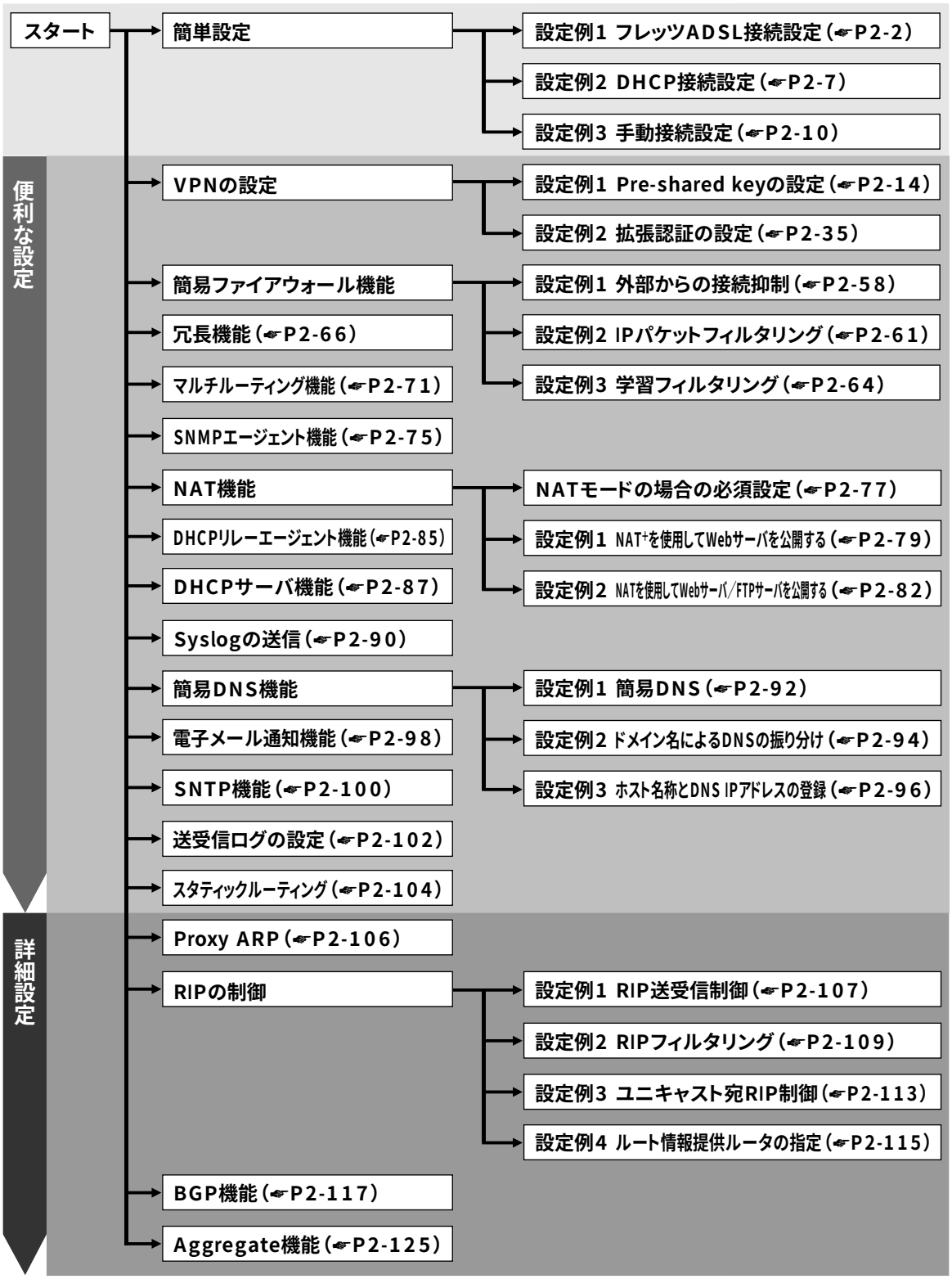
設定について

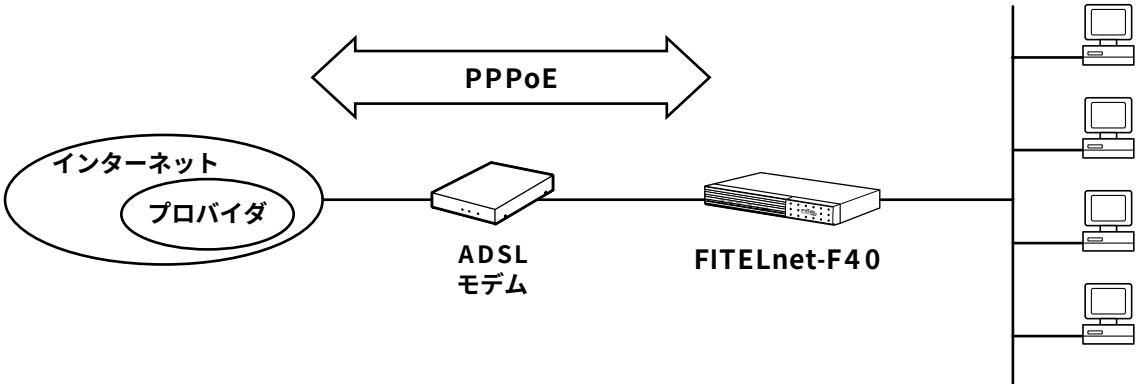
接続例と設定方法を説明しています。
具体的な操作方法は、P2-2～P2-128をご覧ください。



簡単設定

設定例1　フレッツADSL接続設定

フレッツADSLのサービスを利用するときの設定について説明します。
Webブラウザからの設定では、簡単設定だけで操作が完了します。



＜設定データの例＞

分類	画面名	設定項目		入力値
簡単設定	PPP over Ethernet	PPPoE1	名称	Aprovider
			ユーザID	abc012@A.ne.jp
			パスワード	Apass
		PPPoE2	名称	Bprovider
			ユーザID	abc012@B.ne.jp
			パスワード	Bpass
		PPPoE3	名称	Cprovider
			ユーザID	abc012@C.ne.jp
			パスワード	Cpass
		PPPoE4	名称	Dprovider
			ユーザID	abc012@D.ne.jp
			パスワード	Dpass
		デフォルトルート		PPPoE1
		LAN側IPアドレス サブネットマスク		192.168.0.1 255.255.255.0
		DHCPサーバ機能		使用する
		DNSサーバ		通知なし
		簡易DNS		使用する
		NAT動作モード	PPPoE1	NAT+
			PPPoE2	NAT+
			PPPoE3	NAT+
			PPPoE4	NAT+

