セキュア コピー

セキュアコピー（SCP）機能は、デバイス設定またはデバイスイメージファイルをコピーするための安全で認証された方式を提供します。SCP は、セキュアシェル（SSH）、アプリケーション、および Berkeley r ツールスイート（バークレー大学の独自のネットワーキング アプリケーションセット）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。このドキュメントでは、SCP サーバ側機能用にシスコデバイスを設定する手順について説明します。

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。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、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。

セキュア コピーの前提条件

- セキュアコピー（SCP）を有効にする前に、デバイス上でセキュアシェル（SSH）、認証、および許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、デバイスには RSA キーのペアが必要です。

Secure Copy に関する情報

セキュア コピーの動作方法

セキュア コピー（SCP）は一連の Berkeley の r-tools（Berkeley 大学独自のネットワーキング アプリケーション セット）に基づいて設計されているため、その動作内容は Remote Copy Protocol（RCP）と類似しています。ただし、SCP はセキュア シェル（SSH）のセキュリティに対応している点は除きます。加えて、SCP では、ユーザが正しい権限レベルを持っていることをデバイス上で判断できるように、認証、認可、アカウンティング（AAA）認可を設定する必要があります。

SCP を使用すると、**copy** コマンドを使用して Cisco IOS ファイルシステム（IFS）内の任意のファイルのコピーをデバイスとの間で実行できるのは、特権レベルが 15 のユーザのみになります。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 ソフトウェアと一緒に pscp.exe ファイル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

セキュア コピーの設定

シスコ デバイスにセキュア コピー（SCP）サーバ側機能の設定をするには、次の手順を実行します。

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 **aaa new-model**

例：

```
Device(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：

```
Device(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 **username** *name* [**privilege** *level*] **password** *encryption-type encrypted-password*

例：

```
Device(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、この手順を省略できます。

ステップ 6 **ip scp server enable**

例：

```
Device(config)# ip scp server enable
```

SCP サーバ側機能を有効にします。

ステップ 7 **exit**

例：

```
Device(config)# exit
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 8 **show running-config**

例：

```
Device# show running-config
```

（任意）SCP サーバ側機能を表示します。

ステップ 9 **debug ip scp**

例：

```
Device# 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

例：ローカル認証を使用したセキュア コピーの設定

次の例は、セキュア コピー（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 in order 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 scp server enable
```

ネットワークベース認証を使用した SCP サーバ側の設定例

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 Command List, All Releases』

関連項目	マニュアル タイトル
セキュア シェル バージョン 1 と 2 のサポート	『セキュア シェル コンフィギュレーション ガイド』
認証コマンドと認可コマンド	『Cisco IOS Security Command Reference: Commands A to C』
認証と認可の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

用語集

AAA：認証、許可、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（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）に依存しています。RCP は、デバイス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デバイスとやり取りします。

SCP：セキュアコピー。セキュリティを SSH に依存しています。SCP サポートは、Cisco IOS ファイルシステム（IFS）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 ツールスイート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 はシスコソフトウェアに実装されています。