CHAPTER 5

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。

ここでは、次の内容を説明します。

SSH および Telnet の概要

ここでは、次の内容について説明します。

SSH サーバ

SSH サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は認証に強化暗号化を使用します。Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

SSH でサポートされるユーザ認証メカニズムには、RADIUS、TACACS+、およびローカルに保存されたユーザ名とパスワードがあります。

SSH クライアント

SSH クライアントは、SSH プロトコル上で稼働し装置認証および暗号化を提供するアプリケーションです。Cisco NX-OS デバイスは、SSH クライアントを使用して、別の Cisco NX-OS デバイスまたは SSH サーバの稼働する他の装置とセキュアで暗号化された接続を確立できます。この接続を通して、暗号化されたアウトバウンド接続が提供されます。SSH クライアントは、認証および暗号化により、非セキュアなネットワーク上でセキュアな通信ができます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

SSH サーバ鍵

SSH は、Cisco NX-OS デバイスとセキュアな通信を行うためにサーバ鍵が必要です。SSH サーバ鍵は、次の SSH オプションに使用できます。

- SSH バージョン 2（Rivest、Shamir、および Adelman [RSA] 公開鍵暗号法を使用）
- SSH バージョン 2（Digital System Algrorithm [DSA] を使用）

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 サーバ鍵ペアを取得しておいてください。使用する SSH クライアントに応じた SSH サーバ鍵ペアを生成できます。SSH サービスは、SSH バージョン 2 で使用する次の 2 種類の鍵ペアを受け入れます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA 鍵ペアを生成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA 鍵ペアを生成します。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA 鍵を生成します。

SSH は、次の公開鍵形式をサポートします。

- OpenSSH
- IETF SSH（SECSH）
- Privacy-Enhanced Mail（PEM）の公開鍵証明書

注意　SSH 鍵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 接続を可能にします。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークを装置間でやり取りできます。Telnet は、リモート装置アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

デフォルトでは、Telnet サーバは NX-OS デバイス上でディセーブルになっています。

バーチャライゼーション サポート

SSH および Telnet の設定と操作は、Virtual Device Context（VDC）に対してローカルです。VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

SSH および Telnet のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	SSH および Telnet にライセンスは必要ありません。ライセンス パッケージに含まれない機能はすべて、Cisco NX-OS システム イメージにバンドルされており、無償で提供されます。NX-OS のライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide, Release 4.0*』を参照してください。

SSH の前提条件

SSH および Telnet には、次の前提条件があります。

- レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトバンド、またはイーサネット インターフェイス上にインバンドを設定していること。

注意事項および制限事項

SSH および Telnet には、次の設定に関する注意事項と制限事項があります。

- Cisco NX-OS ソフトウェアは、SSH バージョン 2（SSHv2）のみをサポートしています。

（注）　Cisco IOS CLI の知識があるユーザは、この機能に関する Cisco NX-OS のコマンドが Cisco IOS のコマンドで使用されるものと異なる場合があることに注意してください。

SSH の設定

ここでは、次の内容について説明します。

SSH サーバ鍵の生成

セキュリティ要件に応じた SSH サーバ鍵を生成できます。デフォルトの SSH サーバ鍵は、1024 ビットで生成される RSA 鍵です。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **no ssh server enable**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* **[force**]]}
4. **ssh server enable**
5. **exit**
6. **show ssh key**
7. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**no ssh server enable** **例：** `switch(config)# no ssh server enable`	SSH をディセーブルにします。
ステップ 3	**ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]} **例：** `switch(config)# ssh key rsa 2048`	SSH サーバ鍵を生成します。 *bits* 引数は、鍵の生成に使用されるビット数です。指定できる範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存の鍵を交換する場合は、**force** キーワードを使用します。

	コマンド	目的
ステップ 4	**ssh server enable** **例：** `switch(config)# ssh server enable`	SSH をイネーブルにします。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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 6	**show ssh key** **例：** `switch# show ssh key`	（任意）SSH サーバ鍵を表示します。
ステップ 7	**copy running-config startup-config** **例：** `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。

ユーザ アカウントの SSH 公開鍵の指定

SSH 公開鍵を設定して SSH クライアントでのログインに使用すると、パスワードを求められずにログインできます。次の 3 種類の形式のいずれかを SSH 公開鍵に指定できます。