簡単設定

＜Webブラウザ操作＞

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

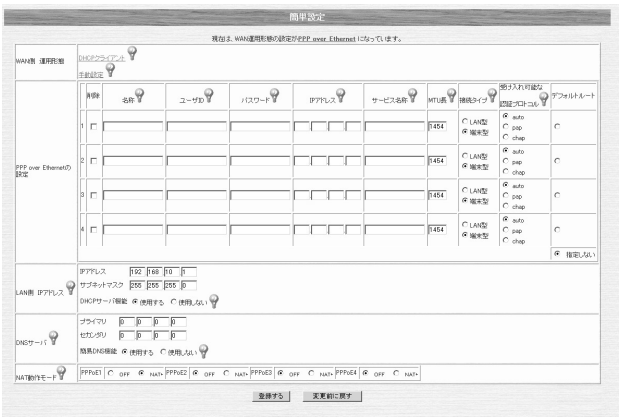
3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 簡単設定のWAN側運用形態から［PPP over Ethernet］をクリックします。

5 簡単設定を設定します。

PPP over Ethernetの各種設定を入力します。



〈次ページへ続く〉

簡単設定

6 設定内容を登録します。

設定項目を入力して、［登録する］をクリックします。

7 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、［装置の再起動］をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

簡単設定

＜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。(☛P1-13)

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

2 EWANをPPPoEで使うための設定をします。

```
conf# wan type=pppoe
```

3 PPPoE関連の設定をします。

```
conf# pppoe add name=Aprovider id=abc012@A.ne.jp password=Apass if=pppoe1
conf# pppoe add name=Bprovider id=abc012@B.ne.jp password=Bpass if=pppoe2
conf# pppoe add name=Cprovider id=abc012@C.ne.jp password=Cpass if=pppoe3
conf# pppoe add name=Dprovider id=abc012@D.ne.jp password=Dpass if=pppoe4
```

4 デフォルトルートを指定します。

```
conf# ipripstatic delete default
conf# ipripstatic add dsf=0.0.0.0 nextif=pppoe1
```

5 簡易DNS機能を設定します。

```
conf#proxydns on
```

6 DHCPサーバ機能を設定します。

```
conf#dhcpserver on
```

7 NAT動作モードを設定します。

```
conf# nat pppoe1 natp
conf# nat pppoe2 natp
conf# nat pppoe3 natp
conf# nat pppoe4 natp
```

〈次ページへ続く〉

簡単設定

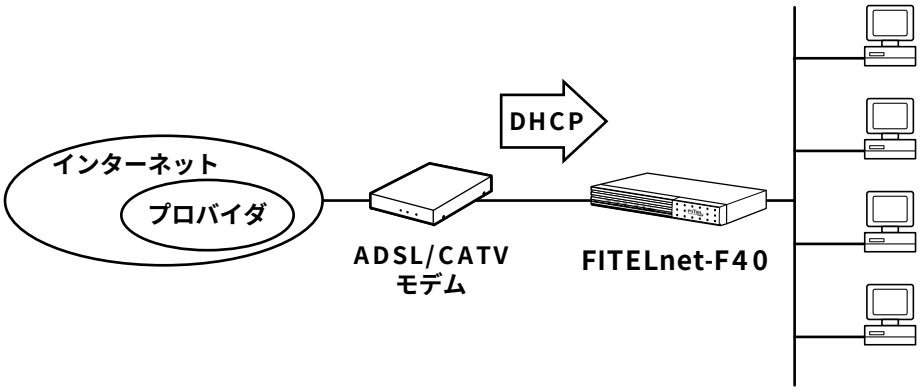
8 設定を保存します。

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

簡単設定

設定例2　DHCP接続設定

EWANをDHCPクライアントとして使用するケースです。



＜設定データの例＞

分類	画面名	設定項目	入力値
簡単設定	DHCPクライアント	MTU	1454
		ホスト名	hostname
		LAN側IPアドレス サブネットマスク	192.168.0.1 255.255.255.0
		DNSサーバ	通知なし
		簡易DNS機能	使用する
		DHCPサーバ機能	使用する
		NAT動作モード	NAT+

＜Webブラウザ操作＞

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

〈次ページへ続く〉

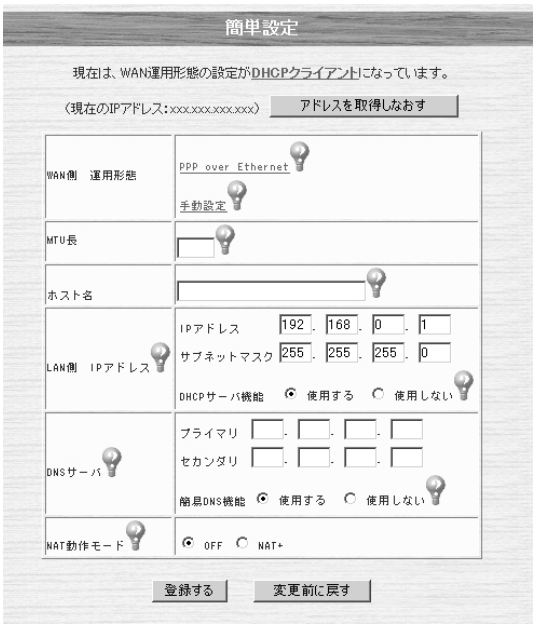
簡単設定

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 簡単設定のWAN側運用形態から［DHCPクライアント］をクリックします。

5 DHCPクライアントの各種設定を入力します。



6 設定内容を登録します。

設定項目を入力して、［登録する］をクリックします。

7 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動]をクリックします。
[装置を再起動する］をチェックしてから、［送信］をクリックします。

ワンポイント

IPアドレスが取得できている場合は、画面上部に取得したIPアドレスが表示されます。IPアドレスを取得しなおす場合は、［アドレスを取得しなおす］を押してください。

簡単設定

＜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。(☛P1-13)

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

2 EWANをDHCPクライアントで使うための設定をします。

```
conf# wan type=dhcp hostname=hostname
```

3 デフォルトルートを指定します。

```
conf# ipripstatic delete default
conf# ipripstatic dsf=0.0.0.0 nextif=wan
```

