セキュア コピー

Secure Copy（SCP; セキュア コピー）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、Secure Shell（SSH; セキュア シェル）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「セキュア コピーの機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

セキュア コピーの前提条件

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。
- SCP のセキュアな転送は SSH に依存しているため、ルータ上に Rivest, Shamir, and Adelman（RSA）キーのペアを設置する必要があります。

セキュア コピーに関する情報

セキュア コピー機能を設定するには、次の概念を理解しておく必要があります。

- 「セキュア コピーの動作方法」（P.2）

セキュア コピーの動作方法

SCP の動作は、SCP のセキュリティが SSH に依存していることを除いて、Berkeley r ツール スイートからのリモート コピー（rcp）の動作に似ています。加えて、SCP は、ユーザが正しい権限レベルを持っていることをルータ上で判断できるように、authentication, authorization, and accounting（AAA; 認証、認可、およびアカウンティング）許可を設定する必要があります。

SCP を使用すれば、適切な許可を得たユーザは、**copy** コマンドを使用して、Cisco IOS File System（IFS; IOS ファイル システム）内に存在する任意のファイルをルータとやり取りすることができます。許可された管理者はワークステーションからこの操作を実行することもできます。

（注） Cisco IOS ソフトウェアと一緒に pscp.exe を使用している場合は、SCP オプションを有効にします。

セキュア コピーの設定方法

ここでは、次の各手順について説明します。

- 「セキュア コピーの設定」（P.2）
- 「セキュア コピーの設定例」（P.4）

セキュア コピーの設定

Cisco ルータを有効にして、SCP サーバ側機能用に設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
5. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]

6. **username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*}
7. **ip scp server enable**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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	**aaa new-model** **例：** `Router(config)# aaa new-model`	ログイン時の AAA 認証を設定します。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] **例：** `Router(config)# aaa authentication login default group tacacs+`	AAA アクセス コントロール システムを有効にします。
ステップ 5	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]] **例：** `Router(config)# aaa authorization exec default group tacacs+`	ネットワークへのユーザ アクセスを制限するパラメータを設定します。 **（注）** **exec** キーワードは、認可を実行してユーザが EXEC シェルの実行を許可されているかどうかを判断します。したがって、SCP を設定するときにこのキーワードを使用する必要があります。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type encrypted-password*} **例：** `Router(config)# username superuser privilege 2 password 0 superpassword`	ユーザ名をベースとした認証システムを構築します。 **（注）** TACACS+ や RADIUS などのネットワークベースの認証メカニズムが設定されている場合は、このステップを省略できます。
ステップ 7	**ip scp server enable** **例：** `Router(config)# ip scp server enable`	SCP サーバ側機能を有効にします。
ステップ 8	**show running-config** **例：** `Router# show running-config`	（任意）SCP サーバ側機能を確認します。

	コマンド	目的
ステップ 9	**debug ip scp** **例：** `Router# debug ip scp`	（任意）SCP 認証問題を解決します。

セキュア コピーの設定例

ここでは、次の設定例について説明します。

ローカル認証を使用した SCP サーバ側設定：例

次の例は、SCP のサーバ側機能の設定方法を示しています。この例では、ローカルに定義されたユーザ名とパスワードを使用します。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

ネットワークベースの認証を使用した SCP サーバ側設定：例

次の例は、ネットワークベースの認証メカニズムを使用した SCP のサーバ側機能の設定方法を示しています。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

その他の参考資料

次の項で、セキュア コピーに関する参考資料を紹介します。

関連資料

内容	参照先
セキュア シェル バージョン 1 と 2 のサポート	• 「Configuring Secure Shell」モジュール • 「Secure Shell Version 2 Support」モジュール
認証コマンドと認可コマンド	『*Cisco IOS Security Command Reference*』
認証と認可の設定	『*Cisco IOS Security Configuration Guide: Securing User Services*, Release 15.0』の「Authentication, Authorization, and Accounting (AAA)」

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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。	http://www.cisco.com/techsupport

セキュア コピーの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　セキュア コピーの機能情報

機能名	リリース	機能情報
セキュア コピー	12.2(2)T 12.0(21)S 12.2(25)S	Secure Copy（SCP; セキュア コピー）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、Secure Shell（SSH; セキュア シェル）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。 この機能は、Cisco IOS Release 12.2(2)T で導入されました。 この機能は、Cisco IOS Release 12.0(21)S に統合されました。 この機能は、Cisco IOS Release 12.2(25)S に統合されました。 **debug ip scp** コマンドと **ip scp server enable** コマンドが導入または変更されました。

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。セキュリティ サービスのフレームワークであり、ユーザの身元確認（認証）、リモート アクセス コントロール（認可）、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信（アカウンティング）の方式を定めています。

rcp：remote copy（リモート コピー）。セキュリティをリモート シェル（Berkeley r ツール スイート）に依存している rcp は、ルータ イメージやスタートアップ設定などのファイルをルータとやり取りします。

SCP：Secure CoPy（セキュア コピー）。セキュリティを SSH に依存している SCP サポートは、Cisco IOS ファイル システム内のあらゆるもののセキュアで認証されたコピーを可能にします。SCP は rcp から派生したものです。

SSH：Secure Shell（セキュア シェル）。Berkeley r ツールのセキュアな代替手段を提供するアプリケーションとプロトコル。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。SSH バージョン 1 は Cisco IOS ソフトウェアに実装されています。