Cisco IOS コマンドライン インターフェイスを使用した基本的なソフトウェア コンフィギュレーション

このマニュアルでは、Cisco IOS コマンドライン インターフェイス（CLI）を使用して、ルータの基本的なソフトウェア コンフィギュレーションを実行する方法を説明します。

目次

このマニュアルでサポートされるプラットフォーム

このマニュアルは、次のプラットフォームに対して使用してください。

- Cisco 1800 シリーズ ルータ
- Cisco 2800 シリーズ ルータ
- Cisco 3800 シリーズ ルータ

Cisco IOS CLI を使用した基本的なソフトウェア コンフィギュレーションのための前提条件

ルータに付属のクイック スタート ガイドの手順に従い、シャーシを設置し、ケーブルを接続し、ルータの電源をオンにしてください。

ワンポイント アドバイス

AutoInstall プロセスが実行されないようにするため、ルータの電源をオンにする前に、ルータからすべての WAN ケーブルを外してください。WAN ケーブルが接続の両側のルータに取り付けられていて、ルータの NVRAM（不揮発性 RAM）に有効なコンフィギュレーション ファイルが保存されていない場合（新しいインターフェイスを追加する場合など）、ルータの電源をオンにすると、AutoInstall の実行が試行される可能性があります。AutoInstall がリモートの TCP/IP ホストに接続されていないとルータが判断するのに、数分間かかることもあります。

Cisco IOS CLI を使用した基本的なソフトウェア コンフィギュレーションの制限事項

ルータに Cisco Router and Security Device Manager（SDM）がインストールされている場合は、ソフトウェアの初期設定に Cisco IOS CLI ではなく Cisco SDM を使用することを推奨します。SDM にアクセスするには、ルータに付属のクイック スタート ガイドを参照してください。

Cisco IOS CLI を使用した基本的なソフトウェア コンフィギュレーションの実行方法

ここでは、次の手順について説明します。

ルータのホスト名の設定

ホスト名は、CLI プロンプトやデフォルト コンフィギュレーション ファイルの名前に使用されます。ルータのホスト名を設定しないと、出荷時に設定されたデフォルトのホスト名「Router」が使用されます。

ホスト名では、大文字と小文字が区別されるとは限りません。インターネット ソフトウェア アプリケーションの多くは大文字と小文字を同じ文字として処理します。一般的に名前の頭文字は大文字にしますが、コンピュータ名の場合はすべて小文字で表記することが習慣となっています。詳細については、RFC 1178 の「*Choosing a Name for Your Computer*」を参照してください。

ホスト名は、Advanced Research Projects Agency Network（ARPANET）ホスト名の規則に従って設定する必要もあります。先頭は英字、末尾は英字か数字にしなければならず、それらの間に使用できるのは英字、数字、およびハイフンだけです。名前は 63 文字以下で指定する必要があります。詳細については、RFC 1035 の「*Domain Names—Implementation and Specification*」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. ルータのプロンプトに新しいホスト名が表示されていることを確認します。
5. **end**

詳細手順

	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 モードを開始します。 • 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** *name* **例：** `Router(config)# hostname myrouter`	ネットワーク サーバのホスト名を指定または変更します。
ステップ 4	ルータのプロンプトに新しいホスト名が表示されていることを確認します。 **例：** `myrouter(config)#`	—
ステップ 5	**end** **例：** `myrouter# end`	（任意）特権 EXEC モードに戻ります。

次の作業

「イネーブル パスワードおよびイネーブル シークレット パスワードの設定」（P.4）に進んでください。

イネーブル パスワードおよびイネーブル シークレット パスワードの設定

セキュリティのレベルを強化するには（特に、ネットワークを通過するパスワードや TFTP サーバに保存されるパスワードのセキュリティを強化するには）、**enable password** コマンドまたは **enable secret** コマンドを使用します。いずれのコマンドを使用しても同じ結果になります。つまり、暗号化されたパスワードを設定でき、特権 EXEC（イネーブル）モードにアクセスする際にはこのパスワードの入力が求められます。

強化された暗号化アルゴリズムが使用されている **enable secret** コマンドを使用することを推奨します。**enable password** コマンドは、Cisco IOS ソフトウェアの古いイメージをブートする場合、または **enable secret** コマンドを認識しない古いブート ROM をブートする場合だけ使用してください。

