Cisco IOS Configuration Fundamentals コンフィギュレーション ガイド

Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.1S

リリース 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco IOS Configuration Fundamentals コンフィギュレーション ガイド

Cisco IOS コマンドライン インターフェイス（CLI）の使用

Cisco IOS コマンドライン インターフェイスの使用

Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）は、シスコ デバイスを設定、モニタリング、メンテナンスするための主要なユーザ インターフェイスです。このユーザ インターフェイスでは、ルータ コンソールまたは端末を使用するか、リモート アクセス方式を使用して、直接簡単に Cisco IOS コマンドを実行できます。

この章では、Cisco IOS CLI の基本的な機能とその使用方法について説明します。この章で扱うトピックは、Cisco IOS コマンド モードの概要、ナビゲーションおよび編集機能、ヘルプ機能、コマンド履歴機能です。

これ以外のユーザ インターフェイスとしては、セットアップ モード（初回起動で使用）、シスコ Web ブラウザ、システム管理者によって設定されるユーザ メニューがあります。セットアップ モードの詳細については、『*Using Setup Mode to Configure a Cisco Networking Device*』および『Using AutoInstall to Remotely Configure Cisco Networking Devices』を参照してください。シスコ Web ブラウザを使用したコマンドの実行については、『Using the Cisco Web Browser User Interface』を参照してください。ユーザ メニューについては、『Managing Connections, Menus, and System Banners』を参照してください。

この章のユーザ インターフェイス コマンドの完全な説明については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Master Command List, All Releases*』を使用します。

機能情報の確認

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Cisco IOS CLI コマンド モードの概要

シスコ デバイスの設定を支援するために、Cisco IOS コマンドライン インターフェイスは、さまざまなコマンド モードにわかれています。各コマンド モードには、ルータとネットワークの動作を設定、メンテナンス、モニタリングするための独自のコマンド セットがあります。ある時点で使用できるコマンドは、そのときのモードに依存します。システム プロンプトに疑問符（**?**）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

特定のコマンドを使用すると、コマンド モードを変更できます。モードにアクセスする標準的な順序は、ユーザ EXEC モード、特権 EXEC モード、グローバル コンフィギュレーション モード、特定のコンフィギュレーション モード、コンフィギュレーション サブモード、およびコンフィギュレーション サブサブモードです。

ルータでセッションを開始するとき、一般にユーザ EXEC モードが開始されます。これは、EXEC モードの 2 つあるアクセス レベルのうちの 1 つです。ユーザ EXEC モードでは、セキュリティ上の目的から、EXEC コマンドの制限されたサブセットだけが使用できます。このアクセス レベルは、ルータのステータスを確認するなど、ルータの設定を変更しない作業のために予約されています。

すべてのコマンドにアクセスするには、特権 EXEC モードを開始する必要があります。これは、EXEC モードの第 2 レベルのアクセスです。通常、特権 EXEC モードを開始するにはパスワードを入力する必要があります。特権 EXEC モードでは、任意の EXEC コマンドを入力できます。これは、特権 EXEC モードが、ユーザ EXEC モード コマンドのスーパーセットであるためです。

ほとんどの EXEC モード コマンドは、現在の設定ステータスを表示する **show** コマンドまたは **more** コマンドや、カウンタやインターフェイスをクリアする **clear** コマンドのように、1 回限りのコマンドです。EXEC モードのコマンドは、ルータをリブートすると保持されません。

特権 EXEC モードからは、グローバル コンフィギュレーション モードを開始できます。このモードでは、一般的なシステム特性を設定するためのコマンドを実行できます。また、グローバル コンフィギュレーション モードを使用して特定のコンフィギュレーション モードを開始することもできます。グローバル コンフィギュレーション モードを含むコンフィギュレーションモードでは、実行コンフィギュレーションを変更できます。後で設定を保存すると、ルータをリブートしてもこれらのコマンドが保持されます。

グローバル コンフィギュレーション モードから、さまざまなプロトコル固有または機能固有のコンフィギュレーション モードを開始できます。CLI 階層では、グローバル コンフィギュレーション モードからしかこれらのコンフィギュレーション モードを開始できません。例として、この章では一般的に使用されるインターフェイス コンフィギュレーション モードについて説明します。

コンフィギュレーション モードから、コンフィギュレーション サブモードを開始できます。コンフィギュレーション サブモードは、特定のコンフィギュレーション モードの範囲内で特定の機能を設定するために使用します。例として、この章では、インターフェイス コンフィギュレーション モードのサブモードであるサブインターフェイス コンフィギュレーション モードについて説明します。

ROM モニタ モードは、ルータが正常にブートしない場合に使用する個別のモードです。システム（ルータ、スイッチ、またはアクセス サーバ）のブート時に適切なシステム イメージが見つからない場合、システムは ROM モニタ モードを開始します。ROM Monitor（ROMMON; ROM モニタ）モードには、起動時にブート シーケンスに割り込むことでもアクセスできます。

次の項では、これらのコマンド モードについて詳しく説明します。

- 「ROM モニタ モード」（P.8）

この項の後にある表 1 に、Cisco IOS の主なコマンド モードの要約を示します。

ユーザ EXEC モード

ルータにログインするとユーザ EXEC コマンド モードになります（ただし、システムがすぐに特権 EXEC モードになるように設定されている場合を除きます）。一般に、ログインにはユーザ名とパスワードが必要です。接続が拒否されるまでにパスワードを 3 回入力できます。

（注） パスワードの設定については、『Configuring Security with Passwords, Privilege Levels and, Login Usernames for CLI Sessions on Networking Devices』を参照してください。

ユーザ レベルで使用できる EXEC コマンドは、特権レベルで使用できるコマンドのサブセットです。一般に、ユーザ EXEC コマンドでは、リモート デバイスへの接続、端末回線の一時的な設定変更、基本的なテストの実行、システム情報の表示を行うことができます。

使用可能なユーザ EXEC コマンドの一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Router> ?`	ユーザ EXEC コマンドの一覧を表示します。

ユーザ EXEC モードのプロンプトは、次の例に示すように、デバイスのホスト名と山カッコ（>）からなります。

```
Router>
```

setup EXEC コマンドを使用した初期設定の際に変更されていない限り、デフォルトのホスト名は Router です。グローバル コンフィギュレーション コマンド **hostname** を使用してホスト名を変更することもできます。

（注） Cisco IOS のマニュアルの例では、デフォルトの名前である「Router」を使用しているものと仮定しています。デバイスが異なれば（アクセス サーバなど）、デフォルトの名前も異なります。ルーティング デバイス（ルータ、アクセス サーバ、またはスイッチ）に、**hostname** コマンドで名前が設定されている場合、デフォルトの名前の代わりにその名前がプロンプトに表示されます。

ユーザ EXEC モードで使用できるコマンドの一覧を表示するには、次の例に示すように疑問符（**?**）を入力します。

```
Router> ?

Exec commands:
 <1-99>           Session number to resume
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from Exec mode
 help             Description of the interactive help system
 lat              Open a lat connection
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from Exec mode and log out
 menu             Start a menu-based user interface
```

```
mbranch           Trace multicast route for branch of tree
mrbranch          Trace reverse multicast route to branch of tree
mtrace            Trace multicast route to group
name-connection   Name an existing telnet connection
pad               Open a X.29 PAD connection
ping              Send echo messages
resume            Resume an active telnet connection
show              Show running system information
systat            Display information about terminal lines
telnet            Open a telnet connection
terminal          Set terminal line parameters
tn3270            Open a tn3270 connection
trace             Trace route to destination
where             List active telnet connections
x3                Set X.3 parameters on PAD
```

コマンドの一覧は、ソフトウェアの機能セットと、使用しているルータ プラットフォームに依存します。

（注） コマンドは、大文字でも、小文字でも、大文字と小文字が混在していてもかまいません。大文字と小文字が区別されるのはパスワードだけです。ただし、Cisco IOS のマニュアルの表記法では、コマンドは常に小文字になっています。

特権 EXEC モード

多くの特権 EXEC モードのコマンドは動作パラメータを設定するため、特権レベルのアクセスはパスワードで保護し、不正使用を防ぐ必要があります。特権 EXEC コマンド セットには、ユーザ EXEC モードのコマンドが含まれます。また、特権 EXEC モードでは、**configure** コマンドを使用することで各種コンフィギュレーション モードにアクセスでき、**debug** などの高度なテスト コマンドも含まれています。

特権 EXEC モードのプロンプトは、次の例に示すように、デバイスのホスト名とポンド記号（#）からなります。

```
Router#
```

特権 EXEC モードにアクセスするには、次のコマンドを使用します。

コマンド	目的
`Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。

特権 EXEC モードは、「イネーブル モード」と呼ばれることもあります。これは、このモードを開始するために **enable** コマンドを使用するためです。

システムでパスワードが設定されている場合、特権 EXEC モードへのアクセスが許可される前にパスワードを入力するよう求められます。パスワードは画面上に表示されず、大文字と小文字が区別されます。enable password が設定されていない場合、特権 EXEC モードには、ルータ コンソール（コンソール ポートに接続された端末）からしかアクセスできません。特権モードへのアクセスを制限するためにパスワードを設定するには、システム管理者はグローバル コンフィギュレーション モードで **enable secret** または **enable password** コマンドを使用します。パスワードの設定については、『*Cisco IOS Security Configuration Guide: Securing User Services*』の「Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices」の章を参照してください。

ユーザ EXEC モードに戻るには、次のコマンドを使用します。

コマンド	目的
Router# **disable**	特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。

次に、特権 EXEC モードにアクセスするプロセスの例を示します。

```
Router> enable
Password:<letmein>
Router#
```

パスワードは入力しても表示されませんが、ここでは説明のために表示してあることに注意してください。特権 EXEC モードで使用できるコマンドの一覧を表示するには、コマンド プロンプトで **?** コマンドを発行します。次の項で説明するように、特権 EXEC モードからグローバル コンフィギュレーション モードにアクセスできます。

（注） 特権 EXEC コマンド セットには、ユーザ EXEC モードで使用できるすべてのコマンドが含まれているため、一部のコマンドはどちらのモードでも実行できます。Cisco IOS のマニュアルでは、ユーザ EXEC モードでも特権 EXEC モードでも入力できるコマンドを EXEC モード コマンドと呼んでいます。マニュアルでユーザ EXEC モードなのか特権 EXEC モードなのかが明記されていない場合、どちらのモードでもそのコマンドを実行できるものと考えてかまいません。

グローバル コンフィギュレーション モード

「グローバル」という言葉は、システム全体に影響する特性や機能を示すために使用されています。グローバル コンフィギュレーション モードは、システムをグローバルに設定したり、インターフェイスやプロトコルなどの特定の要素を設定したりする目的で、特定のコンフィギュレーション モードを開始するために使用します。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードで **configure terminal** コマンドを使用します。

グローバル コンフィギュレーション モードにアクセスするには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **configure terminal**	特権 EXEC モードで、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。

次に、特権 EXEC モードからグローバル コンフィギュレーション モードを開始するプロセスの例を示します。

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

グローバル コンフィギュレーション モードになっていることを示すために、システム プロンプトが変化することに注意してください。グローバル コンフィギュレーション モードのプロンプトは、デバイスのホスト名（config）とポンド記号（#）からなります。特権 EXEC モードで使用できるコマンドの一覧を表示するには、コマンド プロンプトで **?** コマンドを発行します。

グローバル コンフィギュレーション モードでコマンドを入力すると、すぐに実行コンフィギュレーション ファイルが更新されます。つまり、設定に対する変更は、有効なコマンドの後で Enter キーまたは Return キーを押すたびに有効になります。ただし、これらの変更は、EXEC モードで **copy running-config startup-config** コマンドを発行しない限り、スタートアップ コンフィギュレーション ファイルに保存されません。この動作は、このマニュアルの後の項で詳しく説明します。

例に示すように、Ctrl キーと z キーを同時に押すことで、コンフィギュレーション セッションを終了（コンフィギュレーション モードを終了）できることが、システム ダイアログに表示されます。これらのキーを押すと、画面上に **^Z** と表示されます。コンフィギュレーション セッションを終了するための方法としては、実際には Ctrl+Z キーの組み合わせ、**end** コマンドの使用、Ctrl+C キーの組み合わせがあります。現在のコンフィギュレーション セッションを終了することをシステムに示すための方法としては、**end** コマンドが推奨されます。

（注） 有効なコマンドを入力してから、コマンド ラインの最後で Ctrl+Z キーを使用すると、そのコマンドが実行コンフィギュレーション ファイルに追加されます。つまり、Ctrl+Z キーを使用することは、終了前に Enter（復帰）キーを押すことと同じです。このような理由から、**end** コマンドを使用してコンフィギュレーション セッションを終了するほうが安全です。また、Ctrl+C キーの組み合わせを使用して、復帰シグナルを送信せずにコンフィギュレーション セッションを終了することもできます。

また、**exit** コマンドを使用してグローバル コンフィギュレーション モードから EXEC モードに戻ることもできますが、これはグローバル コンフィギュレーション モードだけで使用できます。Ctrl+Z キーを押すか **end** コマンドを入力することにより、どのコンフィギュレーション モードまたはコンフィギュレーション サブモードにいるかにかかわらず、常に EXEC モードに戻ることができます。

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻るには、次のいずれかのコマンドを使用します。

コマンド	目的

`Router(config)# end`
または
`Router(config)# ^Z`
	現在のコンフィギュレーション セッションを終了し、特権 EXEC モードに戻ります。

`Router(config)# exit`	現在のコマンド モードを終了して、前のモードに戻ります。たとえば、グローバル コンフィギュレーション モードを終了して特権 EXEC モードに戻ります。

グローバル コンフィギュレーション モードから、いくつかのプロトコル固有、プラットフォーム固有、機能固有のコンフィギュレーション モードを開始できます。特定のモードに関する情報は、Cisco IOS ソフトウェア マニュアル セット全体を通じて、作業ごとに説明されています。

次の項で説明するインターフェイス コンフィギュレーション モードは、グローバル コンフィギュレーション モードから開始できるコンフィギュレーション モードの 1 つの例です。

インターフェイス コンフィギュレーション モード

グローバル コンフィギュレーション モードから開始する特定のコンフィギュレーション モードの例として、インターフェイス コンフィギュレーション モードがあります。

多くの機能は、インターフェイスごとにイネーブルになります。インターフェイス コンフィギュレーション コマンドは、イーサネット、FDDI、シリアル ポートなど、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは、常にインターフェイス タイプを定義するグローバル コンフィギュレーション モードの **interface** コマンドの後に続きます。

帯域幅やクロック レートなどのように、一般的なインターフェイス パラメータに影響を与えるインターフェイス コンフィギュレーション コマンドの詳細については、『*Cisco IOS Interface and Hardware Component Configuration Guide*』を参照してください。プロトコル固有のコマンドについては、該当する Cisco IOS ソフトウェア コマンド リファレンスを参照してください。

インターフェイス コンフィギュレーション コマンドにアクセスし、その一覧を表示するには、次のコマンドを使用します。

コマンド	目的
`Router(config)# interface type number`	設定するインターフェイスを指定して、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。

次の例では、シリアル インターフェイス 0 に対するインターフェイス コンフィギュレーション モードが開始されます。新しいプロンプト hostname(config-if)# は、インターフェイス コンフィギュレーション モードを示しています。

```
Router(config)# interface serial 0
Router(config-if)#
```

インターフェイス コンフィギュレーション モードを終了しグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。

コンフィギュレーション サブモードは、他のコンフィギュレーション モード（グローバル コンフィギュレーション モード以外）から開始されるコンフィギュレーション モードです。コンフィギュレーション サブモードは、コンフィギュレーション モード内の特定の要素を設定するためにあります。コンフィギュレーション サブモードの 1 つの例は、次の項で説明するサブインターフェイス コンフィギュレーション モードです。

サブインターフェイス コンフィギュレーション モード

インターフェイス コンフィギュレーション モードから、サブインターフェイス コンフィギュレーション モードを開始できます。サブインターフェイス コンフィギュレーション モードは、インターフェイス コンフィギュレーション モードのサブモードの 1 つです。サブインターフェイス コンフィギュレーション モードでは、単一の物理インターフェイス上に複数の仮想インターフェイス（サブインターフェイスと呼びます）を設定できます。サブインターフェイスは、さまざまなプロトコルにとって個別の物理インターフェイスのように見えます。たとえば、フレーム リレー ネットワークには、Permanent Virtual Circuit（PVC; 相手先固定接続）と呼ぶ複数のポイントツーポイント リンクがあります。PVC は、個別のサブインターフェイスにグループ化して、1 つの物理インターフェイス上で設定できます。ブリッジング スパニングツリーの観点からは、各サブインターフェイスは個別のブリッジ ポートに見え、1 つのサブインターフェイスに到着したフレームは、別のサブインターフェイス上で送出できます。

また、サブインターフェイスにより、単一のインターフェイス上でプロトコルの複数のカプセル化を使用できます。たとえば、ルータまたはアクセス サーバは、Advanced Research Projects Agency（ARPA-framed）Internetwork Packet Exchange（IPX）パケットを受信し、同じ物理インターフェイスから Subnetwork Access Protocol（SNAP-framed）IPX パケットとして転送できます。

サブインターフェイスの設定方法の詳細については、Cisco IOS ソフトウェア マニュアル セットの特定のプロトコルの該当するドキュメンテーション モジュールを参照してください。

サブインターフェイス コンフィギュレーション モードにアクセスするには、インターフェイス 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。

コマンド	目的
Router(config-if)# **interface** *type number*	設定する仮想インターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。

次の例では、シリアル ライン 2 のサブインターフェイスで、フレーム リレー カプセル化を設定します。シリアル インターフェイス 2 のサブインターフェイス 1 であることを示すため、サブインターフェイスは「2.1」として識別されます。新しいプロンプト hostname(config-subif)# が、サブインターフェイス コンフィギュレーション モードを示しています。サブインターフェイスは、1 つ以上のフレーム リレー PVC をサポートするように設定できます。

```
Router(config)# interface serial 2
Router(config-if)# encapsulation frame-relay
Router(config-if)# interface serial 2.1
Router(config-subif)#
```

サブインターフェイス コンフィギュレーション モードを終了しインターフェイス コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。コンフィギュレーション セッションを終了し特権 EXEC モードに戻るには、Ctrl+Z キーを押すか、**end** コマンドを入力します。

ROM モニタ モード

ROM モニタ モード（ROMMON）は、特別なソフトウェア イメージから実行され、有効なシステム ソフトウェア イメージを手動で探して、そこからシステムをブートするために使用します（ROM モニタ モードは、「ブート モード」とも呼びます）。

システム（ルータ、スイッチ、またはアクセス サーバ）でロードするための有効なシステム イメージが見つからない場合、システムは ROM モニタ モードになります。ROM モニタ モードには、起動時にブート シーケンスに割り込むことでもアクセスできます。ROM モニタ モードから、デバイスをブートするか診断テストを実行できます。

ほとんどのシステムでは、**reload** EXEC コマンドを実行し、起動の最初の 60 秒間に Break コマンドを使用することで、ROM モニタ モードを開始できます。Break コマンドを発行するには、キーボードの Break キーを押すか、Break キーの組み合わせ（デフォルトの Break キーの組み合わせは Ctrl+C です）を使用します。

（注） Telnet 接続はシステムをリブートすると失われるため、この手順を実行するには、ルータにコンソールを接続する必要があります。

EXEC モードから ROM モニタ モードにアクセスするには、次の手順を実行します。

ステップ 1 EXEC モードで **reload** コマンドを実行します。このコマンドを実行し、必要に応じてシステム プロンプトに応答した後、システムはシステム ソフトウェア イメージのリロードを開始します。

ステップ 2 システム起動の最初の 60 秒間に Break コマンドを実行します。break コマンドを発行するには、Break キーを押すか、Break キーの組み合わせを押します（デフォルトの Break キーの組み合わせは Ctrl+C ですが、システム上で別のものに設定できます）。break コマンドを実行すると、ブート シーケンスが割り込まれ、ROM モニタ モードが開始されます。

ROM モニタ モードを開始するもう 1 つの方法は、ブート時にルータが自動的に ROM モニタ モードになるようにコンフィギュレーション レジスタを設定することです。コンフィギュレーション レジスタの設定については、『Rebooting and Reloading - Configuring Image Loading Characteristics』を参照してください。

ROM モニタ モードでは、コマンド ライン プロンプトとして山カッコ（>）が使用されます。シスコ デバイスの一部では、デフォルトの ROM モニタ モードのプロンプトは rommon > です。ROM モニタ コマンドの一覧を表示するには、**?** コマンドまたは **help** コマンドを入力します。次に、このコマンド一覧の表示例を示します。

```
User break detected at location 0x8162ac6\Œ
rommon 1 > ?

alias               set and display aliases command
boot                boot up an external process
break               set/show/clear the breakpoint
confreg             configuration register utility
cont                continue executing a downloaded image
context             display the context of a loaded image
cpu_card_type       display CPU card type
dev                 list the device table
dir                 list files in file system
dis                 disassemble instruction stream
frame               print out a selected stack frame
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 show all monitor variables
stack               produce a stack trace
sync                write monitor environment to NVRAM
sysret              print out info from last system return
unalias             unset an alias
unset               unset a monitor variable
rommon 2>
```

使用できるコマンドの一覧は、使用しているソフトウェア イメージとプラットフォームに依存します。一部のバージョンの ROMMON では、次のように、別名の形式でコマンドの一覧が表示されます。

```
> ?

$ state      Toggle cache state (? for help)
B [filename] [TFTP Server IP address | TFTP Server Name]
             Load and execute system image from ROM or from TFTP server
C [address]  Continue execution [optional address]
D /S M L V   Deposit value V of size S into location L with modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin execution
H            Help for commands
I            Initialize
K            Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
             Load system image from ROM or from TFTP server, but do not
             begin execution
O            Show configuration register option settings
P            Set the break point
S            Single step next instruction
T function   Test device (? for help)
Deposit and Examine sizes may be B (byte), L (long) or S (short).
Modifiers may be R (register) or S (byte swap).
Register names are: D0-D7, A0-A6, SS, US, SR, and PC
```

ROM モニタ モードを終了するには、**continue** コマンドを使用します。これにより、ブート プロセスが再起動されます。

ROM モニタ モードの特性と ROM モニタ モードの使用方法については、『Rebooting and Reloading - Configuring Image Loading Characteristics』を参照してください。

Cisco IOS の主なコマンド モードの要約

表 1 に、Cisco IOS CLI で使用される主なコマンド モードの要約を示します。

表 1　　Cisco IOS の主なコマンド モードの要約

コマンド モード	アクセス方法	プロンプト	終了方法
ユーザ EXEC	ログイン。	`Router>`	**logout** コマンドを使用します。
特権 EXEC	ユーザ EXEC モードで **enable** EXEC コマンドを使用します。	`Router#`	ユーザ EXEC モードを終了するには、**disable** コマンドを使用します。 グローバル コンフィギュレーション モードを開始するには、**configure terminal** 特権 EXEC コマンドを使用します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure terminal** コマンドを使用します。	`Router(config)#`	終了して特権 EXEC モードに戻るには、**end** コマンドを使用するか、**Ctrl+Z** キーを押します。 インターフェイス コンフィギュレーション モードを開始するには、**interface** コンフィギュレーション コマンドを使用します。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドでインターフェイスを指定して開始します。	`Router(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。 終了して特権 EXEC モードに戻るには、**end** コマンドを使用するか、**Ctrl+Z** キーを押します。 サブインターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドでサブインターフェイスを指定します。
サブインターフェイス コンフィギュレーション	インターフェイス コンフィギュレーション モードで、**interface** コマンドを使用してサブインターフェイスを指定します（このモードを使用できるかどうかは、プラットフォームに依存します）。	`Router(config-subif)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。 終了して特権 EXEC モードに戻るには、**end** コマンドを使用するか、**Ctrl+Z** キーを押します。

ROM モニタ	特権 EXEC モードで、**reload** EXEC コマンドを使用します。システムの起動時、最初の 60 秒以内に Break キーを押します。	`>`
		または
		`boot>`
		または
		`rommon >`
			ロード プロセスに割り込むことで ROM モニタ モードを開始した場合、**continue** コマンドを使用することで、ROM モニタ モードを終了し、ロードを再開できます。

Cisco IOS CLI の作業リスト

Cisco IOS CLI の機能に慣れるために、以降の項で説明する作業を実行してください。

状況依存ヘルプの参照

システム プロンプトで疑問符（**?**）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。また、状況依存ヘルプ機能を使用して、任意のコマンドで使用できる引数とキーワードの一覧を参照できます。

コマンド モード、コマンド名、キーワード、または引数に固有のヘルプを参照するには、次のいずれかのコマンドを使用します。

コマンド	目的
(*prompt*)# **help**	ヘルプ システムの簡単な説明が表示されます。
(*prompt*)# *abbreviated-command-entry***?**	現在のモードの、特定の文字ストリングで始まるコマンドの一覧を表示します。
(*prompt*)# *abbreviated-command-entry*<**Tab**>	特定のコマンド名を補完します。
(*prompt*)# **?**	そのコマンド モードで使用できるすべてのコマンドの一覧を表示します。
(*prompt*)# *command* **?**	そのコマンドで使用可能な構文オプション（引数とキーワード）の一覧を表示します。
(*prompt*)# *command keyword* **?**	そのコマンドで次に使用できる構文オプションの一覧を表示します。

システム プロンプトは、現在のコンフィギュレーション モードによって変わることに注意してください。

状況依存ヘルプを使用する際、疑問符（**?**）の前のスペース（またはスペースの不足）は重要です。特定の文字シーケンスで始まるコマンドの一覧を表示するには、それらの文字を入力した後、すぐに疑問符（**?**）を入力します。スペースは含めません。この形式のヘルプは、単語が補完されることから、ワード ヘルプと呼ばれます。詳細については、この章の「部分的なコマンド名の補完」の項を参照してください。

キーワードまたは引数の一覧を表示するには、キーワードまたは引数の代わりに疑問符（**?**）を入力します。**?** の前にはスペースを挿入します。この形式のヘルプは、コマンド構文ヘルプと呼びます。これは、すでに入力したコマンド、キーワード、および引数に基づいて、使用できるキーワードや引数が表示されるためです。

コマンドやキーワードは、一意になる文字数まで省略できます。たとえば、**configure terminal** コマンドは **config t** に省略できます。コマンドの省略形が一意であるため、ルータによって省略形が受け付けられ、コマンドが実行されます。

help コマンド（どのコマンド モードでも使用できます）を実行すると、次のようにヘルプ システムの説明が表示されます。

```
Router# help

Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must back up until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

help コマンドの出力が示すように、疑問符（**?**）を使用して部分的なコマンド名を補完したり（部分ヘルプ）、現在のコマンドを補完する引数またはキーワードの一覧を表示したりできます。

次に、状況依存ヘルプ機能を使用して、コンフィギュレーション モードでアクセス リストを作成する例を示します。

システム プロンプトで、**co** に続けて疑問符（**?**）を入力します。最後の文字と疑問符の間にはスペースを入れません。システムには **co** で始まるコマンドが表示されます。

```
Router# co?
configure  connect  copy
```

configure コマンドの後にスペースと疑問符を入力すると、そのコマンドのキーワードと簡単な説明の一覧が表示されます。

```
Router# configure ?
  memory    Configure from NV memory
  network   Configure from a TFTP network host
  overwrite-network  Overwrite NV memory from TFTP network host
  terminal  Configure from the terminal
  <cr>
```

一覧中の <cr> 記号（「cr」は復帰を表します）は、Return キーまたは Enter キーを押して、キーワードを追加せずにコマンドを実行することが 1 つの選択肢であることを示します。この例の出力は、configure コマンドのオプションが、**configure memory**（NVRAM から設定）、**configure network**（ネットワーク上のファイルから設定）、**configure overwrite-network**（ネットワーク上のファイルから設定し、NVRAM 内のファイルを置換）、または **configure terminal**（端末接続から手動で設定）のいずれかであることを示しています。ほとんどのコマンドで、<cr> 記号は、入力済みの構文でコマンドを実行できることを示すために使用されます。ただし、configure コマンドは特殊であり、CLI によって不足している構文の入力を求められます。

```
Router# configure
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

? プロンプトに対するデフォルトの応答は、CLI 出力中の行末にある角カッコで囲まれたオプションによって示されます。上の例で、Enter（または Return）キーを押すことは、「terminal」と入力するのと同じです。

グローバル コンフィギュレーション モードを開始するには、**configure terminal** コマンドを実行します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

CLI では、エラー インジケータであるキャレット記号（^）を使用してエラーの位置が示されます。^ 記号は、コマンド構文中の、ユーザが正しくないか認識されないコマンド構文を入力した場所に表示されます。たとえば、次の出力のキャレット記号は、コマンド中の入力ミスした文字を示しています。

```
Router# configure terminal
                     ^
% Invalid input detected at '^' marker.

Router#
```

エラー マーカーを警告するため、画面上にエラー メッセージ（% 記号によって示されます）が表示されることに注意してください。

access-list コマンドの後にスペースと疑問符を入力すると、コマンドで使用できるオプションの一覧が表示されます。

```
Router(config)# access-list ?
 <1-99>            IP standard access list
 <100-199>         IP extended access list
 <1100-1199>       Extended 48-bit MAC address access list
 <1300-1999>       IP standard access list (expanded range)
 <200-299>         Protocol type-code access list
 <2000-2699>       IP extended access list (expanded range)
 <700-799>         48-bit MAC address access list
 dynamic-extended  Extend the dynamic ACL absolute timer
 rate-limit        Simple rate-limit specific access list
```

山カッコ内の 2 つの数値は、包含範囲を表します。アクセス リスト番号 **99** を入力し、再度疑問符を入力すると、キーワードに該当する引数と簡単な説明が表示されます。

```
Router(config)# access-list 99 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
```

deny 引数の後に疑問符（**?**）を入力すると、追加のオプションの一覧が表示されます。

```
Router(config)# access-list 99 deny ?
  A.B.C.D  Address to match
```

一般に大文字は変数（引数）を表します。IP アドレスに続けて疑問符（**?**）を入力すると、追加オプションの一覧が表示されます。

```
Router(config)# access-list 99 deny 172.31.134.0 ?
  A.B.C.D  Mask of bits to ignore
  <cr>
```

この出力で、A.B.C.D は、ワイルドカード マスクを使用できることを示しています。ワイルドカード マスクは、IP アドレスまたは IP アドレスの範囲を照合するための方法の 1 つです。たとえば、ワイルドカード マスク 0.0.0.255 は、IP アドレスの第 4 オクテットの 0 ～ 255 の範囲のどの数値にも一致します。

ワイルドカード マスクに続けて疑問符（**?**）を入力すると、さらにオプションの一覧が表示されます。

```
Router(config)# access-list 99 deny 172.31.134.0 0.0.0.255 ?
<cr>
```

<cr> 記号は、それ以上キーワードや引数がないことを示します。Enter（または Return）キーを押してコマンドを実行します。

```
Router(config)# access-list 99 deny 172.31.134.0 0.0.0.255
```

システムにはエントリがアクセス リスト 99 に追加され、サブネット 172.31.134.0 上のすべてのホストへのアクセスが拒否され、0 ～ 255 の範囲で終わる IP アドレスに対するビットが無視されます。

すべてのユーザ EXEC コマンドの表示

すべてのユーザ EXEC コマンドを表示するように現在のセッションを設定するには、ユーザ EXEC モードまたは特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **terminal full-help**	すべてのユーザ レベル コマンドのヘルプを表示するようにこのセッションを設定します。

システム管理者はライン コンフィギュレーション モードで、**full-help** コマンドを使用して、特定の回線に対して行われた接続については常に完全なヘルプを表示するようにシステムを設定することもできます。

full-help コマンドと **terminal full-help** コマンドを使用すると、**show ?** コマンドを実行したときに、ユーザ EXEC モードで利用可能なすべてのヘルプ メッセージを表示できます。

次に示す、**show ?** コマンドの出力例は、**terminal full-help** コマンドをディセーブルにした場合とイネーブルにした場合の出力です。

```
Router> terminal no full-help
Router> show ?

  bootflash  Boot Flash information
  calendar   Display the hardware calendar
  clock      Display the system clock
  context    Show context information
  dialer     Dialer parameters and statistics
  history    Display the session command history
  hosts      IP domain-name, lookup style, nameservers, and host table
  isdn       ISDN information
  kerberos   Show Kerberos Values
  modemcap   Show Modem Capabilities database
  ppp        PPP parameters and statistics
  rmon       rmon statistics
  sessions   Information about Telnet connections
  snmp       snmp statistics
  terminal   Display terminal configuration parameters
  users      Display information about terminal lines
  version    System hardware and software status

Router> terminal full-help
Router> show ?

  access-expression  List access expression
  access-lists       List access lists
  aliases            Display alias commands
  apollo             Apollo network information
  appletalk          AppleTalk information
  arp                ARP table
  async              Information on terminal lines used as router interfaces
  bootflash          Boot Flash information
  bridge             Bridge Forwarding/Filtering Database [verbose]
  bsc                BSC interface information
  bstun              BSTUN interface information
  buffers            Buffer pool statistics
```

```
calendar            Display the hardware calendar
cdp                 CDP information
clns                CLNS network information
clock               Display the system clock
cls                 DLC user information
cmns                Connection-Mode networking services (CMNS) information
.
.
.
x25                 X.25 information
```

コマンドの no 形式および default 形式の使用

ほぼすべてのコンフィギュレーション コマンドに **no** 形式があります。一般に、**no** 形式を使用すると、機能がディセーブルになります。**no** キーワードなしでコマンドを使用すると、ディセーブルにされた機能を再度イネーブルにしたり、デフォルトでディセーブルになっている機能をイネーブルにすることができます。たとえば、IP ルーティングはデフォルトでイネーブルに設定されています。IP ルーティングをディセーブルにするには、**ip routing** コマンドの **no ip routing** 形式を使用します。再度イネーブルにするには、**ip routing** 形式を使用します。Cisco IOS ソフトウェアのコマンド リファレンスの資料では、コマンドの **no** 形式が使用できる場合は常に **no** 形式の機能について説明しています。

多くの CLI コマンドには、**default** 形式もあります。**default** *command-name command* を実行することで、コマンドをデフォルトの設定にすることができます。Cisco IOS ソフトウェアのコマンド リファレンス マニュアルでは、**default** 形式が、コマンドのプレーン形式か **no** 形式と異なる機能を実行する場合、一般にコマンドの **default** 形式の機能を説明しています。システムで使用できるデフォルト コマンドを表示するには、該当するコマンド モードで **default ?** と入力します。

コマンド履歴の使用

Cisco IOS CLI では、入力したコマンドの履歴（記録）が提供されます。この機能は、アクセス リストなど、長く複雑なコマンドやエントリを呼び出すときに特に便利です。コマンド履歴機能を使用するには、以降の項で説明するいずれかの作業を実行します。

- 「コマンド履歴バッファ サイズの設定」（P.15）
- 「コマンドの呼び出し」（P.16）
- 「コマンド履歴機能のディセーブル化」（P.16）

コマンド履歴バッファ サイズの設定

デフォルトでは、10 個のコマンド ラインが履歴バッファに格納されます。現在の端末セッション中に記録されるコマンドラインの数を設定するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **terminal history** [**size** *number-of-lines*]	現在の端末セッションでコマンド履歴機能をイネーブルにします。

no terminal history size コマンドは、履歴バッファに格納される行数をデフォルトの 10 行にリセットします。

特定の回線のすべてのセッションに対してシステムが記録するコマンドラインの数を設定するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)# history [size number-of-lines]`	コマンド履歴機能をイネーブルにします。

コマンドの呼び出し

履歴バッファからコマンドを呼び出すには、次のコマンドまたはキーの組み合わせのいずれかを使用します。

コマンドまたはキーの組み合わせ	目的
Ctrl+P キーまたは↑キー。[1]	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。このキーを連続して繰り返すと、順に古いコマンドを再呼び出しします。
Ctrl+N キーまたは↓キー。[1]	Ctrl+P キーまたは↑キーでコマンドを呼び出した後に、履歴バッファ内のより新しいコマンドに戻ります。このキーを連続して繰り返すと、順に新しいコマンドを再呼び出しします。
`Router> show history`	ユーザ EXEC モードで、最後に入力したいくつかのコマンドの一覧を表示します。

1. 矢印キーは、American National Standards Institute（ANSI; 米国規格協会）互換の端末だけで機能します。

コマンド履歴機能のディセーブル化

コマンド履歴機能は自動的にイネーブルになります。現在の端末セッションの間この機能をディセーブルにするには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> no terminal history`	現在のセッションに対してコマンド履歴をディセーブルにします。

コマンド履歴機能がディセーブルになるように特定の回線を設定するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)# no history`	回線に対してコマンド履歴をディセーブルにします。

CLI 編集機能とショートカットの使用

Cisco IOS CLI では、さまざまなショートカットと編集機能が使用できます。以降のサブセクションで次の機能について説明します。

- 「コマンドラインでのカーソルの移動」（P.17）
- 「部分的なコマンド名の補完」（P.17）

コマンドラインでのカーソルの移動

表 2 に、修正または変更を行うために、コマンド ライン上でカーソルを移動するために使用できるキーの組み合わせまたはシーケンスを示します。Ctrl は Control キーを示し、対応する文字キーと同時に押す必要があります。Esc は Escape キーを示し、最初に押してから対応する文字キーを押します。キーの大文字と小文字は区別されません。CLI のナビゲーションと編集で使用される文字の多くは、その機能を簡単に覚えておけるように選択されています。表 2 で、「機能の要約」欄の太字の文字は、使用される文字とその機能の間の関係を示します。

表 2　　カーソル移動に使用されるキーの組み合わせ

キーストローク	機能の要約	機能の詳細
←または **Ctrl+B**	1 文字戻る（**B**ack character）	カーソルを 1 文字分だけ後退させます。 複数行にわたってコマンドを入力するときは、←キーまたは Ctrl+B キーを繰り返し押してシステム プロンプトまでスクロール バックして、コマンド エントリの先頭まで移動できます。あるいは Ctrl+A キーを押してコマンド エントリの先頭に移動します。
→または **Ctrl+F**	1 文字進む（**F**orward character）	カーソルを 1 文字分だけ進めます。
Esc、**B**	1 単語戻る（**B**ack word）	カーソルを 1 単語分だけ戻します。
Esc、**F**	1 単語進む（**F**orward word）	カーソルを 1 単語分だけ進めます。
Ctrl+A	行の先頭（Beginning of line）	カーソルを行の先頭に移動します。
Ctrl+E	行末（**E**nd of line）	カーソルをコマンドラインの末尾に移動します。

部分的なコマンド名の補完

完全なコマンド名を思い出せない場合や、入力量を減らす場合は、コマンドの先頭の数文字を入力して、Tab キーを押します。コマンドライン パーサーは、入力されたストリングがコマンド モードに対して一意である場合に、コマンドを補完します。キーボードに Tab キーがない場合は、代わりに **Ctrl+I** キーを押します。

コマンドは、コマンドが一意になるのに十分な文字が入力されていれば認識されます。たとえば、特権 EXEC モードで **conf** と入力すると、エントリを **configure** コマンドと関連付けることができます。これは、**conf** で始まるコマンドが **configure** コマンドしかないためです。

次の例で、Tab キーを押すと、特権 EXEC モードの **conf** に対する一意のストリングが認識されます。

```
Router# conf<Tab>
Router# configure
```

コマンド補完機能を使用すると、CLI により完全なコマンド名が表示されます。Return キーか Enter キーを押すまでコマンドは実行されません。これにより、完全なコマンドが省略形によって意図したものでない場合に、コマンドを修正できます。複数のコマンドに該当する文字列を入力した場合、テキスト ストリングが一意でないことを示すためにブザー音が鳴ります。

コマンドが補完できない場合は、疑問符（**?**）を入力して、その文字で始まるコマンドの一覧を表示します。入力した最後の文字と疑問符（**?**）の間にはスペースを入れません。

たとえば、**co?** と入力すると、現在のコマンド モードで使用可能なすべてのコマンドの一覧が表示されます。

```
Router# co?
configure connect copy
Router# co
```

疑問符の前に入力した文字は、コマンドを完全に入力できるように画面に表示されます。

エントリの削除

入力を間違えた場合や気が変わった場合に、コマンド エントリを削除するには、次のキーまたはキーの組み合わせを使用します。

キーストローク	目的
Delete または **Backspace**	カーソルの左にある文字を削除します。
Ctrl+D	カーソル位置にある文字を削除します。
Ctrl+K	カーソル位置からコマンドラインの末尾までのすべての文字を削除します。
Ctrl+U または **Ctrl+X**	カーソル位置からコマンドラインの先頭までのすべての文字を削除します。
Ctrl+W	カーソルの左にある単語を削除します。
Esc、**D**	カーソルの位置から単語の末尾までを削除します。

削除したエントリの呼び出し

CLI では、削除したコマンドまたはキーワードが履歴バッファに格納されます。スペースで始まるかスペースで終わるストリングだけがバッファに格納され、削除した個別の文字（Backspace または Ctrl+D を使用）は格納されません。バッファには、Ctrl+K、Ctrl+U、または Ctrl+X で削除された最後の 10 個の項目が格納されます。これらの項目を呼び出してコマンドラインに貼り付けるには、次のキーの組み合わせを使用します。

キーストローク	目的
Ctrl+Y	バッファ内の最新のエントリを呼び出します（キーを同時に押します）。
Esc、**Y**	履歴バッファ内の前のエントリを呼び出します（キーは順番に押します）。

Esc、Y キー シーケンスは、最初に Ctrl+Y キーの組み合わせを押さない限り機能しません。Esc、Y を 11 回以上押すと、バッファ内の最新のエントリに戻ります。

折り返されるコマンド ラインの編集

CLI には、画面上の 1 行を超えるコマンドに対する折り返し機能が備わっています。カーソルが右余白に到達すると、コマンド ラインが左に 10 スペース分移動します。行の先頭の 10 文字は見えなくなりますが、スクロールで戻ることで、コマンドの先頭の構文を確認できます。スクロールで戻るには、Ctrl+B キーまたは←キーを繰り返し押してコマンド エントリの先頭に戻るか、Ctrl+A キーを押して直接行の先頭に戻ります。

次の例で、**access-list** コマンド エントリが 1 行を超えています。カーソルが行末に到達すると、行が 10 スペース分左に移動し、再表示されます。ドル記号（$）は、行が左にスクロールされたことを示しています。カーソルが行末に到達するたびに、行が再度左に 10 スペース分移動します。

```
Router(config)# access-list 101 permit tcp 172.31.134.5 255.255.255.0 172.31.1
Router(config)# $ 101 permit tcp 172.31.134.5 255.255.255.0 172.31.135.0 255.25
Router(config)# $t tcp 172.31.134.5 255.255.255.0 172.31.135.0 255.255.255.0 eq
Router(config)# $31.134.5 255.255.255.0 172.31.135.0 255.255.255.0 eq 45
```

入力を完了したら、Return キーを押してコマンドを実行する前に、**Ctrl+A** キーを押して、完全な構文を確認します。行が右にスクロールしていることを示すため、ドル記号（$）が行末に表示されます。

```
Router(config)# access-list 101 permit tcp 172.31.134.5 255.255.255.0 172.31.1$
```

Cisco IOS ソフトウェアでは、幅が 80 カラムの端末画面がデフォルトで設定されます。画面の幅が異なる場合は、ユーザ EXEC モードで **terminal width** コマンドを使用して端末の幅を設定します。

ライン ラップとコマンド履歴機能を組み合わせることで、以前の複雑なコマンド エントリを呼び出したり修正したりできます。以前のコマンド エントリを呼び出す方法については、この章の「コマンドの呼び出し」を参照してください。

--More-- プロンプトでの出力の続行

Cisco IOS CLI を使用する場合、出力が画面に表示可能な長さを超えることがあります。多数の **?**、**show**、または **more** コマンドの出力など、出力が画面の下端を超えて続く場合、出力が一時停止され、--More-- プロンプトが下面の下部に表示されます。出力を再開するには、Return キーを押して下に 1 行スクロールするか、スペースキーを押して出力の次の 1 画面分を表示します。

ヒント 出力が画面上で一時停止していて、--More-- プロンプトが表示されない場合は、ライン コンフィギュレーション モードで **length** コマンドまたは特権 EXEC モードで **terminal length** コマンドを使用して、画面の長さにより小さな値を入力します。**length** の値をゼロにするとコマンド出力は一時停止しなくなります。

--More-- プロンプトからの出力のフィルタリングについては、この章の「CLI 出力の検索とフィルタリング」の項を参照してください。

現在のコマンドラインの再表示

コマンドを入力していて、突然システムから画面にメッセージが表示された場合、現在のコマンド ライン エントリを簡単に呼び出すことができます。現在のコマンド ラインを再表示（画面を更新）するには、次のキーの組み合わせのうちいずれかを使用します。

キーストローク	目的
Ctrl+L または **Ctrl+R**	現在のコマンド ラインを再表示します。

入力ミスした文字の入れ替え

コマンド入力をミスした場合、入力ミスした文字を入れ替えることができます。文字を入れ替えるには、次のキーの組み合わせを使用します。

キーストローク	目的
Ctrl+T	カーソルの左にある文字を、カーソルの右にある文字と置き換えます。

大文字と小文字の制御

単純なキー シーケンスで単語を大文字または小文字にしたり、文字セットを大文字にすることができます。ただし、Cisco IOS コマンドでは、一般に大文字と小文字が区別されず、通常はすべて小文字で入力します。コマンドの大文字と小文字を変更するには、次のキー シーケンスを使用します。

キーストローク	目的
Esc、**C**	カーソルの場所にある文字を大文字にします。
Esc、**L**	カーソルの場所にある単語を小文字にします。
Esc、**U**	カーソルの位置から単語の末尾までを大文字にします。

キーストロークをコマンド エントリとして指定

特定のキーストローク（キーの組み合わせまたはシーケンス）をコマンド エイリアスとして認識するようにシステムを設定できます。つまり、ストロークを、コマンドを実行するためのショートカットとして設定できます。システムにキーストロークをコマンドとして解釈させるには、コマンド シーケンスを入力する前に、次のいずれかのキーの組み合わせを使用します。

キーストローク	目的
Ctrl+V または **Esc**、**Q**	システムが次のキーストロークをユーザ設定コマンド エントリとして受け付けるように設定します（編集コマンドとしてではありません）。

編集機能のディセーブル化と再イネーブル化

これまでの項で説明した編集機能は Cisco IOS Release 9.21 で追加され、システムで自動的にイネーブルになります。しかし、これらの編集機能をディセーブルにすることが望ましい状況がいくつかあります。たとえば、編集機能と競合するスクリプトがある場合です。編集機能をグローバルにディセーブルにするには、ライン 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。

コマンド	目的
`Router(config-line)# no editing`	特定の回線に対して CLI 編集機能をディセーブルにします。

現在の端末セッションに対して編集機能をディセーブルにするには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# no terminal editing`	ローカル ラインに対して CLI 編集機能をディセーブルにします。

現在の端末セッションに対して編集機能を再度イネーブルにするには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# terminal editing`	現在の端末セッションに対して CLI 編集機能をイネーブルにします。

特定の回線に対して編集機能を再度イネーブルにするには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router(config-line)# editing`	CLI 編集機能をイネーブルにします。

CLI 出力の検索とフィルタリング

Cisco IOS CLI には、大量のコマンド出力を検索したり、出力をフィルタリングして不要な情報を除外するための手段が提供されています。これらの機能は、一般に大量のデータが表示される、**show** コマンドと **more** コマンドで使用できます。

（注） **show** コマンドと **more** コマンドは、常にユーザ EXEC モードまたは特権 EXEC モードで実行します。

画面に表示される内容を超えて出力が続く場合、Cisco IOS CLI では --More-- プロンプトが表示されます。Return キーを押すことで次の行が表示され、スペースキーを押すことで次の画面が表示されます。CLI ストリング検索機能を使用すると、--More-- プロンプトからの出力を検索またはフィルタリングできます。

正規表現について

正規表現は、CLI ストリング検索機能によって、**show** コマンドまたは **more** コマンドの出力と照合されるパターン（句、数値、またはより複雑なパターン）です。正規表現では、大文字と小文字が区別され、複雑な一致要件を指定することが可能です。単純な正規表現としては、Serial、misses、138 などがあります。複雑な正規表現としては、00210...、(is)、[Oo]utput などがあります。

正規表現は、単一文字パターンか複数文字パターンです。つまり、正規表現は、コマンド出力中の同じ 1 文字に一致する 1 つの文字か、コマンド出力中の同じ複数の文字に一致する複数の文字です。コマンド出力中のパターンをストリングと呼びます。この項では、単一文字パターンと複数文字パターンの作成について説明します。また、量指定子、選択、位置指定、カッコを使用したより複雑な正規表現についても説明します。

単一文字パターン

最も単純な正規表現は、コマンド出力内の同じ 1 つの文字と一致する単一文字です。単一文字パターンとして、任意の文字（A ～ Z、a ～ z）または数字（0 ～ 9）を使用することができます。他のキーボード文字（! や ~ など）を、単一文字パターンとして使用することもできますが、特定のキーボード文字は、正規表現内で使用した場合特別な意味を持ちます。表 3 に、特別な意味を持つキーボード文字の一覧を示します。

表 3　　特別な意味を持つ文字

文字	特別な意味
.	スペースを含む任意の単一文字と一致します。
*	0 個以上のパターンのシーケンスと一致します。
+	1 個以上のパターンのシーケンスと一致します。
?	0 または 1 回のパターンと一致します。
^	ストリングの最初と一致します。
$	ストリングの最後と一致します。
_（アンダースコア）	カンマ（,）、左波カッコ（{）、右波カッコ（}）、左カッコ（(）、右カッコ（)）、ストリングの先頭、ストリングの末尾、またはスペースと一致します。

これらの特殊文字を単一文字パターンとして使用するときは、各文字の前にバックスラッシュ（\）を置いて特別な意味を除外してください。次の例は、それぞれドル記号、アンダースコア、プラス記号に一致する単一文字パターン マッチングの例です。

\$ _ \+

単一文字パターンを範囲指定して、コマンド出力とのマッチングを行うことができます。たとえば、文字 a、e、i、o、u のいずれかを含むストリングに一致する正規表現を作成できます。パターン マッチングが成功するためには、これらの文字のいずれかだけがストリング中に存在する必要があります。単一文字パターンを範囲指定するには、単一文字パターンを角カッコ（**[ ]**）で囲みます。たとえば、**[aeiou]** は小文字アルファベットの 5 つの母音のうちの任意の 1 文字と一致しますが、**[abcdABCD]** は小文字または大文字アルファベットの最初の 4 つの文字のうちの任意の 1 文字と一致します。

ダッシュ（-）で区切って範囲の終点だけを入力することにより範囲を簡略化することができます。上の範囲は次のように単純化されます。

[a-dA-D]

ダッシュを範囲内の単一文字パターンとして追加するには、ダッシュをもう 1 つ追加し、その前にバックスラッシュを入力します。

[a-dA-D\-]

次に示すように、右角カッコ（]）を、範囲内の単一文字パターンとして追加することもできます。

[a-dA-D\-\]]

上の例は、大文字または小文字のアルファベットの最初の 4 文字、ダッシュ、右角カッコのいずれかに一致します。

範囲の先頭にキャレット（^）を追加することで、範囲の一致を反転させることができます。次の例は、その中の文字以外の文字に一致します。

[^a-dqsv]

次の例は、右角カッコ（]）または文字 d 以外のすべてと一致します。

[^\]d]

複数文字パターン

正規表現を作成するとき、複数の文字を含むパターンを指定することもできます。複数文字正規表現は、文字、数字、特別な意味のないキーボード文字を組み合わせて作成します。たとえば、a4% は複数文字の正規表現です。文字をそのとおりに解釈することを指示するには、特別な意味のあるキーボード文字の前にバックスラッシュを挿入します。

複数文字パターンでは、順序が大切です。正規表現 **a4%** は、a という文字の後に 4 が続き、その後に % 記号が続く文字と一致します。ストリングの中に a4% という文字がその順序で含まれていないと、パターン マッチングは失敗します。複数文字正規表現 **a.** では、ピリオド文字の特別な意味を使用しており、a という文字の後に任意の文字が 1 つ来るストリングと一致します。この例では、ab、a!、または a2 というストリングはすべてこの正規表現と一致します。

ピリオド文字の特別な意味を無効にするには、その前にバックスラッシュを挿入します。たとえば、表現 **a\.** がコマンド構文で使用されている場合、ストリング a. だけが一致します。

すべての文字、すべての数字、すべてのキーボード文字、文字と数字とその他のキーボード文字の組み合わせを含む複数文字正規表現を作成できます。たとえば、**telebit 3107 v32bis** は有効な正規表現です。

量指定子

Cisco IOS ソフトウェアに対して、指定した正規表現の複数の出現に一致させることを指示するため、より複雑な正規表現を作成できます。そのためには、単一文字パターンおよび複数文字パターンとともに、いくつかの特殊文字を使用します。表 4 に、正規表現の「複数回の出現」を示す特殊文字の一覧を示します。

表 4　　量指定子として使用される特殊文字

文字	説明
*	0 以上の単一文字パターンまたは複数文字パターンと一致します。
+	1 以上の単一文字パターンまたは複数文字パターンと一致します。
?	1 以上の単一文字パターンまたは複数文字パターンの 0 回または 1 回の出現と一致します。

次の例は、空文字を含む文字 a の任意の回数の出現と一致します。

a*

次のパターンでは、ストリングが一致するためには、文字 a が少なくとも 1 文字含まれていることが必要です。

a+

次のパターンは、ストリング bb または bab と一致します。

ba?b

次のストリングは、任意の数のアスタリスク（*）と一致します。

******

複数文字パターンとともに量指定子を使用するには、パターンをカッコで囲みます。次の例で、パターンは複数文字ストリング ab の任意の回数の出現と一致します。

(ab)*

より複雑な例として、次のパターンは、英数字のペアの 1 つ以上のインスタンスに一致しますが、空文字には一致しません（つまり、空のストリングは一致しません）。

([A-Za-z][0-9])+

量指定子（*、+、または ?）を使用した一致の順序は、最長構造優先です。ネストした構造は、外側から内側に一致します。連結された構造は、構造の左側から一致します。そのため、この正規表現は A9b3 に一致しますが、9Ab3 には一致しません。これは、英文字が数字の前に指定されているためです。

選択

選択を使用すると、ストリングに対して一致する代替パターンを指定できます。代替パターンは縦線（|）で区切ります。代替パターンのうちの 1 つがストリングに一致します。たとえば、正規表現 **codex|telebit** は、ストリング codex またはストリング telebit に一致しますが、codex と telebit の両方には一致しません。

位置指定

Cisco IOS ソフトウェアに対し、ストリングの先頭または末尾に対して正規表現パターンを一致させることを指示できます。つまり、ストリングの先頭または末尾に特定のパターンが含まれていることを指定できます。ストリングの一部に対してこれらの正規表現を「位置指定」するには、表 5 に示す特殊文字を使用します。

表 5　位置指定に用いられる特殊文字

文字	説明
^	ストリングの最初と一致します。
$	ストリングの最後と一致します。

たとえば、正規表現 **^con** は con で始まるストリングに一致し、**$sole** は sole で終わるストリングに一致します。

^ 記号は、ストリングの先頭を示すのに加えて、角カッコの中で使用された場合に論理的な「not」を示すものとして使用できます。たとえば、正規表現 **[^abcd]** は、a、b、c、または d 以外の任意の単一文字に一致する範囲を示します。

これらの位置指定文字は、特殊文字アンダースコア（_）とともに使用します。アンダースコアは、ストリングの先頭（^）、ストリングの末尾（$）、カッコ（( )）、スペース（ ）、波カッコ（{}）、カンマ（,）、アンダースコア（_）に一致します。アンダースコア文字を使用すると、パターンがストリング中のいずれかの場所に存在することを指定できます。たとえば、**_1300_** は、ストリング中のいずれかの場所に 1300 がある任意のストリングに一致します。ストリング 1300 の前後にスペース、波カッコ、カンマ、アンダースコアのいずれかがあってもかまいません。そのため、{1300_ は正規表現 **_1300_** に一致しますが、21300 や 13000 は一致しません。

アンダースコア文字を使用することで、長い正規表現リストを置き換えることができます。たとえば、**^1300( ) ( )1300$ {1300, ,1300, {1300} ,1300, (1300** と指定する代わりに、**_1300_** と指定できます。

後方参照のためのカッコ

「量指定子」の項に示したように、複数文字正規表現をカッコで囲み、パターンの出現を繰り返すことができます。また、単一文字パターンまたは複数文字パターンをカッコで囲み、Cisco IOS ソフトウェアに対して、正規表現の別の場所で使用するためにパターンを覚えておくことを指示できます。

前のパターンを後方参照する正規表現を作成するには、カッコを使用して特定のパターンの記憶を指示し、バックスラッシュ（\）の後に数字を使用して記憶したパターンを再利用します。数字は、正規表現パターン内のカッコの出現を指定します。正規表現内に複数のパターンがある場合、\1 は最初に記憶したパターンを示し、\2 は 2 番目に記憶したパターンとなり、以下同様となります。

次の正規表現では、後方参照のためにカッコを使用しています。

a(.)bc(.)\1\2

この正規表現は、a の後に任意の文字（これを文字番号 1 とします）、bc、任意の文字（文字番号 2）、文字番号 1、文字番号 2 が続くストリングに一致します。そのため、この正規表現は aZbcTZT に一致します。ソフトウェアは、文字番号 1 が Z であり、文字番号 2 が T であることを記憶し、正規表現の後半で Z と T を再度使用します。

show コマンドの検索とフィルタリング

show コマンドの出力を検索するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show** *any-command* **| begin** *regular-expression*	**show** コマンドのフィルタリングされていない出力を、正規表現を含む最初の行で開始します。

（注） Cisco IOS のマニュアルでは、縦線を、一般に構文の選択肢を示すために使用します。しかし、**show** コマンドと **more** コマンドの出力を検索するには、パイプ文字（縦線）を入力する必要があります。この項では、パイプを入力する必要があることを示すために、太字（|）で表します。

show コマンドの出力をフィルタリングするには、特権 EXEC モードで次のコマンドのいずれかを使用します。

コマンド	目的
Router# **show** *any-command* **| exclude** *regular-expression*	正規表現を含まない出力行を表示します。
Router# **show** *any-command* **| include** *regular-expression*	正規表現を含む出力行を表示します。

ほとんどのシステムで、Ctrl+Z キーの組み合わせを使用して、いつでも出力を中断し特権 EXEC モードに戻ることができます。たとえば、**show running-config | begin hostname** コマンドを使用して、実行コンフィギュレーション ファイルの、ホスト名の設定を含む行から表示を開始できます。次に、関心のある情報の最後まで確認し終えたら、Ctrl+Z を使用します。

（注） 感嘆符（!）またはセミコロン（;）が続く文字は、コメントとして扱われ、コマンドでは無視されます。

more コマンドの検索とフィルタリング

more コマンドは、**show** コマンドと同様に検索できます（**more** コマンドは、**show** コマンドと同じ機能を実行します）。**more** コマンドの出力を検索するには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **more** *any-command* **| begin** *regular-expression*	**more** コマンドのフィルタリングされていない出力を、正規表現を含む最初の行で開始します。

more コマンドは、**show** コマンドと同様にフィルタリングできます。**more** コマンドの出力をフィルタリングするには、ユーザ EXEC モードで次のコマンドのいずれかを使用します。

コマンド	目的
Router# **more** *any-command* **| exclude** *regular-expression*	正規表現を含まない出力行を表示します。
Router# **more** *any-command* **| include** *regular-expression*	正規表現を含む出力行を表示します。

--More-- プロンプトからの検索およびフィルタリング

--More-- プロンプトから出力を検索できます。**show** コマンドまたは **more** コマンドの出力を --More-- プロンプトから検索するには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
-More- **/***regular-expression*	フィルタリングされていない出力を、正規表現を含む最初の行で開始します。

--More-- プロンプトから出力をフィルタリングできます。ただし、各コマンドに対して 1 つのフィルタだけを指定できます。フィルタは、**show** コマンドまたは **more** コマンドの出力が終了するか、出力を中断（Ctrl+Z または Ctrl+6 を使用します）するまで継続されます。そのため、元のコマンドか前の --More-- プロンプトですでにフィルタを指定してある場合、--More-- プロンプトで別のフィルタを追加できません。

（注） 検索とフィルタリングは異なる機能です。**begin** キーワードを使用してコマンド出力を検索し、同時に --More-- プロンプトでフィルタを指定することはできます。

--More-- プロンプトで **show** コマンドまたは **more** コマンドの出力をフィルタリングするには、ユーザ EXEC モードで次のコマンドのいずれかを使用します。

コマンド	目的
-More- **-***regular-expression*	正規表現を含まない出力行を表示します。
-More- **+***regular-expression*	正規表現を含む出力行を表示します。

Cisco IOS CLI の使用：例

以降の項に CLI の使用例を示します。

コマンド構文の確認とコマンド履歴の使用：例

CLI では、エラー インジケータであるキャレット記号（^）を使用してエラーの位置が示されます。^ 記号は、コマンド ストリング内の誤ったコマンド、キーワード、または引数が入力された位置に表示されます。

次の例では、クロックを設定するものとします。状況依存ヘルプを使用して、クロックを設定するための正しいコマンド構文を確認します。

```
Router# clock ?
  set  Set the time and date
Router# clock
```

ヘルプ出力により、**set** キーワードが必要であることが示されます。時刻を入力するための構文を確認します。

```
Router# clock set ?
hh:mm:ss   Current time
Router# clock set
```

現在の時刻を入力します。

```
Router# clock set 13:32:00
% Incomplete command.
```

コマンドを完了するために追加の引数を指定する必要があることがシステムによって示されます。Ctrl+P キーまたは↑キーを押して、以前のコマンド入力を自動的に繰り返します。次にスペースと疑問符（**?**）を追加し、他の引数を確認します。

```
Router# clock set 13:32:00 ?
  <1-31>     Day of the month
  January    Month of the year
  February
  March
  April
  May
  June
  July
  August
  September
  October
  November
  December
```

これでコマンド入力を完了できます。

```
Router# clock set 13:32:00 23 February 01
                                       ^
% Invalid input detected at '^' marker.
```

キャレット記号（^）とヘルプ応答により、01 に誤りがあることが示されます。正しい構文の一覧を表示するために、エラーが発生した場所までコマンドを入力し、疑問符（**?**）を入力します。

```
Router# clock set 13:32:00 23 February ?
```

```
  <1993-2035> Year
Router# clock set 13:32:00 23 February
```

正しい構文を使用して年を入力し、Enter または Return を押してコマンドを実行します。

Router# **clock set 13:32:00 23 February 2001**

CLI 出力の検索とフィルタリング：例

次に、**more nvram:startup-config | begin** 特権 EXEC モード コマンドの部分的な出力例を示します。これは、正規表現を含む最初の行で、フィルタリングされていない出力が開始されています。--More-- プロンプトで、正規表現 ip を含む出力行を除外するためのフィルタを指定します。

```
Router# more nvram:startup-config | begin ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 192.168.48.48
ip name-server 172.16.2.132
!
isdn switch-type primary-5ess
.
.
.
interface Ethernet1
 ip address 10.5.5.99 10.255.255.0
 --More--
-ip
filtering...
 media-type 10BaseT
!
interface Serial0:23
 encapsulation frame-relay
 no keepalive
 dialer string 4001
 dialer-group 1
 isdn switch-type primary-5ess
 no fair-queue
```

次に、**more nvram:startup-config | include** コマンドの部分的な出力例を示します。正規表現 ip を含む行だけが表示されています。

```
Router# more nvram:startup-config | include ip
ip subnet-zero
ip domain-name cisco.com
ip name-server 1192.168.48.48
ip name-server 172.16.2.132
```

次に、**more nvram:startup-config | exclude** コマンドの部分的な出力例を示します。正規表現 service を含む行が除外されています。--More-- プロンプトで、正規表現 Dialer1 をフィルタとして指定します。このフィルタを指定することにより、Dialer1 を含む最初の行で出力が再開されます。

```
Router# more nvram:startup-config | exclude service
!
version 12.2
!
hostname router
!
boot system flash
no logging buffered
!
ip subnet-zero
ip domain-name cisco.com
.
```

```
.
.
--More--
/Dialer1
filtering...
interface Dialer1
 no ip address
 no ip directed-broadcast
 dialer in-band
 no cdp enable
```

次に、出力の検索が指定された、**show interface** コマンドの部分的な出力例を示します。パイプの後でキーワード **begin Ethernet** を使用することで、正規表現 Ethernet を含む最初の行でフィルタリングされていない出力が開始されます。--More-- プロンプトで、正規表現 Serial を含む行だけを表示するフィルタを指定します。

```
Router# show interface | begin Ethernet

Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Description: ip address is 172.1.2.14 255.255.255.0
  Internet address is 172.1.2.14/24
.
.
.
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
--More--
+Serial
filtering...
Serial1 is up, line protocol is up
Serial2 is up, line protocol is up
Serial3 is up, line protocol is down
Serial4 is down, line protocol is down
Serial5 is up, line protocol is up
Serial6 is up, line protocol is up
Serial7 is up, line protocol is up
```

次に、**show buffers | exclude** コマンドの部分的な出力例を示します。正規表現 `0 misses` を含む行が除外されています。--More-- プロンプトで、フィルタされていない出力を、Serial0 を含む最初の行から続行するための検索を指定します。

```
Router# show buffers | exclude 0 misses

Buffer elements:
     398 in free list (500 max allowed)
Public buffer pools:
Small buffers, 104 bytes (total 50, permanent 50):
     50 in free list (20 min, 150 max allowed)
     551 hits, 3 misses, 0 trims, 0 created
Big buffers, 1524 bytes (total 50, permanent 50):
     49 in free list (5 min, 150 max allowed)
Very Big buffers, 4520 bytes (total 10, permanent 10):
.
.
.
Huge buffers, 18024 bytes (total 0 permanent 0):
     0 in free list (0 min, 4 max allowed)
--More--
/Serial0
filtering...
Serial0 buffers, 1543 bytes (total 64, permanent 64):
     16 in free list (0 min, 64 max allowed)
```

```
     48 hits, 0 fallbacks
```

次に、**show interface | include** コマンドの部分的な出力例を示します。パイプ（|）の後で **include (is)** キーワードを使用することにより、正規表現 (is) が含まれる行だけが表示されます。カッコにより、is の前後にスペースが含まれることが指定されます。カッコを使用することで、is の前後にスペースを含む行だけが出力に含まれます（「disconnect」などの文字は検索から除外されます）。

```
router# show interface | include ( is )

ATM0 is administratively down, line protocol is down
  Hardware is ATMizer BX-50
Dialer1 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  DTR is pulsed for 1 seconds on reset
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.6399 (bia 0060.837c.6399)
  Internet address is 172.21.53.199/24
Ethernet1 is up, line protocol is up
  Hardware is Lance, address is 0060.837c.639c (bia 0060.837c.639c)
  Internet address is 10.5.5.99/24
Serial0:0 is down, line protocol is down
  Hardware is DSX1
.
.
.
 --More--
```

--More-- プロンプトで、Serial0:13 を含む最初の行でフィルタリングされた出力を続行する検索を指定します。

```
/Serial0:13
filtering...
Serial0:13 is down, line protocol is down
  Hardware is DSX1
  Internet address is 10.0.0.2/8
     0 output errors, 0 collisions, 2 interface resets
  Timeslot(s) Used:14, Transmitter delay is 0 flag
```

コンフィギュレーション モードでの EXEC コマンド

機能の履歴

リリース	変更点
12.1(11b)E、12.2(7)B、12.2(7)PB、12.0(20)SP、12.0(20)ST、12.0(21)S、12.2(8)T	この機能（**do** コマンド）が導入されました。

このマニュアルでは、コンフィギュレーション モード機能の EXEC コマンドについて説明し、次の項が含まれます。

機能の概要

do コマンドに続いて目的の EXEC コマンドを発行することで、EXEC レベルの Cisco IOS コマンド（**show**、**clear**、**debug** コマンドなど）を任意のコンフィギュレーション モード（グローバル コンフィギュレーション モードなど）で発行できるようになりました。

利点

この機能は現在のコンフィギュレーション モードを終了せずに、EXEC レベルのコマンドを入力できるため便利です。

制約事項

do コマンドを使用して **configure terminal** EXEC コマンドを実行することはできません。これは **configure terminal** コマンドがモードをコンフィギュレーション モードに変更するためです。

関連資料

- 『*Cisco IOS Configuration Fundamentals Command Reference*』

サポートされているプラットフォーム

- このコマンドはこのマニュアルの最初の機能履歴一覧にあるソフトウェア リリース（およびすべての派生リリース）を実行しているすべてのプラットフォームでサポートされています。

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を素早く特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、http://www.cisco.com/register にある指示に従って、Cisco.com 上にアカウントを作成できます。

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://www.cisco.com/go/fn

サポートされている規格、MIB、および RFC

規格

この機能によってサポートされる新しい規格や変更された規格はありません。

MIB

この機能によってサポートされる新しい MIB または変更された MIB はありません。

プラットフォームおよび Cisco IOS リリースによりサポートされている MIB のリストを入手し、MIB モジュールをダウンロードするには、Cisco.com の次のシスコ MIB Web サイトの URL にアクセスしてください。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

この機能によってサポートされる新しい RFC や変更された RFC はありません。

設定作業

コンフィギュレーション モードでの EXEC コマンドの実行機能に関するコンフィギュレーション作業については、次の項を参照してください。

- 「コンフィギュレーション モードでの EXEC コマンドの実行」（任意）

コンフィギュレーション モードでの EXEC コマンドの実行

任意のコンフィギュレーション モード（コンフィギュレーション サブモードを含む）で EXEC レベルのコマンドを実行するには、グローバル コンフィギュレーション モードまたは EXEC コマンドを発行するモードで次のコマンドを発行します。

コマンド	目的

`Router(config)# do command`
`Router(config)#`
 	
または
 	
`Router(config-if)# do command`
`Router(config-if)#`
	任意のコンフィギュレーション モードから任意の EXEC モード コマンドを実行できるようになります。
	• *command*：実行する EXEC コマンド。

設定例

ここでは、次の設定例について説明します。

- 「コンフィギュレーション モードでの EXEC コマンド実行例」

コンフィギュレーション モードでの EXEC コマンド実行例

次に、グローバル コンフィギュレーション モードから EXEC レベルの **show interface** コマンドを実行する例を示します。

```
Router(config)# do show interfaces serial 3/0

Serial3/0 is up, line protocol is up
  Hardware is M8T-RS232
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output 1d17h, output hang never
  Last clearing of "show interface" counters never
.
.
.
Router(config)#
```

次に、VPDN コンフィギュレーション モードから EXEC レベルの **clear vpdn tunnel** コマンドを実行する例を示します。

```
Router(config-vpdn)# do clear vpdn tunnel
Router(config-vpdn)#
```

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **do**

show コマンド出力リダイレクション

この機能は **show** コマンドと **more** コマンド出力を Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）からファイルにリダイレクトする機能を追加します。

show コマンド出力リダイレクション機能の機能仕様

機能の履歴	
リリース	**変更点**
12.0(21)S	この機能が導入されました。
12.2(13)T	この機能は、Cisco IOS Release 12.2 T に統合されました。

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、Cisco.com のアカウントを作成できます。次の URL にある指示に従ってください。

http://www.cisco.com/register

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://www.cisco.com/go/fn

Cisco IOS ソフトウェア イメージの可用性

特定の Cisco IOS ソフトウェア リリースをサポートしているプラットフォームは、そのプラットフォーム用のソフトウェア イメージがあるかどうかによります。一部のプラットフォームのソフトウェア イメージは、事前の通知なしに延期、遅延、または変更される場合があります。各 Cisco IOS ソフトウェア リリースのプラットフォーム サポートおよび利用可能なソフトウェア イメージの更新情報は、オンライン リリース ノートまたは Cisco Feature Navigator（サポートされている場合）を参照してください。

この章の構成

show コマンド出力リダイレクションについて

この機能では Cisco IOS CLI の **show** コマンドを強化し、後から参照するために大量のデータ出力をファイルに直接書き込むことができます。このファイルはフラッシュ、SAN ディスク、あるいは外部メモリ デバイスなどのローカルまたはリモート ストレージ デバイスに保存できます。

発行される各 **show** コマンドにつき、新しいファイルを作成したり、出力を既存のファイルに追加したりできます。**tee** キーワードを使用して、任意で、ファイルにリダイレクトしながらコマンド出力を画面表示できます。パイプ（|）文字を任意の **show** コマンドの後に付け、**redirect**、**append**、または **tee** キーワードと組み合わせることでリダイレクトが可能になります。

発行される各 **show** コマンドにつき、新しいファイルを作成したり、出力を既存のファイルに追加したりできます。**tee** キーワードを使用して、任意で、ファイルにリダイレクトしながらコマンド出力を画面表示できます。パイプ（|）文字を任意の **show** コマンドの後に付け、次のキーワードと組み合わせることでリダイレクトが可能になります。

出力リダイレクション キーワード：

キーワード	用法
append	URL（追加処理に対応した URL のみ）にリダイレクト出力を追加
begin	一致する行から始める
count	regexp に一致する行数をカウント
exclude	一致する行を除外
format	指定された spec ファイルを使用して出力をフォーマット
include	一致する行を含める
redirect	出力を URL にリダイレクトする
tee	出力を URL にコピー

これらの拡張は **more** コマンドにも追加できます。

show コマンドの機能拡張を使用する方法

この機能拡張に関連付けられているコンフィギュレーション作業はありません。使用方法については、「コマンド リファレンス」（P.3）のコマンド ページを参照してください。

その他の関連資料

特定の **show** および **more** コマンドについては、Cisco.com から『Cisco IOS Documentation Set for Release 12.2 T』を参照してください。

この機能に適用される規格、MIB、RFC はありません。

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Command List, All Releases*』を参照してください。

- **more <url> append**
- **show <command> append**
- **show <command> redirect**
- **show <command> tee**

セットアップおよび自動インストールを使用した設定

概要：シスコ ネットワーキング デバイスの基本設定

Cisco IOS ソフトウェアでは、Cisco IOS ベースのネットワーキング デバイスの設定を単純化するために、自動インストールとセットアップ モードの 2 つの機能が提供されています。自動インストールを使用すると、デバイス コンフィギュレーション ファイルを離れた場所から自動的にロードし、それを使用して複数のデバイスを同時に設定できます。セットアップは、システムの基本（スタートアップとも呼びます）設定をガイドする対話型の Cisco IOS ソフトウェア Command-Line Interface（CLI; コマンドライン インターフェイス）モードですが、一度に設定できるのは 1 台のデバイスに制限されます。自動インストールは、設定するデバイスに対する自動的なプロセスですが、セットアップは設定するデバイスに対する手動のプロセスです。

このモジュールでは、それぞれの機能の概要を説明し、機能についての詳しい説明とその使用方法が記載されているモジュールを示します。

*初期設定*という用語と*スタートアップ コンフィギュレーション*という用語は、同じ意味で使用されます。

この章の構成

シスコ ネットワーキング デバイスの基本設定のための前提条件

Cisco IOS 自動インストールの前提条件

- 『Using AutoInstall to Remotely Configure Cisco Networking Devices』モジュールは、Cisco IOS Release 12.4(1) 以降が動作するネットワーキング デバイス向けに書かれています。しかし、このマニュアルのほとんどの情報は、自動インストールをサポートしている、Cisco IOS release 12.4(1) 以降が動作していないネットワーキング デバイスに対して使用できます。念頭に置くべき主な違いは次の 2 つです。
  - 一部のシスコ ネットワーキング デバイスは、DHCP の代わりに BOOTP を使用して、LAN インターフェイス上で IP アドレスを要求します。DHCP サーバで BOOTP のサポートをイネーブルにすることで、この問題が解決されます。
  - 一部のシスコ ネットワーキング デバイスでは、DHCP クライアント ID の形式が、Cisco IOS release 12.4(1) 以降が動作するネットワーキング デバイスのものと異なります。このマニュアルでは、Cisco IOS release 12.4(1) 以降が動作するネットワーキング デバイスで使用されている DHCP クライアント ID 形式についてだけ説明します。現在のシスコ ネットワーキング デバイスが使用している DHCP クライアント ID の形式を特定するには、『Using AutoInstall to Remotely Configure Cisco Networking Devices』モジュールの「Determining the Value for the DHCP Client Identifier Automatically」の項を参照してください
- 自動インストールを使用して設定するネットワーキング デバイス上の NVRAM にコンフィギュレーション ファイルが存在しないこと。
- 自動インストールを使用してネットワーキング デバイス上にロードするコンフィギュレーション ファイルが、ネットワークに接続されている TFTP サーバ上にあること。ほとんどの場合、ファイルは複数あります。たとえば、IP からホスト名へのマッピングが格納されたネットワーク ファイルと、デバイス固有のコンフィギュレーション ファイルです。
- 自動インストールを使用して設定するネットワーキング デバイスをネットワークに接続して電源を投入するために、リモート サイトに誰かがいること。
- 自動インストール プロセス中にネットワーキング デバイスが TFTP サーバからコンフィギュレーション ファイルをロードできるように、ネットワークで IP 接続が可能であること。
- LAN 接続経由で自動インストールを使用してネットワーキング デバイスに IP アドレスを付与するため、ネットワーク上で DHCP サーバが利用できること。

Cisco IOS セットアップ モードの前提条件

- 設定するデバイスのコンソール ポートに端末が接続されていること。
- 設定するインターフェイスがわかっていること。
- イネーブルにするルーティング プロトコルがわかっていること。

  ルーティング プロトコルについては、『*Cisco IOS IP Routing Protocols Configuration Guide*』を参照してください。
- 設定するデバイスがブリッジングを実行するかどうかがわかっていること。
- 設定するデバイスにプロトコル変換がインストールされているかどうかがわかっていること。
- 設定するプロトコルのネットワーク アドレスがわかっていること。

  ネットワーク アドレスについては、『*Cisco IOS IP Addressing Services Configuration Guide*』を参照してください。
- ネットワーク環境のパスワード方針が決まっていること。

パスワードとデバイスのセキュリティについては、『*Cisco IOS Security Configuration Guide*』の「Configuring Security with Passwords, Privilege Levels, and Login User names for CLI Sessions on Networking Devices」を参照してください。

- 設定する製品のマニュアルが手元にあるか、アクセスできること。

シスコ ネットワーキング デバイスの基本設定における制約事項

Cisco IOS 自動インストールの制約事項

- （シリアル インターフェイスだけ）HDLC またはフレーム リレーを使用したシリアル インターフェイスでは、新しいデバイスの最初のシリアル ポート（シリアル インターフェイス 0 またはシリアル インターフェイス x/0）上だけで自動インストールを実行できます。
- （LAN インターフェイスだけ）物理的なジャンパを使用してリング速度を設定した LAN トークンリング インターフェイスだけで自動インストールがサポートされます。

Cisco IOS セットアップ モードの制約事項

- セットアップ モードはハードウェア依存です。設定する製品のマニュアルに記載されている手順に従う必要があります。
- 一部のコンフィギュレーション パラメータは、ネットワーキング デバイスにプロトコル変換オプションがインストールされている場合にだけ適用されます。デバイスにプロトコル変換オプションがインストールされていない場合、これらのパラメータに対するプロンプトは表示されません。

シスコ ネットワーキング デバイスの基本設定について

基本設定を使用してネットワーキング デバイスを設定する前に、次の概念について理解し、要件に基づいて、自動インストールとセットアップ モードのどちらが最適な方法なのかを判断する必要があります。

- 「Cisco IOS 自動インストールと Cisco IOS セットアップ モードの比較」（P.3）
- 「Cisco IOS 自動インストール」（P.3）
- 「Cisco IOS セットアップ モード」（P.4）

Cisco IOS 自動インストールと Cisco IOS セットアップ モードの比較

Cisco IOS 自動インストールを使用すると、デバイス コンフィギュレーション ファイルを離れた場所から自動的にロードし、それを使用して複数のデバイスを同時に設定できます。セットアップは、システムの基本（スタートアップとも呼びます）設定をガイドする対話型の Cisco IOS ソフトウェア CLI モードですが、一度に設定できるのは 1 台のデバイスに制限されます。自動インストールは自動的なプロセスですが、セットアップは手動のプロセスです。

Cisco IOS 自動インストール

自動インストールは、リモートのネットワーキング デバイスを中央から設定できる、Cisco IOS ソフトウェアの機能です。コンフィギュレーション ファイルは、自動インストールを使用して設定するデバイスがアクセス可能な TFTP サーバに格納する必要があります。

自動インストールは、LAN、High-Level Data Link Control（HDLC; ハイレベル データリンク コントロール）カプセル化を使用したシリアル インターフェイス、WAN 用のフレーム リレー カプセル化を使用したシリアル インターフェイス、および WIC-1-DSU-T1v2 カード（他の T1E1 カードでは自動インストールはサポートされていません）に対し、イーサネット、トークンリング、FDDI インターフェイス上でサポートされています。

自動インストールは、リモート サイトでの設置の中央での管理を容易にするように設計されています。自動インストール プロセスは、Cisco IOS ソフトウェアベースのデバイスの電源をオンにし、NVRAM に有効なコンフィギュレーション ファイルがない場合に開始されます。ネットワーキング デバイスに Cisco ルータと Security Device Manager（SDM）または Cisco Network Assistant がすでにインストールされている場合には、自動インストールは開始されません。この場合、自動インストールをイネーブルにするには、SDM をディセーブルにする必要があります。

『Using AutoInstall to Remotely Configure Cisco Networking Devices』モジュールでは、AutoInstall の動作、SDM をディセーブルにする方法、AutoInstall を使用するようにデバイスを設定する方法が説明されています。

Cisco IOS セットアップ モード

Cisco IOS セットアップ モードを使用すると、Cisco IOS CLI またはシステム設定ダイアログを使用して初期設定ファイルを作成できます。初期設定手順がダイアログに表示されるため、シスコの製品や CLI に慣れておらず、CLI によって提供される詳細なレベルでの設定変更が不要な場合に便利です。

セットアップは、デバイスの NVRAM にコンフィギュレーション ファイルがなく、Cisco SDM を使用するように工場で事前設定されていない場合に開始されます。セットアップが完了すると、システム設定ダイアログが表示されます。ダイアログに従ってデバイスとネットワークに関する基本的な情報を入力することで初期設定が行われ、初期設定ファイルが作成されます。ファイルが作成された後、CLI を使用して追加の設定を行うことができます。

『Using Setup Mode to Configure a Cisco Networking Device』では、セットアップを使用して基本設定を作成する方法と、設定を変更する方法について説明しています。

関連情報

『Using AutoInstall to Remotely Configure Cisco Networking Devices』モジュールまたは『Using Setup Mode to Configure a Cisco Networking Device』モジュールに進んでください。

その他の関連資料

このセクションでは、シスコ ネットワーキング デバイスの基本設定に関する参考資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
設定の基本的なコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS ソフトウェアの自動インストール機能を使用した初めてのネットワーキング デバイスの設定	『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using AutoInstall to Remotely Configure Cisco Networking Devices」モジュール
Cisco IOS セットアップ モードを使用したネットワーキング デバイスの設定	『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using Setup Mode to Configure a Cisco Networking Device 」モジュール

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

概要：シスコ ネットワーキング デバイスの基本設定の機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。<

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　概要：シスコ ネットワーキング デバイスの基本設定の機能情報

機能名	リリース	機能情報
概要：シスコ ネットワーキング デバイスの基本設定	12.4(3)	Cisco IOS ソフトウェアでは、Cisco IOS ベースのネットワーキング デバイスの設定を単純化するために、自動インストールとセットアップ モードの 2 つの機能が提供されています。自動インストールを使用すると、デバイス コンフィギュレーション ファイルを離れた場所から自動的にロードし、それを使用して複数のデバイスを同時に設定できます。セットアップは、システムの基本（スタートアップとも呼びます）設定をガイドする対話型の Cisco IOS ソフトウェア Command-Line Interface（CLI; コマンドライン インターフェイス）モードですが、一度に設定できるのは 1 台のデバイスに制限されます。自動インストールは、設定するデバイスに対する自動的なプロセスですが、セットアップは設定するデバイスに対する手動のプロセスです。

セットアップ モードを使用したシスコ ネットワーキング デバイスの設定

セットアップ モードには、新規ネットワーキング デバイスや、NVRAM から startup-config ファイルを削除してしまったデバイスの初期設定ファイル作成を支援するインタラクティブ メニューが用意されています。インタラクティブ メニューに従って、初期設定を最初から最後まで行うことができます。インターフェイス メニューは、シスコ製品や Command Line Interface（CLI; コマンドライン インターフェイス）に慣れていない場合や、コンフィギュレーションの変更が CLI の提供するレベルの詳細設定を必要としていない場合に便利です。また、セットアップ モードを使用して、既存のコンフィギュレーションを変更することもできます。

このモジュールでは、フル コンフィギュレーションで、システム設定ダイアログを使用してシスコのネットワーキング デバイスを準備する方法、および初期設定の完了後にコンフィギュレーションを変更する方法を説明します。

このモジュールでは、ファイル名を読みやすくするために、二重引用符で囲んであります。また、*デバイス*および*ネットワーキング デバイス*という用語は、ルータ、スイッチ、または Cisco IOS ソフトウェアが実行されているその他のデバイスを表します。*初期設定*という用語と*スタートアップ コンフィギュレーション*という用語は、同じ意味で使用されます。

変更履歴

このマニュアルの初版の発行は 2005 年 8 月 9 日 で、最終更新日は 2006 年 10 月 です。

この章の構成

- 「その他の関連資料」（P.16）
- 「シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための機能情報」（P.17）

シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための前提条件

- 『Basic Configuration of a Cisco Networking Device Overview』モジュールを読んでいること。
- 設定の対象となるデバイスのコンソール ポートに ASCII 端末が接続されていること。
- 設定するインターフェイスがわかっていること。
- イネーブルにするルーティング プロトコルがわかっていること。

  ルーティング プロトコルの詳細については、『*Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4』を参照してください。
- 設定するデバイスがブリッジングを実行するかどうかがわかっていること。
- 設定するデバイスにプロトコル変換がインストールされているかどうかがわかっていること。
- 設定するプロトコルのネットワーク アドレスがわかっていること。

  ネットワーク アドレスの詳細については、『*Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4』を参照してください。
- ネットワーク環境のパスワード方針が決まっていること。

  パスワードとデバイス セキュリティの詳細については、『*Cisco IOS Security Configuration Guide*, Release 12.4』の「Configuring Security with Passwords, Privilege Levels, and Login User names for CLI Sessions on Networking Devices」を参照してください。
- 設定する製品のマニュアルが手元にあるか、アクセスできること。

シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための制約事項

- セットアップ モードはハードウェア依存です。設定する製品のマニュアルに記載されている手順に従う必要があります。
- 一部のコンフィギュレーション パラメータは、ネットワーキング デバイスにプロトコル変換オプションがインストールされている場合にだけ適用されます。デバイスにプロトコル変換オプションがインストールされていない場合、これらのパラメータに対するプロンプトは表示されません。

シスコ ネットワーキング デバイスを設定する Cisco IOS セットアップ モードの使用について

シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用する前に、次の概念を理解しておく必要があります。

- 「Cisco IOS セットアップ モード」（P.3）

Cisco IOS セットアップ モード

Cisco IOS セットアップ モードを使用すると、Cisco IOS CLI またはシステム設定ダイアログを使用して初期設定ファイルを作成できます。初期設定手順がダイアログに表示されるため、シスコの製品や CLI に慣れておらず、CLI によって提供される詳細なレベルでの設定変更が不要な場合に便利です。

セットアップは、デバイスの NVRAM にコンフィギュレーション ファイルがなく、Cisco ルータおよび Security Device Manager（SDM）を使用するように工場で事前設定されていない場合に開始されます。セットアップが完了すると、システム設定ダイアログが表示されます。ダイアログに従ってデバイスとネットワークに関する基本的な情報を入力することで初期設定が行われ、初期設定ファイルが作成されます。ファイルが作成された後、CLI を使用して追加の設定を行うことができます。

Cisco Router and Security Device Manager

Cisco Security Device Manager（SDM）は、ネットワーキング デバイスで Cisco IOS ネットワーク接続およびセキュリティ機能を設定するための Web ベースのデバイス管理ツールです。SDM には、デフォルト コンフィギュレーションが 1 つと、シスコ ネットワーキング デバイス、LAN または WAN の追加接続、VPN 接続の設定やファイアウォールの作成、セキュリティ監査の実行について手順を追ってガイドするさまざまなウィザードが用意されています。

初期設定の構築に加え、SDM にはファイアウォール ポリシーや Network Address Translation（NAT; ネットワーク アドレス変換）などの拡張機能を設定するための拡張モードも用意されています。

一部のシスコ製品には、工場出荷時に SDM がインストールされています。デバイスに SDM がプレインストールされているときに、セットアップを使用して、初期設定を行う場合は、まず、SDM のデフォルト コンフィギュレーションをディセーブルにする必要があります。

システム設定ダイアログ

*システム設定ダイアログ*は、インタラクティブな CLI モードで、シスコ ネットワーキング デバイスの初期設定に必要な情報を求めるプロンプトを表示します。CLI と同様、システム設定ダイアログにも、プロンプトごとにヘルプ テキストが用意されています。このヘルプ テキストを表示するには、プロンプトで疑問符（**?**）を入力します。

システム設定ダイアログのプロンプトは、ハードウェア、インストールされているインターフェイス モジュール、およびソフトウェア イメージによって異なります。初期設定でのこのダイアログの使用については、製品付属のマニュアルを参照してください。

プロンプトの隣にある角カッコ内に表示されている値は現在の設定を表しています。これらは工場出荷時のデフォルト設定であることもありますし、デバイスの最新設定であることもあります。この設定をそのまま使用するには、キーボードの **Enter** キーを押します。

変更を行わず、またダイアログの最後までいかずにシステム設定ダイアログを終了し、特権 EXEC モードに戻るには、**Ctrl+C** キーを押します。ダイアログは終了するが、セットアップは続行するという場合は、特権 EXEC モードで **setup** コマンドを発行します。

ダイアログに表示される手順をすべて完了すると、デバイスには変更後のコンフィギュレーション ファイルが表示され、このファイルを使用するかどうかの確認が求められます。yes または no で答える必要があります。このプロンプトにはデフォルト値はありません。yes と答えた場合、このファイル

はスタートアップ コンフィギュレーションとして、NVRAM に保存されます。no の場合、ファイルは保存されません。別の初期設定ファイルを作成する場合は、ダイアログの最初からはじめる必要があります。

すばやく簡単に初期設定を実行するほか、システム設定 ダイアログは初期設定の実行後に、基本的なコンフィギュレーションの変更にも使用できます。

Cisco IOS セットアップ モードを使用する利点

シスコ製品や CLI に詳しくないユーザにとって、Cisco IOS セットアップ モードのシステム設定ダイアログは便利なツールです。ユーザは、このダイアログが表示する設定プロセスのプロンプトに従って基本的な情報を入力することで、デバイスを動作可能にすることができます。一般的な設定変更が必要である場合も、このダイアログが詳細レベルの CLI の代わりになります。

シスコ ネットワーキング デバイスの設定と設定変更における Cisco IOS セットアップ モードの使用方法

この項では、システム設定ダイアログを使用して初期設定ファイルを作成する方法、およびスタートアップ コンフィギュレーションのロード後に、設定変更を行う方法を説明します。

SDM デフォルト コンフィギュレーション ファイルのディセーブル化

使用しているデバイスに SDM がプレインストールされているときに、セットアップを使用して、初期設定ファイルを作成する場合は、次の作業を実行します。SDM はデバイスに残ります。

使用しているデバイスに SDM がプレインストールされているときに、代わりに自動インストールを使用して、デバイスを設定する場合は、次の作業を実行します。SDM はデバイスに残ります。

手順の概要

1. デバイスのコンソール ポートから、PC のシリアル ポートにコンソール ケーブルを接続します。
2. 電源モジュールをデバイスに接続し、この電源モジュールをコンセントに差し込んで、デバイスの電源をオンにします。
3. 端末エミュレーション プログラムを使用して、デバイスに接続します。
4. **enable**
5. **erase startup-config**
6. **reload**

手順の詳細

ステップ 1 デバイスに付属しているコンソール ケーブルを、デバイスのコンソール ポートから PC のシリアル ケーブルに接続します。手順については、使用しているデバイスのハードウェア インストール ガイドを参照してください。

ステップ 2 電源モジュールをデバイスに接続し、この電源モジュールをコンセントに差し込んで、デバイスの電源をオンにします。手順については、使用しているデバイスのクイック スタート ガイドを参照してください。

ステップ 3 使用している PC の Hyperterminal またはこれに準じた端末エミュレーション プログラムで、次のように端末エミュレーション設定を行い、デバイスに接続します。

- 9600 ボー
- 8 データ ビット、パリティなし、1 ストップ ビット
- フロー制御なし

ステップ 4 **enable**

特権 EXEC モードを開始します。

enable

```
Router> enable
Router#
```

ステップ 5 **erase startup-config**

NVRAM から既存のコンフィギュレーションを消去します。

```
Router# erase startup-config
```

ステップ 6 **reload**

リロード プロセスを開始します。ルータはリロード プロセスの終了後、自動インストール プロセスを開始します。

```
Router# reload
```

システム設定ダイアログを使用した初期設定ファイルの作成

シスコ ネットワーキング デバイスの初期設定を作成するには、次の作業を実行します。

前提条件

SDM がインストールされている場合、セットアップを使用する前に、デフォルト コンフィギュレーション ファイルをディセーブルにする必要があります。

制約事項

システム設定ダイアログでは、設定用パラメータをランダムに選択したり、入力したりすることはできません。変更する情報が画面に表示されるまで、ダイアログで手順を 1 つずつ表示していく必要があります。

手順の概要

1. デバイスの電源を入れます。
2. プロンプトで **yes** と入力し、初期設定ダイアログに入ります。
3. この設定ダイアログで続行するかどうかを確認するプロンプトが表示されたら **yes** と入力して、次に進みます（この手順は表示されないこともあります）。
4. プロンプトで **yes** と入力して、基本管理の設定に入ります。
5. デバイスのホスト名を入力します。
6. イネーブル シークレット パスワードを入力します。
7. イネーブル パスワードを入力します。
8. 仮想端末のパスワードを入力します。
9. 使用しているネットワークにあわせて、プロンプトに答えます。
10. デバイスを管理コンソールに接続するためのインターフェイスを選択します。
11. 使用しているネットワークにあわせて、プロンプトに答えます。
12. **2** を入力して、NVRAM にコンフィギュレーション ファイルを保存し、終了します。

手順の詳細

ステップ 1 デバイスの電源を入れます。

ステップ 2 プロンプトで **yes** と入力し、初期設定ダイアログに入ります。

開始シーケンスの最後に、次のメッセージが表示された場合、システム設定ダイアログは自動的に呼び出されます。

```
--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes
```

画面には次のように表示されます。

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

ステップ 3 この設定ダイアログで続行するかどうかを確認するプロンプトが表示されたら **yes** と入力して、次に進みます（この手順は表示されないこともあります）。

```
Continue with configuration dialog? [yes/no]: yes
```

ステップ 4 基本管理画面が表示されます。

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

yes と入力し、基本管理の設定に入ります。

```
Would you like to enter basic management setup? [yes/no]: yes

The screen displays the following:

Configuring global parameters:

Enter host name [R1]:
```

ステップ 5 デバイスのホスト名を入力します。この例では「Router」と入力しています。

```
Configuring global parameters:

Enter host name [R1]: Router

The screen displays the following:

The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret:
```

ステップ 6 イネーブル シークレット パスワードを入力します。このパスワードは暗号化され、コンフィギュレーションを表示しても、見ることはできません。

```
Enter enable secret: 1g2j3mm
```

画面には次のように表示されます。

```
The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password:
```

ステップ 7 イネーブル シークレット パスワードとは異なるイネーブル パスワードを入力します。イネーブル パスワードは暗号化されず、コンフィギュレーションを表示したときに見ることができます。

```
  Enter enable password: cts54tnl
```

画面には次のように表示されます。

```
The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password:
```

ステップ 8 仮想端末のパスワードを入力します。このパスワードは、コンソール ポートを通じてデバイスにアクセスする場合だけ使用します。

```
  Enter virtual terminal password: tls6gato
```

画面には次のように表示されます。

```
Configure SNMP Network Management? [no]:
```

ステップ 9 使用しているネットワークにあわせて、次のプロンプトに答えます。この例では、**Enter** キーを押して、現在の設定 [no] をそのまま使用します。

```
Configure SNMP Network Management? [no]:
```

使用可能なインターフェイスの概要が表示されます。表示されるインターフェイス番号はプラットフォームの種類と、インストールされているインターフェイス モジュールおよびカードによって異なります。

```
Current interface summary
Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                unassigned      YES NVRAM  administratively down dow
Ethernet1/0                unassigned      YES NVRAM  administratively down dow
Serial2/0                  unassigned      YES NVRAM  administratively down dow
Serial3/0                  unassigned      YES NVRAM  administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up

Enter interface name used to connect to the
management network from the above interface summary:
```

ステップ 10 ルータを管理ネットワークに接続するためのインターフェイスを選択します。

```
Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0
```

ステップ 11 使用しているネットワークにあわせて、プロンプトに答えます。この例では、IP を設定しています。IP アドレスを入力し、現在のサブネット マスクをそのまま使用します。画面には、作成されたコマンド スクリプトが表示されています。

```
Configuring interface Ethernet0/0:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.17.1.1
    Subnet mask for this interface [255.255.0.0] :
    Class B network is 172.17.0.0, 16 subnet bits; mask is /16

The following configuration command script was created:

hostname Router
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
line vty 0 4
password tls6gato
no snmp-server
!
no ip routing
!
interface Ethernet0/0
no shutdown
ip address 172.17.1.1 255.255.0.0
!
interface Ethernet1/0
shutdown
no ip address
!
interface Serial2/0
shutdown
no ip address
!
interface Serial3/0
shutdown
no ip address
!
end

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

ステップ 12 「**2**」を入力するか、**Enter** キーを押して、NVRAM にコンフィギュレーション ファイルを保存し、終了します。

```
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
```

画面には次のように表示されます。

```
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

Router#
00:01:32: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:01:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed p
```

この次の手順

「設定の確認」（P.10）に進みます。

システム設定ダイアログを使用した設定変更

設定変更には、CLI が提供するレベルの詳細設定が必要ない場合には、CLI の代わりに *システム設定ダイアログ*を使用します。たとえば、プロトコル スイートの追加、アドレッシング方式の変更、新たにインストールされたインターフェイスの設定には、システム設定ダイアログを使用できます。CLI が提供するコンフィギュレーション モードを使用してこれらの変更を行うこともできますが、*システム設定ダイアログ*では、設定の概要を確認できるうえ、このダイアログに表示される手順に従って、設定を行うことができます。

前提条件

ハードウェアの追加または変更に伴い、設定を更新する必要がある場合、物理および論理ポートの割り当てについては、使用しているプラットフォームのマニュアルを参照してください。

制約事項

システム設定ダイアログでは、設定用パラメータをランダムに選択したり、入力したりすることはできません。変更する情報が画面に表示されるまで、ダイアログで手順を 1 つずつ表示していく必要があります。

手順の概要

1. **enable**
2. **setup**
3. **前述の「システム設定ダイアログを使用した初期設定ファイルの作成」（P.5）にある「手順の詳細」のステップ 3 ～ 12 を実行します。**
4. 設定が正しく変更されていることを確認します。「設定の確認」（P.10）を参照してください。

手順の詳細

ステップ 1 **enable**

enable コマンドにより、特権 EXEC モードが開始されます。

```
Router> enable
Router#
```

ステップ 2 **setup**

setup コマンドにより、ルータは**セットアップ モード**になります。

```
Router# setup
```

画面には次のように表示されます。

```
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

プロンプトで yes を入力し、**ダイアログを続行します。**

```
Continue with configuration dialog? [yes/no]: yes
```

画面には次のように表示されます。

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]:
```

ステップ 3 **前述の「システム設定ダイアログを使用した初期設定ファイルの作成」（P.5）にある「手順の詳細」のステップ 3 ～ 12 を実行します。**

ステップ 4 設定が正しく変更されていることを確認します。「設定の確認」（P.10）を参照してください。

設定の確認

システム設定ダイアログを使用して作成した設定が正常に動作していることを確認するには、次の作業を実行します。

手順の概要

1. **show interfaces**
2. **show ip interface brief**
3. **show configuration**

手順の詳細

ステップ 1 **show interfaces**

このコマンドは、インターフェイスが正常に動作していること、およびこれらのインターフェイスとライン プロトコルが正しいステータス（up または down）であることを検証します。

ステップ 2　show ip interface brief

このコマンドは、IP に対して設定されているインターフェイスのステータスの概要を表示します。

ステップ 3　show configuration

このコマンドは、ホスト名とパスワードが正確に設定されていることを検証します。

例

この例は、「システム設定ダイアログを使用した初期設定ファイルの作成」（P.5）のステップ 1 ～ 12 で作成されたコンフィギュレーション ファイルを検証しています。

```
Router# show interfaces

Ethernet0/0 is up, line protocol is up
  Hardware is AmdP2, address is aabb.cc03.6c00 (bia aabb.cc03.6c00)
  Internet address is 172.17.1.1/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     11 packets output, 1648 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Ethernet1/0 is administratively down, line protocol is down
  Hardware is AmdP2, address is aabb.cc03.6c01 (bia aabb.cc03.6c01)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions     DCD=up  DSR=up  DTR=down  RTS=down  CTS=up

Serial3/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions     DCD=down  DSR=down  DTR=up  RTS=up  CTS=down

Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 1.1.1.1/32
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets

Router# show ip interface brief

Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                172.17.1.1      YES manual up                    up
Ethernet1/0                unassigned      YES manual administratively down dow
Serial2/0                  unassigned      YES manual administratively down dow
Serial3/0                  unassigned      YES manual administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up

