



## 制限事項と制約事項

- [制限事項と制約事項 \(1 ページ\)](#)

### 制限事項と制約事項

- コントロールプレーンポリシング (CoPP) : `system-cpp policy` で設定されたクラスがデフォルト値のままの場合、それらのクラスに関する情報は `show run` コマンドで表示されません。代わりに、特権 EXEC モードで `show policy-map system-cpp-policy` または `show policy-map control-plane` コマンドを使用してください。
- Cisco TrustSec の制約事項 : Cisco TrustSec は物理インターフェイスでのみ設定でき、論理インターフェイスでは設定できません。
- Flexible NetFlow の制限事項
  - イーサネット管理ポート (GigabitEthernet0/0) を使用して NetFlow エクスポートを設定することはできません。
  - レイヤ2 ポートチャネル、ループバック、トンネルなどの論理インターフェイスにフローモニタを設定することはできません。
  - 同じインターフェイスの同じ方向について、同じタイプ (IPv4、IPv6、またはデータリンク) のフローモニタを複数設定することはできません。
- ハードウェアの制限 (光ファイバ) : マルチレート SFP は、自動ネゴシエーションによって一部のポートで速度の不一致が発生する可能性があるため、SVL または DAD リンクには適していません。使用する場合は、両側を同じ速度に設定してください。最高速度が推奨されます (例 : SFP-10/25G の場合は 25G、QSFP-40/100G の場合は 100G)。また、リンクの両側はマルチレート SFP である必要があります。他のすべての SVL または DAD リンクポートはマルチレート SFP を使用する必要があります。デバイスで使用されている SFP の物理プロパティを表示するには、`show interfaces transceiver` コマンドを使用します。
- ハードウェアの制限事項 : Cisco QSFP-4SFP10G-CUxM 直接接続銅ケーブルを使用する場合、自動ネゴシエーションがデフォルトで有効になります。もう一方の接続先で自動ネゴシエーションがサポートされていない場合、リンクは起動しません。

- 相互運用性の制限事項：Cisco QSFP-4SFP10G-CUxM 直接接続銅ケーブルを使用した 40G リンクにおいて、リンクの一方が Catalyst 9400 シリーズ スイッチでもう一方が Catalyst 9500 シリーズ スイッチの場合、リンクは起動しないか一方でのみアップ状態になります。このデバイス間の相互運用性の問題を回避するには、Catalyst 9500 シリーズ スイッチのインターフェイスで **speed nonegotiate** コマンドを適用します。このコマンドは、自動ネゴシエーションを無効にしてリンクをアップ状態にします。自動ネゴシエーションを復元するには、**no speed nonegotiation** コマンドを使用します。
- In-Service Software Upgrade (ISSU)
  - メジャーリリーストレイン (16.x、17.x、または 18.x) 内では、ISSU は 3 年以内にリリースされる 2 つの EM 間でサポートされます。
  - メジャーリリーストレイン内で、ISSU は次の場合にサポートされています。
    - 任意の EM (EM1、EM2、EM3) から別の EM (EM1、EM2、EM3) へ  
例：16.9.x から 16.12.x へ、17.3.x から 17.6.x へ、17.6.x から 17.9.x へ
    - 同一 EM 内のすべてのリリース  
例：16.9.2 から 16.9.3 または 16.9.4 または 16.9.x へ、16.12.1 から 16.12.2 または 16.12.3 または 16.12.x へ、17.3.1 から 17.3.2 または 17.3.3 または 17.3.x へ
  - メジャーリリーストレイン間では、ISSU は次の場合にサポートされていません。
    - メジャーリリーストレインの EM から別のメジャーリリーストレインの EM へ  
例：16.x.x から 17.x.x へ、または 17.x.x から 18.x.x へはサポート対象外
    - SM から EM、または EM から SM へ  
例：16.10.x または 16.11.x から 16.12.x へはサポート対象外
- ISSU は、エンジニアリング スペシャル リリース および .s イメージ (またはそれに類するもの) ではサポートされていません。
- ISSU は、ライセンスデータペイロード暗号化 (LDPE) とペイロード暗号化機能のない (NPE) Cisco IOS XE ソフトウェアイメージ間ではサポートされていません。
- ISSU ダウングレードはサポートされません。
- Cisco IOS XE Fuji 16.9.x から Cisco IOS XE Gibraltar 16.12.x への ISSU の実行時、OSPFv3 で **interface-id snmp-if-index** コマンドが設定されていないとパケット損失が発生する可能性があります。ISSU を実行する際は、メンテナンス期間中かデバイスをネットワークから分離 (メンテナンスモード機能を使用) した後、事前に **interface-id snmp-if-index** コマンドを設定しておいてください。
- ISSU ではダウンタイムなしでアップグレードを実行できますが、メンテナンス期間中にのみ実行することをお勧めします。
- ソフトウェアリリースで導入された新しい機能で設定の変更が必要な機能については、ISSU の実行時に有効にしないでください。

