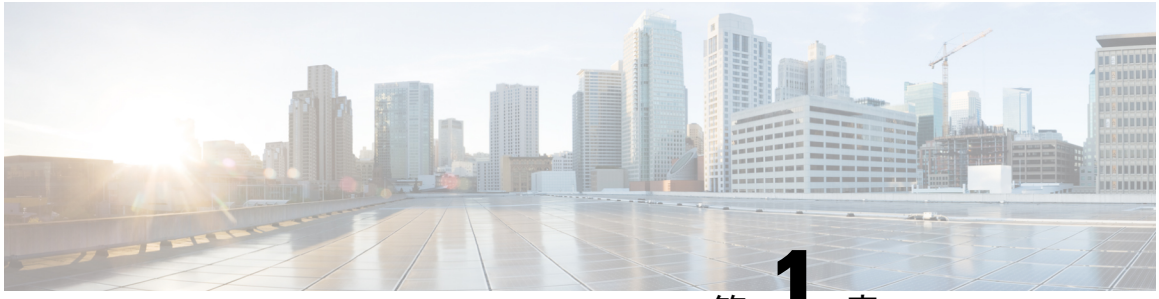
Cisco IOS XE Gibraltar 16.10.x 統合ファイル システム コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

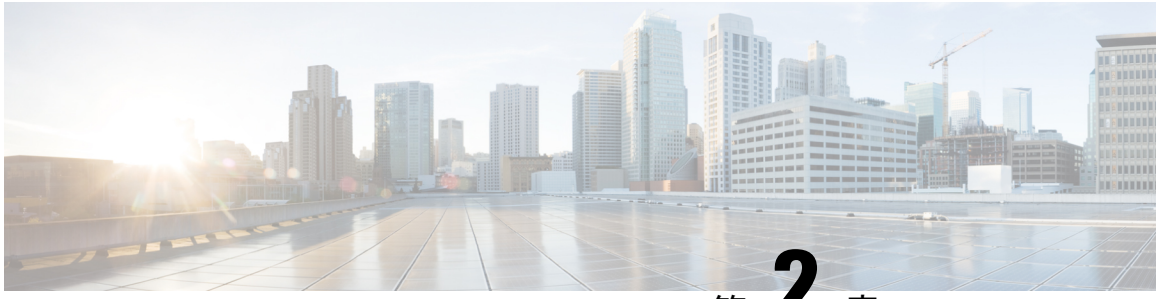
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS Command References, All Releases』

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

基本ファイル転送サービスの設定

基本ファイル転送サービスを使用すると、ルータを簡易ファイル転送プロトコル（TFTP）または逆アドレス解決プロトコル（RARP）サーバとして設定、そのルータが拡張 BOOTP 要求を非同期インターフェイス経由で転送するよう設定、および rcp、rsh、FTP を設定することが可能です。

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。

基本ファイル転送サービスの前提条件

- ユーザには、少なくとも Cisco IOS 環境とコマンドライン インターフェイスに関する基本的な知識が必要です。
- システムでは、少なくとも最小限の設定が実行されていることが必要です。

基本ファイル転送サービスに関する制約事項

- ネットワークが稼働していて、Cisco IOS リリース 12.2 以降のリリースがすでにインストールされている必要があります。
- Cisco IOS コンフィギュレーション コマンドのいくつかは、特定のルータ プラットフォームでのみ使用可能であり、コマンド構文はプラットフォームによって異なる可能性があります。

基本ファイル転送サービスに関する情報

TFTP または RARP サーバとしてのルータの使用

サーバとしてだけ機能するマシンをネットワークの各セグメントに配置するのは、コストがかかり、非効率的です。しかし、すべてのセグメントにサーバがあるのではない場合、ネットワーク セグメントを超えたネットワークの操作によって相当の遅延が引き起こされることがあります。ルータを RARP または TFTP サーバとして機能するよう設定することで、ルータの通常の機能を使用しながらコストと遅延時間を削減できます。

多くの場合、TFTP または RARP サーバとして設定されたルータは、フラッシュ メモリから他のルータにシステム イメージまたはルータ コンフィギュレーション ファイルを提供します。リクエストのような他のタイプのサービス要求に応答するよう、ルータを設定することもできます。

TFTP サーバとしてのルータの使用

TFTP サーバ ホストとして、ルータは TFTP 読み取り要求メッセージに応答し、ROM に含まれるシステム イメージのコピー、またはフラッシュ メモリに含まれるシステム イメージの 1 つを、要求したホストに送出します。TFTP 読み取り要求メッセージは、コンフィギュレーションで指定されたファイル名のいずれかを使用する必要があります。

（注） Cisco 7000 ファミリでは、使用されるファイル名はフラッシュ メモリ内に存在するソフトウェア イメージを表している必要があります。フラッシュ メモリ内にイメージが存在しない場合、クライアント ルータはデフォルトとしてサーバの ROM イメージをブートします。

