暗号・圧縮

概要・基本設定

本製品の暗号・圧縮（ENCO = Encryption and Compression）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および圧縮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、PPP やフレームリレーのデータリンク圧縮機能などは、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。(E) の付いている機能は暗号ボード（AR010）または暗号・圧縮ボード（AR011）が必要です。
また、(X) の付いている機能は 3DES 対応の暗号ボードと追加ライセンスが必要です。

- 暗号アルゴリズム：56 ビット DES(E)、168 ビット 3DES(X)、RSA 公開鍵暗号
- 認証アルゴリズム：HMAC-MD5-96、HMAC-SHA-1-96(E)
- 圧縮アルゴリズム：STAC LZS、Predictor
- 鍵交換アルゴリズム：Diffie-Hellman
- 鍵作成・保存機能

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（39 ページ）を使います。ソフトウェアで実装されている機能であっても、ライセンスがないと使えないものもあります。

✎ 暗号化・認証機能を使用するためには、暗号ボード（AR010）または暗号・圧縮ボード（AR011）が必要です。

✎ 圧縮機能は通常ソフトウェア処理により実現されますが、STAC LZS については、暗号・圧縮ボード（AR011）または圧縮ボード（AR012）を装着することによりハードウェア処理が可能です（CPU への負荷を軽減できます）。

✎ 暗号・圧縮ボード（AR011）、圧縮ボード（AR012）は AR700 シリーズでのみ使用できます。

✎ 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、IPcomp）
DES、3DES、HMAC-MD5-96、HMAC-SHA-1-96、STAC LZS、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。

■ PPP（CCP、ECP）
STAC LZS、Predictor、DES を使用します。また、鍵管理に STAR モジュールを、TCP / IP ヘッダー圧縮では IP モジュールの VJC（Van Jacobson ヘッダー圧縮）を使用します。詳細は「PPP」の章、本章の「リンクレベル暗号化」、「リンクレベル圧縮」および「IP」の章をご覧ください。

■ フレームリレー
STAC LZS、DES を使用します。また、鍵管理には STAR モジュールを使用します。詳細は「フレームリレー」の章、および、本章の「リンクレベル暗号化」、「リンクレベル圧縮」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）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、PPP とフレームリレーのデータリンク暗号化において、セッション鍵として使用されます。

✎ DES を使用するには、暗号ボード（AR010）または暗号・圧縮ボード（AR011）が必要です。

✎ 暗号・圧縮ボード（AR011）は AR700 シリーズでのみ使用できます。

DES で使用する鍵を作成するには、CREATE ENCO KEY コマンド（18 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（18 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（49 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 ↵
```

```
Manager > show enco key=1

  9cemvrwgn5hvek
  0xF888CAC6C66ECF52
```

■ 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（49 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、3DES 対応の暗号ボードと追加ライセンスが必要です。

3DES で使用する鍵を作成するには、CREATE ENCO KEY コマンド（18 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（18 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（49 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=0x1122334455667788112233445566778811223344556677 88 ↵
```

✎ 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。

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るほか、IPsec の鍵交換プロトコル ISAKMP / IKE でも電子署名等に使われます。

■ RSA 鍵ペアを作成するには、CREATE ENCO KEY コマンド（18 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（18 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（18 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（18 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（49 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（49 ページ）を使います。

```
SHOW ENCO KEY=10 ↵
```

```
Manager > show enco key=10

0x1dc8657173468c10aba21dc20ab79695
```

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（49 ページ）を使います。

```
SHOW ENCO KEY=20 ↵
```

```
Manager > show enco key=20

0x6c647f773b61f4f755a3a6a609cc97408e68f28b
```

圧縮アルゴリズム

ENCO モジュールは、データ圧縮アルゴリズムとして、STAC LZS と Predictor をサポートしています。これらのアルゴリズムは、PPP、フレームリレーのデータリンク圧縮や、IPsec の圧縮（IPcomp）で使用されます。

どちらのアルゴリズムともソフトウェア的に実装されていますが、STAC LZS については、暗号・圧縮ボード（AR011）または圧縮ボード（AR012）を装着することにより、ハードウェアで処理させることもできます。ソフトウェア圧縮とハードウェア圧縮は相互運用が可能です。すなわち、データリンク圧縮において、リンクの一方でハードウェアによる STAC LZS 圧縮を使い、もう一方ではソフトウェア処理による STAC LZS 圧縮を使って通信を行うことができます。

✎ 暗号・圧縮ボード（AR011）、圧縮ボード（AR012）は AR700 シリーズでのみ使用できます。

■ ソフトウェア圧縮を使うときは、最初に圧縮処理用のチャンネル（具体的にはメモリー）を設定しておく必要があります。圧縮チャンネルの設定は、SET ENCO SW コマンド（35 ページ）を使います。Predictor を使用するときは PREDCHANNELS パラメーター、STAC LZS を使うときは STACCHANNELS パラメーターでそれぞれ圧縮チャンネルの数を指定します。PREDCHANNELS、STACCHANNELS ともに最大値は 4 です。

```
SET ENCO SW PREDCHANNELS=2 ↵
SET ENCO SW STACCHANNELS=1 ↵
```

✎ これらのコマンドを入力したら、CREATE CONFIG コマンド（「運用・管理」の 132 ページ）で設定をファイルに保存し、SET CONFIG コマンド（「運用・管理」の 253 ページ）で起動スクリプトに指定した上でルーターを再起動してください。圧縮チャンネル用メモリーは連続した領域として確保する必要があるためです。

チャンネル数は接続先の数に応じて調整します。データリンク圧縮の場合、1 拠点なら 1 チャンネル、2 拠点なら 2 チャンネルとなります。また、IPcomp の場合は、接続拠点数にかかわりなく 1 チャンネルを使用します。デフォルトでは、圧縮チャンネルは確保されていません。
STAC LZS 用のチャンネルは 1 つあたり約 13KB のメモリーを消費します。一方、Predictor 用チャンネルは 1 つあたり約 128KB のメモリーを消費します。

