アクセスルータ

IPsec 機能について

FITELnet-E30

古河電工

目次

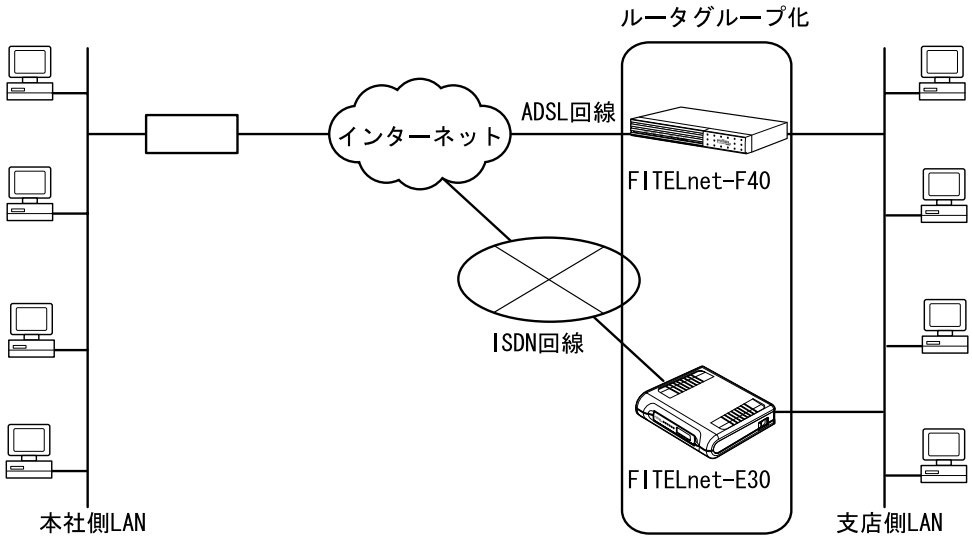
機能概要

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。FITELnet-E30は、
VPNの中の、IPsec（IP Security）をサポートしています。

FITELnet-E30 での、前提条件

FITELnet-E30で、IPsecを使用できる条件として、以下の条件があります。

・FITELnete-F40の冗長機能のバックアップ装置として使用すること



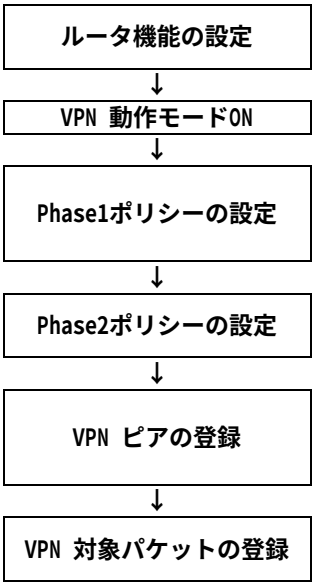
FITELnet-E30のみを使用した、インターネットVPNは、サポートしていません。

本書の構成

IPsecの設定方法	P5に進んでください。 ・VPN動作の設定 ・Phase1ポリシーの設定 ・Phase2ポリシーの設定 ・VPN ピアの登録 ・VPN 対象パケットの登録 ・VPNログモードの設定
IPsecの情報表示	P28に進んでください。 ・VPN SAの状態を表示する ・VPNのログ情報を表示する
設定例	P37に進んでください。
IPsecに関する用語集	P41に進んでください。
IPsecの基本動作	P43に進んでください。

設定の流れ

■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。



通常のルーティング機能の設定を行います。こちらの設定方法は、取扱説明書を参照してください。

VPN を使用するには、VPN 動作モードをON にします。

Phase1をどのような条件で動作させるかを登録します
拡張認証するかどうか／暗号化アルゴリズム／ハッシュアルゴリズムなどを設定します。

IPsec のネゴシエーションで使用するPhase2 ポリシーを設定します。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。

VPN を使用して通信する接続相手のルータ(VPN ピア)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。

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。

［オプション設定］

VPNログにSA確立の情報を載せるかどうかを設定します。（P27）

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。

VPN を使用するときは、VPN 動作モードをON にし、VPN ピア、Phase1 ポリシー、Phase2 ポリシー、VPN 対象パケットを設定します。

＜VPN 動作モード＞

分類	画面名	設定項目	入力値
便利な設定	VPN の設定	VPN 動作モード	ON

＜Phase1 ポリシーの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPN の設定	ポリシー識別子	1
		Phase1 方式	Pre- shared key （拡張認証なし）
		暗号化アルゴリズム	des
		ハッシュアルゴリズム	md5

＜Phase2 ポリシーの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPN の設定	ポリシー識別子	1
		SA ライフタイム	600 秒 1000kbytes
		鍵データの再生成	しない
		暗号化アルゴリズム	des
		認証アルゴリズム	HMAC-MD5

＜VPN ピアの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPN の設定	VPN ピア識別 相手IPアドレス指定 相手名称指定 こちらの名前	 158.xxx.xxx.1 空欄 FITELnet-E30
		FQDNタイプ	UserFQDN
		拡張認証	相手を認証しない
		鍵データ	「文字列」にチェック secret-vpn
		Phase1 IKEモード	アドレスが固定で設定されている場合はMainMode
		KeepAlive	on
		NAT動作モード	off
		Phase1ポリシー識別子	1

＜VPN 対象パケットの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPN の設定	優先度	1
		送信元指定	IPアドレス指定:192.168.0.0/24 全てのポート番号
		宛先指定	IPアドレス指定：158.xxx.xxx.0/24 全てのポート番号
		インタフェース	ISDN1
		プロトコル	全て
		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、回線が確立しても SA確立処理を行わない ・リトライしない
		VPNピア	158.xxx.xxx.1
		Phase2ポリシー	1