詳細については、『*Cisco IOS Security Configuration Guide*』の「Configuring Passwords and Privileges」の章を参照してください。『*Cisco IOS Password Encryption Facts*』テクニカル ノートおよび『*Improving Security on Cisco Routers*』テクニカル ノートも参照してください。

制限事項

enable secret コマンドを設定すると、このコマンドは **enable password** より優先されます。これらの 2 つのコマンドを同時に有効にはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **enable secret** *password*
5. **end**
6. **enable**
7. **end**

詳細手順

	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 モードを開始します。 • 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。

	コマンドまたはアクション	目的
ステップ 3	**enable password** *password* **例：** `Router(config)# enable password pswd2`	（任意）さまざまな特権レベルへのアクセスを制御するためのローカル パスワードを設定します。 • この手順は、Cisco IOS ソフトウェアの古いイメージをブートする場合、または **enable secret** コマンドを認識しない古いブート ROM をブートする場合にだけ実行することを推奨します。
ステップ 4	**enable secret** *password* **例：** `Router(config)# enable secret greentree`	**enable password** コマンドより強力なレベルのセキュリティをさらに指定します。 • ステップ 3 で入力したパスワードと同じパスワードは使用しないでください。
ステップ 5	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**enable** **例：** `Router> enable`	特権 EXEC モードを開始します。 • 新しいイネーブル パスワードまたはイネーブル シークレット パスワードが機能することを確認します。
ステップ 7	**end** **例：** `Router(config)# end`	（任意）特権 EXEC モードに戻ります。

トラブルシューティングのヒント

設定したパスワードを思い出せない場合、または特権 EXEC（イネーブル）モードにアクセスできない場合は、http://www.cisco.com/warp/public/474 で、お使いのルータの『Password Recovery Procedures』を参照してください。

次の作業

コンソール インターフェイスの特権 EXEC タイムアウトを 10 分（デフォルト値）以外の値に設定するには、「コンソールのアイドル特権 EXEC タイムアウトの設定」（P.5）に進みます。

特権 EXEC タイムアウトを変更しない場合は、「デフォルト ルートまたはラスト リゾート ゲートウェイの指定」（P.9）に進みます。

コンソールのアイドル特権 EXEC タイムアウトの設定

ここでは、コンソール回線のアイドル特権 EXEC タイムアウトの設定方法を説明します。デフォルトでは、特権 EXEC コマンド インタープリタは、タイムアウトになる前に、ユーザによる入力を 10 分間待ちます。

コンソール回線を設定する際は、使用中の端末に対して、通信パラメータの設定、autobaud 接続の指定、および端末動作パラメータの設定も行うことができます。コンソール回線の設定の詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』を参照してください。特に、「Configuring Operating Characteristics for Terminals」および「Troubleshooting and Fault Management」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **exec-timeout** *minutes* [*seconds*]
5. **end**
6. **show running-config**
7. **exit**

（注） exec-timeout コマンド、または exec-command 値に対する変更は、EXEC モードを終了してログインし直した場合にだけトリガされます。

詳細手順

	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 モードを開始します。 • 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	**line console 0** **例：** `Router(config)# line console 0`	コンソール回線を設定し、ライン コンフィギュレーション コマンド コレクション モードを開始します。
ステップ 4	**exec-timeout** *minutes* [*seconds*] **例：** `Router(config-line)# exec-timeout 0 0`	アイドル特権 EXEC タイムアウト（特権 EXEC コマンド インタープリタがユーザによる入力を検出するまで待機する間隔）を設定します。 • 例では、タイムアウトなしの指定方法を示しています。
ステップ 5	**end** **例：** `Router(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** **例：** `Router# show running-config`	実行コンフィギュレーション ファイルを表示します。 • アイドル特権 EXEC タイムアウトが正しく設定されていることを確認します。
ステップ 7	**exit** **例：** `Router# exit`	特権 EXEC モードを終了します。 **（注）** exec-timeout コマンドの結果を反映するには、EXEC モードを終了し、ログインし直す必要があります。

例

次の例は、コンソールのアイドル特権 EXEC タイムアウトを 2 分 30 秒に設定する方法を示します。

```
line console
 exec-timeout 2 30
```

次の例は、コンソールのアイドル特権 EXEC タイムアウトを 10 秒に設定する方法を示します。

```
line console
 exec-timeout 0 10
```