フラッシュ メモリは、ネットワーク内の他のネットワークの TFTP ファイル サーバとして使用できます。この機能により、リモートのルータをフラッシュ サーバ メモリ内に存在するイメージを使用してブートすることが可能になります。

シスコデバイスの中には、TFTP サーバとして、さまざまなフラッシュ メモリ位置（**bootflash:**、**slot0:**、**slot1:**、**slavebootflash:**、**slaveslot0:**、または **slaveslot1:**）から 1 つを選択できるものもあります。

RARP サーバとしてのルータの使用

逆アドレス解決プロトコル（RARP）は、MAC（物理）アドレスをもとに IP アドレスを検索する方法をそなえた、TCP/IP スタックのプロトコルです。ブロードキャスト Address Resolution Protocol（ARP）の逆であるこの機能により、ネットワーク層の特定の IP アドレスに対応する MAC レイヤ アドレスをホストが動的に検出できます。RARP はさまざまなシステムをディスクなしで起動させることを可能にします（たとえば、クライアントとサーバが別のサブネットにあるネットワークの Sun ワークステーションや PC のように、起動時点では IP アドレスがわからないディスクレス ワークステーション）。RARP は、MAC レイヤから IP アドレスへのマッピングのキャッシュされたエントリの表を持つ RARP サーバの存在に依存しています。

Cisco ルータは RARP サーバとして設定できます。この機能で、Cisco IOS ソフトウェアは RARP 要求に応答することができます。

Rsh および rcp 用ルータの使用

リモート シェル（rsh）により、コマンドをリモートで実行できるようになります。リモート コピー（RCP）を使用すると、ユーザはネットワーク上のリモート ホストやサーバに存在するファイル システムへのファイル コピーや、ファイル システムからのコピーが行えます。シスコの rsh および rcp の実装は、業界標準の実装と相互運用できます。シスコでは、rsh と rcpの両方を示すために、省略形 RCMD（Remote Command、リモート コマンド）を使用します。

RCMD 送信の発信元インターフェイス

RCMD（rsh と rcp）通信の発信元インターフェイスを指定できます。たとえば、RCMD 接続でループバック インターフェイスをルータから送信されるすべてのパケットの送信元アドレスとして使用するように、ルータを設定できます。source-interface を指定するのは、ループバック インターフェイスの指定に最も一般的に使用される方法です。これにより、RCMD 通信にパーマネント IP アドレスを関連付けることができます。パーマネント IP アドレスを持つことは、セッションの識別に役立ちます（リモート デバイスがセッションの間パケットの送信元を一貫して識別できます）。「既知の」IPアドレスも、アドレスを含めてリモート デバイスにアクセス リストを作成できるよう、セキュリティの目的で使用できます。

RCMD の DNS 逆引き参照について

基本的なセキュリティ チェックとして、Cisco IOS ソフトウェアでは、リモート コマンド（RCMD）アプリケーション（rsh および rcp）の DNS を使用してクライアント IP アドレスの逆引き参照を実行します。このチェックは、ホスト認証プロセスを使用して実行されます。

イネーブルにされている場合、システムは要求元のクライアントのアドレスを記録します。アドレスは、DNS を使用してホスト名にマッピングされます。次に、そのホスト名の IP アドレスに対する DNS リクエストが行われます。受け取った IP アドレスが、元の要求元アドレスと照合されます。そのアドレスが、DNS から受信したアドレスのいずれにも一致しない場合、RCMD 要求は処理されません。

この逆引き参照は、「スプーフィング」に対する保護を促進するためのものです。ただし、このプロセスでは当該 IP アドレスが有効かつルーティング可能なアドレスであることを確認す

るのみであり、ハッカーは引き続き既知のホストの有効な IP アドレスをスプーフィングできるということに注意してください。

rsh の導入

rsh（リモート シェル）を使用すると、アクセス可能なリモート システム上でコマンドを実行できます。**rsh** コマンドを発行すると、リモート システム上でシェルが起動します。シェルにより、ターゲット ホストにログインすることなくリモート システム上でコマンドを実行できます。

そのシステムへの接続、ルータ、アクセス サーバ、さらにコマンド実行後の切断も、rsh を使えば必要ありません。たとえば、rsh を使用すれば、ターゲット デバイスへの接続やコマンドの実行、切断といった手順なしに、リモートで他のデバイスのステータスを見ることができます。この機能は、多数の異なるルータの統計情報を見る場合に役立ちます。rsh を有効化するコンフィギュレーション コマンドは、「remote command（リモート コマンド）」の略語である「rcmd」を使用します。

rsh セキュリティの維持

rshが動作しているリモートシステム（UNIXホストなど）にアクセスするためには、そのユーザがリモートからそのシステムでコマンドを実行する権限を与えられていることを示すエントリが、システムの*.rhosts*ファイルまたはそれに相当するものに存在している必要があります。UNIX システムでは、*.rhosts* ファイルはシステムのコマンドをリモートで実行できるユーザを特定します。