・双方とも拡張認証はしない例です。

・VPN対象パケット以外はインターネット接続するような形態の場合は、<VPN対象パケット>の設定で以下のエントリを追加します。

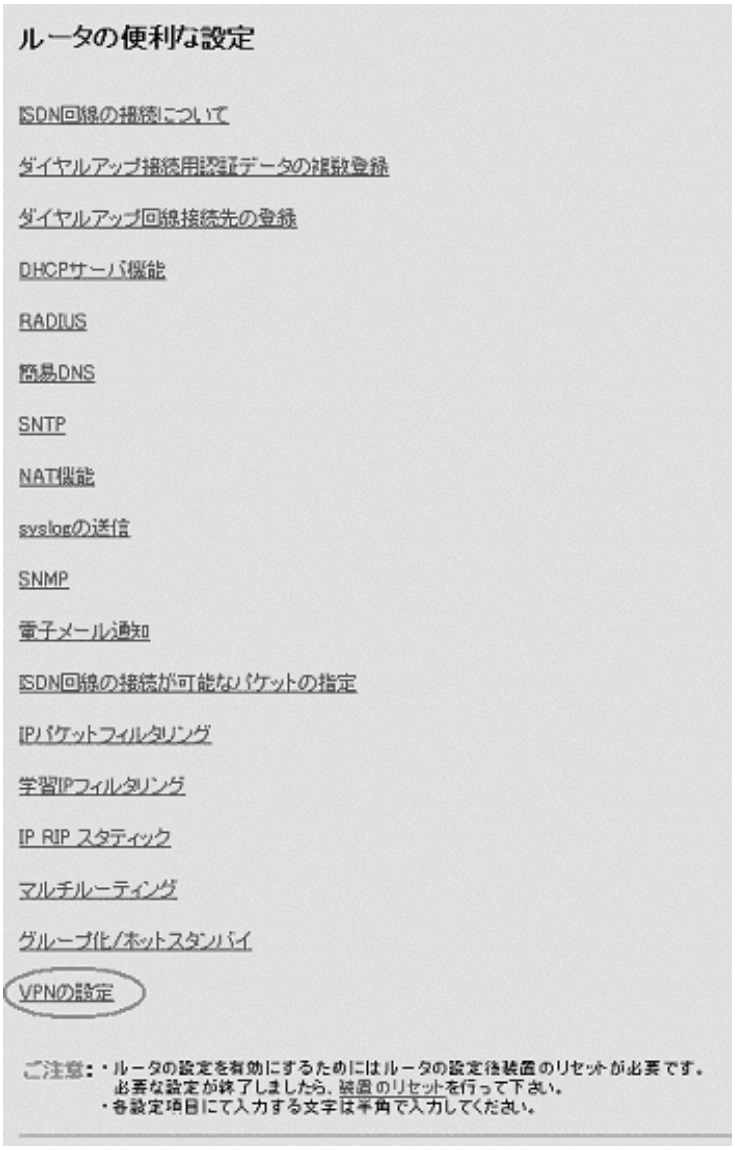
便利な設定	VPN の設定	優先度	32
		送信元指定	全て（ホスト1）
		宛先指定	全て（ホスト1）
		プロトコル	全て
		インタフェース	全て
		IPsec処理タイプ	IPsec処理しないで中継
		SA確立契機	・起動時確立しない ・データ通信時、回線が確立しても SA確立処理を行わない ・リトライしない
		VPNピア	158.xxx.xxx.1
		Phase2ポリシー	1

VPN 動作モード

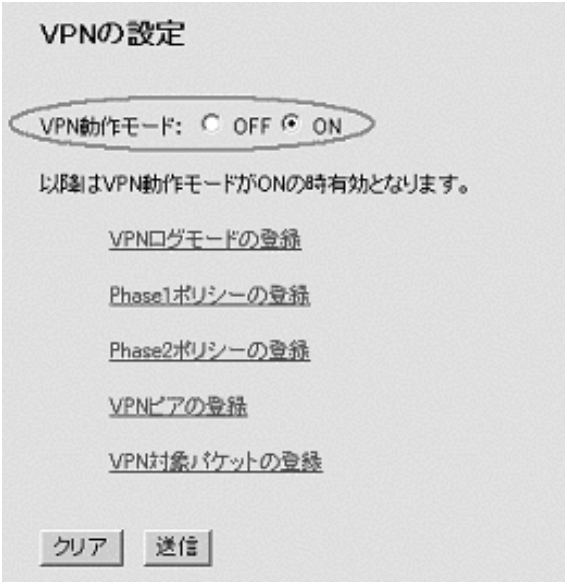
VPN を使用するときは、この画面で VPN 動作モードを ON にし、Phase1,Phase2 ポリシー・VPN ピア・VPN 対象パケットをそれぞれの設定画面で登録します。

1 **画面左側のメニューから【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］を選択して、［送信］をクリックします。



4 VPN を設定します。

- Phase1 ポリシーの登録（P10）
- Phase2 ポリシーの登録（P12）
- VPN ピアの登録（P15）
- VPN 対象パケットの登録（P21）

Phase1 ポリシーの登録

Phase1 をどのような条件で動作させるかを登録します。

拡張認証する/しない、暗号化アルゴリズム、ハッシュアルゴリズムなどを設定します。

1 **VPNの設定画面で、[Phase1ポリシーの登録]をクリックします。**

2 **ポリシー識別子を設定します。**

[1]を入力します。

- **[ポリシー識別子]**

  ポリシー識別子を1 ～16 の間で入力します。

3 **Phase1方式を設定します。**

Pre-shared key（共通鍵方式）で拡張認証を行わない場合は、

［Pre-shared Key（拡張認証なし）］を選択します。

- **[Phase1方式]**

  Pre-shared key（共通鍵方式）で拡張認証するかどうかを選択します。

ワンポイント

● **登録済みのPhase1ポリシーを削除するときは**

手順2で、削除するレコードのチェックボックスをチェックして、［送信］をクリックします。

4 暗号化アルゴリズム・DiffieHellman で使用するOakley Group ・ハッシュアルゴリズムを設定します。

暗号化アルゴリズム［des］、Oakley Group ［group1］、ハッシュアルゴリズム［md5］を選択します。

- **［暗号化アルゴリズム］**
  - ・des：desで暗号化します。
  - ・3des：3desで暗号化します。
- **［DiffieHellman で使用するOakley Group］**

・group1 （768bitMODP ）

  - ・group2 （1024bitMODP ）
- **［ハッシュアルゴリズム］**
  - ・md5：md5でハッシュします。
  - ・SHA：shaでハッシュします。

5 ［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。

Phase2 ポリシーの登録に進みます。

Phase2 ポリシーの登録

IPsec のネゴシエーションで使用する Phase2 ポリシーを設定します。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の設定画面で、[Phase2ポリシーの登録]をクリックします。

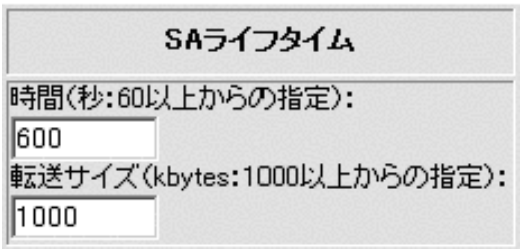
2 ポリシー識別子を設定します。

[1]を入力します。

- **[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。

3 SA ライフタイムを設定します。

時間［600］秒、転送サイズ［1000］kbytesを入力します。



- **[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、SA を開放し、再度SA を確立する必要があるときは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。

