セキュア シェル コマンド

ここでは、セキュア シェル（SSH）を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

SSH の概念、設定作業、および例の詳細については 『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』 の 「*Implementing Secure Shell on* Cisco ASR 9000 Series Router Software」設定モジュールを参照してください。

clear ssh

着信または発信のセキュア シェル（SSH）接続を終了するには、EXEC モードで **clear ssh** コマンドを使用します。

clear ssh {*session-id*| **outgoing** *session-id*}

構文の説明

session-id	**show ssh** コマンドの出力で表示される着信接続のセッション ID 番号。範囲は 0 ～ 1024 です。
outgoing *session-id*	**show ssh** コマンドの出力で表示される発信接続のセッション ID 番号を指定します。 指定できる範囲は 1 ～ 10 です。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

着信または発信の SSH 接続を切断するには、**clear ssh** コマンドを使用します。 着信接続は、ローカル ネットワーキング デバイス上で実行している SSH サーバによって管理されます。 発信接続は、ローカル ネットワーキング デバイスから開始されます。

接続のセッション ID を表示するには、**show ssh** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	execute

例

次の例では、**show ssh** コマンドを使用して、ルータへのすべての着信接続と発信接続を表示します。 そのあと、**clear ssh** コマンドを使用して、ID 番号が 0 の着信セッションを終了します。

```
RP/0/RSP0/CPU0:router# show ssh

SSH version: Cisco-2.0
session     pty  location   state       userid     host        ver
---------------------------------------------------------------------
Incoming sessions
0           vty0 0/33/1  SESSION_OPEN   cisco   172.19.72.182   v2
1           vty1 0/33/1  SESSION_OPEN   cisco   172.18.0.5      v2
2           vty2 0/33/1  SESSION_OPEN   cisco   172.20.10.3     v1
3           vty3 0/33/1  SESSION_OPEN   cisco   3333::50        v2

Outgoing sessions
1               0/33/1  SESSION_OPEN    cisco   172.19.72.182   v2
2               0/33/1  SESSION_OPEN    cisco   3333::50        v2

RP/0/RSP0/CPU0:router# clear ssh 0
```

関連コマンド

コマンド	説明
show ssh, （12 ページ）	ルータへの着信接続と発信接続を表示します。

sftp

セキュア FTP（SFTP）クライアントを起動するには、EXEC モードで **sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] *source-filename dest-filename* [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。 ユーザ名のあとにアットマーク（@）が必要です。
hostname:remote-filename	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。 ホスト名のあとにコロン（:）が必要です。
source-filename	SFTP の発信元（パスを含む）
dest-filename	SFTP の宛先（パスを含む）
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。 詳細については、疑問符（**?**）オンラインヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンラインヘルプを参照してください。
vrf *vrf-name*	発信元インターフェイスに対応づける VRF の名前を指定します。

コマンド デフォルト

username 引数を省略した場合、ルータのログイン名が使用されます。 *hostname* 引数を省略した場合、ファイルはローカルにあると見なされます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SFTP では、ルータとリモート ホストの間でファイルの安全な（および認証された）コピーを行うことができます。 **copy** コマンドと同様に、**sftp** コマンドは EXEC モードでしか実行できません。

ユーザ名を省略すると、ルータのログイン名がデフォルトとして使用されます。 ホスト名を省略すると、ファイルはローカルにあると見なされます。

sftp コマンドで発信元インターフェイスを指定すると、**sftp** インターフェイスが、**ssh client source-interface** コマンドで指定されたインターフェイスよりも優先されます。

ファイルの宛先がローカルパスの場合、すべての発信元ファイルがリモートホスト上になければなりません。その逆の場合も同様です。

複数の発信元ファイルが存在する場合、宛先は、すでに存在するディレクトリでなければなりません。 それ以外の場合、宛先には、ディレクトリ名または宛先ファイル名のいずれかを指定できます。 ファイルの発信元をディレクトリ名にはできません。

ファイルを複数のリモート ホストからダウンロードする場合、つまり、発信元に複数のリモートホストを指定すると、SFTP クライアントによって SSH インスタンスがホストごとに生成されます。そのため、ユーザ認証を複数回要求されることがあります。

