



## SSH および Telnet の設定

この章では、Cisco NX-OS デバイス上でセキュア シェル（SSH） 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。

この章は、次の項で構成されています。

- [SSH および Telnet について, on page 1](#)
- [SSH および Telnet の前提条件, on page 3](#)
- [SSH と Telnet の注意事項と制約事項 \(3 ページ\)](#)
- [SSH および Telnet のデフォルト設定, on page 4](#)
- [SSH の設定 , on page 4](#)
- [Telnet の設定, on page 22](#)
- [SSH および Telnet の設定の確認, on page 23](#)
- [SSH の設定例, on page 24](#)
- [SSH のパスワードが不要なファイル コピーの設定例, on page 25](#)
- [X.509v3 証明書ベースの SSH 認証の設定例 \(27 ページ\)](#)
- [SSH および Telnet に関する追加情報, on page 27](#)

## SSH および Telnet について

ここでは、SSH および Telnet について説明します。

### SSH サーバー

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 は強化暗号化を使用して認証を行います。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 がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service (RADIUS)、TACACS+、LDAP、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。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デバイスとの間で暗号化された安全な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 NX-OS ソフトウェアの SSH クライアントは、無償あるいは商用の SSH サーバと連係して動作します。

## SSH サーバキー

SSH では、Cisco NX-OS 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 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、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 に対応する以下の 2 通りのキーペアを使用できます。

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

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA 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)
- Privacy-Enhanced Mail (PEM) の公開キー証明書



---

**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

デ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 のいずれかで設定されており、無効にされたり期限が切れたりしていなければ、証明書の検証は成功します。

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。

## 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、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス 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 サーバが Cisco NX-OS デバイス上でディセーブルになっています。

## SSH および Telnet の前提条件

レイヤ 3 インターフェイス上で IP、mgmt 0 インターフェイス上でアウトバンド、またはイーサネット インターフェイス上でインバンドを設定していることを確認します。

## SSH と Telnet の注意事項と制約事項

SSH および Telnet に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS ソフトウェアは、SSH バージョン 2（SSHv2）だけをサポートしています。
- **no feature ssh feature** コマンドを使用すると、ポート 22 はディセーブルになりません。ポート 22 は常にオープンで、すべての着信外部接続を拒否する拒否ルールがプッシュされます。
- Poodle の脆弱性により、SSLv3 はサポートされなくなりました。
- IPSG は、次のものではサポートされません。
  - Cisco Nexus® 3550-T スイッチの最後の 6 個の 40 Gb 物理ポート
  - Cisco Nexus® 3550-T スイッチのすべての 40 Gb 物理ポート
- 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。
- SFTP サーバ機能では、通常の SFTP の **chown** および **chgrp** コマンドを発行します。

- SFTP サーバが有効になっている場合は、admin ユーザだけが SFTP を使用してデバイスにアクセスできます。
- 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 のタイムアウト時間は、tac-pac の生成時間よりも長くする必要があります。そうでないと、VSH ログに %VSHD-2-VSHD\_SYSLOG\_EOL\_ERR エラーが記録されることがあります。理想的には、tac-pac または showtech を収集する前に 0 (無限) に設定します。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## SSH および Telnet のデフォルト設定

次の表に、SSH および Telnet 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 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 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	ディセーブル
Telnet ポート番号	23
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	ディセーブル

## SSH の設定

ここでは、SSH の設定方法について説明します。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	SSH を無効にします。
ステップ 3	<b>feature ssh</b> <b>Example:</b> switch(config)# feature ssh	SSH を有効にします。
ステップ 4	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show ssh key [dsa   rsa   ] []</b> <b>Example:</b> switch# show ssh key	SSH サーバキーを表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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