✎ AR720、AR740 は、暗号・圧縮ボード（AR011）または圧縮ボード（AR012）を装着することにより、ハードウェアによる STAC LZS 圧縮処理が可能です。この場合、上記「SET ENCO SW STACCHANNELS=n」で圧縮チャンネルを確保する必要はありません。このコマンドはソフトウェア圧縮処理用のリソース（メモリー）を確保するものです。圧縮ボード装着時に STACCHANNELS を確保してもハードウェアが使用されますが、この場合確保されたメモリーは使われず無駄となりますので、圧縮ボード使用時は上記コマンドを使用しないでください。

■ ソフトウェア処理による STAC LZS 圧縮では、SET ENCO SW コマンド（35 ページ）の STACSPEED パラメーターにより、圧縮率と処理速度のバランスを調整することができます。有効な値は 0〜3 で、0 は圧縮率重視（速度は最低）、3 は速度重視（圧縮率最低）です。このパラメーターはデータを圧縮するときの処理に関するもので、データを伸張するときの処理には影響を与えません。また、ハードウェア処理の場合は常に圧縮率最高となり、本パラメーターの設定は無効となります。

```
SET ENCO SW STACSPEED=3 ↵
```

✎ STACSPEED パラメーターは AR720、AR740 では使用されません。

回線速度	圧縮モード
85kbps〜	3
60〜85kbps	2
40〜59kbps	1
〜40kbps	0

表 1: 回線速度と推奨圧縮モード（STACSPEED）

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（33 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（18 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 132 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、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" ↵
```

リンクレベル圧縮

本製品は、フレームリレーと PPP でデータリンク層の圧縮をサポートしています。圧縮方式等のネゴシエーションには、RFC1962 と RFC1978 で規定されている CCP（Compression Control Protocol）を使います。

圧縮アルゴリズムとしては、PPP では STAC LZS か Predictor、フレームリレーでは FRF.9（STAC LZS）を使用できます。リンクレベル圧縮はソフトウェアで実現されるため特別なハードウェアは必要ありませんが、暗号・圧縮ボード（AR011）または圧縮ボード（AR012）を装着すれば、ハードウェアによる圧縮処理も可能です。

✎ 暗号・圧縮ボード（AR011）、圧縮ボード（AR012）は AR700 シリーズでのみ使用できます。

以下、各圧縮方式を使う場合の基本設定について解説します。

PPP で STAC LZS を使う

PPP リンクで STAC LZS を使う場合は、次のようにします。

1. 圧縮ボードを使用しない場合、SET ENCO SW コマンド（35 ページ）でソフトウェア圧縮チャンネルを確保します。接続先の数に応じて、チャンネル数を指定してください。1 拠点なら 1 チャンネルです。

   ```
   SET ENCO SW STACCHANNELS=1 ↵
   ```

   ✎ 圧縮ボード装着時には、SET ENCO SW コマンド（35 ページ）の設定にかかわらず、つねにハードウェアによる圧縮処理が行われます。ただし、同コマンドで確保したソフトウェアチャンネルは解放されないため、圧縮ボード使用時は SET ENCO SW コマンド（35 ページ）を実行しないでください。

2. 圧縮チャンネルの設定を有効にするため、いったん設定を保存してからルーターを再起動します。

   ```
   CREATE CONFIG=linkcomp.cfg ↵
   SET CONFIG=linkcomp.cfg ↵
   RESTART ROUTER ↵
   ```

3. PPP インターフェースの設定で圧縮を有効にし、アルゴリズムとして STACLZS を指定します。

   ```
   SET PPP=0 COMPRESSION=ON COMPALGORITHM=STACLZS ↵
   ```

PPP で Predictor を使う

PPP リンクで Predictor を使う場合は、次のようにします。

1. 圧縮ボードを使用しない場合、SET ENCO SW コマンド（35 ページ）でソフトウェア圧縮チャンネルを確保します。接続先の数に応じて、チャンネル数を指定してください。1 拠点なら 1 チャンネルです。

   ```
   SET ENCO SW PREDCHANNELS=1 ↵
   ```

2. 圧縮チャンネルの設定を有効にするため、いったん設定を保存してからルーターを再起動します。

