IPv6 を介した SSH サポート

セキュア シェル（SSH）により IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

IPv6 を介した SSH サポートの前提条件

- IPSec（データ暗号規格（DES）または3DES）暗号ソフトウェア イメージがデバイスにロードされている。SSH サーバおよび SSH クライアントへの IPv6 トランスポートには、IPSec 暗号化ソフトウェア イメージが必要です。
- デバイスのホスト名およびホスト ドメインが設定されている。
- SSH を自動的にイネーブルにする Rivest、Shamir、および Adelman（RSA）キー ペアがデバイスに生成されている。
- ローカル アクセスまたはリモート アクセス用にユーザ認証メカニズムがデバイスに設定されている。
- IPv4 トランスポートを介した TACACS+ または RADIUS を設定した後に IPv6 トランスポートを介して SSH サーバ に接続し、SSH クライアントを認証する。

IPv4 トランスポートを介した SSH 用の基本的な制限は、IPv6 トランスポートを介した SSH に適用されます。ローカルに保存されたユーザ名とパスワードの使用は、IPv6 トランスポートを介した SSH によってサポートされる唯一のユーザ認証メカニズムです。TACACS+ および RADIUS ユーザ認証メカニズムは、IPv6 トランスポートを介してサポートされていません。

IPv6 を介した SSH サポートに関する情報

IPv6 トランスポートを介した SSH

IPv6 におけるセキュア シェル（SSH）は、IPv4 における SSH と同じように機能し、同じ利点があります。SSH サーバ機能を使用すると、SSH クライアントは Cisco デバイスへのセキュアな暗号化された接続を確立できます。SSH クライアント機能を使用すると、Cisco デバイスは別の Cisco デバイスまたは SSH サーバが稼働する他のデバイスへのセキュアな暗号化された接続を確立できます。SSH への IPv6 の機能拡張により、IPv6 アドレスがサポートされるため、Cisco デバイスは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

IPv6 を介した SSH サポートを構成する方法

IPv6 デバイスでの SSH のイネーブル化

このタスクはオプションです。SSH パラメータを設定しない場合は、デフォルト値が使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*] 例： `Device(config)# IP ssh timeout 100 authentication-retries 2`	デバイス上で SSH 制御変数を設定します。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**ssh** [**-v** { **1** | **2** } | **c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** } | **-l** *userid* | **-l** *userid:vrfname number ip-address ip-address* | **-l** *userid:rotary number ip-address* | **-m** { **hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96** } | **-o numberofpasswordprompts** *n* | **-p** *port-num*] { **ip-addr** | **hostname**} [**command** | **-vrf**] 例： `Device# ssh -l userid1 2001:db8:2222:1044::72`	リモート ネットワーク デバイスとの暗号化されたセッションを開始します。

IPv6 を介した SSH サポートの設定例

例：IPv6 デバイスでの SSH のイネーブル化

```
Device# configure terminal
Device(config)# ip ssh
Device(config)# exit
Device# ssh -l userid1 2001:db8:2222:1044::72
```

IPv6 を介した SSH サポートに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
SSH バージョン 1 および バージョン 2 サポート	『セキュリティ コンフィギュレーション ガイド』の「セキュアシェルおよびセキュアシェルバージョン 2 サポートの設定」

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 を介した SSH サポートの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	IPv6 を介した SSH サポート	SSH により IPv6 アドレスがサポートされるため、Cisco ルータは IPv6 トランスポートを介してリモート IPv6 ノードとのセキュアな暗号化された接続を受け入れたり、確立したりできます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。