## 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。

### Before you begin

IETF SCHSH 形式の SSH 公開キーを作成します。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>copy server-file bootflash:filename</b> <b>Example:</b> <pre>switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub</pre>	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。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	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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	<b>username username sshkey file bootflash:filename</b> <b>Example:</b> <pre>switch(config)# username User1 sshkey file bootflash:secsh_file.pub</pre>	IETF SECSH 形式の SSH 公開キーを設定します。
ステップ 4	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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) <b>show user-account</b> <b>Example:</b> <pre>switch# show user-account</pre>	ユーザアカウントの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

## OpenSSH 形式の SSH 公開キーの指定

ユーザアカウントに OpenSSH 形式の SSH 公開キーを指定できます。

**Before you begin**

OpenSSH 形式の SSH 公開キーを作成します。

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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> <b>Example:</b> <pre>switch(config)# username User1 sshkey ssh-rsa AAE3NaCly2ZWF5WAF191GZL9G3FXsKQW47A1x79SP hBns6AKi1nIfDumHJqP/Lo7toIMREYGLN089ig3086 XhNjn1B7ihp7h7dtdMwOmYsh6SiH3D/kyzieH54tlx8</pre>	OpenSSH 形式の SSH 公開キーを設定します。
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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) <b>show user-account</b> <b>Example:</b> <pre>switch# show user-account</pre>	ユーザアカウントの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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 ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。



**Note** ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワードベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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>ssh login-attempts <i>number</i></b> <b>Example:</b> <pre>switch(config)# ssh login-attempts 5</pre>	<p>ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は 3 です。値の範囲は 1 ~ 10 です。</p> <p><b>Note</b> このコマンドの <b>no</b> 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の 3 に設定されます。</p>
ステップ 3	<b>(Optional) show running-config security all</b> <b>Example:</b> <pre>switch(config)# show running-config security all</pre>	SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(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 を使用して SSH セッションを開始し、リモートデバイスと接続します。



**Before you begin**

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。

リモートデバイスの SSH サーバを有効にします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>ssh</b> [ <i>username@</i> ]{ <i>ipv4-address</i>   <i>hostname</i> } <b>Example:</b> switch# ssh 10.10.1.1	IPv4 を使用してリモートデバイスとの SSH IPv4 セッションを作成します。

**ブートモードからの SSH セッションの開始**

SSH セッションは、リモートデバイスに接続する Cisco NX-OS デバイスのブートモードから開始できます。

**Before you begin**

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。

リモートデバイスの SSH サーバを有効にします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>ssh</b> [ <i>username@</i> ] <i>hostname</i> <b>Example:</b> switch(boot)# ssh user1@10.10.1.1	リモートデバイスへの SSH セッションを、Cisco NX-OS デバイスのブートモードから作成します。
ステップ 2	<b>exit</b> <b>Example:</b> switch(boot)# exit	ブートモードを終了します。
ステップ 3	<b>copy scp://</b> [ <i>username@</i> ] <i>hostname</i> / <i>filepath</i> <i>directory</i> <b>Example:</b> switch# copy scp://user1@10.10.1.1/users abc	セキュアコピープロトコル (SCP) を使用して、ファイルを Cisco NX-OS デバイスからリモートデバイスへコピーします。

## SSH のパスワードが不要なファイルコピーの設定

Cisco NX-OS デバイスから Secure Copy (SCP) サーバまたは Secure FTP (SFTP) サーバに、パスワードなしでファイルをコピーすることができます。これを行うには、SSH による認証用の公開キーと秘密キーで構成される RSA または DSA のアイデンティティを作成する必要があります。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	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>[no] username <i>username</i> keypair generate {rsa [<i>bits</i> [<i>force</i>]]   dsa [<i>force</i>]}</b> <b>Example:</b> <pre>switch(config)# username user1 keypair generate rsa 2048 force</pre>	<p>SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリ (\$HOME/.ssh) に格納します。Cisco NX-OS デバイスでは、これらのキーを使用してリモート マシンの SSH サーバと通信します。</p> <p><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。</p> <p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーは生成されません。</p>
ステップ 3	<b>(Optional) show username <i>username</i> keypair</b> <b>Example:</b> <pre>switch(config)# show username user1 keypair</pre>	<p>指定したユーザの公開キーを表示します。</p> <p><b>Note</b> セキュリティ上の理由から、このコマンドで秘密キーは表示されません。</p>
ステップ 4	<b>Required: username <i>username</i> keypair export {bootflash:<i>filename</i>   volatile:<i>filename</i>} {rsa   dsa} [<i>force</i>]</b> <b>Example:</b> <pre>switch(config)# username user1 keypair export bootflash:key_rsa rsa</pre>	<p>Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリまたは一時ディレクトリに、公開キーと秘密キーをエクスポートします。</p>