次の作業

「ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスの設定」（P.7）に進んでください。

ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスの設定

ここでは、IP アドレスおよびインターフェイスの記述をルータのイーサネット インターフェイスに割り当てる方法を示します。

ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスの総合的な設定情報については、『*Cisco IOS Interface and Hardware Component Configuration Guide*』の「Configuring LAN Interfaces」の章を参照してください。

インターフェイス番号については、ルータに付属のクイック スタート ガイドを参照してください。

（注） Cisco 1841 および Cisco 2801 のルータには、ファスト イーサネット ポート FE0/0 および FE0/1 に関するハードウェア上の制限事項があります。半二重モードでトラフィックが許容量の 100% 以上（各方向に 5 Mbps 以上発生することと同等）になると、インターフェイスでは衝突の超過が発生し、1 秒ごとにリセットされます。この問題を回避するには、トラフィックを許容量の 100% 未満に抑える必要があります。

手順の概要

1. **enable**
2. **show ip interface brief**
3. **configure terminal**
4. **interface** {**fastethernet** | **gigabitethernet**} **0**/*port*
5. **description** *string*
6. **ip address** *ip-address mask*
7. **no shutdown**
8. **end**
9. **show ip interface brief**

詳細手順

	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 モードを開始します。 • 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 interface brief** **例：** `Router# show ip interface brief`	IP 用に設定された、インターフェイスの簡単なステータスを表示します。 • ルータのイーサネット インターフェイスのタイプ（ファスト イーサネットまたはギガビット イーサネット）を調べます。
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	**interface** {**fastethernet** | **gigabitethernet**} **0/***port*
	
	例：
	`Router(config)# interface fastethernet 0/1`
	
	例：
	`Router(config)# interface gigabitethernet 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。
		（注） インターフェイス番号については、ルータに付属のクイック スタート ガイドを参照してください。

ステップ 5	**description** *string* **例：** `Router(config-if)# description FE int to 2nd floor south wing`	（任意）インターフェイス コンフィギュレーションに説明を追加します。 • 説明を追加することにより、このインターフェイスに何が接続されているかを思いだしやすくなります。また、トラブルシューティングにも有益です。
ステップ 6	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 172.16.74.3 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	**no shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 8	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip interface brief** **例：** `Router# show ip interface brief`	IP 用に設定された、インターフェイスの簡単なステータスを表示します。 • イーサネット インターフェイスが動作しており、正しく設定されていることを確認します。

例

ファスト イーサネット インターフェイスの設定：例

```
!
interface FastEthernet0/0
 description FE int to HR group
 ip address 172.16.3.3 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
```

show ip interface brief コマンドの出力例

```
Router# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            172.16.3.3      YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Router#
```

次の作業

「デフォルト ルートまたはラスト リゾート ゲートウェイの指定」（P.9）に進んでください。

デフォルト ルートまたはラスト リゾート ゲートウェイの指定

ここでは、IP ルーティングをイネーブルにしたデフォルト ルートの指定方法を説明します。デフォルト ルートを指定する別の方法については、『*Configuring a Gateway of Last Resort Using IP Commands*』テクニカル ノートを参照してください。

Cisco IOS ソフトウェアでは、パケットに対してより適切なルートが他にない場合、または宛先がネットワークに接続されていない場合に、ラスト リゾート ゲートウェイ（ルータ）が使用されます。ここでは、ネットワークをデフォルト ルート（ラスト リゾート ゲートウェイを計算するための候補ルート）として選択する方法を説明します。ルーティング プロトコルがデフォルト ルート情報を伝播する方法は、各プロトコルで異なります。

IP ルーティングおよび IP ルーティング プロトコルの総合的な設定情報については、『*Cisco IOS IP Configuration Guide*』を参照してください。特に、「Configuring IP Addressing」の章および「Part 2: IP Routing Protocols」のすべての章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**]
5. **ip default-network** *network-number*
   または
   ip route *dest-prefix mask next-hop-ip-address*
6. **end**
7. **show ip route**

詳細手順

	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 モードを開始します。 • 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 routing** **例：** `Router(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 4	**ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**] **例：** `Router(config)# ip route 192.168.24.0 255.255.255.0 172.28.99.2`	スタティック ルートを確立させます。

ステップ 5	**ip default-network** *network-number*
	または
	ip route *dest-prefix mask next-hop-ip-address*
	