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の例では、ユーザ *abc* がファイル *ssh.diff* を SFTP サーバ *ena-view1* から *disk0* にダウンロードします。

```
RP/0/RSP0/CPU0:router# sftp abc@ena-view1:ssh.diff disk0
```

次の例では、ユーザ *abc* が、disk 0:/sam_* で示される複数のファイルをリモート SFTP サーバ ena-view1 上の /users/abc/ にアップロードします。

```
RP/0/RSP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *run* を *disk0a:* からローカル SFTP サーバ上の *disk0:/v6copy* にダウンロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]:disk0a:/run disk0:/V6copy
Connecting to 2:2:2::2...
Password:

disk0a:/run
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (338172)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0:/V6copy

Directory of disk0:

70144       -rwx  308413      Sun Oct 16 23:06:52 2011  V6copy

2102657024 bytes total (1537638400 bytes free)
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *v6copy* を *disk0:* からローカル SFTP サーバ上の *disk0a:/v6back* にアップロードします。

```
RP/0/RSP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:

/disk0:/V6copy
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (421329)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/v6back

Directory of disk0a:

66016       -rwx  308413      Sun Oct 16 23:07:28 2011  v6back

2102788096 bytes total (2098987008 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile* を *disk0:* からローカル SFTP サーバ上の *disk0a:/sampfile_v4* にダウンロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile disk0a:/sampfile_v4
Connecting to 2.2.2.2...
Password:

disk0:/sampfile
  Transferred 986 Bytes
  986 bytes copied in 0 sec (493000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0a:/sampfile_v4

Directory of disk0a:

131520      -rwx  986         Tue Oct 18 05:37:00 2011  sampfile_v4

502710272 bytes total (502001664 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile_v4* を *disk0a:* からローカル SFTP サーバ上の *disk0:/sampfile_back* にアップロードします。

```
RP/0/RSP0/CPU0:router#sftp disk0a:/sampfile_v4 admin@2.2.2.2:disk0:/sampfile_back
Connecting to 2.2.2.2...
Password:

disk0a:/sampfile_v4
  Transferred 986 Bytes
  986 bytes copied in 0 sec (564000)bytes/sec

RP/0/RSP0/CPU0:router#dir disk0:/sampfile_back

Directory of disk0:

121765      -rwx  986         Tue Oct 18 05:39:00 2011  sampfile_back

524501272 bytes total (512507614 bytes free)
```

関連コマンド

コマンド	説明
ssh client source-interface, （21 ページ）	すべての発信SSH接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
ssh client vrf, （23 ページ）	SSH クライアントで使用される新しい VRF を設定します。

sftp（インタラクティブ モード）

ユーザがセキュア FTP（SFTP）クライアントを起動できるようにするには、EXEC モードで **sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。ユーザ名のあとにアットマーク（@）が必要です。
hostname:remote-filename	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。 ホスト名のあとにコロン（:）が必要です。
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイスタイプ。 詳細については、疑問符（**?**）オンラインヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
vrf *vrf-name*	発信元インターフェイスに対応づける VRF の名前を指定します。

コマンド デフォルト

username 引数を省略した場合、ルータのログイン名が使用されます。 *hostname* 引数を省略した場合、ファイルはローカルにあると見なされます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.9.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SFTP クライアントは、インタラクティブ モードで、ユーザがサポートされているコマンドを入力できるセキュアな SSH チャネルを作成します。 ユーザがインタラクティブ モードで SFTP クライアントを起動すると、SFTP クライアント プロセスによってセキュアな SSH チャネルが作成され、ユーザがサポートされているコマンドを入力できるエディタが開きます。

複数の要求を SFTP サーバに送信してコマンドを実行することができます。 サーバに対する「未確認」または未処理の要求に数の制限はありませんが、サーバは便宜上これらの要求をバッファリングするか、またはキューに入れる場合があります。 このため、要求の順番に論理的な順序があることがあります。

インタラクティブ モードでサポートされる UNIX ベース コマンドは次のとおりです。

- bye
- **cd** *<path>*
- **chmod** *<mode> <path>*
- exit
- **get** *<remote-path> [local-path]*
- help
- **ls** *[-alt] [path]*
- **mkdir <path>**
- **put** *<local-path> [remote-path]*
- pwd
- quit
- **rename <old-path> <new-path>**
- **rmdir <path>**
- **rm <path>**

