NETCONF over SSHv2

セキュア シェル バージョン 2（SSHv2）によるネットワーク設定プロトコル（NETCONF）（Network Configuration Protocol (NETCONF) over Secure Shell Version 2 (SSHv2)）機能を使用して、暗号化転送による Cisco コマンドライン インターフェイス（CLI）を介してネットワーク設定を実行できます。NETCONF クライアントである NETCONF ネットワーク マネージャは、NETCONF サーバへのネットワーク転送としてセキュア シェル バージョン 2（SSHv2）を使用する必要があります。NETCONF サーバには複数の NETCONF クライアントが接続できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

NETCONF over SSHv2 の前提条件

- NETCONF over SSHv2 では、**netconf max-session** コマンドで指定した NETCONF セッションごとに vty 回線を用意する必要があります。

NETCONF over SSH の制約事項

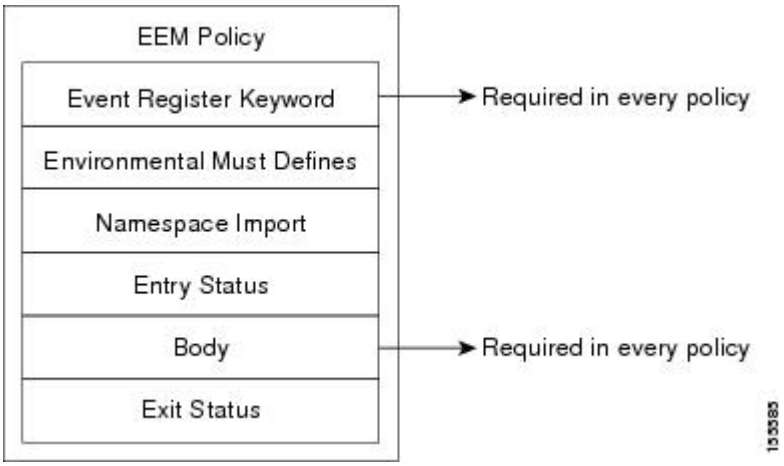
- ネットワーク設定プロトコル（NETCONF）セキュア シェル バージョン 2（SSHv2）は、最大 16 の同時セッションをサポートします。
- SSH バージョン 2 のみサポートされます。

NETCONF over SSHv2 について

NETCONF over SSHv2

NETCONF over SSHv2 機能を実行するために、クライアント（シスコ ソフトウェアが稼働しているシスコ デバイス）はサーバ（NETCONF ネットワーク マネージャ）との SSH 転送接続を確立します。次の図に、基本的な NETCONF over SSHv2 ネットワークの構成を示します。クライアントとサーバは、セキュリティおよびパスワード暗号化に使用するキーを交換します。NETCONF を実行する SSHv2 セッションのユーザ ID およびパスワードは、認可および認証を行うために使用されます。そのユーザの権限レベルが適用されるため、十分に高い権限レベルでなければ、クライアント セッションから NETCONF 動作にフルアクセスできません。認証、認可、アカウンティング（AAA）が設定されている場合は、デバイスに対してユーザが直接 SSH セッションを確立したかのように AAA サービスが使用されます。既存のセキュリティ設定を使用すると、NETCONF への移行がほぼシームレスに行われます。クライアントは認証に成功すると SSH 接続プロトコルを呼び出し、SSH セッションを確立します。SSH セッションが確立されると、ユーザまたはアプリケーションは、「netconf」という SSH サブシステムとして NETCONF を呼び出します。

図 *1 : NETCONF over SSHv2*



SSH バージョン 2

SSHv2は、信頼性の高いトランスポート層の上部で実行され、強力な認証機能と暗号化機能を提供します。SSHv2を使用すると、別のコンピュータにネットワークを介して安全にアクセスして安全にコマンドを実行できるようになります。

NETCONF は SSHv1 をサポートしていません。SSH バージョン 2 サーバの設定は、SSH バージョン 1 の設定と同様です。設定する SSH のバージョンを指定するには、**ip ssh version** コマンドを使用します。このコマンドを設定しない場合、デフォルトで SSH は互換モードで実行されます。バージョン 1 とバージョン 2 両方の接続が利用できます。

（注） SSH バージョン 1 は、標準で定義されていないプロトコルです。未定義のプロトコル（バージョン 1）にデバイスがフォールバックしないようにするには、 **ip ssh version** コマンドを使用してバージョン 2 を指定する必要があります。

