機能概要

VPN(Virtual Private Network)は、インターネットのような開かれたネットワークを、あたかも専用線のような閉ざされたネットワークのように利用する技術です。MUCHO-EVはVPNをサポートしており、専用線を用いなくても、安価にセキュリティの高いネットワークを構築できます。

■VPNを使用して通信するために必要な設定と作業の流れを次に示します。

1 ルータ機能の設定

VPNの設定前に、VPNを除くルータ機能の設定を行います。
●ルータ機能を使う（☛P143）

2 VPN動作モードON

VPNを使用するには、VPN動作モードをONにします。
●VPNの設定（☛P296）

3 VPNピアの登録

VPNを使用して通信する接続相手のルータ（SG）を登録します。登録したVPNピアと鍵交換する際のpre-shared keyも設定します。
●VPNピアの登録（☛P297）

4 暗号化ポリシーの登録

VPNの暗号化・認証に関する動作条件を登録します。
●暗号化ポリシーの登録（☛P299）

5 VPN対象パケットの登録

どのようなパケットに対して、VPN制御を行うかを登録します。
●VPN対象パケットの登録（☛P301）

お知らせ

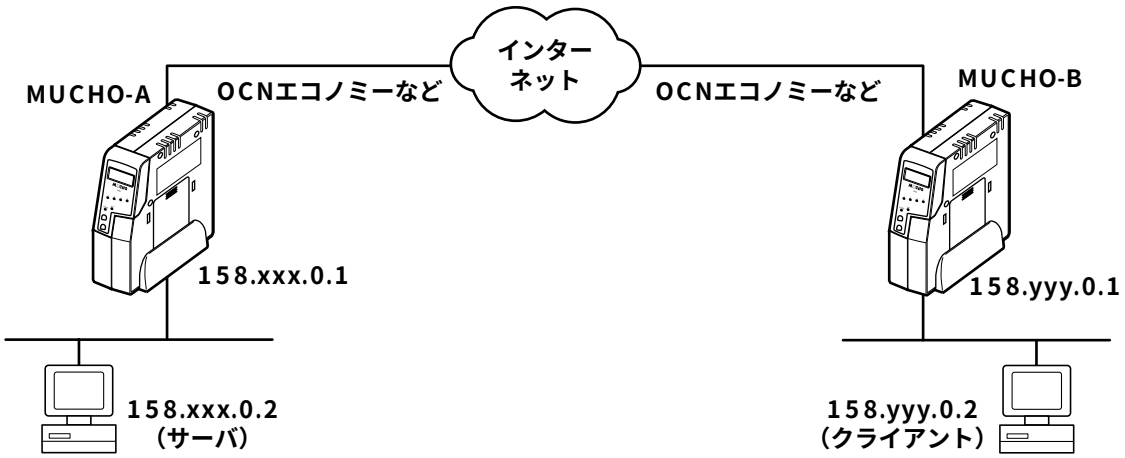
VPN通信を行う際は、データ圧縮機能は動作しません。

具体的な設定方法

設定M

専用線－専用線接続

OCNエコノミーなどを使用している2台のMUCHO-EVをVPN接続する設定について説明します。MUCHO-A側のネットワークとMUCHO-B側のネットワーク間の、全てのパケットを暗号化して送受信する設定です。ここではMUCHO-Aの設定を例にしています。
MUCHO-AとMUCHO-Bの間はVPN接続し、その他の通信はVPN接続しないように設定する場合は、「設定O」をご覧ください。（☛P290）



＜設定データの例＞

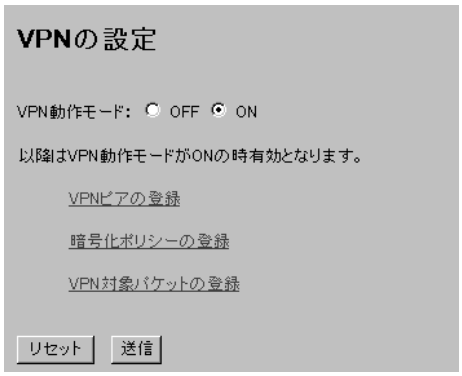
画面名	設定項目	設定例
VPNの設定	VPN動作モード	ON
VPNピアの登録	IPアドレス指定	158.YYY.0.1
	鍵データ（文字列）	secret
	NAT動作モード	off
暗号化ポリシーの登録	ポリシー識別子	1
	SAライフタイム	デフォルトを使用する（28,800秒）
	鍵データ（PFS）の再生成	再生成しない
	暗号化アルゴリズム	DES
	認証アルゴリズム	HMAC-MD5
VPN対象パケットの登録	id	1
	宛先指定	全て
	宛先ポート指定	全てのポート
	送信元指定	全て
	送信元ポート指定	全てのポート
	プロトコル指定	全て
	宛先インタフェース	専用線
	IPsec処理タイプ	IPsec処理して中継
	SA確立契機	起動時確立しない データ通信時
	登録済みVPNピア指定	158.YYY.0.1
	ポリシー識別子による登録済み暗号化ポリシーの指定	1

＜Webブラウザ操作＞

1 ルータの［便利な設定］をクリックします。

2 ［VPNの設定］をクリックします。

3 VPN動作モードの［ON］をクリックします。

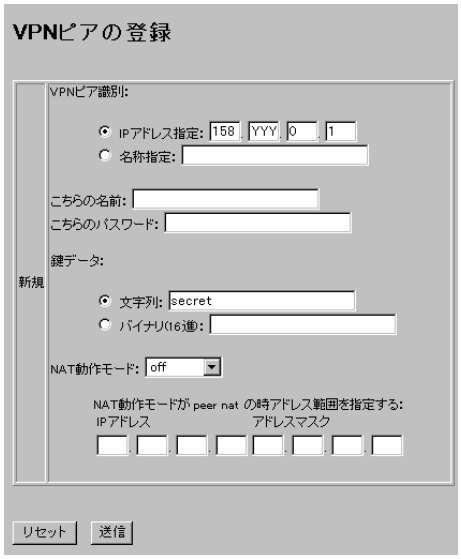


設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

4 ［VPNピアの登録］をクリックします。

5 VPNピア識別と鍵データを設定します。

［新規登録］をクリックします。
IPアドレスや鍵データなどを下記のように入力します。



設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

〈次ページへ続く〉

お知らせ

手順1のあとに、ユーザIDとパスワードの入力画面が表示されることがあります。
ユーザIDとパスワードを入力してください。（☛P37）

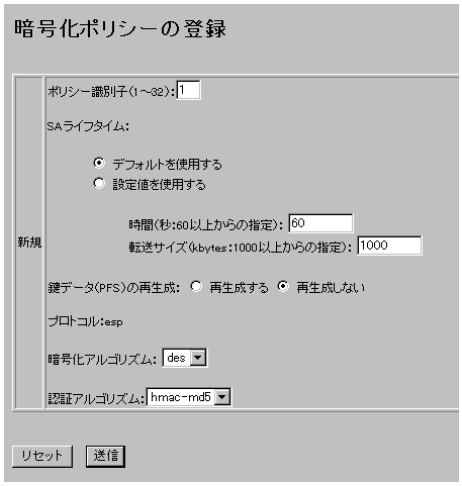
具体的な設定方法

6 ブラウザの［戻る］ボタンをクリックします。

7 ［暗号化ポリシーの登録］をクリックします。

8 暗号化ポリシーを設定します。

［新規登録］をクリックします。
ポリシー識別子や暗号化・認証アルゴリズムなどを下記のように入力します。



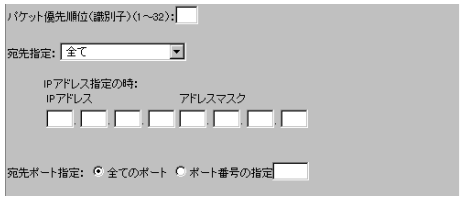
設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