ルータ上のrshサポートを有効化すると、リモート システム上のユーザがコマンドを実行できるようになります。しかし、シスコのrshの実装は、*.rhosts*ファイルをサポートしていません。その代わりに、rsh を使用してリモートでコマンドを実行しようとするユーザによるルータへのアクセスを制御するため、ローカルの認証データベースを設定する必要があります。ローカルの認証データベースは、UNIX *.rhosts* ファイルに似ています。認証データベースで設定する各エントリでは、ローカル ユーザ、リモート ホスト、およびリモート ユーザを特定します。

rcp の導入

リモート コピー（rcp）コマンドは、リモート システムの rsh サーバ（またはデーモン）に依存します。RCPを使用してファイルをコピーする場合、TFTPと異なり、ファイル配布用のサーバを作成する必要はありません。必要なのは、リモート シェル（rsh）をサポートするサーバへのアクセスだけです（ほとんどの UNIX システムが rsh をサポートしています）。ある場所から別の場所にファイルをコピーするため、コピー元のファイルに対する読み取り権限とコピー先のディレクトリに対する書き込み権限が必要です。コピー先ファイルが存在しない場合は、rcp により作成されます。

シスコの rcp 実装は UNIX の rcp 実装（ネットワーク上のシステム間でファイルをコピー）の関数をエミュレートしたものですが、シスコのコマンド構文は UNIX の rcp コマンド構文とは異なります。Cisco IOS ソフトウェアには、rcpをトランスポート メカニズムとして使用する一群のコピー コマンドがあります。これらの rcp コピー コマンドは Cisco IOS TFTP コピー コマンドと類似していますが、より高速なパフォーマンスと信頼性の高いデータ配信を可能にする代替案になっています。このような改善が可能なのは、rcp トランスポート メカニズムが組み

込まれており、Transmission Control Protocol/Internet Protocol（TCP/IP）スタックを使用しているためです。rcp コマンドを使用して、ルータからネットワークサーバ（またはその逆）へシステム イメージおよびコンフィギュレーション ファイルをコピーできます。

また、rcp サポートをイネーブルにすることで、リモート システムのユーザによるルータへの、またはルータからのファイル コピーを許可できます。

/user キーワードおよび引数を指定しない場合、Cisco IOS ソフトウェアはデフォルトのリモート ユーザ名を送信します。リモート ユーザ名のデフォルト値として、現在の TTY プロセスと関連付けられたリモートユーザ名が有効である場合、ソフトウェアはそのユーザ名を送信します。TTY リモート ユーザ名が無効な場合、ソフトウェアはリモートとローカルのユーザ名の両方にルータのホスト名を使用します。

rcp 要求の送信側リモート クライアントの設定

rcp プロトコルでは、クライアントは rcp 要求ごとにリモート ユーザ名をサーバに送信する必要があります。rcp を使用してコンフィギュレーション ファイルをサーバからルータへコピーする場合、Cisco IOS ソフトウェアは次のリストから、最初の有効なユーザ名を送信します。

1. **ip rcmd remote-username** コマンドで設定されたユーザ名（このコマンドが設定されている場合）。
2. 現在の TTY（端末）プロセスに関連付けられているリモートユーザ名。たとえば、ユーザが Telnet を介してルータに接続されていて、**username** コマンドを介して認証された場合は、リモート ユーザ名として Telnet ユーザ名がルータ ソフトウェアによって送信されます。

（注） シスコ製品では、TTY がサーバへのアクセスに広く使用されています。TTY の概念は、UNIX に由来します。UNIX システムでは、各物理デバイスがファイル システムで表現されます。端末は *tty* デバイスと呼ばれます（tty は、UNIX 端末の *teletype* が元になった省略形です）。

1. ルータのホスト名。

rcp を使用した **boot** コマンドで、ソフトウェアはルータ ホスト名を送信します。リモート ユーザ名の明示的な設定はできません。

rcp コピー要求が正常に実行されるためには、ネットワーク サーバ上でリモート ユーザ名のアカウントが定義されている必要があります。

サーバに書き込む場合、ルータ上のユーザからの rcp 書き込み要求を受け入れるように、rcp サーバを適切に設定する必要があります。UNIX システムの場合は、rcp サーバ上のリモート ユーザの *.rhosts* ファイルに対しエントリを追加する必要があります。たとえば、ルータに次の設定行が含まれているとします。

```
hostname Rtr1
ip rcmd remote-username User0
```

