HTTP または HTTPS を使用したファイルの転送

Cisco IOS Release 12.4 には、Cisco IOS ソフトウェアベースのデバイスとリモート HTTP サーバとの間で HTTP/HTTP セキュア（HTTPS）プロトコルを使用してファイル転送を行う機能があります。ファイル システム プレフィックスを使用する Cisco IOS コマンドライン インターフェイス（CLI）コマンド（**copy** コマンドなど）で、送信元や宛先に HTTP や HTTPS を指定できるようになりました。

- 機能情報の確認 （1 ページ）
- HTTP または HTTPS を使用したファイル転送の前提条件 （2 ページ）
- HTTP または HTTPS を使用したファイル転送に関する制約事項 （2 ページ）
- HTTP または HTTPS を使用したファイル転送に関する情報 （2 ページ）
- HTTP または HTTPS を使用したファイル転送方法 （3 ページ）
- HTTP または HTTPS を使用したファイル転送の設定例 （9 ページ）
- その他の参考資料 （11 ページ）
- HTTP または HTTPS を使用したファイル転送の機能情報 （12 ページ）

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。

HTTP または HTTPS を使用したファイル転送の前提条件

リモートHTTPサーバへ、またはサーバからファイルをコピーするためには、使用するシステムがHTTPクライアント機能をサポートしている必要があります。この機能はほとんどのCisco IOS ソフトウェア イメージに統合されています。HTTP クライアントはデフォルトでイネーブルになっています。現在のシステムがHTTPクライアントをサポートしているかどうかを判断するには、**show ip http client all** コマンドを発行します。このコマンドを実行できれば、HTTP クライアントがサポートされています。

埋め込み HTTP クライアントのオプション設定と HTTPS クライアントのためのコマンドも存在しますが、HTTP または HTTPS を使用したファイル転送機能を使用する場合は、デフォルトの設定で十分です。HTTP または HTTP クライアントのオプション特性の設定については、「関連資料」セクションを参照してください。

HTTP または HTTPS を使用したファイル転送に関する制約事項

copy コマンドの既存の制限（ネットワーク間のコピーができないなど）は、HTTP または HTTPS を使用したファイル転送機能でも有効です。

（注） Cisco IOS リリース 12.4T の **copy** コマンドは、古いバージョンの Apache サーバ ソフトウェアと組み合わせて動作させることができません。copy コマンドを使用するには、Apache サーバ ソフトウェアをバージョン 2.0.49 以降にアップグレードする必要があります。

HTTP または HTTPS を使用したファイル転送に関する情報

HTTP または HTTPS を使用してファイルを転送するには、次の概念について理解しておく必要があります。

HTTP または HTTPS を使用したファイル転送機能は、Cisco IOS の **copy** コマンドおよびコマンドライン インターフェイスを使用して、リモート サーバからローカル ルーティング デバイスへ、またはその逆の方向に、Cisco IOS イメージ ファイル、コア ファイル、コンフィギュレーションファイル、ログ ファイル、スクリプトなどのファイルをコピーする機能を提供します。HTTP コピー操作は、FTP や TFTP など、他のリモート ファイル システムからのコピーと同じように動作します。

HTTP コピー操作では、HTTP セキュア転送に組み込み HTTPS クライアントを使用できるので、Public Key Infrastructure（PKI）のコンテキスト内で安全かつ認証されたファイル転送が実現されます。

HTTP または HTTPS を使用したファイル転送方法

ここでは、次の手順について説明します。

（注） 接続にユーザ名とパスワードを要求するサーバとの HTTP 接続では、HTTP を使用したファイル転送機能を使用するために、ユーザ名とパスワードの指定が必要な場合があります。デフォルト設定を使用できますが、カスタム接続特性を指定するコマンドも使用できます。接続とファイルの監視とメンテナンスのためのコマンドも準備されています。

ファイル転送の HTTP 接続特性の設定

HTTP ファイル転送用に、デフォルト値が設定されています。次の作業では、接続特性を使用中のネットワーク用にカスタマイズし、使用するユーザ名とパスワード、接続プライオリティ、リモート プロキシ サーバ、発信元インターフェイスを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http client connection** {**forceclose** | **idletimeout***seconds* | **timeout***seconds*}
4. **ip http client username** *username*
5. **ip http client password** *password*
6. **ip http client proxy-server** {*proxy-name* | *ip-address*} [**proxy-port***port-number*]
7. **ip http client source-interface** *interface-id*
8. **do copy running-config startup-config**
9. **end**