ワンポイント

● **登録済みのPhase2ポリシーを削除するときは**
手順2で、削除するレコードのチェックボックスをチェックして、［送信］をクリックします。

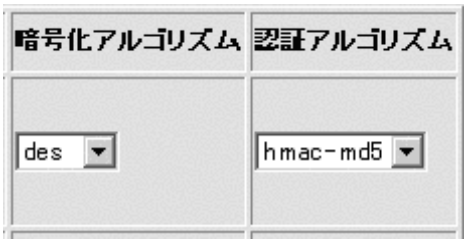
4 鍵データ(PFS)を再生成するかどうか、PFS で使用するOakley Groupを設定します。

鍵データ（PFS）の再生成［しない］、PFS で使用するOakleyGroup［group1］をチェックします。

- **［PFSで使用するOakley Group］**
  - ・group1 （768bitMODP ）
  - ・group2 （1024bitMODP ）

5 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［des］、認証アルゴリズム［hmac-md5］を選択します。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。
  - ・3des：3des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。

6 **［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。

VPNピアの登録に進みます。

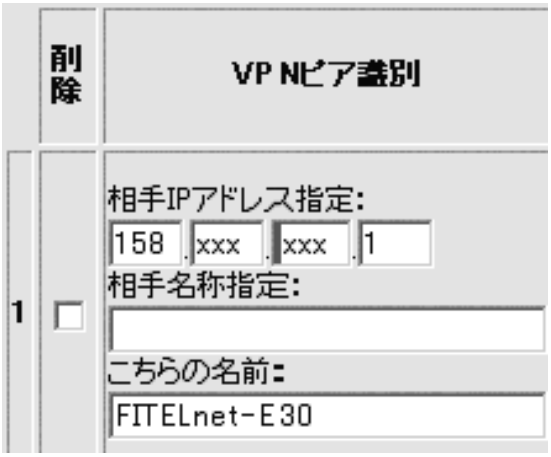
VPNピアの登録

VPN を使用して通信する接続相手のルータ(VPN ピア)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。32 件まで設定できます。

1 VPNの設定画面で、[VPNピアの登録]をクリックします。

2 VPNピア識別を設定します。

相手IPアドレス指定［158.xxx.xxx.1 ］、こちらの名前［FITELnet-E30］と入力します。



- **［相手IPアドレス指定］**
  VPNピアのIPアドレスを登録します。相手がプロバイダからIPアドレスを動的に割り当てられる等の理由で、IPアドレスがわからない場合は、空欄でかまいません。
- **［相手名称指定］**
  相手がプロバイダからIPアドレスを動的に割り当てる理由でIPアドレスが指定できない場合、名称を指定します。この設定は、相手装置と同じ値である必要があります。相手のIPアドレスが固定に割り当てられる場合は、空欄でかまいません。ただし、相手を拡張認証（xauth）する場合は、相手の名称を入力してください。

ワンポイント

● **登録済みのVPNピアを削除するときは**
手順2で、削除するレコードのチェックボックスをチェックして、［送信］をクリックします。

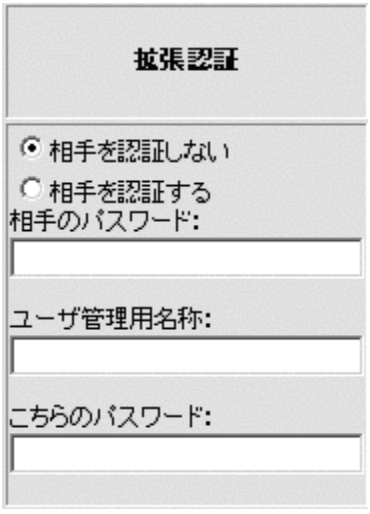
- **［こちらの名前］**
  本装置が、プロバイダからIPアドレスを動的に割り当てられる場合は、こちらの名前を指定します。この設定は、相手装置と同じ値である必要があります。また、相手に拡張認証される場合は、この設定がこちらの名前になります。

3 FQDNタイプを設定します。

本装置がAggressiveモードで動作する場合、nameを通知する方式を選択します。

4 拡張認証を設定します。

［相手を認証しない］をチェックします。また、相手が拡張認証を行う場合は、ユーザ管理用名称、こちらのパスワードを入力します。



- **［相手を認証する／しない］**
  相手を認証するかどうかを指定します。

- **［相手のパスワード］**
  相手を認証する場合は、相手のパスワードを設定します。（相手の名称はVPNピア識別で設定する相手名称指定）
- **［ユーザ管理用名称］**
  相手が本装置を拡張認証する場合で、ユーザ管理用名称がピア識別用名称と別管理になっている場合、ユーザ管理用名称を設定します。ユーザ管理用名称とピア識別用名称が同じ場合は、空欄でかまいません。
- **［こちらのパスワード］**
  相手が本装置を拡張認証する場合の、こちらのパスワードを設定します。

お知らせ

登録済み鍵データは表示されません。鍵データの管理にご注意ください。

5 **共通鍵方式を使用するVPNピアの場合は、鍵データを設定します。**

［secret-vpn］と入力します。

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]のどちらかをチェックし、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 Phase1 IKEモードを選択します。

「アドレスが固定で設定されている場合はMain Mode」を選択します。

- **[Main Mode]**

  Main Modeで接続します。本装置のIPアドレスが設定されている必要があります。最高水準のセキュリティが保証されます。

- **[Aggressive Mode]**

  Aggressive Modeで接続します。IPアドレスが不定の場合でもVPNの通信を行うことができます。

- **[アドレスが固定で設定されている場合はMain Mode]**

  プロバイダからIPアドレスが固定で割り当てられている場合はMain Modeで、IPアドレスが不定の場合はAggressive Modeで接続します。
  本装置がResponderの場合はInitiatorが接続するモードに従います。

