



# CHAPTER 7

## SSH の設定

---

この章では、セキュア シェル (SSH) プロトコルを設定する手順について説明します。

この章は、次の内容で構成されています。

- 「SSH の概要」 (P.7-1)
- 「SSH の前提条件」 (P.7-2)
- 「注意事項および制約事項」 (P.7-2)
- 「デフォルト設定」 (P.7-3)
- 「SSH の設定」 (P.7-3)
- 「SSH の設定の確認」 (P.7-13)
- 「SSH の設定例」 (P.7-14)
- 「その他の関連資料」 (P.7-15)
- 「SSH 機能の履歴」 (P.7-15)

## SSH の概要

ここでは、次の内容について説明します。

- 「SSH サーバ」 (P.7-1)
- 「SSH クライアント」 (P.7-2)
- 「SSH サーバ キー」 (P.7-2)

## SSH サーバ

SSH サーバを使用すると、SSH クライアントはセキュアな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。SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH では、TACACS+ ユーザ認証およびローカルに保存されたユーザ名とパスワードがサポートされます。

## SSH クライアント

SSH クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。SSH クライアントをインストールすると、SSH サーバを実行する任意の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るようになります。この接続を通して、暗号化されたアウトバ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。

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 サーバ キー

SSH では、セキュアな通信を行うためにサーバ キーが必要です。SSH サーバ 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、正しいバージョンの SSH サーバ キー ペアを取得しておいてください。使用する SSH クライアントのバージョンに応じた SSH サーバ キー ペアを生成します。

SSH サービスは、SSH バージョン 2 で使用する次の 2 種類のキー ペアを受け入れます。

- **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、1024 ビットの RSA キーが生成されます。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH (SECSH)
- Privacy-Enhanced Mail (PEM) の公開キー証明書



**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。

---

## SSH の前提条件

SSH 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
- SSH サーバをイネーブルにする前に、SSH キーを取得すること

## 注意事項および制約事項

- SSH バージョン 2 (SSHv2) のみがサポートされます。
- SSH はデフォルトでイネーブルになります。

- Cisco NX-OS のコマンドは Cisco IOS のコマンドと異なる場合があります。

## デフォルト設定

次の表に、SSH のデフォルト設定を示します。

| 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                  |

## 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 キーの生成」(P.7-3)
- 「公開キーを持つユーザアカウントの設定」(P.7-5)
- 「SSH セッションの開始」(P.7-8)
- 「SSH ホストのクリア」(P.7-9)
- 「SSH サーバのディセーブル化」(P.7-9)
- 「SSH サーバ キーの削除」(P.7-10)
- 「SSH セッションのクリア」(P.7-12)

## SSH サーバ キーの生成

セキュリティ要件に応じた SSH サーバ キーを生成するには、次の手順を実行します。

### はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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. `config t`
2. `no feature ssh`
3. `ssh key {dsa [force] | rsa [bits [force]]}`
4. `feature ssh`
5. `exit`
6. `show ssh key`
7. `copy running-config startup-config`

## 手順の詳細

|        | コマンド   | 目的  |
|--------|--|---|
| ステップ 1 | <code>config t</code><br><br>例:<br>n1000v# <code>config t</code><br>n1000v(config)#                                  | CLI 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 | <code>no feature ssh</code><br><br>例:<br>n1000v(config)# <code>no feature ssh</code>                                 | SSH をディセーブルにします。  |
| ステップ 3 | <code>ssh key {dsa [force]   rsa [bits [force]]}</code><br><br>例:<br>n1000v(config)# <code>ssh key dsa force</code>  | SSH サーバ キーを生成します。<br><br><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。<br><br>既存のキーを置き換える場合は、キーワード <b>force</b> を使用します。 |
| ステップ 4 | <code>feature ssh</code><br><br>例:<br>n1000v(config)# <code>feature ssh</code>                                       | SSH をイネーブルにします。   |
| ステップ 5 | <code>show ssh key</code><br><br>例:<br>n1000v# <code>show ssh key</code>   | (任意) SSH サーバ キーを表示します。  |
| ステップ 6 | <code>copy running-config startup-config</code><br><br>例:<br>n1000v# <code>copy running-config startup-config</code> | (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。  |

```

例:
n1000v# config t
n1000v(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# ssh key dsa force
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# feature ssh
n1000v(config)# show ssh key
*****
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki100Id9/tdHhA/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2yws7CpnODjCDXJuDYSPhc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNULJxmQDJkdhMARObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*****
dsa Keys generated:Sun Jul 27 15:20:12 2008