そのルータの IP アドレスを Router1.company.com と変換するとすれば、rcp サーバの User0 の *.rhosts* ファイルは、次の行を含んでいる必要があります。

```
Router1.company.com Rtr1
```

詳細については、ご使用の RCP サーバのマニュアルを参照してください。

このサーバがディレクトリ構造をとっている場合、コンフィギュレーションファイルまたはイメージは、サーバ上のリモートユーザ名と関連付けられたディレクトリに関連して書き込まれるか、そのディレクトリからコピーされます。サーバ上で使用するディレクトリを指定するには、**ip rcmd remote-username** コマンドを使用します。たとえば、システム イメージがサーバ上のあるユーザのホーム ディレクトリに存在する場合、そのユーザの名前をリモート ユーザ名として指定します。

ファイル サーバとして使用されているパーソナル コンピュータにコンフィギュレーション ファイルをコピーする場合、このコンピュータでは rsh がサポートされている必要があります。

FTP 接続用ルータの使用

ネットワーク上のシステム間で File Transfer Protocol（FTP）を使用してファイルを転送するよう、ルータを設定できます。Cisco IOS に実装された FTP により、次の FTP 特性を設定できます。

- パッシブ モード FTP
- ユーザ名
- パスワード
- IP アドレス

基本ファイル転送サービスの設定方法

TFTP サーバとしてのルータの使用の設定

ルータが TFTP サーバとして使用されるよう設定するには、このセクションのタスクを実行します。

始める前に

TFTP 機能の実装前に、サーバとクライアント ルータは互いに到達可能である必要があります。**ping***a.b.c.d* コマンドを使用して（*a.b.c.d* はクライアント デバイスのアドレス）サーバとクライアント ルータとの接続をテストし（いずれかの方向で）、この接続を確認します。**ping** コマンドが発行されると、接続されたことが、一連の感嘆符（!）によって表示されます。接続に失敗した場合は、一連のピリオド（.）に加えて [timed out] または [failed] が表示されます。

接続に失敗し、インターフェイスを再設定する場合は、フラッシュ サーバとクライアント ルータとの間の物理的な接続をチェックし、ping を再実行します。

接続をチェックした後、TFTP ブート可能イメージがサーバ上に存在することを確認します。これは、クライアント ルータがブートするシステム ソフトウェア イメージです。最初のクライアント ブートの後で確認できるように、そのソフトウェア イメージの名前を記録しておきます。

⚠

注意 すべての機能を使用するために、クライアントに送信されるソフトウェアイメージは、クライアント ルータにインストールされた ROM ソフトウェアと同一のタイプのものである必要があります。たとえば、サーバには X.25 ソフトウェアがあり、クライアントの ROM には X.25 ソフトウェアがない場合、フラッシュ メモリ内にあるサーバのイメージからブートしてからも、クライアントには X.25 の機能がありません。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを実行します。
   - **tftp-server flash** [*partition-number*:]*filename1* [**alias***filename2*] [*access-list-number*]
   - **tftp-server flash** *device* **:** *filename*（Cisco 7000 ファミリのみ）
   - **tftp-server flash** [*device*:][*partition-number*:]*filename* （Cisco 1600 シリーズと Cisco 3600 シリーズのみ）
   - **tftp-server rom alias** *filename1* [*access-list-number*]
4. **end**
5. **copy running-config startup-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： `Device> 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： `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	次のいずれかを実行します。 • **tftp-server flash** [*partition-number*:]*filename1* [**alias***filename2*] [*access-list-number*]	読み取り要求の応答として送信されるシステム イメージを指定します。複数行を入力して複数のイメージを指定することができます。

	コマンドまたはアクション	目的
	• **tftp-server flash** *device* **:** *filename*（Cisco 7000 ファミリのみ） • **tftp-server flash** [*device***:**][*partition-number***:**]*filename*（Cisco 1600 シリーズと Cisco 3600 シリーズのみ） • **tftp-server rom alias** *filename1* [*access-list-number*] 例： `Device(config)# tftp-server flash version-10.3 22`	
ステップ 4	**end** 例： `Device(config)# end`	コンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	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 ファイルに保存します。

例

次の例では、フラッシュ メモリ ファイル *version-10.3* の TFTP 読み取りリクエストへの応答として、システムは TFTP を使用してこのファイルのコピーを送信できます。要求送出ホストはアクセス リスト 22 でチェックされます。

```
tftp-server flash version-10.3 22
```

次の例では、ROM イメージ *gs3-k.101* ファイルについての TFTP 読み取り要求への応答として、システムは TFTP を使用して *gs3-k.101* ファイルのコピーを送信できます。

```
tftp-server rom alias gs3-k.101
```

