Cisco IOS リリース 15.1(1)SG（Catalyst 4500 シリーズ スイッチ）リリースノート

現在のリリース
IOS 15.1(1)SG2：2012 年 11 月 1 日

以前のリリース
IOS 15.1(1)SG1 および IOS 15.1(1)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 リリース 15.1(1)SG の機能、変更点、および警告について説明します。

デフォルトイメージである Cisco IOS ソフトウェア リリース 15.1(1)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 4 つのプラットフォーム（Catalyst 4500、Catalyst 4900、Catalyst ME 4900、および Catalyst 4900M/4948E）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

目次

このマニュアルの内容は、次のとおりです。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

Cisco IOS ソフトウェアのパッケージ

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。

IP Base イメージは、ルーテッドアクセスの Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）の「制限付き」スタブルーティング、ノンストップ フォワーディング/ステートフルスイッチオーバー（NSF / SSO）、および RIPv1/v2をサポートします。IP Base イメージは、BGP、Intermediate System-to-Intermediate System（IS-IS）、Internetwork Packet Exchange（IPX）、AppleTalk、Virtual Routing Forwarding（VRF-lite）、GLBP、およびポリシーベースのルーティング（PBR）などの拡張ルーティングはサポートしていません。

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、Cisco IOSリリース12.2(52)XO 以降の Supervisor Engine 6L-E でサポートされます。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。

Cisco IOS リリース 15.0(2)SG 以降、Catalyst 4500 シリーズスイッチでは、NEAT 機能のサポートが IP Base から LAN Base に拡張され、HSRP v2 IPV6 のサポートが Enterprise Services から IP Base に拡張されました。

Cisco IOS リリース（3.3.0SG または 15.1(1)SG）以降、IP SLA と NSF のサポートがエンタープライズサービスから IP Base に拡張されました。

次の内容について説明します。

イメージタイプ別の機能サポート

表 1 に、Cisco IOS ソフトウェア リリース 15.0(2)SG を実行している Catalyst 4500 シリーズ スイッチでサポートされる機能の詳細なリストを示します。サポートされている機能の完全なリストについては、Feature Navigator アプリケーションを確認してください。

http://tools.cisco.com/ITDIT/CFN/

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　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート

機能	LAN ベース	IP Base	Enterprise Services
双方向コミュニティプライベート VLAN	x	○	○
8 方向 CEF ロードバランシング	x	○	○
10 G アップリンクの使用	○	○	○
AAA Server Group	○	○	○
ACL ロギング	○	○	○
すべての MIB	○	○	○
ANCP クライアント	x	○	○
ANSI TIA-1057 LLDP:MED ロケーション拡張	○	○	○
ANSI TIA-1057 LLDP:MED サポート	○	○	○
AppleTalk 1 および 2（Sup 6-E および 6L-Eではサポートされていません）	x	x	○
自動 SmartPorts	○	○	○
自動 QoS	○	○	○
Auto-MDIX	○	○	○
自動音声 VLAN（自動 QoS の一部）	x	○	○
BGP	x	x	○
BGP 4	x	x	○
BGP 4 4Byte ASN（CnH）	x	x	○
BGP 4 マルチパスのサポート	x	x	○
BGP 4 プレフィックス フィルタおよび着信ルート マップ	x	x	○
BGP 条件付きルート インジェクション	x	x	○
BGP リンク帯域幅	x	x	○
BGP ネイバー ポリシー	x	x	○
BGP プレフィックスベース アウトバウンド ルート フィルタリング	x	x	○
BGP ルート マップ継続	x	x	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
アウトバウンド ポリシーに対する BGP ルート マップ継続のサポート	x	x	○
BGP ルートマップ ポリシー リストのサポート	x	x	○
BGP ソフト リセット	x	x	○
BGP ワイルドカード	x	x	○
双方向 PIM（IPv4 のみ）	x	○	○
BOOTP	○	○	○
Bootup GOLD	x	○	○
ブロードキャスト/マルチキャストの抑制	○	○	○
Call Home	x	○	○
CDP/CDPv2	○	○	○
CFM	○	○	○
CGMP：Cisco Group Management Protocol	○	○	○
CiscoView Autonomous Device Manager（ADP）	○	○	○
CNS	○	○	○
コマンド スケジューラ（Kron）	○	○	○
コミュニティ PVLAN のサポート	x	○	○
Config File	○	○	○
コンフィギュレーションの置換とロールバック	○	○	○
コンフィギュレーション ロールバック変更確認	x	x	x
copy コマンド	○	○	○
コンソールアクセス	○	○	○
コントロール プレーン ポリシング（CoPP）	○	○	○
CoS から DSCP へのマップ	○	○	○
レイヤ 3 マルチキャスト制御パケット の CPU の最適化	○	○	○
クラッシュダンプの機能拡張[1]	○	○	○
DAI（ダイナミック ARP インスペクション）	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
DBL（ダイナミックバッファ制限）：アクティブキュー管理	○	○	○
debug コマンド	○	○	○
デバイス管理	○	○	○
プレフィックス委任に関する DHCPv6 リレーエージェントの通知	x	○	○
DHCP クライアント	○	○	○
DHCP サーバ	○	○	○
DHCP スヌーピング	○	○	○
DHCPv6 イーサネットリモート ID オプション	x	○	○
診断ツール	○	○	○
Digital Optical Monitoring（DOM）	○	○	○
ソフトウェアのダウンロード	○	○	○
DSCP から CoS へのマップ	○	○	○
DSCP から出力キューへのマッピング	○	○	○
LLDP 経由の DSCP/CoS	○	○	○
重複ロケーションのレポートの問題	x	○	○
Easy Virtual Network（EVN）	x	x	○
EIGRP	x	x	○
EIGRP Service Advertisement Framework	○	○	○
EIGRP スタブ ルーティング	x	○	○
Embedded Event Manager（EEM）3.2	x	○	○
Embedded Event Manager と EOT の統合	x	○	○
EnergyWise 2.5	○	○	○
EPoE	○	○	○
EtherChannel	○	○	○
イーサネット管理ポート（Fa1 インターフェイス）[2]	○	○	○
イーサネットの操作、管理、保守（OAM）	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
イベント ログ	○	○	○
工場出荷時設定	○	○	○
FHRP：IP SLA の拡張オブジェクトトラッキング	○	x	○
FHRP：GLBP：IP 冗長性 API	x	○	○
FHRP：HSRP：Hot Standby Router Protocol V2	x	○	○
FHRP：オブジェクト トラッキング リスト	x	○	○
FIPS 140-2/3 レベル 2 認定	○	○	○
ファイル管理	○	○	○
Flex Links+（VLAN ロードバランシング）	○	○	○
ゲートウェイ ロード バランシング プロトコル（GLBP）	x	○	○
GOLD オンライン診断	○	○	○
HSRP：Hot Standby Router Protocol	x	○	○
IPv6 グローバルアドレス用 HSRPv2 のサポート	x	○	○
HTTP TACAC+ アカウンティングのサポート	x	x	x
Identity 4.1 ACL ポリシーの機能拡張	○	○	○
Identity 4.2：設定可能なユーザ名/パスワードによる MAB	○	○	○
Identity 4.1 Network Edge Access Topology	○	○	○
ID 4.0 音声 VLAN 割り当て	○	○	○
ID 4.1 フィルタ ID と従量制 ACL	○	○	○
IEEE 802.1ab LLDP（リンク層検出プロトコル）	○	○	○
IEEE 802.1ab LLDP/LLDP-MED	○	○	○
IEEE 802.1ab LLDP の機能拡張（PoE + Layer 2 COS）	○	x	x
IEEE 802.1ag D8.1 標準規格準拠 CFM、Y.1731 マルチキャスト LBM/AIS/RDI/LCK、イーサネット用 IP SLA	○	○	○
IEEE 802.1p サポート	○	○	○
IEEE 802.1p による優先順位付け	○	○	○
IEEE 802.1p/802.1q	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート(続き)

