CHAPTER 7

SSH の設定

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

ここでは、次の内容について説明します。

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

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 は認証に強化暗号化を使用します。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 プロトコルで稼動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。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。

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 サーバ鍵

SSH では、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。

- Rivest, Shamir, and Adelman（RSA）公開鍵暗号法を使用した SSH バージョン 2
- Digital System Algrorithm（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 クライアントのバージョンに応じた SSH サーバ鍵ペアを生成します。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、1024 ビットの RSA 鍵が生成されます。

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。

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 鍵を取得すること

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 サーバ鍵	1024 ビットで生成された RSA 鍵
RSA 鍵生成ビット数	1024

SSH の設定

ここでは、次の内容について説明します。

SSH サーバ鍵の生成

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

始める前に

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。

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**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** n1000v# config t 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	**no ssh server enable** **例：** n1000v(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：** n1000v(config)# ssh key dsa force	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。有効な範囲は 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。
ステップ 4	**ssh server enable** **例：** n1000v(config)# ssh server enable	SSH をイネーブルにします。
ステップ 5	**exit** **例：** n1000v(config)# exit 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 6	**show ssh key** **例：** n1000v# 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：** 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。

例：

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

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/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+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

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

公開鍵を持つユーザ アカウントの設定

SSH 公開鍵を設定して、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。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 鍵の設定

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

始める前に

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 にログインしています。
- OpenSSH 形式の SSH 公開鍵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	**config t**
	
	例：
	`n1000v# config t`
	`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	**username** *username* **sshkey** *ssh-key*	既存のユーザ アカウントで OpenSSH 形式の SSH 公開鍵を設定します。 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。 **username** *name* **password** *pwd*
	例： `n1000v(config)# username user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyK cb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5aw fVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8 QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuD YSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby /ZWx/clTYiXQR1X1VfhQ==`  **例：** `n1000v(config)# exit` `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	**show user-account**	（任意）ユーザ アカウントの設定を表示します。

	例：
	`n1000v# show user-account`
	`user:admin`
	`this user account has no expiry date`
	`roles:network-admin`
	`user:user1`
	`this user account has no expiry date`
	`roles:network-operator`
	`ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdH Ha/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6 /n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EI r/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m 9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1Vf hQ==`	

ステップ 5	**copy running-config startup-config** **例：** `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 鍵の設定

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

始める前に

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 にログインしています。
- 次のいずれかの形式の SSH 公開鍵が生成されています。
  - IETF SECSH 形式
  - PEM 形式の公開鍵証明書

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	**copy** *server-file* **bootflash:***filename*	サーバから 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。

	例：
	`n1000v# copy tftp://10.78.1.10/secsh_file.pub bootflash:secsh_file.pub vrf management`
	`Trying to connect to tftp server......`
	`Connection to server Established.`
	`|`
	`TFTP get operation was successful`
	`n1000v#`	

ステップ 2	**config t**
	
	例：
	`n1000v# config t`
	`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 3	**username** *username* **sshkey file bootflash:***filename* **例：** `n1000v(config)# username User1 sshkey file bootflash:secsh_file.pub`	SSH 公開鍵を設定します。

	コマンド	目的
ステップ 4	**exit** 例： n1000v(config)# exit 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	**show user-account**	（任意）ユーザ アカウントの設定を表示します。

例：

```
n1000v# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user2
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CC
LUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6
mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJN
U1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
```

ステップ 6	**copy running-config startup-config** 例： 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。

始める前に

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 にログインしています。
- 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	**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	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	**clear ssh hosts** **例：** n1000v# 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

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。

始める前に

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 にログインしています。
- 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 サーバ鍵を生成する必要があります。

  「SSH サーバ鍵の生成」の手順（P.7-3）を参照してください。

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**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`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	**no ssh server enable**
	
	例：
	`n1000v(config)# no ssh server enable`
	`XML interface to system may become unavailable since ssh is disabled`
	`n1000v#`
		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：
	`n1000v(config)# exit`
	`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	**show ssh server**
	
	例：
	`n1000v#  show ssh server`
	`ssh is not enabled`
	`n1000v#`
		（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： `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 サーバ鍵の削除

SSH サーバをディセーブルにしたあと、SSH サーバ鍵を削除するには、次の手順を実行します。

始める前に

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 にログインしています。
- 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 サーバ鍵を生成する必要があります。

  「SSH サーバ鍵の生成」の手順（P.7-3）を参照してください。

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**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t 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	**no ssh server enable** 例： n1000v(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： n1000v(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： n1000v(config)# exit 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	**show ssh key** 例： n1000v# 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： 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。

例：

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

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/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+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

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+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

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。

始める前に

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 にログインしています。

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	**show users** 例： n1000v# 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： n1000v# clear line 0	ユーザの SSH セッションをクリアします。
ステップ 3	**show users** 例： 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
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 アカウントに対するデフォルト値が表示されます。
show ssh server	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/oEIZAtlVLY
k/PEzt+ED7lPal/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 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。

```
n1000v# config t
n1000v(config)# no ssh server enable
```

ステップ 2　SSH サーバ鍵を生成します。

```
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)# ssh server enable
```

ステップ 4　SSH サーバ鍵を表示します。

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

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
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。

```
n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+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 ssh server enable
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
n1000v(config)# ssh server enable
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+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+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.7-15）
- 「標準規格」（P.7-15）

関連資料

関連項目	マニュアル タイトル
CLI	『*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*』
Telnet	第 8 章「Telnet の設定」

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

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	この機能が追加されました。