	Command or Action	Purpose
		<p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはエクスポートされません。</p> <p>生成したキー ペアをエクスポートするとき、秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは、指定したファイルとしてエクスポートされ、公開キーは、同じファイル名に <b>.pub</b> 拡張子を付けてエクスポートされます。これで、このキー ペアを任意の Cisco NX-OS デバイスにコピーし、SCP または SFTP を使用してサーバのホーム ディレクトリに公開キー ファイル (*.pub) をコピーできるようになります。</p> <p><b>Note</b> セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。</p>
ステップ 5	<p>Required: <b>username username keypair import {bootflash:filename   volatile:filename} {rsa   dsa} [force]</b></p> <p><b>Example:</b></p> <pre>switch(config)# username user1 keypair import bootflash:key_rsa rsa</pre>	<p>指定したブートフラッシュ ディレクトリまたは一時ディレクトリから、Cisco NX-OS デバイスのホーム ディレクトリに、エクスポートした公開キーと秘密キーをインポートします。</p> <p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはインポートされません。</p> <p>生成したキー ペアをインポートするとき、秘密キーを復号化するパスフレーズを入力するように求められます。秘密キーは指定したファイルとしてインポートされ、公開キーは同じファイル名に <b>.pub</b> 拡張子を付けてインポートされます。</p>

	Command or Action	Purpose
		<p><b>Note</b> セキュリティ上の理由から、このコマンドはグローバルコンフィギュレーションモードでしか実行できません。</p> <p><b>Note</b> パスワードなしでサーバにアクセスできるのは、サーバでキーが設定されているユーザのみです。</p>

### What to do next

SCP サーバまたは SFTP サーバで、次のコマンドを使用して、\*.pub ファイル（たとえば、key\_rsa.pub）に格納された公開キーを authorized\_keys ファイルに追加します。

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

## SCP サーバと SFTP サーバの設定

リモートデバイスとの間でファイルをコピーできるように、Cisco NX-OS デバイスで SCP サーバまたは SFTP サーバを設定できます。SCP サーバまたは SFTP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモートデバイスで SCP または SFTP コマンドを実行できます。



**Note** arcfour および blowfish cipher オプションは SCP サーバではサポートされません。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 2	<b>[no] feature scp-server</b> <b>Example:</b> <pre>switch(config)# feature scp-server</pre>	Cisco NX-OS デバイス上で SCP サーバをイネーブルまたはディセーブルにします。

	Command or Action	Purpose
ステップ 3	Required: <b>[no] feature sftp-server</b> <b>Example:</b> switch(config)# feature sftp-server	Cisco NX-OS デバイス上で SFTP サーバをイネーブルまたはディセーブルにします。
ステップ 4	Required: <b>exit</b> <b>Example:</b> 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	(Optional) <b>show running-config security</b> <b>Example:</b> switch# show running-config security	SCP サーバと SFTP サーバの設定ステータスを表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> <b>例 :</b> 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	<b>username user-id [password [0   5] password]</b> <b>例 :</b> switch(config)# username jsmith password 4Ty18Rnt	ユーザ アカウントを設定します。 <i>user-id</i> 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