4 簡易DNS機能を設定します。

```
conf#proxydns on
```

5 DHCPサーバ機能を設定します。

```
conf#dhcpserver on
```

6 NAT動作モードを設定します。

```
conf# nat wan natp
```

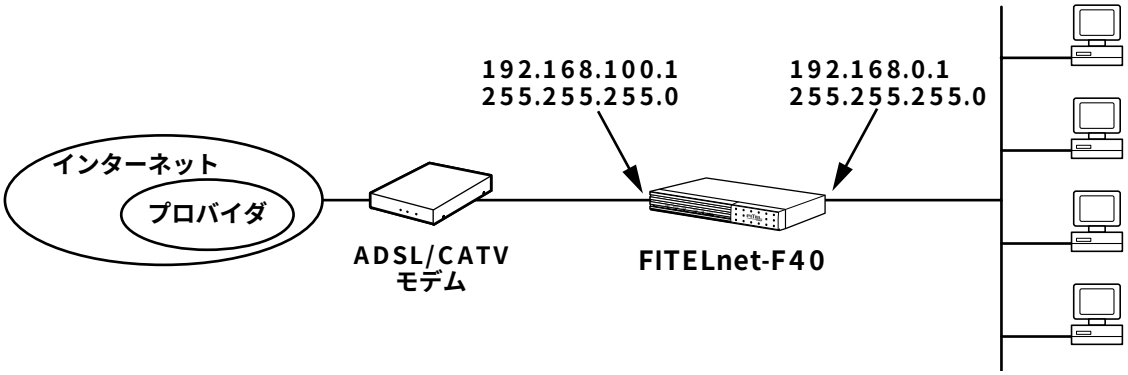
7 設定を保存します。

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

簡単設定

設定例3　手動接続設定

EWANのIPアドレスを、手動で割り当てるケースです。



＜設定データの例＞

分類	画面名	設定項目	入力値
簡単設定	手動設定	MTU	1454
		WAN側IPアドレス サブネットマスク	192.168.100.1 255.255.255.0
		LAN側IPアドレス サブネットマスク	192.168.0.1 255.255.255.0
		DNSサーバ(プライマリ) (セカンダリ)	158.xxx.xxx.1 158.xxx.xxx.2
		簡易DNS機能	使用する
		DHCPサーバ機能	使用する
		デフォルトゲートウェイ	158.xxx.xxx.100
		NAT動作モード	NAT+

＜Webブラウザ操作＞

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

〈次ページへ続く〉

簡単設定

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 簡単設定のWAN側運用形態から［手動設定］をクリックします。

5 手動設定の各種設定を入力します。

6 設定内容を登録します。

設定項目を入力して、［登録する］をクリックします。

7 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動]をクリックします。
[装置を再起動する］をチェックしてから、［送信］をクリックします。

簡単設定

＜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。(☛P1-13)

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

2 EWANを手動設定で使うための設定をします。

```
conf# wan type=manual
```

3 EWANインタフェースのIPアドレスを設定します。

```
conf# interface wan addr=192.168.100.1,255.255.255.0
```

4 DNSのアドレスを登録します。

```
conf#proxydns on nameserverip=158.XXX.XXX.1, 158.XXX.XXX.2
```

5 DHCPサーバ機能を設定します。

```
conf#dhcpserver on
```

6 デフォルトゲートウェイを登録します。

```
conf#ipripstatic delete default
conf#ipripstatic add default=158.XXX.XXX.100
```

7 NAT動作モードを設定します。

```
conf# nat wan natp
```

8 設定を保存します。

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

VPNの設定

FITELnet-F40では、IPsecを使用したVPNをサポートしており、IPsecのPhase1（鍵交換）の方式は、以下の2種類をサポートしています。
・共通鍵方式（Pre-shared Key）
・公開鍵方式（PKI-X.509）
※VPNピアごとに混在することも可能。

FITELnet-F40では、標準で共通鍵方式をサポートしており、オプションとして公開鍵方式をサポートしています。

公開鍵方式を使用する場合は、鍵ペアの生成・電子証明書リクエストデータの作成・電子証明書の登録等、共通鍵方式では必要のない操作が必要となります。公開鍵方式特有の操作については、別冊「PKI（公開鍵基盤）－X.509機能に関する資料」を参照してください。

Phase2ポリシー・ピアの登録・VPN対象パケットの登録は、どちらの方式も共通となりますので、Phase1で公開鍵方式を使用する場合も、本書を参照してください。

＜取扱説明書の構成＞
拡張認証機能を使用しない場合の設定例（☛P2-18）
センター側で拡張認証する場合の設定例（☛P2-39）
公開鍵方式のための証明書登録手順（☛別冊「PKI（公開鍵基盤）－X.509機能に関する資料」）

お知らせ

公開鍵方式（PKI）をご使用になる場合は、PKIキーがインストールされている必要があります。PKIキーがインストールされているかどうかは、Webブラウザ操作の「装置について」または「hereis」コマンドで確認できます。（☛P4-2）

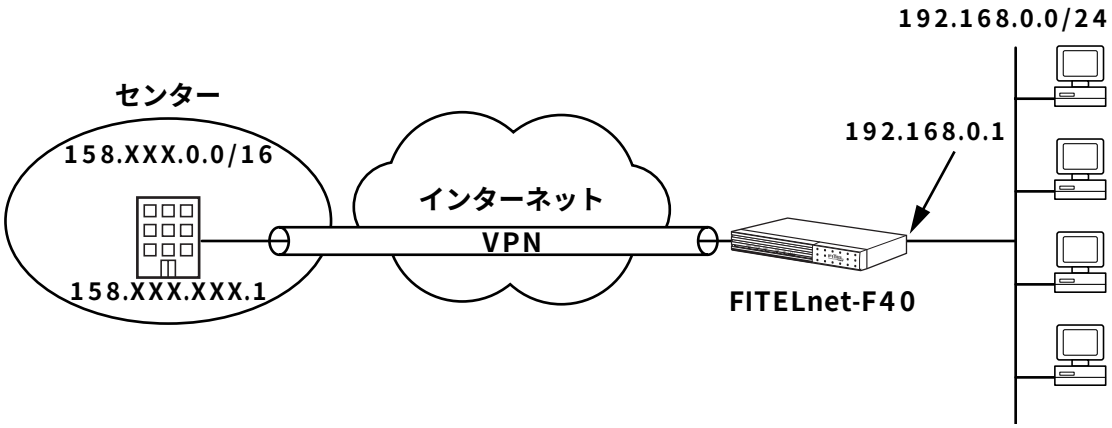
ワンポイント

●PKI（公開鍵基盤）について（☛P5-15）

VPNの設定

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。

設定例1　Pre-shared keyの設定



＜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 0kbytes（設定なし）
		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
		圧縮	圧縮しない
		圧縮ネゴシエーション	しない

VPNの設定

＜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-F40
		FQDNタイプ	User FQDN
		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
		Keep Alive	off
		回線エラー時	SA消去しない
		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 すべてのポート番号
		宛先指定	IPアドレス指定：158.xxx.0.0/16 すべてのポート番号
		プロトコル	全て
		インタフェース	pppoe1
		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確立動作を行わない リトライしない
		VPNピア	158.xxx.xxx.1
		Phase2ポリシー	1

- PPPoEでは、アドレスは自動的に割りあてられます。
- 双方とも拡張認証はしない例です。

VPNの設定

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、VPNピア・Phase1,Phase2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 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［VPNの設定］をクリックします。

〈次ページへ続く〉

VPNの設定

6 VPN動作モードの［ON］を選択して、［送信］をクリックします。

7 VPNを設定します。

- **Phase1ポリシーの登録（☛P2-18）**
- **Phase2ポリシーの登録（☛P2-20）**
- **VPNピアの登録（☛P2-23）**
- **VPN対象パケットの登録（☛P2-29）**

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

VPNの設定

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（☛P2-17）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1～32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）／RSA signature（公開鍵方式）の選択および拡張認証するかどうかを選択します。

〈次ページへ続く〉

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。

お知らせ

●公開鍵方式を使用する場合は、PKIキーがインストールされている必要があります。
●この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