設定済みの Rivest, Shamir, and Adelman（RSA）キーを使用する SSH 接続を有効にするには、**ip ssh rsa keypair-name** コマンドを使用します。 **ip ssh rsa keypair-name** コマンドをキー ペアの名前を指定して設定すると、そのキー ペアが存在する場合は SSH が有効になります。または、後でキー ペアが生成されると SSH が有効になります。このコマンドを使用して SSH を有効にする場合、ホスト名およびドメイン名を設定する必要はありません。

NETCONF over SSHv2 の設定方法

ホスト名およびドメイン名を使用した SSH バージョン 2 の有効化

このタスクを実行して、SSH バージョン 2 のデバイスを、ホスト名とドメイン名を使用して設定します。RSA キーペア設定を使用して、SSH バージョン 2 を設定することもできます（RSA キー ペアを使用した SSH バージョン 2 の有効化 （5 ページ）を参照）。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *name*
5. **crypto key generate rsa**
6. **ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]
7. **ip ssh version 2**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**hostname** *hostname* 例： `Device(config)# hostname host1`	デバイスのホスト名を設定します。
ステップ 4	**ip domain-name** *name* 例： `Device(config)# ip domain-name domain1.com`	デバイスのドメイン名を設定します。
ステップ 5	**crypto key generate rsa** 例：	ローカルおよびリモート認証用に SSH サーバを有効にします。

	コマンドまたはアクション	目的
	`Device(config)# crypto key generate rsa`	
ステップ 6	**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*] 例： `Device(config)# ip ssh timeout 120`	（任意）デバイス上で SSH 制御変数を設定します。
ステップ 7	**ip ssh version 2** 例： `Device(config)# ip ssh version 2`	デバイスで実行する SSH のバージョンを指定します。

RSA キー ペアを使用した SSH バージョン 2 の有効化

このタスクを実行して、ホスト名やドメイン名を設定せずに SSH バージョン 2 を有効にします。設定したキーペアがすでに存在している場合、または後で生成される場合、SSH バージョン 2 が有効になります。ホスト名およびドメイン名の設定を使用して SSH バージョン 2 を設定することもできます（ホスト名およびドメイン名を使用した SSH バージョン 2 の有効化 （4 ページ）を参照）。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh rsa keypair-name** *keypair-name*
4. **crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size*
5. **ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*]
6. **ip ssh version 2**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ip ssh rsa keypair-name** *keypair-name* 例： `Device(config)# ip ssh rsa keypair-name sshkeys`	SSH を使用する際に使用する RSA キー ペアを指定します。 （注） シスコ デバイスには複数の RSA キー ペアを設定できます。
ステップ 4	**crypto key generate rsa usage-keys label** *key-label* **modulus** *modulus-size* 例： `Device(config)# crypto key generate rsa usage-keys label sshkeys modulus 768`	デバイスでローカルおよびリモート認証を行う SSH サーバを有効にします。 SSH バージョン 2 では、絶対サイズは 768 ビット以上である必要があります。 （注） RSA キー ペアを削除するには、**crypto key zeroize rsa** コマンドを使用します。RSA コマンドを削除すると、SSH サーバが自動的に無効になります。
ステップ 5	**ip ssh** [**timeout** *seconds* | **authentication-retries** *integer*] 例： `Device(config)# ip ssh timeout 120`	デバイス上で SSH 制御変数を設定します。
ステップ 6	**ip ssh version 2** 例： `Device(config)# ip ssh version 2`	デバイスで実行する SSH のバージョンを指定します。

リモート デバイスとの暗号化セッションの開始

リモート ネットワーキング デバイスとの暗号化セッションを開始するには、次の作業を実行します（デバイスを有効にする必要はありません。SSH はディセーブル モードで実行できます）。

UNIX または UNIX ライクなデバイスからは、通常、次のコマンドを使用して、SSH セッションを確立します。

```
ssh -2 -s user@router.example.com netconf
```