9 ブラウザの［戻る］ボタンをクリックします。

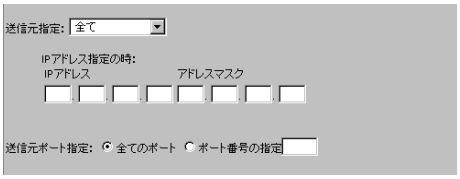
10 ［VPN対象パケットの登録］をクリックします。

11 パケット優先順位および宛先に関する情報を設定します。

［新規登録］をクリックします。
パケット優先順位・宛先指定などを下記のように入力します。

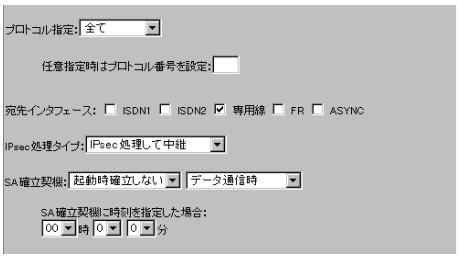


12 送信元に関する情報を設定します。



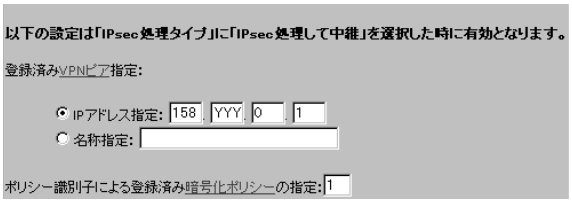
13 プロトコルや宛先インタフェースを設定します。

プロトコル指定・宛先インタフェース・IPsec処理タイプ・SA確立契機を下記のように入力します。



14 登録済みVPNピア指定・暗号化ポリシーの指定をします。

IPアドレスなどを下記のように入力します。



設定が終わったら、[送信] をクリックします。設定内容が本装置に送信され、確認画面が表示されます。[OK] をクリックします。

15 設定内容を有効にするには、MUCHO-EVのリセットが必要です。[リセット] をクリックします。

「リセット」画面が表示されます。

16 [装置をリセットする] をクリックします。

本装置が再起動し、設定内容が有効になります。
MUCHO-Bにも同様の設定を行ってください。

具体的な設定方法

＜コマンド操作＞

1 コンフィグレーションモードに移行します。(☛P39)

```
#conf
Configuration password:
conf#
```

2 VPN使用の設定（vpnコマンド）

「VPN動作モードをON」を設定するため「vpn on」を入力します。

```
conf#vpn on
```

3 VPNピアの登録（vpnpeerコマンド）

「IPアドレス指定(158.YYY.0.1)」、「鍵データ(a,secret)」、「NAT動作モード(off)」を「vpnpeer」コマンドで入力します。

```
conf#vpnpeer add addr=158.YYY.0.1 key=a,secret nat=off
```

4 暗号化ポリシーの登録（vpnpolicyコマンド）

「ポリシー識別子(1)」を「vpnpolicy」コマンドで入力します。

```
conf#vpnpolicy add id=1
```

5 VPN対象パケットの登録（vpnselectorコマンド）

「セレクタID(1)」、「宛先指定(all)」、「送信元指定(all)」、「登録済みVPNピア指定(158.YYY.0.1)」、「ポリシー識別子による登録済み暗号化ポリシーの指定(1)」を「vpnselector」コマンドで入力します。

```
conf#vpnselector add id=1 dst=all src=all peeraddr=158.YYY.0.1
policy=1
```

6 設定を保存します。(☛P42)

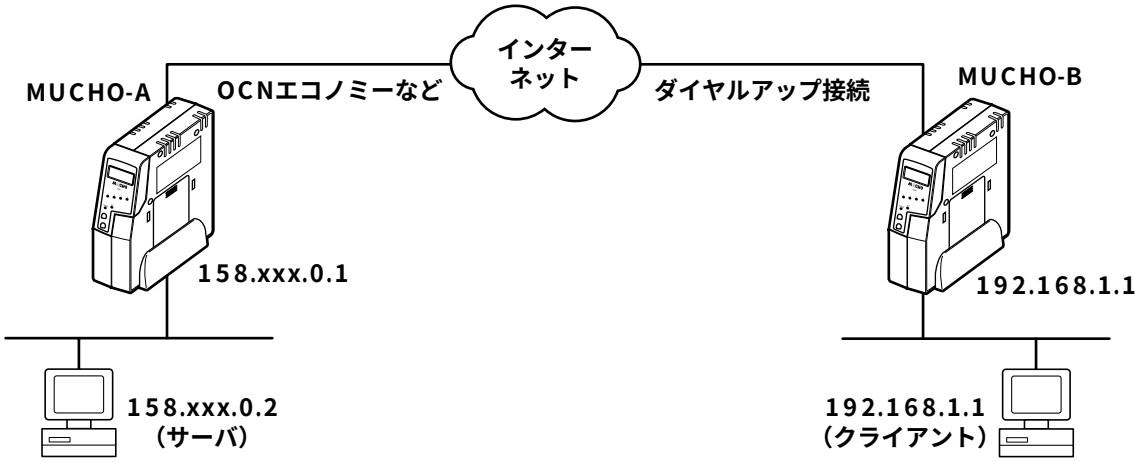
```
conf#exit
Configuration modified. save ok?(y/n):y
please reset#
Do you want to continue(y/n)?:y
```

MUCHO-Bにも同様の設定を行ってください。

設定N

専用線－ダイヤルアップ接続

OCNエコノミーなどで接続したMUCHO-EVと、ダイヤルアップでインターネット接続しているMUCHO-EVを、VPN接続する設定について説明します。MUCHO-A側のネットワークとMUCHO-B側のネットワーク間の、全てのパケットを暗号化して送受信する設定です。この場合、MUCHO-BのWAN側のIPアドレスがダイナミックに割り当てられるため、IPアドレスは事前にはわかりません。したがってVPN接続はMUCHO-Bからのみ行うことができます。ここではMUCHO-Aの設定を例にしています。
MUCHO-AとMUCHO-Bの間はVPN接続し、その他の通信はVPN接続しないように設定する場合は、「設定O」をご覧ください。（☛P290）



＜設定データの例＞

画面名	設定項目	設定例
VPNの設定	VPN動作モード	ON
VPNピアの登録	名称指定	Tokyo
	鍵データ（文字列）	secret
	NAT動作モード	off
暗号化ポリシーの登録	ポリシー識別子	1
	SAライフタイム	デフォルトを使用する (28800秒)
	鍵データ（PFS）の再生成	再生成しない
	暗号化アルゴリズム	DES
	認証アルゴリズム	HMAC-MD5
VPN対象パケットの登録	id	1
	宛先指定	全て
	宛先ポート指定	全てのポート
	送信元指定	全て
	送信元ポート指定	全てのポート
	プロトコル指定	全て
	宛先インタフェース	専用線
	IPsec処理タイプ	IPsec処理して中継
	SA確立契機	起動時確立しない データ通信時
	登録済みVPNピア指定	Tokyo
	ポリシー識別子による登録済み暗号化ポリシーの指定	1