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。（64件）

1 VPNの設定画面（☛P2-17）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1～64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。

〈次ページへ続く〉

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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

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Oakley Group［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］**
  - ・3des：3desで暗号化します。
  - ・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。

〈次ページへ続く〉

6 圧縮・圧縮ネゴシエーションを設定します。

圧縮［圧縮しない］、圧縮ネゴシエーション［しない］を選択します。

- **［圧縮］**
  転送速度をあげたい場合は、「圧縮する」を選択します。相手が圧縮をサポートしている必要があります。圧縮方式はLZSです。
- **［圧縮ネゴシエーション］**
  IPCA（圧縮ネゴシエーション）を行うかどうかを選択します。FITELnet-F40がResponderの場合は、相手に合わせます。

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。

VPNピアの登録に進みます。

VPNの設定

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（☛P2-17）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-F40］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。
- **「こちらの名前］**
  FITELnet-F40が、プロバイダからIPアドレスを動的に割り当てられる（Aggressive Mode）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。

〈次ページへ続く〉

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。

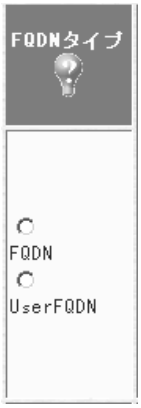
お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

VPNの設定

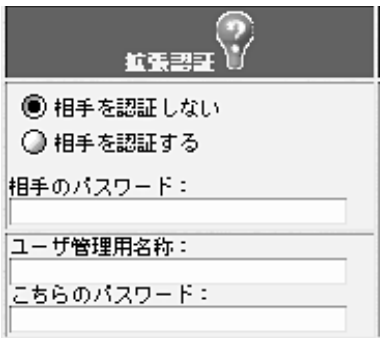
3 FQDNタイプを設定します。

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FITELnet-F40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FITELnet-F40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。

ワンポイント

●**FQDNタイプ（☛P5-17）**

〈次ページへ続く〉

お知らせ

V03.00以降のファームウェアでは登録済み鍵データが非表示となります。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。FITELnet-F40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。PPPoEやDHCPなど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。

〈次ページへ続く〉

- **[アドレスが固定で設定されている場合はMain Mode]**
  PPPoEでIPアドレスが固定で割り当てられている場合や、WANのタイプが手動設定の場合はMain Modeで、IPアドレスが不定の場合はAggressive Modeで接続します。
  FITELnet-F40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。

「OFF」を選択します。

SAが確立されている相手に対して、応答確認を行うかどうかを設定します。
相手装置がIKEのKeepAliveをサポートしている場合は「IKE」を選択します。IKEのKeepAliveをサポートしていない装置とSAを確立する場合には「ICMP」を選択します。「ICMP」を選択した場合には、KeepAliveを行う相手の端末（ルータでなくても良い）のIPアドレスを指定します。ピアに対して応答確認を行う場合は「VPNピア」を選択してください。また、送信元アドレスとして、LAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。

8 NAT-Traversal機能を選択します。

「使用しない」を選択します。

設定しているVPNピアとの通信経路中にNAT動作を行なうルータが存在する場合は、「使用する」を選択します。この場合、VPNピアとのKeepAliveを行ないますので、その送信間隔を設定します。

〈次ページへ続く〉

9 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。

PPPoE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。

10 NAT動作モードを設定します。

［off］を選択します。

- **［NAT動作モード］**
  NATの動作モードを選択します。

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。*

* このモードでNATスタティック登録を使用したい場合はP2-57 VPNを使用したNATスタティックを参照してください。

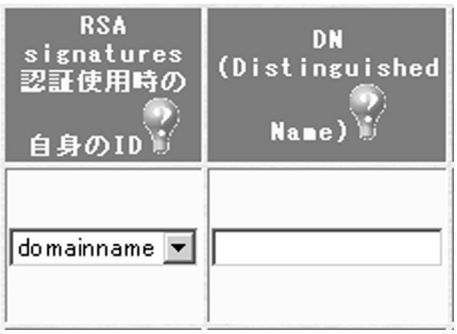
- **［IPアドレス］**
  NAT動作モードで「peer nat」を選択した場合に、NATの変換アドレスを入力します。

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。

〈次ページへ続く〉

11 公開鍵方式を使用する場合は、RSA signatures認証使用時の自身のID、DN（Distinguished Name）を設定します。



- **［RSA　signatures認証使用時の自身のID］**
  証明書に含まれるどのIDで認証するかを選択します。証明書に含まれる情報以外で認証する場合は、“ DN ”を選択し、DNに文字列を入力します。この設定は接続する相手と同じである必要があります。

12 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。

13 ［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の設定

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。（64件）

1 VPNの設定画面（☛P2-17）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1～64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、［すべてのポート］をチェックします。

〈次ページへ続く〉

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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

- **[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。
- **[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。
  ・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。
  ・自局からの送信：ProxyDNSやDHCPリレーエージェントのように、（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

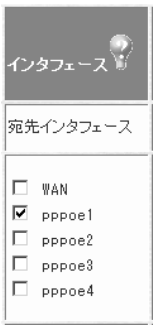
●送信元指定（全て）
VPNピアにこの情報を通知する際に、ホスト部オール0で通知するか、ホスト部オール1で通知するかを選択する必要があります。VPNピアが受信できるマスクに合わせてください。

〈次ページへ続く〉

- **[IPアドレス]**
  ［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アドレスを入力します。
- **[送信元ポート指定]**
  すべ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。

5 インタフェースを選択します。

［pppoe1］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。

〈次ページへ続く〉

7 プロトコル・IPsec処理タイプを選択します。

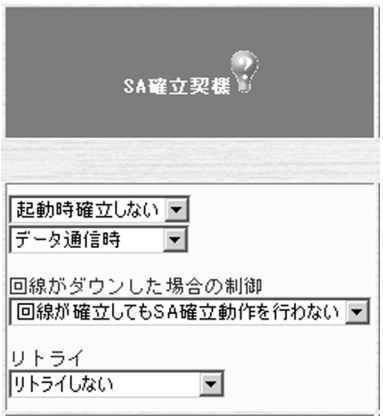
プロトコル［全て］、IPsec処理タイプ［IPsec処理して中継］を選択します。

- **［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］**
  - 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。



〈次ページへ続く〉

- **[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。

VPNの設定

＜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。(☛P1-13)

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

2 VPN機能を使用する設定をします。

```
conf# vpn on
```

3 Phase1ポリシーの設定をします。

```
conf#vpnikepolicy add id=1 method=prekey
```

4 Phase2ポリシーの設定をします。

```
conf#vpnpolicy add id=1 encr=des auth=hmac-md5
```

5 VPNピアの設定をします。

```
conf#vpnpeer add addr=158.xxx.xxx.1 myname=FITELnet-F40
idtype-pre=userfqdn key=a, secret-vpn nat=off ikepolicy=1
```

