ip ssh ～ ipv6 tacacs source-interface

ip ssh

ルータ上で Secure Shell（SSH）コントロール パラメータを設定するには、グローバル コンフィギュレーション モードで **ip ssh** 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。

ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

構文の説明

timeout	（任意）SSH クライアントが応答するまでルータが待機する時間間隔。 この設定は、SSH ネゴシエーション フェーズに適用されます。 EXEC セッションが開始すると、vty に設定された標準のタイムアウトが適用されます。デフォルトでは、定義された 5 つの vty（0 ～ 4）があります。したがって、5 つのターミナル セッションが可能です。 SSH でシェルが実行されると、vty タイムアウトが始動します。 vty タイムアウトのデフォルトは 10 分です。
seconds	（任意）最大 120 秒のタイムアウト切断までの秒数。 デフォルトは 120 秒です。
authentication- retries	（任意）インターフェイスがリセットされるまでの試行回数。
integer	（任意）最大 5 回の認証再試行の再試行回数。デフォルトは 3 です。

コマンド デフォルト

SSH コントロール パラメータはルータのデフォルトの値に設定されます。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(5)S	このコマンドが導入されました。

リリース	変更内容
12.1(1)T	このコマンドが、Cisco IOS Release 12.1(1)T に統合されました。
12.2(17a)SX	このコマンドが、Cisco IOS Release 12.2(17a) SX に統合されました。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。
Cisco IOS XE Release 2.4	このコマンドが、Cisco ASR 1000 シリーズ ルータに実装されました。

使用上のガイドライン

ルータ上でSSHを設定する前に、**crypto key generate rsa** コマンドを使用してSSHサーバをイネーブルにする必要があります。

例

次に、ルータ上で SSH コントロール パラメータを設定する例を示します。

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh dh min size

Secure Shell（SSH）サーバ上でモジュラス サイズを設定するには、特権 EXEC モードで **ip ssh dh min size** コマンドを使用します。 設定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。

ip ssh dh min size [*number*]

no ip ssh dh min size

構文の説明

number	（任意）キー サイズの最小ビット数。 デフォルトは 1024 です。

コマンド デフォルト

ビット キーのサポートはディセーブルです。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.4(20)T	このコマンドが導入されました。
15.1(2)S	このコマンドが Cisco IOS Release 15.1(2)S に統合されました。

使用上のガイドライン

CLI がクライアント側またはサーバ側から正常に解析されたことを確認するには、**ip ssh dh min size** コマンドを使用します。

例

次に、最小モジュラス サイズを 2048 ビットに設定する例を示します。

```
Router> enable
Router# ip ssh dh min size 2048
```

関連コマンド

コマンド	説明
show ip ssh	SSH サーバ接続のステータスを表示します。

ip ssh dscp

Secure Shell（SSH）設定に対して設定できる IP DiffServ コード ポイント（DSCP）値を指定するには、グローバル コンフィギュレーション モードで **ip ssh dscp** 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。

ip ssh dscp *number*

no ip ssh dscp *number*

構文の説明

number	設定できる値。 デフォルト値は 0（ゼロ）です。 • *number*：0 ～ 63。

コマンド デフォルト

IP DSCP 値は指定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.4(20)S	このコマンドが導入されました。
12.2SR	このコマンドは、Cisco IOS Release 12.2SR トレインでサポートされます。特定の 12.2SR トレインにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。特定の 12.2SX トレインにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。
12.4(22)T	このコマンドが Cisco IOS Release 12.4(22)T に統合されました。

使用上のガイドライン

IP DSCP 値は、いずれかの端で生成された SSH トラフィックの SSH クライアントおよび SSH サーバの両方で設定できます。

例

次に、DSCP 値を 35 に設定する例を示します。

```
Router(config)# ip ssh dscp 35
```

関連コマンド

コマンド	説明
ip ssh precedence	設定できる IP precedence 値を指定します。

ip ssh pubkey-chain

SSH サーバ上でのユーザおよびサーバ認証の Secure Shell RSA（SSH-RSA）キーを設定するには、グローバル コンフィギュレーション モードで **ip ssh pubkey chain** コマンドを使用します。 SSH サーバ上でのユーザおよびサーバ認証の SSH-RSA キーを削除するには、このコマンドの **no** 形式を使用します。

ip ssh pubkey-chain

no ip ssh pubkey-chain

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SSH-RSA キーは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.1(1)S	このコマンドが Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

