



セキュアコピー

このドキュメントでは、セキュアコピー（SCP）サーバー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。

- [セキュアコピーの前提条件](#)（1 ページ）
- [Secure Copy に関する情報](#)（1 ページ）
- [セキュアコピーの設定方法](#)（2 ページ）
- [セキュアコピーの設定例](#)（5 ページ）
- [セキュアコピーに関する追加情報](#)（6 ページ）
- [セキュアコピーの機能情報](#)（7 ページ）

セキュアコピーの前提条件

- デバイス上でセキュアシェル（SSH）、認証、および許可を設定します。
- Secure Copy Protocol（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 Rivest、Shamir、Adelman（RSA）キーのペアが必要です。

Secure Copy に関する情報

Secure Copy 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供します。Secure Copy Protocol（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。

SCP は一連の Berkeley の r ツール（Berkeley 大学独自のネットワーク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 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、ユーザー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、許可、およびアカウンティング（AAA）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（Cisco 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 のユーザーのみ

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)
- `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。
 - SSH を機能させるには、RSA 公開キーと秘密キーのペアをデバイスで設定する必要があります。

セキュアコピーのパフォーマンス向上

SSH 一括データ転送モードを使用すると、クライアントまたはサーバーの容量で動作する SCP のスループットパフォーマンスを向上させることができます。このモードはデフォルトでは無効になっていますが、**`ip ssh bulk-mode`** グローバルコンフィギュレーション コマンドを使用して有効にすることができます。一括モードウィンドウサイズが設定されている場合、TCP 選択的確認応答 (SACK) はデフォルトでイネーブルになります。



- (注) このコマンドは、大きなファイルを転送する場合にのみ有効にし、ファイル転送の完了後に無効にすることをお勧めします。

デフォルトの一括モードウィンドウサイズである 128 KB は、ほとんどのネットワーク設定で大きなファイルをコピーするのに最適ですが、ラウンドトリップ時間 (RTT) が広帯域高遅延ネットワークでは、128 KB では不十分です。**`ip ssh bulk-mode window-size`** コマンドを使用して一括モードウィンドウサイズを設定することで、最適な SCP スループットパフォーマンスをイネーブルにできます。たとえば、理想的なラボテスト環境では、200 ミリ秒のラウンドトリップ時間設定で 2 MB のウィンドウサイズを設定すると、デフォルトの 128 KB のウィンドウサイズと比較して、スループットパフォーマンスが約 500% 向上します。

一括モードウィンドウサイズは、ネットワーク帯域幅遅延積（つまり、使用可能な合計帯域幅 (bps) およびラウンドトリップ時間 (秒) の乗数）に従って設定する必要があります。ウィンドウサイズが大きくなると CPU 使用率が増加する可能性があるため、適切なウィンドウサイズを選択してバランスを取ります。

セキュアコピーの設定方法

ここでは、セキュアコピーの設定作業について説明します。

セキュアコピーの設定

シスコデバイスに SCP サーバー側機能の設定をするには、次の手順を実行します。

手順

	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。 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 : 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	debug ip scp 例 : Device# debug ip scp	(任意) SCP 認証問題を解決します。

SSH サーバーでのセキュアコピーのイネーブル化

次のタスクでは、SCPのサーバー側機能の設定方法を示します。このタスクは、デバイスでリモートのワークステーションからファイルを安全にコピーできる一般的な設定を示しています。

手順

	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。 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 : 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	認証、許可、アカウントिंग (AAA) アクセス コントロール モデルをイネーブルにします。
ステップ 4	aaa authentication login default local 例 : Device(config)# aaa authentication login default local	ログイン時の認証にローカルのユーザー名データベースを使用するように AAA 認証を設定します。
ステップ 5	aaa authorization exec default local 例 : Device(config)# aaa authorization exec default local	ユーザーアクセスを制限するパラメータをネットワークに設定します。許可を実行し、ユーザー ID で特権 EXEC シェルの実行を許可するかどうかを定義します。その後、システムで許可にローカルデータベースを使用する必要があることを指定します。
ステップ 6	username name privilege privilege-level password password 例 : Device(config)# username samplename privilege 15 password password1	ユーザー名ベースの認証システムを確立し、ユーザー名、権限レベル、および非暗号化パスワードを指定します。 (注) <i>privilege-level</i> 引数に必要な最小値は 15 です。権限レベルが 15 未満の場合、接続が切断されます。

	コマンドまたはアクション	目的
ステップ 7	ip ssh time-out seconds 例 : Device(config)# ip ssh time-out 120	デバイスが SSH クライアントの応答を待つ時間間隔を、秒単位で設定します。
ステップ 8	ip ssh authentication-retries 整数 例 : Device(config)# ip ssh authentication-retries 3	インターフェイスのリセット後、認証を試行する回数を設定します。
ステップ 9	ip scp server enable 例 : Device(config)# ip scp server enable	デバイスで、リモートワークステーションから安全にファイルをコピーできるようにします。
ステップ 10	ip ssh bulk-mode window-size 例 : Device(config)# ip ssh bulk-mode 33107232	(任意) SSH 一括データ転送モードをイネーブルにして、SCP のスループットパフォーマンスを強化します。
ステップ 11	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 12	debug ip scp 例 : Device# debug ip scp	(任意) SCP 認証の問題に関する診断情報を提供します。

セキュアコピーの設定例

次に、セキュアコピーの設定例を示します。

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ー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.
Device> enable
```

```

Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default local
Device(config)# aaa authorization exec default local
Device(config)# username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
Device(config)# ip scp server enable
Device(config)# end

```

例：ネットワークベース認証を使用したセキュアコピーのサーバー側の設定

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セキュアコピーのサーバー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.
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group tacacs+
Device(config)# aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
Device(config)# ip ssh time-out 120
Device(config)# ip ssh authentication-retries 3
Device(config)# ip scp server enable
Device(config)# end

```

セキュアコピーに関する追加情報

関連資料

関連項目	マニュアルタイトル
セキュアシェルバージョン1と2のサポート	セキュアシェルの設定

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する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	セキュアコピー	Secure Copy 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、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。 次のコマンドが導入または変更されました。 debug ip scp および ip scp server enable
Cisco IOS XE Amsterdam 17.2.1	セキュアコピーのパフォーマンス向上	SSH 一括モードを使用すると、特定の最適化により、大量のデータ転送を伴うプロセスのスループットパフォーマンスを向上できます。このモードは、 ip ssh bulk-mode グローバルコンフィギュレーションコマンドを使用して有効にすることができます。
Cisco IOS XE Bengaluru 17.6.1	大規模な RTT シナリオでのセキュアコピーの改善	大規模な RTT 設定でのセキュアコピーは、 ip ssh bulk-mode コマンドの <i>window-size</i> 変数オプションを使用して設定できます。

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 には、<http://www.cisco.com/go/cfn> からアクセスします。

