



## セキュア シェル (SSH) の設定

- [セキュア シェルを設定するための前提条件 \(1 ページ\)](#)
- [セキュア シェルの設定に関する制約事項 \(2 ページ\)](#)
- [セキュア シェルの設定について \(2 ページ\)](#)
- [セキュア シェルの設定方法 \(5 ページ\)](#)
- [SSH の設定およびステータスのモニタリング \(9 ページ\)](#)
- [セキュア シェルの機能情報 \(9 ページ\)](#)

### セキュア シェルを設定するための前提条件

セキュア シェル (SSH) 用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman (RSA) の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル (SCP) も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंगを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、およびアカウントिंग (AAA) の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System (IFS) のファイルをスイッチに (またはスイッチから) 自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

- セキュア シェル (SSH) サーバは、IPsec (データ暗号規格 (DES) または 3DES) の暗号化ソフトウェアイメージを必要とします。SSH クライアントは、IPsec (DES または 3DES) の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

## セキュア シェルの設定に関する制約事項

セキュアシェル用に デバイス を設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman (RSA) 認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格 (DES) (56 ビット) および 3DES (168 ビット) データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- デバイスは、128 ビットキー、192 ビットキー、または 256 ビットキーの Advanced Encryption Standard (AES) 暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェルバージョン 1 ではサポートされません。セキュア シェルバージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-I キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

## セキュア シェルの設定について

セキュアシェル (SSH) は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2 (SSHv2) をサポートします。

## SSH およびスイッチ アクセス

セキュアシェル (SSH) は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2 (SSHv2) をサポートします。

IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

## SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュアシェル (SSH) 統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSH サーバおよび SSH 統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSH クライアントは、市販の一般的な SSH サーバと連動します。SSH クライアントは、Data Encryption Standard (DES)、3DES、およびパスワード認証の暗号をサポートします。



(注) SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対する Telnet セッションの認証と同様に実行されます。SSH は、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

## SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます (逆の場合も同様です)。
- SSH サーバがアクティブスイッチ上で動作しており、アクティブスイッチに障害が発生した場合、新しいアクティブスイッチは、以前のアクティブスイッチによって生成された RSA キーペアを使用します。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラーメッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。

- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

## Secure Copy Protocol の概要

Secure Copy Protocol (SCP) 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル (SSH) が必要です (Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです)。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 許可が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंगを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。



---

(注) SCP を使用する場合、`copy` コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

---

## Secure Copy Protocol

セキュア コピー プロトコル (SCP) 機能は、device の設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol (RCP) と類似しています。また、SCP では認証、許可、およびアカウントिंग (AAA) の設定が必要なため、device はユーザーが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

# セキュアシェルの設定方法

## SSH を実行するためのデバイスのセットアップ

SSH を実行するようにデバイスをセットアップするには、次の手順を実行してください。

### 始める前に

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を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **hostname *hostname***
4. **ip domain-name *domain\_name***
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <b>configure terminal</b>	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	<b>hostname <i>hostname</i></b> 例： デバイス(config)# <b>hostname your_hostname</b>	デバイスのホスト名および IP ドメイン名を設定します。 (注) この手順を実行するのは、デバイスを SSH サーバーとして設定する場合だけです。

	コマンドまたはアクション	目的
ステップ 4	<b>ip domain-name domain_name</b> 例 : デバイス (config) # <b>ip domain-name your_domain</b>	デバイスのホスト ドメインを設定します。
ステップ 5	<b>crypto key generate rsa</b> 例 : デバイス (config) # <b>crypto key generate rsa</b>	<p>デバイス上でローカルおよびリモート認証用に SSH サーバーを有効にし、RSA キーペアを生成します。デバイスの RSA キーペアを生成すると、SSH が自動的に有効になります。</p> <p>最小モジュラス サイズは、1024 ビットにすることを推奨します。</p> <p>RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。</p> <p>(注) この手順を実行するのは、デバイスを SSH サーバーとして設定する場合だけです。</p>
ステップ 6	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例 : デバイス # <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## SSH サーバの設定

SSH サーバーを設定するには、次の手順を実行します。



(注) デバイスを SSH サーバーとして設定する場合にのみ、この手順が必要です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh version [2]**
4. **ip ssh {time-out *seconds* | authentication-retries *number*}**
5. 次のいずれかまたは両方を使用します。
  - `line vty line_number[ending_line_number]`
  - **transport input ssh**
6. **end**
7. 次のいずれかを使用します。
  - **show ip ssh**
  - **show ssh**
8. **show running-config**
9. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合) 。
ステップ 2	<b>configure terminal</b> 例 :  デバイス# <b>configure terminal</b>	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	<b>ip ssh version [2]</b> 例 :  デバイス (config)# <b>ip ssh version 2</b>	(任意) SSH バージョン 2 を実行するように デバイスを設定します。  このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバーは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。

	コマンドまたはアクション	目的
ステップ 4	<p><b>ip ssh {time-out seconds   authentication-retries number}</b></p> <p>例 :</p> <pre>デバイス(config)# ip ssh time-out 90 OR デバイス(config)# ip ssh authentication-retries 2</pre>	<p>SSH 制御パラメータを設定します。</p> <ul style="list-style-type: none"> <li>• <b>time-out seconds</b> : タイムアウト値は秒単位で指定します (デフォルト値は 120 秒)。指定できる範囲は 0 ~ 120 秒です。このパラメータは、SSH ネゴシエーションフェーズに適用されます。接続が確立されると、デバイスは CLI ベースセッションのデフォルトのタイムアウト値を使用します。</li> <li>• <b>authentication-retries number</b> : クライアントをサーバーへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ~ 5 です。</li> </ul> <p>両方のパラメータを設定する場合はこの手順を繰り返します。</p>
ステップ 5	<p>次のいずれかまたは両方を使用します。</p> <ul style="list-style-type: none"> <li>• <b>line vty line_number[ending_line_number]</b></li> <li>• <b>transport input ssh</b></li> </ul> <p>例 :</p> <pre>デバイス(config)# line vty 1 10</pre> <p>または</p> <pre>デバイス(config-line)# transport input ssh</pre>	<p>(任意) 仮想端末回線設定を設定します。</p> <ul style="list-style-type: none"> <li>• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。 <i>line_number</i> 引数と <i>ending_line_number</i> 引数の有効な範囲は 0 ~ 15 です。</li> <li>• デバイス で SSH 以外の Telnet 接続を防ぎ、デバイスを SSH 接続のみに限定するように指定します。</li> </ul>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config-line)# end</pre>	<p>回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。</p>
ステップ 7	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>show ip ssh</b></li> <li>• <b>show ssh</b></li> </ul>	<ul style="list-style-type: none"> <li>• SSH サーバーのバージョンおよび設定情報を表示します。</li> </ul>



	コマンドまたはアクション	目的
	例 : デバイス# <code>show ip ssh</code>  または デバイス# <code>show ssh</code>	<ul style="list-style-type: none"> <li>• デバイス上の SSH サーバーの接続ステータスを表示します。</li> </ul>
ステップ 8	<b>show running-config</b>  例 :  デバイス# <code>show running-config</code>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b>  例 :  デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 1: SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
<code>show ip ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。
<code>show ssh</code>	SSH サーバのステータスを表示します。

## セキュアシェルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 2:セキュア シェルの機能情報

機能名	リリース	機能情報
セキュア シェル	Cisco IOS XE Everest 16.5.1a	SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェアリリースは SSHv2 をサポートしています。

## 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。