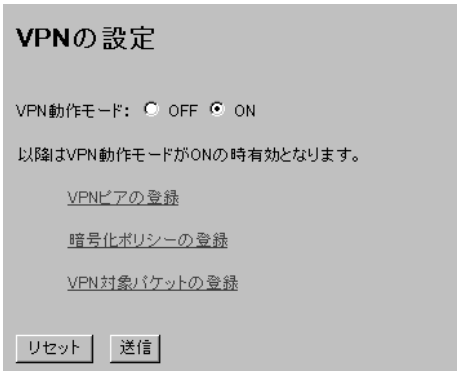
具体的な設定方法

＜Webブラウザ操作＞

1 ルータの［便利な設定］をクリックします。

2 ［VPNの設定］をクリックします。

3 VPN動作モードの［ON］をクリックします。

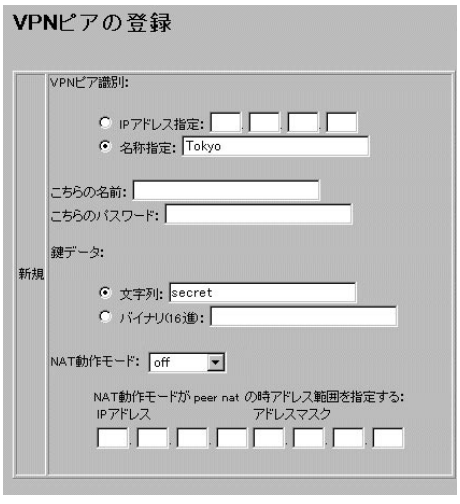


設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

4 ［VPNピアの登録］をクリックします。

5 VPNピア識別と鍵データを設定します。

［新規登録］をクリックします。
VPNピア識別の名称や鍵データを下記のように入力します。



設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

お知らせ

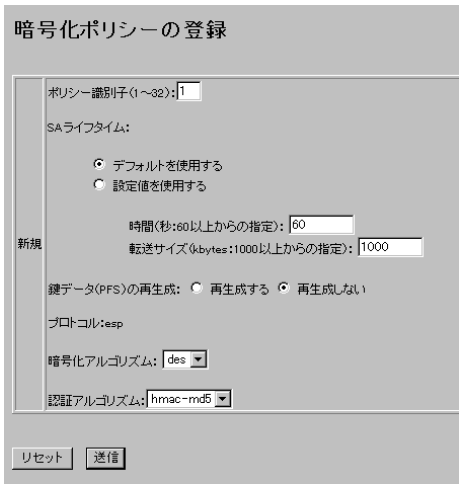
MUCHO-Aの設定では、「VPNピア識別」に名称を指定します（例：Tokyo）。MUCHO-Bはダイヤルアップ接続であり、動的にIPアドレスが割り当てられます。そのため、固定したIPアドレスを指定できないので、名称での指定が必要になります。
MUCHO-Bの設定では「VPNピア識別」にMUCHO-AのIPアドレスを指定し、さらに「こちらの名前」に「Tokyo」を指定します。

6 ブラウザの［戻る］ボタンをクリックします。

7 ［暗号化ポリシーの登録］をクリックします。

8 暗号化ポリシーを設定します。

［新規登録］をクリックします。
ポリシー識別子や暗号化・認証アルゴリズムなどを下記のように入力します。



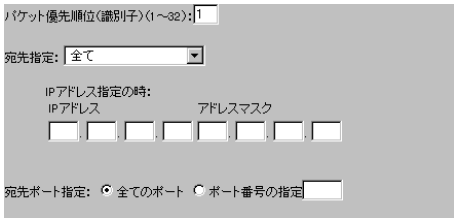
設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

9 ブラウザの［戻る］ボタンをクリックします。

10 ［VPN対象パケットの登録］をクリックします。

11 パケット優先順位および宛先に関する情報を設定します。

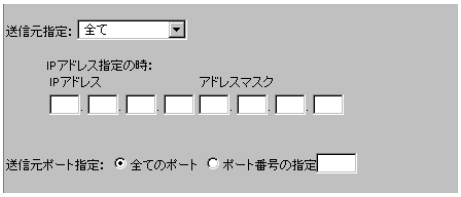
［新規登録］をクリックします。
パケット優先順位・宛先指定などを下記のように入力します。



〈次ページへ続く〉

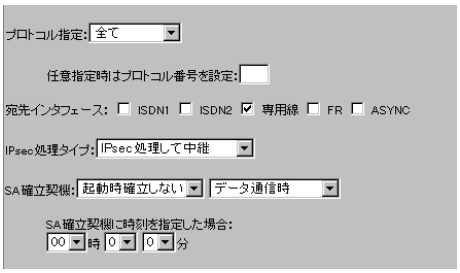
具体的な設定方法

12 送信元に関する情報を設定します。



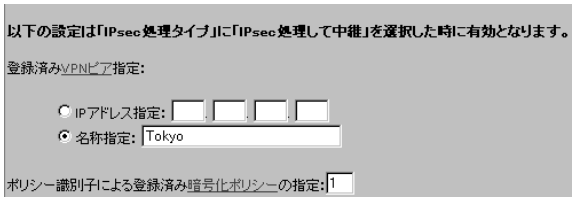
13 プロトコルや宛先インタフェースを設定します。

プロトコル指定・宛先インタフェース・IPsec処理タイプ・SA確立契機を下記のように入力します。



14 登録済みVPNピア指定・暗号化ポリシーの指定をします。

名称などを下記のように入力します。



設定が終わったら、[送信] をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
[OK] をクリックします。

15 設定内容を有効にするには、MUCHO-EVのリセットが必要です。[リセット] をクリックします。

「リセット」画面が表示されます。

16 [装置をリセットする] をクリックします。

本装置が再起動し、設定内容が有効になります。
MUCHO-Bにも同様の設定を行ってください。

お知らせ

手順1のあとに、ユーザIDとパスワードの入力画面が表示されることがあります。
ユーザIDとパスワードを入力してください。(☛P37)

＜コマンド操作＞

1 コンフィグレーションモードに移行します。(☛P39)

```
#conf
Configuration password:
conf#
```

2 VPN使用の設定（vpnコマンド）

「VPN動作モードをON」を設定するため「vpn on」を入力します。

```
conf#vpn on
```

3 VPNピアの登録（vpnpeerコマンド）

「IPアドレス指定(Tokyo)」、「鍵データ(a,secret)」を「vpnpeer」コマンドで入力します。

```
conf#vpnpeer add name=Tokyo key=a,secret
```

4 暗号化ポリシーの登録（vpnpolicyコマンド）

「ポリシー識別子(1)」を「vpnpolicy」コマンドで入力します。

```
conf#vpnpolicy add id=1
```

5 VPN対象パケットの登録（vpnselectorコマンド）

「セレクタID(1)」、「宛先指定(all)」、「送信元指定(all)」、「登録済みVPNピア指定(Tokyo)」、「ポリシー識別子による登録済み暗号化ポリシーの指定(1)」を「vpnselector」コマンドで入力します。

```
conf# vpnselector add id=1 dst=all src=all peername=Tokyo policy=1
```

6 設定を保存します。(☛P42)

```
conf#exit
Configuration modified. save ok?(y/n):y
please reset#
Do you want to continue(y/n)?:y
```