6 VPN対象パケット（VPNセレクタ）の設定をします。

```
conf#vpnselector add id=1 dst=158.xxx.0.0,255.255.0.0
src=192.168.0.0,255.255.255.0 dstif=pppoe1 type=ipsec
peeraddr=158.xxx.xxx.1 policy=1
```

7 設定を保存します。

```
conf#exit
Configuration modified. save ok? (y/n):y
```

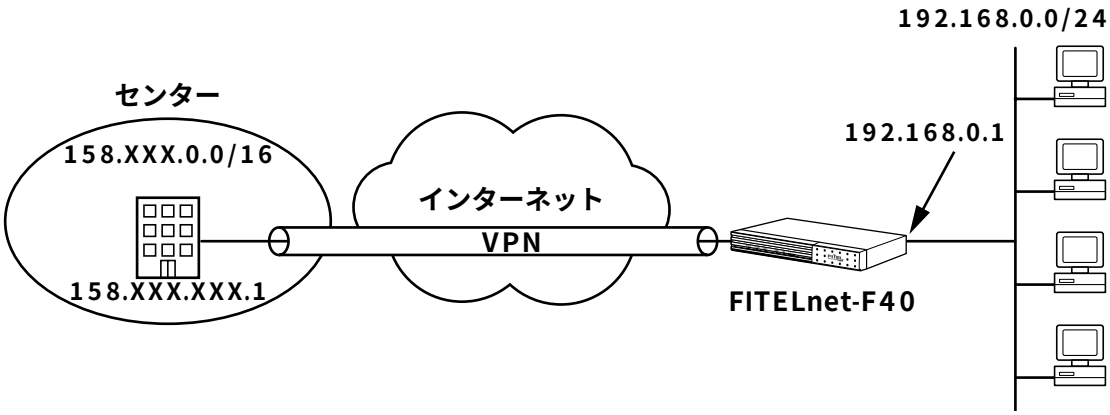
ワンポイント

●VPN以外はインターネット接続を行うためには手順6で、以下のコマンドを設定します。

conf#vpnselector add id=64 dest=all src=all type=bypass

VPNの設定

設定例2　拡張認証の設定



＜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（拡張認証あり）
		暗号化アルゴリズム	des
		ハッシュアルゴリズム	md5

VPNの設定

＜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-F40
		FQDNタイプ	User FQDN
		拡張認証 相手のパスワード ユーザ管理用名称 こちらのパスワード	相手を認証しない * 空欄 admin-FITELnet-F40 secret-F40
		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
		Keep Alive	off
		回線エラー時	SA消去しない
		NAT動作モード	off
		Phase1ポリシー識別子	1

- 先記以外は、設定例1と同じです。

* 相手がFITELnet-F40を拡張認証する場合の設定例です。
FITELnet-F40が拡張認証されるだけの場合は“ 相手を認証しない ”を選択します。

VPNの設定

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、VPNピア・Phase1,Phase2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 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［VPNの設定］をクリックします。

〈次ページへ続く〉

VPNの設定

6 VPN動作モードの［ON］を選択し、［送信］をクリックします。

7 VPNを設定します。

- **Phase1ポリシーの登録（☛P2-39）**
- **Phase2ポリシーの登録（☛P2-41）**
- **VPNピアの登録（☛P2-44）**
- **VPN対象パケットの登録（☛P2-50）**

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

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（☛P2-38）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1～32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）で拡張認証を行う場合は、［Pre-shared Key（拡張認証あり）］を選択します。

- **［Phase1方式］**
  Pre-shared key（共通鍵方式）／RSA signeture（公開鍵方式）の選択および拡張認証するかどうかを選択します。

〈次ページへ続く〉

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。

お知らせ

●公開鍵方式を使用する場合は、PKIキーがインストールされている必要があります。
●この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

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。（64件）

1 VPNの設定画面（☛P2-38）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1～64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。

〈次ページへ続く〉

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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

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Oakley Group［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］**
  - 3des：3desで暗号化します。
  - 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。

〈次ページへ続く〉

6 圧縮・圧縮ネゴシエーションを設定します。

圧縮［圧縮しない］、圧縮ネゴシエーション［しない］を選択します。

- **［圧縮］**
  転送速度をあげたい場合は、「圧縮する」を選択します。相手が圧縮をサポートしている必要があります。圧縮方式はLZSです。
- **［圧縮ネゴシエーション］**
  IPCA（圧縮ネゴシエーション）を行うかどうかを選択します。FITELnet-F40がResponderの場合は、相手に合わせます。

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。

VPNピアの登録に進みます。

VPNの設定

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（☛P2-38）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-F40］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。
- **「こちらの名前］**
  FITELnet-F40が、プロバイダからIPアドレスを動的に割り当てられる（Aggressive Mode）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。

〈次ページへ続く〉

ワンポイント

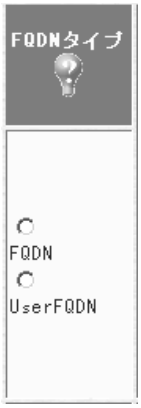
●登録済みのVPNピアを削除するときは
手順2で、削除するレコードのチェックボックスをチェックして、［送信］をクリックします。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

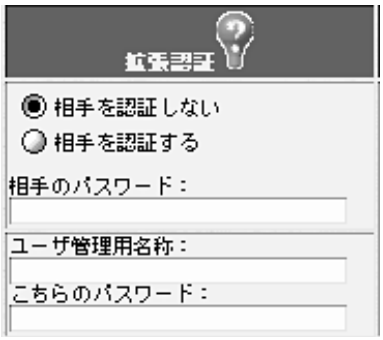
3 FQDNタイプを設定します。

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



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FITELnet-F40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FITELnet-F40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。

ワンポイント

●**FQDNタイプ（☛P5-17）**

〈次ページへ続く〉

お知らせ

V03.00以降のファームウェアでは登録済み鍵データが非表示となります。鍵データの管理にご注意ください。

5 共通鍵方式を使用しる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。FITELnet-F40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。PPPoEやDHCPなど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。

〈次ページへ続く〉

- **[アドレスが固定で設定されている場合はMain Mode]**
  PPPoEでIPアドレスが固定で割り当てられている場合や、WANのタイプが手動設定の場合はMain Modeで、IPアドレスが不定の場合はAggressive Modeで接続します。
  FITELnet-F40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。

「OFF」を選択します。

SAが確立されている相手に対して、応答確認を行うかどうかを設定します。
相手装置がIKEのKeepAliveをサポートしている場合は「IKE」を選択します。IKEのKeepAliveをサポートしていない装置とSAを確立する場合には「ICMP」を選択します。「ICMP」を選択した場合には、KeepAliveを行う相手の端末（ルータでなくても良い）のIPアドレスを指定します。ピアに対して応答確認を行う場合は「VPNピア」を選択してください。また、送信元アドレスとして、LAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。

8 NAT-Traversal機能を選択します。

「使用しない」を選択します。

設定しているVPNピアとの通信経路中にNAT動作を行なうルータが存在する場合は、「使用する」を選択します。この場合、VPNピアとのKeepAliveを行ないますので、その送信間隔を設定します。