SSH サーバおよびユーザの公開キー認証を確保するには、**ip ssh pubkey chain** コマンドを使用します。

例

次に、公開キー生成をイネーブルにする例を示します。

```
Router(config)# ip ssh pubkey-chain
```

関連コマンド

コマンド	説明
ip ssh stricthostkeycheck	SSH サーバでの厳密なホスト キー チェックをイネーブルにします。

ip ssh stricthostkeycheck

Secure Shell（SSH）サーバ上での厳密なホスト キー チェック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 **ip ssh stricthostcheck** コマンドを使用します。 厳密なホスト キー チェック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。

ip ssh stricthostkeycheck

no ip ssh stricthostkeycheck

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

SSH サーバでの厳密なホスト キー チェックはイネーブルではありません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
15.0(1)M	このコマンドが導入されました。
15.1(1)S	このコマンドが Cisco IOS Release 15.1(1)S に統合されました。

使用上のガイドライン

SSH サーバ側の厳密なチェックを確保するには、**ip ssh stricthostkeycheck** コマンドを使用します。 **ip ssh stricthostkeycheck** コマンドを設定すると、すべてのサーバが認証されます。

（注） このコマンドは、SSH バージョン 1 では使用できません。

- **ip ssh pubkey-chain** コマンドが設定されていない場合、**ip ssh stricthostkeycheck** コマンドを使用すると、SSH バージョン 2 の接続障害につながります。

例

次に、厳密なホスト キー チェックをイネーブルにする例を示します。

```
Router(config)# ip ssh stricthostkeycheck
```

関連コマンド

コマンド	説明
ip ssh pubkey-chain	SSH サーバ上でのユーザおよびサーバ認証の SSH-RSA キーを設定します。

ip ssh version

ルータで実行する Secure Shell（SSH）のバージョンを指定するには、グローバル コンフィギュレーション モードで **ip ssh version** コマンドを使用します。 設定された SSH バージョンをディセーブルにし、互換モードに戻るには、このコマンドの **no** 形式を使用します。

ip ssh version [**1**| **2**]

no ip ssh version [**1**| **2**]

構文の説明

1	（任意）ルータは SSH バージョン 1 のみを実行します。
2	（任意）ルータは SSH バージョン 2 のみを実行します。

コマンド デフォルト

このコマンドを設定しない場合、SSH は互換モードで動作します。つまり、バージョン 1 とバージョン 2 の両方がサポートされます。

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
12.3(4)T	このコマンドが導入されました。
12.3(2)XE	このコマンドが、Cisco IOS Release 12.3(2)XE に統合されました。
12.2(25)S	このコマンドが、Cisco IOS Release 12.2(25)S に統合されました。
12.3(7)JA	このコマンドが、Cisco IOS Release 12.3(7)JA に統合されました。
12.0(32)SY	このコマンドが、Cisco IOS Release 12.0(32)SY に統合されました。
12.4(20)T	このコマンドが、Cisco IOS Release 12.4(20)T に統合されました。

使用上のガイドライン

ルータが誤ってセキュリティ レベルの低い SSH バージョン 1 接続を確立しないようにするには、**2** キーワードを指定してこのコマンドを使用できます。

例

次に、SSH バージョン 1 のサポートのみを設定する例を示します。

```
Router (config)# ip ssh version 1
```

次に、SSH バージョン 2 のみを設定する例を示します。

```
Router (config)# ip ssh version 2
```

次に、SSH バージョン 1 および SSH バージョン 2 を設定する例を示します。

```
Router (config)# no ip ssh version
```

関連コマンド

コマンド	説明
debug ip ssh	SSH のデバッグ メッセージを表示します。
disconnect ssh	ルータで SSH 接続を終了します。
ip ssh	ルータで SSH コントロール パラメータを設定します。
ip ssh rsa keypair-name	SSH 接続に使用する RSA キー ペアを指定します。
show ip ssh	ルータの SSH 接続を表示します。

ip verify unicast reverse-path

（注） このコマンドは、Cisco IOS Release 12.0(15)S で有効な **ip verify unicast source reachable-via** コマンドに置き換えられました。 **ip verify unicast source reachable-via** コマンドは、非対称ルーティングのサポートなどの高い柔軟性と機能を実現し、すべてのリバース パス転送の実装において使用する必要があります。 **ip verify unicast reverse-path** コマンドは引き続きサポートされます。