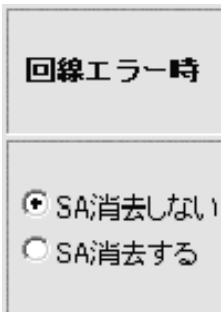
7 KeepAlive機能を選択します。

「ON」を選択します。

VPNピアが動作しているかどうかを定期的に監視するかどうかを設定します。

8 回線エラー時のSA処理を選択します。

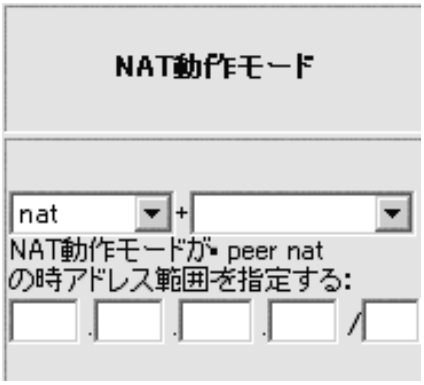
「SA消去しない」を選択します。



PPPが切断されたり、WAN回線が抜けた場合に該当SAを消去するかどうかを選択します。

9 NAT動作モードを設定します。

［off］を選択します。



お知らせ

NAT動作モードのmode-configモードは、設定しているVPNピアから変換アドレスを指定されるモードです。設定しているVPNピアが該当機能をサポートしているかどうかを確認してください。

- **[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	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アドレスでアドレス交換を行います。
nat+	NAT+の変換を行います。
modeconfig	mode-configモード。VPNピアより変換アドレスを指定され、そのアドレスに変換します。

- **[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。

10 Phase1ポリシー識別子を選択します。

このVPNピアとPhase1のネゴシエーションを行うポリシーを設定したPhase1ポリシーの中から選択します。

11 [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。VPN対象パケットの登録に進みます。

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。

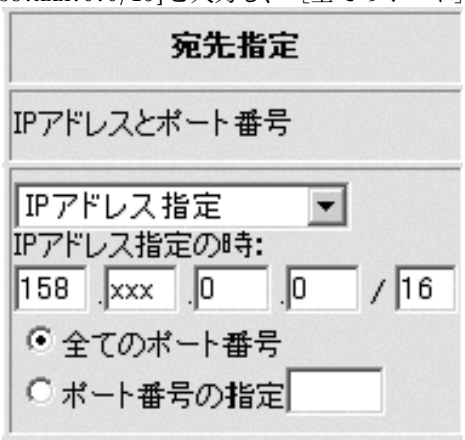
1 VPNの設定画面で、[VPN対象パケットの登録]をクリックします。

2 優先度を設定します。

このエントリの優先度を1～32の間で指定します。対象パケットが複数あった場合、どのポリシーを使用するかの判断に使用します。数字が小さいほど優先度は高くなります。

3 宛先に関する情報を設定します。

[158.xxx.0.0/16]と入力し、［全てのポート］をチェックします。



ワンポイント

- **登録済みのVPN対象パケットを削除するときは**
  手順2で、削除するレコードのチェックボックスをチェックして、［送信］をクリックします。
- **宛先指定（全て）**
  VPNピアにこの情報を通知する際に、ホスト部オール0で通知するか、ホスト部オール1で通知するかを選択する必要があります。VPNピアが受信できるマスクに合わせてください。

・**［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（ホスト1）：全ての送信元のパケットを対象とします。VPNピアにはホスト部オール1で通知します。
・全て（ホスト0）：全ての送信元のパケットを対象とします。VPNピアにはホスト部オール0で通知します。
・宛先がVPNピアの時：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アドレスを入力してください。

・**［IPアドレス］**

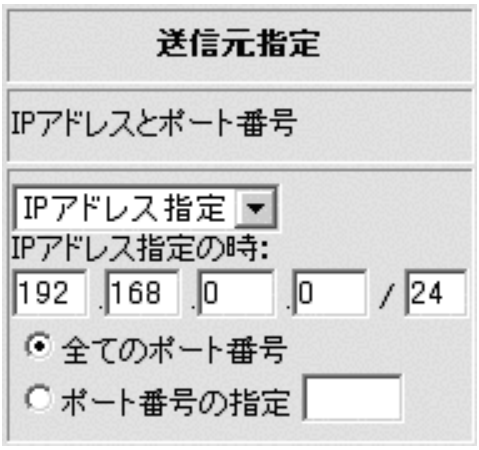
［宛先指定］でIPアドレス指定を選択したときに、宛先のIPアドレスを入力します。どのような宛先のパケットを対象とするかを選択します。

・**［宛先ポート指定］**

すべ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。

4 送信元に関する情報を設定します。

［192.168.0.0/24］と入力し、［すべてのポート］をチェックします。



・**［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（ホスト1）：全ての送信元のパケットを対象とします。VPNピアにはホスト部オール1で通知します。
・　全て（ホスト0）：全ての送信元のパケットを対象とします。VPNピアにはホスト部オール0で通知します。
・　自局からの送信：ProxyDNSを使用する場合等、（中継ではなく）本装置が送信するパケットをVPN の対象とする場合に選択します。

ワンポイント

●送信元指定（全て）

VPNピアにこの情報を通知する際に、ホスト部オール0で通知するか、ホスト部オール1で通知するかを選択する必要があります。VPNピアが受信できるマスクに合わせてください。

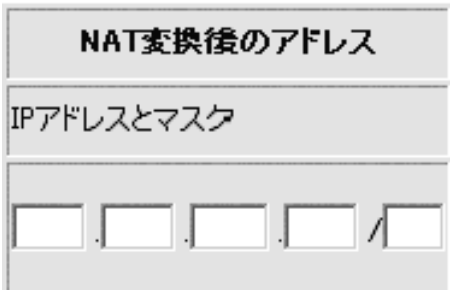
・IPアドレス指定：指定したIPアドレスからのパケットを対象とします。IPアドレスを入力してください。

5 インタフェースを選択します。

［ISDN#1］を選択します。

- **［インタフェース］**
  どのインタフェース宛のパケットを対象とするかを選択します。

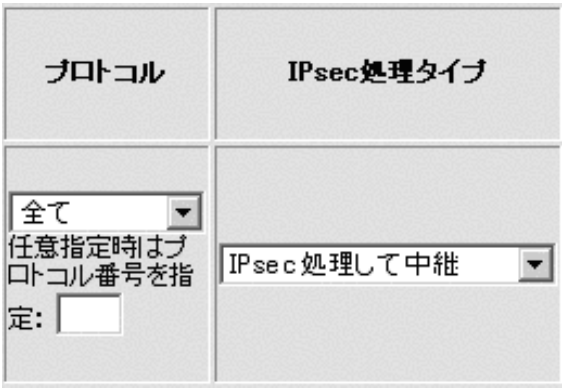
6 NAT変換後のアドレスを設定します。



- **［IPアドレスとマスク］**
  NAT動作モードが“nat”（1対1）の場合で、変換後のアドレスが複数存在する場合に、NAT変換後のアドレスを設定します。