MUCHO-Bにも同様の設定を行ってください。

お知らせ

MUCHO-Bの設定では、VPNピアの登録を、「vpnpeer」コマンドで次のように入力します。

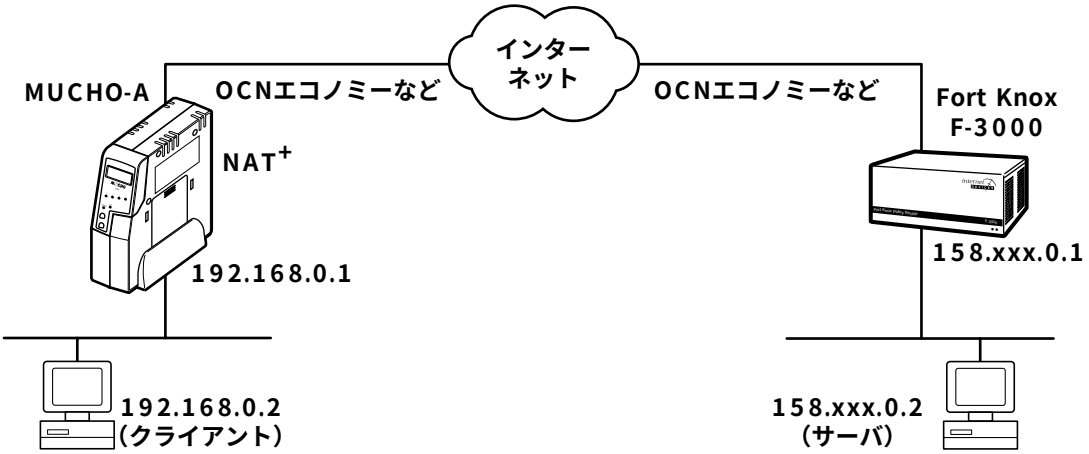
conf#vpnpeer add addr=158.xxx.0.1 myname=Tokyo key=a,secret

具体的な設定方法

設定O

専用線ーFortKnox接続

OCNエコノミーなどで接続したMUCHO-EVとFortKnoxを、VPN接続する設定について説明します。
次のケースを例にしています。
●MUCHO-A側のネットワークとFortKnox側の先にあるサーバ間のパケットを暗号化して送受信する。
●MUCHO-A側のネットワークとFortKnox側サーバ間以外のパケットは、VPNを使用せずにデータ通信を行う。



＜設定データの例＞

画面名	設定項目	設定例
VPNの設定	VPN動作モード	ON
VPNピアの登録	IPアドレス指定	158.XXX.0.1
	こちらの名前	mucho-ev
	こちらのパスワード	himitsu
	鍵データ（文字列）	secret
	NAT動作モード	nat+
暗号化ポリシーの登録	ポリシー識別子	1
	SAライフタイム	デフォルトを使用する (28800秒)
	鍵データ（PFS）の再生成	再生成しない
	暗号化アルゴリズム	DES
	認証アルゴリズム	HMAC-MD5
VPN対象パケットの登録1	id	1
	宛先指定	158.XXX.0.2 255.255.255.255
	宛先ポート指定	全てのポート
	送信元指定	192.168.0.0 255.255.255.0
	送信元ポート指定	全てのポート
	プロトコル指定	全て
	宛先インタフェース	ISDN#1
	IPsec処理タイプ	IPsec処理して中継
	SA確立契機	起動時確立しない データ通信時
	登録済みVPNピア指定	158.XXX.0.1
	ポリシー識別子による登録済み暗号化ポリシーの指定	1

〈次ページへ続く〉

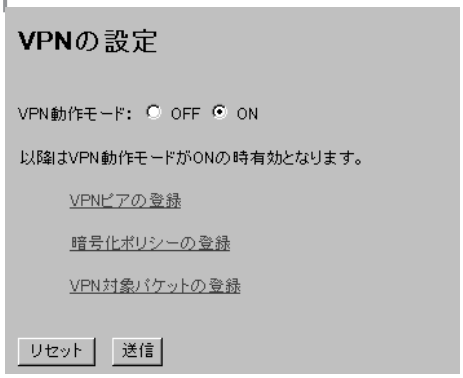
画面名	設定項目	設定例
VPN対象パケットの登録2	id	32
	宛先指定	全て
	宛先ポート指定	全てのポート
	送信元指定	全て
	送信元ポート指定	全てのポート
	プロトコル指定	全て
	宛先インタフェース	ISDN#1
	IPsec処理タイプ	IPsec処理しないで中継

＜Webブラウザ操作＞

1 **ルータの［便利な設定］をクリックします。**

2 **［VPNの設定］をクリックします。**

3 **VPN動作モードの［ON］をクリックします。**



設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

4 **［VPNピアの登録］をクリックします。**

〈次ページへ続く〉

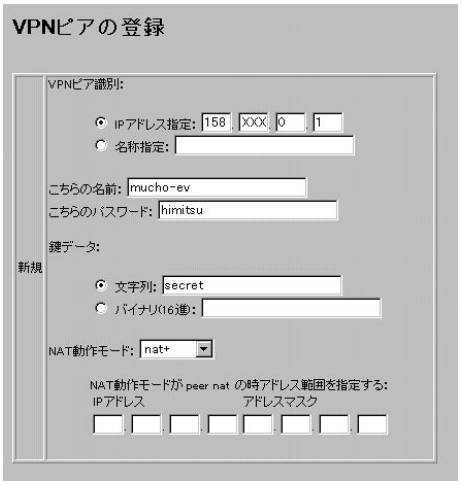
お知らせ

手順1のあとに、ユーザIDとパスワードの入力画面が表示されることがあります。
ユーザIDとパスワードを入力してください。（☛P37）

具体的な設定方法

5 VPNピア識別と鍵データを設定します。

［新規登録］をクリックします。
VPN識別のIPアドレスや鍵データを下記のように入力します。



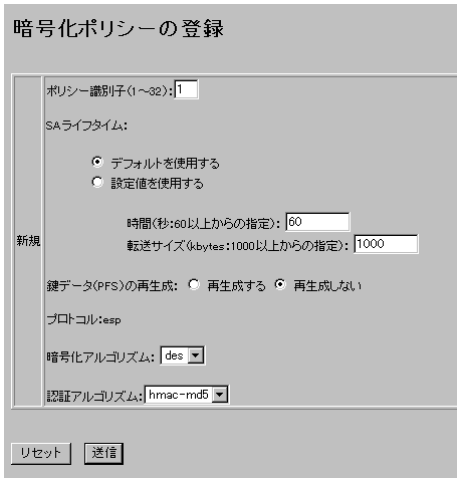
設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。［OK］をクリックします。

6 ブラウザの［戻る］ボタンをクリックします。

7 ［暗号化ポリシーの登録］をクリックします。

8 暗号化ポリシーを設定します。

［新規登録］をクリックします。
ポリシー識別子や暗号化・認証アルゴリズムを下記のように入力します。



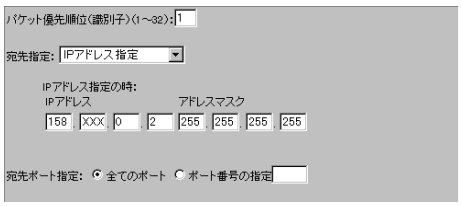
設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

