SSH および Telnet の設定

この章は、次の項で構成されています。

SSH および Telnet の概要

SSH サーバー

セキュア シェル（SSH）プロトコル サーバー機能を使用すると、SSH クライアントは Cisco Nexus 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 は強化暗号化を使用して認証を行います。Cisco Nexus デバイス スイッチの SSH サーバーは、無償あるいは商用の SSH クライアントと連係して動作します。

SSH がサポートするユーザー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ー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、スイッチは、別の Cisco Nexusスイッチとの間、または SSH サーバーを稼働している他の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デバイスの SSH クライアントは、公開されているあるいは商用の SSH サーバーと連係して動作します。

SSH サーバ キー

SSH では、Cisco Nexusデバイスと安全な通信を行うためにサーバー 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 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、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 デバイスは 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）

⚠

Caution 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。

デジタル証明書を使用した SSH 認証

Cisco NX-OS デバイスでの SSH 認証では、ホスト認証用に X.509 デジタル証明書をサポートしています。X.509 デジタル証明書は、メッセージの出所と整合性を保証するデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局（CA）によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書のインフラストラクチャでは、Secure Socket Layer（SSL）に対応し、セキュリティ インフラストラクチャによってクエリーまたは通知を通じて最初に返される証明書が使用されます。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。

X.509v3 証明書（RFC 6187）を使用する SSH 認証を設定できます。X.509v3 証明書ベースの SSH 認証では、スマートカードと組み合わせた証明書を使用して、シスコ デバイスへのアクセスの 2 要素認証を有効にします。SSH クライアントは、シスコパートナーの Pragma Systems によって提供されます。

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ーが別サイトのログイン サーバーとの 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。

デフォルトでは、Telnet サーバは Cisco Nexus デバイス上で無効になっています。

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限事項があります。

- Cisco Nexus デバイスは、SSH バージョン 2（SSHv2）だけをサポートしています。
- SSH パスワードレス ファイル コピーを目的として AAA プロトコル（RADIUS や TACACS+ など）を介してリモート認証されたユーザ アカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカル ユーザ アカウントでない限り、Nexus デバイスがリロードされると保持されません。リモート ユーザ アカウントは、SSH キーがインポートされる前にデバイスで設定されます。

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}
3. switch(config)# **exit**
4. (Optional) switch# **show ssh key [dsa | rsa] [md5]**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}	SSH サーバー キーを生成します。 *bits* 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 ～ 4096 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	(Optional) switch# **show ssh key [dsa | rsa] [md5]**	SSH サーバー キーを表示します。 Cisco NX-OS リリース 7.0(3)I4(6) および 7.0(3)I4(x) 以降のリリースでは、このコマンドはデフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、**md5** オプションが追加されています。
ステップ 5	(Optional) switch# **copy running-config startup-config**	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。

Example

次に、SSH サーバー 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

ユーザー アカウント用に SSH 形式で SSH 公開キーを指定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **username** *username* **sshkey** *ssh-key*
3. switch(config)# **exit**
4. (Optional) switch# **show user-account**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル構成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	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	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。

Example

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
XIeccWk0gS1DQUNZ300xstQsYZUtqnx1bvm5Ninn0McNinn0Mc=
switch(config)# exit
switch# show user-account
switch# copy running-config startup-config
```

Note 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

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

SUMMARY STEPS

1. switch# **copy** *server-file* **bootflash:** *filename*
2. switch# **configure terminal**
3. switch(config)# **username** *username* **sshkey file** *filename*
4. switch(config)# **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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）サーバーを利用できます。
ステップ 2	switch# **configure terminal**	グローバル構成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	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	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。

Example

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

ユーザー 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。

SUMMARY STEPS

1. switch# **copy** *server-file* **bootflash:** *filename*
2. switch# **configure terminal**
3. (Optional) switch# **show user-account**
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバーから 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 サーバーを利用できます。
ステップ 2	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 3	(Optional) switch# **show user-account**	ユーザー アカウントの設定を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	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。

Example

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
```