次のコマンドはサポートされません。

- lcd、lls、lpwd、lumask、lmkdir
- ln、symlink
- chgrp、chown
- !、！コマンド
- ?
- mget、mput

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の例では、ユーザ *admin* が IPv6 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RSP0/CPU0:router#sftp admin@[2:2:2::2]

Connecting to 2:2:2::2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/admin
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/admin/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

次の例では、ユーザ *abc* が IPv4 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RSP0/CPU0:router#sftp abc@2.2.2.2
Connecting to 2.2.2.2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/abc
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

関連コマンド

コマンド	説明
ssh client source-interface, （21 ページ）	すべての発信SSH接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
ssh client vrf, （23 ページ）	SSH クライアントで使用される新しい VRF を設定します。

show ssh

ルータへのすべての着信接続と発信接続を表示するには、EXEC モードで **show ssh** コマンドを使用します。

show ssh

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

セキュア シェル（SSH）Version 1（SSHv1; SSH バージョン 1）と SSH Version 2（SSHv2; SSH バージョン 2）のすべての着信接続と発信接続を表示するには、**show ssh** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、SSH がイネーブルのときに **show ssh** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show ssh

SSH version: Cisco-2.0

id pty      location      state        userid        host           ver
---------------------------------------------------------------------------
Incoming sessions
```

```
0 vty0      0/RSP0/CPU0    SESSION_OPEN    cisco       172.19.72.182    v2
1 vty1      0/RSP0/CPU0    SESSION_OPEN    cisco       172.18.0.5       v2
2 vty2      0/RSP0/CPU0    SESSION_OPEN    cisco       172.20.10.3      v1
3 vty3      0/RSP0/CPU0    SESSION_OPEN    cisco       3333::50         v2

Outgoing sessions

1           0/RSP0/CPU0    SUSPENDED       root        172.19.72.182    v2
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *1*：*show ssh* フィールドの説明

フィールド	説明
id	着信および発信 SSH 接続のセッション ID。
pty	着信セッションに割り当てられた仮想端末ID。発信 SSH 接続の場合は Null になります。
location	着信接続の場合、SSH サーバが稼働している場所を示します。 発信接続の場合、location は、SSH セッションがどのルートプロセッサから開始されるかを示します。
state	接続の現在の SSH 状態。
userid	ルータへ、またはルータからの接続に使用される認証、許可、アカウンティング（AAA）ユーザ名
host	リモート ピアの IP アドレス
ver	接続タイプが SSHv1 と SSHv2 のいずれであるかを示します。

関連コマンド

コマンド	説明
show sessions	開いている Telnet 接続または rlogin 接続に関する情報を表示します。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。
show ssh session details, （14 ページ）	ルータへのすべての着信と発信の SSHv2 接続について、詳細を表示します。

show ssh session details

すべての着信と発信のセキュア シェル バージョン2（SSHv2）接続について詳細を表示するには、EXEC モードで **show ssh session details** コマンドを使用します。

show ssh session details

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータへの SSHv2 接続の詳細レポートを表示するには、**show ssh session details** コマンドを使用します。このレポートには、特定のセッションに選択された暗号化に関する情報が含まれます。

タスク ID

タスク ID	操作
crypto	read

例

次の出力例は、着信と発信のすべての SSHv2 接続の詳細を表示するために、**show ssh session details** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# show ssh session details

SSH version: Cisco-2.0
session     key-exchange   pubkey   incipher   outcipher    inmac     outmac
--------------------------------------------------------------------------------
```

```
Incoming Session
0           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5
Outgoing connection
1           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 2：***show ssh session details*** **フィールドの説明**

フィールド	説明
session	着信および発信 SSH 接続のセッション ID。
key-exchange	相互に認証するために両方のピアによって選択されたキー交換アルゴリズム。
pubkey	キー交換用に選択された公開キー アルゴリズム。
incipher	Rx トラフィック用に選択された暗号化。
outcipher	Tx トラフィック用に選択された暗号化。
inmac	Rx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。
outmac	Tx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。