9 ブラウザの［戻る］ボタンをクリックします。

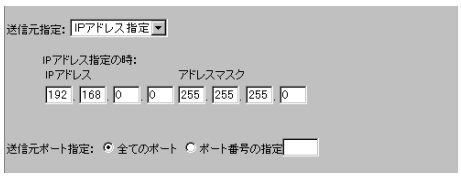
10 ［VPN対象パケットの登録］をクリックします。

11 1件目のVPN対象パケットの登録をします。

［新規登録］をクリックします。
パケット優先順位・宛先指定などを下記のように入力します。

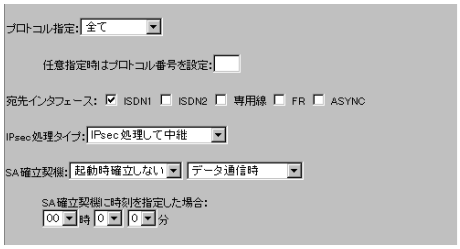


12 送信元に関する情報を設定します。



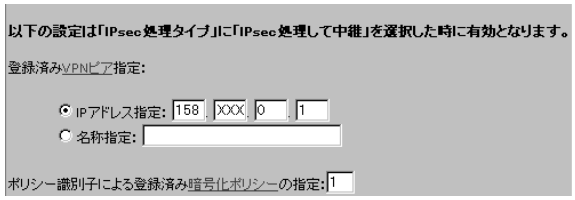
13 プロトコルや宛先インタフェースを設定します。

プロトコル指定・宛先インタフェース・IPsec処理タイプ・SA確立契機を下記のように入力します。



14 登録済みVPNピア指定・暗号化ポリシーの指定をします。

IPアドレスなどを下記のように入力します。



設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。［OK］をクリックします。

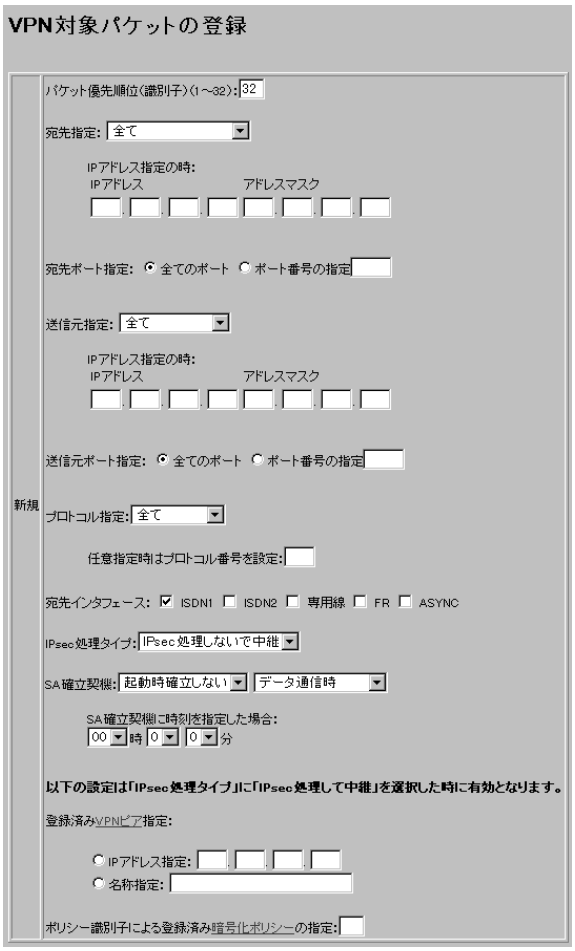
〈次ページへ続く〉

具体的な設定方法

15 ブラウザの［戻る］ボタンをクリックします。

16 2件目のVPN対象パケットの登録をします。

［新規登録］をクリックします。
下記のように入力します。



設定が終わったら、［送信］をクリックします。設定内容が本装置に送信され、確認画面が表示されます。
［OK］をクリックします。

17 設定内容を有効にするには、MUCHO-EVのリセットが必要です。［リセット］をクリックします。

「リセット」画面が表示されます。

18 ［装置をリセットする］をクリックします。

本装置が再起動し、設定内容が有効になります。

＜コマンド操作＞

1 コンフィグレーションモードに移行します。(☛P39)

```
#conf
Configuration password:
conf#
```

2 VPN使用の設定（vpnコマンド）

「VPN動作モードをON」を設定するため「vpn on」を入力します。

```
conf#vpn on
```

3 VPNピアの登録（vpnpeerコマンド）

「IPアドレス指定(158.YYY.0.1)」、「鍵データ(a,secret)」、「NAT(natp)」を「vpnpeer」コマンドで入力します。

```
conf#vpnpeer add addr=158.YYY.0.1 key=a,secret nat=natp
```

4 暗号化ポリシーの登録（vpnpolicyコマンド）

「ポリシー識別子(1)」を「vpnpolicy」コマンドで入力します。

```
conf#vpnpolicy add id=1
```

5 VPN対象パケットの登録（vpnselectorコマンド）

VPNselectorコマンドで以下の2つのエントリを追加します。
①「セレクタID(1)」、「宛先指定(158.XXX.0.2,255.255.255.255)」、「送信元指定(192.168.0.0,255.255.255.0)」、「IPsec処理タイプ(ipsec)」「VPNピア(158.YYY.0.1)」、「ポリシー識別子（1)」
②「セレクタID（32)」、「宛先指定（全て)」、「送信元指定（全て)」、「IPsec処理タイプ（bypass)」

```
conf#vpnselector add id=1 dst=158.XXX.0.2,255.255.255.255
src=192.168.0.0,255.255.255.0
type=ipsec peeraddr=158.YYY.0.1 policy=1
conf#vpnselector add id=32 dst=all src=all type=bypass
```

6 設定を保存します。(☛P42)

```
conf#exit
Configuration modified. save ok?(y/n):y
please reset#
Do you want to continue(y/n)?:y
```

VPNの便利な設定

VPNの設定

VPNを使用するときは、この画面でVPN動作モードをONにし、VPNピア・暗号化ポリシー・VPN対象パケットをそれぞれの設定画面で登録します。

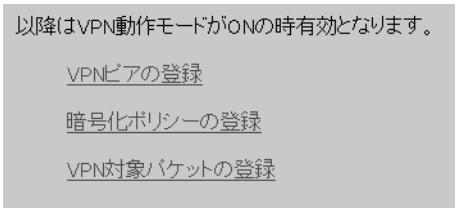
1 ルータの[便利な設定]をクリックします。

2 [VPNの設定] をクリックします。

3 VPN機能を使うときは、[ON] をクリックします。

4 VPNを設定します。

VPNピアの登録（☛P297）
暗号化ポリシーの登録（☛P299）
VPN対象パケットの登録（☛P301）



5 VPNの設定が終わったら、[送信] をクリックします。

設定内容が本装置に送信され、確認画面が表示されます。

6 [OK] をクリックします。

設定内容を有効にするには、本装置のリセットが必要です。（☛P39）

VPNピアの登録

VPNを使用して通信する接続相手のルータ(SG)と本装置の両方のルータに関する情報を登録します。登録したVPNピアと鍵交換する際のpre-shared keyも設定します。16件まで設定できます。

1 VPNの設定画面（☛P296）で、［VPNピアの登録］をクリックします。

2 VPNピアを追加またはレコードを選択します。

新規または追加でVPNピアを登録するときは、［新規登録］をクリックします。

3 VPNピア識別を設定します。

- **［VPNピア識別］**
  通信相手を識別するIPアドレスまたは名称を入力します。相手が専用線などでIPアドレスがわかっている場合は、IPアドレスを指定します。相手がダイヤルアップなどでIPアドレスが確定しない場合は、名称を指定します。
  名称は64文字以内で指定してください。

4 本装置側の識別データを設定します。

本装置がダイヤルアップ接続などIPが可変のときやFortKnoxとVPN接続する場合には、下記の項目の入力が必要です。

- **［こちらの名前］**
  本装置の名前を入力します。接続相手がMUCHOの場合は、接続相手の「VPNピア識別の名称指定」設定と同じである必要があります。接続相手がFortKnoxの場合は、FortKnoxに登録してあるユーザIDを設定します。どちらの場合も64文字以内で入力してください。
- **［こちらのパスワード］**
  本装置のパスワードを入力します。接続相手がFortKnoxの場合は、FortKnoxに登録してあるパスワードを設定します。64文字以内で入力してください。

〈次ページへ続く〉

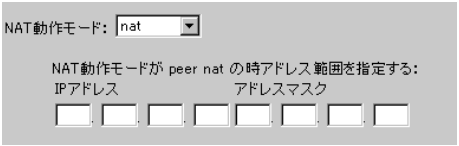
VPNの便利な設定

5 鍵データを設定します。

登録するVPNと鍵交換する際に使用する鍵データ(pre-shared key)を入力します。この設定は接続相手と同じである必要があります。Ascii文字列またはバイナリ(16進数)のどちらかで設定できます。[文字列]または[バイナリ]のどちらかをクリックし、鍵データ(pre-shared key)を入力してください。