	コマンドまたはアクション	目的
		<p>きますが、ローカルユーザ名では使用できません。</p> <p>ユーザ名の先頭は英数字で始まる必要があります。</p> <p>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 <b>0</b> は、パスワードがクリアテキストであり、<b>5</b> 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 <b>0</b> (クリアテキスト) です。</p> <p>(注) パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。</p> <p>(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。</p>
ステップ 3	<p><b>username</b> <i>user-id</i> <b>ssh-cert-dn</b> <i>dn-name</i> {<b>dsa</b>   <b>rsa</b>}</p> <p>例 :</p> <pre>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</pre>	<p>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 <b>emailAddress</b> と <b>ST</b> に設定されていることを確認します。</p>
ステップ 4	<p><b>[no]</b> <b>crypto ca trustpoint</b> <i>trustpoint</i></p> <p>例 :</p> <pre>switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</pre>	<p>トラストポイントを設定します。</p> <p>(注) このコマンドの <b>no</b> 形式を使用してトラストポイントを削除する前に、まず <b>delete crl</b> および <b>delete ca-certificate</b> コマンドを使用して、CRL および CA 証明書を削除する必要があります。</p>
ステップ 5	<p><b>crypto ca authenticate</b> <i>trustpoint</i></p> <p>例 :</p>	<p>トラストポイントの CA 証明書を設定します。</p>

	コマンドまたはアクション	目的
	<pre>switch(config-trustpoint)# crypto ca authenticate winca</pre>	<p>(注) CA 証明書を削除するには、トラストポイント コンフィギュレーション モードで <b>delete ca-certificate</b> コマンドを入力します。</p>
ステップ 6	<p>(任意) <b>crypto ca crl request trustpoint bootflash:static-crl.crl</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# crypto ca crl request winca bootflash:crl1list.crl</pre>	<p>この項はオプションですが、強く推奨されます。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。</p> <p>(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。</p> <p>(注) CRL を削除するには、<b>delete crl</b> コマンドを入力します。</p>
ステップ 7	<p>(任意) <b>show crypto ca certificates</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show crypto ca certificates</pre>	<p>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。</p>
ステップ 8	<p>(任意) <b>show crypto ca crl trustpoint</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show crypto ca crl winca</pre>	<p>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。</p>
ステップ 9	<p>(任意) <b>show user-account</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show user-account</pre>	<p>設定されたユーザアカウントの詳細を表示します。</p>
ステップ 10	<p>(任意) <b>show users</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show users</pre>	<p>デバイスにログオンしているユーザが表示されます。</p>
ステップ 11	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p>	<p>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。</p>

	コマンドまたはアクション	目的
	switch(config-trustpoint)# copy running-config startup-config	

## レガシー SSH アルゴリズム サポートの設定

レガシー SSH セキュリティアルゴリズム、メッセージ認証コード (MAC)、キータイプ、および暗号のサポートを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	(任意) <b>ssh kexalgos [all]</b> 例： switch(config)# ssh kexalgos all	接続ごとのキーの生成に使用されるキー交換方式である、サポートされているすべての <b>KexAlgorithms</b> を有効にするには、 <b>all</b> キーワードを使用します。  サポートされる KexAlgorithmn は次のとおりです。 <ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group1-sha1</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group1-sha1</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> </ul>
ステップ 3	(任意) <b>ssh macs all</b> 例： switch(config)# ssh macs all	トラフィック変更の検出に使用されるメッセージ認証コードである、サポートされているすべての <b>MAC</b> を有効にします。  サポートされる <b>MAC</b> は次のとおりです。 <ul style="list-style-type: none"> <li>• hmac-sha1</li> </ul>



