



CLI セットアッププログラムによるスイッチの設定

- [初期設定情報の入力 \(1 ページ\)](#)

初期設定情報の入力

この章では、スイッチのコマンドラインインターフェイス (CLI) ベースのセットアップ手順について説明します。

スイッチを設定するには、セットアッププログラムを完了する必要があります。セットアッププログラムは、スイッチの電源がオンになると自動的に実行されます。スイッチがローカルルータやインターネットと通信するのに必要な IP アドレスやその他の設定情報を割り当てる必要があります。この情報は、WebUI を使用してスイッチを設定および管理する場合にも必要です。

Cisco IOS XE 17.10.1 以降では、ユーザーのパスワードがプレーンテキストで保存されないように、パスワード暗号化レベルを設定することができます。「[システムセキュリティ設定 \(Cisco IOS XE 17.10.1 以降\) \(4 ページ\)](#)」を参照してください。

スイッチを電源に接続する前に、「[警告](#)」を参照して安全に関する注意事項を確認してください。

スイッチのコンソールポートに PC を接続するには、[コンソールポートへの PC または端末の接続](#)を参照してください。

IP とパスワードの設定

セットアッププログラムを完了するには、ネットワーク管理者から次の情報を入手しておく必要があります。

- 暗号化レベルとマスターキー (Cisco IOS XE 17.10.1 以降)
- スwitchの IP アドレス
- サブネットマスク (IP ネットマスク)

- デフォルト ゲートウェイ (ルータ)
- イネーブル シークレット パスワード
- イネーブル パスワード
- SSH パスワード

初期設定 (Cisco IOS XE 17.9.x 以前)

セットアッププログラムを使用して、スイッチの初期設定を行う手順は次のとおりです。

1. 次の2つのプロンプトで **Yes** と入力します。

```
Would you like to enter the initial 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
```

2. スイッチのホスト名を入力し、**Return** を押します。

指定できるホスト名の文字数は、コマンドスイッチでは28文字、メンバスイッチでは31文字に制限されています。どのスイッチでも、ホスト名の最終文字として **-n** (nは数字) を使用しないでください。

```
Enter host name [Switch]: host_name
```

3. イネーブル シークレット パスワードを入力し、**Return** を押します。

このパスワードは1～25文字の英数字で指定できます。先頭の文字を数字にしてもかまいません。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。シークレットパスワードは暗号化されますが、イネーブルパスワードはプレーンテキストです。

```
Enter enable secret: secret_password
```

4. イネーブルパスワードを入力し、**Return** を押します。

```
Enter enable password: enable_password
```

5. 仮想端末パスワードを入力し、**Return** を押します。

このパスワードは1～25文字の英数字で指定できます。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。

```
Enter virtual terminal password: terminal_password
```

6. (任意) プロンプトに従って、簡易ネットワーク管理プロトコル (SNMP) を設定します。後から、CLI、Device Manager、または Cisco Network Assistant アプリケーションを使用して SNMP を設定することもできます。SNMP を後で設定する場合は、**no** と入力します。

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

7. 管理ネットワークに接続するインターフェイスのインターフェイス名 (物理的なインターフェイスまたは VLAN (仮想 LAN) の名前) を入力して、**Return** を押します。このリリースでは、インターフェイス名には必ず **vlan1** を使用します。



- (注) スイッチは、**vlan1** インターフェイス上で DHCP 検出メッセージを送信します。CLI の初期セットアッププロセスが開始される前にスイッチがネットワークに接続されている場合は、インターフェイスにダイナミック IP アドレスが割り当てられている可能性があります。**vlan1** インターフェイスに IP アドレスが表示されていなくても問題ありません。このプロセスでは、動的に割り当てられた IP アドレスを上書きする管理用の静的 IP アドレスを設定できます。