次の例では、TFTP 読み取り要求への応答として、ルータがフラッシュ メモリ内のファイル *gs7-k.9.17* のコピーを送信します。クライアント ルータはアクセス リスト 1 で指定されたネットワーク内に存在している必要があります。したがって、この例では、ネットワーク 172.16.101.0 にあるすべてのクライアントがファイルへのアクセスを許可されます。

```
Server# configure terminal

Enter configuration commands, one per line. End with CTRL/Z
Server(config)# tftp-server flash gs7-k.9.17 1

Server(config)# access-list 1 permit 172.16.101.0 0.0.0.255
```

```
Server(config)# end

Server# copy running-config startup-config

[ok]
Server#
```

トラブルシューティング

TFTP セッションには障害が発生することがあります。TFTP は TFTP セッション障害の原因判別のために、次の特別な文字を生成します。

- 文字「E」は、TFTP サーバがエラーを含むパケットを受信したことを示します。
- 文字「O」は、TFTP サーバがシーケンスに合わないパケットを受信したことを示します。
- ピリオド（.）はタイムアウトを示します。

転送中の不適当な遅延を診断するために、この出力が役立ちます。トラブルシューティングの手順については、マニュアル『*Internetwork Troubleshooting Guide*』を参照してください。

クライアント ルータの設定

最初にサーバからシステムイメージをロードし、次にバックアップとして、サーバからのロードに失敗した場合に自身の ROM イメージをロードするようクライアント ルータを設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no boot system**
4. **boot system** [**tftp**] *filename* [*ip-address*]
5. **boot system rom**
6. **config-register** *value*
7. **end**
8. **copy running-config startup-config**
9. **reload**

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： `Device> 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）。

	コマンドまたはアクション	目的
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	**no boot system** 例： `Device(config)# no boot system`	（任意）これまでの **bootsystem** 文をすべてコンフィギュレーション ファイルから削除します。
ステップ 4	**boot system** [**tftp**] *filename* [*ip-address*] 例： `Device(config)# boot system c5300-js-mz.121-5.T.bin 172.16.1.1`	クライアント ルータがサーバからシステム イメージをロードするよう指定します。
ステップ 5	**boot system rom** 例： `Device(config)# boot system rom`	クライアントルータがサーバからのロードに失敗した場合に、自身の ROM イメージをロードするように指定します。
ステップ 6	**config-register** *value* 例： `Device(config)# config-register 0x010F`	クライアント ルータがネットワーク サーバからシステムイメージをロードできるよう、コンフィギュレーション レジスタを設定します。
ステップ 7	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 8	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	コンフィギュレーションファイルをスタートアップ コンフィギュレーションに保存します。
ステップ 9	**reload** 例： `Device# reload`	（任意）変更を有効にするため、ルータをリロードします。

例

次の例では、ルータは指定の TFTP サーバからブートするよう設定されます。

```
Client# configure terminal

Enter configuration commands, one per line. End with CTRL/Z
Client(config)# no boot system

Client(config)# boot system c5300-js-mz.121-5.T.bin 172.16.1.1

Client(config)# boot system rom

Client(config)# config-register 0x010F

Client(config)# end

Client# copy running-config startup-config

[ok]
Client# reload
```

この例では、**nobootsystem** コマンドによって、現在コンフィギュレーション メモリ内にある他の **bootsystem** コマンドがすべて無効化され、このコマンドの後に入力される **bootsystem** コマンドが先に実行されるようになります。2 番目のコマンドである **bootsystem***filename address* は、クライアント ルータに対し、IP アドレスが 172.16.111.111 の TFTP サーバにあるファイル c5300-js-mz.121-5.T.bin を探すよう指示しています。これが失敗した場合、クライアント ルータは、ネットワーク障害が生じた場合のバックアップとして含まれている **bootsystemrom** コマンドに応答して、自身のシステム ROM からブートします。**copyrunning-configstartup-config** コマンドは、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へコピーし、**reload** コマンドがシステムをブートします。

（注） サーバからブートするためのシステム ソフトウェアは、サーバのフラッシュ メモリ内に存在している必要があります。フラッシュ メモリにない場合、クライアント ルータはサーバのシステム ROM からブートします。

次の例に、ルータの再起動後に **showversion** コマンドを実行した場合の出力例を示します。

```
Device> show version
Cisco Internetwork Operating System Software
Cisco IOS (tm) 5300 Software (C5300-JS-M), Version 12.1(5)T,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Sat 11-Nov-00 03:03 by joe
Image text-base: 0x60008958, data-base: 0x611C6000
ROM: System Bootstrap, Version 11.2(9)XA, RELEASE SOFTWARE (fc2)
BOOTFLASH: 5300 Software (C5300-BOOT-M), Version 12.0(7)T,  RELEASE SOFTWARE (f)
Router uptime is 8 weeks, 4 days, 22 hours, 36 minutes
System returned to ROM by power-on
System restarted at 00:37:38 UTC Thu Feb 22 2001
System image file is "flash:c5300-js-mz.121-5.T.bin"
.
.
.
Configuration register is 0x010F
```

