第 10 章　VPN 情報の設定

10.1　IPsec 情報

IPsec の Main Mode を使用する場合の設定を行います。IPsec の Aggressive Mode を使用する場合は、remote ap ipsec type を参照してください。

10.1.1　ipsec delete

[機能]

IPsec 情報の削除

[入力形式]

ipsec delete <number>

[パラメタ]

<number>

削除する IPsec 情報を指定します。

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。
- all
  すべての IPsec 定義番号を削除対象とします。

[説明]

<number>で指定した IPsec 情報を削除します。

10.1.2 ipsec move

[機能]

IPsec 情報の定義順序の変更

[入力形式]

ipsec move <number> <new_number>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号移動元のを、0～63 の範囲の 10 進数値を指定します。

<new_number>

- IPsec 定義番号
  移動先の IPsec 定義番号を、0～63 の範囲の 10 進数値を指定します。

[説明]

IPsec 情報の定義順序を変更します。

10.1.3　ipsec range

[機能]

IPsec 情報の対象範囲の設定

[入力形式]

ipsec [<number>] range <src_addr>/<mask> <dst_addr>/<mask>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0〜63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスクビット数は 0〜32(10 進数) が入力可能です。
  例) IPv4: 192.168.1.1/24
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

<dst_addr>/<mask>

IPsec 対象となる宛先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。マスクビット数は 0〜32(10 進数) が入力可能です。
  例) IPv4: 192.168.1.1/24

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)
IPsec 情報は、手動鍵設定と自動鍵設定 (交換) を合わせて、装置に 63 個設定することが可能です。
一つのトンネル (双方向で IPsec を行う) を張るためには、IPsec 情報を入力用と出力用を対にして定義して下さい。
<src_addr>/<dst_addr>の any4 指定は、手動鍵設定の時にのみ有効です。

[注意]

手動鍵設定と自動鍵設定 (交換) について

- 手動鍵設定と自動鍵設定 (交換) の識別方法
  「ipsec path」で path の直後に現れる<spi>に、文字列"ike"が指定されていた場合、その定義を自動鍵設定 (交換) と判断します。
  手動鍵設定を行う場合に、自動鍵設定 (交換) で使用する定義を行っても使用されません。

- 自動鍵設定 (交換) の定義について
  以下のコマンドは、IKE(ISAKMP) で ISAKMP SA および IPsec SA の確立および更新に使用される定義です。
  ipsec path ike ... と定義した場合に使用されます。
  - ipsec pfs
  - ipsec lifetime
  - ipsec lifebyte
  - ipsec newsa initiator
  - ipsec newsa responder
  - ike remote address
  - ike remote port
  - ike remote shared key
  - ike remote proposal encrypt
  - ike remote proposal hash
  - ike remote proposal pfs
  - ike remote proposal lifetime
  - ike remote retry
  - ike remote release

[未設定時]

IPsec 情報の range 設定は設定されません。IPsec を使用する場合は必ず設定してください。

10.1.4　ipsec path

[機能]

IPsec 情報の区間の設定

[入力形式]

ipsec [<number>] path <spi> <src_addr> <dst_addr>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<spi>

- セキュリティパラメタインデックス (SPI)
  セキュリティパラメタインデックスを、16 進数値で指定します。(0x100～0xffffffff の 16 進数)
  但し、自動鍵設定 (交換) を使用する場合は、文字列で"ike"と指定します。

<src_addr>

- IPsec 対象パケットをセキュア化する送信元 IP アドレスを指定します。
  例) IPv4: 192.168.1.1

<dst_addr>

- IPsec 対象パケットをアンセキュア化する宛先 IP アドレスを指定します。
  指定方法は<src_addr>参照。

[説明]

IPsec 対象パケットがセキュア化される区間を設定します。(Security Association Database の情報)

[注意]

<src_addr>の 0.0.0.0/0 指定は、手動鍵設定の時にのみ有効です。自動鍵設定の場合に指定すると正しく動作しません。

[未設定時]

IPsec 対象パケットがセキュア化される区間を定義していないものとみなされます。
IPsec を使用する場合は必ず設定してください。

10.1.5 ipsec encrypt

[機能]

IPsec 情報の暗号情報の設定

[入力形式]

ipsec [<number>] encrypt <enc_algo>[,<enc_algo>...] [<kind> <enc_key> [encrypted]]

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
自動鍵設定として定義する場合は、複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ',' で区切ります。(暗号アルゴリズム定義とセキュリティプロトコルの関係は [説明] を参照)