関連コマンド

コマンド	説明
show sessions	開いている Telnet 接続または rlogin 接続に関する情報を表示します。
show ssh, （12 ページ）	ルータへのすべての着信接続と発信接続を表示します。

ssh

セキュア シェル（SSH）クライアント接続を開始し、SSH サーバへの発信接続をイネーブルにするには、EXEC モードで **ssh** コマンドを使用します。

ssh [**vrf vrf-name**] {**ipv4-address**| **ipv6-address**| **hostname**} [**username** *user-id*] [**cipher des** {**128-cbc**| **192-cbc**| **256-cbc**}][**source-interface** *type interface-path-id*][**command***command-name*]

構文の説明

ipv4-address	A:B:C:D 形式の IPv4 アドレス。
ipv6-address	X:X::X 形式の IPv6 アドレス。
hostname	リモート ノードのホスト名。 このホスト名に IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、IPv6 アドレスが使用されます。
username *user-id*	（任意）SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用するユーザ名を指定します。 ユーザ ID を省略すると、デフォルトとして現在のユーザ ID が使用されます。
cipher des	（任意）暗号スイート。 Version 1（v1; バージョン 1）接続に対してだけ有効です。 暗号スイートを **cipher des** オプションで指定しなければ、トリプル データ暗号規格（トリプル DES）がデフォルトの暗号スイートとして使用されます。 SSHv2 は、3DES だけをサポートします（プロトコルは、128 ビット以上の暗号だけをサポートします）。 SSHv1 は、DES（56 ビット）と 3DES（168 ビット）の両方の暗号スイートをサポートします。
source interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。 詳細については、疑問符（**?**）オンライン ヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
command	（任意）リモート コマンドを指定します。 このキーワードを追加すると、SSHv2 サーバにインタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行するよう要求します。

command name	リモート コマンド キーワードの名前。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 3.9.1	**command** キーワードのサポートが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

発信クライアント接続を行うには、**ssh** コマンドを使用します。 SSH クライアントにより、リモート ピアへの SSHv2 接続が試みられます。 リモート ピアで SSHv1 サーバしかサポートされていない場合、リモート サーバへの SSHv1 接続が内部生成されます。 リモート ピアのバージョンの検出と適切なクライアント接続の生成のプロセスは、ユーザからは見えません。

ssh コマンドで **source-interface** キーワード を指定すると、**ssh** インターフェイスが **ssh client source-interface**コマンド（ssh client source-interface, （21 ページ））で指定されたインターフェイスよりも優先されます。

SSHv2 サーバがインタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行できるようにするには、**command** キーワードを使用します。

タスク ID

タスク ID	操作
crypto	execute
basic-services	execute

例

次の出力例は、発信 SSH クライアント接続をイネーブルにするために、**ssh** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# sshremote-host username userabc

Password:
Remote-host>
```

関連コマンド

コマンド	説明
show ssh, （12 ページ）	ルータへのすべての着信接続と発信接続を表示します。

ssh client knownhost

サーバ公開キー（pubkey）を認証するには、グローバル コンフィギュレーション モードで **ssh client knownhost** コマンドを使用します。 サーバ pubkey の認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh client knownhost device:/**filename**

no ssh client knownhost device:/**filename**

構文の説明

device:/ *filename*	ファイル名の完全なパス（たとえば、slot0:/server_pubkey）。 コロン（:）とスラッシュ（/）が必要です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバ *pubkey* は、クライアント側で全員が知る公開キーとキーのオーナーしか知らない秘密キーの 2 つのキーを使用する暗号化システムです。 証明書がない場合、サーバ pubkey は、アウトオブバンドセキュア チャネルを介してクライアントに転送されます。 クライアントでは、この pubkey がローカルデータベースに保存され、セッション構築ハンドシェイクのキー ネゴシエーションの初期段階にサーバから提供されたキーと比較されます。 キーが一致しない、またはクライアントのローカル データベースにキーが見つからない場合、セッションを許可するか拒否するかを確認するプロンプトが表示されます。

サーバ pubkey が、アウトオブバンド セキュア チャネルを介して最初に取得されたときに、ローカル データベースに保存されることが動作の前提条件になっています。 このプロセスは、UNIX 環境でセキュア シェル（SSH）の実装に採用されている現行のモデルと同じです。

タスク ID

タスク ID	操作
crypto	read, write

例

次の出力例は、**ssh client knownhost** コマンドを実行した結果です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RSP0/CPU0:host1# exit
RP/0/RSP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

すべての発信セキュア シェル（SSH）接続に選択されたインターフェイスの発信元 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **ssh client source-interface** コマンドを使用します。 指定したインターフェイス IP アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh client source-interface *type interface-path-id*

no ssh client source-interface *type interface-path-id*

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。

コマンド デフォルト

発信元インターフェイスは使用されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

指定したインターフェイスの IP アドレスをすべての発信 SSH 接続に対して設定するには、**ssh client source-interface** コマンドを使用します。 このコマンドを設定しなければ、ソケットが接続されるときの TCP の発信元 IP アドレスは、使用される発信インターフェイスに基づいて選択されます。つまり、サーバに到達するために必要なルートに基づきます。 このコマンドは、SSH

セッションだけでなく、セキュア シェル ファイル転送プロトコル（SFTP）セッション上でも発信シェルに適用されます。これらのセッションでは、転送に ssh クライアントが使用されます。

source-interface の設定は、同じアドレス ファミリ内のリモート ホストへの接続にしか影響しません。 システム データベース（Sysdb）により、コマンドで指定されたインターフェイスに、対応する（同じファミリ内の）IP アドレスが設定されているかどうか検証されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、すべての発信 SSH 接続に対して管理イーサネット インターフェイスの IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client source-interface MgmtEth 0/RSP0/CPU0/0
```