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned NO unset up down
GigabitEthernet1/1 unassigned YES unset down down
GigabitEthernet1/2 unassigned YES unset down down
GigabitEthernet1/3 unassigned YES unset down down
GigabitEthernet1/4 unassigned YES unset down down
GigabitEthernet1/5 unassigned YES unset down down
GigabitEthernet1/6 unassigned YES unset down down
GigabitEthernet1/7 unassigned YES unset down down
GigabitEthernet1/8 unassigned YES unset down down
GigabitEthernet1/9 unassigned YES unset down down
GigabitEthernet1/10 unassigned YES unset down down
Enter interface name used to connect to the
management network from the above interface summary: vlan1
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

8. スイッチの IP アドレスとサブネットマスクを入力し、**Return** キーを押してインターフェイスを設定します。ここに示す IP アドレスとサブネットマスクは一例です。

```
Configuring interface Vlan1:
Configure IP on this interface? [yes]:
IP address for this interface: 10.1.1.2
Subnet mask for this interface [255.255.255.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /24
```

9. 次のサマリーが表示されます。

```
The following configuration command script was created:
hostname ie3300
enable secret 9 $9$rkqtjJhIkZyANU$Ib4nfuxrPHBi.lixF.0Ir94k9XWYsW3nyF7Glmc6lkc
enable password cisco
line vty 0 15
password cisco
no snmp-server
!!
interface Vlan1
no shutdown
```

```
ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/9
!
interface GigabitEthernet1/10
!
end
```

セットアッププログラムが完了すると、スイッチは作成されたデフォルト設定を実行できます。次のいずれかのツールを使用すれば、この設定の変更や他の管理タスクを実行できます。

- コマンドライン インターフェイス (CLI)

CLI を使用するには、端末エミュレーションプログラムを使用してコンソールポートから Switch> プロンプトにコマンドを入力します。設定情報については、スイッチの『[Cisco Catalyst IE3x00 Rugged Switch software configuration guides](#)』を参照してください。

システムセキュリティ設定 (Cisco IOS XE 17.10.1 以降)

セキュリティを強化するには、パスワードなどの機密情報を暗号化する必要があります。設定ダイアログには、パスワード暗号化レベルを設定できる [System Security Configuration Dialog] が含まれています。暗号化レベルには、タイプ 6 およびタイプ 7 の暗号化が含まれます。両方のタイプを有効にすることをお勧めします。

- タイプ 6 は、パスワードの暗号化に Advanced Encryption Standard (AES) を使用します。タイプ 6 パスワードの暗号化と暗号解読は、入力するマスターキーと結合されます。マスターキーはリカバリできないため、記憶しておく必要があります。
- マスターキーは、AES 対称暗号を使用してスイッチ設定内の他のすべてのキーを暗号化するために使用されるパスワード/キーです。マスターキーはスイッチ設定には保存されず、スイッチに接続したとしてもどのような方法でも表示も取得もできません。設定されると、マスターキーを使用して、スイッチ設定内の既存または新しいキーが暗号化されます。 **password encryption aes** コマンドを実行するまで、キーは暗号化されません。
- タイプ 7 パスワードは、元のプレーンテキストパスワードを難読化したものです。これは ヴィジュネル暗号に基づいており、設定内の実際のパスワードが誰かに見られるのを防ぎます。

セットアッププログラムを使用して、新しいスイッチと設定済みのスイッチの両方でパスワード暗号化レベルを設定できます。新しいスイッチについては、[初期設定 - タイプ6暗号化 \(5ページ\)](#) または [初期設定 - タイプ7暗号化 \(8ページ\)](#) を参照してください。初期セットアップを実行せずにシステムセキュリティ設定を設定するには、[パスワード暗号化レベルの設定 \(11ページ\)](#) を参照してください。

初期設定 - タイプ6暗号化

タイプ6暗号化とセットアッププログラムを使用して、スイッチの初期設定を行う手順は次のとおりです。

始める前に

[コンソールポートへのPCまたは端末の接続](#)の説明に従ってCLIにアクセスします。

手順

ステップ1 次のプロンプトで **Yes** を入力します。

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

ステップ2 プロンプトで、適用するパスワード暗号化レベルを入力します。

```
-----System Security Configuration Dialog-----  
  
Cisco recommends that for enhanced security users should encrypt sensitive info  
The configuration dialog will allow you to set encryption level  
It is recommended that both type-6 & type-7 encryption should be enabled by user  
For type-6 user will need to create and remember Master key as it cannot be recovered  
  
[0] for both type-6 & type-7 encryption to be applied on the box  
[1] for only type-7 encryption to be applied on the box  
[2] for no encryption to be applied on the box  
  
Enter your encryption selection [2]: 0
```

