暗号

概要・基本設定

本製品の暗号モジュール（ENCO モジュール）について説明します。
ENCO モジュールは、本製品のセキュリティー機能の土台となるベースモジュールです。IPsec や SSH などのセキュリティー機能は、すべて ENCO モジュールを利用して実現されます。
ENCO モジュールが提供する機能は次のとおりです。

- 暗号アルゴリズム：56 ビット DES、168 ビット 3DES、128/192/256 ビット AES、RSA 公開鍵暗号
- 認証アルゴリズム：HMAC-MD5-96、HMAC-SHA-1-96
- 鍵交換アルゴリズム：Diffie-Hellman
- 鍵作成・保存機能

✎ 3DES、AES を使用するにはフィーチャーライセンス AT-FL-12 が必要です。

ENCO モジュールが実際に提供している機能を確認するには、SHOW ENCO コマンド（20 ページ）を使います。

✎ 暗号関連の機能を実際に使用するときは、ルーターの動作モードをセキュリティーモードに変更する必要があります。詳細は「運用・管理」の「セキュリティー」をご覧ください。

ユーザーモジュール

ENCO サービスを利用する上位モジュールを、ENCO モジュールの「ユーザーモジュール」と呼びます。ユーザーモジュールには、以下のものがあります。

■ IPsec（ISAKMP/IKE、AH、ESP）
DES、3DES、AES、HMAC-MD5-96、HMAC-SHA-1-96、Diffie-Hellman を使用します。詳細については「IPsec」の章をご覧ください。

■ SSH
DES と RSA を使用します。詳細については「運用・管理」の「Secure Shell」をご覧ください。
以下、ENCO モジュールが提供する各種サービスの設定方法について説明します。ENCO モジュールは単独で使用するものではなく、より上位のプロトコルやサービスと組み合わせて使用するため、関連する他の章もご参照ください。

暗号アルゴリズム

ENCO モジュールは、共通鍵暗号 DES（鍵長 56 ビット）、3DES（鍵長 168 ビット）、AES（鍵長 128/192/256 ビット）と公開鍵暗号 RSA（鍵長 256～2048 ビット）をサポートしています。

DES

共通鍵暗号 DES（56 ビット）は、IPsec（ESP）、ISAKMP、SSH のセッション鍵として使用されます。
DES で使用する鍵を作成するには、CREATE ENCO KEY コマンド（10 ページ）の TYPE パラメーターに DES を指定します。鍵は、ランダムに生成することも、他のルーターで作成した鍵の値を入力して使うこと

もできます。

■ DES 鍵をランダムに生成するには、RANDOM オプションを使います。

```
CREATE ENCO KEY=1 TYPE=DES DESCRIPTION="my DES key" RANDOM ↵
```

✎ CREATE ENCO KEY コマンド（10 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。

✎ ルーター上で作成した鍵は、設定ファイルとは別個にフラッシュメモリー上に格納されます。鍵はセキュリティーモードでないと再起動によって消えてしまうため、再起動前にセキュリティーモードへの移行を忘れずに行ってください。

■ 作成した鍵の値を表示するには、SHOW ENCO KEY コマンド（28 ページ）を使います。鍵は本製品独自の 5 ビット ASCII 形式と 16 進数形式で表示されます。

```
SHOW ENCO KEY=1 ↵
```

```
SecOff > show enco key=4

  j7amxbbrhun48a
  0x4F40CB84313D1BAF


IP Address:
-
```

■ DES 鍵は値を指定して作成することもできます。これは、他のルーターでランダムに生成した鍵を別のルーターに入力するときに使います。値の指定には、「0x」で始まる 16 進数で指定する方法と、本製品独自の 5 ビット ASCII 形式で指定する方法があります。
16 進数で指定する場合は先頭に「0x」を付けます。長さは 8 バイト（64 ビット）です。

```
CREATE ENCO KEY=1 TYPE=DES DESCRIPTION="DES key"
  VALUE=0xF888CAC6C66ECF52 ↵
```

✎ DES の鍵長は 56 ビットですが、パリティー情報などを含めると 64 ビットになります。

5 ビット ASCII 形式は、小文字のアルファベット a〜z と数字の 2〜9 だけで構成される文字列で指定する方法です。鍵を生成したルーター上で SHOW ENCO KEY コマンド（28 ページ）を実行したときに表示される文字列を入力してください。

```
CREATE ENCO KEY=1 TYPE=DES DESCRIPTION="DES key" VALUE=9cemvrwgn5hvek ↵
```

3DES

共通鍵暗号 3DES（168 ビット）は、IPsec（ESP）、ISAKMP のセッション鍵として使用されます。

✎ 3DES を使用するにはフィーチャーライセンス AT-FL-12 が必要です。

3DES で使用する鍵を作成するには、CREATE ENCO KEY コマンド（10 ページ）の TYPE パラメーターに 3DESOUTER を指定します。鍵は、ランダムに生成することも、他のルーターで作成した鍵の値を入力して使うこともできます。

■ 3DES 鍵をランダムに生成するには、RANDOM オプションを使います。

```
CREATE ENCO KEY=1 TYPE=3DESOUTER DESCRIPTION="my 3DES key" RANDOM ↵
```

✎ CREATE ENCO KEY コマンド（10 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。

✎ ルーター上で作成した鍵は、設定ファイルとは別個にフラッシュメモリー上に格納されます。鍵はセキュリティーモードでないと再起動によって消えてしまうため、再起動前にセキュリティーモードへの移行を忘れずに行ってください。