機能	LAN ベース	IP Base	Enterprise Services
IEEE 802.1Q トンネリング	○	○	○
IEEE 802.1Q VLAN トランキング	○	○	○
IEEE 802.1s マルチスパンニングツリー(MST)標準規格に準拠	○	○	○
IEEE 802.1w スパニングツリーの高速再構成	○	○	○
IEEE 802.1x(認証失敗 VLAN、アカウンティング)	○	○	○
IEEE 802.1x Critical Authorization for Voice and Data	○	○	○
IEEE 802.1x Flexible Authentication	○	○	○
複数の認証済みマルチホストでの IEEE 802.1x	○	○	○
IEEE 802.1x オープン認証	○	○	○
ユーザの分散を備えた IEEE 802.1x	○	○	○
IEEE 802.1x ユーザポートの説明	○	○	○
IEEE 802.1x VLAN 割り当て	○	○	○
IEEE 802.1x VLAN ユーザグループの分散	○	○	○
IEEE 802.1x Wake on LAN	○	○	○
IEEE 802.1x エージェントレス監査のサポート	○	○	○
IEEE 802.1x オーセンティケータ	○	○	○
IEEE 802.1x フォールバックのサポート	○	○	○
IEEE 802.1x ゲスト VLAN	○	○	○
IEEE 802.1x MIB サポート	○	○	○
音声 VLAN の割り当てによる IEEE 802.1x マルチドメイン認証	○	○	○
IEEE 802.1x マルチドメイン認証	○	○	○
IEEE 802.1x プライベートゲスト VLAN	○	○	○
IEEE 802.1x プライベート VLAN 割り当て	○	○	○
IEEE 802.1x RADIUS アカウンティング	○	○	○
IEEE 802.1x RADIUS 提供セッションのタイムアウト	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
IEEE 802.1x および ACL 割り当てを使用した MAB	○	○	○
IEEE 802.3ad Link Aggregation Control Protocol（LACP）	○	○	○
IEEE 802.3ad リンク集約（LACP）ポートチャネル スタンドアロンの無効化	○	○	○
IEEE 802.3ah および CFM のインターワーキング	x	○	○
IEEE 802.3x フロー制御	○	○	○
IEEE 802.1x Web 認証	○	○	○
IGMP フィルタリング	○	○	○
IGMP クエリア	○	○	○
IGMP スヌーピング	○	○	○
IGMP バージョン 1	○	○	○
IGMP バージョン 2	○	○	○
IGMP バージョン 3	○	○	○
IGMPv3 ホスト スタック	○	○	○
入力ポリシング	○	○	○
インターフェイスアクセス（Telnet、コンソール/シリアル、Web）	○	○	○
IOS ベースのデバイスのプロファイリング	x	○	○
IP 拡張 IGRP ルート認証	x	x	○
IP イベント減衰	○	○	○
等コスト パス間での IP マルチキャスト負荷分散	x	○	○
IP 名前付き アクセス コントロール リスト	○	○	○
IPv6トンネル（ソフトウェア内）	○	○	○
IP ルーティング	○	○	○
IP SLA の DHCP 動作	x	○	○
IP SLA 統計情報の配信	x	○	○
IP SLA DNS 動作	x	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
IP SLA FTP 動作	x	○	○
IP SLA 履歴統計	x	○	○
IP SLA HTTP 動作	x	○	○
IP SLA ICMP エコー動作	x	○	○
IP SLA ICMP パス エコー動作	x	○	○
IP SLA マルチ オペレーション スケジューラ	x	○	○
IP SLA 一方向測定	x	○	○
IP SLA パス ジッター動作	x	○	○
IP SLA ランダム スケジューラ	x	○	○
IP SLA 反応のしきい値	x	○	○
IP SLA Responder	○	○	○
IP SLA スケジューラ	x	○	○
IP SLA SNMP のサポート	x	○	○
IP SLA サブミリ秒での精度の改善点	x	○	○
IP SLA TCP 接続動作	x	○	○
IP SLA UDP ベースの VoIP 動作	x	○	○
IP SLA UDP エコー動作	x	○	○
IP SLA UDP ジッター動作	x	○	○
IP SLA VoIP しきい値のトラップ	x	○	○
IPSG（IP ソースガード）v4	○	○	○
スタティックホストの IPSG（IP ソースガード）v4	○	○	○
VLAN-SVI インターフェイスの番号なし IP	x	○	○
IPv6 ホット スタンバイ ルータ プロトコル（HSRP）	x	○	○
IPv6 インターフェイスの統計情報	○	○	○
IPv6 IP SLA（UDP ジッター、UDP エコー、ICMP エコー、TCP 接続）	x	○	○
IPv6（Internet Protocol Version 6）	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
IPV6 MLD スヌーピング V1 および V2	○	○	○
IPv6 マルチキャスト	x	○	○
IPv6 マルチキャスト：ブートストラップ ルータ（BSR）	x	○	○
IPv6 マルチキャスト：Multicast Listener Discovery（MLD）Protocol、バージョン 1 および 2	x	○	○
IPv6 マルチキャスト：PIM Accept Register	x	○	○
IPv6 マルチキャスト：PIM Source-Specific Multicast（PIM-SSM）	x	○	○
IPv6 マルチキャスト：PIM スパース モード（PIM-SM）	x	○	○
IPv6 マルチキャスト：ルーティング可能なアドレスの Hello オプション	x	○	○
IPv6 ネイバー探索	x	○	○
IPv6 OSPFv3 高速コンバージェンス	x	対応[3]	○
IPsecv3/IKEv2（管理トラフィック専用）	○	○	○
IPv6 OSPFv3 NSF/SSO	x	対応[3]	○
Identity 4.1 Network Edge Access Topology	○	○	○
IPv6 RA ガード	○	○	○
IPv6 の再編成	NA	○	○
IPv6 ルータ アドバタイズメント（RA）ガード	○	○	○
IPv6 ルーティング：EIGRP サポート	x	x	○
IPv6 ルーティング：OSPF for IPv6（OSPFv3）	x	対応[3]	○
IPv6 ルーティング：RIP for IPv6（RIPng）	x	○	○
IPv6 スイッチング：CEFv6 スイッチド自動 IPv4 互換トンネル（ソフトウェア内）	x	○	○
IPv6 スイッチング：CEFv6 スイッチド IPv6 over IPv4 トンネル（ソフトウェア内）	x	○	○
IPv6 スイッチング：CEFv6 スイッチド ISATAP トンネル（ソフトウェア内）	x	○	○
IPv6 トンネリング：自動 6to4 トンネル（ソフトウェア内）	x	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
IPv6 トンネリング：自動 IPv4 互換トンネル（ソフトウェア内）	x	○	○
IPv6 トンネリング：IPv4 GRE トンネルを介した IPv6（ソフトウェア内）	x	○	○
IPv6 トンネリング：ISATAP トンネルのサポート（ソフトウェア内）	x	○	○
IPv6 トンネリング：手動で設定された IPv6 over IPv4 トンネル（ソフトウェア内）	x	○	○
ISIS for IPv4 and IPv6	x	x	○
ISL Trunk	○	○	○
ISSU（IOS In-Service Software Upgrade）	x	○	○
ジャンボ フレーム	○	○	○
レイヤ 2 制御パケット	○	○	○
レイヤ 2 デバッグ	○	○	○
レイヤ 2 プロトコルトンネリング（L2PT）	x	○	○
レイヤ 2 Traceroute	○	○	○
レイヤ 3 マルチキャストルーティング（PIM SM、SSM、Bidir）	x	○	○
リンクステート トラッキング	○	○	○
ローカル Web 認証	○	○	○
音声 VLAN での MAB（MAC 認証バイパス）	○	○	○
MAC アドレスのフィルタリング	○	○	○
MAC ベースのアクセスリスト	○	○	○
MAC の移動と置換	○	○	○
管理 IPv6 ポート	○	○	○
Medianet 2.0：AutoQoS SRND4 マクロ	x	○	○
Medianet 2.0：統合ビデオ トラフィック シミュレータ（ハードウェア支援 IP SLA）、IPSLA レスポンダのみ	x	○	○
Medianet 2.0：フローメタデータ	x	○	○
Medianet 2.0：メディアサービスプロキシ	x	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
Medianet 2.0：メディアモニタリング（パフォーマンスモニタリングおよび Mediatrace）	x	○	○
Multicast BGP（MBGP）	x	x	○
Multicast Routing Monitor（MRM）	x	○	○
Multicast Source Discovery Protocol（MSDP）	○	○	○
マルチ認証と VLAN 割り当て	○	○	○
マルチ VRF のサポート（VRF Lite）	x	x	○
NAC - L2 IEEE 802.1x	○	○	○
NAC：L2 IP	○	○	○
ND キャッシュ制限/インターフェイス	x	○	○
NEAT 拡張：ユーザ設定に基づく BPDU ガードの再有効化	○	○	○
Network Edge Access Topology（NEAT）	○	○	○
ネットワーク タイム プロトコル（NTP）	○	○	○
NMSP の機能拡張 • ロケーションに対する GPS によるサポート • スイッチレベルでのロケーション • ローカルタイムゾーンの変更 • 名前と値のペア • MIB の優先順位設定	x	○	○
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	○	○	○
QoS フィルタの数 セキュリティ ACE の数	○（4K エントリ）	○	○
No Service Password Recovery	○	○	○
VLAN のサポートの数	2048	4096	4096
NSF：BGP	x	x	○
NSF：EIGRP	x	○	○
NSF：OSPF（バージョン 2 のみ）	x	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
NSF/SSO（ステートフル スイッチオーバーを使用したノンストップ フォワーディング）	x	x	○
NTP for IPv6	○	○	○
VRF 対応の NTP	x	x	○
On Demand Routing（ODR）	x	x	○
OSPF	x	対応[3]	○
OSPF v3 認証	x	対応[3]	○
OSPF フラッディングの削減	x	対応[3]	○
ルーテッド アクセスの OSPF	x	○	○
OSPF Incremental Shortest Path First（i-SPF）のサポート	x	対応[3]	○
OSPF リンク ステート データベース オーバーロードの防止	x	対応[3]	○
OSPF Not-So-Stubby Areas（NSSA）	x	対応[3]	○
OSPF パケット同期	x	対応[3]	○
OSPF Shortest Paths First スロットリング	x	対応[3]	○
『OSPF Stub Router Advertisement』	x	対応[3]	○
fast hello に対する OSPF サポート	x	対応[3]	○
リンク ステート アドバタイズメント（LSA）スロットリングに対する OSPF サポート	x	対応[3]	○
CE ルータでの OSPF マルチ VRF サポート	x	対応[3]	○
OSPF アップデート パケット ペーシング タイマー設定	x	対応[3]	○
アウトオブバンド管理ポート	○	○	○
PAgP	○	○	○
パスワード パスワードクリアの防止	○	○	○
インターフェイス単位での IGMP のステート制限	○	○	○
インターフェイス単位での Mroute のステート制限	○	○	○
802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポート	○	○	○
VLAN 単位での学習	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
PIM スパースモードバージョン 4	x	x	○
PIM バージョン 1	x	○	○
PM バージョン 2	x	○	○
PoE（最大 15.4 W のみ）	○	○	○
PoE+ 対応	○	○	○
LLDP を介した PoEP	○	○	○
Policy-Based Routing（PBR）	x	x	○
ポートアクセス制御リスト（PACL）	○	○	○
ポートモニタリング（インターフェイス統計情報）	○	○	○
ポート セキュリティ	対応	○（1,024 個の MAC のみ）	○
投稿ステータス	○	○	○
Pragmatic General Multicast（PGM）	○	○	○
プライベート VLAN	○	○	○
CDP を介したロケーション情報の伝達	○	○	○
EtherChannel を介した PVLAN	○	○	○
PVST+（Per VLAN Spanning Tree Plus）	○	○	○
Q-in-Q	x	○	○
RACL（DSCP ベース）	○	○	○
RADIUS/TACACS+（AAA）	○	○	○
アクセス要求内の RADIUS 属性 44（アカウンティングセッション ID）	○	○	○
RADIUS 許可の変更	○	○	○
VLAN 単位の高速スパニングツリー（Rapid-PVST）	○	○	○
リモート SPAN（RSPAN）	○	○	○
REP（Resilient Ethernet Protocol）	○	○	○
REP：エッジネイバー拡張なし	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
RIP v1	x	○	○
RMON	○	○	○
ロールベースのアクセス制御 CLI コマンド（RBAC）	○	○	○
RPR	○	○	○
RPVST+	○	○	○
RSPAN	○	○	○
セキュアコピー（SCP）	○	○	○
セキュアシェル SSH バージョン 1、2 サーバのサポート	○	○	○
セキュアシェル SSH バージョン 1、2 クライアントのサポート	○	○	○
Service Advertisement Framework（SAF）	x	x	○
SmartPorts（ロールベースのマクロ）	○	○	○
SNMP（簡易ネットワーク管理プロトコル）	○	○	○
SNMPv3（SNMP バージョン 3）	○	○	○
送信元ポートフィルタリング（プライベート VLAN）	○	○	○
Source Specific Multicast（SSM）	x	○	○
Source Specific Multicast（SSM）：IGMPv3、IGMP v3 Lite、および URD	○	○	○
Source Specific Multicast（SSM）マッピング	○	○	○
SPAN（セッションの数）：ポートミラーリング	○（2 セッション）	○（8 双方向セッション）	○
SSHv2/セキュアコピー、FTP、SSL、Syslog、Sys 情報	○	○	○
SSO（ステートフル スイッチオーバー）	x	○	○
スタティックルーティング（IPv4/IPv6）	○	○	○
ストーム制御：ポート単位のマルチキャスト抑制	○	○	○
スタブ IP マルチキャスト ルーティング	x	○	X
サブ秒 UDLD	○	○	○
SVI（スイッチ仮想インターフェイス）自動ステート除外	○	○	○