ssh client vrf

SSH クライアントで使用される新しい VRF を設定するには、グローバル コンフィギュレーション モードで **ssh client vrf** コマンドを使用します。 指定した VRF を削除するには、このコマンドの **no** 形式を使用します。

ssh client vrf *vrf-name*

no ssh client vrf *vrf-name*

構文の説明

vrf-name	SSH クライアントが使用する VRF の名前を指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.8.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSH クライアントには VRF を 1 つだけ設定できます。

特定の VRF が SSH クライアント用に設定されていない場合、ssh client knownhost, （19 ページ）、ssh client source-interface, （21 ページ） などの他の SSH クライアント関連のコマンドを適用する際にデフォルトの VRF が使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、指定された VRF から起動するように設定されている SSH クライアントの例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh client vrf green
```

関連コマンド

コマンド	説明
ssh client dscp <0 ～ 63 の値>	SSH クライアントは発信パケットの DSCP 値の設定をサポートします。 設定されていない場合、（クライアントとサーバ両方の）パケット内に設定されるデフォルト DSCP 値は 16 です。

ssh server

セキュア シェル（SSH）サーバを起動し、そのサーバで使用するために 1 つ以上の VRF を設定するには、グローバル コンフィギュレーション モードで **ssh server** コマンドを使用します。 SSH サーバが指定された VRF の接続をこれ以上受信しないようにするには、このコマンドの **no** 形式を使用します。

ssh server [**vrf vrf-name**| **v2**]

no ssh server [**vrf vrf-name**| **v2**]

構文の説明

vrf *vrf-name*	SSH サーバが使用する VRF の名前を指定します。 VRF の最大長は 32 文字です。 （注） VRF が指定されていない場合、デフォルトの VRF が使用されます。
v2	SSH サーバ バージョンを強制的に 2 だけにします。

コマンド デフォルト

デフォルトの SSH サーバ バージョンは 2（SSHv2）です。着信 SSH クライアント接続が SSHv1 に設定されると、1（SSHv1）になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 3.8.0	**vrf** キーワードがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSH サーバは少なくとも 1 つの VRF に対して設定する必要があります。 デフォルトを含め、設定済みのすべての VRF を削除すると、SSH サーバのプロセスは停止します。 **ssh client knownhost**、**ssh client source-interface** などの他のコマンドを適用する際に SSH クライアントに特定の VRF を設定していない場合、デフォルトの VRF が使用されます。

SSH サーバは、ポート 22 で着信クライアント接続を待ち受けます。 このサーバでは、IPv4 と IPv6 の両方のアドレス ファミリに対してセキュア シェル バージョン 1（SSHv1）と SSHv2 の両方の着信クライアント接続が処理されます。 セキュア シェル バージョン 2 の接続だけを許可するには、ssh server v2, （33 ページ） コマンドを使用します。

SSH サーバが起動し、稼働中であることを確認するには、**show process sshd** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、SSH サーバが起動され、VRF「green」の接続を受信します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server
```