- OpenSSH 形式
- IETF SECSH 形式
- PEM 形式の公開鍵証明書

OpenSSH 形式の SSH 公開鍵の指定

ユーザ アカウントに OpenSSH 形式の SSH 公開鍵を指定できます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

OpenSSH 形式の SSH 公開鍵を生成します。

手順の概要

1. **config t**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. **show user-account**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例**： switch# config t switch(config)#	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	**username** *username* **sshkey** *ssh-key* **例**： switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1X swK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/ DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG 30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH 3UD/vKyziEh5S4Tplx8=	OpenSSH 形式の SSH 公開鍵を設定します。
ステップ 3	**exit** **例**： switch(config)# exit switch#	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	**show user-account** **例**： 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	**copy running-config startup-config** **例**： 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。

IETF SECSH 形式の SSH 公開鍵の指定

ユーザ アカウントに IETF SECSH 形式の SSH 公開鍵を指定できます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

IETF SCHSH 形式の SSH 公開鍵を生成しておきます。

手順の概要

1. **copy** *server-file* **bootflash:***filename*
2. **config t**
3. **username** *username* **sshkey file bootflash:***filename*
4. **exit**
5. **show user-account**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**copy** *server-file* **bootflash:***filename* **例**： `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	サーバから IETF SECSH 形式の SSH 鍵が入ったファイルをダウンロードします。サーバは FTP、secure copy（SCP）、secure FTP（SFTP）または TFTP のいずれかを使用できます。

ステップ 2	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**username** *username* **sshkey file bootflash:***filename* **例**： `switch(config)# username User1 sshkey file bootflash:secsh_file.pub`	IETF SECSH 形式の SSH 公開鍵を設定します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show user-account** **例**： `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 6	**copy running-config startup-config** **例**： `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 セッションの開始

Cisco NX-OS デバイスから IPv4 または IPv6 を使用して SSH セッションを開始し、リモート装置と接続します。

作業を開始する前に

リモート装置のホスト名と、必要な場合はリモート装置のユーザ名を取得します。

リモート装置の SSH サーバをイネーブルにします。

手順の概要

1. **ssh** [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]
   ssh6 [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]

詳細な手順

	コマンド	目的
ステップ 1	**ssh** [*username***@**]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*] **例**： switch# ssh 10.10.1.1	IPv4 を使用してリモート装置との SSH IPv4 セッションを作成します。デフォルトの VRF はデフォルト VRF です。
	ssh6 [*username***@**]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*] **例**： switch# ssh6 HostA	IPv6 を使用してリモート装置との SSH IPv6 セッションを作成します。

SSH ホストのクリア

サーバから SCP または SFTP を使用してファイルをダウンロードする場合、またはこの装置からリモート ホストに SSH セッションを開始する場合には、そのサーバと信頼できる SSH 関係が確立されます。ユーザ アカウントの信頼できる SSH サーバのリストはクリアすることができます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **clear ssh hosts**

詳細な手順

	コマンド	目的
ステップ 1	**clear ssh hosts** **例**： 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

デフォルトでは、SSH サーバは NX-OS デバイス上でイネーブルになっています。SSH サーバをディセーブルにすると、SSH でスイッチにアクセスすることを防止できます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **no ssh server enable**
3. **exit**
4. **show ssh server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**no ssh server enable** **例：** switch(config)# no ssh server enable	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	**exit** **例：** switch(config)# exit switch#	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	**show ssh server** **例：** switch# show ssh server	（任意）SSH サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** 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 サーバ鍵の削除

SSH サーバをディセーブルにしたら、SSH サーバ鍵を削除できます。

（注） SSH を再度イネーブルにする場合は、まず SSH サーバ鍵を生成する必要があります（「SSH サーバ鍵の生成」[p.5-4] を参照）。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **no ssh server enable**
3. **no ssh key [dsa | rsa]**
4. **exit**
5. **show ssh key**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**no ssh server enable** **例：** `switch(config)# no ssh server enable`	SSH サーバをディセーブルにします。
ステップ 3	**no ssh key** [**dsa** | **rsa**] **例：** `switch(config)# no ssh key rsa`	SSH サーバ鍵を削除します。 デフォルトでは、すべての SSH 鍵が削除されます。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show ssh key** **例：** `switch# show ssh key`	（任意）SSH サーバ鍵の設定を表示します。
ステップ 6	**copy running-config startup-config** **例：** `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