この例の重要情報は、最初の行の「Cisco IOS (tm)..」と「System image file....」で始まる行とに含まれています。「Cisco IOS (tm)...」という行では、NVRAM のオペレーティング システムのバージョンが表示されています。「System image file....」という行は、TFTP サーバからロードされたシステム イメージのファイル名を表示しています。

次の作業

システムをリロードしたら、**showversion** EXEC モード コマンドを使用して、目的とするイメージでシステムがブートしたことを確認する必要があります。

⚠

注意 次の例にあるとおり、**nobootsystem** コマンドを使用すると、現在クライアント ルータのシステム コンフィギュレーションにある他のブート システム コマンドがすべて無効化されます。次に進む前に、バックアップ コピーの目的でクライアント ルータに格納されたシステム コンフィギュレーションを先に TFTP ファイル サーバに保存するか（アップロードするか）を決定します。

RARP サーバとしてのルータの設定

ルータを RARP サーバに設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type* [*slot*/]*port*
4. **ip rarp-server** *ip-address*

手順の詳細

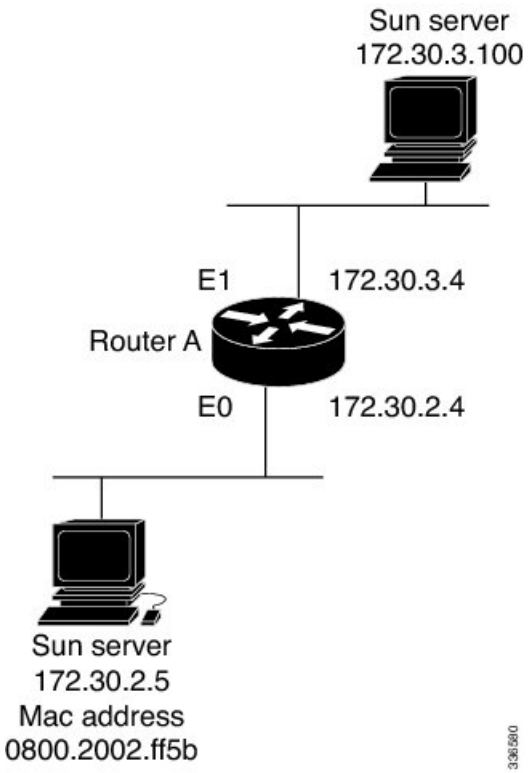
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type* [*slot*/]*port* 例： `Device(config)# interface Gigabitethernet 0/0`	RARP サービスを設定するインターフェイスを指定し、指定したインターフェイスのインターフェイス 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 4	**ip rarp-server** *ip-address* 例： `Device(config-if)# ip rarp-server 172.30.3.100`	ルータの RARP サービスを有効化します。

例

以下の図は、ルータがディスクレス ワークステーションの RARP サーバとして機能するネットワークの設定を示しています。この例では、Sun ワークステーションは自身の MAC（ハードウェア）アドレスを IP アドレスに解決するために SLARP 要求を送信し、要求はルータによって Sun サーバへ転送されます。

図 *1 : RARP* サーバとしてのルータの設定



ルータ A は次のように設定されています。

```
! Allow the router to forward broadcast portmapper requests
ip forward-protocol udp 111
! Provide the router with the IP address of the diskless sun
arp 172.30.2.5 0800.2002.ff5b arpa
interface Gigabitethernet 0/0
! Configure the router to act as a RARP server, using the Sun Server's IP
! address in the RARP response packet.
```

```
ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
ip helper-address 172.30.3.100
```

Sun のクライアントとサーバの IP アドレスには、現在の SunOS デーモン *rpc.bootparamd* での制限により、同じメジャー ネットワーク番号を使用する必要があります。

次の例では、アクセス サーバが RARP サーバとして機能するよう設定されています。

```
! Allow the access server to forward broadcast portmapper requests
 ip forward-protocol udp 111
! Provide the access server with the IP address of the diskless sun
 arp 172.30.2.5 0800.2002.ff5b arpa
 interface Gigabitethernet 0/0
! Configure the access server to act as a RARP server, using the Sun Server's
! IP address in the RARP response packet.
 ip rarp-server 172.30.3.100
! Portmapper broadcasts from this interface are sent to the Sun Server.
 ip helper-address 172.30.3.100
```

rsh および rcp を使用するためのルータの設定

RCMD 送信での送信元インターフェイスの指定

RCMD 接続でルータから送信されるすべてのパケットの送信元アドレスとしてループバック インターフェイスを使用するようにルータを設定するには、このセクションのタスクを実行することにより、RCMD 通信に関連付けられている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 rcmd source-interface** *interface-id*