```

```
ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvH1lEh
GnaiHhqarOlcEKqLbIbuqtKTCvfa+YlhBIAhWVjglUR3/M22jqxnfhnXL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAFQDbRabAjZa6GfDpwjXw5smRhrELJwAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNB6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9g1B
0IOM2mgHHyoAAACAFRir27hHy+fw8Cxp1sK0R6cFhxYyd/qYYogXFKYIOpXpLoYrjqODeOFThU7TJuBz
aS97eXiruzbfHwzUGfXgmQT5o9IMZRTC1WPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*****
```

## 公開キーを持つユーザ アカウントの設定

SSH 公開キーを設定して、SSH クライアントでパスワードの入力を求められずにログインするには、次の手順を実行します。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。

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

### OpenSSH キーの設定

ユーザ アカウントに OpenSSH 形式の SSH 公開キーを指定するには、次の手順を実行します。

#### はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- OpenSSH 形式の SSH 公開キーが生成されています。
- ユーザ アカウントがすでに存在しています。

#### 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`

## 手順の詳細

|        | コマンド   | 目的   |
|--------|--|--|
| ステップ 1 | <b>config t</b><br><br>例:<br>n1000v# config t<br>n1000v(config)#   | CLI 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 | <b>username username sshkey ssh-key</b><br><br>例:<br>n1000v(config)# username user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki100Id9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPbc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGyAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmQDJkOdhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==  | 既存のユーザ アカウントで OpenSSH 形式の SSH 公開キーを設定します。<br><br>ユーザ アカウントを作成するには、次のコマンドを使用します。<br><br><b>username name password pwd</b> |
| ステップ 3 | <b>exit</b><br><br>例:<br>n1000v(config)# exit<br>n1000v#   | グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。   |
| ステップ 4 | <b>show user-account</b><br><br>例:<br>n1000v# show user-account<br>user:admin<br>this user account has no expiry date<br>roles:network-admin<br>user:user1<br>this user account has no expiry date<br>roles:network-operator<br>ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki100Id9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPbc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGyAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmQDJkOdhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ== | (任意) ユーザ アカウントの設定を表示します。   |
| ステップ 5 | <b>copy running-config startup-config</b><br><br>例:<br>n1000v# 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 または PEM キーの設定

ユーザアカウントに IETF SECSH または PEM 形式の SSH 公開キーを指定するには、次の手順を実行します。

### はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 次のいずれかの形式の SSH 公開キーが生成されています。
  - Internet Engineering Task Force (IETF) SECSH 形式
  - Privacy Enhanced Mail (PEM) 形式の公開キー証明書

### 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`

### 手順の詳細

|        | コマンド   | 目的   |
|--------|--|--|
| ステップ 1 | <code>copy server-file bootflash:filename</code>   | サーバから SSH キー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。 |
|        | 例:<br>n1000v# copy tftp://10.78.1.10/secsh_file.pub bootflash:secsh_file.pub vrf management<br>Trying to connect to tftp server.....<br>Connection to server Established.<br> <br>TFTP get operation was successful<br>n1000v# |  |
| ステップ 2 | <code>config t</code>  | CLI 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。   |
|        | 例:<br>n1000v# config t<br>n1000v(config)#  |  |
| ステップ 3 | <code>username username sshkey file bootflash:filename</code>  | SSH 公開キーを設定します。  |
|        | 例:<br>n1000v(config)# username User1 sshkey file bootflash:secsh_file.pub  |  |

|        | コマンド   | 目的   |
|--------|--|--|
| ステップ 4 | <b>exit</b><br><br>例:<br>n1000v(config)# exit<br>n1000v#   | グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。       |
| ステップ 5 | <b>show user-account</b><br><br>例:<br>n1000v# <b>show user-account</b><br>user:admin<br>this user account has no expiry date<br>roles:network-admin<br>user:user2<br>this user account has no expiry date<br>roles:network-operator<br>ssh public key: ssh-rsa<br>AAAAB3NzaC1yc2EAAAABIwAAAQEAYKcb7Nv9Ki100Id9/tDHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CC<br>LUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPbc+A6/n3FVroyRwupMki6<br>mWoM6UwaGID5gsVPqFjFNSgMWTbhjo97XVKhgjFW+wOvt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f<br>FzTGYAxMvYZI+BrN47aoH2yws7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJN<br>U1JxmQDJk0dhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ== | (任意) ユーザ アカウントの設定を表示します。                       |
| ステップ 6 | <b>copy running-config startup-config</b><br><br>例:<br>n1000v# 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