- **[文字列]**
  Ascii文字64文字以内で入力してください。
- **[バイナリ(16進数)]**
  64bytes以内で入力してください。

6 NAT動作モードを設定します。



- **[NAT動作モード]**
  NATの動作モードを選択します。本装置のNAT機能を使用しているときに、ここでの選択が有効になります。

動作モード	説明
nat	NAT装置モード。NATモードと変換アドレスは、本装置のNATの設定にしたがいます。
off	NAT動作モードを使用しません。
peer nat	設定したIPアドレスとアドレスマスクでアドレス交換を行います。
nat+	NAT+の変換を行います。

- **[IPアドレス]**
  NAT動作モードで「peer nat」を選択した場合に、NATの変換アドレスを入力します。
- **[アドレスマスク]**
  NAT動作モードで「peer nat」を選択した場合に、NATの変換アドレスマスクを入力します。

7 [送信] をクリックします。

設定内容が本装置に送信され、確認画面が表示されます。

8 [OK] をクリックします。

設定内容を有効にするには、本装置のリセットが必要です。(☛P39)

ワンポイント

登録済みのVPNピアを修正するときは
手順2で、修正するレコード番号をクリックしてください。レコード内容が表示されたら、内容を修正します。以降の操作は新規登録時と同じ操作です。

暗号化ポリシーの登録

VPNをどのような条件で動作させるかを登録します。暗号化アルゴリズム・認証アルゴリズムなどを設定します。

1 VPNの設定画面（☞P296）で、［暗号化ポリシーの登録］をクリックします。

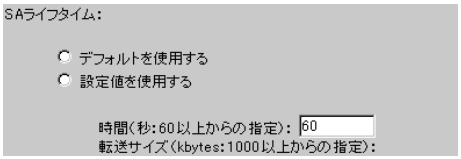
2 暗号化ポリシーを追加またはレコードを選択します。

新規または追加で暗号化ポリシーを登録するときは、［新規登録］をクリックします。

3 ポリシー識別子を設定します。

- **［ポリシー識別子］**
  ポリシー識別子を1～32の間で入力します。

4 SAライフタイムを設定します。

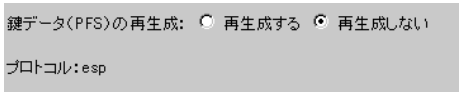


- **［デフォルトを使用する］**
  デフォルト設定値のSAライフタイムを使用するときに選択します。デフォルト設定値は次の通りです。
  ・時間：28800秒（8時間）
- **［設定値を使用する］**
  SAライフタイムを任意の時間に設定するときに選択します。ここを選択した場合は、SAライフタイムの時間または転送サイズを設定してください。どちらも0の場合は、28800秒（8時間）で動作します。
- **［時間］**
  IPsecSAの生存時間を設定します。IPsecSA確立後、ここに設定した時間を経過した場合、IPsecSAを確立し直します。秒を単位として、60以上で入力してください。
- **［転送サイズ］**
  IPsecSAの累積転送サイズを設定します。IPsecSA確立後、ここに設定した累積転送サイズの中継を行った場合に、IPsecSAを確立し直します。Kbytesを単位として、1000以上で入力してください。

〈次ページへ続く〉

VPNの便利な設定

5 鍵データ(PFS)を再生成するかどうかを設定します。



6 暗号化アルゴリズム・認証アルゴリズムを設定します。

暗号化アルゴリズム・認証アルゴリズムの両方ともnullのときは、エントリは無効になります。

- **[暗号化アルゴリズム]**
  - ・DES：DESで暗号化します。
  - ・null：暗号化しません。
- **[認証アルゴリズム]**
  - ・hmac-md5：HMAC-MD5で認証します。
  - ・hmac-sha：HMAC-SHA-1で認証します。
  - ・null：認証しません。

7 [送信] をクリックします。

設定内容が本装置に送信され、確認画面が表示されます。

8 [OK] をクリックします。

設定内容を有効にするには、本装置のリセットが必要です。(☛P39)

ワンポイント

登録済みの暗号化ポリシーを修正するときは

手順2で、修正するレコード番号をクリックしてください。レコード内容が表示されたら、内容を修正します。以降の操作は新規登録時と同じ操作です。

VPN対象パケットの登録

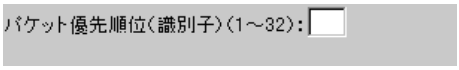
どのようなパケットに対してVPN制御を行うかを登録します。登録した情報に一致したパケットをVPNで暗号化し、VPN通信を行います。

1 VPNの設定画面（☛P296）で、［VPN対象パケットの登録］をクリックします。

2 VPN対象パケットを追加またはレコードを選択します。

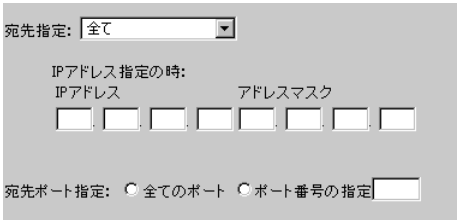
新規または追加でVPN対象パケットを登録するときは、［新規登録］をクリックします。

3 パケット優先順位を設定します。



- **［パケット優先順位］**
  1～32の範囲で入力してください。数値が小さいほど、優先順位が高くなります。

4 宛先に関する情報を設定します。

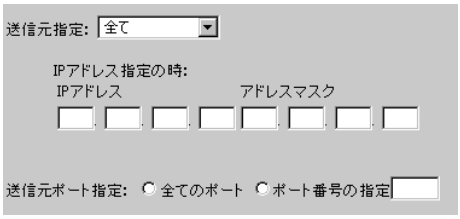


- **［宛先指定］**
  どのような宛先のパケットを対象とするかを選択します。
  - ・ 全て：全ての宛先のパケットを対象とします。
  - ・ 宛先がVPNピアのとき：宛先がVPNピアのパケットを対象とします。
  - ・ IPアドレス指定：指定したIPアドレス宛のパケットを対象とします。IPアドレスとアドレスマスクを入力してください。
- **［IPアドレス］［アドレスマスク］**
  ［宛先指定］でIPアドレス指定を選択したときに、宛先のIPアドレスとアドレスマスクを入力します。
- **［宛先ポート指定］**
  全ての宛先ポートを対象とするのか、あるいはポート番号を指定するのかを選択します。ポート番号を指定するときは、1～65535の範囲で入力してください。

〈次ページへ続く〉

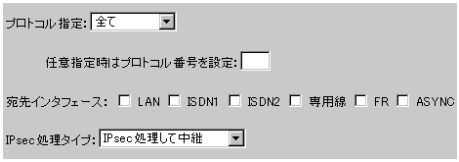
VPNの便利な設定

5 送信元に関する情報を設定します。



- **[送信元指定]**
  どのような送信元のパケットを対象とするかを選択します。
  - ・ 全て：全ての送信元のパケットを対象とします。
  - ・ IPアドレス指定：指定したIPアドレスからのパケットを対象とします。IPアドレスとアドレスマスクを入力してください。
- **[IPアドレス] [アドレスマスク]**
  [送信元指定] でIPアドレス指定を選択したときに、送信元のIPアドレスとアドレスマスクを入力します。
- **[送信元ポート指定]**
  全てのポートからのパケットを対象とするのか、あるいはポート番号を指定するのかを選択します。ポート番号を指定するときは、1～65535の範囲で入力してください。