Cisco NX-OS デバイスから SSH セッションをクリアできます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**show users** **例：** `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **例：** `switch(config)# clear line pts/12`	ユーザの SSH セッションをクリアします。

Telnet の設定

ここでは、次の内容について説明します。

Telnet サーバのイネーブル化

Telnet サーバを Cisco NX-OS デバイス上でイネーブルにできます。デフォルトでは、Telnet はディセーブルです。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **telnet server enable**
3. **exit**
4. **show telnet server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**telnet server enable** **例：** `switch(config)# telnet server enable`	Telnet サーバをイネーブルにします。デフォルトはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show telnet server** **例：** `switch# show telnet server`	（任意）Telnet サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `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。

リモート装置との Telnet セッションの開始

Cisco NX-OS デバイスから SSH セッションを開始して、リモート装置と接続できます。

作業を開始する前に

リモート装置のホスト名と、必要な場合はリモート装置のユーザ名を取得します。

NX-OS デバイス上で Telnet サーバをイネーブルにします（「Telnet サーバのイネーブル化」[p.5-11]を参照）。

リモート装置の Telnet サーバをイネーブルにします。

手順の概要

1. **telnet** {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

詳細な手順

	コマンド	目的
ステップ 1	**telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf** *vrf-name*] **例：** `switch# telnet 10.10.1.1`	IPv4 を使用してリモート装置との Telnet セッションを作成します。デフォルトのポート番号は 23 です。有効値の範囲は 1 ～ 65535 です。デフォルトの VRF は、デフォルト VRF です。

Telnet セッションのクリア

Telnet セッションを Cisco NX-OS デバイスからクリアできます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

NX-OS 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. **show users**
2. **clear line** *vty-line*

詳細な手順

	コマンド	目的
ステップ 1	**show users** **例：** `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line** *vty-line* **例：** `switch(config)# clear line pts/12`	ユーザの 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 および Telnet の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show ssh key [dsa | rsa]	SSH サーバ鍵ペアの情報を表示します。
show running-config security [**all**]	実行コンフィギュレーション内の SSH およびユーザ アカウントの設定を表示します。**all** キーワードを使用すると、SSH およびユーザ アカウントのデフォルト値を表示します。
show ssh server	SSH サーバの設定を表示します。
show telnet server	Telnet サーバの設定を表示します。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

SSH の設定例

OpenSSH 鍵を使用する SSH を設定するには、次の作業を行います。

ステップ 1　SSH サーバをディセーブルにします。

```
switch# config t
switch(config)# no ssh server enable
```

ステップ 2　SSH サーバ鍵を生成します。

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

ステップ 3　SSH サーバをイネーブルにします。

```
switch(config)# ssh server enable
```

ステップ 4　SSH サーバ鍵を表示します。

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*************************************
could not retrieve dsa key information
*************************************
```

ステップ 5　OpenSSH 形式の SSH 公開鍵を指定します。

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1
nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXH
YshXmSiH3UD/vKyziEh5S4Tplx8=
```

ステップ 6　設定を保存します。

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

デフォルト設定

表 5-1 に、SSH および Telnet パラメータのデフォルト設定を示します。

表 5-1　デフォルトの SSH および Telnet 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 サーバ鍵	1024 ビットで生成された RSA 鍵
RSA 鍵生成ビット数	1024
Telnet サーバ	ディセーブル

その他の参考資料

RBAC の実装に関連する詳細情報については、次を参照してください。

- 関連資料（p.5-15）
- 規格（p.5-15）
- MIB（p.5-15）

関連資料

関連事項	タイトル
ライセンス	『*Cisco NX-OS Licensing Guide, Release 4.0*』
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
VRF の設定	『*Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0*』

規格

規格	タイトル
この機能によりサポートされた新規規格または改訂規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB のリンク
• CISCO-SECURE-SHELL-MIB	MIB の確認とダウンロードを行うには、次の URL にアクセスします。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml