暗号化事前共有鍵

暗号化事前共有鍵機能を使用すると、プレーンテキストのパスワードをタイプ 6（暗号化）形式で NVRAM へセキュアに保存できます。

暗号化事前共有鍵の機能履歴

リリース	変更点
12.3(2)T	この機能が追加されました。

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

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。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。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の場合は、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

暗号化事前共有鍵の制約事項

- 旧来の ROM Monitor（ROMMON; ROM モニタ）やブート イメージでは、新たに導入されたタイプ 6 のパスワードを認識できません。そのため、旧来の ROMMON から起動すると、エラーが発生します。
- Cisco 836 ルータでは、Advanced Encryption Standard（AES; 高度暗号化規格）を使用できるのは IP Plus イメージ上に限ります。

暗号化事前共有鍵について

暗号化事前共有キーを使用するためには、次に説明する事柄について十分な知識が必要です。

- 「暗号化事前共有鍵を使用したパスワードのセキュアな保存」（P.2）
- 「暗号化事前共有キーの設定方法」（P.3）

暗号化事前共有鍵を使用したパスワードのセキュアな保存

暗号化事前共有鍵機能を使用すると、Command-Line Interface（CLI; コマンドライン インターフェイス）から、プレーンテキストのパスワードをタイプ 6 形式で NVRAM へセキュアに保存できます。タイプ 6 のパスワードは暗号化されています。暗号化されたパスワード自体を、確認したり取得したりすることは可能ですが、それを復号化して実際のパスワードを特定することは困難です。**key config-key password-encryption** コマンドおよび **password encryption aes** コマンドを使用すると、パスワードを設定してイネーブルにできます（鍵の暗号化には、対称鍵暗号である AES が使用されます）。**config-key password-encryption** コマンドを使用して設定されたパスワード（鍵）は、ルータ内のその他すべての鍵を暗号化するマスター暗号鍵として使用されます。

password encryption aes コマンドを設定する際、同時に **key config-key password-encryption** コマンドを設定しないと、**show running-config** コマンドや **copy running-config startup-config** コマンドなどが設定されている起動時や Nonvolatile Generation（NVGEN; 不揮発性生成）プロセス中に次のようなメッセージが出力されます。

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

パスワードの変更

key config-key password-encryption コマンドを使用してパスワード（マスター鍵）が変更された場合、または再暗号化された場合には、リスト レジストリから、タイプ 6 暗号が使用されているアプリケーション モジュールへ、変更前の鍵と変更後の鍵が渡されます。

パスワードの削除

key config-key password-encryption コマンドを使用して設定されたマスター鍵がシステムから削除されると、タイプ 6 のパスワードすべてが使用不可になるという内容の警告が出力されます（同時に、確認用のプロンプトも表示されます）。いったん暗号化されたパスワードは、セキュリティ対策上、Cisco IOS ソフトウェアにおいて復号化されることはありません。ただし、すでに説明したように、パスワードを再暗号化することはできます。

注意 **key config-key password-encryption** コマンドを使用して設定されたパスワードは、一度失われると回復できません。パスワードは、安全な場所に保存することを推奨します。

パスワード暗号化の設定解除

no password encryption aes コマンドを使用してパスワード暗号化の設定を解除しても、既存のタイプ 6 パスワードはいずれも変更されません。またタイプ 6 パスワードは、**key config-key password-encryption** コマンドを使用して設定されたパスワード（マスター鍵）が存在する限り、アプリケーションからの要求に応じて復号化されます。

パスワードの保存

（**key config-key password-encryption** コマンドを使用して設定された）パスワードは誰にも「判読」できないため、ルータからパスワードを取得する方法はありません。既存の管理ステーションでは、その内部に鍵が格納されるような機能を有効にすることで初めて、パスワードの内容を「知る」ことができます。その場合には、管理ステーション内部にパスワードをセキュアに保存する必要があります。TFTP を使用して保存された設定は、スタンドアロンではないため、ルータにはロードできません。設定をルータにロードする前後には、（**key config-key password-encryption** コマンドを使用して）パスワードを手動で追加する必要があります。このパスワードは、保存された設定に手動で追加できますが、それによって設定内のすべてのパスワードを誰もが復号化できるようになるため、手動によるパスワードの追加は行わないことを推奨します。

新規パスワードまたは不明パスワードの設定

入力またはカット アンド ペーストした暗号文は、それがマスター鍵に適合しない場合やマスター鍵が存在しない場合でも、受理または保存されます。ただしこの場合にはアラート メッセージが出力されます。アラート メッセージの内容は次のとおりです。

```
“ciphertext>[for username bar>] is incompatible with the configured master key.”
```

マスター鍵を新規に設定すると、プレーンテキストの鍵はすべて暗号化され、タイプ 6 の鍵になります。すでにタイプ 6 である鍵は暗号化されず、現在の状態が維持されます。