SSH 送信元インターフェイスの構成

SSH は、特定のインターフェイスを使用するように構成できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip ssh source-interface** *type slot/port*
3. switch(config)# **show ip ssh source-interface**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **ip ssh source-interface** *type slot/port*	すべての SSH パケットの送信元インターフェイスを構成します。次のリストに、*interface* として有効な値を示します。 • ethernet • loopback • mgmt • port-channel • vlan
ステップ 3	switch(config)# **show ip ssh source-interface**	構成済みの SSH 送信元インターフェイスを表示します。

例

次に、SSH 送信元インターフェイスを構成する例を示します。

```
switch(config)# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip ssh source-interface ethernet 1/7
switch(config)# show ip ssh source-interface
VRF Name                                Interface
default                                 Ethernet1/7
```

リモート デバイスとの SSH セッションの開始

Cisco Nexus デバイスからリモート デバイスに接続する SSH セッションを開始できます。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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 *hostname* 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 を使用してサーバーからファイルをダウンロードする場合は、サーバーと信頼性のある SSH 関係を確立します。

SUMMARY STEPS

1. switch# **clear ssh hosts**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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 デバイスでは、デフォルトで SSH サーバーが有効になっています。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] feature ssh**
3. switch(config)# **exit**
4. (Optional) switch# **show ssh server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **[no] feature ssh**	SSHサーバーをイネーブル/ディセーブルにします。デフォルトでは有効になっています。
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	(Optional) switch# **show ssh server**	SSH サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	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 サーバーをディセーブルにした後、SSH サーバー キーを削除できます。

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no feature ssh**
3. switch(config)# **no ssh key** [**dsa** | **rsa**]
4. switch(config)# **exit**
5. (Optional) switch# **show ssh key**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバー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。

	Command or Action	Purpose
		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	(Optional) switch# **show ssh key**	SSH サーバーの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	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 セッションは Cisco Nexus デバイスからクリアできます。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザー 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。

SUMMARY STEPS

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 サーバー 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。

DETAILED STEPS

Procedure

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
```

Note
SSH サーバーはデフォルトでイネーブルになっているため、この手順は必要ありません。

ステップ 3 SSH サーバー 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
```

X.509v3 証明書ベースの SSH 認証の設定

X.509v3 証明書を使用する SSH 認証を設定できます。

始める前に

リモート デバイスの SSH サーバをイネーブルにします。

手順の概要

1. **configure terminal**
2. **username** *user-id* [**password** [**0** | **5**] *password*]
3. **username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**}
4. [**no**] **crypto ca trustpoint** *trustpoint*
5. [**no**] **crypto ca authentication** *trustpoint*
6. **crypto ca crl request** *trustpoint* **bootflash:***static-crl***.crl**
7. （任意） **show crypto ca certificates**
8. （任意） **show crypto ca crl** *trustpoint*
9. （任意） **show user-account**
10. （任意） **show users**
11. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`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** *user-id* [**password** [**0** | **5**] *password*] 例： `switch(config)# username jsmith password 4Ty18Rnt`	ユーザ アカウントを設定します。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン（-）、ピリオド（.）、アンダースコア（_）、プラス符号（+）、および等号（=）です。アットマーク（@）はリモート ユーザ名では使用できますが、ローカル ユーザ名では使用できません。 ユーザ名の先頭は英数字で始まる必要があります。

	コマンドまたはアクション	目的
		デフォルト パスワードは定義されていません。オプションの **0** は、パスワードがクリア テキストであり、**5**はパスワードが暗号化されていることを意味します。デフォルトは **0**（クリア テキスト）です。 （注） パスワードを指定しなかった場合、ユーザーは Cisco NX-OS デバイスにログインできません。 （注） 暗号化パスワードオプションを使用してユーザアカウントを作成する場合、対応する SNMP ユーザは作成されません。
ステップ 3	**username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**} 例： `switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa`	既存のユーザ アカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ emailAddress と ST に設定されていることを確認します。
ステップ 4	[**no**] **crypto ca trustpoint** *trustpoint* 例： `switch(config)# crypto ca trustpoint winca`	トラストポイントを設定します。
ステップ 5	[**no**] **crypto ca authentication** *trustpoint* 例： `switch(config)# crypto ca authentication winca`	トラストポイントの証明書チェーンを構成します。
ステップ 6	**crypto ca crl request** *trustpoint* **bootflash:***static-crl***.crl** 例： `switch(config)# crypto ca crl request winca bootflash:crllist.crl`	トラストポイントの証明書失効リスト（CRL）を設定します。CRL ファイルは、トラストポイントによって失効した証明書のリストのスナップショットです。このスタティック CRL リストは、認証局（CA）からデバイスに手動でコピーされます。 （注） スタティック CRL は、サポートされている唯一の失効チェック方式です。
ステップ 7	（任意） **show crypto ca certificates** 例： `switch(config)# show crypto ca certificates`	設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。