- des-cbc
- 3des-cbc
- null
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵
- text
  文字列鍵

<enc_key>

暗号鍵を指定します。

鍵種別 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc 3des-cbc	1～16桁 1～48桁	8文字 24文字

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで"0"でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。
  以下に、入力範囲を示します。
- 暗号化された暗号鍵
  暗号化された暗号鍵を指定します。
  show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化暗号鍵指定
  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[説明]

送受信パケットを暗号化／復号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
show ipsec [<number>] encrypt を実行すると、暗号化していない暗号鍵が表示されます。

表 10.1　認証／暗号アルゴリズム定義とセキュリティプロトコルの関係

auth(認証)	encrypt(暗号)	セキュリティプロトコル
―	―	ESP(null encrypt)
○	―	AH(認証)
―	○	ESP(暗号)
○	○	ESP(認証 + 暗号)

○:定義あり ―:定義なし

- 手動鍵設定としての暗号アルゴリズム
  暗号アルゴリズムが"none"または"null"の場合、暗号鍵は入力できません。
- 自動鍵設定としての暗号アルゴリズム
  暗号鍵は自動生成されるので、設定は不要です。
  暗号アルゴリズムを複数指定する場合、指定順序に関わらず以下の優先順位となります。

  1. 3des-cbc
  2. des-cbc
  3. null

[注意]

- 暗号アルゴリズムの複数指定は、自動鍵設定のみの機能なので、暗号アルゴリズムの複数指定と、暗号鍵を同時に指定することはできません。
  認証／暗号アルゴリズムの未定義は、認証アルゴリズムを"none"、暗号アルゴリズムを"null"と指定した場合と同じ動作となります。
- weak key
  手動鍵設定で指定する暗号鍵では、RFC2409 の Appendix A に記載されている weak key を指定できません。

```
RFC2409のAppendix Aに記載されているweak key

0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

3des-cbc の場合は、暗号鍵を 16 桁毎に 3 つの鍵に分割し、いずれかの鍵が weak key となるような指定はできません。

[未設定時]

暗号アルゴリズムを指定しないものとみなされます。

```
ipsec <number> encrypt none
```

10.1.6　ipsec auth

[機能]

IPsec 情報の認証情報の設定

[入力形式]

ipsec [<number>] auth <auth_algo>[,<auth_algo>...] [<kind> <auth_key> [encrypted]]

[パラメタ]

<number>

- IPsec 定義番号

  IPsec 定義番号を、0～63 の 10 進数値で指定します。

  省略した場合は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。

自動鍵設定として定義する場合は、複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ',' で区切ります。(認証アルゴリズム定義とセキュリティプロトコルの関係は、「ipsec encrypt コマンドの [説明]」を参照)

- hmac-md5
- hmac-sha1
- none

<kind>

鍵種別を指定します。

- hex

  16 進数鍵

- text

  文字列鍵

<auth_key>

認証鍵を指定します。

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-md5	1～32 桁	16 文字
hmac-sha1	1～40 桁	20 文字

- 暗号化されていない認証鍵

  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで"0"でパディングされます。

  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

- 暗号化された認証鍵を指定します。

  show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。

  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証鍵指定
  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[説明]

送受信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。
show ipsec [<number>] encrypt を実行すると、暗号化していない認証鍵が表示されます。

- 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵を省略することができます。
- 自動鍵設定としての認証アルゴリズム
  認証鍵は自動生成されるので、設定は不要です。
  認証アルゴリズムを複数指定する場合、指定順序に関わらず以下の優先順位となります。

  1. hmac-md5
  2. hmac-sha1

[注意]

認証アルゴリズムの複数指定は、自動鍵設定のみの機能なので、認証アルゴリズムの複数指定と、認証鍵を同時に指定することはできません。

[未設定時]

認証アルゴリズムを指定しないものとみなされます。

```
ipsec <number> auth none
```

10.1.7　ipsec pfs

[機能]

IPsec 情報の PFS グループの設定

[入力形式]

ipsec [<number>] pfs <pfs_group>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024
- off
  Diffie-Hellman グループを使用しません。

[説明]

IPsec で使用する鍵の交換データを保護する、PFS グループの設定を行います。PFS グループを使用する場合、MODP1024 が強い暗号強度となりますが処理に時間がかかりますので、ネゴシエーション時間が長くなります。

[注意]

PFS グループに off を指定した場合、PFS による鍵交換データ保護は行いません。
セキュア通信を行いたい場合は適切な PFS グループを設定して下さい。

[未設定時]

PFS グループに Diffie-Hellman のグループを使用しないものとみなされます。

