セキュア コピー

セキュア コピー（SCP）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、セキュア シェル（SSH）、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。

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 は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

セキュアコピーのパフォーマンス向上に関する制限事項

- ウィンドウ サイズの増加は、主に SCP 操作に対してのみ使用する必要があります。
- プラットフォームのタイプによっては、ウィンドウ サイズが最大の場合に CPU 使用率が高くなることがあります。
- 万一に備えて、デフォルト サイズの 4 倍まで増やすことができます。

Secure Copy に関する情報

SCP の機能

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。加えて、SCP は、ユーザー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、認証、許可、アカウンティング（AAA）許可を設定する必要があります。

SCP を使用すると、適切な許可を得たユーザーは、**copy** コマンドを使用して、Cisco IOS XE ファイル システム（IFS）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。

SCP の設定方法

SCP の設定

Cisco ルータを有効にして、SCP サーバー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

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `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。

	コマンドまたはアクション	目的
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 システムをイネーブルにします。
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） **The exec** キーワードは、認可を実行してユーザーが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`	ユーザー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、この手順を省略できます。
ステップ 7	**ip scp server enable** 例： `Router (config)# ip scp server enable`	SCP サーバー側機能を有効にします。

SCP の確認

SCP サーバー側機能を確認するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show running-config**

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： `Router> 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	**show running-config** 例： `Router# show running-config`	SCP サーバー側機能を確認します。

SCP のトラブルシューティング

手順の概要

1. **enable**
2. **debug ip scp**

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： `Router> 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	**debug ip scp** 例： `Router# debug ip scp`	SCP 認証問題を解決します。

セキュア コピーの設定例

ローカル認証を使用した SCP サーバー側の設定例

次の例は、SCP のサーバー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 tiger 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認証を使用した SCP サーバー側の設定例

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

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 Master Commands List, All Releases』
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、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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。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。	http://www.cisco.com/cisco/web/support/index.html

セキュア コピーの機能情報

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 リリースだけを示しています。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:* セキュア コピーの機能情報

機能名	リリース	機能の設定情報
セキュア コピー	Cisco IOS XE Release 2.1	セキュア コピー（SCP）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、セキュア シェル（SSH）、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 XE Release2.1 で、Cisco ASR 1000 シリーズアグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました：**debug ip scp**、**ip scp server enable**。

用語集

AAA：認証、許可、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、ユーザーの身元確認（認証）、リモート アクセス コントロール（許可）、課金、監査、およびレポートに使用するセキュリティ サーバー情報の収集と送信（アカウンティング）の方式を定めています。

rcp ：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 コンフィギュレーションなどのファイルをルータとやり取りします。

SCP ：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 XE 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 ：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 XE ソフトウェアに実装されています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。