



特記事項

- [特記事項 \(1 ページ\)](#)

特記事項

- [サポートされていない機能](#)
- [サポートされる機能の全リスト](#)
- [隠しコマンドへのアクセス](#)
- [デフォルトの動作](#)

サポートされていない機能

- **Cisco TrustSec**
 - Cisco TrustSec ネットワーク デバイス アドミッション コントロール (NDAC) (アップリンク)
- **ハイアベイラビリティ**
 - Cisco StackWise Virtual ソリューションでは、Resilient Ethernet Protocol (REP) および Remote Switched Port Analyzer (RSPAN) はサポートされていません。
- **インターフェイスおよびハードウェア**
 - 高速 PoE
- **レイヤ 2**
 - オーディオビデオブリッジング (IEEE802.1AS、IEEE 802.1Qat、および IEEE 802.1Qav を含む)
- **セキュリティ**
 - IPsec VPN

- C9400-SUP-1XL-Y での MACsec スイッチ間接続。
 - オーバーレイネットワークでのスイッチからホストへの MACsec 接続。
 - 仮想ルーティングおよび転送 (VRF) 対応 Web 認証
- システム管理
 - パフォーマンスモニタリング (PerfMon)
 - ブランチ展開のための統合アクセス
 - ネットワーク ロード バランシング (NLB)

サポートされる機能の全リスト

プラットフォームでサポートされている機能の完全なリストについては、[Cisco Feature Navigator](#) を参照してください。

隠しコマンドへのアクセス

Cisco IOS XE Fuji 16.8.1a 以降では、セキュリティ対策の強化として、隠しコマンドにアクセスする方法が変更されています。

隠しコマンドは Cisco IOS XE に以前からありましたが、CLI ヘルプは用意されていませんでした。つまり、システムプロンプトで疑問符 (?) を入力しても、使用できるコマンドの一覧は表示されません。これらのコマンドは、Cisco TAC による高度なトラブルシューティングでの使用のみを目的としており、文書化もされていませんでした。

Cisco IOS XE Fuji 16.8.1a より、隠しコマンドは次のカテゴリで使用できます。

- カテゴリ 1：特権 EXEC モードまたはユーザー EXEC モードの隠しコマンド。これらのコマンドにアクセスするには、最初に **service internal** コマンドを入力します。
- カテゴリ 2：いずれかのコンフィギュレーションモード（グローバルやインターフェイスなど）の隠しコマンド。これらのコマンドについては、**service internal** コマンドは必要ありません。

さらに、カテゴリ 1 および 2 の隠しコマンドには以下が適用されます。

- コマンドの CLI ヘルプがあります。システムプロンプトで疑問符 (?) を入力すると、使用できるコマンドの一覧が表示されます。

注：カテゴリ 1 では、疑問符を入力する前に **service internal** コマンドを入力します。これは、カテゴリ 2 では必要ありません。

- 隠しコマンドを使用すると、%PARSER-5-HIDDEN syslog メッセージが生成されます。次に例を示します。

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header' is a hidden command.  
Use of this command is not recommended/supported and will be removed in future.
```

カテゴリ 1 および 2 以外の内部コマンドは CLI に表示されます。それらのコマンドについては、%PARSER-5-HIDDEN syslog メッセージは生成されません。



重要 隠しコマンドは TAC からの指示の下でのみ使用することを推奨します。

隠しコマンドの使用が見つかった場合は、TAC ケースを開き、隠しコマンドと同じ情報を収集する別の方法（EXEC モードの隠しコマンドの場合）、隠しコマンド以外を使用して同じ機能を設定する方法（コンフィギュレーションモードの隠しコマンドの場合）を探してください。

デフォルトの動作

Cisco IOS XE Gibraltar 16.12.5 以降では、IP パケットの Do not fragment ビット（DF ビット）は、すべての発信 RADIUS パケット（デバイスから RADIUS サーバーに向かうパケット）に対して常に 0 に設定されます。

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。