```
CREATE CONFIG=linkcomp.cfg ↵
SET CONFIG=linkcomp.cfg ↵
RESTART ROUTER ↵
```

3. PPP インターフェースの設定で圧縮を有効にし、アルゴリズムとして Predictor を指定します。

   ```
   SET PPP=0 COMPRESSION=ON COMPALGORITHM=PREDICTOR ↵
   ```

フレームリレーで FRF.9 を使う

フレームリレーで FRF.9 圧縮を使う場合は、次のようにします。

1. 圧縮ボードを使用しない場合、SET ENCO SW コマンド（35 ページ）でソフトウェア圧縮チャンネルを確保します。接続先の数に応じて、チャンネル数を指定してください。1 拠点なら 1 チャンネルです。

   ```
   SET ENCO SW STACCHANNELS=1 ↵
   ```

2. 圧縮チャンネルの設定を有効にするため、いったん設定を保存してからルーターを再起動します。

   ```
   CREATE CONFIG=linkcomp.cfg ↵
   SET CONFIG=linkcomp.cfg ↵
   RESTART ROUTER ↵
   ```

3. フレームリレーインターフェースの設定で圧縮を有効にします。この場合は、同インターフェース上のすべての論理パス（DLC）で圧縮が有効になります。

   ```
   SET FR=0 DEFCOMPRESSION=ON ↵
   ```

リンクレベル暗号化

本製品は、フレームリレーと PPP で DES によるデータリンクレベルの暗号化をサポートしています。

✎ PPP リンクを暗号化するには、通信データの暗号化と復号化を行うすべてのルーターに暗号ボード（AR010）または暗号・圧縮ボード（AR011）を装着する必要があります。

✎ 暗号・圧縮ボード（AR011）は AR700 シリーズでのみ使用できます。

データリンクの暗号化に使う鍵は、本製品の独自方式（STAR モジュール）を使って管理します。

STAR 鍵交換モジュール

STAR 鍵交換モジュールは、データリンクの暗号化で使用する鍵を管理する本製品独自のメカニズムです。

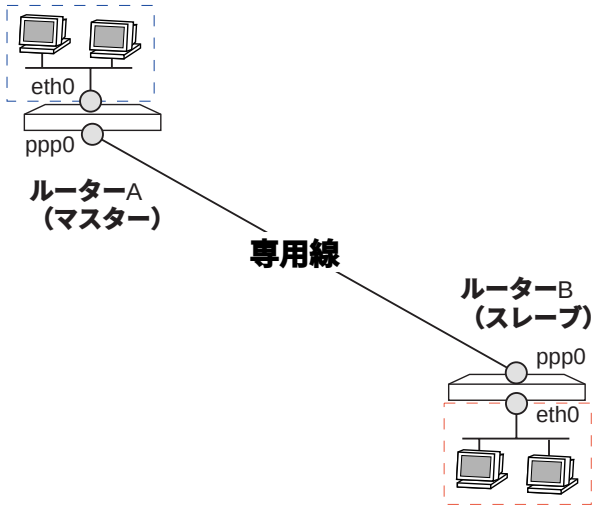
STAR 鍵交換では以下の役割を持つルーターが必要です。

- マスタールーター（1 台）：鍵を生成し、他のルーターに配布する役割を持つルーター
- スタンバイルーター（オプション。1 台）：マスタールーターに障害が発生したときに役割を引き継ぐルーター
- スレーブルーター（1 台以上）：マスタールーターから鍵の配布を受けるその他のルーター

また、STAR モジュールでは以下に示す複数の鍵を使います。

- セッションキー：リンク上を流れる通信データを暗号化するための共通鍵。マスタールーター上で自動的に生成され、スレーブルーターに配布される。このとき、マスターキーによって暗号化が施される。ランダムな間隔で再生成されるほか、データリンクの確立時やリンクエラー発生時にも新しく作り直される。
- マスターキー（テーブル）：マスタールーターからスレーブルーターにセッションキーを転送するときに使う共通鍵。マスターキーテーブルは 160 個のマスターキーをセットにしたもので、マスタールーター上で管理者が生成し、手動でスレーブルーターに転送する。データリンク暗号化を利用するためには、リンク上のすべてのルーターに同じマスターキーテーブルがインストールされている必要がある。
- ネットワークキー：マスタールーターからスレーブルーターにマスターキーテーブルを転送するときに使う共通鍵。管理者があらかじめマスタールーター上でネットワークキー生成し、これを安全な方法で（コンソールから）スレーブルーターに入力しておく必要がある。

ここでは、PPP リンクで接続されている次のようなネットワークを例に、データリンク暗号化の設定手順を示します。ルーター A と B は専用線で接続されているものと仮定します。



ルーター A（マスタールーター）の設定

1. 専用線と PPP の設定を行います。

```
SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
CREATE TDM GROUP=remote INT=bri0 SLOTS=1-2 ↵
CREATE PPP=0 OVER=TDM-remote ↵
ENABLE IP ↵
ADD IP INT=eth0 IP=192.168.10.1 MASK=255.255.255.0 ↵
ADD IP INT=ppp0 IP=0.0.0.0 ↵
ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0 INT=ppp0 NEXT=0.0.0.0 ↵
```

2. STAR モジュールの有効範囲を示す STAR エンティティー「0」を作成します。ルーター A は鍵を配布する側なので、MODE パラメーターには MASTER を指定します。ENCALGORITHM には暗号アルゴリズムを指定します（現在サポートしているのは DES のみ）。

   ```
   CREATE STAR=0 MODE=MASTER ENCALGORITHM=DES ↵
   ```

3. PPP インターフェースでリンク暗号化を有効にします。STARENTITY パラメーターで STAR エンティティー番号を指定してください。

   ```
   SET PPP=0 ENCRYPTION=ON STARENTITY=0 ↵
   ```

4. ネットワークキーを生成します。これは、マスターキーテーブルの配布時に使用する共通秘密鍵です。マスタールーター上でランダムに生成した後、他のルーターに手動で入力します。

   ```
   SET STAR=0 NETKEY RANDOM ↵
   ```

5. 作成したネットワークキーの値を表示させます。ルーター B（スレーブルーター）にも同じ値を設定するので、安全に気を付けつつメモしておいてください。

   ```
   SHOW STAR=0 NETKEY ↵
   ```

   ```
   Manager > show star=0 netkey

     fbj5m5ap7wasgd
   ```

6. マスターキーテーブルを作成します。これは、実際の通信の暗号化に使うセッションキーを暗号化するための鍵を複数まとめたものです。マスタールーター上で生成し、PPP リンク経由でスレーブルーターに転送します。

   ```
   SET STAR=0 MKT RANDOM ↵
   ```

   マスターキーテーブルは、管理者が手動で時々作成しなおしてください。鍵を再作成したときは、手順 7〜10 を繰り返してください。

7. スレーブルーターにネットワークキーを入力したら、マスターキーテーブルを転送します。マスターキーテーブルの転送は、マスタールーター側だけで行う作業です。最初に PPP リンクをいったんリセットします。これにより、セッションキーの再交換が行われ、結果としてスレーブルーターがマスターキーテーブルの転送を要求してきます。

```
RESET PPP=0 ↵
```

8. 次のコマンドを実行して、スレーブルーターからのマスターキーテーブル転送要求を確認します。

```
SHOW STAR MKTTRANSFER LOG ↵
```

```
Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
---
41849368            0  PPP        0 RECEIVED  16:22:27 08-Nov-
2001          8
-------------------------------------------------------------------------------
---
```

9. 要求を確認したら、次のコマンドを実行してマスターキーテーブルを実際に転送します。MKT-TRANSFER パラメーターには、スレーブルーターのシリアル番号を指定します。

```
ENABLE STAR MKTTRANSFER=41849368 ↵
```

10. 転送の進行状況は SHOW STAR MKTTRANSFER LOG コマンド（55 ページ）で確認できます。State 欄が SENDING なら転送中、COMPLETED なら転送完了です。

```
Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
---
41849368            0  PPP        0 SENDING   16:22:27 08-Nov-
2001         48
-------------------------------------------------------------------------------
---
```