Router# show configuration

Using 1029 out of 8192 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
!
no aaa new-model
!
resource manager
!
clock timezone PST -8
ip subnet-zero
no ip routing
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 no ip route-cache
!
interface Ethernet0/0
 ip address 172.17.1.1 255.255.0.0
 no ip route-cache
!
interface Ethernet1/0
 no ip address
 no ip route-cache
 shutdown
!
interface Serial2/0
 no ip address
 no ip route-cache
 shutdown
```

```
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
!
ip classless
no ip http server
!
!
!
!
control-plane
!
!
line con 0
 transport preferred all
 transport output all
line aux 0
 transport preferred all
 transport output all
line vty 0 4
 password tls6gato
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための設定例

ここでは、次の設定例について説明します。

- 「システム設定ダイアログを使用したイーサネット インターフェイス 0 の設定：例」（P.14）

システム設定ダイアログを使用したイーサネット インターフェイス 0 の設定：例

次の例では、システム設定ダイアログを使用して、イーサネット インターフェイス 0 と IP アドレスを設定しています。

（注） プロンプト、およびこれらが画面に表示される順番は、プラットフォーム、およびデバイスにインストールされているインターフェイスによって異なります。

```
R1# setup

--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help.
```

```
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [R1]: Router

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: 1g2j3mmc

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: cts54tnl

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: tls6gato
  Configure SNMP Network Management? [no]:

Current interface summary
Interface                  IP-Address      OK? Method Status                Prol
Ethernet0/0                172.17.1.1      YES manual up                    up
Ethernet1/0                unassigned      YES manual administratively down dow
Serial2/0                  unassigned      YES manual administratively down dow
Serial3/0                  unassigned      YES manual administratively down dow
Loopback0                  1.1.1.1         YES NVRAM  up                    up

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 172.17.1.1
    Subnet mask for this interface [255.255.0.0] :
    Class B network is 172.17.0.0, 16 subnet bits; mask is /16

The following configuration command script was created:

hostname Router
enable secret 5 $1$1Gg9$GuxXfUUBBfVqGvlW4psIm1
enable password cts54tnl
line vty 0 4
password tls6gato
no snmp-server
!
no ip routing

!
interface Ethernet0/0
no shutdown
ip address 172.17.1.1 255.255.0.0
!
interface Ethernet1/0
shutdown
no ip address
!
```

```
interface Serial2/0
shutdown
no ip address
!
interface Serial3/0
shutdown
no ip address
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

Router#
00:01:32: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:01:33: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed p
```

その他の関連資料

次の項では、シスコ ネットワーキング デバイスの設定での Cisco IOS セットアップの使用に関連する参考資料を示します。

関連資料

関連項目	参照先
シスコ ネットワーキング デバイスの設定に使用される Cisco IOS セットアップ モードと自動インストールの概要	『Basic Configuration of a Cisco Networking Device Overview』
Cisco IOS 自動インストール機能を使用したシスコ ネットワーキング デバイスの設定	『Using AutoInstall to Remotely Configure Cisco Networking Devices』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対する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
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport

シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) または 12.0(3)S 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　シスコ ネットワーキング デバイスの設定に Cisco IOS セットアップ モードを使用するための機能情報

機能名	リリース	機能設定情報
Cisco IOS Release 12.2(1) 以降で導入または変更された機能はないため、この表は意図的に空白のままにしてあります。この表は、このモジュールに機能情報が追加された場合に更新されます。	—	—

自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

自動インストールを使用すると、ネットワーキング デバイスをリモートから自動的に設定できます。一般に、自動インストールは、新しいネットワーキング デバイスをリモートからセットアップするために使用します。ただし、既存のネットワーキング デバイスについても、NVRAM からコンフィギュレーション ファイルを削除した後で、自動インストールを使用して設定できます。自動インストール プロセスは、TFTP サーバにあらかじめ格納されているコンフィギュレーション ファイルを使用します。

このモジュールでは、*ネットワーキング デバイス*という用語は、Cisco IOS ソフトウェアが動作するルータを指します。また、次の用語は同じ意味で使用されます。

- *初期設定とスタートアップ コンフィギュレーション*
- *セットアップと設定*

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「自動インストールを使用したシスコのネットワーキング デバイスの設定に関する機能情報」（P.54）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

- 「自動インストールを使用してシスコ ネットワーキング デバイスをリモートで設定する方法」（P.16）
- 「自動インストールを使用してシスコのネットワーキング デバイスをリモートで設定する例」（P.34）
- 「その他の関連資料」（P.51）
- 「自動インストールを使用したシスコのネットワーキング デバイスの設定に関する機能情報」（P.54）

自動インストールを使用してシスコのネットワーキング デバイスをリモートで設定するための前提条件

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Overview: Basic Configuration of a Cisco Networking Device」モジュールを読んでおく必要があります。
- このマニュアルは、特に Cisco IOS Release 12.4(1) 以降が動作するネットワーキング デバイス向けに書かれています。しかし、このマニュアルのほとんどの情報は、自動インストールをサポートしている、Cisco IOS release 12.4(1) 以降が動作していないネットワーキング デバイスに対して使用できます。念頭に置くべき主な違いは次の 2 つです。
  - 一部のシスコ ネットワーキング デバイスは、DHCP の代わりに BOOTP を使用して、LAN インターフェイス上で IP アドレスを要求します。DHCP サーバで BOOTP のサポートをイネーブルにすることで、この問題が解決されます。
  - 一部のシスコ ネットワーキング デバイスでは、DHCP クライアント ID の形式が、Cisco IOS release 12.4(1) 以降が動作するネットワーキング デバイスのものと異なります。このマニュアルでは、Cisco IOS release 12.4(1) 以降が動作するネットワーキング デバイスで使用されている DHCP クライアント ID 形式についてだけ説明します。現在のシスコ ネットワーキング デバイスが使用している DHCP クライアント ID 形式を特定する方法については、「自動的な DHCP クライアント ID の特定：例」（P.37）を参照してください。
- 自動インストールを使用して設定するネットワーキング デバイス上の NVRAM にコンフィギュレーション ファイルが存在しないこと。
- 自動インストールを使用してネットワーキング デバイス上にロードするコンフィギュレーション ファイルが、ネットワークに接続されている TFTP サーバ上にあること。ほとんどの場合、ファイルは複数あります。たとえば、IP からホスト名へのマッピングが格納されたネットワーク ファイルと、デバイス固有のコンフィギュレーション ファイルです。
- 自動インストールを使用して設定するネットワーキング デバイスをネットワークに接続して電源を投入するために、リモート サイトに誰かがいること。
- 自動インストール プロセス中にネットワーキング デバイスが TFTP サーバからコンフィギュレーション ファイルをロードできるように、ネットワークで IP 接続が可能であること。
- LAN 接続経由で自動インストールを使用してネットワーキング デバイスに IP アドレスを付与するため、ネットワーク上で DHCP サーバが利用できること。

自動インストールを使用してシスコのネットワーキング デバイスをリモートで設定するための制約事項

- （シリアル インターフェイスだけ）HDLC またはフレーム リレーを使用したシリアル インターフェイスでは、新しいデバイスの最初のシリアル ポート（シリアル インターフェイス 0 またはシリアル インターフェイス x/0）上だけで自動インストールを実行できます。
- （LAN インターフェイスだけ）物理的なジャンパを使用してリング速度を設定した LAN トークンリング インターフェイスだけで自動インストールがサポートされます。
- 自動インストールは、T1 インターフェイス上では自動的に実行されません。自動インストールを T1 インターフェイス上で動作させるには、T1 インターフェイスを手動で設定してシリアル インターフェイスを作成した後、IP アドレスとネットワーク マスクをそのシリアル インターフェイスに割り当てます。

自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

自動インストールを設定または使用する前に、次の概念を理解しておく必要があります。

- 「自動インストールの概要」（P.3）
- 「自動インストールを使用してシスコ ネットワーキング デバイスをリモートで設定することの利点」（P.15）

自動インストールの概要

自動インストールでは、最終的で全体的な設定か、部分的で一時的な設定を、自動インストールを使用して設定するネットワーキング デバイスにロードできます。

ヒント 自動インストールを使用して部分的で一時的な設定をロードする場合、デバイスの設定を手動で完了する必要があります。

自動インストール用にネットワークをプロビジョニングするための要件と、自動インストールをプロビジョニングするための設定オプションについては、次の項で説明しています。

- 「自動インストールで使用するサービスとサーバ：IP アドレスのダイナミックな割り当て」（P.4）
- 「自動インストールで使用されるサービスとサーバ：IP とホスト名のマッピング」（P.7）
- 「自動インストールが使用するサービスとサーバ：コンフィギュレーション ファイルの格納と転送」（P.8）
- 「自動インストールで使用されるネットワーキング デバイス」（P.9）
- 「自動インストールで使用するコンフィギュレーション ファイル」（P.11）
- 「自動インストールの設定オプション」（P.14）
- 「自動インストール プロセス」（P.14）

自動インストールで使用するサービスとサーバ：IP アドレスのダイナミックな割り当て

ネットワークは、自動インストールを使用して設定するネットワーキング デバイスに対する IP アドレスのダイナミックな割り当てが可能であることが必要です。使用する IP アドレス割り当てサーバの種類は、自動インストールを使用して設定するネットワーキング デバイスのネットワークに対する接続の種類によって変わります。

自動インストールは次の種類の IP アドレス サーバを使用します。

- 「DHCP サーバ」（P.4）
- 「SLARP サーバ」（P.5）
- 「BOOTP サーバ」（P.6）

DHCP サーバ

LAN 接続上で自動インストールを使用するネットワーキング デバイスには、ダイナミックに IP アドレスを提供するために DHCP サーバが必要です。この要件は、イーサネット、トークン リング、および FDDI インターフェイスに適用されます。DHCP サーバと、LAN 接続上で自動インストールを使用するすべてのデバイスとの間で、IP 接続が可能なようにネットワークが設定されている必要があります。

DHCP（RFC 2131 で規定）は、ブートストラップ プロトコル（RFC 951 で規定）により提供される機能を拡張したものです。DHCP は、設定情報を TCP/IP ネットワーク上のホストに渡すためのフレームワークを提供します。DHCP では、再利用可能なネットワーク アドレスと、ルータ（ゲートウェイ）の IP アドレス、TFTP サーバの IP アドレス、ロードするブート ファイルの名前、使用するドメイン名など、追加の設定オプションを自動的に割り当てる機能が追加されています。DHCP サーバは、ルータ、UNIX サーバ、Microsoft Windows ベースのサーバ、その他のプラットフォーム上で設定できます。

一般に DHCP サーバは、IP アドレスのプールからランダムに IP アドレスを割り当てます。DHCP を使用するデバイスは、ネットワークに接続するたびに異なる IP アドレスを取得することがあります。この動作は、自動インストール プロセスの間、特定のデバイスに特定のホスト名を割り当てる必要がある場合に問題になります。たとえば、リモート サイトの異なる階にルータを設置し、各ルータに、**ChicagoHQ-1st** や **ChicagoHQ-2nd** など、その場所を示す名前を割り当てる場合、各デバイスの IP アドレスが、その正しいホスト名にマッピングされるようにする必要があります。

デバイスに特定の IP アドレスが割り当てられるようにするためのプロセスは、*予約の作成*と呼びます。予約とは、IP アドレスと、デバイス上の LAN インターフェイスの物理レイヤ アドレスの間の関係を、手動で設定することです。多くの Cisco IOS ベースのデバイスは、DHCP を通じて IP アドレスを要求する際に、その MAC アドレスを使用しません。代わりに、より長いクライアント ID を使用します。予約を事前に設定するためには、クライアント ID を特定しなくてはならず、新しいデバイスがその MAC アドレスとクライアント ID のどちらを使用するのかを知らなくてはなりません。デバイスが MAC アドレスとクライアント ID のどちらを使用しているかを特定するために、新しいデバイスが最初に DHCP 予約を使用せずに IP アドレスを取得できるようにすることを推奨します。新しいデバイスが DHCP サーバに対して自身を識別する方法がわかったら、その形式をメモして、そのデバイス用の予約を作成します。次回デバイスがリブートした際に、予約した IP アドレスが取得され、新しいデバイスに正しいホスト名が割り当てられます。DHCP の予約の作成について、使用している DHCP サーバ ソフトウェアに付属している情報を参照してください。Cisco IOS ベースの DHCP サーバを使用した予約の作成手順については、「自動インストールを使用した LAN に接続されているデバイスの設定：例」（P.37）を参照してください。この項には、DHCP 予約を事前に設定できるように、デバイスがネットワークに接続される前にクライアント ID を特定するための手順が含まれています。

（注） このマニュアルでは、自動インストールを使用して LAN に接続されているネットワーキング デバイスを設定するために、シスコのルータを DHCP サーバとして使用します。別のデバイスを DHCP サーバとして使用する場合は、設定時に参照できるように、そのユーザ マニュアルを手元に置いてください。

（注） コンフィギュレーション パラメータには、TFTP サーバ アドレス、DNS サーバ アドレス、ドメイン名など、さまざまなものがあります。これらのパラメータは、DHCP サーバにより、IP アドレスをクライアントに割り当てるプロセスの中で、LAN に接続されたクライアントに渡すことができます。これらのパラメータは自動インストールでは必要がないため、このマニュアルでは触れていません。これらのパラメータの使用方法を知っている場合は、自動インストールを使用してネットワーキング デバイスを設定するときに、DHCP サーバの設定に含めることができます。

DHCP サービスの詳細については、IETF RFC のサイト（http://www.ietf.org/rfc.html）で DHCP に関する RFC を参照してください。ほとんどのサーバ オペレーティング システムが DHCP サーバをサポートしています。詳細については、使用しているオペレーティング システムに付属しているマニュアルを参照してください。

SLARP サーバ

HDLC カプセル化を使用してシリアル インターフェイス上で自動インストールを使用して設定するルータは、ステージング ルータに接続されているシリアル インターフェイス上の IP アドレスに対する Serial Line ARP（SLARP; シリアル ライン ARP）要求を送信します。

ステージング ルータのシリアル インターフェイスには、192.168.10.1 や 192.168.10.2 など、ホスト ポートが 1 または 2 の IP アドレスが設定されている必要があります。ステージング ルータは、自動インストールで設定するルータに、ステージング ルータが使用していない値が格納された SLARP 応答を送信します。たとえば、自動インストールで設定するルータに接続されているステージング ルータ上のインターフェイスが、IP アドレスとして 192.168.10.1 を使用している場合、ステージング ルータは、自動インストールで設定するルータに対し、値が 192.168.10.2 の SLARP 応答を送信します。

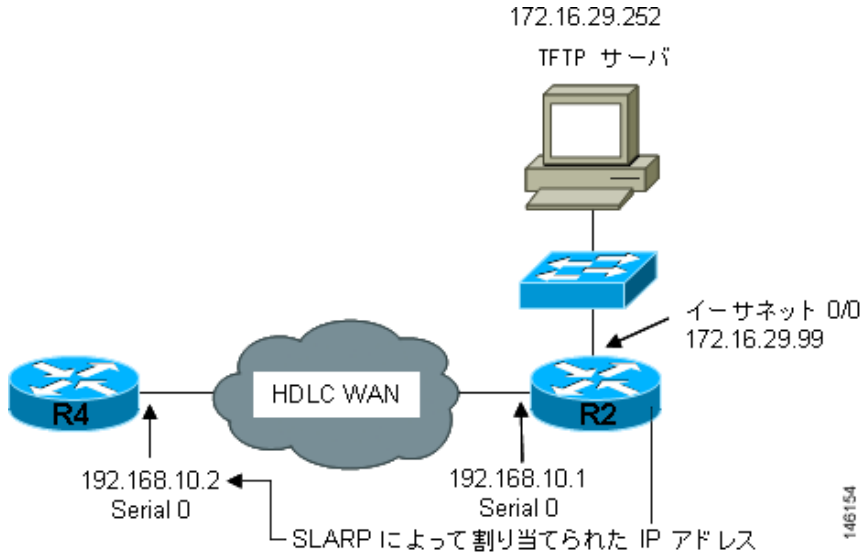
ヒント ステージング ルータのシリアル インターフェイス上でマスク 255.255.255.252 を使用している場合、SLARP は使用可能な IP ホスト アドレスを新しいデバイスに割り当てます。たとえば、IP アドレス 198.162.10.5 255.255.255.252 をステージング ルータの serial 0 に割り当てる場合、SLARP は 198.162.10.6 を新しいデバイスに割り当てます。IP アドレス 198.162.10.6 255.255.255.252 をステージング ルータの serial 0 に割り当てる場合、SLARP は 198.162.10.5 を新しいデバイスに割り当てます。

図 1 に SLARP の例を示します。

自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

図 1 で、ステージング ルータ（R2）上のシリアル インターフェイス 0 の IP アドレスは 192.168.10.1 です。そのため、SLARP は IP アドレス 192.168.10.2 を新しいルータのシリアル インターフェイス 0 に割り当てます。

図 1　　SLARP を使用した新しいデバイスへの IP アドレスの割り当て



（注） HDLC を使用したシリアル インターフェイス上の自動インストールは、新しいデバイスの最初のシリアル ポート（シリアル インターフェイス 0 またはシリアル インターフェイス x/0）上だけで実行できます。ステージング ルータと新しいデバイスは、serial 0/0 や serial 2/0（シリアル ポートがデバイスの第 2 スロットにある場合）など、新しいデバイス上の最初のシリアル インターフェイス ポートを使用して直接接続されている必要があります。

ヒント ステージング ルータから SLARP により自動インストールを使用して設定するルータに割り当てられる IP アドレスは、自動インストールの network-confg または cisconet.cfg ファイルの **ip host** *hostname ip-address* コマンドで使用する必要があります。これは、自動インストールを使用して設定するルータが、ホスト固有のコンフィギュレーション ファイルを要求できるように、正しいホスト名が割り当てられるようにするためです。

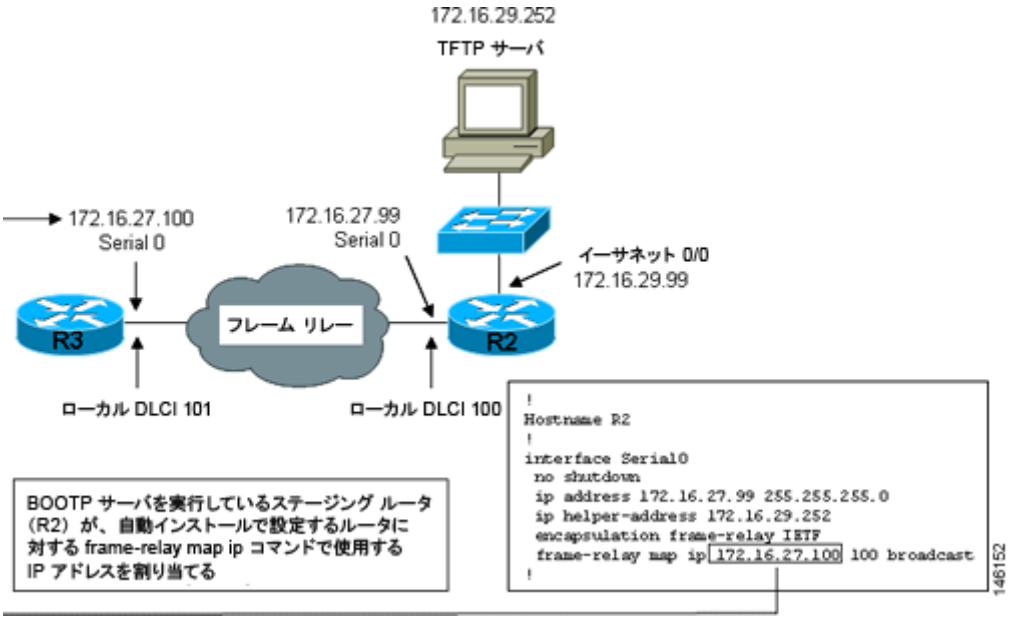
BOOTP サーバ

シリアル インターフェイス経由でフレーム リレー カプセル化を使用して自動インストールで設定するルータは、ステージング ルータに接続されているシリアル インターフェイス上で IP アドレスの BOOTP 要求を送信します。

ステージング ルータは、自動インストールで設定するルータに対する BOOTP 応答で提供すべき正しい IP アドレスを、自動インストールで設定するルータに接続するために使用しているインターフェイス上で設定されている **frame-relay map ip** *ip-address dlci* コマンドを調べることで取得します。

図 2 で、R2 がステージング ルータです。R2 では、インターフェイス serial 0 上で **frame-relay map ip 172.16.27.100 100** ブロードキャスト コマンドが設定されています。R2 が自動インストールプロトコルセル中に R3 から IP アドレスの BOOTP 要求を受信すると、R2 は 172.16.27.100 で応答します。

図 2　　フレーム リレー上の自動インストールで BOOTP を使用する例



ヒント　新しいデバイスとステージング ルータの IP アドレスが .1 または .2 で終わっていなければならないという SLARP での制限は、BOOTP には適用されません。フレーム リレー上の自動インストールのための BOOTP は、自動インストールで設定するルータとステージング ルータの間のフレーム リレー回線に割り当てられた、IP アドレス サブネットに対するすべてのホスト アドレスをサポートします。

ヒント　ステージング ルータから BOOTP により自動インストールを使用して設定するルータに割り当てられる IP アドレスは、自動インストールの network-confg ファイルまたは cisconet.cfg ファイルの **ip host** *hostname ip-address* コマンドで使用する必要があります。これは、自動インストールを使用して設定するルータが、ホスト固有のコンフィギュレーション ファイルを要求できるように、正しいホスト名が割り当てられるようにするためです。

（注）　フレーム リレー カプセル化を使用したシリアル インターフェイス上の自動インストールは、新しいデバイスの最初のシリアル ポート（シリアル インターフェイス 0 またはシリアル インターフェイス x/0）上だけで実行できます。ステージング ルータと新しいデバイスは、serial 0/0 や serial 2/0（シリアル ポートがデバイスの第 2 スロットにある場合）など、新しいデバイス上の最初のシリアル インターフェイス ポートを使用して直接接続されている必要があります。

自動インストールで使用されるサービスとサーバ：IP とホスト名のマッピング

自動インストール プロセス中にネットワーキング デバイスに完全なコンフィギュレーション ファイルをロードするには、そのネットワーキング デバイス用に作成したコンフィギュレーション ファイルを要求できるように、ネットワーキング デバイスがそのホスト名を決定できる必要があります。

自動インストール用に IP アドレスからホスト名へのマッピングをプロビジョニングするためには、次の点に注意してください。

- 自動インストールで設定するネットワーキング デバイスは、そのいずれかの自動インストール ネットワーク コンフィギュレーション ファイル（network-confg または cisconet.cfg）を TFTP サーバからロードすることで、そのホスト名を決定できます。このファイルには、**ip host** *hostname ip-address* コマンドが含まれています。たとえば、ホスト R3 を IP アドレス 198.162.100.3 にマッピングするには、network-confg ファイルまたは cisconet.cfg ファイルに **ip host r3 198.162.100.3** コマンドが含まれている必要があります。
- LAN インターフェイス上で自動インストールを使用して設定するネットワーキング デバイスは、DNS サーバに問い合せることでもそのホスト名を決定できます。DNS サーバが同じ LAN に接続されていない場合、デバイスは、DHCP サーバからダイナミックに割り当てられた IP アドレスを取得するプロセスの中で、DNS サーバの IP アドレスを DHCP サーバから取得する必要があります。

DNS サーバ

DNS サーバは、ホスト名を IP アドレスに、IP アドレスをホスト名に（逆 DNS ルックアップ）マッピングするネットワーク サービスを提供するために使用します。PC がホスト名を使用してホストへの IP 接続を開始するときには、必ず接続先のホスト名に割り当てられている IP アドレスを特定する必要があります。たとえば、シスコの Web サイト（http://www.cisco.com/）を参照すると、PC は DNS サーバに DNS クエリーを送信して、シスコの Web サイトに接続するために使用可能な現在の IP アドレスを知ります。

DNS サービスの詳細については、IETF RFC のサイト（http://www.ietf.org/rfc.html）で DNS に関する RFC を参照してください。ネーム サーバ ルックアップ ツール（nslookup）は、DNS の詳細を知るのに非常に便利です。検索すると、nslookup に関する優れた Web サイトがいくつも見つかります。

自動インストールが使用するサービスとサーバ：コンフィギュレーション ファイルの格納と転送

TFTP は、ネットワーク上のデバイス間でファイルを転送するために使用するプロトコルです。TFTP サーバは、TFTP を使用してデバイスにファイルを転送するデバイスです。TFTP サーバは、UNIX サーバ、Microsoft Windows ベースの PC およびサーバ、その他のプラットフォーム上で設定できます。

ヒント TFTP サーバがない場合は、Cisco IOS ベースのルータを TFTP サーバとして設定できます。そのためには、**tftp-server file-system**:*filename* コマンドを使用します。ルータを TFTP サーバとして設定する方法の詳細については、『*Configuring Basic File Transfer Services*』を参照してください。

シスコのルータは、TFTP を使用して、自動インストールで必要なコンフィギュレーション ファイルをロードします。ファイルの格納と、自動インストールを使用するデバイスへのファイル転送のために、ネットワークに TFTP サーバを配置する必要があります。

TFTP サービスの詳細については、IETF RFC のサイト（http://www.ietf.org/rfc.html）で TFTP に関する RFC を参照してください。検索すると、TFTP に関する優れた Web サイトがいくつも見つかります。インターネットでは、さまざまなオペレーティング システムおよびハードウェア プラットフォーム向けのフリーウェアとシェアウェア版の TFTP サーバがいくつも利用できます。

自動インストール向けに TFTP サーバをプロビジョニングする際には、次の点に注意してください。

- LAN 経由で自動インストールを使用するデバイス：TFTP サーバと自動インストールを使用するデバイスが異なる LAN セグメント上にある場合、自動インストールを使用するデバイスからの TFTP セッション初期化要求を受信するすべてのインターフェイス上で、**ip helper-address** *address* コマンドを設定する必要があります。

- WAN 経由で自動インストールを使用するデバイス：自動インストールを使用するデバイスが WAN に接続されている場合、自動インストールを使用するデバイスからの TFTP セッション初期化要求を受信するすべてのインターフェイス上で、**ip helper-address** *address* コマンドを設定する必要があります。

ip helper-address

新しいデバイスが、TFTP サーバの IP アドレスを、DHCP オプション 150 経由で取得しない場合、TFTP セッション初期化要求を、IP 宛先ブロードキャスト アドレス 255.255.255.255 を使用したネットワーク レイヤ ブロードキャストとして送信します。ルータはネットワーク レイヤ ブロードキャスト データグラムをブロックするため、TFTP セッション開始要求が TFTP サーバに到達せず、自動インストールは失敗します。この問題を解決するには、**ip helper-address** *address* コマンドを使用します。**ip helper-address** *address* コマンドは、TFTP セッション開始要求のブロードキャスト アドレスを、255.255.255.255 から、*address* 引数で設定されるアドレスに変更します。たとえば、**ip helper-address 172.16.29.252** コマンドは、IP 宛先ブロードキャスト アドレス 255.255.255.255 を 172.16.29.252 に変更します。

自動インストールで使用されるネットワーキング デバイス

自動インストールでは次のネットワーキング デバイスが使用されます。

- 「自動インストールで設定するデバイス」（P.9）（必須）
- 「ステージング ルータ」（P.9）（必須）
- 「フレーム リレー /ATM 間スイッチング デバイス」（P.10）（任意）

自動インストールで設定するデバイス

自動インストールで設定するデバイスは、自動インストールをサポートし、NVRAM にコンフィギュレーション ファイルがない、任意の Cisco IOS ベースのルータです。

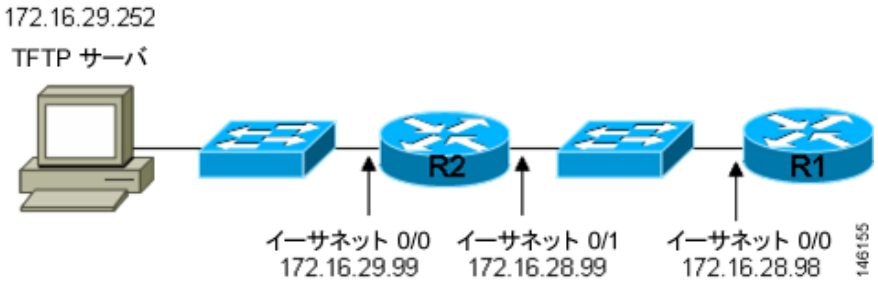
ステージング ルータ

ステージング ルータは、新しいデバイスと TFTP サーバが異なるネットワークに接続されている場合に、TFTP サーバ（IP 接続可能であることが必要です）と、自動インストールで設定されるデバイスの間の仲介役として振る舞います。図 3 で、R1 にはステージング ルータが必要です。これは、R1 が TFTP サーバと異なる LAN セグメントに接続されているためです。

ステージング ルータは、次の状況で必要です。

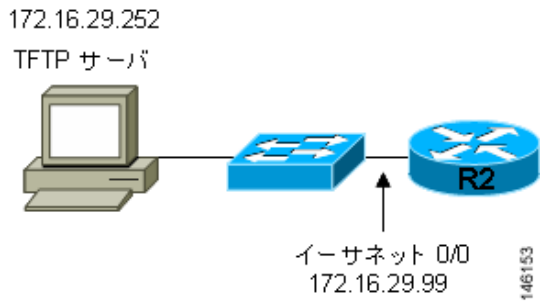
- LAN 経由で自動インストールを使用するデバイス：TFTP サーバと DHCP サーバのいずれかまたは両方と、自動インストールを使用するデバイスが異なる LAN セグメントにある場合は、ステージング ルータを使用する必要があります。
- WAN 上で自動インストールを使用するデバイス：自動インストールを使用するデバイスが WAN に接続されている場合、自動インストールを使用するデバイスからの TFTP セッション初期化要求を受信する、直接接続されたすべてのインターフェイス上で、**ip helper-address** *address* コマンドを設定する必要があります。

図 3　　ステージング ルータが必要な自動インストールの例



自動インストールで設定する新しいデバイスが、TFTP サーバおよび DHCP サーバと同じ LAN セグメントに接続されている場合には、ステージング ルータは不要です。図 4 で、R2 は、TFTP サーバと同じ LAN セグメント上にあるため、自動インストールを使用するためにステージング サーバは必要ありません。

図 4　　ステージング ルータが不要な自動インストールの例



フレーム リレー /ATM 間スイッチング デバイス

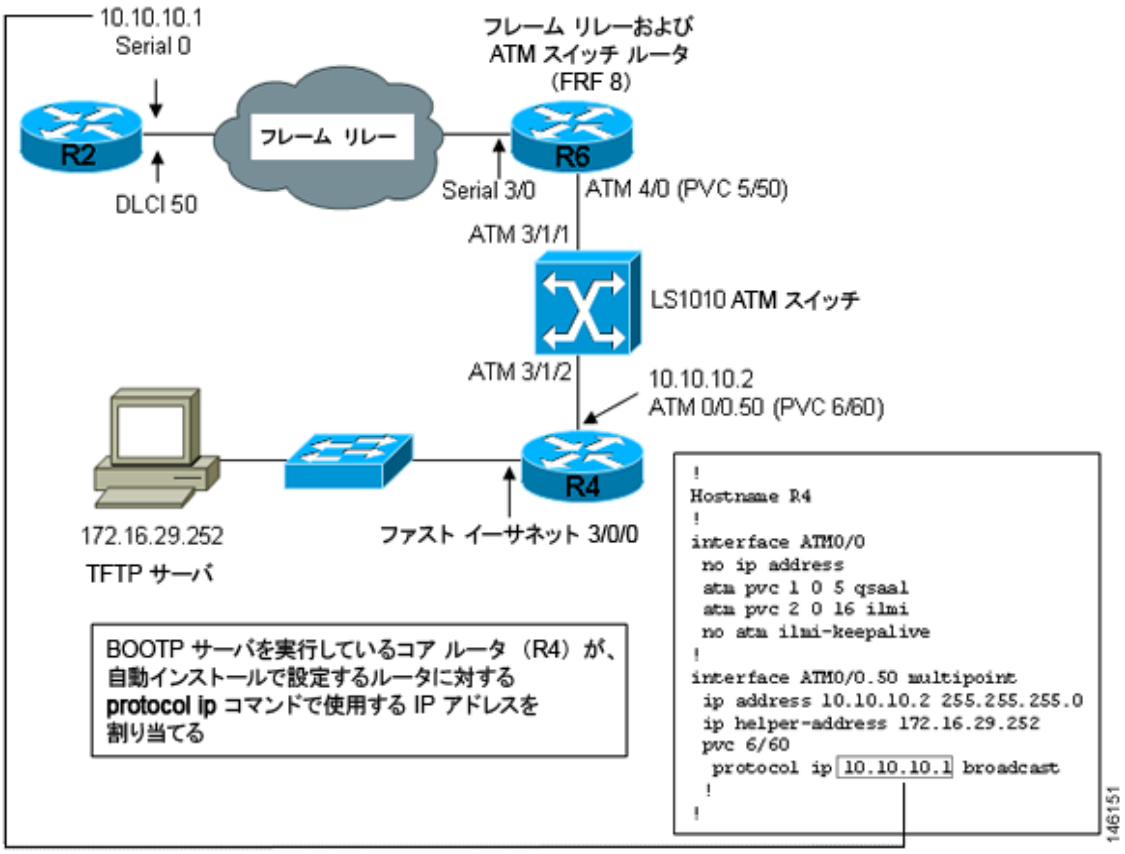
フレーム リレー /ATM 間スイッチング デバイスは、ルーティングとスイッチング動作の両方を実行できるデバイスです。フレーム リレー /ATM 間スイッチング デバイスは、フレーム リレー ネットワークと ATM ネットワークを接続するために使用します。

フレーム リレー /ATM 間インターワーキング接続上の自動インストール機能は、自動インストール プロセスを、シスコが定義したフレーム リレー カプセル化ではなく、IETF 標準で定義されたフレーム リレー カプセル化を使用するように、自動インストール プロセスを変えたものです。

図 5 に、フレーム リレー /ATM 間インターワーキング接続上の自動インストール機能を使用するトポロジ例を示します。ルータ R6 は、フレーム リレー DLCI 50 から ATM VPI/VCI 5/50 への、フレーム リレー /ATM 間サービス インターワーキング（FRF8）変換を行います。LS1010 スイッチは、R6（5/50）が使用する VPI と VCI の組み合わせを、R4（6/60）が使用する VPI と VCI の組み合わせにルーティングします。

自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

図 5　フレーム リレー /ATM 間インターワーキング接続上の自動インストールのトポロジ例



自動インストールで使用するコンフィギュレーション ファイル

コンフィギュレーション ファイルは、事前に定義されたコマンドと設定を実行し、デバイスがネットワーク上で機能できるようにします。選択するコンフィギュレーション ファイルの種類によって、自動インストール用にネットワークを設定する方法の多くの側面が決まります。

自動インストールでは次の種類のファイルが使用されます。

- 「ネットワーク コンフィギュレーション ファイル」（P.11）（必須）
- 「ホスト固有のコンフィギュレーション ファイル」（P.12）（必須）
- 「デフォルト コンフィギュレーション ファイル」（P.12）（任意）

ネットワーク コンフィギュレーション ファイル

ネットワーク コンフィギュレーション ファイルは、自動インストール プロセスが使用を試みる最初のファイルです。デバイスが IP アドレスを取得した後、IP アドレスからホスト名へのマッピングが格納されたネットワーク コンフィギュレーション ファイルをダウンロードすることで、デバイスはホスト名を見つけようとします。

ホスト固有のコンフィギュレーション ファイルをデバイスがダウンロードできるように、network-confg ファイルからホスト名を知るようにするには、ネットワーク コンフィギュレーション ファイル network-confg にデバイスのエントリを追加する必要があります。エントリの構文は、**ip host** *hostname ip-address* です。ここで、*hostname* はホストで使用する名前、*ip-address* はホストが IP

アドレス サーバから受信するアドレスです。たとえば、新しいデバイスで Australia という名前を使用し、新しいデバイスにダイナミックに割り当てられる IP アドレスが 172.16.29.103 である場合、ネットワーク コンフィギュレーション ファイルに **ip host australia 172.16.29.103** コマンドを含むエントリを作成する必要があります。

ネットワーク コンフィギュレーション ファイルのファイル名は、network-confg または cisconet.cfg です。自動インストールを実行するルータは、まず TFTP サーバから network-confg をロードしようとします。TFTP サーバに network-confg がない場合、自動インストール プロセスは cisconet.cfg ファイルをロードしようとします。ファイル名 cisconet.cfg は、8.3 形式のファイル名しかサポートしていない DOS ベースの TFTP サーバで使用されていました。自動インストールは、network-confg のロードがタイムアウトした後で cisconet.cfg ファイルのロードを試みます。これによる遅延を避けるために、ファイル名 network-confg を使用することを推奨します。

自動インストールを使用して複数のデバイスを設定する場合、各デバイス用のエントリが格納された 1 つのネットワーク コンフィギュレーション ファイルを作成できます。

ホスト固有のコンフィギュレーション ファイル

ホスト固有のコンフィギュレーション ファイルは、新しい各デバイス用の完全なコンフィギュレーションです。ホスト固有のファイルを使用することに決めた場合、自動インストールを使用して設定する新しいデバイスごとに、個別のファイルを作成する必要があります。

ホスト固有のコンフィギュレーション ファイルのファイル名は、*name-confg* または *name.cfg* です。ここで、name はルータのホスト名です。たとえば、hqrouter という名前のルータ用のファイル名は、hqrouter-confg または hqrouter.cfg です。

自動インストールを実行するルータは、まず *name-confg* という形式を使用して、TFTP サーバからホスト固有のコンフィギュレーション ファイルをロードしようとします。*name-confg* ファイルが TFTP サーバ上にない場合、自動インストール プロセスは *name.cfg* ファイルのロードを試みます。*name.cfg* というファイル名形式は、以前の 8.3 形式しかサポートしていない DOS ベースの TFTP サーバで使用されます。自動インストールは、*name-confg* のロードがタイムアウトした後で *name.cfg* ファイルのロードを試みます。これによる遅延を避けるために、ファイル名 *name-confg* を使用することを推奨します。

ヒント ホスト固有のコンフィギュレーション ファイルで *name.cfg* 形式を使用する場合、8 文字よりも長いホスト名に対しては、ファイル名を先頭の 8 文字に切り詰める必要があります。たとえば、ホスト名が australia のデバイスに対しては、ファイル名を australi.cfg に切り詰めます。自動インストールは、新しいルータに割り当てられた IP アドレスを、ネットワーク コンフィギュレーション ファイル中のホスト名 australia にマッピングするとき、ホスト固有のファイル名 austrailia-confg のロードに失敗した後で、australi.cfg という名前のホスト固有のコンフィギュレーション ファイルをダウンロードしようとします。

ヒント 新しい各デバイスが適切に設定されるように、ホスト固有のファイル オプションを使用して新しいデバイスを設定することを推奨します。

デフォルト コンフィギュレーション ファイル

最小限のコンフィギュレーション情報が格納されたデフォルト コンフィギュレーション ファイルを使用すると、新しいデバイスに telnet で接続し、手動でデバイスを設定できます。

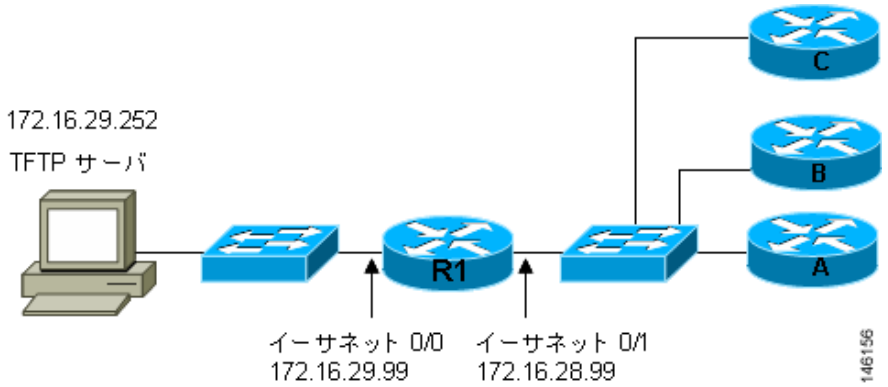
自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

ヒント 新しいデバイスが、ネットワーク コンフィギュレーション ファイルをロードした後でホスト名を取得した場合、デフォルト コンフィギュレーション ファイルは使用されません。リモート CLI セッションのパスワードなどの機能を設定するには、代わりにホスト固有のファイルを使用する必要があります。

図 6 は、デフォルト コンフィギュレーション ファイルを使用して、リモートでの手動設定用に新しいルータを準備する例です。ルータ A、B、および C は、ネットワークに一度に 1 台ずつ追加する新しいルータです。最初のルータを接続し、ルータがデフォルト コンフィギュレーション ファイルをロードするのを待ちます。デフォルト コンフィギュレーション ファイルには、新しいルータが、Telnet セッションを使用してその設定を完了するために使用する PC と通信するために十分な情報が格納されている必要があります。デフォルトのコンフィギュレーション ファイルが新しいルータにロードされたら、Telnet を使用してルータに接続し、その設定を完了します。次のルータを設定するためにデフォルト コンフィギュレーション ファイルを使用できるように、そのインターフェイスに新しい一意の IP アドレスを割り当てる必要があります。

注意 Telnet を使用してリモートで設定しているルータで IP アドレスを変更しないと、次のルータがデフォルト コンフィギュレーション ファイルをロードしたときに LAN 上で IP アドレスが重複します。この状況になると、Telnet を使用してどちらのルータにも接続できなくなります。この問題を解決するには、いずれかのルータを切断する必要があります。

図 6　デフォルト コンフィギュレーション ファイルを使用して、リモートの手動設定用にルータを準備する例



ヒント リモート Telnet アクセスと特権 EXEC モードへのアクセス用のパスワードを設定するためのコマンドを含める必要があります。ルータにリモートでアクセスして設定を完了する場合は、そのコンフィギュレーション ファイルを NVRAM に保存します。

デフォルトのネットワーキング コンフィギュレーション ファイルに対して使用されるファイル名は、router-confg または router.cfg です。自動インストールを実行するルータは、まず TFTP サーバから router-confg をロードしようとします。TFTP サーバに router-confg がない場合、自動インストール プロセスは router.cfg ファイルをロードしようとします。ファイル名 router.cfg は、8.3 形式のファイル名しかサポートしていない DOS ベースの TFTP サーバで使用されていました。自動インストールは、router-confg のロードがタイムアウトした後で router.cfg ファイルのロードを試みます。これによる遅延を避けるために、ファイル名 router-confg を使用することを推奨します。

自動インストールを使用して、LAN に接続されたデバイスを設定する場合、DHCP オプション 067 で、異なるデフォルト ブート ファイル名を指定できます。

自動インストールの設定オプション

デバイスとサービスのいくつかの異なる組み合わせを使用して、自動インストールをサポートするようにネットワークをプロビジョニングできます。次に例を示します。

- 自動インストールで必要なすべてのサービス（シスコのルータで実行する必要がある、SLARP または BOOTP を使用したダイナミックな IP アドレスの割り当てを除く）を、1 台のネットワーク サーバ上にプロビジョニングすることも、各サービスを異なるネットワーク サーバにプロビジョニングすることもできます。
- DHCP サービスは、シスコのルータ上にプロビジョニングできます。
- 自動インストールを使用するデバイスの IP アドレスを DNS サーバから特定するか、**ip host** *hostname ip-address* コマンドを含むいずれかの自動インストールネットワーク コンフィギュレーション ファイル（network-confg または cisconet.cfg）を使用できます。
- 自動インストールを使用するデバイスに、完全なコンフィギュレーションをロードするか部分的なコンフィギュレーションをロードするように自動インストールをプロビジョニングできます。

このモジュールでは、主に自動インストールをプロビジョニングするための最も一般的な方法のいくつかを扱います。自動インストールをプロビジョニングするための最も一般的な方法については、「自動インストールを使用してシスコ ネットワーキング デバイスをリモートで設定する方法」（P.16）を参照してください。

自動インストール プロセス

自動インストール プロセスは、NVRAM にファイルが何もないネットワーキング デバイスをネットワークに接続したときに開始されます。

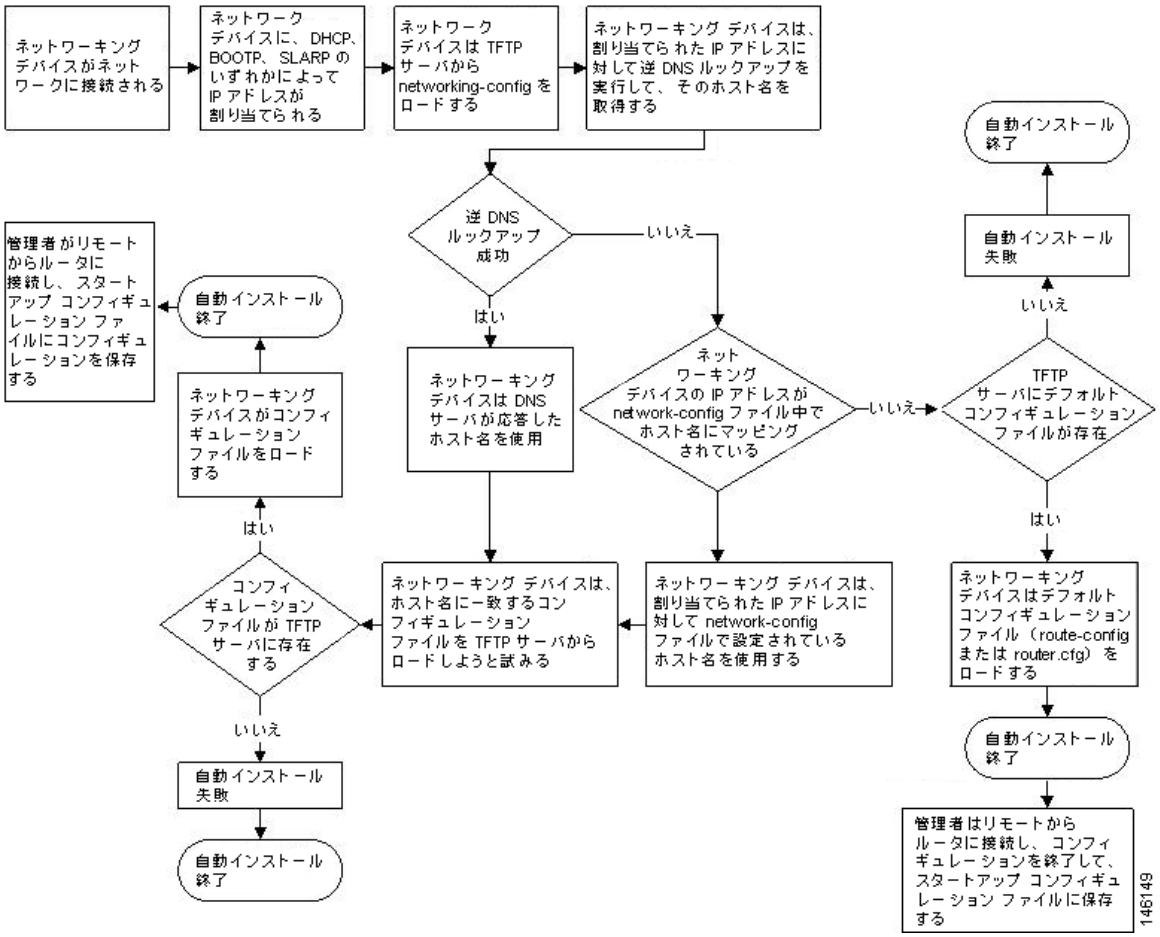
ワンポイント アドバイス

自動インストール プロセスが終了するまでは、ネットワーキング デバイス上の自動インストールで使用するインターフェイスだけを接続することで、自動インストールが完了するまでに要する時間を短縮できます。たとえば、WAN インターフェイス経由でネットワーキング デバイスに対する自動インストールを実行する場合、その LAN インターフェイスと WAN インターフェイスを接続すると、ネットワーキング デバイスは、WAN インターフェイスの使用を試みる前に、LAN インターフェイス上で自動インストールの実行を試みます。自動インストール プロセスが完了するまで LAN インターフェイスを接続しないでおくことで、ネットワーキング デバイスはすぐに WAN インターフェイス上で自動インストール プロセスを開始します。

図 7 に、自動インストール プロセスの基本的な流れを示します。

自動インストールを使用したシスコのネットワーキング デバイスのリモートでの設定

図 7　　自動インストール プロセスのフローチャート



自動インストールを使用してシスコ ネットワーキング デバイスをリモートで設定することの利点

自動インストールを使用することで、中央からルータに対するセットアップ手順を管理できるため、Cisco ルータの配置が容易になります。ルータの物理的な設置を担当する人には、詳しいネットワーキング スキルは不要です。設置者に必要なスキルは、物理的にルータを設定し、電源ケーブルとネットワーキング ケーブルを接続し、電源を投入する能力だけです。コンフィギュレーション ファイルは、中央の TFTP サーバに格納されて管理されます。自動インストールを使用することで、中央のサイトにいる 1 人のネットワーク技術者が、短期間で複数のルータの配置を管理できます。

自動インストールに対して次の 2 つの拡張があります。

- 「LAN インターフェイスに DHCP を使用した自動インストール」
- 「フレーム リレー /ATM 間インターワーキング接続上の自動インストール」

LAN インターフェイスに DHCP を使用した自動インストール

LAN インターフェイスに DHCP を使用した自動インストール機能では、LAN インターフェイス（特にイーサネット、トークンリング、FDDI インターフェイス）上での Cisco IOS 自動インストール用に、Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）の使用を Dynamic Host Configuration Protocol（DHCP）の使用で置き換えることで、自動インストールの利点が強化されます。

DHCP（RFC 2131 で規定）は、BOOTP（RFC 951 で規定）により提供されている機能を拡張したものです。DHCP は、設定情報を TCP/IP ネットワーク上のホストに渡すためのフレームワークを提供します。DHCP では、再利用可能なネットワーク アドレスの自動的な割り当て機能と、追加の設定オプションが追加されています。Cisco IOS Release 12.1(5)T 以降のリリースでは、イーサネット、トークンリング、FDDI インターフェイスの自動インストール プロセスの IP アドレスの獲得フェーズは、DHCP を使用して行われます。このリリースの前までは、LAN インターフェイスの IP アドレスは、自動インストール プロセス中の BOOTP または RARP を使用して獲得されていました。また、この機能では、ユニキャスト TFTP を使用したコンフィギュレーション ファイルのアップロードも可能です。

フレーム リレー /ATM 間インターワーキング接続上の自動インストール

フレーム リレー /ATM 間インターワーキング接続上の自動インストール機能では、ATM インターフェイスを持つルータを、離れた場所で接続する新しいルータに対する BOOTP サーバとして使用できるようにすることで、自動インストールの機能がさらに拡張されます。

自動インストールを使用してシスコ ネットワーキング デバイスをリモートで設定する方法

ここでは、ルータを自動インストール用に準備する方法、フレーム リレー /ATM 間サービス インターワーキングで自動インストールを使用する方法、LAN に接続された新しいルータに対して自動インストールを使用する方法について説明します。フレーム リレー /ATM 間サービス インターワーキングを使用せずに、LAN、HDLC WAN、およびフレーム リレー ネットワークに接続された新しいルータに対して自動インストールを使用する例は、「自動インストールを使用してシスコのネットワーキング デバイスをリモートで設定する例」（P.34）に示します。

ほとんどの場合、自動インストールを実行する新規デバイスが TFTP、BOOTP、および DNS 要求を送信するときに経由するステージング ルータを設定する必要があります。

ヒント いずれの場合にも、自動インストール プロセスが完了した後、ネットワーキング デバイス上でコンフィギュレーションを確認し保存する必要があります。コンフィギュレーションを保存しない場合、プロセス全体を繰り返す必要があります。

- 「SDM デフォルト コンフィギュレーション ファイルのディセーブル化」（P.16）
- 「フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの使用」（P.18）
- 「自動インストールを使用した LAN に接続されているデバイスの設定」（P.30）

SDM デフォルト コンフィギュレーション ファイルのディセーブル化

この作業は、Security Device Manager（SDM）がデバイスにプレインストールされており、代わりに自動インストールを使用してデバイスを設定する場合に実行します。SDM はデバイスに残ります。

手順の概要

1. デバイスのコンソール ポートから、PC のシリアル ポートにコンソール ケーブルを接続します。
2. 電源モジュールをデバイスに接続し、この電源モジュールをコンセントに差し込んで、デバイスの電源をオンにします。
3. 端末エミュレーション プログラムを使用して、デバイスに接続します。
4. **enable**
5. **erase startup-config**
6. **reload**

手順の詳細

ステップ 1 デバイスに付属しているコンソール ケーブルを、デバイスのコンソール ポートから PC のシリアル ケーブルに接続します。手順については、使用しているデバイスのハードウェア インストール ガイドを参照してください。

ステップ 2 電源モジュールをデバイスに接続し、この電源モジュールをコンセントに差し込んで、デバイスの電源をオンにします。手順については、使用しているデバイスのクイック スタート ガイドを参照してください。

ステップ 3 使用している PC の Hyperterminal またはこれに準じた端末エミュレーション プログラムで、次のように端末エミュレーション設定を行い、デバイスに接続します。

- 9600 ボー
- 8 データ ビット、パリティなし、1 ストップ ビット
- フロー制御なし

ステップ 4 **enable**

特権 EXEC モードを開始します。

enable

```
Router> enable
Router#
```

ステップ 5 **erase startup-config**

NVRAM から既存のコンフィギュレーションを消去します。

```
Router# erase startup-config
```

ステップ 6 **reload**

リロード プロセスを開始します。ルータはリロード プロセスの終了後、自動インストール プロセスを開始します。

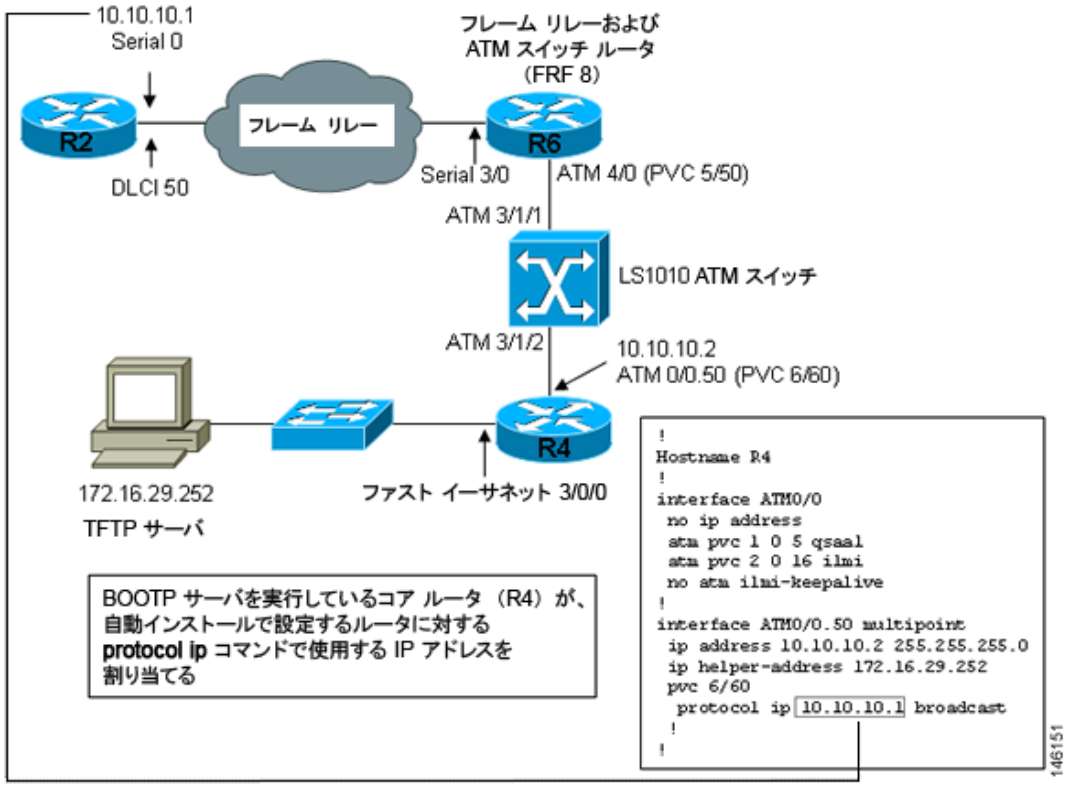
```
Router# reload
```

フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの使用

この作業で使用するネットワーク例については、図 8 を参照してください。フレーム リレー /ATM 間サービス インターワーキング（FRF8）で自動インストールを使用してルータ R2 を設定できるように、ルータ R6、R4、および LS1010 ATM スイッチを設定するには、ここで説明する作業を実行します。

ヒント 自動インストール プロセスの最中とその後に R2 上の Serial 0 に割り当てられる IP アドレス（10.10.10.1/24）と、R4 上の ATM 0/0.50 に割り当てられる IP アドレス（10.10.10.2/24）は、同じサブネット（10.10.10.0/24）上にあります。同じサブネット上の IP アドレスを使用することが必要な理由は、R6 と LS10101 スイッチ上のインターフェイスが、レイヤ 2 で R2 と R4 の間で IP パケットをスイッチングするためです。

図 8　フレーム リレー /ATM 間インターワーキング接続上の自動インストールのトポロジ例



ここでは、次の作業について説明します。

- 「フレーム リレー /ATM 間サービス インターネットワーキングでの R6 の設定」（P.19）
- 「R6 上のフレーム リレー /ATM 間サービス インターワーキングの確認」（P.22）
- 「R4 でのフレーム リレー /ATM 間サービス インターワーキングの設定」（P.22）
- 「IP ルーティング R4 の設定」（P.25）
- 「LS1010 スイッチの設定」（P.26）
- 「フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの確認」（P.27）

フレーム リレー /ATM 間サービス インターネットワーキングでの R6 の設定

ルータ R6 は、フレーム リレー DLCI 50 から ATM VPI/VCI 5/50 への、フレーム リレー /ATM 間サービス インターワーキング（FRF8）変換を行います。

（注） R6 上の、ATM サービス インターワーキング（FRF8）で使用されるシリアル インターフェイスと ATM インターフェイスには IP アドレスがありません。この構成では、これらのインターフェイスがレイヤ 2 スイッチング インターフェイスとして使用されるためです。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **interface serial** *interface-number*
5. **no ip address**
6. **encapsulation frame-relay ietf**
7. **frame-relay interface-dlci** *dlci* **switched**
8. **exit**
9. **frame-relay lmi-type ansi**
10. **frame-relay intf-type dce**
11. **exit**
12. **interface atm** *interface-number*
13. **no ip address**
14. **pvc** *vpi*/*vci* **qsaal**
15. **pvc** *vpi*/*vci* **ilmi**
16. **no atm ilmi-keepalive**
17. **pvc** *vpi*/*vci*
18. **encapsulation aal5mux fr-atm-srv**
19. **exit**
20. **exit**
21. **connect** *name* **serial** *slot*/*port dlci* **atm** *slot*/*port vpi*/*vci* **service-interworking**
22. **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。 • 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：** `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。
ステップ 3	**hostname** *hostname* **例：** `Router(config)# hostname R6`	ホスト（ルータ）の名前を R6 に変更します。
ステップ 4	**interface serial** *interface-number* **例：** `R6(config)# interface serial 3/0`	自動インストールで設定するルータに接続するシリアル インターフェイスを指定し、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。
ステップ 5	**no ip address** **例：** `R6(config-if)# no ip address`	既存の IP アドレスを削除します。 **（注）** このインターフェイスは、この構成でレイヤ 2 スイッチ インターフェイスとして使用されます。IP レイヤ 3 エンドポイントではありません。そのため、IP アドレスは必要ありません。
ステップ 6	**encapsulation frame-relay ietf** **例：** `R6(config-if)# encapsulation frame-relay IETF`	フレーム リレー カプセル化方式をイネーブルにして使用します。 **（注）** この作業では、この作業で必要なフレーム リレー コマンドとキーワードだけを説明しています。他のフレーム リレー コマンドとキーワードの詳細については、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。
ステップ 7	**frame-relay interface-dlci** *dlci* **switched** **例：** `R6(config-if)# frame-relay interface-dlci 50 switched`	フレーム リレー Data-Link Connection Identifier（DLCI; データリンク接続識別子）が切り替えされることを指定し、フレーム リレー DLCI コンフィギュレーション モードを開始します。
ステップ 8	**exit** **例：** `R6(config-fr-dlci)# exit`	フレーム リレー DLCI コンフィギュレーション モードを終了し、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。
ステップ 9	**frame-relay lmi-type ansi** **例：** `Router(config-if)# frame-relay lmi-type ansi`	ルータが、American National Standards Institute（ANSI; 米国規格協会）規格 T1.617 によって定義されている Annex D を LMI タイプとして使用することを指定します。
ステップ 10	**frame-relay intf-type dce** **例：** `R6(config-if)# frame-relay intf-type dce`	ルータが、ルータに接続されたスイッチとして機能することを指定します。

	コマンドまたはアクション	目的
ステップ 11	**exit** **例：** `R6(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**interface atm** *interface-number* **例：** `R6(config)# interface ATM4/0`	ATM インターフェイスを指定し、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。 **（注）** この作業では、この作業で必要な ATM コマンドとキーワードだけを説明しています。他のフレーム リレー コマンドとキーワードの詳細については、『*Cisco IOS Asynchronous Transfer Mode Command Reference*』を参照してください。
ステップ 13	**no ip address** **例：** `R6(config-if)# no ip address`	既存の IP アドレスを削除します。 **（注）** このインターフェイスは、この構成でレイヤ 2 スイッチ インターフェイスとして使用されます。IP レイヤ 3 エンドポイントではありません。そのため、IP アドレスは必要ありません。
ステップ 14	**pvc** *vpi*/*vci* **qsaal** **例：** `R6(config-if)# pvc 0 5 qsaal`	PVC で QSAAL1 シグナリングを設定します。
ステップ 15	**pvc** *vpi*/*vci* **ilmi** **例：** `R6(config-if)# pvc 0 16 ilmi`	PVC で ILMI シグナリングを設定します。
ステップ 16	**no atm ilmi-keepalive** **例：** `R6(config-if)# no atm ilmi-keepalive`	ATM ILMI キープアライブをディセーブルにします。
ステップ 17	**pvc** *vpi*/*vci* **例：** `R6(config-if)# pvc 5/50`	PVC を設定します。PVC を設定するときに、まず使用可能な最も小さい VPI 番号と VCI 番号を設定し、インターフェイス ATM VC コンフィギュレーション モードを開始します。 **（注）** すべての VPI 上の VCI 0 ～ 31 は予約されています。
ステップ 18	**encapsulation aal5mux fr-atm-srv** **例：** `R6(config-if-atm-vc)# encapsulation aal5mux fr-atm-srv`	フレーム リレー /ATM 間インターワーキング サービスをイネーブルにします。
ステップ 19	**exit** **例：** `R6(config-if-atm-vc)# exit`	インターフェイス ATM VC コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 20	**exit** **例：** `R6(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 21	**connect** *name* **serial** *slot*/*port dlci* **atm** *slot*/*port vpi*/*vci* **service-interworking** 例： `R6(config)# connect r2 serial3/0 50 ATM4/0 5/50 service-interworking`	フレーム リレー DLCI と ATM PVC の間に、フレーム リレー /ATM 間インターワーキング サービスのための接続を作成し、FRF .8 コンフィギュレーション モードを開始します。
ステップ 22	**end** 例： `R6(config-frf8)# end`	特権 EXEC モードに戻ります。

R6 上のフレーム リレー /ATM 間サービス インターワーキングの確認

show connection name r2 コマンドを使用して、サービス インターワーキング接続がアップ状態かどうかを確認します。

show connection name r2 コマンドの出力は、サービス インターワーキング接続がアップ状態であることを示しています。

```
R6# show connection name r2

FR/ATM Service Interworking Connection: r2
  Status    - UP
  Segment 1 - Serial3/0 DLCI 50
  Segment 2 - ATM4/0 VPI 5 VCI 50
Interworking Parameters -
    service translation
    efci-bit 0
    de-bit map-clp
    clp-bit map-de
```

R4 でのフレーム リレー /ATM 間サービス インターワーキングの設定

R4 は、この作業におけるフレーム リレー/ATM 間サービス インターワーキングのエンドポイントの 1 つです。他方のエンドポイントは R2 です。R4 は、フレーム リレー ネットワークに直接接続されていません。そのため、R4 では、フレーム リレー /ATM 間サービス インターワーキングのエンドポイントとして動作するための ATM コマンドだけが必要です。

R4 は、TFTP サーバがある LAN に接続するコア ルータです。R4 は、R2 が自動インストールを実行するときに、R2 で必要な IP アドレス（10.10.10.1/24）を提供する BOOTP サーバです。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **interface ethernet** *module/slot/port*
5. **ip address** *ip-address mask*
6. **exit**
7. **interface atm** *interface-number*
8. **no ip address**

9. **pvc** *vpi*/*vci* **qsaal**
10. **pvc** *vpi*/*vci* **ilmi**
11. **no atm ilmi-keepalive**
12. **exit**
13. **interface atm** *slot*/*port*.*subinterface-number* **multipoint**
14. **ip address** *ip-address mask*
15. **ip helper-address** *ip-address*
16. **pvc** *vpi*/*vci*
17. **protocol ip** *ip-address* **broadcast**
18. **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。 • 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： `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。
ステップ 3	**hostname** *hostname* 例： `Router(config)# hostname R4`	ホスト（ルータ）の名前を R4 に変更します。
ステップ 4	**interface ethernet** *module*/*slot*/*port* 例： `R4(config)# interface ethernet 3/0/0`	イーサネット インターフェイスを指定し、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。
ステップ 5	**ip address** *ip-address mask* 例： `R4(config-if)# ip address 172.16.29.97 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 6	**exit** 例： `R4(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface atm** *interface-number* 例： `R4(config)# interface atm0/0`	ATM インターフェイスを指定し、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。 **（注）** この作業では、この作業で必要な ATM コマンドとキーワードだけを説明しています。他のフレーム リレー コマンドとキーワードの詳細については、『*Cisco IOS Asynchronous Transfer Mode Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 8	**no ip address** **例：** `R4(config-if)# no ip address`	メイン ATM インターフェイスには、この構成では IP アドレスは必要ありません。IP アドレスは、ステップ 9 で複数のサブインターフェイスに割り当てられます。
ステップ 9	**pvc** *vpi*/*vci* **qsaal** **例：** `R4(config-if)# pvc 0 5 qsaal`	PVC で QSAAL1 シグナリングを設定します。
ステップ 10	**pvc** *vpi*/*vci* **ilmi** **例：** `R4(config-if)# pvc 0 16 ilmi`	PVC で ILMI シグナリングを設定します。
ステップ 11	**no atm ilmi-keepalive** **例：** `R4(config-if)# no atm ilmi-keepalive`	ATM ILMI キープアライブをディセーブルにします。
ステップ 12	**exit** **例：** `R4(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface atm** *slot*/*port*.*subinterface-number* **multipoint** **例：** `R4(config-if)# interface atm0/0.50 multipoint`	ATM マルチポイント仮想サブインターフェイスを作成し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**ip address** *ip-address mask* **例：** `R4(config-subif)# ip address 10.10.10.2 255.255.255.0`	サブインターフェイスの IP アドレスを指定します。
ステップ 15	**ip helper-address** *ip-address* **例：** `R4(config-subif)# ip helper-address 172.16.29.252`	TFTP サーバの IP アドレスを指定します。この IP アドレスは、R2 が、TFTP サーバとの接続を確立しようとするときに使用する 255.255.255.255 IP 宛先ブロードキャスト アドレスを置き換えるために使用されます。
ステップ 16	**pvc** *vpi*/*vci* **例：** `R4(config-subif)# pvc 6/60`	PVC を設定します。PVC を設定するときに、まず使用可能な最も小さい VPI 番号と VCI 番号を設定し、ATM VC コンフィギュレーション モードを開始します。 **（注）** すべての VPI 上の VCI 0 ～ 31 は予約されています。
ステップ 17	**protocol ip** *ip-address* **broadcast** **例：** `R4(config-if-atm-vc)# protocol ip 10.10.10.1 broadcast`	この PVC の他方の端にあるデバイスの IP アドレスを指定します。この例ではデバイス R2 です。 • この例で、このアドレスは、自動インストール プロセス中に R4 上の BOOTP サーバによって R2 に割り当てられる IP アドレスです。
ステップ 18	**end** **例：** `R4(config-if-atm-vc)# end`	特権 EXEC モードに戻ります。

IP ルーティング R4 の設定

自動インストール プロセスが完了した後、R4 が IP トラフィックをネットワーク 172.16.29.0 の R2 の間で転送できるようにするためには、R4 で IP ルーティングを設定する必要があります。

（注） 「R2 のコンフィギュレーション ファイルの作成：例」（P.36）に示されている R2 用のコンフィギュレーション ファイルには、RIP バージョン 2 を使用して R2 用の IP ルーティング接続を確立するために必要な IP ルーティング コマンドが含まれています。

手順の概要

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** *version*
5. **network** *ip-network*
6. 他の IP ネットワークに対してステップ 5 を繰り返します。
7. **no auto-summary**
8. **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。 • 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： `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。
ステップ 3	**router rip** 例： `Router(config)# router rip`	R4 で RIP ルーティグをイネーブルにします。 （注） この作業では、この作業で必要な RIP コマンドとキーワードだけを説明しています。他の RIP コマンドとキーワードの詳細については、『*Cisco IOS Routing Protocols Command Reference*』を参照してください。
ステップ 4	**version** *version* 例： `Router(config-router)# version 2`	ルータが使用する RIP のバージョンを指定します。
ステップ 5	**network** *ip-network* 例： `Router(config-router)# network 172.16.0.0`	RIP がルーティング サービスを提供する IP ネットワークを指定します。

	コマンドまたはアクション	目的
ステップ 6	他の IP ネットワークに対してステップ 5 を繰り返します。 例： `Router(config-router)# network 10.0.0.0`	—
ステップ 7	**no auto-summary** 例： `Router(config-router)# no auto-summary`	RIP V2 のデフォルトの動作である、ルーティング アドバタイズメントでの IP サブネットの集約をディセーブルにします。
ステップ 8	**end** 例： `Router(config-router)# end`	特権 EXEC モードに戻ります。

LS1010 スイッチの設定

この作業では、R6 と R4 の間で PVC をルーティングするために LS1010 スイッチを設定する方法について説明します。R6 は、LS1010 スイッチ上の ATM 3/1/1 に接続されています。R4 は、LS1010 スイッチ上の ATM 3/1/2 に接続されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *module/slot/port*
4. **pvc** *vpi vci* **interface atm** *interface-number vpi vci*
5. **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。 • 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： `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。
ステップ 3	**interface atm** *module/slot/port* 例： `Router(config)# interface ATM3/1/2`	ATM インターフェイスを指定し、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。 **（注）** この作業では、この作業で必要な LS1010 ATM コマンドとキーワードだけを説明しています。LS1010 で使用可能な他の ATM コマンドとキーワードの詳細については、『*Lightstream 1010 ATM Switch Documents*』を参照してください。

	コマンドまたはアクション	目的
ステップ 4	**pvc** *vpi vci* **interface atm** *interface-number vpi vci* **例：** `Router(config-if)# pvc 6 60 interface ATM3/1/1 5 50`	スタティック PVC ルートを設定します。 • この例では、R6（5/50）から R4（6/60）へのルートを設定しています。
ステップ 5	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの確認

この作業は、図 8 に示す、R2 を設定することによるフレーム リレー /ATM 間サービス インターネットワーキングを使用した自動インストールの設定を確認するために実行します。

前提条件

この作業を実行する前に、次の前提条件を満たしている必要があります。

- ネットワーク上に、R4 上で **ip helper-address** *ip-address* コマンドで指定した IP アドレスを持つ TFTP サーバがあることが必要です。
- TFTP サーバ上に、r2-confg という名前の R2 用のコンフィギュレーション ファイルが必要です。
- TFTP サーバ上に、network-confg という名前のネットワーク コンフィギュレーション ファイルがあり、**ip host r2 10.10.10.1** コマンドが含まれている必要があります。
- この項の以前の作業で説明した手順に従って、R6、R4、および LS1010 ATM スイッチ（または ATM スイッチと機能的に同等のもの）が設定されている必要があります。
- R2 の NVRAM にコンフィギュレーション ファイルがないことが必要です。

手順の概要

ステップ 1 コンソール端末を R2 に接続します。

ステップ 2 R2 の電源をいったんオフにしてオンにするか、電源をオンにします。

ステップ 3 初期設定の入力を求めるダイアログが表示されたら、「no」と答えます。

ステップ 4 自動インストールを終了するかどうかを質問されたら、「no」と答えます。

ステップ 5 自動インストール プロセスは、完了までに数分かかります。自動インストール プロセスが完了するまでは、R2 の端末セッションで何もキーを押さないでください。

ステップ 6 **copy running-configuration startup-configuration** コマンドで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にコピーします。

手順の詳細

ステップ 1 コンソール端末を R2 に接続します。

使用している PC の Hyperterminal またはこれに準じた端末エミュレーション プログラムで、次のように端末エミュレーション設定を行い、デバイスに接続します。

- 9600 ボー
- 8 データ ビット、パリティなし、1 ストップ ビット
- フロー制御なし

ステップ 2 R2 の電源をいったんオフにしてオンにするか、電源をオンにします。

ステップ 3 初期設定の入力を求めるダイアログが表示されたら、「no」と答えます。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

ステップ 4 自動インストールを終了するかどうかを質問されたら、「no」と答えます。

```
Would you like to terminate autoinstall? [yes]: no
```

自動インストールが開始されます。

```
Please Wait. Autoinstall being attempted over Serial0 !!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

ステップ 5 自動インストール プロセスは、完了までに数分かかります。自動インストール プロセスが完了するまでは、R2 の端末セッションで何もキーを押さないでください。

この出力は、自動インストール プロセスが成功した場合の出力です。

（注） エラー メッセージ「%PARSER-4-BADCFG: Unexpected end of configuration file」は無視してかまいません。この問題による自動インストール プロセスへの悪影響はありません。

（注） 最後の 2 行の %SYS-5-CONFIG_I メッセージは、network-confg ファイルと r2-confg ファイルが正常に受信されたことを示します。

```
Press RETURN to get started!

*Mar  1 00:00:11.155: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
*Mar  1 00:00:11.159: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar  1 00:00:11.527: %LINK-3-UPDOWN: Interface Serial1, changed state to down
*Mar  1 00:00:12.271: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,changed
state to up
*Mar  1 00:00:29.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed
state to down
*Mar  1 00:00:32.347: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to up
*Mar  1 00:00:40.355: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to down
*Mar  1 00:00:45.551: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to up
*Mar  1 00:01:58.499: %IP-5-WEBINST_KILL: Terminating DNS process
*Mar  1 00:02:00.035: %LINK-5-CHANGED: Interface Ethernet0, changed state to
administratively down
*Mar  1 00:02:00.039: %LINK-5-CHANGED: Interface Serial1, changed state to
administratively down
*Mar  1 00:02:01.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to down
*Mar  1 00:02:50.635: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(13a), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Tue 26-Apr-05 12:52 by ssearch
*Mar  1 00:02:50.643: %SNMP-5-COLDSTART: SNMP agent on host Router is undergoing
```

```
 a cold start
*Mar  1 00:03:54.759: %PARSER-4-BADCFG: Unexpected end of configuration file.

*Mar  1 00:03:54.763: %SYS-5-CONFIG_I: Configured from tftp://172.16.29.252/network-confg
by console

*Mar  1 00:04:12.747: %SYS-5-CONFIG_I: Configured from tftp://172.16.29.252/r2-confg by
console
```

TFTP サーバでロギングがイネーブルになっている場合、ログに次のテキストのようなメッセージが出力されます。

```
Sent network-confg to (10.10.10.1), 76 bytes
Sent r2-confg to (10.10.10.1),687 bytes
```

ステップ 6 **copy running-config startup-config** コマンドで、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にコピーします。

トラブルシューティング

5 分程度待っても %SYS-5-CONFIG_I メッセージが出力されず、R2 のプロンプトが工場出荷時の Router> のままである場合、自動インストール プロセスは失敗しています。

ステップ 1 TFTP サーバで、ファイルが見つからなかったことを示すエラー メッセージを探します。最もよくある間違いは、テキスト エディタによって拡張子 .txt が r2-confg ファイルに追加されることです（r2-confg.txt）。オペレーティング システムで、TFTP のルート ディレクトリを参照したときに、登録されているファイル タイプの拡張子が非表示になっていることがあります。[Hide file extensions for known file types] オプションをディセーブルにします。

ヒント ファイル名を二重引用符で囲むことで（"filename"）、ほとんどのテキスト エディタでファイル名に拡張子が追加されなくなります。たとえば、ファイルを "r2-confg" として保存することで、r2-confg だけが使用されます。

ステップ 2 作成したコンフィギュレーション ファイルで R2 を設定することで、ネットワークの接続性をテストします。R2 用のコンフィギュレーションを R2 にコピーするには、コンソール端末セッションに貼り付けます。

コンフィギュレーションを R2 にコピーした後、10.10.10.2 に ping を試みます。これが失敗する場合、R2 と R4 の間に問題があります。ケーブル接続、インターフェイスのステータス、ルータ上の設定を確認します。

R2 が 10.10.10.2 に ping できる場合は、R2 から TFTP サーバ（172.16.29.252）への ping を試みます。これが失敗する場合、R4 と TFTP サーバの間のいずれかの場所に設定上の問題があります。ケーブル接続、インターフェイスのステータス、ルータ上の設定を確認します。TFTP サーバ上の IP アドレスと IP デフォルト ゲートウェイを確認します。

ヒント TFTP サーバ上の IP デフォルト ゲートウェイは、172.16.29.97（R4 上のローカル イーサネット インターフェイス）になっている必要があります。

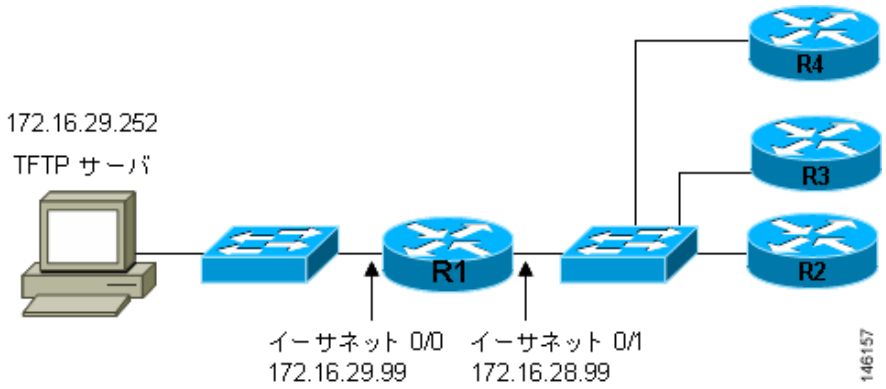
R2 が TFTP サーバ（172.16.29.252）に ping できる場合、TFTP サーバ自体に問題があります。TFTP サーバでよくある間違いは、ファイルの受信はするものの、送信しないように設定されていることです。UNIX ベースの TFTP サーバでよくあるもう 1 つの間違いは、ファイルのアクセス権が正しくないことです。UNIX TFTP サーバでは、ファイルのアクセス権を rw-rw-rw に設定する必要があります。

ステップ 3 IP 接続が機能しており、TFTP サーバが正しく設定されている場合は、R4 上で **ip helper-address** *ip-address* コマンドを正しく入力したことを確認してください。

自動インストールを使用した LAN に接続されているデバイスの設定

自動インストールを使用して LAN に接続されているデバイスを設定するには、図 9 に示すネットワークを使用します。この作業では、自動インストールを使用してルータ R2、R3、および R4 を設定する方法を示します。ルータ R1 は、自動インストール プロセス中に新しいルータ上のイーサネット 0 に IP アドレスを割り当てる DHCP サーバです。

図 9　特定のデバイスに対する自動インストール コンフィギュレーション ファイルを割り当てるためのネットワーク トポロジ



すべての DHCP クライアントには、固有の DHCP クライアント ID があります。DHCP クライアント ID は、DHCP サーバによって、IP アドレスのリースを追跡し、IP アドレスの予約を設定するために使用されます。DHCP IP アドレス予約を設定するためには、自動インストールを使用して設定する各ネットワーキング デバイスの DHCP クライアント ID を知る必要があります。これにより、各デバイスに正しい IP アドレスが提供され、その後固有のコンフィギュレーション ファイルが提供されます。DHCP クライアント ID は手動または自動で特定できます。

自動インストールを使用してルータ R2、R3、および R4 を設定するには、次の作業を実行します。

- 「手動での DHCP クライアント ID の特定」（P.30）
- 「自動的な DHCP クライアント ID の特定」（P.34）

手動での DHCP クライアント ID の特定

クライアント ID の値を自動的に特定する場合は、この作業を実行する必要はありません。「自動的な DHCP クライアント ID の特定：例」（P.37）に進みます。

ヒント 自動インストールを使用して、12.4(1) 以降でない Cisco IOS リリースが動作するネットワーキング デバイスを設定する場合は、DHCP クライアント ID は異なる形式を使用します。この場合、「自動的な DHCP クライアント ID の特定：例」（P.37）で説明する手順を使用します。

クライアント ID を手動で特定するためには、自動インストール プロセス中にルータを LAN に接続するために使用されるイーサネット インターフェイスの MAC アドレスを知っておく必要があります。クライアント ID を手動で特定するには、端末をルータに接続し、その電源をオンにし、**show interface** *interface-type interface-number* コマンドを入力します。

クライアント ID は次のように表示されます。

0063.6973.636f.2d30.3030.362e.3533.6237.2e38.6537.312d.4661.332f.30

形式は nullcisco-0006.53b7.8e71-fa3/0 です。0006.53b7.8e71 は MAC アドレスであり、fa3/0 は IP アドレスを要求するインターフェイスの短いインターフェイス名です。

short-if-name フィールドの値は、Cisco MIB がインストールされた SNMP ワークステーションから取得できます。次に、ifIndex を Cisco IOS 上のインターフェイスにマッピングする例を示します。

```
snmpwalk -c public ponch ifName
IF-MIB::ifName.1 = STRING: AT2/0
IF-MIB::ifName.2 = STRING: Et0/0
IF-MIB::ifName.3 = STRING: Se0/0
IF-MIB::ifName.4 = STRING: BR0/0
```

show interface *interface-type interface-number* コマンドを使用して、ファスト イーサネット インターフェイスの情報と統計情報を表示します。

```
R6> show interface fastethernet 3/0
FastEthernet3/0 is up, line protocol is up
  Hardware is AmdFE, address is 0006.53b7.8e71 (bia 0006.53b7.8e71)
.
.
.
R6>
```

R6 上のファスト イーサネット 3/0 の MAC アドレスは 0006.53b7.8e71 です。このインターフェイスのクライアント ID の形式は nullcisco-0006.53b7.8e71-fa3/0 です。

（注） ファスト イーサネット インターフェイスの短いインターフェイス名は fa です。

表 1 に、文字をその対応する 16 進数に変換するための値を示します。表 2 の最後の行は、R6 上のファスト イーサネット 3/0 のクライアント ID（nullcisco-0006.53b7.8e71-fa3/0）を示します。

表 1　16 進数から文字への変換表

16 進数	文字	16 進数	文字	16 進数	文字	16 進数	文字	16 進数	文字
00	NUL	1a	SUB	34	4	4e	N	68	h
01	SOH	1b	ESC	35	5	4f	O	69	I
02	STX	1c	FS	36	6	50	P	6a	j
03	ETX	1d	GS	37	7	51	Q	6b	k
04	EOT	1e	RS	38	8	52	R	6c	l
05	ENQ	1f	US	39	9	53	S	6d	m

表 1　16 進数から文字への変換表 （続き）

16 進数	文字	16 進数	文字	16 進数	文字	16 進数	文字	16 進数	文字
06	ACK	20		3a	:	54	T	6e	n
07	BEL	21	!	3b	;	55	U	6f	o
08	BS	22	"	3c	<	56	V	70	p
09	TAB	23	#	3d	=	57	W	71	q
0A	LF	24	$	3e	>	58	X	72	r
0B	VT	25	%	3f	?	59	Y	73	s
0C	FF	26	&	40	@	5a	Z	74	t
0D	CR	27	'	41	A	5b	[	75	u
0E	SO	28	(	42	B	5c	\	76	v
0F	SI	29	)	43	C	5d	]	77	w
10	DLE	2a	*	44	D	5e	^	78	x
11	DC1	2b	+	45	E	5f	_	79	y
12	DC2	2c	,	46	F	60	`	7a	z
13	DC3	2d	-	47	G	61	a	7b	{
14	DC4	2e	.	48	H	62	b	7c	|
15	NAK	2f	/	49	I	63	c	7D	}
16	SYN	30	0	4a	J	64	d	7e	~
17	ETB	31	1	4b	K	65	e	7f	D
18	CAN	32	2	4c	L	66	f		
19	EM	33	3	4d	M	67	g		

表 2　nullcisco-0006.53b7.8e71-fa3/0 からクライアント ID への変換

00	c	i	s	c	o	-	0	0	0	6	.	5	3	b	7	.	8	e	7	1	-	f	a	3	/	0
00	63	69	73	63	6f	2d	30	30	30	36	2e	35	33	62	37	2e	38	65	37	31	2d	46	61	33	2f	30

R4

show interface *interface-type interface-number* コマンドを使用して、R4 上のイーサネット 0 の情報と統計情報を表示します。

```
R4> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb0e (bia 00e0.1eb8.eb0e)
```

R4 上のイーサネット 0 の MAC アドレスは 00e0.1eb8.eb0e です。このインターフェイスのクライアント ID の形式は nullcisco-00e0.1eb8.eb0e-et0 です。

（注）　イーサネット インターフェイスの短いインターフェイス名は et です。

表 1 の、文字を対応する 16 進数に変換するための値を使用した、R4 上のイーサネット 0 のクライアント ID を、表 3 の最後の行に示します。

表 3　　null.cisco-00e0.1eb8.eb0e-et0 から R4 のクライアント ID への変換

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	e	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	65	2d	45	74	30

R3

show interface *interface-type interface-number* コマンドを使用して、R3 上のイーサネット 0 の情報と統計情報を表示します。

```
R3> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb73 (bia 00e0.1eb8.eb73)
```

R3 上のイーサネット 0 の MAC アドレスは 00e0.1eb8.eb73 です。このインターフェイスのクライアント ID の形式は nullcisco-00e0.1eb8.eb73-et0 です。

表 1 の、文字を対応する 16 進数に変換するための値を使用した、R3 上のイーサネット 0 のクライアント ID を、表 4 の最後の行に示します。

表 4　　null.cisco-00e0.1eb8.eb73-et0 から R3 のクライアント ID への変換

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	7	3	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	37	33	2d	45	74	30

R2

show interface *interface-type interface-number* コマンドを使用して、R2 上のイーサネット 0 の情報と統計情報を表示します。

```
R2> show interface ethernet 0
Ethernet0 is up, line protocol is up
  Hardware is Lance, address is 00e0.1eb8.eb09 (bia 00e0.1eb8.eb09)
```

R2 上のイーサネット 0 の MAC アドレスは 00e0.1eb8.eb09 です。このインターフェイスのクライアント ID の形式は nullcisco-00e0.1eb8.eb09-et0 です。

表 1 の、文字を対応する 16 進数に変換するための値を使用した、R2 上のイーサネット 0 のクライアント ID を、表 5 の最後の行に示します。

表 5　　null.cisco-00e0.1eb8.eb09-et0 から R2 のクライアント ID への変換

00	c	i	s	c	o	-	0	0	e	0	.	1	e	b	8	.	e	b	0	9	-	e	t	0
00	63	69	73	63	6f	2d	30	30	65	30	2e	31	65	62	38	2e	65	62	30	39	2d	45	74	30

これで各ルータのクライアント ID の値が特定できました。最後の手順は、次に示すように、左から右に 4 文字ずつのグループにし、その後にピリオドを追加することです。

- R4–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

この次の手順

値をテキスト ファイルに保存し、「各ルータ用のプライベート DHCP プールの作成：例」（P.40）に進みます。

自動的な DHCP クライアント ID の特定

クライアント ID の値を手動で特定する場合は、この作業を実行する必要はありません。「各ルータ用のプライベート DHCP プールの作成：例」（P.40）に進みます。

この作業では、R1 上に、1 つの IP アドレスだけを提供する DHCP サーバを構築します。この IP アドレスは、ルータのクライアント ID の値を特定する間、新しい各ルータによって順番に使用されます。IP アドレスの範囲を単一の IP アドレスに制限することで、どのルータを操作しているかに関する混乱を避けることができます。誰かが別のルータの電源をオンにし、自動インストール プロセスが開始されると、そのルータは IP アドレスを取得できません。

ヒント network-confg またはルータ コンフィギュレーション ファイル（r4-confg、r3-confg、または r2-confg）は、まだ TFTP サーバのルート ディレクトリに格納しないでください。ルータが正しいコンフィギュレーション ファイルをロードするように、各ルータが DHCP サーバから正しい IP アドレスを取得することを確認するまでは、これらのファイルをルータがロードしないようにします。

この作業はいくつかの作業にわかれています。詳細については、「手動での DHCP クライアント ID の特定」（P.30）の項を参照してください。

自動インストールを使用してシスコのネットワーキング デバイスをリモートで設定する例

ここでは、次の設定例について説明します。

- 「フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの使用：例」（P.34）
- 「自動インストールを使用した LAN に接続されているデバイスの設定：例」（P.37）
- 「自動インストールを使用した WAN に接続されているデバイスの設定：例」（P.45）

フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの使用：例

次に、フレーム リレー /ATM 間サービス インターネットワーキングで自動インストールを設定する例を示します。

- 「フレーム リレー /ATM 間サービス インターネットワーキングのための R6 の設定：例」（P.35）
- 「フレーム リレー /ATM 間サービス インターネットワーキングのための R4 の設定：例」（P.35）
- 「フレーム リレー /ATM 間サービス インターネットワーキングのための R4 の設定：例」（P.35）
- 「LS1010 スイッチの設定：例」（P.36）
- 「R2 のコンフィギュレーション ファイルの作成：例」（P.36）

フレーム リレー /ATM 間サービス インターネットワーキングのための R6 の設定：例

次に、フレーム リレー /ATM 間サービス インターネットワーキング（FRF8）のために R6 を設定する例を示します。

```
!
hostname R6
!
interface Serial3/0
 no ip address
 encapsulation frame-relay IETF
 frame-relay interface-dlci 50 switched
 frame-relay lmi-type ansi
 frame-relay intf-type dce
!
interface ATM4/0
 pvc 0 5 qsaal
 pvc 0 16 ilmi
 no atm ilmi-keepalive
 pvc 5/50
  encapsulation aal5mux fr-atm-srv
!
connect r2 serial3/0 50 atm4/0 5/50 service-interworking
!
```

フレーム リレー /ATM 間サービス インターネットワーキングのための R4 の設定：例

次の例では、R4 を、フレーム リレー /ATM 間サービス インターネットワーキング（FRF8）を使用した自動インストールのためのコア ルータとして設定します。

```
!
hostname R4
!
interface FastEthernet3/0/0
 ip address 172.16.29.97 255.255.255.0
!
interface ATM0/0
 no ip address
 pvc 0 5 qsaal
 pvc 0 16 ilmi
 no atm ilmi-keepalive
!
interface ATM0/0.50 multipoint
 ip address 10.10.10.2 255.255.255.0
 ip helper-address 172.16.29.252
 pvc 6/60
  protocol ip 10.10.10.1 broadcast
 !
!
```

フレーム リレー /ATM 間サービス インターネットワーキングのための R4 の設定：例

次に、R4 上で IP ルーティングを設定する例を示します。

```
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
!
```

LS1010 スイッチの設定：例

次に、R6 と R4 の間で PVC をルーティングするために LS1010 ATM スイッチを設定する例を示します。

```
!
atm address 47.0091.8100.0000.0010.11b9.6101.0010.11b9.6101.00
atm router pnni
 no aesa embedded-number left-justified
 node 1 level 56 lowest
  redistribute atm-static
!
interface ATM2/0/0
 no ip address
 no ip directed-broadcast
 atm maxvp-number 0
!
interface ATM3/1/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
interface ATM3/1/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
interface ATM3/1/2
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 pvc 6 60 interface ATM3/1/1 5 50
!
interface ATM3/1/3
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
!
```

R2 のコンフィギュレーション ファイルの作成：例

ここでは、R2 のコンフィギュレーション ファイルの内容について説明します。

手順の概要

1. 提供された情報を使用して R2 のコンフィギュレーション ファイルを作成します。
2. コンフィギュレーション ファイルを、TFTP サーバに r2-confg という名前で格納します。

手順の詳細

ステップ 1 R2 用に次のコンフィギュレーション ファイルを作成します。

```
!
hostname R2
!
!
enable secret 7gD2A0
!
interface Ethernet0
 no ip address
 shutdown
```

```
!
interface Serial0
 ip address 10.10.10.1 255.255.255.0
 encapsulation frame-relay IETF
 frame-relay map ip 10.10.10.2 50 broadcast
 frame-relay interface-dlci 50
 frame-relay lmi-type ansi
!
interface Serial1
 no ip address
 shutdown
!
!
router rip
 version 2
 network 10.0.0.0
 no auto-summary
!
ip http server
ip classless
!
line vty 0 4
 password 87F3c0m
 login
!
end
```

ステップ 2　コンフィギュレーション ファイルを、TFTP サーバに r2-confg という名前で格納します。

```
Router# copy running-config tftp:
Address or name of remote host []? 192.0.2.1
Destination filename [running-config]? r2-config
!!!
1030 bytes copied in 9.612 secs (107 bytes/sec)
Router#
```

自動インストールを使用した LAN に接続されているデバイスの設定：例

次に、自動インストールを使用して LAN に接続されたデバイスを設定する例を示します。

- 「自動的な DHCP クライアント ID の特定：例」（P.37）
- 「各ルータ用のプライベート DHCP プールの作成：例」（P.40）
- 「各ルータ用のコンフィギュレーション ファイルの作成：例」（P.41）
- 「ネットワーク コンフィギュレーション ファイルの作成：例」（P.42）
- 「自動インストールを使用したルータの設定：例」（P.42）
- 「ルータ上でのコンフィギュレーション ファイルの保存：例」（P.44）
- 「R1 からのプライベート DHCP アドレス プールの削除：例」（P.45）

自動的な DHCP クライアント ID の特定：例

次に、DHCP クライアント ID の値を自動的に特定する例を示します。

- 「R1 上のインターフェイスの IP の設定：例」（P.38）
- 「R1 上の DHCP プールの設定：例」（P.38）
- 「R1 上の DHCP プールから 1 つを除くすべての IP アドレスを除外する：例」（P.38）

R1 上のインターフェイスの IP の設定：例

次に、Ethernet0/1 上で **ip helper-address** *ip-address* コマンドを設定する例を示します。

```
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
 ip helper-address 172.16.29.252
!
```

R1 上の DHCP プールの設定：例

次に、R1 上で一時的な DHCP サーバを設定するためにコマンドを設定する例を示します。

（注） R1 上では DHCP サーバを 1 つだけ動作させることが必要です。このサーバは、自動インストールを使用して設定するルータがアクセスできる唯一の DHCP サーバであることが必要です。

```
!
ip dhcp pool get-client-id
   network 172.16.28.0 255.255.255.0
!
```

R1 上の DHCP プールから 1 つを除くすべての IP アドレスを除外する：例

次に、**ip dhcp excluded-address** コマンドを使用して、172.16.28.1 以外のすべての IP アドレスを DHCP プールから除外する例を示します。

（注） DHCP サーバからは常に 1 つの IP アドレスだけが利用できるようにする必要があります。

```
!
ip dhcp excluded-address 172.16.28.2 172.16.28.255
!
```

R1 の設定の確認：例

次に、R1 の設定を確認する例を示します。

R1 用のコンフィギュレーション ファイルに、1 つの IP アドレス（172.16.28.1）を DHCP クライアントに提供する、DHCP サーバ プールが設定されていることを確認します。

コンフィギュレーション ファイルに、イーサネット インターフェイスの IP アドレスと **ip helper-address** *ip-address* コマンドが含まれていることを確認します。

```
!
ip dhcp excluded-address 172.16.28.2 172.16.28.255
!
```

```
ip dhcp pool get-client-id
   network 172.16.28.0 255.255.255.0
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
 ip helper-address 172.16.29.252
!
```

R1 上での debug ip dhcp server events のイネーブル化：例

次に、R1 上で **debug ip dhcp server events** コマンドをイネーブルにする例を示します。

R1 に接続された端末上で **debug ip dhcp server events** コマンドからの出力を使用し、各ルータのクライアント ID を特定します。

```
R1# debug ip dhcp server events
```

各ルータでのクライアント ID の値の特定：例

次に、各ルータのクライアント ID の値を特定する例を示します。

次の手順は、各ルータで繰り返します。一度に 1 台のルータの電源だけをオンにする必要があります。ルータのクライアント ID フィールドの値を特定したら、そのルータの電源をオフにし、次のルータに進みます。

R4

R4 をイーサネット ネットワークに接続し、電源をオンにします。R4 に IP アドレス 172.16.28.1 が割り当てられると、R1 に接続された端末に次のメッセージが表示されます。

```
DHCPD: assigned IP address 172.16.28.1 to client
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30.
```

クライアント ID 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30 をテキスト ファイルにコピーして保存します。テキスト ファイルは、次の 2 台のルータ用に開いたままにします。

R4 の電源をオフにします。

R1 上で **clear ip dhcp binding *** コマンドを使用し、R1 上の DHCP バインディングから R4 の IP アドレス バインディングを解放します。

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

R3

R3 をイーサネット ネットワークに接続し、電源をオンにします。R3 に IP アドレス 172.16.28.1 が割り当てられると、R1 に接続された端末に次のメッセージが表示されます。

```
DHCPD: assigned IP address 172.16.28.1 to client
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30.
```

クライアント ID 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30 をテキスト ファイルにコピーして保存します。テキスト ファイルは、最後のルータ用に開いたままにします。

R3 の電源をオフにします。

R1 上で **clear ip dhcp binding *** コマンドを使用し、R1 上の DHCP バインディングから R3 の IP アドレス バインディングを解放します。

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

R2

R2 をイーサネット ネットワークに接続し、電源をオンにします。R2 に IP アドレス 172.16.28.1 が割り当てられると、R1 に接続された端末に次のメッセージが表示されます。

```
DHCPD: assigned IP address 172.16.28.1 to client
0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30.
```

クライアント ID 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30 をテキスト ファイルにコピーして保存します。

R2 の電源をオフにします。

R1 上で **clear ip dhcp binding *** コマンドを使用し、R1 上の DHCP バインディングから R2 の IP アドレス バインディングを解放します。

```
R1# clear ip dhcp binding *
R1#
01:16:11: DHCPD: returned 172.16.28.1 to address pool get-client-id.
```

R4、R3、および R2 のクライアント ID

これで各ルータのクライアント ID の値が特定できました。

- R4–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30
- R3–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
- R2–0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30

ネットワーク 172.16.28.0/24 用の R1 上の DHCP プールの削除：例

次に、ルータ上の不要になった一時的な DHCP プールを削除する例を示します。

```
R1(config)# no ip dhcp pool get-client-id
```

R1 からの除外されたアドレス範囲の削除：例

次に、ルータ上の DHCP プールから、172.16.28.1 以外のすべての IP アドレスを除外するためのコマンドを削除する例を示します。

```
R1(config)# no ip dhcp excluded-address 172.16.28.2 172.16.28.255
```

各ルータ用のプライベート DHCP プールの作成：例

次に、各ルータに、ネットワーク コンフィギュレーション ファイル中でそのホスト名にマッピングされる IP アドレスが割り当てられるように、各ルータ用のプライベート DHCP アドレス プールを作成する例を示します。

```
!
ip dhcp pool r4
   host 172.16.28.100 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.652d.4574.30

!
ip dhcp pool r3
   host 172.16.28.101 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6237.332d.4574.30
```

```
!
ip dhcp pool r2
   host 172.16.28.102 255.255.255.0
   client-identifier 0063.6973.636f.2d30.3065.302e.3165.6238.2e65.6230.392d.4574.30
```

各ルータ用のコンフィギュレーション ファイルの作成：例

次に、各ルータ用のコンフィギュレーション ファイルを作成し、TFTP サーバのルート ディレクトリに格納する例を示します。

ヒント ルータにリモートからアクセスしてそのコンフィギュレーション ファイルを NVRAM に保存する場合は、リモート Telnet アクセスと特権 EXEC モードへのアクセス用のパスワードを設定するためのコマンドを含める必要があります。

r2-confg

```
!
hostname R2
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.102 255.255.255.0
!
interface Serial0
 ip address 192.168.100.1 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.5 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

r3-confg

```
!
hostname R3
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.13 255.255.255.252
```

```
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

r4-confg

```
!
hostname R3
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.101 255.255.255.0
!
interface Serial0
 ip address 192.168.100.9 255.255.255.252
 no shutdown
!
interface Serial1
 ip address 192.168.100.13 255.255.255.252
 no shutdown
!
no ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
line vty 0 4
 password 5Rf1k9
 login
!
end
```

ネットワーク コンフィギュレーション ファイルの作成：例

次に、**ip host** *hostname ip-address* コマンドを含むネットワーク コンフィギュレーション ファイルを作成する例を示します。このコマンドは、DHCP サーバで割り当てる IP アドレスをホスト名にマッピングします。