既存のマスター鍵が失われた場合、またはその内容が不明の場合は、**no key config-key password-encryption** コマンドを使用してそのマスター鍵を削除できます。**no key config-key password-encryption** コマンドを使用してマスター鍵を削除しても、既存の暗号化パスワードは、暗号化された状態のままルータの設定内に保持されます。これらのパスワードは復号化されません。

暗号化事前共有キーのイネーブル化

password encryption aes コマンドを使用すると、暗号化パスワードをイネーブルにできます。

暗号化事前共有キーの設定方法

ここでは、次の各手順について説明します。

- 「暗号化事前共有鍵の設定」（P.4）（必須）
- 「暗号化事前共有鍵のモニタリング」（P.5）（任意）
- 「ISAKMP 事前共有鍵の設定」（P.6）（任意）
- 「ISAKMP 鍵リングの ISAKMP 事前共有鍵の設定」（P.7）（任意）
- 「ISAKMP アグレッシブ モードの設定」（P.8）（任意）

- 「Unity サーバ グループ ポリシーの設定」（P.9）（任意）
- 「Easy VPN クライアントの設定」（P.10）（任意）

暗号化事前共有鍵の設定

暗号化事前共有鍵を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key config-key password-encryption** [*text*]
4. **password encryption aes**

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	**key config-key password-encryption** [*text*] **例：** `Router (config)# key config-key password-encryption`	タイプ 6 の暗号鍵をプライベート NVRAM に保存します。 • （Enter キーを使用して）インタラクティブにキーボード操作を行う場合、暗号鍵がすでに存在すれば、Old key、New key、Confirm key という 3 つのプロンプトが表示されます。 • インタラクティブにキーボード操作を行う場合、暗号鍵が存在しなければ、New key、Confirm key という 2 つのプロンプトが表示されます。 • すでに暗号化されているパスワードを削除する場合は、「WARNING: All type 6 encrypted keys will become unusable.Continue with master key deletion?[yes/no]:」というプロンプトが表示されます。
ステップ 4	**password encryption aes** **例：** `Router (config)# password-encryption aes`	暗号化事前共有鍵のイネーブル化

トラブルシューティングのヒント

「ciphertext >[for username bar>] is incompatible with the configured master key」という警告メッセージが表示された場合は、入力またはカット アンド ペーストした暗号文がマスター鍵に適合しないか、またはマスター鍵が存在しないと判断できます（暗号文は受理または保存されます）。この警告メッセージを手掛かりにすれば、設定の不具合箇所を特定できます。

暗号化事前共有鍵のモニタリング

暗号化事前共有鍵に関するロギングを出力するには、次の手順を実行します。

1. **enable**
2. **password logging**

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	**password logging** **例：** `Router# password logging`	タイプ 6 パスワードの処理に関するデバッグ出力のログを表示します。

例

次に示すのは、**password logging** によるデバッグ出力の表示例です。ここでは、マスター鍵が新規に設定された場合と、その新しいマスター鍵を使用してその他の鍵が暗号化された場合が表示されています。

```
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:40:57: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master keypas

Router (config)# key config-key password-encrypt
Old key:
New key:
Confirm key:
Router (config)#
01:42:11: TYPE6_PASS: Master key change heralded, re-encrypting the keys
with the new master key
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
01:42:11: TYPE6_PASS: Mac verification successful
```

次の作業

次に示す作業を実行できます。これらの各作業は、互いに独立したものです。

- 「ISAKMP 事前共有鍵の設定」（P.6）
- 「ISAKMP 鍵リングの ISAKMP 事前共有鍵の設定」（P.7）
- 「ISAKMP アグレッシブ モードの設定」（P.8）
- 「Unity サーバ グループ ポリシーの設定」（P.9）
- 「Easy VPN クライアントの設定」（P.10）

ISAKMP 事前共有鍵の設定

ISAKMP 事前共有鍵を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp key** *keystring* **address** *peer-address*
4. **crypto isakmp key** *keystring* **hostname** *hostname*

手順の詳細

	コマンド	説明
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 isakmp key** *keystring* **address** *peer-address* **例：** `Router (config)# crypto isakmp key cisco address 10.2.3.4`	事前共有認証キーを設定します。 • *peer-address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 4	**crypto isakmp key** *keystring* **hostname** *hostname* **例：** `Router (config)# crypto isakmp key foo hostname foo.com`	事前共有認証キーを設定します。 • *hostname* 引数には、ピアの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を指定します。

例

次に示すのは、暗号化事前共有鍵が設定された場合の出力例です。

```
crypto isakmp key 6 _Hg[^^ECgLGGPF^RXTQfDDWQ][YAAB address 10.2.3.4
crypto isakmp key 6 `eR\eTRaKCUZPYYQfDgXRWi_AAB hostname foo.com
```