```
Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
---
41849368            0  PPP        0 COMPLETED 16:22:27 08-Nov-
2001         48
-------------------------------------------------------------------------------
---
```

11. 設定は以上です。SHOW PPP コマンド（「PPP」の 75 ページ）でリンクの状態を確認してみましょう。LCP、ECP、NCP（ここでは IPCP）がすべて OPENED になっているはずです。

```
Manager > show ppp=0
```

```
  Name            Enabled  ifIndex  Over                  CP           State
  ------------------------------------------------------------------------
----
  ppp0              YES      04                           IPCP         OPENED
                                                          ECP          OPENED
                                    acc-remote            LCP          OPENED
  ------------------------------------------------------------------------
----
```

マスターキーテーブルを作成しなおした場合は、手順 7〜10 を再度繰り返してください。

ルーター B（スレーブルーター）の設定

1. 専用線と PPP の設定を行います。

   ```
   SET BRI=0 MODE=TDM ACTIVATION=ALWAYS TDMSLOTS=1-2 ↵
   CREATE TDM GROUP=remote INT=bri0 SLOTS=1-2 ↵
   CREATE PPP=0 OVER=TDM-remote ↵
   ENABLE IP ↵
   ADD IP INT=eth0 IP=192.168.20.1 MASK=255.255.255.0 ↵
   ADD IP INT=ppp0 IP=0.0.0.0 ↵
   ADD IP ROUTE=192.168.10.0 MASK=255.255.255.0 INT=ppp0 NEXT=0.0.0.0 ↵
   ```

2. STAR モジュールの有効範囲を示す STAR エンティティー「0」を作成します。ルーター B はマスタールーターから鍵の配布を受ける側なので、MODE パラメーターには SLAVE を指定します。ENCALGORITHM には暗号アルゴリズムを指定します（現在サポートしているのは DES のみ）。

   ```
   CREATE STAR=0 MODE=SLAVE ENCALGORITHM=DES ↵
   ```

3. PPP インターフェースでリンク暗号化を有効にします。STARENTITY パラメーターで STAR エンティティー番号を指定してください。

   ```
   SET PPP=0 ENCRYPTION=ON STARENTITY=0 ↵
   ```

4. マスタールーター上で生成したネットワークキーを入力します。

   ```
   SET STAR=0 NETKEY VALUE=fbj5m5ap7wasgd ↵
   ```

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

STAR 鍵交換

CREATE ENCO KEY

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

CREATE ENCO KEY=*key-id* TYPE={**DES**|**3DESOUTER**|**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）または 3DESOUTER（168 ビット 3DES 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。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
```

■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（23 ページ）
SET ENCO KEY（34 ページ）
SHOW ENCO KEY（49 ページ）

CREATE STAR

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

CREATE STAR=*star-id* MODE={**MASTER**|**SLAVE**|**STANDBY**} **ENCALGORITHM=**{**DES**}

star-id: STAR エンティティー番号（0〜255）

解説

リンク暗号化で使う鍵を管理する STAR エンティティーを作成する。
STAR エンティティーは、STAR モジュールの有効範囲を示すもので、鍵を作成し配布するマスタールーター 1 台と、鍵の配布を受けるスレーブルーター 1 台以上で構成される。また、オプションでスタンバイルーター（マスタールーターのバックアップ）を用意することもできる。

パラメーター

STAR　STAR エンティティー番号
MODE　STAR エンティティーの動作モード。STAR 鍵交換における本ルーターの役割を指定する。MASTER を指定した場合は、暗号鍵の生成と配布をつかさどるマスタールーターとして機能する。SLAVE は、マスタールーターから鍵を受け取るスレーブルーターとして機能する。STANDBY は、マスタールーター障害時に代役を務めることのできるスタンバイルーターとして機能する。
ENCALGORITHM　マスターキーテーブルとセッションキーを配布するときに使う暗号アルゴリズム。DES のみをサポートしている。

例

■マスタールーター上で STAR エンティティー「0」を作成する。

```
CREATE STAR=0 MODE=MASTER ENCALGORITHM=DES
```

■スレーブルーター上で STAR エンティティー「0」を作成する。

```
CREATE STAR=0 MODE=SLAVE ENCALGORITHM=DES
```

関連コマンド

DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）

DESTROY ENCO KEY

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY ENCO KEY=*key-id* [LOCATION=FLASH]

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
LOCATION　鍵が格納されている場所。FLASH を指定する。省略可。

関連コマンド

CREATE ENCO KEY（18 ページ）
SET ENCO KEY（34 ページ）
SHOW ENCO KEY（49 ページ）

DESTROY STAR

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

DESTROY STAR=*star-id* [NETKEY|MKT]

star-id: STAR エンティティー番号（0〜255）

解説

STAR エンティティーを削除する。あるいは、STAR エンティティーのネットワークキーまたはマスターキーテーブルを削除する。

パラメーター

STAR　STAR エンティティー番号
NETKEY　ネットワークキーを削除するときに指定する。ネットワークキーは、マスターキーテーブルを転送するときに使用する共通秘密鍵
MKT　マスターキーテーブルを削除するときに指定する。マスターキーテーブルは、実際の通信を暗号化するセッションキーの転送に使われる鍵を複数まとめたもの

関連コマンド

CREATE STAR（21 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SET STAR（37 ページ）
SHOW STAR（51 ページ）
SHOW STAR MKTTRANSFER LOG（55 ページ）
SHOW STAR NETKEY（57 ページ）

DISABLE ENCO COMPSTATISTICS

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

DISABLE ENCO COMPSTATISTICS

解説

圧縮チャンネルの圧縮率統計・保存機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE ENCO COMPSTATISTICS（28 ページ）
SHOW ENCO（39 ページ）
SHOW ENCO CHANNEL（42 ページ）