```
ip host r4 172.16.28.100
ip host r3 172.16.28.101
ip host r2 172.16.28.102
```

自動インストールを使用したルータの設定：例

次に、自動インストールを使用して 3 台のルータ（R4、R3、および R2）を設定する例を示します。

自動インストールの進行状況を監視するには、ルータに端末を接続します。使用している PC の Hyperterminal またはこれに準じた端末エミュレーション プログラムで、次のように端末エミュレーション設定を行い、デバイスに接続します。

- 9600 ボー
- 8 データ ビット、パリティなし、1 ストップ ビット
- フロー制御なし

TFTP サーバのルート ディレクトリに次のファイルを格納しておきます。

- network-confg
- r4-confg
- r3-confg
- r2-confg

TFTP サーバが動作している必要があります。

各ルータの電源をオンにします。

ワンポイント アドバイス 3 台のルータを同時に設定できます。

R4

次に示すのは、自動インストール プロセス中に R4 のコンソール端末に表示されるメッセージの一部です。

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.100 to r4
Loading r4-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

R3

次に示すのは、自動インストール プロセス中に R3 のコンソール端末に表示されるメッセージの一部です。

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.101 to r3
Loading r3-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

R2

次に示すのは、自動インストール プロセス中に R2 のコンソール端末に表示されるメッセージの一部です。

```
Loading network-confg from 172.16.29.252 (via Ethernet0): !
[OK - 76 bytes]
Configuration mapped ip address 172.16.28.102 to r2
Loading r2-confg from 172.16.29.252 (via Ethernet0): !
[OK - 687 bytes]
```

TFTP サーバ ログ

TFTP サーバ ログには、次のようなメッセージが出力されます。

```
Sent network-confg to (172.16.28.100), 76 bytes
Sent r4-confg to (172.16.28.100),687 bytes
Sent network-confg to (172.16.28.101), 76 bytes
Sent r3-confg to (172.16.28.101),687 bytes
Sent network-confg to (172.16.28.102), 76 bytes
Sent r2-confg to (172.16.28.102),687 bytes
```

ルータ上でのコンフィギュレーション ファイルの保存：例

次に、各ルータ上の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に保存し、電源を再投入してもコンフィギュレーションが保持されるようにします。

R4

```
R1# telnet 172.16.28.100
Trying 172.16.28.100 ... Open


User Access Verification

Password:
R4> enable
Password:

R4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit

[Connection to 172.16.28.100 closed by foreign host]
R1#
```

R3

```
R1# telnet 172.16.28.101
Trying 172.16.28.101 ... Open


User Access Verification

Password:
R3> enable
Password:

R3# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3# exit

[Connection to 172.16.28.101 closed by foreign host]
R1#
```

R2

```
R1# telnet 172.16.28.102
Trying 172.16.28.102 ... Open


User Access Verification

Password:
R2> enable
Password:

R2# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
R2# exit

[Connection to 172.16.28.102 closed by foreign host]
R1#
```

R1 からのプライベート DHCP アドレス プールの削除：例

次に、R1 からプライベート DHCP アドレス プールを削除する例を示します。

```
R1(config)# no ip dhcp pool r4
R1(config)# no ip dhcp pool r3
R1(config)# no ip dhcp pool r2
```

この作業は、自動インストールを使用して LAN に接続されたデバイスを設定するための最後の手順です。

自動インストールを使用した WAN に接続されているデバイスの設定：例

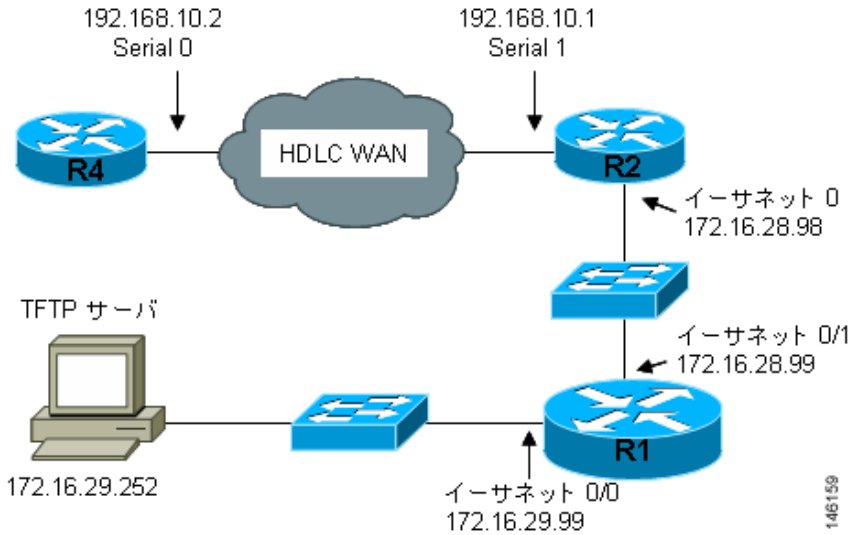
次に、自動インストールを使用して WAN に接続されたデバイスを設定する例を示します。

- 「HDLC WAN 接続：例」（P.45）
- 「フレーム リレー WAN 接続：例」（P.48）

HDLC WAN 接続：例

次に示す例では、図 10 のネットワークを使用しています。この例では、自動インストールを使用して R4 を設定します。R2 は、SLARP を使用して R4 に自動インストールで必要な IP アドレス（192.168.20.2）を提供します。

図 10　自動インストールを使用して HDLC WAN に接続されたルータを設定するためのネットワーク トポロジ



次に、自動インストールを使用してルータ R2 を設定する例を示します。

- 「R4 のコンフィギュレーションの作成：例」（P.46）

R4 のコンフィギュレーションの作成：例

次に、R4 用のコンフィギュレーション ファイルを作成し、TFTP サーバに r4-confg という名前で保存する例を示します。

```
!
hostname R4
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 10.89.45.1 255.255.255.0
 no shutdown
!
interface Serial0
 ip address 192.168.10.2 255.255.255.0
 no fair-queue
!
router rip
 version 2
 network 168.192.0.0
 no auto-summary
!
ip http server
ip classless
ip default-network 0.0.0.0
ip route 0.0.0.0 0.0.0.0 Serial0
!
line vty 0 4
password 6T2daX9
!
end
```

ネットワーク コンフィギュレーション ファイルの作成：例

次に、R4 用のネットワーク コンフィギュレーション ファイルを作成し、TFTP サーバに network-confg という名前で保存する例を示します。

```
ip host r4 192.168.10.2
```

R1 と R2 の設定：例

次に、次の設定を使用して R1 と R2 を設定する例を示します。

R1

```
!
hostname R1
!
enable secret 7gD2A0
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
```

```
 ip address 172.16.28.99 255.255.255.0
!
interface Serial2
 ip helper-address 172.16.29.252
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
ip classless
ip http server
!
line vty 0 4
 password 67F2SaB
!
end
```

R2

```
!
hostname R2
!
enable secret 7gD2A0
!
interface Ethernet0
 ip address 172.16.28.98 255.255.255.0
!
interface Serial1
 ip address 192.168.10.1 255.255.255.0
 clockrate 64000
!
router rip
 version 2
 network 172.16.0.0
 network 192.168.10.0
 no auto-summary
!
ip http server
ip classless
!
line vty 0 4
 password u58Hg1
!
end
```

自動インストールを使用した R4 の設定：例

次に、自動インストールを使用して R4 を設定する例を示します。

R4 を HDLC WAN ネットワークに接続します。

R4 の電源をオンにします。

自動インストール プロセスは約 5 分以内に完了します。

TFTP サーバ ログ

TFTP サーバ ログには、次のようなメッセージが出力されます。

```
Sent network-confg to (192.168.10.2), 76 bytes
Sent r4-confg to (192.168.10.2),687 bytes
```

R4 上でのコンフィギュレーション ファイルの保存：例

次に、R4 上で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に保存し、R4 の電源を再投入してもコンフィギュレーションが保持されるようにする例を示します。

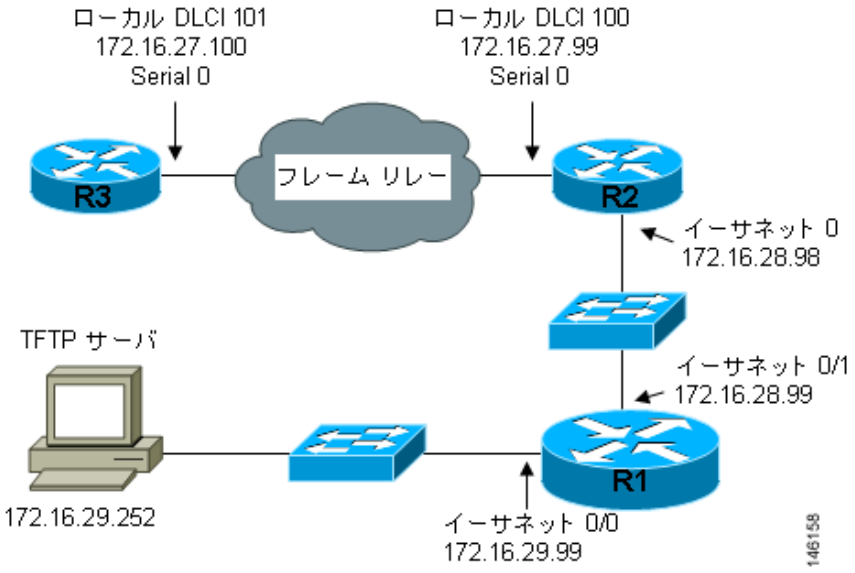
```
R1# telnet 192.168.10.2
Trying 192.168.10.2 ... Open

User Access Verification

Password:
R4> enable
Password:

R4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit

[Connection to 192.168.10.2 closed by foreign host]
R1#
```

フレーム リレー WAN 接続：例

この例では、図 11 に示すネットワークを使用しています。この例では、自動インストールを使用して R4 を設定します。

R2 は、BOOTP を使用して R4 に自動インストールで必要な IP アドレス（172.16.27.100）を提供します。R2 は、BOOTP を使用して R3 に提供する IP アドレスとして 172.16.27.100 を使用します。これは、この IP アドレスが、R3 上の serial 0 を指す、serial 0 上の **frame-relay map ip 172.16.27.100 100 broadcast** コマンド中の IP アドレスであるためです。

図 11　自動インストールを使用してフレーム リレー WAN に接続されたルータを設定するためのネットワーク トポロジ



次に、自動インストールを使用してルータ R3 を設定する例を示します。

R3 のコンフィギュレーションの作成：例

次に、R4 用のコンフィギュレーション ファイルを作成し、TFTP サーバに r3-confg という名前で保存する例を示します。

```
!
hostname R3
!
enable secret 8Hg5Zc20
!
interface Ethernet0
 no ip address
 shutdown
!
interface Serial0
 ip address 172.16.27.100 255.255.255.0
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay map ip 172.16.27.99 101 broadcast
 frame-relay interface-dlci 101
!
interface Serial1
 no ip address
 shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 67Td3a
 login
!
end
```

ネットワーク コンフィギュレーション ファイルの作成：例

次に、R3 用のネットワーク コンフィギュレーション ファイルを作成し、TFTP サーバに network-confg という名前で保存する例を示します。

```
ip host r3 172.16.27.100
```

R1 と R2 の設定：例

次に、次の設定を使用して R1 と R2 を設定する例を示します。

R1

```
!
hostname R1
!
```

```
enable secret 86vC7Z
!
interface Ethernet0/0
 ip address 172.16.29.99 255.255.255.0
!
interface Ethernet0/1
 ip address 172.16.28.99 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 6Gu8z0s
!
!
end
```

R2

```
!
hostname R2
!
enable secret 67Hfc5z2
!
interface Ethernet0
 ip address 172.16.28.98 255.255.255.0
 ip helper-address 172.16.29.252
!
interface Serial0
 ip address 172.16.27.99 255.255.255.0
 ip helper-address 172.16.29.252
 encapsulation frame-relay IETF
 no fair-queue
 frame-relay map ip 172.16.27.100 100 broadcast
 frame-relay interface-dlci 100
!
interface Serial1
 no ip address
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
line vty 0 4
 password 9Jb6Z3g
!
end
```

自動インストールを使用した R3 の設定：例

次に、自動インストールを使用して R3 を設定する例を示します。

R3 をフレーム リレー ネットワークに接続します。

R3 の電源をオンにします。

自動インストール プロセスは約 5 分以内に完了します。

TFTP サーバ ログ

TFTP サーバ ログには、次のようなメッセージが出力されます。

```
Sent network-confg to (172.16.27.100), 76 bytes
Sent r3-confg to (172.16.27.100),687 bytes
```

R3 上でのコンフィギュレーション ファイルの保存：例

次に、R3 上で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に保存し、R3 の電源を再投入してもコンフィギュレーションが保持されるようにする例を示します。

```
R1# telnet 172.16.27.100
Trying 172.16.27.100 ... Open

User Access Verification

Password:
R3> enable
Password:

R3# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R4# exit

[Connection to 192.168.10.2 closed by foreign host]
R1#
```

その他の関連資料

ここでは、自動インストールを使用したシスコのネットワーキング デバイスのリモートからの設定に関する参考資料を示します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
設定の基本的なコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
フレーム リレー /ATM 間サービス インターワーキング（FRF.8）	• 『*Cisco IOS Wide-Area Networking Configuration Guide*』の「Frame Relay-ATM Interworking Supported Standards」モジュール • 『*Cisco IOS Wide-Area Networking Configuration Guide*』の「Configuring Frame Relay-ATM Interworking」モジュール
シスコ ネットワーキング デバイスの設定に使用される Cisco IOS セットアップ モードと自動インストールの概要	『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Overview: Basic Configuration of a Cisco Networking Device」モジュール
セットアップ モードを使用したシスコのネットワーキング デバイスの設定	『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Using Setup Mode to Configure a Cisco Networking Device」モジュール

MIB

MIB	MIB リンク
IF-MIB	IF-MIB の IFNAME オブジェクトを使用すると、Cisco IOS デバイスが DHCP クライアントとして設定されているときに、その DHCP サーバ クライアント ID で使用されている短いインターフェイス名の値を特定できます。 選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

自動インストールを使用したシスコのネットワーキング デバイスの設定に関する機能情報

表 6 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) または 12.0(3)S 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

（注） 表 6 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 6　自動インストールによる Cisco ネットワーキング デバイスのリモート設定の機能情報

機能名	リリース	機能設定情報
フレーム リレー /ATM 間インターワーキング接続上の自動インストール	12.2(4)T	フレーム リレー /ATM 間インターワーキング接続上の自動インストール機能は、既存の Cisco IOS 自動インストール機能を拡張するものです。フレーム リレー上の自動インストールでカプセル化されたシリアル インターフェイスは従来からサポートされていますが、この機能は、中央の（既存の）ルータにフレーム リレー インターフェイスではなく ATM インターフェイスがある場合にも、同じ機能を提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「フレーム リレー /ATM 間スイッチング デバイス」 • 「フレーム リレー /ATM 間サービス インターネットワーキングでの自動インストールの使用」 この機能のために追加または変更されたコマンドはありません。この機能で使用するすべてのコマンドの説明は、『*Cisco IOS Configuration Fundamentals Command Reference*』にあります。
LAN インターフェイスに DHCP を使用した自動インストール	12.1(5)T 12.2(33)SRC	LAN インターフェイスに DHCP を使用した自動インストール機能では、LAN インターフェイス（特にイーサネット、トークンリング、FDDI インターフェイス）上での Cisco IOS 自動インストール用に、Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）の使用を Dynamic Host Configuration Protocol（DHCP）の使用で置き換えることで、自動インストールの利点が強化されます。 この機能に関する詳細については、次の項を参照してください。 • 「LAN インターフェイスに DHCP を使用した自動インストール」

端末の動作特性の設定

端末の動作特性の設定

この章では、端末の動作特性を設定する方法について説明します。この章の端末操作コマンドの詳細については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「Terminal Operating Characteristics Commands」の章を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index*』を使用するかオンラインで検索します。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。詳細については、『About Cisco IOS Software Documentation』の章の「Identifying Platform Support for Cisco IOS Software Features」の項を参照してください。

端末動作特性の設定作業リスト

端末の動作特性を設定するには、次の項で説明されている作業を実行します。この章のすべての作業は任意です。

- 「現在の端末セッションに関する情報の表示」
- 「ローカル端末パラメータの設定」
- 「セッション間でのローカル設定の保存」
- 「セッションの終了」
- 「端末セッション パラメータの変更」
- 「コンソールおよび端末でのデバッグ メッセージの表示」
- 「シリアル デバイス ロケーションの記録」
- 「端末ポート キューの再試行間隔の変更」
- 「プリンタの LPD プロトコル サポートの設定」

（注） 端末サービスの設定の詳細については、『Release 12.2 *Cisco IOS Terminal Services Configuration Guide*』および『Release 12.2 *Cisco IOS Dial Technologies Configuration Guide*』を参照してください。

現在の端末セッションに関する情報の表示

端末回線情報を表示するには、必要に応じて、ユーザまたは特権 EXEC モードで、次のコマンドを使用します。

コマンド	目的
Router> **show whoami** *text*	ホスト名、回線番号、回線速度および場所など、現在のセッションで使用されている端末回線に関する情報を表示します。コマンドの引数にテキストが含まれる場合、そのテキストは、回線の追加データの一部として表示されます。
Router> **where**	現在の端末回線に関連付けられているすべてのオープン セッションをリストします。出力のアスタリスク（*）は、現在の端末セッションを示します。

次に、**show whoami** コマンドの出力例を示します。

```
Router> show whoami

Comm Server "Router", Line 0 at 0bps.  Location "Second floor, West"

--More--
Router>
```

情報を画面に表示させるため、**show whoami** コマンドは、常に CLI プロンプトに戻る前に --More-- プロンプトを表示します。スペースキーを押すと、プロンプトに戻ります。

ローカル端末パラメータの設定

terminal EXEC モード コマンドは、現在のセッションだけで機能をイネーブルまたはディセーブルにします。これらのコマンドを使用すると、保存されているコンフィギュレーション ファイルを変更せずに、端末回線設定を一時的に変更できます。

現在のセッションの端末パラメータを設定するコマンドのリストを表示するには、EXEC モードで次のコマンドを実行します。

コマンド	目的
Router# **terminal ?**	端末パラメータを設定するコマンドをリストします。

次に、**terminal ?** コマンドの出力例を示します。ルーティング デバイスで使用できるコマンドは、使用するソフトウェア イメージおよびハードウェアにより異なります。

```
Router> terminal ?
  autohangup              Automatically hangup when last connection closes
  data-character-bits     Size of characters being handled
  databits                Set number of data bits per character
  dispatch-character      Define the dispatch character
  dispatch-timeout        Set the dispatch timer
  download                Put line into 'download' mode
  editing                 Enable command line editing
  escape-character        Change the current line's escape character
  exec-character-bits     Size of characters to the command exec
  flowcontrol             Set the flow control
```

```
full-help               Provide help to unprivileged user
help                    Description of the interactive help system
history                 Enable and control the command history function
hold-character          Define the hold character
ip                      IP options
keymap-type             Specify a keymap entry to use
lat                     DEC Local Area Transport (LAT) protocol-specific
                        configuration
length                  Set number of lines on a screen
no                      Negate a command or set its defaults
notify                  Inform users of output from concurrent sessions
padding                 Set padding for a specified output character
parity                  Set terminal parity
rxspeed                 Set the receive speed
special-character-bits  Size of the escape (and other special) characters
speed                   Set the transmit and receive speeds
start-character         Define the start character
stop-character          Define the stop character
stopbits                Set async line stop bits
telnet                  Telnet protocol-specific configuration
telnet-transparent      Send a CR as a CR followed by a NULL instead of a CR
                        followed by a LF
terminal-type           Set the terminal type
transport               Define transport protocols for line
txspeed                 Set the transmit speeds
width                   Set width of the display terminal
```

この章では、複数の端末設定を、すべての端末セッションまたは現在の端末セッションだけに設定できます。すべての端末セッションでの設定は、コンフィギュレーション モードで行い、保存できます。現在のセッションでの設定は、通常 **terminal** という単語から始まる、EXEC モード コマンドを使用して指定します。

セッション間でのローカル設定の保存

セッション間でローカル パラメータ（**terminal** EXEC モード コマンドで設定）を保存するように、Cisco IOS ソフトウェアを設定できます。これらのローカル設定を保存すると、ユーザが設定するパラメータが、端末セッション間でも有効になります。この機能は、プライベート オフィスのサーバに役立ちます。セッション間でローカル設定を保存するには、次のコマンドをライン コンフィギュレーション モードで使用します。

コマンド	目的
`Router(config-line)# private`	ローカル設定をセッション間で保存します。

private ライン コンフィギュレーション コマンドが使用されていない場合、ユーザ設定の端末パラメータは、**exit** EXEC モード コマンドによりセッションを終了するとき、または **exec-timeout** ライン コンフィギュレーション コマンドで設定されたインターバルが経過したときにクリアされます。

セッションの終了

セッションを終了するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **quit**	現在のセッションを終了します。

セッションの終了および接続の切断の詳細については、「接続、メニュー、およびシステム バナーの管理」の章を参照してください。

端末セッション パラメータの変更

ここでは、特定の回線およびローカルの両方で端末およびライン設定を変更する方法について説明します。ローカル設定には、**terminal** EXEC モード コマンドを使用します。この設定は、システム管理者が行った設定を一時的に上書きし、システムを終了するまで有効になります。ライン コンフィギュレーション モードで、次に回線パラメータを変更するまで、そのラインで有効になる端末動作特性を設定できます。

次の項では、端末および回線設定での一般的な変更を行うときに使用される作業について説明します。

- 「エスケープ文字およびその他のキー シーケンスの定義」
- 「Telnet 動作特性の指定」
- 「ファイル転送のデータ透過性の設定」
- 「国際文字表示の指定」

次の項では、端末および回線設定での特別な変更を行うときに使用される作業について説明します。

- 「文字の埋め込みの設定」
- 「端末およびキーボード タイプの指定」
- 「端末の画面長および画面幅の変更」
- 「出力保留通知のイネーブル化」
- 「文字およびパケット ディスパッチ シーケンスの作成」
- 「現在のセッションでのフロー制御の変更」
- 「セッション ロックのイネーブル化」
- 「自動ボー レート検出の設定」
- 「非セキュア回線の設定」
- 「端末ポートの通信パラメータの設定」

エスケープ文字およびその他のキー シーケンスの定義

システム エスケープ、端末のアクティベーション、切断、端末の一時停止の機能を実行するときに使用されるデフォルト キーを定義または変更できます。通常、使用されるキーは、コントロール（Ctrl）キーおよび別のキー（または複数のキー）を同時に押すなど、キーの組み合わせ（Ctrl+^ など）です。Ctrl キーと別のキーを押し、また別のキーを押すなどのキー シーケンス（たとえば、Ctrl+^、x）も使用されることがあります。ただし、各キーまたはキーの組み合わせは 1 つの ASCII 文字で表されるため、いずれの場合でも、これらのキーは文字と示されます。使用できる ASCII 文字と数字、および同様のキーボードのリストについては、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の付録「ASCII Character Set」を参照してください。

エスケープ文字およびその他のキー シーケンスのグローバルな定義

端末セッションのアクティベーション、切断、エスケープまたは一時停止に関連するデフォルトのキー シーケンスを定義または変更するには、必要に応じて、ライン 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。

コマンド	目的
`Router(config-line)# escape-character {ascii-number | ascii-character | break | default | none}`	システム エスケープ文字を変更します。1 ～ 30 の 10 進数で表される ASCII 文字を使用することを推奨します。エスケープ文字は、単一の文字（’ など）、キーの組み合わせ（Ctrl+X）、またはキー シーケンス（Ctrl+^、X）です。デフォルトのエスケープ文字（キーの組み合わせ）は、Ctrl+Shift+6（Ctrl+^）または Ctrl+Shift+6, X（Ctrl+^、X）です。
`Router(config-line)# activation-character ascii-number`	セッション アクティベーション文字を定義します。この文字を空の端末に入力すると、端末セッションが開始します。デフォルトのアクティベーション文字は、Return キーです。
`Router(config-line)# disconnect-character ascii-number`	セッション切断文字を定義します。この文字を端末で入力すると、ルータのセッションが終了します。デフォルトの切断文字はありません。
`Router(config-line)# hold-character ascii-number`	画面への出力を一時停止するホールド文字を定義します。この文字が設定されると、ユーザは、この文字を入力して、いつでも端末セッションへの出力を一時停止できます。出力を再開するには、任意のキーを押します。通常の通信でホールド文字を使用するには、エスケープを前に付けて使用します。デフォルトのホールド文字はありません。

説明されているコマンドのほとんどについては、**no** 形式を使用することで、デフォルト値に戻すことができます。ただし、エスケープ文字をデフォルトに戻すには、**escape-character default** ライン コンフィギュレーション コマンドを使用します。

（注） autoselect 機能（**autoselect** ライン コンフィギュレーション コマンドを使用してイネーブルにされます）を使用している場合は、アクティベーション文字をデフォルト値 Return から変更しないでください。このデフォルト値を変更すると、autoselect 機能が動作しないことがあります。

現在のセッションのエスケープおよび一時停止文字の定義

現在の端末セッションで、キー シーケンスを変更して、システム エスケープおよび端末一時停止の機能を実行できます。これらのシーケンスを変更するには、必要に応じて、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal escape-character** *ascii-number*	現在のセッションのシステム エスケープ シーケンスを変更します。エスケープ シーケンスは、その後のコードが特殊な意味を持つことを示します。デフォルトのキーの組み合わせは、Ctrl+Shift+6（Ctrl+^）です。
Router> **terminal hold-character** *ascii-number*	このセッションで端末画面への出力を一時停止するホールド シーケンスまたは文字を定義します。デフォルトのシーケンスはありません。出力を続行するには、ホールド文字の後に任意の文字を入力します。通常の通信でホールド文字を使用するには、エスケープを前に付けて使用します。コンソール端末の出力を中断することはできません。

terminal escape-character EXEC コマンドは、たとえば、デフォルトのエスケープ文字がキーボード ファイルで異なる目的に定義されている場合に役立ちます。ルータが別のデバイスと接続しているときに、エスケープ文字の後に X キーを入力すると、ルータが EXEC モードに戻ります。

Telnet 動作特性の指定

アクセス サーバの Telnet 動作特性を設定するには、次の項で説明されている作業を実行します。

- 「リバース Telnet 接続のハードウェア ブレーク信号の生成」
- 「全二重リモート エコー接続を拒否するように回線を設定する」
- 「転送速度ネゴシエーションの許可」
- 「ブレーク信号の同期化」
- 「行末文字の変更」

（注） この項のコマンドは、アクセス サーバだけに適用されます。

リバース Telnet 接続のハードウェア ブレーク信号の生成

現在の回線およびセッションのリバース Telnet 接続に関連付けられている EIA/TIA-232 回線に対するハードウェア ブレーク信号がアクセス サーバに生成されるためには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal telnet break-on-ip**	現在の回線およびセッションのリバース Telnet 接続に関連付けられている EIA/TIA-232 回線に対するハードウェア ブレーク信号を生成します。

ハードウェア ブレーク信号は、Telnet Interrupt-Process コマンドがその接続で受け取られたときに発生します。このコマンドは、Telnet IP コマンドの X.25 ブレーク インジケータへの変換を制御するときに使用できます。

このコマンドは、次の状況に役立つ回避策でもあります。

- 複数のユーザ Telnet プログラムが、Interrupt-Process コマンドを送信するが、Telnet ブレーク信号を送信できない場合。
- 一部の Telnet プログラムが、Interrupt-Process コマンドを送信するブレーク信号を実装する場合。

一部の EIA/TIA-232 ハードウェア デバイスは、ハードウェア ブレーク信号をさまざまな目的で使用します。ハードウェア ブレーク信号は、Telnet Break コマンドが受信されると生成されます。

全二重リモート エコー接続を拒否するように回線を設定する

Cisco IOS ソフトウェアで他方からの全二重リモート エコー接続要求を拒否できるように回線を設定できます。この拒否により、Telnet リモート エコーおよび Suppress Go Ahead オプションのネゴシエーションが抑制されます。現在のセッションの全二重または着信接続のリモート エコー オプションのネゴシエーションを拒否するように現在の回線を設定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal telnet refuse-negotiations`	現在のセッションの全二重のネゴシエーションを拒否するように現在の回線を設定します。

転送速度ネゴシエーションの許可

現在の回線およびセッションの転送速度ネゴシエーションを Cisco IOS ソフトウェアに許可するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal telnet speed default-speed maximum-speed`	現在の回線およびセッションの転送速度ネゴシエーションを Cisco IOS ソフトウェアに許可します。

基準として、リバース Telnet のリモート システム、アクセス サーバを介してネットワークに接続されているホスト マシン、またはアクセス サーバに接続されているコンソール回線のグループ（接続のローカルとリモートで使用される回線速度が異なる場合）の回線速度を使用できます。回線速度ネゴシエーションは、RFC 1080 で定義されている Remote Flow Control オプションに従います。

ブレーク信号の同期化

Telnet ブレーク信号を受信したときにリバース Telnet 回線に Telnet 同期信号を送信させるようにアクセス サーバの回線を設定できます。TCP 同期信号は、データ パスをクリアしますが、着信コマンドを解釈します。現在の回線およびセッションで Telnet ブレーク信号を受信したときに Cisco IOS ソフトウェアに Telnet 同期信号を送信させるには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal telnet sync-on-break`	現在の回線およびセッションで Telnet ブレーク信号を受信したときに Cisco IOS ソフトウェアに Telnet 同期信号を送信させます。

行末文字の変更

端末に入力される各行は、CR+LF（復帰および改行）信号で終了します。CR+LF 信号は、Enter または Return キーが押されたときに送信されます。現在の端末回線で、Line Feed（LF; 改行）が続く CR ではなく、null が続く CR として CR 信号を送信させるには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal telnet transparent**	現在の端末回線で、LF が続く CR ではなく、null が続く CR として CR 信号を送信させます。

このコマンドは、Telnet プロトコル仕様での行末処理の解釈が異なる場合に対応します。

ファイル転送のデータ透過性の設定

データ透過性により、Cisco IOS ソフトウェアは、データが制御文字と解釈されることなく、端末接続でデータを渡すことができます。

端末動作中、いくつかの文字は特殊文字として予約されます。たとえば、キーの組み合わせ Ctrl+Shift+6、X（^^x）は、セッションを中断します。端末接続を介してファイルを転送する場合（たとえば、Xmodem または Kermit プロトコルを使用）、ファイルを転送できるように、これらの特殊文字の認識を中断する必要があります。このプロセスは、*データ透過性*と呼ばれます。

Kermit、Xmodem および CrossTalk などのプログラムが端末回線を介してファイルをダウンロードできるように、透過的なパイプとして機能するように回線を設定できます。ファイル転送の透過的なパイプとして機能するように回線を一時的に設定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal download**	ファイル転送の透過的なパイプとして機能するように回線を設定します。

terminal download コマンドは、次のすべてのコマンドを使用した場合と同じ効果があります。

- **terminal telnet transparent**
- **terminal no escape-character**
- **terminal no hold-character**
- **terminal no padding 0**
- **terminal no padding 128**
- **terminal parity none**
- **terminal databits 8**

国際文字表示の指定

従来の米国 ASCII 文字設定は、7 ビット（128 文字）に制限されます。これにより、ほとんどの米国での表示が適切に表現されます。モデル ルータのほとんどのデフォルトは、7 ビット パスで正常に機能します。ただし、国際文字セットおよび特殊記号の表示では、8 ビット ワイド パスおよびその他の処理が必要です。

7 ビットの文字セット（ASCII など）を使用したり、8 ビットの国際文字セット（ISO 8859 など）をイネーブルにしたりできます。バナーやプロンプトに特殊な図形文字および国際文字を使用したり、ソフトウェア フロー制御などの特殊文字を追加したりすることもできます。文字セットは、グローバル、回線ごと、またはユーザ レベルでローカルに設定できます。どのコンフィギュレーション モードでこの国際文字表示を設定するかについては、次の基準に従って判断してください。

- 多数の接続端末がデフォルトの ASCII ビット設定以外をサポートする場合は、グローバル コンフィギュレーション コマンドを使用します。
- デフォルトの ASCII ビット設定以外をサポートする接続端末がごく少数の場合は、ライン コンフィギュレーション コマンドまたは EXEC ローカル端末設定コマンドを使用します。

（注） EXEC の文字幅を 8 ビット文字セットに設定すると、エラーが起きることがあります。パリティを送信している端末のユーザが **help** コマンドを入力すると、「unrecognized command」メッセージが表示されます。これは、システムが読み取っているのは 8 ビットすべてであり、**help** コマンドに 8 番目のビットは不要なためです。

autoselect 機能を使用する場合、アクティベーション文字はデフォルトの Return、EXEC 文字ビットは 7 に設定してください。これらのデフォルトを変更すると、アプリケーションはアクティベーション要求を認識しなくなります。

すべての回線の文字表示の指定

文字セットをすべての回線で（グローバルに）指定するには、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の一方または両方を使用します。

コマンド	目的
`Router(config)# default-value exec-character-bits {7 | 8}`	コマンド文字で使用する文字セットを指定します。
`Router(config)# default-value special-character-bits {7 | 8}`	ソフトウェア フロー制御、ホールド、エスケープ、切断などの特殊文字で使用する文字セットを指定します。

回線の文字表示の指定

ハードウェアまたはソフトウェアに基づいて、あるいは 1 行ずつ文字セットを指定するには、ライン 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。

コマンド	目的
`Router(config-line)# databits {5 | 6 | 7 | 8}`	ハードウェアに生成および解釈させる 1 文字あたりのデータ ビット数を設定します。
`Router(config-line)# data-character-bits {7 | 8}`	ソフトウェアに生成および解釈させる 1 文字あたりのデータ ビット数を設定します。
`Router(config-line)# exec-character-bits {7 | 8}`	EXEC およびコンフィギュレーション コマンドの文字で使用する文字セットを 1 行ずつ指定します。
`Router(config-line)# special-character-bits {7 | 8}`	ソフトウェア フロー制御、ホールド、エスケープ、切断などの特殊文字で使用する文字セットを 1 行ずつ指定します。

現在のセッションの文字表示の指定

現在の端末セッションで、ハードウェアまたはソフトウェアに基づいて、あるいは 1 行ずつ文字セットを指定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal databits** {**5** | **6** | **7** | **8**}	現在のセッションでハードウェアに生成および解釈させる 1 文字あたりのデータ ビット数を設定します。
Router> **terminal data-character-bits** {**7** | **8**}	現在のセッションでソフトウェアに生成および解釈させる 1 文字あたりのデータ ビット数を設定します。
Router> **terminal exec-character-bits** {**7** | **8**}	現在のセッションで EXEC およびコンフィギュレーション コマンドの文字で使用する文字セットを 1 行ずつ指定します。
Router> **terminal special-character-bits** {**7** | **8**}	現在のセッションでソフトウェア フロー制御、ホールド、エスケープ、切断などの特殊文字で使用する文字セットを 1 行ずつ指定します。

文字の埋め込みの設定

文字を埋め込むと、行末に null が数バイト追加され、行を所定の長さにすることができます。特定の出力文字について、文字の埋め込みを変更できます。

回線での文字の埋め込みの設定

回線での文字の埋め込みを設定するには、ライン 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。

コマンド	目的
Router(config-line)# **padding** *ascii-number count*	指定された行の特定の出力文字の埋め込みを設定します。

現在のセッションの文字の埋め込みの変更

現在のセッションの特定の出力文字の埋め込みを変更するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal padding** *ascii-number count*	現在のセッションの指定された行の特定の出力文字の埋め込みを設定します。

端末およびキーボード タイプの指定

回線に接続される端末のタイプを指定できます。この機能には 2 つのメリットがあります。まず、回線に接続されている端末のタイプを記録できるということと、ディスプレイ管理のために端末タイプをリモート ホストに通知する Telnet 端末ネゴシエーションで使用できるということです。

回線の端末タイプの指定

回線の端末タイプを指定するには、ライン 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。

コマンド	目的
`Router(config-line)# terminal-type {terminal-type}`	端末タイプを指定します。*terminal-type* 引数には任意のストリングを使用できます。

この機能は、Telnet プロトコルによりエンド ホストに渡されるキーマップおよび ttycap を識別するときに TN3270 端末で使用されます。

現在のセッションでの端末およびキーボード タイプの指定

現在のセッションの現在の回線に接続される端末のタイプを指定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal terminal-type terminal-type`	現在のセッションの端末タイプを指定します。

デフォルトの VT100 と異なる場合、端末タイプを示します。このデフォルトは、ディスプレイ管理のために TN3270 端末で使用され、また、リモート ホストに端末タイプを通知するために Telnet および rlogin で使用されます。

セッションの現在のキーボード タイプを指定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal keymap-type keymap-name`	現在のセッションのキーボード タイプを指定します。

デフォルトの VT100 以外のキーボードを使用している場合、キーボード タイプを指定する必要があります。システム管理者は、他のキーボード タイプを定義して（**terminal-type** ライン コンフィギュレーション コマンドを使用します）、これらの名前を端末ユーザに提供できます。

端末の画面長および画面幅の変更

デフォルトでは、Cisco IOS ソフトウェアの表示画面は 24 行、80 文字です。これらの値は端末の条件に合わせて変更できます。設定する画面値は、rsh および rlogin セッション中に渡されます。

設定した値は、端末ネゴシエーションでこの種の情報を使用するホスト システムに学習させることができます。画面の表示の一時停止をディセーブルにするには、画面長の値を 0 に設定します。

指定した画面長は、リモート ホストに学習させることができます。たとえば、rlogin プロトコルは、画面長を使用して、リモート UNIX ホストの端末パラメータを設定します。指定した画面幅も、リモート ホストに学習させることができます。

回線の端末の画面長および画面幅の設定

回線のすべてのセッションで端末の画面長および画面幅を設定するには、必要に応じて、ライン コンフィギュレーション モードで次のコマンドのいずれかを使用します。

コマンド	目的
Router(config-line)# **length** *screen-length*	画面長を設定します。
Router(config-line)# **width** *characters*	画面幅を設定します。

現在のセッションの端末の画面長および画面幅の設定

現在のセッションの現在の端末画面で行数または文字カラム数を設定するには、必要に応じて、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal length** *screen-length*	現在のセッションの画面長を設定します。
Router> **terminal width** *characters*	現在のセッションの画面幅を設定します。

出力保留通知のイネーブル化

アクティブ接続以外の接続で出力が保留になっているときにユーザに通知するよう、システムをイネーブルにできます。この機能は、ユーザがシステムで複数の同時 Telnet 接続を使用する可能性がある場合に役立ちます。たとえば、別の接続でメールまたはメッセージが受信される場合、これをユーザに知らせる必要があります。

回線の出力保留通知のイネーブル化

回線の出力保留通知をイネーブルにするには、ライン 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。

コマンド	目的
Router(config-line)# **notify**	別の接続で出力が保留されていることをユーザに通知するように回線をイネーブルにします。

現在のセッションの出力保留通知の設定

現在のセッションで出力保留通知を設定するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal notify**	現在のセッションで出力が保留されていることをユーザに通知するように回線を設定します。

文字およびパケット ディスパッチ シーケンスの作成

Cisco IOS ソフトウェアは、定義された文字または文字のシーケンスを受け取ったときだけデータ パケットを送信するディスパッチ シーケンスおよび TCP ステート マシンをサポートしています。パケットをバッファに入れ、文字を受信したときに送信できるディスパッチ文字を設定できます。また、パ

ケットをバッファに入れ、文字を受信したときに送信できるステート マシンを設定できます。この機能は、ユーザがファンクション キー（通常、Esc I C などの文字のシーケンスとして定義されています）を押したときにパケット転送をイネーブルにします。

TCP ステート マシンは、事前に定義されている文字シーケンスのセットで TCP プロセスを制御できます。デバイスの現在のステートにより、予測された文字シーケンスを受け取ったときに、次に何が発生するかが決まります。ステート マシン コマンドは、特定の文字シーケンスを検索および認識して、ステートのセットを繰り返すようにサーバを設定します。ユーザはこれらのステートを 8 つまで定義できます（各ステートは、割り当てられたコンフィギュレーション コマンドおよび受信した文字シーケンスのタイプに基づいてサーバが実行する作業と考えてください）。

Cisco IOS ソフトウェアは、非同期ポートからのデータをネットワークに送信するかどうかを決定するユーザ指定ステート マシンをサポートしています。この機能は、ディスパッチ文字の概念を拡張するもので、マルチキャラクタ ディスパッチ ストリングと同様の機能を可能にします。

ステート マシンに設定できるステートは最大で 8 つまでです。データ パケットは、適切な文字またはシーケンスにより転送がトリガーされるまでバッファに入れられます。遅延およびタイマー メトリックにより、システム リソースをより効率的に使用できます。TCP ステート マシンで定義される文字は、ディスパッチ文字で定義されている文字よりも優先されます。

回線での文字およびパケット ディスパッチ シーケンスの設定

現在のシステムを設定するには、ライン 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。

コマンド	目的
Router(config-line)# **state-machine** *name state firstchar lastchar* [*nextstate* | **transmit**]	TCP ステート マシンのステートの移行基準を指定します。
Router(config-line)# **dispatch-machine** *name*	TCP パケット ディスパッチのステート マシンを指定します。
Router(config-line)# **dispatch-character** *ascii-number* [*ascii-number2 . . . ascii-number*]	パケット転送をトリガーする文字を定義します。
Router(config-line)# **dispatch-timeout** *milliseconds*	ディスパッチ タイマーを設定します。
Router(config-line)# **buffer-length** *length*	転送するデータ ストリームの最大長を指定します。

現在のセッションでのパケット ディスパッチ文字の変更

現在のセッションでパケット ディスパッチ文字を変更するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal dispatch-character** *ascii-number1* [*ascii-number2 . . . ascii-number*]	現在のセッションでパケット転送をトリガーする文字を定義します。

現在のセッションでのフロー制御の変更

このセッションのルータと接続デバイス間のフロー制御を変更するには、必要に応じて、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **terminal flowcontrol** {**none** | **software** [**in** | **out**] | **hardware**}	このセッションの端末フロー制御を設定します。
Router> **terminal start-character** *ascii-number*[1]	現在のセッションのフロー制御開始文字を設定します。
Router> **terminal stop-character** *ascii-number*[1]	現在のセッションのフロー制御停止文字を設定します。

1. このコマンドは通常、使用されません。通常、**terminal flowcontrol** コマンドだけを使用する必要があります。

（注） EE スイッチ コンソールでは、ソフトウェアのフロー制御はデフォルトでイネーブルになっています。

（注） フロー制御の設定、および現在のセッション以外での回線のフロー制御の設定の詳細については、『Dial Solutions Configuration Guide』の「Configuring Modem Support and Asynchronous Devices」の章を参照してください。X.25 フロー制御については、『Cisco IOS Wide-Area Networking Configuration Guide』の「Configuring X.25 and LAPB」の章を参照してください。

セッション ロックのイネーブル化

lock EXEC コマンドは、セッションへのアクセスを一時的にロックし、他のユーザへのアクセスを拒否します。セッション ロックは、**lock** コマンドを使用する回線でイネーブルにする必要があります。特定の回線または回線のグループでユーザによるセッション ロックを許可するには、ライン 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。

コマンド	目的
Router(config-line)# **lockable**	一時的な端末ロック メカニズムをイネーブルにします。

自動ボー レート検出の設定

使用されるボー レートを自動的に検出するように回線を設定できます。自動ボー レート検出を設定するには、ライン 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。

コマンド	目的
Router(config-line)# **autobaud**	ボー レートを自動検出するように回線を設定します。

（注） **autobaud** コマンドと **autoselect** コマンドは併用しないでください。

自動ボー レート検出が有効な通信を開始するには、端末から Return キーを複数回押します。600、1800 または 19200 ボー レート回線でボー レートを検出する場合、Return キーを 3 回押す必要があります。その他のボー レートに回線を設定する場合、Return キーを 2 回だけ押します。ボー レートの検出後に Return キーを押すと、EXEC ファシリティにより、別のシステム プロンプトが表示されます。

非セキュア回線の設定

非セキュア ダイヤルアップ回線として表示されるように端末回線を設定できます。この情報は、このようなダイヤルアップ接続をリモート システムに報告する、Local-Area Transport（LAT; ローカルエリア トランスポート）ソフトウェアにより使用されます。

回線を非セキュア回線として設定するには、ライン 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。

コマンド	目的
`Router(config-line)# insecure`	回線をダイヤルアップ回線として設定します。

前のリリースの Cisco IOS ソフトウェアでは、モデル制御を使用する回線は、LAT プロトコルを介するダイヤルアップ接続として報告されていました。このコマンドを使用することで、回線をより直接的に制御できます。

端末ポートの通信パラメータの設定

接続されている端末またはホストの要件を満たすため、必要に応じて、次のパラメータを変更できます。これらのパラメータを変更するには、必要に応じて、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> terminal {speed | txspeed | rxspeed} bps`	現在のセッションの回線速度を設定します。回線速度、転送速度または受信速度から選択します。
`Router> terminal databits {5 | 6 | 7 | 8}`	現在のセッションのデータ ビットを設定します。
`Router> terminal stopbits {1 | 1.5 | 2}`	現在のセッションの停止ビットを設定します。
`Router> terminal parity {none | even | odd | space | mark}`	現在のセッションのパリティ ビットを設定します。

コンソールおよび端末でのデバッグ メッセージの表示

現在のセッションで EXEC モードの **debug** コマンドの出力およびシステム エラー メッセージを表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# terminal monitor`	現在の端末で EXEC モードの **debug** コマンドの出力およびシステム エラー メッセージを表示します。

端末パラメータ コンフィギュレーション コマンドはすべてローカルで設定され、セッション終了後は無効になるので注意してください。デバッグ メッセージを表示するには、各セッションの特権レベル EXEC プロンプトでこのコマンドを使用する必要があります。

シリアル デバイス ロケーションの記録

シリアル デバイスのロケーションを記録できます。ロケーションに提供されるテキストは、EXEC モニタリング コマンドの出力に表示されます。デバイス ロケーションを記録するには、ライン 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。

コマンド	目的
Router(config-line)# **location** *text*	シリアル デバイスのロケーションを記録します。

端末ポート キューの再試行間隔の変更

ビジー状態のプリンタなどのリモート デバイスに接続しようとした場合、この接続試行は、端末ポート キューに送られます。再試行間隔が長すぎ、いくつかのルータまたは他のデバイスが、そのリモート デバイスに接続されている場合、接続試行により長い遅延が発生します。端末ポート キューの再試行間隔を変更するには、ライン 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。

コマンド	目的
Router(config)# **terminal-queue entry-retry-interval** *interval*	端末ポート キューの再試行間隔を変更します。

プリンタの LPD プロトコル サポートの設定

Cisco IOS ソフトウェアは、UNIX システム間でプリント ジョブを送信するときに使用される Berkeley UNIX Line Printer Daemon（LPD; ライン プリンタ デーモン）プロトコルのサブセットをサポートしています。この LPD プロトコルのサブセットにより、次のことが許可されます。

- ステータス情報の改善
- プリント ジョブのキャンセル
- 一般的なプリント障害でのプリントおよび自動再試行の確認
- 標準 UNIX ソフトウェアの使用

Cisco では LPD を実装できるため、いくつかのタイプのデータ（たとえば、PostScript またはロー テキスト）をプリント ジョブとして送信できるようにプリンタを設定できます。

LPD プロトコルのプリンタを設定するには、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。

コマンド	目的
Router(config)# **printer** *printername* {**line** *number* | **rotary** *number*} [**newline-convert**]	プリンタを設定して、デバイスの 1 つ以上の TTY 回線を指定します。

printer コマンドを使用する場合、UNIX システムの /etc/printcap ファイルを変更して、ルータのリモート プリンタの定義を示す必要があります。新しい行を復帰、改行文字シーケンスに変換して単一文字の行終了子を処理しない UNIX システムでは、オプションの **newline-convert** キーワードを使用します。

次に、ホスト memphis での saturn という名前のプリンタの設定例を示します。

```
commlpt|Printer on cisco AccessServer:\
    :rm=memphis:rp+saturn:\
    :sd+/usr/spool/lpd/commlpt:\
    :lf=?var/log/lpd/commlpt:
```

実際のファイルの内容は、現在の UNIX システムの設定により異なる場合があります。

印刷する場合、標準の UNIX lpr コマンドを使用します。

LPD プロトコルのサポートにより、各プリンタで現在定義されているプリンタおよび現在の使用状況の統計情報のリストを表示できます。このようにするには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **show printer**	現在定義されているプリンタおよび現在の使用状況に関する統計情報をリストします。

LPD 機能へのアクセスを提供するには、システム管理者は、プリンタを設定して、そのプリンタに 1 つ以上の TTY 回線を割り当てる必要があります。また、管理者は、UNIX システム /etc/printcap ファイルを変更して、Cisco IOS ソフトウェアのリモート プリンタの定義を示す必要があります。

接続、メニュー、およびシステム バナーの管理

接続、メニュー、およびシステム バナーの管理

この章では、他のホストへの接続を管理する方法、ルータのユーザ用にバナー メッセージを設定する方法、および特定のユーザ作業のメニューを作成する方法について説明します。

このマニュアルでは、Cisco IOS Release 12.2 で初めて使用可能になったコマンドを扱います。以降のリリースおよび派生のリリースで追加の補足マニュアルが利用できる場合があります。この章で扱うコマンドの詳しいマニュアルを見つけるには、『*Cisco IOS Release 12.4 Master Indexes*』を使用してください。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索します。詳細については、「About Cisco IOS Software Documentation」の章を参照してください。

接続、メニュー、およびシステム バナーの管理の作業リスト

接続を管理し、メッセージとバナーを設定し、ユーザ メニューを作成するには、必要に応じて次の項で説明する作業のいずれかを実行します。この章のすべての作業は任意です。

これらの項の例は、章末の「接続管理、システム バナー、およびユーザ メニュー コンフィギュレーションの例」の項にあります。

接続の管理

サポートされている接続プロトコルすべてに適用できる接続管理アクティビティを設定するには、次の項で説明する作業を実行します。すべての作業は任意です。

現在の端末設定の表示

端末回線接続用の現在の設定を表示するには、特権 EXEC モードまたはユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show terminal**	端末用の現在の設定を表示します。

次に、出力の例を示します。

```
AccessServer1> show terminal

Line 2, Location: "", Type: "VT220"
Length: 24 lines, Width: 80 columns
Baud rate (TX/RX) is 9600/9600
Status: PSI Enabled, Ready, Active, No Exit Banner
Capabilities: none
Modem state: Ready
Group codes:    0
Special Chars: Escape  Hold  Stop  Start  Disconnect  Activation
                ^^x    none   -     -       none
Timeouts:      Idle EXEC    Idle Session   Modem Answer  Session   Dispatch
               00:10:00        never                        none     not set
                            Idle Session Disconnect Warning
                              never
                            Login-sequence User Response
                             00:00:30
                            Autoselect Initial Wait
                              not set
Modem type is unknown.
Session limit is not set.
Time since activation: 00:01:07
Editing is enabled.
History is enabled, history size is 10.
DNS resolution in show commands is enabled
```

```
Full user help is disabled
Allowed transports are lat pad v120 mop telnet rlogin nasi.  Preferred is lat.
No output characters are padded
No special data dispatching characters
```

端末セッションのエスケープおよび他の接続への切り替え

接続を開始した後、エスケープ キー シーケンス（デフォルトでは Ctrl+Shift+6 キーを押してから X）を使用して現在の端末セッションからエスケープできます。コマンド文字は、Ctrl キーを押したままでも、Ctrl キーから指を離しても入力できます。また、大文字、小文字のどちらでも入力できます。

（注） 2 つのキャレット（^^）記号が並んで表示されている画面出力例では、最初のキャレットはコントロール キー（Ctrl）を表し、2 番目のキャレットはキー シーケンス Shift+6 を表します。この二重キャレットの組み合わせ（^^）は、Ctrl キーを押したまま Shift キーと 6 キーを押すことを意味しています。

デフォルトでは、エスケープ キー シーケンスは Ctrl+Shift+6、X です。ただし、**escape-character** ライン コンフィギュレーション コマンドを使用してエスケープ キー シーケンスを変更できます。エスケープ文字の現在の設定を確認するには、**show terminal** 特権またはユーザ EXEC コマンドを使用します。

複数のセッションを同時に開き、開いたセッションの間を行き来できます。

同時に開くことができるセッションの数は、**session-limit VDPN** コンフィギュレーション モード コマンドで定義されています。

1 つのセッションからエスケープし、前に開いたセッションを再開することでセッションを切り替えるには、次の手順を実行します。

ステップ 1 エスケープ キー シーケンス（デフォルトでは Ctrl+Shift+6 キーを押してから X（Ctrl^、X））を押して現在のセッションからエスケープして EXEC プロンプトに戻ります。

ステップ 2 **where** 特権 EXEC コマンドを入力して開いているセッションのリストを表示します。現在の端末回線に関連付けられ、開いているセッションのすべてが表示されます。

ステップ 3 **resume** 特権 EXEC コマンドとセッション番号を入力し、接続を確立します。

リターン キーを押すことで前のセッションを再開することもできます。

Ctrl^、X キーの組み合わせ、**where** および **resume** 特権 EXEC コマンドは、サポートされているすべての接続プロトコル（たとえば Telnet）で使用できます。

接続への論理名の割り当て

接続に論理名を割り当てるには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **name-connection**	接続に論理名を割り当てます。

論理名は、複数の接続を追跡する場合に役立ちます。

割り当てる接続番号と名前を求めるプロンプトが表示されます。**where** 特権 EXEC コマンドにより、割り当て論理接続名のリストが表示されます。

ログイン ユーザ名の変更

現在のログイン ユーザ名を発信アクセス リストの要件またはその他のログイン プロンプトの要件に一致させる必要がある場合は、ログイン ユーザ名を変更できます。このコマンドを使用するには、ログイン サーバが稼動中で、利用可能である必要があります。ログイン ユーザ名を変更するには、ユーザ EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router> login`	現在のログイン ユーザ名を変更する目的で、システムに 2 回目のログインができます。

このコマンドを入力すると、システムによりユーザ名とパスワードを要求するプロンプトが表示されます。新しいユーザ名と元のパスワードを入力します。ユーザ名が一致しなくても、パスワードが一致した場合は、Cisco IOS ソフトウェアにより、**login** コマンドで試行された新しいユーザ名でセッションが更新されます。たとえば、user1 としてログインしたユーザがログイン名を user2 に変更する必要があるとします。

```
Router> login
Username: user2
Password: <letmein>
Router>
```

この例では、パスワード letmein は初回にログインした際に使用したパスワードと同じです（この例の山カッコは、パスワードを入力しても画面には表示されないことを示しています）。2 回目の `Router>` プロンプトで、ユーザは user2 としてログインしていることになります。

ログイン時にユーザ名およびパスワードが必要となるようにネットワーク管理者が指定していなかった場合は、ユーザ名およびパスワードを求めるプロンプトは表示されません。ユーザ名およびパスワードの両方を正しく入力した場合、セッションは指定されたユーザ名と関連付けられます。

TACACS セキュリティを備えたシステムにアクセスするには、次の手順で示すように、「Username:」プロンプトが表示されたときに現在のログイン名を入力するか、*user@tacacs-server* 構文を使用して TACACS サーバを指定します。

	コマンド	目的
ステップ 1	`Router> login`	現在のログイン ユーザ名を変更する目的で、システムに 2 回目のログインができます。
ステップ 2	`Username: user@tacacs-server`	新しいユーザ名を指定して、*tacacs-server* 引数で指定されたサーバでユーザ名を認証します。
ステップ 3	`Password: <password>`	ステップ 2 で指定されたユーザ名の TACACS パスワードを指定します。

ユーザ認証情報には、指定されたホスト（tacacs-server）だけがアクセスされます。

次に、user2 が TACACS ホスト host1 を指定してパスワードを認証する例を示します。

```
Router> login
Username: user2@host1
Translating "HOST1"...domain server (131.108.1.111) [OK]
Password: <letmein2>
```

ホストを指定しない場合、ルータは応答を受信するまでリスト内の各 TACACS サーバを試行します。指定したホストが応答しない場合、その他の TACACS サーバにクエリーが実行されることはありません。ルータはアクセスを拒否するか、または **tacacs-server last-resort** グローバル コンフィギュレーション コマンドが設定されていれば、このコマンドで指定されたアクションに応じて機能します。*user@tacacs-server* 引数で TACACS サーバ ホストを指定した場合、指定された TACACS サーバは以降のすべての認証または通知クエリーで使用されますが、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）アドレス クエリーは例外となる場合があります。

TACACS の設定に関する詳細については、『*Cisco IOS Security Command Reference*』の「TACACS, Extended TACACS, and TACACS+ Commands」の章にある **tacacs-server host** グローバル コンフィギュレーション コマンドを参照してください。

ログイン名を変更する例については、章末の「ログイン ユーザ名およびパスワードの変更：例」の項を参照してください。

端末へのアクセスのロック

一時的なパスワードを設定することにより、コネクションを開いたまま端末セッションへのアクセスを防止できます。この一時的なロック機能が動作するためには、まず（**lockable** ライン コンフィギュレーション モード コマンドを使用して）回線がロックを許可するように設定する必要があります。端末へのアクセスをロックするには、次の手順を実行します。

ステップ 1 ユーザ EXEC モードまたは特権 EXEC モードで **lock** コマンドを発行します。

このコマンドを発行すると、システムによりパスワードを求めるプロンプトが表示されます。

ステップ 2 パスワードを入力します。任意のストリングを使用できます。システムによりパスワードの確認を求めるプロンプトが表示されます。画面がクリアされ、メッセージ「Locked」が表示されます。

ステップ 3 セッションへのアクセスを戻すには、パスワードを再入力します。

Cisco IOS ソフトウェアは、ロックされた回線上でもセッション タイムアウトを受け入れます。この機能を削除するには、回線をクリアする必要があります。

次に、**lock** コマンドが入力された後に表示されるプロンプトの例を示します。入力したパスワードは画面には表示されないため、注意してください。

```
Router# lock
Password:
Again:
                        Locked
Password:
Router#
```

他の端末へのメッセージの送信

1 つまたはすべての端末へメッセージを送信できます。一般的には、すぐにシャットダウンを実行することをユーザに知らせるために実行します。他の端末へメッセージを送信するには、ユーザ EXEC モードまたは特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# send {line-number | *}`	他の端末へメッセージを送信します。* を使用すると、メッセージはすべての端末に送信されます。

システムによりメッセージを入力するプロンプトが表示されます。メッセージの長さは最大 500 文字です。Ctrl+Z キーを押してメッセージを終了します。Ctrl+C キーを押してコマンドを中断します。

TCP 接続のクリア

TCP 接続をクリアするには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# clear tcp {line line-number | local host-name port remote host-name port | tcb tcb-address}`	TCP 接続をクリアします。

clear tcp コマンドは、機能していない TCP 接続をクリアする場合に特に便利です。

clear tcp line *line-number* コマンドは、指定された TTY 回線上の TCP 接続を終了します。この TTY 回線から開始されたすべての TCP セッションも終了します。

clear tcp local *host-name port* **remote** *host-name port* コマンドは、ローカル ルータおよびリモート ルータのホスト名とポートのペアによって識別された特定の TCP 接続を終了します。

ルータから開始されたセッションの終了

セッションを開始するために使用されたプロトコルによって、そのセッションの終了方法が決まります。

SLIP および PPP 接続を終了するには、通常は現在のダイヤルイン ソフトウェアがサポートするコマンドで、ダイヤルイン接続を切断する必要があります。

ルータからリモート デバイスに対して開始された Local Area Transport（LAT; ローカル エリア トランスポート）、Telnet、rlogin、TN3270、または X.3 Packet Assembler/Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）セッションを終了するには、エスケープ キー シーケンス（一部のシステムのデフォルトは Ctrl+Shift+6 を押してから X（Ctrl^X）、その他のシステムのデフォルトは Ctrl+Z）を押し、EXEC プロンプトで **disconnect** コマンドを入力します。リモート システムからのログアウトもできます。

アクティブな端末セッションを終了するには、EXEC モードで **exit** または **logout** コマンドのいずれも使用できます。

Telnet セッションを終了してルータに*戻る*には、次の「ルータからのログアウト」の項を参照してください。

ルータからのログアウト

ルータとの接続を解除しログアウトするために使用する方法は、ルータに対するユーザの位置、およびログインしているルータ上のポートによって異なります。

端末エミュレーション アプリケーションを実行している端末またはコンピュータがルータのコンソール ポートにリモートで接続されている場合は、現在の端末エミュレーション パッケージが使用するコマンドまたはキー シーケンスを発行することによって接続解除します。たとえば、InterCon Corporation の TCP/Connect アプリケーションを実行している Macintosh コンピュータ上では、ユーザ EXEC または特権 EXEC プロンプトで Ctrl+] キーを押して接続解除します。

リモートの端末上で、ルータ上の同期インターフェイスを介して VTY に接続している場合は、ユーザ EXEC または特権 EXEC モードで次のいずれかのコマンドを発行してログアウトできます。

- **exit**
- **logout**

回線の接続解除

（注） セッションを終了するために回線を接続解除することは避けてください。代わりに、ホストからログアウトし、ルータが接続をクリアできるようにします。アクティブなセッションからログアウトできない場合（たとえば、回線のスタックまたはフリーズ）にだけ、回線を接続解除する必要があります。

回線を接続解除するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# disconnect [connection]`	回線を接続解除します。

端末エミュレーション アプリケーションを実行している端末またはコンピュータがルータのコンソール ポートに物理的に接続されている場合は、ルータのコンソール ポートから物理的にケーブルを取りはずすことでも、ルータから接続解除できます。

端末メッセージの設定

システムに接続している端末のユーザに対して表示できるメッセージを設定するには、次の項の作業のいずれかを実行します。すべての作業は任意です。

- 「アイドル端末メッセージのイネーブル化」（P.8）
- 「「Line in Use」（ライン使用中）メッセージの設定」（P.8）
- 「「Host Failed」（ホスト障害）のメッセージの設定」（P.8）

アイドル端末メッセージのイネーブル化

コンソールまたは端末が使用されていない場合にメッセージ表示するようにシステムを設定できます。*空きメッセージ*とも呼ばれるこのメッセージは、ユーザがシステムにログインしたときに表示されるバナー メッセージとは異なります。アイドル端末メッセージをイネーブルにするには、ライン 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。

コマンド	目的
`Router(config-line)# vacant-message [d message d]`	アイドル端末メッセージを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

ヒント この章全体では、区切り文字（*d* 引数）の必要なコマンドが共通して使用されます。区切り文字にはどのような文字でも使用できますが、引用符（"）の使用を推奨します。これは、メッセージ自体の中でこの文字を使用することが通常はないためです。その他のよく使用される区切り文字にはパーセント記号（%）やフォワード スラッシュ（/）がありますが、これらの文字は特定の Cisco IOS コマンドでは意味を持っているため、推奨されません。たとえば、`This terminal is idle` という空きメッセージを設定するには、**vacant-message " This terminal is idle "** というコマンドを入力します。

「Line in Use」（ライン使用中）メッセージの設定

着信接続が試行され、そのときにすべてのロータリー グループまたはその他の回線が使用中である場合に、「Line in Use」（ライン使用中）のメッセージを表示するようにシステムを設定するには、ライン 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。

コマンド	目的
`Router(config-line)# refuse-message d message d`	「Line in Use」（ライン使用中）のメッセージを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

このようなメッセージを定義しなかった場合、すべての回線が使用中であれば、ユーザはシステムが生成したエラー メッセージを受け取ります。このメッセージを使用してユーザにより詳しい指示を提供することもできます。

「Host Failed」（ホスト障害）のメッセージの設定

特定のホストとの Telnet 接続が失敗した場合に「Host Failed」（ホスト障害）のメッセージを表示するようにシステムを設定するには、ライン 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。

コマンド	目的
`Router(config-line)# busy-message hostname d message d`	「Host Failed」（ホスト障害）のメッセージを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

端末バナーのイネーブル化

バナーとは、ユーザに対して表示できる情報メッセージです。端末バナーをイネーブルにするには、次の項の作業のいずれかを実行します。すべての作業は任意です。

- 「Message-of-The-Day バナーの設定」（P.10）
- 「ログイン バナーの設定」（P.10）
- 「EXEC バナーの設定」（P.10）
- 「着信接続に対し送信されるバナーの設定」（P.10）
- 「SLIP-PPP バナー メッセージの設定」（P.11）
- 「バナー表示のイネーブル化またはディセーブル化」（P.11）

端末バナー メッセージを表示する例については、章末の「バナーの設定：例」の項を参照してください。

バナー トークンの使用

バナー トークンの使用により、バナーをカスタマイズできます。トークンは $（*トークン*）形式中のキーワードであり、バナー メッセージ内で使用される場合はトークン引数（たとえばルータ ホスト名、ドメイン名、IP アドレス）の現在設定されている値を表示します。これらのトークンを使用して、現在の Cisco IOS 設定変数を表示する独自のバナーを設計できます。Cisco IOS でサポートされているトークンだけ使用できます。独自のトークンを定義するファシリティはありません。

表 8 に、さまざまな **banner** コマンドでサポートされているトークンを示します。

表 8　　バナー タイプで許可されるトークン

トークン	説明	Message-of-The-Day（MOTD）バナー	ログイン バナー	EXEC バナー	着信バナー	SLIP-PPP バナー
$(hostname)	ルータのホスト名	あり	あり	あり	あり	あり
$(domain)	ルータのドメイン名	あり	あり	あり	あり	あり
$(peer-ip)	ピア マシンの IP アドレス	なし	なし	なし	なし	あり
$(gate-ip)	ゲートウェイ マシンの IP アドレス	なし	なし	なし	なし	あり
$(encap)	カプセル化のタイプ（SLIP または PPP）	なし	なし	なし	なし	あり
$(encap-alt)	SLIP ではなく SL/IP と表示されるカプセル化のタイプ	なし	なし	なし	なし	あり
$(mtu)	最大伝送ユニット サイズ	なし	なし	なし	なし	あり
$(line)	VTY または TTY（非同期）回線番号	あり	あり	あり	あり	なし
$(line-desc)	ユーザ指定の回線の説明	あり	あり	あり	あり	なし

Message-of-The-Day バナーの設定

接続されたすべての端末上に Message-of-The-Day（MOTD; 今日のお知らせ）バナーを表示するように設定できます。このバナーはログイン時に表示され、すべてのネットワーク ユーザに影響するメッセージ（すぐにシステムをシャットダウンするなど）を送信する場合に役立ちます。これを実行するには、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。

コマンド	目的
`Router(config)# banner motd d message d`	Message-of-The-Day バナーを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

ログイン バナーの設定

接続されたすべての端末上にログイン バナーが表示されるように設定できます。このバナーは MOTD バナーの後、ログイン プロンプトの前に表示されます。

ログイン バナーを設定するには、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。

コマンド	目的
`Router(config)# banner login d message d`	ユーザ名およびパスワードのログイン プロンプトの前にバナーを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

ログイン バナーは回線ごとにディセーブルにできません。ログイン バナーをグローバルにディセーブルにするには、**no banner login** コマンドでログイン バナーを削除する必要があります。

EXEC バナーの設定

EXEC プロセスが開始されるたびにバナーが表示されるように設定できます。たとえば、このバナーは Telnet を使用してシステムにアクセスするユーザが、ユーザ名およびパスワードを入力してから、ユーザ EXEC モード プロンプトが表示される前に表示されます。EXEC バナーを設定するには、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。

コマンド	目的
`Router(config)# banner exec d message d`	EXEC プロセスが開始されるたびにバナーを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

着信接続に対し送信されるバナーの設定

リバース Telnet 回線に接続された端末上にバナーが表示されるように設定できます。このバナーは、これらのタイプの接続を使用するユーザに対し、指示を提供する場合に役立ちます。リバース Telnet 接続に関する詳細は、『Release 12.4 *Cisco IOS Dial Technologies Configuration Guide*』の「Configuring and Managing External Modems」の章で説明されています。

着信接続に対して送信されるバナーを設定するには、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。

コマンド	目的
Router(config)# **banner incoming** *d message d*	ネットワーク上のホストから端末回線に接続着信があったときにバナーを表示するようにシステムを設定します。引数 *d* は、任意の区切り文字を表します。

SLIP-PPP バナー メッセージの設定

デフォルトのバナー メッセージは、他社製の SLIP および PPP ダイヤルアップ ソフトウェアの一部で接続の問題を引き起こす場合のあることが知られています。SLIP-PPP バナー メッセージをカスタマイズして、シスコの SLIP および PPP が他社製のダイヤルアップ ソフトウェアと互換性を持つようにできます。SLIP-PPP バナー メッセージを設定するには、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。

コマンド	目的
Router(config)# **banner slip-ppp** *d message d*	カスタマイズされたメッセージを表示するように SLIP-PPP バナーを設定します。引数 *d* は、任意の区切り文字を表します。

バナー表示のイネーブル化またはディセーブル化

MOTD および回線アクティベーション（EXEC）バナーの表示を制御できます。デフォルトでは、これらのバナーはすべての回線上で表示されます。このようなバナーの表示をイネーブルまたはディセーブルにするには、必要に応じてライン 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。

コマンド	目的
Router(config-line)# **no exec-banner**	MOTD および EXEC バナーの表示を抑制します。
Router(config-line)# **exec-banner**	EXEC または MOTD バナーの表示を元に戻します。
Router(config-line)# **no motd-banner**	MOTD バナーの表示を抑制します。
Router(config-line)# **motd-banner**	MOTD バナーの表示を元に戻します。

これらのコマンドは、EXEC セッションを作成したときに、ルータが EXEC バナーおよび MOTD バナーを表示するかどうかを決定します。これらのバナーは、**banner motd** および **banner exec** グローバル コンフィギュレーション コマンドで定義されます。デフォルトでは、MOTD バナーおよび EXEC バナーは、すべての回線上でイネーブルです。

no exec-banner コマンドを使用して、EXEC および MOTD バナーをディセーブルにします。

MOTD バナーは、**no motd-banner** ライン コンフィギュレーション コマンドでもディセーブルにできます。このコマンドは、回線上の MOTD バナーをディセーブルにします。回線上で **no exec-banner** コマンドが設定されている場合、**motd-banner** コマンドがイネーブルかディセーブルかに関係なく、MOTD バナーはディセーブルになります。表 9 に、**exec-banner** コマンドおよび **motd-banner** コマンドの組み合わせの影響をまとめています。

表 9　exec-banner および motd-banner コマンドの組み合わせで表示されるバナー

	exec-banner（デフォルト）	**no exec-banner**
motd-banner（デフォルト）	MOTD バナー EXEC バナー	なし
no motd-banner	EXEC バナー	なし

リバース Telnet 接続の場合、EXEC バナーが表示されることはありません。代わりに、着信バナーが表示されます。MOTD バナーはデフォルトでは表示されますが、**no exec-banner** コマンドまたは **no motd-banner** コマンドのいずれかが設定されている場合はディセーブルになります。表 10 に、リバース Telnet 接続での **exec-banner** コマンドおよび **motd-banner** コマンドの組み合わせの影響をまとめています。

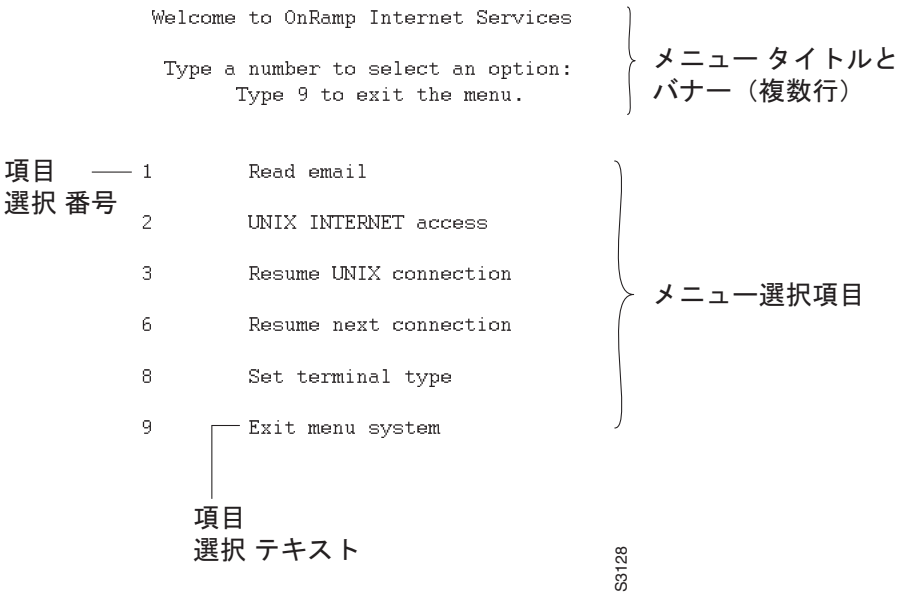
表 10　非同期回線へのリバース Telnet セッションで exec-banner および motd-banner コマンドの組み合わせに基づいて表示されるバナー

	exec-banner（デフォルト）	**no exec-banner**
motd-banner（デフォルト）	MOTD バナー 着信バナー	着信バナー
no motd-banner	着信バナー	着信バナー

メニューの作成

メニューとは、表示されるアクションのリストです。ユーザは、下位のコマンドレベルの詳細を知らなくても、このリストからアクションを選択できます。メニュー システム（ユーザ メニューともいいます）は、ユーザがアクセスできる機能を効率的に制御します。図 6 は、一般的なメニューを構成する部分を図示したものです。

図 6　一般的なメニューの例



コンフィギュレーション モードに移行できるユーザであれば、誰でもメニューを作成できます。メニューを作成する場合は、次の注意事項に留意してください。

- 各メニュー項目は、それぞれ 1 つのユーザ コマンドを表しています。
- メニュー システムのデフォルトは標準の「ダム」端末で、24 行× 80 列形式のテキストだけを表示します。
- 1 つのメニューに含められるメニュー項目は、最大で 18 個です。メニュー項目が 9 個を超える場合、メニューは自動的にシングル スペース メニューとして設定されます。メニュー項目が 9 個以下の場合、メニューは自動的にダブル スペース メニューとして設定されますが、**menu single-space** 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シングル スペース メニューに設定することも可能です（メニューの表示設定オプションに関する詳細については、この章の「メニュー表示設定オプションの指定」の項を参照してください）。
- 項目キーには、数字、文字、ストリングを使用できます。ストリングを使用する場合は、**menu line-mode** グローバル コンフィギュレーション コマンドを設定する必要があります。
- メニューを作成するときは、ユーザがメニューを終了する方法と、終了後のユーザの行き先を必ず指定してください。たとえば **menu-exit** コマンド（この章の「メニュー項目の下位コマンドの指定」の項で説明されています）を使用するなどしてメニューからの出口を提供しないと、ユーザはメニューから出られなくなります。

exec-timeout ライン コンフィギュレーション コマンドを使用して、アイドル メニューを閉じ、クリーンアップできます。**session-timeout** コマンドを使用して、接続が開いているメニューをクリーンアップできます。

メニューの作業リストの作成

メニューを作成するには、次の項で説明する作業を実行します。

- 「メニュー タイトルの指定」（P.14）（必須）

- 「メニュー プロンプトの指定」（P.15）（任意）
- 「メニュー項目テキストの指定」（P.15）（必須）
- 「メニュー項目の下位コマンドの指定」（P.16）（必須）
- 「メニューのデフォルト コマンドの指定」（P.17）（必須）
- 「サブメニューの作成」（P.18）（任意）
- 「非表示メニュー エントリの作成」（P.19）（任意）
- 「メニュー表示設定オプションの指定」（P.19）（任意）
- 「項目ごとのメニュー オプションの指定」（P.21）（任意）
- 「メニューの呼び出し」（P.21）（必須）
- 「コンフィギュレーションからのメニューの削除」（P.22）（任意）

メニュー タイトルの指定

メニューに識別のためのタイトルを指定できます。メニュー タイトルを指定するには、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。

コマンド	目的
`Router(config)# menu` *menu-name* `title` *d title d*	メニューのタイトルを指定します。引数 *d* は、任意の区切り文字を表します。

次に、OnRamp メニューが選択されたときに表示されるタイトルを指定する例を示します。タイトルは、次の 4 つの主要な要素で構成されます。

- **menu title** コマンド
- タイトル テキストを開いたり閉じたりする区切り文字
- 画面をクリアするエスケープ文字（任意）
- タイトル テキスト

次に、図 6 に示したメニューのタイトルを作成するために使用されるコマンドの例を示します。

```
Router(config)# menu OnRamp title %^[[H^[[J

Enter TEXT message.  End with the character '%'.
                Welcome to OnRamp Internet Services

          Type a number to select an option;
               Type 9 to exit the menu.
%
Router(config)#
```

タイトル テキストの前に空白文字を入れると、メニューのタイトルの水平位置を決めることができます。Enter キーを押すことにより、タイトルの上下にスペース行を追加することもできます。

この例では、タイトル テキストは次の要素で構成されています。

- 1 行のタイトル
- スペース
- 2 行のメニュー指示バナー

タイトル テキストはテキスト区切り文字（この例ではパーセント記号（%））で囲む必要があります。タイトル テキストの区切り文字は、スラッシュ（/）、二重引用符（"）、または波ダッシュ（~）などの、通常はタイトルのテキスト内に現れない文字です。通常はタイトルのテキスト内では使用されない文字であれば、どのような文字でも区切り文字として使用できます。Ctrl+C キーは特殊用途に予約されているため、タイトルのテキスト内では使用できません。

このタイトル テキストの例には、メニューを表示する前に画面をクリアするため、エスケープ文字シーケンスも含まれています。この場合、ストリング ^[[H^[[J は、多くの VT100 互換端末で画面をクリアするために使用されるエスケープ ストリングです。このストリングを入力するには、Ctrl+V キーを入力してから、各エスケープ文字（^[）を入力する必要があります。

メニュー タイトルに端末固有のストリングを埋め込む代わりに、**menu clear-screen** 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メニューおよびサブメニューを表示する前に画面をクリアすることもできます。このオプションはルータ内で定義された termcap エントリとユーザの端末用に設定された端末のタイプに基づいて、端末に依存しないメカニズムを使用します。**menu clear-screen** コマンドを使用すると、メニュー タイトルの中に端末固有のストリングを埋め込まなくても、複数の端末のタイプで同じメニューを使用できるようになります。termcap エントリに clear ストリングが含まれていない場合、メニュー システムにより新たに 24 行が挿入され、既存のテキストすべてを端末画面の上部へスクロールさせてクリアします。

メニューを表示する前に画面をクリアするには、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。

コマンド	目的
`Router(config)# menu menu-name clear-screen`	メニューおよびサブメニューを表示する前に、スクリーンをクリアするように指定します。

次に、OnRamp メニューまたはサブメニューを移動させる前に画面をクリアする例を示します。

```
Router(config)# menu OnRamp clear-screen
```

メニュー プロンプトの指定

メニュー プロンプトを指定するには、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。

コマンド	目的
`Router(config)# menu menu-name prompt d prompt d`	メニューのプロンプトを指定します。引数 *d* は、任意の区切り文字を表します。

メニュー項目テキストの指定

表示される各メニュー エントリは、選択キー（数字、文字、またはストリング）および実行されるアクションを説明するテキストで構成されています。最大 18 のメニュー項目に対し、説明テキストを指定できます。各メニュー エントリは、それぞれ 1 つのユーザ インターフェイス コマンドを表すため、メニュー項目テキストは 1 回につき 1 エントリずつ指定する必要があります。メニュー項目テキストを指定するには、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。

コマンド	目的
Router(config)# **menu** *menu-name* **text** *menu-item menu-text*	メニュー項目のテキストを指定します。

次に、OnRamp メニュー内の 3 つのエントリに対して表示されるテキストを指定する例を示します。

```
Router(config)# menu OnRamp text 1 Read email
Router(config)# menu OnRamp text 2 UNIX Internet Access
Router(config)# menu OnRamp text 9 Exit menu system
```

「ヘルプ サーバ」ホストを作成し、そのホストとの接続を確立するメニュー エントリを使用して、状況依存ヘルプへのアクセスを可能にできます。

メニュー選択キーは連続している必要はありません。特定の数字、文字、またはストリングをヘルプや終了などの特殊機能に割り当てることにより、メニュー内のメニュー エントリ数に関係なく複数のメニュー間に一貫性を持たせることができます。たとえば、メニュー エントリ H を、すべてのメニューでヘルプとして予約できます。

1 つのメニューで 9 個を超えるメニュー項目が定義された場合、**menu line-mode** および **menu single-space** グローバル コンフィギュレーション コマンドが自動的にアクティブになります。このコマンドは、9 項目以下のメニューに明示的に設定できます。これらのコマンドに関する詳細については、この章の「メニュー表示設定オプションの指定」の項を参照してください。

メニュー項目の下位コマンドの指定

ユーザが表示された各メニュー エントリのキーを入力すると、そのメニュー エントリにより、ユーザ インターフェイス コマンドが発行されます。各メニュー エントリに関連付けられるコマンドは、1 つだけです。下位のメニュー項目コマンドを指定するには、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。

コマンド	目的
Router(config)# **menu** *menu-name* **command** *menu-item command*	メニュー項目を選択したときに実行されるコマンドを指定します。

次に、OnRamp メニューの 3 つのエントリに関連付けられるコマンドを指定する例を示します。

```
Router(config)# menu OnRamp command 1 rlogin mailsys
Router(config)# menu OnRamp command 2 rlogin unix.cisco.com
Router(config)# menu OnRamp command 9 menu-exit
```

menu-exit コマンドは、メニューの中からだけ使用できます。このコマンドは、上位レベルのメニューへ戻るか、またはメニュー システムを終了するためにあります。

接続を確立できるメニュー項目の場合、そのメニュー項目には接続を再開するために使用できるエントリも含まれている必要があります。そのようなエントリが含まれていないと、接続からエスケープしてメニューに戻った後、セッションを再開する手段がありません。セッションは、ユーザがログアウトするまでアイドルになります。

ユーザが接続を再開できるようにメニュー エントリ内に **resume connection** ユーザ EXEC コマンドを構築するか、または **escape-char none** コマンドを使用して、ユーザがセッションからエスケープできないように回線を設定できます。

メニュー項目コマンドの一部として接続の再開を指定するには、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。

コマンド	目的
Router(config)# **menu** *menu-name* **command** *menu-item* **resume** [*connection*] **/connect** [*connect string*]	メニュー項目が選択されたときに **resume** コマンドが実行されることを指定します。

menu コマンドの中に **resume** コマンドを埋め込むと、ユーザは指名された接続を再開するか、またはその名前のアクティブな接続がなければ、指定された名前を使用して別の接続を確立できるようになります。オプションとして、初期接続に必要な接続ストリングを指定することも可能です。この接続ストリングを指定しない場合、指定された接続名がコマンドにより使用されます。

次のメニュー エントリで **resume** コマンドを使用できます。

- メニュー エントリに埋め込んで使用する。
- 独立した特定のメニュー エントリとして使用する。
- 複数の接続を順番に回る「ロータリー」メニュー エントリとして使用する。

次に、**menu** コマンドの中に **resume** コマンドが埋め込まれている例を示します。この例では、メニュー項目を選択すると、指定された接続セッションが（まだ開かれていなければ）開始されるか、または（すでに開かれたセッションがあれば）セッションが再開されます。

```
Router(config)# menu newmenu text 1 Read email
Router(config)# menu newmenu command 1 resume mailsys /connect rlogin mailsys
```

次に、特定の接続を再開するために、**resume** コマンドが独立したメニュー エントリ（エントリ 3）内で使用されている例を示します。

```
Router(config)# menu newmenu text 3 Resume UNIX Internet Access
Router(config)# menu newmenu command 3 resume unix.cisco.com
```

ユーザの接続リスト内の次の開いた接続を再開するには、**resume/next** コマンドを使用します。このコマンドにより、すべてのユーザ接続を進んでいく 1 つのメニュー エントリを作成できます。メニュー項目コマンドの一部として **resume/next** での接続の再開を指定するには、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。

コマンド	目的
Router(config)# **menu** *menu-name* **command** *menu-item* **resume/next**	**resume/next** での接続の再開を指定します。

次に、すべてのユーザ接続を進むために作成されたメニュー エントリ（エントリ 6）の例を示します。

```
Router(config)# menu newmenu text 6 Resume next connection
Router(config)# menu newmenu command 6 resume/next
```

メニューのデフォルト コマンドの指定

ユーザが項目を指定しないで Enter キーを押した場合、ルータによりデフォルト項目用のコマンドが実行されます。デフォルト項目を指定するには、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。

コマンド	目的
Router(config)# **menu** menu-*name* **default** *menu-item*	メニュー ユーザがメニュー項目を選択しなかった場合に実行されるコマンドを指定します。

サブメニューの作成

上位レベルのメニュー エントリを選択すると開くサブメニューを作成するには、**menu** コマンドを使用してライン メニュー エントリ内のメニューを呼び出します。サブメニュー項目コマンドを指定するには、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。

	コマンド	目的
ステップ 1	Router(config)# **menu** *menu-name* **text** *menu-item menu-text*	サブメニューを呼び出すメニュー項目を指定します。
ステップ 2	Router(config)# **menu** *menu-name* **command** *menu-item* **menu** *menu-name2*	メニュー項目が選択されたときに使用されるコマンドを指定します。
ステップ 3	Router(config)# **menu** *menu-name* **title** *delimiter menu-title delimiter*	サブメニューのタイトルを指定します。
ステップ 4	Router(config)# **menu** *menu-name* **text** *menu-item menu-text*	サブメニュー項目を指定します。
ステップ 5	Router(config)# **menu** *menu-name* **command** *menu-item command*	サブメニュー項目が選択されたときに使用されるコマンドを指定します。必要に応じてこのコマンドを繰り返します。

次に、OnRamp メニュー内のサブメニューがメニュー項目（エントリ 8）でアクティブ化されるように指定する例を示します。

```
Router(config)# menu OnRamp text 8 Set terminal type
```

次に、OnRamp メニュー内でメニュー項目（エントリ 8）が選択されたときに実行されるコマンドを指定する例を示します。

```
Router(config)# menu OnRamp command 8 menu Terminals
```

次に、Terminals サブメニューのタイトルを指定する例を示します。

```
Router(config)# menu Terminals title /
                    Supported Terminal Types

       Type a number to select an option;
      Type 9 to return to the previous menu.
```

次に、Terminals サブメニューのサブメニュー項目を指定する例を示します。

```
Router(config)# menu Terminals text 1 DEC VT420 or similar
Router(config)# menu Terminals text 2 Heath H-19
Router(config)# menu Terminals text 3 IBM 3051 or equivalent
Router(config)# menu Terminals text 4 Macintosh with gterm emulator
Router(config)# menu Terminals text 9 Return to previous menu
```

次に、Terminals サブメニューの項目に関連付けられるコマンドを指定する例を示します。

```
Router(config)# menu Terminals command 1 term terminal-type vt420
Router(config)# menu Terminals command 2 term terminal-type h19
Router(config)# menu Terminals command 3 term terminal-type ibm3051
Router(config)# menu Terminals command 4 term terminal-type gterm
Router(config)# menu Terminals command 9 menu-exit
```

メイン メニューでエントリ 8 を選択すると、次の Terminals サブメニューが表示されます。

```
     Supported Terminal Types

  Type a number to select an option;
```

```
Type 9 to return to the previous menu.

1     DEC VT420 or similar

2     Heath H-19

3     IBM 3051 or equivalent

4     Macintosh with gterm emulator

9     Return to previous menu
```

（注） メニューに多くのレベルをネストし過ぎると、システムにより端末にエラー メッセージが表示され、前のメニュー レベルに戻ります。

非表示メニュー エントリの作成

非表示メニュー エントリとは、選択キーは含まれているものの、実行されるアクションを説明するテキストがないメニュー項目のことです。ユーザにヘルプを提供するシステム管理者を支援するために、このタイプのメニュー エントリを含めます。通常の手順は、メニュー コマンドを指定し、項目のテキスト指定を省略します。非表示メニュー項目を作成するには、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。

コマンド	目的
Router(config)# **menu** *menu-name* **command** *menu-item command*	非表示メニュー エントリが選択されたときに使用されるコマンドを指定します。

次に、OnRamp メニューのサブメニュー エントリに関連付けられたコマンドの例を示します。

```
Router(config)# menu OnRamp command 7 show whoami
```

show whoami コマンドに追加テキストが付加されている場合、そのテキストが回線に関するデータの一部として表示されます。たとえば、このコマンドによって作成された非表示メニュー エントリ、

```
Router(config)# menu OnRamp command 7 show whoami Terminals submenu of OnRamp Internet
Access menu
```

は次のような情報を表示します。

```
Comm Server "cs101", Line 0 at 0 bps. Location "Second floor, West"
Additional data: Terminals submenu of OnRamp Internet Access menu
```

メニュー表示により画面がクリアされたときにこの情報が失われないようにするために、このコマンドは戻る前に常に --More-- プロンプトを表示します。

メニュー表示設定オプションの指定

menu clear-screen グローバル コンフィギュレーション コマンド（「メニュー タイトルの指定」の項で説明）に加えて、次の 3 つの **menu** コマンドによりメニュー機能が定義されます。

- **menu line-mode**
- **menu single-space**
- **menu status-line**

ライン モードで動作するメニューの設定

項目が 9 個以下のメニューでは、通常、項目の番号または文字を入力してメニュー項目を選択します。ライン モードでは、項目キーを入力して Enter キーを押すことで、メニュー エントリを選択します。ライン モードでは、Backspace キーで選択を取り消し、別の項目を選択してから Enter キーを押してコマンドを発行できます。この機能により、コマンドを呼び出す前に選択を変更できます。

ライン モードで動作するようにメニューを設定するには、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。

コマンド	目的
`Router(config)# menu menu-name line-mode`	メニュー項目の入力にライン モードを使用するようにメニューを設定します。

ラインモード オプションは、定義されているメニュー項目が 9 個を超える場合は自動的に呼び出されますが、項目が 9 個以下のメニューでも、明示的に設定できます。

選択キーとしてストリングを使用するには、**menu line-mode** コマンドをイネーブルにする必要があります。

シングルスペース メニューの表示

メニュー項目が 9 個以下の場合、Cisco IOS ソフトウェアは、通常、ダブルスペースで区切ってメニュー項目を表示します。項目が 9 個を超えるメニューでは、メニューを通常 24 行の端末画面に収めるために **single-space** オプションは自動的にアクティブになります。ただし、項目が 9 個以下のメニューでも、**single-space** オプションを明示的に設定できます。

single-space オプションを使用してシングルスペースで区切られたメニューを表示するには、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。

コマンド	目的
`Router(config)# menu menu-name single-space`	シングルスペース区切りで表示されるようにメニューを設定します。

情報ステータス行の表示

status-line オプションでは、メニュー タイトルが表示される前に、端末画面の一番上の行に現在のユーザに関するステータス情報が表示されます。ステータス行には、ルータのホスト名、ユーザの回線番号、および現在の端末のタイプとキーマップのタイプ（ある場合）が表示されます。

informational status line を表示するには、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。

コマンド	目的
`Router(config)# menu menu-name status-line`	ステータス行を表示するように指定されたメニューを設定します。

項目ごとのメニュー オプションの指定

項目ごとのメニュー オプションを設定するには、必要に応じてグローバル 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。

コマンド	目的
Router(config)# **menu** *menu-name* **options** *menu-item* **pause**	ユーザが指定されたメニュー項目を選択した後、一時停止するようにシステムを設定します。このコマンドは、一時停止するメニュー項目ごとに 1 回ずつ入力します。
Router(config)# **menu** *menu-name* **options** *menu-item* **login**	コマンドを実行する前に、ログインが要求されるように指定されたメニュー項目を設定します。このコマンドは、ログインを要求するメニュー項目ごとに 1 回ずつ入力します。

メニューの呼び出し

メニューを呼び出す（メニューにアクセスする）には、ユーザ EXEC モードまたは特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **menu** *menu-name*	設定済みのユーザ メニューを呼び出します。

特権 EXEC コマンドが含まれるメニューも定義できますが、そのメニューを起動するユーザは特権アクセスを持っている必要があります。

回線上でメニューが確実に自動的に呼び出されるようにするには、ユーザ自身では操作できないインターフェイスにユーザを取り残してしまう終了パスがメニューに含まれていないことを確認してから、**autocommand menu** *menu-name* ライン コンフィギュレーション コマンドでその回線を設定します（**autocommand menu** *menu-name* コマンドは、回線上でユーザが接続を開始したときに、**menu** *menu-name* コマンドが自動的に実行されるように回線を設定します）。

autocommand コマンドをローカル ユーザ名に定義することにより、ユーザ単位でメニューが呼び出されるようにすることもできます。

次に、OnRamp メニューが呼び出される例を示します。

```
Router# menu OnRamp

      Welcome to OnRamp Internet Services

       Type a number to select an option;
            Type 9 to exit the menu.

1     Read email

2     UNIX Internet access

3     Resume UNIX connection


6     Resume next connection

9     Exit menu system
```

コンフィギュレーションからのメニューの削除

コンフィギュレーションからメニューを削除するには、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。

コマンド	目的
`Router(config)# no menu menu-name`	メニュー名を指定してメニューを削除します。

メニューを再度使用するには、メニュー全体を再設定する必要があります。

次に、コンフィギュレーションから OnRamp メニューを削除する例を示します。

```
Router(config)# no menu OnRamp
```

接続管理、システム バナー、およびユーザ メニュー コンフィギュレーションの例

ここでは、次の例について説明します。

ログイン ユーザ名およびパスワードの変更：例

次に、ログイン ユーザ名およびパスワードの変更方法の例を示します。この例では、user1 というユーザ名で現在ログインしているユーザが、ログイン名を user2 に変更しようとしています。**login** コマンドを入力した後、ユーザは新しいユーザ名を入力していますが、誤ったパスワードを入力しています。入力したパスワードが元のパスワードと一致しないため、システムによりユーザ名の変更が拒否されます。

```
Router> login
Username: user2
Password:
% Access denied
Still logged in as "user1"
```

次に、ユーザは user2 というユーザ名を使用して再びログインの変更を試み、今回は正しい（元の）パスワードを入力します。今度はパスワードが現在のログイン情報に一致したため、ログイン ユーザ名が user2 に変更され、ユーザはユーザ ログイン情報にアクセスすることを許可されました。

```
Router> login
Username: user2
Password:
Router>
```

他の端末へのメッセージの送信：例

次に、ルータのすべての端末接続へメッセージを送信する例を示します。

```
Router# send *
Enter message, end with CTRL/Z; abort with CTRL/C:
this is a message^Z
Send message? [confirm]
Router#


***
***
*** Message from tty50 to all terminals:
***
this is a message


Router#
```

TCP/IP 接続のクリア：例

次に、TTY 回線番号を使用して TCP 接続をクリアする例を示します。**show tcp** EXEC コマンドにより、**clear tcp** 特権 EXEC コマンド モードで使用された回線番号（TTY2）が表示されます。

```
Router# show tcp

    tty2, virtual tty from host router20.cisco.com
    Connection state is ESTAB, I/O status: 1, unread input bytes: 0
    Local host: 171.69.233.7, Local port: 23
    Foreign host: 171.69.61.75, Foreign port: 1058

    Enqueued packets for retransmit: 0, input: 0, saved: 0

    Event Timers (current time is 0x36144):
    Timer          Starts    Wakeups            Next
    Retrans             4          0             0x0
    TimeWait            0          0             0x0
    AckHold             7          4             0x0
    SendWnd             0          0             0x0
    KeepAlive           0          0             0x0
    GiveUp              0          0             0x0
    PmtuAger            0          0             0x0

    iss: 4151109680  snduna: 4151109752  sndnxt: 4151109752     sndwnd:  24576
    irs: 1249472001  rcvnxt: 1249472032  rcvwnd:       4258  delrcvwnd:     30

    SRTT: 710 ms, RTTO: 4442 ms, RTV: 1511 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 300 ms

Router# clear tcp line 2

    [confirm]
     [OK]
```

次に、ローカル ルータのホスト名とポート、およびリモート ルータのホスト名とポートを指定することにより、TCP 接続をクリアする例を示します。**show tcp brief** 特権 EXEC コマンドにより、**clear tcp** 特権 EXEC コマンド内で使用するローカル（Local Address）およびリモート（Foreign Address）のホスト名およびポートが表示されます。

```
Router# show tcp brief

    TCB       Local Address           Foreign Address        (state)
    60A34E9C  router1.cisco.com.23      router20.cisco.1055  ESTAB

Router# clear tcp local router1 23 remote router20 1055

    [confirm]
     [OK]
```

次に、TCB アドレスを使用して TCP 接続をクリアする例を示します。**show tcp brief** EXEC コマンドにより、**clear tcp** EXEC コマンド内で使用する TCB アドレスが表示されます。

```
Router# show tcp brief

    TCB       Local Address           Foreign Address        (state)
    60B75E48  router1.cisco.com.23      router20.cisco.1054  ESTAB

Router# clear tcp tcb 60B75E48

    [confirm]
     [OK]
```

バナーの設定：例

次に、**banner** 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、サーバに新しいソフトウェアがリロードされようとしていることをユーザに通知する方法の例を示します。**no exec-banner** ライン コンフィギュレーション コマンドは、VTY 回線上の EXEC バナーと Message-of-The-Day バナーをディセーブルにするために使用されます。

```
!
line vty 0 4
 no exec-banner
!
banner exec /
 This is Cisco Systems training group router.

 Unauthorized access prohibited.
 /
!
banner incoming /
 You are connected to a Hayes-compatible modem.