7 プロトコル・IPsec処理タイプを選択します。

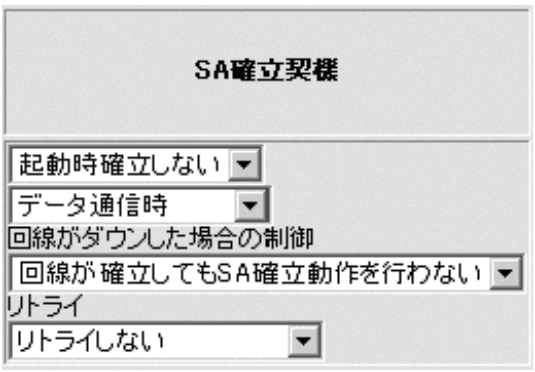
プロトコル［全て］、IPsec処理タイプ［IPsec処理して中継］を選択します。



- **［プロトコル］**
  プロトコルを選択します。選択肢にない場合は、［任意］を選択し、プロトコル番号を下の入力欄に入力してください。
- **［IPsec処理タイプ］**
  プロトコルを選択します。選択肢にない場合は、［任意］を選択し、プロトコル番号を下の入力欄に入力してください。
  - 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。

8 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。
［起動時確立しない］、［データ通信時］、［回線が確立してもSA確立動作を行わない］、［リトライしない］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。
- **[回線がダウンした場合の制御]**

  回線ダウン後、回線が復旧した場合にSAを再確立するかどうかを指定します。
- **[リトライ]**

  SA確立に失敗した場合に、リトライするかどうかを設定します。［リトライする］を選択した場合、トラフィックあり／なしにかかわらずSA確立動作を行います。SAを常時確立しておきたい場合に有効です。

9 登録済みVPNピアとPhase2ポリシーを選択します。

VPNピア［158.xxx.xxx.1］、Phase2ポリシー［1］を選択します。

- **[VPNピア]**

  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選択します。
- **[Phase2ポリシー]**

  設定しているVPN対象パケットをどのPhase2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。ポリシー識別子を選択してください。

10 [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。

11 再起動

設定内容を有効にするために、本装置を再起動します。
画面左側のメニューの中から、［リセット］をクリックします。
［装置をリセットする］をチェックしてから、［送信］をクリックします。

VPNログモードの設定

VPN ログに SA 確立の情報を載せるかどうかを設定します。

1 **VPNの設定画面で、[VPNログモードの登録]をクリックします。**

2 **優先度を設定します。**

VPNログ（P）に、SA確立の情報を載せるかどうかを設定します。

3 **［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。

4 **再起動**

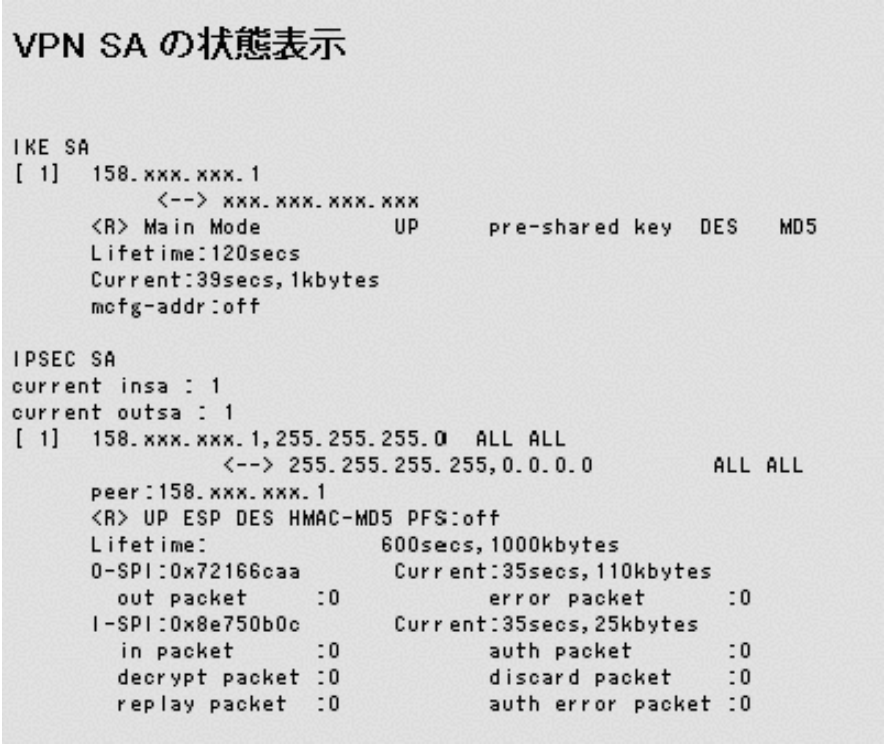
設定内容を有効にするために、本装置を再起動します。
画面左側のメニューの中から、［リセット］をクリックします。
［装置をリセットする］をチェックしてから、［送信］をクリックします。

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画面で、[VPN ログの表示]をクリックします。**



<コマンド操作>

1 **「IKE SAの情報を参照する場合は、「vpnsainfo ike」、IPsec SAの情報を参照する場合は「vpnsainfo ipsec」と入力します。**

```
#vpnsainfo ipsec
```

2 **VPN SAの情報が表示されます。**

vpnsainfo ikeの実行結果

```
IKE SA
[ 1]  158.xxx.xxx.1
          <--> xxx.xxx.xxx.xxx
     <R> Main Mode         UP    pre-shared key  DES   MD5
     Lifetime:120secs
     Current:39secs,1kbytes
     mcfg-addr:off
```

vpnsainfo ipsecの実行結果

```
current insa : 1
current outsa : 1
[ 1]  158.xxx.xxx.1,255.255.255.0  ALL ALL
             <-->255.255.255.255,0.0.0.0   ALL ALL
     peer:158.xxx.xxx.1
     <R>UP ESP DES HMAC-MD5 PFS:off
     Lifetime:           600secs,1000kbytes
     O-SPI:0x72166caa      Current:35secs,110kbytes
       out packet      :0        error packet      :0
     I-SPI:0x8e750b0c      Current:35secs,25kbytes
       in packet       :0        auth packet       :0
       decrypt packet  :0        discard packet    :0
       replay packet   :0        auth error packet :0
```

●vpnsa ikeの状態画面のみかた

・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
・mode-config機能の状態

●vpnsa ipsecの状態画面のみかた

・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 ）305
<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