- ダウングレード後のバージョンのソフトウェアイメージで使用できない機能については、ISSUを開始する前に無効にしてください。
- M.2 SATA SSD ドライブ：ブートローダーバージョン 16.6.2r では、M.2 SATA SSD ドライブに ROMMON プロンプト (`rommon> dir disk0`) でアクセスすることはできません。対応するファイルシステムプロトコルがデバイスで見つからないことを示すエラーメッセージが表示されます。このドライブにブートローダーバージョン 16.6.2r でアクセスする場合は、起動後に Cisco IOS プロンプトからアクセスしてください。
- No service password recovery：ROMMON バージョン R16.6.1r および R16.6.2r では、「no service password-recovery」機能は使用できません。
- QoS の制約事項
  - QoS キューイングポリシーを設定する際は、キューイングバッファの合計が 100% を超えないようにしてください。
  - サブインターフェイスでのポリシングおよびマーキングポリシーがサポートされています。
  - スイッチ仮想インターフェイス (SVI) でのポリシーのマーキングがサポートされています。
  - ポートチャンネルインターフェイス、トンネルインターフェイス、およびその他の論理インターフェイスでは QoS ポリシーはサポートされません。
  - スタックキューイングおよびスケジューリング (SQS) は、1.4 Gbps を超える CPU バウンドパケットをドロップします。
- 冗長性：スーパーバイザモジュール（ハードウェア）では冗長性がサポートされます。ソフトウェアの冗長性は Cisco IOS XE Everest 16.6.2 以降でサポートされています。ただし、関連する Route Processor Redundancy (RPR) 機能はサポートされません。Cisco StackWise Virtual を使用した Route Processor Redundancy (RPR) 搭載のクラウドスーパーバイザもサポートされません。

スイッチオーバーを実行する前に、**show redundancy**、**show platform**、**show platform software iomd redundancy** コマンドを使用して、両方の SSO が形成されていること、および IOMD プロセスが完了していることを確認してください。

次の **show redundancy** の出力例では、両方の SSO が形成されていることを確認できます。

```
Switch# show redundancy
Redundant System Information :
-----
Available system uptime = 3 hours, 30 minutes
Switchovers system experienced = 2
Standby failures = 0
Last switchover reason = active unit removed

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up
```

```

Current Processor Information :
-----
Active Location = slot 3
Current Software state = ACTIVE
Uptime in current state = 2 hours, 57 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
  Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

Peer Processor Information :
-----
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 2 hours, 47 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
  Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

```

次の **show platform software iomd redundancy** コマンドの出力例では、両方の SSO が形成されていること、および HA\_STATE フィールドが ready になっていることを確認できます。

```

Switch# show platform software iomd redundancy
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Local RF state = ACTIVE
Peer RF state = STANDBY HOT

slot  PSM STATE   SPA INTF   HA_STATE HA_ACTIVE
   1    ready    started   ready    00:01:16
   2    ready    started   ready    00:01:22
   3    ready    started   ready    00:01:27 ***active RP
   4    ready    started   ready    00:01:27
<output truncated>

```

次の **show platform** コマンドの出力例では、すべてのラインカードモジュールとスーパーバイザモジュールの state が ok になっていることを確認できます。これは、IOMD プロセスが完了したことを示します。

```

Switch# show platform
Chassis type: C9407R

Slot      Type                State                Insert time (ago)
-----
1         C9400-LC-24XS      ok                   3d09h
2         C9400-LC-48U       ok                   3d09h
R0        C9400-SUP-1        ok, active          3d09h
R1        C9400-SUP-1        ok, standby         3d09h
P1        C9400-PWR-3200AC   ok                   3d08h
P2        C9400-PWR-3200AC   ok                   3d08h
P17       C9407-FAN           ok                   3d08h
<output truncated>

```

- セキュア シェル (SSH)