ISAKMP 鍵リングの ISAKMP 事前共有鍵の設定

IPSec Virtual Route Forwarding（VRF; 仮想経路フォワーディング）で使用される ISAKMP リングの ISAKMP 事前共有鍵を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto keyring** *keyring-name*
4. **pre-shared-key address** *address* **key** *key*
5. **pre-shared-key hostname** *hostname* **key** *key*

手順の詳細

	コマンド	説明
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 keyring** *keyring-name* **例：** `Router (config)# crypto keyring foo`	Internet Key Exchange（IKE; インターネット キー エクスチェンジ）認証で使用する暗号鍵リングを定義し、鍵リング 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	**pre-shared-key address** *address* **key** *key* **例：** `Router (config-keyring)# pre-shared-key address 10.2.3.5 key cisco`	IKE 認証に使用する事前共有鍵を定義します。 • *address* 引数には、リモート ピアの IP アドレスを指定します。
ステップ 5	**pre-shared-key hostname** *hostname* **key** *key* **例：** `Router (config-keyring)# pre-shared-key hostname foo.com key cisco`	IKE 認証に使用する事前共有鍵を定義します。 • *hostname* 引数には、ピアの FQDN を指定します。

例

次に示すのは、ISAKMP 鍵リングの事前共有鍵が設定された場合の **show-running-config** による出力例です。

```
crypto keyring foo
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname foo.com key 6 aE_REHDcOfYCPF^RXTQfDJYVVNSAAB
```

ISAKMP アグレッシブ モードの設定

ISAKMP アグレッシブ モードを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp peer ip-address** *ip-address*
4. **set aggressive-mode client-endpoint** *client-endpoint*
5. **set aggressive-mode password** *password*

手順の詳細

	コマンド	説明
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 isakmp peer ip-address** *ip-address* **例：** `Router (config)# crypto isakmp peer ip-address 10.2.3.4`	アグレッシブ モードのトンネル アトリビュートに関し、IP Security（IPSec; IP セキュリティ）ピアによる AAA の IKE クエリーをイネーブルにし、ISAKMP ピア 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	**set aggressive-mode client-endpoint** *client-endpoint* **例：** `Router (config-isakmp-peer)# set aggressive-mode client-endpoint fqdn cisco.com`	ISAKMP ピア設定内で、Tunnel-Client-Endpoint アトリビュートを指定します。
ステップ 5	**set aggressive-mode password** *password* **例：** `Router (config-isakmp-peer)# set aggressive-mode password cisco`	ISAKMP ピア設定内で、Tunnel-Password アトリビュートを指定します。

例

次に示すのは、ISAKMP アグレッシブ モードの暗号化事前共有鍵が設定された場合の **show-running-config** による出力例です。

```
crypto isakmp peer address 10.2.3.4
 set aggressive-mode password 6 ^aKPIQ_KJE_PPF^RXTQfDTIaLNeAAB
 set aggressive-mode client-endpoint fqdn cisco.com
```

Unity サーバ グループ ポリシーの設定

Unity サーバ グループ ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **pool** *name*
5. **domain** *name*
6. **key** *name*

手順の詳細

	コマンド	説明
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 isakmp client configuration group** *group-name* **例：** `Router (config)# crypto isakmp client configuration group foo`	定義するグループのポリシー プロファイルを指定し、ISAKMP グループ 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	**pool** *name* **例：** `Router (config-isakmp-group)# pool foopool`	ローカル プール アドレスを定義します。
ステップ 5	**domain name** **例：** `Router (config-isakmp-group)# domain cisco.com`	グループが属する Domain Name Service（DNS; ドメイン ネーム サービス）ドメインを指定します。
ステップ 6	**key** *name* **例：** `Router (config-isakmp-group)# key cisco`	グループ ポリシー アトリビュートの定義に使用する IKE 事前共有鍵を指定します。

例

次に示すのは、Unity サーバ グループ ポリシーに対して暗号化された鍵が設定された場合の **show-running-config** による出力例です。

```
crypto isakmp client configuration group foo
```

```
key 6 cZZgDZPOE\dDPF^RXTQfDTIaLNeAAB
domain cisco.com
pool foopool
```

Easy VPN クライアントの設定

Easy VPN クライアントを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. crypto ipsec client ezvpn *name*
4. peer *ipaddress*
5. mode client
6. group *group-name* key *group-key*
7. connect manual

手順の詳細

	コマンド	説明
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 ipsec client ezvpn** *name* **例：** `Router (config)# crypto ipsec client ezvpn foo`	Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote 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	**peer** *ipaddress* **例：** `Router (config-isakmp-peer)# peer 10.2.3.4`	VPN 接続に対して、ピアの IP アドレスを設定します。
ステップ 5	**mode client** **例：** `Router (config-isakmp-ezpvy)# mode client`	Network Address Translation（NAT; ネットワーク アドレス変換）または Peer Address Translation（PAT; ピア アドレス変換）を使用する Cisco Easy VPN クライアント モード用にルータを自動設定します。

