるエクスプロイトの対象になります。

  シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。これらの脆弱性に対しては回避策があります。

  このアドバイザリは、次の URL に掲載されています。

  http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html

  （CSCsi01470）

- Cisco IOS Release 12.2（37）SG1 から Cisco IOS Release 12.2（37）SG にダウングレードする場合、プロセスがスロット 2 のアクティブ スーパバイザ エンジンで開始されると、runversion でダウングレードに失敗します。

  回避策：ありません。（CSCsj83688）

トラブルシューティング

ここでは、IOS スーパバイザ エンジンを実行している Catalyst 4000 ファミリのトラブルシューティングについて説明します。

ROMMON からのネットブーティング

ブートローダ イメージを使用するネットブーティングは、サポートされていません。代わりに、次のいずれかのオプションを使用してイメージを起動します。

1. 次のコマンドを入力して、コンパクトフラッシュ カードから起動します。

   ```
   rommon 1> boot slot0:<bootable_image>
   ```

2. ROMMON TFTP ブートを使用します。

   ROMMON TFTP ブートは、次の点以外は BOOTLDR TFTP ブートと非常によく似ています。

   - BOOTLDR 変数は設定しないでください。
   - スーパバイザ エンジンのイーサネット管理ポートから TFTP サーバに接続できるようにしておく必要があります。

   ROMMON から起動するには、ROMMON モードで次の手順を実行します。

a. スーパバイザ エンジンのイーサネット管理ポートが物理的にネットワークに接続されていることを確認します。

b. unset bootldr コマンドを入力して、ブートローダー環境が設定されていないことを確認します。

c. set interface fa1 ip_address> <ip_mask コマンドを入力して、スーパバイザエンジンのイーサネット管理ポートの IP アドレスを設定します。

   たとえば、スーパバイザ エンジンのイーサネット管理ポートに IP アドレス 172.16.1.5 と IP マスク 255.255.255.0 を設定するには、次のコマンドを入力します。

   ```
   rommon 2> set interface fa1 172.16.1.5 255.255.255.0
   ```

d. set ip route default gateway_ip_address コマンドを入力して、スーパバイザエンジンのイーサネット管理ポートのデフォルトゲートウェイを設定します。デフォルト ゲートウェイは、スーパバイザ エンジンのイーサネット管理ポート サブネットに直接接続する必要があります。

e. **ping** <*tftp_server_ip_address*> コマンドで TFTP サーバに ping して、イーサネット管理ポートがサーバに接続されていることを確認します。

f. ping が成功したら、**boot tftp://***tftp_server_ip_address*>/<*image_path_and_file_name コマンドを入力して、TFTP サーバからイメージを起動します。*

   たとえば、TFTP サーバ 172.16.1.8 にあるイメージ名 cat4000-is-mz.160 を起動するには、次のコマンドを入力します。

   ```
   rommon 3> boot tftp://172.16.1.8/tftpboot/cat4000-is-mz
   ```

システム レベルでのトラブルシューティング

ここでは、システム レベルの問題のトラブルシューティングについて取り上げます。

- システムが起動しパワーオン診断を実行するときは、スイッチをリセットしないでください。
- スーパバイザ エンジンには、シリアル ケーブルとイーサネット ケーブルを混合して接続しないでください。スーパバイザ エンジンのファスト イーサネット ポート（10/100）は、すべての Catalyst 4500 Cisco IOS リリースで機能しません。ファスト イーサネット ポートに接続されているイーサネット ケーブルは、ROMMON モードでのみアクティブになります。

モジュールのトラブルシューティング

ここでは、モジュールのトラブルシューティングについて取り上げます。

- モジュールをシャーシにホット インサートするときは、常にモジュールの前面にあるイジェクト レバーを使用して、バックプレーン ピンを正しく装着してください。イジェクト レバーを使用せずにモジュールをインサートすると、スーパバイザ エンジンにモジュールに関する不正なメッセージが表示されることがあります。モジュールのインストール手順については、Catalyst 4500 シリーズ モジュール インストレーション ガイド [英語] を参照してください。
- デュプレックスがエンド ステーションまたは別のネットワーキング デバイスに自動ネゴシエーションするよう設定されたインターフェイスを接続するときは、もう一方のデバイスでも自動ネゴシエーションが設定されていることを必ず確認してください。もう一方のデバイスに自動ネゴシエーションが設定されていない場合、自動ネゴシエーションするよう設定されたポートが半二重モードのままとなり、これによりデュプレックスの不一致が発生してパケット損失やレイト コリジョン、およびリンクでのライン エラーが発生する場合があります。