ユニキャスト リバース パス転送（ユニキャスト RPF）をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip verify unicast reverse-path** コマンドを使用します。 ユニキャスト RPF 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。

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

構文の説明

list	（任意）次の範囲の番号付きアクセス コントロール リスト（ACL）を指定します。 • 1 ～ 99（IP 標準アクセス リスト） • 100 ～ 199（IP 拡張アクセス リスト） • 1300 ～ 1999（IP 標準アクセス リスト、拡張範囲） • 2000 ～ 2699（IP 拡張アクセス リスト、拡張範囲）

コマンド デフォルト

ユニキャスト RPF はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
11.1(CC) 12.0	このコマンドが導入されました。 このコマンドは Cisco IOS Release 11.2 または Cisco IOS Release 11.3 には含まれません。
12.1(2)T	*list* 引数を使用した ACL のサポートを追加しました。 ドロップまたは抑制されたパケットのインターフェイス単位の統計情報を追加しました。
12.0(15)S	**ip verify unicast source reachable-via** コマンドにより、このコマンドが置き換えられ、**allow-default**、**allow-self-ping**、**rx**、および **any** のキーワードが **ip verify unicast source reachable-via** コマンドに追加されました。
12.1(8a)E	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.1（8a）E に統合されました。
12.2(14)S	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(14)SX	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(14)SX に統合されました。
12.2(33)SRA	**ip verify unicast reverse-path** コマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。

使用上のガイドライン

ルータが受信した変造または偽造（スプーフィング）された IP 送信元アドレスによって発生する問題を軽減するには、**ip verify unicast reverse-path interface** コマンドを使用します。 変造または偽造された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づくサービス拒否（DoS）攻撃を示している可能性があります。

インターフェイスでユニキャスト RPF をイネーブルにすると、ルータはそのインターフェイスで受信されるすべてのパケットを検査します。 ルータの確認により、送信元アドレスが転送情報ベース（FIB）で表示されること、およびパケットを受信したインターフェイスと一致することが確保されます。 ルックアップは FIB の存在に依存するため、この「後方参照」機能はシスコ エクスプレス フォワーディングがルータでイネーブルになっている場合にだけ使用可能です。 シスコ エクスプレス フォワーディングでは、その動作の一部として FIB が生成されます。

ユニキャスト RPF を使用するには、ルータでシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングをイネーブルにします。 シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はあ

りません。 シスコ エクスプレス フォワーディングがルータ上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

（注） ルータでシスコ エクスプレス フォワーディングをグローバルに設定することが非常に重要です。 ユニキャスト RPF は、シスコ エクスプレス フォワーディングがないと動作しません。

（注） ユニキャスト RPF は入力機能であり、入力方向においてのみルータのインターフェイスに適用されます。

ユニキャスト リバース パス転送機能は、ルータ インターフェイスで受信されたパケットが、パケットの送信元への最良リターン パスのいずれかに到達しているかどうかを確認します。 この機能は、シスコ エクスプレス フォワーディング テーブルで逆ルックアップを実行することで、この処理を行います。 ユニキャスト RPF がパケットのリターン パスを見つけることができない場合、ユニキャスト RPF は、ACL がユニキャスト リバース パス転送コマンドで指定されているかどうかに応じてパケットをドロップまたは転送できます。 コマンドで ACL を指定し、パケットがユニキャスト RPF の確認に失敗した場合にのみ、ACL を確認して（ACL で deny ステートメントを使用して）パケットをドロップするか、（ACL で permit ステートメントを使用して）転送するかを参照します。 パケットがドロップされるか転送されるかにかかわらず、パケットは、ユニキャスト RPF ドロップのグローバル IP トラフィック統計情報とユニキャスト RPF のインターフェイス統計情報でカウントされます。

ACL がユニキャスト リバース パス転送コマンドで指定されていない場合、ルータは偽造または変造されたパケットをただちにドロップし、ACL ロギングは行われません。 ルータおよびインターフェイス ユニキャスト RPF カウンタが更新されます。

ユニキャスト RPF イベントは、ユニキャスト リバース パス転送コマンドで使用する ACL エントリのロギング オプションを指定することでロギングできます。 ログ情報を使用して、送信元アドレスや時間など、攻撃に関する情報を収集できます。