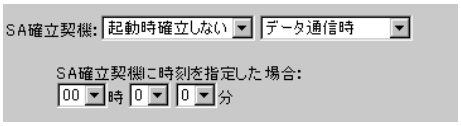
6 プロトコル・宛先インタフェース・IPsec処理タイプを設定します。



- **[プロトコル指定]**
  プロトコルを選択します。任意の指定を選択したときは、[任意指定時はプロトコル番号を設定]にIPプロトコルを、0～255の範囲で入力してください。
- **[宛先インタフェース]**
  宛先インタフェースを選択します。複数選択ができます。
- **[IPsec処理タイプ]**
  - ・ IPsec処理して中継：VPNを使用してパケットを通します。
  - ・ IPsec処理しないで中継：VPNを使わずにパケットを通します（バイパス）。
  - ・ 廃棄：セレクタに登録したエントリのパケットを「破棄」するという意味です。例えば、192.168.100.1宛に対してVPNの通信はするが、telnetは中継したくないような場合には、dst=192.168.100.1 protocol=all IPsectype=IPsec dst=all protocol=telnet IPsectype=discard のように登録します。

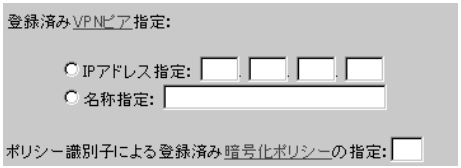
7 SA確立契機を設定します。

まず起動時にSAを確立するかどうかを選択し、次に確立タイプを選択します。



- **［SA確立契機］（起動時SA確立）**
  起動時にSAを確立するかどうかを選択します。
- **［SA確立契機］（SA確立タイプ）**
  - ・ データ通信時：トラフィックによりSAを確立します。
  - ・ ライフタイム満了時：トラフィックがなくてもSAを常時確立し続けます。
  - ・ 指定時刻時：トラフィックがなくても、指定した時刻にSAを確立します。指定時刻時を選択したときは、［SA確立契機に時刻を指定した場合］に、時刻を設定してください。
- **［SA確立契機に時刻を指定した場合］**
  ［SA確立契機］（SA確立タイプ）で、指定時刻を選択したとき、SAを確立する時刻を設定します。

8 登録済みVPNピアと登録済み暗号化ポリシーを設定します。



- **［登録済みVPNピア指定］**
  設定しているVPN対象パケットをどのVPNピアと結びつけるか設定します。通信相手を識別するIPアドレスまたは名称を入力します。
- **［ポリシー識別子による登録済み暗号化ポリシーの指定］**
  設定しているVPN対象パケットをどの暗号化ポリシーと結び付けたらよいかを、ポリシー識別子により設定します。ポリシー識別子を入力してください。

9 ［送信］をクリックします。

設定内容が本装置に送信され、確認画面が表示されます。

10 ［OK］をクリックします。

設定内容を有効にするには、本装置のリセットが必要です。(☛P39)

ワンポイント

●登録済みのVPN対象パケットを修正するときは

手順2で、修正するレコード番号をクリックしてください。レコード内容が表示されたら、内容を修正します。以降の操作は新規登録時と同じ操作です。

●VPNピアの登録方法（☛P297）

VPN SAの状態を表示するには（vpnsainfoコマンド）

IKE SAとIPsec SAの状態を表示することができます。

＜Webブラウザ操作＞

1 ［インフォメーション］をクリックします。

［インフォメーション］画面が表示されます。

2 ［VPN SAの状態表示］をクリックします。

IKE SAとIPsec SAの状態が表示されます。

VPN SA の状態表示

```
IKE SA
[1]     xxx.xxx.xxx.xxx 相手名前
                <--> xxx.xxx.xxx.xxx 自身名前
         Aggressive Mode     XAUTH   pre-shared key  DES     MD5
        Lifetime:86400secs              Now:0secs
[2]     xxx.xxx.xxx.xxx
                <--> xxx.xxx.xxx.xxx
        Main Mode   UP      pre-shared key  DES     SHA
        Lifetime:172800secs,4000000kbytes       Now:123456secs,123456kbytes

IPSEC SA
[1]     xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx 0 0              --- 宛先
                <--> xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx 0 0        --- 送信元
        peer:xxx.xxx.xxx.xxx 相手名前
         UP  ESP  DES  HMAC-MD5 PFS:off  Lifetime:28800secs
        O-SPI:12345     Now:1234secs
          out packet      :123          error packet          :0
        I-SPI:67890     Now:1234secs
          in packet       :89           auth packet           :89
          decrypt packet  :89           discard packet        :0
          replay packet   :0            auth error packet     :0
[2]     xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx TCP 100
                <--> xxx.xxx.xxx.xxx,xxx.xxx.xxx.xxx TCP 0
        peer:xxx.xxx.xxx.xxx 相手名前
         UP  ESP  DES  HMAC-SHA  PFS:on  Lifetime:86400secs,2000000kbytes
        O-SPI:1357      Now:3333secs,3456kbytes
          out packet      :34           error packet          :0
        I-SPI:67893     Now:3333secs,1234567kbytes
          in packet       :12345        auth packet           :12345
          decrypt packet  :12345        discard packet        :0
          replay packet   :0            auth error packet     :0
```

● VPN SAの状態画面のみかた

- IKE SA（ISAKMP SA）状態情報
  確立しているIKE SAエントリの情報です。
  - ・ID
  - ・相手ピア（IP address、name）
  - ・自身（IP address、name）
  - ・交換モード(Main Mode / Aggressive Mode)
  - ・state（XAUTH(拡張認証中) / UP）
  - ・I/R（Initiator/Responder）
  - ・認証方法（pre-shared key）
  - ・暗号アルゴリズム（DES）
  - ・ハッシュアルゴリズム（MD5 / SHA）
  - ・Lifetime（秒、Kbytes）
  - ・現在時間、現在Kbytes数
- IPsec SA状態情報
  確立しているIPsec SAエントリの情報です。
  - ・ID
  - ・送信元アドレス、マスク、プロトコル、ポート番号
  - ・宛先アドレス、マスク、プロトコル、ポート番号
  - ・ピア（IP address、名前）
  - ・I/R（Initiator/Responder）
  - ・state（UP）
  - ・プロトコル（ESP）
  - ・I-SPI, O-SPI
  - ・PFS on/off
  - ・ESP暗号アルゴリズム（DES）
  - ・ESP認証アルゴリズム（HMAC-MD5 / HMAC-SHA）
  - ・Lifetime（秒、Kbytes）

<Outbound>
・現在時間、現在Kbytes数
・送信パケット数
・送信エラー数（mbuf不足、Sequence Numberオーバフロー等）

<Inbound>
・現在時間、現在Kbytes数
・受信パケット数
・認証チェックしたパケット数
・復号処理したパケット数
・廃棄パケット数（リプレイアタックエラー＋認証チェックエラー＋その他（policy error等））
・リプレイアタックエラー数
・認証チェックエラー数

＜コマンド操作＞

1 「vpnsainfo」と入力します。

IKE SA、IPsec SA個別の状態を表示するには、「vpnsainfo」のあとに以下のオプションをつけてください。

オプション	表示種別
ike	IKE SA
ipsec	IPsec SA
省略	IPsec SA

（例）IKE SAの状態を表示する。

```
#vpnsainfo ike
```

2 VPN SAの状態を表示します。

（表示例）

```
#vpnsainfo ike
IKE SA
[ 2] xxx.xxx.xxx.xx
        <--> yyy.yyy.yyy.yyy
    <I> Main Mode       UP    pre-shared key  DES   MD5
    Lifetime:86400secs
    Current:5668secs,2kbytes
#
#vpnsainfo
IPSEC SA
[ 3] xxx.xxx.xxx.xxx,255.255.255.0    ALL ALL
           <--> yyy.yyy.yyy.yyy,255.255.255.0     ALL ALL
    peer:192.168.132.32
    <I> UP ESP DES HMAC-MD5 PFS:off
    Lifetime:                  600secs
    O-SPI:0xf710666c      Current:4secs,1kbytes
     out packet    :1        error packet     :0
    I-SPI:0x8c3751bb      Current:4secs,1kbytes
     in packet     :1       auth packet      :1
     decrypt packet :1        discard packet   :0
     replay packet  :0        auth error packet :0
```