DISABLE ENCO DEBUGGING

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

DISABLE ENCO DEBUGGING={**PACKET**}

解説

暗号・圧縮（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（29 ページ）

DISABLE STAR DEBUGGING

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

DISABLE STAR DEBUGGING

解説

STAR モジュールのデバッグ機能を無効にする。デフォルトは無効。

関連コマンド

ENABLE STAR DEBUGGING（30 ページ）
SHOW STAR（51 ページ）

ENABLE ENCO COMPSTATISTICS

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

ENABLE ENCO COMPSTATISTICS

解説

圧縮チャンネルの圧縮率統計・保存機能を有効にする。デフォルトは無効。
圧縮率統計は SHOW ENCO CHANNEL コマンドで見ることができる。

関連コマンド

DISABLE ENCO COMPSTATISTICS（25 ページ）
SHOW ENCO（39 ページ）
SHOW ENCO CHANNEL（42 ページ）

ENABLE ENCO DEBUGGING

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

ENABLE ENCO DEBUGGING={**PACKET**}

解説

暗号・圧縮（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。

関連コマンド

DISABLE ENCO DEBUGGING（26 ページ）

ENABLE STAR DEBUGGING

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE STAR DEBUGGING

解説

STAR モジュールのデバッグ機能を有効にする。デフォルトは無効。
デバッグ機能を有効にすると、パケットをエンコード / デコードするたびにコンソールにメッセージが表示される。

入力・出力・画面例

```
Manager > enable star debugging

Manager > DEBUG - starEncode

Manager > DEBUG - starDecode

Manager > DEBUG - starEncode

Manager > DEBUG - starDecode

Manager > DEBUG - starEncode
```

関連コマンド

DISABLE STAR DEBUGGING（27 ページ）
SHOW STAR（51 ページ）

ENABLE STAR MKTTRANSFER

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

ENABLE STAR MKTTRANSFER=*sernum*

sernum: シリアル番号（1〜15 文字の数字）

解説

マスタールーター上で作成したマスターキーテーブルを、指定したシリアル番号を持つスレーブルーターに転送する。本コマンドはマスタールーター上で実行する。
転送状況は SHOW STAR MKTTRANSFER LOG コマンドで確認できる（State 欄）。

パラメーター

MKTTRANSFER　転送先ルーターのシリアル番号を指定する。SHOW STAR MKTTRANSFER LOG コマンドで表示された番号を指定する。また、自機のシリアル番号は SHOW SYSTEM コマンドで確認できる。

例

■マスターキーテーブルをスレーブルーター（シリアル番号 12345678）に転送する。

```
ENABLE STAR MKTTRANSFER=12345678
```

関連コマンド

SHOW STAR MKTTRANSFER LOG（55 ページ）

RESET ENCO COUNTER

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

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

解説

暗号・圧縮（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、STAC、PRED 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（46 ページ）

SET ENCO DHPRIORITY

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

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（39 ページ）

SET ENCO KEY

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

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（18 ページ）
DESTROY ENCO KEY（23 ページ）
SHOW ENCO KEY（49 ページ）

SET ENCO SW

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

SET ENCO SW [PREDCHANNELS=*0..4*] [STACCHANNELS=*0..4*] [STACSPEED=*0..3*]

解説

ソフトウェア圧縮機能の設定パラメーターを変更する。

パラメーター

PREDCHANNELS　Predictor 用圧縮チャンネルの数。1 チャンネル当たり 128KB の連続したメモリー空間を必要とする。メモリー容量 4MB の機種では最大チャンネル数は 2 に制限される。

STACCHANNELS　STAC LZS 用圧縮チャンネルの数。1 チャンネル当たり 13KB の連続したメモリー空間を必要とする。

STACSPEED　STAC LZS の圧縮モードを指定する。0（圧縮率最大。速度最低）から 3（圧縮率最低。速度最高）までの 4 モードがある。回線速度に応じた推奨値は別表を参照。

回線速度	圧縮モード
85kbps～	3
60～85kbps	2
40～59kbps	1
～40kbps	0

表 2: 回線速度と推奨圧縮モード（STACSPEED）

例

■STAC LZS 用のソフトウェア圧縮チャンネルを 2 チャンネル確保する。

```
SET ENCO SW STACCHANNELS=2
```

備考・注意事項

圧縮チャンネルを確保したときは、設定をファイルに保存し、ルーターを再起動する必要がある。
STACSPEED パラメーターは、AR720 と AR740 では使用されない。また、ハードウェア圧縮を使用しているときは、STACSPEED パラメーターの設定にかかわらず、常に圧縮率最高の処理となる。

関連コマンド

SHOW ENCO（39 ページ）

SET STAR

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

SET STAR=*star-id* {**MODE=**{**MASTER**|**SLAVE**|**STANDBY**}|**NETKEY** {**RANDOM**|
VALUE=*string*}|**MKT RANDOM**}

star-id: STAR エンティティー番号（0〜255）
string: 文字列（1〜14 文字。英小文字 a〜z と数字 2〜9 の組み合わせ。0 と 1 は使えない）

解説

STAR エンティティーのモード変更、ネットワークキーの作成、入力、マスターキーテーブルの作成を行う。

パラメーター

STAR STAR エンティティー番号
MODE STAR エンティティーの動作モード。STAR 鍵交換における本ルーターの役割を指定する。MASTER を指定した場合は、暗号鍵の生成と配布をつかさどるマスタールーターとして機能する。SLAVE は、マスタールーターから鍵を受け取るスレーブルーターとして機能する。STANDBY は、マスタールーター障害時に代役を務めることのできるスタンバイルーターとして機能する。
NETKEY ネットワークキーを作成あるいは入力するときに指定する。
RANDOM ランダムなネットワークキーを生成する。
VALUE 指定した値のキーを作成する。
MKT マスタールーター上で 160 個の DES 鍵からなるテーブルを作成し、それを STAR エンティティーのマスターキーテーブルとする。鍵はランダムに作成される。

例

■マスタールーター上で STAR エンティティー「0」のネットワークキーを生成する。

```
SET STAR=0 NETKEY RANDOM
```

■マスタールーター上で作成したネットワークキーをスレーブルーターに入力する。マスタールーター上で「SHOW STAR=0 NETKEY」を実行して表示された文字列を指定する。

```
SET STAR=0 NETKEY VALUE=fbj5m5ap7wasgd
```

■マスタールーター上でマスターキーテーブルを生成する。

```
SET STAR=0 MKT RANDOM
```

関連コマンド

CREATE STAR（21 ページ）
DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SHOW STAR（51 ページ）
SHOW STAR COUNTERS（53 ページ）
SHOW STAR MKTTRANSFER LOG（55 ページ）
SHOW STAR NETKEY（57 ページ）