関連コマンド

コマンド	説明
show processes	SSH サーバに関する情報を表示します。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。
ssh server v2, （33 ページ）	SSH サーバ バージョンを強制的に 2（SSHv2）だけにします。
ssh server dscp <0 ～ 63 の値>	SSH サーバは発信パケットの DSCP 値の設定をサポートします。 設定されていない場合、（クライアントとサーバ両方の）パケット内に設定されるデフォルト DSCP 値は 16 です。

ssh server logging

SSH サーバのロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **ssh server logging** コマンドを使用します。 SSH サーバのロギングを停止するには、このコマンドの **no** 形式を使用します。

ssh server logging

no ssh server logging

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.8.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSHv2 クライアント接続だけが許可されます。

ロギングを設定すると、次のメッセージが表示されます。

- Warning: The requested term-type is not supported
- SSH v2 connection from %s succeeded (*user:%s, cipher:%s, mac:%s, pty:%s*)

警告メッセージは、サポートされていない端末タイプを使用して接続しようとした場合に表示されます。 Cisco IOS XR ソフトウェアを実行しているルータがサポートするのは vt100 端末タイプだけです。

2 番めのメッセージでログインに成功したことを確認します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、SSH サーバのロギングの開始例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server logging
```

関連コマンド

コマンド	説明
ssh server, （25 ページ）	SSH サーバを開始します。

ssh server rate-limit

1 分間あたりに許可される着信セキュア シェル（SSH）接続要求の数を制限するには、グローバル コンフィギュレーション モードで **ssh server rate-limit** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server rate-limit *rate-limit*

no ssh server rate-limit

構文の説明

rate-limit	1 分間あたりに許可される着信 SSH 接続要求の数。 範囲は 1 ～ 120 です。

コマンド デフォルト

rate-limit：1 分間あたり 60 個の接続要求

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

コマンド履歴

リリース	変更内容
リリース 2.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

着信 SSH 接続要求を設定レートに制限するには、**ssh server rate-limit** コマンドを使用します。 このレート制限を超える接続要求は、SSH サーバから拒否されます。 レート制限の変更は、確立している SSH セッションには影響しません。

たとえば、*rate-limit* 引数を 30 に設定すると、1 分間で 30 個の要求が許可されます。より正確には、接続の行われる間隔が 2 秒に制限されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、着信 SSH 接続要求の制限を 1 分あたり 20 に設定する方法です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

許可される同時着信セキュア シェル（SSH）セッションの数を設定するには、グローバル コンフィギュレーション モードで **ssh server session-limit** コマンドを使用します。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server session-limit *sessions*

no ssh server session-limit

構文の説明

sessions	ルータで許可される着信 SSH セッションの数。 有効な範囲は 1 ～ 1024 です。

コマンド デフォルト

sessions：ルータあたり 64

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

許可される同時着信 SSH 接続の制限を設定するには、**ssh server session-limit** コマンドを使用します。 発信接続はこの制限に含まれません。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、着信 SSH 接続の制限を 50 に設定する方法です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh server session-limit 50
```

ssh server v2

SSH サーバ バージョンを強制的に 2（SSHv2）だけにするには、グローバル コンフィギュレーション モードで **ssh server v2** コマンドを使用します。 SSHv2 の SSH サーバを停止するには、このコマンドの **no** 形式を使用します。

ssh server v2

no ssh server v2

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

SSHv2 クライアント接続だけが許可されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例は、SSH サーバ バージョンを SSHv2 に限定して開始する方法です。

```
 RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)# ssh server v2
```

関連コマンド

ssh timeout

認証、許可、アカウンティング（AAA）ユーザ認証のタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。 タイムアウト値をデフォルト時間に設定するには、このコマンドの **no** 形式を使用します。

ssh timeout *seconds*

no ssh timeout *seconds*

構文の説明

seconds	ユーザ認証の時間（秒単位）。 範囲は 5 ～ 120 です。

コマンド デフォルト

seconds：30

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

AAA に対するユーザ認証のタイムアウト値を設定するには、**ssh timeout** コマンドを使用します。 設定された時間内にユーザ自身の認証が AAA に対してできないと、接続は中断されます。 値を設定しなければ、30 秒のデフォルト値が使用されます。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、AAA ユーザ認証のタイムアウト値が 60 秒に設定されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# ssh timeout 60
```