	コマンドまたはアクション	目的
ステップ 4	(任意) <code>ssh ciphers [ all ]</code> 例 : <pre>switch(config)# ssh ciphers all</pre>	サポートされているすべての暗号を有効にして接続を暗号化するには、 <b>all</b> キーワードを使用します。 サポート対象の暗号方式 : <ul style="list-style-type: none"> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>
ステップ 5	(任意) <code>ssh keytypes all</code> 例 : <pre>switch(config)# ssh keytypes all</pre>	サーバがクライアントに対して自身を認証するために使用できる公開キーアルゴリズムである、サポートされているすべての <code>PubkeyAcceptedKeyType</code> を有効にします。 サポートされるキータイプは次のとおりです。 <ul style="list-style-type: none"> <li>• ssh-dss</li> <li>• ssh-rsa</li> </ul>

## サポートされるアルゴリズム : FIPモードが有効の場合

FIP モードが有効な場合にサポートされるアルゴリズムのリストは次のとおりです。

表 2: サポートされるアルゴリズム : FIPモードが有効の場合

アルゴリズム	サポート対象	サポート対象外
ciphers	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> </ul>

アルゴリズム	サポート対象	サポート対象外
hmac	<ul style="list-style-type: none"> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• hmac-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha1-etm@openssh.com</li> </ul>
kexalgo	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group14-sha256</li> </ul>	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• curve25519-sha256@libssh.org</li> </ul>
keytypes	<ul style="list-style-type: none"> <li>• rsa-sha2-256</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> </ul>	ssh-rsa

## デフォルトの SSH サーバポートの変更

SSHv2 のポート番号をデフォルトのポート番号 22 から変更できます。。デフォルトの SSH ポートの変更時に使用される暗号化により、より強力なプライバシーとセッション整合性をサポートする接続が実現します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	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>no feature ssh</b> 例 : <pre>switch(config)# no feature ssh</pre>	SSH を無効にします。
ステップ 3	<b>show sockets local-port-range</b> 例 :	使用可能なポート範囲を表示します。

	コマンドまたはアクション	目的
	switch(config)# show sockets local port range (15001 - 58000) switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535)	
ステップ 4	<b>ssh port local-port</b> 例： switch(config)# ssh port 58003	ポートを設定します。
ステップ 5	<b>feature ssh</b> 例： switch(config)# feature ssh	SSH を有効にします。
ステップ 6	<b>exit</b> 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 7	(任意) <b>show running-config security all</b> 例： switch# ssh port 58003	セキュリティの設定を表示します。
ステップ 8	(任意) <b>copy running-config startup-config</b> 例： 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 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、またはこのデバイスからリモート 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>clear ssh hosts</b> Example: switch# clear ssh hosts	SSH ホスト セッションおよび既知のホスト ファイルをクリアします。

## SSH サーバのディセーブル化

Cisco NX-OS 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。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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	SSH を無効にします。
ステップ 3	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show ssh server</b> <b>Example:</b> switch# show ssh server	SSH サーバの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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 サーバをディセーブルにした後、Cisco NX-OS デバイス上の SSH サーバ 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 キーを生成する必要があります。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	SSH を無効にします。
ステップ 3	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show ssh key</b> <b>Example:</b> switch# show ssh key	SSH サーバ キーの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## Related Topics

[SSH サーバ キーの生成 \(5 ページ\)](#)

## 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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>show users</b> <b>Example:</b> switch# 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> <b>Example:</b> switch(config)# clear line pts/12	ユーザ SSH セッションをクリアします。

## Telnet の設定

ここでは、Cisco NX-OS デバイスで Telnet を設定する手順を説明します。

### Telnet サーバのイネーブル化

Cisco NX-OS デバイス上で Telnet サーバを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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>feature telnet</b> <b>Example:</b> switch(config)# feature telnet	Telnet サーバをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show telnet server</b> <b>Example:</b> switch# show telnet server	Telnet サーバの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