■ 作成した鍵の値を表示するには、SHOW ENCO KEY コマンド（28 ページ）を使います。鍵は本製品独自の 5 ビット ASCII 形式と 16 進数形式で表示されます。

```
SHOW ENCO KEY=1 ↵
```

■ 3DES 鍵は値を指定して作成することもできます。これは、他のルーターでランダムに生成した鍵を別のルーターに入力するときに使います。値の指定には、「0x」で始まる 16 進数で指定する方法と、本製品独自の 5 ビット ASCII 形式で指定する方法があります。
16 進数で指定する場合は先頭に「0x」を付けます。長さは 24 バイト（192 ビット）です。

```
CREATE ENCO KEY=1 TYPE=DES DESCRIPTION="DES key"
  VALUE=0x112233445566778811223344556677881122334455667788 ↵
```

✎ 3DES の鍵長は 168 ビットですが、パリティー情報などを含めると 192 ビットになります。

AES

共通鍵暗号 AES（128/192/256 ビット）は、IPsec（ESP）、ISAKMP のセッション鍵として使用されます。

✎ AES を使用するにはフィーチャーライセンス AT-FL-12 が必要です。

AES で使用する鍵を作成するには、CREATE ENCO KEY コマンド（10 ページ）の TYPE パラメーターに AES128、AES192、AES256 を指定します。鍵は、ランダムに生成することも、他のルーターで作成した鍵の値を入力して使うこともできます。

■ AES 鍵をランダムに生成するには、RANDOM オプションを使います。

```
CREATE ENCO KEY=1 TYPE=AES192 DESCRIPTION="192-bit AES key" RANDOM ↵
```

✎ CREATE ENCO KEY コマンド（10 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファ

イルにこのコマンドを記述しておいても無効ですのでご注意ください。

✎ ルーター上で作成した鍵は、設定ファイルとは別個にフラッシュメモリー上に格納されます。鍵はセキュリティーモードでないと再起動によって消えてしまうため、再起動前にセキュリティーモードへの移行を忘れずに行ってください。

■ 作成した鍵の値を表示するには、SHOW ENCO KEY コマンド（28 ページ）を使います。AES 鍵は 16 進数形式で表示されます。

```
SHOW ENCO KEY=1 ↵
```

■ AES 鍵は値を指定して作成することもできます。これは、他のルーターでランダムに生成した鍵を別のルーターに入力するときに使います。値は「0x」で始まる 16 進数で指定します。
16 進数で指定する場合は先頭に「0x」を付けます。

```
CREATE ENCO KEY=1 TYPE=AES DESCRIPTION="His 192-bit AES key"
  VALUE=0x1a39dd7a7caa5523192138a5a4996347366879531329e0f8 ↵
```

✎ AES 鍵の入力時には 5 ビット ASCII 形式は使用できません。

RSA

RSA 公開鍵は、SSH のサーバー鍵、ホスト鍵、認証鍵として使われます。

■ RSA 鍵ペアを作成するには、CREATE ENCO KEY コマンド（10 ページ）の TYPE パラメーターに RSA を指定し、LENGTH で鍵の長さ（ビット）を指定します。有効範囲は 256～2048 ビットです。鍵は長いほど安全性が高まりますが、作成に時間がかかるようになります。現実的な鍵長は 1024 ビットと言われています。

```
CREATE ENCO KEY=2 TYPE=RSA LENGTH=1024 DESCRIPTION="my key pair" ↵
```

✎ RSA 鍵の作成には時間がかかります。上記コマンドを入力すると「RSA Key Generation process started.」と表示されます。鍵の作成中は CPU 負荷が高くなります。鍵の作成が終わると「RSA Key generation process completed.」と表示されます。

✎ CREATE ENCO KEY コマンド（10 ページ）はコンソールから入力したときだけ有効なコマンドです。設定ファイルにこのコマンドを記述しておいても無効ですのでご注意ください。

✎ ルーター上で作成した鍵は、設定ファイルとは別個にフラッシュメモリー上に格納されます。鍵はセキュリティーモードでないと再起動によって消えてしまうため、再起動前にセキュリティーモードへの移行を忘れずに行ってください。

■ 作成した鍵ペアから公開鍵をファイルに書き出すには、CREATE ENCO KEY コマンド（10 ページ）の FILE パラメーターで書き出し先のファイル名（拡張子は.key）を指定し、KEY パラメーターには作成した鍵ペアの番号を指定します。鍵ファイルのフォーマットを FORMAT パラメーターで指定することもでき

ます。

```
CREATE ENCO KEY=2 TYPE=RSA FILE=mypublic.key ↵
```

■ 鍵ファイルから公開鍵を取り込むには、CREATE ENCO KEY コマンド（10 ページ）の FILE パラメーターに既存の鍵ファイル（拡張子は.key）を指定し、KEY パラメーターには未作成の（空いている）鍵番号を指定します。また、鍵ファイルのフォーマットを FORMAT パラメーターで指定することもできます。

```
CREATE ENCO KEY=3 TYPE=RSA FILE=hispublc.key DESCRIPTION="His public
  key" ↵
```

■ 作成した鍵の情報は SHOW ENCO KEY コマンド（28 ページ）で確認できます。

```
SHOW ENCO KEY ↵
SHOW ENCO KEY=3 ↵
```

```
Manager > show enco key

  ID  Type       Length Digest   Description              Mod   IP
  ------------------------------------------------------------------------
   1  DES             8 1F35B264 my DES key               -     -
   2  RSA-PRIVATE  1024 EA83BD2C my key pair              -     -
   3  RSA-PUBLIC    768 0ADBE436 His public key           -     -
```