(注) Cisco IOS XE 17.10.1 では、タイプ6とタイプ7の両方の暗号化[0]を選択すると、ユーザー名のみがタイプ6に自動的に変換され、イネーブルパスワードと回線 vty パスワードはタイプ6ではなくタイプ7に自動的に変換されます。

ステップ3 スイッチの他のすべてのキーの暗号化に使用するマスターキーを入力します。

```
Enter the Master key min 8 chars & max 127 chars, Master key should not begin with '!',  
#, ;' : *****
```

ステップ4 マスターキーをもう一度入力して確定します。

```
Confirm the master key: *****  
  
The following configuration command script was created:  
  
key config-key password-encrypt
```

```
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

(注) このデバイスを交換する場合に必要なため、マスターキーは保存しておく必要があります。

ステップ 5 プロンプトで **2** を入力して、システムセキュリティ設定を保存します。

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

ステップ 6 プロンプトで **yes** と入力して、基本管理設定を設定します。

```
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
Configuring global parameters:
```

ステップ 7 スイッチのホスト名を入力します。

```
Enter host name [Switch]: Switch123
```

ステップ 8 イネーブル シークレット パスワードを入力します。

```
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.
-----
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-----
Enter enable secret: *****
```

ステップ 9 イネーブル シークレット パスワードをもう一度入力して確定します。

```
Confirm enable secret: *****
```

ステップ 10 イネーブルパスワードを入力します。

```
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 11 仮想端末のパスワードを入力します。

このパスワードは 1 ～ 25 文字の英数字で指定できます。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。

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

ステップ 12 管理ネットワークに接続するインターフェイスのインターフェイス名（物理的なインターフェイスまたは VLAN（仮想 LAN）の名前）を入力します。このリリースでは、インターフェイス名には必ず **vlan1** を使用します。

(注) スイッチは、**vlan1** インターフェイス上で DHCP 検出メッセージを送信します。CLI の初期セットアッププロセスが開始される前にスイッチがネットワークに接続されている場合は、インターフェイスにダイナミック IP アドレスが割り当てられている可能性があります。**vlan1** インターフェイスに IP アドレスが表示されていなくても問題ありません。このプロセスでは、動的に割り当てられた IP アドレスを上書きする管理用の静的 IP アドレスを設定できます。

```
Current interface summary
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	10.16.1.120	YES	DHCP	up	up
GigabitEthernet1/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	down	down
GigabitEthernet1/3	unassigned	YES	unset	up	up
GigabitEthernet1/4	unassigned	YES	unset	down	down
GigabitEthernet1/5	unassigned	YES	unset	down	down
GigabitEthernet1/6	unassigned	YES	unset	down	down
GigabitEthernet1/7	unassigned	YES	unset	up	up
GigabitEthernet1/8	unassigned	YES	unset	up	up
GigabitEthernet1/9	unassigned	YES	unset	down	down
GigabitEthernet1/10	unassigned	YES	unset	down	down
AppGigabitEthernet1/1	unassigned	YES	unset	up	up

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

```
Configuring interface Vlan1:
```

```
IP address for this interface [10.16.1.120]:
Subnet mask for this interface [255.0.0.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /8
```

```
The following configuration command script was created:
```

```
hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JV0k$Cwi3/tNTc7uHy7CBsBf0Wo6ulq/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
```

```
interface GigabitEthernet1/1
!  
interface GigabitEthernet1/2
!  
interface GigabitEthernet1/3
!  
interface GigabitEthernet1/4
```

ステップ 13 設定を保存するには、**2** と入力します。

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