IP を使用して SSH セッションを開始し、リモート装置と接続するには、次の手順を実行します。

### はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- リモート装置のホスト名と、必要な場合はユーザ名を取得済みです。
- リモート装置で SSH サーバがイネーブルになっています。

### 手順の概要

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



## 手順の詳細

|        | コマンド   | 目的  |
|--------|--|---|
| ステップ 1 | <pre>ssh [root@]{ip address   hostname} [vrf vrf-name]  例: n1000v(config)# ssh root@172.28.30.77 root@172.28.30.77's password: Last login: Sat Jul 26 11:07:23 2008 from 171.70.209.64</pre> | IP を使用してリモート装置との SSH IP 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。 |

## 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した際、またはリモート ホストへの SSH セッションを開始した際に追加された信頼できる SSH サーバのリストをアカウントからクリアするには、次の手順を実行します。

## 手順の概要

## 1. clear ssh hosts

## 手順の詳細

|        | コマンド   | 目的                   |
|--------|--|----------------------|
| ステップ 1 | <pre>clear ssh hosts  例: n1000v# clear ssh hosts</pre> | 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

SSH サーバをディセーブルにしてスイッチへの SSH アクセスを防止するには、次の手順を実行します。デフォルトでは、SSH サーバはイネーブルになっています。

## はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

「SSH サーバ キーの生成」(P.7-3) の手順を参照してください。

## 手順の概要

1. `config t`
2. `no feature ssh`
3. `show ssh server`
4. `copy running-config startup-config`

## 手順の詳細

|        | コマンド   | 目的   |
|--------|--|--|
| ステップ 1 | <code>config t</code><br><br>例:<br>n1000v# config t<br>n1000v(config)#   | CLI 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 | <code>no feature ssh</code><br><br>例:<br>n1000v(config)# no feature ssh<br>XML interface to system may become unavailable since ssh is disabled<br>n1000v(config)# | 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 | <code>show ssh server</code><br><br>例:<br>n1000v(config)# show ssh server<br>ssh is not enabled<br>n1000v(config)#   | (任意) SSH サーバの設定を表示します。                         |
| ステップ 4 | <code>copy running-config startup-config</code><br><br>例:<br>n1000v(config)# 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あと、SSH サーバ キーを削除するには、次の手順を実行します。

## はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

「SSH サーバ キーの生成」(P.7-3) の手順を参照してください。

## 手順の概要

1. `config t`
2. `no feature ssh`

3. `no ssh key [dsa | rsa]`
4. `show ssh key`
5. `copy running-config startup-config`

手順の詳細

|        | コマンド   | 目的   |
|--------|--|--|
| ステップ 1 | <code>config t</code><br><br>例:<br>n1000v# <code>config t</code><br>n1000v(config)#  | CLI 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 | <code>no feature ssh</code><br><br>例:<br>n1000v(config)# <code>no feature ssh</code>   | SSH サーバをディセーブルにします。                                  |
| ステップ 3 | <code>no ssh key [dsa   rsa]</code><br><br>例:<br>n1000v(config)# <code>no ssh key rsa</code>                                 | SSH サーバ キーを削除します。<br><br>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 | <code>show ssh key</code><br><br>例:<br>n1000v(config)# <code>show ssh key</code>   | (任意) SSH サーバ キーの設定を表示します。                            |
| ステップ 5 | <code>copy running-config startup-config</code><br><br>例:<br>n1000v(config)# <code>copy running-config startup-config</code> | (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。       |

```
例:
n1000v# config t
n1000v(config)# no feature ssh
n1000v(config)# no ssh key rsa
n1000v(config)# show ssh key
*****
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki100Id9/tdHHA/ngQujlvK5mXyL/n+DeOxK
fVhHbX2a+V0cm7CCLUkBh+BvZRpmOVtmU/5awfVhVxMKXMiPOPbc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMwtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmQDJkQodhMARObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*****
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvH1lEh
GnaiHhgarOlcEKqLbIbuqtKTCvfa+YlhBIAhWVjg1UR3/M22jqxnfhnXL5YRc1Q7fcesFax0myayAIU
nXrkO5iww9XHTu+EInRc4kJOXrG9SxtLmDe/fi2ZAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWhtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIoOrGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAFrir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODEOfThU7TJuBz
```

```

aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju409YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*****
mcs-srvr43(config)# no ssh key rsa
mcs-srvr43(config)# show ssh key
*****
could not retrieve rsa key information
*****
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEB0DMUmq9bSq2N+KAcvH1lEh
GnaiHhqrOlceKqhlbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iww9XHTu+EIInRc4kJOXrG9SxtLmDe/fi2ZAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHTMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGg
svdg7T TecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAFrir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjq0DeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju409YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*****
mcs-srvr43(config)# no ssh key dsa
mcs-srvr43(config)# show ssh key
*****
could not retrieve rsa key information
*****
could not retrieve dsa key information
*****
no ssh keys present. you will have to generate them
*****
n1000v#

