



セキュア シェルの設定

- [セキュア シェルの設定について \(1 ページ\)](#)
- [セキュア シェルを設定するための前提条件 \(4 ページ\)](#)
- [セキュア シェルの設定に関する制約事項 \(4 ページ\)](#)
- [SSH 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 \(8 ページ\)](#)

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 1 (SSHv1) および SSH バージョン 2 (SSHv2) をサポートしています。

SSH およびデバイスアクセス

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 1 (SSHv1) および SSH バージョン 2 (SSHv2) をサポートしています。

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。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートします。



(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せん（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。

SFTP のサポート

SFTPクライアントのサポートは、Cisco IOS XE Gibraltar 16.10.1 リリース以降で導入されています。SFTPクライアントはデフォルトで有効になっており、個別の設定は必要ありません。

SFTP プロシージャは、`scp` および `tftp` コマンドの場合と同様に、`copy` コマンドを使用して呼び出すことができます。`sftp` コマンドを使用した一般的なファイルダウンロード手順は、次のように実行できます。

```
copy sftp://user :password @server-ip/file-name flash0:// file-name
```

`copy` コマンドの詳細については、次の URL を参照してください。

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

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、およびアカウンティング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、およびアカウンティング (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。

- `device` 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、`-l` キーワード、`userid` :{number} {ip-address} デリミタ、および引数が必須です。
- FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。その場合は、`crypto key generate rsa general-keys exportable label label-name` コマンドを使用します。

SSH の設定方法

SSH を実行するためのデバイスの設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# 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 2	hostname hostname 例： Device(config)# hostname your_hostname	device 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、device を SSH サーバとして設定する場合だけです。
ステップ 3	ip domain name domain_name 例： Device(config)# ip domain name	device のホストドメインを設定します。

	コマンドまたはアクション	目的
	<code>your_domain</code>	
ステップ 4	crypto key generate rsa 例 : Device(config)# crypto key generate rsa	<p>device 上でローカルおよびリモート認証用に SSHサーバをイネーブルにし、RSA キー ペアを生成します。device の RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。</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、device を SSH サーバとして設定する場合だけです。</p>
ステップ 5	end 例 : Device(config)# end	設定モードを終了します。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。



(注) デバイスを SSH サーバとして設定する場合にのみ、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	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 2	ip ssh version [2] 例 : Device(config)# ip ssh version 2	(任意) SSH バージョン 2 を実行するように device を設定します。

	コマンドまたはアクション	目的
ステップ 3	<p>ip ssh {timeout <i>seconds</i> authentication-retries <i>number</i>}</p> <p>例 :</p> <pre>Device(config)# ip ssh timeout 90 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"> 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。 <p>デフォルトでは、ネットワーク上の複数の CLI ベースセッション (セッション 0 ~ 4) に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベースセッションのタイムアウト値はデフォルトの 10 分に戻ります。</p> <ul style="list-style-type: none"> クライアントをサーバ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。 <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 4	<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"> line vty <i>line_number</i> [<i>ending_line_number</i>] transport input ssh <p>例 :</p> <pre>Device(config)# line vty 1 10</pre> <p>または</p> <pre>Device(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"> 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> および <i>ending_line_number</i> には、回線のペアを指定します。指定できる範囲は 0 ~ 15 です。 非 SSH Telnet によるデバイスへの接続を許可しない設定です。これにより、ルータは SSH 接続に限定されます。

	コマンドまたはアクション	目的
		<p>(注) 仮想端末 (VTY) 回線が使い果たされると、Telnet または SSH は失敗します。Telnet または SSH セッションを切断して VTY 回線を解放するか、以下の回復手順に従って VTY 回線をクリアして Telnet または SSH をリロードします。</p> <pre>Device# configure terminal Device(config)# clear line line number</pre>
ステップ 5	<p>end</p> <p>例 :</p> <pre>Device(config-line)# end</pre>	特権 EXEC モードに戻ります。

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

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。