 Enter the appropriate AT commands.
 Remember to reset anything you have changed before disconnecting.
 /
!
banner motd /
 The router will go down at 6pm today for a software upgrade
 /
```

ユーザがルータに接続すると、ログイン プロンプトの前に MOTD バナーが表示されます。ユーザがルータにログインした後、接続のタイプに応じて EXEC バナーまたは着信バナーがルータに表示されます。リバース Telnet ログインの場合、ルータに着信バナーが表示されます。その他すべての接続の場合、ルータに EXEC バナーが表示されます。

バナー トークンを使用した SLIP-PPP バナーの設定：例

次に、複数のトークンと区切り文字であるパーセント記号（%）を使用して SLIP-PPP バナーを設定する例を示します。

```
Router(config)# banner slip-ppp %

Enter TEXT message.  End with the character '%'.
Starting $(encap) connection from $(gate-ip) to $(peer-ip) using a maximum packet size of
$(mtu) bytes... %
```

ユーザが **slip** コマンドを使用すると、ユーザは次のバナーを見ることになります。**$(***token***)** 構文が対応する設定変数に置き換えられていることに注意してください。

```
Starting SLIP connection from 192.168.69.96 to 172.16.80.8 using a maximum packet size of
1500 bytes...
```

メニューの設定：例

次に、メニュー ユーザが Telnet を使用して 3 つの異なるマシンのいずれかにアクセスすることを許可する例を示します。ユーザは **show user** EXEC コマンドの出力を表示してメニューを終了することもできます。システム管理者は、1 つの非表示メニュー項目（`menu new command here show version` として設定）で現在のソフトウェア バージョンを表示できます。

```
menu new title ^C


              Telnet Menu


^C
menu new prompt ^C

Please enter your selection: ^C
menu new text 1 telnet system1
menu new command 1 telnet system1
menu new options 1 pause
menu new text 2 telnet system2
menu new command 2 telnet system2
menu new options 2 pause
menu new text b telnet system3
menu new command b telnet system3
menu new options b pause
menu new text me show user
menu new command me show user
menu new options me pause
menu new command here show version
menu new text Exit Exit
menu new command Exit menu-exit
menu new clear-screen
menu new status-line
menu new default me
menu new line-mode
!
```

Cisco Web ブラウザ ユーザ インターフェイスの使用

Cisco IOS ソフトウェアには、Cisco IOS コマンドを発行できる Web ブラウザ ユーザ インターフェイス（UI）が含まれています。Cisco IOS Web ブラウザ UI はルータのホーム ページからアクセスでき、ビジネス環境に合わせてカスタマイズできます。たとえば、異なる言語でページを表示したり、フラッシュ メモリにページを保存して簡単に取得したりできます。この章では、Cisco Web ブラウザ UI の使用方法とカスタマイズに関する作業について説明します。

この章の Cisco Web ブラウザ UI コンフィギュレーション コマンドの完全な説明については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「Cisco IOS Web Browser User Interface Commands」の章を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index*』を使用するかオンラインで検索します。

Cisco Web ブラウザ UI 作業リスト

システムの Cisco IOS ソフトウェアが生成したホーム ページに接続して、Web ブラウザを使用して、Cisco IOS コマンドのほとんどを発行できます。大部分の Cisco ルータとアクセス サーバは HTTP サーバがデバイスでイネーブルになるときに、自動的にパスワード保護されたホーム ページを生成します。ホーム ページにアクセスするには、コンピュータがルータと同じネットワークになければなりません。

Cisco Web ブラウザ UI を使用するには、ワールド ワイド ウェブ ブラウザ アプリケーションが必要です。Cisco Web ブラウザ UI は、Internet Explorer や Netscape Navigator をはじめとするほとんどの Web ブラウザで動作します。Web ブラウザはフォームの読み込みと送信ができなければなりません。

Cisco Web ブラウザ UI を使用するには、次の項の作業を実行します。

- 「Cisco Web ブラウザ UI のイネーブル化」（必須）
- 「Cisco Web ブラウザ UI へのアクセス設定」（必須）
- 「Cisco Web ブラウザ UI のアクセスと使用」（必須）
- 「Cisco Web ブラウザ UI のカスタマイズ」（任意）

Cisco Web ブラウザ UI のイネーブル化

Web ブラウザ UI は Cisco 1003、Cisco 1004、Cisco 1005 ルータで自動的にイネーブルになり、ClickStart を使用してルータを設定できます。その他のすべてのシスコ デバイスでは、このマニュアルで説明する方法で Cisco Web ブラウザ UI をイネーブルにする必要があります。

Cisco Web ブラウザ UI をイネーブルにするには、ルータ上で HTTP サーバをイネーブルにする必要があります。HTTP サーバをイネーブルにするには、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。

コマンド	目的
`Router(config)# ip http server`	システムで HTTP サーバ（Web サーバ）をイネーブルにします。

Cisco Web ブラウザ UI へのアクセス設定

Cisco Web ブラウザ UI へのアクセスを制御するには、HTTP サーバの認証方式を指定し、HTTP サーバにアクセス リストを適用してから、次の項で説明する方法で HTTP サーバのポート番号を割り当てます。

ユーザ認証方式の指定

HTTP サーバのユーザ認証方式を指定するには、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。

コマンド	目的
`Router(config)# ip http authentication {aaa | enable | local | tacacs}`	HTTP サーバのユーザ認証方式を指定します。

ip http authentication コマンドは、クライアントが HTTP サーバに接続するときにログインで使用する認証方式を指定します。**ip http authentication aaa** コマンド オプションの使用を推奨します。**enable**、**local**、および **tacacs** 方式は **aaa authentication login** コマンドを使用して指定する必要があります。

このコマンドを使用しない場合は、デフォルトの認証方式が使用されます。HTTP サーバのデフォルトの認証方式は、設定された「enable」パスワードを使用することです。「enable」パスワードは **enable password** グローバル コンフィギュレーション コマンドで設定されます。enable password を HTTP サーバ ログイン認証方式として使用する場合は、クライアントはデフォルトの特権レベル 15 を使用して HTTP サーバに接続します。

（注） 「enable」パスワードを HTTP サーバ ログイン認証方式として使用する場合は、入力したユーザ名は無視され、サーバは「enable」パスワードだけを検証します。このため攻撃者によるルータへのアクセスが簡単になる可能性があります。ユーザ名とパスワードの組み合わせは認証でパスワードだけを使用する場合に比べよりセキュアなため、認証で「enable」パスワードだけを使用することは決して推奨しません。代わりに、グローバル Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）フレームワークの一部で設定されている **local** または **tacacs** 認証オプションを使用することを推奨します。
AAA ポリシーの一部として HTTP アクセスを設定するには、**ip http authentication aaa** コマンド オプションを使用します。「local」、「tacacs」、「enable」認証方式は、**aaa authentication login** コマンドを使用して設定する必要があります。

ローカル ユーザ名データベースにユーザを追加する方法については、『*Cisco IOS Security Configuration Guide*』を参照してください。

例：HTTP サーバ認証方式の設定

次に、AAA で設定した方式を使用して HTTP サーバ ユーザ認証を実行するように指定する例を示します。AAA ログイン方式は、「local」ユーザ名 / パスワード認証方式として設定されます。

```
Router(config)# ip http authentication aaa
Router(config)# aaa authentication login default local
```

HTTP サーバへのアクセス リストの適用

Cisco Web ブラウザ UI が使用する HTTP サーバにアクセスするホストを制御するには、HTTP サーバにアクセス リストを適用します。HTTP サーバにアクセス リストを適用するには、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。

コマンド	目的
`Router(config)# ip http access-class {access-list-number | access-list-name}`	Cisco IOS ClickStart ソフトウェアまたは Cisco Web ブラウザ ユーザ インターフェイスが使用する HTTP サーバにアクセス リストを適用します。

例：HTTP サーバ アクセスのアクセス リストの設定

次に、「20」として指定されたアクセス リストを定義して HTTP サーバに割り当てる例を示します。

```
Router(config)# ip access-list standard 20
Router(config-std-nacl)# permit 209.165.202.0 0.0.0.255
Router(config-std-nacl)# permit 209.165.0.0 0.0.255.255
Router(config-std-nacl)# permit 209.0.0.0 0.255.255.255
! (Note: all other access implicitly denied)
Router(config-std-nacl)# exit
Router(config)# ip http access-class 20
```

HTTP サーバ ポート番号の変更

デフォルトでは、HTTP サーバはルータ上でポート 80 を使用します。Cisco Web ブラウザ UI を別のポートに割り当てるには、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。

コマンド	目的
`Router(config)# ip http port number`	Cisco Web ブラウザ インターフェイスが使用するポート番号を割り当てます。

Cisco Web ブラウザ UI のアクセスと使用

この項では、Cisco Web ブラウザ UI にアクセスし、コマンドを発行するための作業について説明します。

ルータ ホーム ページへのアクセス

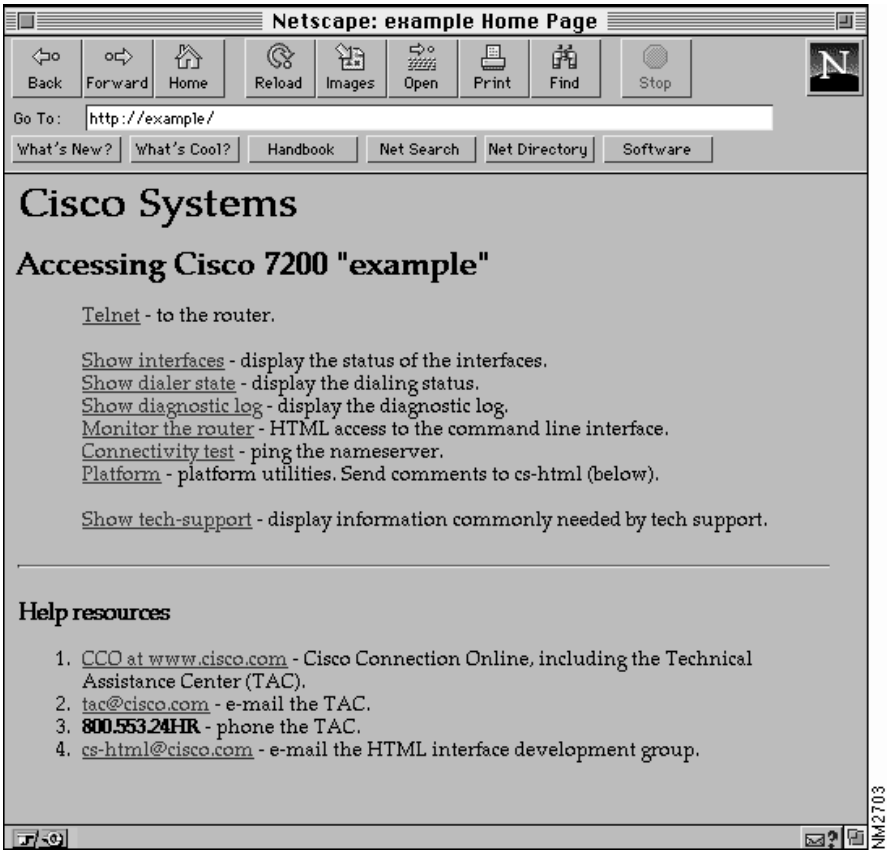
ルータ ホーム ページにアクセスするには、次の手順を実行します。

ステップ 1 Web ブラウザの URL フィールドに **http://***router-name***/** と入力し、**Return** キーを押します（たとえば、cacophony という名前の Cisco ルータにアクセスする場合は **http://cacophony/**）。この後、ブラウザはパスワード プロンプトを表示します。

ステップ 2 パスワードを入力します。必要なパスワードは HTTP サーバで（**ip http authentication** 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）設定されたユーザ認証方式によって異なります。

パスワードを入力した後、ルータ ホーム ページがブラウザに表示されます。図 7 にルータ ホーム ページの例を示します。

図 7　　Cisco 7200 シリーズ ルータのホーム ページの例



ルータ ホーム ページにアクセスするときのデフォルト特権レベルは 15（グローバル アクセス）です。特権レベルがルータで設定され、15 以外の特権レベルが割り当てられている場合は、特権レベルを指定して、ルータ ホーム ページにアクセスする必要があります。

特権レベルを指定すると、Cisco Web ブラウザ UI が表示され、ユーザ レベルで定義されたコマンドだけを許可します（特権レベルの詳細については、『Release 12.2 *Cisco IOS Security Configuration Guide*』の「Configuring Passwords and Privileges」の章を参照してください）。

デフォルトの 15 以外に割り当てられた特権レベルのルータ Web ページにアクセスするには、次の手順を実行します。

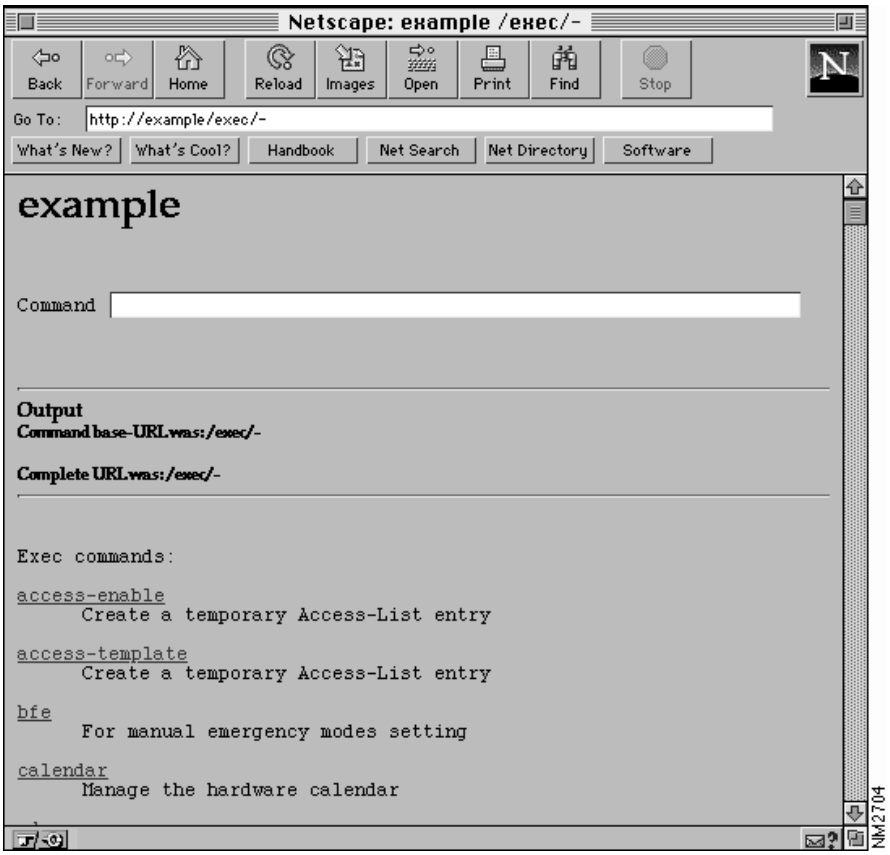
ステップ 1　Web ブラウザの URL フィールドに **http://***router-name***/level/***level***/exec** と入力し、**Return** キーを押します。たとえば、cacophony という名前の Cisco ルータでユーザ特権レベル 12 で EXEC モードへのアクセス要求をするには、**http://cacophony/level/12/exec** と入力します。ブラウザはユーザ名とパスワード入力プロンプトを表示します。

ステップ 2　ユーザ名とパスワードを入力して、**Return** キーを押します。必要なパスワードは HTTP サーバで設定されたユーザ認証方式によって異なります。Web ブラウザはユーザ特権レベルに合った Web ページを表示します。

Cisco Web ブラウザ UI を使用したコマンドの発行

ルータ ホーム ページから、[Monitor the Router] というハイパーテキスト リンクをクリックします。このリンクで [Command] フィールドがある Web ページに移動します。例を 図 8 に示します。Cisco IOS コマンドライン インターフェイスを使用してコマンドを入力する場合と同じ方法で、コマンド フィールドにコマンドを入力できます。ページにはコマンドのリストも表示されます。ハイパーテキスト リンクをクリックするように、コマンドをクリックして実行できます。

図 8　　example という名前のルータのコマンド フィールド Web ページ



ハイパーテキスト リンクを使用したコマンドの入力

ハイパーテキスト リンクを使用してコマンドを入力するには、画面の下部のコマンド一覧をスクロールして、実行するコマンドをクリックします。リンクが完全なコマンドの場合は実行されます。コマンドにパラメータが必要な場合は、別のコマンド ハイパーテキスト リンクのリストが表示されます。この次のリストをスクロールして実行するものをクリックします。

show EXEC コマンドなどコマンドが情報要求の場合は、情報が Web ブラウザ ウィンドウに表示されます。

コマンドに変数が必要な場合は、変数入力フォームが表示されます。

コマンド フィールドを使用したコマンドの入力

コマンド フィールドを使用したコマンドの入力は端末コンソールでの入力方法と類似しています。『Cisco IOS Command Reference』にある構文を使用してコマンドを入力します。特定のコマンドで利用可能なオプションがわからない場合は、疑問符（**?**）を入力します。

たとえば、コマンド フィールドに **show ?** と入力すると、**show** EXEC コマンドのパラメータが表示されます。Cisco Web ブラウザ UI にはハイパーテキスト リンクとしてパラメータが表示されます。パラメータを選択するには、リンクのいずれかをクリックするか、コマンド フィールドにパラメータを入力します。

URL ウィンドウを使用したコマンドの入力

Web ブラウザの URL ウィンドウを使用してコマンドを発行できます。URL ウィンドウを使用してコマンドを発行するには、次の構文を使用します。

http://*router-name*/[**level/***level*/]*command-mode*/*command*

表 13 に、Web ページを要求するときに使用する必要がある URL 引数の一覧を示します。

表 13　　Web ブラウザ URL 引数の説明

引数	説明
router-name	設定するルータ名。
level/*level*	（任意）アクセス要求時に要求している特権レベル。
mode	EXEC、コンフィギュレーション、インターフェイスなどコマンドを実行するモード。
command	実行するコマンド。フォワード スラッシュを使用してコマンド構文のスペースを置換します。URL でコマンドを指定しない場合は、ブラウザには指定されたコマンド モードで利用可能なすべてのコマンド一覧 Web ページが表示されます。

たとえば、example という名前のルータで **show running-configuration** EXEC コマンドを実行するには、URL ウィンドウに次を入力します。

```
http://example/exec/show/running-configuration
```

このコマンドを発行すると、Cisco Web ブラウザ UI がルータの実行コンフィギュレーションを表示します。

[Command] フィールドでのコマンドの入力と URL ウィンドウでの入力の違いは、URL ウィンドウではコマンド構文のスペースの代わりにフォワード スラッシュを使用する必要があるという点です。

Cisco Web ブラウザ UI のカスタマイズ

Cisco Web ブラウザ UI が使用する HTML ページをカスタマイズして、Cisco IOS コマンド出力と Cisco IOS プラットフォーム固有の変数（ルータのホスト名やルータのアドレスなど）を表示できます。カスタム HTML ページに挿入される HTML 形式の Server Side Include（SSI）を使用してこの情報を表示できます。主に PDS の FEAT-106（IOS インターナショナル）および FEAT-108（HTTP セキュリティ）を参照してください。EDCS の機能仕様書の『ENG-11035』も参照してください。詳細な計画については、『ENG-84169』を参照してください。

SSI の概要

SSI は HTML 形式のコマンドまたは変数で、Web ブラウザの Cisco IOS プラットフォーム コンフィギュレーション ページをカスタマイズするときに HTML ページに挿入します。これらの SSI コマンドと SSI 変数は Cisco IOS コマンド出力と Cisco IOS プラットフォーム固有の変数を表示します。

（注） この項で説明するカスタマイズ機能の大部分は、Cisco 1000 シリーズ、Cisco 1003/1004 シリーズ、Cisco 1005 シリーズ ルータ専用の ClickStart EZsetup 機能向けです。

Cisco IOS ソフトウェアは HTML ページのカスタマイズ用の 2 つの HTML SSI コマンド（SSI EXEC コマンドと SSI ECHO コマンド）をサポートしています。SSI EXEC コマンドの HTML 形式は、**<!--#exec cmd="***xxx***"-->** であり、SSI ECHO コマンドの HTML 形式は、**<!--#echo var="***yyy***"-->** です（これらのコマンドの使用方法については、この章の後半の「SSI を使用した HTML ページのカスタマイズ」の項を参照してください）。

この 2 つの SSI コマンドに加え、Cisco IOS ソフトウェアは HTML ページのカスタマイズ用に定義された複数の SSI 変数をサポートします。SSI 変数は SSI ECHO コマンドとともに使用します。1 つの SSI 変数はすべての Cisco IOS プラットフォーム（SERVER_NAME）に対して定義され、その他の SSI 変数は特に ISDN、フレーム リレー、非同期シリアル プラットフォーム向けに定義されています。すべての利用可能な SSI 変数の形式と説明については、表 14 を参照してください（SSI ECHO コマンドとともにこれらの SSI 変数を使用する方法については、この章の後半の「SSI を使用した HTML ページのカスタマイズ」の項を参照してください）。

SSI EXEC コマンドはすべてのプラットフォームでサポートされています。SSI 変数と使用する SSI ECHO コマンドは、表 14 の一覧にあるすべてのプラットフォームでサポートされています。

表 14　SSI 変数の説明

HTML 形式の SSI 変数	ブラウザ ページに表示される変数の説明	Cisco IOS プラットフォーム。この SSI は次でサポートされています。
SERVER_NAME	HTTP サーバのホスト名。	すべての Cisco IOS プラットフォーム
EZSETUP_PASSWORD	パスワードをイネーブルにします（現在はブランク）。	Cisco 1000 シリーズ
EZSETUP_PASSWORD_VERIFY	enable password を繰り返し正確性を検証します（現在はブランク）。	Cisco 1000 シリーズ
EZSETUP_ETHERNET0_ADDRESS	イーサネット インターフェイス 0 の IP アドレス。	Cisco 1000 シリーズ
EZSETUP_ETHERNET0_MASK	イーサネット インターフェイス 0 の IP マスク。	Cisco 1000 シリーズ
EZSETUP_DNS_ADDRESS	ルータが使用する Domain Name System（DNS; ドメイン ネーム システム）アドレス。	Cisco 1000 シリーズ
EZSETUP_STANDARD_DEBUG_Y	標準デバッグ変数。TRUE に設定すると CHECKED を返します。そうでない場合はブランクです。	Cisco 1000 シリーズ
EZSETUP_STANDARD_DEBUG_N	標準デバッグ変数。FALSE に設定すると CHECKED を返します。そうでない場合はブランクです。	Cisco 1000 シリーズ
EZSETUP_ISDN_SWITCHTYPE	ISDN スイッチ タイプ。	Cisco 1003 および Cisco 1004

表 14　SSI 変数の説明 （続き）

HTML 形式の SSI 変数	ブラウザ ページに表示される変数の説明	Cisco IOS プラットフォーム。この SSI は次でサポートされています。
EZSETUP_ISDN_REMOTE_NAME	リモート ISDN システム名。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_REMOTE_NUMBER	リモート ISDN システムの電話番号。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_CHAP_PASSWORD	リモート ISDN システムの CHAP パスワード。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_SPID1	ISDN SPID 1。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_SPID2	ISDN SPID 2。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_SPEED_56	ISDN インターフェイスの速度。56K に設定すると CHECKED を返します。そうでない場合はブランクです。	Cisco 1003 および Cisco 1004
EZSETUP_ISDN_SPEED_64	ISDN インターフェイスの速度。64K に設定すると CHECKED を返します。そうでない場合はブランクです。	Cisco 1003 および Cisco 1004
EZSETUP_FR_ADDRESS	フレーム リレー IP アドレス。	Cisco 1005
EZSETUP_FR_MASK	フレーム リレー IP マスク。	Cisco 1005
EZSETUP_FR_DLCI	フレーム リレー DLCI。	Cisco 1005
EZSETUP_ASYNC_REMOTE_NAME	リモート システム名。	Cisco 1005
EZSETUP_ASYNC_REMOTE_NUMBER	リモート システムの電話番号。	Cisco 1005
EZSETUP_ASYNC_CHAP_PASSWORD	リモート システムの CHAP パスワード。	Cisco 1005
EZSETUP_ASYNC_LINE_PASSWORD	非同期回線パスワード。	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED	非同期モデムの速度（14.4K または 28.8K）。	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_144K	非同期モデムの速度が 14.4K の場合は、CHECKED を返します。そうでない場合はブランクです。	Cisco 1005
EZSETUP_ASYNC_MODEM_SPEED_288K	非同期モデムの速度が 28.8K の場合は、CHECKED を返します。そうでない場合はブランクです。	Cisco 1005

SSI を含む HTML ページ セットを設計したら、これらのページを Cisco IOS プラットフォームのフラッシュ メモリにコピーできます。フラッシュ メモリからこれらのページを取得して、Web ブラウザで表示すると、これらのページに設計された SSI コマンドは Cisco IOS コマンド出力、あるいは現行の変数または 表 14 で定義された ID のいずれかを表示します。たとえば、SSI ECHO コマンドと変数 SERVER_NAME は現在使用している HTTP サーバのホスト名を表示し、SSI ECHO コマンドと変数 EZSETUP_ISDN_SWITCHTYPE は現在使用している ISDN スイッチを表示します。

SSI を使用すると、HTML ページ セットをカスタマイズして、英語以外の言語を表示し、これらのページを複数の Cisco IOS プラットフォーム上のフラッシュ メモリにコピーできます。Cisco IOS プラットフォームのフラッシュ メモリからこれらのページを取得すると、現在使用しているプラットフォームに関連付けられた変数と ID が表示されます。SSI を使用すると、これらの国際ページ（8 ビットまたは複数バイト文字を含む比較的大規模なイメージと見なされます）を複製し、使用している各プラットフォームのソース コードに保存する必要がなくなります。

SSI を使用した HTML ページのカスタマイズ

Web ブラウザの HTML ページをカスタマイズするときには、HTML ファイルの、ブラウザ ページで Cisco IOS コマンド出力を表示する場所に **<!--#exec md=***"xxx"***->** と入力します。*xxx* 変数の部分は任意の Cisco IOS EXEC モード コマンドで置き換えます。

Web ブラウザの HTML ページをカスタマイズするときには、HTML ファイルの、ブラウザ ページで特定の Cisco IOS プラットフォーム（ISDN またはフレーム リレー プラットフォームなど）に関連付ける値または ID を表示する場所に **<!--#echo var="***yyy***"-->** と入力します。*yyy* 変数の部分は 表 14 に示す SSI 変数で置き換えます。

HTML ページのフラッシュ メモリへのコピー

SSI を使用して HTML ページをカスタマイズした場合、HTML ページを Cisco IOS プラットフォームのフラッシュ メモリにコピーします。これを行うには、「.shtml」が付いたファイル名（*filename*.shtml など）を使用してページを保存し、**copy** EXEC コマンド（**copy tftp flash** コマンドなど）を使用してファイルをフラッシュ メモリにコピーします（使用中のプラットフォームに対応する **copy** コマンドについては、『Cisco IOS Command References』を参照してください）。

SSI を含む HTML ファイルの表示

Cisco Web ブラウザ UI をイネーブルにすると、フラッシュ メモリから HTML ページを取得し、URL ウィンドウに **http://***router***/flash/***filename* と入力して Cisco Web ブラウザで表示できます。*router* の部分は現在使用している Cisco IOS プラットフォームのホスト名または IP アドレスで置き換え、*filename* は「.shtml」を付けて作成したファイル名（http://myrouter/flash/ssi_file.shtml など）に置き換えます。

Cisco Web ブラウザ UI カスタマイズ例

ここでは、次の例について説明します。

- 「SSI EXEC コマンドの使用例」
- 「SSI ECHO コマンドの使用例」

SSI EXEC コマンドの使用例

次に、HTML SSI EXEC コマンドを使用して、コマンドを実行する例を示します。この例では、Cisco IOS **show users** EXEC コマンドを実行します。

フラッシュ メモリ内の HTML ファイルの内容は次のとおりです。

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
<PRE>
<!--#exec cmd="show users"-->
</PRE>
```

```
<BR>
</BODY>
</HTML>
```

HTML ファイルをフラッシュ メモリから取得するときに、Web ブラウザが取得する内容は次のとおりです。

```
<HTML>
<HEAD>
<TITLE> SSI EXEC Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI EXEC command
<HR>
USERS:<BR>
<PRE>

Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com

</PRE>
<BR>
</BODY>
</HTML>
```

Web ブラウザは次のテキストを表示します。

```
This is an example of the SSI EXEC command
----------------------------------------
USERS:
Line    User  Host(s) Idle  Location
0 con 0       idle      12
2 vty 0       idle       0  router.cisco.com
```

SSI ECHO コマンドの使用例

次に、HTML SSI ECHO コマンドと SSI 変数 *SERVER_NAME*（表 5 を参照）を使用して Cisco IOS プラットフォームのホスト名「rain」を表示する例を示します。

フラッシュ メモリ内の HTML ファイルの内容は次のとおりです。

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
<!--#echo var="SERVER_NAME"-->
<BR>
</BODY>
</HTML>
```

HTML ファイルをフラッシュ メモリから取得するときに、Web ブラウザが取得する内容は次のとおりです。

```
<HTML>
<HEAD>
<TITLE>SSI Echo Command Example</TITLE>
```

```
</HEAD>
<BODY>
This is an example of the SSI echo command
<HR>
The name of this server is:<BR>
rain
<BR>
</BODY>
</HTML>
```

Web ブラウザは次のテキストを表示します。

```
This is an example of the SSI echo command
----------------------------------------
The name of this server is:
rain
```

Cisco IOS 統合ファイル システムの使用

Cisco IOS 統合ファイル システムの使用

この章では、現在のルーティング デバイスで使用可能なすべてのファイル システムで単一のインターフェイスが使用できる Cisco IOS File System（IFS）機能について説明します。次のものを含みます。

- フラッシュ メモリ ファイル システム
- ネットワーク ファイル システム（TFTP、rcp、FTP）
- その他、すべてのデータ読み取り、書き込み用エンドポイント（NVRAM、実行コンフィギュレーション、ROM、RAW システム メモリ、システム バンドル マイクロコード、X モデム、フラッシュ ロード ヘルパー ログ、モデム、BRI 多重化デバイス（mux）インターフェイスなど）

本章の IFS コマンドの詳細な説明については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「File Management Commands」にある「Cisco IOS File System Commands」の章を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index*』を使用するかオンラインで検索します。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。詳細については、「About Cisco IOS Software Documentation」の章の「Identifying Platform Support for Cisco IOS Software Features」の項を参照してください。

IFS 使用および管理作業のリスト

この章では、Cisco IFS を使用して実行できる、ファイル管理の作業について説明します。IFS についての情報と、オプションのファイル管理作業について、次の項で説明します。

- 「IFS の概要」
- 「URL を使用したファイルのコピー」
- 「コマンド内での URL の使用」
- 「ファイル システムの管理」
- 「フラッシュ メモリ ファイル システム タイプ」
- 「リモート ファイル システムの管理」
- 「NVRAM ファイル システムの管理」
- 「System ファイル システムの管理」

IFS の概要

次の項で、IFS の機能と利点を説明します。

ファイルの表示と分類

IFS を使用して、リモート サーバにあるファイルも含め、すべてのファイルを表示し、分類する（画像やテキスト ファイルなど）ことができます。たとえば、リモートのサーバにある画像ファイルをコピーする前に、有効な画像ファイルであることを確認するため、サイズや画像の種類を明確にする場合があります。リモート サーバにあるコンフィギュレーション ファイルを表示して、正しいコンフィギュレーション ファイルであることをルータにロードする前に確認することもできます。

プラットフォームに依存しないコマンド

IFS を使用すれば、ファイル システムのユーザ インターフェイスはプラットフォームに依存しなくなります。使用されているプラットフォームにかかわらず、コマンドの構文は同一になります。このため、どのルータでも同じコマンドを使用することが可能になります。

ただし、どのプラットフォームとファイル システムでもすべてのコマンドがサポートされているわけではありません。ファイル システムはそれぞれ異なる動作をサポートしているため、コマンドによっては一部のファイルシステムで使用できないことがあります。プラットフォームは、使用しているファイル システムのコマンドをサポートします。

コマンドの入力要求の最小化

IFS では、多くのコマンドで入力要求が最小化されています。**copy** EXEC コマンドはその一例です。システムが要求したときに情報を入力するのではなく、必要な情報をすべてコマンド ラインに入力することができます。たとえば、ファイルを FTP サーバにコピーする場合、ソース ファイルのルータ上の位置、コピー先ファイルの FTP サーバ上の位置、さらに FTP サーバ接続時に使用するユーザ名とパスワードまでを 1 行で指定することができます。ただし、最小限の形でコマンドを入力することで、必要な情報をルータのプロンプトで入力するようにもできます。

現在の **file prompt** グローバル コンフィギュレーション コマンドの設定、および入力したコマンドの種類によっては、すべての情報をコマンドとともに入力した場合でも、ルータが確認のプロンプトを表示する場合があります。その場合、デフォルト値はコマンドで入力された値になります。値を確認するには、Enter キーを押します。

ディレクトリの作成と移動

IFS を使用して、さまざまなディレクトリやディレクトリ内のファイルのリストへ移動できます。最近のプラットフォームでは、フラッシュ メモリやディスクにサブディレクトリを作成することもできます。

URL を使用したファイルのコピー

新しいファイル システム インターフェイスでは、ファイルの位置の指定に Uniform Resource Locator（URL; ユニフォーム リソース ロケータ）を使用します。URL は、ワールドワイド ウェブ上でファイルや位置の指定に広く使用されています。シスコのルータでは、ルータやリモートのファイル サーバにあるファイルの位置の指定に使用できるようになりました。

シスコのルータでは、ファイルやディレクトリの位置を指定するために、コマンド内で URL を使用します。たとえば、ファイルをある位置から他の位置へコピーする場合、**copy** *source-url destination-url* EXEC コマンドを使用します。

ルータで使用される URL の形式は、これまで使い慣れた形式と異なる場合があります。また、ファイルの位置によって、さまざまな形式を使用できます。

URL を使用したファイルのコピーについては、次の項で説明されています。

ネットワーク サーバ上のファイルの指定

ネットワーク サーバ上のファイルを指定するには、次の形式のいずれかを使用します。

- **ftp:**[[//[*username*[:*password*]@]*location*]/*directory*]/*filename*
- **rcp:**[[//[*username*@]*location*]/*directory*]/*filename*
- **tftp:**[[//*location*]/*directory*]/*filename*

location は、IP アドレスまたはホスト名です。*username* 変数でユーザ名を指定した場合、**ip rcmd remote-username** や **ip ftp username** グローバル コンフィギュレーション コマンドで指定したユーザ名を上書きします。*password* で指定するパスワードは、**ip ftp password** グローバル コンフィギュレーション コマンドで指定したパスワードを上書きします。

ファイル パス（ディレクトリとファイル名）は、ファイル転送に使用されたディレクトリからの相対パスで指定します。たとえば、UNIX ファイル サーバでは、TFTP パス名は /tftpboot ディレクトリから始まり、rcp および FTP パスはユーザ名に関連付けられたホーム ディレクトリから始まります。

次の例では、myserver.cisco.com という名前の TFTP サーバ上にある c7200-j-mz.112-current という名前のファイルを指定しています。ファイルは /tftpboot/master というディレクトリ内に位置しています。

```
tftp://myserver.cisco.com/master/c7200-j-mz.112-current
```

次の例では、enterprise.cisco.com という名前のサーバ上にある mill-config という名前のファイルを指定しています。ルータは、ユーザ名 liberty とパスワード secret を使用して、FTP でこのサーバにアクセスします。

```
ftp://liberty:secret@enterprise.cisco.com/mill-config
```

ローカル ファイルの指定

ルータ上にあるファイルを指定するには、*prefix*:[*directory*/]*filename* という構文を使用します。フラッシュ メモリや NVRAM にあるファイルを指定するために、この構文を使用できます。

たとえば、nvram:startup-config は NVRAM 内のスタートアップ コンフィギュレーションを、flash:configs/backup-config はフラッシュ メモリの configs ディレクトリ内にある backup-config という名前のファイルをそれぞれ指定しています。

ファイルではなくファイル システムを参照する場合、*prefix*: という形式を使用します。これは、ファイル システム内にあるファイルではなく、ファイル システムそのものを指定する形式です。ファイル システム内のファイルをリストするコマンドや、ファイル システムをフォーマットするコマンドなど、ファイル システムそのものにコマンドを発行する場合、この形式を使用します。

たとえば、slot0: は slot 0 内の最初の Personal Computer Memory Card International Association（PCMCIA; パーソナル コンピュータ メモリ カード国際協会）フラッシュ メモリ カードを指示します。

URL プレフィクスの使用

URL プレフィクスは、ファイル システムを指定します。使用可能なファイル システムのリストは、プラットフォームと操作によって異なります。現在のプラットフォームで使用可能なプレフィクスについて知るには、製品マニュアルを参照するか、**show file systems** EXEC コマンドを使用します。ファイル システム プレフィクスは、表 15 にリストされています。

表 15　ファイル システム プレフィクス

プレフィクス	ファイルシステム
bootflash:	ブート フラッシュ メモリ。
disk0:	回転式メディア。
flash:	フラッシュ メモリ。このプレフィクスはすべてのプラットフォームで使用可能です。flash: という名前のデバイスを持たないプラットフォームでは、flash: というプレフィクスは slot0: のエイリアスとなります。そのため、すべてのプラットフォームで flash: というプレフィクスを使用してメイン フラッシュ メモリのストレージ領域を参照できます。
flh:	フラッシュ ロード ヘルパー ログ ファイル。
ftp:	FTP ネットワーク サーバ。
null:	コピーで使用する空のコピー先。リモートのファイルを null にコピーすることで、ファイルのサイズを知ることができます。
nvram:	NVRAM。
rcp:	リモート コピー プロトコル ネットワーク サーバ。
slavebootflash:	High System Availability（HSA; 拡張高システム可用性）用に設定されたルータのスレーブ RSP カードの内部フラッシュ メモリ。
slavenvram:	HSA 用に設定されたルータのスレーブ Route/Switch Processor（RSP; ルート スイッチ プロセッサ）カード上の NVRAM。
slaveslot0:	HSA 用に設定されたルータのスレーブ RSP カード上の最初の PCMCIA カード。
slaveslot1:	HSA 用に設定されたルータのスレーブ RSP カード上の 2 枚目の PCMCIA カード。
slot0:	1 枚目の PCMCIA フラッシュ メモリ カード。

表 15　ファイル システム プレフィクス （続き）

プレフィクス	ファイルシステム
slot1:	2 枚目の PCMCIA フラッシュ メモリ カード。
system:	実行コンフィギュレーションを含め、システム メモリを持つ。
tftp:	TFTP ネットワーク サーバ。
xmodem:	ネットワーク マシンから Xmodem プロトコルを使用してファイルを取得する。
ymodem:	ネットワーク マシンから Ymodem プロトコルを使用してファイルを取得する。

（注）　Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）のファイル システムとしてのサポートは終了しました。

すべてのコマンドで、ファイル システム名の後にはコロンが必須です。しかし、以前はコロンを必要としなかったコマンドについては、サポートが続けられます。ただし、状況依存ヘルプは使用できなくなります。

パーティション デバイスの URL プレフィクス

パーティション デバイスでは、URL プレフィクスにパーティション番号を含めます。パーティション デバイスのプレフィクスの構文は、*device*:*partition-number*: です。

たとえば、flash:2: はフラッシュ メモリの 2 番目のパーティションを示します。

URL コンポーネント長

表 16 に、さまざまな URL コンポーネントの文字列の最大長のリストを示します。

表 16　URL コンポーネント長

コンポーネント	長さ（文字数）
プレフィクス	31
ユーザ名	15
パスワード	15
ホスト名	31
ディレクトリ	63
ファイル名	63

コマンド内での URL の使用

使用するコマンドによって、使用できるファイル システムは異なります。一部のファイル システムはファイルの送信元になりますが、宛先には使用できません。たとえば、Xmodem では別のマシンへのコピーはできません。また、**format** や **erase** といった操作は、特定のプラットフォーム上の特定のファイル システムだけでサポートされています。

次の項で、コマンド内で URL を使用する方法について説明します。

- 「コマンドをサポートするファイル システムの判別」
- 「デフォルトのファイル システムの使用」
- 「タブ補完の使用」
- 「ファイル システム内のファイルのリスト」

コマンドをサポートするファイル システムの判別

特定のコマンドにどのファイル システムが使用できるかを判別するには、状況依存ヘルプを使用します。次の例で、状況依存ヘルプは **copy** EXEC コマンドのコピー元として使用可能なのはどのファイル システムかを表示しています。出力結果はプラットフォームによって異なります。

```
Router# copy ?
  /erase      Erase destination file system.
  bootflash:  Copy from bootflash: file system
  flash:      Copy from flash: file system
  ftp:        Copy from ftp: file system
  null:       Copy from null: file system
  nvram:      Copy from nvram: file system
  rcp:        Copy from rcp: file system
  system:     Copy from system: file system
  tftp:       Copy from tftp: file system
```

デフォルトのファイル システムの使用

ほとんどのコマンドでは、ファイル システムが指定されない場合、ファイルは **cd** コマンドで指定されたデフォルト ディレクトリ内にあるものと仮定されます。

```
Router# pwd
slot0:
Router# dir
Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  foo
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)
Router# cd nvram:
Router# dir
Directory of nvram:/

  1  -rw-        2725              <no date>  startup-config
  2  ----           0              <no date>  private-config
  3  -rw-        2725              <no date>  underlying-config

129016 bytes total (126291 bytes free)
```

タブ補完の使用

コマンド入力時の文字数を減らすため、タブ補完を使用できます。ファイル名の最初の数文字を入力してから、Tab キーを押します。その文字があるファイル名だけに一致する場合、ルータがそのファイル名の入力を補完します。通常通りコマンドの入力を続け、Enter キーを押してコマンドを実行します。

次の例では、ルータが startup-config というファイル名の入力を補完しています。nvram: ファイル システム内で「s」で始まるファイルは 1 つだけであるためです。

```
Router# show file info nvram:s<tab>
Router# show file info nvram:startup-config<Enter>
```

文字を入力せずにタブ補完を使用すると、ルータはファイル システム内の最初のファイルを使用します。

```
Router# show file info nvram:<tab>
Router# show file info nvram:private-config<Enter>
```

ファイル システム内のファイルのリスト

多くのコマンドでは、状況依存ヘルプを使用して、ファイル システム内のファイルのリストを表示できます。次の例では、ルータは NVRAM: 内にあるファイルをリストしています。

```
Router# show file info nvram:?
nvram:private-config  nvram:startup-config  nvram:underlying-config
```

ファイル システムの管理

ファイル システムを管理するには、次の項で説明されている作業を実行します。

- 「使用可能なファイル システムのリスト」
- 「デフォルト ファイル システムの設定」
- 「現在のデフォルト ファイル システムの表示」
- 「ファイル システム上のファイル情報の表示」
- 「ファイルの表示」

使用可能なファイル システムのリスト

各プラットフォームですべてのファイル システムがサポートされているわけではありません。現在のプラットフォームで使用可能なファイル システムをリストするには、次の EXEC モード コマンドを実行します。

コマンド	目的
`Router> show file systems`	現在のプラットフォームで使用可能なファイル システムをリストします。このコマンドは、各ファイル システムの情報も表示します。

デフォルト ファイル システムの設定

ファイル システムまたはディレクトリをデフォルト ファイル システムとして指定できます。デフォルト ファイル システムを指定すると、関連コマンド内でオプションの *filesystem*: 引数の入力を省略できるようになります。*filesystem*: 引数をオプションとして持つ EXEC コマンドでは、オプションの *filesystem*: 引数が省略された場合、システムは **cd** EXEC コマンドで指定されたファイル システムを使用します。たとえば、**dir** EXEC コマンドは、オプションとして *filesystem*: 引数を持ち、そのファイル システム上のファイルのリストを表示します。

デフォルト ファイル システムを設定するには、次のコマンドを EXEC モードで使用します。

コマンド	目的
Router> **cd** *filesystem*:	デフォルト フラッシュ メモリ デバイスを設定します。

次の例では、デフォルト ファイル システムを slot 0: に挿入されたフラッシュ メモリ カードに設定します。

```
cd slot0:
```

現在のデフォルト ファイル システムの表示

cd EXEC コマンドで指定された現在のデフォルト ファイル システムを表示するには、次のコマンドを EXEC モードで使用します。

コマンド	目的
Router> **pwd**	現在のファイル システムを表示します。

次の例では、slot 0: がデフォルト ファイル システムです。

```
Router> pwd
slot0:
```

次の例では、**cd** コマンドを使用してデフォルト ファイル システムを system に変更し、さらに **pwd** コマンドを使用してデフォルト ファイル システムが変更されたことを確認しています。

```
Router> cd system:
Router> pwd
system:
```

ファイル システム上のファイル情報の表示

あるファイル システムの内容を操作する前に、内容のリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、そのファイル システムに同じ名前のコンフィギュレーション ファイルがないことを確認する場合があります。同様に、フラッシュ コンフィギュレーション ファイルを別の場所へコピーする場合、別のコマンドでの使用のためファイル名を確認しておきたい場合もあります。

ファイル システム上のファイル情報を表示するには、必要に応じて EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **dir** [**/all**] [*filesystem*:][*filename*]	ファイル システムのファイル リストを表示します。
Router# **show file systems**	ファイル システム上の各ファイルについて、詳細情報を表示します。
Router# **show file information** *file-url*	指定したファイルの情報を表示します。
Router# **show file descriptors**	オープン ファイル記述子のリストを表示します。

次の例では、第 1 スロットの PCMCIA カードのファイル情報の表示に使用されるさまざまなコマンドを比較しています。**dir /all** コマンドの出力では削除されたファイルが表示されるのに対し、**dir** コマンドの出力では表示されないことに注意してください。

```
Router# dir slot0:
Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  foo
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)

Router# dir /all slot0:
Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  3  -rw-     7982828   Oct 01 1997 18:48:14  [rsp-jsv-mz]
  4  -rw-         639   Oct 02 1997 12:09:17  [the_time]
  5  -rw-         639   Oct 02 1997 12:09:32  foo
  6  -rw-         639   Oct 02 1997 12:37:01  [the_time]
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)

Router# show slot0:
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. unknown  317FBA1B  4A0694   24  4720148 Aug 29 1997 17:49:36 hampton/nitz
2   .. unknown  9237F3FF  92C574   11  4767328 Oct 01 1997 18:42:53 c7200-js-mz
3   .D unknown  71AB01F1 10C94E0   10  7982828 Oct 01 1997 18:48:14 rsp-jsv-mz
4   .D unknown  96DACD45 10C97E0    8      639 Oct 02 1997 12:09:17 the_time
5   .. unknown  96DACD45 10C9AE0    3      639 Oct 02 1997 12:09:32 foo
6   .D unknown  96DACD45 10C9DE0    8      639 Oct 02 1997 12:37:01 the_time
7   .. unknown  96DACD45 10CA0E0    8      639 Oct 02 1997 12:37:13 the_time

3104544 bytes available (17473760 bytes used)
```

ファイルの表示

リモート ファイル システムのファイルを含め、何らかの読み取り可能なファイルの内容を表示するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **more** [**/ascii** | **/binary** | **/ebcdic**] *file-url*	指定されたファイルを表示します。

次の例では、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示します。

```
Router# more tftp://serverA/hampton/savedconfig

!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
```

```
!
end
```

フラッシュ メモリ ファイル システム タイプ

シスコのプラットフォームでは、次の 3 つの異なるフラッシュ メモリ ファイル システム タイプのいずれかを使用します。

- 「クラス A フラッシュ ファイル システム」
- 「クラス B フラッシュ ファイル システム」
- 「クラス C フラッシュ ファイル システム」

ファイルの消去、削除、復元に使用される方法はフラッシュ ファイル システムのクラスに依存します。コマンドの一部は、1 つまたは 2 つのシステム タイプだけでサポートされています。コマンド リファレンス ドキュメンテーションは、すべてのファイル システム タイプでサポートされていないコマンドについて注記しています。

現在のプラットフォームがどのフラッシュ メモリ ファイル システム タイプを使用しているか知るには、表 17 を参照してください。

表 17　フラッシュ メモリ ファイル システム タイプ

タイプ	プラットフォーム
クラス A	Cisco 7000 シリーズ（Cisco 7500 シリーズを含む）、Cisco 12000 ギガビット スイッチ ルータ（GSR）、LS1010
クラス B	Cisco 1003、Cisco 1004、Cisco 1005、Cisco 2500 シリーズ、Cisco 3600 シリーズ、Cisco 4000 シリーズ、Cisco AS5200
クラス C	Cisco MC3810、SC3640 の disk0

クラス A フラッシュ ファイル システム

クラス A フラッシュ ファイル システムでは、**delete** EXEC コマンドを使用して個別のファイルを削除し、その後 **undelete** EXEC コマンドを使用してそれらのファイルを回復できます。**delete** コマンドは削除されたファイルを「deleted」とマークしますが、それらのファイルは実際にはフラッシュ メモリの容量を消費し続けています。ファイルを恒久的に削除するには、**squeeze** EXEC コマンドを実行します。**squeeze** コマンドは、「deleted」とマークされたファイルすべてを指定されたフラッシュ メモリ デバイスから削除します。ファイルは回復できなくなります。フラッシュ デバイスのファイルすべてを消去するには、**format** EXEC コマンドを使用します。

フラッシュ メモリ デバイス上のファイルの削除

フラッシュ メモリ デバイス上のファイルが必要なくなった場合、削除できます。ファイルを削除すると、ルータはただファイルに deleted マークを付けるだけで、ファイルを消去することはしません。次の項で説明するとおり、この機能によって削除されたファイルを回復することが可能になります。新しいイメージやコンフィギュレーション ファイルが壊れてしまったために、「deleted」のイメージやコンフィギュレーション ファイルを回復させる場合があります。

指定されたフラッシュ メモリ デバイスからファイルを削除するには、次の EXEC モード コマンドを実行します。

コマンド	目的
Router# **delete** [*device*:]*filename*	ファイルをフラッシュ メモリ デバイスから削除します。

device を省略した場合、ルータは **cd** EXEC コマンドで指定されたデフォルト デバイスを使用します。

CONFIG_FILE や BOOTLDR 環境変数で指定されたファイルを削除しようとすると、システムは削除確認のプロンプトを表示します。また、BOOT 環境変数で指定された、最後の有効なシステム イメージを削除しようとした場合も、システムは削除確認のプロンプトを表示します。

次に、スロット 0 に挿入されたフラッシュ メモリ カードから myconfig という名前のファイルを削除する例を示します。

```
delete slot0:myconfig
```

フラッシュ メモリ デバイス上の削除ファイルの回復

削除されたファイルを回復できます。たとえば、現在のコンフィギュレーション ファイルが壊れているため、以前のファイルに戻す場合があります。

フラッシュ メモリ デバイス上で削除されたファイルを回復するには、EXEC モードで次のコマンドを実行します。

	コマンド	目的
ステップ 1	Router# **dir /all** [*filesystem*:]	削除されたファイルのインデックスを判別します。
ステップ 2	Router# **undelete** *index* [*filesystem*:]	削除されたファイルをフラッシュ メモリ デバイスに復元します。

ファイルの回復はインデックスを使用する必要があります。同じ名前の削除されたファイルが複数存在することがあるためです。たとえば、「deleted」リストに router-config という名前のコンフィギュレーション ファイルが複数存在する場合があります。リストに複数存在する router-config ファイルのうちどのファイルを回復するか、インデックスを使用して指示します。回復するファイルのインデックス番号を知るには、**dir** コマンドを **/all** オプションとともに使用します。

同名の有効なファイルが存在する場合、ファイルの回復はできません。この場合、まず既存のファイルを削除してから、ファイルの回復を行います。たとえば、以前あった router-config という名前のファイルを、削除したときと同じ名前で回復する場合、インデックスで以前のバージョンを回復するだけではうまくいきません。まず既存の router-config ファイルを削除してから、以前の router-config ファイルをインデックスで回復させる必要があります。**squeeze** EXEC コマンドで恒久的に消去したファイルでない限り、ファイルの回復が可能です。同じファイルの削除と回復は、15 回まで可能です。

次の例では、インデックス番号 1 の削除されたファイルを slot 0: に挿入されたフラッシュ メモリ カードに復元します。

```
undelete 1 slot0:
```

フラッシュ メモリ デバイス上のファイルの恒久的削除

フラッシュ メモリ デバイスがいっぱいになった場合、削除されたファイルが占めている空間を再度利用できるようにするため、ファイルの再配置が必要になる場合があります。フラッシュ メモリ デバイスがいっぱいかどうかを知るには、**dir** EXEC コマンドを使用します。

フラッシュ メモリ デバイス上のファイルを恒久的に削除するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **squeeze** *filesystem*:	「deleted」とマークされたフラッシュ メモリ デバイス上のファイルすべてを恒久的に削除します。

Cisco 2600 および 3600 シリーズのルータでは、**squeeze** コマンドを使用可能にするために、まずフラッシュ ファイル システム全体をいったん消去する必要があります。いったん消去が実行されると、そのフラッシュ ファイル システム上では、それ以降のフラッシュ ファイル システムの使用履歴を通じて squeeze コマンドが正常に動作するようになります。

Cisco 2600 または 3600 シリーズのルータでフラッシュ ファイル システム全体を消去するには、次の手順に従います。

コマンド	目的
Router# **no partition** *flash-filesystem:*	指定したフラッシュ ファイル システムのパーティションをすべて削除します。 **（注）** パーティションを削除するのは、フラッシュ ファイル システム全体を確実に消去するためです。いったんフラッシュ ファイル システムを消去すると、その後はパーティション付きのフラッシュ ファイル システムで **squeeze** コマンドを使用できます。
Router# **erase** *filesystem*:	指定されたフラッシュ ファイル システム上のファイルをすべて消去します。

squeeze コマンドを発行すると、ルータは有効なファイルすべてをフラッシュ メモリへフラッシュ メモリの先頭からコピーし、「deleted」とマークされたファイルすべてを消去します。この時点で、削除ファイルの回復はできなくなり、フラッシュ メモリの空間を再度書き込みに利用できるようになります。

（注） フラッシュ メモリ容量のほぼ全体にわたって消去と再書き込みを行うため、squeeze 操作には数分かかります。

フラッシュの確認

クラス A フラッシュ ファイル システムのフラッシュ メモリ内にあるファイルのチェックサムを再計算して確認するには、**verify** EXEC コマンドを使用します。

クラス A フラッシュ ファイル システムの削除と回復の例

次の例では、c7200-js-mz という名前のイメージが削除され、回復されます。削除されたファイルは最初の **dir** EXEC コマンドの出力には表示されないものの、**dir /all** EXEC コマンドの出力には表示されることに注意してください。

```
Router# delete slot1:
Delete filename []? c7200-js-mz
Delete slot1:c7200-js-mz? [confirm]
Router# dir slot1:
Directory of slot1:/
```

```
No such file

20578304 bytes total (15754684 bytes free)
Router# dir /all slot1:
Directory of slot1:/

  1  -rw-     4823492   Dec 17 1997 13:21:53  [c7200-js-mz]

20578304 bytes total (15754684 bytes free)
Router# undelete 1 slot1:
Router# dir slot1:
Directory of slot1:/

  1  -rw-     4823492   Dec 17 1997 13:21:53 c7200-js-mz

20578304 bytes total (15754684 bytes free)
```

次の例では、イメージが削除されます。削除されたファイルが使用しているスペースを再利用するために、**squeeze** EXEC コマンドが発行されています。

```
Router# delete slot1:c7200-js-mz
Delete filename [c7200-js-mz]?
Delete slot1:c7200-js-mz? [confirm]
Router# squeeze slot1:
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]
Erasing squeeze log
Squeeze of slot1: complete
Router# dir /all slot1:
Directory of slot1:/

No such file

20578304 bytes total (20578304 bytes free)
```

クラス B フラッシュ ファイル システム

クラス B フラッシュ ファイル システムでは、個別のファイルを **delete** EXEC コマンドで削除できます。**delete** コマンドは、ファイルを「deleted」とマークします。ファイルは引き続きフラッシュ メモリ上に存在し、空間を消費します。ファイルを回復するには、**undelete** EXEC コマンドを使用します。フラッシュ メモリ内の空間を再利用するには、フラッシュ ファイル システム全体を **erase** EXEC コマンドを使用して消去する必要があります。

フラッシュ メモリ デバイス上のファイルの削除

フラッシュ メモリ デバイス上のファイルが必要なくなった場合、削除できます。ファイルを削除すると、ルータはただファイルに deleted マークを付けるだけで、ファイルを消去することはしません。次の項で説明するとおり、この機能によって削除されたファイルを回復することが可能になります。新しいイメージやコンフィギュレーション ファイルが壊れてしまったために、「deleted」のイメージやコンフィギュレーション ファイルを回復させる場合があります。

指定されたフラッシュ メモリ デバイスからファイルを削除するには、次の EXEC モード コマンドを実行します。

コマンド	目的
Router# **delete** [*device*:]*filename*	ファイルをフラッシュ メモリ デバイスから削除します。

device を省略した場合、ルータは **cd** EXEC コマンドで指定されたデフォルト デバイスを使用します。

次に、スロット 0 に挿入されたフラッシュ メモリ カードから myconfig という名前のファイルを削除する例を示します。

```
delete slot0:myconfig
```

フラッシュ メモリ デバイス上の削除ファイルの回復

削除されたファイルを回復できます。たとえば、現在のコンフィギュレーション ファイルが壊れているため、以前のファイルに戻す場合があります。

フラッシュ メモリ デバイス上で削除されたファイルを回復するには、EXEC モード コマンドを使用します。

	コマンド	目的
ステップ 1	Router# **dir /all** [*filesystem*:]	削除されたファイルのインデックスを判別します。
ステップ 2	Router# **undelete** *index* [*filesystem*:]	削除されたファイルをフラッシュ メモリ デバイスに回復します。

ファイルの回復はインデックスを使用する必要があります。同じ名前の削除されたファイルが複数存在することがあるためです。たとえば、「deleted」リストに router-config という名前のコンフィギュレーション ファイルが複数存在する場合があります。リストに複数存在する router-config ファイルのうちどのファイルを回復するか、インデックスを使用して指示します。回復するファイルのインデックス番号を知るには、**dir** コマンドを **/all** オプションとともに使用します。

同名の有効な（回復された）ファイルが存在する場合、ファイルの回復はできません。この場合、まず既存のファイルを削除してから、ファイルの回復を行います。たとえば、router-config の回復されたバージョンがあって、その代わりに削除された以前のバージョンを使用する場合、以前のバージョンをインデックスで回復するだけではうまくいきません。まず既存の router-config ファイルを削除してから、以前の router-config ファイルをインデックスで回復させる必要があります。**erase** EXEC コマンドでファイル システムを恒久的に消去したのでない限り、ファイルの回復が可能です。同じファイルの削除と回復は、15 回まで可能です。

次の例では、インデックス番号 1 の削除されたファイルを slot 0: に挿入されたフラッシュ メモリ カードに復元します。

```
undelete 1 slot0:
```

フラッシュ メモリの消去

フラッシュ メモリ内でファイルが消費している空間を再利用するために、**erase flash:** または **erase bootflash:** EXEC コマンドを使用して、ファイル システム全体を消去する必要があります。この過程で、これらのコマンドでは削除済みかどうかにかかわらずファイルすべてを消去し、フラッシュ メモリの全空間を再利用します。消去されたファイルは回復できません。フラッシュ メモリの消去実行前に、取っておきたいファイルをすべて別の位置（FTP サーバなど）に保存しておきます。デバイスの消去完了後、ファイルをフラッシュ メモリにコピーします。

フラッシュ メモリ デバイスを消去するには、次のコマンドを EXEC モードで実行します。

コマンド	目的
Router# **erase** *filesystem*:	フラッシュ ファイル システムを消去します。

ファイル システムの消去例

次の例では、フラッシュ メモリの 2 番目のパーティション内のファイルをすべて消去します。

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/gate/c1600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]

Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

フラッシュの確認

クラス B フラッシュ ファイル システムのフラッシュ メモリ内にあるファイルのチェックサムを再計算して確認するには、**verify** EXEC コマンドを使用します。

クラス C フラッシュ ファイル システム

クラス C フラッシュ メモリ ファイル システムでは、個別のファイルを **delete** EXEC コマンドで削除できます。一度削除されたファイルは、再利用できません。その代わり、フラッシュ ファイル システムの空間をダイナミックに再利用できます。フラッシュ内のファイルすべてを消去するには、**format** EXEC コマンドを使用します。

フラッシュ メモリ デバイス上のファイルの削除

フラッシュ メモリ デバイス上のファイルが必要なくなった場合、削除できます。クラス C ファイル システムでファイルを削除すると、ファイルは恒久的に削除されます。ルータは空間をダイナミックに再利用します。

指定したフラッシュ デバイスからファイルを削除するには、次のコマンドを EXEC モードで実行します。

コマンド	目的
`Router# delete [device:]filename`	ファイルをフラッシュ メモリ デバイスから削除します。

device を省略した場合、ルータは **cd** EXEC コマンドで指定されたデフォルト デバイスを使用します。

CONFIG_FILE や BOOTLDR 環境変数で指定されたファイルを削除しようとすると、システムは削除確認のプロンプトを表示します。また、BOOT 環境変数で指定された、最後の有効なシステム イメージを削除しようとした場合も、システムは削除確認のプロンプトを表示します。

次の例では、slot 0: に挿入されたフラッシュ メモリ カードから myconfig という名前のファイルを恒久的に削除します。

```
delete slot0:myconfig
```

フラッシュのフォーマット

クラス C フラッシュ ファイル システムをフォーマットするには、次のコマンドを EXEC モードで実行します。

コマンド	目的
Router# **format** *filesystem*	フラッシュ ファイル システムのフォーマット

フラッシュ デバイスをフォーマットすると、ファイルはすべて消去され、回復できなくなります。

ディレクトリの作成と削除

クラス C フラッシュ ファイル システムでは、**mkdir** EXEC コマンドを使用して新しいディレクトリを作成できます。ディレクトリをフラッシュ ファイル システムから削除するには、**rmdir** EXEC コマンドを使用します。

クラス C フラッシュ ファイル システムでは、**rename** EXEC コマンドを使用してファイルをリネームできます。

フラッシュ ファイル システムのチェック

クラス C フラッシュ ファイル システムでは、**fsck** EXEC コマンドを使用して、ファイル システムの損傷をチェックして問題を修復することができます。

リモート ファイル システムの管理

リモートファイル システム（FTP、rcp、TFTP サーバのファイル システム）で、次の作業を実行できます。

- **more** EXEC コマンドを使用して、ファイルの中身を参照する。
- **copy** EXEC コマンドを使用して、ルータへ、またはルータからファイルをコピーする。
- **show file information** EXEC コマンドを使用して、ファイル情報を表示する。

（注） リモート システムではファイルの削除はできません。

NVRAM ファイル システムの管理

ほとんどのプラットフォームでは、NVRAM がスタートアップ コンフィギュレーションを含んでいます。クラス A フラッシュ ファイル システムでは、環境変数 CONFIG_FILE でスタートアップ コンフィギュレーションの位置を指定します。しかし、CONFIG_FILE 環境変数にかかわらず、ファイル URL nvram:startup-config はいつでもスタートアップ コンフィギュレーションを指示します。

startup-config の表示（**more nvram:startup-config** EXEC コマンドを使用）、startup config の新しいコンフィギュレーション ファイルへの置換（**copy** *source-url* **nvram:startup-config** EXEC コマンドを使用）、スタートアップ コンフィギュレーションの別位置への保存（**copy nvram:startup-config**

destination-url EXEC コマンドを使用）、NVRAM の内容の消去（**erase nvram:** EXEC コマンドを使用）が行えます。CONFIG_FILE 変数で別の位置が指定されている場合、**erase nvram:** コマンドでもスタートアップ コンフィギュレーションを消去できます。

次の例は、スタートアップ コンフィギュレーションを表示します。

```
nnm3640-2# more nvram:startup-config
Using 2279 out of 129016 bytes
!
! Last configuration change at 10:57:25 PST Wed Apr 22 1998
! NVRAM config last updated at 10:57:27 PST Wed Apr 22 1998
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
...
end
```

次の例は、クラス A フラッシュ ファイル システム プラットフォーム上の NVRAM ファイル システムの内容を表示します。startup-config という名前のファイルが現在のスタートアップ コンフィギュレーション ファイルで、物理 NVRAM またはフラッシュ メモリ内にあります。ファイルがフラッシュ ファイル システム内にある場合、このエントリは実体ファイルへのシンボリック リンクです。underlying-config と名付けられたファイルは、いつでもコンフィギュレーションの NVRAM バージョンです。

```
Router# dir nvram:
  Directory of nvram:/

    1  -rw-        2703             <no date>  startup-config
    2  ----           5             <no date>  private-config
    3  -rw-        2703             <no date>  underlying-config

  129016 bytes total (126313 bytes free)
```

System ファイル システムの管理

「system」ファイル システムは、システム メモリと現在の実行コンフィギュレーションをふくんでいます。現在のコンフィギュレーションの表示（**show running-config** または **more system:running-config** EXEC コマンドを使用）、現在のコンフィギュレーションの別位置への保存（**copy system:running-config** *destination-url* EXEC コマンドを使用）、現在のコンフィギュレーションへのコンフィギュレーション コマンドの追加（**copy** *source-url* **system:running-config** EXEC コマンドを使用）を実行できます。

次の例では、「system」ファイル システムを変更して内容を表示し、実行コンフィギュレーションを表示します。

```
Router# cd ?
  bootflash:  Directory name
  flash:      Directory name
  lex:        Directory name
  modem:      Directory name
  null:       Directory name
  nvram:      Directory name
  system:     Directory name
  vfc:        Directory name
  <cr>

Router# cd system:?
system:memory  system:running-config  system:ucode  system:vfiles

Router# cd system:
Router# dir
Directory of system:/

    6  dr-x           0              <no date>  memory
    1  -rw-        7786   Apr 22 2001 03:41:39  running-config

No space information available

nnm3640-2# more system:running-config
!
! No configuration change since last restart
!
version 12.2
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!
.
.
.
end
```

プラットフォームによっては、次のように system ファイル システムが ucode ディレクトリにマイクロコードを含んでいます。

```
Router# dir system:/ucode
Directory of system:/ucode/

 21  -r--       22900             <no date>  aip20-13
 18  -r--       32724             <no date>  eip20-3
 25  -r--      123130             <no date>  feip20-6
 19  -r--       25610             <no date>  fip20-1
 22  -r--        7742             <no date>  fsip20-7
 23  -r--       17130             <no date>  hip20-1
```

```
 24  -r--       36450             <no date>  mip22-2
 29  -r--      154752             <no date>  posip20-0
 28  -r--      704688             <no date>  rsp220-0
 20  -r--       33529             <no date>  trip20-1
 26  -r--      939130             <no date>  vip22-20
 27  -r--     1107862             <no date>  vip222-20

No space information available
```

PCMCIA ATA ディスクのファイル システム チェックおよび修復

PCMCIA ATA ディスクのファイル システム チェックおよび修復機能は、Personal Computer Memory Card International Association（PCMCIA; パーソナル コンピュータ メモリ カード国際協会）ディスクの File Allocation Table（FAT）ファイル システムの Cisco IOS ソフトウェアでファイル システム チェック（fsck）ユーティリティを導入します。このユーティリティはブート セクタやパーティション テーブルのチェック、ファイルとディレクトリ構造のチェック、未使用ディスク領域の解放、FAT ファイル構造の更新などの機能を実行します。

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「PCMCIA ATA ディスクのファイル システム チェックおよび修復の機能情報」（P.4）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

このマニュアルの構成は、次のとおりです。

PCMCIA ATA ディスクのファイル システム チェックおよび修復について

ここでは、次の内容について説明します。

PCMCIA ATA ディスクのファイル システム チェックおよび修復の概要

Cisco IOS Release 12.2(13)T でファイル システム チェック（fsck）ユーティリティが導入される前は、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、Advanced Technology Attachment（ATA）ディスクから破損したファイルを削除できませんでした。

ATA ディスクのファイル（またはファイル メタデータ）は、電源障害やシステムのクラッシュ、単純な TFTP コピー エラーなどさまざまなイベントにより破損する可能性があります。ファイル システム チェック（fsck）ユーティリティが導入される前は、ディスクの削除、再フォーマットあるいは再インストールをせずに使用可能な ATA ディスクから破損したファイルを削除できませんでした。

fsck 特権 EXEC コマンドでは、CLI から直接、便利な方法で不要なディスク領域を回復できます。

（注） FAT16 フォーマット ディスクに追加できるルート ディレクトリ エントリは 512 だけです。この上限はルート ディレクトリの下に保存するファイルの最大数を制限します。ファイルが保存するルート ディレクトリのエントリ数はファイル名の長さに比例します。FAT32 フォーマット ディスクにはこのルート ディレクトリ エントリ制限はありません。FAT16 または FAT32 フォーマット ディスクのサブディレクトリにも、保存するファイルの最大数に関する制限はありません。

PCMCIA ATA ディスクのファイル システム チェックおよび修復の使用方法

fsck ユーティリティはデフォルトでイネーブルです。コンフィギュレーションは必要ありません。詳細については、**fsck** コマンド ページを参照してください。

その他の関連資料

次の項に、PCMCIA ATA ディスクのファイル システム チェックおよび修復機能に関する参考資料を示します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
コンフィギュレーション基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

PCMCIA ATA ディスクのファイル システム チェックおよび修復の機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　PCMCIA ATA ディスクのファイル システム チェックおよび修復の機能情報

機能名	リリース	機能情報
PCMCIA ATA ディスクのファイル システム チェックおよび修復	12.0(22)S 12.2(13)T	この機能は PCMCIA ディスクの FAT ファイルシステムの Cisco IOS ソフトウェアにファイル システム チェック (fsck) ユーティリティを導入します。このユーティリティはブート セクタやパーティション テーブルのチェック、ファイルとディレクトリ構造のチェック、未使用ディスク領域の解放、FAT ファイル構造の更新などの機能を実行します。 次のコマンドが導入または修正されました。**fsck**

USB でのデータ保存

Universal Serial Bus（USB）ストレージ機能を使用すると、特定のモデルのシスコ製のルータで USB フラッシュ モジュールをサポートし、USB キー フォーム ファクタ（別名 USB eToken）で SmartCard テクノロジー（Aladdin Knowledge Systems 社製）を使用してルータへのセキュアなアクセスを提供できます。

USB eToken はセキュアなコンフィギュレーション配布を実現し、配置用にユーザによる Virtual Private Network（VPN; バーチャル プライベート ネットワーク）認証資格情報の保存を可能にします。USB フラッシュ ドライブを使用すると、イメージとコンフィギュレーションをルータ外に保存できます。

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「USB でのデータ保存の機能情報」（P.19）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

USB にデータを保存する場合の前提条件

USB フラッシュ モジュールまたは eToken を使用する前に、次のシステム要件を満たしていなければなりません。

- Cisco 871 ルータ、Cisco 1800 シリーズ、Cisco 2800 シリーズ、あるいは Cisco 3800 シリーズ ルータ。
- サポートされているいずれかのプラットフォーム上で、少なくとも Cisco IOS Release 12.3(14)T イメージが稼動していること。
- シスコ対応の USB フラッシュまたは USB eToken。
- USB eToken サポートには k9 イメージが必要（ただし、USB フラッシュ サポートはすべてのイメージで利用可能です）。

USB にデータを保存する場合の制限事項

- USB eToken がサポートされるためには、ファイルをセキュアに保存できる 3DES（k9）Cisco IOS ソフトウェア イメージが必要です。
- USB ハブは現在、サポートされていません。そのため、サポートされるデバイスの数は、多くてもルータ シャーシで使用できる USB ポートの数までです。
- eToken または USB フラッシュからイメージを起動することはできません（ただし、eToken とフラッシュの両方からコンフィギュレーションを起動することはできます）。

USB へのデータ保存について

ルータで USB フラッシュ モジュールとセキュアな eToken を使用するには、次の概念を理解する必要があります。

- 「USB eToken と USB フラッシュの役割」（P.2）
- 「USB ストレージ ファイルシステム サポート」（P.4）
- 「USB にデータを保存する利点」（P.4）

USB eToken と USB フラッシュの役割

USB eToken と USB フラッシュ モジュールの両方を使用してファイル（ルータ コンフィギュレーションなど）を保存できます。次の項では、各デバイスの機能方法と各デバイス間の差異について説明します。

- 「USB eToken の動作の仕組み」（P.2）
- 「USB フラッシュの動作の仕組み」（P.3）
- 「eToken と USB フラッシュの機能的差異」（P.3）

USB eToken の動作の仕組み

SmartCard はプラスティック製の小型カードで、データの保存や処理を行うためのマイクロプロセッサやメモリが搭載されています。USB インターフェイスを備えた SmartCard が SmartCard eToken です。eToken では、記憶域の容量（32KB）内であれば、どのようなタイプのファイルでもセキュアに保存

できます。eToken に保存されたコンフィギュレーション ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。ルータにコンフィギュレーション ファイルをロードするには、ルータのコンフィギュレーション ファイルをセキュアに配布できるよう適切な PIN が設定されている必要があります。

eToken をルータに装着したら、その eToken にログインする必要があります。ログイン後は、ユーザ PIN（デフォルトは 1234567890）や、ログインが拒否されるようになるまで許容されるログイン試行の失敗回数（デフォルトは 15 回）など、さまざまなデフォルト設定を変更できます。eToken のアクセス方法および設定方法については、「eToken のアクセスと設定」を参照してください。

eToken へ正常にログインした場合は、**copy** コマンドを使用して、ルータから eToken へファイルをコピーできます。デフォルトでは、ルータから eToken を削除した後、関連付けられているすべての RSA キーが削除され、次回の Internet Key Exchange（IKE; インターネット キー エクスチェンジ）ネゴシエーション期間まで、IPSec トンネルは切断されません（デフォルトの動作を変更し、IPSec トンネルが切断されるまでの時間を指定する場合は、**crypto pki token removal timeout** コマンドを発行します）。

Aladdin Knowledge Systems 社製の eToken の詳細については、Aladdin 社の Web サイト http://www.aladdin.com/etoken/cisco/ を参照してください。

USB フラッシュの動作の仕組み

Cisco USB フラッシュ モジュールでは、ルータ構成と Cisco IOS ソフトウェア イメージの保存と配置ができます。Cisco USB フラッシュ モジュールには 64MB、128MB、256MB のバージョンがあります。

（注） USB フラッシュはルータの起動に必要なルータ コンパクト フラッシュの代わりになるものではありません。

USB フラッシュ モジュールをルータに挿入すると、スタートアップ コンフィギュレーションに **boot config** コマンドが含まれ、**boot config usbflash0: new-config** などの USB フラッシュ デバイスにある新しいコンフィギュレーションを指定している場合は、コンフィギュレーション ファイルを自動的に起動します。

eToken と USB フラッシュの機能的差異

eToken と USB フラッシュの両方がセカンダリ ストレージを提供しますが、各デバイスにはそれぞれ利点と制限事項があります。ニーズに合ったデバイスを検討する際に役立つよう、表 1 で eToken と USB フラッシュの機能的差異をハイライトしています。

表 1　eToken と USB フラッシュの機能的差異

機能	USB eToken	USB フラッシュ
アクセシビリティ	デジタル証明書、事前共有鍵、およびルータ設定を eToken からルータへセキュアに保存したり転送したりするためのものです。	USB フラッシュからルータのルータ構成とイメージを保存して配置するために使用します。
ストレージのサイズ	32KB	• 64MB • 128MB • 256MB

表 1　eToken と USB フラッシュの機能的差異 （続き）

機能	USB eToken	USB フラッシュ
ファイル タイプ	• 通常、IPSec VPN 用のデジタル証明書、事前共有鍵、およびルータ設定を保存する場合に使用します。 • eToken は Cisco IOS イメージを保存できません。	コンパクト フラッシュに保存できるファイル タイプを保存します。
セキュリティ	• ファイルに対する暗号化およびアクセスは、ユーザ PIN を介してだけ行えます。 • ファイルは、ノンセキュアなフォーマットでも保存できます。	ファイルは、ノンセキュアなフォーマットでだけ保存できます。
ブート設定	• ルータではブート時に、USB トークンに保存されている設定を使用できます。 • ルータではブート時に、eToken に保存されているセカンダリ設定を使用できます（セカンダリ設定を使用すると、ユーザは各自の IPSec 設定をロードできます）。	• **boot config** コマンドが発行される場合（**boot config usbflash0: new-config** など）は、コンフィギュレーション ファイルは自動的に USB フラッシュからルータに転送できます。

USB ストレージ ファイルシステム サポート

USB ストレージ デバイス容量は拡大しているため、DOSFS と usbflash コンポーネントを修正して、大容量 USB ストレージ デバイスを使用可能にしておく必要があります。USB ストレージ ファイルシステム サポート機能は USB フラッシュ デバイスの DOSFS サポートを拡張します。この機能を使用すると、大容量 USB ストレージ デバイスにデータを保存できます。

USB にデータを保存する利点

Cisco ルータでの USB フラッシュ ドライブと USB eToken サポートは次のアプリケーションに関する利点を提供します。

移動可能な証明書：配置する VPN クレデンシャルを外部デバイスに保存できます。

Aladdin eToken は SmartCard テクノロジーを使用して、デジタル証明書と IPSec VPN 導入用のコンフィギュレーションを保存できます。これにより、ルータにおいて RSA 公開鍵を生成し、少なくとも 1 つの IPSec トンネルを認証できるようになりました（ルータでは複数の IPSec トンネルを開始できるため、eToken には、必要に応じて複数の証明書を保存できるようになっています）。

VPN クレデンシャルを外部デバイスに保存すると、機密データが漏洩する危険性は低くなります。

ファイルをセキュアに配置するための PIN 設定

Aladdin eToken は、ユーザ設定 PIN 経由でのルータ上での暗号化をイネーブルにするために使用できるコンフィギュレーション ファイルを保存できます（つまり、デジタル証明書、事前共有鍵、および VPN は使用されません）。

軽減されるまたは不要になる手動での設定作業

eToken と USB フラッシュの両方がほとんど手作業なしにリモート ソフトウェア コンフィギュレーションとプロビジョニングを提供できます。設定は自動プロセスとして構成されます。つまり、いずれのデバイスも eToken または USB フラッシュがルータに挿入された後、ルータが起動するために使用できるブートストラップ設定を保存できます。さらにこのルータは、ブートストラップ設定によって TFTP サーバへ接続され、その TFTP サーバに保存されている設定に基づいて、すべてのルータ設定が行われます。

Cisco ルータで USB モジュールをセットアップおよび使用する方法

ここでは、USB モジュールをサポートするためのルータの設定手順について説明します。

外部 USB フラッシュ ドライブまたは eToken のコンフィギュレーションの保存

次の作業を使用して、USB フラッシュ ドライブ モジュールまたは eToken にコンフィギュレーション ファイルを保存します。

手順の概要

1. **enable**
2. **configure terminal**
3. **boot config** *file-system-prefix*:[*directory*/]*filename* [**nvbypass**]

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。 • 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：** `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。
ステップ 3	**boot config** *file-system-prefix*:[*directory*/]*filename* [**nvbypass**] **例：** `Router(config)# boot config usbflash0:`	USB フラッシュ ドライブまたはセキュアな eToken にスタートアップ コンフィギュレーション ファイルが保存されていることを指定します。 **（注）** USB フラッシュ ドライブを使用する場合は、**flash:** からブート ヘルパーが起動します。ブート ヘルパーは Cisco IOS イメージで **flash:** にあります。使用する Cisco IOS イメージは USB を認識する必要があります。

eToken のアクセスと設定

eToken を Cisco ルータに挿入した後、次に示す方法で eToken にログインする必要があります。

- 「eToken へのログイン」（P.6）（必須）

eToken にログインしたら、次に示す方法でユーザ PIN の変更やルータから eToken へのファイル コピーなどの管理作業を実行できます。

- 「eToken での管理者機能の設定」（P.8）（任意）

RSA キーと eToken の使用

- RSA キーは、eToken がルータへ正常にログインした後にロードされます。
- デフォルトの場合、新規に生成された RSA キーは、最後に装着された eToken に保存されます。再生成されたキーは、元の RSA キーが生成されたのと同じ場所に保存する必要があります。

eToken へのログイン

この作業を使用して、eToken に手動または自動でログインします。

自動ログイン

自動ログインを使用すると、ユーザやオペレータが介入することなく、ルータを完全な稼動状態に戻せます。PIN は、プライベート コンフィギュレーションに保存されるため、スタートアップ コンフィギュレーションや実行コンフィギュレーションには表示されません。

（注） 手動で生成されたスタートアップ コンフィギュレーションには、配置用に自動ログイン コマンドを指定できますが、手動で生成されたそのコンフィギュレーションをプライベート コンフィギュレーションに取り込むには、**copy system:running-config nvram: startup-config** コマンドを発行する必要があります。

手動ログイン

手動ログインは、PIN をルータ上に保存するのが適していない場合に使用できます。手動ログインは、権限の有無にかかわらず実行できます。また、手動ログインを実行すると、eToken 上のファイルおよび RSA キーが、Cisco IOS ソフトウェアで使用可能になります。セカンダリ コンフィギュレーション ファイルを設定する場合は、ログインを実行するユーザの権限がある場合にだけ手動ログインを実行できます。そのため、何らかの目的で、手動ログインを実行し、eToken 上にセカンダリ コンフィギュレーション ファイルを設定する場合は、権限をイネーブルにする必要があります。

手動ログインは、失われたルータ設定のリカバリを行う場合にも使用できます。通常 VPN を使用してコア ネットワークへ接続しているリモート サイトが存在する状況では、設定および RSA キーが失われた場合、eToken が備えているアウトオブバンド サービスが必要となります。eToken には、ブート設定、セカンダリ設定、および接続を認証するための RSA キーを保存できます。

また、初期導入時やハードウェア交換時に、ルータを現地の業者から調達したり、リモート サイトへ直送したりする場合にも、手動ログインが適しています。

自動ログインとは異なり、手動ログインを使用する場合は、ユーザが実際の eToken PIN を把握している必要があります。ユーザが物理的に eToken にアクセスできる場合は、Aladdin の Windows ベースのユーティリティを使用して、RSA キーとセカンダリ コンフィギュレーション ファイルを eToken からコピーできます。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **login** [*pin*]

   または

   configure terminal
3. **crypto pki token** *token-name* **user-pin** [*pin*]
4. exit
5. **show usbtoken**[**0-9**]**:***filename*

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。 • 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	**crypto pki token** *token-name* [**admin**] **login** [*pin*]
	
	例：
	`Router# crypto pki token usbtoken0 admin login 5678`
	
	または
	
	configure terminal
	
	例：
	`Router# configure terminal`
		手動で eToken にログインします。
		後でユーザ PIN を変更する場合は、**admin** キーワードを指定する必要があります。
		
		または
		ルータのモードを、eToken の自動ログインを設定できるグローバル コンフィギュレーション モードにします。

ステップ 3	**crypto pki token** *token-name* **user-pin** [*pin*] **例：** `Router(config)# crypto pki token usbtoken0 user-pin 1234`	（任意）ルータが自動的に起動時に USB eToken にログインできるように PIN を作成します。 **（注）** すでに手動ログインを設定している場合は、このコマンドを発行しないでください。
ステップ 4	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show usbtoken**[**0-9**]:*filename* **例：** `Router#`	（任意）USB eToken がルータにログインしているかどうかを確認します。

eToken での管理者機能の設定

この作業を使用して、ユーザ PIN および eToken 上の失敗回数の上限などのデフォルト設定を変更します。

手順の概要

1. **enable**
2. **crypto pki token** *token-name* [**admin**] **change-pin** [*pin*]
3. **configure terminal**
4. **crypto pki token** {*token-name* | **default**} **removal timeout** [*minutes*]
5. **crypto pki token** {*token-name* | **default**} **max-retries** [*number*]
6. **exit**
7. **copy usbflash**[**0-9**]:*filename destination-url*
8. **show usbtoken**[**0-9**]:*filename*
9. **crypto pki token** *token-name* **logout**

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。 • 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	**crypto pki token** *token-name* [**admin**] **change-pin** [*pin*] **例：** `Router# crypto pki token usbtoken0 admin change-pin`	（任意）USB eToken 上のユーザ PIN 番号を変更します。 • PIN が変更されない場合は、デフォルトの PIN（1234567890）が使用されます。 **（注）** PIN の変更後は、ログインの失敗回数を 0 にリセットする必要があります（**crypto pki token max-retries** コマンドを使用）。許容されるログインの失敗回数の上限は、15（デフォルト）に設定されています。
ステップ 3	**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。
ステップ 4	**crypto pki token** {*token-name* | **default**} **removal timeout** [*seconds*] **例：** `Router(config)# crypto pki token usbtoken0 removal timeout 60`	（任意）eToken がルータから取り外されてから、eToken に保存されている RSA キーが削除されるまで、ルータが待機する時間を秒単位で設定します。 **（注）** このコマンドが発行されない場合は、eToken がルータから取り外された直後に、すべての RSA キーが削除される他、eToken に関連付けられている IPSec トンネルもすべて切断されます。
ステップ 5	**crypto pki token** {*token-name* | **default**} **max-retries** [*number*] **例：** `Router(config)# crypto pki token usbtoken0 max-retries 20`	（任意）eToken へのアクセスが拒否されるまでに許容されるログイン試行の連続失敗回数の上限を設定します。 • デフォルト値は 15 です。
ステップ 6	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 7	`copy usbflash[0-9]:`*filename destination-url* **例：** `Router# copy usbflash0:`	ルータから eToken にファイルをコピーします。 • *destination-url*：サポートされているオプションのリストについては、**copy** コマンドに関するセクションを参照してください。
ステップ 8	**show usbtoken**[0-9]:*filename* **例：** `Router#`	（任意）USB eToken に関する情報を表示します。このコマンドを使用すると、USB eToken がルータにログインしているかどうかを確認できます。

ステップ 9	`crypto pki token` *token-name* `logout`
	
	例：
	`Router# crypto pki toke usbtoken0 logout`
		USB eToken からルータをログアウトします。
		（注） USB eToken に何らかのデータを保存する場合は、再度 eToken にログインする必要があります。

USB フラッシュ ドライブと eToken のトラブルシューティング

ここでは、次の各 Cisco IOS コマンドについて説明します。これらのコマンドは、USB フラッシュまたは USB eToken の使用中に発生し得る問題についてのトラブルシューティングに使用できます。

show file systems コマンド

ステップ 1 **show file systems** コマンドを使用すると、USB モジュールが USB ポートに差し込まれていることをルータが認識しているかどうかを判定できます。差し込まれている USB モジュールは、ファイル システムのリスト上に表示されます。これらのモジュールがリスト上に表示されない場合は、次のいずれかの問題が発生している可能性があります。

- USB モジュールとの接続の問題
- ルータ上で稼動している Cisco IOS イメージが USB モジュールをサポートしない
- USB モジュールそのもののハードウェア上の問題

ステップ 2 USB モジュールが以前に正常にフォーマットされている場合は、**show file systems** コマンドを使用します。Cisco ルータと互換性を持たせるには、USB フラッシュ モジュールを FAT16 形式でフォーマットする必要があります。これが当てはまらない場合は、**show file systems** コマンドを使用すると、互換性のないファイル システムであることを示すエラーが表示されます。

USB フラッシュ モジュールと USB eToken を示す **show file systems** コマンドのサンプル出力を次に示します。USB モジュールが現れるのはリストの最下行です。

```
Router# show file systems

File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
*  129880064    69414912      disk     rw   flash:#
      491512      486395     nvram     rw   nvram:
           -           -    opaque     wo   syslog:
           -           -    opaque     rw   xmodem:
           -           -    opaque     rw   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
    63158272    33037312  usbflash     rw   usbflash0:
       32768         858  usbtoken     rw   usbtoken1:
```

show usb device コマンド

ステップ 1 **show usb device** コマンドを使用すると、USB モジュールがシスコによりサポートされているかどうかを判別できます。モジュールがサポートされているかどうかを示す USB フラッシュと USB eToken の両方のサンプル出力が、次のサンプル出力例で強調表示されています。

次のサンプル出力は USB フラッシュ モジュールのものです。

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0x15
Max. Packet Size of Endpoint Zero:64
Number of Configurations:1
Speed:Full
Selected Configuration:1
Selected Interface:0

Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:140 mA

    Interface:
        Number:0
        Description:
        Class Code:8
        Subclass:6
        Protocol:80
        Number of Endpoints:2

        Endpoint:
            Number:1
            Transfer Type:BULK
            Transfer Direction:Device to Host
            Max Packet:64
            Interval:0

        Endpoint:
            Number:2
            Transfer Type:BULK
            Transfer Direction:Host to Device
            Max Packet:64
            Interval:0
```

次のサンプル出力はサポートされている USB eToken のものです。

```
Router# show usb device
```

```
Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0

Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA

    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

show usb controllers コマンド

ステップ 1 **show usb controllers** コマンドを使用すると、USB フラッシュ モジュールにハードウェア上の問題があるかどうかを判別できます。**show usb controllers** コマンドの出力結果にエラーが表示された場合は、USB モジュールにハードウェア上の問題があると考えられます。

USB フラッシュ モジュールに対するコピー操作が正常に行われていることを確認する場合にも、この **show usb controllers** コマンドを使用できます。ファイルのコピーを実行した後で、**show usb controllers** コマンドを発行すると、データ転送が正常に行われたことを示す内容が表示されます。

次に示すのは、使用中の USB フラッシュ モジュールの **show usb controllers** コマンドによる出力例です。

```
Router# show usb controllers

Name:1362HCD
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
```

```
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF

Int Level:1
Transfer Completion Codes:
         Success              :920            CRC              :0
         Bit Stuff            :0              Stall            :0
         No Response          :0              Overrun          :0
         Underrun             :0              Other            :0
         Buffer Overrun       :0              Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2              Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0              Bulk Transfer   :0
         Isochronous Transfer :0              Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0              Bulk Transfer   :26
         Isochronous Transfer :0              Control Transfer:894

USBD Failures:
         Enumeration Failures :0              No Class Driver Found:0
         Power Budget Exceeded:0

USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3              Command Fail    :0
         Good Status Timed out:0              Device not Found:0
         Device Never Opened  :0              Drive Init Fail :0
         Illegal App Handle   :0              Bad API Command :0
         Invalid Unit Number  :0              Invalid Argument:0
         Application Overflow :0              Device in use   :0
         Control Pipe Stall   :0              Malloc Error    :0
         Device Stalled       :0              Bad Command Code:0
         Device Detached      :0              Unknown Error   :0
         Invalid Logic Unit Num:0

USB Aladdin Token Driver Counters:
         Token Inserted       :1              Token Removed   :0
         Send Insert Msg Fail :0              Response Txns   :434
         Dev Entry Add Fail   :0              Request Txns    :434
         Dev Entry Remove Fail:0              Request Txn Fail:0
```

```
         Response Txn Fail    :0                Command Txn Fail:0
         Txn Invalid Dev Handle:0

USB Flash File System Counters:
         Flash Disconnected   :0                Flash Connected :1
         Flash Device Fail    :0                Flash Ok        :1
         Flash startstop Fail :0                Flash FS Fail   :0

USB Secure Token File System Counters:
         Token Inserted       :1                Token Detached  :0
         Token FS success     :1                Token FS Fail   :0
         Token Max Inserted   :0                Create Talker Failures:0
         Token Event          :0                Destroy Talker Failures:0
         Watched Boolean Create Failures:0
```

dir コマンド

ステップ 1 **dir** コマンドと **usbflash[0-9]:** または **usbtoken[0-9]:** キーワードを使用して、USB フラッシュまたは USB eToken のすべてのファイル、ディレクトリ、および権限文字列を表示します。

次の出力例は、USB フラッシュに関するディレクトリ情報を表示したものです。

```
Router# dir usbflash0:

Directory of usbflash0:/

    1  -rw-    30125020  Dec 22 2032 05:31:32 +00:00  c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)
```

次の出力例は、USB eToken に関するディレクトリ情報を表示したものです。

```
Router# dir usbtoken1:

Directory of usbtoken1:/

    2  d---           64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---         4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---            0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---          512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---            0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---            0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---            0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----          940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----         1423  Jun 27 1992 12:51:14 +00:00  myrunning-config

32768 bytes total (858 bytes free)
```

次の出力例は、ルータにより認識されているすべてのデバイスについてのディレクトリ情報を表示したものです。

```
Router# dir all-filesystems

Directory of archive:/

No files in directory

No space information available
Directory of system:/

    2  drwx           0                    <no date>  its
```

```
  115  dr-x           0                    <no date>  lib
  144  dr-x           0                    <no date>  memory
    1  -rw-        1906                    <no date>  running-config
  114  dr-x           0                    <no date>  vfiles

No space information available
Directory of flash:/

    1  -rw-    30125020  Dec 22 2032 03:06:04 +00:00  c3825-entservicesk9-mz.123-14.T

129880064 bytes total (99753984 bytes free)
Directory of nvram:/

  476  -rw-        1947                    <no date>  startup-config
  477  ----          46                    <no date>  private-config
  478  -rw-        1947                    <no date>  underlying-config
    1  -rw-           0                    <no date>  ifIndex-table
    2  ----           4                    <no date>  rf_cold_starts
    3  ----          14                    <no date>  persistent-data

491512 bytes total (486395 bytes free)
Directory of usbflash0:/

    1  -rw-    30125020  Dec 22 2032 05:31:32 +00:00  c3825-entservicesk9-mz.123-14.T

63158272 bytes total (33033216 bytes free)
Directory of usbtoken1:/

    2  d---          64  Dec 22 2032 05:23:40 +00:00  1000
    5  d---        4096  Dec 22 2032 05:23:40 +00:00  1001
    8  d---           0  Dec 22 2032 05:23:40 +00:00  1002
   10  d---         512  Dec 22 2032 05:23:42 +00:00  1003
   12  d---           0  Dec 22 2032 05:23:42 +00:00  5000
   13  d---           0  Dec 22 2032 05:23:42 +00:00  6000
   14  d---           0  Dec 22 2032 05:23:42 +00:00  7000
   15  ----         940  Jun 27 1992 12:50:42 +00:00  mystartup-config
   16  ----        1423  Jun 27 1992 12:51:14 +00:00  myrunning-config

32768 bytes total (858 bytes free)
```

セキュアなトークン サポートの設定例

ここでは、次の設定例を示します。

- 「ログインして RSA キーを eToken に保存：例」（P.15）

ログインして RSA キーを eToken に保存：例

次に示すのは、eToken にログインして RSA キーを生成し、その RSA キーを eToken に保存する場合の設定例です。

```
! Configure the router to automatically log into the eToken
configure terminal
 crypto pki token default user-pin 0 1234567890
! Generate RSA keys and enroll certificates with the CA.
crypto pki trustpoint IOSCA
 enrollment url http://10.23.2.2
 exit
```

```
crypto ca authenticate IOSCA
Certificate has the following attributes:
       Fingerprint MD5:23272BD4 37E3D9A4 236F7E1A F534444E
      Fingerprint SHA1:D1B4D9F8 D603249A 793B3CAF 8342E1FE 3934EB7A

% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
crypto pki enroll
crypto pki enroll IOSCA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include:c2851-27.cisco.com
% Include the router serial number in the subject name? [yes/no]:no
% Include an IP address in the subject name? [no]:no
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate IOSCA verbose' command will show the fingerprint.