認証アルゴリズム

ENCO モジュールは、データ認証アルゴリズムとして、ハッシュ関数 HMAC-MD5-96 と HMAC-SHA-1-96 をサポートしています。これらのアルゴリズムは、IPsec（AH、ESP）や ISAKMP のデータ認証処理に使用されます。
ハッシュアルゴリズムはソフトウェア的に実装されています。

HMAC-MD5-96

HMAC-MD5-96 では、16 バイト（128 ビット）の汎用鍵を使います。

■ 鍵をランダムに生成するには次のようにします。

```
CREATE ENCO KEY=10 TYPE=GENERAL LENGTH=16 RANDOM DESCR="My MD5 key 1" ↵
```

■ 鍵の値を 16 文字の文字列で指定することもできます。

```
CREATE ENCO KEY=11 TYPE=GENERAL VALUE="jogefogejogefoge" DESCR="My MD5
  key 2" ↵
```

■ 鍵の値を 16 バイトの 16 進数で指定することもできます。

```
CREATE ENCO KEY=12 TYPE=GENERAL VALUE=0x000102030405060708090a0b0c0d0e0f
  DESCR="My MD5 key 3" ↵
```

■ 作成した鍵の値を表示するには、SHOW ENCO KEY コマンド（28 ページ）を使います。

```
SHOW ENCO KEY=10 ↵
```

```
SecOff > show enco key=10

0x281bd343a63e63d37b49f10c0b217dd2

IP Address:
-
```

HMAC-SHA-1-96

HMAC-SHA-1-96 では、20 バイト（160 ビット）の汎用鍵を使います。

■ 鍵をランダムに生成するには次のようにします。

```
CREATE ENCO KEY=20 TYPE=GENERAL LENGTH=20 RANDOM DESCR="My SHA key 1" ↵
```

■ 鍵の値を 20 文字の文字列で指定することもできます。

```
CREATE ENCO KEY=21 TYPE=GENERAL VALUE="fugafugafugafugafuga" DESCR="My
  SHA key 2" ↵
```

■ 鍵の値を 20 バイトの 16 進数で指定することもできます。

```
CREATE ENCO KEY=22 TYPE=GENERAL
  VALUE=0x000102030405060708090a0b0c0d0e0f00010203 DESCR="My SHA key 3" ↵
```

■ 作成した鍵の値を表示するには、SHOW ENCO KEY コマンド（28 ページ）を使います。

```
SHOW ENCO KEY=20 ↵
```

```
SecOff > show enco key=20

0xca59ba48cd4e1c8d5ed3ad62ce786758cb01dcf3

IP Address:
-
```

鍵交換アルゴリズム

ENCO モジュールは、鍵交換のためのアルゴリズムとして Diffie-Hellman アルゴリズムをサポートしてい

ます。
Diffie-Hellman アルゴリズムの処理は、大きくわけて 2 つの段階に分けられます。最初の段階では、鍵交換を行う両者がそれぞれ乱数を生成し、既定式との計算結果を互いに交換します。第 2 段階では、相手から入手した値と自分で生成した乱数値から秘密鍵の値を求めます。これら 2 つの段階は、内部的にはさらに細かく分割されており、ルーター本来の処理に与える影響を少なくしています。
いずれにしても、鍵の計算処理は非常に CPU 時間を消費する処理です。本製品では、SET ENCO DHPRIORITY コマンド（18 ページ）で、Diffie-Hellman アルゴリズムの処理優先度を変更できるようになっています。優先度には、HIGH、MEDIUM、LOW の 3 つがあり、デフォルトは HIGH です。Diffie-Hellman 処理の優先度を低くするには次のようにします。

```
SET ENCO DHPRIORITY=LOW ↵
```

ENCO モジュールでは、Diffie-Hellman アルゴリズムで使用される公開値のうち、RFC2412 で規定されている Diffie-Hellman（OAKLEY）グループ 1（768 ビット値）とグループ 2（1024 ビット値）をサポートしています。

鍵作成・保存機能

ENCO モジュールの重要な機能の 1 つに、各種の暗号・認証アルゴリズムで使用する鍵の作成と保存のための機能があります。
本製品上で鍵を使用するには、CREATE ENCO KEY コマンド（10 ページ）を実行して、ENCO モジュールに鍵を登録する必要があります。鍵は、ランダムに生成して登録することも、他のルーターで生成した鍵の値を入力することによって登録することも、また、あらかじめ定められた形式のファイルから鍵を取り込んで登録することもできます。また、作成した RSA 鍵ペアの公開鍵をファイルに書き出し、他者に配布することもできます。
登録された鍵は、CREATE CONFIG コマンド（「運用・管理」の 124 ページ）で作成する設定スクリプトは別個にフラッシュメモリー上に格納されます。ただし、セキュリティーモードでない場合は、ルーターの再起動によって消去されてしまうため、鍵を使用する場合は必ずセキュリティーモードに移行するようにしてください。
鍵の作成方法は、使用するアルゴリズムによって異なります。DES、3DES、AES、RSA、MD5、SHA で使用する鍵の作成方法については、各アルゴリズムの設定手順をご覧ください。ここでは、これらに当てはまらない ISAKMP の事前共有鍵の作成方法についてのみ解説します。