- SSH バージョン 2 を使用してください。SSH バージョン 1 はサポートされていません。
- SCP および SSH の暗号化操作の実行中は、SCP の読み取りプロセスが完了するまで、デバイスの CPU が高くなることが想定されます。SCP は、ネットワーク上のホスト間でのファイル転送をサポートしており、転送に SSH を使用します。

SCP および SSH の操作は現在はハードウェア暗号化エンジンでサポートされていないため、暗号化と復号化のプロセスがソフトウェアで実行されることで CPU が高くなります。SCP および SSH のプロセスによる CPU 使用率が 40 ~ 50% になる場合がありますが、デバイスがシャットダウンされることはありません。

- ポリシーを使用したスマートライセンス：Cisco IOS XE Amsterdam 17.3.2a 以降、ポリシーを使用したスマートライセンスの導入により、製品インスタンスまたはデバイスのホスト名を設定しても、Unique Device Identifier (UDI) のみが表示されます。この表示の変更は、以前のリリースでホスト名が表示されていたすべてのライセンスユーティリティとユーザーインターフェイスで確認できます。これにより何らかのライセンス機能が影響を受けることはありません。この制限に対する回避策はありません。

この制限の影響を受けるライセンスユーティリティとユーザーインターフェイスには、Cisco Smart Software Manager (CSSM)、Cisco Smart License Utility (CSLU)、Smart Software Manager On-Prem (SSM On-Prem) のみが含まれます。

この制限は、Cisco IOS XE Cupertino 17.9.1 から削除されました。ホスト名を設定し、ホスト名のプライバシーを無効にすると (**no license smart privacy hostname** グローバル コンフィギュレーションコマンド)、ホスト名情報が製品インスタンスから送信され、該当するユーザーインターフェイス (CSSM、CSLU、SSM オンプレミス) に表示されます。詳細については、このリリースのコマンドリファレンスを参照してください。

- TACACS レガシーコマンド：レガシー **tacacs-server host** コマンドを設定しないでください。このコマンドは廃止されました。デバイス上で実行されているソフトウェアバージョンが Cisco IOS XE Gibraltar 16.12.2 以降のリリースである場合、レガシーコマンドを使用すると認証が失敗する可能性があります。グローバル コンフィギュレーションモードで **tacacs server** コマンドを使用します。
- アップリンクの対称性：冗長なスーパーバイザモジュールを取り付ける場合は、スイッチオーバー時のパケット損失を最小限に抑えるために、アップリンクを対称な状態にすることを推奨します。

アップリンクの対称な状態とは、両方のスーパーバイザモジュールの同じインターフェイスに同じタイプのトランシーバモジュールがある状態のことです。たとえば、トランシーバが取り付けられていない TenGigabitEthernet インターフェイスがデフォルトの 10G モードで動作しているとします。この場合、もう一方のスーパーバイザの対応するインターフェイスに 10G トランシーバがあれば、それらは対称な状態となります。対称な状態にすることで、SWO パケット損失とユーザーエクスペリエンスが最適化されます。

アップリンクが非対称になるのは、一方のスーパーバイザにトランシーバ速度がもう一方のスーパーバイザと一致しないインターフェイスのペアが 1 つ以上ある場合です。

- USB の認証 : Cisco USB ドライブをスイッチに接続すると、既存の暗号化事前共有キーでドライブの認証が試行されます。USB ドライブからは認証用のキーが送信されないため、**password encryption aes** コマンドを入力するとコンソールに次のメッセージが表示されません。

```
Device(config)# password encryption aes  
Master key change notification called without new or old key
```

- Catalyst 9000 シリーズ スイッチは、MACsec スイッチ間接続をサポートします。オーバーレイネットワークでスイッチからホストへの MACsec 接続を設定することは推奨されません。既存のスイッチからホストへの MACsec の実装または設計レビューについては、シスコの営業担当者またはチャンネルパートナーにお問い合わせください。
- VLAN の制限: スイッチの設定時にデータと音声ドメインを定義し、スイッチスタック全体で音声 VLAN とは異なるデータ VLAN を維持するには、明確に定義された分離を行うことをお勧めします。1 つのインターフェイス上のデータと音声ドメインに対して同じ VLAN が設定されている場合、CPU 使用率が高くなり、デバイスが影響を受ける可能性があります。
- YANG データモデリングの制限事項 : サポートされる NETCONF の最大同時セッション数は 20 セッションです。
- Embedded Event Manager : ID イベントディテクタは、Embedded Event Manager ではサポートされていません。
- ファイルシステムチェック (fsck) ユーティリティは、インストールモードではサポートされません。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。