〈次ページへ続く〉

9 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。

PPPoE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。

10 NAT動作モードを設定します。

［off］を選択します。

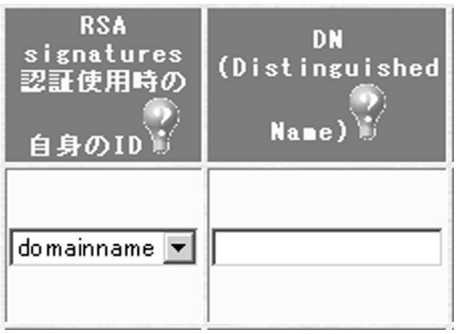
- **［NAT動作モード］**
  NATの動作モードを選択します。

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。*

* このモードでNATスタティック登録を使用したい場合はP2-57 VPNを使用したNATスタティックを参照してください。

- **［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。

11 公開鍵方式を使用する場合は、RSA signatures認証使用時の自身のID、DN（Distinguished Name）を設定します。



- **［RSA　signatures認証使用時の自身のID］**
  証明書に含まれるどのIDで認証するかを選択します。証明書に含まれる情報以外で認証する場合は、“ DN ”を選択し、DNに文字列を入力します。この設定は接続する相手と同じである必要があります。

12 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。

13 ［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。

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。

VPNの設定

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。（64件）

1 VPNの設定画面（☛P2-38）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1～64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、［すべてのポート］をチェックします。

〈次ページへ続く〉

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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）

VPNの設定

- **[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。
- **[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。
  ・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。
  ・自局からの送信：ProxyDNSやDHCPリレーエージェントのように、（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

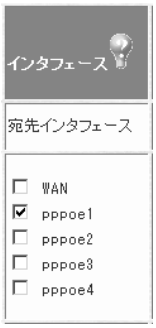
●送信元指定（全て）
VPNピアにこの情報を通知する際に、ホスト部オール0で通知するか、ホスト部オール1で通知するかを選択する必要があります。VPNピアが受信できるマスクに合わせてください。

〈次ページへ続く〉

- **[IPアドレス]**
  ［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アドレスを入力します。
- **[送信元ポート指定]**
  すべ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。

5 インタフェースを選択します。

［pppoe1］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。

〈次ページへ続く〉

7 プロトコル・IPsec処理タイプを選択します。

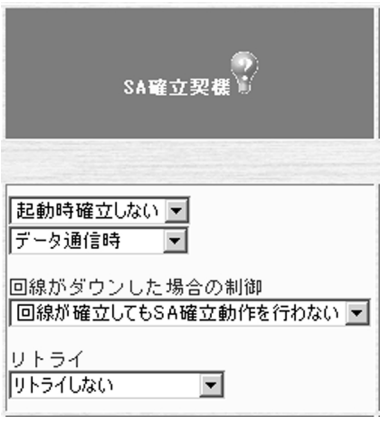
プロトコル［全て］、IPsec処理タイプ［IPsec処理して中継］を選択します。

- **［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］**
  - 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］を選択します。



〈次ページへ続く〉

- **[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。

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。

VPNの設定

＜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。(☛P1-13)

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

2 VPN機能を利用する設定をします。

```
conf# vpn on
```

3 Phase1ポリシーの設定をします。

```
conf#vpnikepolicy add id=1 method=prekeyxauth
```

4 Phase2ポリシーの設定をします。

```
conf#vpnpolicy add id=1 encr=des auth=hmac-md5
```

5 VPNピアの設定をします。

```
conf#vpnpeer add addr=158.xxx.xxx1 myname=FITELnet-F40
idtype-pre=userfqdn myname_xauth=admin-FITELnet-F40
mypasswd=secret-F40 key=a,secret-vpn nat=off ikepolicy=1
```

〈次ページへ続く〉

6 VPN対象パケット（VPNセレクタ）の設定をします。

```
conf#vpnselector add id=1 dst=158.xxx.0.0,255.255.0.0
src=192.168.0.0,255.255.255.0 dstif pppoe1 type=ipsec
peeraddr=158.xxx.xxx.1 policy=1
```

7 設定を保存します。

```
conf#exit
Configuration modified. save ok? (y/n):y
```

ワンポイント

●VPN以外はインターネット接続を行うためには手順6で、以下のコマンドを設定します。

conf#vpnselector add id=64
dest=all src=all type=bypass

VPNの設定

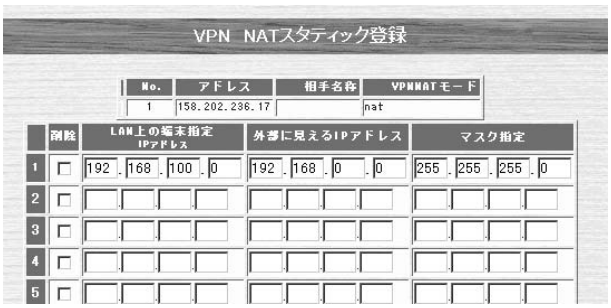
VPNを使用したNATスタティック機能

VPN上ではNATスタティックを使用し、VPNを使用しない（インターネット接続等）ではNAT+を使用するようなケースでは、VPNピア毎にNATスタティック登録を行い、制御することができます。

VPN上でのNATスタティック機能を設定するには、VPN設定画面で「VPN NATスタティック登録」を選択し、設定します。VPN設定画面への移行手順は、P2-16を参照してください。

1 NATスタティックを使用するVPNピアを選択します。

2 NATスタティック設定をします。



NATスタティックの設定方法については、P2-82を参照してください。

設定例1　外部からの接続抑制

FITELnet-F40は、telnetやFTP、Webからの設定で装置にアクセスすることができますが、悪意のあるユーザは、この機能を利用してLANへのアクセスを試みる場合があります。
この不正アクセスを防ぐのがアクセス制御機能です。
不正アクセスフィルタリングには、2種類の機能があります。
（1）アクセスを許可するインタフェースまたはIPアドレスを指定。
（2）パスワードを指定回数以上間違えたときにはアクセス拒否。
（2）のケースが起こったときは、電子メール通知機能により管理者にメールで通知します。（☛P2-98）