*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint MD5:E6DDAB1B
 0E30EFE6 54529D8A DA787DBA
*Jan 13 06:47:19.413:CRYPTO_PKI: Certificate Request Fingerprint SHA1:3B0F33B
7 57C02A10 3935042B C4B6CD3D 61039251
*Jan 13 06:47:21.021:%PKI-6-CERTRET:Certificate received from Certificate Authority
! Issue the write memory command, which will automatically save the RSA keys to the eToken
! instead of private NVRAM.
Router# write memory
Building configuration...
[OK]

*Jan 13 06:47:29.481:%CRYPTO-6-TOKENSTOREKEY:Key c2851-27.cisco.com stored on
Cryptographic Token eToken Successfully
```

次に示すのは、eToken から正常にロードされた保存済みクレデンシャルの **show crypto key mypubkey rsa** コマンドによる出力例です。eToken 上に保存されているクレデンシャルは、保護領域内に存在します。eToken 上にクレデンシャルを保存する場合、それらのファイルは /keystore というディレクトリに保存されます。ただし、キー ファイルは CLI からは非表示になります。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at:06:37:26 UTC Jan 13 2005
Key name:c2851-27.cisco.com
 Usage:General Purpose Key
 Key is not exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E3C644 43AA7DDD
  732E0F4E 3CA0CDAB 387ABF05 EB8F22F2 2431F1AE 5D51FEE3 FCDEA934 7FBD3603
  7C977854 B8E999BF 7FC93021 7F46ABF8 A4BA2ED6 172D3D09 B5020301 0001
% Key pair was generated at:06:37:27 UTC Jan 13 2005
Key name:c2851-27.cisco.com.server
 Usage:Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DD96AE 4BF912EB
  2C261922 4784EF98 2E70E837 774B3778 7F7AEB2D 87F5669B BF5DDFBC F0D521A5
```

```
56AB8FDC 9911968E DE347FB0 A514A856 B30EAFF4 D1F453E1 003CFE65 0CCC6DC7
21FBE3AC 2F8DEA16 126754BC 1433DEF9 53266D33 E7338C95 BB020301 0001
```

その他の関連資料

次の項に、USB 機能を使用したデータの保存に関する参考資料を示します。

関連資料

関連項目	参照先
ルータへの USB モジュールの接続	『*Cisco Access Router USB Flash Module and USB eToken Hardware Installation Guide*』
eToken および USB フラッシュのデータ シート	『*USB eToken and USB Flash Features Support*』
ファイル管理（ファイルのロード、コピー、および再起動）	『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』の「*File Management*」の項
デジタル証明書暗号化の設定	『*Cisco IOS Security Configuration Guide*』の「*Configuring Certification Authority Interoperability*」の章

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

USB でのデータ保存の機能情報

表 2 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　USB でのデータ保存の機能情報

機能名	リリース	機能情報
USB ストレージ	12.3(14)T	USB ストレージ機能は特定のモデルの Cisco ルータで USB フラッシュ モジュールをサポートし、USB キー フォーム ファクタ（別名 USB eToken）で SmartCard テクノロジー（Aladdin Knowledge Systems 社製）を使用してルータにセキュアなアクセスを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「USB へのデータ保存について」（P.2） • 「Cisco ルータで USB モジュールをセットアップおよび使用する方法」（P.5） • 「セキュアなトークン サポートの設定例」（P.15） 次のコマンドが導入または修正されました。**crypto pki token change-pin**、**crypto pki token login**、**crypto pki token logout**、**crypto pki token max-retries**、**crypto pki token removal timeout**、**crypto pki token secondary config**、**crypto pki token user-pin**、**debug usb**、**driver**、**show usb driver**、**show usb controllers**、**show usb device**、**show usb driver**、**show usb port**、**show usbtoken**、**show usb tree**、**boot config**、**copy**、**delete**、**dir**、**format**
USB ストレージ ファイルシステム サポート	12.2(33)SRE	USB ストレージ ファイルシステム サポート機能は USB フラッシュ デバイスの DOSFS サポートを拡張します。この機能を使用すると、大容量 USB ストレージ デバイスにデータを保存できます。 12.2(33)SRE では、この機能は Cisco 7200-NPE-G2 で導入されました。 この機能に関する詳細については、次の各項を参照してください。 • 「USB ストレージ ファイルシステム サポート」（P.4） 次のコマンドが導入または修正されました。**cd**, **verify**、**mkdir**、**fsck**

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の設定

このモジュールでは、ルータを Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）または Reverse Address Resolution Protocol（RARP; 逆アドレス解決プロトコル）サーバとして設定する方法、非同期インターフェイスを通して拡張 BOOTP 要求を転送するようルータを設定する方法、および Cisco IOS Release 12.2 での rcp、rsh、FTP の設定方法について説明します。

この章で述べられているファイル転送機能コマンドについて、詳しくは、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。

基本ファイル転送サービスの設定作業リスト

基本ファイル転送サービスを設定するには、次の項で説明されている作業のいずれかを実行します。

- 「ルータを TFTP または RARP サーバとして設定」
- 「システム BOOTP パラメータの設定」
- 「rsh および rcp 使用時のルータ設定」
- 「FTP 接続使用時のルータ設定」

この章のすべての作業は任意です。

ルータを TFTP または RARP サーバとして設定

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。

ルータを TFTP サーバに設定

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:**、**slaveslot1:**）から 1 つを選ぶことができるものもあります。

次の説明では、1 台の Cisco 7000 ルータが *フラッシュ サーバ*と呼ばれ、他のルータはすべて *クライアント ルータ*と呼ばれています。フラッシュ サーバとクライアント ルータのコンフィギュレーション例には、必要なだけのコマンドが含まれています。

TFTP ルータ設定の前提作業

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** コマンドの発行後、接続可能かどうかが一連の感嘆符（!）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、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た後にクライアントが X.25 の機能を持つようになることはありません。

TFTP サーバのイネーブル化

TFTP サーバの動作をオンにするには、次のコマンドを実行します。特権 EXEC モードで始めます。

	コマンド	目的
ステップ 1	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。
ステップ 2	Router(config)# **tftp-server flash** [*partition-number*:]*filename1* [**alias** *filename2*] [*access-list-number*] または Router(config)# **tftp-server flash** *device*:*filename* (Cisco 7000 family only) または Router(config)# **tftp-server flash** [*device*:][*partition-number*:]*filename* (Cisco 1600 series and Cisco 3600 series only) または Router(config)# **tftp-server rom alias** *filename1* [*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。
ステップ 3	Router(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 4	Router# **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。

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。

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 を使用してそ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* ファイルに対する 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* のコピーを送信する例です。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 内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#
```

クライアント ルータの設定作業

最初にサーバからシステム イメージをロードするよう、クライアント ルータを設定します。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にクライアント ルータを設定します。クライアント ルータを設定するには、次のコマンドを使用します。特権 EXEC モードで始めます。

	コマンド	目的
ステップ 1	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。
ステップ 2	Router(config)# **no boot system**	（任意）これまでの **boot system** 文すべてを、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 3	Router(config)# **boot system** [**tftp**] *filename* [*ip-address*]	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 4	Router(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 5	Router(config)# **config-register** *value*	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 6	Router(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 7	Router# **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 8	Router# **reload**	（任意）変更を有効にするため、ルータをリロードします。

システムをリロードした後、**show version** EXEC モード コマンドを使用して、システムが希望のイメージで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、**no boot system** 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。

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 172.16.111.111
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、**no boot system** 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 **boot system** 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 **boot system** 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 **boot system** *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。これに失敗すると、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た **boot system rom** 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。**copy running-config startup-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 メモリでない場合、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 **show version** コマンドを実行したサンプル出力を示します。

```
Router> 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 内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。

ルータを RARP サーバに設定

Reverse Address Resolution Protocol（RARP; 逆アドレス解決プロトコル）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。この機能は、ホストがネットワーク レイヤの特定の IP アドレスに対応する物理レイヤの MAC アドレスをダイナミックに見つけるために使用される Address Resolution Protocols（ARP; アドレス解決プロトコル）のブロードキャストとちょうど逆の機能になります。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。

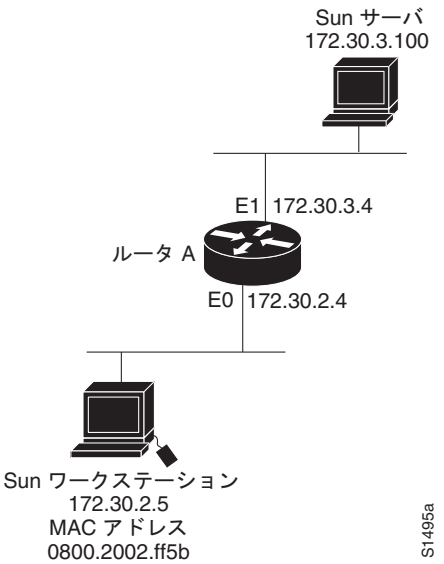
Cisco ルータは RARP サーバとして設定可能です。この機能により、Cisco IOS ソフトウェアが RARP 要求に応答できるようになります。

ルータを RARP サーバとして設定するには、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。

コマンド	目的
`Router(config)# interface type [slot/]port`	RARP サービスの設定を行うインターフェイスを指定し、その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 モードに入ります。
`Router(config-if)# ip rarp-server ip-address`	ルータで RARP サービスをイネーブルにします。

図 13 に、ルータをディスクレス ワークステーションの RARP サーバとして動作するよう設定するネットワーク設定を示します。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 13　ルータを RARP サーバに設定



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 ethernet 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 クライアントとサーバの IP アドレスは、現行の SunOS *rpc.bootparamd* デーモンの制限により、同一のメジャー ネットワーク番号を使用している必要があります。

次の例では、アクセス サーバが RARP サーバとして動作するよう設定されます。

```
! 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 ethernet 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
```

システム BOOTP パラメータの設定

非同期インターフェイス用 Boot Protocol（BOOTP）サーバは、拡張された BOOTP 要求（RFC 1084 で定義されたもの）をサポートしています。補助ポートを非同期インターフェイスとして使用する場合、次のコマンドが役立ちます。

非同期インターフェイス用拡張 BOOTP パラメータを設定するには、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。

コマンド	目的
Router(config)# **async-bootp** *tag* [:*hostname*] *data*	非同期インターフェイス用拡張 BOOTP 要求を設定します。

次のコマンドを EXEC モードで使用すると、BOOTP 応答内で送信される拡張されたデータを表示できます。

コマンド	目的
Router# **show async bootp**	BOOTP 応答のパラメータを表示します。

たとえば、DNS サーバのアドレスが BOOTP 応答の拡張データとして指定された場合、次のような出力が表示されます。

```
Router# show async bootp
The following extended data will be sent in BOOTP responses:

dns-server 172.22.53.210
```

ご使用のシスコ デバイスを BOOTP サーバとして設定することについて、詳しくは「Using AutoInstall and Setup」の章を参照してください。

rsh および rcp 使用時のルータ設定

Remote Shell（RSH; リモート シェル）を使用すると、ユーザはコマンドをリモートで実行できるようになります。Remote Copy（RCP; リモート コピー）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、業界の標準的実装と相互運用できます。シスコは、rsh と rcp の両方を指すのに RCMD（リモート コマンド）という略語を使用しています。

この項は、次の各部にわかれています。

- 「発信 RCMD コミュニケーションの発信元インターフェイス指定」
- 「RCMD のための DNS 逆ルックアップ」
- 「rsh の使用とイネーブル化」
- 「rcp のイネーブル化と使用」

発信 RCMD コミュニケーションの発信元インターフェイス指定

RCMD（rsh および rcp）コミュニケーションの発信元インターフェイスを指定できます。たとえば、RCMD コネクションがループバック インターフェイスをルータから出て行くパケットすべての送信元アドレスとして使用するよう、ルータを設定できます。RCMP に関連付けるインターフェイスを指定するには、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。

コマンド	目的
`Router(config)# ip rcmd source-interface interface-id`	発信 rsh および rcp トラフィックすべてのラベルとして使用するインターフェイスのアドレスを指定します。

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、パーマネント IP アドレスを RCMD コミュニケーションと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）。セキュリティ上の理由から、「既知の」IP アドレスが使用されることもあります。そうすることで、リモート デバイスにそのアドレスを含むアクセス リストを作成できます。

RCMD のための DNS 逆ルックアップ

Cisco IOS ソフトウェアは、基本的なセキュリティ チェックとして、リモート コマンド（RCMD）アプリケーション（rsh および rcp）のために、DNS を使用してクライアント IP アドレスの逆ルックアップを行います。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。その後、そのホスト名の IP アドレスの DNS 要求が行われます。受取った IP アドレスが、元の要求元アドレスと照合されます。アドレスが DNS から受け取ったどのアドレスとも一致しない場合、rcmd 要求は実行されません。

この逆ルックアップは、「スプーフィング」の防止策とされています。ただし、このプロセスで確認できるのは、IP アドレスがルーティングできる有効なアドレスかどうかだけである点に注意してください。ハッカーが既知のホストの有効な IP アドレスでスプーフする可能性は残っています。

この機能は、デフォルトでイネーブルにされています。次のコマンドをグローバル コンフィギュレーション モードで実行して、RCMD（rsh および rcp）アクセスの DNS チェックをディセーブルにできます。

コマンド	目的
`Router(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。

rsh の使用とイネーブル化

rsh（リモート シェル）を使用して、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スタートします。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 をイネーブル化するコンフィギュレーション コマンドは、「remote command」の略語である「rcmd」を使用します。

rsh セキュリティの維持

UNIX ホストのように rsh が動作しているリモート システム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させ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* ファイルによってそのシステムでリモートからコマンドを実行可能なユーザを識別します。

ルータで rsh サポートをイネーブルにすることで、リモート システムのユーザがコマンドを実行することを可能にできます。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するユーザによるルータへのアクセスを制御するために、ローカル認証データベースを設定する必要があります。ローカル認証データベースは、UNIX の *.rhosts* ファイルに類似しています。認証データベースで設定する各エントリで、ローカル ユーザ、リモート ホスト、リモート ユーザを識別します。

リモート ユーザによる rsh を使用したコマンド実行を許可するルータ設定

ルータを rsh サーバとして設定するには、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実行します。

	コマンド	目的
ステップ 1	`Router(config)# ip rcmd remote-host` *local-username* {*ip-address* | *host*} *remote-username* [**enable** [*level*]]	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 2	`Router(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。

ソフトウェアの受信 rsh コマンドのサポートをディセーブルにするには、**no ip rcmd rsh-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。

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
```

rmtnetad1 および *netadmin4* という名前のユーザは、両者とも IP アドレス 172.16.101.101 のリモート ホスト上にいます。ユーザは両方とも同じリモート ホスト上にいますが、それぞれのユーザのために専用のエントリを含める必要があります。ユーザは両方とも、ルータへの接続と、ルータが rsh をイネーブル化した後にリモートからルータ上で rsh コマンドを実行することを許可されます。*netadmin4* という名前のユーザは、ルータ上で特権 EXEC モード 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 2 つのエントリは、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イネーブルにします。

.

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 シェル プロトコルをサポートするネットワーク サーバ上で、リモートからコマンドを実行させることができます。このコマンドを使用するには、ネットワーク サーバの *.rhosts* ファイル（または同等のファイル）に、そのホスト上でのリモートからのコマンド実行を許可するエントリが含まれている必要があります。

UNIX システムのようにリモート サーバがディレクトリ構造を有している場合、発行した rsh コマンドは **/user** *username* というキーワードと引数のペアで指定したリモート ユーザ アカウントのディレクトリから、リモートで実行されます。

/user キーワードと引数を指定しなかった場合、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。

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。

	コマンド	目的
ステップ 1	`Router> enable [password]`	特権 EXEC モードを開始します。
ステップ 2	`Router# rsh {ip-address | host} [/user username] remote-command`	rsh を使用してリモートからコマンドを実行します。

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。

```
Router# enable
```

```
Router# rsh mysys.cisco.com /user sharon ls -a
.
..
.alias
.cshrc
.emacs
.exrc
.history
.login
.mailrc
.newsrc
.oldnewsrc
.rhosts
.twmrc
.xsession
jazz
Router#
```

rcp のイネーブル化と使用

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 サーバのように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 システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーする以上、コピー元ファイルの読み取り権限と、コピー先ディレクトリの書き込み権限が必要になります。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 実装機能をエミュレートした、ファイルをネットワーク上のシステム間でコピーするものですが、シスコのコマンド構文は UNIX の rcp コマンド構文と異なっています。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。これらの改善は、rcp のトランスポート メカニズムがコネクション型の Transmission Control Protocol/Internet Protocol（TCP/IP）スタック上に構築されており、これを使用しているために可能になりました。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。

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。

	コマンド	目的
ステップ 1	`Router(config)# ip rcmd remote-host` *local-username* {*ip-address* | *host*} *remote-username* [**enable** [*level*]]	ローカル認証データベースで、rcp 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 2	`Router(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。

ソフトウェアの受信 rcp 要求のサポートをディセーブルにするには、**no ip rcmd rcp-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。

次の例に、リモート ユーザ用に認証データベースに 2 つのエントリを追加し、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イネーブルに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 2 つのエントリは、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 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（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 経由でルータに接続しており、**username** コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。

（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、元の UNIX の端末だった *teletype* を表す *TTY デバイス* と呼ばれています。

3. 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
```

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 のための *.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できます。

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。

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。

コマンド	目的
`Router(config)# ip rcmd remote-username username`	リモート ユーザ名を指定します。

リモート ユーザ名を削除してデフォルト値に戻す場合、**no ip rcmd remote-username** コマンドを使用します。

FTP 接続使用時のルータ設定

File Transfer Protocol（FTP; ファイル転送プロトコル）を使用してネットワーク上のシステム間でファイルを転送するようルータを設定します。Cisco IOS の FTP 実装では、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

FTP 特性を設定するには、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のいずれかを使用します。

コマンド	目的
`Router(config)# ip ftp username string`	FTP 接続で使用されるユーザ名を指定します。
`Router(config)# ip ftp password [type] password`	FTP 接続で使用されるパスワードを指定します。

`Router(config)# ip ftp passive`
または
`Router(config)# no ip ftp passive`
	パッシブ モード FTP 接続だけを使用するよう、ルータを設定します。
	または
	すべての種類の FTP 接続を許可します（デフォルト）。

`Router(config)# ip ftp source-interface interface`	FTP 接続の発信元 IP アドレスを指定します。

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、パスワード sword を使用して、IP アドレス 192.168.10.3 の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 creates the core dump in the event the system at IP address
! 192.168.10.3 crashes
exception dump 192.168.10.3
```

HTTP または HTTPS を使用したファイルの転送

Cisco IOS Release 12.4 では、使用する 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 や HTTP Secure（HTTPS; HTTP セキュア）プロトコルを使用してファイル転送を行う機能が準備されています。Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドのうち、ファイル システム プレフィクスを使用する **copy** などのコマンドで、送信元や宛先を指定する際に HTTP や HTTPS を使用した位置指定が可能になりました。

機能情報の入手方法

最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「HTTP または HTTPS を使用したファイル転送の機能情報」（P.14）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 Cisco IOS と Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

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」（P.12）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の制約事項

ネットワークからネットワークへのコピーができないといった **copy** コマンドに存在した制限は、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 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ついて

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 **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 イメージファイルやコア 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 セキュア転送に埋め込み HTTPS クライアントを使用して、Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）のコンテキスト内でのセキュアな認証済みファイル転送を行えます。

HTTP または HTTPS を使用したファイル転送方法

ここでは、次の各手順について説明します。

- 「ファイル転送の HTTP 接続特性の設定」（P.3）（必要な場合）
- 「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」（P.5）（必須）
- 「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」（P.7）（必須）
- 「HTTP を使用したファイル転送の維持とモニタリング」（P.9）（任意）

（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** | **idle timeout** *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。 • 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：** `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。
ステップ 3	**ip http client connection** {**forceclose** | **idle timeout** *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**：デフォルトの持続的接続をディセーブルにします。 • **idle timeout** *seconds*：アイドル接続の許容時間を 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ときに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。例として、「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：例」（P.10）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ときに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。例として、「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：例」（P.10）を参照してください。

	コマンドまたはアクション	目的
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 サーバのポート番号を指定します。
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`
	`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. **copy** [**/erase**] [**/noverify**] **http://***remote-source-url local-destination-url*

   または

   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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**copy** [**/erase**] [**/noverify**] **http://***remote-source-url local-destination-url*
	
	または
	
	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 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ディセーブルになります。
		• *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、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* 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、**ip http client username** および **ip http client password** グローバル コンフィギュレーション コマンドによるこれらの認証ストリング指定の代わりになります。
		• *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、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、詳しくは「その他の関連資料」（P.11）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、**debug ip http client all** 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. **copy** [**/erase**] [**/noverify**] *local-source-url* **http://***remote-destination-url*

   または

   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。 • 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	**copy** [**/erase**] [**/noverify**] *local-source-url* **http://***remote-destination-url*
	
	または
	
	copy *local-source-url* **https://***remote-destination-url*
	
	例：
	`Router# http://user1:mypassword@209.165.202.129:8080/image_files/c7200-i-mx_backup`
	
	例：
	`Router# copy flash:c7200-i-mx 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。
		• **/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ディセーブルになります。
		• *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、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* 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、**ip http client username** および **ip http client password** グローバル コンフィギュレーション コマンドによるこれらの認証ストリング指定の代わりになります。
		• *remote-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、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、詳しくは「その他の関連資料」（P.11）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、**debug ip http client all** 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。 • 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	**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

ここでは、次の設定例について説明します。

- 「ファイル転送の HTTP 接続特性の設定：例」（P.10）
- 「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：例」（P.10）
- 「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：例」（P.10）
- 「リモート HTTP サーバからフラッシュ メモリへのファイル ダウンロード：例」（P.11）

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：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：例

次の例に、フラッシュ メモリからリモート HTTP サーバへファイルをコピーする方法を示します。この例は、**copy** 特権 EXEC コマンドを使用したファイル転送で予想されるプロンプトと表示内容を示しています。

```
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 ダウンロード: 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。この例は、**copy** 特権 EXEC コマンドを使用したファイル転送で予想されるプロンプトと表示内容を示しています。

```
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 ...
```

その他の関連資料

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	参照先
セキュアな HTTP コミュニケーション	『*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 埋め込み Web クライアント	『*HTTP 1.1 Client*』
ネットワーク管理コマンド：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 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*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットに対する MIB を特定してダウンロードするには、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
RFC 2616	『*Hypertext Transfer Protocol -- HTTP/1.1*』、R.Fielding, et al.
RFC 2617	『*HTTP Authentication: Basic and Digest Access Authentication*』、J. Franks, et al.

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

HTTP または HTTPS を使用したファイル転送の機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/fn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

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へファイルをコピーできます。 この機能に関する詳細については、次の項を参照してください。 • 「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」（P.5）

表 1　HTTP または HTTPS を使用したファイル転送の機能情報（続き）

機能名	リリース	機能情報
HTTP を使用したファイルのアップロード	12.3(7)T	この機能に関する詳細については、次の項を参照してください。 • 「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」（P.7）
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 ファイルやコア 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。 この機能は、Cisco IOS ソフトウェアベースのプラットフォームから、HTTP と HTTPS のいずれかを使用して、HTTP サーバへファイルをコピーすることをサポートします。 この機能に関する詳細については、次の各項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ついて」（P.2） • 「HTTP または HTTPS を使用したファイル転送方法」（P.2）

着信 RSH および RCP 要求の ACL 認証

機能の履歴

リリース	変更点
12.2(8)T	この機能が導入されました。

このマニュアルでは、Cisco IOS Release 12.2(8)T の着信 RSH および RCP 要求の ACL 認証機能について説明します。次の項で構成されています。

機能の概要

Cisco IOS ソフトウェアをイネーブルにして着信 Remote Shell（RSH; リモート シェル）プロトコルおよび Remote Copy Protocol（RCP; リモート コピー プロトコル）要求を受信するには、認証データベースを設定して、ルータへのアクセスを制御する必要があります。この設定は **ip rcmd remote-host** コマンドを使用して実行できます。

現在、このコマンドを使用するときには、データベース認証コンフィギュレーションでローカル ユーザ、リモート ホスト、およびリモート ユーザを指定する必要があります。複数ホストからルータへのコマンドを実行できる場合は、次に示す各ホストにつき 1 つずつ、複数データベース認証コンフィギュレーション エントリを使用する必要があります。

```
ip rcmd remote-host local-user1 remote-host1 remote-user1
ip rcmd remote-host local-user1 remote-host2 remote-user1
ip rcmd remote-host local-user1 remote-host3 remote-user1
ip rcmd remote-host local-user1 remote-host4 remote-user1
```

この機能では、指定されたユーザのアクセス リストを指定できます。アクセス リストはユーザがアクセスできるホストを指定します。追加された新しい引数 *access-list* をこのコマンドとともに使用して、次のようにアクセス リストを指定できます。

```
ip rcmd remote-host local-user1 access-list remote-user1
```

アクセス リストで指定したホストへのアクセスをユーザに許可するには、まずアクセス リストを定義します。アクセス リストが定義されていない場合は、ホストへのアクセスは拒否されます。アクセス リストの定義については、『*Cisco IOS Security Configuration Guide*, Release 12.2』を参照してください。

修正された **ip rcmd remote-host** コマンドの使用については、このマニュアルの後半の 「コマンド リファレンス」の項を参照してください。

関連資料

- 『*Cisco IOS Configuration Fundamentals Command Reference,* Release 12.2』
- 『*Cisco IOS Security Configuration Guide*, Release 12.2』
- 『*Cisco IOS Security Command Reference,* Release 12.2』

サポートされているプラットフォーム

- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1400 シリーズ
- Cisco 1600 シリーズ
- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 2420
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 2500 シリーズ
- Cisco 2600 シリーズ
- Cisco 7100 シリーズ
- Cisco 7200 シリーズ
- Cisco 7500 シリーズ
- Cisco uBR7200 シリーズ
- Cisco Voice Gateway 200
- Universal Route Module（URM）

Cisco Feature Navigator を使用したプラットフォーム サポートの特定

Cisco IOS ソフトウェアは、特定のプラットフォームがサポートされている機能セットにパッケージングされています。この機能のプラットフォーム サポートに関連した更新情報を取得するには、Cisco Feature Navigator にアクセスします。新しいプラットフォーム サポートが機能に追加されると、Cisco Feature Navigator によって、サポートされているプラットフォームのリストが自動的に更新されます。

Cisco Feature Navigator は Web ベースのツールであり、特定の機能セットがサポートされている Cisco IOS ソフトウェア イメージ、および、特定の Cisco IOS イメージ内でサポートされている機能を素早く特定できます。機能またはリリースごとに検索できます。リリース セクションでは、各リリースを横に並べて比較し、各ソフトウェア リリースに固有の機能と共通機能の両方を表示できます。

Cisco Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E メールで届きます。資格のあるユーザは、http://www.cisco.com/register にある指示に従って、Cisco.com 上にアカウントを作成できます。

Cisco Feature Navigator は定期的に更新されています（Cisco IOS ソフトウェアの主要なリリース時およびテクノロジー リリース時）。最新情報については、次の URL から Cisco Feature Navigator ホームページにアクセスしてください。

http://www.cisco.com/go/fn

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **ip rcmd remote-host**

コンフィギュレーション ファイルの管理

コンフィギュレーション ファイルの管理

この章では、コンフィギュレーション ファイルを作成、ロード、および保守する方法について説明します。コンフィギュレーション ファイルには、現在のシスコ製ルーティング デバイスの機能性をカスタマイズする、ユーザ設定コマンド セットが含まれます。

この章で説明する作業は、現在のシステムで少なくとも最小限の設定を実行していることが前提となっています。**setup** コマンドを使用して基本的なコンフィギュレーション ファイルを作成できます（詳細については、『Using Setup Mode to Configure a Cisco Networking Device』を参照してください）。

この章で扱うコンフィギュレーション ファイル管理コマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。詳細については、『About Cisco IOS Software Documentation』の章を参照してください。

この章で紹介する機能情報の入手方法

使用する Cisco IOS ソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「コンフィギュレーション ファイルの管理の機能情報」（P.31）を参照してください。

プラットフォームと Cisco IOS および Catalyst OS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーション ファイルの概要

コンフィギュレーション ファイルには、現在のシスコ製ルーティング デバイス（ルータ、アクセス サーバ、スイッチなど）の機能をカスタマイズするために使用される、Cisco IOS ソフトウェア コマンドが含まれています。コマンドは、システムを起動したとき（startup-config ファイルから）、またはコンフィギュレーション モードで CLI にコマンドを入力したときに、Cisco IOS ソフトウェアによって解析（変換および実行）されます。

コンフィギュレーション ファイルのタイプ

スタートアップ コンフィギュレーション ファイル（startup-config）は、ソフトウェアを設定するためにシステムの起動時に使用されます。実行コンフィギュレーション ファイル（running-config）には、ソフトウェアの現在の設定が含まれています。2 つのコンフィギュレーション ファイルは異なっている可能性があります。たとえば、コンフィギュレーションを永続的ではなく短期間で変更する場合があります。このような場合、**configure terminal** EXEC コマンドを使用して実行コンフィギュレーションを変更しますが、**copy running-config startup-config** EXEC コマンドを使用して設定を保存することはありません。

実行コンフィギュレーションを変更するには、この章の「CLI でのコンフィギュレーション ファイルの変更」の項の説明に従って、**configure terminal** コマンドを使用します。Cisco IOS コンフィギュレーション モードの使用時には、通常コマンドはすぐに実行され、入力直後またはコンフィギュレーション モードを終了した時点で実行コンフィギュレーション ファイルに保存されます。

スタートアップ コンフィギュレーション ファイルを変更するには、**copy running-config startup-config** EXEC コマンドを使用してスタートアップ コンフィギュレーションに実行コンフィギュレーション ファイルを保存するか、ファイル サーバからスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします（詳細については、「ネットワーク サーバからルータへのコンフィギュレーション ファイルのコピー」の項を参照してください）。

コンフィギュレーション ファイルの場所

コンフィギュレーション ファイルは、次の場所に格納されます。

- 実行コンフィギュレーションは RAM に格納されます。
- クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、スタートアップ コンフィギュレーションは Nonvolatile Random-Access Memory（NVRAM; 不揮発性 RAM）に格納されます。
- クラス A フラッシュ ファイル システムのプラットフォーム上では、スタートアップ コンフィギュレーションは CONFIG_FILE 環境変数で指定された場所に格納されます（詳細については、「クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定」の項を参照してください）。CONFIG_FILE 変数は、デフォルトでは NVRAM になりますが、次のファイル システムのファイルも指定できます。
  - **nvram:**（NVRAM）
  - **bootflash:**（内部フラッシュ メモリ）
  - **slot0:**（PCMCIA の第 1 スロット）
  - **slot1:**（PCMCIA の第 2 スロット）

コンフィギュレーション ファイルの管理の作業リスト

Cisco IOS ソフトウェア コンフィギュレーション ファイルの管理を理解するには、次の項で説明する作業を実行します。

コンフィギュレーション ファイル情報の表示

コンフィギュレーション ファイルに関する情報を表示するには、必要に応じて EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show bootvar**	BOOT 環境変数の内容、CONFIG_FILE 環境変数によって指定されているコンフィギュレーション ファイルの名前、および BOOTLDR 環境変数の内容を示します。
Router# **more** *file-url*	指定されたファイルの内容を表示します。
Router# **show running-config**	実行コンフィギュレーション ファイルの内容を表示します（**more system:running-config** コマンドのコマンド エイリアス）。
Router# **show startup-config**	スタートアップ コンフィギュレーション ファイルの内容を表示します（**more nvram:startup-config** コマンドのコマンド エイリアス）。 クラス A フラッシュ ファイル システム プラットフォーム以外のすべてのプラットフォーム上では、通常、デフォルトの startup-config ファイルは NVRAM に格納されます。クラス A フラッシュ ファイル システム プラットフォーム上では、CONFIG_FILE 環境変数はデフォルトの startup-config ファイルを指定します。CONFIG_FILE 変数のデフォルトは NVRAM になります。

コンフィギュレーション モードの開始とコンフィギュレーション ソースの選択

ルータ上でコンフィギュレーション モードを開始するには、特権 EXEC プロンプトで **configure** コマンドを入力します。Cisco IOS ソフトウェアは次のプロンプトで応答し、端末、メモリ、またはネットワーク サーバ（ネットワーク）上に格納されたファイルのいずれかを、コンフィギュレーション コマンドのソースとして指定するように要求されます。

```
Configuring from terminal, memory, or network [terminal]?
```

端末からの設定では、コマンドラインにコンフィギュレーション コマンドを入力できます（次の項を参照してください）。メモリからの設定では、スタートアップ コンフィギュレーション ファイルがロードされます。詳細については、「スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行」の項を参照してください。ネットワークからの設定では、ネットワーク経由でコンフィギュレーション コマンドをロードして実行できます。詳細については、「ネットワーク サーバからルータへのコンフィギュレーション ファイルのコピー」の項を参照してください。

CLI でのコンフィギュレーション ファイルの変更

Cisco IOS ソフトウェアは、1 行につき 1 つのコンフィギュレーション コマンドを受け入れます。コンフィギュレーション コマンドは、必要なだけ入力できます。

コンフィギュレーション ファイルには、入力したコマンドを説明するコメントを追加できます。コメントの先頭には、感嘆符（!）を付けます。コメントは NVRAM にもコンフィギュレーション ファイルのアクティブ コピーにも格納*されない*ため、**show running-config** または **more system:running-config** EXEC コマンドでアクティブな設定のリストを表示しても、コメントは表示されません。また、**show startup-config** または **more nvram:startup-config** EXEC モード コマンドでスタートアップ コンフィギュレーションのリストを表示しても、コメントは表示されません。コメントは、コンフィギュレーション ファイルがルータにロードされたときにコンフィギュレーション ファイルから削除されます。ただし、File Transfer Protocol（FTP; ファイル転送プロトコル）、Remote Copy Protocol（RCP; リモート コピー プロトコル）、または Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバ上に格納されているコンフィギュレーション ファイルのコメントのリストは表示できます。

CLI を使用してソフトウェアは設定するときは、ユーザの入力に従ってソフトウェアによりコマンドが実行されます。CLI を使用してソフトウェアを設定するには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`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。
ステップ 2		必要なコンフィギュレーション コマンドを入力します。Cisco IOS マニュアル セットに、テクノロジー別に編成されたコンフィギュレーション コマンドが説明されています。

ステップ 3	`Router(config)# end`
	または
	`Router(config)# ^Z`
		コンフィギュレーション セッションを終了し、EXEC モードに戻ります。
		（注） Ctrl キーと Z キーを同時に押すと、画面に ^Z と表示されます。

ステップ 4	`Router# copy system:running-config nvram:startup-config`	実行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 ファイルとして保存します。 **copy running-config startup-config** コマンド エイリアスも使用できますが、このコマンドは精度が高くないため、注意する必要があります。ほとんどのプラットフォーム上では、このコマンドによりコンフィギュレーションは NVRAM に保存されます。クラス A フラッシュ ファイル システムのプラットフォーム上では、この手順によりコンフィギュレーションは CONFIG_FILE 環境変数によって指定された場所に保存されます（デフォルトの CONFIG_FILE 変数では、ファイルの保存先は NVRAM に指定されています）。

次の例では、ルータのルータ プロンプト名が設定されています。感嘆符（!）で示されたコメント行では、いずれのコマンドも実行されません。

この例では、**hostname** コマンドはルータ名を Router から new_name に変更するために使用されています。Ctrl+Z（^Z）キーを押すか、**end** コマンドを入力すると、コンフィギュレーション モードが終了します。**copy system:running-config nvram:startup-config** コマンドにより、現在のコンフィギュレーションがスタートアップ コンフィギュレーションに保存されます。

```
Router# configure terminal
Router(config)# !The following command provides the router host name.
Router(config)# hostname new_name
new_name(config)# end
```

```
new_name# copy system:running-config nvram:startup-config
```

スタートアップ コンフィギュレーションが NVRAM にある場合は、スタートアップ コンフィギュレーションには現在の設定情報がコンフィギュレーション コマンドとしてテキスト形式で格納され、デフォルト以外の設定だけが記録されます。破損データから保護するために、メモリはチェックサム算出されます。

（注） 一部の特定のコマンドは、NVRAM に保存されない場合があります。これらのコマンドは、マシンをリブートしたときに再入力する必要があります。これらのコマンドは、マニュアルに記載されています。リブート後にすばやくルータを再設定できるように、これらの設定のリストを持っておくことを推奨します。

ルータからネットワークサーバへのコンフィギュレーション ファイルのコピー

FTP、rcp、または TFTP を使用して、ルータからファイル サーバへコンフィギュレーション ファイルをコピーできます。たとえば、内容を変更する前に現在のコンフィギュレーション ファイルのバックアップをサーバに作成するためにこの作業を実行します。これにより、後で元のコンフィギュレーション ファイルをサーバから復元できます。

ルータからサーバへコンフィギュレーション ファイルをコピーするには、次の項で説明する作業を実行します。

- 「ルータから TFTP サーバへのコンフィギュレーション ファイルのコピー」
- 「ルータから rcp サーバへのコンフィギュレーション ファイルのコピー」
- 「ルータから FTP サーバへのコンフィギュレーション ファイルのコピー」

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これは、FTP および rcp がコネクション型の TCP/IP スタックを使用しているためです。

ルータから TFTP サーバへのコンフィギュレーション ファイルのコピー

一部の TFTP 実装では、TFTP サーバ上にダミー ファイルを作成し、読み取り、書き込み、および実行を許可してから、ダミー ファイルを上書きする形でファイルをコピーする必要があります。詳細については、ご使用の TFTP のマニュアルを参照してください。

設定情報を TFTP ネットワーク サーバ上にコピーするには、必要に応じて EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **copy system:running-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]	TFTP サーバへ実行コンフィギュレーション ファイルをコピーします。
Router# **copy nvram:startup-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]	TFTP サーバへスタートアップ コンフィギュレーション ファイルをコピーします。

copy コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

次に、ルータから TFTP サーバへコンフィギュレーション ファイルをコピーする例を示します。

```
Tokyo# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y

Writing tokyo-confg!!! [OK]
```

ルータから rcp サーバへのコンフィギュレーション ファイルのコピー

ルータから rcp サーバへコンフィギュレーション ファイルをコピーできます。

ネットワークを UNIX コミュニティでリソースとして使用する最初の試みの 1 つは、Remote Shell（RSH; リモート シェル）およびリモート コピー（rcp）機能が含まれた、リモート シェル プロトコルの設計および実装につながりました。rsh および rcp により、ユーザはリモートでコマンドを実行し、ネットワーク上のリモート ホストまたはサーバにあるファイル システムからまたはファイル システムへファイルをコピーすることが可能になります。シスコの rsh および rcp 実装は、標準実装と相互運用できます。

rcp の **copy** コマンドは、リモート システム上の 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ために、TFTP のように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 システムは rsh をサポートしています）。ファイルをある場所から別の場所へコピーするため、コピー元ファイルに対する読み取り権限と、コピー先ファイル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。シスコの rcp サポートは、rcp をトランスポート メカニズムとして使用する **copy** コマンドのセットを提供しています。これらの rcp **copy** コマンドは、シスコの TFTP **copy** コマンドに類似していますが、高速で信頼性の高いデータ配信を実現する代替方法を備えている点が異なります。これらの改善は、rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。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し、リモート システムのユーザがルータからまたはルータへファイルをコピーできるようにすることも可能です。

リモート ユーザがルータからまたはルータへファイルをコピーできるように Cisco IOS ソフトウェアを設定するには、**ip rcmd rcp-enable** グローバル コンフィギュレーション コマンドを使用します。

rcp ユーザ名について

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 を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 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 経由でルータに接続しており、**username** コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。

4. ルータのホスト名。

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。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書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、そのユーザの名前をリモート ユーザ名として指定できます。

ip rcmd remote-username コマンドを使用して、すべてのコピーに対してユーザ名を指定します（rcmd は、スーパーユーザ レベルで使用される UNIX ルーチンで、予約されたポート番号に基づいた認証スキームを使用してリモート マシン上でコマンドを実行します。rcmd は「Remote Command（リモート コマンド）」の略です）。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

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
```

ルータの IP アドレスが Router1.company.com に変換される場合、rcp サーバ上の User0 の .rhosts ファイルには、次の行が含まれているはずです。

```
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。

ルータから rcp サーバへのコンフィギュレーション ファイルのコピー

ルータから rcp サーバへスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをコピーするには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **configure terminal**	（任意）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 2	Router(config)# **ip rcmd remote-username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 3	Router(config)# **end**	（任意）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 4	Router# **copy system:running-config rcp:**[[[**//**[*username***@**]*location*]**/***directory*]**/***filename*]	ルータの実行コンフィギュレーション ファイルが rcp サーバ上に格納されることを指定します。
	または	または
	Router# **copy nvram:startup-config rcp:**[[[**//**[*username***@**]*location*]**/***directory*]**/***filename*]	ルータのスタートアップ コンフィギュレーション ファイルが rcp サーバ上に格納されることを指定します。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcp サーバ上に実行コンフィギュレーション ファイルを格納する例

次に、rtr2-confg という名前の実行コンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
Router# copy system:running-config rcp://netadmin1@172.16.101.101/Rtr2-confg
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Router#
```

rcp サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例

次に、rcp を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
Rtr2# configure terminal
Rtr2(config)# ip rcmd remote-username netadmin2
Rtr2(config)# end
Rtr2# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
![OK]
```

ルータから FTP サーバへのコンフィギュレーション ファイルのコピー

ルータから FTP サーバへコンフィギュレーション ファイルをコピーできます。

FTP ユーザ名およびパスワードの概要

FTP プロトコルでは、クライアントは FTP 要求ごとにリモート ユーザ名およびパスワードをサーバに送信する必要があります。FTP を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 匿名。

ルータは次の順番で最初に発見した有効なパスワードを送信します。

1. **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. ルータは、*username@routername.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバ上のアカウントと関連付けら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 FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

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、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、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。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** 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、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** EXEC コマンドにユーザ名を含めます。

ルータから FTP サーバへのコンフィギュレーション ファイルのコピー

ルータから FTP サーバへスタートアップ コンフィギュレーション ファイルまたは実行コンフィギュレーション ファイルをコピーするには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **configure terminal**	（任意）端末からコンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 2	Router(config)# **ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 3	Router(config)# **ip ftp password** *password*	（任意）デフォルトのパスワードを指定します。
ステップ 4	Router(config)# **end**	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 5	Router# **copy system:running-config ftp:**[[[**//**[*username*[:*password*]**@**]*location*] **/***directory*]**/***filename*] または Router# **copy nvram:startup-config ftp:**[[[**//**[*username*[:*password*]**@**]*location*] **/***directory*]**/***filename*]	FTP サーバへ実行コンフィギュレーションまたはスタートアップ コンフィギュレーション ファイルをコピーします。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

FTP サーバ上に実行コンフィギュレーション ファイルを格納する例

次に、rtr2-confg という名前の実行コンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート ホスト上の netadmin1 ディレクトリにコピーする例を示します。

```
Router# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/Rtr2-confg
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
Router#
```

FTP サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例

次に、FTP を使用してファイルをコピーすることによって、サーバ上にスタートアップ コンフィギュレーション ファイルを格納する例を示します。

```
Rtr2# configure terminal
Rtr2(config)# ip ftp username netadmin2
Rtr2(config)# ip ftp password mypass
```

```
Rtr2(config)# end
Rtr2# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
![OK]
```

ネットワークサーバからルータへのコンフィギュレーション ファイルのコピー

TFTP、rcp、または FTP サーバからルータの実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーできます。この機能は、次のいずれかの理由により実行する場合があります。

- バックアップしたコンフィギュレーション ファイルを復元するため。
- 別のルータにコンフィギュレーション ファイルを使用するため。たとえば、別のルータをネットワークに追加して、そのルータのコンフィギュレーションを元のルータと同様にする場合です。新しいルータにファイルをコピーすることにより、ファイル全体を再作成するのではなく、該当部分を変更できます。
- 同一のコンフィギュレーション コマンドをネットワーク内のすべてのルータにロードして、すべてのルータのコンフィギュレーションを同様にするため。

コマンドラインにコマンドを入力した場合と同様に、**copy** {**ftp:** | **rcp:** | **tftp:**} **system:running-config** EXEC コマンドはルータにコンフィギュレーション ファイルをロードします。コマンドを追加する前に、ルータにより既存の実行コンフィギュレーションが消去されることはありません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられた場合、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに含まれている特定のコマンドの IP アドレスが、既存のコンフィギュレーションと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内の一部のコマンドには、置き換えられたり無効になったりしないものもあります。このような場合、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルで混成されたコンフィギュレーション ファイルが作成され、コピーされたコンフィギュレーション ファイルが優先されます。

コンフィギュレーション ファイルをサーバ上に格納されているファイルの正確なコピーとして復元するには、その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直接コピーし（**copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** コマンドを使用）、ルータをリロードする必要があります。

サーバからルータへコンフィギュレーション ファイルをコピーするには、次の項で説明する作業を実行します。

- 「TFTP サーバからルータへのコンフィギュレーション ファイルのコピー」
- 「rcp サーバからルータへのコンフィギュレーション ファイルのコピー」
- 「FTP サーバからルータへのコンフィギュレーション ファイルのコピー」

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これらの改善は、FTP および rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。

TFTP サーバからルータへのコンフィギュレーション ファイルのコピー

TFTP サーバからルータへコンフィギュレーション ファイルをコピーするには、必要に応じて EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **copy tftp:**[[[**//***location*]**/***directory*]**/***filename*] **system:running-config**	TFTP サーバから実行コンフィギュレーションへコンフィギュレーション ファイルをコピーします。
Router# **copy tftp:**[[[**//***location*]**/***directory*]**/***filename*] **nvram:startup-config**	TFTP サーバからスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

次に、IP アドレス 172.16.2.155 にある、tokyo-config という名前のファイルからソフトウェアを設定する例を示します。

```
Router1# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

rcp サーバからルータへのコンフィギュレーション ファイルのコピー

rcp サーバからルータへコンフィギュレーション ファイルをコピーできます。

rcp ユーザ名の概要

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 を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 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 経由でルータに接続しており、**username** コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。
4. ルータのホスト名。

rcp コピー要求が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。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書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、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。

rcp サーバからルータへのコンフィギュレーション ファイルのコピー

rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	（任意）端末からコンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 を参照）。
ステップ 2	`Router(config)# ip rcmd remote-username username`	（任意）リモート ユーザ名を指定します。
ステップ 3	`Router(config)# end`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 を参照）。

ステップ 4	`Router# copy rcp:[[[//[username@]location]/directory]/filename] system:running-config`
	または
	`Router# copy rcp:[[[//[username@]location]/directory]/filename] nvram:startup-config`
		rcp サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcp の Running-Config をコピーする例

次に、host1-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、ルータ上でコマンドをロードし実行する例を示します。

```
Router# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

rcp の Startup-Config をコピーする例

次に、リモート ユーザ名 netadmin1 を指定する例を示します。この例では、次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
Rtr2# configure terminal
Rtr2(config)# ip rcmd remote-username netadmin1
Rtr2(config)# end
Rtr2# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
```

```
Loading 1112 byte file host2-confg:![OK]
[OK]
Rtr2#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

FTP サーバからルータへのコンフィギュレーション ファイルのコピー

FTP サーバからルータへコンフィギュレーション ファイルをコピーできます。

FTP ユーザ名およびパスワードの概要

FTP プロトコルでは、クライアントは FTP 要求ごとにリモート ユーザ名およびパスワードをサーバに送信する必要があります。FTP を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 匿名。

ルータは次の順番で最初に発見した有効なパスワードを送信します。

1. **copy** EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** グローバル コンフィギュレーション コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. ルータは、*username@routername.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバ上のアカウントと関連付けら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 FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

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、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、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。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** 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、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

FTP サーバからルータへのコンフィギュレーション ファイルのコピー

FTP サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーするには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	（任意）グローバル コンフィギュレーション モードを開始できます。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 2	`Router(config)# ip ftp username username`	（任意）デフォルトのリモート ユーザ名を指定します。
ステップ 3	`Router(config)# ip ftp password password`	（任意）デフォルトのパスワードを指定します。
ステップ 4	`Router(config)# end`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。

ステップ 5	`Router# copy ftp:[[[//[username[:password]@]location]/directory]/filename] system:running-config`
	
	または
	
	`Router# copy ftp:[[[//[username[:password]@]location]/directory]/filename] nvram:startup-config`
		FTP を使用して、ネットワーク サーバから実行メモリまたはスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

FTP の Running-Config をコピーする例

次に、host1-confg という名前のホスト コンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからコピーし、ルータ上でコマンドをロードし実行する例を示します。

```
Router# copy rcp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

FTP の Startup-Config をコピーする例

次に、リモート ユーザ名 netadmin1 を指定する例を示します。この例では、次に host2-confg という名前のコンフィギュレーション ファイルを、IP アドレスが 172.16.101.101 のリモート サーバ上の netadmin1 ディレクトリからスタートアップ コンフィギュレーションへコピーします。

```
Rtr2# configure terminal
Rtr2(config)# ip ftp username netadmin1
Rtr2(config)# ip ftp password mypass
Rtr2(config)# end
Rtr2# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
Rtr2#
```

```
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

NVRAM より大きいコンフィギュレーション ファイルの保守

NVRAM のサイズを超えるコンフィギュレーション ファイルを保守するには、以降の項で説明する作業を実行します。

- 「コンフィギュレーション ファイルの圧縮」
- 「コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納」
- 「ネットワークからのコンフィギュレーション コマンドのロード」

コンフィギュレーション ファイルの圧縮

service compress-config グローバル コンフィギュレーション コマンドは、コンフィギュレーション ファイルを圧縮して NVRAM に格納することを指定します。コンフィギュレーション ファイルが圧縮されると、ルータは正常に機能します。システムの起動時に、システムはコンフィギュレーション ファイルが圧縮されていることを認識し、圧縮されたコンフィギュレーション ファイルを展開して、正常に処理を進めます。**more nvram:startup-config** EXEC コマンドにより、コンフィギュレーションが展開されてから表示されます。

コンフィギュレーション ファイルを圧縮する前に、適切なハードウェアのインストレーションおよびメンテナンス マニュアルを参照してください。現在のシステムの ROM がファイル圧縮をサポートしていることを確認します。サポートしていない場合、ファイル圧縮をサポートしている新しい ROM をインストールできます。

コンフィギュレーション ファイルを圧縮するには、グローバル コンフィギュレーション モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# service compress-config`	コンフィギュレーション ファイルを圧縮することを指定します。
ステップ 2	`Router(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 3	FTP、rcp、または TFTP を使用して、新しいコンフィギュレーションをコピーします。NVRAM サイズの 3 倍を超える大きさのコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。 「[buffer overflow - *file-size/buffer-size* bytes]」 または `Router# configure terminal`	新しいコンフィギュレーションを入力します。
ステップ 4	`Router(config)# copy system:running-config nvram:startup-config`	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

コンフィギュレーションのサイズは、NVRAM のサイズの 3 倍を超えてはいけません。NVRAM のサイズが 128 KB の場合、展開できる最大のコンフィギュレーション ファイルのサイズは 384 KB です。

service compress-config グローバル コンフィギュレーション コマンドは、Cisco IOS ソフトウェア Release 10 以降のブート ROM を使用している場合に限り実行できます。新しい ROM をインストールするのは 1 回限りの操作で、ROM に Cisco IOS Release 10 がない場合だけ必要です。ブート ROM が圧縮コンフィギュレーションを認識しない場合は、次のメッセージが表示されます。

```
Boot ROMs do not support NVRAM compression Config NOT written to NVRAM
```

次に、129 KB のコンフィギュレーション ファイルを 11 KB に圧縮する例を示します。

```
Router# configure terminal
Router(config)# service compress-config
Router(config)# end
Router# copy tftp://172.16.2.15/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
Router# copy system:running-config nvram:startup-config
Building configuration...
Compressing configuration from 129648 bytes to 11077 bytes
[OK]
```

コンフィギュレーションのクラス A フラッシュ ファイル システム上のフラッシュ メモリへの格納

クラス A フラッシュ ファイル システムのルータ上では、内部フラッシュ メモリのファイルまたは PCMCIA スロットのフラッシュ メモリのファイルに CONFIG_FILE 環境変数を設定することにより、スタートアップ コンフィギュレーションをフラッシュ メモリに格納できます。

スタートアップ コンフィギュレーションをフラッシュ メモリに格納するには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **copy nvram:startup-config** *flash-filesystem:filename*	新しい場所に現在のスタートアップ コンフィギュレーションをコピーして、コンフィギュレーション ファイルを作成します。
ステップ 2	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。
ステップ 3	Router(config)# **boot config flash-filesystem:***filename*	CONFIG_FILE 環境変数を設定することにより、フラッシュ メモリにスタートアップ コンフィギュレーション ファイルを格納することを指定します。
ステップ 4	Router(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 5	FTP、rcp、または TFTP を使用して、新しいコンフィギュレーションをコピーします。NVRAM サイズの 3 倍を超える大きさのコンフィギュレーションをロードしようとすると、次のエラー メッセージが表示されます。 「[buffer overflow - *file-size/buffer-size* bytes]」 または Router# **configure terminal**	新しいコンフィギュレーションを入力します。
ステップ 6	Router# **copy system:running-config nvram:startup-config**	実行コンフィギュレーションの変更が終わったら、新しいコンフィギュレーションを保存します。

詳細については、「クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定」の項を参照してください。

次に、コンフィギュレーション ファイルをスロット 0 に格納する例を示します。

```
Router# copy nvram:startup-config slot0:router-config
Router# configure terminal
Router(config)# boot config slot0:router-config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

大きいコンフィギュレーションを編集または変更する場合は、注意する必要があります。**copy system:running-config nvram:startup-config** EXEC コマンドが発行されるたびにフラッシュ メモリ領域が使用されます。空き領域の最適化などのフラッシュ メモリのファイル管理は自動的に行われないため、利用可能なフラッシュ メモリに十分注意を払う必要があります。**squeeze** コマンドを使用して、使用済み領域を再要求します。20 MB 以上の大容量フラッシュ カードを使用することを推奨します。

ネットワークからのコンフィギュレーション コマンドのロード

大きいコンフィギュレーションを FTP、rcp、TFTP のいずれかのサーバに格納しておき、システムの起動時にそのコンフィギュレーションをダウンロードすることもできます。ネットワーク サーバを使って大きいコンフィギュレーションを保存するには、特権 EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# copy system:running-config {ftp: | rcp: | tftp:}`	実行コンフィギュレーションを FTP、rcp、TFTP のいずれかのサーバに保存します。
ステップ 2	`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。
ステップ 3	`Router(config)# boot network {ftp:[[[//[username[:password]@]location]/directory]/filename] | rcp:[[[//[username@]location]/directory]/filename] | tftp:[[[//location]/directory]/filename]}`	起動時にスタートアップ コンフィギュレーション ファイルをネットワーク サーバからロードすることを指定します。
ステップ 4	`Router(config)# service config`	システムの起動時にコンフィギュレーション ファイルをダウンロードするように、ルータをイネーブルにします。
ステップ 5	`Router(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 6	`Router# copy system:running-config nvram:startup-config`	コンフィギュレーションを保存します。

これらのコマンドの詳細については、「ルータからネットワーク サーバへのコンフィギュレーション ファイルのコピー」および「コンフィギュレーション ファイルをダウンロードするルータの設定」の項を参照してください。

パーサー キャッシュの制御

Cisco IOS ソフトウェアの Cisco IOS コマンドライン パーサーは、コマンドラインを変換および実行（解析）します。パーサー キャッシュ機能は、大きいコンフィギュレーション ファイルを迅速に処理するために開発されました。これにより、ロード時間が大幅に改善されます。

パーサー キャッシュ機能では、簡略化された解析グラフをダイナミックに作成、キャッシュ、および再使用することにより、コンフィギュレーション ファイル内の、前回使用された設定行と微妙に異なる設定行（たとえば pvc 0/100、pvc 0/101 など）が、迅速に認識および変換できるようになります。この改善は、主に同じようなコマンドを何百回、何千回と繰り返すコンフィギュレーション ファイルに役立ちます。このようなコンフィギュレーション ファイルには、サブインターフェイス用に何千もの仮想回線を設定する必要のある場合や、何百ものアクセス リストを設定する必要のある場合などがあります。数値の引数だけが異なる同一のコマンドが繰り返し使用されているファイルのほとんどで、性能が向上します。

パーサー キャッシュは、Cisco IOS Release 12.1(5)T 以降のリリースを使用するすべてのプラットフォームで、デフォルトでイネーブルにされています。ただし、大きいコンフィギュレーション ファイルを必要としないシスコ デバイスを使用しているユーザの場合は、パーサー キャッシュをディセーブルにし、この機能で使用されるリソースを解放できます（この機能により使用されるメモリは、解析されるコンフィギュレーション ファイルのサイズに依存しますが、通常は 512 KB 未満です）。

パーサー キャッシュ機能を制御するには、次の項で説明する作業を実行します。これらの作業はすべて任意です。

パーサー キャッシュのクリア

リソースを解放またはパーサー キャッシュのメモリをリセットするために、パーサー キャッシュ機能に格納されている解析エントリおよびヒット数とミス数の統計情報をクリアする場合があります。パーサー キャッシュ機能に格納されている情報をクリアするには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# clear parser cache`	パーサー キャッシュ機能に格納されている解析キャッシュ エントリおよびヒット数とミス数の統計情報をクリアします。

パーサー キャッシュのディセーブル化

パーサー キャッシュ機能は、デフォルトでイネーブルにされています。パーサー キャッシュ機能をディセーブルにするには、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。

コマンド	目的
`Router(config)# no parser cache`	パーサー キャッシュ機能をディセーブルにします。

パーサー キャッシュがディセーブルになると、**no parser cache** コマンドラインが実行コンフィギュレーション ファイルに書き込まれます。

ヒント システム リソースを解放するためにパーサー キャッシュをディセーブルにする場合は、**no parser cache** コマンドを発行する前にパーサー キャッシュをクリアする必要があります。パーサー キャッシュをディセーブルにした後は、パーサー キャッシュをクリアできません。

パーサー キャッシュの再イネーブル化

パーサー キャッシュ機能をディセーブルにした後、再度イネーブルにするには、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。

コマンド	目的
`Router(config)# parser cache`	パーサー キャッシュ機能をイネーブルにします。

パーサーのモニタリング

最後に解析されたコンフィギュレーション ファイルに関する統計情報は、パーサー キャッシュ機能により解析されたコマンドのヒット数とミス数の統計情報とともにシステム メモリに格納されます。「hits（ヒット数）」および「misses（ミス数）」は、前回使用された類似するコマンドに対し、コンフィギュレーション セッション中にパーサー キャッシュが検出した一致数を示しています。一致したコマンド（「hits」）は、より効率的に解析されます。一致しなかったコマンド（「misses」）の解析時間は、パーサー キャッシュにより改善されることはありません。

パーサーの統計情報を表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# show parser statistics`	最後に解析されたコンフィギュレーション ファイルに関する統計情報およびパーサー キャッシュ機能のステータスを表示します。

次に、**show parser statistics** コマンドからの出力例を示します。

```
Router# show parser statistics
Last configuration file parsed:Number of Commands:1484, Time:1272 ms

Parser cache:disabled, 0 hits, 0 misses
```

show parser statistics コマンドにより、次の 2 セットのデータが表示されます。

- コンフィギュレーション ファイル内のコマンドのうち、最後に実行コンフィギュレーションにコピーされたコマンドの数、およびシステムがこれらのコマンドを解析するために要した時間（コンフィギュレーション ファイルはシステムの起動時または **copy** *source* **running-config** EXEC コマンドなどのコマンドを発行することによって実行コンフィギュレーションにロードされます）。
- パーサー キャッシュのステータス（イネーブルまたはディセーブル）、およびシステムの起動以降またはパーサー キャッシュのクリア以降に一致したコマンドの数（ヒット数またはミス数）。

前述の例では、ヒット数とミス数の統計情報（0/0）が最後に解析されたコンフィギュレーション ファイル内のコマンド数（1484）と一致していません。これは、コンフィギュレーション ファイルが最後にロードされたときに、パーサー キャッシュがディセーブルになっていたことを示しています。

異なる場所の間でのコンフィギュレーション ファイルのコピー

多くのプラットフォーム上では、内部フラッシュ メモリまたは PCMCIA スロット内のフラッシュ メモリ カードなどのフラッシュ メモリ デバイスから他の場所へ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、FTP、rcp、TFTP のいずれかのサーバからフラッシュ メモリへコンフィギュレーション ファイルをコピーできます。

フラッシュ メモリからスタートアップまたは実行コンフィギュレーションへのコンフィギュレーション ファイルのコピー

フラッシュ メモリから現在の NVRAM にあるスタートアップ コンフィギュレーションまたは実行コンフィギュレーションへコンフィギュレーション ファイルを直接コピーするには、必要に応じて EXEC モードで次のいずれかのコマンドを入力します。

コマンド	目的
Router> **copy** *filesystem*:[*partition-number*:][*filename*] **nvram:startup-config**	NVRAM にコンフィギュレーション ファイルを直接ロードします。
Router> **copy** *filesystem*:[*partition-number*:][*filename*] **system:running-config**	現在の実行コンフィギュレーションにコンフィギュレーション ファイルをコピーします。

次に、スロット 0 にあるフラッシュ メモリ PC カードのパーティション 4 からルータのスタートアップ コンフィギュレーションへ ios-upgrade-1 という名前のファイルをコピーする例を示します。

```
Router# copy slot0:4:ios-upgrade-1 nvram:startup-config

Copy 'ios-upgrade-1' from flash device
  as 'startup-config' ? [yes/no] yes
[OK]
```

フラッシュ メモリ ファイル システム間でのコンフィギュレーション ファイルのコピー

複数のフラッシュ メモリ ファイル システムを備えたプラットフォーム上では、内部フラッシュ メモリまたは PCMCIA スロット内のフラッシュ メモリ カードなどのフラッシュ メモリ ファイル システムから他のフラッシュ メモリ ファイル システムへファイルをコピーできます。異なるフラッシュ メモリ ファイル システムへファイルをコピーすることで、使用中のコンフィギュレーションのバックアップ コピーを作成し、他のルータにコンフィギュレーションを複製できます。

フラッシュ メモリ ファイル システム間でコンフィギュレーション ファイルをコピーするには、EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router> **show** *source-filesystem*:	フラッシュ メモリのレイアウトと内容を表示して、ファイル名を確認します。
ステップ 2	Router> **copy** *source-filesystem*:[*partition-number*:][*filename*] *dest-filesystem*:[*partition-number*:][*filename*]	フラッシュ ファイル メモリ デバイス間でコンフィギュレーション ファイルをコピーします。
ステップ 3	Router> **verify** *dest-filesystem*:[*partition-number*:][*filename*]	コピーしたファイルのチェックサムを検証します。

（注） コピー元デバイスとコピー先デバイスは同じにはできません。たとえば、**copy slot1: slot1:** コマンドは無効です。

ローカル フラッシュ メモリ デバイス間でコンフィギュレーション ファイルをコピーする例

次に、内部フラッシュ メモリのパーティション 1 から Cisco 3600 シリーズ ルータ上のスロット 1 のパーティション 1 へ running-config という名前のファイルをコピーする例を示します。この例では、コピー元のパーティションが指定されていないため、ルータからパーティション番号を要求されます。

```
Router# copy flash: slot1:

System flash

Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3070K     1025K     4096K      Read/Write     Direct
  2        16384K   1671K    14712K     8192K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/network/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]

PCMCIA Slot1 flash directory:
File  Length   Name/status
  1   1711088  dirt/gate/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]

Source file name? running-config

Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
  as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
...erased
!
 [OK - 850/4194304 bytes]
```

```
Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

サーバからフラッシュ メモリ デバイスへのコンフィギュレーション ファイルのコピー

FTP サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 2	`Router(config)# ip ftp username username`	（任意）リモート ユーザ名を指定します。
ステップ 3	`Router(config)# ip ftp password password`	（任意）リモート パスワードを指定します。
ステップ 4	`Router(config)# end`	（任意）コンフィギュレーション モードを終了します。この手順は、デフォルトのリモート ユーザ名を上書きにする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 5	`Router# copy ftp: [[[//[username:password@]location]/directory]/file name] flash-filesystem:[partition-number:][filename]`	FTP を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。

copy EXEC コマンドを発行した後、追加情報またはアクションの確認を求めるプロンプトが表示される場合があります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcp サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーするには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	（任意）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。この手順は、デフォルトのリモート ユーザ名を上書きにする場合にだけ必要です（ステップ 2 を参照）。
ステップ 2	`Router(config)# ip rcmd remote-username username`	（任意）リモート ユーザ名を指定します。
ステップ 3	`Router(config)# end`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 を参照）。
ステップ 4	`Router# copy rcp:[[[//[username@]location]/directory]/filename] flash-filesystem:[partition-number:][filename]`	rcp を使用してネットワーク サーバからフラッシュ メモリ デバイスへコンフィギュレーション ファイルをコピーします。追加情報または確認を要求するルータからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** コマンドの現在の設定によって異なります。

TFTP サーバからルータへコンフィギュレーション ファイルをコピーするには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **copy tftp:**[[[**//***location*]**/***directory*]**/***filename*] *flash-filesystem*:[*partition-number*:][*filename*]	TFTP サーバからフラッシュ メモリ デバイスへファイルをコピーします。追加情報または確認を要求するルータからのプロンプトに対し応答します。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** コマンドの現在の設定によって異なります。

次の例は、TFTP サーバから Cisco 7500 シリーズ ルータの Network Processing Engine（NPE; ネットワーク処理エンジン）または Route Switch Processor（RSP; ルート スイッチ プロセッサ）カードのスロット 0 に挿入されたフラッシュ メモリ カードへ router-config という名前のコンフィギュレーション ファイルをコピーする例を示します。コピーされたファイルの名前は new-config に変更されます。

```
Router# copy tftp:router-config slot0:new-config
```

スタートアップ コンフィギュレーション ファイルでのコンフィギュレーション コマンドの再実行

スタートアップ コンフィギュレーション ファイルにあるコマンドを再実行するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **configure memory**	スタートアップ コンフィギュレーション ファイルにあるコンフィギュレーション コマンドを再実行します。

設定情報のクリア

スタートアップ コンフィギュレーションから設定情報をクリアできます。スタートアップ コンフィギュレーションなしでルータをリブートした場合は、ルータを最初から設定できるように、ルータは Setup コマンド ファシリティに移行します。

スタートアップ コンフィギュレーションのクリア

スタートアップ コンフィギュレーションの内容をクリアするには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **erase nvram:**	スタートアップ コンフィギュレーションの内容をクリアします。

クラス A フラッシュ ファイル システムのプラットフォーム以外のすべてのプラットフォームでは、このコマンドにより NVRAM が消去されます。スタートアップ コンフィギュレーション ファイルは、いったん削除すると復元できません。

クラス A フラッシュ ファイル システムのプラットフォーム上では、**erase startup-config** EXEC コマンドを使用すると、CONFIG_FILE 環境変数により指定されたコンフィギュレーションが、ルータにより削除されます。この変数が NVRAM を指定している場合は、ルータにより NVRAM が消去されます。CONFIG_FILE 環境変数がフラッシュ メモリ デバイスとコンフィギュレーション ファイル名を指定している場合は、ルータによりコンフィギュレーション ファイルが削除されます。つまり、そのコンフィギュレーション ファイルはルータにより消去するのではなく、「削除済み」としてマークされます。この機能では、削除されたファイルを回復できます。

指定されたコンフィギュレーション ファイルの削除

特定のフラッシュ デバイス上にある指定されたコンフィギュレーションを削除するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router> **delete** *flash-filesystem:filename*	指定されたフラッシュ デバイス上の指定されたコンフィギュレーション ファイルを削除します。

クラス A および B フラッシュ ファイル システムでは、フラッシュ メモリ内の特定のファイルを削除すると、そのファイルは削除済みとしてシステムによりマークされます。これにより、**undelete** EXEC コマンドを使用して、削除したファイルを後で回復できるようになります。消去されたファイルは回復できません。コンフィギュレーション ファイルを完全に消去するには、**squeeze** EXEC コマンドを使用します。

クラス C フラッシュ ファイル システムでは、削除されたファイルは回復できません。

CONFIG_FILE 環境変数で指定されたコンフィギュレーション ファイルを消去または削除しようとした場合、システムにより削除の確認を求めるプロンプトが表示されます。

次に、スロット 0 に挿入されたフラッシュ メモリ カードから myconfig という名前のファイルを削除する例を示します。

```
Router# delete slot0:myconfig
```

スタートアップ コンフィギュレーション ファイルの指定

通常、起動時には NVRAM にあるスタートアップ コンフィギュレーション ファイルまたは（クラス A フラッシュ ファイル システムに限り）CONFIG_FILE 環境変数により指定されたフラッシュ ファイル システムがルータにより使用されます。CONFIG_FILE 変数の設定に関する詳細については、「クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定」の項を参照してください。

起動時に 2 つのコンフィギュレーション ファイルを自動的に要求し、ネットワーク サーバから受信するようにルータを設定することもできます。詳細については、「コンフィギュレーション ファイルをダウンロードするルータの設定」の項を参照してください。

クラス A フラッシュ ファイル システムでの CONFIG_FILE 環境変数の指定

クラス A フラッシュ ファイル システムでは、CONFIG_FILE 環境変数で指定されたスタートアップ コンフィギュレーション ファイルをロードするように Cisco IOS ソフトウェアを設定できます。CONFIG_FILE 変数のデフォルトは NVRAM になります。CONFIG_FILE 環境変数を変更するには、EXEC モードを開始して次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router> **copy** [*flash-url* | *ftp-url* | *rcp-url* | *tftp-url* | **system:running-config** | **nvram:startup-config**] *dest-flash-url*	フラッシュ ファイル システムにコンフィギュレーション ファイルをコピーします。再起動時には、ここからルータにファイルがロードされます。
ステップ 2	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。
ステップ 3	Router(config)# **boot config** *dest-flash-url*	CONFIG_FILE 環境変数を設定します。この手順により、実行時の CONFIG_FILE 環境変数が変更されます。
ステップ 4	Router(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 5	Router> **copy system:running-config nvram:startup-config**	スタートアップ コンフィギュレーションにステップ 3 で実行されたコンフィギュレーションを保存します。
ステップ 6	Router> **show bootvar**	（任意）CONFIG_FILE 環境変数の内容を確認できます。

スタートアップ コンフィギュレーション ファイルの場所を指定すると、**nvram:startup-config** コマンドはスタートアップ コンフィギュレーション ファイルの新しい場所のエイリアスとなります。**more nvram:startup-config** EXEC コマンドにより、スタートアップ コンフィギュレーションの場所に関係なく、スタートアップ コンフィギュレーションが表示されます。**erase nvram:startup-config** EXEC コマンドにより、NVRAM の内容が消去され、CONFIG_FILE 環境変数で指定されたファイルが削除されます。

copy system:running-config nvram:startup-config コマンドを使用してコンフィギュレーションを保存した場合、ルータによりコンフィギュレーション ファイルの完全バージョンは CONFIG_FILE 環境変数により指定された場所に保存され、抽出バージョンは NVRAM に保存されます。抽出バージョンとは、アクセス リスト情報を含まないバージョンです。NVRAM に完全バージョンのコンフィギュレーション ファイルが含まれている場合は、ルータは完全バージョンを抽出バージョンで上書きすることを確認するプロンプトを表示します。NVRAM に抽出コンフィギュレーションが含まれている場合は、ルータは確認のプロンプトを表示しないで NVRAM にある既存の抽出バージョンのコンフィギュレーション ファイルを上書きする処理を進めます。

（注） フラッシュ デバイスにあるファイルを CONFIG_FILE 環境変数として指定した場合、**copy system:running-config nvram:startup-config** コマンドでコンフィギュレーション ファイルを保存するたびに、古いコンフィギュレーション ファイルは「削除済み」とマークされ、新しいコンフィギュレーション ファイルがそのデバイスに保存されます。それでも古いコンフィギュレーション ファイルはメモリを使用するため、最終的にフラッシュ メモリは一杯になります。**squeeze** EXEC コマンドを使用して古いコンフィギュレーション ファイルを完全に削除し、領域を解放してください。

次に、Cisco 7500 シリーズ ルータの RSP カードの最初の PCMCIA スロットに実行コンフィギュレーション ファイルをコピーする例を示します。このコンフィギュレーションは、後でシステムを再起動した際にスタートアップ コンフィギュレーションとして使用されます。

```
Router# copy system:running-config slot0:config2
Router# configure terminal
Router(config)# boot config slot0:config2
Router(config)# end
Router# copy system:running-config nvram:startup-config
[ok]
Router# show bootvar
BOOT variable = slot0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = slot0:config2

Configuration register is 0x010F
```

コンフィギュレーション ファイルをダウンロードするルータの設定

システムの起動時に 1 つまたは 2 つのコンフィギュレーション ファイルをロードするようにルータを設定できます。コンフィギュレーション ファイルは、コマンドラインにコマンドを入力した場合と同様に、メモリにロードされ読み込まれます。したがって、ルータのコンフィギュレーションは、元のスタートアップ コンフィギュレーションと 1 つまたは 2 つのダウンロードされたコンフィギュレーション ファイルで混成されたものになります。

ネットワークとホストのコンフィギュレーション ファイル

歴史的な理由から、ルータが最初にダウンロードするファイルは、ネットワーク コンフィギュレーション ファイルと呼ばれます。ルータが 2 番目にダウンロードするファイルは、ホスト コンフィギュレーション ファイルと呼ばれます。2 つのコンフィギュレーション ファイルは、ネットワーク上のすべてのルータが、同一コマンドの多くを使用する場合に使用できます。ネットワーク コンフィギュレーション ファイルには、すべてのルータを設定するために使用される標準コマンドが含まれます。ホスト コンフィギュレーション ファイルには、特定の 1 つのホストに固有のコマンドが含まれます。2 つのコンフィギュレーション ファイルをロードする場合、ホスト コンフィギュレーション ファイルを、もう 1 つのファイルより優先させる必要があります。ネットワーク コンフィギュレーション ファイルおよびホスト コンフィギュレーション ファイルは、両方とも TFTP、rcp、FTP のいずれかを介して到達可能なネットワーク サーバ上にあり、読み取り可能である必要があります。

rcp ユーザ名の概要

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 を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **boot network** または **boot host** グローバル コンフィギュレーション コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 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 経由でルータに接続しており、**username** コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。
4. ルータのホスト名。

rcp コピー要求が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。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書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、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 ユーザ名およびパスワードの概要

FTP プロトコルでは、クライアントは FTP 要求ごとにリモート ユーザ名およびパスワードをサーバに送信する必要があります。FTP を使用してルータからサーバへコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは次の順番で最初に発見した有効なユーザ名を送信します。

1. **copy** EXEC コマンドで指定されたユーザ名（ユーザ名が指定されている場合）。

2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 匿名。

ルータは、次のリストのうち最初の有効なパスワードを送信します。

1. **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。
3. ルータは、*username@routername.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバ上のアカウントと関連付けら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 FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

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、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。たとえば、システム イメージがサーバ上のユーザのホーム ディレクトリにある場合は、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。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** コマンドを使用して、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

コンフィギュレーション ファイルをダウンロードするルータの設定

ネットワーク コンフィギュレーションおよびホスト コンフィギュレーション ファイル名の順序付きリストを指定できます。Cisco IOS ソフトウェアは、適切なネットワークまたはホスト コンフィギュレーション ファイルをロードするまで、このリストをスキャンします。

システムの起動時にコンフィギュレーション ファイルをダウンロードするようにルータを設定するには、次の項で説明する作業を少なくとも 1 つ実行します。

- 「ネットワーク コンフィギュレーション ファイルをダウンロードするルータの設定」
- 「ホスト コンフィギュレーション ファイルをダウンロードするルータの設定」

起動中にコンフィギュレーション ファイルをロードできなかった場合、要求されたファイルがホストから提供されるまで、ルータは 10 分ごと（デフォルト設定）に再試行します。試行が失敗するたびに、ルータにより次のメッセージがコンソール端末に表示されます。

```
Booting host-confg... [timed out]
```

トラブルシューティングの手順については、『*Internetwork Troubleshooting Guide*』を参照してください。

スタートアップ コンフィギュレーション ファイルに何らかの問題がある場合、またはコンフィギュレーション レジスタが NVRAM を無視するように設定されている場合は、ルータは Setup コマンド ファシリティに移行します。Setup コマンド ファシリティに関する詳細については、マニュアルの「Using the Setup Command Facility for Configuration Changes」の章を参照してください。

ネットワーク コンフィギュレーション ファイルをダウンロードするルータの設定

起動時にサーバからネットワーク コンフィギュレーション ファイルをダウンロードするように Cisco IOS ソフトウェアを設定するには、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。

	コマンド	目的
ステップ 1	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。
ステップ 2	Router(config)# **boot network** {**ftp:**[[[**//**[*username*[:*password*]**@**]*location*]**/***directory*]**/***filename*] | **rcp:**[[[**//**[*username***@**]*location*]**/***directory*]**/***filename*] | **tftp:**[[[**//***location*]**/***directory*]**/***filename*]}	起動時にダウンロードするネットワーク コンフィギュレーション ファイルおよび使用されるプロトコル（TFTP、rcp、FTP のいずれか）を指定します。
ステップ 3	Router(config)# **service config**	再起動時にネットワーク ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 4	Router(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 5	Router# **copy system:running-config nvram: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。

ステップ 2 でネットワーク コンフィギュレーション ファイル名を指定しなかった場合、Cisco IOS ソフトウェアはデフォルトのファイル名 network-confg を使用します。アドレスを省略した場合、ルータはブロードキャスト アドレスを使用します。

複数のネットワーク コンフィギュレーション ファイルを指定できます。ソフトウェアは、ネットワーク コンフィギュレーション ファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。

ホスト コンフィギュレーション ファイルをダウンロードするルータの設定

起動時にサーバからホスト コンフィギュレーション ファイルをダウンロードするように Cisco IOS ソフトウェアを設定するには、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。

	コマンド	目的
ステップ 1	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。
ステップ 2	Router(config)# **boot host** {**ftp:**[[[**//**[*username*[:*password*]**@**]*location*]**/***directory*]**/***filename*] | **rcp:**[[[**//**[*username***@**]*location*]**/***directory*]**/***filename*] | **tftp:**[[[**//***location*]**/***directory*]**/***filename*] }	起動時にダウンロードするホスト コンフィギュレーション ファイルおよび使用されるプロトコル（FTP、rcp、TFTP のいずれか）を指定します。
ステップ 3	Router(config)# **service config**	再起動時にホスト ファイルを自動的にロードするようにシステムをイネーブルにします。
ステップ 4	Router(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 5	Router# **copy system:running-config nvram: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。

ホスト コンフィギュレーション ファイル名を指定しなかった場合、ルータはルータ自身の名前を使用してホスト コンフィギュレーション ファイル名を形成します。このとき、ルータの名前はすべて小文字に変換され、すべてのドメイン情報は削除され、「-confg」が追加されます。ホスト名情報が使用できない場合、ソフトウェアはデフォルトのホスト コンフィギュレーション ファイル名 router-confg を使用します。アドレスを省略した場合、ルータはブロードキャスト アドレスを使用します。

複数のホスト コンフィギュレーション ファイルを指定できます。Cisco IOS ソフトウェアは、ホスト コンフィギュレーション ファイルをロードできるまで、入力された順に試行します。この手順は、異なる設定情報を持つ、ネットワーク サーバ上にロードされるファイルを複数保持する場合に役立ちます。

システムの起動時にコンフィギュレーション ファイルをダウンロードするルータの設定の例

次に、hostfile1 という名前のホスト コンフィギュレーション ファイルおよび networkfile1 という名前のネットワーク コンフィギュレーション ファイルをダウンロードするようにルータを設定する例を示します。ルータは TFTP およびブロードキャスト アドレスを使用してファイルを取得します。

```
Router# configure terminal
Router(config)# boot host tftp:hostfile1
Router(config)# boot network tftp:networkfile1
Router(config)# service config
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

この章で扱うコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

コンフィギュレーション ファイルの管理の機能情報

表 1 に、コンフィギュレーション ファイルの管理に関連する機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーション ファイル管理機能の機能情報

機能名	リリース	機能情報
パーサー キャッシュ	Cisco IOS	Cisco IOS ソフトウェアの Cisco IOS コマンドライン パーサーは、コマンドラインを変換および実行（解析）します。パーサー キャッシュ機能は、大きいコンフィギュレーション ファイルを迅速に処理するために開発されました。これにより、ロード時間が大幅に改善されます。 Cisco IOS ソフトウェアの機能サポートに関する情報については、Feature Navigator を使用してください。 この機能に関する詳細については、次の項を参照してください。 • 「パーサー キャッシュの制御」

コンフィギュレーション生成のパフォーマンス拡張

コンフィギュレーション生成のパフォーマンス拡張機能は、実行中のコンフィギュレーション ファイル情報の収集を高速化することでコンフィギュレーション管理を支援します。この機能は特に多数のインターフェイスが構成されている大規模ネットワークを管理する場合に便利です。

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「コンフィギュレーション生成のパフォーマンス拡張に関する機能情報」（P.7）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーション生成のパフォーマンス拡張に関する制限事項

コンフィギュレーション生成のパフォーマンス拡張機能を使用するデバイスには、大規模インターフェイス コンフィギュレーション ファイルを保存（キャッシュ保存）するための十分なメモリが必要です。たとえば、インターフェイス コンフィギュレーションが 15 KB のメモリを使用する場合は、この機能を使用することで追加の 15 KB の空きメモリ領域が必要になります。

モジュールに **parser config cache interface** コマンドがある場合は、構成されたインターフェイスのパフォーマンスが改善されます。Network Analysis Module（NAM; ネットワーク解析モジュール）などの物理インターフェイスがない場合は、モジュールではパフォーマンスの改善は見られません。

コンフィギュレーション生成のパフォーマンス拡張について

コンフィギュレーション生成のパフォーマンス拡張機能を有効にする前に、次の概念を理解しておくことを推奨します。

- 「Cisco IOS ソフトウェアのコンフィギュレーション ストレージ」（P.2）
- 「コンフィギュレーション生成のパフォーマンス拡張の利点」（P.2）

Cisco IOS ソフトウェアのコンフィギュレーション ストレージ

Cisco IOS のソフトウェア コンフィギュレーション モデルでは、コンフィギュレーション状態は分散して維持され、各コンポーネントは独自のコンフィギュレーション状態を保持します。設定情報を取得するには、ソフトウェアは各コンポーネントをポーリングして、分散された情報を収集する必要があります。このコンフィギュレーション状態の取得処理は Nonvolatile Generation（NVGEN; 不揮発性生成）として知られるプロセスによって実行され、**show running-config**、**write memory**、**copy system:running-configuration** などの Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドで使用され、実行中のシステム構成を表示またはコピーします。呼び出すと、NVGEN 各システム コンポーネントとインターフェイスまたはその他のコンフィギュレーション オブジェクトの各インスタンスを照会します。NVGEN がこれらのクエリーを実行しているシステムを通過するときに、実行中のコンフィギュレーション ファイルが作成されます。

（注） ルータのメモリが少なく、バックアップ バッファを割り当てられないときに、**write memory** コマンドを設定すると、「Not enough space」というエラー メッセージが表示され、コマンドは失敗します。**write memory** コマンドが新しいコンフィギュレーションを適用できない場合は、バックアップ コンフィギュレーションを使用して元のコンフィギュレーションを復元します。

コンフィギュレーション生成のパフォーマンス拡張の利点

コンフィギュレーション生成のパフォーマンス拡張機能が導入される前は、NVGEN は必ずシステム全体を照会する必要があり、全体コンフィギュレーションだけを生成できました。NVGEN 処理の完了にはかなりの時間がかかるため、実行中のコンフィギュレーションの処理にかかる時間がコンフィギュレーション管理におけるパフォーマンスの問題を引き起こします。

コンフィギュレーション生成のパフォーマンス拡張機能は NVGEN 処理の実行時間を短縮し、特に多数のインターフェイス コンフィギュレーションを含む大規模なコンフィギュレーション ファイルの管理で有用です。この機能はシステム メモリのインターフェイス コンフィギュレーション情報をキャッシュに保存し、変更された設定情報だけを取得することで、実行中のシステム構成を処理するコマンドの実行を高速化します。

コンフィギュレーション生成のパフォーマンス拡張を設定する方法

ここでは、次の手順について説明します。

- 「コンフィギュレーション生成のパフォーマンス拡張の設定」（P.3）（必須）

コンフィギュレーション生成のパフォーマンス拡張の設定

コンフィギュレーション生成のパフォーマンス拡張をイネーブルにする作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **parser config cache interface**
4. **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。 • 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：** `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。
ステップ 3	**parser config cache interface** **例：** `Router(config)# parser config cache interface`	特に大規模コンフィギュレーション ファイルの場合に、実行中のシステム構成を管理するコマンドを CLI で実行するのに要する時間を短縮します。
ステップ 4	**end** **例：** `Router(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、特権 EXEC モードに戻ります。

コンフィギュレーション生成のパフォーマンス拡張の設定例

ここでは、次の設定例について説明します。

コンフィギュレーション生成のパフォーマンス拡張の設定：例

次に、コンフィギュレーション生成のパフォーマンス拡張機能をイネーブルにする方法の例を示します。

```
Router(config)# parser config cache interface
```

コンフィギュレーション生成のパフォーマンス拡張の検証：例

システム コンフィギュレーション ファイルのコマンドをチェックして、**parser config cache interface** コマンドがイネーブルになっていることを確認できます。これは **show running-configuration** EXEC コマンドを入力すると表示されます。

（注） 初めてコンフィギュレーション ファイルを表示する場合は、インターフェイス キャッシュが少ないため、それほどパフォーマンスの改善は見られません。ただし、**show running-config** EXEC コマンドなどの連続した NVGEN タイプのコマンドを入力するとパフォーマンス改善を確認できます。

インターフェイス コンフィギュレーションが変更されるたびに、指定されたインターフェイスのキャッシュがフラッシュされます。その他のインターフェイス データはそのままキャッシュに残ります。インターフェイス コンフィギュレーションの修正後に NVGEN タイプのコマンドを入力すると、次回の NVGEN タイプのコマンドが入力されるまで改善はほとんど見られません。

```
Router# show running-config
!
!
parser config cache interface
!
!
```

その他の関連資料

次の項に、コンフィギュレーション生成のパフォーマンス拡張機能に関する参考資料を示します。

関連資料

関連項目	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
システム コンフィギュレーション ファイル管理コマンド	使用するソフトウェア リリースに対応する『*Cisco IOS Configuration Fundamentals Command Reference*』
システム コンフィギュレーション ファイル管理	『*Cisco IOS Configuration Fundamentals* Configuration Guide』の「Managing Configuration Files」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

コンフィギュレーション生成のパフォーマンス拡張に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーション生成のパフォーマンス拡張機能に関する機能情報

機能名	リリース	機能情報
コンフィギュレーション生成のパフォーマンス拡張	12.3(7)T 12.2(25)S 12.2(33)SRC 12.2(33)SB 12.2(33)SXI	コンフィギュレーション生成のパフォーマンス拡張機能は、実行中のコンフィギュレーション ファイル情報の収集を高速化することでコンフィギュレーション管理を支援します。この機能は特に多数のインターフェイスが構成されている大規模ネットワークを管理する場合に便利です。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション生成のパフォーマンス拡張について」 • 「コンフィギュレーション生成のパフォーマンス拡張を設定する方法」 次のコマンドが導入または修正されました。**parser config cache interface**

設定のロック

Cisco IOS ソフトウェアでは、実行コンフィギュレーションをロックし、他のユーザが同時に Cisco IOS コンフィギュレーションにアクセスするのを防ぐための方法が提供されています。このモジュールでは、コンフィギュレーションをロックするための情報と設定作業について説明します。

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「設定のロックに関する機能情報」（P.10）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

設定のロックについて

設定をロックするには、次の概念について理解する必要があります。

排他的設定変更アクセスおよびアクセス セッション ロッキング

Cisco IOS ソフトウェアが動作するデバイスは、デバイスのコンフィギュレーション状態を決定する実行コンフィギュレーションを保持しています。実行コンフィギュレーションを変更すると、デバイスの動作が変わります。Cisco IOS ソフトウェアでは、複数のユーザがデバイスの CLI（デバイス コンソールと telnet Secure Shell（SSH; セキュア シェル）を含みます）を通じて実行コンフィギュレーションを変更できるため、一部の動作環境では、複数のユーザが Cisco IOS の実行コンフィギュレーションを同時に変更するのを防ぐことは有用です。Cisco IOS の実行コンフィギュレーションへのアクセスを一時的に制限することにより、不注意による競合や、2 人のユーザが実行コンフィギュレーションの同じ部分を設定しようとするのを防ぐことができます。

排他的設定変更アクセス機能（「設定ロック」機能とも呼びます）を使用すると、Cisco IOS の実行コンフィギュレーションに排他的に変更アクセスし、複数のユーザが同時に設定を変更するのを防ぐことができます。

この機能は、**configure terminal** コマンドを使用してグローバル コンフィギュレーション モードを開始したときから、Cisco IOS 実行コンフィギュレーションへの排他的変更アクセスを提供します。これにより、「設定のロック」の効果が得られ、他のユーザが Cisco IOS 実行コンフィギュレーションを変更できなくなります。設定ロックは、Cisco IOS コンフィギュレーション モードを終了すると自動的に解放されます。

排他的設定変更アクセス機能をイネーブルにするには、グローバル コンフィギュレーション モードで **configuration mode exclusive** コマンドを使用します。排他的設定変更アクセスは、**auto** に設定すると、誰かが **configure terminal** コマンドを使用したときに Cisco IOS コンフィギュレーション モードがロックされます。また、**manual** に設定すると、**configure terminal lock** コマンドを発行したときだけ Cisco IOS コンフィギュレーション モードがロックされます。

排他的設定変更アクセス機能は、Cisco IOS Release 12.2(25)S および 12.3(7)T で導入されたコンフィギュレーションの置換とロールバック機能を補完するロック機構です。

アクセス セッション ロッキング

アクセス セッション ロッキング機能は、設定のロックを保持しているユーザが入力した **show** コマンドと **debug** コマンドの実行が常に優先されるように、排他的設定変更アクセス機能を拡張します。この機能は、同時設定アクセスを防ぐとともに、別のユーザが入力した **show** コマンドのように、他のコンフィギュレーション コマンドの実行中に同時に処理が実行されるのを防ぐためのオプションも提供します。この機能をイネーブルにすると、設定ロックを保持しているユーザが入力したコマンド（コンフィギュレーション コマンドなど）が、他のユーザが入力したコマンドよりも常に優先されます。

パーサーの並行処理およびロッキングの改善

排他的設定変更アクセス機能によって発生する次の制限事項を克服するために、パーサーの並行処理およびロッキングの改善機能が Cisco IOS Release 12.2(33)SRE に追加されました。

- 排他的設定変更アクセス機能は、他のユーザに対して設定をロックします。ロックを保持している人がコンフィギュレーション モードを終了すると、ロックは自動的に解放されます。コンフィギュレーション モードの他のユーザは、ロックを取得すると EXEC モードに戻ります。また、どのユーザも **clear configuration lock** コマンドを実行し、強制的にロックを解放し、すべてのユーザに通常アクセスを許可できます。

- 同じクライアントに属する複数の書き込みプロセスが、共有モードで同時に Cisco IOS の設定にアクセスした場合、ルータがリロードすることがあります。
- EXEC コマンドがデータ構造に同時にアクセスした場合に、ルータがリロードすることがあります。

Cisco IOS Release 12.2(33)SRE から、並行処理およびロッキングの改善機能は、Cisco IOS ソフトウェアの複数のユーザによる同時設定を防ぐために使用される主なロック メカニズムです。

パーサーの並行処理およびロッキングの改善機能は、要求したプロセスに対して排他的なアクセスを許可し、他のプロセスが Cisco IOS の設定に同時にアクセスできないようにするための、共通のインターフェイスを提供します。ロックを保持しているユーザだけにアクセスを許可し、他のクライアントが設定にアクセスできないようにします。

Cisco IOS Release 12.2(33)SRE から、**configuration mode exclusive** {**auto** | **manual**} コマンドは、Cisco IOS CLI のシングルユーザ アクセス機能を可能にするために使用できなくなります。ロックを保持するユーザだけに設定へのアクセスを許可し、他のクライアントが設定にアクセスできないようにするには、**parser command serializer** コマンドを使用します。

設定ロックの設定方法

ここでは、次の各手順について説明します。

- 「排他的設定変更アクセスおよびアクセス セッション ロッキングのイネーブル化」（P.3）（必須）
- 「排他的設定変更アクセスの取得」（P.4）（任意）
- 「パーサーの並行処理およびロッキングの改善のイネーブル化」（P.5）（必須）
- 「設定ロックのモニタリングとトラブルシューティング」（P.6）（任意）

排他的設定変更アクセスおよびアクセス セッション ロッキングのイネーブル化

（注） Cisco IOS Release 12.2(33)SRE から、排他的設定変更アクセスおよびアクセス セッション ロッキング機能は、Cisco IOS ソフトウェアで使用できなくなりました。この機能の代わりに、パーサーの並行処理およびロッキングの改善機能を使用してください。詳細については、「パーサーの並行処理およびロッキングの改善のイネーブル化」（P.5）を参照してください。

排他的設定変更アクセスおよびアクセス セッション ロッキング機能をイネーブルにするには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **configuration mode exclusive** {**auto** | **manual**}
4. **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。 • 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：** `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。
ステップ 3	**configuration mode exclusive** {**auto** | **manual**} **例：** `Router(config)# configuration mode exclusive auto`	排他的設定変更アクセス（設定ロック機能）をイネーブルにします。 • コマンドがイネーブルになると、コンフィギュレーション セッションがシングルユーザ（排他）モードで実行されます。 • **auto** キーワードは、**configure terminal** コマンドを使用するたびに、コンフィギュレーション セッションを自動的にロックします。これがデフォルトです。 • **manual** キーワードは、コンフィギュレーション セッションのロックを手動で選択したり、ロックされないままにします。**manual** キーワードを使用する場合、「排他的設定変更アクセスの取得」（P.4）に説明がある作業を実行する必要があります。
ステップ 4	**end** **例：** `Router(config)# end`	コンフィギュレーション セッションを終了し、特権 EXEC モードに戻ります。

排他的設定変更アクセスの取得

設定セッションの間排他的設定変更アクセスを取得するには、この作業を実行します。**lock** キーワードを **configure terminal** コマンドで使用することは、排他的コンフィギュレーション モードが **manual** に設定されている場合にだけ必要です（「排他的設定変更アクセスおよびアクセス セッション ロッキングのイネーブル化」の項を参照）。

手順の概要

1. **enable**
2. **configure terminal**
3. **configure terminal lock**
4. 変更を実行コンフィギュレーションに入力してシステムを設定します。
5. **end**
   または
   exit

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。 • 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：** `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。
ステップ 3	**configure terminal lock** **例：** `Router(config)# configure terminal lock`	（任意）Cisco IOS ソフトウェアを排他（シングルユーザ）モードでロックします。 • このコマンドは、**configuration mode exclusive** コマンドを使用して設定ロックをイネーブルにしてある場合にだけ使用できます。 • このコマンドは、Cisco IOS Release 12.3(14)T 以降のリリースで使用できます。
ステップ 4	変更を実行コンフィギュレーションに入力してシステムを設定します。	—

ステップ 5	**end**
	または
	exit
	
	例：
	`Router(config)# end`
	または
	
	例：
	`Router(config)# exit`
		コンフィギュレーション セッションを終了し、ステップ 1 で取得したセッション ロックを解放し、特権 EXEC モードに戻ります。
		（注） **end** コマンド、**exit** コマンド、Ctrl+Z のキーの組み合わせのいずれかで設定ロックを解放します。推奨される方法は **end** コマンドの使用です。

パーサーの並行処理およびロッキングの改善のイネーブル化

設定ロックを保持しているユーザだけに設定アクセスを許可し、他のクライアントが実行コンフィギュレーションにアクセスできないようにするには、この作業を実行します。

制約事項

パーサーの並行処理およびロッキングの改善機能では、Cisco IOS の設定のクリティカル セクション内に 2 つ以上のプロセスが同時に存在することを防ぎます。

この機能は、その出力を生成するために非常に長時間かかる場合や、その使用により 10 KB を超える出力が生成される場合に、そのシリアル化を防ぐため、コマンドを発行します。シリアル化されないコマンドの例としては、**show terminal** コマンドや **show running-config** コマンドがあります。

手順の概要

1. **enable**

2. **configure terminal**
3. **parser command serializer**
4. **exit**

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。 • 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： `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。
ステップ 3	**parser command serializer** 例： `Router(config)# parser command serializer`	Cisco IOS の設定へのアクセスをシリアル化するために排他的ロックを導入します。
ステップ 4	**exit** 例： `Router(config)# exit`	（任意）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。

設定ロックのモニタリングとトラブルシューティング

排他的設定変更アクセスおよびアクセス セッション ロッキング機能をモニタリングまたはトラブルシューティングするには、この作業のいずれかの手順または両方の手順を実行します。

手順の概要

1. **show configuration lock**
2. **debug configuration lock**

手順の詳細

ステップ 1　show configuration lock

所有者、ユーザ、端末、ロック状態、ロッククラスなど、現在の設定ロックのステータスと詳細を表示するには、このコマンドを使用します。

グローバル コンフィギュレーション モードを開始できない場合、このコマンドを使用して、コンフィギュレーション セッションが別のユーザにロックされているかどうかと、誰がロックしているかを確認できます。

```
Router# show configuration lock

Parser Configure Lock
-----------------------------------------------------
Owner PID                       : 3
User                            : unknown
```

```
TTY                                 : 0
Type                                : EXCLUSIVE
State                               : LOCKED
Class                               : EXPOSED
Count                               : 1
Pending Requests                    : 0
User debug info                     : configure terminal
Session idle state                  : TRUE
No of exec cmds getting executed    : 0
No of exec cmds blocked             : 0
Config wait for show completion     : FALSE
Remote ip address                   : Unknown
Lock active time (in Sec)           : 6
Lock Expiration timer (in Sec)      : 593
Router(config)#
```

ステップ 2　debug configuration lock

Cisco IOS 設定ロックのデバッグをイネーブルにするには、このコマンドを使用します（公開クラス ロックまたはロールバック クラス ロック）。

```
Router# debug configuration lock

Session1 from console
==========================

Router# configure terminal lock

Configuration mode locked exclusively. The lock will be cleared once you exit out of
configuration mode using end/exit
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Parser : LOCK REQUEST in EXCLUSIVE mode
Parser: <configure terminal lock> - Config. Lock requested by process <3> client <PARSER
Client>
Parser: <configure terminal lock> - Config. Lock acquired successfully !
Router(config)#
```

設定をロックするための設定例

ここでは、次の設定例について説明します。

- 「自動モードでの排他的ロックの設定：例」（P.7）
- 「手動モードでの排他的ロックの設定：例」（P.8）
- 「パーサーの並行処理およびロッキングの改善の設定：例」（P.8）

自動モードでの排他的ロックの設定：例

次に、**configuration mode exclusive auto** コマンドを使用し、シングルユーザ自動コンフィギュレーション モードに対して、自動モードで排他的ロックをイネーブルにする例を示します。Cisco IOS 設定ファイルが排他的にロックすると、**show configuration lock** コマンドを使用してこの設定を確認できるようになります。

```
Router# configure terminal
Router(config)# configuration mode exclusive auto
Router(config)# exit
```

```
Router# configure terminal

! Locks configuration mode exclusively.

Router# show configuration lock

Parser Configure Lock

Owner PID        :  10
User             :  User1
TTY              :  3
Type             :  EXCLUSIVE
State            :  LOCKED
Class            :  Exposed
Count            :  0
Pending Requests :  0
User debug info  :  0
```

手動モードでの排他的ロックの設定：例

次に、**configuration mode exclusive manual** コマンドを使用して、手動モードで排他的ロック機能をイネーブルにする例を示します。手動排他モードを設定すると、**configure terminal lock** コマンドを使用してコンフィギュレーション モードをロックできるようになります。このモードでは、**configure terminal** コマンドでパーサー コンフィギュレーション モードが自動的にロックされません。

```
Router# configure terminal
Router(config)# configuration mode exclusive manual
Router(config)# exit

Router# configure terminal lock

Enter configuration commands, one per line.  End with CNTL/Z.