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 モードをイネーブルにします。 • 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：	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
	`Router# configure terminal`	
ステップ 3	**ip http client connection** {**forceclose** | **idletimeout***seconds* | **timeout***seconds*} 例： `Router(config)# ip http client connection timeout 15`	すべてのファイル転送について、リモート HTTP サーバへの HTTP クライアント接続の特性を設定します。 • **forceclose**：デフォルトの永続的接続を無効化します。 • **idle timeout** *seconds*：アイドル接続が許容される時間を 1 秒から 60 秒の範囲で設定します。デフォルト タイムアウトは 30 秒です。 • **timeout** *seconds*：HTTP クライアントの接続待ち時間の上限を 1 秒から 60 秒の範囲で設定します。デフォルトは 10 秒です。
ステップ 4	**ip http client username** *username* 例： `Router(config)# ip http client username user1`	ユーザ認証を要求する HTTP クライアント接続で使用するユーザ名を指定します。 （注） CLI で **copy** コマンドを発行する際、ユーザ名を指定することもできます。その場合、そこで入力されるユーザ名がこのコマンドの設定を上書きします。例については、「HTTP またはHTTPS を使用したリモートサーバからのファイルのダウンロードの例」セクションを参照してください。
ステップ 5	**ip http client password** *password* 例： `Router(config)# ip http client password letmein`	ユーザ認証を要求する HTTP クライアント接続で使用するパスワードを指定します。 （注） CLI で **copy** コマンドを発行する際、パスワードを指定することもできます。その場合、そこで入力されるパスワードがこのコマンドの設定を上書きします。例については、「HTTP またはHTTPS を使用したリモートサーバからのファイルのダウンロードの例」セクションを参照してください。
ステップ 6	**ip http client proxy-server** {*proxy-name* | *ip-address*} [**proxy-port***port-number*] 例： `Router(config)# ip http client proxy-server edge2 proxy-port 29`	HTTP ファイル システム クライアント接続のために HTTP クライアントをリモート プロキシ サーバに接続するよう設定します。 • オプションの **proxy-port***port-number* キーワードおよび引数で、リモート プロキシ サーバのプロキシ ポート番号を指定します。

	コマンドまたはアクション	目的
ステップ 7	**ip http client source-interface** *interface-id* 例： `Router(config)# ip http client source-interface Ethernet 0/1`	すべての HTTP クライアント コネクションの送信元アドレスにインターフェイスを指定します。
ステップ 8	**do copy running-config startup-config** 例： `Router(config)# do copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルとして保存します。 • **do** コマンドを使用すると、グローバル コンフィギュレーション モードで特権 EXEC モード コマンドを実行できます。

ステップ 9	**end**
	例：
	`Router(config)# end`
	例：
	`Router#`
		コンフィギュレーション セッションを終了し、CLI をユーザ EXEC モードに戻します。

HTTP または HTTPS を使用したリモート サーバからのファイルのダウンロード

HTTP または HTTPS を使用してリモート サーバからファイルをダウンロードするには、次の作業を実行します。**copy** コマンドで、どのようなファイルでもコピー元からコピー先へコピーすることができます。

手順の概要

1. **enable**
2. 次のいずれかを実行します。
   - **copy** [**/erase**] [**/noverify**] **http://***remote-source-urllocal-destination-url*
   - **copy https://** *remote-source-url local-destination-url*

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：	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	`Router> enable` 例：	

ステップ 2	次のいずれかを実行します。
	• **copy** [**/erase**] [**/noverify**] **http:**//*remote-source-urllocal-destination-url*
	• **copy https://** *remote-source-url local-destination-url*
	例：
	`Router# copy http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx flash:c7200-i-mx`
	例：
	`Router# copy`
	例：
	`copy https://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx flash:c7200-i-mx`
		HTTP または HTTPS を使用して、リモート Web サーバからローカル ファイル システムへファイルをコピーします。
		• **/erase** ：コピー前にローカルのコピー先ファイル システムを消去します。このオプションは、限られたメモリ容量のクラス B ファイル システム プラットフォーム用に準備されたもので、ローカルのフラッシュ メモリ スペースを簡単にクリアできます。
		• **/noverify** ：コピーするファイルがイメージ ファイルの場合、このキーワードを使用すると、イメージがコピーされた後に発生するイメージの自動確認が無効化されます。
		• *remote-source-url* 引数は、コピーするファイルのコピー元の位置を示す URL（またはエイリアス）であり、標準の Cisco IOS ファイル システムの HTTP 構文では次のようになります。
		http:// [[*username*:*password*]**@**] {*hostname* | *host-ip*}[/*filepath*]/*filename*
		（注） オプションの *username* 引数および *password* 引数は、ユーザ認証が必要な HTTP サーバにログインするときに使用され、グローバル コンフィギュレーション コマンド **iphttpclientusername** および **iphttpclientpassword** の設定により当該の認証文字列を指定する代わりになります。
		• *local-destination-url* は、コピーするファイルを置く位置の URL（またはエイリアス）であり、標準の Cisco IOS ファイル システムの HTTP 構文では次のようになります。
		filesystem **:** [/*filepath*][/*filename*]
		（注） **copy** コマンド使用時の URL 構文についての詳細は、「その他の参考資料」セクションを参照してください。