```
Press RETURN to get started!
```

次のタスク

セットアップ プログラムが完了すると、スイッチは作成されたデフォルト設定を実行できます。次のいずれかのツールを使用すれば、この設定の変更や他の管理タスクを実行できます。

- コマンドライン インターフェイス (CLI)
- Web ユーザインターフェイス (WebUI)

CLIを使用するには、端末エミュレーションプログラムを使用してコンソールポートから、または Telnet を使用してネットワークから、*Switch* > プロンプトにコマンドを入力します。設定情報については、[Cisco IE3x00 スイッチの設定ガイド](#)を参照してください。

WebUIを使用するには、WebUI のオンライン ヘルプを参照してください。

初期設定 - タイプ7 暗号化

タイプ7暗号化のみとセットアッププログラムを使用して、スイッチの初期設定を行う手順は次のとおりです。

始める前に

[コンソール ポートへの PC または端末の接続](#) の説明に従って CLI にアクセスします。

手順

ステップ 1 次のプロンプトで **Yes** を入力します。


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

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

ステップ2 プロンプトで **1** を入力して、タイプ7パスワード暗号化のみを適用します。

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

```
Cisco recommends that for enhanced security users should encrypt sensitive info
The configuration dialog will allow you to set encryption level
It is recommended that both type-6 & type-7 encryption should be enabled by user
For type-6 user will need to create and remember Master key as it cannot be recovered
```

```
[0] for both type-6 & type-7 encryption to be applied on the box
[1] for only type-7 encryption to be applied on the box
[2] for no encryption to be applied on the box
```

```
Enter your encryption selection [2]: 1
```

ステップ3 プロンプトで **2** を入力して、システムセキュリティ構成を保存します。

```
[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
```

```
Building configuration...
```

```
[OK]
```

```
Use the enabled mode 'configure' command to modify this configuration.
```

ステップ4 プロンプトで **yes** と入力して、基本管理設定を設定します。

```
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
Configuring global parameters:
```

ステップ5 スイッチのホスト名を入力します。

```
Enter host name [Switch]: Switch123
```

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。

```
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.
```

```
-----
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-----
```

```
Enter enable secret: *****
```

ステップ7 イネーブルシークレットパスワードをもう一度入力して確定します。

```
Confirm enable secret: *****
```

ステップ 8 イネーブルパスワードを入力します。

```
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 9 仮想端末のパスワードを入力します。

このパスワードは 1～25 文字の英数字で指定できます。大文字と小文字が区別されます。スペースも使えますが、先頭のスペースは無視されます。

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

```
Enter virtual terminal password: *****
```

ステップ 10 管理ネットワークに接続するインターフェイスのインターフェイス名（物理的なインターフェイスまたは VLAN（仮想 LAN）の名前）を入力します。このリリースでは、インターフェイス名には必ず **vlan1** を使用します。

(注) スイッチは、**vlan1** インターフェイス上で DHCP 検出メッセージを送信します。CLI の初期セットアッププロセスが開始される前にスイッチがネットワークに接続されている場合は、インターフェイスにダイナミック IP アドレスが割り当てられている可能性があります。**vlan1** インターフェイスに IP アドレスが表示されていなくても問題ありません。このプロセスでは、動的に割り当てられた IP アドレスを上書きする管理用の静的 IP アドレスを設定できます。

```
Current interface summary
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	10.16.1.120	YES	DHCP	up	up
GigabitEthernet1/1	unassigned	YES	unset	up	up
GigabitEthernet1/2	unassigned	YES	unset	down	down
GigabitEthernet1/3	unassigned	YES	unset	up	up
GigabitEthernet1/4	unassigned	YES	unset	down	down
GigabitEthernet1/5	unassigned	YES	unset	down	down
GigabitEthernet1/6	unassigned	YES	unset	down	down
GigabitEthernet1/7	unassigned	YES	unset	up	up
GigabitEthernet1/8	unassigned	YES	unset	up	up
GigabitEthernet1/9	unassigned	YES	unset	down	down
GigabitEthernet1/10	unassigned	YES	unset	down	down
AppGigabitEthernet1/1	unassigned	YES	unset	up	up

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1
```

```
Configuring interface Vlan1:
```

```
IP address for this interface [10.16.1.120]:
Subnet mask for this interface [255.0.0.0] :
Class A network is 10.0.0.0, 8 subnet bits; mask is /8
```

```
The following configuration command script was created:
```

```
hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVok$Cwi3/tNTc7uHy7CBsBfOWo6ulq/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
```

```
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 10.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4
```

ステップ 11 設定を保存するには、**2** と入力します。

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

Press RETURN to get started!

