



セキュア シェル

ここでは、次の内容について説明します。

- [セキュア シェルの概要 \(1 ページ\)](#)
- [セキュア シェルの設定方法 \(3 ページ\)](#)
- [セキュア コピーに関する情報 \(10 ページ\)](#)
- [その他の参考資料 \(12 ページ\)](#)

セキュア シェルの概要

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。

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) 用にデバイス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RSAの公開キーと秘密キーのペアが必要です。
- 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。グローバルコンフィギュレーション モードで `hostname` コマンドと `ip domain-name` コマンドを使用します。

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ルータを設定するための制約事項は、次のとおりです。

- ルータはRSA認証をサポートしています。

- 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。



(注) 3DES 暗号化はより強力であるため、シスコでは強く推奨しています。詳細については、<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>の Cisco IOS-XE デバイス強化ガイドを参照してください。

- このソフトウェア リリースは、IP Security (IPSec) をサポートしています。
- ルータは、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。
- 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。シスコが優れたセキュリティのため推奨しているセキュア シェル バージョン 2 で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。

SSH とルータ 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。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

デバイスを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）。
- **crypto key generate rsa global** 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 hostname 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IP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。

セキュア シェルの設定方法

この項の内容は、次のとおりです。

SSH を実行するためのルータのセットアップ

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	enable 例 : <pre>router> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例 : <pre>router# configure terminal</pre>	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	hostname <i>hostname</i> 例 : <pre>router(config)# hostname your_hostname</pre>	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 4	ip domain-name <i>domain_name</i> 例 : <pre>router(config)# ip domain-name your_domain_name</pre>	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
ステップ 5	crypto key generate rsa 例 : <pre>router(config)# crypto key generate rsa</pre>	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。 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。 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。 (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 6	end 例 : <pre>router(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : <pre>router# show running-config</pre>	入力を確認します。
ステップ 8	copy running-config startup-config 例 : <pre>router# copy running-config startup-config</pre>	(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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh version [2]**
4. **ip ssh {timeout 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. `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	enable 例 : <pre>router> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例 : <pre>router# configure terminal</pre>	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 version [2] 例 : <pre>router(config)# ip ssh version 2</pre>	(任意) SSH バージョン 2 を実行するように device 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。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 4	ip ssh {timeout seconds authentication-retries number} 例 : <pre>router(config)# ip ssh timeout 90 ip ssh authentication-retries 2</pre>	SSH 制御パラメータを設定します。 <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。 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。

	コマンドまたはアクション	目的
		<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 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"> line vty line_number [<i>ending line number</i>] transport input ssh <p>例 :</p> <pre>router(config)# line vty 1 10</pre> <p>または</p> <pre>router(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> 引数と <i>ending_line_number</i> 引数の有効な範囲は0～15です。 device 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。
ステップ 6	<p>end</p> <p>例 :</p> <pre>router(config-line)# end</pre>	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。
ステップ 7	<p>show running-config</p> <p>例 :</p> <pre>router# show running-config</pre>	入力を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例 :</p> <pre>router# copy running-config startup-config</pre>	(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

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。

ルータのローカル認証および許可の設定

ローカルモードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。ルータは、認証と許可を処理します。この設定ではアカウントینگ機能は使用できません。

ローカルモードで AAA を実装するようにルータを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。



(注) AAA 方式を使用して HTTP アクセスに対しルータのセキュリティを確保するには、`ip http authentication aaa` グローバル コンフィギュレーション コマンドで設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しルータのセキュリティは確保しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec local**
6. **aaa authorization network local**
7. **username name privilege level password encryption-type password**
8. **end**
9. **show running-config**
10. **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	enable 例： <code>router> enable</code>	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	configure terminal 例： <code>router# configure terminal</code>	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	aaa new-model 例： <code>router(config)# aaa new-model</code>	AAA の有効化

	コマンドまたはアクション	目的
ステップ 4	aaa authentication login default local 例 : <pre>router(config)# aaa authentication login default local</pre>	ローカル ユーザ名データベースを使用するログイン認証を設定します。default キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 5	aaa authorization exec local 例 : <pre>router(config-line)# aaa authorization exec local</pre>	ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	aaa authorization network local 例 : <pre>router(config-line)# aaa authorization network local</pre>	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	username name privilege level password encryption-type password 例 : <pre>router(config-line)# username your_user_name privilege 1 password 7 secret567</pre>	<p>ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。</p> <p>ユーザごとにコマンドを繰り返し入力します。</p> <ol style="list-style-type: none"> name には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 (任意) level には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 encryption-type には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 password には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 8	end 例 :	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。

	コマンドまたはアクション	目的
	<code>router(config-line)# end</code>	
ステップ 9	show running-config 例： <code>router# show running-config</code>	入力を確認します。
ステップ 10	copy running-config startup-config 例： <code>router# 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。

セキュア コピーに関する情報

セキュア コピー (SCP) 機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、セキュア シェル (SSH)、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

セキュア コピーの前提条件

セキュア シェル (SSH) 用にデバイスを設定するための前提条件は、次のとおりです。

- SCP を有効にする前に、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 に依存して安全な伝送を行っているため、ルータには RSA キー 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 コピーの設定に関する制約事項

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。

- 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。

セキュアコピーの設定

シスコのルータにセキュアコピー（SCP）サーバー側機能を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2...]**
5. **username name [privilege level] password encryption-type encrypted-password**
6. **ip scp server enable**
7. **exit**
8. **show running-config**
9. **debug ip scp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： router> enable	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	configure terminal 例： router# 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	aaa new-model 例： router(config)# aaa new-model	ログイン時の AAA 認証を設定します。
ステップ 4	aaa authentication login {default list-name} method1 [method2...] 例： router(config)# aaa authentication login default group tacacs+	AAA アクセス コントロール システムをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	username name [privilege level] password encryption-type encrypted-password 例 : <pre>router(config)# username superuser privilege 2 password 0 superpassword</pre>	ユーザ名をベースとした認証システムを構築します。 (注) TACACS+ や RADIUS などのネットワークベースの認証メカニズムが設定されている場合は、この手順を省略できます。
ステップ 6	ip scp server enable 例 : <pre>router(config)# ip scp server enable</pre>	SCP サーバ側機能を有効にします。
ステップ 7	exit 例 : <pre>router(config)# exit</pre>	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。
ステップ 8	show running-config 例 : <pre>router# show running-config</pre>	(任意) SCP サーバ側機能を表示します。
ステップ 9	debug ip scp 例 : <pre>router# debug ip scp</pre>	(任意) SCP 認証問題を解決します。

例

```
router# copy scp <somefile> your_username@remotehost:/<some/remote/directory>
```

その他の参考資料

ここでは、SSH 機能に関する関連資料について説明します。

関連項目	マニュアルタイトル
セッション アウェアなネットワークングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE』 : https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf

関連項目	マニュアル タイトル
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『 Secure Shell Configuration Guide, Cisco IOS XE Gibraltar 16.11.x』 : https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_secure_shell__ssh_.html

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。