トラブルシューティングのヒント

リモート Web サーバからのファイル転送に失敗した場合、次の点を確認します。

- ルータとインターネットとの接続はアクティブか。
- 正しいパスとファイル名が指定されているか。
- リモート サーバがユーザ名とパスワードを要求しているか。
- リモートサーバに非標準のコミュニケーション ポートが設定されていないか（HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443）。

失敗したコピー要求の原因を判別できるよう、CLI はエラー メッセージを返します。コピープロセスについての追加情報は、**debugiphttpclientall** コマンドで表示できます。

HTTP または HTTPS を使用したリモート サーバへのファイルのアップロード

HTTP または HTTPS を使用してリモート サーバへファイルをアップロードするには、次の作業を実行します。

手順の概要

1. **enable**
2. 次のいずれかを実行します。
   - **copy** [**/erase**] [**/noverify**] *local-source-url***http://***remote-destination-url*
   - **copy** *local-source-url* **https://** *remote-destination-url*

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	次のいずれかを実行します。 • **copy** [**/erase**] [**/noverify**] *local-source-url***http://***remote-destination-url* • **copy** *local-source-url* **https://** *remote-destination-url* 例： `Router# http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx_backup`	HTTP または HTTPS を使用して、ローカル ファイル システムからリモート Web サーバへファイルをコピーします。 • **/erase** ：コピー前にローカルのコピー先ファイル システムを消去します。このオプションは、限られたメモリ容量のクラス B ファイル システム プラットフォーム用に準備されたもので、ローカルのフラッシュ メモリ スペースを簡単にクリアできます。

	コマンドまたはアクション	目的
	例： `Router# copy flash:c7200-i-mx http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx_backup` 例：	• **/noverify** ：コピーするファイルがイメージファイルの場合、このキーワードを使用すると、イメージがコピーされた後に発生するイメージの自動確認が無効化されます。 • *local-source-url* 引数は、コピーするファイルのコピー元の位置を示す URL（またはエイリアス）であり、標準の Cisco IOS ファイル システムの構文では次のようになります。 **http:**// [[*username*:*password*]**@**] {*hostname* | *host-ip*}[/*filepath*]/*filename* （注） オプションの *username* 引数および *password* 引数は、ユーザ認証が必要な HTTP サーバにログインするときに使用され、グローバル コンフィギュレーション コマンド **iphttpclientusername** および **iphttpclientpassword** の設定により当該の認証文字列を指定する代わりになります。 • *remote-destination-url* は、コピーするファイルを置く URL（またはエイリアス）であり、標準の Cisco IOS ファイル システムの HTTP 構文では次のようになります。 *filesystem* **:** [/*filepath*][/*filename*] （注） **copy** コマンド使用時の URL 構文についての詳細は、「その他の参考資料」セクションを参照してください。

トラブルシューティングのヒント

リモート Web サーバからのファイル転送に失敗した場合、次の点を確認します。

- ルータとインターネットとの接続はアクティブか。
- 正しいパスとファイル名が指定されているか。
- リモート サーバがユーザ名とパスワードを要求しているか。
- リモート サーバに非標準のコミュニケーション ポートが設定されていないか（HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443）。

失敗したコピー要求の原因を判別できるよう、CLI はエラー メッセージを返します。コピープロセスについての追加情報は、**debugiphttpclientall** コマンドで表示できます。

HTTP を使用したファイル転送の維持とモニタリング

HTTP 接続の維持と監視を行うには、次の作業を実行します。ステップ 2 から 4 は任意の順序で実行できます。

手順の概要

1. **enable**
2. **show ip http client connection**
3. **show ip http client history**
4. **show ip http client session-module**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip http client connection** 例： `Router# show ip http client connection`	アクティブな HTTP クライアント接続の詳細を表示します。
ステップ 3	**show ip http client history** 例： `Router# show ip http client history`	HTTP クライアントがアクセスした URL のうち最新の 20 を表示します。
ステップ 4	**show ip http client session-module** 例： `Router# show ip http client session-module`	HTTP クライアントで登録されたセッション（アプリケーション）の詳細を表示します。