＜Webブラウザ操作＞

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

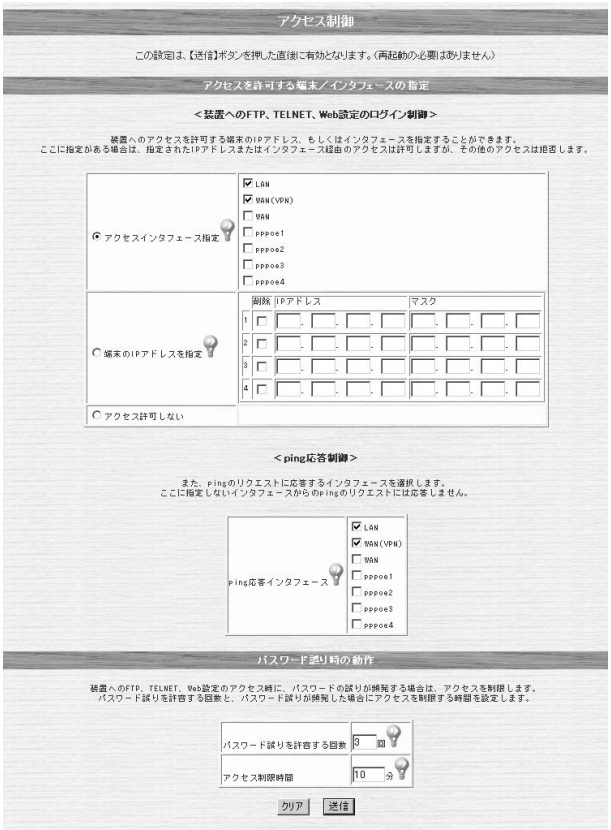
変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［アクセス制御］をクリックします。

〈次ページへ続く〉

6 アクセスを許可する端末／インタフェースの指定を設定します。



＜装置へのFTP、telnet、Web設定のログイン制御＞

- **［アクセスインタフェース指定］**
  インタフェースで装置へのアクセスを制御する場合に、アクセスを許可するインタフェースを選択します。
- **［端末のIPアドレスを指定］**
  送信元端末のIPアドレスで装置のアクセスを制御する場合に、アクセスを許可する端末のIPアドレスを入力します。
- **［アクセス許可しない］**
  リモートアクセスを許可しない場合に選択します。

＜ping応答制御＞

pingのリクエストに応答するインタフェースを選択します。

ワンポイント

●登録済みの端末のIPアドレスを削除するには

手順6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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

〈次ページへ続く〉

＜パスワード誤り時の動作＞

装置へのアクセス時にパスワード誤りが発生する場合は、その端末からのアクセスを制限します。

- **［パスワード誤りを許容する回数］**
  FITELnet-F40へのアクセスに対して、パスワード誤りを許可する回数を指定します。ここで設定した回数以上のパスワード誤りがあった場合、一定時間その端末からのアクセスは拒否します。
- **［アクセス制限時間］**
  指定した回数のパスワード誤りが起こった場合、ここで設定した時間、その端末からのアクセスを拒否します。

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。

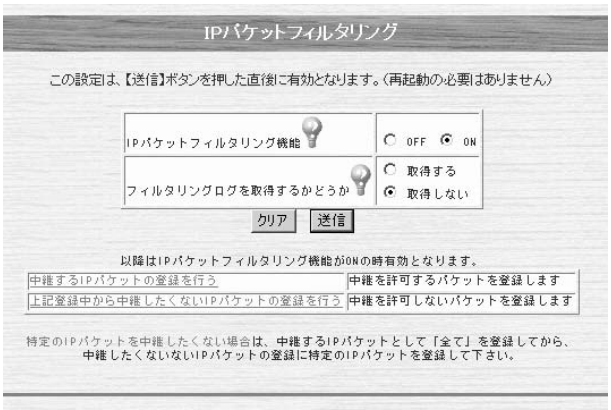
設定例2　IPパケットフィルタリング

中継用・遮断用それぞれに、宛先IPアドレス、送信元IPアドレス、プロトコルを指定して、その条件に合ったデータを中継または遮断するように設定することができます。中継用は32件、遮断用は16件まで設定できます。

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 ［IPパケットフィルタリング］をクリックします。

3 IPパケットフィルタリング機能を使うときは、［ON］をクリックします。また、フィルタリングログを取得するかどうかを選択します。選択した後、［送信］をクリックします。



- **［フィルタリングログを取得するかどうか］**
  IPパケットフィルタリング機能により廃棄されたパケットに関するログを表示するかどうかを選択します。

4 中継するIPパケットまたは遮断するIPパケットを登録します。

- **中継するIPパケットの登録を行う（☛P2-62）**
- **上記登録中から中継したくないIPパケットの登録を行う（☛P2-63）**

5 中継または遮断するIPパケットの登録が終わったら、［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。

ワンポイント

●フィルタリングログを見るには（☛P4-27）

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

中継するIPパケットの登録を行う

中継するIPパケットを登録します。32件まで登録できます。この機能はIPパケットフィルタリング機能がONのときに有効です。特定のIPパケットだけを遮断するときは、ここではすべてのIPパケットを中継するように登録し、中継したくないIPパケットだけを別途登録してください。（☞P2-63）

1 IPパケットフィルタリング画面（☞P2-61）で、［中継するIPパケットの登録を行う］をクリックします。

2 中継するIPパケットを設定します。

- **［パケット送信元指定］**
  中継するパケットの送信元のIPアドレス、IPアドレスマスク、ポート番号を入力します。
- **［パケット受信先指定］**
  中継するパケットの宛先のIPアドレス、IPアドレスマスク、ポート番号を入力します。
- **［プロトコル］**
  中継する指定プロトコルを選択します。任意を選択したときは、0～255の範囲でプロトコルを指定してください。
- **［インタフェースの指定:受信］**
  中継する受信インタフェースを選択します。
- **［インタフェースの指定:送信］**
  中継する送信インタフェースを選択します。

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。

ワンポイント

●登録済みの中継するIP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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

簡易ファイアウォール機能

中継しないIPパケットの登録を行う

中継の対象となっているIPパケットのうちで遮断するIPパケットを登録します。16件まで登録できます。この機能はIPパケットフィルタリング機能がONのときに有効です。

1 IPパケットフィルタリング画面（☛P2-61）で［上記登録中から中継したくないIPパケットの登録を行う］をクリックします。

2 遮断するIPパケットを設定します。

- **［パケット送信元指定］**
  遮断するパケットの送信元のIPアドレス、IPアドレスマスク、ポート番号を入力します。
- **［パケット受信先指定］**
  遮断するパケットの宛先のIPアドレス、IPアドレスマスク、ポート番号を入力します。
- **［プロトコル］**
  遮断する指定プロトコルを選択します。任意を選択したときは、0～255の範囲でプロトコルを指定してください。
- **［インタフェースの指定:受信］**
  遮断する受信インタフェースを選択します。
- **［インタフェースの指定:送信］**
  遮断する送信インタフェースを選択します。

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。

ワンポイント

●**登録済みの中継しないIP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。

お知らせ

この設定は、［送信］をクリックした直後に有効となります。（再起動の必要はありません。）したがって、［送信］をクリックした瞬間Web設定ができなくなることがありますので注意してください。