```

## SSH セッションのクリア

デバイスから SSH セッションをクリアするには、次の手順を実行します。

### はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

### 手順の概要

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

手順の詳細

|        | コマンド   | 目的                    |
|--------|--|-----------------------|
| ステップ 1 | <b>show users</b><br><br>例:<br>n1000v# show users            | ユーザ セッション情報を表示します。    |
| ステップ 2 | <b>clear line vty-line</b><br><br>例:<br>n1000v# clear line 0 | ユーザ SSH セッションをクリアします。 |
| ステップ 3 | <b>show users</b><br><br>例:<br>n1000v# show users            | ユーザ セッション情報を表示します。    |

```

例:
n1000v# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     tty1      Jul 25 19:13  old          2867
admin     pts/0     Jul 28 09:49  00:02        28556 (10.21.148.122)
admin     pts/1     Jul 28 09:46  .            28437 (::ffff:10.21.148.122)*
n1000v# clear line 0
n1000v# show users
NAME      LINE      TIME          IDLE          PID COMMENT
admin     tty1      Jul 25 19:13  old          2867
admin     pts/1     Jul 28 09:46  .            28437 (::ffff:10.21.148.122)*
mcs-srvr43(config)#
    
```

## SSH の設定の確認

SSH の設定情報を表示するには、次のいずれかのコマンドを使用します。

| コマンド                                      | 目的  |
|---|---|
| <b>show ssh key [dsa   rsa]</b>           | SSH サーバ キー ペアの情報を表示します。   |
| <b>show running-config security [all]</b> | 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 <b>all</b> 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。 |
| <b>show ssh server</b>                    | SSH サーバの設定を表示します。   |

```

例:
n1000v# show ssh key rsa
*****
rsa Keys generated:Mon Jul 28 09:49:18 2008

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAGEAv0a4p6VulQMW4AMgoPfApB2KegF3QTojCzed51iVQnEkNglNm7A/oEIZAt1VLY
k/PEzt+ED71Pal/8pomaqjgRxHSeK2gw1cJKSDbcYH5na8uox1Hr50eK0q2+ZfvMqV

bitcount:768
    
```

```
fingerprint:
76:6c:a0:5c:79:a6:ae:3d:cb:27:a1:86:62:fa:09:df
*****
```

## SSH の設定例

OpenSSH キーを使用する 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。

```
n1000v# config t
n1000v(config)# no feature ssh
```

**ステップ 2** SSH サーバ キーを生成します。

```
n1000v(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。

```
n1000v(config)# feature ssh
```

**ステップ 4** SSH サーバ キーを表示します。

```
n1000v(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDmt923siNiv5aSga60K361r39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtX1DhliEmn4HVXOjChFhONE=
```

```
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 公開キーを指定します。

```
n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK30iW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKuilnIf/
DQhum+lJNqJP/eLowb7ubO+lVkrXFY/G+lJNlQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

**ステップ 6** 設定を保存します。

```
n1000v(config)# copy running-config startup-config
```

例:

```
n1000v# config t
n1000v(config)# no feature ssh
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
n1000v(config)# feature ssh
n1000v(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
*****

n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKuiInIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXYF/G+lJNlQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyzIEh5S4Tplx8=
n1000v(config)# copy running-config startup-config
[#####] 100%
n1000v(config)#

```

## その他の関連資料

RBAC の実装に関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.7-15)
- 「標準」 (P.7-15)

## 関連資料

| 関連項目   | 参照先  |
|--------|--|
| CLI    | 『Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)』 |
| Telnet | <a href="#">第8章「Telnet の設定」</a>  |

## 標準

| 標準   | タイトル |
|--|------|
| この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。 | —    |

## SSH 機能の履歴

ここでは、SSH のリリース履歴を示します。

| 機能名 | リリース         | 機能情報          |
|-----|--------------|---------------|
| SSH | 4.0(4)SV1(1) | この機能が導入されました。 |

