



SSH および Telnet の設定

この章では、Cisco NX-OS デバイス上で Secure Shell (SSH; セキュア シェル) プロトコルおよび Telnet を設定する手順について説明します。

- [SSH および Telnet の設定, 1 ページ](#)

SSH および Telnet の設定

SSH および Telnet の概要

SSH サーバ

Secure Shell (SSH) サーバ機能を使用すると、SSH クライアントが Cisco Nexus 3000 シリーズ スイッチに対して、セキュアで暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco Nexus 3000 シリーズ スイッチの SSH サーバは、無償あるいは商用の SSH クライアントと連携して動作します。

SSH がサポートするユーザ認証メカニズムには、RADIUS、TACACS+、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアント機能は、SSH プロトコルを介して実行されるアプリケーションで、認証と暗号化を行います。SSH クライアントを使用すると、Cisco Nexus 3000 シリーズ スイッチは、別の Cisco Nexus 3000 シリーズ スイッチまたは SSH サーバを稼働している他の任意のデバイスと、セキュアな暗号化された接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco Nexus 3000 シリーズ スイッチの SSH クライアントは、無償あるいは商用の SSH サーバと連携して動作します。

SSH サーバキー

SSH では、Cisco Nexus 3000 シリーズ スイッチとのセキュアな通信を行うためにサーバ キーが必要です。SSH キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman (RSA) 公開キー暗号化を使用した SSH バージョン 2
- Digital System Algorithm (DSA) を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバキー ペアを取得してください。使用中の SSH クライアントバージョンに応じて、SSH サーバキー ペアを生成します。SSH サービスでは、SSH バージョン 2 に対応する 2 とおりのキー ペアを使用できます。

- dsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- rsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Cisco Nexus 3000 シリーズ スイッチは 1024 ビットの RSA キーを生成します。SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)



注意 SSH キーをすべて削除すると、SSH サービスを開始できません。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別サイトのログインサーバとの TCP 接続を確立して、システム間でキーストロークをやり取りできます。Telnet は、リモートシステムのアドレスとして、IP アドレスまたはドメイン名を受け取ります。

Cisco Nexus 3000 シリーズ スイッチでは、デフォルトで Telnet サーバがイネーブルになっています。

SSH の注意事項および制約事項

SSH には、次の注意事項および制約事項があります。

- Cisco Nexus 3000 シリーズ スイッチは、SSH バージョン 2 (SSHv2) だけをサポートしています。

SSH の設定

SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ssh key {dsa [force] | rsa [bits [force]]}**
3. switch(config)# **exit**
4. (任意) switch# **show ssh key**
5. (任意) switch# **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	switch# configure terminal	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	switch(config)# ssh key {dsa [force] rsa [bits [force]]}	SSH サーバ キーを生成します。 <i>bits</i> 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ~ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード force を使用します。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show ssh key	(任意) SSH サーバ キーを表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、SSH サーバ キーを生成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 2048
switch(config)# exit
switch# show ssh key
switch# copy running-config startup-config
```

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- Open SSH 形式
- Internet Engineering Task Force (IETF) SECSH 形式
- Privacy Enhanced Mail (PEM) 形式の公開キー証明書

Open SSH 形式による SSH 公開キーの指定

ユーザ アカウント用に SSH 形式で SSH 公開キーを指定できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **username username sshkey ssh-key**
3. switch(config)# **exit**
4. (任意) switch# **show user-account**
5. (任意) switch# **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	switch# configure terminal	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	switch(config)# username username sshkey ssh-key	SSH 形式で SSH 公開キーを設定します。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show user-account	(任意) ユーザ アカウントの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、Open SSH 形式で SSH 公開キーを指定する例を示します。

```
switch# configure terminal
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CFTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnXlbvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```



(注) 上記の例の username コマンドは、読みやすくするために改行されていますが、単一行です。

IETF SECSH 形式による SSH 公開キーの指定

ユーザアカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

手順の概要

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. switch(config)# **username username sshkey file filename**
4. switch(config)# **exit**
5. (任意) switch# **show user-account**
6. (任意) switch# **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	switch# copy server-file bootflash: filename	サーバから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。File Transfer Protocol (FTP)、SCP、SSH File Transfer Protocol (SFTP)、または Trivial File Transfer Protocol (TFTP) サーバを利用できます。
ステップ 2	switch# configure terminal	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	switch(config)# username username sshkey file filename	SSH 形式で SSH 公開キーを設定します。
ステップ 4	switch(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ます。
ステップ 5	switch# show user-account	(任意) ユーザアカウントの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、IETF SECSH 形式で SSH 公開キーを指定する例を示します。

```
switch#copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

PEM フォーマット化された公開キー証明書形式による SSH 公開キーの指定

ユーザアカウント用に PEM フォーマット化された公開キー証明書形式で SSH 公開キーを指定できます。

手順の概要

1. switch# **copy server-file bootflash: filename**
2. switch# **configure terminal**
3. (任意) switch# **show user-account**
4. (任意) switch# **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	switch# copy server-file bootflash: filename	サーバから PEM フォーマット化された公開キー証明書形式の SSH キーを含むファイルをダウンロードします。FTP、SCP、SFTP、または TFTP サーバを利用できます。
ステップ 2	switch# configure terminal	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	switch# show user-account	(任意) ユーザアカウントの設定を表示します。
ステップ 4	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、PEMフォーマット化された公開キー証明書形式でSSH公開キーを指定する例を示します。