手順の概要

1. 次のいずれかを実行します。
   - **ssh** [**-v** {**1** | **2**}] [**-c** {**3des**| **aes128-cbc** | **aes192-cbc**| **aes256-cbc**}] [**-m**{**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**l** *userid*] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	次のいずれかを実行します。
	• **ssh** [**-v** {**1** | **2**}] [**-c** {**3des**| **aes128-cbc** | **aes192-cbc**| **aes256-cbc**}] [**-m**{**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}] [**l** *userid*] [**-o numberofpasswordprompts** *n*] [**-p** *port-num*] {*ip-addr* | *hostname*} [*command*]
	例：
	`Device# ssh -v 2 -c aes256-cbc -m hmac-sha1-96 -l user2 10.76.82.24`
	例：
	`Device# ssh -v 2 -c aes256-cbc -m hmac-sha1-96 user2@10.76.82.24`
		リモート ネットワーク デバイスとの暗号化されたセッションを開始します。
		1 つめの例は、SSH バージョン 2 の規定に準拠しています。より自然で一般的なセッション開始方法は、ユーザ名をホスト名に結合することです。たとえば、2 つめの設定例でも、1 つめの例と同じ結果が得られます。

トラブルシューティングのヒント

ip ssh version コマンドは、SSH の設定のトラブルシューティングに使用できます。バージョンを変更することによって、問題がある SSH バージョンを特定できます。

次の作業

ssh コマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

セキュア シェル接続のステータスの確認

デバイス上の SSH 接続のステータスを表示するには、次の作業を実行します。

（注） 次の **show** コマンドは、ユーザ EXEC モードまたは特権 EXEC モードで使用できます。

手順の概要

1. **enable**
2. **show ssh**
3. **show ip ssh**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	（任意）特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ssh** 例： `Device# show ssh`	SSH サーバ接続のステータスを表示します。
ステップ 3	**show ip ssh** 例： `Device# show ip ssh`	SSH のバージョンおよび設定データを表示します。

例

次の **show ssh** コマンドの出力には、SSH バージョン 2 の接続に関するステータスが表示されています。

```
Device# show ssh
Connection Version Mode Encryption  Hmac                State
Username
1          2.0     IN   aes128-cbc  hmac-md5     Session started       lab
1          2.0     OUT  aes128-cbc  hmac-md5     Session started       lab
%No SSHv1 server connections running.
```

次の **show ip ssh** コマンドの出力には、有効になっている SSH のバージョン、認証タイムアウト値、および認証の再試行回数が表示されています。

```
Device# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

NETCONF over SSHv2 の有効化

NETCONF over SSHv2 を有効にするには、次の作業を実行します。

始める前に

SSHv2 を有効にする必要があります。

（注） 同時 NETCONF セッションと同じ数以上の vty 行が設定されている必要があります。

（注）
- 4 個以上の同時 NETCONF セッションを設定する必要があります。
- 最大 16 個の同時 NETCONF セッションを設定できます。
- NETCONF では SSHv1 はサポートされません。

手順の概要

1. **enable**
2. **configure terminal**
3. **netconf ssh** [**acl** *access-list-number*]
4. **netconf lock-time** *seconds*
5. **netconf max-sessions** *session*
6. **netconf max-message** サイズ

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**netconf ssh** [**acl** *access-list-number*] 例： `Device(config)# netconf ssh acl 1`	NETCONF over SSHv2 を有効にします。 • 任意で、この NETCONF セッションのアクセス コントロール リストを設定できます。
ステップ 4	**netconf lock-time** *seconds* 例： `Device(config)# netconf lock-time 60`	（任意）NETCONF 設定を中間操作が行われないようにロックする最長時間を秒単位で指定します。 • 有効な範囲は、1 ～ 300 秒です。デフォルト値は 10 秒です。
ステップ 5	**netconf max-sessions** *session* 例： `Device(config)# netconf max-sessions 5`	（任意）許容される同時 NETCONF セッションの最大数を指定します。 • 有効な範囲は、4 ～ 16 です。デフォルト値は 4 です。

	コマンドまたはアクション	目的
ステップ 6	**netconf max-message** サイズ 例： `Device(config)# netconf max-message 37283`	（任意）NETCONF セッションで受信するメッセージの最大サイズをキロバイト（KB）で指定します。 • 有効な範囲は、1 ～ 2147483 KB です。デフォルト値は無限です。 • 最大サイズを無限に設定するには、**no netconf max-message** コマンドを使用します。

NETCONF over SSHv2 の設定例

例：ホスト名およびドメイン名を使用した SSHv2 の有効化

```
configure terminal
hostname host1
ip domain-name example.com
crypto key generate rsa
ip ssh timeout 120
ip ssh version 2
```

RSA キーを使用したセキュア シェル バージョン 2 の有効化の例

次に、RSA キーを使用してセキュア シェル バージョン 2 を有効にする例を示します。