ISAKMP の事前共有鍵（pre-shared key）

ISAKMP で使用する事前共有鍵は、任意の長さの汎用鍵（パスフレーズ）です。次のようにして作成してください。

```
CREATE ENCO KEY=30 TYPE=GENERAL VALUE="onetwothree" DESCRIPTION="ISAKMP
  pre-shared key" ↵
```

コマンドリファレンス編

機能別コマンド索引

一般コマンド

CREATE ENCO KEY

カテゴリー：暗号 / 一般コマンド

CREATE ENCO KEY=*key-id* TYPE={DES|3DESOUTER|AES128|AES192|AES256|GENERAL|RSA} [DESCRIPTION=*string*] [FILE=*filename*] [FORMAT={HEX|NIQ|SSH}] [IPADDRESS=*ipadd*] [LENGTH=*2..2048*] [MODULE=*module-id*] [{RANDOM|VALUE={*enco-str*|*enco-5bit*|*enco-hex*}]

key-id: 鍵番号（0〜65535）
string: 文字列（1〜25 文字。空白を含む場合はダブルクォートで囲む）
filename: ファイル名（拡張子は.key）
ipadd: IP アドレス
module-id: モジュール名またはモジュール番号（0〜255）
enco-str: 文字列
enco-5bit: 5 ビット ASCII 文字列（英小文字 a〜z と数字 2〜9 の組み合わせ）
enco-hex: バイト列（16 進数。先頭に「0x」を付けること）

解説

暗号化や認証に用いる鍵を作成する。
RSA 公開鍵をファイルから取り込んだり、ファイルに書き出すときにも本コマンドを使用する。
作成した鍵の情報は、CREATE CONFIG コマンドで作成する設定ファイルとは別個に、フラッシュメモリー上に保存される。鍵の情報は、ノーマルモードではシステム再起動によって失われるため、通常運用時にはセキュリティーモードへの移行が必要。

パラメーター

KEY　鍵番号

TYPE　鍵の種類。DES（56 ビット DES 鍵）、3DESOUTER（168 ビット 3DES 鍵）、AES128（128 ビット AES 鍵）、AES192（192 ビット AES 鍵）、AES256（256 ビット AES 鍵）を指定した場合は、RANDOM オプションか VALUE パラメーターが必須。RSA（RSA 公開鍵）を指定した場合は、LENGTH あるいは FILE パラメーターが必要。FILE を指定した場合は、KEY で指定した番号の鍵がすでに存在しているかどうかによって動作が異なる。鍵が存在していない場合は、指定ファイルから公開鍵を取り込む。KEY で指定した鍵がすでに存在するときは、指定ファイルに公開鍵を書き出す。FILE を指定せずに LENGTH だけを指定した場合は、指定した長さの RSA 公開鍵ペアがランダムに作成される。GENERAL（汎用パスフレーズ）を指定した場合は、LENGTH か VALUE の指定が必須。GENERAL 鍵は、認証用ハッシュ関数の鍵や ISAKMP の事前共有鍵（pre-shared key）として使用する。

DESCRIPTION　鍵の説明文（コメント）

FILE　RSA 公開鍵ファイル名。拡張子は.key。鍵ファイルの形式は FORMAT パラメーターで指定する（必須）。KEY パラメーターで指定した RSA 公開鍵ペアが存在し、FILE で指定したファイルが存在していない場合は、指定ファイルに公開鍵が書き出される。KEY パラメーターで指定した鍵が存在せず、

FILE で指定したファイルが存在している場合は、指定ファイルから公開鍵がインポートされる。

FORMAT　RSA 公開鍵ファイルのフォーマットを指定する。FILE パラメーター指定時は必須。SSH は Secure Shell 用（SSH サーバーのホスト鍵を登録するときなど）。NIQ は本ルーター独自形式でルーター間で RSA 鍵を交換するようなときに使う。HEX は他ベンダーの機器と鍵を交換するときなどに使う形式。デフォルトは HEX。

IPADDRESS　鍵に関連付ける IP アドレス。ISAKMP と SSH は、通信相手の RSA 鍵を探すときにこの値を用いる。

LENGTH　作成する鍵の長さ。RSA 公開鍵の場合はビットで指定する。RSA 公開鍵の長さは 32 の倍数でなくてはならず、有効な長さの範囲は 256～2048 ビット。一方、GENERAL 鍵の場合はバイト（文字数）で指定する。有効な長さの範囲は 2～64 バイト。

MODULE　鍵に関連付けるモジュール名

RANDOM　乱数で鍵を作成するときに指定する。GENERAL 鍵の場合、LENGTH の指定がないときは 20 バイト（160 ビット）の鍵が作成される。

VALUE　鍵の内容を指定する。DES、3DES 鍵の場合は、SHOW ENCO KEY コマンドで表示される 5 ビット ASCII か 16 進数フォーマットで指定する。また、AES 鍵の場合は、SHOW ENCO KEY コマンドで表示される 16 進フォーマットで指定する。16 進数の場合は先頭に「0x」を付けること。GENERAL 鍵の場合は文字列または 16 進数で指定する。鍵の内容は、SHOW ENCO KEY コマンドで確認できる。

例

■DES 暗号鍵をランダムに生成する。作成した鍵の値は SHOW ENCO KEY コマンドで確認できる。同じ鍵を他のルーターに入力するときは、表示された値（ASCII 文字列か 16 進数）を使う。

```
CREATE ENCO KEY=1 TYPE=DES RANDOM DESCRIPTION="My DES key"
```

■他のルーターで作成した DES 鍵を 16 進フォーマットで入力する。鍵長は 64 ビット（8 バイト。DES 鍵 56 ビット＋パリティー情報）

```
CREATE ENCO KEY=2 TYPE=DES DESCRIPTION="Imported DES key"
  VALUE=0xBB09BAC150913E82
```