*Mar 25 17:02:45.928:  Configuration mode locked exclusively. The lock will be cleared
once you exit out of configuration mode using end/exit
```

パーサーの並行処理およびロッキングの改善の設定：例

次に、**parser command serializer** コマンドを使用してパーサーの並行処理およびロッキングの改善機能を設定する例を示します。

```
Router# configure terminal
Router(config)# parser command serializer
Router(config)# exit
```

その他の関連資料

ここでは、設定のロックに関する関連資料について説明します。

関連資料

関連項目	参照先
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Management Command Reference*』
コンフィギュレーション ファイルの管理についての情報	『*Managing Configuration Files*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

設定のロックに関する機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　　設定のロックに関する機能情報

機能名	リリース	機能情報
排他的設定変更アクセスおよびアクセス セッション ロッキング	12.3(14)T 12.0(31)S 12.2(33)SRA 12.4(11)T 12.2(33)SXH 12.2(33)SB	排他的設定変更アクセス機能（「設定ロック」機能とも呼びます）を使用すると、Cisco IOS の実行コンフィギュレーションに排他的に変更アクセスし、複数のユーザが同時に設定を変更するのを防ぐことができます。 この機能に対してアクセス セッション ロッキングを追加することで、排他的設定変更アクセス機能が拡張され、設定ロックを保持しているユーザが実行する **show** コマンドと **debug** コマンドの実行が常に優先されるようになります。他のユーザによって入力される **show** コマンドと **debug** コマンドは、設定ロックの所有者が開始したプロセスが終了した後でしか実行を許可されません。 排他的設定変更アクセス機能は、コンフィギュレーションの置換とロールバック機能（「ロールバック ロック」）を補完するロック メカニズムです。 設定ロック機能が Release 12.0S に統合され、アクセス セッション ロッキング機能拡張が実装されました。**configuration mode exclusive** コマンドが拡張され、キーワード オプション **config_wait**、**expire**、**interleave**、**lock-show**、**retry_wait**、および **terminate** が追加されました。**show configuration lock** コマンドの出力が改良されました。 拡張機能が Release 12.2(33)SRA、12.4(11)T、12.2(33)SXH、および 12.2(33)SB に統合されました。 この機能に関する詳細については、次の各項を参照してください。 • 「設定のロックについて」 • 「設定ロックの設定方法」 **clear configuration lock**、**configuration mode exclusive**、**configure terminal lock** の各コマンドが追加または変更されました。
パーサーの並行処理およびロッキングの改善	12.2(33)SRE 15.1(1)T	パーサーの並行処理およびロッキングの改善機能は、要求したプロセスに対して排他的なアクセスを許可し、他のプロセスが Cisco IOS の設定に同時にアクセスできないようにするための、共通のインターフェイスを提供します。ロックを保持しているユーザだけにアクセスを許可し、他のクライアントが設定にアクセスできないようにします。 この機能に関する詳細については、次の各項を参照してください。 • 「パーサーの並行処理およびロッキングの改善」 • 「パーサーの並行処理およびロッキングの改善のイネーブル化」 **parser command serializer**、**test parser session-lock** の各コマンドが追加または変更されました。

コンフィギュレーションの置換とロールバック

コンフィギュレーションの置換とロールバック機能により、現在の実行コンフィギュレーションを、保存しておいた Cisco IOS コンフィギュレーション ファイルで置換することができます。この機能は、コンフィギュレーションを保存しておいた状態へ戻すために使用でき、そのコンフィギュレーション ファイルが保存された後にどのような変更が加えられても、効果的にロールバックさせることができます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、「コンフィギュレーションの置換とロールバックの機能情報」（P.18）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーションの置換とロールバックの前提条件

- コンフィギュレーションの置換とロールバックへの入力ファイルとなるコンフィギュレーション ファイルの形式は、次の標準 Cisco IOS ソフトウェア コンフィギュレーション ファイルのインデント規則に準拠している必要があります。
  - 新しい行のすべてのコマンドは、コマンドがコンフィギュレーション サブモードにない限り、インデントなしで開始します。
  - レベル 1 コンフィギュレーション サブモード内のコマンドは、スペース 1 個分インデントします。
  - レベル 2 コンフィギュレーション サブモード内のコマンドは、スペース 2 個分インデントします。
  - 以降のサブモードのコマンドも同様にインデントします。

  Cisco IOS ソフトウェアが **show running-config** や **copy running-config** *destination-url* といった Cisco IOS コマンド用に作成するコンフィギュレーション ファイルは、これらの字下げ規則に従っています。Cisco IOS デバイスが作成するコンフィギュレーション ファイルはすべてこれらの規則に準拠します。
- 2 つのコンフィギュレーション ファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きな空きメモリが必要です。

コンフィギュレーションの置換とロールバックの制約事項

- 2 つのコンフィギュレーション ファイル（現在の実行コンフィギュレーションと、保存された置換用コンフィギュレーション）を合わせたサイズより大きい空きメモリがルータにない場合、コンフィギュレーションの置換操作は実行できません。
- ネットワーキング デバイスの物理コンポーネント（物理インターフェイスなど）に関係する特定の Cisco IOS コンフィギュレーション コマンドは、実行コンフィギュレーションへの追加や削除が行えません。一例として、コンフィギュレーションの置換操作では、あるインターフェイスが物理的にそのデバイス上に存在する場合、現在の実行コンフィギュレーションから **interface ethernet 0** コマンドラインを削除できません。同様に、実際には物理的にデバイス上に存在しないインターフェイスについて、実行コンフィギュレーションに **interface ethernet 1** コマンドラインを追加することもできません。コンフィギュレーションの置換操作で前述のような変更を行おうとした場合、コマンドラインの実行が失敗したことを示すエラー メッセージが表示されます。
- 非常にまれなケースですが、ルータをリロードしない限り特定の Cisco IOS コンフィギュレーション コマンドを Cisco IOS 実行コンフィギュレーションから削除できないことがあります。コンフィギュレーションの置換操作で前述のようなコマンドを削除しようとした場合、コマンドラインの実行が失敗したことを示すエラー メッセージが表示されます。

コンフィギュレーションの置換とロールバックについて

コンフィギュレーションの置換とロールバック機能を使用するには、次の概念を理解しておく必要があります。

- 「コンフィギュレーション アーカイブ」（P.3）
- 「コンフィギュレーションの置換」（P.3）
- 「コンフィギュレーションのロールバック」（P.4）
- 「コンフィギュレーションの置換とロールバックの利点」（P.5）

コンフィギュレーション アーカイブ

Cisco IOS コンフィギュレーション アーカイブは、**configure replace** コマンドを使用するコンフィギュレーションのロールバック機能を強化するために、Cisco IOS コンフィギュレーション ファイルのアーカイブの保存、編成、管理を行うことを目的としたメカニズムです。この機能の導入前にも、実行コンフィギュレーションのコピーを **copy running-config** *destination-url* コマンドを使用して保存し、ローカルやリモートに置換ファイルを保管することはできました。しかし、この方式には自動化されたファイル管理が欠けていました。一方、コンフィギュレーションの置換とロールバック機能では、実行コンフィギュレーション ファイルを自動的に Cisco IOS コンフィギュレーション アーカイブに保存できます。アーカイブされたファイルはコンフィギュレーションのチェックポイントとして参照でき、**configure replace** コマンドを使用して以前のコンフィギュレーション状態へ戻すために使用できます。

archive config コマンドを使用すると、標準の保存先と、プレフィクスに保存ファイルごとの連番となるバージョン番号（タイムスタンプも選択可能）を自動で追加したファイル名とを使用して、Cisco IOS コンフィギュレーションをコンフィギュレーション アーカイブへ保存できます。この機能により、保存した Cisco IOS コンフィギュレーション ファイルを一貫して識別できます。アーカイブに保存する実行コンフィギュレーションの数は指定可能です。アーカイブ内のファイル数が上限値に達すると、次に最新のファイルが保存されるときに、最も古いファイルが自動的に消去されます。**show archive** コマンドで、Cisco IOS コンフィギュレーション アーカイブに保存されているすべてのコンフィギュレーション ファイルの情報を表示できます。

Cisco IOS コンフィギュレーション アーカイブにはコンフィギュレーション ファイルを保存しておき、**configure replace** コマンドで使用することができます。アーカイブは次のファイル システム上に作成できます。

- disk0 があるプラットフォーム：disk0:、disk1:、ftp:、pram:、rcp:、slavedisk0:、slavedisk1:、tftp:。
- disk0 がないプラットフォーム：ftp:、http:、pram:、rcp:、tftp:。

コンフィギュレーションの置換

configure replace コマンドにより、現在の実行コンフィギュレーションを、保存しておいた Cisco IOS コンフィギュレーション ファイルで置換することができます。この機能は、コンフィギュレーションを保存しておいた状態へ戻すために使用でき、そのコンフィギュレーション状態が保存された後にどのような変更が加えられても、効果的にロールバックさせることができます。

configure replace コマンドを使用するときは、現在の実行コンフィギュレーションと置換する、保存された Cisco IOS コンフィギュレーション ファイルを指定する必要があります。置換ファイルは、Cisco IOS デバイスによって作成された完全なコンフィギュレーション（**copy running-config** *destination-url* コマンドによって作成されたものなど）であることが必要です。置換ファイルを外部的に作成することもできますが、Cisco IOS デバイスが作成するファイル形式に完全に準拠していなければなりません。**configure replace** コマンドを入力すると、現在の実行コンフィギュレーションが指定された置換コンフィギュレーションと比較され、一連の diff が生成されます。2 つのファイルの比較に使用されるアルゴリズムは、**show archive config differences** コマンドで使用されるものと同じです。それから、置換コンフィギュレーションの状態になるよう、diff の結果が Cisco IOS パーサーによって適用されます。diff だけが適用されるため、現在の実行コンフィギュレーション上にすでに存在していたコンフィギュレーション コマンドを再適用することに起因する、潜在的なサービスの中断を避けられます。このアルゴリズムでは、順序に依存するコマンド（アクセス リストなど）へのコンフィギュレーション変更を、複数のパス プロセスを通して効果的に実行します。通常の環境では、コンフィギュレーション置換操作の完了に必要なパスは 3 つまでであり、ループ動作を防ぐためのパスは最大 5 つまでに制限されます。

Cisco IOS **copy** *source-url* **running-config** コマンドは、保存された Cisco IOS コンフィギュレーション ファイルを実行コンフィギュレーションへコピーするためにしばしば使用されます。**copy** *source-url* **running-config** コマンドを **configure replace** *target-url* コマンドの代わりに使用する場合、主な相違点として次の点に注意が必要です。

- **copy** *source-url* **running-config** コマンドはマージ動作であり、ソース ファイルと現在の実行コンフィギュレーションの両方のコマンドがすべて保持されます。このコマンドでは、現在の実行コンフィギュレーションにだけ含まれ、ソース ファイルには存在しないコマンドが削除されることはありません。これに対し、**configure replace** *target-url* コマンドでは、置換ファイルに存在しないコマンドは現在の実行コンフィギュレーションから削除され、現在の実行コンフィギュレーションに追加が必要なコマンドが追加されます。
- **copy** *source-url* **running-config** コマンドでは、現在の実行コンフィギュレーションにすでに存在するかどうかにかかわらず、ソース ファイル中のすべてのコマンドが適用されます。このアルゴリズムは効率的でない上、場合によってはサービスの停止が発生します。これに対し、**configure replace** *target-url* コマンドでは適用が必要なコマンドだけを適用します。すでに現在の実行コンフィギュレーションに存在しているコマンドは再適用されません。
- **copy** *source-url* **running-config** コマンドでは部分的なコンフィギュレーション ファイルもコピー元として使用できますが、**configure replace** *target-url* コマンドの置換ファイルとして使用できるのは、完全な Cisco IOS コンフィギュレーション ファイルだけです。

（注） Cisco IOS Release 12.2(25)S および 12.3(14)T では、コンフィギュレーション置換動作にロック機能が導入されました。**configure replace** コマンドが使用されると、コンフィギュレーション置換の動作中、デフォルトで実行コンフィギュレーション ファイルがロックされます。このロック メカニズムによって、置換動作の実行中に他のユーザが実行コンフィギュレーションを変更しようとしたために、置換動作の不正終了が発生することを防止できます。**nolock** キーワードを **configure replace** コマンドの実行時に使用すれば、実行コンフィギュレーションのロックをディセーブルにできます。

実行コンフィギュレーションのロックは、コンフィギュレーションの置換動作終了時に自動的にクリアされます。**show configuration lock** コマンドを使用すれば、現在実行コンフィギュレーションに適用されているロックをすべて表示できます。

コンフィギュレーションのロールバック

ロールバックの概念は、データベースの操作では一般的なトランザクション プロセス モデルに由来します。データベース トランザクションでは、あるデータベースのテーブルに一連の変更を加えることがあります。その後、変更を実行する（変更を恒久的に適用する）か、変更をロールバックする（変更を破棄してテーブルを以前の状態に戻す）かを選択することになります。この文脈でロールバックが意味するのは、変更のログを含んだジャーナル ファイルが破棄され、何の変更も加えられないことです。ロールバック操作の結果として、加えた変更が適用される前の状態に戻ります。

configure replace コマンドを使えば、以前のコンフィギュレーション状態へ戻ることが可能になり、コンフィギュレーション状態の保存後に加えた変更を効率的にロールバックさせることができます。Cisco IOS コンフィギュレーション ロールバックは、適用された一連の変更をもとにロールバック動作を行うのではなく、保存された Cisco コンフィギュレーション ファイルに基づいた特定のコンフィギュレーション状態へ戻るというコンセプトを採用しています。このコンセプトは、チェックポイント（データベースの保存されたバージョン）に特定の状態を保存しておくという、データベースの考え方に類似しています。

コンフィギュレーションのロールバック機能が必要な場合、コンフィギュレーションの変更に先立って Cisco IOS 実行コンフィギュレーションを保存する必要があります。そして、コンフィギュレーションへの変更を入力した後に、保存しておいたコンフィギュレーション ファイルを変更のロールバックに

使用できます（**configure replace** *target-url* コマンドを使用）。さらに、保存された Cisco IOS コンフィギュレーション ファイルならどれでも置換コンフィギュレーションとして指定できるため、ジャーナル ファイルによるロールバック モデルの一部のように、ロールバックの数が制限されることもありません。

コンフィギュレーション ロールバック変更確認

コンフィギュレーション ロールバック変更確認機能は、コンフィギュレーションの変更に確認条件を追加できる機能です。この機能では、要求された変更の確認が設定された時間内に受信できなかった場合、ロールバックを発生させることができます。コマンドの失敗をトリガーに設定してコンフィギュレーションをロールバックさせることも可能です。

次に、このプロセスを実施するための手順の概要を示します。

1. コンフィギュレーション モードに入るとき、この新しいオプションによってコンフィギュレーション変更の確認を要求することができます（確認の制限時間指定が必要）。
2. コンフィギュレーション モードから出た後、確認コマンドを入力する必要があります。要求された制限時間内に確認を入力しないと、コンフィギュレーションは以前の状態に戻ります。

コンフィギュレーションの置換とロールバックの利点

- コンフィギュレーションの変更を効率的にロールバックさせて、以前のコンフィギュレーション状態へ戻ることが可能。
- ルータをリロードしたり、CLI で実行コンフィギュレーション ファイルに加えた変更を手動で元に戻したりすることなく、現在の実行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 ファイルと置換できるため、システムのダウンタイムが減少。
- 保存しておいたどの Cisco IOS コンフィギュレーション状態に戻すことも可能。
- 追加や削除が必要なコマンドだけが影響される場合、ルータに完全なコンフィギュレーション ファイルを適用することができるため、コンフィギュレーションの変更がシンプルに。
- **configure replace** コマンドを **copy** *source-url* **running-config** コマンドの代用として使用する場合、現在の実行コンフィギュレーションにも存在しているコマンドを再適用することがないため、より効率的かつサービスの停止リスクを回避可能。

コンフィギュレーションの置換とロールバックの使用方法

ここでは、次の各手順について説明します。

- 「コンフィギュレーション アーカイブの作成」（P.6）（任意）
- 「コンフィギュレーションの置換やロールバック操作の実行」（P.8）（必須）
- 「コンフィギュレーションの置換とロールバック機能のモニタリングとトラブルシューティング」（P.10）（任意）

コンフィギュレーション アーカイブの作成

configure replace コマンドを使用するために、前提条件となる設定はありません。**configure replace** コマンドと Cisco IOS コンフィギュレーション アーカイブおよび **archive config** コマンドとの併用は任意ですが、コンフィギュレーション ロールバックの使用にあたっては大きな利点があります。**archive config** コマンドを使用する前に、コンフィギュレーション アーカイブを設定しておく必要があります。コンフィギュレーション アーカイブの特性を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **path** *url*
5. **maximum** *number*
6. **time-period** *minutes*
7. **end**
8. **archive 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 モードをイネーブルにします。 • 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： `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。
ステップ 3	**archive** 例： `Router(config)# archive`	アーカイブ 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	**path** *url* 例： `Router(config-archive)# path disk0:myconfig`	Cisco IOS コンフィギュレーション アーカイブの場所と、ファイル名のプレフィクスを指定します。 • *url* 引数は、Cisco IOS コンフィギュレーション アーカイブで実行コンフィギュレーション ファイルのアーカイブ ファイルを保存するために使用する URL です（Cisco IOS ファイル システムがアクセス可能なもの）。アーカイブは、使用しているプラットフォームがサポートするどのファイル システムにも設定できます（「コンフィギュレーション アーカイブ」（P.3）を参照）。 **（注）** パスのところでファイルの代わりにディレクトリを指定する場合、ディレクトリ名は path flash:/directory/ のように後ろにスラッシュを付ける必要があります。このスラッシュはファイル名の後ろでは必要ありません。ディレクトリを指定する場合にだけ使います。
ステップ 5	**maximum** *number* 例： `Router(config-archive)# maximum 14`	（任意）Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイル数の上限値を設定します。 • *number* 引数は、Cisco IOS コンフィギュレーション アーカイブに保存される実行コンフィギュレーションのアーカイブ ファイルの数の上限値です。有効値は、1 ～ 14 です。デフォルト値は 10 です。 **（注）** このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィクスを指定しておく必要があります。
ステップ 6	**time-period** *minutes* 例： `Router(config-archive)# time-period 10`	（任意）Cisco IOS コンフィギュレーション アーカイブに実行コンフィギュレーションのアーカイブ ファイルを自動保存する間隔を設定します。 • Cisco IOS コンフィギュレーション アーカイブに現在の実行コンフィギュレーションのアーカイブ ファイルをどれほどの頻度で保存するかを、minutes 引数により分単位で指定します。 **（注）** このコマンドを使用する前に、**path** コマンドを設定して Cisco IOS コンフィギュレーション アーカイブの位置とファイル名プレフィクスを指定しておく必要があります。
ステップ 7	**end** 例： `Router(config-archive)# end`	特権 EXEC モードに戻ります。
ステップ 8	**archive config** 例： `Router# archive config`	現在の実行コンフィギュレーション ファイルをコンフィギュレーション アーカイブに保存します。 **（注）** このコマンドを使用する前に、**path** コマンドを設定する必要があります。

コンフィギュレーションの置換やロールバック操作の実行

保存された Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換するには、次の作業を実行します。

（注） この手順の前に、コンフィギュレーション アーカイブを作成しておく必要があります。詳しくは、「コンフィギュレーション アーカイブの作成」（P.6）を参照してください。次に、現在の実行コンフィギュレーションで問題が生じた場合に、アーカイブしておいたコンフィギュレーションに戻す手順の詳細を紹介します。

手順の概要

1. **enable**
2. **configure replace** *target-url* [**nolock**] [**list**] [**force**] [**ignorecase**] [**revert trigger** [**error**] [**timer** *minutes*] | **time** ***minutes***]
3. **configure revert** {**now** | **timer** {***minutes*** | **idle** *minutes*}}
4. **configure confirm**
5. **exit**

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。 • 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 replace** *target-url* [**nolock**] [**list**] [**force**] [**ignorecase**] [**revert trigger** [**error**] [**timer** *minutes*] | **time** *minutes*] **例：** `Router# configure replace disk0:myconfig-1 list time 30`	保存しておいた Cisco IOS コンフィギュレーション ファイルで現在の実行コンフィギュレーション ファイルを置換します。 • *target-url* 引数は、**archive config** コマンドで作成されたコンフィギュレーション ファイルなど、現在の実行コンフィギュレーションと置換する、保存された Cisco IOS コンフィギュレーション ファイルの URL です（Cisco IOS ファイル システムでアクセス可能なもの）。 • **list** キーワードは、コンフィギュレーション置換動作のパスごとに、Cisco IOS ソフトウェア パーサーによって適用されるコマンド ラインのリストを表示します。実行されたパスの総数も表示されます。 • **force** キーワードは、現在の実行コンフィギュレーションから指定した Cisco IOS コンフィギュレーション ファイルへの置換を、確認プロンプトを出さずに実行します。 • **time** *minutes* キーワードおよび引数は、現在の実行コンフィギュレーション ファイルの置換確認のために **configure confirm** コマンドを入力する制限時間（分単位）を指定します。**configure confirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在の実行コンフィギュレーション ファイルが **configure replace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。 • **nolock** キーワードは、コンフィギュレーション置換操作中に他のユーザが実行コンフィギュレーションを変更しないように実行コンフィギュレーション ファイルをロックする機能をオフにします。 • **revert trigger** キーワードは、元のコンフィギュレーションへ戻すトリガーを次の内容から設定します。 – **error**：エラー時に元のコンフィギュレーションに戻します。 – **timer** *minutes*：指定した時間が過ぎると元のコンフィギュレーションに戻します。 • **ignorecase** キーワードで、コンフィギュレーションに確認コマンドの大文字と小文字の区別を無視させることができます。

	コマンドまたはアクション	目的
ステップ 3	**configure revert** {**now** | **timer** {*minutes* | **idle** *minutes*}} 例： `Router# configure revert now`	（任意）時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、特権 EXEC モードで **configure revert** コマンドを使用します。 • **now**：ロールバックをただちにトリガーします。 • **timer**：コンフィギュレーションを元に戻すタイマーをリセットします。 – 元に戻す時間を分単位で新たに指定するには、*minutes* 引数を **timer** キーワードとともに使用します。 – 保存されたコンフィギュレーションに戻すまでに、操作が行われないアイドル時間を最大どれほど長く許容できるかを設定するには、分単位の時間とともに **idle** キーワードを使用します。
ステップ 4	**configure confirm** 例： `Router# configure confirm`	（任意）現在の実行コンフィギュレーションの保存された Cisco IOS コンフィギュレーション ファイルへの置換を確認します。 **（注）** このコマンドは、**configure replace** コマンドで **time** *seconds* キーワードおよび引数が指定されている場合にだけ使用します。
ステップ 5	**exit** 例： `Router# exit`	ユーザ EXEC モードに戻ります。

コンフィギュレーションの置換とロールバック機能のモニタリングとトラブルシューティング

コンフィギュレーションの置換とロールバック機能のモニタリングとトラブルシューティングを行うには、次の作業を実行します。

手順の概要

1. **enable**
2. **show archive**
3. **debug archive versioning**
4. **debug archive config timestamp**
5. **exit**

手順の詳細

ステップ 1　enable

このコマンドを使用して、特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。次に例を示します。

```
Router> enable
Router#
```

ステップ 2　show archive

このコマンドを使用して、Cisco IOS コンフィギュレーション アーカイブに保存されたファイルの情報を表示させます。次に例を示します。

```
Router# show archive

There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
 Archive #  Name
   0
   1       disk0:myconfig-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10
   11
   12
   13
   14
```

次に、実行コンフィギュレーションのアーカイブ ファイルをいくつか保存した状態で **show archive** コマンドを使用した場合の出力例を示します。この例では、保存するアーカイブ ファイルは最大 3 つに設定されています。

```
Router# show archive

There are currently 3 archive configurations saved.
The next archive file will be named disk0:myconfig-8
 Archive #  Name
   0
   1       :Deleted
   2       :Deleted
   3       :Deleted
   4       :Deleted
   5       disk0:myconfig-5
   6       disk0:myconfig-6
   7       disk0:myconfig-7 <- Most Recent
   8
   9
   10
   11
   12
   13
   14
```

ステップ 3　debug archive versioning

コンフィギュレーションの置換とロールバックのモニタおよびトラブルシューティングのため、このコマンドを使用して Cisco IOS コンフィギュレーション アーカイブのデバッグ動作をイネーブルにします。次に例を示します。

```
Router# debug archive versioning

Jan  9 06:46:28.419:backup_running_config
Jan  9 06:46:28.419:Current = 7
```

```
Jan  9 06:46:28.443:Writing backup file disk0:myconfig-7
Jan  9 06:46:29.547: backup worked
```

ステップ 4　debug archive config timestamp

このコマンドを使用して、コンフィギュレーション置換操作の各必須段階の処理時間、および操作中のコンフィギュレーション ファイルのサイズのデバッグをイネーブルにします。次に例を示します。

```
Router# debug archive config timestamp
Router# configure replace disk0:myconfig force

Timing Debug Statistics for IOS Config Replace operation:
       Time to read file slot0:sample_2.cfg = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054

Starting Pass 1
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:93
       Size of file        :2539
       Time taken for positive rollback pass = 320 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for negative incremental diffs pass = 59 msec (0 sec)
       Time taken by PI to apply changes = 0 msec (0 sec)
       Time taken for Pass 1 = 380 msec (0 sec)
Starting Pass 2
       Time to read file system:running-config = 0 msec (0 sec)
       Number of lines read:55
       Size of file        :1054
       Time taken for positive rollback pass = 0 msec (0 sec)
       Time taken for negative rollback pass = 0 msec (0 sec)
       Time taken for Pass 2 = 0 msec (0 sec)

Total number of passes:1
Rollback Done
```

ステップ 5　exit

このコマンドを使用して、ユーザ EXEC モードを終了します。次に例を示します。

```
Router# exit
Router>
```

コンフィギュレーションの置換とロールバックの設定例

ここでは、次の設定例について説明します。

- 「コンフィギュレーション アーカイブの作成：例」（P.13）
- 「実行コンフィギュレーションの保存された Cisco IOS コンフィギュレーション ファイルへの置換：例」（P.13）
- 「スタートアップ コンフィギュレーション ファイルへの復帰：例」（P.13）
- 「configure confirm コマンドによるコンフィギュレーション置換操作の実行：例」（P.14）
- 「コンフィギュレーション ロールバック操作の実行：例」（P.14）

コンフィギュレーション アーカイブの作成：例

次の例に、Cisco IOS コンフィギュレーション アーカイブの初期設定方法を示します。この例では、disk0:myconfig がコンフィギュレーション アーカイブの保存位置およびファイル名のプレフィクスとして設定され、保存するアーカイブ ファイルが最大 10 個に設定されます。

```
configure terminal
!
archive
 path disk0:myconfig
 maximum 10
 end
```

実行コンフィギュレーションの保存された Cisco IOS コンフィギュレーション ファイルへの置換：例

次の例に、現在の実行コンフィギュレーションを disk0:myconfig という名前で保存された Cisco IOS コンフィギュレーション ファイルで置換する方法を示します。**configure replace** コマンドでは、確認プロンプトでインタラクティブに操作を進めます。

```
Router# configure replace disk0:myconfig

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y

Total number of passes: 1
Rollback Done
```

次の例では、コンフィギュレーション置換操作中に適用されるコマンド ラインを表示するために、**list** キーワードを指定しています。

```
Router# configure replace disk0:myconfig list

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y

!Pass 1

!List of Commands:
no snmp-server community public ro
snmp-server community mystring ro
end

Total number of passes: 1
Rollback Done
```

スタートアップ コンフィギュレーション ファイルへの復帰：例

次の例に、**configure replace** コマンドを使用して Cisco IOS スタートアップ コンフィギュレーション ファイルへ復帰する方法を示します。この例では、インタラクティブなユーザ プロンプトを上書きする、オプションの **force** キーワードの使用方法も示しています。

```
Router# configure replace nvram:startup-config force

Total number of passes: 1
Rollback Done
```

configure confirm コマンドによるコンフィギュレーション置換操作の実行：例

次に、**configure replace** コマンドを **time** *seconds* キーワードおよび引数とともに使用する例を示します。現在の実行コンフィギュレーション ファイルの置換を実行するには、指定の制限時間内に **configure confirm** コマンドを入力する必要があります。**configure confirm** コマンドが指定の制限時間内に入力されない場合、コンフィギュレーション置換操作は自動的に戻されます（つまり、現在の実行コンフィギュレーション ファイルが **configure replace** コマンド入力以前のコンフィギュレーション状態へと回復されます）。

```
Router# configure replace nvram:startup-config time 120

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: Y

Total number of passes: 1
Rollback Done

Router# configure confirm
```

次に、**configure revert** コマンドを **time** キーワードとともに使用する例を示します。時間指定ロールバックをキャンセルしてロールバックを即時トリガーする、または時間指定ロールバックのパラメータをリセットするには、**configure revert** コマンドを使用します。

```
Router# configure revert timer 100
```

コンフィギュレーション ロールバック操作の実行：例

次の例に、現在の実行コンフィギュレーションに変更を加えた後、変更をロールバックする方法を示します。コンフィギュレーション ロールバック操作の一部として、ファイルに変更を加える前に現在の実行コンフィギュレーションを保存する必要があります。この例では、現在の実行コンフィギュレーションの保存に **archive config** コマンドが使用されています。**configure replace** コマンドの出力結果は、ロールバック操作を完了するために実行されたパスが 1 つだけだったことを示しています。

（注） **archive config** コマンドを使用する前に、**path** コマンドで Cisco IOS コンフィギュレーション アーカイブのファイルの位置とファイル名のプレフィクスを指定する必要があります。

まず、次のように現在の実行コンフィギュレーションをコンフィギュレーション アーカイブへ保存します。

```
archive config
```

それから、次の例に示すようにコンフィギュレーションの変更を入力します。

```
configure terminal
!
user netops2 password rain
```

```
user netops3 password snow
exit
```

実行コンフィギュレーション ファイルに変更を加えた後、それらの変更をロールバックさせて、変更前のコンフィギュレーションに戻したくなったとします。置換ファイルとして使用されるコンフィギュレーションのバージョンを確認するために、**show archive** コマンドが使用されています。それから、次の例に示すように、**configure replace** コマンドで置換コンフィギュレーション ファイルへ戻しています。

```
Router# show archive

There are currently 1 archive configurations saved.
The next archive file will be named disk0:myconfig-2
 Archive #  Name
   0
   1       disk0:myconfig-1 <- Most Recent
   2
   3
   4
   5
   6
   7
   8
   9
   10

Router# configure replace disk0:myconfig-1

Total number of passes: 1
Rollback Done
```

その他の関連資料

ここでは、コンフィギュレーションの置換とロールバック機能に関する関連資料について説明します。

関連資料

関連項目	参照先
コンフィギュレーションのロック	『*Exclusive Configuration Change Access and Access Session Locking*』
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』
コンフィギュレーション ファイルの管理についての情報	『*Managing Configuration Files*』
コンフィギュレーションのコンテキスト差分ユーティリティ機能の使用	『*Contextual Configuration Diff Utility*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

コンフィギュレーションの置換とロールバックの機能情報

表 1 に、この機能のリリース履歴を示します。ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/cfn にある Cisco Feature Navigator にアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーションの置換とロールバックの機能情報

機能名	リリース	機能情報
コンフィギュレーションの置換とロールバック	12.3(7)T 12.2(25)S 12.3(14)T 12.2(27)SBC 12.2(31)SB2 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	コンフィギュレーションの置換とロールバック機能により、現在の実行コンフィギュレーションを、保存しておいた Cisco IOS コンフィギュレーション ファイルで置換することができます。この機能は、コンフィギュレーションを保存しておいた状態へ戻すために使用でき、そのコンフィギュレーション ファイルが保存された後にどのような変更が加えられても、ロールバックさせることができます。 この機能は、12.3(7)T で導入されました。 12.2(25) では、Cisco IOS 12.2S リリースのサポートが追加されました。コンフィギュレーション置換時のロック メカニズム（排他的設定変更アクセス機能）が導入されました。 12.3(14)T では、Cisco IOS 12.3T リリース向けに、コンフィギュレーション置換時のロック メカニズム（排他的設定変更アクセス機能）が導入されました。 12.2(27)SBC では、Cisco IOS 12.2SB リリースのサポートが追加されました。 12.2(33)SRA では、Cisco IOS 12.2SR リリースのサポートが追加されました。 12.2(31)SB2 では、この機能が Cisco 10000 シリーズに実装されました。 12.2(33)SXH では、「コンフィギュレーション ロールバック」機能がリリース 12.2SX に実装されました。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 機能情報について、次の項で説明します。 • 「コンフィギュレーション アーカイブ」（P.3） • 「コンフィギュレーションの置換」（P.3） • 「コンフィギュレーションのロールバック」（P.4） • 「コンフィギュレーションの置換とロールバックの利点」（P.5） • 「コンフィギュレーション アーカイブの作成」（P.6） • 「コンフィギュレーションの置換やロールバック操作の実行」（P.8） • 「コンフィギュレーションの置換とロールバック機能のモニタリングとトラブルシューティング」（P.10） この機能により、次のコマンドが変更されました。**archive config**、**configure confirm**、**configure replace**、**debug archive config timestamp**、**debug archive versioning**、**maximum**, **path**（アーカイブ設定）、**show archive**、**show configuration lock**、**time-period**。

表 1　コンフィギュレーションの置換とロールバックの機能情報 （続き）

機能名	リリース	機能情報
コンフィギュレーションのバージョン管理	12.3(7)T 12.2(25)S 12.2(33)SRA	コンフィギュレーションのバージョン管理機能により、Cisco IOS 実行コンフィギュレーションのコピーをデバイス上やデバイス外で維持および管理することができます。コンフィギュレーション置換機能では、実行コンフィギュレーションの保存されたコピーへのロールバックを行うためにコンフィギュレーション バージョン管理機能を使用します。
排他的設定変更アクセス	12.3(14)T 12.0(31)S 12.2(33)SRA 12.4(11)T 12.2(33)SXH 12.2(33)SB	排他的設定変更アクセス機能（「コンフィギュレーション ロック」機能とも呼びます）を使用すると、Cisco IOS の実行コンフィギュレーションに排他的に変更アクセスし、複数のユーザが同時に設定を変更するのを防ぐことができます。 この機能により、**show configuration lock** コマンドが変更され、コンフィギュレーションの置換とロールバック機能に適用されます。 詳しくは、別のモジュール『Exclusive Configuration Change Access and Access Session Locking』を参照してください。
コンフィギュレーション ロールバック変更確認	12.2(33)SRC 12.2(33)SB 12.4(20)T 12.2(33)SXI	コンフィギュレーション ロールバック変更確認機能により、コンフィギュレーション変更の実行に際して確認を要求するようオプションで設定できます。 この確認が受信できない場合、コンフィギュレーションは変更が適用される前の状態に戻されます。 このメカニズムは、ネットワーク デバイスとユーザまたは管理アプリケーションとの接続に、誤ったコンフィギュレーション変更に起因する切断を防止するものです。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション ロールバック変更確認」（P.5） • 「コンフィギュレーションの置換やロールバック操作の実行」（P.8） この機能により、次のコマンドが変更されました。**configure confirm**、**configure replace**、**configure revert**、**configure terminal**

コンフィギュレーションのコンテキスト差分ユーティリティ

コンフィギュレーションのコンテキスト差分ユーティリティ機能は、2 つのコンフィギュレーション ファイル（Cisco IOS Integrated File System（IFS）を通じてアクセス可能）を行ごとに比較し、その間の違いの一覧を生成する機能を提供します。生成される出力には、追加、変更、削除された設定行と、変更された設定行が存在するコンフィギュレーション モードに関する情報が含まれています。

この章で紹介する機能情報の入手方法

ご使用の Cisco IOS ソフトウェア リリースで、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。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「コンフィギュレーションのコンテキスト差分ユーティリティの機能情報」（P.8）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーションのコンテキスト差分ユーティリティの前提条件

コンフィギュレーションのコンテキスト差分ユーティリティ機能で使用されるコンフィギュレーション ファイルの形式は、次に示す標準的な Cisco IOS コンフィギュレーション ファイルのインデント ルールに準拠している必要があります。

- 新しい行のすべてのコマンドは、コマンドがコンフィギュレーション サブモードにない限り、インデントなしで開始します。
- レベル 1 コンフィギュレーション サブモード内のコマンドは、スペース 1 個分インデントします。
- レベル 2 コンフィギュレーション サブモード内のコマンドは、スペース 2 個分インデントします。
- 以降のサブモードのコマンドも同様にインデントします。

ルータには、比較する 2 つのコンフィギュレーション ファイルを合わせたサイズよりも大きい連続したメモリ ブロックが必要です。

コンフィギュレーションのコンテキスト差分ユーティリティの制約事項

ルータに、比較する 2 つのコンフィギュレーション ファイルを合わせたサイズよりも大きい連続したメモリ ブロックがない場合、比較操作に失敗します。

コンフィギュレーションのコンテキスト差分ユーティリティについて

コンフィギュレーションのコンテキスト差分ユーティリティ機能を使用する前に、次の概念について理解してください。

- 「コンフィギュレーションのコンテキスト差分ユーティリティの利点」（P.2）
- 「コンフィギュレーションのコンテキスト差分ユーティリティの出力形式」（P.3）

コンフィギュレーションのコンテキスト差分ユーティリティの利点

コンフィギュレーションのコンテキスト差分ユーティリティ機能は、2 つのコンフィギュレーション ファイル（Cisco IOS File System（IFS）を通じてアクセス可能）を行ごとに比較し、その間の違いの一覧を生成する機能を提供します。生成された出力に、次の項目に関する情報が含まれます。

- 追加、変更、削除された設定行。
- 変更された設定行が存在するコンフィギュレーション モード。
- 順序による影響を受ける設定行の場所の変更。たとえば、**ip access-list** コマンドと **community-lists** コマンドは、コンフィギュレーション ファイル内での、同じ種類の他の Cisco IOS コマンドとの相対的な順序による影響を受けます。

コンフィギュレーションのコンテキスト差分ユーティリティの出力形式

比較操作

コンフィギュレーションのコンテキスト差分ユーティリティ機能は、2 つのコンフィギュレーション ファイルのファイル名を入力として使用します。比較操作が指定したファイルに対して実行され、2 つのファイルの間の差分が出力として生成されます。出力の解釈は、2 つのファイルの設定順序に依存します（**show archive config differences** コマンド）。このため、最初に入力したファイルのファイル名が file1、2 番目に入力したファイルのファイル名を file2 とします。生成される出力リストの各エントリの前には、見つかった差分の種類を示す固有のテキスト記号が付与されます。テキスト記号とその意味は次のとおりです。

- マイナス記号（-）は、設定行が file1 に存在し file2 に存在しないことを示します。
- プラス記号（+）は、設定行が file2 に存在し file1 に存在しないことを示します。
- 感嘆符（!）と説明用のコメントは、順序による影響を受ける設定行の場所が、file1 と file2 で異なることを示します。

差分比較操作

一部のアプリケーションでは、比較操作で生成される出力に、変更されていない（つまりマイナス記号もプラス記号もない）設定行が含まれている必要があります。そのようなアプリケーションのために、差分比較操作を実行できます。この操作では、指定されたコンフィギュレーション ファイルを実行コンフィギュレーション ファイルと比較します（**show archive config incremental-diffs** コマンド）。

差分比較操作を実行すると、実行コンフィギュレーション ファイルにない設定行（つまり、実行コンフィギュレーション ファイルと比較する、指定したファイルだけに現れる設定行）が出力として生成されます。感嘆符（!）と説明用のコメントは、順序による影響を受ける設定行の場所が、指定したコンフィギュレーション ファイルと実行コンフィギュレーション ファイルで異なることを示します。

コンフィギュレーションのコンテキスト差分ユーティリティの使用方法

ここでは、次の手順について説明します。

- 「コンフィギュレーションのコンテキスト差分ユーティリティの使用」（P.3）（必須）

コンフィギュレーションのコンテキスト差分ユーティリティの使用

この作業では、コンフィギュレーションのコンテキスト差分ユーティリティ機能を使用する方法について説明します。

手順の概要

1. **enable**
2. **show archive config differences** [*file1* [*file2*]]
   または
   show archive config incremental-diffs [*file*]
3. **exit**

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。 • 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	**show archive config differences** [*file1* [*file2*]]
	または
	show archive config incremental-diffs *file*
	
	例：
	`Router# show archive config differences running-config startup-config`
	または
	
	例：
	`Router# show archive config incremental-diffs nvram:startup-config`
		2 つのコンフィギュレーション ファイル（IFS を通じてアクセス可能）を行ごとに比較し、その間の差分の一覧を生成します。
		または
		指定したコンフィギュレーション ファイルと実行コンフィギュレーション ファイルを行ごとに比較し、実行コンフィギュレーション ファイルにない設定行の一覧を生成します。

ステップ 3	**exit** **例：** `Router# exit`	ユーザ EXEC モードに戻ります。

コンフィギュレーションのコンテキスト差分ユーティリティの設定例

ここでは、次の設定例について説明します。

- 「比較操作：例」（P.4）
- 「差分比較操作：例」（P.6）

比較操作：例

この例では、実行コンフィギュレーション ファイルとスタートアップ コンフィギュレーションに対して比較操作を行います。表 1 に、この例で使用するコンフィギュレーション ファイルを示します。

表 1　比較操作の例で使用するコンフィギュレーション ファイル

実行コンフィギュレーション ファイル	スタートアップ コンフィギュレーション ファイル

no ip subnet-zero
ip cef
interface Ethernet1/0
  ip address 10.7.7.7 255.0.0.0
  no ip route-cache
  no ip mroute-cache
  duplex half
no ip classless
snmp-server community public RO
	ip subnet-zero
	ip cef
	ip name-server 10.4.4.4
	voice dnis-map 1
	  dnis 111
	interface Ethernet1/0
	  no ip address
	  no ip route-cache
	  no ip mroute-cache
	  shutdown
	  duplex half
	ip default-gateway 10.5.5.5
	ip classless
	access-list 110 deny ip any host 10.1.1.1
	access-list 110 deny ip any host 10.1.1.2
	access-list 110 deny ip any host 10.1.1.3
	snmp-server community private RW

次に、**show archive config differences** コマンドからの出力例を示します。この出力例は、表 1 のコンフィギュレーション ファイルに対して比較操作を行った結果です。

```
Router# show archive config differences running-config startup-config

+ip subnet-zero
+ip name-server 10.4.4.4
+voice dnis-map 1
 +dnis 111
interface Ethernet1/0
 +no ip address
 +shutdown
+ip default-gateway 10.5.5.5
+ip classless
+access-list 110 deny ip any host 10.1.1.1
+access-list 110 deny ip any host 10.1.1.2
+access-list 110 deny ip any host 10.1.1.3
+snmp-server community private RW
-no ip subnet-zero
interface Ethernet1/0
 -ip address 10.7.7.7 255.0.0.0
-no ip classless
-snmp-server community public RO
```

差分比較操作：例

この例では、スタートアップ コンフィギュレーション ファイルと実行コンフィギュレーション ファイルに対して差分比較操作を行っています。表 2 に、この例で使用するコンフィギュレーション ファイルを示します。

表 2　差分比較操作の例で使用するコンフィギュレーション ファイル

スタートアップ コンフィギュレーション ファイル	実行コンフィギュレーション ファイル

ip subnet-zero
ip cef
ip name-server 10.4.4.4
voice dnis-map 1
  dnis 111
interface Ethernet1/0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  duplex half
ip default-gateway 10.5.5.5
ip classless
access-list 110 deny ip any host 10.1.1.1
access-list 110 deny ip any host 10.1.1.2
access-list 110 deny ip any host 10.1.1.3
snmp-server community private RW
	no ip subnet-zero
	ip cef
	interface Ethernet1/0
	  ip address 10.7.7.7 255.0.0.0
	  no ip route-cache
	  no ip mroute-cache
	  duplex half
	no ip classless
	snmp-server community public RO

次に、**show archive config incremental-diffs** コマンドからの出力例を示します。この出力例は表 2 のコンフィギュレーション ファイルに対して差分比較操作を行った結果です。

```
Router# show archive config incremental-diffs startup-config

ip subnet-zero
ip name-server 10.4.4.4
voice dnis-map 1
 dnis 111
interface Ethernet1/0
 no ip address
 shutdown
ip default-gateway 10.5.5.5
ip classless
 access-list 110 deny   ip any host 10.1.1.1
 access-list 110 deny   ip any host 10.1.1.2
 access-list 110 deny   ip any host 10.1.1.3
snmp-server community private RW
```

その他の関連資料

ここでは、コンフィギュレーションのコンテキスト差分ユーティリティ機能に関する参考資料について説明します。

関連資料

関連項目	参照先
コンフィギュレーション ファイルの管理についての情報	『Managing Configuration Files』
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **show archive config differences**
- **show archive config incremental-diffs**

コンフィギュレーションのコンテキスト差分ユーティリティの機能情報

表 3 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/cfn にある Cisco Feature Navigator にアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 3 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 3　コンフィギュレーションのコンテキスト差分ユーティリティの機能情報

機能名	リリース	機能情報
コンフィギュレーションのコンテキスト差分ユーティリティ	12.3(4)T 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	コンフィギュレーションのコンテキスト差分ユーティリティ機能は、2 つのコンフィギュレーション ファイルを行ごとに比較し、その間の違いの一覧を生成する機能を提供します。生成される出力には、追加、変更、削除された設定行と、変更された設定行が存在するコンフィギュレーション モードに関する情報が含まれています。 この機能は、12.3(4)T で初めて導入されました。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーションのコンテキスト差分ユーティリティの利点」（P.2） • 「コンフィギュレーションのコンテキスト差分ユーティリティの出力形式」（P.3） • 「コンフィギュレーションのコンテキスト差分ユーティリティの使用」（P.3） この機能によって変更されたコマンドは、**show archive config differences**、**show archive config incremental-diffs** です。

コンフィギュレーション変更通知およびロギング

この機能が導入されるまでは、Cisco IOS ソフトウェアの設定が変更されたかどうかを判断するための唯一の方法は、実行コンフィギュレーションとスタートアップ コンフィギュレーションのコピーをローカル コンピュータに保存し、行単位で比較することでした。この比較方法では、変更を特定できますが、変更が行われた順序や、変更に責任を持つ人は特定できません。

コンフィギュレーション変更通知およびロギング（コンフィギュレーション ログ アーカイブ）機能を使用すると、アーカイブ機能を実装することにより、設定変更をセッションごとおよびユーザごとに追跡できます。このアーカイブでは、適用された各コンフィギュレーション コマンド、コマンドを適用した人、コマンドの Parser Return Code（PRC）、コマンドを適用した時刻を追跡する「設定ログ」が保存されます。また、この機能により、設定ログが変化したときに非同期通知を登録されたアプリケーションに送信する、通知メカニズムも追加されます。

この章で紹介する機能情報の入手方法

ご使用の Cisco IOS ソフトウェア リリースで、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。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「コンフィギュレーション変更通知およびロギングの機能情報」（P.12）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーション変更通知およびロギングの制約事項

- コンフィギュレーション モードの完全なコマンド入力だけがログに記録されます。
- **copy** コマンドを使用して適用されたコンフィギュレーション ファイルの一部であるコマンドは、ログに記録されません。

コンフィギュレーション変更通知およびロギングについて

コンフィギュレーション変更通知およびロギング機能を設定するには、次の概念について理解する必要があります。

設定ログ

コンフィギュレーション変更通知およびロギング機能は、Cisco IOS ソフトウェアの実行コンフィギュレーションに対する変更を、設定ログを保持することで追跡します。この設定ログは、Command-Line Interface（CLI; コマンドライン インターフェイス）または HTTP を通じて実行された変更だけを追跡します。最終的にアクション ルーチンが呼び出される完全なコマンドだけがログに記録されます。次の種類の入力はログに記録されません。

- 結果的に構文エラー メッセージが表示されるコマンド
- ルータのヘルプ システムを呼び出す部分的なコマンド

実行される各コンフィギュレーション コマンドに対し、次の情報がログに記録されます。

- 実行されたコマンド
- コマンドを実行したユーザの名前
- 設定変更のシーケンス番号
- コマンドに対する Parser Return Code

（注） 一部の環境では、コンフィギュレーション モードとコマンドが実行された時刻もログされます。

設定ログの情報を表示するには、**show archive log config** コマンドを使用します。ただし、Parser Return Code は、Cisco IOS アプリケーションの内部だけで使用されるため、除外されます。

コンフィギュレーション変更通知およびコンフィギュレーション変更ロギング

設定変更の通知を Cisco IOS ソフトウェア システム ロギング（syslog）プロセスに送信するように、コンフィギュレーション変更通知およびロギング機能を設定できます。syslog 通知機能を使用すると、ポーリングや情報収集作業を実行しなくても、設定ログ情報をモニタリングできます。

コンフィギュレーション変更通知およびロギング機能では、セッションごとまたはユーザごとにユーザが入力した設定変更を追跡できます。このツールを使用すると、管理者は、Cisco IOS ソフトウェアの実行コンフィギュレーションに対して行われた変更を追跡し、変更を行ったユーザを特定できます。

EAL4+ 認定のための設定ロガーの機能拡張

Cisco IOS Release 12.3(14)T では、設定変更ロギング プロセスに対してさらなる機能拡張が行われています。これらの機能拡張は、ロギング プロセスが、Conformance to Common Criteria, Evaluation Assurance Level 4+（EAL4+）Firewall Protection Profiles で規定されている要件を満たすようにするための作業を支援します。これらの機能拡張には、次の要件を満たすための変更が含まれています。

- ロギング パラメータを変更した場合、変更がログに記録されます。これは、実行コンフィギュレーションに対する各変更に対し、コピー操作（たとえば、**copy** *source* **running-config** の実行時）から syslog メッセージを送信することで実現されます。
- 管理ユーザ グループに対する変更、特権 EXEC モード（「イネーブル」モード）へのアクセスの失敗がログに記録されます。

（注） シスコでは、Cisco IOS Release 12.3(14)T に対する EAL 認定を要求していません。これは、将来的な認定の基盤となるものです。

上記のロギング アクションは、デフォルトでディセーブルになっています。これらのロギング特性をイネーブルにするには、「コンフィギュレーション変更通知およびロギング機能の設定」（P.4）に示す作業を実行します。

コンフィギュレーション変更通知およびロギング機能を設定する方法

ここでは、次の各手順について説明します。

コンフィギュレーション変更通知およびロギング機能の設定

コンフィギュレーション変更通知およびロギング機能をイネーブルにするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging enable**
6. **logging size** *entries*
7. **hidekeys**
8. **notify syslog**
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。 • 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： `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。
ステップ 3	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 5	**logging enable** 例： `Router(config-archive-log-config)# logging enable`	設定変更のロギングをイネーブルにします。 • 設定変更のロギングはデフォルトでディセーブルになっています。

	コマンドまたはアクション	目的
ステップ 6	**logging size** *entries* 例： `Router(config-archive-log-config)# logging size 200`	（任意）設定ログに保持する最大エントリ数を指定します。 • *entries* 引数の有効な値の範囲は、1 ～ 1000 です。デフォルト値は 100 エントリです。 • 設定ログが一杯になると、新しいエントリを追加するたびに最も古いエントリが削除されます。 （注） 現在のログ サイズよりも小さいログ サイズが新たに指定された場合、ログ エントリの経過時間にかかわらず、新しいログ サイズになるまで最も古いログ エントリがすぐに削除されます。
ステップ 7	**hidekeys** 例： `Router(config-archive-log-config)# hidekeys`	（任意）設定ログ ファイル内のパスワード情報の表示を抑止します。 （注） **hidekeys** コマンドをイネーブルにすると、パスワード情報が設定ログ ファイルに表示されなくなるため、セキュリティが高まります。
ステップ 8	**notify syslog** 例： `Router(config-archive-log-config)# notify syslog`	（任意）設定変更の通知のリモート syslog への送信をイネーブルにします。
ステップ 9	**end** 例： `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

設定ログ エントリと統計情報の表示

設定ログのエントリまたは設定ログのメモリ使用量に関する統計情報を表示するには、ここに示す作業を実行します。

設定ログ エントリを表示し、設定ログのメモリ使用量を監視するために、コンフィギュレーション変更通知およびロギング機能に **show archive log config** コマンドが用意されています。

手順の概要

1. **enable**
2. **show archive log config** *number* [*end-number*]
3. **show archive log config all provisioning**
4. **show archive log config statistics**
5. **exit**

手順の詳細

ステップ 1　enable

このコマンドを使用して、特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。たとえば次のコマンドを実行します。

```
Router> enable
```

ステップ 2　show archive log config *number* [*end-number*]

このコマンドを使用して、設定ログ エントリをレコード番号ごとに表示します。オプションの *end-number* 引数でレコード番号を指定すると、レコード番号が *number* 引数と *end-number* 引数で指定した値の間にあるすべてのログ エントリが表示されます。次に例を示します。

```
Router# show archive log config 1 2

idx   sess   user@line        Logged command
 1     1     user1@console    logging enable
 2     1     user1@console    logging size 200
```

この例では、設定ログ エントリ番号 1 と 2 が表示されています。*number* 引数と *end-number* 引数の値の有効範囲は 1 ～ 2147483647 です。

ステップ 3　show archive log config provisioning

このコマンドを使用して、すべての設定ログ ファイルを、表形式ではなく、コンフィギュレーション ファイルに現れるとおりに表示します。次に例を示します。

```
Router# show archive log config all provisioning

archive
 log config
  logging enable
  logging size 200
```

この表示では、ログに記録されたコマンドを正しく適用するために必要な、コンフィギュレーション モードを変更するために使用したコマンドも表示されています。

ステップ 4　show archive log config statistics

このコマンドを使用して、設定のメモリ使用量情報を表示します。次に例を示します。

```
Router# show archive log config statistics

Config Log Session Info:
   Number of sessions being tracked: 1
   Memory being held: 3910 bytes
   Total memory allocated for session tracking: 3910 bytes
   Total memory freed from session tracking: 0 bytes

Config Log log-queue Info:
   Number of entries in the log-queue: 3
   Memory being held in the log-queue: 671 bytes
   Total memory allocated for log entries: 671 bytes
   Total memory freed from log entries:: 0 bytes
```

ステップ 5　exit

このコマンドを使用して、ユーザ EXEC モードを終了します。次に例を示します。

```
Router# exit
Router>
```

設定ログ エントリのクリア

設定ログのエントリは、2 つのうちいずれかの方法でクリアできます。設定ログのサイズを小さくするには、**logging size** コマンドを使用します。また、**logging enable** コマンドで、設定ログをいったんディセーブルにしてから再度イネーブルにします。

ここでは、次の各手順について説明します。

- 「ログ サイズを小さくすることによる設定ログのクリア」（P.7）
- 「設定ログをディセーブルすることによる設定ログのクリア」（P.8）

ログ サイズを小さくすることによる設定ログのクリア

logging size コマンドを使用して設定ログのエントリをクリアするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging size** *entries*
6. **logging size** *entries*
7. **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。 • 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： `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。
ステップ 3	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー 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 5	**logging size** *entries* **例：** `Router(config-archive-log-config)# logging size 1`	設定ログに保持する最大エントリ数を指定します。 **（注）** 設定ログのサイズを 1 に設定すると、最新のエントリ以外のエントリが削除されます。
ステップ 6	**logging size** *entries* **例：** `Router(config-archive-log-config)# logging size 200`	設定ログに保持する最大エントリ数を指定します。 **（注）** 設定ログのサイズは、設定ログをクリアした後で目的の値にリセットする必要があります。
ステップ 7	**end** **例：** `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

例

次に、サイズを 1 に減らしてからサイズを目的の値にリセットすることで、設定ログをクリアする例を示します。

```
Router# configure terminal

Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging size 1
Router(config-archive-log-config)# logging size 200
Router(config-archive-log-config)# end
```

設定ログをディセーブルすることによる設定ログのクリア

logging enable コマンドを使用して設定ログのエントリをクリアするには、ここに示す作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **no logging enable**
6. **logging enable**
7. **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。 • 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： `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。
ステップ 3	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	設定変更ロガー コンフィギュレーション モードを開始します。
ステップ 5	**no logging enable** 例： `Router(config-archive-log-config)# no logging enable`	設定変更のロギングをディセーブルにします。 **（注）** 設定ログをディセーブルにすると、すべてのレコードが削除されます。
ステップ 6	**logging enable** 例： `Router(config-archive-log-config)# logging enable`	設定変更のロギングをイネーブルにします。
ステップ 7	**end** 例： `Router(config-archive-log-config)# end`	特権 EXEC モードに戻ります。

例

次に、設定ログをディセーブルにしてからイネーブルにすることで設定ログをクリアする例を示します。

```
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# no logging enable
Router(config-archive-log-config)# logging enable
Router(config-archive-log-config)# end
```

コンフィギュレーション変更通知およびロギング機能の設定例

ここでは、次の設定例について説明します。

- 「コンフィギュレーション変更通知およびロギング機能の設定：例」

コンフィギュレーション変更通知およびロギング機能の設定：例

次に、設定ログの最大エントリ数を 200 にして設定ロギングをイネーブルにする例を示します。この例では、設定ログ レコード内のパスワード情報の表示を抑止することでセキュリティを向上させ、syslog 通知を有効にしています。

```
configure terminal

archive
 log config
 logging enable
 logging size 200
 hidekeys
 notify syslog
```

その他の関連資料

ここでは、コンフィギュレーション変更通知およびロギング機能に関する関連資料について説明します。

関連資料

関連項目	参照先
コンフィギュレーション ファイルの管理についての情報	『Managing Configuration Files』
コンフィギュレーション ファイルを管理するためのコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **archive**
- **hidekeys**
- **log config**
- **logging enable**（**config-archive-log**）
- **logging size**（**config-archive-log**）
- **notify syslog**
- **show archive log config**

コンフィギュレーション変更通知およびロギングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/cfn にある Cisco Feature Navigator にアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーション変更通知およびロギングの機能情報

機能名	リリース	機能情報
コンフィギュレーション変更通知およびロギング	12.3(4)T 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	コンフィギュレーション変更通知およびロギング（コンフィギュレーション ロギング）機能を使用すると、設定ログを実装することで、セッションごとまたはユーザごとに設定変更を追跡できます。設定ログは、適用された各コンフィギュレーション コマンド、コマンドを適用した人、コマンドに対する Parser Return Code、コマンドを適用した時刻を追跡します。また、この機能により、設定ログが変化したときに非同期通知を登録されたアプリケーションに送信する、通知メカニズムも追加されます。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション変更通知およびコンフィギュレーション変更ロギング」（P.3） • 「コンフィギュレーション変更通知およびロギング機能の設定」（P.4） • 「設定ログ エントリと統計情報の表示」（P.5） この機能により、**archive**、**hidekeys**、**log config**、**logging enable**、**logging size**、**notify syslog**、**show archive log config** の各コマンドが変更されました。
EAL4+ 認定のための設定ロガーの機能拡張	12.3(14)T 12.2(27)SBC	Cisco IOS Release 12.3(14)T および 12.2(27)SBC では、設定変更ロギング プロセスに対してさらなる機能拡張が行われています。これらの機能拡張は、ロギング プロセスが、Conformance to Common Criteria, Evaluation Assurance Level 4+（EAL4+）Firewall Protection Profiles で規定されている要件を満たすようするための作業を支援します。 この機能に関する詳細については、次の項を参照してください。 • 「EAL4+ 認定のための設定ロガーの機能拡張」（P.3）

コンフィギュレーション ロガー永続性

コンフィギュレーション ロガー永続性機能は「クイック保存」機能を実装することで、Cisco IOS コンフィギュレーションとプロビジョニング アクションの運用上の堅牢性を高めます。コンフィギュレーション ロガー永続性機能を設定すると、Cisco IOS ソフトウェアはスタートアップ コンフィギュレーション全体を保存するのではなく、最後の startup-config ファイルが生成された時点から入力されたコマンドだけを保存します。

この章で紹介する機能情報の入手方法

使用する Cisco IOS ソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「コンフィギュレーション ロガー永続性の機能情報」（P.9）を参照してください。

プラットフォームと Cisco IOS および Catalyst OS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

この章の構成

コンフィギュレーション ロガー永続性の前提条件

コンフィギュレーション ロガー永続性機能をイネーブルにするには、disk0: を構成し、ルータ上に外部フラッシュ カードを挿入する必要があります。

コンフィギュレーション ロガー永続性機能の最適な結果を実現するためには、Cisco IOS Release 12.2(33)SRA、Release 12.4(11)T、Release 12.2(33)SXH、あるいは Release 12.2(33)SB をシステムにインストールする必要があります。

コンフィギュレーション ロガー永続性について

コンフィギュレーション ロガー永続性機能を理解して使用するには、次の概念をよく理解しておくことを推奨します。

- 「コンフィギュレーション ロガー永続性を使用したコンフィギュレーション ファイルの保存」
- 「保持されたコマンド」

コンフィギュレーション ロガー永続性を使用したコンフィギュレーション ファイルの保存

Cisco IOS ソフトウェアは startup-config コンフィギュレーション ファイルを使用して、リロード全体でルータ コンフィギュレーション コマンドを保存します。この 1 つのファイルには、ルータの再起動時に適用する必要があるコマンドがすべて含まれています。**write memory** コマンドまたは **copy** *url* **startup-config** コマンドを入力するたびに、startup-config コンフィギュレーション ファイルが更新されます。running-config ファイルのサイズが大きくなると、startup-config ファイルを NVRAM ファイル システムに保存する時間が長くなります。startup-config ファイルは 1 MB 以上になることもあります。このサイズのファイルの場合、startup-config ファイルの 1 行を変更すると、ほとんどのコンフィギュレーションが変更されていない場合でも、全体の startup-config ファイルを再度保存する必要があります。

コンフィギュレーション ロガー永続性機能は「クイック保存」機能を実装します。この目的は、startup-config ファイルの変更を保存する時間が保存する（startup-config ファイルと相対した）差分変更のサイズに比例する「コンフィギュレーション保存」メカニズムを提供することです。

Cisco IOS コンフィギュレーション ロガーはコマンドライン プロンプトから手動で入力したすべての変更をログ出力します。この機能では、ログの変更が発生したときに登録済みのクライアントに通知します。設定ログの内容はランタイム メモリに保存されます。ログの内容は再起動後は保持されません。

コンフィギュレーション ロガー永続性機能は、リロード全体でユーザが入力したコンフィギュレーション コマンドを保持するメカニズムです。Command-Line Interface（CLI; コマンドライン インターフェイス）で入力したコマンド（コンフィギュレーション モードで入力したコマンド）だけがリロード全体で保持されます。この機能は Cisco IOS のセキュア ファイル システムを使用して、生成されるコンフィギュレーション コマンドを保持します。

（注） Cisco IOS コンフィギュレーション ロガーはシステム メッセージ ロギング（syslog）ファシリティとは異なります。Syslog はシステム メッセージを追跡するための一般的なログ ファシリティです。コンフィギュレーション ロガーは CLI で入力されたコンフィギュレーション コマンドに関する情報を追跡します。

保持されたコマンド

Cisco IOS コンフィギュレーション ロガーで保持されたコマンドはスタートアップ コンフィギュレーションの拡張として使用されます。これらの保存済みコマンドはクイック保存機能を提供します。startup-config ファイル全体を保存するのではなく、Cisco IOS ソフトウェアは最後の startup-config ファイル生成以降入力されたコマンドだけを保存します。

ログ出力されたコマンドだけが保持されます。コンフィギュレーション ロガーの次の追加データは保持*されません*。

- コマンドを出力したユーザ
- ユーザがログインした IP アドレス
- ログ出力されたコマンドのセッションとログ インデックス
- コマンドの入力時刻
- 入力されたコマンドに関連付けられている前後の NVGEN 出力
- 入力されたコマンドの Parser Return Code 出力

保持されたコマンドの主な目的は、startup-config ファイルのクイック保存拡張として使用することです。コンフィギュレーション コマンドに関連付けられている追加情報はクイック保存目的では有用ではありません。（監査目的などで）再起動後に追加情報を保持する場合は、次の手順を実行します。

1. Syslog へのコンフィギュレーション ロガー通知をイネーブルにします。
2. Syslog 保持機能をイネーブルにします。

あるいは、Cisco Networking Services、CiscoView、Cisco IOS デバイスを管理して標準外のストレージ ソリューションの構成変更を追跡するその他のネットワーク管理システムを使用できます。

デフォルトでは、リロード時に保持されたコマンドが startup-config ファイルに追加されます。CLI コンフィギュレーション コマンドを使用して明示的にこの動作を設定した場合にだけこれらのコマンドが適用されます。

コンフィギュレーション ロガー永続性機能を設定する方法

この項では、次について説明します。

- 「コンフィギュレーション ロガー永続性機能のイネーブル化」（必須）
- 「コンフィギュレーション ロガー永続性機能の検証とトラブルシューティング」（任意）

コンフィギュレーション ロガー永続性機能のイネーブル化

コンフィギュレーション ロガー永続性機能はクイック保存メカニズムを実装するため、スタートアップ コンフィギュレーションの変更を保存するためにかかる時間が、保存する必要がある（スタートアップ コンフィギュレーションと相対した）差分変更のサイズに比例します。Cisco IOS コンフィギュレーション ロガーで保持されたコマンドはスタートアップ コンフィギュレーションの拡張として使用されます。スタートアップ コンフィギュレーションの拡張として使用される保存済みコマンドはクイック保存機能を提供します。startup-config ファイル全体を保存するのではなく、Cisco IOS ソフトウェアは最後の startup-config ファイル生成以降入力されたコマンドだけを保存します。

コンフィギュレーション ロガー永続性機能をイネーブルにするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging persistent** {**auto** | **manual**}
6. **logging persistent reload**
7. **logging size** *entries*

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。 • 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： `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。
ステップ 3	**archive** 例： `Router(config)# archive`	アーカイブ コンフィギュレーション モードを開始します。
ステップ 4	**log config** 例： `Router(config-archive)# log config`	アーカイブ configuration-log コンフィギュレーション モードをイネーブルにします。
ステップ 5	**logging persistent** {**auto** | **manual**} 例： `Router(config-archive-log-cfg)# logging persistent auto`	コンフィギュレーション ロギング永続機能をイネーブルにします。 • **auto** キーワードは、各コンフィギュレーション コマンドが自動的に Cisco IOS セキュア ファイル システムに保存されることを指定します。 • **manual** キーワードは、コンフィギュレーション コマンドを Cisco IOS セキュア ファイル システムにオンデマンドで保存できることを指定します。これを実行するには、**archive log config persistent save** コマンドを使用する必要があります。 （注） **logging persistent auto** コマンドをイネーブルにするには、disk0: を構成し、ルータ上に外部フラッシュ カードを挿入する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**logging persistent reload** 例： `Router(config-archive-log-cfg)# logging persistent reload`	続いて、リロード後に、コンフィギュレーション ロガー データベースに保存された（最後の **write memory** コマンド以降）コンフィギュレーション コマンドを running-config ファイルに適用します。
ステップ 7	**logging size** *entries* 例： `Router(config-archive-log-cfg)# logging size 10`	設定ログに保持する最大エントリ数を指定します。 • 有効な値の範囲は、1 ～ 1000 です。 • デフォルト値は 100 エントリです。

コンフィギュレーション ロガー永続性機能の検証とトラブルシューティング

3 つのコマンドを使用して、設定ログの内容を検証、アーカイブ、クリアできます。トラブルシューティングでは、ステップ 4 のコマンドでデバッグをオンにします。

手順の概要

1. **show archive log config persistent**
2. **clear archive log config persistent**
3. **archive log config persistent save**
4. **debug archive log config persistent**

手順の詳細

ステップ 1　show archive log config persistent

このコマンドは設定ログに保持されたコマンドを表示します。このコマンドは configlet 形式で表示されます。次に、このコマンドのサンプル出力を示します。

```
Router# show archive log config persistent

!Configuration logger persistentarchive
 log config
 logging persistent auto
 logging persistent reload
archive
 log config
logging size 10
logging console
interface loop 101
 ip address 10.1.1.1 255.255.255.0
 ip address 10.2.2.2 255.255.255.0
 no shutdown
```

ステップ 2　clear archive log config persistent

このコマンドはコンフィギュレーション ロギング永続データベース エントリをクリアします。コンフィギュレーション ロギング データベース ファイルのエントリだけが削除されます。新しいエントリをログ出力するために使用されるため、ファイル自体は削除されません。このコマンドを入力すると、アーカイブ ログがクリアされたことを示すメッセージが表示されます。

```
Router# clear archive log config persistent

Purged the config log persist database entries successfully
```

```
Router#
```

ステップ 3 **archive log config persistent save**

このコマンドは Cisco IOS セキュア ファイル システムに設定ログを保存します。このコマンドが動作するには、**archive log config persistent save** コマンドを設定する必要があります。

ステップ 4 **debug archive log config persistent**

このコマンドはデバッグ機能をオンにします。デバッグがオンになっていることを示すメッセージが返されます。

```
Router# debug archive log config persistent

debug archive log config persistent debugging is on
```

コンフィギュレーション ロガー永続性機能の設定例

この項では、Cisco 7200 シリーズ ルータでのコンフィギュレーション ロガー永続性機能の設定例を示します。

- 「Cisco 7200 シリーズ ルータでのコンフィギュレーション ロガー永続性機能の設定：例」

Cisco 7200 シリーズ ルータでのコンフィギュレーション ロガー永続性機能の設定：例

この例では、各コンフィギュレーション コマンドが自動的に Cisco IOS セキュア ファイル システムに保存され、（最後の **write memory** コマンドの実行以降）コンフィギュレーション ロガー データベースに保存されたコンフィギュレーション コマンドが running-config ファイルに適用され、設定ログに保持される最大エントリ数が 10 に設定されます。

```
Router> enable
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-config)# logging persistent auto

configuration log persistency feature enabled. Building configuration... [OK]

Router(config-archive-log-config)# logging persistent reload
Router(config-archive-log-config)# logging size 10
Router(config-archive-log-config)# archive log config persistent save
Router(config-archive-log-config)# end
Router#
```

その他の関連資料

次の項に、コンフィギュレーション ロガー永続性機能に関する参考資料を示します。

関連資料

関連項目	参照先
包括的なコマンドリファレンス情報	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格や変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
この機能によってサポートされる新しい RFC や変更された RFC 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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、Cisco IOS マスター コマンド リストを参照してください。

- **archive log config persistent save**
- **clear archive log config**
- **debug archive log config persistent**
- **logging persistent（config-archive-log-cfg）**
- **logging persistent reload**
- **show archive log config**

コンフィギュレーション ロガー永続性の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　コンフィギュレーション ロガー永続性の機能情報

機能名	リリース	機能情報
コンフィギュレーション ロガー永続性	12.2(33)SRA 12.4(11)T 12.2(33)SXH 12.2(33)SB	コンフィギュレーション ロガー永続性機能は「クイック保存」機能を実装することで、Cisco IOS コンフィギュレーションとプロビジョニング アクションの運用上の堅牢性を高めます。Cisco IOS Release 12.2(33)SRA、Release 12.4(11)T、Release 12.2(33)SXH、Release 12.2(33)SB で有効な Cisco IOS ソフトウェアはスタートアップ コンフィギュレーション全体を保存するのではなく、最後の startup-config ファイルが生成された時点から入力されたコマンドだけを保存します。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション ロガー永続性について」（P.2） • 「コンフィギュレーション ロガー永続性機能を設定する方法」（P.3）

用語集

API：アプリケーション プログラミング インターフェイス。

CAF：コマンド アクション機能。

CDP：Cisco Discovery Protocol。

CSB：コマンド ステータス ブロック。

HA：高可用性アーキテクチャ。

MIB：Management Information Base（管理情報ベース）。

NAF：NVGEN アクション機能。

NVGEN：不揮発性生成。

NVRAM：不揮発性ランダム アクセス メモリ。

parse chain：Cisco IOS コマンドの構文を定義する一連の C 言語マクロ。

RP：Route Processor（ルート プロセッサ）。

SNMP：Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。

XML：eXtensible マークアップ言語。

コンフィギュレーション パーティショニング

コンフィギュレーション パーティショニング機能によって実行コンフィギュレーション状態をモジュール化（「パーティショニング」）して、Cisco IOS ソフトウェアで実行コンフィギュレーションに柔軟にアクセスできるようにします。

この機能が搭載された Cisco IOS ソフトウェア イメージではデフォルトでオンになっています。

デバイスのコンフィギュレーション状態は、**show running-config** コマンドがユーザによって実行されるとダイナミックに取得されます。コンフィギュレーション パーティショニング機能がイネーブルの場合、システムによってデバイスのコンフィギュレーション状態が分割され、グループ化（「パーティション」と呼ばれる）されます。これにより、実行コンフィギュレーションで表示されるコマンド リストの生成時にユーザが確認したいコンフィギュレーション状態のみを取得できます。この機能により、システムのコンフィギュレーション状態全体が処理される従来の処理方法とは異なり、実行コンフィギュレーション コマンドのリストの生成時に実行コンフィギュレーション状態の一部のみが処理されるため、コンフィギュレーションが複雑なハイエンド システムのパフォーマンスを向上できます。

デフォルトのコンフィギュレーション パーティションはこの機能を導入することで提供されます。将来のリリースでは、他の Cisco IOS ソフト機能によって独自のコマンド パーティションが提供される可能性があります。

この章で紹介する機能情報の入手方法

この機能は、Cisco 7600 シリーズ向けソフトウェア イメージの リリース 12.2(33)SRB で追加されました。その他のリリース統合アップデートは、「コンフィギュレーション パーティショニングの機能情報」（P.19）に随時追加されます。

プラットフォームと Cisco IOS および Catalyst OS ソフトウェア イメージのサポート情報の検索

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

目次

コンフィギュレーション パーティショニングについて

コンフィギュレーション パーティショニング機能を使用するには、次の概念を理解しておく必要があります。

- 「システム実行コンフィギュレーション」
- 「実行コンフィギュレーションを取得して表示またはコピーする」
- 「実行コンフィギュレーションをパーティショニングする利点」

システム実行コンフィギュレーション

Cisco IOS ソフトウェアベース デバイスのコンフィギュレーション管理には、不揮発性メモリに格納されたスタートアップ コンフィギュレーション（startup-config）およびシステムに適用されているすべてのコンフィギュレーション オプションである実行コンフィギュレーション（running-config）を管理する必要があります。通常、スタートアップ コンフィギュレーション ファイルはシステム起動時にロードされ、コマンドラインインターフェイスを使用して適用されたシステムに対する実行コンフィギュレーションの変更は、実行コンフィギュレーションをコンフィギュレーション ファイルにコピーすることで保存されます（ローカルまたはネットワーク上）。ファイルは、起動時にデバイスをコンフィギュレーションする場合、または他のデバイスをコンフィギュレーションする場合に使用されます。

実行コンフィギュレーションを取得して表示またはコピーする

Cisco IOS のソフトウェア コンフィギュレーション モデルでは、コンフィギュレーション状態は分散して維持され、各コンポーネントは独自のコンフィギュレーション状態を保持します。グローバル コンフィギュレーション情報を取得するには、ソフトウェアは各コンポーネントをポーリングして、分散された情報を収集する必要があります。このコンフィギュレーション状態の取得処理は Nonvolatile Generation（NVGEN; 不揮発性生成）として知られる処理によって実行され、現在のコンフィギュレーション状態を表示するコマンドの **show running-config** や、実行コンフィギュレーションをファイルにコピーして保存するコマンドの **copy system:running-configuration** によって呼び出されます。取得処理が呼び出されると、NVGEN 処理によって各システム コンポーネント、各インターフェイス インスタンス、およびその他すべてのコンフィギュレーションされたコンポーネント オブジェクトが標準の順序でクエリーされます。NVGEN がこれらのクエリーを実行しているシステムを通過するときに、実行コンフィギュレーション ファイルが作成されます。表示およびコピーには作成された「仮想ファイル」が使用されます。

実行コンフィギュレーションをパーティショニングする利点

コンフィギュレーション パーティショニング機能は、Cisco IOS ソフトウェアに追加された一連のコンフィギュレーション生成のパフォーマンス拡張機能の最新機能です（関連機能については、「関連マニュアル」（P.17）を参照してください）。この機能によって、**show running-config** コマンドの実行時に表示したいシステム コンポーネントのみがクエリーされるため、システム応答時間が短縮されます。

コンフィギュレーション パーティショニング機能がイネーブルの場合、システムによってデバイスのコンフィギュレーション状態が分割されグループ化（「パーティション」と呼ばれる）されます。これにより、仮想実行コンフィギュレーション ファイル（コンフィギュレーション コマンドのリスト）が生成されます。新しいコマンド、**show running-config partition** を使用すると、一度に実行コンフィギュレーションをすべて表示したり、特定のストリングに一致する行のみを表示するのではなく、検証したい実行コンフィギュレーションの部分のみを表示することができます。

この機能は、ユーザが表示したいシステム コンポーネントのグループ（特定のインターフェイスなど）のみの NVGEN 処理をシステムで実行してシステムのパフォーマンスを向上できることが主な利点であると言えます。この特徴は、システム コンポーネントをすべて処理した後に生成されたリストをフィルタする **show running-config** コマンドのその他の拡張とは対照的です。

実行コンフィギュレーションを部分的に生成するため、システムのコンフィギュレーション状態を選択的に処理することを「コンフィギュレーション パーティショニング」と呼びます。

コンフィギュレーション情報に柔軟にアクセスできることで、サイズの大きいコンフィギュレーション ファイルがあるハイエンドなルーティング プラットフォームにパフォーマンスの重大な利点をもたらし、同時に詳細なコンフィギュレーション機能を細かに実装することでコンフィギュレーション管理を強化します。詳細なコンフィギュレーション オプションには、Cisco IOS ソフトウェアのカスタマー サービスのプロビジョニング、コンフィギュレーション ロールバック、コンフィギュレーション ロッキング、およびコンフィギュレーション アクセス コントロールのサポートが含まれます。

コンフィギュレーション パーティショニング機能を使用するには

ここでは、次の作業について説明します。

- 「コンフィギュレーション パーティションの表示」（P.3）（任意）
- 「コンフィギュレーション パーティショニング機能をディセーブルにする」（P.5）（任意）

コンフィギュレーション パーティションの表示

この機能を活用するには、主に特権 EXEC モードで **show running-config partition** *part* コマンドを使用します。このコマンドは、**show running-config** コマンド専用の拡張です。

（注） **partition** *part* コマンドの拡張は、**more:system running-config** コマンドでは利用できません。

この機能は既存のコマンドのパフォーマンスを向上するので、この機能が搭載された Cisco IOS ソフトウェア イメージではデフォルトでオンになっています。お使いのシステムでサポートおよび実行されているかどうかを簡単に判断するには、特権 EXEC モードで **show running-config partition ?** コマンドを実行します。

手順の概要

1. **show running-config partition ?**
2. **show runningconfig partition** *part*

手順の詳細

ステップ 1 **show running-config partition ?**

このコマンドを実行すると、システムに表示できる実行コンフィギュレーションの部分が表示されます。

コンフィギュレーション パーティショニング機能がシステムでサポートされており、イネーブルの場合は、ヘルプ出力の 1 行目に「config partition is TRUE」というストリングが表示されます。

ここに示すコマンド構文を入力するとエラー メッセージが表示される場合は、この機能はシステムでサポートされていません。実行コンフィギュレーションの部分のみを表示できる他のリリースで利用可能な **show running-config** コマンドの既存の拡張については、コマンドのマニュアルを参照してください。

（注） 利用できるコンフィギュレーションの部分は、ソフトウェア イメージによって異なり、コンフィギュレーションされている機能に依存します。

```
Router# show running-config partition ?
 config partition is TRUE
  access-list       All access-list configurations
  boot              All boot configurations
  class-map         All class-map configurations
  common            All remaining unregistered configurations
  global-cdp        All global cdp configurations
  interface         All Interface specific Configurations
  ip-as-path        All IP as-path configurations
  ip-community      All IP community list configurations
  ip-domain-list    All ip domain list configurations
  ip-prefix-list    All ip prefix-list configurations
  ip-static-routes  All IP static configurations
  line              All line mode configurations
  policy-map        All policy-map configurations
  route-map         All route-map configurations
  router            All routing configurations
  snmp              All SNMP configurations
  tacacs            All TACACS configurations
```

表示する実行コンフィギュレーションの部分を選択して、ステップ 2 で関連キーワードを *part* 引数として使用します。

ステップ 2 **show running-config partition** *part*

たとえば、システムで NVGEN 処理を実行コンフィギュレーション状態の access-list 部分に関連するコンポーネントのみで実行して、access-list に関連するコンポーネントのみを表示する場合は、**show running-config partition access-list** コマンドを入力します。

```
Router# show running-config partition access-list
        Building configuration...

Current configuration : 127 bytes
!
Configuration of Partition access-list
!
!
!
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
!
end
```

（注） このコマンドを使用すると、NVGEN 処理を実行して、特定のインターフェイスに関する結果出力を表示します。複数のインターフェイスがアクティブなシステムで使用できる設計のこの動作がコンフィギュレーション パーティショニング機能の主な役割です。

次の例では、メインのコンフィギュレーション パーティションはインターフェイス コンフィギュレーションです。生成される特定のコンフィギュレーション部分は、ファスト イーサネット インターフェイス 0/0 のコンフィギュレーションです。

```
Router# show running-config partition interface fastethernet0/0
Building configuration...

Current configuration : 213 bytes
!
Configuration of Partition interface FastEthernet0/0
!
!
interface FastEthernet0/0
 ip address 10.4.2.39 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex half
 ipv6 enable
 no cdp enable
!
!
end
```

コンフィギュレーション パーティショニング機能をディセーブルにする

この機能は既存のコマンドのパフォーマンスを向上させるので、この機能が搭載された Cisco IOS ソフトウェア イメージではデフォルトでオンになっています。しかし、この機能は少量のシステム リソース（メモリおよび CPU）を消費するため不要な場合、ディセーブルにしたい場合があります。コンフィギュレーション パーティショニングをディセーブルにするには、次の手順を実行してください。手順はユーザ EXEC モードで起動されていることを前提としています。

手順の概要

1. **enable**
2. **configure terminal**
3. **no parser config partition**

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。 • 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：** `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。

ステップ 3	**no parser config partition**
	
	例：
	`Router(config)# no parser config partition`
	`Disabling config partitioning`
	`Router(config)#`
		コンフィギュレーション パーティショニング機能をディセーブルにします。

次の作業

機能をディセーブルにした後、イネーブルにするには、グローバル コンフィギュレーション モードで **parser config partition** コマンドを使用します。

（注） この機能はデフォルトでイネーブルになっているので、実行コンフィギュレーション ファイルには、**no** 形式のみが表示されます。または、**copy running-config startup-config** コマンドを実行するとスタートアップ コンフィギュレーション ファイルに書き込まれます。

コンフィギュレーション パーティショニングするためのコンフィギュレーション例

ここでは、**show running-config partition** コマンドを使用してコンフィギュレーション パーティションを表示する例を示します。

- 「コンフィギュレーション パーティションの表示：例」

コンフィギュレーション パーティションの表示：例

この例では、管理者が特定のインターフェイスの状態、およびシステムの他のコンポーネントの一部のコンフィギュレーションを確認するために実行する一連の手順で **show running-config partition** と関連コマンドを一緒に使用しています。標準の **show running-config** コマンド（例：**show running-config | include** access-list）による、同等のフィルタされた出力もデモとして含まれます。

（注） *part* 引数には **show running-config part router eigrp 1** のように複数のパーティション名キーワードを含めることができます。

```
gt3-7200-3# show running-config partition ?
  access-list       All access-list configurations
  boot              All boot configurations
  class-map         All class-map configurations
  global-cdp        All global cdp configurations
  interface         All Interface specific Configurations
  ip-as-path        All IP as-path configurations
  ip-community      All IP community list configurations
  ip-domain-list    All ip domain list configurations
  ip-static-routes  All IP static configurations
  line              All line mode configurations
  policy-map        All policy-map configurations
  route-map         All route-map configurations
  router            All routing configurations
  service           All service configurations
  snmp              All SNMP configurations

gt3-7200-3# show running-config partition access-list
Building configuration...

Current configuration : 87 bytes
!
!
!
!
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
!
end

gt3-7200-3# show running-config | include access-list
access-list 90 permit 0.0.0.0 1.2.3.5
access-list 100 permit 10 any any
gt3-7200-3#

gt3-7200-3# show running-config partition boot
Building configuration...

Current configuration : 51 bytes
!
boot network tftp:/service_config.txt
!
!
!
end

gt3-7200-3# show running-config partition class-map
Building configuration...

Current configuration : 78 bytes
!
!
!
class-map match-all abc
  match any
class-map match-all xyz
!
!
!
end

gt3-7200-3# show running-config | begin class-map
class-map match-all abc
  match any
```

```
class-map match-all xyz
!
!

gt3-7200-3# show running-config partition global-cdp
Building configuration...

Current configuration : 43 bytes
!
!
!
cdp timer 20
cdp holdtime 100
!
end

gt3-7200-3# show running-config | include global-cdp
cdp timer 20
cdp holdtime 100
gt3-7200-3#

gt3-7200-3# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
Ethernet2/0                10.4.2.32       YES NVRAM  up                    up
Ethernet2/1                unassigned      YES NVRAM  administratively down down
Ethernet2/2                unassigned      YES NVRAM  administratively down down
Ethernet2/3                unassigned      YES NVRAM  administratively down down
Serial3/0                  unassigned      YES NVRAM  administratively down down
Serial3/1                  unassigned      YES NVRAM  administratively down down
Serial3/2                  unassigned      YES NVRAM  administratively down down
Serial3/3                  unassigned      YES NVRAM  administratively down down
Loopback0                  unassigned      YES NVRAM  administratively down down
Loopback234                unassigned      YES NVRAM  administratively down down

gt3-7200-3# show running-config partition interface fastethernet0/0
Building configuration...

Current configuration : 98 bytes
!
!
!
interface FastEthernet0/0
 no ip address
 no ip route-cache
 shutdown
 duplex half
!
!
end

gt3-7200-3# show running-config partition interface ethernet2/0
Building configuration...

Current configuration : 122 bytes
!
!
!
interface Ethernet2/0
 ip address 10.4.2.32 255.255.255.0
 no ip proxy-arp
 no ip route-cache
 duplex half
!
```

```
!
end

gt3-7200-3# show running-config partition interface ethernet2/1
Building configuration...

Current configuration : 94 bytes
!
!
!
interface Ethernet2/1
 no ip address
 no ip route-cache
 shutdown
 duplex half
!
!
end

gt3-7200-3# show running-config partition interface ethernet2/2
Building configuration...

Current configuration : 94 bytes
!
!
!
interface Ethernet2/2
 no ip address
 no ip route-cache
 shutdown
 duplex half
!
!
end

gt3-7200-3# show running-config partition interface ethernet2/3
Building configuration...

Current configuration : 94 bytes
!
!
!
interface Ethernet2/3
 no ip address
 no ip route-cache
 shutdown
 duplex half
!
!
end

gt3-7200-3# show running-config partition interface serial3/0
Building configuration...

Current configuration : 103 bytes
!
!
!
interface Serial3/0
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
```

```
!
end

gt3-7200-3# show running-config partition interface serial3/1
Building configuration...

Current configuration : 103 bytes
!
!
!
interface Serial3/1
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
!
end

gt3-7200-3# show running-config partition interface serial3/2
Building configuration...

Current configuration : 103 bytes
!
!
!
interface Serial3/2
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
!
end

gt3-7200-3# show running-config partition interface serial3/3
Building configuration...

Current configuration : 103 bytes
!
!
!
interface Serial3/3
 no ip address
 no ip route-cache
 shutdown
 serial restart-delay 0
!
!
end

gt3-7200-3# show running-config partition interface loopback0
Building configuration...

Current configuration : 79 bytes
!
!
!
interface Loopback0
 no ip address
 no ip route-cache
 shutdown
!
!
```

```
end

gt3-7200-3# show running-config partition interface loopback1
                                                              ^
% Invalid input detected at '^' marker.

gt3-7200-3# show running-config partition interface loopback234
Building configuration...

Current configuration : 81 bytes
!
!
!
interface Loopback234
 no ip address
 no ip route-cache
 shutdown
!
!
end

gt3-7200-3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
gt3-7200-3(config)# interface ethernet 2/0.1
gt3-7200-3(config-subif)# exit
gt3-7200-3(config)# exit

gt3-7200-3#
00:13:05: %SYS-5-CONFIG_I: Configured from console by console
gt3-7200-3# show running-config partition interface ethernet2/0.1
Building configuration...

Current configuration : 58 bytes
!
!
!
interface Ethernet2/0.1
 no ip route-cache
!
!
end
gt3-7200-3# show run partition ip?
ip-as-path  ip-community  ip-domain-list  ip-static-routes

gt3-7200-3#sh run part ip-as
gt3-7200-3#sh run part ip-as-path

Building configuration...

Current configuration : 125 bytes
!
!
!
ip as-path access-list 2 permit $ABC
ip as-path access-list 2 permit $xyz*
ip as-path access-list 2 permit qwe*
!
end
gt3-7200-3# show running-config partition ip-community
Building configuration...

Current configuration : 92 bytes
!
!
```

```
!
ip community-list standard asd permit
ip community-list expanded qwe deny uio*
!
end

gt3-7200-3# show running-config | include ip community
ip community-list standard asd permit
ip community-list expanded qwe deny uio*
gt3-7200-3#
gt3-7200-3# show running-config partition ip-domain-list
Building configuration...

Current configuration : 70 bytes
!
ip domain-list iop
ip domain-list tyu
ip domain-list jkl
!
!
!
end
gt3-7200-3# show running-config partition ip-static-routes
Building configuration...

Current configuration : 98 bytes
!
!
!
ip route 0.0.0.0 0.0.0.0 Ethernet2/0
ip route 171.69.1.129 255.255.255.255 10.4.29.1
!
end

gt3-7200-3# show running-config partition line
Building configuration...

Current configuration : 489 bytes
!
!
!
!
line con 0
 exec-timeout 0 0
 transport output lat pad v120 mop telnet rlogin udptn nasi
 stopbits 1
line aux 0
 transport output lat pad v120 mop telnet rlogin udptn nasi
 stopbits 1
line vty 0
 password lab
 login
 transport input lat pad v120 mop telnet rlogin udptn nasi
 transport output lat pad v120 mop telnet rlogin udptn nasi
line vty 1 4
 login
 transport input lat pad v120 mop telnet rlogin udptn nasi
 transport output lat pad v120 mop telnet rlogin udptn nasi
!
end
gt3-7200-3# show running-config partition policy-map
Building configuration...

Current configuration : 162 bytes
```

```
!
!
!
policy-map qwer
 description policy-map qwer.
  class xyz
    shape peak 8000 32 32
policy-map p1
policy-map sdf
  class abc
   set precedence 4
!
!
!
end
gt3-7200-3# show running-config partition route-map
Building configuration...

Current configuration : 65 bytes
!
!
!
route-map iop permit 10
!
route-map rty permit 10
!
!
end
gt3-7200-3#sh run part router bgp 1
Building configuration...

Current configuration : 111 bytes
!
!
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 distance bgp 2 2 2
 no auto-summary
!
!
end

gt3-7200-3#sh run part router egp ?
<0-65535>  Remote autonomous system number

gt3-7200-3#sh run part router egp 1
Building configuration...

Current configuration : 46 bytes
!
!
!
router egp 1
 timers egp 20 20
!
!
end

gt3-7200-3# show running-config partition router ?
  bgp       Border Gateway Protocol (BGP)
  egp       Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
```

```
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

gt3-7200-3# show running-config partition router eigrp ?
<1-65535>  Autonomous system number

gt3-7200-3# show running-config partition router eigrp 1
Building configuration...

Current configuration : 13 bytes
!
!
!
!
end

gt3-7200-3#
gt3-7200-3# sh run part router eigrp 2
Building configuration...

Current configuration : 57 bytes
!
!
!
router eigrp 2
 variance 10
 auto-summary
!
!
end

gt3-7200-3# show running-config partition router ?
  bgp       Border Gateway Protocol (BGP)
  egp       Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

gt3-7200-3# show running-config partition router isis ?
  WORD  ISO routing area tag
  |     Output modifiers
  <cr>

gt3-7200-3# show running-config partition router isis qwe
Building configuration...

Current configuration : 86 bytes
!
!
!
router isis qwe
 set-attached-bit route-map qwer
 use external-metrics
!
!
end
```

```
gt3-7200-3# show running-config partition router isis ?
  WORD  ISO routing area tag
  |     Output modifiers
  <cr>

gt3-7200-3# show running-config partition router iso
gt3-7200-3# show running-config partition router iso-igrp ?
  WORD  ISO routing area tag
  |     Output modifiers
  <cr>

gt3-7200-3# show running-config partition router iso-igrp
Building configuration...

Current configuration : 31 bytes
!
!
!
router iso-igrp
!
!
end

gt3-7200-3# show running-config | begin iso
router iso-igrp
!
router isis qwe
 set-attached-bit route-map qwer
 use external-metrics
!
router egp 1
 timers egp 20 20
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 distance bgp 2 2 2
 no auto-summary
!


gt3-7200-3# show running-config partition router ?
  bgp       Border Gateway Protocol (BGP)
  egp       Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

gt3-7200-3# show running-config partition router mobile ?
  |  Output modifiers
  <cr>

gt3-7200-3# show running-config partition router mobile
Building configuration...

Current configuration : 42 bytes
!
!
!
```

```
router mobile
 distance 20
!
!
end


gt3-7200-3# sh run | include router
router mobile
router odr
router eigrp 2
router ospf 4
router iso-igrp
router isis qwe
router egp 1
router bgp 1

gt3-7200-3# show running-config partition router ?
  bgp       Border Gateway Protocol (BGP)
  egp       Exterior Gateway Protocol (EGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  rip       Routing Information Protocol (RIP)

gt3-7200-3# show running-config partition router ospf ?
  <1-65535>  Process ID

gt3-7200-3# show running-config partition router ospf 4
Building configuration...

Current configuration : 64 bytes
!
!
!
router ospf 4
 log-adjacency-changes
 distance 4
!
!
end

gt3-7200-3# sh run part service
Building configuration...

Current configuration : 190 bytes
!
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
service tcp-small-servers
!
!
!
end
gt3-7200-3# sh run part snmp
Building configuration...
```

```
Current configuration : 84 bytes
!
!
!
snmp-server community user101 RW
snmp mib target list qwe host 0.0.0.0
!
end
```

その他の参考資料

次の項に、コンフィギュレーション パーティショニング機能に関する参考資料を示します。

関連マニュアル

関連項目	参照先
実行コンフィギュレーションのパフォーマンス拡張：インターフェイスの **parser config cache**	『Configuration Generation Performance Enhancement』
カスタマー サービスのプロビジョニング 、コンフィギュレーション ロールバック、コンフィギュレーション ロッキング、およびコンフィギュレーション アクセス コントロール	『Contextual Configuration Diff Utility』
コンフィギュレーション管理：コンフィギュレーション変更およびロギング	『Configuration Change Notification and Logging』
コンフィギュレーション管理：コンフィギュレーション変更ロギングの簡易保存[1]	『Configuration Logger Persistency』
Cisco IOS ソフトウェアのコンフィギュレーション アクセス コントロールおよびコンフィギュレーション セッション ロッキング（「コンフィギュレーションのロック」）	『Exclusive Configuration Change Access and Access Session Locking』

1. 「コンフィギュレーション ロガー永続性」機能を設定すると、スタートアップ コンフィギュレーション全体を保存するのではなく、最後の startup-config ファイルが生成された時点から入力されたコマンドだけを保存します。

規格

規格	タイトル
この機能に関連する規格はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **parser config partition**
- **show running-config partition**

コンフィギュレーション パーティショニングの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その Cisco IOS ソフトウェア リリース トレインの以降のリリースでもその機能はサポートされます。

表 1　コンフィギュレーション パーティショニングの機能情報

機能名	リリース	機能情報
コンフィギュレーション パーティショニング	12.2(33)SRB 12.2(33)SB 12.2(33)SXI	コンフィギュレーション パーティショニング機能によって実行コンフィギュレーション状態をモジュール化（「パーティショニング」）して、Cisco IOS ソフトウェアで実行コンフィギュレーションに柔軟にアクセスできるようにします。この機能が搭載された Cisco IOS ソフトウェア イメージではデフォルトでオンになっています。 12.2(33)SB では、この機能が Cisco 10000 シリーズに実装されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンフィギュレーション パーティショニングについて」 • 「コンフィギュレーション パーティショニング機能を使用するには」

システム イメージのロードおよびメンテナンス

システム イメージのロードと管理

この章では、Cisco IOS ソフトウェア システム イメージのロードと管理の方法を説明します。この章では、マイクロコードのロードに関連する作業について説明します。システム イメージにはシステム ソフトウェアが含まれます。通常、マイクロコードにはシステム イメージ、またはさまざまなハードウェア デバイスに直接ロードできるハードウェア固有のソフトウェアが含まれます。

この章で説明するシステム イメージとマイクロコード コマンドの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index, Release 12.4*』を使用するかオンラインで検索します。

イメージの概要

Cisco IOS ソフトウェアは、システム イメージにパッケージされています。ルータには出荷時に、すでにイメージが入っています。しかし、ある時点で、別のイメージをルータにロードする必要が発生する可能性があります。たとえば、ソフトウェアを最新リリースにアップグレードしたり、ネットワーク上のすべてのルータで同じバージョンのソフトウェアを使う必要が発生したりする可能性があります。システム イメージが異なれば、入っている Cisco IOS 機能のセットも異なります。使用しているシステムで実行されている Cisco IOS ソフトウェアのバージョン（リリース番号）と、このシステム イメージのファイル名を判断するには、ユーザ EXEC、または特権 EXEC モードで **show version** コマンドを使用します。たとえば、「Version 12.4」は Cisco IOS Release 12.4 を、「c7200-js-mz」は「enterprise」機能セット（jz）を含む Cisco 7200 シリーズ ルータ（c7200）のシステム イメージを示します。

イメージのタイプ

ルータで使用される可能性のあるイメージのタイプは主に次の 2 種類です。

- システム イメージ：Cisco IOS ソフトウェアすべて。このイメージは、ルータの起動時にロードされ、ほとんど常に使用されます。

  大半のプラットフォームでは、イメージはフラッシュ メモリに入っています。複数のフラッシュ メモリ ファイル システム（フラッシュ、ブート フラッシュ、スロット 0、スロット 1 など）を持つプラットフォームでは、イメージは既存のフラッシュ ファイル システムのいずれにでも保存可能です。使用しているルータでサポートされているファイル システムを判断するには、**show file systems** 特権 EXEC モード コマンドを使用します。これらのイメージがデフォルトで入っている場所については、ハードウェア マニュアルを参照してください。

- ブート イメージ : Cisco IOS ソフトウェアのサブセット。このイメージは、ネットワークの起動や、ルータへの Cisco IOS イメージのロードに使用されます。また、このイメージは、ルータが有効なシステム イメージを見つけられなかった場合にも使用されます。使用しているプラットフォームによっては、このイメージは xboot イメージ、rxboot イメージ、ブートストラップ イメージ、またはブート ローダ イメージ、ヘルパー イメージと呼ばれることもあります。

  一部のプラットフォームでは、ブート イメージは ROM に入っています。また、ブート イメージがフラッシュ メモリに格納されているプラットフォームもあります。このようなプラットフォームでは、**boot bootldr** 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、ブート イメージとして使用するイメージを指定できます。使用しているルータで使用されているブート イメージについての情報は、ハードウェア マニュアルを参照してください。

イメージの命名規則

プラットフォーム、機能、イメージの場所は、イメージの名前から判断できます。命名規則は、イメージの *platform-featureset-type* です。

platform 変数は、このイメージを使用できるプラットフォームを示します。たとえば、rsp（RSP7000 搭載 Cisco 7000 シリーズ、および Cisco 7500 シリーズ）、c1600（Cisco 1600 シリーズ）、および c1005（Cisco 1005）などを *platform* 変数に使用できます。

featureset 変数は、イメージに含まれる機能パッケージを表します。Cisco IOS ソフトウェアは、特定の動作環境に合わせて設定、または特定の Cisco ハードウェア プラットフォーム用にカスタマイズされた機能セットに入っています。

type 変数は、次のように、イメージの特徴を示すコードです。

- f : イメージはフラッシュ メモリから実行されます。
- m : イメージは RAM から実行されます。
- r : イメージは ROM から実行されます。
- l : イメージは再配置可能です。
- z : イメージは zip 圧縮されています。
- x : イメージは mzip 圧縮されています。

コピー操作における一般的な出力規則

コピー操作中、次のいずれかの文字が画面に表示されることがあります。

- ポンド記号（#）は通常、フラッシュ メモリ デバイスがクリア、初期化されることを意味します（フラッシュメモリをクリアしていることを示す方法は、プラットフォームによって異なります）。
- 感嘆符（!）は、10 個のパケットが転送されたことを意味します。
- 連続する「V」文字は、ファイルをフラッシュ メモリに書き込んだ後で、ファイルのチェックサム検証が行われていることを意味します。
- 「O」1 個は、順番がずれているパケットを表します。
- ピリオド（.）は、タイムアウトを意味します。

出力の最終行は、コピーが成功したかどうかを示します。

システム イメージの使用方法

システム イメージを管理するには、次の項で説明する作業のいずれかを実行します。

システム イメージ情報の表示

システム ソフトウェアに関する情報を表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show bootvar**	BOOT 環境変数の内容、CONFIG_FILE 環境変数によって指定されているコンフィギュレーション ファイルの名前、および BOOTLDR 環境変数の内容を示します。
Router# **show** *flash-filesystem:* [**partition** *number*] [**all** | **chips** | **detailed** | **err** | **summary**]	クラス B ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show** *flash-filesystem:* [**all** | **chips** | **filesys**]	クラス A ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show** *flash-filesystem:*	クラス C ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show microcode**	マイクロコード情報を表示します。
Router# **show version**	現在実行中のシステム イメージ ファイル名、システム ソフトウェアのリリース バージョン、コンフィギュレーション レジスタ設定などの情報をリストします。

これらのコマンドの例については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

フラッシュ メモリからネットワーク サーバにイメージをコピー

イメージ ファイルをバックアップ コピーとしてリモート サーバにコピーしたり、後日、フラッシュ メモリ内のコピーを保存されているコピーと比較して、チェックしたりする必要が生じることがあります。

フラッシュ メモリからリモート サーバにシステム イメージをコピーするには、FTP、Remote Copy Protocol（RCP; リモート コピー プロトコル）、または TFTP を使用します。Cisco IOS Software Release 12.4 では、HTTP または HTTPS を使用したサーバへのアップロード（または、サーバからのダウンロード）もサポートされています。これ以降の項では、次の作業について説明します。

- 「TFTP を使用してフラッシュ メモリからイメージをコピー」（P.4）
- 「フラッシュ メモリから rcp サーバにイメージをコピー」（P.5）
- 「フラッシュ メモリから FTP サーバにイメージをコピー」（P.7）

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これらの改善は、FTP および rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。

コピー処理を中止するには、**Ctrl**+^、または **Ctrl+Shift+6** を押します。

出力では、感嘆符（!）は、コピー処理が行われていることを示します。感嘆符（!）はそれぞれ、10 個のパケットが転送されたことを示します。

フラッシュ メモリの問題を解決する手順については、『*Internetwork Troubleshooting Guide*』を参照してください。

TFTP を使用してフラッシュ メモリからイメージをコピー

システム イメージを TFTP ネットワーク サーバにコピーできます。一部の TFTP の実装では、最初に TFTP サーバで「ダミー」ファイルを作成し、これに読み書きおよび実行権限を与えてから、この上にファイルをコピーする必要があります。詳細については、ご使用の TFTP のマニュアルを参照してください。

TFTP ネットワーク サーバにシステム イメージをコピーするには、EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show flash-filesystem:`	（任意）フラッシュ メモリ内のシステム イメージ ファイル名を表示します。このコマンドを使用して、この次のコマンドで使用するために、ファイルの URL パスとシステム イメージ ファイル名の正確なスペルを確認します。
ステップ 2	`Router# copy flash-url tftp:[[[//location]/directory]/filename]`	フラッシュ メモリから TFTP サーバにシステム イメージをコピーします。ファイルの場所とファイル名を *flash-url* 引数として指定します。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

フラッシュ メモリから TFTP サーバにイメージをコピーする例

次に、**show flash:** EXEC コマンドを使用して、システム イメージ ファイルの名前を調べ、**copy flash: tftp:** EXEC コマンドを使用して、システム イメージを TFTP サーバにコピーする例を示します。

```
RouterB# show flash:

System flash directory:
```

```
File  Length   Name/status
  1   4137888  c3640-c2is-mz.Feb24
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\

Router# copy flash: tftp:

IP address of remote host [255.255.255.255]? 172.16.13.110
filename to write on tftp host? c3640-c2is-mz.Feb24
writing c3640-c2is-mz.Feb24 !!!!...
successful tftp write.
```

パーティションされたフラッシュ メモリから TFTP サーバにイメージをコピーする例

この例では、your-ios という名前のファイルを、スロット 0 にあるフラッシュ メモリ PC カードのパーティション 1 から、172.23.1.129 にある TFTP サーバにコピーします。このファイルは、リモート ユーザ名を持つディレクトリに対する dirt/sysadmin ディレクトリに your-ios という名前で保存されます。

```
Router# copy slot0:1:your-ios tftp://172.23.1.129/dirt/sysadmin/your-ios

Verifying checksum for 'your-ios' (file # 1)...  OK
Copy 'your-ios' from Flash to server
  as 'dirt/sysadmin/ios-2'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

フラッシュ メモリから rcp サーバにイメージをコピー

システム イメージをフラッシュ メモリから rcp ネットワーク サーバにコピーできます。

ファイル サーバとして使用されている PC 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 Remote Shell（RSH; リモート シェル）プロトコルがサポートされている必要があります。

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、ルータからサーバにイメージをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドでリモート ユーザ名が指定されている場合は、そのユーザ名。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 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 経由でルータに接続しており、**username** グローバル コンフィギュレーション コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。
4. ルータのホスト名。

rcp コピー要求が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。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。コピーされるすべてのファイルおよびイメージのパスは、リモート ユーザのホーム ディレクトリで始まります。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 ディレクトリに常駐している場合は、このユーザの名前をリモート ユーザ名に指定します。

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
```

ルータの IP アドレスが Router1.domain.com に変換される場合、rcp サーバ上の User0 の .rhosts ファイルには、次の行が含まれます。

```
Router1.domain.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。

システム イメージをフラッシュ メモリから rcp サーバにコピーするには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **show** *flash-filesystem*:	（任意）フラッシュ メモリ内のシステム イメージ ファイル名を表示します。このコマンドを使用して、**copy** 特権 EXEC コマンドで使用するために、ファイルの *url-path* とシステム イメージ ファイル名の正確なスペルを確認します。
ステップ 2	Router# **configure terminal**	（任意）端末からグローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを変更する場合にだけ必要です（ステップ 3 を参照）。
ステップ 3	Router(config)# **ip rcmd remote-username** *username*	（任意）リモート ユーザ名を設定します。
ステップ 4	Router(config)# **end**	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを変更する場合にだけ必要です（ステップ 3 を参照）。
ステップ 5	Router# **copy** *flash-url* **rcp:**[[[**//**[*username***@**]*location*]**/***directory*]**/***filename*]	rcp を使用して、フラッシュ メモリからネットワーク サーバにシステム イメージをコピーします。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

フラッシュから RCP サーバへのコピーの例

次に、172.16.1.111 にあるネットワーク サーバに rcp とユーザ名 netadmin1 を使用して、c5200-ds-l という名前のシステム イメージをコピーする例を示します。

```
Router# copy flash:c5200-ds-l rcp:netadmin1@172.16.1.111/c5200-ds-l

Verifying checksum for 'c5200-ds-l' (file # 1)...[OK]
Writing c5200-ds-l -
```

Slot1 から RCP サーバへのコピーの例

次に、rcp を使用して、test という名前のシステム イメージ ファイルを 2 つ目の Personal Computer Memory Card International Association（PCMCIA; パーソナル コンピュータ メモリ カード国際協会）スロットからネットワーク サーバにコピーする例を示します。リモート ユーザ名は netadmin1 です。コピー先のアドレスとファイル名が指定されていないため、ルータからこれらの情報を求めるプロンプトが表示されます。

```
Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)# end
Router# copy slot1:test rcp:
Address or name of remote host [UNKNOWN]? 172.16.1.111
File name to write to? test
Verifying checksum for 'test' (file # 1)...[OK]
Writing test
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:08 [hh:mm:ss]
```

フラッシュ メモリから FTP サーバにイメージをコピー

システム イメージをフラッシュ メモリから FTP ネットワーク サーバにコピーできます。

FTP ユーザ名およびパスワードの概要

FTP プロトコルでは、クライアントは FTP 要求ごとにリモート ユーザ名およびパスワードをサーバに送信する必要があります。FTP を使用して、ルータからサーバにコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドでユーザ名が指定されている場合は、そのユーザ名。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 匿名。

ルータは次のうち、最初に発見した有効なパスワードを送信します。

1. **copy** 特権 EXEC コマンドでパスワードが指定されている場合は、そのパスワード。
2. **ip ftp password** グローバル コンフィギュレーション コマンドで設定されたパスワード（コマンドが設定されている場合）。

ルータは、*username@routername.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバ上のアカウントと関連付けら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 FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

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、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。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 ディレクトリに常駐している場合は、このユーザの名前をリモート ユーザ名に指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** コマンドを使用して、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

フラッシュ メモリから FTP サーバにコピーする作業

FTP ネットワーク サーバにシステム イメージをコピーするには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **configure terminal**	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 2	Router(config)# **ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 3	Router(config)# **ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 4	Router(config)# **end**	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 2 および 3 を参照）。
ステップ 5	Router# **show** *flash-filesystem*:	（任意）指定されたフラッシュ ディレクトリのシステム イメージ ファイルを表示します。フラッシュ メモリ内のシステム イメージ ファイル名を知らない場合は、このファイル名の正確なスペルをメモしておきます。
ステップ 6	Router# **copy** *flash-filesystem*:*filename* **ftp:**[[[**//**[*username* [:*password*]**@**]*location*]**/***directory*]**/***filename*]	このイメージを FTP サーバにコピーします。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

フラッシュ メモリから FTP サーバへのコピーの例

次に、**show flash:** 特権 EXEC コマンドを使用して、システム イメージ ファイルの名前を調べ、**copy flash: tftp:** 特権 EXEC コマンドを使用して、システム イメージ（c3640-c2is-mz）を TFTP サーバにコピーする例を示します。ルータはデフォルトのユーザ名とパスワードを使用します。

```
Router# show flash:

System flash directory:
File  Length   Name/status
  1   4137888  c3640-c2is-mz
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\

Router# copy flash: tftp:

IP address of remote host [255.255.255.255]? 172.16.13.110
filename to write on tftp host? c3600-c2is-mz
writing c3640-c2is-mz !!!!...
```

```
successful ftp write.
```

Slot1 から FTP サーバへのコピーの例

次に、**show slot1:** 特権 EXEC コマンドを使用して、2 つ目の PCMCIA スロットにあるシステム イメージ ファイルの名前を表示し、ファイル（test）を FTP サーバにコピーする例を示します。

```
Router# show slot1:

-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. 1        46A11866 2036C   4    746      May 16 1995 16:24:37 test

Router# copy slot1:test ftp://thisuser:thatpass@172.16.13.110/test

writing test!!!!...
successful ftp write.
```

パーティションされたフラッシュ メモリから FTP サーバへのコピーの例

この例では、your-ios という名前のファイルを、スロット 0 にあるフラッシュ メモリ PC カードのパーティション 1 から、172.23.1.129 にある TFTP サーバにコピーします。このファイルは、リモート ユーザ名を持つディレクトリに対する dirt/sysadmin ディレクトリに your-ios という名前で保存されます。

```
Router# show slot0: partition 1

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 your-ios
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy slot0:1:your-ios ftp://myuser:mypass@172.23.1.129/dirt/sysadmin/your-ios

Verifying checksum for 'your-ios' (file # 1)...  OK
Copy 'your-ios' from Flash to server
  as 'dirt/sysadmin/ios-2'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

イメージをネットワーク サーバからフラッシュ メモリへコピー

TFTP、rcp、または FTP サーバからフラッシュ メモリ ファイル システムへシステム イメージ、またはブート イメージをコピーし、ルータ上の Cisco IOS ソフトウェア、またはブート イメージをアップグレード、または変更できます。

使用するプロトコルは、使用しているサーバのタイプによって異なります。FTP および rcp のトランスポート メカニズムは、TFTP よりも高速でデータ配信の信頼性も優れています。これらの改善は、FTP および rcp のトランスポート メカニズムがコネクション型の TCP/IP スタック上に構築されており、これを使用しているために可能になりました。

これ以降の項では、次のコピーに関する作業について説明します。最初の 2 つの作業と最後の作業は必須です。フラッシュから実行するシステムを使用している場合は、3 つ目の項の作業が必須です。使用しているファイル転送プロトコルに応じて、残りの作業の 1 つを実行します。

（注） 別の Cisco IOS リリースにアップグレード、または変更する場合は、該当するリリース ノートを参照して、システム要件および制約事項を確認してください。

ファイルの名前付けに関する制約事項

フラッシュ メモリ内のファイル名は最大 63 文字です。大文字、小文字は区別されませんが、常に小文字に変換されます。

（注） 宛先ファイル名は英数字で表す（すべて英字、または英字と数字の組み合わせ）必要があります。たとえば、「1」は無効なファイル名です。

ファイル名は大文字でも、小文字でもかまいません。システムは大文字小文字の違いを無視します。大文字小文字に関係なく、フラッシュに同じ名前のファイルを複数個コピーした場合、最後にコピーしたファイルが有効なファイルになります。

フラッシュ メモリ領域に関する考慮事項の概要

フラッシュ メモリにファイルをコピーする前に、十分な領域が使用できることを確認してください。**show** *flash-filesystem***:** 特権 EXEC コマンドを使用して、コピーするファイルのサイズと、使用可能なフラッシュ メモリの領域のサイズを比較します。使用可能な領域が必要なサイズよりも小さい場合、**copy** 特権 EXEC コマンドは部分的に実行されますが、ファイル全体がフラッシュ メモリにコピーされることはありません。エラーメッセージ「buffer overflow - *xxxx/xxxx*」が表示されます。ここで、*xxxx/xxxx* には、ソース ファイルから読み込まれたバイト数とコピー先デバイスで使用可能なバイト数が入ります。

注意 フラッシュ メモリに有効なイメージがない場合、ルータをリブートしないでください。

（注） Cisco 3600 シリーズのルータで、ネットワーク サーバにアクセスできないときに、システム イメージをダウンロードしなければならない場合、Xmodem または Ymodem プロトコルを使用して、ローカルまたはリモート コンピュータ（PC、UNIX ワークステーション、または Macintosh）からイメージをコピーする必要があります。この章の「Xmodem または Ymodem を使用したシステム イメージの回復」を参照してください。

Cisco 2500、Cisco 3000、および Cisco 4000 システムでは、フラッシュ メモリにダウンロードされるファイルが圧縮されていないシステム イメージである場合、**copy** コマンドはダウンロード中のファイルのサイズを自動的に判断し、フラッシュ メモリで使用できる領域に適したサイズであるかどうかを確認します。

クラス B フラッシュ ファイル システムでは、書き込み前に、フラッシュ メモリ内の既存のコンテンツを消去するかどうかを確認するメッセージが表示されます。空いているフラッシュ メモリがない場合、またはこれまでフラッシュ メモリにファイルを書き込んだことがない場合、新しいファイルをコピーできるようにするには、消去ルーチンが必要です。フラッシュ メモリに十分な空きがある場合、書き込み前に、既存のフラッシュ メモリを消去するかどうかを確認するメッセージが表示されます。システムはこのメッセージでこのような条件を知らせ、ユーザからの応答を求めます。

（注） 「Erase flash before writing?」プロンプトに続けて **n** と入力すると、コピー処理が続行されます。**y** と入力し、消去を確認すると、消去ルーチンが開始されます。フラッシュ メモリに十分な領域があることを確認してから、消去プロンプトに **n** を入力してください。

フラッシュ メモリにすでに入っているファイルをコピーしようとすると、同じ名前のファイルがすでに存在することを知らせるプロンプトが表示されます。先にフラッシュ メモリに入っていたファイルは、新しいファイルをコピーすると削除されます。

- クラス A および B フラッシュ ファイル システムでは、最新バージョンが優先されるため、先に入っていたファイルはそのままフラッシュ メモリに残りますが使用できない状態になり、**show** *flash-filesystem***:** 特権 EXEC コマンドを実行すると、「deleted」タグつきでリストされます。コピー処理を打ち切ると、ファイル全体がコピーされず、有効にはならないため、新しいファイルが「deleted」とマークされます。この場合、フラッシュ メモリに先に入っていたファイルが有効で、システムはこのファイルを使用できます。
- クラス C フラッシュ ファイル システムでは、先に入っていたファイルが削除されます。

フラッシュ メモリには、通常のイメージ、または圧縮したイメージをコピーできます。圧縮したシステム イメージは、どのような UNIX プラットフォームでも、**compress** インターフェイス コンフィギュレーション コマンドを使用して作成できます。**compress** コマンドの正確な使用方法については、ご使用の UNIX プラットフォームのマニュアルを参照してください。

一部のプラットフォームでは、フラッシュ メモリに書き込みできるようにするには、フラッシュ セキュリティ ジャンパの設定が必要です。さらに、一部のプラットフォームには、書き込み保護スイッチがあり、フラッシュ メモリに書き込むためには、このスイッチを *unprotected* に設定する必要があります。

イメージのダウンロード プロセスに対する出力

出力とダイアログは、プラットフォームによって異なります。

パーティションされたフラッシュ メモリに対する出力

コマンドの入力後、ファイルのダウンロード方法を示すために、次のプロンプトの 1 つが表示されます。

- None：このファイルはコピーできません。
- RXBOOT-Manual：イメージをコピーするには、ROM 内の rxboot イメージを手動でリロードする必要があります。
- RXBOOT-FLH：コピーは、ブート ROM に入っているフラッシュ ロード ヘルパー ソフトウェア経由で自動的に行われます。

- Direct：コピーは直接行われます。

ファイルを複数のパーティションにダウンロードできる場合は、パーティション番号の入力が求められます。ヘルプを表示するには、パーティション番号の代わりに、次の文字のいずれかを入力します。

- **?**：すべてのパーティションのディレクトリ リストを表示します。
- **?1**：1 つ目のパーティションのディレクトリを表示します。
- **?2**：2 つ目のパーティションのディレクトリを表示します。
- **q**：**copy** コマンドを終了します。

フラッシュから実行されるシステムでのフラッシュ メモリへのコピー

フラッシュ メモリからシステムを実行し、同時にこのメモリにコピーすることはできません。したがって、フラッシュから実行されるシステムでは、フラッシュにコピーする前に、次の作業のいずれかを実行します。

- フラッシュ メモリからコピーしている間に、フラッシュ メモリからシステムを実行できるようにするには、フラッシュ メモリをパーティションするか、フラッシュ ロード ヘルパーを使用します。
- システムをリロードして、ブート ROM にあるシステム イメージを使用します。

フラッシュから実行されるシステムの詳細については、このマニュアルの「Maintaining System Memory」の章にある「Understanding Memory Types and Functions」の項を参照してください。

使用しているコンフィギュレーションで必要なジャンパ設定に関する詳細については、該当するハードウェアの設置および保守に関するマニュアルを参照してください。

TFTP サーバからフラッシュ メモリ ファイル システムへのイメージのコピー

システム イメージ、またはブート イメージをフラッシュ メモリにコピーする前に、現在のソフトウェア イメージ、またはブートストラップ イメージのバックアップ コピーを作成しておく必要があります。詳細は「フラッシュ メモリからネットワーク サーバにイメージをコピー」（P.3）を参照してください。

システム イメージを TFTP サーバからフラッシュ メモリ ファイル システムへコピーするには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **copy tftp:** [[[**//***location*]/*directory*]/*filename*] *flash-filesystem*:[*filename*]	システム イメージまたはブート イメージをフラッシュ メモリにコピーします。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

TFTP サーバからフラッシュ メモリへのコピー：例

次の例では、TFTP サーバから Slot1 にファイルをコピーしています。

```
Router# copy tftp://theserver/tftpboot/space2/sub2/c7200-js-mz slot1:
Destination filename [c7200-js-mz]?
```

```
Accessing tftp://theserver/tftpboot/space2/sub2/c7200-js-mz...Translating
"theserver"...domain server (192.168.2.132) [OK]

Loading tftpboot/space2/sub2/c7200-js-mz from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4823492 bytes]

4823492 bytes copied in 264.312 secs (18270 bytes/sec)
```

次に、フラッシュ メモリがいっぱいでファイルをコピーできない場合に、igs-p-l というシステム イメージを TFTP サーバから クラス B フラッシュ ファイル システムにコピーする例を示します。

```
Router# copy tftp: flash:

IP address or name of remote host [255.255.255.255]? dirt
Translating "DIRT"...domain server (255.255.255.255) [OK]

Name of file to copy? igs-p-l
Copy igs-p-l from 172.16.13.111 into flash memory? [confirm]
Flash is filled to capacity.
Erasure is needed before flash may be written.
Erase flash before writing? [confirm]
Erasing flash EPROMs bank 0

Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee

Erasing flash EPROMs bank 1

Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee

Erasing flash EPROMs bank 2

Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee

Erasing flash EPROMs bank 3

Zeroing bank...zzzzzzzzzzzzzzzz
Verify zeroed...vvvvvvvvvvvvvvvv
Erasing bank...eeeeeeeeeeeeeeee

Loading from 172.16.1.111:!!!!...
 [OK - 1906676 bytes]
Verifying via checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvv
```

```
Flash verification successful. Length = 1906676, checksum = 0x12AD
```

同じ名前のファイルがすでに存在するときに、TFTP サーバからフラッシュへコピー：例

次に、igs-p-l というシステム イメージを、igs-p-l というファイルがすでに存在する現在のフラッシュ コンフィギュレーションにコピーする方法の例を示します。

```
Router# copy tftp://172.16.13.111/igs-p-l flash:igs-p-l

File igs-p-l already exists; it will be invalidated!
Copy igs-p-l from 172.16.13.111 into flash memory? [confirm]
2287500 bytes available for writing without erasure.
Erase flash before writing? [confirm]n
Loading from 172.16.1.111:!!!!...
[OK - 1906676 bytes]
Verifying via checksum...
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv
vvvvvvvvvvvvvvvvvvvvvvvvvvvvv
Flash verification successful. Length = 1902192, checksum = 0x12AD
```

セキュリティ ジャンパが設定されていないときに、TFTP サーバからフラッシュへコピー：例

次の例では、フラッシュ セキュリティ ジャンパが設定されていないため、フラッシュ メモリへファイルを書き込めません。

```
Router# copy tftp: flash:

Flash: embedded flash security jumper(12V)
       must be strapped to modify flash memory
```

TFTP サーバからパーティションされたフラッシュへのコピー：例

次の例では、172.23.1.129 にある TFTP サーバ上の c3600-i-mz というファイルを、内蔵フラッシュ メモリの 1 つ目のパーティションにコピーします。

```
Router# copy tftp://172.23.1.129/c3600-i-mz flash:1:c3600-i-mz/c3600-i-mz

Accessing file 'c3600-i-mz' on 172.23.1.129...
Loading c3600-i-mz from 172.23.1.129 (via Ethernet1/0): ! [OK]
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'c3600-i-mz' from server
  as 'c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeee ...erased
Loading c3600-i-mz from 172.23.1.129 (via Ethernet1/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1711088 bytes]

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:17 [hh:mm:ss]
```

rcp サーバからフラッシュ メモリ ファイル システムにイメージをコピー

rcp ネットワーク サーバからフラッシュ メモリ ファイル システムへシステム イメージをコピーできます。

ファイル サーバとして使用されている PC 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。

rcp ユーザ名の概要

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、ルータからサーバにイメージをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドでリモート ユーザ名が指定されている場合は、そのユーザ名。
2. **ip rcmd remote-username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 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 経由でルータに接続しており、**username** グローバル コンフィギュレーション コマンドで認証された場合、ルータ ソフトウェアにより Telnet ユーザ名がリモート ユーザ名として送信されます。
4. ルータのホスト名。

rcp コピー要求が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。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。コピーされるすべてのファイルおよびイメージのパスは、リモート ユーザのホーム ディレクトリで始まります。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 ディレクトリに常駐している場合は、このユーザの名前をリモート ユーザ名に指定します。

rcp サーバからフラッシュ メモリへのコピー

rcp サーバからフラッシュ メモリにイメージをコピーするには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	「フラッシュ メモリからネットワーク サーバにイメージをコピー」の項の手順を参照してください。	現在のシステム、またはブートストラップ ソフトウェア イメージのバックアップ コピーを作成します。
ステップ 2	`Router# configure terminal`	（任意）端末からグローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名を上書きする場合にだけ必要です（ステップ 3 を参照）。
ステップ 3	`Router(config)# ip rcmd remote-username username`	（任意）リモート ユーザ名を指定します。
ステップ 4	`Router# end`	（任意）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。この手順は、デフォルトのリモート ユーザ名を上書きする場合にだけ必要です（ステップ 3 を参照）。
ステップ 5	`Router# copy rcp: [[[//[username@]location]/directory] /filename] flash-filesystem:[filename]`	rcp サーバからフラッシュ メモリ ファイル システムにイメージをコピーします。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

rcp サーバからフラッシュ メモリへのコピーの例

次に、mysysim1 というシステム イメージを IP アドレスが 172.16.101.101 のリモート サーバ SERVER1.CISCO.COM にある netadmin1 ディレクトリからフラッシュ メモリにコピーする例を示します。コピーするシステム イメージを保存するために十分な領域をフラッシュ メモリに確保するために、Cisco IOS ソフトウェアでは、まず、フラッシュ メモリの内容を消去できます。

```
Router1# configure terminal
Router1(config)# ip rcmd remote-username netadmin1
Router1(config)# end
Router# copy rcp: flash:

System flash directory:
File name/status
   1 mysysim1
[2076072 bytes used, 21080 bytes available]

Address or name of remote host[UNKNOWN]? 172.16.101.101
Name of file to copy? mysysim1
Copy mysysim1 from SERVER1.CISCO.COM?[confirm]

Checking for file 'mysysim1' on SERVER1.CISCO.COM...[OK]

Erase Flash device before writing?[confirm]
Are you sure?[confirm]
Erasing device...ezeeze...erased.