3 コマンド入力待ち状態になります。

```
#
```

VPNログを表示するには（vpnlogコマンド）

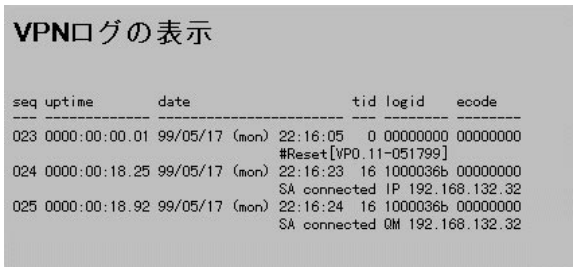
VPNに関するログ情報を参照することができます。

- **通し番号**
- **ロギング時刻**
- **タスクID**
- **ログID**
- **エラーコード**
- **ログメッセージ**

<Webブラウザ操作>

1 ［インフォメーション］画面で、［VPNログの表示］をクリックします。

VPNのログ情報が表示されます。ブラウザで再読み込み操作を行うと，最新の状態が表示されます。



<コマンド操作>

1 「vpnlog」と入力します。

```
#vpnlog
```

2 VPNに関するログが以下のように表示されます。

```
#vpnlog
seq  uptime         date                        tid logid     ecode
--- ------------- ----------------------- --- -------- --------
023 0000:00:00.01 99/05/17 (mon) 22:16:05   0 00000000 00000000
                                #Reset[V01.00-051799]
024 0000:00:18.25 99/05/17 (mon) 22:16:23  16 1000036b 00000000
                                SA connected IP 192.168.132.32
025 0000:00:18.92 99/05/17 (mon) 22:16:24  16 1000036b 00000000
                                SA connected QM 192.168.132.32
```

3 コマンド入力待ち状態になります。

VPNの通信手順と用語

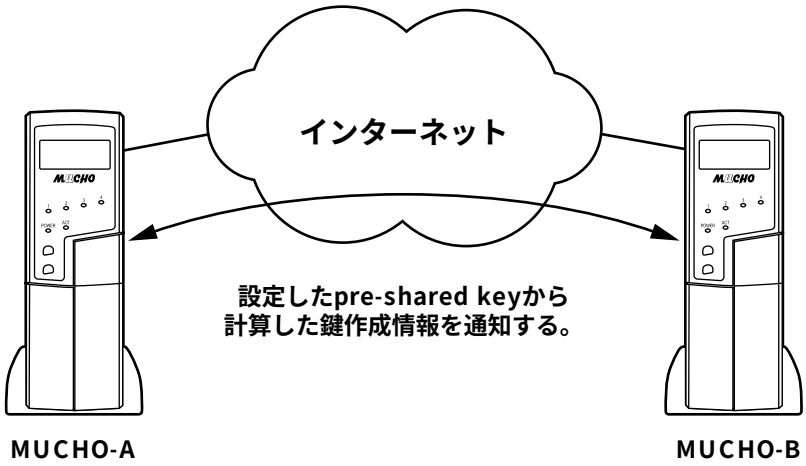
参考資料として、VPNの通信手順の説明と用語集を記載します。

VPNの通信手順

IKE（Internet Key Exchange）プロトコルにより、暗号化および認証用の鍵交換を自動的に行い、VPNの通信を行う手順について説明します。

①IKE SAの確立

設定した鍵データ（pre-shared key）から計算した鍵作成情報をお互いに通知します。設定する鍵データは、VPNを確立するルータ同士（MUCHO-AとMUCHO-B）で同じでなくてはいけません。鍵作成情報が正しい場合（すなわちpre-shared keyが正しい場合）にVPN通信を開始することができます（IKE SA確立）。IKE SAを確立した際は、鍵作成情報から鍵を作成します。複数の相手とVPN接続する場合には、相手ごとの鍵が作成されます。IKE SAは、確立されてから1日間利用され、その後通信があれば更新されます。



②IPsec SAの確立

設定したVPN対象パケットに一致するパケットをLANから受信した場合、VPN対象パケットで設定してある相手に対して、IPsec SAを確立するためのネゴシエーションを開始します。IPsec SAのためのネゴシエーションには、①で作成された鍵を使用します。IPsec SA通信では、指定したポリシーで提案します。指定したポリシーでネゴシエーションが拒否された場合、通信はできません。IPsec SAを確立した際は、確立したIPsec SAを使用して通信する際の中継データを暗号化・認証するために使用する鍵が作成されます。
IPsec SAは、設定したLifetime間後に消滅します。消滅したあとにデータ通信があれば再度、鍵交換のネゴシエーションを行います。

③暗号化

設定したVPN対象パケットに一致するパケットをLANから受信した場合、そのデータを暗号化します。暗号化はIPsec SAで確立したポリシーにしたがい、②で作成した鍵を使用します。データを暗号化することにより、盗聴されても判別できなくなります。データを復号する際も、②で作成した鍵を使用して復号します。

VPNの通信手順と用語

用語集

AH(Authentication Header)
旧IPsecでは認証にはAHが必要だったが、新仕様（RFC2406）からESPで認証が可能となり効率がよくなった。MUCHO-EVではサポートしていない。

DES-CBS
暗号化アルゴリズムの1つ。

Diffie-Hellman
共通鍵交換方式で、第三者に盗聴されることなく鍵交換を行うしくみ。ISAKMPで鍵交換を行う際に使用している。

ESP(Encapsulation Security Payload)
IPsecで規定されている認証・暗号のパケット方式。MUCHO-EVでは、暗号アルゴリズムとしてDES-CBC 56bit・NULL Encryption（暗号化しない）、ハッシュアルゴリズムとしてHMAC with MD5・HMAC with SHAをサポートしている（RFC2406）。

HMAC-MD5
認証アルゴリズムの一つ。

HMAC-SHA
認証アルゴリズムの一つ。

IKE（Internet Key Exchange）
自動鍵管理プロトコル（RFC2409）。通信相手とのネゴシエーションにより自動で鍵を交換しSAを確立する方式。

Initiator
VPNネゴシエーションを行う側を指す。

IPsec
インターネットで暗号通信を行うための規格。

ISAKMP（Internet Security Association and Key Management Protocol）
IKEを実現するためのプロトコル。ISAKMPで、「暗号アルゴリズム（DES-CBC）」、「ハッシュアルゴリズム（MD5 or SHA-1）」、「認証方法（pre-shared keys）」、「Oakley Group description（Default 768-bit MODP group(group1)）」、「鍵Lifetime秒」「鍵Lifetimeバイト長」の交換を行う。これらの情報をまとめて「ポリシー」という（RFC2408）。

Pre-Shared Key
自動鍵管理プロトコルでの鍵交換を行う際の、認証方法の一つ。共通鍵方式の暗号および認証鍵を生成する元データとしても利用する。

Responder
VPNネゴシエーションを受ける側を指す。

SA(Security Association)
VPN通信するための相手と確立する論理的なコネクション。SAには、暗号アルゴリズム・認証アルゴリズム等のセキュリティ情報を含んでいる。

SG(Security GateWay)
VPNのコネクションを確立する通信相手ルータ。（MUCHO-EVではVPNピアと表現します。）