	コマンド	説明
ステップ 6	**group** *group-name* **key** *group-key* **例：** `Router (config-isakmp-ezvpn)# group foo key cisco`	VPN 接続に使用するグループ名および鍵値を指定します。
ステップ 7	**connect manual** **例：** `Router (config-isakmp-ezvpn)# connect manual`	手動設定を指定して、Cisco Easy VPN Remote クライアントに対し、コマンドまたは API のコールを待ってから、Cisco Easy VPN Remote 接続の確立を試行するよう指示します。

例

次に示すのは、Easy VPN クライアントが設定された場合の **show-running-config** による出力例です。この鍵は暗号化されています。

```
crypto ipsec client ezvpn foo
 connect manual
 group foo key 6 gdMI`S^^[GIcPF^RXTQfDFKEO\RAAB
 mode client
 peer 10.2.3.4
```

暗号化事前共有キーに関する設定例

ここでは、次の設定例について説明します。

- 「暗号化事前共有鍵：例」（P.11）
- 「鍵が存在しない場合：例」（P.12）
- 「鍵が存在する場合：例」（P.12）
- 「鍵が存在する状況でユーザがインタラクティブにキーボード操作を行う場合：例」（P.12）
- 「鍵が存在しない状況でユーザがインタラクティブにキーボード操作を行う場合：例」（P.12）
- 「パスワード暗号化の設定解除」（P.12）

暗号化事前共有鍵：例

次に示すのは、タイプ 6 の事前共有鍵が暗号化された場合の設定例です。この中には、ユーザに対して表示されるプロンプトやメッセージも含まれています。

```
Router (config)# crypto isakmp key cisco address 10.0.0.2
Router (config)# exit
Router# show runnning-config | include crypto isakmp key
 crypto isakmp key cisco address 10.0.0.2
Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# password encryption aes
Router (config)# key config-key password-encrypt
New key:
Confirm key:
Router (config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Router (config)# exit
```

```
Router # show running-config | include crypto isakmp key
crypto isakmp key 6 CXWdhVTZYB_Vcd^`cIHDOahiFTa address 10.0.0.2
```

鍵が存在しない場合：例

次に示すのは、鍵が存在しない場合の設定例です。

```
Router (config)# key config-key password-encryption testkey 123
```

鍵が存在する場合：例

次に示すのは、鍵が存在する場合の設定例です。

```
Router (config)# key config-key password-encryption testkey123
Old key:
Router (config)#
```

鍵が存在する状況でユーザがインタラクティブにキーボード操作を行う場合：例

次に示すのは、鍵が存在する状況でユーザがインタラクティブにキーボード操作を行う場合の設定例です。**key config-key password-encryption** コマンドを入力し、Enter キーを押して対話モードを開始すると、画面には Old key、New key、Confirm key という 3 つのプロンプトが表示されます。

```
Router (config)# key config-key password-encryption
Old key:
New key:
Confirm key:
```

鍵が存在しない状況でユーザがインタラクティブにキーボード操作を行う場合：例

次に示すのは、鍵が存在しない状況でユーザがインタラクティブにキーボード操作を行う場合の設定例です。対話モードを開始すると、画面には New key および Confirm key という 2 つのプロンプトが表示されます。

```
Router (config)# key config-key password-encryption
New key:
Confirm key:
```

パスワード暗号化の設定解除

次に示すのは、ユーザがパスワード暗号化の設定を解除する場合の設定例です。対話モードを開始すると、画面には「WARNING: All type 6 encrypted keys will become unusable.Continue with master key deletion?[yes/no]:」というプロンプトが表示されます。

```
Router (config)# no key config-key password-encryption

WARNING: All type 6 encrypted keys will become unusable. Continue with master key
deletion ? [yes/no]: y
```

関連情報

その他の事前共有キーを設定します。

その他の参考資料

ここでは、暗号化事前共有鍵に関する関連資料について説明します。

関連資料

内容	参照先
パスワードの設定	• 『*Cisco IOS Security Command Reference*』 • 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「About Cisco IOS Software Documentation」の章

規格

規格	タイトル
この機能には、新しいまたは変更された規格はありません。	—

MIB

MIB	MIB リンク
この機能には、新しいまたは変更された MIB はありません。	選択したプラットフォーム、Cisco IOS ソフトウェア 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
この機能には、新しいまたは変更された 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、この章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 Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。

- **crypto ipsec client ezvpn（グローバル）**
- **crypto isakmp client configuration group**
- **crypto isakmp key**
- **key config-key password-encryption**
- **password encryption aes**
- **password logging**
- **pre-shared-key**
- **set aggressive-mode password**