次のタスク

セットアッププログラムが完了すると、スイッチは作成されたデフォルト設定を実行できます。次のいずれかのツールを使用すれば、この設定の変更や他の管理タスクを実行できます。

- コマンドラインインターフェイス (CLI)
- Web ユーザインターフェイス (WebUI)

CLIを使用するには、端末エミュレーションプログラムを使用してコンソールポートから、または Telnet を使用してネットワークから、*Switch* > プロンプトにコマンドを入力します。設定情報については、[Cisco IE3x00 スイッチの設定ガイド](#)を参照してください。

WebUI を使用するには、WebUI のオンライン ヘルプを参照してください。

パスワード暗号化レベルの設定

この手順に従って、初期セットアップを実行せずにシステムセキュリティ設定（タイプ6およびタイプ7暗号化）を設定します。

手順

ステップ1 次のプロンプトで **No** を入力します。

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

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1

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

ステップ2 プロンプトでイネーブルシークレットを入力します。

```
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.
-----
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-----
Enter enable secret: *****
Confirm enable secret: *****

The following configuration command script was created:

enable secret 9 $9$YMkVvPLbxKn4bE$OAOX/akBBsukkRV1L.Tk7p2KaM0BXLQI.HbyGbXB8/g
!
end
```

ステップ3 **2** を入力して設定を保存し、システムセキュリティ設定に移動します。

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

ステップ4 プロンプトで、適用するパスワード暗号化レベルを入力します。

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

Cisco recommends that for enhanced security users should encrypt sensitive info
The configuration dialog will allow you to set encryption level
It is recommended that both type-6 & type-7 encryption should be enabled by user
For type-6 user will need to create and remember Master key as it cannot be recovered

[0] for both type-6 & type-7 encryption to be applied on the box
[1] for only type-7 encryption to be applied on the box
[2] for no encryption to be applied on the box

Enter your encryption selection [2]: 0
```

ステップ5 スイッチの他のすべてのキーの暗号化に使用するマスターキーを入力します。

```
Enter the Master key min 8 chars & max 127 chars, Master key should not begin with '!',
#, ;' : *****
```

ステップ6 マスターキーをもう一度入力して確認します。

```
Confirm the master key: *****
```

```
The following configuration command script was created:
```

```
key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
end
```

(注) このデバイスを交換する場合には必要になるため、マスターキーは保存しておく必要があります。

ステップ7 プロンプトで 2 を入力して、システムセキュリティ設定を保存します。

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

```
Press RETURN to get started!
```

```
Switch>
```

CLI セットアップの例

初期設定の例

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

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

-----System Security Configuration Dialog-----

Cisco recommends that for enhanced security users should encrypt sensitive info
The configuration dialog will allow you to set encryption level
It is recommended that both type-6 & type-7 encryption should be enabled by user
For type-6 user will need to create and remember Master key as it cannot be recovered

[0] for both type-6 & type-7 encryption to be applied on the box
[1] for only type-7 encryption to be applied on the box
```

```
[2] for no encryption to be applied on the box

Enter your encryption selection [2]: 0

Enter the Master key min 8 chars & max 127 chars, Master key should not begin with '!',
#, ;' : *****

Confirm the master key: *****

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
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]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

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 [Switch]: Switch123

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.
-----
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-----
Enter enable secret: *****
Confirm enable secret: *****

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: *****

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