	例：
	`Router(config)# ip default-network 192.168.24.0`
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 172.28.99.1`
		ラスト リゾート ゲートウェイを計算するための候補ルートとして、ネットワークを 1 つ選択します。
		ラスト リゾート ゲートウェイを計算するため、ネットワーク 0.0.0.0 0.0.0.0 へのスタティック ルートを作成します。

ステップ 6	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip route** **例：** `Router# show ip route`	現在のルーティング テーブル情報を表示します。 • ラスト リゾート ゲートウェイが設定されていることを確認します。

例

デフォルト ルートの指定：例

```
!
ip routing
!
ip route 192.168.24.0 255.255.255.0 172.28.99.2
!
ip default-network 192.168.24.0
!
```

show ip route コマンドの出力例

```
Router# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is 172.28.99.2 to network 192.168.24.0

     172.24.0.0 255.255.255.0 is subnetted, 1 subnets
C       172.24.192.0 is directly connected, FastEthernet0
S       172.24.0.0 255.255.0.0 [1/0] via 172.28.99.0
S*    192.168.24.0 [1/0] via 172.28.99.2
     172.16.0.0 255.255.255.0 is subnetted, 1 subnets
C       172.16.99.0 is directly connected, FastEthernet1
Router#
```

次の作業

「リモート コンソール アクセス用の仮想端末回線の設定」（P.11）に進んでください。

リモート コンソール アクセス用の仮想端末回線の設定

仮想端末（vty）回線は、ルータへのリモート アクセスを許可するために使用されます。ここでは、仮想端末回線を設定してパスワードを指定し、許可されたユーザだけがリモートからルータにアクセスできるようにする方法を示します。

ルータには、デフォルトで 5 つの仮想端末回線があります。ただし、『Cisco IOS Terminal Services Configuration Guide』の「*Configuring Protocol Translation and Virtual Asynchronous Devices*」の章に示すように、仮想端末回線を追加で作成することもできます。

回線パスワードおよびパスワード暗号化の詳細については、『Cisco IOS Security Configuration Guide』の「*Configuring Passwords and Privileges*」の章を参照してください。『*Cisco IOS Password Encryption Facts*』テクニカル ノートも参照してください。

アクセス リストを使用して vty 回線をセキュリティ保護するには、『*Cisco IOS Security Configuration Guide*』の「Part 3: Traffic Filtering and Firewalls」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**
6. **end**
7. **show running-config**
8. 別のネットワーク デバイスから、ルータへの Telnet セッションを開始します。

詳細手順

	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 モードを開始します。 • 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	**line vty** *line-number* [*ending-line-number*] **例：** `Router(config)# line vty 0 4`	コンソールに対するリモート アクセスを実現するための仮想端末回線（vty）用のライン コンフィギュレーション コマンド コレクション モードを開始します。 • ルータ上のすべての vty 回線を必ず設定してください。 **（注）** ルータ上の vty 回線の数を確認するには、**line vty ?** コマンドを使用します。
ステップ 4	**password** *password* **例：** `Router(config-line)# password guessagain`	回線にパスワードを指定します。
ステップ 5	**login** **例：** `Router(config-line)# login`	ログイン時のパスワード チェックをイネーブルにします。
ステップ 6	**end** **例：** `Router(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** **例：** `Router# show running-config`	実行コンフィギュレーション ファイルを表示します。 • リモート アクセス用の仮想端末回線が正しく設定されていることを確認します。

ステップ 8	別のネットワーク デバイスから、ルータへの Telnet セッションを開始します。
	
	例：
	`Router# 172.16.74.3`
	`Password:`
		リモートからルータにアクセスできること、および仮想端末回線のパスワードが正しく設定されていることを確認します。

例

次に、仮想端末回線にパスワードを設定する例を示します。

```
!
line vty 0 4
 password guessagain
 login
!
```

次の作業

vty 回線を設定したら、次の手順を実行します。

- （任意）仮想端末回線のパスワードを暗号化するには、『Cisco IOS Security Configuration Guide』の「*Configuring Passwords and Privileges*」の章を参照してください。『*Cisco IOS Password Encryption Facts*』テクニカル ノートも参照してください。
- （任意）アクセス リストを使用して VTY 回線をセキュリティ保護するには、『*Cisco IOS Security Configuration Guide*』の「Part 3: Traffic Filtering and Firewalls」を参照してください。
- ルータ用の基本的なソフトウェア コンフィギュレーションを続けるには、「補助回線の設定」（P.13）に進みます。