### リモート デバイスとの 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 デバイスと接続できます。IPv4 のいずれかを使用して Telnet セッションを開始できます。

**Before you begin**

リモートデバイスのホスト名または IP アドレスと、必要な場合はリモート デバイスのユーザ名を取得します。

Cisco NX-OS 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 サーバを有効にします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>telnet</b> { <i>ipv4-address</i>   <i>host-name</i> } [ <i>port-number</i> ]  <b>Example:</b> switch# telnet 10.10.1.1	IPv4 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。値の範囲は 1 ~ 65535 です。

**Related Topics**

[Telnet サーバのイネーブル化](#) (22 ページ)

## Telnet セッションのクリア

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

**Before you begin**

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>show users</b>  <b>Example:</b> switch# 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>  <b>Example:</b> switch(config)# clear line pts/12	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 および Telnet 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	目的
<b>show ssh key [dsa   rsa] []</b>	SSH サーバ キーを表示します。

コマンド	目的
<code>show running-config security [all]</code>	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。 <b>all</b> キーワードを指定すると、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。
<code>show ssh server</code>	SSH サーバの設定を表示します。
<code>show telnet server</code>	Telnet サーバの設定を表示します。
<code>show username <i>username</i> keypair</code>	指定したユーザの公開キーを表示します。
<code>show user-account</code>	設定されたユーザアカウントの詳細を表示します。
<code>show users</code>	デバイスにログオンしているユーザが表示されます。

## SSH の設定例

次の例は、OpenSSH キーを使用して SSH を設定する方法を示しています。

### Procedure

ステップ 1 SSH サーバをディセーブルにします。

#### Example:

```
switch# configure terminal
switch(config)# no feature ssh
```

ステップ 2 SSH サーバ キーを生成します。

#### Example:

```
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。

#### Example:

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

ステップ 4 SSH サーバ キーを表示します。

#### Example:

ステップ 5 OpenSSH 形式の SSH 公開キーを指定します。

#### Example:



```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZ19G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhoBYmsi6PAVKu1nIf/DQhum+1JNqJP/eLowb7ubO+1VKRXFY/G+1JNlQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyzIEh5
4Tplx8=
```

**ステップ 6** 設定を保存します。

**Example:**

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

## SSH のパスワードが不要なファイルコピーの設定例

次に、Cisco NX-OS デバイスから Secure Copy (SCP) サーバまたは Secure FTP (SFTP) サーバに、パスワードなしでファイルをコピーする例を示します。

### Procedure

**ステップ 1** SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリに格納します。

**Example:**

```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits).....
generated rsa key
```

**ステップ 2** 指定したユーザの公開キーを表示します。

**Example:**

```
switch(config)# show username admin keypair

*****

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
```

**ステップ 3** Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリに、公開キーと秘密キーをエクスポートします。

**Example:**

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
    951      Jul 09 11:13:59 2013  key_rsa
    221      Jul 09 11:14:00 2013  key_rsa.pub
.
.
```

**ステップ 4** これら 2 つのファイルを他の Cisco NX-OS デバイスへコピーした後、**copy scp** または **copy sftp** コマンドを使用して、Cisco NX-OS デバイスのホーム ディレクトリにインポートします。

**Example:**

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
*****

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByPyDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoaJzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
*****

could not retrieve dsa key information
*****
switch(config)#
```

**ステップ 5** SCP サーバまたは SFTP サーバで、key\_rsa.pub に格納されている公開キーを authorized\_keys ファイルに追加します。

**Example:**

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

ステップ 6 (Optional) DSA キーについてこの手順を繰り返します。

## 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 authenticate 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
```

## SSH および Telnet に関する追加情報

ここでは、SSH および Telnet の実装に関する追加情報について説明します。

## 関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	<i>Cisco NX-OS</i> ライセンス ガイド
VRF コンフィギュレーション	<i>Cisco Nexus</i> <sup>®</sup> 3550- <i>T</i> ユニキャスト ルーティングの構成ガイド

## MIB

MIB	MIB のリンク
SSH および Telnet に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>

## 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。