```

Enter virtual terminal password: *****

Current interface summary

Interface                IP-Address      OK? Method Status      Protocol
Vlan1                    12.16.1.120    YES DHCP    up          up
GigabitEthernet1/1      unassigned     YES unset   up          up
GigabitEthernet1/2      unassigned     YES unset   down       down
GigabitEthernet1/3      unassigned     YES unset   up          up
GigabitEthernet1/4      unassigned     YES unset   down       down
GigabitEthernet1/5      unassigned     YES unset   down       down
GigabitEthernet1/6      unassigned     YES unset   down       down
GigabitEthernet1/7      unassigned     YES unset   up          up
GigabitEthernet1/8      unassigned     YES unset   up          up
GigabitEthernet1/9      unassigned     YES unset   down       down
GigabitEthernet1/10     unassigned     YES unset   down       down
AppGigabitEthernet1/1  unassigned     YES unset   up          up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  IP address for this interface [12.16.1.120]:
  Subnet mask for this interface [255.0.0.0] :
  Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JVok$Cwi3/tNTc7uHy7CBsBfOWo6ulq/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface GigabitEthernet1/3
!
interface GigabitEthernet1/4

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

Press RETURN to get started!

```

システムセキュリティ設定の例

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

Would you like to enter the initial configuration dialog? [yes/no]:
Autoinstall trying DHCPv6 on Vlan1  yes

-----System Security Configuration Dialog-----

Cisco recommends that for enhanced security users should encrypt sensitive info
The configuration dialog will allow you to set encryption level
It is recommended that both type-6 & type-7 encryption should be enabled by user
For type-6 user will need to create and remember Master key as it cannot be recovered

[0] for both type-6 & type-7 encryption to be applied on the box
[1] for only type-7 encryption to be applied on the box
[2] for no encryption to be applied on the box

Enter your encryption selection [2]: 0

Enter the Master key min 8 chars & max 127 chars, Master key should not begin with '!,
#, ;' : *****

Confirm the master key: *****

The following configuration command script was created:

key config-key password-encrypt
Testkey12345
!
password encryption aes
service password-encryption
!
!
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]: 2
Building configuration...
[OK]
Use the enabled mode 'configure' command to modify this configuration.

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 [Switch]: Switch123

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.
-----
secret should be of minimum 10 characters and maximum 32 characters with
at least 1 upper case, 1 lower case, 1 digit and
should not contain [cisco]
-----
Enter enable secret: *****
Confirm enable secret: *****

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: *****

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

Current interface summary

Interface                IP-Address      OK? Method Status          Protocol
Vlan1                    12.16.1.120    YES DHCP    up              up
GigabitEthernet1/1      unassigned     YES unset    up              up
GigabitEthernet1/2      unassigned     YES unset    down            down
GigabitEthernet1/3      unassigned     YES unset    up              up
GigabitEthernet1/4      unassigned     YES unset    down            down
GigabitEthernet1/5      unassigned     YES unset    down            down
GigabitEthernet1/6      unassigned     YES unset    down            down
GigabitEthernet1/7      unassigned     YES unset    up              up
GigabitEthernet1/8      unassigned     YES unset    up              up
GigabitEthernet1/9      unassigned     YES unset    down            down
GigabitEthernet1/10     unassigned     YES unset    down            down
AppGigabitEthernet1/1  unassigned     YES unset    up              up

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  IP address for this interface [12.16.1.120]:
  Subnet mask for this interface [255.0.0.0] :
  Class A network is 12.0.0.0, 8 subnet bits; mask is /8

The following configuration command script was created:

hostname Switch123
enable secret 9 $9$4kYFyV4Hh9JV0k$Cwi3/tNTc7uHy7CBsBfOWo6u1q/Sg07in3NJ5e7Yy0U
enable password 0 password
service password-encryption
line vty 0 15
password 0 password
no snmp-server
!
!
interface Vlan1
no shutdown
ip address 12.16.1.120 255.0.0.0
!
interface GigabitEthernet1/1

```

```
!  
interface GigabitEthernet1/2  
!  
interface GigabitEthernet1/3  
!  
interface GigabitEthernet1/4  
  
[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  
Building configuration...  
[OK]  
Use the enabled mode 'configure' command to modify this configuration.  
  
Press RETURN to get started!
```

翻訳について

このドキュメントは、米国シスコ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。