```
ipsec <number> pfs off
```

10.1.8 ipsec lifetime

[機能]

IPsec 情報の SA 有効時間の設定

[入力形式]

ipsec [<number>] lifetime <lifetime>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  IPsec 用 Security Association(SA) 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間の設定を行います。

[未設定時]

SA 有効時間に 8 時間を指定したものとみなされます。

```
ipsec <number> lifetime 8h
```

10.1.9　ipsec lifebyte

[機能]

IPsec 情報の SA 有効パケット量の設定

[入力形式]

ipsec [<number>] lifebyte <lifebyte>

[パラメタ]

<number>

- IPsec 定義番号

  IPsec 定義番号を、0〜63 の 10 進数値で指定します。

  省略した場合は、0 を指定したものとみなされます。

<lifebyte>

- SA 有効パケット量

  IPsec 用 Security Association(SA) 有効パケット量のバイト数を、0k あるいは 2400k〜110592000k の範囲で指定します。

  単位は以下の 3 種類です。1k は 1024 バイトで計算されます。

  k: キロバイト (例: 2400k → 2400k)

  m: メガバイト (例: 4m → 4096k)

  g: ギガバイト (例: 1g → 1048576k)

  0 を指定した場合は、lifebyte による IPsec SA の更新を行いません。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効パケット量 (キロバイト) の設定を行います。

[未設定時]

SA 有効パケット量に 0 バイトを指定したものとみなされます。

```
ipsec <number> lifebyte 0
```

10.1.10 ipsec newsa initiator

[機能]

IPsec 情報の New SA Initiator(更新時間) の設定

[入力形式]

ipsec [<number>] newsa initiator <time>

[パラメタ]

<number>

- IPsec 定義番号

  IPsec 定義番号を、0～63 の 10 進数値で指定します。

  省略した場合は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間

  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Initiator の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。

相手側の New SA Responder と同じ時間にならないように設定して下さい。

[未設定時]

Initiator SA 更新時間に 90 秒を指定したものとみなされます。

```
ipsec <number> newsa initiator 90s
```

10.1.11　ipsec newsa responder

[機能]

IPsec 情報の New SA Responder(更新時間) の設定

[入力形式]

ipsec [<number>] newsa responder <time>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Responder の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。

[未設定時]

Responder SA 更新時間に 30 秒を指定したものとみなされます。

```
ipsec <number> newsa responder 30s
```

10.2 IKE 情報

10.2.1 ike remote delete

[機能]

IKE 情報の削除

[入力形式]

ike remote delete <ike_number>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
- all
  すべての IKE 定義番号を削除対象とします。

[説明]

<ike_number>で指定した IKE 情報を削除します。IKE 情報を削除しても<ike_number>のソートはしません。

10.2.2　ike remote address

[機能]

IKE 情報の宛先アドレスの設定

[入力形式]

ike remote [<ike_number>] address <address>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 宛先アドレス
  相手装置のアドレスを指定します。0.0.0.0 が設定された場合は、定義なしとなります。

[説明]

IKE セッションを確立する、相手装置の IP アドレスの設定を行います。

[未設定時]

IKE 情報の宛先アドレスは設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.3 ike remote port

[機能]

IKE 情報の相手側 IKE ポート番号の設定

[入力形式]

ike remote [<ike_number>] port <port>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

- 相手側 IKE(ISAKMP) ポート番号
  相手側 IKE(ISAKMP) ポート番号を指定します。(デフォルト: 500 番)

[説明]

SA 確立のネゴシエーションを行う、相手側 IKE(ISAKMP) サーバのポート番号の設定を行います。

[未設定時]

相手側 IKE(ISAKMP) ポート番号に標準ポート番号である 500 を指定したものとみなされます。