表 1　Catalyst 4500 シリーズ スイッチでの LAN ベース/IP ベースのイメージのサポート（続き）

機能	LAN ベース	IP Base	Enterprise Services
TACACS+	○	○	○
IPv6- 用 TACACS+ および RADIUS	○	○	○
時刻ベースのアクセス リスト	○	○	○
タイムドメイン反射率計（TDR）[4]	x	○	○
タイムプロトコル（SNTP、TimeP）	○	○	○
トラフィックミラーリング（SPAN）	○	○	○
信頼境界（LLDP および CDP ベース）	○	○	○
TrustSec：IEEE 802.1ae MACSec レイヤ 2 の暗号化	x	○	○
TrustSec：ユーザ向けポートでの IEEE 802.1ae MACSec の暗号化	x	○	○
TrustSec：ユーザ向けポート SSO での IEEE 802.1ae MACSec の暗号化	x	○	○
TrustSec：Cisco SAP（Security Association Protocol）を使用したスイッチ間リンク間での IEEE 802.1ae MACSec の暗号化	x	○	○
ユニキャスト RPF（uRPF）	○	○	○
単一方向リンク検出（UDLD）	○	○	○
仮想ルータ冗長プロトコル（VRRP）	x	○	○
VLAN アクセス制御リスト（VACL）	○	○	○
VLAN マッピング（VLAN 変換）	x	○	○
音声 VLAN	○	○	○
VRF 対応 TACACS+	x	x	○
VTP（Virtual Trunking Protocol）バージョン 2	○	○	○
VTP バージョン 3	○	○	○
受信インターフェイスでの WCCP のリダイレクション	x	○	○
WCCP バージョン 2	x	○	○
XML-PI	○	○	○

1. Supervisor Engine 6-E と Supervisor Engine 6L- でのみサポート
2. Cisco IOS リリース 12.2(46)SG 以降
3. IP Base は、OSPFv2 インスタンスと OSPFv3 インスタンスのそれぞれ 1 つのみと、動的に学習された最大 1,000 のルートをサポートします。
4. TDR は 46xx ラインカードではサポートされていません。

(注) IP Base に移動することなく、LAN Base イメージで 10 ギガビットアップリンクを有効にする特別なライセンスを購入できます。

Catalyst 4500 シリーズ スイッチでサポートされていない機能

次の機能は、Catalyst 4500 シリーズ スイッチの Cisco IOS リリース 15.1(1)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(「フォールバック ブリッジング」とも呼ばれる)
- 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
- IPv6 トラフィックの QoS(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
- WCCP バージョン 1
- CFM CoS
- EOT を使用した PBR

発注可能な製品番号

表 2　　Catalyst 4500 シリーズスイッチの発注可能な製品番号

製品番号	説明	Image
S45EIPB- 15101SG (=)	Cisco Catalyst 4500 Supervisor Engine 6-E および Sup6L-E 用の Cisco IOS ソフトウェア（IP Base イメージ）	Cat4500e-ipbase-mz
S45EIPBK9-15101SG(=)	Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E および Sup6L-E 用の Cisco IOS ソフトウェア（3DES を使用した IP Base イメージ）	Cat4500e-ipbasek9-mz
S45EES-15101SG (=)	Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E および Sup6L-E 用の Cisco IOS ソフトウェア（エンタープライズ サービス イメージ）	Cat4500e-entservices-mz
S45EESK9-15002SG(=)	Cisco Catalyst 4500 シリーズ Supervisor Engine 6-E および Sup6L-E 用の Cisco IOSソフトウェア（3DES を使用した Enterprise Services イメージ）	Cat4500e-entservicesk9-mz
S45EESU-15002SG(=)	Supervisor Engine 6-E および Supervisor Engine 6L-E の LAN Base からの Cisco IOS エンタープライズイメージのアップグレード	Cat4500e-entservices-mz
S45EESUK915002SG(=)	Supervisor Engine 6-E および Supervisor Engine 6L-E 用の LAN Base からの 3DES アップグレードを使用した Cisco IOS Enterprise	Cat4500e-entservicesk9-mz
S45EIPBU-15002SG(=)	Catalyst 4500 シリーズ Supervisor Engine 6-E および Sup6L-E IOS IP Base アップグレード用の Cisco IOS ソフトウェア	Cat4500e-ipbase-mz
S45EIBUK9-15002SG(=)	Catalyst 4500 シリーズ Supervisor Engine 6-E および Sup6L-E IOS IP Base アップグレード SSH 用の Cisco IOS ソフトウェア	Cat4500e-ipbasek9-mz

Cisco Classic IOS のリリース戦略

Catalyst 4500 シリーズ スイッチで Supervisor Engine 6-E または 6L-E を使用しているお客様で、最新のハードウェアおよびソフトウェアの機能が必要な場合は、Cisco IOS リリース 15.1(1)SG に移行する必要があります。

（注） このリリースでは、II+、III、IV、V、V-10GE などの古いスーパーバイザエンジンはサポートされていません。

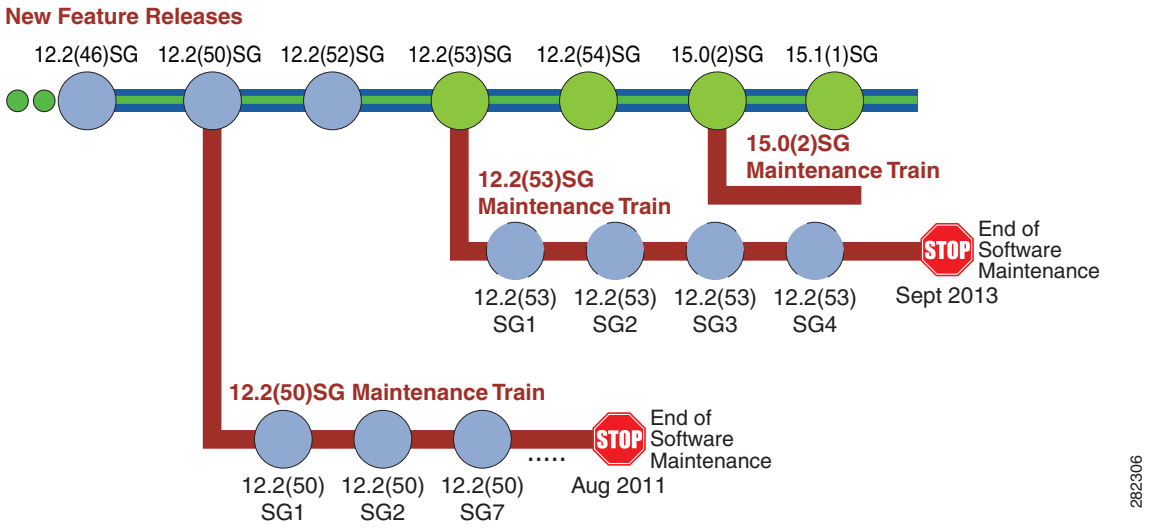
Catalyst 4500 シリーズ スイッチには、2 つのメンテナンストレインがあります。メンテナンストレインが付属したリリースが必要なお客様の場合は、Cisco IOS リリース 15.0(2)SG を推奨します。

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

図 1 に、2 つのアクティブなトレイン、12.2(53)SG と 15.0(2)SG を示します。

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



サポート

Cisco IOS ソフトウェア リリース 15.1(1)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（19 ページ）
- 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（24 ページ）

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 3 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 3　　サポート対象ハードウェア

製品名（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
スーパーバイザ エンジン		
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

表 3　サポート対象ハードウェア(続き)

製品名(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-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
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-X4640-CSFP-E	ギガビット Compact SFP 搭載 80 ポート(4:1 オーバーサブスクライブ型)、40 モジュールのギガビット SFP ラインカード(1000BaseX)、スロットあたり 24 ギガビットの容量を装備(SFP オプション)(2:1 オーバーサブスクライブ型) (注)　WS-X4640-CSFP-E は 10 スロットシャーシではサポートされていません。	15.1(1)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

表 3　サポート対象ハードウェア(続き)

製品名(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-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
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 Engines 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

表 3　サポート対象ハードウェア(続き)

製品名(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
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(25 ページ)を参照してください。

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
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
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

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-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 ラインカードのみ使用できます。 • ファン トレイ

各着脱可能モジュールでサポートされる最小リリースについては、次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 4　Catalyst 4500 シリーズ スイッチでの DOM サポートは次のモジュールに適用されます。

トランシーバ モジュール
CWDM- SFP-*xx*
DWDM-GBIC-*xx*
DWDM-SFP
DWDM-X2-*xx*
GLC-BX-D
GLC-BX-U
GLC-LH-SMD
GLC-EX-SMD
GLC-FE-100EX
GLC-FE-100ZX
GLC-FE-100FX
SFP-10G-SR
SFP-10G-LR
SFP-10G-LRM
SFP-10G-ER
SFP-10G-ZR

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ーバイザエンジンに加えて、Cisco IOS ソフトウェア リリース 15.0(2)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 シリーズのハードウェアの簡単なリスト（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
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 6-E または Supervisor Engine 6L-E で使用する場合、スロット 8、9、および 10 は 6 Gbps 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 または Supervisor Engine 6L-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 6 Gbps を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

表 5　サポートされている E シリーズのハードウェア（続き）

製品番号	説明
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、シャーシとスーパー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ーの互換性

シャーシ	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4506-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R+E	M:12.2(54)SG	M:12.2(54)SG
WS-C4510R-E	M: 12.2(40)SG	
WS-C4510R+E	M:12.2(54)SG	

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 15.1(1)SG1 の新しいハードウェア機能

リリース 15.1(1)SG1 では、Catalyst 4500 シリーズ スイッチの新しいハードウェアは提供されていません。

リリース 15.1(1)SG1 の新しいソフトウェア機能

リリース 15.1(1)SG1 では、Catalyst 4500 シリーズ スイッチに新しいソフトウェアは提供されていません。

リリース 15.1(1)SG の新しいハードウェア機能

リリース 15.1(1)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-X4248-FE-SFP のファストイーサネット SFP ポート用 GLC-FE-100EX および GLC-FE-100ZX
- WS-X4640-CSFP-E、WS-X4612-SFP-E、および WS-X4624-SFP-E のギガビットイーサネット SFP ポート用 GLC-GE-100FX

（注） GLC-GE-100FX はギガビットイーサネット SFP ポートに接続しますが、帯域幅は 100 M です。

- すべてのギガビットイーサネット SFP ポート用 GLC-EX-SMD
- WS-X4640-CSFP-E

リリース 15.1(1)SG の新しいソフトウェア機能

リリース 15.1(1)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。

- IOS ベースのデバイスのプロファイリング
- SXP syslog の機能拡張
- Medianet 2.0
  - モニタリング（パフォーマンスモニタリングと Mediatrace など）
  - フロー メタデータ
  - メディア サービス プロキシ
  - 統合ビデオ トラフィック シミュレータ（ハードウェア支援 IP SLA）

    IPSLA レスポンダのみ
  - AutoQoS マクロ
- Medianet2.0：NMSP の機能拡張
  - スイッチレベルでのロケーション
  - ローカルタイムゾーンの変更
  - ロケーションに対する GPS によるサポート
  - MIB の優先順位設定
  - 名前と値のペア
- EnergyWise バージョン 2.5

  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/net_mgmt/cisco_configuration_professional/v2_5/olh/ccp.pdf

http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2_5/ios/release/notes/ol23554.html