```
Device# configure terminal

Device(config)# ip ssh rsa keypair-name sshkeys

Device(config)# crypto key generate rsa usage-keys label sshkeys modulus 768
Device(config)# ip ssh timeout 120
Device(config)# ip ssh version 2
```

リモート デバイスとの暗号化セッションの開始の例

次に、UNIX または UNIX 系のデバイスから、リモート ネットワーキング デバイスとの暗号化 SSH セッションを開始する例を示します。

```
Device(config)# ssh -2 -s user@router.example.com netconf
```

NETCONF over SSHv2 の設定例

次に、NETCONF over SSHv2 を設定する例を示します。

```
Device# configure terminal
Device(config)# netconf ssh acl 1
Device(config)# netconf lock-time 60
Device(config)# netconf max-sessions 5
Device(config)# netconf max-message 2345
Device# ssh-2 -s username@10.1.1.1 netconf
```

次に、ループバック インターフェイス 113 の設定を取得する例を示します。

手順の概要

1. 最初に、「hello」を送信します。
2. 次に、get-config 要求を送信します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	最初に、「hello」を送信します。 例： <?xml version="1.0" encoding=\"UTF-8\"?> <hello><capabilities> <capability>u?rn:ietf:params:netconf:base:1.0</capability> <capability>urn:ietf:params:netconf:capability:writeable-running:1.0</capability> <capability>urn:ietf:params:netconf:ca?pability:roll?back-on-error:1.0</capability> <capability>urn:ietf:params:netconf:capability:startup:1.0</capability> <capability>urn:ietf:params:netconf:ca?pability:url:?1.0</capability> <capability>urn:cisco:params:netconf:capability:pi-data-model:1.0</capability> <capability>urn:cisco:params:netconf:capabili?ty:notificati?on:1.0</capability> </capabilities> </hello>]]>]]>	
ステップ 2	次に、get-config 要求を送信します。 例： <?xml version="1.0"?> <rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"xmlns:cpi="http://www.cisco.com/cpi_10/schema" message-id="101"> <get-config> <source> <running/>	

	コマンドまたはアクション	目的
	</source> <filter> <config-format-text-cmd> <text-filter-spec> interface Loopback113 </text-filter-spec> </config-format-text-cmd> </filter> </get-config> </rpc>]]>]]>	

デバイスに次の出力が表示されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101"xmlns=\"urn:ietf:params:netconf:base:1.0\">
   <data>
      <cli-config-data>
interface Loopback113
description test456
no ip address
load-interval 30
end
       </cli-config-data>
    </data>
</rpc-rep?ly>]]>]]>
```

NETCONF over SSHv2 に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Command References』、すべてのリリース
NETCONF コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用に関する注意事項、および例	『*Cisco IOS Cisco Networking Services Command Reference*』
IP アクセス リスト コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例 セキュリティ コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『*Cisco IOS Security Command Reference*』

関連項目	マニュアル タイトル
IP アクセス リスト	『Cisco IOS Security Configuration Guide: Securing the Data Plane』の「IP Access List Overview」および「Creating an IP Access List and Applying It to an Interface」の章
セキュア シェルおよびセキュア シェル バージョン 2	『Cisco IOS Security Configuration Guide: Securing User Services』の『Configuring Secure Shell』モジュール

標準および RFC

RFC	タイトル
RFC 2246	*The TLS Protocol Version 1.0*
RFC 4251	*The Secure Shell (SSH) Protocol Architecture*
RFC 4252	*The Secure Shell (SSH) Authentication Protocol*
RFC 4741	NETCONF Configuration Protocol
RFC 4742	Using the NETCONF Configuration Protocol over Secure SHell (SSH)

シスコのテクニカル サポート

説明	リンク
シスコのサポートならびにドキュメントの Web サイトではリソースをオンラインで提供しており、マニュアル、ソフトウェア、およびツールをダウンロードできます。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NETCONF over SSHv2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : NETCONF over SSHv2* の機能情報

機能名	リリース	機能情報
NETCONF over SSHv2	Cisco IOS XE Release 2.1 12.2(33)SB 12.2(33)SRA 12.2(33)SXI 12.4(9)T	NETCONF over SSHv2 機能を使用すると、暗号化されたトランスポート上で Cisco コマンドライン インターフェイス（CLI）によるネットワーク設定を実行できます。 この機能により、次のコマンドが導入または変更されました。**netconf lock-time**、**netconf max-message**、**netconf max-sessions** **netconf ssh**