補助回線の設定

ここでは、補助回線のライン コンフィギュレーション モードを開始する方法を説明します。補助回線の設定方法は、補助（AUX）ポートの実装に応じて変わります。補助回線の設定については、次のマニュアルを参照してください。

『*Configuring a Modem on the AUX Port for EXEC Dialin Connectivity*』テクニカル ノート

http://www.cisco.com/warp/public/471/mod-aux-exec.html

『*Configuring Dialout Using a Modem on the AUX Port*』設定例

http://www.cisco.com/warp/public/471/mod-aux-dialout.html

『*Connecting a SLIP/PPP Device to a Router's AUX Port*』テクニカル ノート

http://www.cisco.com/warp/public/701/6.html

『*Configuring AUX-to-AUX Port Async Backup with Dialer Watch*』設定例

http://www.cisco.com/warp/public/471/aux-aux-watch.html

『*Modem-Router Connection Guide*』テクニカル ノート

http://www.cisco.com/warp/public/76/9.html

手順の概要

1. **enable**
2. **configure terminal**
3. **line aux 0**
4. テクニカル ノートおよび設定例を参照して、独自の AUX ポートの実装に合った回線を設定してください。

詳細手順

	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 モードを開始します。 • 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	**line aux 0** **例：** `Router(config)# line aux 0`	補助回線用のライン コンフィギュレーション コマンド コレクション モードを開始します。
ステップ 4	テクニカル ノートおよび設定例を参照して、独自の AUX ポートの実装に合った回線を設定してください。	—

次の作業

「ネットワーク接続の確認」（P.14）に進んでください。

ネットワーク接続の確認

ここでは、ルータのネットワーク接続を確認する方法を説明します。

前提条件

- このマニュアルで説明したすべての設定作業を完了します。
- ルータは、正しく設定されたネットワーク ホストに接続されている必要があります。

手順の概要

1. **enable**
2. **ping** [*ip-address* | *hostname*]
3. **telnet** {*ip-address* | *hostname*}

詳細手順

	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 モードを開始します。 • 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	**ping** [*ip-address* | *hostname*] **例：** `Router# ping 172.16.74.5`	基本的なネットワーク接続を診断します。 • 接続を確認するには、設定済みの各インターフェイスのネクストホップ ルータまたは接続先ホストに対して ping を実行します。
ステップ 3	**telnet** {*ip-address* | *hostname*} **例：** `Router# telnet 10.20.30.40`	Telnet をサポートするホストにログインします。 • vty 回線のパスワードをテストする場合は、ルータの IP アドレスを使用して、別のネットワーク デバイスからこの手順を実行します。

例

次に、IP アドレス 192.168.7.27 に ping を実行した場合の ping コマンドの出力例を示します。

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

次に、IP ホスト名「donald」に ping を実行した場合の ping コマンドの出力例を示します。

```
Router# ping donald

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

次の作業

「ルータの設定の保存」（P.15）に進んでください。

ルータの設定の保存

ここでは、実行コンフィギュレーションを NVRAM のスタートアップ コンフィギュレーションに保存することによって、次回のシステム リロード時または電源の再投入時にコンフィギュレーションが失われないようにする方法を説明します。

手順の概要

1. **enable**
2. **copy running-config startup-config**

詳細手順

	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 モードを開始します。 • 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 running-config startup-config** **例：** `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に保存します。

次の作業

「コンフィギュレーションおよびシステム イメージのバックアップ コピーの保存」（P.16）に進んでください。

コンフィギュレーションおよびシステム イメージのバックアップ コピーの保存

ファイル破損時のファイルの復元を円滑にし、ダウンタイムを最小限に抑えるために、サーバ上のスタートアップ コンフィギュレーション ファイルおよびCisco IOS ソフトウェア システム イメージ ファイルのバックアップ コピーを保存することを推奨します。

詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』の「Managing Configuration Files」および「Loading and Maintaining System Images」の章を参照してください。

手順の概要

1. **enable**
2. **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**}
3. **show flash:**
4. **copy flash:** {**ftp:** | **rcp:** | **tftp:**}

詳細手順

	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 モードを開始します。 • 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 nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} **例：** `Router# copy nvram:startup-config ftp:`	スタートアップ コンフィギュレーション ファイルをサーバにコピーします。 • コンフィギュレーション ファイルのコピーは、バックアップ コピーとして使用できます。 • プロンプトが表示されたら、コピー先の URL を入力します。
ステップ 3	**show flash:** **例：** `Router# show flash:`	フラッシュ メモリ ファイル システムのレイアウトと内容を表示します。 • システム イメージ ファイルの名前を確認します。
ステップ 4	**copy flash:** {**ftp:** | **rcp:** | **tftp:**} **例：** `Router# copy flash: ftp:`	フラッシュ メモリからサーバにファイルをコピーします。 • バックアップ コピーとして使用するシステム イメージ ファイルをサーバにコピーします。 • プロンプトが表示されたら、ファイル名とコピー先 URL を入力します。

例

TFTP サーバへのスタートアップ コンフィギュレーションのコピー：例

次の例では、TFTP サーバにスタートアップ コンフィギュレーションをコピーします。

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

フラッシュ メモリから TFTP サーバへのコピー：例

次に、特権 EXEC モードで **show flash:** コマンドを使用してシステム イメージ ファイル名を確認し、**copy flash: tftp:** 特権 EXEC コマンドを使用してシステム イメージ（c3640-2is-mz）を TFTP サーバにコピーする方法を示します。ルータではデフォルトのユーザ名とパスワードが使用されます。