■他のルーターで作成した DES 鍵を本製品独自の 5 ビット ASCII フォーマットで入力する。

```
CREATE ENCO KEY=2 TYPE=DES DESCRIPTION="Imported DES key"
  VALUE=xme5vqkqse9iem
```

■3DES 暗号鍵をランダムに生成する。

```
CREATE ENCO KEY=3 TYPE=3DESOUTER RANDOM DESCRIPTION="My 3DES key"
```

■192 ビットの AES 暗号鍵をランダムに生成する。

```
CREATE ENCO KEY=4 TYPE=AES192 RANDOM DESCRIPTION="My 192-bit AES key"
```

■SSH サーバーのホスト鍵を登録する。該当サーバーに初めて接続したときは、サーバーのホスト鍵が ssh.key という名前でファイルに保存される。その場合はこのコマンドを実行すること。このとき FORMAT に SSH を指定する。

```
CREATE ENCO KEY=100 TYPE=RSA FILE=ssh.key FORMAT=SSH
```

■RSA 公開鍵ペアを作成する。鍵長の有効範囲は 256～2048 ビット。

```
CREATE ENCO KEY=3 TYPE=RSA LENGTH=1024 DESCRIPTION="my key pair"
```

■作成した RSA 鍵ペアの公開鍵を SSH フォーマットでファイル mypublic.key に書き出す。

```
CREATE ENCO KEY=3 TYPE=RSA FILE=mypublic.key FORMAT=SSH
```

■他者から入手した公開鍵ファイル hispub.key を鍵番号「4」としてインポートする。

```
CREATE ENCO KEY=4 TYPE=RSA FILE=hispub.key FORMAT=SSH DESCRIPTION="His
  public key"
```

■16 バイトの MD5 認証鍵をランダムに作成する。

```
CREATE ENCO KEY=5 TYPE=GENERAL LENGTH=16 RANDOM DESCR="My MD5 Hash key"
```

■16 バイトの MD5 認証鍵を文字列指定で作成する。

```
CREATE ENCO KEY=5 TYPE=GENERAL VALUE="jogefogejogefoge" DESCR="My MD5
  Hash key"
```

■ISAKMP の事前共有鍵（pre-shared key）を作成する。

```
CREATE ENCO KEY=6 TYPE=GENERAL VALUE="fugafugafuga" DESCR="ISAKMP
  pre-shared key"
```

関連コマンド

DESTROY ENCO KEY（13 ページ）
SET ENCO KEY（19 ページ）
SHOW ENCO KEY（28 ページ）

DESTROY ENCO KEY

カテゴリー：暗号 / 一般コマンド

DESTROY ENCO KEY=*key-id*

key-id: 鍵番号（0～65535）

解説

指定した鍵を削除する。
フラッシュメモリー上の鍵が格納されていた領域は上書きされ、鍵情報が取得できないように処置される。

パラメーター

KEY　鍵番号

関連コマンド

CREATE ENCO KEY（10 ページ）
SET ENCO KEY（19 ページ）
SHOW ENCO KEY（28 ページ）

DISABLE ENCO DEBUGGING

カテゴリー：暗号 / 一般コマンド

DISABLE ENCO DEBUGGING={**PACKET**}

解説

暗号（ENCO）モジュールのデバッグオプションを無効にする。

パラメーター

DEBUGGING　デバッグオプションを指定する。現在唯一サポートされているオプションは PACKET（ENCO モジュールが生成したパケットの内容表示）。

関連コマンド

ENABLE ENCO DEBUGGING（15 ページ）

ENABLE ENCO DEBUGGING

カテゴリー：暗号 / 一般コマンド

ENABLE ENCO DEBUGGING={**PACKET**}

解説

暗号（ENCO）モジュールのデバッグオプションを有効にする。
デバッグ情報は、コマンドを入力した端末画面に出力される。

パラメーター

DEBUGGING　デバッグオプション。現在唯一サポートされている PACKET オプションは、ENCO モジュールが生成したパケットの内容を端末画面に表示するもの。

備考・注意事項

本コマンドは、トラブルシューティング時など、内部情報の確認が必要な場合を想定したものですので、ご使用に際しては弊社技術担当にご相談ください。

関連コマンド

DISABLE ENCO DEBUGGING（14 ページ）

RESET ENCO COUNTER

カテゴリー：暗号 / 一般コマンド

RESET ENCO COUNTER={**DES**|**DH**|**HMAC**|**JOBPROCESSING**|**RSA**|**USER**|**UTIL**}

解説

暗号（ENCO）モジュールの各種統計カウンターをリセットする。

パラメーター

COUNTER　統計カウンター。省略時はすべてのカウンターをリセットする。USER、UTIL、JOBPROCCESSING の各カウンターは、ENCO モジュールの全般的情報を示すもの。DES、DH、HMAC、RSA は特定のプロセスを対象としたもの。

関連コマンド

SHOW ENCO COUNTERS（25 ページ）

SET ENCO DHPADDING

カテゴリー：暗号 / 一般コマンド

SET ENCO DHPADDING={**ON**|**OFF**}

解説

Diffie Hellman 鍵交換アルゴリズムにおける鍵の計算方式を変更する。

パラメーター

DHPADDING　鍵の計算方式。ON を指定した場合は、計算方式を他社製 IPsec 機器とあわせる。OFF を指定した場合は、計算方式を従来の AR ルーターとあわせる。他社製 IPsec 機器との接続で PFS を使用する場合は ON のまま使用するのがよい。AR ルーター同士を接続するときは両者の設定を同じにすること。特に、本コマンド未実装の AR ルーターとの接続においては、本機の設定を OFF にすること。デフォルトは ON。