HTTP または HTTPS を使用したファイル転送の設定例

ファイル転送の HTTP 接続特性の設定：例

次の例に、全ユーザの認証を行うリモートサーバへの接続のために HTTP パスワードとユーザ名を設定する方法を示します。この例はまた、接続のアイドル時間制限を 20 秒に設定する方法も示しています。HTTP クライアントの接続待ち時間の上限は、デフォルトの 10 秒のままです。

```
Router(config)# ip http client connection idle timeout 20
Router(config)# ip http client password Secret
Router(config)# ip http client username User1
Router(config)# do show running-config | include ip http client
```

HTTP または HTTPS を使用したリモート サーバからのファイルのダウンロードの例

次の例に、ファイル c7200-i-mx をリモート サーバから HTTP を使用してフラッシュ メモリへコピーする設定方法を示します。この例はまた、ユーザ認証を行う HTTP サーバ用にコマンドラインからユーザ名とパスワードを入力する方法も示しています。

```
Router# copy http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx
flash:c7200-i-mx
```

フラッシュからリモート HTTP サーバへのファイル アップロードの例

次の例は、フラッシュ メモリからリモート HTTP サーバにファイルをコピーする方法を示しています。この例では、**copy** 特権 EXEC コマンドを使用したファイル転送で予期されるプロンプトと表示について示しています。

```
Router# copy flash:c7200-js-mz.ELL2 http://172.19.209.190/user1/c7200-js-mz.ELL2
Address or name of remote host [172.19.209.190]?
Destination filename [user1/c7200-js-mz.ELL2]?
Storing http://172.19.209.190/user1/c7200-js-mz.ELL2 !!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
17571956 bytes copied in 57.144 secs (307503 bytes/sec)
```

リモートHTTPサーバからフラッシュメモリへのファイルのダウンロードの例

次の例は、リモート HTTP サーバからフラッシュ メモリへファイルをコピーする方法を示しています。この例では、**copy** 特権 EXEC コマンドを使用したファイル転送で予期されるプロンプトと表示について示しています。

```
Router# copy http://172.19.209.190/user1/c7200-i-mz.test  flash:c7200-i-mz.test
Destination filename [c7200-i-mz.test]?
Loading http://172.19.209.190/user1/c7200-i-mz.test
.
.
.
11272788 bytes copied in 527.104 secs (21386 bytes/sec)
```

HTTP または HTTPS を使用したリモート サーバへのファイルのアップロード

次の例は、HTTP または HTTPS を使用してファイルをリモート サーバにコピーする方法を示しています。

```
router#copy flash
: http:
Source filename []? running-config
Address or name of remote host []? 10.1.102.1 Destination filename [pilot-confg]?file1
...
```

その他の参考資料

ここでは、HTTP または HTTPS を使用したファイル転送に関する情報について説明します。

関連資料

関連項目	マニュアル タイトル
セキュア HTTP 通信	『*HTTPS—HTTP Server and Client with SSL 3.0*』
Cisco IOS 埋め込み Web サーバ	『*HTTP 1.1 Web Server and Client*』
Cisco IOS 組み込み Web クライアント	『*HTTP 1.1 Client*』
ネットワーク管理コマンド：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 Network Management Command Reference*』
コンフィギュレーション基礎コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上の注意、例	『*Cisco IOS Configuration Fundamentals Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、URL http://www.cisco.com/go/mibs にある Cisco MIB Locator を使用します。

RFC

RFC	タイトル
RFC 2616	『*Hypertext Transfer Protocol -- HTTP/1.1*』R. Fielding 他
RFC 2617	『*HTTP Authentication: Basic and Digest Access Authentication*』J. Franks 他

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 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/en/US/support/index.html

HTTP または HTTPS を使用したファイル転送の機能情報

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 : HTTP* または *HTTPS* を使用したファイル転送の機能情報

機能名	リリース	機能情報
HTTP を使用したファイルのダウンロード	12.3(2)T	HTTP を使用したファイルのダウンロード機能により、HTTP サーバから Cisco IOS ソフトウェアベースのプラットフォームにファイルをコピーすることができます。
HTTP を使用したファイルのアップロード	12.3(7)T	
HTTP を使用したファイル転送	12.3(7)T	HTTP を使用したファイル転送機能は、Cisco IOS **copy** コマンドおよびコマンドライン インターフェイスを使用して、リモート サーバから使用するローカル ルーティング デバイスへ、またはその逆の方向に、Cisco IOS イメージファイル、コア ファイル、コンフィギュレーション ファイル、ログ ファイル、スクリプトなどのファイルをコピーする機能を提供します。HTTP コピー操作は、FTP や TFTP など、他のリモート ファイル システムからのコピーと同じように動作します。 これにより、HTTP または HTTPS を使用して Cisco IOS ソフトウェアベースのプラットフォームから HTTP サーバへファイルをコピーする機能がサポートされます。