SHOW ENCO

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

SHOW ENCO

解説

暗号・圧縮（ENCO）モジュールの全般的な設定情報を表示する。
表示される内容は、フィーチャーライセンスの有無や、暗号・圧縮ボードの有無によって異なる。

入力・出力・画面例

```
Manager > show enco

ENCO Module Configuration

  Hardware ............................... MAC
  Lowest valid channel ................... 1
  Highest valid channel .................. 511
  Compression Statistics Enabled ......... FALSE
  Diffie Hellman Priority ................ HIGH

  SW Processes available
    STAC - Stac Compression
    PRED - Predictor Compression
    RSA  - RSA Encryption
    DH   - Diffie Hellman
    HMAC - Message Digest

  Stac LZS compression performance level . 3
  Stac LZS compression footprint ......... 9989
  Stac LZS compression history size ...... 0
  Stac LZS decompression history size .... 0
  Stac LZS channels configured ........... 2
  Stac LZS channels available ............ 0
  Predictor channels configured .......... 1
  Predictor channels available ........... 0

  MAC Processes available
    DES  - DES Encryption
```

Hardware	暗号・圧縮ハードウェアの有無。AR010/AR011/AR011 V2/AR012 装着時は「MAC」、AR061 装着時（AR740 のみ）は「PAC」と表示される

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
Compression Statistics Enabled	圧縮チャンネルの統計保存機能の有効・無効
Diffie Hellman Priority	Diffie Hellman 鍵交換アルゴリズムの処理の優先度。HIGH、MEDIUM、LOW がある
SW Processes available	ソフトウェアで実現できる機能の一覧。NONE、DMAN、PREDICTOR、STAC、RSA、DH、HMAC などがある
MAC Processes available	ハードウェア（暗号・圧縮ボード）で実現できる機能の一覧。NONE、DMAN、DES、3DES、STAC などがある

表 3:

関連コマンド

SET ENCO DHPRIORITY（33 ページ）
SHOW ENCO CHANNEL（42 ページ）
SHOW ENCO COUNTERS（46 ページ）

SHOW ENCO CHANNEL

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

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

channel: チャンネル番号（0〜127）

解説

暗号・圧縮（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      SSH 00000001 1584    16        DES
     2       UP      SSH 00000002 1584    16        DES
  ---------------------------------------------------------------

SecOff > show enco channel=1

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

  Type ........................ ENCODE/DECODE
  State ....................... UP
  User ........................ SSH
  User ID ..................... 00000001
  Maximum Data Length ......... 1584
  Packet Overhead ............. 16
  Process ..................... DES
  Process Configuration:
    Des Type.........DES - 56 bit
    Channel Type......ENCODE/DECODE
    History Mode......On
    IV Type..........Specified
```

```
    Hardware..........MAC

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
 encode bad priorities            0  decode bad priorities            0
 encode bad length                0  decode bad length                0
 encode actions sent            123  decode actions sent            111
 good encodes                   123  good decodes                   111
 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 encode jobs            0  discarded decode 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（PPP、FR、MIOX、TEST、SA、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・圧縮プロセスの種類（PREDICTOR、STAC、RSA、DH、DES、HMAC）

表 4: 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（PPP、FR、MIOX、TEST、SA、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・圧縮プロセスの種類（PREDICTOR、STAC、RSA、DH、DES、HMAC）
Process Configuration	暗号・圧縮プロセスの詳細。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（XOR8、NONE（STAC LZS）、CRCCCITT、CRC16（Predictor））
Des Type	（DES のみ）DES アルゴリズム。「DES - 56 bit」、「3DES - 112 bit - outer CBC」、「3DES - 168 bit - inner CBC」、「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
Compression Statistics	圧縮プロセスの統計情報。ENABLE ENCO COMPSTATISTICS コマンドで有効に設定されているときだけ表示される
Number of Packets Compressed	圧縮処理されたパケット数
Best Compression Ratio	最大圧縮率
Mean Compression Ratio	平均圧縮率
Worst Compression Ratio	最低圧縮率

表 5: チャンネル番号指定時

関連コマンド

SHOW ENCO（39 ページ）
SHOW ENCO COUNTERS（46 ページ）

SHOW ENCO COUNTERS

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR320、AR720、AR740

SHOW ENCO COUNTERS={**DES**|**DH**|**HMAC**|**JOBPROCESSING**|**PRED**|**RSA**|**STAC**|**USER**|**UTIL**}

解説

暗号・圧縮（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）、JOBPROCESSING は、ENCO モジュールの全般的情報を示すもの。DES、DH（Diffie Hellman）、HMAC、RSA、STAC、PRED は個々の暗号・圧縮プロセスを対象としたもの。