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： `Device> 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： `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。

	コマンドまたはアクション	目的
ステップ 3	**ip rcmd source-interface** *interface-id* 例： `Device(config)# ip rcmd source-interface`	rsh と rcp のすべての送信トラフィックにラベル付けするために使用するインターフェイス アドレスを指定します。

RCMD の DNS 逆引き参照の無効化

rcmd の DNS 逆引き参照はデフォルトで有効化されています。このセクションのタスクを実行することにより、RCMD（rsh および rcp）アクセスの DNS チェックを無効化できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip rcmd domain-lookup**

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： `Device> 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： `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	**no ip rcmd domain-lookup** 例： `Device(config)# no ip rcmd domain-lookup`	リモート コマンド（RCMP）アプリケーション（rsh および rcp）の Domain Name Service（DNS）逆ルックアップ機能をディセーブルにします。

リモート ユーザが rsh を使用してコマンドを実行できるようにするためのルータの設定

リモート ユーザが rsh を使用してコマンドを実行できるようにルータを設定するには、このセクションのタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]]
4. **ip rcmd rsh-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： `Device> 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： `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	**ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]] 例： `Device(config)# ip rcmd remote-host Router1 172.16.101.101 netadmin4 enable`	ローカル認証データベースで、rsh コマンド実行を許可するリモートユーザそれぞれにエントリを作成します。
ステップ 4	**ip rcmd rsh-enable** 例： `Device(config)# ip rcmd rsh-enable`	ソフトウェアの受信 rsh コマンドのサポートをイネーブルにします。 （注） ソフトウェアの受信 rsh コマンドのサポートを無効化するには、**noiprcmdrsh-enable** コマンドを使用します。 （注） 受信 rsh コマンドのサポートがディセーブルにされた場合でも、リモート シェル プロトコルをサポートする他のルータおよびネットワーク上の UNIX ホストで実行される rsh コマンドを発行することができます。

例

次に、リモート ユーザのために 2 つのエントリを認証データベースに追加し、リモート ユーザからの rsh コマンドをサポートするようルータをイネーブルにする例を示します。

```
ip rcmd remote-host Router1 172.16.101.101 rmtnetad1
ip rcmd remote-host Router1 172.16.101.101 netadmin4 enable
ip rcmd rsh-enable
```

名前が *rmtnetad1* というユーザと *netadmin4* というユーザはいずれも、リモート ホストの IP アドレス 172.16.101.101 に存在します。ユーザはいずれも同じリモート ホスト上

にいますが、各ユーザに対して一意のエントリを含める必要があります。ルータを rsh に対して有効化すると、いずれのユーザも、そのルータに接続してリモートで rsh コマンドを実行できるようになります。*netadmin4* という名前のユーザは、ルータ上での特権 EXEC モード コマンドの実行を許可されます。認証データベース上のいずれのエントリも、ローカルのユーザ名として、ルータのホスト名 *Router1* を使用します。最後のコマンドで、リモート ユーザが発行した rsh コマンドのルータでのサポートを有効化します。

rsh を使用したリモートでのコマンド実行

rsh を使用してリモートからネットワーク サーバでコマンドを実行するには、ユーザ EXEC モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **rsh** {*ip-address* | *host* } [/**user***username*] *remote-command*

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： `Device> 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	**rsh** {*ip-address* | *host* } [/**user***username*] *remote-command* 例： `Device# rsh mysys.cisco.com /user sharon ls -a`	rsh を使用してリモートからコマンドを実行します。

例

次の例では、mysys.cisco.com 上で、ユーザ sharon のホーム ディレクトリから rsh を使用して「ls -a」コマンドを実行します。

```
Device# enable
Device# rsh mysys.cisco.com /user sharon ls -a
.
..
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
```

```
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
jazz
Device#
```

リモート ユーザからの rcp 要求受け入れのためのルータ設定

Cisco IOS ソフトウェアが受信 rcp 要求をサポートするよう設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]]
4. **ip rcmd rcp-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： `Device> 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： `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	**ip rcmd remote-host** *local-username* {*ip-address* | *host* } *remote-username* [**enable**[*level*]] 例： `Device(config)# ip rcmd remote-host Router1 172.16.101.101 netadmin3`	ローカルの認証データベースで、rcp コマンドの実行を許可されているリモートユーザそれぞれにエントリを作成します。 （注） ソフトウェアの受信 rcp 要求のサポートを無効化するには、**noiprcmdrcp-enable** コマンドを使用します。 （注） 受信 rcp 要求のサポートをディセーブルにした場合でも、rcp コマンドを使用してリモート サーバへイメージをコピーできます。受信 rcp 要求のサポートは、発信 rcp 要求を扱う際の機能とは異なっています。