- IPv6 OSPFv3 NSF/SSO
- IPv6 OSPFv3 高速コンバージェンス

- OSPFv3 Authentication
- IPsecv3/IKEv2（管理トラフィック専用）
- FIPS 140-2/3 レベル 2 認定
- No Service Password Recovery
- Easy Virtual Network（EVN）
- インターフェイス単位の ND キャッシュ制限
- IPv6 グローバルアドレス用 HSRPv2 のサポート
- Identity 4.2：設定可能なユーザ名/パスワードを使用する MAB
- BGP ワイルドカード
- BGP 4 バイト ASN（CnH）
- ネイバー単位の BGP グレースフルリスタート
- BGP ネクストホップトラッキング
- ダイナミック PBR API
- マルチキャスト コール アドミッション コントロール：インターフェイス単位のルートステート制限
- マルチキャスト用の帯域幅ベースのコール アドミッション コントロール ポリシー
- mcast グループ範囲を拒否する機能
- IPv6 SSM マッピング：MLD v1 レシーバ
- IPv6 BSR：RP マッピングを設定する機能
- MSDP MD5 パスワード認証
- MLD グループ制限
- IPv6 マルチキャスト：グループ範囲の無効化
- IGMP スタティックグループ範囲のサポート
- PIM によってトリガーされた参加
- conn. add in autoRP cand. の直接サポートRP
- マルチキャストマルチパスの機能拡張
- IGMP-STD-MIB の導入
- OSPF MIB フィールドで int-id として SNMP MIBII ifindex を使用するためのノブ
- OSPF トラフィック統計情報の機能拡張
- 接続されたプレフィックスを除外するための OSPF メカニズム
- OSPF TTL セキュリティ チェック
- OSPF グレースフル シャットダウン
- OSPFv2 int. enabling：OSPF エリアのコマンド
- OSPFv3 IPSec の機能拡張
- IP-RIP：遅延起動
- AAA アカウンティング：CLI レコード停止の機能拡張
- RADIUS サーバのロードバランシングのポーティング
- AAA Double Authentication Secured by Absolute Timeout

- サブスクライバプロファイルによるローカル AAA 属性のサポート
- メソッドリスト、サーバグループの拡張性
- BGP:Dual AS Accept の導入
- IP Base の NSF
- IGMPv3 ホストスタック
- インターフェイス単位での IGMP のステート制限
- インターフェイス単位での Mroute のステート制限
- IPv6 用 TACACS+ および RADIUS
- IPv6 用 NTP（VRF にも対応）

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 と Supervisor Engine 6L-E で Cisco IOS リリース 15.0(2)SG を実行するには、少なくとも 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。12.2(44r)SG9 が推奨されています。

注意 ほとんどのスーパーバイザ 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 7　スーパーバイザ 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	推奨 ROMMON リリース
6-E	12.2(44r)SG9
6L-E	12.2(44r)SG9

表 8　ROMMON リリースと Promupgrade プログラム

ROMMON リリース	Promupgrade プログラム
12.2(31r)SGA4	cat4500-e-ios-promupgrade-122_31r_SGA4
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5
12.2(44r)SG9	cat4500-e-ios-promupgrade-122_44r_SG9
12.2(44r)SG10	cat4500-e-ios-promupgrade-122_44r_SG10

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。

スーパーバイザエンジン 1（sup1）が ROMMON で、スーパーバイザエンジン 2（sup2）が IOS の場合、sup2 のみがシャーシの idprom の 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 スーパーバイザ 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。

注意 Supervisor Engine 6-E および 6L-E で ROMMON をアップグレードすると、アップリンク インターフェイスがリセットされることがあります。Cisco IOS リリース 15.0(2)SG より前のソフトウェアは、スタンバイ スーパーバイザ エンジンの ROMMON がアップグレードされたときに、この状況を検出せず、回復しませんでした。次に説明する冗長スーパーバイザエンジンの ROMMON アップグレードプロセスは、アクティブなスーパーバイザエンジンが Cisco IOS リリース 15.0(2)SG を実行している場合にのみ機能します。冗長システムの場合は、まずソフトウェアを Cisco IOS リリース 15.0(2)SG にアップグレードしてから ROMMON をアップグレードします。

コンソールからのスーパーバイザ 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） この項の例では、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 12.2(44r)SG9 と Cisco IOS リリース 12.2(50)SG を使用しています。その他のリリースでは、ROMMON リリースと Cisco IOS ソフトウェアのリリースを適切なリリースとファイル名に置き換えます。このドキュメントでは、シングル スーパーバイザ エンジン システムの手順について説明します。デュアル スーパーバイザ エンジン システムでは、各スーパーバイザエンジンでプロセスを実行する必要があります。

スーパーバイザエンジン 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、スーパー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 cat4500-e-ios-promupgrade-122_44r_SG9 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内の TFTP サーバに配置します。

cat4500-e-ios-promupgrade-122_44r_SG9 プログラムは、Catalyst 4500 システムイメージをダウンロードしたのと同じ場所から Cisco.com で入手できます。

ステップ 3 **dir bootflash:** コマンドを使用して、PROM アップグレードイメージを保存するフラッシュメモリに十分なスペースがあることを確認します。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。

（注） CSCsu36751 により、現在の ROMMON バージョンが 12.2(44r)SG3 より前の場合は、このアップグレードにブートフラッシュを使用する必要があります。それ以外の場合は、リブート後にコンパクトフラッシュを取り付け直すことが必要な場合があります。

ステップ 4 **copy tftp** コマンドを使用して cat4500-e-ios-promupgrade-122_44r_SG9 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 cat4500-e-ios-promupgrade-122_44r_SG9 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 [cat4500-e-ios-promupgrade-122_44r_SG9]?
Destination filename [cat4500-e-ios-promupgrade-122_44r_SG9]?
Accessing tftp://172.20.58.78/cat4500-e-ios-promupgrade-122_44r_SG9...
Loading cat4500-e-ios-promupgrade-122_44r_SG9 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 2404172 bytes]

2404172 bytes copied in 28.536 secs (84250 bytes/sec)
Switch#
```

ステップ 5 デュアル スーパーバイザ システムで、**copy bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 slavebootflash** コマンドを使用して、同じ ROMMON イメージをスタンバイ スーパーバイザ エンジンにコピーします。

ステップ 6 **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。

（注） 冗長システムでは、このアクションによってスイッチオーバーが発生します。

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 ?


 Rom Monitor Program Version 12.2(44r)SG3


.
.(output truncated)
.

 Established physical link 1Gb Full Duplex
 Network layer connectivity may take a few seconds
rommon 1 >
```

ステップ 7 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:cat4500-e-ios-promupgrade-122_44r_SG9

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には、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、スーパーバイザ エンジンのリセット、電源の再投入、または OIR は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:cat4500-e-ios-promupgrade-122_44r_SG9

Image Name : Cat4K_Mpc8548_Rommon
 Image size : 1048576 bytes

 Uncompressing image.....
 Done!

 ********************************************************
 *        ** Now Upgrading Primary ROMMON Image **        *
 ********************************************************

 Offset: 7E00000
erasing... writing... reading... verifying...  Done!


 ********************************************************
 *            ** Now Programming FPGA Image **            *
 ********************************************************

 Image Name : Cat4K_JAWA_Fpga
```

```
 Image size : 524288 bytes

 Uncompressing image.....
 Done!

Device ID 12, status  0, size 524288 bytes, we have 524288 bytes
erasing... writing/verifying sectors... 0 1 2 3 4 5 6 7 Done!
 ********************************************************
 System will now reset itself and reboot within few seconds
 ********************************************************
*!*

 ********************************************************
 *                                                      *
 * Welcome to Rom Monitor for WS-X45-SUP6-E System.     *
 * Copyright (c) 2003-2010 by Cisco Systems, Inc.       *
 * All rights reserved.                                 *
 *                                                      *
 ********************************************************
….
Rom Monitor Program Version 12.2(44r)SG9
 CPU Rev: 2.0, Board Rev: 4, Board Type: 10, CPLD Jawa Rev: 20
…
rommon 1>
```

ステップ 8 Cisco IOS ソフトウェアイメージを起動します。これは、システムが自動起動するように設定されている場合は自動的に実行されることがあります。

ステップ 9 冗長システムで、現在アクティブなスーパバイザーエンジンにコンソールを接続します。システムが SSO 状態になったら、ステップ 6 ～ 8 を繰り返します。

ステップ 10 **show module** コマンドを使用して、ROMMON がアップグレードされていることを確認します。

```
Switch# show module
Chassis Type : WS-C4510R-E

Power consumed by backplane : 40 Watts

Mod Ports Card Type                              Model              Serial No.
---+-----+--------------------------------------+------------------+-----------
 3    48  10/100/1000BaseT POE E Series          WS-X4648-RJ45V-E   JAE1129QL9N
 4    48  10/100/1000BaseT Premium POE E Series  WS-X4648-RJ45V+E   JAE1129QSAV
 5     6  Sup 6-E 10GE (X2), 1000BaseX (SFP)     WS-X45-SUP6-E      JAE1225MJMN
 6     6  Sup 6-E 10GE (X2), 1000BaseX (SFP)     WS-X45-SUP6-E      JAE1224LAOS
 7    48  10/100/1000BaseT (RJ45)V, Cisco/IEEE   WS-X4548-RJ45V+    JAB1229BCMD
 8    24  10/100/1000BaseT (RJ45)V, Cisco/IEEE   WS-X4524-GB-RJ45V  JAB0815059Q

M MAC addresses                    Hw  Fw           Sw               Status
--+-------------------------------+---+------------+----------------+---------
 3 001c.58f8.2240 to 001c.58f8.226f 0.3                               Ok
 4 001c.58f8.2090 to 001c.58f8.20bf 0.3                               Ok
 5 0017.94c9.85c0 to 0017.94c9.85c5 1.1 12.2(44r)SG9  12.2(50)SG      Ok
 6 0017.94c9.85c6 to 0017.94c9.85cb 1.1 12.2(44r)SG9  12.2(50)SG      Ok
 7 000a.8aff.3830 to 000a.8aff.385f 0.1                               Ok
 8 0030.850e.3e78 to 0030.850e.3e8f 0.6                               Ok   ….
Switch#
```

ステップ 11 アクティブなスーパーバイザで **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ます。

次に、ブートフラッシュから cat4500-e-ios-promupgrade-122_44r_SG9 イメージを削除する例を示します。

```
Switch# delete bootflash:cat4500-e-ios-promupgrade-122_44r_SG9
```

ステップ 12 冗長システムでは、スタンバイ スーパーバイザエンジンからアップグレードファイルも削除します。