ネットワークで RPF を使用する場所

ユニキャスト RPF は、有効な送信元ネットワーク（FIB に含まれているネットワーク）からのパケットを 1 つのパスにおいてのみ許可するインターフェイスで使用できます。 有効なネットワークが着信インターフェイスによってスイッチングされる限り、ユニキャスト RPF は、ルータに特定のネットワークへの複数のパスがある場合にも使用できます。 無効なネットワークのパケットはドロップされます。 たとえば、インターネット サービス プロバイダー（ISP）ネットワークのエッジにあるルータには、対称リバース パスが設定されている可能性があります。 さらに、重みやローカル プリファレンスなどの任意のボーダー ゲートウェイ プロトコル（BGP）属性を使用して、対称ルーティングが実現されていることを条件として、ユニキャスト RPF を特定のマルチホームの状況において適用できる場合もあります。

ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在し、ルーティング コスト（ホップ カウント、重みなど）に関して他のパスと同等で、ルートが FIB に存在する場合、ユニキャスト RPF は機能します。 ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

たとえば、ISP のネットワークのエッジにあるルータは、ISP ネットワークのコアにあるルータよりも対称リバースパスを持つ可能性が高くなります。ISP ネットワークのコアにあるルータでは、ルータからの最良の転送パスがルータへ返されるパケットに対して選択されるパスとなることが保証されません。 このシナリオでは、非対称ルーティングの可能性がある場合、コマンドの新しい形式の **ip verify unicast source reachable-via** を使用する必要があります。

例

次に、ユニキャスト リバース パス転送機能がシリアル インターフェイスでイネーブルにされている例を示します。

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

次の例では、ごくシンプルなシングルホームの ISP を使用して、ユニキャスト RPF と併用される入力および出力フィルタの概念について説明します。 この例では、ISP が割り当てたクラスレスドメイン間ルーティング（CIDR）ブロック 192.168.202.128/28 を示します。アップストリーム インターフェイスでインバウンドおよびアウトバウンドフィルタの両方があります。ただし、通常の ISP はシングルホームではありません。そのため、（アウトバウンド トラフィックがあるリンクから送出され、別のリンク経由で返送される場合）非対称フローのプロビジョニングを ISP の境界ルータ上のフィルタに設計する必要があります。

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

次に、ユニキャスト RPF に ACL とロギングを使用する例を示します。 この例では、拡張 ACL 197 に、特定のアドレス範囲についてネットワーク トラフィックを拒否または拒否するエントリが設定されています。 ユニキャスト RPF はイーサネット インターフェイス 0 に設定され、そのインターフェイスに到達するパケットを確認します。

たとえば、192.168.201.10 の送信元アドレスを持つパケットがイーサネット インターフェイス 0 に到達すると、ACL 197 の deny ステートメントのためにドロップされます。 この場合、ACL 情報はロギングされます（この ACL エントリではロギング オプションが有効です）。また、ドロップされたパケットはインターフェイスごと、または全体としてカウントされます。192.168.201.100 の送信元アドレスを持つパケットがイーサネット インターフェイス 0 に到達すると、ACL 197 の permit ステートメントのために転送されます。 ドロップまたは抑制されたパケットに関する ACL

情報は、ログ サーバにロギングされます（この ACL エントリではロギング オプションが有効です）。

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny   ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

関連コマンド

コマンド	説明
ip cef	ルート プロセッサ カードでシスコ エクスプレス フォワーディングをイネーブルにします。

ipv6 tacacs source-interface

TACACS パケットの送信元アドレスに使用するインターフェイスを指定するには、グローバル コンフィギュレーション モードで **ipv6 tacacs source-interface** コマンドを使用します。 コンフィギュレーションから指定したインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 tacacs source-interface *interface*

no ipv6 tacacs source-interface *interface*

構文の説明

interface	TACACS パケットの送信元アドレスに使用するインターフェイス。

コマンド デフォルト

インターフェイスは指定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

ipv6 tacacs source-interface コマンドは、TACACS パケットの送信元アドレスに使用するインターフェイスを指定します。

例

次に、TACACS パケットの送信元アドレスとして使用するギガビットイーサネットインターフェイスを設定する例を示します。

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS+ サーバ コンフィギュレーション モードを開始します。