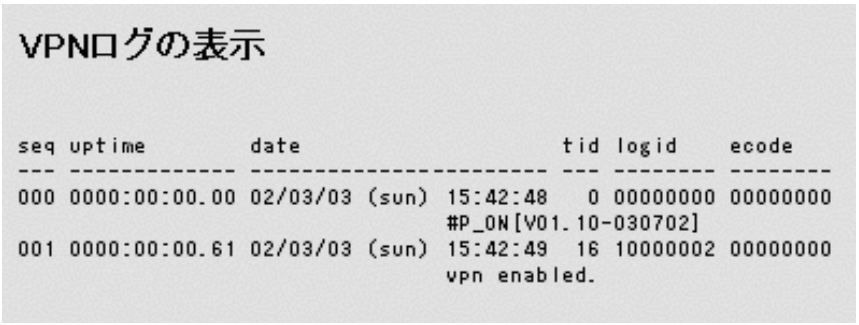
VPN ログを表示するには（vpnlogコマンド）

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
- ログID
- ロギング時刻
- エラーコード
- タスクID
- 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。**



<コマンド操作>

1 **「vpnlog」と入力します。**

```
#vpnlog
```

2 **VPN に関するログが表示されます。**

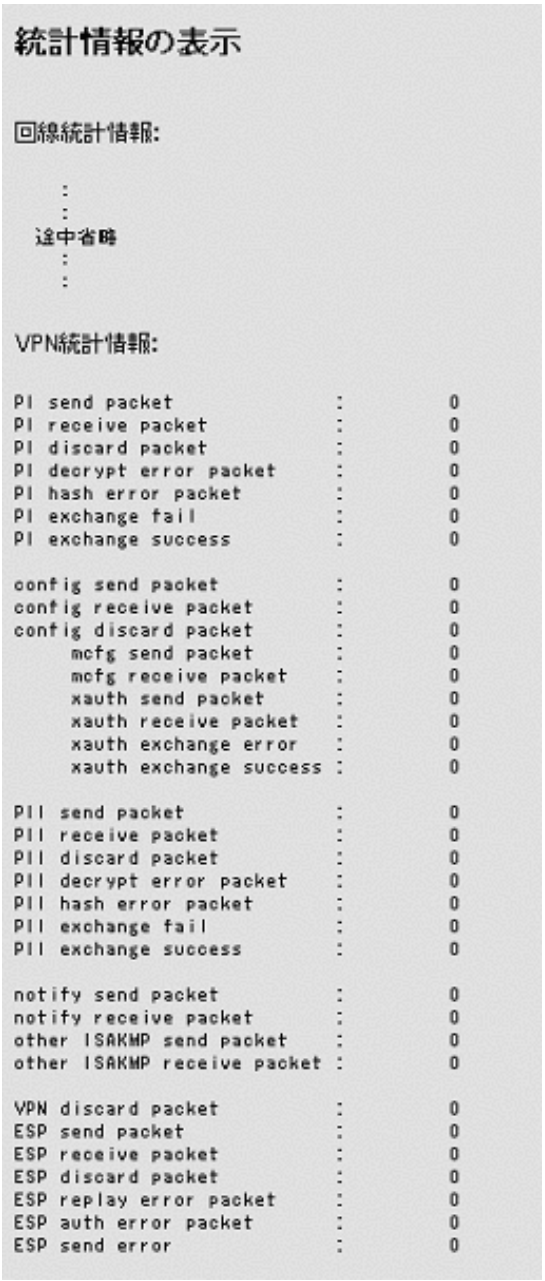
```
seq uptime       date                  tid logid    ecode
--- ------------ --------------------- --- -------- --------
000 0000:00:00.00 02/03/03 (sun) 15:42:48   0 00000000 00000000
                            #P_ON[Vv1.10-030702]
001 0000:00:00.61 02/03/03 (sun) 15:42:49  16 10000002 00000000
                            vpn enabled.
```

VPN の統計状態を表示するには（vpnstat コマンド）

VPN 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画面で、[IP統計情報の表示]をクリックします。**



統計情報の表示

回線統計情報:

:
:
途中省略
:
:

VPN統計情報:

```
PI send packet                :          0
PI receive packet             :          0
PI discard packet             :          0
PI decrypt error packet       :          0
PI hash error packet          :          0
PI exchange fail              :          0
PI exchange success           :          0

config send packet            :          0
config receive packet         :          0
config discard packet         :          0
     mcfg send packet         :          0
     mcfg receive packet      :          0
     xauth send packet        :          0
     xauth receive packet     :          0
     xauth exchange error     :          0
     xauth exchange success   :          0

PII send packet               :          0
PII receive packet            :          0
PII discard packet            :          0
PII decrypt error packet      :          0
PII hash error packet         :          0
PII exchange fail             :          0
PII exchange success          :          0

notify send packet            :          0
notify receive packet         :          0
other ISAKMP send packet      :          0
other ISAKMP receive packet   :          0

VPN discard packet            :          0
ESP send packet               :          0
ESP receive packet            :          0
ESP discard packet            :          0
ESP replay error packet       :          0
ESP auth error packet         :          0
ESP send error                :          0
```

<コマンド操作>

1 **「IKE SAの情報を参照する場合は、「vpnstat」と入力します。**

```
#vpnstat
```

2 **VPN SAの情報が表示されます。**

```
PI send packet              :       0
PI receive packet           :       0
PI discard packet           :       0
PI decrypt error packet     :       0
PI hash error packet        :       0
PI exchange fail            :       0
PI exchange success         :       0

config send packet          :       0
config receive packet       :       0
config discard packet       :       0
    mcfg send packet        :       0
    mcfg receive packet     :       0
    xauth send packet       :       0
    xauth receive packet    :       0
    xauth exchange error    :       0
    xauth exchange success  :       0

PII send packet             :       0
PII receive packet          :       0
PII discard packet          :       0
PII decrypt error packet    :       0
PII hash error packet       :       0
PII exchange fail           :       0
PII exchange success        :       0

notify send packet          :       0
notify receive packet       :       0
other ISAKMP send packet    :       0
other ISAKMP receive packet :       0

VPN discard packet          :       0
ESP send packet             :       0
ESP receive packet          :       0
ESP discard packet          :       0
ESP replay error packet     :       0
ESP auth error packet       :       0
ESP send error
```

●vpnsa ikeの状態画面のみかた

PI send packet	Phase I 送信パケット数
PI receive packet	Phase I 受信パケット数
PI discard packet	Phase I 廃棄パケット数
PI decrypt error packet	Phase I 復号化エラーパケット数
PI hash error packet	Phase I ハッシュエラーパケット数
PI exchange fail	IKE SA 確立エラー数
PI exchange success	IKE SA 確立数

config send packet	transaction exchange 送信パケット数
config receive packet	transaction exchange 受信パケット数
config discard packet	transaction exchange 廃棄パケット数
mcfg send packet	transaction exchange packet の mode-config についての送信パケット数
mcfg receive packet	transaction exchange packet の mode-config についての受信パケット数
xauth send packet	transaction exchange packet の XAUTH についての送信パケット数
xauth receive packet	transaction exchange packet の XAUTH についての受信パケット数
xauth exchange error	XAUTH 失敗数
xauth exchange success	XAUTH 成功数