```
Switch# delete slavebootflash:cat4500-e-ios-promupgrade-122_44r_SG9
```

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（38 ページ）を参照してください。

Telnet を使用したスーパーバイザエンジン 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。

スーパーバイザエンジンの ROMMON をリリース 12.2(44r)SG9 にアップグレードするには、次の手順を実行します。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 bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 を使用します。

ステップ 1 スーパー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 bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 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内の TFTP サーバに配置します。

bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 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のと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 cbootflash:cat4500-e-ios-promupgrade-122_44r_SG9 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 bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 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 [bootflash:cat4500-e-ios-promupgrade-122_44r_SG9]?
Destination filename [bootflash:cat4500-e-ios-promupgrade-122_44r_SG9]?
```

```
Accessing tftp://172.20.58.78/ bootflash:cat4500-e-ios-promupgrade-122_44r_SG9...
Loading bootflash:cat4500-e-ios-promupgrade-122_44r_SG9 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、設定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
12.2(44r)SG9. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 15.0(2)SG.

config-register to 0x0102.

Switch# configure terminal
Switch(config)# boot system flash bootflash:
bootflash:cat4500-e-ios-promupgrade-122_44r_SG9
Switch(config)# boot system flash bootflash:cat4500e-entservices-mz.1550-1.SG
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　起動設定を確認するには、**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、スーパー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# show 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、またはスーパーバイザ 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使用されていない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# show 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（38 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 リリース 15.01(2) をダウンロードし、アップグレードするスーパーバイザ エンジンからアクセスできるディレクトリ内の TFTP サーバに配置します。

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 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、またはスーパーバイザエンジンの 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。

- リリース IOS XE 3.3.0SG および IOS 15.1(1)SG 以降では、次の 7 つの RP の制約事項が削除されました。
- **permit any any ?** コマンドを入力すると、**octal** コマンドが表示されますが、このコマンドは Cisco IOSリリース12.2(54)SG ではサポートされていません。

  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、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、次の行は次のようになります。

```
    <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 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ています（つまり、CLI で許可されます）が、CLI の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。
- 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、この変更を反映します。

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）

- Catalyst 4500 プラットフォームでは、1 秒未満の PIM クエリ間隔を設定できますが、このようなアクションはコンバージェンス（反応時間）と他の多くの要因（mroute の数、CPU 使用率のベースライン、CPU 速度、1 m-route あたりの処理オーバーヘッドなど）との間での妥協を意味します。PIM タイマーを 1 秒未満に設定する場合は、これらの要因を考慮する必要があります。PIM クエリ間隔は 2 秒以上に設定することを推奨します。使用可能なパラメータを調整することで、完全な動作を実現できます。つまり、特定のセットアップでのコンバージェンス時間あたりのマルチキャストルートの上位数。
- Cisco IOS リリース XE 3.2.1SGでは、メモリ設定が有効になっています。

```
Switch(config)# memory ?
  chunk    chunk related configuration
  free     free memory low water mark
  record   configure memory event/traceback recording options
  reserve  reserve memory
  sanity   Enable memory sanity
```

この 設定は、以前のリリースで誤って削除されていました。

- 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ー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ー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ー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、スーパーバイザエンジンを切り替えるとクリアされます。アドレスのクリアリング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**、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（75 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ー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ーバイザエンジンを取り外すと、スロット 2 にあるスーパー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ーバイザ 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、両方のスーパー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を使用できません。
  - 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、コンパクトフラッシュ（slot0）に FAT ファイルシステムを使用します。コンパクトフラッシュが 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 以外のスーパーバイザエンジンのコンパクトフラッシュなど）、スイッチはそのコンパクトフラッシュを認識しません。
- 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ーバイザエンジンの起動中にスタンバイ スーパーバイザ 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 スーパーバイザ 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ー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 間で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参照するとき、参照するホストが多数ある場合は、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、出力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 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 に注意事項はありません。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 Series Module Installation Guide』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 1 G 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、10 G 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トするように設定されており、インターフェイスが 10 G 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 ポートで高速 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ー、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)
- Energywise WOL がハイバネーションモードまたはスタンバイモードの PC を「起動」していません。

  回避策：ありません。CSCtr51014
- **show module** コマンドの出力の ROMMON バージョン番号列が切り捨てられます。

  回避策：**show version** コマンドを使用します。CSCtr30294
- IP SLA セッションの作成は、さまざまな 4 タプルでランダムに失敗します。

  回避策：代替宛先または送信元ポートを選択します。CSCty05405

- システムは MSP およびメタデータがイネーブルの状態で 512 を超える SIP フローに拡張することはできません。

  回避策：ありません。CSCty79236

- IOS リリース15.0(2)SG3 を実行している次のラインカード。
  - 48 10/100/1000BaseT Premium POE E Series WS-X4648-RJ45V+E（JAE14310RHU）
  - 6 Sup 6-E 10GE（X2）、1000BaseX (SFP) WS-X45-SUP6-E（JAE13104VVY）

  次の制約事項が適用されます。
  - サブインターフェイスは、1 ギガビットおよび 10 ギガビットのインターフェイスではサポートされていません。
  - ポートチャネルメンバーは、QoS ポリシーの複数の分類基準をサポートしていません。
  - uRFP が有効で、TCAM が完全に使用されている場合、CEF は自動的に無効になります。
- IPv6 アクセスリストの設定中に、v6 アクセスリストモードで最初のステートメントとして「ハードウェア統計情報」を指定した場合（つまり、他の v6 ACE ステートメントを発行する前）、この設定は有効になりません。同様に、**show running** コマンドの出力から「hardware statistics」の設定が失われます。

  回避策：IPv6 アクセスリストの設定時に、「hardware statistics」ステートメントの前に 1 つ以上の IPv6 ACE を設定します。CSCuc53234
- 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。
- Cisco IOS 15.1(1)SG または 3.3.0SG より前のリリース間で ISSU を実行して Cisco IOS 15.1(1)SG（または 3.3.0SG）以降をリリースすると、アップグレードが完了した後にマルチキャストルーティングを実行するスイッチがトラフィックを永続的にドロップすることがあります。シャーシをリロードすることで、マルチキャスト トラフィックを回復できます。または、ISSU の前にすべてのマルチキャスト設定を削除し、ISSU の完了時に追加し直すこともできます。CSCuj42672

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『Caveats for Cisco IOS リリース 12.4 』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

Cisco IOS リリース 15.1(1)SG2 の未解決の警告

この項では、Cisco IOS リリース 15.1(1)SG2 で未解決の警告について説明します。

- **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てい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ーバイザエンジンとスタンバイ スーパーバイザ エンジンでそれぞれ個別に生成され、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

- 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** コマンドでの出力で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ーバイザエンジンとスタンバイ スーパーバイザ エンジンのバージョンが異なる場合、スタンバイ スーパーバイザ 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

- 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ー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 スーパーバイザ 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ーバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパーバイザ 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ーバイザエンジンとスタンバイ スーパーバイザ 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ー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 スーパーバイザ 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、Cisco IOS リリース 12.2(50)SG を実行中のクラッシックまたは E シリーズの Catalyst 4500 スーパバイザーエンジンに適用されます。

  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 スーパーバイザ 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ー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ーバイザエンジンの 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 が再度取得され、スタンバイ スーパーバイザ エンジンに同期されるようになります。CSCsw91661

- 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、表示された情報が誤っているため、無視する必要があります。

  CSCsz34522

- 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ー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ー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

- 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、10 GE 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

- 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

- RADIUS サーバテスト機能が有効になっているか、または RADIUS サーバの dead-criteria が設定されており、RADIUS サーバの deadtime が 0 に設定されているか、または設定されていない場合、RADIUS サーバステータスが AAA に正しくリレーされません。

  回避策：dead-criteria と deadtime の両方を設定します。

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

- オープン認証を設定し、SSO を実行すると、スパニングツリーの状態と MAC アドレスが新しいスタンバイ スーパーバイザ エンジンに同期されません。この動作は、2 回目のスイッチオーバーの後にのみトラフィックを中断します。これは、新しいスタンバイ スーパーバイザ エンジンが最初のスイッチオーバー後に誤った状態を保有し、2 回目のスイッチオーバーがブロッキング状態でポートを起動するためです。

  回避策：ポートで **shut** と **no shut** を入力して、STP 状態を同期します。CSCtf52437

- 2 番目のポート TLV 対応の電話機の背後に接続されているゲスト VLAN 内のデバイスは、SSO フェールオーバー後にパケット損失が発生します。電話機から最初の CDP フレームが着信した後、デバイスで認証の再起動が行われます。

  回避策：ありません。CSCto46018

- スイッチを再起動すると、ポートチャネル インターフェイスの要素に対するインターフェイス MTU サイズの設定値は、IPv6 トラフィックに対して機能しません。

  回避策：スイッチがリロードされたら、ポートチャネル インターフェイスで **shut** と **no shut** を入力します。

  CSCto27085

- レイヤ 3 CE 側インターフェイスが 2 つあり、それぞれが CE に接続して CE 間で WCCP を分割し、WCCP サービス（60（ftp-native）など）を一方のインターフェイスから他方に移動すると、ターゲットインターフェイスで古い CE から新しい CE にサービスを完全に転送できません。

  回避策：CE 側インターフェイスをシャットダウンします。すべての mask-value エントリがターゲット CE をポイントした後、CE 側インターフェイスをシャットダウンします。CSCtl09941

- dscp/ipp/tos、log/log-input、フラグメント、tcp フラグ演算子などの高度な演算子が含まれていると、ダイナミック ACL は正しく機能しません。

  回避策：ダイナミック ACL からこれらの演算子を削除します。CSCts05302

- 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

- WS-X45-SUP6-E スーパーバイザの 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バイザーー エンジンが IOS を実行しており、スタンバイ スーパバイザーー エンジンが ROMMON で実行され、スタンバイ スーパバイザー 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

- 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

- 多数の VLAN マッピングが設定されている場合、メンバーポートがポートチャネルに参加できず、警告が発行されないことがあります。

  回避策：VLAN マッピングの数を減らします。CSCtn56208

- マルチキャスト グループ アドレスを持つサービスグループが未設定の場合、WCCP サービスが再取得されず、再設定されます。

  回避策：IP マルチキャストルーティングをグローバルに設定し、CE 側インターフェイスで IP PIM スパースデンスモードを確立します。CSCtl97692

- IP アドレスがルータ ID として使用されているインターフェイスが削除またはシャットダウンされた場合で、サービスグループをマルチキャスト グループ アドレスで設定している場合、CE へのパケットリダイレクションが停止し、パケットは宛先に直接転送されます。

  回避策：サービスグループの設定を解除して再設定します。CSCtn88087

- スイッチが SVI またはレイヤ 3 インターフェイスに対して有効になっていない場合、新しく展開されたスイッチでグローバル WCCP サービス設定を有効にできません（WCCP グローバル設定は受け入れられますが、NVGEN は失敗します）。

  回避策：実行コンフィギュレーションでレイヤ 3 インターフェイスを有効にします。CSCsc88636

- **issu changeversion** コマンドで **quick** オプションを使用すると、次のことが発生する場合があります。
  - さまざまなレイヤ 3 プロトコルのリンクフラップ。
  - アップグレードプロセス中の数秒のトラフィック損失の発生。

  回避策：**issu changeversion** コマンドで **quick** オプションを使用しないでください。CSCto51562

- 事前に AS でポリシーが変更されている場合、ピアポリシーは再認証後に更新されません。再認証後、元のピアポリシーは保持されます。

  回避策：ポートで **shut** と **no shut** を入力します。CSCts29515

- Cisco TrustSec と RADIUS アカウンティングの両方を有効にすると、RADIUS クライアント（Ciscoスイッチ）と RADIUS/CTS サーバの間で、DOT1X/RADIUS アカウンティングメッセージのヘッダーのオーセンティケータフィールドの計算方法に相違が生じます。