関連コマンド

CREATE IPSEC POLICY（「IPsec」の 39 ページ）
SET IPSEC POLICY（「IPsec」の 78 ページ）
SHOW ENCO（20 ページ）

SET ENCO DHPRIORITY

カテゴリー：暗号 / 一般コマンド

SET ENCO DHPRIORITY={**HIGH**|**MEDIUM**|**LOW**}

解説

Diffie Hellman 鍵交換アルゴリズムの処理にどの程度の優先度を与えるかを指定する。
鍵の計算は CPU 負荷のかかる処理なので、IPsec による接続先が多いような場合に必要であれば本コマンドで鍵交換処理の優先度を下げることができる。

パラメーター

DHPRIORITY　鍵交換処理の優先度。HIGH（高）、MEDIUM（中）、LOW（低）から選択する。デフォルトは HIGH。

関連コマンド

SHOW ENCO（20 ページ）

SET ENCO KEY

カテゴリー：暗号 / 一般コマンド

SET ENCO KEY=*key-id* [DESCRIPTION=*string*] [IPADDRESS=*ipadd*]
[MODULE=*module-id*]

key-id: 鍵番号（0～65535）
string: 文字列（1～25 文字。空白を含む場合はダブルクォートで囲む）
ipadd: IP アドレス
module-id: モジュール名またはモジュール番号（0～255）

解説

既存鍵の説明、IP アドレス、関連モジュールを変更する。

パラメーター

KEY　鍵番号
DESCRIPTION　鍵の説明
IPADDRESS　鍵に関連付ける IP アドレス。ISAKMP と SSH は、通信相手の RSA 鍵を探すときにこの値を用いる。
MODULE　鍵に関連付けるモジュール。

関連コマンド

CREATE ENCO KEY（10 ページ）
DESTROY ENCO KEY（13 ページ）
SHOW ENCO KEY（28 ページ）

SHOW ENCO

カテゴリー：暗号 / 一般コマンド

SHOW ENCO

解説

暗号（ENCO）モジュールの全般的な情報を表示する。

入力・出力・画面例

```
Manager > show enco

ENCO Module Configuration:
  Hardware ............................... PRESENT
  Lowest valid channel ................... 1
  Highest valid channel .................. 2047
  Compression Statistics ................. DISABLED
  Diffie Hellman Priority ................ HIGH
  Diffie Hellman Padding ................. ON

  SW Processes available
    SSL  - Secure Socket Layer

  HW Processes available
    DES  - DES Encryption
    3DES - Triple DES Encryption
    AES  - AES Encryption
    RSA  - RSA Encryption
    DH   - Diffie Hellman
    HMAC - Message Digest
    IPSEC - IP Security
```

Hardware	暗号ハードウェアの有無
Lowest valid channel	上位モジュールが使用可能なチャンネルのうちでもっとも若い番号
Highest valid channel	上位モジュールが使用可能なチャンネルのうちでもっとも大きい番号
Diffie Hellman Priority	Diffie Hellman 鍵交換アルゴリズムの処理の優先度。HIGH、MEDIUM、LOW のいずれか
Diffie Hellman Padding	Diffie Hellman の鍵計算方式を他ベンダーの機器にあわせるかどうか。
SW Processes available	ソフトウェアで実現できる機能の一覧
HW Processes available	ハードウェアで実現できる機能の一覧

表 1:

関連コマンド

SET ENCO DHPADDING（17 ページ）
SET ENCO DHPRIORITY（18 ページ）
SHOW ENCO CHANNEL（22 ページ）
SHOW ENCO COUNTERS（25 ページ）

SHOW ENCO CHANNEL

カテゴリー：暗号 / 一般コマンド

SHOW ENCO CHANNEL[=*channel*] [COUNTERS]

channel: チャンネル番号（0〜127）

解説

暗号（ENCO）モジュール用チャンネルの情報を表示する。

パラメーター

CHANNEL ENCO チャンネル番号。省略時はすべてのアクティブなチャンネルの情報が簡潔に表示される。指定時は該当チャンネルの詳細情報が表示される。

COUNTERS 指定したチャンネルの統計情報を表示するときに指定する。チャンネルを指定しない場合は無効。

入力・出力・画面例

```
SecOff > show enco channel

  Channel  State    User UserID   MDL   pktOverhead Process
  ---------------------------------------------------------------
     1       UP    IPSEC 00010000 1800   100         DES
     2       UP    IPSEC 00020000 1800   100         HMAC
     3       UP    IPSEC 00000001 1800   100         HMAC
  ---------------------------------------------------------------


SecOff > show enco channel=1

  Channel ........................ 1

  Type ........................... ENCODE/DECODE
  State .......................... UP
  User ........................... IPSEC
  User ID ........................ 00010000
  Maximum Data Length ............ 1800
  Packet Overhead ................ 100
  Process ........................ DES
  Process Configuration:
    Des Type.........DES - 56 bit
    Channel Type......ENCODE/DECODE
    History Mode......Off
```

```
    IV Type...........Specified
    Hardware..........N/A


SecOff > show enco channel=1 counters

Channel Counters:


  UP events ....................... 1       DOWN events ..................... 0
  start config .................... 1       attach good ..................... 1
  encode NULL packets ............. 0       decode NULL packets ............. 0
  enc bad priorities .............. 0       dec bad priorities .............. 0
  encode bad length ............... 0       decode bad length ............... 0
  encode actions sent .......... 1258       decode actions sent .......... 1283
  good encodes ................. 1258       good decodes ................. 1283
  bad encodes ..................... 0       bad decodes ..................... 0
  reset E actions sent ............ 0       reset D actions sent ............ 0
  good encode resets .............. 0       good decode resets .............. 0
  bad encode codes ................ 0       bad decode resets ............... 0
  discarded enc jobs .............. 0       discarded dec jobs .............. 0
```