PII send packet	Phase II 送信パケット数
PII receive packet	Phase II 受信パケット数
PII discard packet	Phase II 廃棄パケット数
PII decrypt error packet	Phase II 復号化エラーパケット数
PII hash error packet	Phase II ハッシュエラーパケット数
PII exchange fail	IPsec SA 確立エラー数
PII exchange success	IPsec SA 確立数

notify send packet	Notify メッセージ送信数
notify receive packet	Notify メッセージ受信数
other ISAKMP send packet	その他の ISAKMP パケット送信数
other ISAKMP receive packet	その他の ISAKMP パケット受信数

VPN discard packet	VPN 廃棄対象パケットとして廃棄したパケット数
ESP send packet	ESP 送信パケット数
ESP receive packet	ESP 受信パケット数
ESP discard packet	ESP 廃棄パケット数
ESP replay error packet	ESP リプレイアタックされたパケット数
ESP auth error packet	ESP 認証エラーパケット数
ESP send error	ESP 送信失敗数

IKE SA/IPsec SAの消去

確立している SA を消去します。

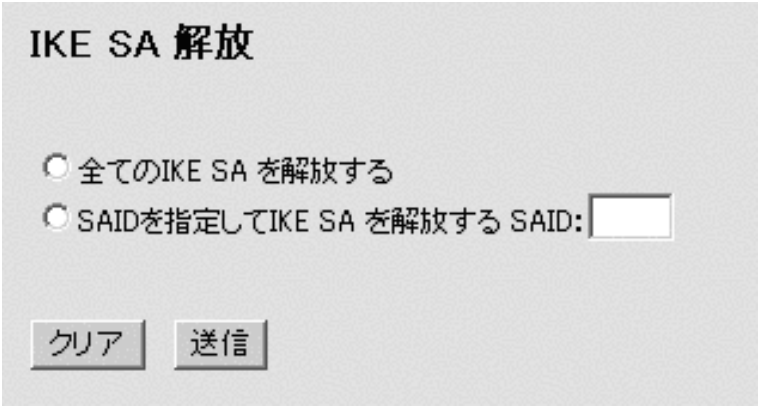
<Web ブラウザ操作>

1 **画面左側のメニューから【VPN制御】をクリックします。**

2 **IKE SA を消去する場合は［IKE SA 解放］、IPsec SA を消去する場合は［IPsec SA 解放］を選択します。**

3 **全消去するSAを選択します。**

全てのIKE SA を消去する場合は［全てのIKESA を解放する］にチェック、特定のIKE SA を消去する場合は［SAID:□を解放する］にチェックし、四角の中に消去するSA 番号をいれ、［送信］をクリックします。



IPsec SA の消去でも、同様の手順で消去できます。

<コマンド操作>

1 **ログインモードで、IKE SA を消去する場合は「ikeclear 」コマンド、IPsec SA を消去する場合は「ipsecclear 」コマンドを実行します。**

パラメータとして、全てのSA を消去する場合は「all 」、特定のSA を消去する場合は「SAID 番号」を指定します。
IKE SA のSAID 番号は「vpnsainfo ike 」コマンド、IPsec SA のSAID 番号は「vpnsainfo ipsec 」コマンドで確認できます。

（例）SAID=1 のIKE を消去する場合

```
#ikeclear 1
```

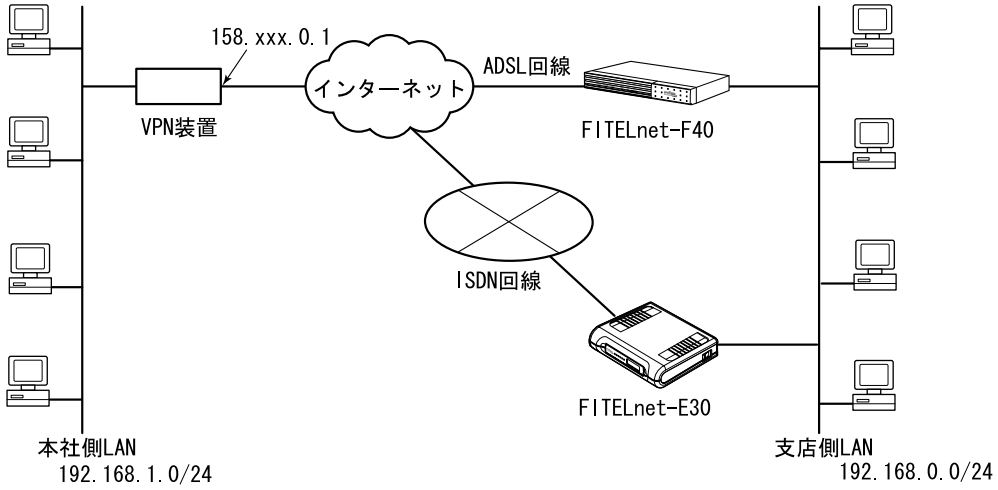
2 **消去確認メッセージが表示されます。**

消去しても良い場合は、「y」を入力できます。

```
clear all ikesa OK?(y/n)
```

設定例

FITELnet-F40 の冗長（ホットスタンバイ）として使用する際の設定例です。



	FITELnet-F40	FITELnet-E30
WAN	PPPoE	ISDN（1B のみ使用）
LAN 側 IP アドレス	192.168.0.1	192.168.0.2
WAN 側 IP アドレス	PPPoE で割り当て	PPP で割り当て
ID/PASSWORD	F40@xxxx.ne.jp/F40pass	E30/E30pass
アクセスポイントの電話番号	－	03-xxxx-xxxx
デフォルトルート	インターネット	インターネット
NAT	NAT+	NAT+
DHCP サーバ	on	off
冗長機能設定		
冗長モード	ON	ON
代表 IP アドレス	192.168.0.254	
経路監視	する	しない
経路監視を行う IP アドレス	158.xxx.0.1	
フィルタリング対象アドレス	158.xxx.0.0/255.255.0.0	