```
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.
```

関連情報

- 基本的なソフトウェア コンフィギュレーションが完了したら、ルータを保護するため、ルーティング プロトコルかアクセス リストの実装を検討するか、その他のセキュリティ強化策を検討します。「関連資料：その他の設定」（P.19）に記載されているマニュアルを参照してください。
- ルータの機能を設定するには、「機能マニュアルの検索」を参照してください。

その他の参考資料

ここでは、Cisco IOS CLI を使用した基本的なソフトウェア コンフィギュレーションに関連する資料について説明します。

関連資料：基本的なソフトウェア コンフィギュレーション

トピック	関連するマニュアルのタイトルまたはリンク
シャーシの設置、ケーブルの接続、電源投入の手順、およびインターフェイスの番号付け	ご使用のルータのクイック スタート ガイド
Cisco Security Device Manager（SDM）	http://www.cisco.com/go/sdm
ルータのホスト名を割り当てるためのガイドライン	RFC 1035、「*Domain Names—Implementation and Specification*」 RFC 1178、「*Choosing a Name for Your Computer*」
アクセス リスト、パスワード、および特権	『*Cisco IOS Security Configuration Guide*』
パスワードおよびパスワードの暗号化	『*Cisco IOS Password Encryption Facts*』テクニカル ノート
シスコ製品のパスワード回復手順	『Password Recovery Procedures』
コンソール回線の設定、コンフィギュレーション ファイルの管理、およびシステム イメージのロードおよび維持	『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』
インターフェイスの設定	『*Cisco IOS Interface and Hardware Component Configuration Guide*』
IP ルーティングおよび IP ルーティング プロトコル	『*Cisco IOS IP Configuration Guide*』
デフォルト ルートまたはラスト リゾート ゲートウェイの設定	『*Configuring a Gateway of Last Resort Using IP Commands*』テクニカル ノート

トピック	関連するマニュアルのタイトルまたはリンク
仮想端末回線の設定	『*Cisco IOS Terminal Services Configuration Guide*』
補助（AUX）ポートの設定	『*Configuring a Modem on the AUX Port for EXEC Dialin Connectivity*』テクニカル ノート 『*Configuring Dialout Using a Modem on the AUX Port*』設定例 『*Connecting a SLIP/PPP Device to a Router's AUX Port*』テクニカル ノート 『*Configuring AUX-to-AUX Port Async Backup with Dialer Watch*』設定例 『*Modem-Router Connection Guide*』テクニカル ノート

関連資料：その他の設定

トピック	関連するマニュアルのタイトルまたはリンク
セキュリティ強化のため、ルータ上（特に境界ルータ上）でネットワーク管理者が変更を検討すべきシスコのコンフィギュレーション設定	『*Improving Security on Cisco Routers*』テクニカル ノート **（注）** このマニュアルを表示するには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。
IP ルーティングおよび IP ルーティング プロトコル	『*Cisco IOS IP Configuration Guide*』
アクセス リスト	『*Cisco IOS Security Configuration Guide*』

シスコのテクニカル サポート

説明	リンク
Technical Assistance Center（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