	コマンドまたはアクション	目的
ステップ 8	（任意） **show crypto ca crl** *trustpoint* 例： `switch(config)# show crypto ca crl winca`	指定したトラストポイントの CRL リストの内容を表示します。
ステップ 9	（任意） **show user-account** 例： `switch(config)# show user-account`	設定されたユーザアカウントの詳細を表示します。
ステップ 10	（任意） **show users** 例： `switch(config)# show users`	デバイスにログオンしているユーザが表示されます。
ステップ 11	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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。

X.509v3 証明書ベースの SSH 認証の設定例

次の例は、X.509v3 証明書を使用する SSH 認証の設定方法を示しています。

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
 rsa
crypto ca trustpoint tp1
crypto ca authentication tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /CN=SecDevCA
    Last Update: Aug 8 20:03:15 2016 GMT
    Next Update: Aug 16 08:23:15 2016 GMT
    CRL extensions:
        X509v3 Authority Key Identifier:
            keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A
```

```
show user-account
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
NAME       LINE         TIME           IDLE      PID          COMMENT
user1      pts/1        Jul 27 18:43   00:03     18796      (10.10.10.1)   session=ssh
```

Telnet の設定

Telnet サーバのイネーブル化

デフォルトでは、Telnet サーバーはイネーブルに設定されています。Cisco Nexus デバイスの Telnet サーバーを無効にできます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **[no] feature telnet**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **[no] feature telnet**	Telnet サーバーをイネーブル/ディセーブルにします。デフォルトではイネーブルになっています。

Telnet サーバーの再イネーブル化

Cisco Nexus デバイスの Telnet サーバーが無効にされていた場合は、再度有効にすることができます。

SUMMARY STEPS

1. switch(config)# **[no] feature telnet**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch(config)# **[no] feature telnet**	Telnet サーバーを再度イネーブルにします。

Telnet 送信元インターフェイスの構成

Telnet は、特定のインターフェイスを使用するように構成できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip telnet source-interface** *type slot/port*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル構成モードを開始します。
ステップ 2	switch(config)# **ip telnet source-interface** *type slot/port*	すべての Telnet パケットの送信元インターフェイスを設定します。次のリストに、*interface* として有効な値を示します。 • ethernet • loopback • mgmt • port-channel • vlan

例

次に、Telnet 送信元インターフェイスを構成する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip telnet source-interface ethernet 1/6
switch(config)# show ip telnet source-interface
VRF Name                                Interface
default                                 Ethernet1/6
switch(config)#
```

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ます。必要に応じて、リモートデバイスのユーザー名も取得します。
- Cisco Nexus デバイス上で Telnet サーバを有効にします。
- リモート デバイス上で Telnet サーバーをイネーブルにします。

SUMMARY STEPS

1. switch# **telnet** *hostname*

DETAILED STEPS

Procedure

	Command or Action	Purpose
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 *hostname* には、IPv4 アドレス、またはホスト名を指定します。

Example

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

Telnet セッションは Cisco Nexus デバイスからクリアできます。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **show users**	ユーザー 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。

コマンドまたはアクション	目的
switch# **show ssh key [dsa | rsa][md5]**	SSH サーバー キーを表示します。
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。all キーワードを指定すると、SSH およびユーザー アカウントのデフォルト値が表示されます。
switch# **show ssh server**	SSH サーバー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。
switch# **show users**	デバイスにログオンしているユーザが表示されます。
switch# **show crypto ca certificates**	X.509v3証明書ベースのSSH認証に設定された証明書チェーンおよび関連するトラストポイントを表示します。
switch# **show crypto ca crl** *trustpoint*	指定したトラストポイントの CRL リストの内容を表示します。

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。

Table 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

パラメータ	デフォルト
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	有効（Enabled）

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。