Channel	チャンネル番号
State	チャンネルの状態（UP か DOWN）
User	チャンネルを使用している上位モジュール（SSH、ISAKMP、IPSEC）
UserID	上位モジュールがこのチャンネルを識別するために使っている識別子
MDL	このチャンネル上で受け入れ可能なパケットの最大データサイズ（Maximum Data Length）
pktOverhead	パケットのオーバーヘッドバイト数。上位モジュールが、エンコードされたデータの前に pktOverhead バイトの空きを求めていることを示す
Process	このチャンネルを使用する暗号プロセスの種類（RSA、DH、DES、HMAC）

表 2: チャンネル番号無指定時

Channel	チャンネル番号
Type	チャンネルモード（ENCODE/DECODE、ENCODE ONLY、DECODE ONLY）
State	チャンネルの状態（UP か DOWN）
User	チャンネルを使用している上位モジュール（SSH、ISAKMP、IPSEC）
UserID	上位モジュールがこのチャンネルを識別するために使っている識別子
Maximum Data Length	このチャンネル上で受け入れ可能なパケットの最大データサイズ
Packet Overhead	パケットのオーバーヘッドバイト数。上位モジュールが、エンコードされたデータの前に Packet Overhead バイトの空きを求めていることを示す

Process	このチャンネルを使用する暗号プロセスの種類（RSA、DH、DES、HMAC）
Process Configuration	暗号プロセスの詳細。表示内容はプロセスの種類によって異なる
Check Type	使用するチェックサムの種類
Des Type	（DES のみ）DES アルゴリズム。「DES - 56 bit」、「3DES - 168 bit - outer CBC」などがある
Channel Type	（DES のみ）チャンネルモード。ENCODE/DECODE、ENCODE ONLY、DECODE ONLY のいずれか
History Mode	（DES のみ）DES ヒストリーモードの有効・無効
IV Type	（DES のみ）IV（Initialisation Vector）の種類。Zero、Random、Specified のいずれか
RSA mode	（RSA のみ）RSA 暗号化モード。PUBLIC か PRIVATE
Mode	（DH のみ）Diffie Hellman のモード。Phase 1 か Phase 2
Group Type	（DH のみ）Oakley グループの種類。現時点では MODP のみサポート
Group	Oakley グループ。512-bit MODP（グループ 0）、768-bit MODP（グループ 1）、1024-bit MODP（グループ 2）のいずれか
Algorithm	（HMAC のみ）HMAC アルゴリズム。MD5 か SHA
Key Length	（HMAC のみ）HMAC 鍵長

表 3: チャンネル番号指定時

関連コマンド

SHOW ENCO（20 ページ）
SHOW ENCO COUNTERS（25 ページ）

SHOW ENCO COUNTERS

カテゴリー：暗号 / 一般コマンド

SHOW ENCO COUNTERS={**AES**|**DES**|**DH**|**HARDWARE**|**HMAC**|**JOBPROCESSING**|**RSA**|**USER**|**UTIL**}

解説

暗号（ENCO）モジュールの各種統計カウンターを表示する。

パラメーター

COUNTERS　表示する統計カウンターを指定する。USER（ENCO モジュールを利用する上位モジュール）、UTIL（ユーティリティージョブ）、HARDWARE（暗号処理ハードウェア）、JOBPROCESSING は、ENCO モジュールの全般的情報を示すもの。AES、DES、DH（Diffie Hellman）、HMAC、RSA は個々の暗号プロセスを対象としたもの。

