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、『*System Security Configuration Guide for Cisco NCS 5000 Series Routers*』の「Implementing Secure Shell」の章を参照してください。

（注） 現在、デフォルトの VRF のみがサポートされています。VPNv4、VPNv6、および VPN ルーティング/転送（VRF）アドレス ファミリは、今後のリリースでサポートされます。

clear ssh

着信または発信セキュア シェル（SSH）接続を終了するには、**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** コマンドの出力での表示のとおりに、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

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

clear ssh コマンドを使用して着信 SSH 接続または発信 SSH 接続を切断します。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	動作
crypto	実行

例

次に、**show ssh** コマンドを使用して、ルータに対するすべての着信接続および発信接続を表示します。その後で、**clear ssh** コマンドを使用し、ID 番号 0 で着信セッションを終了します。

```
RP/0/RP0/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/RP0/CPU0:router# clear ssh 0
```

次に、リリース 6.0 以降に適用される **clear ssh** の出力を示します。

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0


id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1               0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password

RP/0/RP0/CPU0:router# clear ssh 0
```

clear netconf-yang agent session

指定した netconf エージェント セッションをクリアするには、EXEC モードで **clear netconf-yang agent session** を使用します。

clear netconf-yang agent session *session-id*

構文の説明

session-id	クリアする必要があるセッション ID。

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 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

show netconf-yang clients コマンドを使用して必要なセッション ID を取得できます。

タスク ID

タスク ID	動作
config-services	読み取り、書き込み

例

次に、**clear netconf-yang agent session** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  clear netconf-yang agent session 32125
```

netconf-yang agent ssh

SSH（セキュア シェル）で netconf エージェント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 **netconf-yang agent ssh** コマンドを使用します。netconf 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。

netconf-yang agent ssh

nonetconf-yang agent ssh

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

グローバル設定

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

現在、SSH は Netcof でサポートされている転送方式です。

タスク ID

タスク ID	動作
config-services	読み取り、書き込み

例

次に、**netconf-yang agent ssh** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  netconf-yang agent ssh
```

sftp

セキュア FTP（SFTP）クライアントを起動するには、**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-filenam*e	（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てください。
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**） ルータ上に現在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するには、XR EXEC モードで **showinterfaces** コマンドを使用します。 ルータの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 引数を指定しない場合は、ルータのログイン名が使用されます。*hostname* 引数を指定しない場合は、ファイルがローカルと見なされます。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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 XR EXEC モードでのみ呼び出すことができます。

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。

送信元インターフェイスが **sftp** コマンド内に指定されている場合、**sftp** インターフェイスは **ssh client source-interface** コマンド内に指定されている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	動作
crypto	実行
basic-services	実行

例

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

```
RP/0/RP0/CPU0:router#sftp abc@ena-view1:ssh.diff disk0
```

次の例では、ユーザ *abc* が disk 0:/sam_* から ena-view1 というリモート SFTP サーバ上の /users/abc/ に複数のファイルをアップロードします。

```
RP/0/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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/RP0/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)
```

sftp（インタラクティブ モード）

ユーザをイネーブルにして、セキュア FTP（SFTP）クライアントを起動するには、**sftp** コマンドを使用します。

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

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てください。
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） ルータ上に現在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するには、XR EXEC モードで **showinterfaces** コマンドを使用します。 ルータの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

username 引数を指定しない場合は、ルータのログイン名が使用されます。*hostname* 引数を指定しない場合は、ファイルがローカルと見なされます。

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
crypto	実行
basic-services	実行

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/RP0/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/RP0/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>
```

show netconf-yang clients

netconf-yangに関するクライアントの詳細情報を表示するには、XR EXECモードで**show netconf-yang clients** コマンドを使用します。