  Cisco IOS AAA クライアントは、PAC シークレットを使用してオーセンティケータを計算します。Cisco Secure ACS 5.2 は共有秘密を使用します。この動作により不一致が発生し、アカウンティングメッセージが拒否され、クライアントはサーバを無応答としてマークします。

  回避策：ありません。802.1X アカウンティングを無効にする必要があります。CSCts26844

- ダウンストリームスイッチで複数の等コストマルチパス（ECMP）が使用可能で、フロー統計を提供するために Mediatrace が呼び出された場合、動的ポリシーはフローの統計を表示しません。

  Mediatrace は正しいインバウンド インターフェイスを検出できず、メディアフローに使用されるものとは異なるインターフェイスにダイナミックポリシーを適用します。

  回避策：ありません。CSCts20229

- スイッチオーバーが Mediatrace レスポンダで作成された場合、監視対象のフロータプル用に作成されたダイナミックアクセスリストは削除されません。スイッチオーバー後に Mediatrace イニシエータは別のダイナミックアクセスリストのセットを作成しますが、古いアクセスリストは設定に残ります。

古いダイナミックアクセスリストの影響は、不要なトラフィックをモニタすることです。

回避策:

- スイッチオーバーがスケジュールされている場合は、イニシエータでスケジュールされたセッションを削除します。新しいアクティブなスーパーバイザエンジンがレスポンダで起動した後にセッションを再度スケジュールします。
- Mediatrace レスポンダ SSO が計画されていない場合は、新しいアクティブなスーパーバイザエンジンが起動した後、古いダイナミックアクセスリストを手動で削除します。CSCty75070

- **unidirectional send-only | receive-only** コマンドを使用してインターフェイスを単方向として設定しても、そのインターフェイスは双方向モードでパケットを送信（送信専用単方向イーサネットモードとして設定）、または受信（受信専用単方向イーサネットモードとして設定）できます。

  回避策：ありません。CSCtx95359

- **snmp server host** *x.x.x.x* コンフィギュレーション コマンドに「bfd」サフィックスを追加すると、BFD トラップ ciscoBfdSessUp と ciscoBfdSessDown が生成されません。

  回避策：**snmp-server host** *x.x.x.x* コンフィギュレーション コマンドで「bfd」サフィックスを指定しないでください。CSCtx51561

- **write mem** を入力せずに startup-config をスイッチに直接転送し、startup-configに **hw-module uplink shared-backplane** コマンドが含まれていると、Supervisor Engine 6-E の 4 つのポートが後続のリロードでアクティブになりません。各スーパーバイザエンジンの 2 番目のポートは非アクティブのままです。

  回避策：コンソールまたは VTY から **hw-module uplink shared-backplane** を設定し、**write mem** と入力します。CSCtx43568

- システムまたはユーザのいずれかが開始したリロード操作中に、システムがシャットダウンすると次のメッセージが表示されます。

  ```
  HARDWARE WATCHDOG
  ```

  このメッセージは、システムの起動中には表示されません。

  回避策：不要です。これは単なる情報メッセージです。CSCtz15738

- IGMP スヌーピングが有効になっている場合、トンネルインターフェイスを介して受信したマルチキャストトラフィックは、発信インターフェイスリストに転送されません。

  回避策：IGMP スヌーピングを無効にします。CSCuc65538

- CDP スピーカーに接続されたポートがダウンすると、小規模なメモリリーク（通常は 300 バイト未満）が発生します。

  回避策：頻繁にフラップすることがあるインターフェイスで CDP を無効にします。CSCub85948

- 着脱可能な GLC-GE-100FX は WS-X4624-SFP-E、WS-X4640-CSFP-E、または WS-X4612-SFP-E モジュールで使用すると動作しません。

  回避策：なし。CSCui23911

Cisco IOS リリース 15.1(1)SG2 で解決済みの警告

この項では、Cisco リリース 15.1(1)SG2 で解決済みの警告について説明します。

- Cisco IOS XE 3.3.0SG または 3.3.1SG を搭載したスイッチを暗号化（k9）イメージを使用して起動すると、ラインカードに Auth Fail というステータスが表示され、オンラインにならない場合があります。非暗号化イメージは影響を受けません。

  回避策：**hw-module module** *m* **reset** コマンドを使用するか、または手動 OIR でラインカードをリセットします。CSCuc64146

- Cisco IOS XE 3.3.1SG へのアップグレード後、タイプ PWR-C45-4200ACV の電源を備えたスイッチで、次のいずれかのメッセージが表示されることがあります。

```
%C4K_CHASSIS-3-INSUFFICIENTPOWERSUPPLIESDETECTED: Insufficient power supplies present
for specified config
%C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the chassis are receiving
different voltage inputs
%C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the chassis are of different
types (AC/DC) or wattage
```

  電源または電源の入力は 220 V と表示されるべきところ、110 V と誤って表示されます。1 台の電源にのみ問題がある場合、電源は err-disable 状態になることがあります。両方の電源に問題があり、両方とも 110 V と認識される場合、err-disable 状態にはなりません。また、スイッチ内の他のモジュールの電源が拒否され、電源がオンにならない場合があります。

  回避策：電源入力を取り外し、電源を取り外すか再挿入してから、電源入力を復元します。CSCuc07562

Cisco IOS リリース 15.1(1)SG1 の未解決の警告

この項では、Cisco IOS リリース 15.1(1)SG1 で未解決の警告について説明します。

- **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。
  - 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てい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ーバイザエンジンとスタンバイ スーパーバイザ エンジンでそれぞれ個別に生成され、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

- 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** コマンドでの出力で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ーバイザエンジンとスタンバイ スーパーバイザ エンジンのバージョンが異なる場合、スタンバイ スーパーバイザ 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

- 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ー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 スーパーバイザ 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ーバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパーバイザ 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ーバイザエンジンとスタンバイ スーパーバイザ 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ー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 スーパーバイザ 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、Cisco IOS リリース 12.2(50)SG を実行中のクラッシックまたは E シリーズの Catalyst 4500 スーパーバイザエンジンに適用されます。

  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 スーパーバイザ 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ー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ーバイザエンジンの 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 が再度取得され、スタンバイ スーパーバイザ エンジンに同期されるようになります。CSCsw91661

- 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、表示された情報が誤っているため、無視する必要があります。

  CSCsz34522

- 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ー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ー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

- 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、10 GE 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

- 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

- RADIUS サーバテスト機能が有効になっているか、または RADIUS サーバの dead-criteria が設定されており、RADIUS サーバの deadtime が 0 に設定されているか、または設定されていない場合、RADIUS サーバステータスが AAA に正しくリレーされません。

  回避策：dead-criteria と deadtime の両方を設定します。

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

- オープン認証を設定し、SSO を実行すると、スパニングツリーの状態と MAC アドレスが新しいスタンバイ スーパーバイザ エンジンに同期されません。この動作は、2 回目のスイッチオーバーの後にのみトラフィックを中断します。これは、新しいスタンバイ スーパーバイザエンジンが最初のスイッチオーバー後に誤った状態を保有し、2 回目のスイッチオーバーがブロッキング状態でポートを起動するためです。

  回避策：ポートで **shut** と **no shut** を入力して、STP 状態を同期します。CSCtf52437

- 2 番目のポート TLV 対応の電話機の背後に接続されているゲスト VLAN 内のデバイスは、SSO フェールオーバー後にパケット損失が発生します。電話機から最初の CDP フレームが着信した後、デバイスで認証の再起動が行われます。

  回避策：ありません。CSCto46018

- スイッチを再起動すると、ポートチャネル インターフェイスの要素に対するインターフェイス MTU サイズの設定値は、IPv6 トラフィックに対して機能しません。

  回避策：スイッチがリロードされたら、ポートチャネル インターフェイスで **shut** と **no shut** を入力します。

  CSCto27085

- レイヤ 3 CE 側インターフェイスが 2 つあり、それぞれが CE に接続して CE 間で WCCP を分割し、WCCP サービス（60（ftp-native）など）を一方のインターフェイスから他方に移動すると、ターゲットインターフェイスで古い CE から新しい CE にサービスを完全に転送できません。

  回避策：CE 側インターフェイスをシャットダウンします。すべての mask-value エントリがターゲット CE をポイントした後、CE 側インターフェイスをシャットダウンします。CSCtl09941

- dscp/ipp/tos、log/log-input、フラグメント、tcp フラグ演算子などの高度な演算子が含まれていると、ダイナミック ACL は正しく機能しません。

  回避策：ダイナミック ACL からこれらの演算子を削除します。CSCts05302

- 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

- WS-X45-SUP6-E スーパーバイザの 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

- 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

- 多数の VLAN マッピングが設定されている場合、メンバーポートがポートチャネルに参加できず、警告が発行されないことがあります。

  回避策：VLAN マッピングの数を減らします。CSCtn56208

- マルチキャスト グループ アドレスを持つサービスグループが未設定の場合、WCCP サービスが再取得されず、再設定されます。

  回避策：IP マルチキャストルーティングをグローバルに設定し、CE 側インターフェイスで IP PIM スパースデンスモードを確立します。CSCtl97692

- IP アドレスがルータ ID として使用されているインターフェイスが削除またはシャットダウンされた場合で、サービスグループをマルチキャスト グループ アドレスで設定している場合、CE へのパケットリダイレクションが停止し、パケットは宛先に直接転送されます。

  回避策：サービスグループの設定を解除して再設定します。CSCtn88087

- スイッチが SVI またはレイヤ 3 インターフェイスに対して有効になっていない場合、新しく展開されたスイッチでグローバル WCCP サービス設定を有効にできません（WCCP グローバル設定は受け入れられますが、NVGEN は失敗します）。

  回避策：実行コンフィギュレーションでレイヤ 3 インターフェイスを有効にします。CSCsc88636.