VPN 機能設定			
Phase1 ポリシー		Pre-key、DES、MD5	Pre-key、DES、MD5
Phase2 ポリシー		DES、HMAC-MD5	DES、HMAC-MD5
VPN ピア	相手アドレス	158.xxx.0.1	158.xxx.0.1
	こちらの名前	F40	E30
	拡張認証	しない	しない
	鍵データ	F40-VPNpass	E30-VPNpass
	NAT	off	nat+
VPN 対象パケット	優先度	1	1
	宛先指定	192.168.1.0/24 宛 全てのポート	192.168.1.0/24 宛 全てのポート
	送信元指定	192.168.0.0/24	192.168.0.0/24
	インタフェース	PPPoE1	ISDN1
	IPsec 処理タイプ	IPsec 処理して中継	IPsec 処理して中継

その他の設定は、装置のデフォルト値を想定します。

FITELnet-E30の設定例（工場出荷状態から設定）

```
#
#configuration
Configuration password:
conf#wan isdn single
conf#interface lan addr=192.168.0.2,255.255.255.0
conf#interface isdn1 addr=0.0.0.0 remote=0.0.0.0
conf#hostname add default=E30 password=E30pass
conf#target add name=ISP dial=03xxxxxxxx host=default
conf#ipripstatic add default=ISP
conf#nat natp if=isdn1
conf#dhcpserver off
conf#rgrouping on gipaddr=192.168.0.254
conf#pathchk off
conf#pathchktable add pathchkipaddr=158.xxx.0.1
conf#pathfilter add pathchkipaddr=158.xxx.0.1 addr=192.168.1.0,255.255.255.0
conf#vpn on
conf#vpnikepolicy add id=1 method=prekey encr=des hash=md5
conf#vpnpolicy add id=1 encr=des auth=hmac-md5
conf#vpnpeer add addr=158.xxx.0.1 myname=E30 xauth=off key=a,E30-VPNpass nat=natp
ikepolicy=1
conf#vpnselector add id=1 dst=192.168.1.0,255.255.255.0 src=192.168.0.0,255.255.255.0
dstif=isdn1 type=ipsec peeraddr=158.xxx.0.1 policy=1
conf#exit
configuration modified. save OK ? (y/n): y
please reset#reset
Do you want to continue (y/n)?: y
```

※　VPN 対象パケット以外はインターネット接続するような形態の場合は、

vpnselector add id=32 dst=all src=all type=bypass

を設定します。

［参考　FITELnet-F40（V02.02）の設定例］

```
#
# configuration
Configuration password:
conf#?
conf#wan type=pppoe
conf#pppoe add name=ISP if=pppoe1 id=F40@xxxx.ne.jp password=F40pass
conf#interface lan addr=192.168.0.1,255.255.255.0
conf#iprip add dst=0.0.0.0,0.0.0.0 nextif=pppoe1
conf#nat pppoe1 natp
conf#dhcpserver on
conf#rgrouping on gipaddr=192.168.0.254
conf#pathchk on
conf#pathchktable add pathchkipaddr=158.xxx.0.1
conf#pathfilter add pathchkipaddr=158.xxx.0.1 addr=192.168.1.0,255.255.255.0
conf#vpn on
conf#vpnikepolicy add id=1 method=prekey encr=des hash=md5
conf#vpnpolicy add id=1 encr=des auth=hmac-md5
conf#vpnpeer add addr=158.xxx.0.1 myname=F40 xauth=off key=a,F40-VPNpass nat=off
ikepolicy=1
conf#vpnselector add id=1 dst=192.168.1.0,255.255.255.0 src=192.168.0.0,255.255.255.0
dstif=pppoe1 type=ipsec peeraddr=158.xxx.0.1 policy=1
conf# vpnselector add id=32 dst=all src=all type=bypass
conf#exit
configuration modified. save OK ? (y/n): y
please reset#reset
Do you want to continue (y/n)?: y
```

用語集

【アルファベット】

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仕組みです。ISAKMP で鍵交換を行う際に使用しています。

ESP(Encapsulation Security Payload)

IPsec で規定されている認証・暗号のパケット方式。本装置では、暗号アルゴリズムとして DES(56bit),3DES,NULL,ハッシュアルゴリズムとして HMAC with MD5･HMAC with SHA をサポートしています(RFC2406)

FQDN タイプ

本装置が Aggressive モードで動作する場合に通知する name の情報の送信形式を、FQDN or UserFQDN から選択します。

IPsec を確立する相手(VPN ピア)が受信できる形式である必要がありますので、Aggressive モードで動作する場合は、相手に確認が必要です。

HMAC-MD5

ハッシュアルゴリズムの一つ

HMAC-SHA

ハッシュ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します。

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です。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」の交換を行います。これらの情報をまとめて「ポリシー」といいます(RFC2408)

mode-config

VPN 通信を行う相手から、VPN で使用する IP アドレスを指定してもらい動作するしくみを、mode-config といいます。

本装置は、IP アドレスを割り当てる機能はサポートしていません。

PFS

SA 確立時に、新しい鍵情報を指定するかどうかを選択します。新しい鍵情報を使用する方が、セキュリティは高いですが、鍵生成に時間がかかります。

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します。

Responder

VPN ネゴシエーションを受ける側を指します。

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・認証アルゴリズムなどのセキュリティ情報を含んでいます。

VPN

VPN(Vitual 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。本装置は VPN の中の、ネットワーク層の暗号化／認証に特化した IPsec(IP Security)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。

【か】

拡張認証

本装置では、IPsec の拡張認証(zauth)に対応しています。

拡張認証では、Phase1 終了後に ID/パスワードの認証を行います。

IPsecの基本動作

①Phase1（IKE SA） の確立

設定した pre-shared key から計算した鍵作成情報を通知します。

共通鍵方式の場合は、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（FITELnet- A と FITELnet- 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。

②拡張認証

VPN 通信を行う相手が、本当に思いどおりの相手であることを再度確認するため、名称、パスワードの問い合わせを行い、確認します。

③mode-config

VPN 通信を行う相手から、VPN で使用する IP アドレスを指定してもらい動作します。センター側で、VPN の IP アドレスを一括管理するような場合に有効な機能です。本装置は、IP アドレスを割り当てる機能はサポートしていません。

④Phase2（IPsec SA） の確立

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 のネゴシエーションには、①で作成した鍵情報で暗号化されます。

なお、IPsec SA のネゴシエーションでは、設定したポリシーを提案します。

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。

⑤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、④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。データを複号する際も、④で作成した鍵を使用して複号します。

- 本書は改善のため事前連絡なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権その他の権利について、弊社はその責を負いません。
- 無断転載を禁じます。

発行責任：古河電気工業株式会社

130-B0314-AK01-A

2002.05