show netconf-yang clients

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
config-services	読み取り

例

次に、**show netconf-yang clients** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  sh netconf-yang clients
Netconf clients
client session ID|   NC version|    client connect time|        last OP time|        last
OP type|    <lock>|
 22969|                     1.1|          0d  0h  0m  2s|            11:11:24|
close-session|        No|
 15389|                     1.1|          0d  0h  0m  1s|            11:11:25|
get-config|        No|
```

表 *1*：フィールド説明

フィールド名	説明
Client session ID	割り当てられたセッション ID
NC version	hello メッセージでアドバタイズされる Netconf クライアントのバージョン
Client connection time	クライアントが接続されてからの経過時間
Last OP time	最終操作時刻
Last OP type	最終操作タイプ
Lock（yes または no）	設定データストアにセッションのロックが保持されているかどうかを確認します。

show netconf-yang statistics

netconf-yangに関する統計詳細情報を表示するには、システム管理EXECモードで**show netconf-yang statistics** コマンドを使用します。

show netconf-yang statistics

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
config-services	読み取り

例

次に、**show netconf-yang statistics** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  sh netconf-yang statistics
Summary statistics
                          # requests|             total time|   min time per request|   max
 time per request|   avg time per request|
other                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
close-session                      4|       0h  0m  0s   3ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
kill-session                       0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-schema                         0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get                                0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
```

```
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-config                        1|       0h  0m  0s   1ms|       0h  0m  0s   1ms|
 0h  0m  0s   1ms|       0h  0m  0s   1ms|
edit-config                       3|       0h  0m  0s   2ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
commit                            0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
cancel-commit                     0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
lock                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
unlock                            0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
discard-changes                   0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
validate                          0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
xml parse                         8|       0h  0m  0s   4ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
netconf processor                 8|       0h  0m  0s   6ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
```

表 *2*：フィールド説明

フィールド名	説明
Requests	特定のタイプの処理済みの要求の総数
Total time	特定のタイプのすべての要求の合計処理時間
Min time per request	特定のタイプの要求の最小処理時間
Max time per request	特定のタイプの要求の最大処理時間
Avg time per request	要求タイプの平均処理時間

show ssh

ルータに対するすべての発着信接続を表示するには、**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または引数はありません。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

show ssh コマンドを使用して、セキュア シェル（SSH）バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）のすべての発着信接続を表示します。

タスク ID

タスク ID	動作
crypto	読み取り

例

次に、SSH がイネーブルになっている場合の **show ssh** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# show ssh

SSH version : Cisco-2.0

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

Outgoing sessions
1         0/3/CPU0    SESSION_OPEN    lab     12.22.57.     v2        password
```

```
2          0/3/CPU0     SESSION_OPEN    lab      12.22.57.75   v2         keyboard-interactive
```

次に、IOS-XR 6.0 リリース以降に適用される **show ssh** コマンドの出力を示します。

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0

id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1              0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password
```

次の表に、この出力で表示される重要フィールドの説明を示します。

表 *3*：*show ssh* 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。
chan	着信（v2）SSH接続のチャネルID。SSH v1 セッションについては NULL。
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	着信接続用のSSHサーバの場所を指定します。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

フィールド	説明
ver	接続タイプが SSHv1 と SSHv2 のいずれであるかを示します。
authentication	ユーザが選択した認証方式のタイプを指定します。
connection type	この接続で実行されるアプリケーション（コマンドライン インターフェイス、リモート コマンド、SCP、SFTP サブシステム、または Netconf サブシステム）を指定します。

show ssh session details

セキュア シェル バージョン2（SSHv2）のすべての発着信接続に関する詳細情報を表示するには、**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または引数はありません。

コマンド デフォルト

なし

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

show ssh session details コマンドを使用して、ルータに対する SSHv2 接続に関する特定のセッションに選択した暗号を含む詳細レポートを表示します。

タスク ID

タスク ID	動作
crypto	読み取り

例

次に、SSHv2 のすべての発着信接続に関する詳細を表示する **show ssh session details** コマンドによる出力の例を示します。

```
RP/0/RP0/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
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 *4*：*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。

ssh

セキュア シェル（SSH）クライアント接続を開始し、SSHサーバへのアウトバウンド接続をイネーブルにするには、**ssh** コマンドを使用します。

ssh {**ipv4-address**| **ipv6-address**| **hostname**} [**username** *user-id*] [**cipher aes** {**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。
cipheraes	（任意）SSH クライアント接続の暗号化として Advanced Encryption Standard（AES）を指定します。 （注） 管理者によって特定の暗号化が指定されていない場合、クライアントは互換性を確保するためにデフォルトとしてトリプルDESを提案します。
128-CBC	CBC モードの 128 ビット キー。
192-CBC	CBC モードの 192 ビット キー。
256-CBC	CBC モードの 256 ビット キー。
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てください。
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） ルータ上に現在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するには、XR EXEC モードで **showinterfaces** コマンドを使用します。 ルータの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、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、実行するように SSHv2 に要求します。

コマンド デフォルト

3DES cipher

コマンド モード

XR EXEC モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ssh コマンドを使用して、アウトバウンド クライアント接続を行います。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。

VRF が **ssh** コマンドに指定されている場合は、**ssh** インターフェイスが ssh client source-interface, （28 ページ）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。

cipher aes を設定した場合は、指定した 1 つ以上のキーサイズを含めて、SSH サーバへの要求の一部として SSH クライアントが提案を行います。SSH サーバは、サーバがサポートする暗号化およびクライアントの提案に基づいて最適な暗号化を選択します。

（注） AES 暗号化アルゴリズムは、SSHv1 サーバおよびクライアントではサポートされていません。SSHv2 クライアントから SSHv1 サーバに送信された AES 暗号の要求はすべて無視されます。代わりにサーバではトリプル DES を使用します。

SSH を実行するには VRF が必要ですが、これはデフォルト VRF またはユーザによって指定された VRF のいずれかです。ssh client source-interface, （28 ページ）または ssh client knownhost, （26 ページ）コマンドの設定時に VRF を指定しなかった場合は、デフォルトの VRF が使用されます。

command キーワードを使用して、SSHv2 サーバをイネーブルにし、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、実行します。

タスク ID

タスク ID	動作
crypto	実行
basic-services	実行

例

次に、アウトバウンド SSH クライアント接続をイネーブルにする **ssh** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# ssh vrf green  username userabc

Password:
Remote-host>
```