入力・出力・画面例

```
Manager > show enco counters=des

ENCO Process DES/3DES Counters:

  configGood                     5  configBad                      0
  configNoResource               0  configNotSSH                   0
  badBuffer                      0  badAlign                       0
  badLength                      0  nohistory                      0
  desJobs                     1508  3Des2KeyJobs                   0
  3DesInnerJobs                  0  d3DesOuterJobs                 0
  noHistJobs                     0  desMacJobs                     0
  badDesType                     0  badJobType                     0

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

  goodDecrypt                  732  goodEncrypt                  776
  badDecrypt                     0  badEncrypt                     0

  DMA1Start                   1508  DMA2Start                   1486
  DMA1Done                    1508  DMA2Done                    1486
  DMABed                         0  DMABes                         0
  DMABrkp                        0  DMAConf                        0
  DMA1TimeOut                    0  DMA2TimeOut                    0
```

```
Manager > show enco counters=jobprocessing
  Input queue lengths
     Immediate queue..............          0
     Priority queue 0 (high)......          0
     Priority queue 1.............          0
     Priority queue 2.............          0
     Priority queue 3.............          0
     Priority queue 4.............          0
     Priority queue 5.............          0
     Priority queue 6.............          0
     Priority queue 7.............          0
     Priority queue 8 (low).......          0
     Total actions queued.........          0

  Lowest Input Priority Queue.....          4
  Highest Input Priority Queue....          0
  Input Queue Length Limit........        250

  Input Queue discards
     Immediate queue..............          0
     Priority queue 0 (high)......          0
     Priority queue 1.............          0
     Priority queue 2.............          0
     Priority queue 3.............          0
     Priority queue 4.............          0
     Priority queue 5.............          0
     Priority queue 6.............          0
     Priority queue 7.............          0
     Priority queue 8 (low).......          0
  Total Input Queue discards......          0

  Input Queue jobs processed
     Immediate queue..............         22
     Priority queue 0 (high)......          0
     Priority queue 1.............          0
     Priority queue 2.............          0
     Priority queue 3.............          0
     Priority queue 4.............       1521
     Priority queue 5.............          0
     Priority queue 6.............          0
     Priority queue 7.............          0
     Priority queue 8 (low).......          0
  Total Input Queue jobs processed       1543

  Output queue length.............          0
  Output queue jobs completed.....       1521
  Output queue discards...........          0

Manager > show enco counters=rsa
```

```
ENCO Process RSA Counters:

  goodPublicEncrypt                0  badPublicEncrypt                 0
  goodPrivateDecrypt              10  badPrivateDecrypt                0
  goodPrivateEncrypt               0  badPrivateEncrypt                0
  goodPublicDecrypt                0  badPublicDecrypt                 0
  goodGenerateKey                  3  badGenerateKey                   0
  badDataLength                    0  badKey                           0

Manager > show enco counters=user

ENCO User Interface Counters:

  startConfig                      5  startReconfig                    0
  attachGood                       5  attachFail                       0
  attachNoConfig                   0  attachBadUserType                0
  attachedInvalidChannel           0  attachedUnusedChannel            0
  attachProcNotAvail               0

  reconfigInvalidChannel           0  reconfigUnusedChannel            0
  reconfigNoConfig                 0

  detachInvalidChannel             0  detachUnusedChannel              0
  detachedInvalidChannel           0  detachedUnusedChannel            0
  detachGood                       4

  decodeInvalidChannel             0  decodeUnusedChannel              0
  encodeInvalidChannel             0  encodeUnusedChannel              0
  codedInvalidChannel              0  codedUnusedChannel               0
  resetInvalidChannel              0  resetUnusedChannel               0
  resetDoneInvalidChannel          0  resetDoneUnusedChannel           0

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

  discardInvalidChannel            0  discardUnusedChannel             0

Manager > show enco counters=util

ENCO Utility Counters:

  codeNullPacket                   0  codeBadPacketPriority            0
  codeBadPacketLength              0  codeBadConfig                    0
  actionSentEncode                 0  actionSentDecode                 0
  configureGood                   13  configureFail                    0
  encodeGood                       3  decodeGood                      10
  encodeBad                        0  decodeBad                        0
```

SHOW ENCO KEY

カテゴリー：暗号・圧縮 / 一般コマンド
対象機種：AR300 V2、AR300L V2、AR720、AR740

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

```
Manager > show enco key

   ID  Type      Length Digest   Description              Mod   IP
   ------------------------------------------------------------------------
    1  RSA-PRIVATE 1024 0536D310 my host_key              -     -
    2  RSA-PRIVATE  768 D9D3606F SSH Server Key           SSH   -
  100  RSA-PUBLIC  1024 7576F36A -                        -     -

Manager > show enco key=2

768
0x010001
0x53541c868ab4849446fb17519fec7eda3f57f74d382c1fa5c933c10ccc532aae
1b5482e2d577b705fe697845f1ffa72e62cc8033a33fe64e39b38cb7bdcd345f
01b9a849e46945bb68a4967cbe1fe5d22fe0c1787fcd62ec7a7cebfca35a6a95
```

ID	鍵番号
Algorithm	鍵の種類。DES、3DES2KEY、3DESINNER、RSA-PRIVATE、RSA-PUBLIC、GENERAL
Length	鍵の長さ
Digest	鍵データのメッセージダイジェスト（MD5）

Description	鍵の説明（CREATE ENCO KEY コマンドの DESCRIPTION パラメーター）
Module	鍵を使用するユーザーモジュール
IP Address	鍵に関連付けられた IP アドレス

表 6:

関連コマンド

CREATE ENCO KEY（18 ページ）
DESTROY ENCO KEY（23 ページ）
SET ENCO KEY（34 ページ）

SHOW STAR

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW STAR[=*star-id*]

star-id: STAR エンティティー番号（0〜255）

解説

STAR エンティティーに関する情報を表示する。

パラメーター

STAR STAR エンティティー番号。省略時はすべてのエンティティーについて、簡潔な情報が表示される。指定時は指定したエンティティーの詳細情報が表示される。

入力・出力・画面例

```
Manager > show star

Star Entities

       0

Manager > show star=0
  Star ID ......................... 0
  Star Mode ....................... MASTER
  Key Transfer Encryption Algorithm. DES - 56 bit
  Netkey Valid .................... TRUE
  Master Key Table Valid .......... TRUE
  Netkey Digest ................... 071e435b
  Master Key Table Digest ......... 5214c3e0
  Transfer State .................. INITIAL
```

Star ID	STAR エンティティー番号
Star Mode	STAR エンティティーの動作モード。SLAVE、STANDBY、MASTER のいずれか
Key Transfer Encryption Algorithm	暗号鍵の転送時に用いる暗号アルゴリズム。DES - 56 bit、3DES - 112 bit - outer CBC、3DES - 168 bit - inner CBC のいずれか

Netkey Valid	ネットワークキーが有効かどうか
Master Key Table Valid	マスターキーテーブルが有効かどうか
Netkey Digest	ネットワークキーの MD5 ダイジェスト
Master Key Table Digest	マスターキーテーブルの MD5 ダイジェスト
Transfer State	マスターキーテーブル配布処理の状態。INITIAL、ENABLED、DISABLED、UNKNOWN のいずれか

表 7:

関連コマンド

CREATE STAR（21 ページ）
DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SET STAR（37 ページ）
SHOW STAR COUNTERS（53 ページ）
SHOW STAR MKTTRANSFER LOG（55 ページ）
SHOW STAR NETKEY（57 ページ）