- **issu changeversion** コマンドで **quick** オプションを使用すると、次のことが発生する場合があります。
  - さまざまなレイヤ 3 プロトコルのリンクフラップ。
  - アップグレードプロセス中の数秒のトラフィック損失の発生。

  回避策：**issu changeversion** コマンドで **quick** オプションを使用しないでください。CSCto51562

- 事前に AS でポリシーが変更されている場合、ピアポリシーは再認証後に更新されません。再認証後、元のピアポリシーは保持されます。

  回避策：ポートで **shut** と **no shut** を入力します。CSCts29515

- Cisco TrustSec と RADIUS アカウンティングの両方を有効にすると、RADIUS クライアント（Cisco スイッチ）と RADIUS/CTS サーバの間で、DOT1X/RADIUS アカウンティングメッセージのヘッダーのオーセンティケータフィールドの計算方法に相違が生じます。

  Cisco IOS AAA クライアントは、PAC シークレットを使用してオーセンティケータを計算します。Cisco Secure ACS 5.2 は共有秘密を使用します。この動作により不一致が発生し、アカウンティングメッセージが拒否され、クライアントはサーバを無応答としてマークします。

  回避策：ありません。802.1X アカウンティングを無効にする必要があります。CSCts26844

- ダウンストリームスイッチで複数の等コストマルチパス（ECMP）が使用可能で、フロー統計を提供するために Mediatrace が呼び出された場合、動的ポリシーはフローの統計を表示しません。

  Mediatrace は正しいインバウンドインターフェイスを検出できず、メディアフローに使用されるものとは異なるインターフェイスにダイナミックポリシーを適用します。

  回避策：ありません。CSCts20229

- スイッチオーバーが Mediatrace レスポンダで作成された場合、監視対象のフロータプル用に作成されたダイナミックアクセスリストは削除されません。スイッチオーバー後に Mediatrace イニシエータは別のダイナミックアクセスリストのセットを作成しますが、古いアクセスリストは設定に残ります。

  古いダイナミックアクセスリストの影響は、不要なトラフィックをモニタすることです。

  回避策：
  - スイッチオーバーがスケジュールされている場合は、イニシエータでスケジュールされたセッションを削除します。新しいアクティブなスーパーバイザエンジンがレスポンダで起動した後にセッションを再度スケジュールします。
  - Mediatrace レスポンダ SSO が計画されていない場合は、新しいアクティブなスーパーバイザエンジンが起動した後、古いダイナミックアクセスリストを手動で削除します。CSCty75070

- **unidirectional send-only | receive-only** コマンドを使用してインターフェイスを単方向として設定しても、そのインターフェイスは双方向モードでパケットを送信（送信専用単方向イーサネットモードとして設定）、または受信（受信専用単方向イーサネットモードとして設定）できます。

  回避策：ありません。CSCtx95359

- **snmp server host** *x.x.x.x* コンフィギュレーション コマンドに「bfd」サフィックスを追加すると、BFD トラップ ciscoBfdSessUp と ciscoBfdSessDown が生成されません。

  回避策：**snmp-server host** *x.x.x.x* コンフィギュレーション コマンドで「bfd」サフィックスを指定しないでください。CSCtx51561

- **write mem** を入力せずに startup-config をスイッチに直接転送し、startup-configに **hw-module uplink shared-backplane** コマンドが含まれていると、Supervisor Engine 6-E の 4 つのポートが後続のリロードでアクティブになりません。各スーパーバイザエンジンの 2 番目のポートは非アクティブのままです。

  回避策：コンソールまたは VTY から **hw-module uplink shared-backplane** を設定し、**write mem** と入力します。CSCtx43568

- システムまたはユーザのいずれかが開始したリロード操作中に、システムがシャットダウンすると次のメッセージが表示されます。

  ```
  HARDWARE WATCHDOG
  ```

  このメッセージは、システムの起動中には表示されません。

  回避策：不要です。これは単なる情報メッセージです。CSCtz15738

- Cisco IOS XE 3.3.0SG または 3.3.1SG を搭載したスイッチを暗号化（k9）イメージを使用して起動すると、ラインカードに Auth Fail というステータスが表示され、オンラインにならない場合があります。非暗号化イメージは影響を受けません。

  回避策：**hw-module module** *m* **reset** コマンドを使用するか、または手動 OIR でラインカードをリセットします。CSCuc64146

- Cisco IOS XE 3.3.1SG へのアップグレード後、タイプ PWR-C45-4200ACV の電源を備えたスイッチで、次のいずれかのメッセージが表示されることがあります。

  ```
  %C4K_CHASSIS-3-INSUFFICIENTPOWERSUPPLIESDETECTED: Insufficient power supplies present
  for specified config
  %C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the chassis are receiving
  different voltage inputs
  %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the chassis are of different
  types (AC/DC) or wattage
  ```

  電源または電源の入力は 220 V と表示されるべきところ、110 V と誤って表示されます。1 台の電源にのみ問題がある場合、電源は err-disable 状態になることがあります。両方の電源に問題があり、両方とも 110 V と認識される場合、err-disable 状態にはなりません。また、スイッチ内の他のモジュールの電源が拒否され、電源がオンにならない場合があります。

  回避策：電源入力を取り外し、電源を取り外すか再挿入してから、電源入力を復元します。CSCuc07562

- Cisco IOS 15.0(2)SG5 から 15.1(1)SG1 への ISSU アップグレードが失敗します。

  ただし、Cisco IOS 15.0(2)SG5 から 15.1(1)SG2、または Cisco IOS 15.0(2)SG5 から 15.1(2)SG にアップグレードできます。

  回避策：

  - Cisco IOS 15.0(2)SG5 または 15.1(1)SG1 の組み合わせ（アップグレードまたはダウングレード）に RPR を使用します。
  - Cisco IOS 15.1(1)SG1 からのダウングレード。15.0(2)SG4 以前のリリースを使用。
  - Cisco IOS 15.0(2)SG5 からのアップグレード。代わりに 15.1(1)SG2 を使用。

  CSCuc54012

- IGMP スヌーピングが有効になっている場合、トンネルインターフェイスを介して受信したマルチキャストトラフィックは、発信インターフェイスリストに転送されません。

  回避策：IGMP スヌーピングを無効にします。CSCuc65538

- CDP スピーカーに接続されたポートがダウンすると、小規模なメモリリーク（通常は 300 バイト未満）が発生します。

  回避策：頻繁にフラップすることがあるインターフェイスで CDP を無効にします。CSCub85948

- 着脱可能な GLC-GE-100FX は WS-X4624-SFP-E、WS-X4640-CSFP-E、または WS-X4612-SFP-E モジュールで使用すると動作しません。

  回避策：なし。CSCui23911

Cisco IOS リリース 15.1(1)SG1 で解決済みの警告

この項では、Cisco リリース 15.1(1)SG1 で解決済みの警告について説明します。

- Bidir PIM で有効になっているスイッチに、RP アップストリームをポイントするソフトウェア トンネル インターフェイスがある場合、パケットドロップが発生します。

  回避策：ありません。RP アップストリームをポイントする物理インターフェイスの使用を検討します。

  CSCtz11352

- SPAN を使用すると、Cisco XE 3.3.0SG 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。CSCua12869

- コンフィギュレーションに「ip vrf」セクションか「vrf definition」セクションが含まれており、IOS-XE の IP Base または LAN Base のブートレベルを使用しているときに「wr mem」と入力すると、次のメッセージが表示されます。

  回避策：ありません。これは単なる情報メッセージです。CSCtw93140

- 「Authorization succeeded for client (Unknown MAC)」とログに記録した後、次の条件が当てはまるとスイッチがクラッシュします。
  - スイッチポートが次の両方で設定されています。

    authentication event server dead action authorize...

    authentication 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り、dot1x クライアントが認証を試みます。

  回避策：ありません。CSCtx61557

- キューイングポリシーで設定された EtherChannel メンバーインターフェイスの特定の tx キューでトラフィックがドロップされます。ただし、EtherChannel の出力スパンセッションには引き続き表示されます。

  show platform software interface tx-queue コマンドが設定されたキューの数を正しく表示しません（トラフィックをドロップしていない EtherChannel メンバーと比較します）。

  回避策：ポートで shut と入力してから no shut と入力します。CSCua66962

- アクティブなスーパーバイザエンジンか、またはスタンバイ スーパーバイザエンジンが Cisco IOS 15.1(1)SG を実行している場合、スタンバイ スーパーバイザ エンジンはスタンバイコールドまたはスタンバイホットの状態になり、リロードし続けます。

  回避策：他のスーパーバイザエンジンを一時的に取り外すか、別のシャーシにスーパーバイザエンジンを移動して、スーパーバイザエンジンをダウングレードまたはアップグレードします。CSCtz44577

- Cisco 15.0(2)SG4 または 15.1(1)SG で、PoE を搭載した 4648* または 4748* ラインカードを実行しているスイッチで、ラインカードの 1 つのポートが通常はリンクを頻繁にプリッピングした後にリンクアップに失敗します。

  回避策：ポートで **shut** と入力してから **no shut** と入力します。CSCtz94862

- PoE を搭載した 4648* または 4748* ラインカードで Cisco 15.0(2)SG4 または 15.1(1)SGを実行しているスイッチでは、PoE デバイスは 1 つのポートで起動しませんが、同じラインカードの他のポートで動作します。

  回避策：

  - 非 PoE デバイスをポートに接続します。
  - ポートで shutと入力してから no shut と入力します。CSCua63562

- Supervisor Engine 7L-E を搭載する Catalyst 4500E シリーズ スイッチには、デバイスのリロードの原因となる特別に作成されたパケットを処理する際に DoS の脆弱性が含まれます。

  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。

  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-20120926-ecc

  CSCty88456

- Cisco IOS ソフトウェアには、認証されていないリモートの攻撃者がサービス拒否（DoS）状態を引き起こす可能性のある脆弱性が存在します。攻撃者は、影響を与えるデバイスに対して、またはそのデバイスを介して 1 つの DHCP パケットを送信してこの脆弱性を不正に利用し、デバイスをリロードさせ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。この脆弱性を軽減する回避策が利用可能です。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-20120926-dhcp

  CSCty96049

Cisco IOS リリース 15.1(1)SG の未解決の警告

この項では、Cisco IOS リリース 15.1(1)SG で未解決の警告について説明します。

- **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。
  - 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てい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ーバイザエンジンとスタンバイ スーパーバイザ エンジンでそれぞれ個別に生成され、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

- 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** コマンドでの出力で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ーバイザエンジンとスタンバイ スーパーバイザ エンジンのバージョンが異なる場合、スタンバイ スーパーバイザ 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

- 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ー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 スーパーバイザ 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ーバイザエンジンは、バルク同期の一部としてこの設定をスタンバイ スーパーバイザ 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ーバイザエンジンとスタンバイ スーパーバイザ 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ー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 スーパーバイザ 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、Cisco IOS リリース 12.2(50)SG を実行中のクラッシックまたは E シリーズの Catalyst 4500 スーパーバイザエンジンに適用されます。

  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 スーパーバイザ 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ー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ーバイザエンジンの 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 が再度取得され、スタンバイ スーパーバイザ エンジンに同期されるようになります。CSCsw91661

- 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、表示された情報が誤っているため、無視する必要があります。

CSCsz34522

- 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ー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ー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

- 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、10 GE 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

- 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

- RADIUS サーバテスト機能が有効になっているか、または RADIUS サーバの dead-criteria が設定されており、RADIUS サーバの deadtime が 0 に設定されているか、または設定されていない場合、RADIUS サーバステータスが AAA に正しくリレーされません。

  回避策：dead-criteria と deadtime の両方を設定します。

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

- オープン認証を設定し、SSO を実行すると、スパニングツリーの状態と MAC アドレスが新しいスタンバイ スーパーバイザ エンジンに同期されません。この動作は、2 回目のスイッチオーバーの後にのみトラフィックを中断します。これは、新しいスタンバイ スーパーバイザエンジンが最初のスイッチオーバー後に誤った状態を保有し、2 回目のスイッチオーバーがブロッキング状態でポートを起動するためです。

  回避策：ポートで **shut** と **no shut** を入力して、STP 状態を同期します。CSCtf52437

- 2 番目のポート TLV 対応の電話機の背後に接続されているゲスト VLAN 内のデバイスは、SSO フェールオーバー後にパケット損失が発生します。電話機から最初の CDP フレームが着信した後、デバイスで認証の再起動が行われます。