ssh client knownhost

サーバ パブリック キー（pubkey）を認証するには、**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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
crypto	読み取り、書き込み

例

次に、**ssh client knownhost** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/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/RP0/CPU0:host1# exit
RP/0/RP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

すべての発信セキュア シェル（SSH）接続に選択したインターフェイスの送信元 IP アドレスを指定するには、**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の 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） ルータ上に現在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するには、**showinterfaces** コマンドを使用します。 ルータの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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ssh client source-interface コマンドを使用して、すべての発信 SSH 接続に指定したインターフェイスの IP アドレスを設定します。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	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client source-interface MgmtEth 0/RP0/CPU0/0
```

ssh server

セキュア セル（SSH）サーバを起動状態にし、1 つ以上の VRF を使用できるようにするには、**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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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** や **ssh client source-interface** などの他のコマンドを適用する際に SSH クライアントに対して特定の VRF を設定しない場合は、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, （37 ページ）コマンドを使用します。

SSH サーバが起動し、実行してい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	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh serverserver vrf green
```

ssh server logging

SSH サーバのロギングをイネーブルにするには、**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または引数はありません。

コマンド デフォルト

なし

コマンド モード

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
crypto	読み取り、書き込み

例

次に、SSH サーバのロギングの開始例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server logging
```

ssh server rate-limit

1 分間に許可する着信セキュア シェル（SSH）接続要求の数を制限するには、**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。 1 分間あたりの再試行回数を 60 に設定すると、基本的に 1 秒間に 1 回が許可されることになります。2 つの異なるコンソールから同時に 2 つのセッションをセットアップする場合、そのうちの 1 つのレートは制限されます。これは、SSH サーバへの接続試行であり、インターフェイス/ユーザ名などのバインドはベースになりません。したがって、30 という値は 2 秒ごとに 1 セッションということになります。

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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ssh server rate-limit コマンドを使用して、着信 SSH 接続要求を設定済みのレートに制限します。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 分間に 30 の要求が許可されます。また、より厳密には、接続間に 2 秒のインターバルが適用されることになります。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

許容可能な同時着信セキュア シェル（SSH）セッションの数を設定するには、**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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ssh server session-limit コマンドを使用して、許容可能な同時着信 SSH 接続を設定します。発信接続はこの制限に含まれません。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server session-limit 50
```

ssh server v2

SSH サーバのバージョンを 2（SSHv2）に限定するには、**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または引数はありません。

コマンド デフォルト

なし

コマンド モード

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

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	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)# ssh server v2
```

ssh server netconf

netconf SSH サーバにポートを設定するには、XR コンフィギュレーション モードで **ssh server netconf port** を使用します。設定済みのポートの netconf 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 server netconf[**port***port-number*]

nossh server netconf[**port***port-number*]

構文の説明

port-number	netconf SSH サーバのポート番号（デフォルトのポート番号は 830）。

コマンド デフォルト

デフォルトのポート番号は 830 です。

コマンド モード

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次に、**ssh server netconf port** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  ssh server netconf port 830
```

ssh timeout

認証、認可、およびアカウンティング（AAA）に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。タイムアウト値をデフォルトの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

XR コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

ssh timeout コマンドを使用して、AAA に対してユーザ認証のタイムアウト値を設定します。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	動作
crypto	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh timeout 60
```