SHOW STAR COUNTERS

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW STAR[=*star-id*] **COUNTERS**

star-id: STAR エンティティー番号（0〜255）

解説

STAR モジュールに関するカウンター情報を表示する。

パラメーター

STAR　STAR エンティティー番号

入力・出力・画面例

```
Manager > show star counters

General Star Counters

  attachNoConfig                    0  attachBadId                    0
  detachInvalidChannel              0  detachUnusedChannel            0
  setCompInvalidChannel             0  setCompUnusedChannel           0
  resetInvalidChannel               0  resetUnusedChannel             0
  resetENoStar                      0  resetDNoStar                   0
  encodeInvalidChannel              0  decodeInvalidChannel           0
  encodeUnusedChannel               0  decodeUnusedChannel            0
  encoEventUnusedChannel            0  encoEventStarUnused            0

  getMKTUnusedChannel               0  getMKTInvalidChannel           0
  getMKTGood                        0  getMKTNoStar                   0
  setMKTUnusedChannel               0  setMKTInvalidChannel           0
  setMKTGood                        0  setMKTNoStar                   0

  getSKUnusedChannel                0  getSKNoStar                    0
  setSKUnusedChannel                0  setSKNoStar                    0
  getInfoUnusedChannel              8  getInfoNoStar                  0

  transferTimeoutChanUnused         0  transferTimeoutNoStar          0
  transferRequestChanUnused         0  transferRequestNoStar          0
  transferEnableChanUnused          0  transferEnableNoStar           1
  transEndNotifyChanUnused          0  transferEndNotifyNoStar        0
  sessTimeoutUnusedChannel          0  sessTimeoutNoStar              0
  createStar                        1  destroyStar                    0
```

```
  destroyNetKey                     0  destroyMKT                        0
  setStarMode                       0  setStarEncAlgorithm               0
  setStarNetKey                     1  setStarMKTRandom                  1

Manager > show star=0 counters
  encrConfGood                      3  compConfGood                      0
  confGood                          3  compConfGoodDetachE               0
  encrConfFail                      0  compConfFail                      0
  confFail                          0  compConfFailDetachE               0
  encrDetached                      2  compDetached                      0
  detached                          2  detachedConfFail                  0
  encodeGood                      210  encodeFailed                      0
  decodeGood                      210  decodeFailed                      0
  encodeDiscarded                   0  decodeDiscarded                   0
  resetGetSKAlreadyCurr             0  resetSetSKAlreadyCurr             0
  resetDNoSessionKey                0  resetDBadMKTIndex                 0
  resetCompHist                     0

  getMKTAlreadyCurrent              0  getMKTStarInvalid                 0
  getMKTEncodeFailed                0  getMKTGood                        4
  setMKTNULLBuffer                  0  setMKTAlreadyCurrent              0
  setMKTNoStar                      0  setMKTDecodeFailed                0
  setMKTGood                        0

  getSKAlreadyCurrent               0  getSKMKTInvalid                   0
  getSKEncodeFailed                 0  getSKResetFailed                  0
  getSKGood                        66
  setSKNULLBuffer                   0  setSKAlreadyCurrent               0
  setSKDecodeFailed                 0  setSKMKTInvalid                   0
  setSKResetFailed                  0  setSKGood                         4
```

関連コマンド

CREATE STAR（21 ページ）
DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SET STAR（37 ページ）
SHOW STAR（51 ページ）
SHOW STAR MKTTRANSFER LOG（55 ページ）
SHOW STAR NETKEY（57 ページ）

SHOW STAR MKTTRANSFER LOG

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW STAR MKTTRANSFER LOG

解説

スレーブルーターからのマスターキーテーブル転送要求を表示する。

入力・出力・画面例

```
Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
41849368            0  PPP        0 RECEIVED  16:22:27 08-Nov-2001          8
-------------------------------------------------------------------------------

Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
41849368            0  PPP        0 SENDING   16:22:27 08-Nov-2001         48
-------------------------------------------------------------------------------

Manager > show star mkttransfer log

Star Master Key Table transfer request log:
Serial Number  StarID User UserID   State     Time     Date        Requests
-------------------------------------------------------------------------------
41849368            0  PPP        0 COMPLETED 16:22:27 08-Nov-2001         48
-------------------------------------------------------------------------------
```

Serial Number	マスターキーテーブルを要求しているルーターのシリアル番号
StarID	STAR エンティティー番号
User	要求を受信したチャンネルのユーザーモジュール
UserID	要求を受信したチャンネルのユーザーモジュール ID
State	マスターキーテーブル転送要求の状態。RECEIVED（転送要求を受信）、BADKEY、SENDING（転送中）、FAILED、COMPLETED（転送完了）のいずれか

Time	最初の転送要求を受信した時刻
Date	最初の転送要求を受信した日付
Requests	同一の転送要求を受信した回数

表 8:

関連コマンド

CREATE STAR（21 ページ）
DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SET STAR（37 ページ）
SHOW STAR（51 ページ）
SHOW STAR COUNTERS（53 ページ）
SHOW STAR NETKEY（57 ページ）

SHOW STAR NETKEY

カテゴリー：暗号・圧縮 / STAR 鍵交換
対象機種：AR300 V2、AR300L V2、AR720、AR740

SHOW STAR=*star-id* NETKEY

star-id: STAR エンティティー番号（0〜255）

解説

指定した STAR エンティティーのネットワークキーを ASCII 形式で表示する。マスタールーター上でのみ実行可能。

パラメーター

STAR　STAR エンティティー番号

入力・出力・画面例

```
Manager > show star=0 netkey

  fbj5m5ap7wasgd
```

関連コマンド

CREATE STAR（21 ページ）
DESTROY STAR（24 ページ）
DISABLE STAR DEBUGGING（27 ページ）
ENABLE STAR DEBUGGING（30 ページ）
ENABLE STAR MKTTRANSFER（31 ページ）
SET STAR（37 ページ）
SHOW STAR（51 ページ）
SHOW STAR COUNTERS（53 ページ）
SHOW STAR MKTTRANSFER LOG（55 ページ）