  回避策：ありません。CSCto46018

- スイッチを再起動すると、ポートチャネル インターフェイスの要素に対するインターフェイス MTU サイズの設定値は、IPv6 トラフィックに対して機能しません。

  回避策：スイッチがリロードされたら、ポートチャネル インターフェイスで **shut** と **no shut** を入力します。

  CSCto27085

- レイヤ 3 CE 側インターフェイスが 2 つあり、それぞれが CE に接続して CE 間で WCCP を分割し、WCCP サービス（60（ftp-native）など）を一方のインターフェイスから他方に移動すると、ターゲットインターフェイスで古い CE から新しい CE にサービスを完全に転送できません。

  回避策：CE 側インターフェイスをシャットダウンします。すべての mask-value エントリがターゲット CE をポイントした後、CE 側インターフェイスをシャットダウンします。CSCtl09941

- dscp/ipp/tos、log/log-input、フラグメント、tcp フラグ演算子などの高度な演算子が含まれていると、ダイナミック ACL は正しく機能しません。

  回避策：ダイナミック ACL からこれらの演算子を削除します。CSCts05302

- 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

- WS-X45-SUP6-E スーパーバイザの 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

- 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

- 多数の VLAN マッピングが設定されている場合、メンバーポートがポートチャネルに参加できず、警告が発行されないことがあります。

  回避策：VLAN マッピングの数を減らします。CSCtn56208

- マルチキャスト グループ アドレスを持つサービスグループが未設定の場合、WCCP サービスが再取得されず、再設定されます。

  回避策：IP マルチキャストルーティングをグローバルに設定し、CE 側インターフェイスで IP PIM スパースデンスモードを確立します。CSCtl97692

- IP アドレスがルータ ID として使用されているインターフェイスが削除またはシャットダウンされた場合で、サービスグループをマルチキャスト グループ アドレスで設定している場合、CE へのパケットリダイレクションが停止し、パケットは宛先に直接転送されます。

  回避策：サービスグループの設定を解除して再設定します。CSCtn88087

- スイッチが SVI またはレイヤ 3 インターフェイスに対して有効になっていない場合、新しく展開されたスイッチでグローバル WCCP サービス設定を有効にできません（WCCP グローバル設定は受け入れられますが、NVGEN は失敗します）。

  回避策：実行コンフィギュレーションでレイヤ 3 インターフェイスを有効にします。CSCsc88636

- **issu changeversion** コマンドで **quick** オプションを使用すると、次のことが発生する場合があります。
  - さまざまなレイヤ 3 プロトコルのリンクフラップ。
  - アップグレードプロセス中の数秒のトラフィック損失の発生。

  回避策：**issu changeversion** コマンドで **quick** オプションを使用しないでください。CSCto51562

- 事前に AS でポリシーが変更されている場合、ピアポリシーは再認証後に更新されません。再認証後、元のピアポリシーは保持されます。

  回避策：ポートで **shut** と **no shut** を入力します。CSCts29515

- Cisco TrustSec と RADIUS アカウンティングの両方を有効にすると、RADIUS クライアント（Ciscoスイッチ）と RADIUS/CTS サーバの間で、DOT1X/RADIUS アカウンティングメッセージのヘッダーのオーセンティケータフィールドの計算方法に相違が生じます。

  Cisco IOS AAA クライアントは、PAC シークレットを使用してオーセンティケータを計算します。Cisco Secure ACS 5.2 は共有秘密を使用します。この動作により不一致が発生し、アカウンティングメッセージが拒否され、クライアントはサーバを無応答としてマークします。

  回避策：ありません。802.1X アカウンティングを無効にする必要があります。CSCts26844

- ダウンストリームスイッチで複数の等コストマルチパス（ECMP）が使用可能で、フロー統計を提供するために Mediatrace が呼び出された場合、動的ポリシーはフローの統計を表示しません。

  Mediatrace は正しいインバウンド インターフェイスを検出できず、メディアフローに使用されるものとは異なるインターフェイスにダイナミックポリシーを適用します。

  回避策：ありません。CSCts20229

- スイッチオーバーが Mediatrace レスポンダで作成された場合、監視対象のフロータプル用に作成されたダイナミックアクセスリストは削除されません。スイッチオーバー後に Mediatrace イニシエータは別のダイナミックアクセスリストのセットを作成しますが、古いアクセスリストは設定に残ります。

  古いダイナミックアクセスリストの影響は、不要なトラフィックをモニタすることです。

  回避策：
  - スイッチオーバーがスケジュールされている場合は、イニシエータでスケジュールされたセッションを削除します。新しいアクティブなスーパーバイザエンジンがレスポンダで起動した後にセッションを再度スケジュールします。
  - Mediatrace レスポンダ SSO が計画されていない場合は、新しいアクティブなスーパーバイザエンジンが起動した後、古いダイナミックアクセスリストを手動で削除します。CSCty75070

- **unidirectional send-only | receive-only** コマンドを使用してインターフェイスを単方向として設定しても、そのインターフェイスは双方向モードでパケットを送信（送信専用単方向イーサネットモードとして設定）、または受信（受信専用単方向イーサネットモードとして設定）できます。

  回避策：ありません。CSCtx95359

- **snmp server host** *x.x.x.x* コンフィギュレーション コマンドに「bfd」サフィックスを追加すると、BFD トラップ ciscoBfdSessUp と ciscoBfdSessDown が生成されません。

  回避策：**snmp-server host** *x.x.x.x* コンフィギュレーション コマンドで「bfd」サフィックスを指定しないでください。CSCtx51561

- **write mem** を入力せずに startup-config をスイッチに直接転送し、startup-configに **hw-module uplink shared-backplane** コマンドが含まれていると、Supervisor Engine 6-E の 4 つのポートが後続のリロードでアクティブになりません。各スーパーバイザエンジンの 2 番目のポートは非アクティブのままです。

  回避策：コンソールまたは VTY から **hw-module uplink shared-backplane** を設定し、**write mem** と入力します。CSCtx43568

- Bidir PIM で有効になっているスイッチに、RP アップストリームをポイントするソフトウェア トンネル インターフェイスがある場合、パケットドロップが発生します。

  回避策：ありません。RP アップストリームをポイントする物理インターフェイスの使用を検討します。

  CSCtz11352

- システムまたはユーザのいずれかが開始したリロード操作中に、システムがシャットダウンすると次のメッセージが表示されます。

  ```
  HARDWARE WATCHDOG
  ```

  このメッセージは、システムの起動中には表示されません。

  回避策：不要です。これは単なる情報メッセージです。CSCtz15738

- SPAN を使用すると、Cisco XE 3.3.0SG 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。CSCua12869

- コンフィギュレーションに「ip vrf」セクションか「vrf definition」セクションが含まれており、IOS-XE の IP Base または LAN Base のブートレベルを使用しているときに「wr mem」と入力すると、次のメッセージが表示されます。

  回避策：ありません。これは単なる情報メッセージです。CSCtw93140

- 「Authorization succeeded for client (Unknown MAC)」とログに記録した後、次の条件が当てはまるとスイッチがクラッシュします。
  - スイッチポートが次の両方で設定されています。

    authentication event server dead action authorize...

    authentication 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り、dot1x クライアントが認証を試みます。

  回避策：ありません。CSCtx61557

- キューイングポリシーで設定された EtherChannel メンバーインターフェイスの特定の tx キューでトラフィックがドロップされます。ただし、EtherChannel の出力スパンセッションには引き続き表示されます。

  show platform software interface tx-queue コマンドが設定されたキューの数を正しく表示しません（トラフィックをドロップしていない EtherChannel メンバーと比較します）。

  回避策：ポートで shut と入力してから no shut と入力します。CSCua66962

- アクティブなスーパーバイザエンジンか、またはスタンバイ スーパーバイザ エンジンが Cisco IOS 15.1(1)SG を実行している場合、スタンバイ スーパーバイザ エンジンはスタンバイコールドまたはスタンバイホットの状態になり、リロードし続けます。

  回避策：他のスーパーバイザエンジンを一時的に取り外すか、別のシャーシにスーパーバイザエンジンを移動して、スーパーバイザエンジンをダウングレードまたはアップグレードします。CSCtz44577

- Cisco 15.0(2)SG4 または 15.1(1)SG で、PoE を搭載した 4648* または 4748* ラインカードを実行しているスイッチで、ラインカードの 1 つのポートが通常はリンクを頻繁にプリッピングした後にリンクアップに失敗します。

  回避策：ポートで **shut** と入力してから **no shut** と入力します。CSCtz94862

- PoE を搭載した 4648* または 4748* ラインカードで Cisco 15.0(2)SG4 または 15.1(1)SGを実行しているスイッチでは、PoE デバイスは 1 つのポートで起動しませんが、同じラインカードの他のポートで動作します。

  回避策：

  - 非 PoE デバイスをポートに接続します。
  - ポートで shutと入力してから no shut と入力します。CSCua63562

- Cisco IOS XE 3.3.0SG または 3.3.1SG を搭載したスイッチを暗号化（k9）イメージを使用して起動すると、ラインカードに Auth Fail というステータスが表示され、オンラインにならない場合があります。非暗号化イメージは影響を受けません。

  回避策：**hw-module module** *m* **reset** コマンドを使用するか、または手動 OIR でラインカードをリセットします。CSCuc64146

- IGMP スヌーピングが有効になっている場合、トンネルインターフェイスを介して受信したマルチキャストトラフィックは、発信インターフェイスリストに転送されません。

  回避策：IGMP スヌーピングを無効にします。CSCuc65538

- CDP スピーカーに接続されたポートがダウンすると、小規模なメモリリーク（通常は 300 バイト未満）が発生します。

  回避策：頻繁にフラップすることがあるインターフェイスで CDP を無効にします。CSCub85948

- 着脱可能な GLC-GE-100FX は WS-X4624-SFP-E、WS-X4640-CSFP-E、または WS-X4612-SFP-E モジュールで使用すると動作しません。

  回避策：なし。CSCui23911

Cisco IOS リリース 15.1(1)SG で解決済みの警告

この項では、Cisco リリース 15.1(1)SG で解決済みの警告について説明します。

- スパニングツリーが PVST から Rapid PVST に変更されたときに **show spanning-tree vlan** コマンドを入力すると、無差別トランクとして設定されたポートがスパニングツリーの一部として表示されません。

  回避策：ポートで **shut** と入力してから **no shut** と入力します。CSCtn88228

- **clear ip mroute ?** コマンドを入力すると、**vrf** オプションのみが表示されます。**Hostname** オプションと「*」オプションはシステムで許可されていても、表示されません。**clear ip mroute** コマンドは予期どおりに機能します。

  回避策：ありません。CSCto59368

トラブルシューティング

ここでは、IOS スーパー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。
   - スーパーバイザ 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. スーパーバイザ 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、スーパーバイザ 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、スーパーバイザ 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、スーパーバイザ 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。
- スーパーバイザ エンジンには、シリアル ケーブルとイーサネット ケーブルを混在させ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 MGT）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、スーパーバイザ 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。インストール手順については、『Catalyst 4500 Series Module Installation Guide』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

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:

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:

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 15.0(2)SG リリースノート