Connected to 172.16.101.101

Loading 2076007 byte file mysysim1:!!!!...
[OK]

Verifying checksum... (0x87FD)...[OK]
```

rcp サーバからパーティションされた Slot0 へのコピー：例

次の例では、IP アドレス 172.23.1.129 の rcp サーバにある c3600-i-mz というファイルを、スロット 0 のパーティション 3 にコピーします。ユーザ名が指定されていないため、ルータはデフォルトの rcp リモート ユーザ名を使用します。

```
Router# show slot0: partition 3

PCMCIA Slot0 flash directory, partition 3:
File  Length   Name/status
  1   426      running-config
[492 bytes used, 4193812 available, 4194304 total]

Router# copy rcp://172.23.1.129/tftpboot/gate/c3600-i-mz slot0:3:/tftpboot/gate/c3600-i-mz

Accessing file '/tftpboot/gate/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy '/tftpboot/gate/c3600-i-mz' from server
  as '/tftpboot/gate/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:16 [hh:mm:ss]
```

FTP サーバからフラッシュ メモリ ファイル システムにイメージをコピー

FTP サーバからフラッシュ メモリ ファイル システムへシステム イメージをコピーできます。

FTP ユーザ名およびパスワードの概要

FTP プロトコルでは、クライアントは FTP 要求ごとにリモート ユーザ名およびパスワードをサーバに送信する必要があります。FTP を使用して、ルータからサーバにコンフィギュレーション ファイルをコピーする場合、Cisco IOS ソフトウェアは、次のうち、最初に発見した有効なユーザ名を送信します。

1. **copy** 特権 EXEC コマンドでユーザ名が指定されている場合は、そのユーザ名。
2. **ip ftp username** グローバル コンフィギュレーション コマンドで設定されたユーザ名（コマンドが設定されている場合）。
3. 匿名。

ルータは次のうち、最初に発見した有効なパスワードを送信します。

1. **copy** 特権 EXEC コマンドでパスワードが指定されている場合は、そのパスワード。
2. **ip ftp password** コマンドで設定されたパスワード（コマンドが設定されている場合）。

ルータは、*username@routername.domain* というパスワードを生成します。変数 *username* は現在のセッションに関連付けられたユーザ名、*routername* は設定済みのホスト名、*domain* はルータのドメインです。

ユーザ名およびパスワードは、FTP サーバ上のアカウントと関連付けら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 FTP 書き込み要求を受け入れるように、FTP サーバを適切に設定する必要があります。

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、サーバ上のユーザ名と関連付けられたディレクトリに書き込まれるか、そのディレクトリからコピーされます。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 ディレクトリに常駐している場合は、このユーザの名前をリモート ユーザ名に指定します。

詳細については、ご使用の FTP サーバのマニュアルを参照してください。

ip ftp username および **ip ftp password** コマンドを使用して、すべてのコピーに対してユーザ名とパスワードを指定します。当該のコピー操作だけに対してユーザ名を指定する場合は、**copy** コマンドにユーザ名を含めます。

FTP サーバからフラッシュ メモリへのコピー

システム イメージを FTP サーバからフラッシュ メモリ ファイル システムへコピーするには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	「フラッシュ メモリからネットワーク サーバにイメージをコピー」の項の手順を参照してください。	現在のソフトウェア イメージ、またはブートストラップ イメージのバックアップ コピーを作成します。
ステップ 2	`Router# configure terminal`	（任意）端末からグローバル コンフィギュレーション モードを開始します。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 3	`Router(config)# ip ftp username username`	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 4	`Router(config)# ip ftp password password`	（任意）デフォルトのパスワードを変更します。
ステップ 5	`Router(config)# end`	（任意）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。この手順は、デフォルトのリモート ユーザ名またはパスワードを上書きする場合にだけ必要です（ステップ 3 および 4 を参照）。
ステップ 6	`Router# copy ftp: [[[//[username[:password]@]location] /directory]/filename] flash-filesystem:[filename]`	コンフィギュレーション ファイルをネットワーク サーバから稼動中のメモリ、または rcp を使用してスタートアップ コンフィギュレーションにコピーします。

copy 特権 EXEC コマンドの発行後、追加情報の入力や、アクションの確認を求めるプロンプトが表示されることがあります。このプロンプトは、**copy** コマンドで入力した情報量および **file prompt** グローバル コンフィギュレーション コマンドの現在の設定によって異なります。

FTP サーバからフラッシュ メモリへのコピーの例

次に、ユーザ名 myuser、パスワード mypass を使用して、FTP サーバから c7200-js-mz というファイルをコピーする例を示します。

```
Router# copy ftp://myuser:mypass@theserver/tftpboot/sub3/c7200-js-mz slot1:c7200-js-mz

Accessing ftp://theserver/tftpboot/sub3/c7200-js-mz...Translating "theserver"...domain
server (192.168.2.132) [OK]

Loading c7200-js-mz from 192.168.2.132 (via Ethernet3/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4823492 bytes]

4823492 bytes copied in 264.312 secs (18270 bytes/sec)
```

フラッシュ メモリ内のイメージの確認

フラッシュ メモリから起動する前に、**verify** 特権 EXEC コマンドを使用して、フラッシュ メモリ内のイメージのチェックサムが、システム ソフトウェア イメージとともに配布された README ファイルに記載されているチェックサムと一致することを確認します。フラッシュ メモリ内のイメージの

チェックサムは、**copy** 特権 EXEC コマンドを発行してイメージをコピーしたときに、画面の下部に表示されます。この README ファイルは、サーバにシステム ソフトウェア イメージをインストールしたときに、自動的にネットワーク サーバにコピーされています。

注意 チェックサムの値が README ファイルの値と一致しない場合、ルータをリブートしてはいけません。代わりに、**copy** コマンドを発行して、もう一度、チェックサムを比較してください。何度やっても正しいチェックサムが得られない場合は、フラッシュ メモリからルータをリブートする*前に*、フラッシュ メモリ オリジナルのシステム ソフトウェア イメージをフラッシュ メモリにコピーしてください。フラッシュ メモリに壊れたイメージが入っている場合に、フラッシュから起動を試みると、ルータは ROM に保存されているシステム イメージを起動します（ネットワーク サーバからの起動が設定されていないことが前提です）。ROM に完全に機能するシステム イメージが入っていない場合、ルータは機能しないため、直接コンソール ポートに接続して再設定する必要があります。

フラッシュ メモリのコンテンツ リストには、個々のファイルのチェックサムは含まれていません。イメージをフラッシュ メモリまたはフラッシュ メモリ デバイスにコピーした後でイメージ チェックサムを再計算し、確認するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **verify** *flash-filesystem*:[*partition-number*:] [*filename*]	イメージをフラッシュ メモリにコピーした後で、イメージ チェックサムを再計算し、確認します。

コマンドでファイル名を指定しなかった場合、ルータからプロンプトが表示されます。デフォルトでは、フラッシュ内の最後の（最新の）ファイルの入力が求められます。デフォルト ファイルのチェックサムを再計算するには、Return キーを押すか、プロンプトに別のファイルの名前を入力します。ただし、マイクロコード イメージのチェックサムは、常に 0x0000 です。

次に、slot0 内の c7200-js-mz というイメージを確認する例を示します。

```
Router# verify slot0:c7200-js-mz

Verified slot0:c7200-js-mz
```

HTTP または HTTPS を使用したイメージのコピー

Cisco IOS Release 12.4 は、HTTP または Secure HTTP（HTTPS）プロトコルを使用して、Cisco IOS ソフトウェア ベースのデバイスと、リモートの HTTP サーバの間のファイル転送をサポートします。

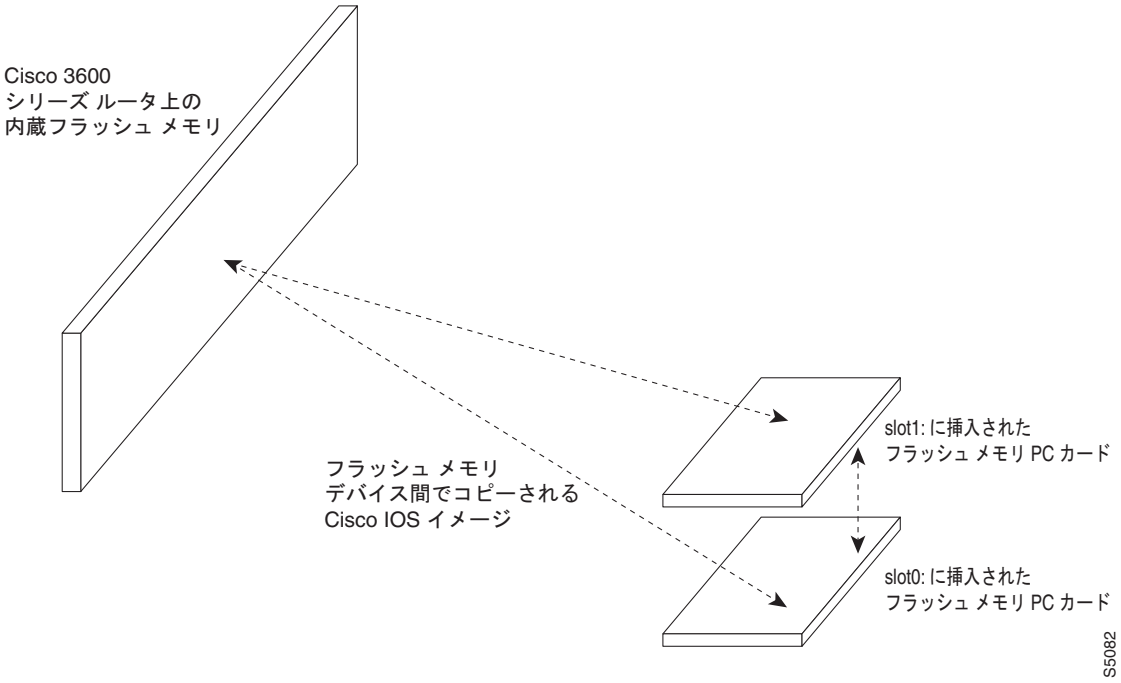
リモート HTTP サーバの間でファイルをコピーするには、システム イメージが、大半の Cisco IOS ソフトウェア イメージに統合されている HTTP クライアント機能をサポートしている必要があります。HTTP クライアントはデフォルトでイネーブルになっています。使用しているシステムで HTTP クライアントがサポートされているかどうかを判断するには、**show ip http client all** 特権 EXEC モード コマンドを発行します。このコマンドを実行できれば、HTTP クライアントがサポートされています。

この機能の詳細については、「Transferring Files Using HTTP or HTTPS」モジュールを参照してください。

ローカル フラッシュ メモリ デバイス間でのイメージのコピー

複数のフラッシュ メモリ デバイスを持つルータでは、図 9 に示すように、内部フラッシュ メモリや PCMCIA スロットのフラッシュ メモリ カードなどのフラッシュ メモリ ファイル システムから、別のフラッシュ メモリ デバイスにイメージをコピーできます。イメージを別のフラッシュ デバイスにコピーする理由の 1 つにバックアップ コピーの作成があります。

図 9　　フラッシュ メモリ ファイル システム間でのイメージのコピー



注意　新しいフラッシュ デバイスにコピーする前に、まず、デバイスをフォーマットする必要があります。新しいメディアはすべて、フォーマットが必要です。シスコ デバイスで使用されるメモリ メディアは、通常、あらかじめフォーマットされていません。あらかじめフォーマットされていたとしても、Cisco ファイル システムを使用して最初にフォーマットすることにより、互換性のないフォーマットの持つ潜在的な問題を回避しやすくなります。
フォーマットされていないフラッシュ デバイスや、フォーマットが不適切なフラッシュ デバイスにイメージをコピーしようとしても、一部のデバイスではエラー メッセージが生成されない可能性があります。このため、次の表に示す **show** および **verify** 手順を強く推奨します。
フラッシュ デバイスのフォーマット手順については、「Maintaining System Memory」の章を参照してください。

フラッシュ メモリ デバイス間でイメージをコピーするには、特権 EXEC モードで、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show flash-filesystem:`	フラッシュ メモリのレイアウトとコンテンツを表示します。
ステップ 2	`Router# copy source-url destination-url`	ローカル フラッシュ メモリ デバイス間でイメージをコピーします。
ステップ 3	`Router# verify flash-filesystem:filename`	コピーしたイメージのチェックサムを確認します（使用しているイメージの MD5 チェックサムは Cisco.com から取得できます）。

（注） コピー元デバイスとコピー先デバイスは同じにはできません。たとえば、**copy slot1: slot1:** コマンドは無効です。

ローカル フラッシュ メモリ デバイス間でファイルをコピーする例

次に、new-ios というファイルを内部フラッシュ メモリのパーティション 1 からスロット 0 にコピーする例を示します。

```
Router# show flash: partition 1

System flash directory, partition 1:
File  Length   Name/status
  1   3142748 admin/images/new-ios
[3142812 bytes used, 1051492 available, 4194304 total]

Router# show slot0:

PCMCIA Slot0 flash directory
File  Length   Name/status
  1   1711088  /tftpboot/gate/c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy flash:1:admin/images/new-ios slot0:admin/images/new-ios

Verifying checksum for 'admin/images/new-ios' (file # 1)...  OK

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]
Copy 'admin/images/new-ios' from flash: device
  as 'admin/images/new-ios' into slot0: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 [OK - 3142748 bytes]

Flash device copy took 00:00:50 [hh:mm:ss]
Verifying checksum...  OK (0xB732)
```

```
Router# show slot0:

PCMCIA Slot0 flash directory
File  Length   Name/status
  1   3142748 admin/images/new-ios
[3142812 bytes used, 1051492 available, 4194304 total]

Router# verify slot0:
Verify filename []? new-ios
! long pause ...
Verifying file integrity of slot0:new-ios.....................!
Embedded Hash   MD5 : E1A04D4DE1ED00407E6E560B315DA505
Computed Hash   MD5 : E1A04D4DE1ED00407E6E560B315DA505
CCO Hash        MD5 : C03EC4564F86F9A24201C88A9DA67317

Signature Verified
Verified slot0:

Router#
```

コンフィギュレーション ファイルでのスタートアップ システム イメージの指定

スタートアップ コンフィギュレーション ファイル、または BOOT 環境変数に複数のブート コマンドを入力して、ルータにシステム イメージをロードするためのバックアップ方法を提供できます。システム イメージをロードする方法には、次の 3 種類があります。

- フラッシュ メモリから：フラッシュ メモリにより、ROM を変更することなく、新しいシステム イメージをコピーできます。フラッシュ メモリに格納されている情報は、サーバからシステム イメージをロードしているときに発生する可能性のあるネットワーク エラーに対して脆弱ではありません。
- ネットワーク サーバから：フラッシュ メモリが破損したときに、Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）、TFTP、rcp、または FTP を予備の起動方法として使用して、ネットワーク サーバからシステム イメージをロードするように指定できます。一部のプラットフォームでは、TFTP、rcp、または FTP を使用して、ネットワーク サーバからブート イメージをロードするように指定できます。
- ROM から：フラッシュ メモリの破損とネットワーク障害が同時に発生した場合に起動するための最後の手段として、ROM からシステム イメージをロードするように指定します。ROM に格納されたシステム イメージは、フラッシュ メモリや、ネットワーク サーバに格納されたものとは異なり、必ずしも最新の状態ではない可能性があります。

（注） 一部のプラットフォームは ROM から起動できません。

スタートアップ コンフィギュレーション ファイル、または BOOT 環境変数には、さまざまなタイプのブート コマンドを任意の順序で入力できます。複数のブート コマンドが入力されている場合、Cisco IOS ソフトウェアは、これらのコマンドを入力されている順序で試行します。

（注） ROM からの起動は、フラッシュ メモリからの起動よりも高速です。しかし、フラッシュ メモリからの起動は、ネットワーク サーバからの起動よりも、さらに早く、高い信頼性を持っています。

フラッシュ メモリからのシステム イメージのロード

ルータがフラッシュ メモリから起動されるように設定するには、次の項で説明する作業を実行します。フラッシュ メモリにより、ネット経由でしかアクセスできないファイルへの依存度が小さくなるため、ネットワーク障害の影響を受けにくくなります。

フラッシュ メモリの設定

フラッシュ メモリ内のシステム イメージをロードするように、ルータを設定するには、次の手順を実行します。

	タスク
ステップ 1	（任意）TFTP、rcp、または FTP を使用して、システム イメージ、またはブート イメージをフラッシュ メモリにコピーします。この手順の実行の詳細については、「イメージをネットワーク サーバからフラッシュ メモリへコピー」の項を参照してください。
ステップ 2	フラッシュ メモリ、またはブート フラッシュ メモリ内の希望するファイルおよび場所から、自動的に起動するようにシステムを設定します。「フラッシュ メモリ内のイメージからルータの自動起動を設定」を参照してください。
ステップ 3	（任意）現在のコンフィギュレーション レジスタ設定に応じて、コンフィギュレーション レジスタの値を変更します。コンフィギュレーション レジスタの変更の詳細については、「フラッシュ メモリ内のイメージからルータの自動起動を設定」の項を参照してください。
ステップ 4	（任意）一部のプラットフォームについて、BOOTLDR 環境変数を設定して、ブート イメージの場所を変更します。
ステップ 5	設定を保存します。
ステップ 6	電源をオフにしてから再びオンにし、システムをリブートして、すべてが期待しているとおりに動作していることを確認します。

フラッシュ メモリ内のイメージからルータの自動起動を設定

フラッシュ メモリ内のイメージから自動的に起動するようにルータを設定するには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	端末からグローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# boot system flash` [*flash-filesystem:*] [*partition-number:*] *filename*	フラッシュ メモリに格納されている、起動に使用すべきイメージ ファイルの名前を指定します。
ステップ 3	`Router(config)# config-register` *value*	コンフィギュレーション ファイルで指定されたシステム イメージをロードできるように、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 4	`Router(config)# end`	コンフィギュレーション セッションを終了し、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 5	`Router# copy system:running-config nvram:startup-config`	システム実行コンフィギュレーションを、デバイス スタートアップ コンフィギュレーション（startup-config ファイル）として保存します。

	コマンド	目的
ステップ 6	`Router# more nvram:startup-config`	（任意）スタートアップ コンフィギュレーションのコンテンツを検証できるようにします。
ステップ 7	`Router# reload`	システムをリブートします。

パーティションされているルータについては、パーティションを指定しなかった場合、ルータは 1 つ目のパーティションから起動します。ファイル名を指定しなかった場合、ルータはパーティション内で発見された最初の有効なイメージから起動します。

複数のイメージ ファイル名を入力した場合、ルータはこれらのファイル名を、入力された順に試行します。

コンフィギュレーション ファイルからファイル名を削除するには、**no boot system flash** グローバル コンフィギュレーション コマンドを入力し、ファイルの場所を指定します。

（注） **no boot system** コンフィギュレーション コマンドは、引数に関係なく、すべての **boot system** コンフィギュレーション コマンドをディセーブルにします。**no boot system** コマンドに対して **flash** キーワード、または *filename* 引数を指定すると、これらの引数で指定されたコマンドだけがディセーブルになります。

フラッシュ メモリからのルータの起動を設定する例

次に、フラッシュ メモリ内のイメージから自動的に起動するようにルータを設定する例を示します。

```
Router# configure terminal
Router(config)# boot system flash new-image
Router(config)# config-register 0x010F
Router(config)# end
Router# copy system:running-config nvram:startup-config
[ok]
Router# reload
[confirm]

%SYS-5-RELOAD: Reload requested
System Bootstrap, Version 12.0(7)W5(15) RELEASE SOFTWARE
     Copyright (c) 1986-2001 by Cisco Systems, Inc.
RP1 processor with 16384 Kbytes of memory
F3: 1871404+45476+167028 at 0x1000

Booting new-image from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK - 1916912 bytes]
F3: 1871404+45476+167028 at 0x1000

              Restricted Rights Legend
.
.
.
```

ネットワーク サーバからのシステム イメージのロード

FTP、TFTP、rcp、または MOP を使用して、ネットワーク サーバからシステム イメージをロードするように、Cisco IOS ソフトウェアを設定できます。

MOP を使用してネットワーク サーバから起動することがなく、FTP、TFTP、または rcp を指定していない場合、デフォルトでは、指定したシステム イメージは、TFTP 経由でネットワーク サーバから起動されます。

（注） ネットワーク サーバとして Sun ワークステーション、ファイルの転送に TFTP を使用している場合は、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）チェックサムの確認と生成ができるように、ワークステーションを設定します。詳細は、Sun のマニュアルを参照してください。

パフォーマンスと信頼性を向上させるには、rcp を使用して、ネットワーク サーバからシステム イメージを起動します。rcp 実装では TCP が使用されます。これにより、データが確実に配信されるようになります。

boot ROM モニタ コマンドを発行する場合、リモート ユーザ名を具体的に指定することはできません。代わりに、ルータのホスト名を使用します。リモート サーバが UNIX システムと同様にディレクトリ構造を持っている場合、rcp を使用して、ネットワーク サーバからルータを起動すると、Cisco IOS ソフトウェアは、このリモート ユーザ名を持つディレクトリに対するサーバ上のシステム イメージを検索します。

また、ネットワーク サーバ上の圧縮されたイメージから起動することもできます。圧縮されたイメージを使用する理由の 1 つは、格納用メモリを十分に確保することにあります。EPROM に ROM から実行されるイメージが含まれていないルータでは、ルータがネットワーク サーバからソフトウェアを起動した場合、起動されるイメージと実行中のイメージの両方がメモリに収まらなければなりません。実行中のイメージが大きい場合、メモリには、ネットワーク サーバから起動されるイメージを使用できる余地がない可能性があります。

ネットワーク サーバから通常のイメージを起動するのに十分な余地がメモリにはない場合、どのような UNIX プラットフォームでも、**compress** インターフェイス コンフィギュレーション コマンドを使用して、圧縮されたソフトウェア イメージを作成できます。**compress** コマンドの使用方法については、ご使用の UNIX プラットフォームのマニュアルを参照してください。

FTP ネットワーク サーバからのシステム イメージのロードを指定するには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	`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。

ステップ 2	`Router(config)# boot system [rcp | tftp] filename [ip-address]`
	または
	`Router(config)# boot system mop filename [mac-address] [interface]`
		rcp、TFTP、または MOP を使用して、ネットワーク サーバから起動されるシステム イメージ ファイルを指定します。

ステップ 3	`Router(config)# config-register value`	コンフィギュレーション ファイルで指定されたイメージをロードできるように、コンフィギュレーション レジスタを設定します。

	コマンド	目的
ステップ 4	`Router(config)# exit`	コンフィギュレーション モードを終了します。

ステップ 5	`Router# copy system:running-config nvram:startup-config`
	または
	`Router# copy run start`
		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。

次の例では、ルータは rcp を使用して、IP アドレス 172.16.0.1 のネットワーク サーバにある testme5.tester システム イメージ ファイルを起動しています。

```
Router# configure terminal
Router(config)# boot system rcp testme5.tester 172.16.0.1
Router(config)# config-register 0x010F
Router(config)# exit
Router# copy system:running-config nvram:startup-config
```

次の項では、**boot system mop** コマンドを使用して起動されるようにシステムを設定した場合に、要求の再試行回数と頻度を変更する方法を説明します。

MOP 要求パラメータの変更

MOP を使用して、ネットワーク サーバから起動（**boot system mop** グローバル コンフィギュレーション モード コマンドを使用）するようにルータを設定している場合、このルータは、始動中、コンフィギュレーション ファイル要求を MOP ブート サーバに送信します。デフォルトでは、MOP ブート サーバからの応答を必要とする要求を送信したときに、このサーバが応答しなかった場合、このメッセージは 4 秒後に再送信されます。この再送信は最高 8 回行われます。MOP デバイス コードは、デフォルトでシスコ デバイス コードに設定されています。

MOP ブート サーバとルータが低速のシリアル リンクで分断されている場合、ルータがメッセージへの応答を受け取るまでには 4 秒以上かかる可能性があります。したがって、このようなリンクを使用している場合は、4 秒以上待ってからメッセージを再送信するように、ソフトウェアを設定することができます。また、MOP 要求や MOP デバイス コードについては、最大再試行回数を変更することもできます。

MOP サーバへの起動要求の送信に使用される Cisco IOS ソフトウェア要求パラメータを変更するには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# configure terminal`	端末からグローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# mop device-code {cisco | ds200} mop retransmit-timer seconds mop retries count`	MOP サーバ パラメータを変更します。
ステップ 3	`Router(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 4	`Router# 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。

次の例では、ルータがメッセージを送信してから 10 秒以内に MOP ブート サーバが応答しなかった場合、メッセージが再送信されます。

```
Router# configure terminal
Router (config)# mop retransmit-timer 10
Router (config)# end
Router# copy running-config startup-config
```

ROM からのシステム イメージのロード

ROM システム イメージをバックアップとしてコンフィギュレーション ファイルのその他のブート指示にロードするには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的
ステップ 1	`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。
ステップ 2	`Router(config)# boot system rom`	バックアップ イメージとして、ROM システム イメージを使用することを指定します。
ステップ 3	`Router(config)# config-register value`	コンフィギュレーション ファイルで指定されたシステム イメージをロードできるように、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 4	`Router(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 5	`Router# copy system:running-config nvram: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。

次の例では、ルータは ROM から起動されるように設定されています。

```
Router# configure terminal
Router(config)# boot system rom
Router(config)# config-register 0x010F
Router(config)# end
Router# copy system:running-config nvram:startup-config
```

（注） Cisco 7000 シリーズのルータを ROM からロードすることはできません。

耐障害性のある起動ストラテジの使用

ネットワーク障害により、ネットワーク サーバからの起動が不可能になることがあります。ネットワーク障害の影響を抑えるために、次の起動ストラテジを検討してください。フラッシュを取り付け、設定した後で、次の順序でルータが起動されるように設定します。

1. イメージをフラッシュから起動
2. イメージをネットワーク サーバから起動
3. ROM イメージから起動

この順序で起動すると、最も耐障害性が強くなります。特権 EXEC モードで始まる次のコマンドを使用して、ルータをまずフラッシュから起動し、次にネットワーク サーバのシステム ファイルから、最後に ROM から起動します。

	コマンド	目的
ステップ 1	`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。
ステップ 2	`Router(config)# boot system flash [flash-filesystem:][partition-number:] filename`	フラッシュ メモリから起動するようにルータを設定します。

	コマンド	目的
ステップ 3	`Router(config)# boot system [rcp | tftp] filename [ip-address]`	ネットワーク サーバから起動するようにルータを設定します。
ステップ 4	`Router(config)# boot system rom`	ROM から起動されるようにルータを設定します。
ステップ 5	`Router(config)# config-register value`	コンフィギュレーション ファイルで指定されたシステム イメージをロードできるように、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 6	`Router(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 7	`Router# copy system:running-config nvram: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。

次の例では、ルータはまず、内部フラッシュ イメージ *gsxx* を起動するように設定されています。このイメージが失敗したら、ルータはネットワーク サーバからコンフィギュレーション ファイル *gsxx* を起動します。この方法も失敗した場合は、ROM から起動します。

```
Router# configure terminal
Router(config)# boot system flash gsxx
Router(config)# boot system gsxx 172.16.101.101
Router(config)# boot system rom
Router(config)# config-register 0x010F
Router(config)# end
Router# copy system:running-config nvram:startup-config
[ok]
```

このストラテジでは、ルータ 1 つあたり、起動源を 3 種類、使用できることになります。これらの起動源は、ネットワークやファイル サーバの不具合による悪影響の軽減に役立ちます。

Xmodem または Ymodem を使用したシステム イメージの回復

ネットワーク サーバにアクセスできないときに、システム イメージをダウンロードする必要がある場合（アップデートが必要な場合、またはフラッシュ メモリ内のシステム イメージがすべて何らかの理由で破損または消去された場合）、Xmodem または Ymodem プロトコルを使用して、PC、UNIX ワークステーション、Macintosh などのローカル コンピュータまたはリモート コンピュータからイメージをコピーすることができます。この機能は主に障害回復のために使用されます。これを図に表すと、図 10 のようになります。

（注） Xmodem または Ymodem を使用したシステム イメージの回復は、Cisco 1600 シリーズ、および Cisco 3600 シリーズ ルータだけで可能です。

Xmodem と Ymodem はファイル転送に使用される一般的なプロトコルで、Windows 3.1（TERMINAL.EXE）、Windows 95（HyperTerminal）、Windows NT 3.5x（TERMINAL.EXE）、Windows NT 4.0（HyperTerminal）、Linux UNIX フリーウェア（minicom）などのアプリケーションに含まれています。

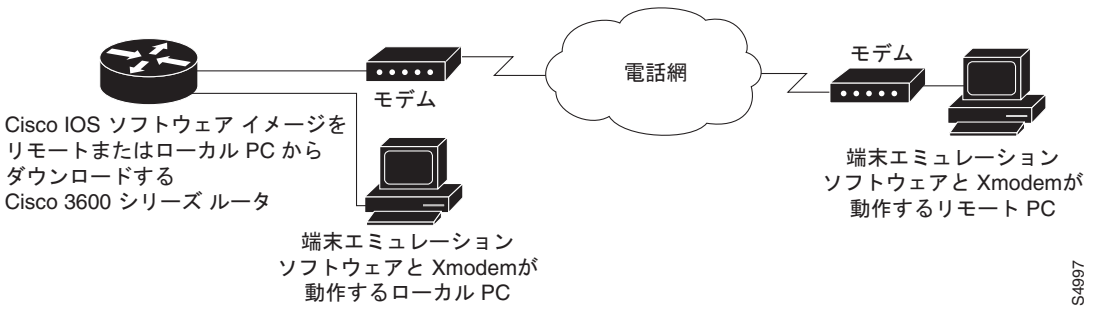
Cisco 3600 シリーズ ルータでは、Cisco IOS ソフトウェアの障害回復技術である XBOOT 機能はサポートされていません。また、ブート ヘルパー（rxboot）イメージも持っていません。

Xmodem や Ymodem によるダウンロードは低速ですから、これらはネットワーク サーバにアクセスできない場合だけ使用してください。転送速度を上げるには、転送ポートの速度を 115200 bps に設定します。

Cisco 3600 シリーズのルータでは、Cisco IOS ソフトウェアを使用して、ファイル転送を行うことができます。また、ローカル システム イメージがすべて破損している、または消去されている場合は、ROM モニタを使用できます。Xmodem または Ymodem ファイル転送に Cisco IOS ソフトウェアを使用する場合、転送は AUX ポート、またはコンソール ポートで行われます。ハードウェア フロー制御をサポートしている AUX ポートの使用を推奨します。ROM モニタからのファイル転送では、コンソール ポートを使用する必要があります。

Cisco 1600 シリーズのルータでは、ROM モニタだけから、コンソール ポート経由でファイル転送を実行できます。

図 10　Xmodem または Ymodem を使用して Cisco 3600 シリーズ ルータにシステム イメージをコピー



Xmodem または Ymodem プロトコルを使用して、コンピュータまたはワークステーションからルータに Cisco IOS イメージをコピーするには、必要に応じて、次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **copy xmodem:** *flash-filesystem*:[*partition*:][*filename*] または Router# **copy ymodem:** *flash-filesystem*:[*partition*:][*filename*]	EXEC モードで、Cisco IOS ソフトウェアを使用して、コンピュータからフラッシュ メモリへシステム イメージをコピーします（Cisco 3600 シリーズのルータだけの機能）。
ステップ 2	ROMMON > **xmodem** [**-c**] [**-y**] [**-e**] [**-f**] [**-r**] [**-x**] [**-s** *data-rate*] [*filename*]	Cisco 1600 シリーズのルータでは、ROM モニタ モードでコンピュータからフラッシュ メモリにシステム イメージをコピーします。 **-c** オプションは CRC-16 チェックサムを提供します。**-y** は Ymodem プロトコルを使用します。**-e** はフラッシュ メモリ内の先頭パーティションを消去します。**-f** はフラッシュ メモリ全体を消去します。**-r** はイメージを DRAM にダウンロードします（デフォルトはフラッシュ メモリです）。**-x** は、ダウンロード後にイメージが実行されないようにします。**-s** はコンソール ポートのデータ レートを設定します。
ステップ 3	ROMMON > **xmodem** [**-c** | **-y** | **-r** | **-x**] [*filename*]	Cisco 3600 シリーズのルータでは、ROM モニタ モードでコンピュータからフラッシュ メモリにシステム イメージをコピーします。

Cisco IOS イメージの転送元コンピュータでは、端末エミュレーション ソフトウェアと Xmodem または Ymodem プロトコルが稼動されている必要があります。

Cisco 1600 シリーズのルータでは、**-r** オプション（DRAM へのダウンロード）を指定した場合、転送中のファイルを保存できるだけの容量がルータの DRAM に必要です。フラッシュ メモリから実行する場合、イメージはフラッシュ メモリの先頭ファイルの位置になければなりません。フラッシュ メモリから、起動する新しいイメージをコピーする場合、まず、既存のファイルをすべて削除してください。

Cisco IOS ソフトウェアを使用した Xmodem 転送

次に、Cisco IOS ソフトウェア、および Xmodem プロトコルを使用したファイル転送作業を示します。Ymodem プロトコルの場合も、**copy ymodem:** 特権 EXEC コマンドを使用して、同様の手順で行います。

（注） この機能が使用できるのは、Cisco 3600 シリーズのルータだけです。

端末エミュレーション ソフトウェアと Xmodem プロトコルが稼動しているコンピュータから Cisco IOS イメージを転送するには、次の手順を実行します。

ステップ 1 Cisco IOS ソフトウェア イメージをリモート コンピュータのハード ドライブに保存します。イメージは Cisco.com からダウンロードできます。

ステップ 2 リモート コンピュータから転送するには、モデムを Cisco 3600 シリーズ ルータの AUX ポートと標準電話ネットワークに接続します。AUX ポートはデフォルトで速度 9600 bps、2 ストップ ビット、パリティなしに設定されています。最高速度は 115200 bps です。**modem inout** ライン コンフィギュレーション コマンドを入力して、受信コールと発信コールの両方についてルータを設定します。

リモート コンピュータと電話ネットワークにモデムを接続します。リモート コンピュータは電話ネットワークにダイヤルして、ルータに接続します。

ローカル コンピュータから転送するには、null モデム ケーブルを使用して、ルータの AUX ポートをコンピュータのシリアル ポートに接続します。ルータで設定されている AUX の速度は、ローカル コンピュータで設定されている転送速度と一致していなければなりません。

ステップ 3 コンピュータの端末エミュレータ ウィンドウの特権 EXEC プロンプトに対して、**copy xmodem: flash:** 特権 EXEC コマンドを入力します。

```
Router# copy xmodem: flash:
                          **** WARNING ****
x/ymodem is a slow transfer protocol limited to the current speed
settings of the auxiliary/console ports. The use of the auxiliary
port for this download is strongly recommended.
During the course of the download no exec input/output will be
available.
                          ---- ******* ----
```

ステップ 4 **Enter** キーを押して、続行します。

ステップ 5 Cyclic Redundancy Check（CRC; 巡回冗長検査）ブロック チェックサムを使用するかどうかを指定します。CRC はデータがコンピュータからルータに正確に転送されたことを検証するテストです。使用しているコンピュータで CRC ブロック チェックサムがサポートされていない場合は、プロンプトに **no** と入力します。

```
Proceed? [confirm]
Use crc block checksumming? [confirm] no
```

ステップ 6 ソフトウェアが不良データ ブロックの受信を試行する回数の上限を決定します。この回数を超えると、コピー操作は失敗であると宣言されます。デフォルトの試行回数は 10 回です。ノイズの多い電話回線では、この回数を大きめに設定する必要が生じる場合があります。再試行回数を無制限に設定することができます。

```
Max Retry Count [10]: 7
```

ステップ 7 このファイルが、有効な Cisco 3600 シリーズ イメージであることを確認するかどうかを決定します。

```
Perform image validation checks? [confirm]
Xmodem download using simple checksumming with image validation
Continue? [confirm]
```

転送の開始後、イメージが有効であれば、ソフトウェアにより転送に必要なフラッシュ メモリの空き容量がルータ上に存在するかどうかが判断されます。

```
System flash directory:
File  Length   Name/status
  1   1738244  images/c3600-i-mz
[1738308 bytes used, 2455996 available, 4194304 total]
```

ステップ 8 転送先のファイル名を入力します。

```
Destination file name ? new-ios-image
```

ステップ 9 ファイル転送の前に内蔵フラッシュ メモリの内容を消去する必要がない場合は、**no** を入力します。

```
Erase flash device before writing? [confirm] no

Copy '' from server
  as 'new-ios-image' into Flash WITHOUT erase? [yes/no] yes
Ready to receive file...........
```

ステップ 10 コンピュータ上の、ルータにシステム イメージを送信している端末エミュレーション ソフトウェアを使って、Xmodem または Ymodem 転送操作を開始します。ファイル転送を実行する手順については、使用しているエミュレーション ソフトウェア アプリケーションのマニュアルを参照してください。使用しているアプリケーションによっては、エミュレーション ソフトウェアから、ファイル転送の進捗状況が表示されることがあります。

ROM モニタを使用した Xmodem 転送

ここでは、ROM モニタ、および Xmodem プロトコルを使用したファイル転送について説明します。Ymodem プロトコルを使用して送信するには、**xmodem -y** ROM モニタ コマンドを使用します。

Cisco 3600 シリーズのルータでは、コピー先がフラッシュ メモリである場合でも、転送中のファイルを保存できるだけの容量がルータの DRAM に必要です。イメージは内蔵フラッシュ メモリの最初のファイルにコピーされます。フラッシュ メモリ内の既存のファイルは消去されます。フラッシュ パーティション、または 2 番目のファイルの位置にファイルをコピーすることはできません。

注意 電話ネットワークからコンソール ポートにモデムで接続すると、セキュリティ上の問題が発生します。この接続を有効にする前に、この問題について検討してください。たとえば、リモート ユーザはこのモデムにダイヤルインし、ルータの設定にアクセスできます。

ステップ 1 Cisco IOS ソフトウェア イメージをリモート コンピュータのハード ドライブに保存します。イメージは Cisco.com、または Feature Pack（Cisco 1600 シリーズのルータだけの機能）からダウンロードできます。

ステップ 2 リモート コンピュータから転送するには、モデムをルータのコンソール ポートと標準電話ネットワークに接続します。モデムとコンソール ポートの通信速度は同じでなければなりません。これはモデムでサポートされている速度によっても異なりますが、9600 ～ 115200 bps（Cisco 3600 シリーズ ルータ）、または 1200 ～ 115200 bps（Cisco 1600 シリーズ ルータ）になります。ルータのコンソール ポート転送速度の設定には、**confreg** ROM モニタ コマンドを使用します。Cisco 1600 シリーズのルータでは、**-s** オプションを使用して、転送速度を設定することもできます。

リモート コンピュータと電話ネットワークにモデムを接続します。リモート コンピュータは電話ネットワークにダイヤルして、ルータに接続します。

ローカル コンピュータから転送するには、null モデム ケーブルを使用して、ルータのコンソール ポートをコンピュータのシリアル ポートに接続します。ルータで設定されているコンソール ポートの速度は、ローカル コンピュータで設定されている転送速度と一致していなければなりません。

（注） ローカル コンピュータから転送する場合、Request To Send（RTS; 送信要求）信号または Data Terminal Ready（DTR; データ端末動作可能）信号を無視するように、端末エミュレーション プログラムを設定する必要があります。

ステップ 3 端末エミュレーション ウィンドウに ROM モニタ プロンプトが表示されます。

```
rommon >
```

xmodem ROM モニタ コマンドを入力します。このとき、必要なコピー オプションや、オプションで Cisco IOS イメージのファイル名を指定することができます。デフォルトでは、イメージはフラッシュ メモリにロードされます。代わりに DRAM にダウンロードするには、**-r** オプションを使用します。このイメージは、通常、ファイル転送の最後に実行されます。実行されないようにするには、**-x** オプションを使用します。**-c** オプションは CRC-16 チェックサムの指定を表します。これは標準のチェックサムよりも洗練され、徹底的なチェックサムですが、一部のコンピュータではサポートされていません。

```
rommon > xmodem -c new-ios-image

Do not start the sending program yet...
         File size           Checksum   File name
   1738244 bytes (0x1a8604)   0xdd25 george-admin/c3600-i-mz


WARNING: All existing data in flash will be lost!
Invoke this application only for disaster recovery.
Do you wish to continue? y/n  [n]:  yes
Ready to receive file new-ios-image ...
```

ステップ 4 Xmodem 転送操作を開始します。これは、リモート コンピュータ上の、ルータにシステム イメージを送信している端末エミュレーション ソフトウェアから開始されます。Xmodem ファイル転送を実行する手順については、使用しているエミュレーション ソフトウェア アプリケーションのマニュアルを参照してください。

ステップ 5 Cisco IOS イメージが転送、実行されます。リモート コンピュータから転送している場合、新しい Cisco IOS イメージの実行が開始された後でも、このコンピュータはコンソール ポートの制御権を持ち続けます。制御をローカル端末に戻すには、リモート コンピュータのルータ プロンプトから **speed** *bps* ライン コンフィギュレーション コマンドを入力して、ルータのコンソール ポートの速度が、ローカル端末の速度と一致するように再構成します。

```
Router# configure terminal
Router(config)# line 0
Router(config-line)# speed 9600
```

リモート接続が解除されます。この結果、モデムをコンソール ポートから切断し、端末回線を再接続できるようになります。

マイクロコード イメージのロード、アップグレード、および検証

Cisco 7200、7500、12000 シリーズのインターネット ルータを含む一部の Cisco ルータでは、マイクロコードを周辺コンポーネントにロードして、アップデートすることができます。この項では、マイクロコード イメージのロード、アップグレードおよび検証について、次のサブセクションに分けて説明します。

マイクロコード イメージの概要

マイクロコードは ROM に保存され、新しい機械語命令を追加できるようにします。新しい命令が必要になったときに、電子回路に組み込む必要はありません。マイクロコード イメージには、さまざまなハードウェア デバイスから実行できるマイクロコード ソフトウェアが含まれます。たとえば、マイクロコードは、Cisco 7500 シリーズ ルータの Channel Interface Processor（CIP; チャネル インターフェイス プロセッサ）や、Cisco 7200 シリーズ ルータの Channel Port Adapter（CPA; チャネル ポート アダプタ）でアップデートできます。

デフォルトでは、Cisco IOS システム ソフトウェア イメージにバンドルされたマイクロコードがロードされます。このマイクロコードはデフォルト マイクロコード イメージと呼ばれます。しかし、フラッシュに格納されているマイクロコードを使用するようにルータを設定できます。

RSP7000 を搭載した Cisco 7000 シリーズのルータ、および Cisco 7500 シリーズのルータには、マイクロコードを格納するための Writable Control Store（WCS）があります。アップデート後のマイクロコードは、ブート フラッシュ、または Route/Switch Processor（RSP; ルート スイッチ プロセッサ）カードの PCMCIA スロットの 1 つに挿入されたフラッシュ メモリ カードから WCS にロードできます。

copy 特権 EXEC コマンドを使用して、マイクロコードをフラッシュ ファイル システムにコピーすることにより、物理的にルータにアクセスすることなく、マイクロコードをアップデートできます。

マイクロコード イメージの場所の指定

マイクロコード イメージのロード元を指定するには、特権 EXEC モードで始まる次のコマンドを使用します。

	コマンド	目的

ステップ 1	`Router# copy tftp: flash:`
	または
	`Router# copy tftp: file-id`
		（任意）マイクロコード ファイルをフラッシュにコピーします。この手順は、マイクロコードをフラッシュからロードする必要がある場合だけ実行してください。
		イメージをフラッシュ メモリにコピーする方法の詳細については、「イメージをネットワーク サーバからフラッシュ メモリへコピー」の項を参照してください。

ステップ 2	`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。
ステップ 3	`Router(config)# microcode interface [flash-filesystem:filename [slot] | system [slot]]`	メモリの指定された位置から目的のインターフェイスにマイクロコードをロードするようにルータを設定します。
ステップ 4	`Router(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 5	`Router# copy system:running-config nvram:startup-config`	新しい設定情報を保存します。

マイクロコード イメージをダウンロードしようとしたときにエラーが発生した場合は、デフォルトのシステム マイクロコード イメージがロードされます。

（注） マイクロコード イメージは圧縮できません。

マイクロコード イメージのリロード

ロードされるマイクロコードを指定するコンフィギュレーション コマンドは次の 3 つのイベントのいずれかに続けて実装されます。

- システムの起動
- カードの挿入、または取り出し
- **microcode reload** グローバル コンフィギュレーション コマンドの発行

マイクロコード コンフィギュレーション コマンドを入力し、これらのイベントの 1 つが発生した後で、すべてのカードがリセットされ、適切なソースからマイクロコードがロードされます。その後、テストされ、動作可能になります。

マイクロコード コンフィギュレーション コマンドがすべて入力され、プロセッサ カードをリロードすべきであることをシステムに知らせるには、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。

コマンド	目的
`Router(config)# microcode reload`	コンフィギュレーションで指定されたソースから、すべてのインターフェイスおよびプロセッサ カードにマイクロコードをリロードします。

microcode reload グローバル コンフィギュレーション コマンドを入力した直後、Return キーを押すと、すべてのマイクロコードがリロードされます。グローバル コンフィギュレーション モードはイネーブルのままです。リロードの完了後、**exit** グローバル コンフィギュレーション コマンドを入力して、特権 EXEC プロンプトに戻ります。

カードの取り出し、または挿入中でフラッシュ メモリが使用中である場合、またはフラッシュのロック中に **microcode reload** コマンドを実行した場合、これらのファイルは使用できず、ボード上の ROM マイクロコードがロードされます。フラッシュ メモリが使用可能になったら、もう一度、**microcode reload** コマンドを実行すると、適切なマイクロコードがロードされます。**show flash** 特権 EXEC コマンドは、別のユーザやプロセスがフラッシュ メモリをロックしているかどうかを表示します。

（注） フラッシュの使用中には、**microcode reload** コマンドを使用してはいけません。たとえば、**copy** {**ftp:** | **rcp:** | **tftp:**} *flash-filesystem*、または **show** *flash-filesystem***:** 特権 EXEC コマンドがアクティブであるときに、このコマンドを使用してはいけません。

すべてのプロセッサを ROM からロードするというシステムのデフォルト動作を変更するマイクロコード コマンドを発行すると、**microcode reload** コマンドが自動的に実行中のコンフィギュレーションに追加されます。

次に、メモリに書き込まれたマイクロコード コンフィギュレーション コマンドに従って、すべてのコントローラをリセットし、指定されたマイクロコードをロードしてから、CxBus complex を再初期化する例を示します。

```
Router# configure terminal
Router(config)# microcode reload
Router(config)# end
```

マイクロコード イメージ情報の表示

マイクロコード イメージ情報を表示するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show microcode**	マイクロコード情報を表示します。

特定プラットフォームでのマイクロコードの使用

マイクロコードを操作するためのコマンドは、プラットフォームによって異なります。この項では、その他の Cisco IOS マニュアルに記載されている特別な設定情報を紹介します。

System Processing Engine（SPE）を使用した、Cisco アクセス サーバ（Cisco AS5800 など）にあるモデムへのマイクロコード（モデムのファームウェアおよびポートウェア）のダウンロードについては、『*Cisco IOS Dial Technologies Configuration Guide Release 12.4*』を参照してください。

Cisco 7000、7200、および 7500 シリーズ ルータのアダプタへの CIP および CPA マイクロコードのロードに関する詳細は、『*Cisco IOS Bridging and IBM Networking Configuration Guide*』の「IBM Networking」にある「Configuring Cisco Mainframe Channel Connection Adapters」の章を参照してください。

Cisco 12000 インターネット ルータへのマイクロコード イメージのロード

インターネット ルータに常駐する Cisco IOS イメージに加えて、Cisco 12000 シリーズのライン カードそれぞれが Cisco IOS イメージを持っています。ルータがリロードされると、指定された Cisco IOS イメージが GRP にロードされ、このイメージがすべてのライン カードに自動的にダウンロードされます。

通常、インターネット ルータとライン カードすべてでは同じ Cisco IOS イメージが使用されます。しかし、テストや不具合の修復を目的として、ライン カードの 1 つを新しいバージョンのマイクロコードでアップグレードする必要がある場合は、そのライン カードにすでに入っているものとは異なるマイクロコード システム イメージをロードすることができます。また、ライン カードの 1 つだけに影響を与えている問題に対処する場合も、このライン カードに新しいイメージをロードする必要があるでしょう。

ライン カードに Cisco IOS イメージをロードするには、まず、**copy tftp** 特権 EXEC コマンドを使用して、Cisco IOS イメージを、PCMCIA フラッシュ カードの 1 つにあるスロットにダウンロードします。フラッシュ カードに Cisco IOS イメージをダウンロードしたら、グローバル コンフィギュレーション モードの始めに次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router(config)# **microcode** {**oc12-atm** | **oc12-pos** | **oc3-pos-4**} **flash** *file-id slot-number*	ライン カードのタイプ、マイクロコード イメージの場所、イメージのダウンロード先となるライン カードのスロットを指定します。スロット番号を省略した場合、マイクロコード イメージはすべてのライン カードにダウンロードされます。
ステップ 2	Router(config)# **microcode reload** *slot-number*	指定されたライン カードでマイクロコードをリロードします。

	コマンド	目的
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

ステップ 4	`Router# execute-on slot slot-number show version`
	
	または
	
	`Router# attach slot-number`
		ライン カードに接続し、ディスプレイ出力のバージョン番号をチェックして、新しい Cisco IOS イメージがこのライン カードに入ったことを確認します。

Cisco 12000 シリーズ ルータでの設定情報の詳細については、Cisco IOS Release 11.2、Cisco IOS Release 12.0S、および Cisco IOS Release 12.2S のマニュアルを参照してください。これらは、Cisco.com にあります。プラットフォーム固有のマニュアルについては、http://www.cisco.com/univercd/cc/td/doc/product/core/ を参照してください。

MD5 ファイル検証

MD5 ファイル検証機能は、Cisco IOS File System（IFS）で Message Digest 5（MD5）アルゴリズムを使用してファイルを検証するために使用できる Cisco IOS ソフトウェア コマンドを提供します。

MD5 ファイル検証機能を使用すると、MD5 チェックサムの値を、イメージに対する既知の MD5 チェックサムの値と比較することで、Cisco IOS ソフトウェア イメージの完全性をチェックすることができます。すべての Cisco IOS ソフトウェア イメージの MD5 値は、ローカル システムのイメージの値と比較するために、Cisco.com から入手できるようになっています。

機能情報の入手方法

使用するソフトウェア リリースで、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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「MD5 ファイル検証の機能情報」（P.6）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

MD5 ファイル検証の制約事項

MD5 ファイル検証機能は、Cisco IOS デバイスに格納されている Cisco IOS ソフトウェア イメージの完全性のチェックのためだけに使用できます。リモート ファイル システムにあるイメージや、メモリ内で動作しているイメージの完全性をチェックするためには使用できません。

MD5 ファイル検証について

MD5 ファイル検証機能を設定するには、次の概念を理解しておく必要があります。

- 「MD5 ファイル検証の概要」（P.2）

MD5 ファイル検証の概要

MD5 ファイル検証機能は、システムのイメージファイルが壊れていたり不完全でないことをユーザが確認するためのメカニズムを提供します。この機能では、業界標準の MD5 アルゴリズムを使用して、信頼性とセキュリティを高めます。MD5 ファイル検証では、Cisco IOS Command-Line Interface（CLI; コマンドライン インターフェイス）から MD5 値を計算および表示します。ファイルを別のデバイスに対してチェックする必要はありません。

（注） Cisco IOS ソフトウェア イメージを確認するために、MD5 ファイルがルータ上にある必要はありません。

MD5 アルゴリズムを使用したファイルの検証方法

ここでは、次の作業について説明します。

- 「イメージの確認」（P.2）

イメージの確認

MD5 ファイル検証機能を使用すると、ルータに格納されている Cisco IOS イメージの MD5 チェックサムを生成し、Cisco.com で公開されている値と比較して、ルータ上のイメージが壊れていないことを確認できます。

イメージ ファイルを転送した後で MD5 完全性チェックを実行するには、ここで説明する作業を実行します。

イメージ情報

システム イメージの MD5 値は、Cisco.com の Software Center から入手できます。この値を入手するための最も便利な方法は、ダウンロード前にファイルの名前をクリックすることです。たとえば、3640 プラットフォーム用の Enterprise Plus 機能セットを含む 12.2.2T4 リリースを選択した場合、[Download] ボタンをクリックする前に、イメージのファイル名（c3640-js-mz.122-2.T4.bin）をクリックすることで、イメージ情報が表示されます。

一般に、イメージ情報には、イメージのリリース、説明、ファイル サイズ、BSD チェックサム、ルータ チェックサム、公開日、MD5 値が含まれています。ダウンロードする前にイメージの MD5 値をメモします。ただし、以前ダウンロードしたイメージの MD5 値がない場合は、Cisco.com で同じイメージを選択し（イメージのダウンロード時と同じ手順を使用します）、MD5 値を入手します。

手順の概要

1. **enable**
2. **verify /md5** *filesystem*:*filename*

   または

   verify /md5 *filesystem*:*filename md5-value*

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。 • 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	**verify /md5** *filesystem*:*filename*
	または
	verify /md5 *filesystem*:*filename md5-value*
	
	例：
	`Router# verify /md5 disk1:c7200-js-mz`
	または
	
	例：
	`Router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3`
		フラッシュ メモリ ファイル システム上のファイルのチェックサムを確認するか、ファイルの MD5 シグニチャを計算します。
		• 例では、ファイルシステムとして disk1 を指定し、ファイル名として c7200-js-mz を指定しています。
		または
		MD5 値が一致するかどうかを示すメッセージを表示します。
		• 例では、md5-value として 0f369ed9e98756f179d4f29d6e7755d3 を指定しています。

トラブルシューティングのヒント

MD5 値が一致しない場合、イメージが壊れているか、正しくない MD5 値を入力したことを意味します。

MD5 ファイル検証の設定例

ここでは、次の設定例について説明します。

• 「イメージの確認：例」（P.3）

イメージの確認：例

次の例では、デバイスの disk1 に格納されているイメージの MD5 値を表示するために、**/md5** キーワードを使用しています。最後の行に表示されている MD5 を Cisco.com で提供されている値と比較できます。

```
Router# verify /md5 disk1:
Verify filename []? c7200-js-mz
.....................................
.....................................
.....................................
.....................................
.....................................
.................................Done!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

次の例では、イメージの既知の MD5 値を **verify** コマンドで指定しており、その値が格納されている値と照合されます。

```
Router# verify /md5 disk1:c7200-js-mz ?
  WORD  Expected md5 signature
  <cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.....................................
.....................................
.....................................
.....................................
.....................................
.................................Done!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

その他の関連資料

ここでは、MD5 ファイル検証機能に関する関連資料について説明します。

関連資料

関連項目	参照先
システム イメージのロード、メンテナンス、リブートのための追加のコマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
RFC 1321	『*MD5 Message-Digest Algorithm*』

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup で Command Lookup Tool を使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html にある『*Cisco IOS Master Command List, All Releases*』を使用してください。

- **verify**

MD5 ファイル検証の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　MD5 ファイル検証の機能情報

機能名	リリース	機能情報
MD5 ファイル検証	12.2(4)T 12.0(22)S	MD5 ファイル検証機能を使用すると、MD5 チェックサムの値を、イメージに対する既知の MD5 チェックサムの値と比較することで、Cisco IOS ソフトウェア イメージの完全性をチェックすることができます。 **verify** コマンドが追加または変更されています。

ウォーム アップグレード

ウォーム アップグレード機能は Cisco IOS イメージが別の Cisco IOS イメージを読み取って解凍し、コントロールをこの新しいイメージに移す機能を提供します。この機能により、計画された Cisco IOS ソフトウェア アップグレードまたはダウングレード中のデバイスのダウンタイムが削減されます。ウォーム アップグレード機能は Cisco IOS Release 12.3(2)T で導入されたウォーム リロード機能を補完する機能です。

ウォーム アップグレード機能の機能履歴

リリース	変更点
12.3(11)T	この機能が導入されました。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

ウォーム アップグレードについて

ウォーム アップグレード機能を使用するには、次の概念を理解しておく必要があります。

ウォーム アップグレード機能

ウォーム アップグレード機能は Cisco IOS イメージが別の Cisco IOS イメージを読み取って解凍し、コントロールをこの新しいイメージに移す機能を提供します。この機能により、計画された Cisco IOS ソフトウェア アップグレードまたはダウングレード中のデバイスのダウンタイムが削減されます。ウォーム アップグレードを実行するには、**reload warm file** *url* コマンドを使用します。ウォーム アップグレード機能は Cisco IOS Release 12.3(2)T で導入されたウォーム リロード機能を補完する機能です。

ウォーム アップグレード機能が導入される前、Cisco IOS イメージはコントロールを ROM Monitor（ROMMON; ROM モニタ）モードに移し、Cisco IOS ソフトウェア アップグレードまたはダウングレードを実行していました。ROMMON は起動ローダ イメージを使用して、必要なアップグレードまたはダウングレード手順を実行していました。この処理の実行中はネットワーキング デバイスがダウンします。ウォーム アップグレード機能が導入されると、新しい Cisco IOS の読み取りおよび解凍中にパケット転送が引き続き可能となります。現在のイメージが新しいイメージで上書きされ、新しいイメージがオペレーティング システムをロードして再構成しているときにだけデバイスがダウンします。

ウォーム アップグレード処理に失敗すると、一部または全体が上書きされていない場合は、現在の Cisco IOS イメージが引き続き実行されるはずです。この場合、ROMMON は設定した任意のイメージをロードできます。

（注） Cisco IOS イメージを **reload** コマンドのイメージ検証機能をサポートしていないイメージにダウングレードする場合には、ウォーム アップグレード処理を実行する前に、イメージにデジタル署名がないことを示す警告メッセージが表示されます。

ウォーム アップグレード機能を使用して Cisco IOS イメージをリロードする方法

ここでは、次の各手順について説明します。

- 「ウォーム アップグレード機能を使用した Cisco IOS イメージのリロード」（P.2）（必須）
- 「ウォーム アップグレード機能のモニタリングとトラブルシューティング」（P.3）（任意）

ウォーム アップグレード機能を使用した Cisco IOS イメージのリロード

この作業を実行して、ウォーム アップグレード機能を使用して Cisco IOS イメージをリロードします。

前提条件

- Cisco IOS Release 12.3(2)T で導入されたウォーム リロード機能をイネーブルにする必要があります。
- ウォーム アップグレード機能を使用した Cisco IOS イメージのアップグレードまたはダウングレード機能は、現在の Cisco IOS イメージがウォーム アップグレード機能をサポートしていることを前提としています。ただし、現在のイメージがアップグレードまたはダウングレードされる新しいイメージでウォーム アップグレード機能に対応している必要はありません。

制約事項

ウォーム アップグレード機能を使用したソフトウェアのアップグレードまたはダウングレードは、システム内に解凍した Cisco IOS イメージを格納する十分なメモリ空き領域がある場合にだけ実行できます。

手順の概要

1. **enable**
2. **reload** [**/verify** | **/noverify**] [**warm** [**file** *url*]] [**in** [*hh*:]*mm* | **at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [*text*]

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。 • 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	**reload** [**/verify** | **/noverify**] [**warm** [**file** *url*]] [**in** [*hh*:]*mm* | **at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [*text*] 例： `Router> reload warm file flash:c3745-ipvoice-mz.12.3.11.T.bin`	オペレーティング システムをリロードします。 • **reload warm file** *url* コマンドを使用して、場所と名前を *url* 引数で指定した新しいイメージでオペレーティング システムをリロードします。ウォーム アップグレード機能を使用してリロードが実行されます。 • ルータのリロード時にウォーム再起動機能を上書きしない場合は、**warm** キーワードを発行する必要があります。

ウォーム アップグレード機能のモニタリングとトラブルシューティング

この作業を実行して、ウォーム アップグレード機能をモニタリングおよびトラブルシューティングします。

手順の概要

1. **show warm-reboot**
2. **debug warm-reboot**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show warm-reboot** **例：** `Router> show warm-reboot`	試行したウォーム再起動の統計情報を表示します。
ステップ 2	**debug warm-reboot** **例：** `Router> debug warm-reboot`	ウォーム再起動デバッグ情報を表示します。

ウォーム アップグレード機能の設定例

ここでは、次の設定例について説明します。

- 「ウォーム アップグレード機能を使用した Cisco IOS の設定：例」（P.4）

ウォーム アップグレード機能を使用した Cisco IOS の設定：例

次に、場所と名前が tftp://9.1.0.1/c7200-p-mz.port である新しいイメージを使用してオペレーティング システムをリロードする方法の例を示します。ウォーム アップグレード機能を使用してリロードが実行されます。

```
Router> reload warm file tftp://9.1.0.1/c7200-p-mz.port

Proceed with reload? [confirm]
Loading c7200-p-mz.port from 9.1.0.1 (via Ethernet5/0):!!!
[OK - 15323964 bytes]

Decompressing the image :### [OK]

02:37:42:%SYS-5-RELOAD:Reload requested by console. Reload Reason:Reload Command.
             Restricted Rights Legend
.
.
.
Press RETURN to get started!

00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/0, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/1, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/2, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface Ethernet5/3, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface FastEthernet6/0, changed state to up
00:00:12:%LINK-3-UPDOWN:Interface FastEthernet6/1, changed state to up
00:00:12:%SYS-5-CONFIG_I:Configured from memory by console
00:00:13:%SYS-5-RESTART:System restarted --
00:00:13:%SYS-6-BOOTTIME:Time taken to reboot after reload =   25 seconds
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/0, changed state to up
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/1, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/2, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Ethernet5/3, changed state to down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet6/0, changed state to
down
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet6/1, changed state to
down
```

```
00:00:14:%LINEPROTO-5-UPDOWN:Line protocol on Interface Fddi4/0, changed state to down
00:00:14:%LINK-5-CHANGED:Interface Fddi4/0, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/1, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/2, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface Ethernet5/3, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface FastEthernet6/0, changed state to administratively down
00:00:14:%LINK-5-CHANGED:Interface FastEthernet6/1, changed state to administratively down
```

その他の関連資料

ここでは、ウォーム アップグレード機能に関する関連資料について説明します。

関連資料

関連項目	参照先
ルータの再起動に関する詳細	『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3*』の「*File* Management」の項の「Rebooting」の章。
その他の起動コマンド	『*Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3T*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **debug warm-reboot**
- **reload**

再起動とリロード：イメージ ロード特性の設定

この章では、シスコ デバイス（ルータなど）が再起動時に実行する基本手順、手順の変更方法、ROM モニタの使用方法について説明します。

この章で説明する起動コマンドの詳細については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「Booting Commands」の章を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index*』を使用するかオンラインで検索します。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。詳細については、「About Cisco IOS Software Documentation」の章の「Identifying Platform Support for Cisco IOS Software Features」の項を参照してください。

再起動手順の概要

ここでは、ルータの再起動時に行われることを説明します。

- 「ルータは起動時にどのコンフィギュレーション ファイルを使用するか」
- 「ルータは起動時にどのイメージを使用するか」

ルータは起動時にどのコンフィギュレーション ファイルを使用するか

クラス A フラッシュ ファイル システムのプラットフォームを除くすべてのプラットフォームの場合：

- コンフィギュレーション レジスタが NVRAM を無視するように設定されている場合、ルータはセットアップ モードを開始します。
- コンフィギュレーション レジスタが NVRAM を無視するように設定されていない場合、
  - スタートアップ ソフトウェアは、NVRAM 内の設定情報を確認します。
  - NVRAM が有効なコンフィギュレーション コマンドを保持している場合、Cisco IOS ソフトウェアは起動時にコマンドを自動的に実行します。
  - NVRAM または NVRAM に含まれる設定（CRC チェックサム エラー）に関連する問題をソフトウェアが検出した場合は、**セットアップ** モードが開始されて、設定を求めるプロンプトが表示されます。

クラス A フラッシュ ファイル システムのプラットフォームの場合：

- コンフィギュレーション レジスタが NVRAM を無視するように設定されている場合、ルータはセットアップ モードを開始します。
- コンフィギュレーション レジスタが NVRAM を無視するように設定されていない場合、
  - スタートアップ ソフトウェアは、CONFIG_FILE 環境変数によって指定された設定を使用します。
  - CONFIG_FILE 環境変数が存在しない、または null である場合（最初のスタートアップ時など）、ルータは NVRAM をデフォルト スタートアップ デバイスとして使用します。
  - ルータが NVRAM を使用して起動し、システムが NVRAM や NVRAM に含まれる設定に関する問題を検出すると、ルータは **セットアップ** モードを開始します。

問題には、NVRAM 内の情報のチェックサム不良や、NVRAM が空で設定情報を持たないことなどがあります。トラブルシューティング手順については、マニュアル『*Internetwork Troubleshooting Guide*』の「Troubleshooting Hardware and Booting Problems」の章を参照してください。**setup** コマンド ファシリティの詳細については、マニュアルの「Using Setup for Configuration Changes」の章を参照してください。環境変数の詳細については、「環境変数の設定」の章を参照してください。

ルータは起動時にどのイメージを使用するか

ルータが電源投入または再起動されると、次のようなことが発生します。

- ROM モニタが初期化されます。
- ROM モニタがコンフィギュレーション レジスタ内のブート フィールド（下位 4 ビット）をチェックします。
  - ブート フィールドの最終桁が 0（たとえば、0x100）である場合、システムは起動しません。その代わりに、システムは ROM モニタ モードを開始して、ユーザの介入を待ちます。ROM モニタ モードから、**boot** または **b** コマンドを使用して、システムを手動で起動できます。
  - ブート フィールドの最終桁が 1（たとえば、0x101）である場合、ブート ヘルパー イメージが ROM からロードされます（一部のプラットフォームでは、ブート ヘルパー イメージが BOOTLDR 環境変数によって指定されます）。
  - ブート フィールドの最終桁が 2 ～ F（たとえば、0x102 ～ 0x10F）である場合、ルータはコンフィギュレーション ファイルによって指定された、または BOOT 環境変数によって指定された最初の有効なイメージを起動します。

（注） コンフィギュレーション レジスタのブート フィールド値は、16 進で表されます。ブート フィールドにはコンフィギュレーション レジスタ値の最終 4 ビット（最終の 16 進桁）だけが含まれるため、この説明で重要な唯一の桁は最終桁です。このため、0x1（0000 0001）と 0x101（1 0000 0001）は、両方とも最終 4 ビットが 0001 であることから、ブート フィールドの説明上は同等になります。

ブート フィールドが 0x102 ～ 0x10F である場合、ルータは、有効なイメージを起動するまで、各 **boot system** コマンドを順番に処理します。コンフィギュレーション レジスタ内のビット 13 が設定されている場合は、各コマンドが 1 回試行されます（ビット 13 は、次の 16 進表記の *b* の位置で示されます：0x*b*000）。ビット 13 が設定されない場合、ネットワーク サーバを指定する **boot system** コマンドが、さらに 5 回まで試行されます。連続した各試行間のタイムアウトは、2、4、16、256、300 秒です。

ルータが有効なイメージを検索できない場合は、次のイベントが発生します。

- システム コンフィギュレーション ファイル内のすべてのブート コマンドがネットワーク サーバからの起動を指定して、すべてのコマンドが失敗した場合、システムはフラッシュ メモリ内の最初の有効なファイルを起動しようとします。
- コンフィギュレーション レジスタで「boot-default-ROM-software」オプションが設定されている場合、ルータはブート イメージ（ブート ROM に含まれるイメージ、または BOORLDR 環境変数によって指定される ROM）を起動します。
- コンフィギュレーション レジスタで「boot-default-ROM-software」オプションが設定されていない場合、システムは ROM モニタ プロンプトでのユーザの介入を待ちます。ルータを手動で起動する必要があります。
- 完全に機能しているシステム イメージが見つからない場合は、ルータが機能しないため、直接コンソール ポートに接続して再設定する必要があります。

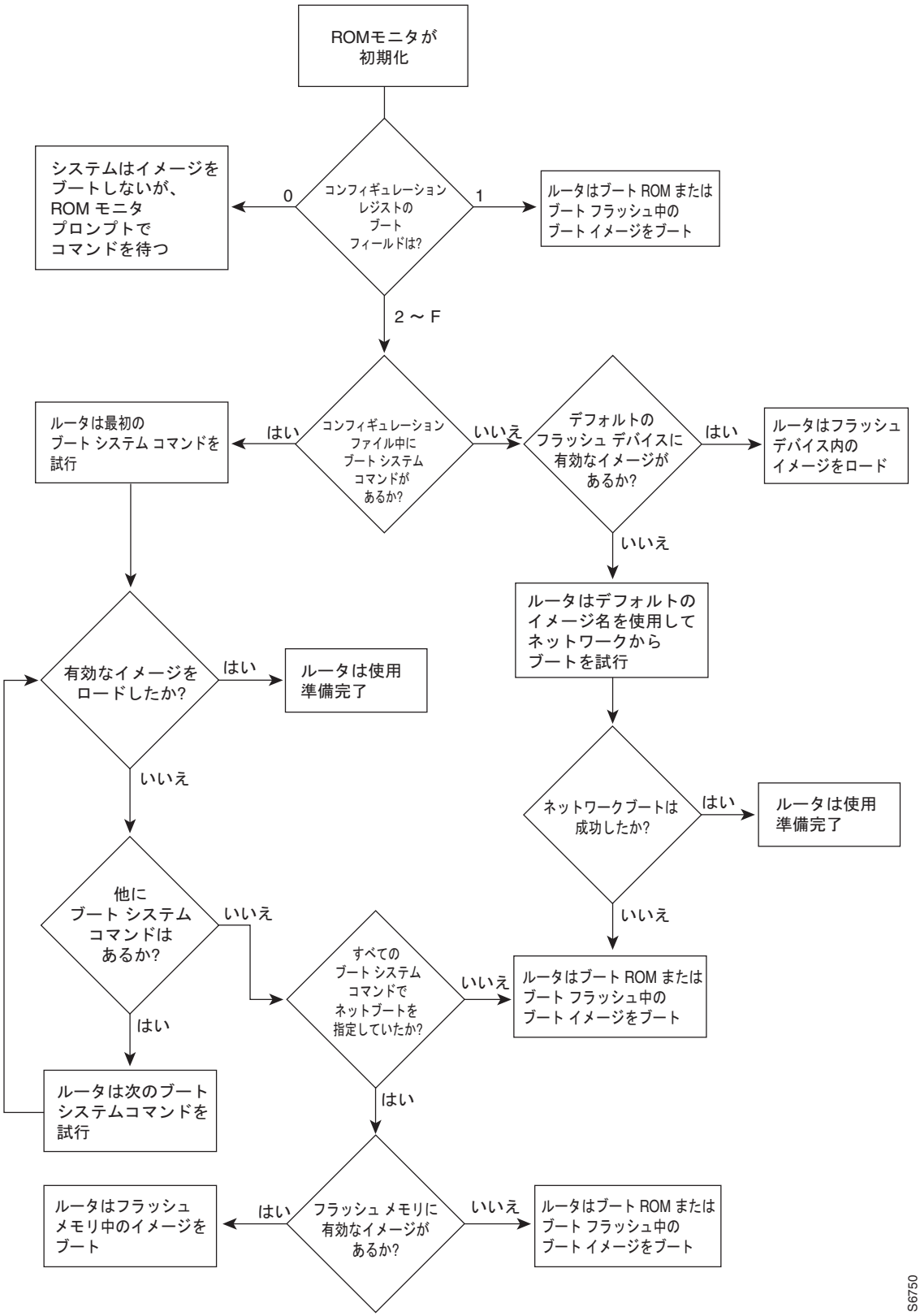
（注） ブート イメージのデフォルトの場所については、プラットフォームのマニュアルを参照してください。

フラッシュ メモリ内のブート可能ファイルを検索する場合は、次のようなことが発生します。

- システムがフラッシュ メモリ内のファイル名を検索します。ファイル名が指定されない場合、ソフトウェアは、フラッシュ メモリ ディレクトリ全体で、最初のファイルだけでなく、ブート可能ファイルを検索します。
- システムがフラッシュ メモリ内のファイルを認識しようとします。ファイルが認識された場合、ソフトウェアは次のチェックを実行して、そのファイルがブート可能であるかどうかを判断します。
  - フラッシュから実行される（run-from-Flash）イメージの場合、ソフトウェアは、そのファイルが正しい実行アドレスにロードされているかどうかを識別します。
  - RAM から実行される（run-from-RAM）イメージの場合、ソフトウェアは、イメージを実行するだけの十分な RAM がシステムにあるかどうかを識別します。

図 12 に、基本的な起動決定プロセスを示します。

図 12　起動プロセス


ROMモニタが
初期化
コンフィギュレーション
レジストの
ブート
フィールドは?
0
1
システムはイメージを
ブートしないが、
ROM モニタ
プロンプトで
コマンドを待つ
ルータはブート ROM または
ブート フラッシュ中の
ブート イメージをブート
2 ～ F
コンフィギュレーション
ファイル中に
ブート システム
コマンドが
あるか?
はい
いいえ
ルータは最初の
ブート システム コマンドを
試行
デフォルトの
フラッシュ デバイスに
有効なイメージが
あるか?
はい
ルータはフラッシュ
デバイス内の
イメージをロード
いいえ
有効なイメージを
ロードしたか?
はい
ルータは使用
準備完了
いいえ
ルータはデフォルトの
イメージ名を使用して
ネットワークから
ブートを試行
ネットワークブートは
成功したか?
はい
ルータは使用
準備完了
いいえ
他に
ブート システム
コマンドは
あるか?
いいえ
はい
すべての
ブート システム
コマンドで
ネットブートを
指定していたか?
いいえ
ルータはブート ROM または
ブート フラッシュ中の
ブート イメージをブート
はい
ルータは次のブート
システムコマンドを
試行
フラッシュ メモリに
有効なイメージが
あるか?
はい
ルータはフラッシュ
メモリ中のイメージを
ブート
いいえ
ルータはブート ROM または
ブート フラッシュ中の
ブート イメージをブート
S6750

再起動作業リスト

再起動に関連する作業について次の項で説明します。

- 「起動情報の表示」
- 「コンフィギュレーション レジスタのブート フィールドの変更」
- 「環境変数の設定」
- 「システム イメージのリロードのスケジューリング」
- 「ROM モニタ モードの開始」
- 「ROM モニタからのシステム イメージの手動ロード」

起動情報の表示

EXEC モードで次のコマンドを使用して、システム ソフトウェア、システム イメージ ファイル、およびコンフィギュレーション ファイルに関する情報を表示します。

コマンド	目的
`Router# show bootvar`	BOOT 環境変数の内容、CONFIG_FILE 環境変数によって指定されているコンフィギュレーション ファイルの名前、および BOOTLDR 環境変数の内容を示します。
`Router# more nvram:startup-config`	スタートアップ コンフィギュレーション情報を示します。 クラス A フラッシュ ファイル システムを除くすべてのプラットフォームでは、スタートアップ コンフィギュレーションは通常 NVRAM 内にあります。クラス A フラッシュ ファイル システムでは、CONFIG_FILE 環境変数が、NVRAM にデフォルト設定されるスタートアップ コンフィギュレーションを指定します。
`Router# show version`	システム ソフトウェアのリリース バージョン、システム イメージ名、コンフィギュレーション レジスタ設定、および他の情報を示します。

これらのコマンドの例については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ROM モニタ モードで o コマンド（または、一部のプラットフォームでは **confreg** コマンド）を使用して、いくつかのプラットフォームのコンフィギュレーション レジスタ設定を示すこともできます。

コンフィギュレーション レジスタのブート フィールドの変更

コンフィギュレーション レジスタのブート フィールドは、ルータが オペレーティング システム イメージをロードするかどうかを指定し、ロードする場合は、このシステム イメージを取得した場所を指定します。この項には次のトピックがあります。

- 「ルータがブート フィールドを使用する方法」
- 「ハードウェアとソフトウェア コンフィギュレーション レジスタ ブート フィールド」

- 「ソフトウェア コンフィギュレーション レジスタ ブート フィールドの変更」

コンフィギュレーション レジスタの詳細については、プラットフォームのマニュアルを参照してください。

ルータがブート フィールドを使用する方法

ブート フィールドは、16 ビット コンフィギュレーション レジスタの下位 4 ビット（ビット 3、2、1、および 0）で構成されます。次のブート フィールド値は、ルータがオペレーティング システムをロードするかどうかを指定し、また、ルータがシステム イメージを取得する場所を指定します。

- ブート フィールド全体が 0-0-0-0（0x0）に等しい場合、ルータはシステム イメージをロードしません。代わりに、ルータは ROM モニタ モードまたは「メンテナンス」モードを開始して、ROM モニタ コマンドを入力してシステム イメージを手動でロードできるようになります。ROM モニタ モードの詳細については、「ROM モニタからのシステム イメージの手動ロード」の項を参照してください。
- ブート フィールド全体が 0-0-0-1（0x1）に等しい場合、ルータはブート ヘルパーまたは rxboot イメージをロードします。
- ブート フィールド全体が 0-0-1-0（0x2）～ 1-1-1-1（0xF）の値に等しい場合、ルータは、スタートアップ コンフィギュレーション ファイル内の **boot system** コマンドで指定されるシステム イメージをロードします。スタートアップ コンフィギュレーション ファイルに **boot system** コマンドが含まれていない場合、ルータはネットワーク サーバ上に保存されているデフォルト システム イメージをロードしようとします。

  ネットワーク サーバからデフォルト システム イメージをロードする場合、ルータはコンフィギュレーション レジスタを使用して、ネットワーク サーバから起動するためのデフォルト システム イメージ ファイル名を決定します。ルータは、cisco で始まり、コンフィギュレーション レジスタ内のブート フィールド番号の 8 進値、さらにハイフン（-）とプロセッサ タイプ名（cisco*nn-cpu*）が続くデフォルト ブート ファイル名を形成します。コンフィギュレーション レジスタおよびデフォルト ファイル名の詳細については、適切なハードウェア インストレーション ガイドを参照してください。

ハードウェアとソフトウェア コンフィギュレーション レジスタ ブート フィールド

ブート フィールドの変更は、プラットフォームに応じて、ハードウェア コンフィギュレーション レジスタまたはソフトウェア コンフィギュレーション レジスタのいずれかから行います。

ほとんどのプラットフォームでは、ソフトウェア コンフィギュレーション レジスタが使用されます。プラットフォームのコンフィギュレーション レジスタの詳細については、ハードウェア マニュアルを参照してください。

ハードウェア コンフィギュレーション レジスタは、Dual In-Line Package（DIP）スイッチをルータの後部に置いたプロセッサ カード上だけで変更できます。ハードウェア コンフィギュレーション レジスタの変更の詳細については、適切なハードウェア インストレーション ガイドを参照してください。

ソフトウェア コンフィギュレーション レジスタ ブート フィールドの変更

ソフトウェア コンフィギュレーション レジスタ ブート フィールドを 変更するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show version`	現行のコンフィギュレーション レジスタ設定を取得します。コンフィギュレーション レジスタは、16 進値として示されます。
ステップ 2	`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。
ステップ 3	`Router(config)# config-register value`	既存のコンフィギュレーション レジスタ設定を変更して、システム イメージをロードする方法を反映させます。コンフィギュレーション レジスタ値は、「0x」で始まる 16 進形式で指定します。
ステップ 4	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 5	`Router# show version`	（任意）コンフィギュレーション レジスタ設定が正しいことを確認します。設定が正しくない場合は、ステップ 2 ～ 5 を繰り返します。
ステップ 6	`Router# copy running-config startup-config`	実行中の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に保存します。
ステップ 7	`Router# reload`	（任意）ルータを再起動して変更内容を有効にします。

ROM モニタ モードでは、一部のプラットフォーム上で、**o** コマンドまたは **confreg** コマンドを使用すると、ソフトウェア コンフィギュレーション レジスタ ブート フィールドの値が表示されます。

現在のコンフィギュレーション レジスタ設定を変更して、システム イメージをロードする方法を反映させます。上記の手順を実行するには、最下位の 16 進の桁を、次のいずれかに変更します。

- 0：ROM モニタ モードで **boot** コマンドを使用して、システム イメージを手動でロードします。
- 1：システム イメージをブート ROM からロードします。Cisco 7200 シリーズおよび Cisco 7500 シリーズでは、この設定により、システムがブートフラッシュからシステム イメージを自動的にロードするように設定されます。
- 2 ～ F：スタートアップ コンフィギュレーション ファイル内の **boot system** コマンドから、またはネットワーク サーバ上に保存されたデフォルト システム イメージからシステム イメージをロードします。

たとえば、現在のコンフィギュレーション レジスタ設定が 0x101 で、スタートアップ コンフィギュレーション ファイル内の **boot system** コマンドからシステム イメージをロードする場合、コンフィギュレーション レジスタ設定を 0x102 に変更することがあります。

ソフトウェア コンフィギュレーション レジスタ ブート フィールドの変更例

次に、**show version** コマンドによって、ルータが自動的にオペレーティング システム イメージをロードしないように現在のレジスタが設定されていることが表示される例を示します。代わりに、ルータが ROM モニタ モードを開始して、ユーザによる ROM モニタ コマンドの入力を待機します。新しい設定は、ルータにスタートアップ コンフィギュレーション ファイル内のコマンドから、またはネットワーク サーバ上に保存したデフォルト システム イメージからシステムイメージをロードするように指示します。

```
Router1# show version

Cisco IOS (tm) Software
4500 Software (C4500-J-M), Version 11.1(10.4), RELEASE SOFTWARE
Copyright (c) 1986-1997 by Cisco Systems, Inc.
Compiled Mon 07-Apr-97 19:51 by lmiller
Image text-base: 0x600088A0, data-base: 0x60718000

ROM: System Bootstrap, Version 5.1(1), RELEASE SOFTWARE (fc1)
```

```
FLASH: 4500-XBOOT Bootstrap Software, Version 10.1(1), RELEASE SOFTWARE (fc1)

Router1 uptime is 6 weeks, 5 days, 2 hours, 22 minutes
System restarted by error - a SegV exception, PC 0x6070F7AC
System image file is "c4500-j-mz.111-current", booted via flash

cisco 4500 (R4K) processor (revision 0x00) with 32768K/4096K bytes of memory.
Processor board ID 01242622
R4600 processor, Implementation 32, Revision 1.0
G.703/E1 software, Version 1.0.
Bridging software.
SuperLAT software copyright 1990 by Meridian Technology Corp).
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
TN3270 Emulation software (copyright 1994 by TGV Inc).
Basic Rate ISDN software, Version 1.0.
2 Ethernet/IEEE 802.3 interfaces.
2 Token Ring/IEEE 802.5 interfaces.
4 ISDN Basic Rate interfaces.
128K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
4096K bytes of processor board Boot flash (Read/Write)

Configuration register is 0x2100

Router1# configure terminal
Router1(config)# config-register 0x210F
Router1(config)# end
Router1# reload
```

環境変数の設定

多数のプラットフォームが複数の場所からイメージを起動できるため、これらのシステムは特別な ROM モニタ環境変数を使用して、ルータによって使用されるイメージの場所およびファイル名を指定します。さらに、クラス A フラッシュ ファイル システムは複数の場所からコンフィギュレーション ファイルをロードでき、また、環境変数を使用してスタートアップ コンフィギュレーションを指定できます。

これらの特別な環境変数は次のとおりです。

- 「BOOT 環境変数」
- 「BOOTLDR 環境変数」
- 「CONFIG_FILE 環境変数」

BOOT 環境変数

BOOT 環境変数は、さまざまなファイル システム上のブート可能なシステム イメージのリストを指定します。『*Configuration Fundamentals Configuration Guide*』の「Loading and Maintaining System Images and Microcode」の章の「Specify the Startup System Image in the Configuration File」の項を参照してください。BOOT 環境変数をスタートアップ コンフィギュレーションに保存すると、ルータは起動時に変数を確認して、起動対象のイメージのデバイスおよびファイル名を識別します。

ルータは、BOOT 環境変数リスト内の最初のイメージを起動しようとします。ルータがイメージの起動に失敗した場合は、リスト内で指定された次のイメージを起動しようとします。ルータは、イメージの起動に成功するまで、リスト内の各イメージを起動しようとします。ルータが BOOT 環境変数リスト内のどのイメージも起動できない場合、ルータはブート イメージを起動しようとします。

BOOT 環境変数リスト内のエントリでデバイスが指定されていない場合、ルータはそのデバイスが **tftp** であると想定します。BOOT 環境変数リスト内のエントリが有効なデバイスを指定している場合、ルータはそのエントリをスキップします。

BOOTLDR 環境変数

BOOTLDR 環境は、有効なシステム イメージを検索できなかった場合、ROM モニタが使用するブート イメージを含んでいるフラッシュ ファイル システムおよびファイル名を指定します。さらに、ブート イメージは、イメージを持つルータをネットワーク サーバから起動する必要があります。

ブート ROM ではなく、ソフトウェア ブート イメージを使用するプラットフォーム上で BOOTLDR 環境変数を変更できます。これらのプラットフォームでは、ブート ROM を置き換えなくても、ブート イメージを変更できます。

この環境変数を使用すると、複数のブート イメージを持つことができます。BOOTLDR 環境変数をスタートアップ コンフィギュレーションに保存すると、ルータは起動時に変数を確認して、システムがロードできない場合にどのブート イメージを使用するかを決定します。

（注） ブート イメージのデフォルトの場所については、プラットフォームのマニュアルを参照してください。

CONFIG_FILE 環境変数

クラス A フラッシュ ファイル システムの場合、CONFIG_FILE 環境変数は、ファイル システムおよび、初期化（起動）に使用するコンフィギュレーション ファイルのファイル名を指定します。有効なファイル システムには、**nvram:**、**bootflash:**、**slot0:**、および **slot1:** を含めることができます。デバイスの詳細については、「Managing Configuration Files」の章を参照してください。CONFIG_FILE 環境変数をスタートアップ コンフィギュレーションに保存すると、ルータは起動時に変数を確認して、初期化に使用するコンフィギュレーション ファイルの場所とファイル名を決定します。

CONFIG_FILE 環境変数が存在しない、または null である場合（最初のスタートアップ時など）、初期化中にルータは NVRAM コンフィギュレーションを使用します。ルータが NVRAM の問題またはチェックサム エラーを検出した場合、ルータは **セットアップ** モードを開始します。**setup** コマンド ファシリティの詳細については、マニュアルの「Using Setup for Configuration Changes」の章を参照してください。

環境変数の管理

環境変数は ROM モニタによって管理されますが、特定のコマンドで作成、変更または表示できます。BOOT、BOOTLDR、および CONFIG_FILE 環境変数を作成または変更するには、それぞれ **boot system**、**boot bootldr**、および **boot config** グローバル コンフィギュレーション コマンドを使用します。

BOOT 環境変数の設定の詳細については、マニュアルの「Loading and Maintaining System Images」の章の「Specify the Startup System Image in the Configuration File」の項を参照してください。CONFIG_FILE 変数の設定の詳細については、このマニュアルの「Managing Configuration Files」の章の「Specify the Startup Configuration File」の項を参照してください。

（注） この 3 つのグローバル コンフィギュレーション コマンドを使用すると、実行コンフィギュレーションだけが影響を受けます。情報を ROM モニタの管理下にして、環境変数を想定どおりに機能させるには、環境変数設定をスタートアップ コンフィギュレーションに保存する必要があります。環境変数を実行コンフィギュレーションからスタートアップ コンフィギュレーションに保存するには、**copy system:running-config nvram:startup-config** コマンドを使用します。

show bootvar コマンドを発行することによって、BOOT、BOOTLDR、および CONFIG_FILE 環境変数の内容を表示できます。実行コンフィギュレーション設定がスタートアップ コンフィギュレーション設定と異なる場合、このコマンドはこれらの変数の設定を、スタートアップ コンフィギュレーションおよび実行コンフィギュレーション内に存在するとおりに表示します。

CONFIG_FILE 環境変数によって指定されるコンフィギュレーション ファイルの内容を表示するには、**more nvram:startup-config** コマンドを使用します。

BOOTLDR 環境変数の設定

BOOTLDR 環境変数を設定するには、特権 EXEC モードの開始時に次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **dir** [*flash-filesystem*:]	内部フラッシュまたはブートフラッシュに、ブート ヘルパー イメージが含まれていることを確認します。
ステップ 2	Router# **configure terminal**	端末から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	Router(config)# **boot bootldr** *file-url*	BOOTLDR 環境変数がフラッシュ デバイスおよびブート ヘルパー イメージのファイル名を指定するように設定します。この手順で、実行時の BOOTLDR 環境変数を変更します。
ステップ 4	Router# **end**	コンフィギュレーション モードを終了します。
ステップ 5	Router# **copy system:running-config nvram:startup-config**	実行したコンフィギュレーションをシステム 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 6	Router# **show bootvar**	（任意）BOOTLDR 環境変数の内容を確認します。

次に、ブート ヘルパー イメージの場所が内部フラッシュからスロット 0 に変更されるように BOOTLDR 環境を設定する例を示します。

```
Router# dir bootflash:
-#- -length- -----date/time------ name
1   620       May 04 1995 26:22:04 rsp-boot-m
2   620       May 24 1995 21:38:14 config2

7993896 bytes available (1496 bytes used)
Router# configure terminal
Router (config)# boot bootldr slot0:rsp-boot-m
Router (config)# end
Router# copy system:running-config nvram:startup-config
[ok]
Router# show bootvar
BOOT variable = slot0:rsp-boot-m
CONFIG_FILE variable = nvram:
Current CONFIG_FILE variable = slot0:router-config