```
ike remote <ike_number> port 500
```

10.2.4　ike remote shared key

[機能]

IKE セッション確立時の共通鍵 (Pre-shared key) の設定

[入力形式]

ike remote [<ike_number>] shared key <kind> <shared_key> [encrypted]

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵
- text
  文字列鍵

<shared_key>

認証鍵を指定します。

- 暗号化されていない共通鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

16 進数鍵	文字列鍵
1～256 桁	1 文字～128 文字

- 暗号化された共通鍵を指定します。
  show コマンドで表示される暗号化された共通鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化共通鍵指定
  <shared_key>に暗号化された共通鍵を指定する場合に指定します。

[説明]

SA 確立のネゴシエーションの時に接続相手を認証するための、共通鍵の設定を行います。
show コマンドでは、暗号化された共通鍵が encrypted と共に表示されます。
show ike remote [<ike_number>] shared key を実行すると、暗号化していない認証鍵が表示されます。

[未設定時]

IKE セッション確立時の共通鍵 (Pre-shared key) は設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.5 ike remote proposal delete

[機能]

IKE 情報の Proposal 定義の削除

[入力形式]

ike remote [<ike_number>] proposal delete <count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する Proposal 定義を指定します。

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
- all
  <ike_number>で指定した IKE 情報のすべての Proposal 定義を削除対象とします。

[説明]

<ike_number>で指定した IKE 情報の<count>で指定される Proposal 定義または、すべての Proposal 定義を削除します。

10.2.6　ike remote proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[入力形式]

ike remote <ike_number> proposal move <count> <new_count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  移動元の Proposal 定義優先順序を指定します。

<new_count>

- Proposal 定義番号
  移動先の Proposal 定義優先順序を指定します。

[説明]

<ike_number>で指定した IKE セッション用の Proposal 定義優先順序を変更します。

表 10.2　IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	ハッシュ情報	hmac-md5	0	...
c	PFS グループ	modp768	modp1024	...
d	SA 有効時間	600s	0	...

※ a を複数指定 (<count>0,1,2 を定義) した場合、他の情報は定義しなければ各情報のデフォルト値を採用します。

IKE セッションのネゴシエーションは、Proposal 単位 (a～d を一組) として行います。その中で a～c は相手装置の定義と一致することが条件となります。

複数定義した場合の<count>が 1 以降の定義は、Main モードで自側が Initiator の場合に使用されます。

自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。

10.2.7 ike remote proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[入力形式]

ike remote <ike_number> proposal [<count>] encrypt <enc_algo>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<enc_algo>

- 暗号アルゴリズム
  暗号アルゴリズムを指定します。
  des-cbc
  3des-cbc

[説明]

IKE セッションの送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。

[未設定時]

暗号アルゴリズムは設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.8　ike remote proposal hash

[機能]

IKE セッション用ハッシュ情報の設定

[入力形式]

ike remote <ike_number> proposal [<count>] hash <hash_algo>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<hash_algo>

ハッシュアルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

ハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
ike remote <ike_number> proposal hash hmac-md5
```

10.2.9 ike remote proposal pfs

[機能]

IKE セッション用 PFS グループの設定

[入力形式]

ike remote <ike_number> proposal [<count>] pfs <pfs_group>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024

[説明]

IKE セッションのネゴシエーションパケットを保護するための、PFS グループの設定を行います。

[未設定時]

PFS グループに modp768 を指定したものとみなされます。

```
ike remote <ike_number> proposal pfs modp768
```

10.2.10　ike remote proposal lifetime

[機能]

IKE 用 SA 有効時間の設定

[入力形式]

ike remote <ike_number> proposal [<count>] lifetime <lifetime>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<lifetime>

- IKE 用 Security Association(SA) 有効時間
  SA 有効時間の時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IKE セッションのネゴシエーションパケットを保護する SA の有効時間 (秒) の設定を行います。

[未設定時]

IKE SA 有効時間に 1 日 (24 時間) を指定したものとみなされます。

```
ike remote <ike_number> proposal lifetime 1d
```

10.2.11 ike remote retry

[機能]

IKE 情報の初回再送時間 (再送時間) および再送回数の設定

[入力形式]

ike remote <ike_number> retry <time> <count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 初回再送時間
  初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[説明]

IKE セッションのネゴシエーションパケットに対する再送時間および再送回数の設定を行います。

[未設定時]

IKE 情報の初回再送時間に 10 秒、再送回数設定に 3 回を指定したものとみなされます。

```
ike remote <ike_number> retry 10s 3
```

10.2.12　ike remote release

[機能]

IPsec / IKE 情報の解放動作の設定

[入力形式]

ike remote [<ike_number>] release <mode>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0〜31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPsec / IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[説明]

自動鍵設定で作成された SA 情報の解放動作を設定します。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンド は以下の回線切断動作時に有効です。

- ISDN(回線交換) を使用した時

[未設定時]

回線切断時に IKE SA 情報の解放動作を行うものとみなされます。

```
ike remote <ike_number> release on
```