	コマンドまたはアクション	目的
ステップ 4	**ip rcmd rcp-enable** 例： `Device(config)# ip rcmd rcp-enable`	ソフトウェアの受信 rcp 要求のサポートをイネーブルにします。

例

次の例に、認証データベースにリモート ユーザ用の 2 つのエントリを追加してから、ソフトウェアでリモートユーザからのリモートコピー要求のサポートを有効化する方法を示します。IP アドレス 172.16.15.55 のリモート ホストの *netadmin1* というユーザと、IP アドレス 172.16.101.101 のリモート ホストの *netadmin3* というユーザは両方とも、ルータへの接続、およびルータが rcp サポートをイネーブル化した後にリモートから rcp コマンドを実行することを許可されます。認証データベース上のいずれのエントリも、ローカルのユーザ名として、ホスト名 *Router1* を使用します。最後のコマンドで、リモートユーザからの rcp 要求のルータでのサポートをイネーブルにします。

```
ip rcmd remote-host Router1 172.16.15.55 netadmin1
ip rcmd remote-host Router1 172.16.101.101 netadmin3
ip rcmd rcp-enable
```

rcp 要求の送信側リモートの設定

rcp 要求で送信されるデフォルトのリモート ユーザ名を上書きするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip rcmd remote-username** *username*

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： `Device> 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： `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。

	コマンドまたはアクション	目的
ステップ 3	**ip rcmd remote-username** *username* 例： `Device(config)# ip rcmd remote-username sharon`	リモート ユーザ名を指定します。 （注） リモート ユーザ名を削除してデフォルト値に戻すには、**noiprcmdremote-username** コマンドを使用します。

FTP 接続使用時のルータ設定

ネットワークのシステム間で File Transfer Protocol（FTP）を使用してファイルを転送するようルータを設定して、このセクションのタスクである FTP 特性の設定を完了するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip ftp username** *string*
4. **ip ftp password** [*type*] *password*
5. 次のいずれかを実行します。
   - **ip ftp passive**
   -
   -
   - **no ip ftp passive**
6. **ip ftp source-interface** *interface*

手順の詳細

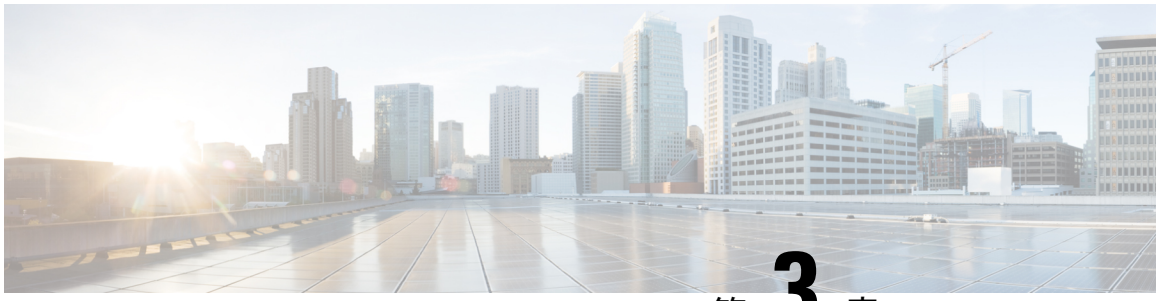
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ftp username** *string* 例： `Device(config)# ip ftp username zorro`	FTP 接続で使用されるユーザ名を指定します。

	コマンドまたはアクション	目的
ステップ 4	**ip ftp password** [*type*] *password* 例： `Device(config)# ip ftp password sword`	FTP 接続で使用されるパスワードを指定します。
ステップ 5	次のいずれかを実行します。 • **ip ftp passive** • • • **no ip ftp passive** 例： `Device(config)# ip ftp passive`	パッシブ モード FTP 接続のみを使用するようルータを設定します。 または すべてのタイプのFTP 接続（デフォルト）を許可します。
ステップ 6	**ip ftp source-interface** *interface* 例： `Device(config)# ip ftp source-interface to1`	FTP 接続の発信元 IP アドレスを指定します。

例

次の例に、Cisco IOS の FTP 機能を使用してコア ダンプを取り込む方法を示します。ルータはログイン名 zorro とパスワード sword により IP アドレス 192.168.10.3 でサーバにアクセスします。デフォルトのパッシブ モード FTP が使用され、コア ダンプが発生するルータ上のトークン リング インターフェイス to1 を使用してサーバへのアクセスが行われます。

```
ip ftp username zorro
ip ftp password sword
ip ftp passive
ip ftp source-interface to1
! The following command allows the core-dump code to use FTP rather than TFTP or RCP
exception protocol ftp
! The following command identifies the FTP server
! 192.168.10.3 crashes
exception dump 192.168.10.3
```



第 3 章

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

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。