```
switch# copy tftp://10.10.1.1/cert.pem bootflash:cert.pem
switch# configure terminal
switch# show user-account
switch# copy running-config startup-config
```

リモート デバイスとの SSH セッションの開始

Cisco Nexus 3000 シリーズ スイッチから SSH セッションを開始して、リモート デバイスと接続できます。

手順の概要

1. switch# **ssh** {hostname | username@hostname} [vrf vrf-name]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# ssh {hostname username@hostname} [vrf vrf-name]	リモート デバイスとの SSH セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、またはホスト名を指定します。

SSH ホストのクリア

SCP または SFTP を使用してサーバからファイルをダウンロードする場合は、サーバと信頼性のある SSH 関係を確立します。

手順の概要

1. switch# **clear ssh hosts**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# clear ssh hosts	SSH ホストセッションをクリアします。

SSH サーバのディセーブル化

Cisco Nexus 3000 シリーズ スイッチでは、デフォルトで SSH サーバがイネーブルになっています。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **exit**
4. (任意) switch# **show ssh server**
5. (任意) switch# **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	switch# configure terminal	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	switch(config)# no feature ssh	SSH サーバをディセーブルにします。 デフォルトはイネーブルです。
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show ssh server	(任意) SSH サーバの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、SSH サーバ キーを削除できます。



(注) SSH を再度イネーブルにするには、まず、SSH サーバ キーを生成する必要があります。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **no ssh key [dsa | rsa]**
4. switch(config)# **exit**
5. (任意) switch# **show ssh key**
6. (任意) switch# **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	switch# configure terminal	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	switch(config)# no feature ssh	SSH サーバをディセーブルにします。
ステップ 3	switch(config)# no ssh key [dsa rsa]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	switch(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ます。
ステップ 5	switch# show ssh key	(任意) SSH サーバの設定を表示します。
ステップ 6	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH セッションのクリア

SSH セッションを Cisco Nexus 3000 シリーズ スイッチからクリアできます。

手順の概要

1. switch# **show users**
2. switch# **clear line vty-line**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show users	ユーザ セッション情報を表示します。
ステップ 2	switch# clear line vty-line	ユーザ SSH セッションをクリアします。

SSH の設定例

次に、SSH を設定する例を示します。

手順の概要

1. SSH サーバ キーを生成します。
2. SSH サーバをイネーブルにします。
3. SSH サーバ キーを表示します。
4. Open SSH 形式による SSH 公開キーを指定します。
5. 設定を保存します。

手順の詳細

ステップ 1 SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

ステップ 2 SSH サーバをイネーブルにします。

```
switch# configure terminal
switch(config)# feature ssh
```

(注) SSH サーバはデフォルトでイネーブルなので、この手順は必要ありません。

ステップ 3 SSH サーバ キーを表示します。

```
switch(config)# show ssh key
rsa Keys generated:Fri May  8 22:09:47 2009

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYzCfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZ/
cTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4ZXIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5/
Ninn0Mc=

bitcount:1024

fingerprint:
4b:4d:f6:b9:42:e9:d9:71:3c:bd:09:94:4a:93:ac:ca
*****
could not retrieve dsa key information
*****
```

ステップ 4 Open SSH 形式による SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAri3mQy4W1AV9Y2t2hrEWgbUEYz
CfTPO5B8LRkedn56BEy2N9ZcdpqE6aqJLZwfZcTFEzaAAZp9AS86dgBAjsKGS7UxnhGySr8ZELv+DQBsDQH6rZt0KR+2Da8hJD4Z
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
```

ステップ 5 設定を保存します。

```
switch(config)# copy running-config startup-config
```

Telnet の設定

Telnet サーバのディセーブル化

デフォルトでは、Telnet サーバはイネーブルに設定されています。Cisco Nexus 3000 シリーズ スイッチで Telnet サーバをディセーブルにできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature telnet**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config)# feature telnet	Telnet サーバをディセーブルにします。デフォルトはイネーブルです。

Telnet サーバの再イネーブル化

Cisco Nexus 3000 シリーズ スイッチの Telnet サーバがディセーブルにされた場合は、再度イネーブルにできます。

手順の概要

1. switch(config)# **feature telnet**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch(config)# feature telnet	Telnet サーバを再度イネーブルにします。

リモート デバイスとの Telnet セッションの開始

Telnet セッションを開始してリモート デバイスに接続する前に、次の作業を行う必要があります。

- リモート デバイスのホスト名を取得し、必要なら、リモート デバイスのユーザ名も取得します。
- Cisco Nexus 3000 シリーズ スイッチ上で Telnet サーバをイネーブルにします。
- リモート デバイス上で Telnet サーバをイネーブルにします。

手順の概要

1. switch# telnet hostname

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# telnet hostname	リモート デバイスとの Telnet セッションを作成します。引数 <i>hostname</i> には、IPv4 アドレス、IPv6 アドレス、またはデバイス名を指定します。

次に、Telnet セッションを開始してリモート デバイスに接続する例を示します。

```
switch# telnet 10.10.1.1
Trying 10.10.1.1...
Connected to 10.10.1.1.
Escape character is '^]'.
switch login:
```

Telnet セッションのクリア

Cisco Nexus 3000 シリーズ スイッチから Telnet セッションをクリアできます。

手順の概要

1. switch# show users
2. switch# clear line vty-line

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# show users	ユーザセッション情報を表示します。
ステップ 2	switch# clear line vty-line	ユーザ Telnet セッションをクリアします。

SSH および Telnet の設定の確認

SSH の設定情報を表示するには、次のいずれかの作業を行います。

- `switch# show ssh key [dsa | rsa]`
SSH サーバ キー ペアの情報を表示します。
- `switch# show running-config security [all]`
実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。キーワード `all` を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
- `switch# show ssh server`
SSH サーバの設定を表示します。
- `switch# show user-account`
ユーザ アカウント情報を表示します。

SSH のデフォルト設定

次の表に、SSH パラメータのデフォルト設定を示します。

表 1: デフォルトの SSH パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024
Telnet サーバ	イネーブル