MIB のトラブルシューティング

MIB、RMON グループ、およびトラップの詳細については、Cisco public MIB ディレクトリ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）を参照してください。Catalyst 4500 シリーズ スイッチでサポートされている特定の MIB の詳細については、ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html の Catalyst 4000 MIB サポート リストを参照してください。

関連資料

4 つのプラットフォーム（Catalyst 4500、Catalyst 4900、Catalyst ME 4900、および Catalyst 4900M）のリリースノートは別々ですが、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ガイド、およびシステムメッセージガイドは共通しています。追加情報については、次のホームページを参照してください。

- 『Catalyst 4500 Series Switch Documentation Home』
  http://www.cisco.com/go/cat4500/docs
- 『Catalyst 4900 Series Switch Documentation Home』
  http://www.cisco.com/go/cat4900/docs
- 『Cisco ME 4900 Series Ethernet Switches Documentation Home』
  http://www.cisco.com/en/US/products/ps7009/tsd_products_support_series_home.html

ハードウェア マニュアル

仕様および関連する安全に関する情報が記載されたインストレーション ガイドおよびインストレーション ノートは、次の URL から入手できます。

- 『*Catalyst 4500 Series Switches Installation Guide*』

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html

- 『*Catalyst 4500 E-series Switches Installation Guide*』

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html

- 個々のスイッチング モジュールおよびスーパーバイザの詳細については、次の URL にある『*Catalyst 4500 Series Module Installation Guide*』を参照してください。

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- 『*Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*』

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html

- 特定のスーパーバイザ エンジンまたはアクセサリ ハードウェアのインストレーション ノートは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- Catalyst 4900 ハードウェアおよび Catalyst 4900M ハードウェアの設置に関する情報は、次の URL から入手できます。

  http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html

- Cisco ME 4900 シリーズ イーサネット スイッチの設置に関する情報は、次の URL から入手できます。

  http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

ソフトウェア マニュアル

ソフトウェアのリリース ノート、コンフィギュレーション ガイド、コマンド リファレンス、およびシステム メッセージ ガイドは、次の URL から入手できます。

- Catalyst 4500 のリリース ノートは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html

- Catalyst 4900 のリリース ノートは、次の URL で入手できます。

  http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html

- Cisco ME4900 4900 シリーズ イーサネット スイッチのリリース ノートは、次の URL から入手できます。

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Catalyst 4500 Classic、Catalyst 4500 E シリーズ、Catalyst 4900、Cisco ME 4900 シリーズ イーサネット スイッチのソフトウェア マニュアルは、次の URL で入手できます。

- 『Catalyst 4500 Series Software Configuration Guide』

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

- 『Catalyst 4500 Series Software Command Reference』
  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- 『Catalyst 4500 Series Software System Message Guide』
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS マニュアル

プラットフォームに依存しない Cisco IOS のマニュアルは、Catalyst 4500 および 4900 スイッチにも役立ちます。これらのマニュアルは、次の URL から入手できます。

- Cisco IOS コンフィギュレーション ガイド、リリース 12.x
  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- Cisco IOS コマンド リファレンス、リリース 12.x
  http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html
  次の URL では、コマンド検索ツールも使用できます。
  http://tools.cisco.com/Support/CLILookup/cltSearchAction.do
- Cisco IOS システム メッセージ、バージョン 12.x
  http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html
  次の URL では、エラー メッセージ デコーダ ツールも使用できます。
  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- MIB については、次の URL を参照してください。
  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml [英語]

通告

本ソフトウェア ライセンスに関連する通知内容を以下に示します。

OpenSSL/Open SSL Project

本製品には、OpenSSL Toolkit（http://www.openssl.org/）で使用するために OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。

本製品には、Eric Young 氏（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。

本製品には、Tim Hudson 氏（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

本製品には、Eric Young 氏（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。本製品には、Tim Hudson 氏（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

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 Really Simple Syndication（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。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。

Catalyst 4500 シリーズ スイッチ、Cisco IOS リリース 12.2(54)SG リリースノート