Configuration register is 0x0
```

システム イメージのリロードのスケジューリング

ルータでのシステム イメージのリロードが後で実行されるようにスケジューリングする場合（たとえば、ルータが使用されない夜中または週末）や、リロードをネットワーク全体で同期させる場合（たとえば、ネットワーク内のすべてのルータでソフトウェア アップグレードを実行する）があります。

（注） スケジューリングされたリロードは、約 24 日以内に実行される必要があります。

スケジューリングされたリロードの設定

Cisco IOS ソフトウェアを後でリロードするようにルータを設定するには、特権 EXEC コマンド モードで次のいずれかのコマンドを使用します。

コマンド	目的
Router# **reload in** [*hh*:]*mm* [*text*]	ソフトウェアのリロードが今から *mm* 分（または *hh* 時間と *mm* 分）後に有効になるようにスケジューリングします。
Router# **reload at** *hh*:*mm* [*month day* | *day month*] [*text*]	ソフトウェアのリロードが（24 時間制で）指定された時間に有効になるようにスケジューリングします。月日が指定されている場合は、リロードが指定された日時に行われるようにスケジューリングされます。月日が指定されていない場合は、リロードが（指定された時間が現在の時間よりも遅い場合は）現在の日の指定された時間、または（指定された時間が現在の時間よりも早い場合は）翌日の指定された時間に行われます。00:00 に指定すると、リロードが真夜中にスケジューリングされます。

（注） **at** キーワードを使用できるのは、ルータでシステム クロックが（NTP、ハードウェア カレンダー、または手動で）設定されている場合だけです。この時間は、ルータの設定された時間帯と相対的です。リロードが複数のルータで同時に行われるようにスケジューリングするには、各ルータの時間が NTP と同期している必要があります。NTP の設定手順については、『*Cisco IOS Network Management Configuration Guide*, Release 12.4』の「Performing Basic System Management」の章を参照してください。

次に、**reload** コマンドを使用して、ルータでソフトウェアを現在の日の午後 7 時 30 分にリロードする例を示します。

```
Router# reload at 19:30
Reload scheduled for 19:30:00 UTC Wed Jun 5 1996 (in 2 hours and 25 minutes)
Proceed with reload? [confirm]
```

次に、**reload** コマンドを使用して、ルータでソフトウェアを将来リロードする例を示します。

```
Router# reload at 02:00 jun 20
Reload scheduled for 02:00:00 UTC Thu Jun 20 1996 (in 344 hours and 53 minutes)
Proceed with reload? [confirm]
```

スケジューリングされたリロードに関する情報の表示

以前にスケジューリングされたリロードに関する情報を表示したり、ルータでリロードがスケジューリングされているどうかを判断したりするには、EXEC コマンド モードで次のコマンドを使用します。

コマンド	目的
Router# **show reload**	リロードがスケジューリングされる時間、およびリロードの理由（リロードがスケジューリングされたときに指定済みである場合）を含むリロード情報を表示します。

スケジューリングされたリロードの取り消し

以前にスケジューリングされたリロードを取り消すには、特権 EXEC コマンド モードで次のコマンドを使用します。

コマンド	目的
Router# **reload cancel**	以前にスケジューリングされたソフトウェアのリロードを取り消します。

次に、**reload cancel** コマンドを使用して、スケジューリングされたリロードを中止する例を示します。

```
Router# reload cancel
Router#
***
*** --- SHUTDOWN ABORTED ---
***
```

ROM モニタ モードの開始

起動時の最初の 60 秒以内に、ルータの起動を強制的に中止できます。ルータが ROM モニタ モードを開始したら、コンフィギュレーション レジスタ値の変更、または手動でのルータの起動を実行できます。

起動を中止して ROM モニタ モードを開始するには、EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	Router# **reload** Press the Break[1] key during the first 60 seconds while the system is booting.	特権 EXEC モードから ROM モニタ モードを開始します。
ステップ 2	**?**	ROM モニタ コマンドを表示します。

1. このキーは、Cisco 7000 上では、少なくとも Cisco IOS Release 10 ブート ROM がない限り動作しません。

ワンポイントアドバイス

ROM モニタ モードを定期的に使用したり、ユーザに ROM モニタ コマンドを使用してロードさせたりする場合は、デフォルトで ROMMON になるようにシステムを設定できます。システムを自動的に ROM モニタ モードで起動するには、**config-register 0x0** コンフィギュレーション コマンドを使用して、コンフィギュレーション レジスタを 0x0 にリセットします。新しいコンフィギュレーション レジスタ値の 0x0 は、ルータまたはアクセス サーバが **reload** コマンドで再起動された後に有効になります。コンフィギュレーションを 0x0 に設定する場合は、ルータまたはアクセス サーバをリロードするたびにコンソールからシステムを手動で起動する必要があります。

ROMMON モードを終了するには、continue コマンドを使用します。コンフィギュレーションを変更した場合は、**copy running-config startup-config** コマンドを使用した後、**reload** コマンドを発行してコンフィギュレーションの変更内容を保存します。

エイリアス ROM モニタリング コマンド

ROM モニタは、Korn シェルに組み込まれたエイリアス機能に基づくコマンド エイリアスをサポートしています。エイリアス名を設定および表示するには、**alias** コマンドを使用します。この機能により、ユーザはコマンド名に文字または単語のエイリアスを指定できます。エイリアスは、コマンド名を短くしたり、コマンド オプションを自動的に呼び出したりする場合によく使用されます。

エイリアスは NVRAM に保存され、電源が切断されている間も保持されます。次に、いくつかの設定済みエイリアスを示します。

- **b** : boot
- **h** : history
- **i** : intialize/reset
- **r** : repeat
- **k** : stack
- **?** : help

次の例は、ROMMON コマンドのエイリアス設定済みのメニュー型リストです。

```
> ?
$ state      Toggle cache state (? for help)
B [filename] [TFTP Server IP address | TFTP Server Name]
             Load and execute system image from ROM or from TFTP server
C [address]  Continue execution [optional address]
D /S M L V   Deposit value V of size S into location L with modifier M
E /S M L     Examine location L with size S with modifier M
G [address]  Begin execution
H            Help for commands
I            Initialize
K            Stack trace
L [filename] [TFTP Server IP address | TFTP Server Name]
             Load system image from ROM or from TFTP server, but do not
             begin execution
O            Show configuration register option settings
P            Set the break point
S            Single step next instruction
T function   Test device (? for help)
Deposit and Examine sizes may be B (byte), L (long) or S (short).
Modifiers may be R (register) or S (byte swap).
Register names are: D0-D7, A0-A6, SS, US, SR, and PC
```

オプションが上記のメニュー型形式で表示された場合は、一覧表示されたエイリアス コマンドを使用できます。ルータまたはアクセス サーバを初期化するには、**i** コマンドを使用します。**i** コマンドを使用すると、ブートストラップ プログラムがハードウェアの再初期化、メモリ内容のクリア、およびシステム起動を実行します。システム イメージ ファイルを起動するには、**b** コマンドを使用します。

ROM モニタ ソフトウェアの特性は、プラットフォームにより異なります。ROM モニタ モード コマンドの詳細については、適切なハードウェア インストレーション ガイドを参照するか、Cisco.com で検索を実行してください。

ROM モニタからのシステム イメージの手動ロード

ルータが有効なシステム イメージを検出しない場合、そのコンフィギュレーション ファイルが起動時に破損した場合、または ROM モニタ モードを開始するようにコンフィギュレーション レジスタが設定されている場合は、システムが ROM モニタ モードを開始します。このモードでは、次の場所からシステム イメージを手動でロードできます。

- 内部フラッシュ メモリ、またはフラッシュ メモリ PC カード
- ネットワーク サーバ ファイル
- ROM
- Xmodem プロトコルまたは Ymodem プロトコルを使用したローカル コンピュータまたはリモート コンピュータ（Cisco 1600 シリーズ ルータおよび Cisco 3600 シリーズ ルータ限定）

起動できるのは、ルータがイメージを保存できる場所からだけです。したがって、すべてのプラットフォームについてこれらの場所から手動でロードできるわけではありません。

ルータを再起動して **Break** キーを押すか、または起動時の最初の 60 秒以内に Telnet セッションから「send break」コマンドを発行することでも、ROM モニタ モードを開始できます。

ROMMON 内のフラッシュ メモリからの手動起動

フラッシュ メモリから手動で起動するには、ROM モニタ モードで次のコマンドを使用します。

コマンド	目的

`ROMMON > ` **`boot flash`** `[`*`filename`*`]`
`ROMMON > ` **`boot flash`** *`partition-number`*`:[`*`filename`*`]`
`ROMMON > ` **`boot flash flash:`**`[ `*`partition-number`*`:] [`*`filename`*`]`
`ROMMON > ` **`boot`** `[`*`flash-fs`*`:][`*`partition-number`*`:][`*`filename`*`]`
`(Cisco 1600 series and Cisco 3600 series)`
`ROMMON >`
`boot` *`device`*`:[`*`filename`*`] (Cisco 7000 family)`
	フラッシュ メモリからルータを手動で起動します。使用するこのコマンドの正しい形式については、ハードウェア マニュアルを参照してください。

ファイル名が指定されていない場合は、デバイスやパーティションで検索された最初のブート可能ファイルが使用されます。

次に、ルータがフラッシュ メモリから手動で起動される例を示します。オプションの *filename* 引数がないため、フラッシュ メモリ内の最初の有効なファイルがロードされます。

```
> boot flash
F3: 1858656+45204+166896 at 0x1000

Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
```

```
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR [OK -
1903912/13765276 bytes]
F3: 1858676+45204+166896 at 0x1000

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
```

次に、ファイル名 gs7-k（ロードされたファイルの名前）を指定して **boot flash** コマンドが使用される例を示します。

```
> boot flash gs7-k
F3: 1858656+45204+166896 at 0x1000

Booting gs7-k from flash memory RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRR [OK - 1903912/13765276 bytes]
F3: 1858676+45204+166896 at 0x1000

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
System Bootstrap, Version 4.6(1012) [mlw 99], INTERIM SOFTWARE
Copyright (c) 1986-1992 by cisco Systems
RP1 processor with 16384 Kbytes of memory
```

次のコマンドは、内部フラッシュ メモリの最初のパーティション内にある最初のファイルを起動するように ROM モニタに指示します。

```
> boot flash:
```

このコマンドは、スロット 0 のフラッシュ メモリ カードの 2 番目のパーティション内にある最初のファイルを起動するように ROM モニタに指示します。

```
> boot slot0:2:
```

次に、ROM モニタが、スロット 0 のフラッシュ メモリ カードの 3 番目のパーティションから image name の名前が付いたファイルを起動する例を示します。

```
> boot slot0:3:imagename
```

次のコマンドでは有効なデバイス タイプ（**flash:**、**slot0:**、または **slot1:**）が指定されていないため、ROM モニタがブート ヘルパーを呼び出してシステム イメージを起動します。

```
> boot flash
```

ROMMON 内のネットワーク ファイルからの手動起動

ネットワーク ファイルから手動で起動するには、ROM モニタ モードで次のコマンドを使用します。

コマンド	**目的**
`ROMMON > boot filename [ip-address]`	ルータをネットワーク ファイルから手動で起動します。

次に、ルータがネットワーク ファイル *network1* から手動で起動される例を示します。

```
>boot network1
```

ROMMON 内の ROM からの手動起動

ルータを ROM から手動で起動するには、ROM モニタ モードで次のコマンドを使用します。

コマンド	目的
ROMMON > **boot**	ルータを ROM から手動で起動します。

Cisco 7200 シリーズおよび Cisco 7500 シリーズでは、**boot** コマンドによって、最初の bootflash 内にあるブート可能イメージがロードされます。

次に、ルータが ROM から手動で起動される例を示します。

```
>boot
```

ROMMON 内の MOP を使用した手動起動

MOP を使用してシステム ソフトウェアをインタラクティブに起動できます。通常は、システム ソフトウェア イメージを自動的に起動するようにルータを設定する前に、システム ソフトウェアが MOP ブート サーバ上にインストールされているかを確認するためにこれを実行します。

MOP を使用してルータを手動で起動するには、ROM モニタ モードで次のコマンドを使用します。

コマンド	目的
ROMMON > **boot system mop** *filename* [*mac-address*] [*interface*]	MOP を使用したルータの手動起動

Cisco 7200 シリーズおよび Cisco 7500 シリーズは、**boot mop** コマンドをサポートしません。

次に、ルータが MOP サーバから手動で起動される例を示します。

```
>boot mop network1
```

ROMMON の終了

ROM モニタから EXEC モードに戻るには、デフォルト システム イメージからのロードを継続する必要があります。ROMMON モードを終了してロードを再開するには、ROM モニタ モードで次のコマンドを使用します。

コマンド	目的
ROMMON > **continue**	スタートアップ コンフィギュレーション ファイルのロードを再開して、ユーザは EXEC モードに戻ります。

ウォーム リロード

ウォーム リロード機能では、ストレージからイメージを読み取らずにルータをリロードできます。つまり、以前メモリに保存したコピーから読み取り / 書き込みデータを復元し、フラッシュからメモリにイメージまたはイメージの自己解凍をコピーせずに実行を開始することで、ROM Monitor（ROMMON; ROM モニタ）モード介入なしで Cisco IOS イメージが再起動します。したがって、ルータの起動時間が大幅に短縮され、システム全体の可用性が高まります。

この章で紹介する機能情報の入手方法

ご使用の Cisco IOS ソフトウェア リリースで、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。この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「ウォーム リロードの機能情報」（P.6）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォーム、Cisco IOS ソフトウェア イメージ、および Cisco Catalyst OS ソフトウェア イメージの各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。Cisco.com のアカウントは必要ありません。

この章の構成

ウォーム リロードの制限事項

追加のメモリ消費

初期化された変数のコピーが保存されることでウォーム再起動が機能するため、メモリ消費量が増加します。ただし、メモリ消費量を最小化するには、初期化された変数のコピーを圧縮形式で保存します。この圧縮ファイルは「読み取り専用」とすることで破損を防止します。

ソフトウェア サポート限定

ウォーム再起動は強制ソフトウェア クラッシュ時にだけ使用するようにしてください。何らかのハードウェア障害の場合はコールド再起動が必要です。

ウォーム リロードについて

ウォーム再起動機能を使用するには、次の概念を理解しておくことを推奨します。

- 「ウォーム リロードの利点」（P.2）
- 「ウォーム リロード機能」（P.2）

ウォーム リロードの利点

ルータ リロードの高速化

フラッシュからメモリにイメージをコピーして解凍する必要がないため、ルータのリロード時間が 2 ～ 4 分短縮されます。BOOTLDR イメージをロードして BOOTLDR イメージでコンフィギュレーション ファイルを解析する追加手順がなくなるため、BOOTLDR イメージを使用するプラットフォームでは、さらに時間を短縮できます。

フラッシュ カードの除去

フラッシュ カードを除去した場合でも、強制コールド再起動（電源障害など）が必要でない限りは再起動可能であるため、ルータの実用性は変わりません。

ウォーム リロード機能

クラッシュが発生すると、Cisco IOS イメージはコントロールを ROMMON に移し、ストレージ デバイス（通常はフラッシュ）からメイン メモリにシステム イメージをコピーし、システム イメージを解凍してから、コントロールを Cisco IOS に戻します。ウォーム再起動ではイメージをメモリのテキスト セグメントの開始位置に戻し、その位置から再起動を実行できるため、ROMMON 介入が不要になります。初期化された変数はメモリに保持され、初期化された変数が保存されている既存のメモリの場所を上書きするために使用されます。したがって、CPU がテキスト セグメントの開始位置に戻り、処理を開始すると、バイナリがフラッシュから読み取られ解凍された後に実行された場合と同じ情報が得られます。

ウォーム リロードの使用方法

ここでは、次の各手順について説明します。

- 「ウォーム リロードの設定」（P.3）

- 「ウォーム リロード機能を無効にせずにシステムをリロード」（P.4）

ウォーム リロードの設定

この作業では、グローバル コンフィギュレーション モードでウォーム リロード用にルータを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **warm-reboot** [**count** *number*] [**uptime** *minutes*]
4. **exit**
5. **show warm-reboot**

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。 • 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： `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。
ステップ 3	**warm-reboot** [**count** *number*] [**uptime** *minutes*] 例： `Router(config)# warm-reboot count 10 uptime 10`	ルータのウォーム再起動をイネーブルにします。 • **count** *number*：介入するコールド再起動間で許可されたウォーム再起動の最大数。有効な値の範囲は、1 ～ 50 です。デフォルト値は 5 回です。 • **uptime** *minutes*：ウォーム再起動を試行する前に初期システム構成から例外発生までに経過しなければならない最小時間（分）。指定した時間が経過する前にシステムがクラッシュした場合、ウォーム再起動は試行されません。有効な値の範囲は、0 ～ 120 分です。デフォルト値は 5 分です。 **（注）** ウォーム再起動がイネーブルになると、ウォーム再起動は初期化されたメモリのコピーが必要であるため、次回のコールド再起動までイネーブルになりません。
ステップ 4	**exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	**show warm-reboot** 例： `Router# show warm-reboot`	（任意）試行したウォーム再起動の統計情報を表示します。

ウォーム リロード機能を無効にせずにシステムをリロード

warm-reboot グローバル コマンドを設定した後に **reload** コマンドを発行すると、コールド起動が実行されます。したがって、システムをリロードし、ウォーム再起動機能を上書きしない場合は、**warm** キーワードを指定して **reload** コマンドを実行する必要があります。この作業を使用して、システムをリロードしながらウォーム再起動するようにルータを設定します。

手順の概要

1. **enable**
2. **reload** [[**warm**] *text* | [**warm**] **in** [*hh*:]*mm* [**text**] | [**warm**] **at** *hh*:*mm* [*month day* | *day month*] [*text*] | [**warm**] **cancel**]
3. **show 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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**reload** [[**warm**] *text*	[**warm**] **in** [*hh*:]*mm* [*text*]	[**warm**] **at** *hh*:*mm* [*month day*	*day month*] [*text*]	[**warm**] **cancel**] 例： `Router# reload warm at 10:30`	オペレーティング システムをリロードします。 ルータのリロード時にウォーム再起動機能を上書きしない場合は、**warm** キーワードを発行する必要があります。
ステップ 3	**show reload** 例： `Router# show reload`	ルータのリロード ステータスを表示します。

Cisco IOS ウォーム リロードの設定例

ここでは、次の設定例を示します。

- 「ウォーム リロードの設定：例」（P.4）

ウォーム リロードの設定：例

次に、ウォーム再起動をイネーブルにして検証する例を示します。

```
Router#(config) warm-reboot count 10 uptime 10
Router#(config) exit
!
Router# show warm-reboot

Warm Reboot is enabled

Statistics:
```

```
10 warm reboots have taken place since the last cold reboot
XXX KB taken up by warm reboot storage
```

その他の関連資料

ここでは、ウォーム リロード機能に関する関連資料について説明します。

関連資料

関連項目	参照先
ルータの再起動に関する詳細	『*Rebooting and Reloading - Configuring Image Loading Characteristics*』
その他の起動コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

シスコのテクニカル サポート

説明	リンク
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **reload**
- **show warm-reboot**
- **warm-reboot**

用語集

コールド再起動：Cisco IOS イメージをリロードするプロセス。ROMMON がフラッシュなどのストレージ デバイスからメイン メモリに設定されたイメージをコピーします。この後に、イメージが解凍され、実行が開始します。

ウォーム再起動：ROMMON 介入なしで Cisco IOS イメージをリロードするプロセス。イメージが以前メモリに保存したコピーから読み取り / 書き込みデータを復元し、実行を開始します。コールド再起動とは異なり、このプロセスではフラッシュからメモリへのコピーやイメージの自己解凍は必要ありません。

（注） この用語集に記載されていない用語については、『*Internetworking Terms and Acronyms*』を参照してください。

ウォーム リロードの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　ウォーム リロードの機能情報

機能名	リリース	機能情報
ウォーム リロード	12.3(2)T 12.2(18)S 12.2(27)SBC	ウォーム リロード機能では、ストレージからイメージを読み取らずにルータをリロードできます。 この機能に関する詳細については、次の各項を参照してください。 • 「ウォーム リロードについて」 • 「ウォーム リロードの使用方法」

Cisco IOS Auto-Upgrade Manager の設定

Cisco IOS Auto-Upgrade Manager（AUM）機能を使用すると、新しい Cisco IOS イメージを指定、ダウンロード、アップグレードするための単純なインターフェイスが利用できるようになり、ソフトウェア イメージのアップグレード プロセスが単純化されます。

Auto-Upgrade Manager の指示に従ってプロセスを進めることにより、対話モードで新しい Cisco IOS イメージにアップグレードできます。また、単一の Cisco IOS コマンドまたは一連のコマンドを実行してアップグレードを行うこともできます。3 つの方法すべてで、ウォーム アップグレード機能を使用してアップグレードが行われ、ダウンタイムが最小化されます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース 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、「Cisco IOS Auto-Upgrade Manager の機能情報」（P.13）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Cisco IOS Auto-Upgrade Manager のための前提条件

- シスコからダウンロードするために、ルータ上で DNS サーバの IP アドレスを設定する必要があります。詳細については、「DNS サーバの IP アドレスの設定：例」（P.10）および「関連資料」（P.11）を参照してください。
- シスコからダウンロードするために、ルータ上でシスコの Web サイト（www.cisco.com）から取得した Secure Socket Layer（SSL）証明書を設定する必要があります。この設定は、シスコ以外のサーバからダウンロードする場合は不要です。詳細については、「シスコからのダウンロードのための SSL 証明書の設定」（P.5）および「関連資料」（P.11）を参照してください。
- 暗号化 Cisco IOS ソフトウェア イメージをダウンロードする場合は、暗号化ソフトウェアのダウンロードのために、シスコシステムズに登録する必要があります。

Cisco IOS Auto-Upgrade Manager の制約事項

要求された Cisco IOS ソフトウェア イメージをロードおよび格納するための十分なメモリ リソースがルータにない場合、Cisco IOS Auto-Upgrade Manager は最後まで完了しません。Cisco IOS ソフトウェア イメージは、ルータで現在動作している Cisco IOS ソフトウェア イメージが暗号化イメージの場合にだけ www.cisco.com からダウンロードできます。

Cisco IOS Auto-Upgrade Manager について

Cisco IOS Auto-Upgrade Manager を使用するには、次の概念について理解しておく必要があります。

- 「Cisco IOS Auto-Upgrade Manager の概要」（P.2）
- 「シスコの Web サイトからの特定の Cisco IOS ソフトウェア イメージのダウンロード」（P.4）
- 「シスコ以外のサーバからの特定の Cisco IOS ソフトウェア イメージのダウンロード」（P.4）
- 「対話型およびシングル コマンド ライン モード」（P.5）

Cisco IOS Auto-Upgrade Manager の概要

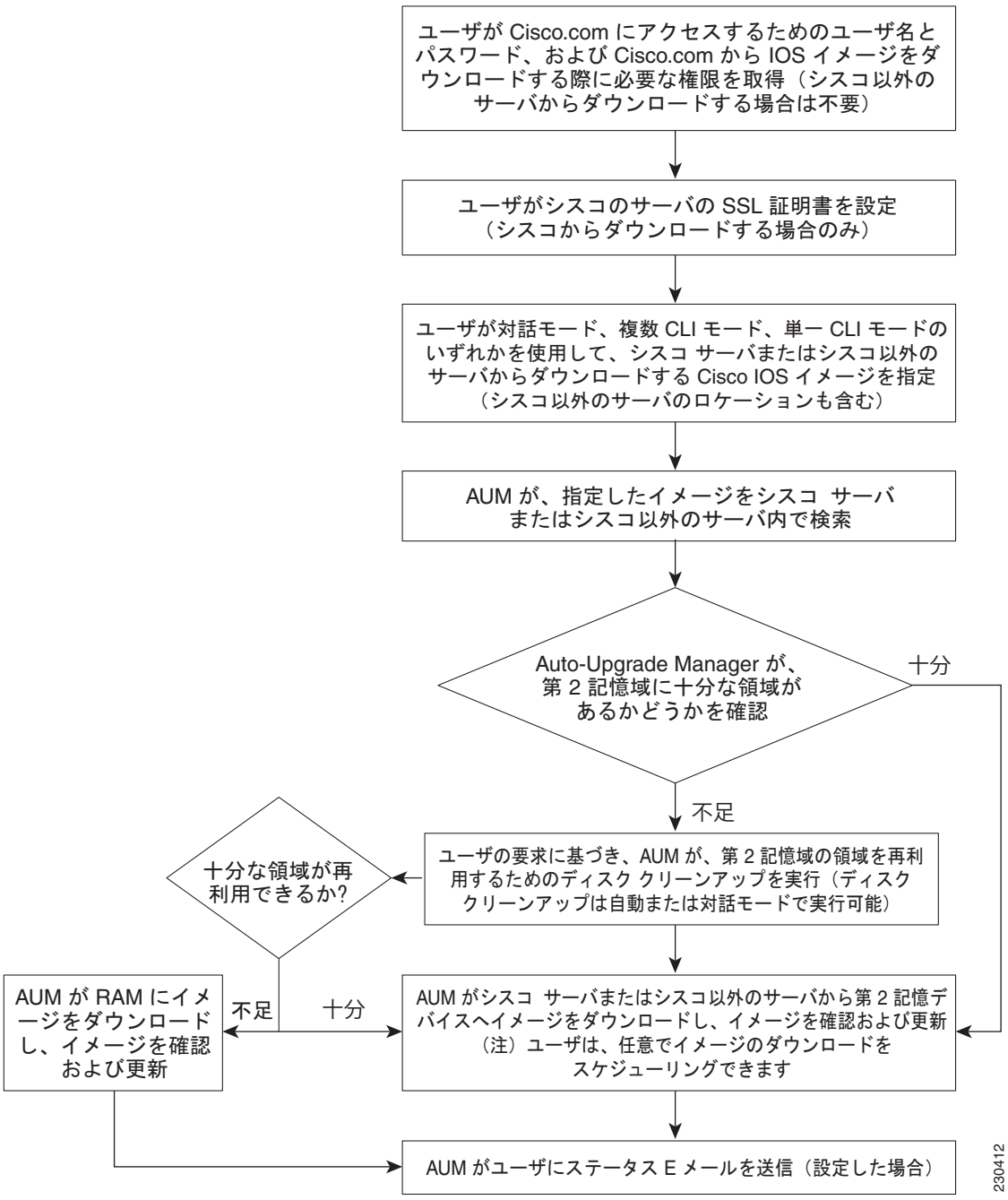
Cisco IOS Auto-Upgrade Manager は、新しい Cisco IOS ソフトウェア イメージのアップグレード プロセスを効率化します。Cisco IOS Auto-Upgrade Manager は、Command-Line Interface（CLI; コマンドライン インターフェイス）を通じて実行できます。AUM では、ルータをシスコの Web サイト（www.cisco.com）に接続し、cisco.com のユーザ名とパスワードを認証のために送信できます。認証後、ルータは、ユーザが指定した Cisco IOS ソフトウェア イメージの名前をシスコのサーバに渡します。シスコのサーバは、Cisco IOS ソフトウェア イメージの完全な URL をルータに返します。

ルータで設定された Cisco IOS Auto-Upgrade Manager は、Cisco IOS ソフトウェア イメージへのアップグレード プロセス全体を管理します。AUM は、次の作業を実行することにより、ユーザによって指定された時刻に、ソフトウェア イメージを使用してルータをアップグレードします。

- Cisco IOS ソフトウェア イメージの検索とダウンロード
- すべての要件の確認
- 第 2 記憶域の管理
- Cisco IOS ソフトウェア イメージの検証
- ウォームアップグレードのスケジューリング

図 1 に、Cisco IOS Auto-Upgrade Manager のワークフローを示します。

図 1　　Cisco IOS Auto-Upgrade Manager のワークフロー



（注） ルータが、ユーザが指定した Cisco IOS ソフトウェア イメージのロードに失敗すると、コンソール ウィンドウと syslog バッファに、エラーの理由を示すエラー メッセージが表示されます。ユーザが暗号化ソフトウェアをダウンロードする許可を持っていない場合、このサービスに登録するようユーザに求めるエラー メッセージが生成されます。

同様に、いずれかの CLI 設定文がブート時にパーサーに理解されない場合、エラー メッセージが生成され、無効な設定行のログが nvram:invalid-config ファイルに格納されます。このエラー メッセージは、ユーザが指定した Cisco IOS ソフトウェア イメージが、以前の Cisco IOS ソフトウェア イメージと同じ機能セットをサポートしていないことを示します。

ルータに、両方のイメージをサポートするために十分な第 2 記憶域がなく、新しいイメージのアップグレードに成功した場合、再度シスコのサーバに接続して、第 2 記憶域に Cisco IOS ソフトウェア イメージをダウンロードします。このプロセスにより既存のイメージが消去されます。

シスコの Web サイトからの特定の Cisco IOS ソフトウェア イメージのダウンロード

www.cisco.com から特定の Cisco IOS ソフトウェア イメージをダウンロードできます。AUM は、セキュアな接続のために Secure Socket Layer（SSL）を使用するため、ユーザ側で証明書を設定する必要があります。ルータは、Cisco IOS ソフトウェア イメージの名前を、www.cisco.com サーバにログインするためのユーザ名およびパスワードとともに渡します。シスコのサーバは、特定の Cisco IOS ソフトウェア イメージの完全な URL をルータに返します。

Cisco IOS Auto-Upgrade Manager は、ユーザが指定した Cisco IOS ソフトウェア イメージを自動的に www.cisco.com からダウンロードして確認し、ダウンロードしたイメージでルータをアップグレードします。

（注） Intelligent Download Application（IDA）は、AUM に対するシスコのインターフェイスであり、AUM に関しては *シスコのサーバ*と同じ意味で使用されます。

また、Cisco IOS Auto-Upgrade Manager では、次のオプション サービスが提供されます。

- ディスク クリーンアップ ユーティリティ
- アップグレードのスケジューリング

これらのサービスは、シスコのサーバとシスコ以外のサーバからのダウンロードに対して、対話モードとコマンド ラインモードの両方で使用できます。

シスコ以外のサーバからの特定の Cisco IOS ソフトウェア イメージのダウンロード

ローカルまたはシスコ以外の TFTP サーバまたは FTP サーバに存在する Cisco IOS ソフトウェア イメージをダウンロードできます。FTP ダウンロードのための FTP ユーザ名とパスワードは、**ip ftp username** および **ip ftp password** 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指定します。Cisco IOS Auto-Upgrade Manager では、特定の Cisco IOS ソフトウェアのシスコ以外のサーバからのダウンロードとウォーム アップグレード サービスのプロセスが自動化されます。また、新しい Cisco IOS ソフトウェアをダウンロードするために必要な領域が十分でない場合に使用する、ファイルを削除するためのディスク クリーンアップ ユーティリティも提供されています。

対話型およびシングル コマンド ライン モード

CLI を使用するか、次のユーザ インターフェイスを通じて、特定の Cisco IOS ソフトウェア イメージを www.cisco.com からダウンロードできます。

- 「対話モード」（P.5）
- 「シングル コマンド ライン モード」（P.5）

対話モード

Auto-Upgrade Manager に従って、対話モードで新しい Cisco IOS イメージにアップグレードできます。自動アップグレードを選択すると、対話モードでいくつかの問題に答えるだけでデバイスのアップグレードが完了します。対話モードを開始するには、オプションなしで **upgrade automatic** コマンドを実行します。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

シングル コマンド ライン モード

対話型でないシングル ライン CLI は、上級ユーザ向けです。**upgrade automatic getversion** コマンドを使用し、必要なすべての引数を指定することで、シスコのサーバまたはシスコ以外のサーバから新しい Cisco IOS ソフトウェア イメージをダウンロードし、アップグレードできます。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

対話モードとシングル ライン CLI モードは、シスコのサーバとシスコ以外のサーバからのダウンロードに適用されます。

Cisco IOS Auto-Upgrade Manager を使用した Cisco IOS ソフトウェア イメージのアップグレード方法

ここでは、次の各手順について説明します。

- 「シスコからのダウンロードのための SSL 証明書の設定」（P.5）（シスコからのダウンロードで必要）
- 「Cisco IOS Auto-Upgrade Manager の設定」（P.7）（必須）
- 「Cisco IOS ソフトウェア イメージのダウンロード」（P.8）（任意）
- 「新しい Cisco IOS ソフトウェア イメージを使用したルータのリロード」（P.8）（任意）
- 「Cisco IOS ソフトウェア イメージのリロードの取り消し」（P.9）（任意）

シスコからのダウンロードのための SSL 証明書の設定

この作業では、シスコからダウンロードするための SSL 証明書を設定します。

前提条件

SSL 証明書を、cisco.com からダウンロードするように設定しておく必要があります。証明書は、セキュアな HTTP 通信のために必要です。SSL 証明書は、シスコの Web サイト（www.cisco.com）からダウンロードしてルータ上で設定します。

シスコの Web サイトから SSL 証明書を取得するには、次の作業を実行します。

1. Internet Explorer（IE）の [Tools] メニューから [Internet Options] を選択します。
2. [Advanced] タブで [Warn if changing between secure and not secure mode.] を選択します。
3. IE に URL として https://www.cisco.com/ と入力します。セキュリティ警告のポップアップ ボックスが表示されたら、「You are about to leave a secure Internet connection.Do you want to continue?」という質問に対して [No] をクリックします。
4. IE のステータス バーにある鍵のアイコンをダブルクリックします。これにより、証明書の詳細を示すダイアログ ボックスが表示されます。
5. [Certification Path] タブをクリックします。タブには証明書チェーンが表示されます。
6. CA 証明書をそれぞれ選択して [View Certificate] をクリックします。これにより、証明書の詳細を示すウィンドウが表示されます。
7. 表示された証明書ウィンドウの [Details] タブを選択して、[Copy to File] をクリックします。これにより、証明書のエクスポート ウィザードが開きます。
8. 証明書を Base-64 符号化形式でファイル（cisco.cert など）に保存します。
9. cisco.cert ファイルをメモ帳で開き、ルータを設定するために必要な証明書データを取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal**
5. **revocation-check none**
6. **exit**
7. **crypto ca authenticate** *name*

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。 • 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： `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。
ステップ 3	**crypto pki trustpoint** *name* 例： `Router(config)# crypto pki trustpoint cisco_ssl_cert`	Certification Authority（CA; 認証局）を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 4	**enrollment terminal** 例： `Router(ca-trustpoint)# enrollment terminal`	コンソール端末上に証明書要求を表示し、発行された証明書データを端末上に入力できるようにします。

	コマンドまたはアクション	目的
ステップ 5	**revocation-check none** 例： `Router(ca-trustpoint)# revocation-check none`	証明書の確認が必要ないことを指定します。
ステップ 6	**exit** 例： `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto ca authenticate** *name* 例： `Router(config)# crypto ca authenticate cisco_ssl_cert`	CA の自己署名証明書を取得することで、CA がルータに対して認証されます。

Cisco IOS Auto-Upgrade Manager の設定

Cisco IOS Auto-Upgrade Manager を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**}
4. **autoupgrade ida url** *url*
5. **autoupgrade status email** {**recipient** *email-address* | **smtp-server** *name-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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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： `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。
ステップ 3	**autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**} 例： `Router(config)# autoupgrade disk-cleanup crashinfo`	Cisco IOS Auto-Upgrade Manager ディスク クリーンアップ ユーティリティを設定します。

	コマンドまたはアクション	目的
ステップ 4	**autoupgrade ida url** *url* 例： `Router(config)# autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl`	Cisco IOS Auto-Upgrade Manager によってイメージ ダウンロード要求が送信される、www.cisco.com 上で動作しているシスコのサーバの URL を設定します。 **（注）** この手順は、デフォルトの URL が変更された場合にだけ必要です。
ステップ 5	**autoupgrade status email** {**recipient** *email-address* | **smtp-server** *name-address*} 例： `Router(config)# autoupgrade status email smtp-server smtpserver.abc.com`	ルータによるステータス E メールの送信先となる、E メール アドレスと送信 E メール サーバを設定します。

Cisco IOS ソフトウェア イメージのダウンロード

Cisco IOS ソフトウェア イメージをシスコの Web サイト（www.cisco.com）またはシスコ以外のサーバからダウンロードするには、この作業を実行します。

手順の概要

1. **enable**
2. **upgrade automatic getversion** {**cisco username** *username* **password** *password* **image** *image* | *url*} [**at** *hh*:*mm* | **now** | **in** *hh*:*mm*] [**disk-management** {**auto** | **confirm** | **no**}]

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。 • 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	**upgrade automatic getversion** {**cisco username** *username* **password** *password* **image** *image* | *url*} [**at** *hh*:*mm* | **now** | **in** *hh*:*mm*] [**disk-management** {**auto** | **confirm** | **no**}] 例： `Router# upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin at now disk-management auto`	www.cisco.com またはシスコ以外のサーバから、直接イメージをダウンロードします。

新しい Cisco IOS ソフトウェア イメージを使用したルータのリロード

新しい Cisco IOS ソフトウェア イメージを使用してルータをリロードするには、ここで説明する作業を実行します。

手順の概要

1. **enable**

2. **upgrade automatic runversion** [**at** *hh*:*mm* | **now** | **in** *hh*:*mm*]

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。 • 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	**upgrade automatic runversion** [**at** *hh*:*mm* | **now** | **in** *hh*:*mm*] **例：** `Router# upgrade automatic runversion at 7:30`	新しいイメージでルータをリロードします。 **（注）** また、**upgrade automatic getversion** コマンドを使用して、新しい Cisco IOS ソフトウェア イメージでルータをリロードすることもできます。ただし、**upgrade automatic getversion** コマンドを使用してすでに Cisco IOS ソフトウェア イメージをダウンロードしてある場合は、**upgrade automatic runversion** コマンドを使用してルータをリロードする必要があります。

Cisco IOS ソフトウェア イメージのリロードの取り消し

特定の Cisco IOS ソフトウェア イメージのスケジューリングされたリロードを取り消すには、この作業を実行します。

次の状況でイメージのリロードを取り消すことができます。

- ルータをリロードするようスケジューリングされた時刻が十分でない場合。
- ルータを新しいイメージにアップグレードしない場合。

手順の概要

1. **enable**
2. **upgrade automatic abortversion**

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。 • 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	**upgrade automatic abortversion** **例：** `Router# upgrade automatic abortversion`	Cisco IOS ソフトウェア イメージのアップグレードを取り消します。

Cisco IOS Auto-Upgrade Manager の設定例

ここでは、次の設定例について説明します。

DNS サーバの IP アドレスの設定：例

Cisco IOS Auto-Upgrade Manager を設定する前に、ルータ上で DNS サーバの IP アドレスを設定する必要があります。このイベント シーケンスにより、ルータは **ping** コマンドで IP アドレスではなくホスト名を使用できるようになります。ルータ上で DNS サーバの IP アドレスを設定した後、シスコの Web サイト（www.cisco.com）に正常に ping できるようになります。このアクションにより、ルータがインターネットに接続されていることも確認できます。

次に、ルータ上で DNS サーバの IP アドレスを設定する例を示します。DNS サーバの IP アドレスを設定した後、www.cisco.com に正常に ping できるようになります。

```
configure terminal
 ip domain name mycompany.com
 ip name-server 10.2.203.1
 end
  ping www.cisco.com
```

シスコからのダウンロードのための SSL 証明書の設定：例

Cisco IOS Auto-Upgrade Manager を使用してシスコの Web サイトからイメージをダウンロードする前に、ルータ上でシスコのサーバの SSL 証明書を設定する必要があります。

次に、SSL 証明書を設定する例を示します。

```
configure terminal
 crypto pki trustpoint cisco_ssl_cert
  enrollment terminal
  revocation-check none
  exit
 crypto ca authenticate cisco_ssl_cert

!Enter the base 64 encoded CA certificate and end this with a blank line or the word quit.
!The console waits for the user input. Paste the SSL certificate text and press Return.
-----BEGIN CERTIFICATE-----

<The content of the certificate>

-----END CERTIFICATE-----

!Trustpoint 'cisco_ssl_cert' is a subordinate CA and holds a non self signed cert
!Trustpoint 'cisco_ssl_cert' is a subordinate CA.
!but certificate is not a CA certificate.
!Manual verification required
!Certificate has the following attributes:
      ! Fingerprint MD5: 49CE9018 C0CC41BA 1D2FBEA7 AD3011EF
      ! Fingerprint SHA1: A88EAA5D 73D63CB7 BF25197B 9C35ED97 023BB57B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Cisco IOS Auto-Upgrade Manager の設定：例

次に、ルータ上で Cisco IOS Auto-Upgrade Manager を設定する例を示します。

```
configure terminal
autoupgrade disk-cleanup crashinfo
autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl
autoupgrade status status email smtp-server
```

その他の関連資料

次の項では、Cisco IOS Auto-Upgrade Manager の関連資料について説明します。

関連資料

関連項目	参照先
Cisco IOS Auto-Upgrade Manager 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、使用ガイドライン、および例	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco ルータでの DNS の設定	『*Configuring DNS on Cisco Routers* technical note』
ウォーム アップグレード	『*Warm Upgrade* feature module』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする – Product Alert の受信登録 – Field Notice の受信登録 – Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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

Cisco IOS Auto-Upgrade Manager の機能情報

表 1 に、このモジュールに記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.4(15)T 以降のリリースで導入または変更された機能だけを示します。

すべてのコマンドがご使用の Cisco IOS ソフトウェア リリースで使用できるとは限りません。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 により、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していない限り、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Cisco IOS Auto-Upgrade Manager の機能情報

機能名	リリース	機能情報
Cisco IOS Auto-Upgrade Manager	12.4(15)T	Cisco IOS Auto-Upgrade Manager を使用すると、新しい Cisco IOS イメージを指定、ダウンロード、アップグレードするための単純なインターフェイスが利用できるようになり、ソフトウェア イメージのアップグレード プロセスが単純化されます。 12.4(15)T で、この機能が Cisco 1800、Cisco 2800、および Cisco 3800 シリーズ ルータに追加されました。 この機能によって次のコマンドが追加/変更されました。**autoupgrade disk-cleanup**、**autoupgrade ida url**、**autoupgrade status email**、**debug autoupgrade**、**show autoupgrade configuration unknown**、**upgrade automatic abortversion**、**upgrade automatic getversion**、**upgrade automatic runversion**

用語集

CLI：コマンドライン インターフェイス

IDA またはシスコ サーバ：Intelligent Download Application

Cisco IOS：Cisco Internetworking Operating System

システム メモリのメンテナンス

システム メモリのメンテナンス

この章では、さまざまなタイプのメモリをルータで保守および使用する方法について説明します。このマニュアルは、Cisco IOS Release 12.2 に適用されます。

この章に記載されているメモリ コマンドの詳細については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「Router Memory Commands」の章を参照してください。この章で説明される他のコマンドの資料を検索するには、『*Cisco IOS Command Reference Master Index*』を使用するかオンラインで検索します。

特定の機能がサポートされているハードウェアまたはソフトウェアを識別するには、Cisco.com にある Feature Navigator を使用して機能に関する情報を検索するか、または特定のリリースのソフトウェア リリース ノートを参照してください。詳細については、「About Cisco IOS Software Documentation」の章の「Identifying Platform Support for Cisco IOS Software Features」の項を参照してください。

メモリ タイプおよび機能の概要

ルータには、イメージ、コンフィギュレーション ファイルおよびマイクロコードを格納できる場所が多数あります。ルーティング デバイスに含まれるメモリのタイプ、ファイルを格納（保存）できる場所、イメージおよびブート イメージのデフォルトの場所の詳細については、ご使用のハードウェアのマニュアルを参照してください。ここでは、次のメモリ タイプについて説明します。

- 「ダイナミック ランダムアクセス メモリ（DRAM）」
- 「EPROM」
- 「NVRAM」
- 「フラッシュ メモリ」

ダイナミック ランダムアクセス メモリ（DRAM）

Dynamic Random-Access Memory（DRAM; ダイナミック ランダムアクセス メモリ）には、次の 2 種類のメモリがあります。

- プライマリ、メイン、またはプロセッサ メモリ。CPU で Cisco IOS ソフトウェアを実行し、実行コンフィギュレーションおよびルーティング テーブルを保持するために予約されています。
- 共有、パケット、または I/O メモリ。ルータのネットワーク インターフェイスにより送受信されるデータをバッファに入れます。

Cisco 3600 シリーズ ルータで、メイン メモリおよび共有メモリに割り当てる DRAM の割合を設定するには、**memory-size iomem** コマンドを使用します。

DRAM は通常 Dual in-line Memory Module（DIMM）に搭載されます。

EPROM

Erasable Programmable Read-Only Memory（EPROM）は単純に ROM と呼ばれることもあります。シスコ デバイスでは、EPROM には次のものが含まれます。

- ROM モニタ ソフトウェア。ROM のトラブルシューティング用のユーザ インターフェイスを提供します。
- ブート ローダ/ヘルパー ソフトウェア。有効な Cisco IOS イメージをフラッシュ メモリで検出できない場合にルータ ブートをサポートします。

NVRAM

Non-Volatile Random-Access Memory（NVRAM; 不揮発性 RAM）は、次の情報を格納します。

- クラス A フラッシュ ファイル システム プラットフォームを除く、すべてのプラットフォームのスタートアップ コンフィギュレーション ファイル（クラス A フラッシュ ファイル システム プラットフォームでは、スタートアップ コンフィギュレーションの場所は、CONFIG_FILE 環境変数により異なります）。
- ソフトウェア コンフィギュレーション レジスタ。ルータのブート時に使用するイメージの判別に使用されます。

フラッシュ メモリ

フラッシュ メモリは、Cisco IOS ソフトウェア イメージを格納します。ほとんどのプラットフォームでは、ブート イメージまたはコンフィギュレーション ファイル、あるいはこれらの両方を格納できます。

ハードウェア プラットフォームによっては、フラッシュ メモリを EPROM、Single In-line Memory Module（SIMM; シングル インライン メモリ モジュール）Dual in-line Memory Module（DIMM）、フラッシュ メモリ カードとして使用できます。各プラットフォームで使用できるフラッシュ メモリのタイプについては、該当するハードウェア インストールおよびメンテナンス ガイドを参照してください。

プラットフォームによっては、フラッシュ メモリを次の形式で使用できます。

- 内部フラッシュ メモリ
  - 内部フラッシュ メモリにはシステム イメージが含まれます。
  - プラットフォームによっては、1 つのインライン メモリ モジュール（つまり 1 つの SIMM）に複数バンクのフラッシュ メモリが使用されます。SIMM で 2 バンクのフラッシュ メモリが使用される場合、これは、*デュアル バンク フラッシュ メモリ*と呼ばれます。バンクは、個別の論理デバイスにパーティショニングできます。フラッシュ メモリをパーティショニングする方法については、「フラッシュ メモリのパーティショニング」の項を参照してください。
- ブートフラッシュ
  - ブートフラッシュには、通常、ブート イメージが含まれます。
  - ブートフラッシュには、ROM モニタが含まれることもあります。

- フラッシュ メモリ PC カードまたは PCMCIA カード

  Personal Computer Memory Card International Association（PCMCIA; パーソナル コンピュータ メモリ カード国際協会）スロットに挿入されるフラッシュ メモリ カード。このカードは、システム イメージ、ブート イメージおよびコンフィギュレーション ファイルの格納に使用されます。

（注） Cisco 3600 シリーズおよび Cisco 7000 ファミリなど、一部のプラットフォームによっては、いくつかの場所からイメージをブートし、コンフィギュレーション ファイルを読み込むことができます。このようなシステムでは、特殊な ROM モニタ環境変数を使用して、ルータがさまざまな機能で使用するイメージおよびコンフィギュレーション ファイルの場所とファイル名を指定します。

通常、Cisco ルータは、システム イメージをフラッシュ ストレージから RAM にロードし、Cisco IOS を実行します。ただし、Cisco 1600 シリーズおよび Cisco 2500 シリーズなど、一部のプラットフォームは、Cisco IOS オペレーション システムをフラッシュ メモリから直接実行します。このようなプラットフォームは、run-from-Flash メモリ システムです。

フラッシュ メモリをパーティショニングする場合、再配置可能なイメージを使用する必要があります。再配置可能なイメージは、フラッシュの任意の場所から実行でき、イメージを任意の場所にダウンロードできます。再配置不可能なイメージを再配置可能なイメージにアップグレードする場合、イメージがフラッシュ メモリの最初のファイルとしてダウンロードされるように、ダウンロード中にフラッシュ メモリを消去する必要があります。Cisco IOS リリース 11.0 以降の run-from-Flash プラットフォームでは、すべてのイメージが再配置可能です。イメージがフラッシュから実行される（run-from-Flash）イメージか、再配置可能かを判別するには、「システム イメージのロードおよびメンテナンス」の章の「イメージの命名規則」の項を参照してください。

フラッシュ メモリは、偶発的な消去やプログラミング変更に対する書き込み保護を提供します。プラットフォームによっては、書き込み保護ジャンパがあります。このジャンパを取り外すと、フラッシュ メモリのプログラミング変更を防ぐことができます。プログラミングが必要な場合、このジャンパを取り付けます。また、プラットフォームによっては、フラッシュ メモリ カードで書き込み保護が提供されています。この機能は、データの保護に使用できます。フラッシュ メモリ カードにデータを書き込むには、このスイッチを*非保護*に設定する必要があります。セキュリティ ジャンパおよび書き込み保護スイッチについては、ご使用のハードウェアのマニュアルを参照してください。

（注） システムの内部フラッシュおよびフラッシュ メモリ カードは、フラッシュ メモリの連続するバンクとして使用することはできません。

システム メモリ メンテナンスの作業リスト

次に示す項では、フラッシュ メモリに関する作業を実行できます。

- 「システム メモリ情報の表示」
- 「Cisco 3600 シリーズでの DRAM メモリの再割り当て」
- 「フラッシュ メモリのパーティショニング」
- 「フラッシュ ロード ヘルパーを使用した Run-from-Flash システムでのソフトウェアのアップグレード」
- 「フラッシュ メモリのフォーマット」

この章で示す作業は、変更が必要な設定が最小であることを前提としています。

システム メモリ情報の表示

システム メモリに関する情報を表示するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **show** *flash-filesystem*: [**all** | **chips** | **filesys**]	クラス A ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show** *flash-filesystem*: [**partition** *number*] [**all** | **chips** | **detailed** | **err** | **summary**]	クラス B ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show** *flash-filesystem*:	クラス C ファイル システムのフラッシュ メモリに関する情報を表示します。
Router# **show file systems**	ルータで現在サポートされているファイル システムの名前を表示します。

フラッシュ メモリのパーティショニング

ほとんどのクラス B フラッシュ ファイル システムでは、フラッシュ メモリのバンクを個別の論理デバイスにパーティショニングできます。これにより、ルータは、さまざまな種類のソフトウェア イメージを複数保持および保守できるようになります。このパーティショニングにより、ソフトウェアをフラッシュ メモリに書き込みながら、フラッシュ メモリの別のバンクでソフトウェアを実行できます。

パーティショニングをサポートするシステム

フラッシュ メモリをパーティショニングするには、少なくとも 2 バンクのフラッシュ メモリが必要です。バンクは、4 チップのセットです。また、システムが、2 バンクのフラッシュ メモリを使用するシングル SIMM をサポートしている必要があります。パーティショニングの最小サイズは、バンクのサイズです。

（注） CiscoFlash MIB 変数は、パーティショニングされたフラッシュをサポートしています。

フラッシュ メモリをパーティショニングするメリット

フラッシュ メモリをパーティショニングすると、次のようなメリットがあります。

- システムでは、1 つの論理フラッシュ メモリ デバイスを使用するのではなく、パーティショニングすることで、フラッシュ メモリのさまざまなファイルをより簡潔に管理できます。これは、特に、フラッシュ メモリのサイズが大きい場合に有効です。
- フラッシュ メモリからコードを実行するシステムでは、パーティショニングすることで、フラッシュ メモリ バックのファイル システムに新しいイメージをダウンロードしつつ、他のバンクのファイル システムから、イメージを実行することができます。ダウンロードは簡単で、ネットワーク停止やダウンタイムも発生しません。ダウンロードが完了したら、必要なときに、新しいイメージに切り替えることができます。
- 1 つのシステムで 2 種類の異なるイメージを保持し、その 1 つをもう一方のバックアップとして使用できます。そのため、ダウンロードされたイメージが何らかの理由でブートできない場合、それよりも前に実行していた正常なイメージを利用できます。各バンクは、個別のデバイスとして扱われます。

フラッシュ ロード ヘルパーとデュアル フラッシュ バンク

フラッシュ ロード ヘルパーは、フラッシュ メモリのシングル バンクが 1 つある run-from-Flash システムでシステム ソフトウェアをアップグレードできるソフトウェア オプションです。これは、1 つの SIMM で 2 バンクのフラッシュ メモリを必要とする、デュアル バンク フラッシュよりも低コストなソフトウェア アップグレード ソリューションです。フラッシュ ロード ヘルパーは、Cisco 2500 シリーズ、Cisco 3000、Cisco 5200 など、run-from-Flash プラットフォームだけで使用できます。

次のいずれかの場合、フラッシュを 2 つのバンクにパーティショニングせずに、フラッシュ ロード ヘルパーを使用します。

- 現在のシステム イメージが実行されているバンクと同じバンクに新しいファイルをダウンロードする。
- バンクよりサイズの大きいファイルをダウンロードするため、シングル バンク モードに切り替える。
- シングル バンク Flash SIMM が 1 つだけインストールされている。この場合、フラッシュ ロード ヘルパーは、ソフトウェアのアップグレードに最適です。

フラッシュ ロード ヘルパーの使用については、「フラッシュ ロード ヘルパーを使用した Run-from-Flash システムでのソフトウェアのアップグレード」の項を参照してください。

フラッシュ メモリのパーティショニング

フラッシュ メモリをパーティショニングするには、グローバル コンフィギュレーション モードで、次のコマンドをいずれかの形式で使用します。

コマンド	目的
`Router(config)# partition flash partitions [size1 size2]`	フラッシュ メモリをパーティショニングします。
`Router(config)# partition flash-filesystem: [number-of-partitions] [partition-size]`	Cisco 1600 および 3600 シリーズでフラッシュ メモリをパーティショニングします。

この作業が正常に行われるのは、システムに少なくとも 2 バンクのフラッシュ メモリがある場合だけです。パーティショニングにより、フラッシュ メモリの既存のファイルがパーティション間で分割されることはありません。

Cisco 1600 シリーズおよび Cisco 3600 シリーズ以外のすべてのプラットフォームでは、フラッシュ メモリは 2 つのパーティションだけにパーティショニングできます。

Cisco 1600 シリーズおよび Cisco 3600 シリーズでは、フラッシュ メモリ デバイスで作成できるパーティションの数は、デバイスのバンクの数と同じになります。フラッシュ メモリ デバイスのバンクの数を表示するには、**show** *flash-filesystem*: **all** コマンドを入力します。設定するパーティション サイズ エントリの数は、指定するパーティションの数と同じでなければなりません。たとえば、**partition slot0: 2 8 8** コマンドは、各サイズ 8 MB の 2 つのパーティションを設定します。最初の 8 は、最初のパーティションに対応し、2 番目の 8 は、2 番目のパーティションに対応します。

（注） このパーティションを削除するには、**no partition** コマンドを使用します。

フラッシュ ロード ヘルパーを使用した Run-from-Flash システムでのソフトウェアのアップグレード

フラッシュ ロード ヘルパーは、フラッシュ メモリのシングル バンクが 1 つある run-from-Flash システムでシステム ソフトウェアをアップグレードできるソフトウェア オプションです。これは、1 つの SIMM で 2 バンクのフラッシュ メモリを必要とする、デュアル バンク フラッシュよりも低コストなソフトウェア アップグレード ソリューションです。

フラッシュ ロード ヘルパーのソフトウェア アップグレード プロセスは簡単で、追加のハードウェアも必要ありませんが、ネットワーク ダウンタイムが若干発生します。フラッシュから実行しているシステム イメージは、ブート ROM がフラッシュ ロード ヘルパーをサポートしている場合だけ、フラッシュ ロード ヘルパーを使用できます。それ以外の場合、フラッシュ アップグレードを手動で実行する必要があります。「Manually Boot from Flash Memory」の項を参照してください。

フラッシュ ロード ヘルパーは、ROM ベース イメージのリロード、ソフトウェアのフラッシュ メモリへのダウンロード、フラッシュ メモリ内のシステム イメージのリブートを行う自動化された手順です。フラッシュ ロード ヘルパーは、チェックおよび検証を行い、フラッシュ アップグレードを最大限成功させ、フラッシュ メモリが消去された状態、またはブートできないファイルが書き込まれている状態にすることを最小限に押さえます。

run-from-Flash システムでは、ソフトウェア イメージは、RAM ではなくフラッシュ EPROM に格納され、ここから実行されます。これにより、メモリ コストが軽減します。run-from-Flash システムには、イメージを保持できるだけの十分なフラッシュ EPROM、およびルーティング テーブルとデータ構造を保持できるだけの十分なメイン システム RAM が必要です。ただし、フル イメージは RAM に常駐しないため、run-from-RAM システムと同じ容量のメイン システム RAM は必要ありません。run-from-Flash システムには、Cisco 2500 シリーズおよび一部の Cisco 3000 シリーズが含まれます。

フラッシュ ロード ヘルパーの機能

フラッシュ ロード ヘルパーは、次の機能を実行します。

- 指定サーバの指定ソース ファイルへのアクセスを確認してから、フラッシュ メモリを消去し、実際のアップグレードの ROM イメージにリロードします。
- ダウンロードされるイメージがシステムに適切でない場合、警告します。
- システムで自動ブートが設定されていないで、ユーザがコンソール端末上にない場合、フラッシュ アップグレードの ROM イメージへのリロードを防ぎます。アップグレード中に重大な障害が発生した場合、フラッシュ ロード ヘルパーは、ROM モニタがコンソール端末からの入力を求めるまでシステムに強制的に待機させるのではなく、最後の手段としてブート ROM イメージを起動できます。
- フラッシュ ダウンロードは自動的に 6 回まで再試行されます。この再試行は次のように行われます。
  - 初回の試行
  - すぐに再試行
  - 30 秒後に再試行
  - ROM イメージをリロードして再試行
  - すぐに再試行
  - 30 秒後に再試行
- システム イメージを終了する前に行った設定の変更を保存できます。
- 予期せぬ接続の切断が行われないように、間もなくブート ROM イメージへの切り替えが行われることを、システムにログインしているユーザに通知します。

- フラッシュ ロード ヘルパー動作中のコンソール出力を、システム リロード前後でも保持されるバッファに記録します。バッファの内容は、実行中のイメージから取得できます。この出力は、コンソール アクセスが使用できない場合、またはダウンロード動作中に障害が発生した場合に役立ちます。

フラッシュ ロード ヘルパーは、フラッシュ メモリ パーティショニングをサポートする複数バンクのフラッシュ メモリのシステムでも使用できます。フラッシュ ロード ヘルパーを使用すると、システムがイメージを実行しているパーティションと同じパーティションに新しいファイルをダウンロードできます。

システムが 2 種類のイメージを保持できるように複数バンクのフラッシュ メモリをパーティショニングする方法については、「フラッシュ メモリのパーティショニング」の項を参照してください。

フラッシュ ロード ヘルパーを使用したファイルのダウンロード

フラッシュ ロード ヘルパーを使用して新しいファイルをフラッシュ メモリにダウンロードするには、ブート ROM がフラッシュ ロード ヘルパーをサポートしていることを確認して、特権 EXEC モードで次のいずれかのコマンドを使用します。

コマンド	目的
Router# **copy tftp: flash:** Router# **copy rcp: flash:** Router# **copy ftp: flash:**	指定のファイルをフラッシュ メモリにロードします。

Telnet セッションを使用していて、システムが手動ブートに設定されている場合（コンフィギュレーション レジストリのブート ビットがゼロの場合）、次のエラー メッセージが表示されます。

```
ERR: Config register boot bits set for manual booting
```

フラッシュ メモリ アップグレード中に重大な障害が発生した場合、このエラー メッセージにより、システムが ROM モニタ モードになり、リモート Telnet ユーザが制御できなくなる可能性が最小限に押さえられます。

システムは、イメージをフラッシュ メモリからブートできない場合、少なくともブート ROM イメージを起動しようとします。**copy:** コマンドを再実行する前に、**config-register** 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、コンフィギュレーション レジスタ ブート フィールドをゼロ以外の値に設定する必要があります。

copy コマンドは、応答する必要がある一連のプロンプトを開始します。次のようなダイアログが表示されます。

```
Router# copy tftp: flash:

************************** NOTICE ******************************
Flash load helper v1.0
This process will accept the TFTP copy options and then terminate
the current system image to use the ROM based image for the copy.
Router functionality will not be available during that time. If
you are logged in via telnet, this connection will terminate. Users
with console access can see the results of the copy operation.
****************************************************************

There are active users logged into the system.

Proceed? [confirm] y
System flash directory:
File Length  Name/status
1    2251320 abc/igs-kf.914
```

```
[2251384 bytes used, 1942920 available, 4194304 total]
Address or name of remote host [255.255.255.255]? 172.16.1.111
Source file name? abc/igs-kf.914
Destination file name [default = source name]? <Return>
Accessing file 'abc/igs-kf.914' on 172.16.1.111....
Loading from 172.16.13.111:
Erase flash device before writing? [confirm] n
File 'abc/igs-kf.914' already exists; it will be invalidated!
Invalidate existing copy of 'abc/igs-kf.914' in flash memory? [confirm] y
Copy 'abc/igs-kf.914' from TFTP server
as 'abc/igs-kf.914' into Flash WITHOUT erase? y

%SYS-5-RELOAD: Reload requested
%FLH: rxboot/igs-kf.914r from 172.16.1.111 to flash...
```

フラッシュ ロード ヘルパーの動作は、リモート サーバからシングル ブロックをコピーしようとすることで、実行中のイメージから要求を確認します。次に、フラッシュ ロード ヘルパーが実行され、システムが ROM ベースのシステム イメージをリロードします。ファイルがシステムの有効なイメージではないと思われる場合、警告が表示され、この確認が求められます。

設定が変更されたが、まだ保存されていない場合、設定を保存するよう要求されます。

```
System configuration has been modified. Save? [confirm]
```

オープン Telnet 接続を使用している場合、次のように、システム リロードが通知されます。

```
**System going down for Flash upgrade**
```

コピー プロセスが失敗すると、コピー操作が最高 3 回まで再試行されます。コピー操作の途中で失敗し、ファイルの一部だけがフラッシュ メモリに書き込まれた場合、消去操作を指定するまで、再試行によりフラッシュ メモリが消去されることはありません。一部だけ書き込まれたファイルには、削除マークが付けられ、同じ名前の新しいファイルが開きます。このプロセス中、フラッシュ メモリの空き容量がなくなると、コピー操作は終了します。

フラッシュ ロード ヘルパーがコピーを終了すると（コピー操作が成功したかどうかに関係なく）、次のように、コンフィギュレーション レジスタ ブート フィールドのビット ゼロの値に従って、自動ブートまたは手動ブートを自動的に試行します。

- ビット ゼロが 0 の場合、システムは、フラッシュ メモリからデフォルト ブートを試行して、フラッシュ メモリの最初のブート可能ファイルを読み込みます。このデフォルト ブートは、ROM モニタ プロンプトで **boot flash** コマンドを手動で入力した場合と同じです。
- ビット ゼロが 1 の場合、システムは、ブート コンフィギュレーション コマンドに基づいてブートを試行します。ブート コンフィギュレーション コマンドが存在しない場合、システムは、フラッシュ メモリからデフォルト ブートを試行、つまり、フラッシュ メモリの最初のブート可能ファイルを読み込もうとします。

フラッシュ ロード ヘルパーの動作中に生成されるシステム コンソール出力を表示するには、フラッシュ メモリのアップグレード後にブートしたイメージを使用します。特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
Router# **more flh:logfile**	フラッシュ ロード ヘルパーの動作中に生成されるコンソール出力を表示します。

コンソール接続なしでフラッシュ アップグレードを実行するリモート Telnet ユーザの場合、この作業を実行することで、Telnet 接続が ROM イメージへの切り替えのために終了した場合にコンソール出力を表示できます。この出力は、ダウンロード中に何が発生したかを示します。これは、特にダウンロードが失敗した場合に役立ちます。

フラッシュ メモリのフォーマット

クラス A およびクラス C フラッシュ ファイル システムでは、フラッシュ メモリをフォーマットできます。フォーマットすると、フラッシュ メモリのすべての情報が消去されます。

Cisco 7000 ファミリでは、新しいフラッシュ メモリ カードを PCMCIA スロットで使用するには、その前にフォーマットする必要があります。

フラッシュ メモリ カードには、障害となるセクタがあります。特定のフラッシュ メモリ セクタを他のセクタで障害が発生した場合の「スペア」として予約できます。**format** コマンドを使用して、0 ～ 16 セクタをスペアとして指定します。いくつかのスペア セクタを緊急用に予約する場合、フラッシュ メモリ カードのほとんどを利用できるため、容量を無駄に使用しないようにしてください。スペア セクタを指定せずに、一部のセクタが失敗した場合、フラッシュ メモリ カードを再フォーマットする必要があります。この場合、既存のデータはすべて消去されます。

フォーマット動作には、少なくとも Cisco IOS Release 11.0 システム ソフトウェアが必要です。

フラッシュ メモリ フォーマット プロセス

注意 次のフォーマット手順では、フラッシュ メモリのすべての情報が消去されます。重要なデータが失われないように、十分に注意して処理を続けてください。

次の手順に従い、フラッシュ メモリをフォーマットします。ブートフラッシュなど、内部フラッシュ メモリをフォーマットする場合、最初の手順を飛ばしてもかまいません。フラッシュ メモリ カードをフォーマットする場合、両方の手順を完了します。

ステップ 1 新しいフラッシュ メモリ カードを PCMCIA スロットに差し込みます。この手順の説明については、ご使用のルータのハードウェア マニュアルで、ルータのメンテナンスおよび PCMCIA カードの交換に関する説明を参照してください。

ステップ 2 フラッシュ メモリをフォーマットします。

フラッシュ メモリをフォーマットするには、次の EXEC モード コマンドを使用します。

コマンド	目的
Router# **format** [**spare** *spare-number*] *device1*: [[*device2*:][*monlib-filename*]]	フラッシュ メモリをフォーマットします。

次に、スロット 0 に挿入されているフラッシュ メモリ カードをフォーマットする **format** コマンドの例を示します。

```
Router# format slot0:
Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

ルータが EXEC プロンプトに戻ると、新しいフラッシュ メモリ カードが正常にフォーマットされ、使用できるようになります。

ロックされたブロックの回復

ロックされたブロックを回復するには、フラッシュ メモリ カードを再フォーマットします。フラッシュ メモリは、電源を損失した場合、または書き込みや消去操作中にフラッシュ メモリ カードの電源が抜かれた場合、ブロックがロックされます。フラッシュ メモリのブロックがロックされると、書き込みまたは消去ができなくなり、その後も特定のブロックでのこれらの操作が失敗します。ロックされたブロックを回復する唯一の方法は、**format** コマンドを使用してフラッシュ メモリ カードを再フォーマットすることです。

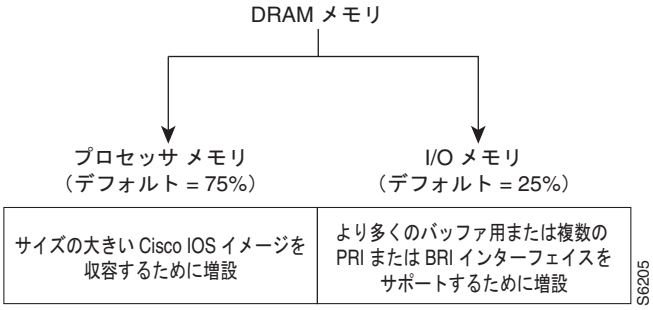
注意 フラッシュ メモリ カードを再フォーマットしてロックされたブロックを回復すると、既存のデータが失われます。

Cisco 3600 シリーズでの DRAM メモリの再割り当て

Cisco 3600 シリーズ ルータの DRAM メモリは、プロセッサ メモリおよび I/O メモリ間で分割される、隣接したアドレス レンジとして編成されます。ルータで設定したネットワーク インターフェイスのタイプと数によっては、パーティショニングされた DRAM メモリをプロセッサ メモリおよび I/O メモリに再割り当てする必要があります。

通常、Cisco 3600 シリーズ ルータでは、アドレス レンジの 25% が I/O メモリに、75% がプロセッサ メモリに割り当てられています。ただし、複数の ISDN PRI インターフェイスを注文された場合、DRAM メモリは、アドレス レンジの 40% を I/O メモリに、60% をプロセッサ メモリに割り当てられるように設定されます（図 11 を参照）。シスコシステムズは、各ルータの出荷前にこれらの DRAM メモリ調整を行っています。

図 11　Cisco 3600 シリーズ ルータの DRAM メモリのコンポーネントおよび使用



（注） 2 つ以上の ISDN PRI インターフェイス、または 12 以上の ISDN BRI インターフェイスを実行するルータでは、DRAM メモリの 40% を I/O メモリに、60% をプロセッサ メモリに割り当てる必要があります。

ただし、場合によっては、シスコ システムズからルータを受け取った後に、プロセッサ メモリと I/O メモリに割り当てられた DRAM メモリを再割り当てする必要があります。

たとえば、次の実行コンフィギュレーションで Cisco 3640 ルータを受け取ったとします。

- 2 イーサネットおよび 2 WAN インターフェイス カード
- NT1 ネットワーク モジュールでの 8 ポート ISDN BRI

- IP 機能セット
- 16 MB の DRAM メモリ（デフォルトでは、プロセッサ メモリ = 75%、I/O メモリ = 25%）
- 4 MB のフラッシュ メモリ

その後、4 ポート ISDN BRI ネットワーク モジュールをルータに追加しました。これで、現在ルータで実行している ISDN BRI インターフェイスは 12 になりました。ここで、**memory-size iomem** コマンドを使用して、アドレス レンジの 40% を I/O メモリに、60% をプロセッサ メモリに割り当てる必要があります。

現在のプロセッサおよび I/O メモリを表示し、これに従いメモリ分散を再割り当てするには、特権 EXEC モードで次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show version`	ルータにあるメモリの総容量を表示します。
ステップ 2	`Router# show memory`[1]	メモリの空き容量を表示します。
ステップ 3	`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。
ステップ 4	`Router(config)# memory-size iomem` *I/O-memory-percentage*[2]	プロセッサ メモリおよび I/O メモリを割り当てます。
ステップ 5	`Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	`Router# copy system:running-config nvram:startup-config`	設定を NVRAM に保存します。
ステップ 7	`Router# reload`	ルータをリロードして新しいイメージを実行します。

1. **show memory コマンドの出力の Free(b) カラムは、使用できる I/O メモリの容量を示しています。**
2. デフォルトは、I/O メモリが 40%、プロセッサ メモリが 60% です。

有効な I/O メモリの割合値は、10、15、20、25、30、40（デフォルト）、50 です。I/O メモリ サイズは、合計メモリ サイズの指定割合で、1 MB 単位で切り捨てられます。I/O メモリには、少なくとも 4 MB のメモリが必要です。残りのメモリはプロセッサ メモリに割り当てられます。

memory-size iomem コマンドが有効になるのは、**copy system:running-config nvram:startup-config** EXEC コマンドを使用して NVRAM に保存して、ルータをリロードした後です。ただし、このコマンドを入力すると、ソフトウェアにより、新しいメモリ分散で、現在実行されている Cisco IOS イメージに十分なプロセッサ メモリを割り当てることができるかどうかチェックされます。プロセッサ メモリに十分なメモリがない場合、次のメッセージが表示されます。

```
Warning: Attempting a memory partition that does not provide enough Processor memory for
the current image.If you write memory now, this version of software may not be able to
run.
```

reload コマンドを入力して新しいイメージを実行すると、ソフトウェアにより、新しいプロセッサおよび I/O メモリ割り当てが計算されます。十分なプロセッサ メモリがない場合、I/O メモリが別の設定に自動的に減らされ、イメージがロードされます。これでも実行するイメージに十分なプロセッサ メモリがない場合、DRAM が十分にないことになります。

プロセッサ メモリおよび I/O メモリの再割り当ての例

次に、DRAM の 40% を I/O メモリに、残りの 60% をプロセッサ メモリに割り当てる例を示します。この例では、メモリの現在の割り当てを表示し、この割り当てを変更して保存し、変更が有効になるようにルータをリロードします。**show memory** コマンド出力の Free(b) カラムは、使用できる I/O メモリの容量を示しています。

```
Router# show memory
               Head   Total(b)    Used(b)    Free(b)  Lowest(b) Largest(b)
Processor  60913730    3066064     970420    2095644    2090736    2090892
      I/O    C00000    4194304    1382712    2811592    2811592    2805492
--More--

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# memory-size iomem 40
Router(config)# exit
Router#
Router# copy system:running-config nvram:startup-config
Building configuration...
[OK]

Router# reload

rommon > boot
program load complete, entry point: 0x80008000, size: 0x32ea24
Self decompressing the image :
########################################################################################
########################################################################################
############################################################## [OK]
```

Cisco 7500 シリーズでのメモリ スキャンの使用

Cisco 7500 シリーズ ルータ（RSP7000 カード アップグレードでの 7000 シリーズなど）では、メモリ スキャン機能を使用できます。この機能は、インストールされているすべてのダイナミック ランダム アクセス メモリ（DRAM）でパリティ エラーがないかチェックする、ロープライオリティのバックグラウンド プロセスを追加します。未使用のメモリ領域でエラーが検出された場合、エラーのスクラビング（削除）が試行されます。メモリ スキャンとスクラビングの 1 サイクルを完了するまで、10 分から数時間かかります。これは、インストールされているメモリの容量により異なります。Central Processing Unit（CPU; 中央処理装置）に与えるメモリ スキャン機能の影響はわずかです。この機能は、新しい **memory scan** および **show memory scan** Command-Line Interface（CLI; コマンドライン インターフェイス）コマンドで制御および監視できます。

メモリ スキャン機能は、DRAM の情報の種類を区別しません。つまり、テキスト、データおよびヒープ情報を同様に認識します。この機能は、異なる領域で検出されたエラーに対して異なった反応をすることもありますが、メモリ セルがビジー状態の場合でも機能を続けます。エラーへの対応は、次の 1 つ以上の方法で行われます。

- 検出されたすべてのエラーに対してメッセージが記録されます。各メッセージには、エラーの説明が示され、必要に応じて推奨対策が示されます。
- ヒープ ストレージ制御ブロックのエラーの場合、空きブロックのエラーをスクラビングしようとします。エラーがスクラビングされる場合、これ以上のアクションは行われませんが、エラー ログに記録されます。スクラビングされない場合、エラーが検出されたブロックは、ユーザに割り当てられない異常メモリ リストにリンクされます。このメモリ ブロックのサイズが大きい場合、ブロックは分割され、エラーが検出された部分だけが、異常メモリ リストにリンクされます。

- ビジー ブロックのエラーの場合、またはテキストやデータなどの他の領域でのエラーの場合、エラー メッセージが生成されますが、データを損傷しないように、これ以上のアクションは行われません。

メモリ スキャンの設定および確認

この機能をイネーブルにするには、グローバル コンフィギュレーション モードで **memory scan** コマンドを使用します。

メモリ スキャンが実行コンフィギュレーションにあるか確認するには、特権 EXEC モードで **more system:running-configuration** コマンドを使用します。

システムでのパリティ エラーの数およびタイプを監視するには、**show memory scan** コマンドを使用します。**show memory scan** コマンドは、特権 EXEC モードで使用します。次の例では、この機能がイネーブルにされ、パリティ エラーは検出されません。

```
Router# show memory scan
Memory scan is on.
No parity error has been detected.
```

メモリ スキャン機能が設定されていない場合、またはディセーブルにされている場合、**show memory scan** コマンドはレポートを生成します。次の例では、メモリ スキャンはディセーブルです。

```
Router# show memory scan
Memory scan is off
No parity error has been detected.
```

システムでエラーが検出されると、**show memory scan** コマンドは、エラー レポートを生成します。次の例では、メモリ スキャンは、パリティ エラーを検出しました。

```
Router# show memory scan
Memory scan is on.
Total Parity Errors 1.
Address BlockPtr BlckSize Disposit   Region Timestamp
6115ABCD 60D5D090   9517A4  Scrubed    Local 16:57:09 UTC Thu Mar 18
```

エラー レポート フィールドの説明については、『Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*』の「Router Memory Commands」の章で **show memory scan** コマンドに関する詳細を参照してください。

メモリ リーク ディテクタ

メモリ リーク ディテクタ機能は、Cisco IOS ソフトウェアを実行しているルータのメモリ リークを検出するために使用できるツールです。メモリ リーク ディテクタ機能は、すべてのメモリ プール、パケット バッファ、およびチャンクのリークを検出できます。

メモリ リーク ディテクタの機能の履歴

リリース	変更点
12.3(8)T1	この機能が導入されました。
12.2(25)S	この機能は、Cisco IOS Release 12.2(25)S に統合されました。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

メモリ リーク ディテクタについて

メモリ リーク ディテクタの機能を使用する前に、次の概念を理解しておく必要があります。

メモリ リーク

メモリ リークは、有用な目的をまったく果たさない、メモリのスタティック割り当てまたはダイナミック割り当てです。スタティックに割り当てられたメモリ間でのリーク検出に使用できるテクノロジーがありますが、このマニュアルでは、ダイナミックに行われるメモリ割り当てに焦点を当てます。

メモリ リークの検出

検出の観点から、ダイナミックに割り当てられたメモリ ブロック間のリークは、次の 3 つのタイプに分類できます。

- タイプ 1 のリークにはリファレンスがありません。メモリのこれらのブロックにはアクセスできません。
- タイプ 2 のリークは割り当ての 1 つ以上のサイクルに含まれますが、このサイクル内のどのブロックにもサイクル外からはアクセスできません。各サイクル内のブロックは、サイクル内の他の要素へのリファレンスを持ちます。タイプ 2 のリークの例として、今では必要とされない循環リストがあります。個別の要素は到達可能ですが、循環リストは到達可能ではありません。
- タイプ 3 のリークはアクセス可能または到達可能ですが必要でなく、たとえば、今では必要とされないデータ構造の要素が該当します。タイプ 3 のリークのサブクラスには、割り当ては行われますが書き込みは決して行われません。**show memory debug reference unused** コマンドを使用して、このサブクラス リークを探索できます。

メモリ リーク ディテクタ機能により、タイプ 1 およびタイプ 2 のメモリ リークを検出するテクノロジーが提供されます。

メモリ リーク ディテクタ機能は、次の 2 つのモードで動作します。

- ノーマル モード：メモリ リーク ディテクタはメモリを使用して動作を高速化します。
- ロー メモリ モード：メモリ リーク ディテクタは、メモリの割り当てを試行せずに実行します。

ロー メモリ モードはノーマル モードよりもかなり低速で、ブロックだけしか処理できません。ロー メモリ モードではチャンクがサポートされません。ロー メモリ モードは、ルータの使用可能なメモリが少ない場合、またはない場合に役立ちます。

メモリ リーク ディテクタは簡単なインターフェイスを備えており、いつでも Command Line Interface（CLI; コマンドライン インターフェイス）から呼び出してメモリ リークのレポートを取得できます。テスト用途の場合は、すべてのテストを実行した後、メモリ リーク ディテクタを呼び出してリークに関するレポートを取得できます。テストのときだけに生成されるリークだけが重要となる場合、メモリ リーク ディテクタには、テスト開始時にイネーブルにされるインクリメンタル オプションがあります。テストの終了後、インクリメンタル オプションがイネーブルにされた後に発生したリークだけのレポートを取得できます。

偽りのアラームを減らすには、メモリ リーク ディテクタを複数回呼び出して、すべてのレポートで一貫して表示されるリークだけをリークとして解釈することが必要です。これは特に、パケット バッファ リークの場合に当てはまります。

（注） メモリ リーク ディテクタのレポートに基づく障害を連絡する場合は、障害レポートのアトリビュート フィールドに「メモリ リーク検出」と記入してください。

警告 **重大なメモリ リークの問題があるデバイス上でメモリ リーク検出コマンドを発行すると、接続が失われる場合があります。**

メモリ リーク ディテクタの使用方法

ここでは、次の各手順について説明します。

メモリ リーク情報の表示

次の作業は、検出されたメモリ リークの情報を表示する方法を示します。

手順の概要

1. **enable**
2. **show memory debug leaks** [**chunks** | **largest** | **lowmem** | **summary**]

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。 • 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	**show memory debug leaks**
	または
	show memory debug leaks [**chunks**]
	または
	show memory debug leaks [**largest**]
	または
	show memory debug leaks [**lowmem**]
	または
	show memory debug leaks [**summary**]
	
	例：
	`Router# show memory debug leaks`
	または
	
	例：
	`Router# show memory debug leaks chunks`
	または
	
	例：
	`Router# show memory debug leaks largest`
	または
	
	例：
	`Router# show memory debug leaks lowmem`
	または
	
	例：
	`Router# show memory debug leaks summary`
		ノーマル モードでメモリ リーク検出を実行して、検出されたメモリ リークを表示します。チャンク内のメモリ リークは検出されません。
		または
		(任意）ノーマル モードでメモリ リーク検出を実行して、チャンク内の検出されたメモリ リークを表示します。
		または
		(任意）メモリ リーク検出を実行して、上位 10 のリークの allocator_pcs、およびリークしたメモリの合計量を表示します。さらに、このコマンドが実行されるたびに、以前の実行時のレポートが呼び出されて、現在の実行のレポートと比較されます。
		または
		(任意）ロー メモリ モードでメモリ リーク検出を実行して、検出されたメモリ リークを表示します。分析にかかる時間は、ノーマル モードの場合よりもかなり長くなります。このコマンドの出力は、**show memory debug leaks** コマンドと類似しています。
		または
		(任意）ノーマル モードでメモリ リーク検出を実行して、検出されたメモリ リークを allocator_pc に基づいて表示した後、ブロックのサイズに基づいて表示します。

例

ここでは、次の出力例について説明します。

show memory debug leaks コマンドのサンプル出力

次に、**show memory debug leaks** コマンドにオプション キーワードを指定しない場合の出力例を示します。

```
Router# show memory debug leaks

Adding blocks for GD...

                PCI memory
Address    Size   Alloc_pc  PID  Name

                I/O memory
Address    Size   Alloc_pc  PID  Name

                Processor memory
Address    Size   Alloc_pc  PID  Name
62DABD28       80 60616750  -2   Init
62DABD78       80 606167A0  -2   Init
62DCF240       88 605B7E70  -2   Init
62DCF298       96 605B7E98  -2   Init
62DCF2F8       88 605B7EB4  -2   Init
62DCF350       96 605B7EDC  -2   Init
63336C28      104 60C67D74  -2   Init
63370D58       96 60C656AC  -2   Init
633710A0      304 60C656AC  -2   Init
63B2BF68       96 60C659D4  -2   Init
63BA3FE0    32832 608D2848  104  Audit Process
63BB4020    32832 608D2FD8  104  Audit Process
```

表 1 に、この出力で表示される重要なフィールドについて説明します。

表 1　show memory debug leaks のフィールドの説明

フィールド	説明
Address	リークされたブロックの 16 進数のアドレス。
Size	リークされたブロックのサイズ（バイト単位）。
Alloc_pc	ブロックに割り当てられたシステム コールのアドレス。
PID	ブロックに割り当てられたプロセスのプロセス ID。
Name	ブロックに割り当てられたプロセスの名前。

show memory debug leaks chunks コマンドのサンプル出力

次に、**show memory debug leaks chunks** コマンドからの出力例を示します。

```
Router# show memory debug leaks chunks

Adding blocks for GD...

                PCI memory
Address    Size   Alloc_pc  PID  Name

Chunk Elements:
Address  Size  Parent   Name

                I/O memory
Address    Size   Alloc_pc  PID  Name

Chunk Elements:
```

```
Address  Size  Parent   Name

                Processor memory
Address    Size   Alloc_pc  PID  Name
62DABD28       80 60616750  -2   Init
62DABD78       80 606167A0  -2   Init
62DCF240       88 605B7E70  -2   Init
62DCF298       96 605B7E98  -2   Init
62DCF2F8       88 605B7EB4  -2   Init
62DCF350       96 605B7EDC  -2   Init
63336C28      104 60C67D74  -2   Init
63370D58       96 60C656AC  -2   Init
633710A0      304 60C656AC  -2   Init
63B2BF68       96 60C659D4  -2   Init
63BA3FE0    32832 608D2848  104  Audit Process
63BB4020    32832 608D2FD8  104  Audit Process

Chunk Elements:
Address  Size  Parent   Name
62D80DA8    16 62D7BFD0 (Managed Chunk )
62D80DB8    16 62D7BFD0 (Managed Chunk )
62D80DC8    16 62D7BFD0 (Managed Chunk )
62D80DD8    16 62D7BFD0 (Managed Chunk )
62D80DE8    16 62D7BFD0 (Managed Chunk )
62E8FD60   216 62E8F888 (IPC Message He)
```

表 2 に、この出力で表示される重要なフィールドについて説明します。

表 2　　show memory debug leaks chunks のフィールドの説明

フィールド	説明
Address	リークされたブロックの 16 進数のアドレス。
Size	リークされたブロックのサイズ（バイト単位）。
Alloc_pc	ブロックに割り当てられたシステム コールのアドレス。
PID	ブロックに割り当てられたプロセスのプロセス ID。
Name	ブロックに割り当てられたプロセスの名前。
Size	（チャンク要素）リークされた要素のサイズ（バイト）。
Parent	（チャンク要素）リークされたチャンクの親チャンク。
Name	（チャンク要素）リークされたチャンクの名前。

show memory debug leaks largest コマンドのサンプル出力

次に、**show memory debug leaks largest** コマンドからの出力例を示します。

```
Router# show memory debug leaks largest

Adding blocks for GD...

                PCI memory
Alloc_pc    total leak size

                I/O memory
Alloc_pc    total leak size

                Processor memory
Alloc_pc    total leak size
608D2848    32776     inconclusive
608D2FD8    32776     inconclusive
```

```
60C656AC    288       inconclusive
60C67D74    48        inconclusive
605B7E98    40        inconclusive
605B7EDC    40        inconclusive
60C659D4    40        inconclusive
605B7E70    32        inconclusive
605B7EB4    32        inconclusive
60616750    24        inconclusive
```

次に、**show memory debug leaks largest** コマンドの 2 回目の実行からの出力例を示します。

```
Router# show memory debug leaks largest

Adding blocks for GD...

                PCI memory
Alloc_pc    total leak size

                I/O memory
Alloc_pc    total leak size

                Processor memory
Alloc_pc    total leak size
608D2848    32776
608D2FD8    32776
60C656AC    288
60C67D74    48
605B7E98    40
605B7EDC    40
60C659D4    40
605B7E70    32
605B7EB4    32
60616750    24
```

show memory debug leaks summary コマンドのサンプル出力

次に、**show memory debug leaks summary** コマンドからの出力例を示します。

```
Router# show memory debug leaks summary

Adding blocks for GD...

                PCI memory

Alloc PC        Size     Blocks      Bytes    What

                I/O memory

Alloc PC        Size     Blocks      Bytes    What

                Processor memory

Alloc PC        Size     Blocks      Bytes    What

0x605B7E70 0000000032 0000000001 0000000032    Init
0x605B7E98 0000000040 0000000001 0000000040    Init
0x605B7EB4 0000000032 0000000001 0000000032    Init
0x605B7EDC 0000000040 0000000001 0000000040    Init
0x60616750 0000000024 0000000001 0000000024    Init
0x606167A0 0000000024 0000000001 0000000024    Init
0x608D2848 0000032776 0000000001 0000032776    Audit Process
0x608D2FD8 0000032776 0000000001 0000032776    Audit Process
0x60C656AC 0000000040 0000000001 0000000040    Init
```

```
0x60C656AC 0000000248 0000000001 0000000248    Init
0x60C659D4 0000000040 0000000001 0000000040    Init
0x60C67D74 0000000048 0000000001 0000000048    Init
```

表 3 に、この出力で表示される重要なフィールドについて説明します。

表 3　show memory debug leaks summary のフィールドの説明

フィールド	説明
Alloc PC	ブロックに割り当てられたシステム コールのアドレス。
Size	リークされたブロックのサイズ。
Blocks	リークされたブロックの数。
Bytes	リークされたメモリの合計量。
What	ブロックを所有するプロセスの名前。

メモリ デバッグのインクリメンタル開始時刻の設定

次の作業は、メモリ リークのインクリメンタル分析の開始時刻を設定する方法を示します。インクリメンタル分析の場合は、**set memory debug incremental starting-time** コマンドを使用して開始点を定義します。開始時刻が設定されると、開始時刻以降に割り当てられたメモリだけがリークとしてレポートされる対象になります。

手順の概要

1. **enable**
2. **set memory debug incremental starting-time**

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。 • 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	**set memory debug incremental starting-time** 例： `Router# set memory debug incremental starting-time`	インクリメンタル分析の開始時刻をコマンドが発行される時刻に設定します。

メモリ リーク情報の段階的な表示

次の作業は、開始時刻が確定された後のメモリ リーク情報を表示する方法を示します。

手順の概要

1. **enable**

2. **set memory debug incremental starting-time**
3. **show memory debug incremental {allocations | leaks [lowmem] | status}**

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。 • 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	**set memory debug incremental starting-time** **例：** `Router# set memory debug incremental starting-time`	インクリメンタル分析の開始時刻をコマンドが発行される時刻に設定します。

ステップ 3	**show memory debug incremental allocations**
	または
	show memory debug incremental leaks
	または
	show memory debug incremental leaks lowmem
	または
	show memory debug incremental status
	
	例：
	`Router# show memory debug incremental allocations`
	または
	
	例：
	`Router# show memory debug incremental leaks`
	または
	
	例：
	`Router# show memory debug incremental leaks lowmem`
	または
	
	例：
	`Router# show memory debug incremental status`
		set memory debug incremental starting-time コマンドの発行後に割り当てられたすべてのメモリ ブロックを表示します。表示されるメモリ ブロックは単なるメモリ割り当てであり、必ずしもリークとは限りません。
		または
		set memory debug incremental starting-time コマンドの発行後にリークされたメモリだけを表示することを除き、**show memory debug leaks** コマンドと類似した出力を表示します。
		または
		メモリ リーク検出を強制的にロー メモリ モードで動作させます。このコマンドの出力は、**set memory debug incremental starting-time** コマンドの発行後にリークされたメモリだけを表示することを除き、**show memory debug leaks** コマンドと類似しています。
		• ロー メモリ モードでは、分析時間がノーマル モードよりもかなり長くなります。
		• （ノーマル モードでのメモリ リーク検出呼び出し時の失敗経験などによって）ノーマル モードでのメモリ リーク検出が失敗することがすでにわかっている場合にこのコマンドを使用できます。
		または
		インクリメンタル分析の開始点が設定されて、その後、時間が経過しているかどうかを表示します。

例

ここでは、次の出力例について説明します。

- 「show memory debug incremental allocations コマンドのサンプル出力」（P.10）
- 「show memory debug incremental status コマンドのサンプル出力」（P.10）

show memory debug incremental allocations コマンドのサンプル出力

次に、**show memory debug incremental** コマンドを **allocations** キーワードを指定して入力した場合の出力例を示します。

```
Router# show memory debug incremental allocations

Address    Size   Alloc_pc  PID  Name
62DA4E98      176 608CDC7C  44   CDP Protocol
62DA4F48       88 608CCCC8  44   CDP Protocol
62DA4FA0       88 606224A0  3    Exec
62DA4FF8       96 606224A0  3    Exec
635BF040       96 606224A0  3    Exec
63905E50      200 606A4DA4  69   Process Events
```

show memory debug incremental status コマンドのサンプル出力

次に、**show memory debug incremental** コマンドを **status** キーワードを指定して入力した場合の出力例を示します。

```
Router# show memory debug incremental status

Incremental debugging is enabled
Time elapsed since start of incremental debugging: 00:00:10
```

その他の関連資料

メモリ リーク ディテクタに関する関連資料については、次の各項目を参照してください。

関連資料

関連項目	参照先
その他のコマンド：complete コマンド構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T*』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
TAC のホームページには、3 万ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/public/support/tac/home.shtml

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **set memory debug incremental starting-time**
- **show memory debug incremental**
- **show memory debug leaks**

コンソール アクセス用予約メモリ

コンソール アクセス機能の予約メモリは、Command-Line Interface（CLI; コマンドライン インターフェイス）およびソフトウェア拡張機能を実装しており、これにより、ルータ コンソールへのログインや、管理作業およびトラブルシューティングを実行するために十分なメモリを予約できます。これらの拡張機能によって、管理者はどのような状況でも、ルータのメモリが不足しているときでさえ、ルータにログインできるようになります。

この章で紹介する機能情報の入手方法

*ご使用の Cisco IOS ソフトウェア リリースで、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。*この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、「Reserve Memory for Console Access の機能情報」（P.6）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

Reserve Memory for Console Accessについて

コンソール アクセス用に予約されたメモリの容量を増やす前に、次の概念を理解しておく必要があります。

コンソール アクセス用のメモリ増設の利点

Cisco IOS 12.0(22)S ソフトウェアのリリースよりも前では、ルータがメモリ不足であったり、非常に小さくフラグメント化されたりしている場合はルータ コンソールにアクセスできませんでした。ルータを最適なパフォーマンス レベルに維持するには、必要な場合にコンソールにアクセスしてトラブルシューティングを実行できる必要があります。

コンソール アクセスの予約メモリ機能のリリースに伴う利点は、ルータがメモリ不足であったり、非常に小さくフラグメント化されたりしても、どのような状況でもルータ コンソールにログインして管理作業やトラブルシューティングを実行するための十分なメモリを予約できることです。

コンソール アクセスの予約メモリ増設に関するガイドライン

Cisco IOS ソフトウェアでは、デフォルトでコンソール アクセス用に 256 KB のメモリが予約されています。この予約メモリは、Reserve Memory for Console Access機能で提供される **memory reserved console** コマンドを使用して増設できます。

このコマンドの使用上のガイドラインとして、NVRAM の使用バイト数の 3 倍を超える値を設定することを推奨します。**dir nvram:** コマンドの出力から、NVRAM の使用バイト数を取得できます。たとえば、コマンド **dir nvram:** の出力で表示される NVRAM の使用バイト数の合計が 129016 バイトである場合は、四捨五入されて近似値が 129 KB になります。この値に 3 を掛けて 387 KB になります。ガイドラインに従って、**memory reserved console** コマンドの *number-of-kilobytes* 引数の値として、387 を入力します。コンソール アクセス用の予約メモリは、最大 4096 KB まで増設できます。

コンソールに予約されたメモリの現在の使用可能サイズを表示するには、**show memory console reserved** コマンドを使用できます。

Reserve Memory for Console Accessの設定方法

ここでは、次の手順について説明します。

コンソール アクセス用の予約メモリの設定

コンソール アクセス用の予約メモリを設定するには、次の作業を実行します。ルータがメモリ不足であったり、非常に小さくフラグメント化されたりしている場合は、コンソール アクセス用に予約されたメモリの容量を増設する必要があることがあります。メモリを増設すると、ルータ コンソールにアクセスしてトラブルシューティングや他の管理作業を実行して、ルータを最適なパフォーマンス レベルに維持できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **memory reserve console** *number-of-kilobytes*
4. **exit**
5. show memory console reserved

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。 • 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： `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。
ステップ 3	**memory reserved console** *number-of-kilobytes* 例： `Router(config)# memory reserved console 512`	コンソール アクセス用に予約されたメモリの容量を増やします。 • *number-of-kilobytes* 引数は、予約されたメモリの容量です（KB 単位）。有効な値は 1 ～ 4096 KB です。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 exit モードを終了します。
ステップ 5	**show memory console reserved** 例： `Router# show memory console reserved`	予約されているメモリの容量を表示します。

例

次に、**show memory console reserved** コマンドの出力例を示します。

```
Router# show memory console reserved

Memory reserved for console is 201400
```

Reserve Memory for Console Access の設定例

ここでは、次の設定例について説明します。

- 「コンソール アクセス用の予約メモリの設定：例」

コンソール アクセス用の予約メモリの設定：例

次に、コンソール アクセス用の予約メモリを 1024 KB まで増やす例を示します。

```
enable
!
configure terminal
!
memory reserved console 1024
end
```

次に、コンソール アクセス用の予約メモリの増設をディセーブルにする例を示します。

```
enable
!
configure terminal
!
no memory reserved console
end
```

その他の関連資料

ここでは、Reserve Memory for Console Access 機能に関する関連資料について説明します。

関連資料

関連項目	参照先
Cisco IOS コンフィギュレーションの基本コマンド	『*Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2』
Cisco IOS コンフィギュレーションの基本コンフィギュレーション作業および基本概念	『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2』

規格

規格	タイトル
この機能によりサポートされた新規標準または改訂標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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。またこの機能で既存 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
シスコのテクニカル サポートおよびドキュメンテーション Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **memory reserved console**
- **show memory console reserved**

Reserve Memory for Console Accessの機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco IOS ソフトウェア イメージは、Cisco IOS ソフトウェア リリース、機能セット、プラットフォームそれぞれに固有です。Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、以降の Cisco IOS ソフトウェアのメンテナンス リリースでもサポートされます。

表 1　Reserve Memory for Console Accessの機能情報

機能名	リリース	機能情報
コンソール アクセス用予約メモリ	12.0(22)S 12.2(28)SB 12.4(15)T	コンソール アクセス機能の予約メモリは、Command-Line Interface（CLI; コマンドライン インターフェイス）およびソフトウェア拡張機能を実装しており、これにより、ルータ コンソールへのログインや、管理作業およびトラブルシューティングを実行するために十分なメモリを予約できます。これらの拡張機能によって、管理者はどのような状況でも、ルータのメモリが不足しているときでさえ、ルータにログインできるようになります。 この機能は、12.0(22)S で初めて導入されました。 この機能は、12.2(28)SB で Cisco IOS 12.2SB リリースに統合されました。 この機能は、12.4(15)T で Cisco IOS 12.2T リリースに統合されました。 この機能に関する詳細については、次の各項を参照してください。 • 「コンソール アクセス用のメモリ増設の利点」（P.2） • 「コンソール アクセスの予約メモリ増設に関するガイドライン」（P.2） • 「コンソール アクセス用の予約メモリの設定」（P.2） この機能により、**memory reserved console** および **show memory console reserved** コマンドが変更されました。

高度なインフラストラクチャの管理

ゼロ化

ゼロ化は、潜在的なすべての機密情報をルータ メモリから消去します。消去されるメモリは、メイン メモリ、キャッシュ メモリ、およびその他のパケット データ、NVRAM、フラッシュ メモリなどのメモリです。ゼロ化を呼び出すには、前面プレートの [Zeroization] ボタンを使用します。ゼロ化のパラメータを設定することはできますが、Command-Line Interface（CLI; コマンドライン インターフェイス）から呼び出すことはできません。

ゼロ化はデフォルトでディセーブルです。

ゼロ化の機能履歴

リリース	変更点
12.3(8)YD	この機能が導入されました。
12.4(2)T	この機能は、Cisco IOS Release 12.4(2)T に統合されました。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の入手方法

Cisco Feature Navigator を使用すると、プラットフォームおよび Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明な場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

ゼロ化に関する制約事項

- ゼロ化は、Cisco 3200 シリーズ ルータだけでサポートされています。
- ゼロ化がイネーブルの場合、補助（AUX）ポートは、プッシュ ボタンなど、アクチュエータ以外の機能には使用しないでください。AUX ポートに接続されているデバイスがゼロ化を起動するかどうかを確実に確かめることはできません。ゼロ化がイネーブルの場合、ゼロ化アクチュエータを除き、AUX ポートにデバイスを接続しないでください。ゼロ化がイネーブルの場合、AUX ポート設定に関する制約事項がいくつか適用されます。
- ゼロ化は、ローカルだけで呼び出せます。Telnet セッションを介してリモートで呼び出すことはできません。
- ゼロ化は、すべてのネットワーク インターフェイスをシャット ダウンし、揮発性メモリに含まれるルータのすべての IP アドレスなど、Cisco IOS 設定およびオブジェクト コード ファイルのゼロ化を呼び出します。

ゼロ化について

ゼロ化を起動するには、次の概念を理解する必要があります。

- 「ルータ メモリのスクラビング」（P.2）

ルータ メモリのスクラビング

*スクラビング*とは、メモリ領域間でいくつかのパスを実行して、各パスに個々のデータ パターンを使用してメモリを上書きすることです。スクラビングに使用されるデータ パターンは、個々のパスで構成されます。各パスは、次のデータ パターンをメモリに書き込みます。

- すべて 1（つまり、0xffff ffff）
- 1 と 0 の交互（つまり、0xa5a5 a5a5）
- 0 と 1 の交互（つまり、0x5a5a 5a5a）
- すべて 0（つまり、0x0000 0000）

これらのデータ パターンにより、次のことが行われます。

- メモリの各ビットが 0 にクリアされ、少なくとも一度 1 に設定される。
- メモリの最後の状態が、それ以前のすべての情報が消去された状態になる。

ルータ メモリで次のものがスクラビングされます。

- CPM のデュアルポート RAM
- メイン メモリ

実際のスクラビングを実行するスモール プログラム ループを含むメモリ領域を除き、すべてのメイン メモリがスクラビングされます。

ルータ メモリで次のものはスクラビングされません。

- コンソールおよび AUX ポート UART FIFO キュー。一連の文字が、FIFO キューに強制的に追加され、FIFO キューのすべての機密情報がフラッシュされます。
- NVRAM。全体的に消去されます。
- フラッシュ メモリ ファイル システム。全体的に消去されます。

- キャッシュ。フラッシュおよび無効化され、すべての情報が削除されます。メイン メモリをスクラビングすると、すべてのキャッシュ ラインにスクラビング データ パターンが含まれます。

（注） 場合によっては、完全にスクラビングできないこともあります。たとえば、デバイスによっては、スクラビング パターンをメモリに書き込むことができるフル データ パスを提供せずに、メモリを *リセット* または *無効化* します。

コマンド リファレンス

次に示すコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。これらのコマンドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』（http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html）を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、または『*Cisco IOS Master Commands List*』を参照してください。

- **show declassify**