「Encrypted Preshared Key」

暗号化事前共有キー機能を使用すると、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 に安全に保管できます。

暗号化事前共有キーの制約事項

- 古い ROM モニタ（ROMMON）およびブート イメージでは、新しいタイプ 6 パスワードが認識されません。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）を使用できるのは IP Plus イメージ上に限ります。

暗号化事前共有キーに関する情報

暗号化事前共有キーの使用によるパスワードのセキュアな保存

暗号化事前共有キー機能を使用すると、コマンドライン インターフェイス（CLI）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** コマンドを **password encryption aes** コマンドとともに使用すると、パスワードを設定してイネーブルにできます（キーの暗号化には対称キー暗号である 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（キー）は、ルータ内のその他すべてのキーを暗号化するマスター暗号キー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** 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不揮発性生成（NVGEN）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（マスターキー）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、変更前のキーと変更後のキーが渡されます。

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キー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）。セキュリティ対策として、暗号化されたパスワードは、ソフトウェアによって復号されることはなくなります。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 パスワードはすべて変更されずに残されます。**key config-key password-encryption** コマンドを使用して設定したパスワード（マスターキー）があれば、アプリケーションで必要に応じてタイプ 6 パスワードを復号できます。

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、その内部にキーが格納されるよう強化されることで初めて、パスワードの内容を「知る」ことができます。その場合、パスワードは管理ステーション内部に安全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 キーに適合しない場合やマスター キー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."
```

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

既存のマスターキーが失われた場合、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キーを削除できます。**no key config-key password-encryption** コマンドを使用してマスターキーを削除しても、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、暗号化されたパスワードを有効化できます。

暗号化事前共有キーの設定方法

暗号化事前共有キーの設定

暗号化事前共有キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**key config-key password-encryption** [*text*] 例： `Router (config)# key config-key password-encryption`	タイプ 6 の暗号キーをプライベート 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、暗号キー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、暗号キーが存在しなければ、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、次のプロンプトが表示されます。「WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:」
ステップ 4	**password encryption aes** 例： `Router (config)# password-encryption aes`	暗号化事前共有キーのイネーブル化

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 キーに適合しないか、またはマスター キー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。

暗号化事前共有キーのモニタリング

暗号化事前共有キー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**

手順の概要

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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、マスターキーが新規に設定された場合と、その新しいマスターキーを使用してそのキー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 事前共有キーの設定

ISAKMP 事前共有キーを設定するには、次の手順を実行します。

手順の概要

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

4. **crypto isakmp key** *keystring* **hostname** *hostname*

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 mykey hostname mydomain.com`	事前共有認証キーを設定します。 • *hostname* 引数には、ピアの完全修飾ドメイン名（FQDN）を指定します。

例

次に示すのは、暗号化事前共有キー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 mydomain.com
```

ISAKMP キーリングの ISAKMP 事前共有キーの設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto 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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 mykeyring`	インターネット キー交換（IKE）認証で使用する暗号キーリングを定義し、キーリング 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キーを定義します。 • *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 mydomain.com key cisco`	IKE 認証に使用する事前共有キーを定義します。 • *hostname* 引数には、ピアの FQDN を指定します。

例

次に示すのは、ISAKMP キーリングの暗号化された事前共有キーが設定された場合の **how-running-config** による出力例です。

```
crypto keyring mykeyring
  pre-shared-key address 10.2.3.5 key 6 `WHCJYR_Z]GRPF^RXTQfDcfZ]GPAAB
  pre-shared-key hostname mydomain.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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 モードのトンネル属性に関し、IP セキュリティ（IPSec）ピアによる認証、許可、アカウンティング（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 属性を指定します。
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 属性を指定します。

例

次に示すのは、ISAKMP アグレッシブモードで、暗号化された事前共有キーが設定された場合の **how-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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 mygroup`	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 mypool`	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`	グループが属するドメイン ネーム サービス（DNS）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 ポリシー属性の定義に使用する IKE 事前共有キーを指定します。

例

次に示すのは、暗号化されたキーが Unity サーバーグループポリシーに対して設定された場合の **show-running-config** による出力例です。

```
crypto isakmp client configuration group mygroup
 key 6 cZZgDZPOE\dDPF^RXTQfDTIaLNeAAB
 domain cisco.com
 pool mypool
```

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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 myclient`	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：	VPN 接続に対して、ピアの IP アドレスを設定します。

	コマンドまたはアクション	目的
	`Router (config-isakmp-peer)# peer 10.2.3.4`	
ステップ 5	**mode client** 例： `Router (config-isakmp-ezpvy)# mode client`	ネットワーク アドレス変換（NAT）またはピア アドレス変換（PAT）を使用する Cisco Easy VPN クライアント モードでの動作用にルータを自動設定します。
ステップ 6	**group** *group-name* **key** *group-key* 例： `Router (config-isakmp-ezvpn)# group mygroup key cisco`	VPN 接続に使用するグループ名およびキー値を指定します。
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、コマンドまたはアプリケーション プログラミング インターフェイス（API）のコールを待機してから、Cisco Easy VPN リモート接続の確立を試行するよう指示します。

例

次に、Easy VPN クライアントが設定されていることを示す **show-running-config** の出力例を示します。このキーは暗号化されています。

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

暗号化事前共有キーの設定例

暗号化事前共有キー：例

次に示すのは、タイプ 6 の事前共有キー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 running-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
```

キーが存在しない場合の例

次の設定例には、以前のキーがありません。

```
Router (config)#
```

キーが存在する場合の例

次の設定例には、キーがすでに存在しています。

```
Router (config)#
Old key:
Router (config)#
```

キーが存在する状況でユーザがインタラクティブにキーを入力する場合の例

次の設定例では、ユーザは対話形式の入力を求めていますが、キーはすでに存在しています。**key config-key** 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)#
Old key:
New key:
Confirm key:
```

キーが存在しない状況でユーザがインタラクティブにキーを入力する場合の例

次に示すのは、キー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)#
```

```
New key:
Confirm key:
```

パスワード暗号化の設定解除の例

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。「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画面に表示されます（インタラクティブ モードの場合）。

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

次の作業

その他の事前共有キーを設定します。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
パスワードの設定	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの 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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

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。