入力・出力・画面例

```
SecOff > show enco counters=des

ENCO Process DES/3DES Counters:
  configGood ..................... 6       configBad ..................... 0
  configNoResource ............... 0       configNotSSH .................. 0
  badBuffer ...................... 0       badAlign ...................... 0
  badLength ...................... 0       nohistory ..................... 0
  desJobs ..................... 2710       3Des2KeyJobs .................. 0
  3DesInnerJobs .................. 0       d3DesOuterJobs ................ 0
  noHistJobs ................... 2710       desMacJobs .................... 0
  badDesType ..................... 0       badJobType .................... 0

  unknownJob ..................... 0       error ......................... 0
  reset .......................... 0       confNotDes .................... 0
  commWaitTimeOut ................ 0       dataInnWaitTimeOut ............ 0
  dataOutWaitTimeOut ............. 0

  goodDecrypt ................. 1368       goodEncrypt ................. 1342
  badDecrypt ..................... 0       badEncrypt .................... 0

SecOff > show enco counters=dh

ENCO Process Diffie Hellman Counters:
  goodPhase1 ..................... 1       badPhase1 ..................... 0
  goodPhase2 ..................... 1       badPhase2 ..................... 0
  badGroupType ................... 0       badGroup ...................... 0
```

```
  badGroupParameters ..... 0       badDataLength ..... 0
  noResources ..... 0

SecOff > show enco counters=hmac

ENCO Process HMAC Counters:
  goodHashMD5 ..... 2877       badHashMD5 ..... 0
  goodHashSHA ..... 2877       badHashSHA ..... 0
  goodConfigure ..... 0        badConfigure ..... 0
  badAlgorithm ..... 0         noResources ..... 0
  badKeyLength ..... 0         unknownJob ..... 0
  badDataLength ..... 0

SecOff > show enco counters=jobprocessing

  ENCO Queues                          Queued  Discarded  Processed
  ------------------------------------------------------------------
     Immediate Input queue                0          0          0
     Priority 0 Input queue (high)        0          0          0
     Priority 1 Input queue               0          0          0
     Priority 2 Input queue               0          0          0
     Priority 3 Input queue               0          0          0
     Priority 4 Input queue               0          0          9
     Priority 5 Input queue               0          0       8715
     Priority 6 Input queue               0          0          0
     Priority 7 Input queue               0          0          0
     Priority 8 Input queue (low)         0          0          0
     Output queue                         0          0       8724
  ------------------------------------------------------------------


  Input queue length limit ......... 250
  Lowest input priority queue ...... 5
  Highest input priority queue ..... 0

SecOff > show enco counters=rsa

ENCO Process RSA Counters:
  goodPublicEncrypt ..... 0        badPublicEncrypt ..... 0
  goodPrivateDecrypt ..... 0       badPrivateDecrypt ..... 0
  goodPrivateEncrypt ..... 0       badPrivateEncrypt ..... 0
  goodPublicDecrypt ..... 0        badPublicDecrypt ..... 0
  goodGenerateKey ..... 2          badGenerateKey ..... 0
  badDataLength ..... 0            badKey ..... 0

SecOff > show enco counters=user

ENCO User Interface Counters:
  startConfig ..... 3              startReconfig ..... 0
  attachGood ..... 3               attachFail ..... 0
  attachNoConfig ..... 0           attachBadUserType ..... 0
```

```
  attachedInvalidChan ..... 0       attachedUnusedChan ..... 0
  attachProcNotAvail ..... 0

  reconfigInvalidChan ..... 0       reconfigUnusedChan ..... 0
  reconfigNoConfig ..... 0

  detachInvalidChannel ..... 0      detachUnusedChannel ..... 0
  detachedInvalidChan ..... 0       detachedUnusedChan ..... 0
  detachGood ..... 0

  decodeInvalidChannel ..... 0      decodeUnusedChannel ..... 0
  encodeInvalidChannel ..... 0      encodeUnusedChannel ..... 0
  codedInvalidChannel ..... 0       codedUnusedChannel ..... 0
  resetInvalidChannel ..... 0       resetUnusedChannel ..... 0
  resetDoneInvalidChan ..... 0      resetDoneUnusedChan ..... 0

  configBadMode ..... 0             configBadUserType ..... 0
  configBadPktLength ..... 0        configBadEncrType ..... 0
  configBadCompType ..... 0         configBadHistoryMode ..... 0
  configBadCheckType ..... 0

  discardInvalidChan ..... 0        discardUnusedChannel ..... 0

SecOff > show enco counters=util

ENCO Utility Counters:
  codeNullPacket ..... 0            codeBadPacketPriorit ..... 0
  codeBadPacketLength ..... 0       codeBadConfig ..... 0
  actionSentEncode ..... 0          actionSentDecode ..... 0
  configureGood ..... 9             configureFail ..... 0
  encodeGood ..... 6                decodeGood ..... 3
  encodeBad ..... 0                 decodeBad ..... 0
```

SHOW ENCO KEY

カテゴリー：暗号 / 一般コマンド

SHOW ENCO KEY[=*key-id*]

key-id: 鍵番号（0～65535）

解説

鍵の情報を表示する。

パラメーター

KEY 鍵番号。本パラメーターを指定した場合は、該当する鍵の内容が表示される。表示形式は鍵の種類によって異なる。本パラメーターを省略した場合は、ENCO モジュールが保持している鍵の一覧が表示される。

入力・出力・画面例

```
SecOff > show enco key

   ID  Type      Length Digest   Description              Mod   IP
   ------------------------------------------------------------------------
    1  GENERAL        8 2DEB32E2 -                        -     -
    2  RSA-PRIVATE 1024 B18DFD5D My host_key              -     -
    3  RSA-PRIVATE  768 E61E0F25 My server_key            -     -

SecOff > show enco key=2

1024
0x010001
0x961c0dc80c8728b6e48fa2362b6ac0b59ba569e28112be4c3e260bb359e0b651
2bdd539a5572529f6aa190984fabcdb3f19d6b9068e88f86a41ee810ed499555
223025288091ebbe959596542235a5446a99600d969d9a3e9ec777f726a0d4ae
8bf542d7f38ae249c898c5471cb59addc66f79294494d39821828d9e2d647fd9

IP Address:
-
```

ID	鍵番号
Type	鍵の種類。DES、3DESOUTER、AES128、AES192、AES256、RSA-PRIVATE、RSA-PUBLIC、GENERAL がある

Length	鍵の長さ。RSA 鍵のみビット表示。その他はバイト
Digest	鍵データのメッセージダイジェスト
Description	鍵の説明（CREATE ENCO KEY コマンドの DESCRIPTION パラメーター）
Mod	鍵を使用するユーザーモジュール
IP	鍵に関連付けられた IP アドレス

表 4:

関連コマンド

CREATE ENCO KEY（10 ページ）
DESTROY ENCO KEY（13 ページ）
SET ENCO KEY（19 ページ）