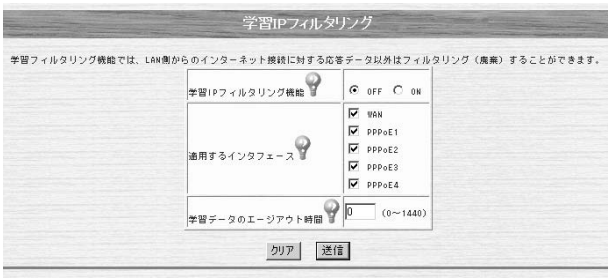
設定例3　学習フィルタリング

FITELnet-F40では、常にインターネットに接続しており、セキュリティとしては危険な状態に常にさらされています。
学習フィルタリング機能では、LAN側からのインターネット接続に対する応答データ以外はフィルタリング（廃棄）することができます。
学習フィルタリング機能を使用する場合は、外部からのアクセス（Web等）はできなくなります。（アクセスを許可するアドレスを限定することはできます）
ただし、VPNからの受信に関してはフィルタリングを行いません。

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 ［学習フィルタリング］をクリックします。

3 学習フィルタリング機能を設定します。



- **［学習IPフィルタリング機能］**
  学習フィルタリング機能を使用するかどうかを設定します。
- **［適用するインタフェース］**
  学習フィルタリング機能を適用するインタフェースを選択します。
- **［学習データのエージアウト時間］**
  学習したデータを覚えておく時間を設定します。ここで設定した時間以上、そのアドレスからのデータがなければ、そのアドレスからの中継は廃棄します。

〈次ページへ続く〉

4 必要に応じてWAN→LANへの中継を許可するWAN側の装置のIPアドレスを設定します。

- **[IPアドレス]**
  WAN→LANへの中継を許可するWAN側の装置のIPアドレスを設定します。
- **[サブネットマスク]**
  WAN→LANへの中継を許可するWAN側の装置を範囲指定する場合に、マスク値を設定します。

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。

6 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

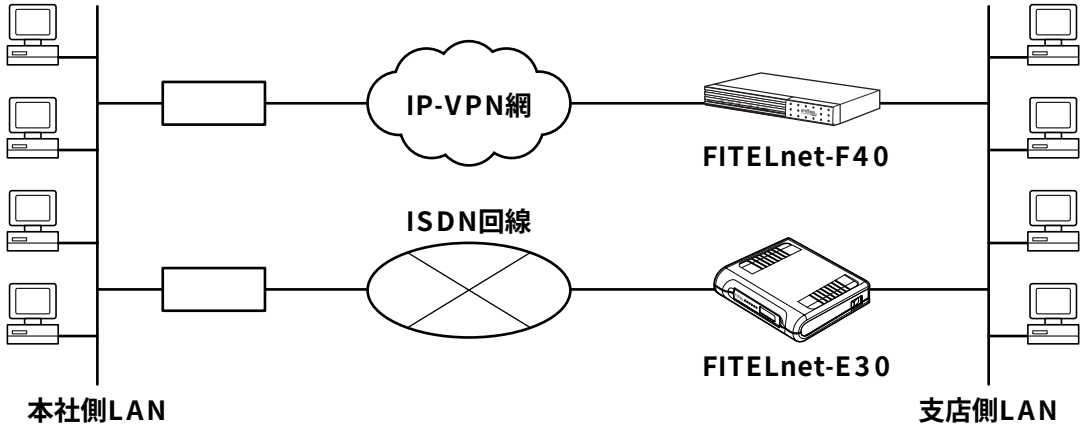
ワンポイント

●VPNを使用する場合
FITELnet-F40をResponderとして使用する場合は、このテーブルにVPNピアのIPアドレスを登録しておく必要があります。

冗長機能

接続しているADSL/CATVインターネットや、IP-VPN網に障害が発生したり、FITELnet-F40自身が動作できない（コンセントが抜けてしまった等）状態になった場合に、同じLANに接続しているFITELnet-E30を使用して、運用を継続できる機能を、冗長機能といいます。

冗長機能は、以下のような形態で利用します。



支店側LANから本社側LANへは、通常FITELnet-F40を経由して通信を行うが、IP-VPN網に問題があったり、FITELnet-F40に障害が発生して通信できないような場合は、FITELnet-E30に経路を切り替え、ISDN経由で本社LANに接続する。

FITELnet-F40の冗長機能は、
・ルータグループ化機能
・Layer3監視機能
の2種類があり、組み合わせて使用できます。

お知らせ

- 上記の構成ではFITELnet-E30でNAT機能を必要とするため、本社側からの契機によるバックアップを行うことはできません。
- ルータグループ化機能ではFITELnet-F40に障害が発生した場合のバックアップができます。IP-VPN網内の障害等経路上の問題に関してもバックアップを行う場合は、Layer3監視機能の設定も併せて行います。（☛P2-69）

冗長機能

ルータグループ化機能

FITELnet-F40とFITELnet-E30を同一LAN上に配置し、バックアップ経路として使用するためには、双方のルータがルータグループを確立している必要があります（ルータグループ化機能）。
ルータグループ化機能は、以下のように設定します。

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 ［冗長機能］をクリックします。

3 ルータグループ化機能をONを選択し、［送信］をクリックした後、［ルータグループ化機能の設定］をクリックします。

〈次ページへ続く〉

4 ルータグループ化機能の各項目を設定します。

- **[グループ内の優先度]**
  ルータグループを形成する場合の、優先度を設定します。値が小さいほど優先度は高くなります。FITELnet-F40をマスタールータとして使用する場合は、ルータグループを形成する他のルータ（FITELnet-E30）より、優先度を高くします。
- **[宛先UDPポート番号]**
  ルータグループを形成するルータどうしで交換するデータが使用するUDPポート番号を指定します。ルータグループを形成するルータどうしでは、同じポート番号になるように設定します。
- **[代表IPアドレス]**
  グループのIPアドレスを設定します。このアドレスは、LANのサブネットに属し、どの端末も使用していないIPアドレスを設定します。またルータグループを形成するルータどうしでは、同じIPアドレスを設定します。
  LAN上のPCで、FITELnet-F40をデフォルトゲートウェイにしたい場合は、FITELnet-F40のLANに設定したIPアドレスではなく、ここで設定する代表IPアドレスをデフォルトゲートウェイに設定してください。
- **[グループ内共有データの送信間隔]**
  ルータグループ内で共有するデータの送信間隔を設定します。グループを形成している他のルータの待ち時間よりも、短い間隔とします。
- **[グループ内のルータを異常とみなすまでの時間]**
  ルータグループ内で共有するデータを受信しなかった場合、そのルータを異常とみなすまでの時間を設定します。グループを形成している他のルータの送信間隔より、長い時間を設定します。

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。

6 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

冗長機能

Layer3監視機能

宛先までの経路を監視することで、IP-VPNサービスのようなベストエフォート型ネットワークにおいても途中経路障害を検出できます。ルータグループ化機能と組み合わせることにより、FITELnet-E30でバックアップし、通信を継続することができます。
Layer3監視機能は、以下のように設定します。

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 ［冗長機能］をクリックします。

3 Layer3監視機能を使用するを選択し、［送信］をクリックした後、［経路監視先の登録(Layer3監視機能)］をクリックします。

〈次ページへ続く〉

お知らせ

Layer3監視機能だけでは、冗長機能を実現できません。ルータグループ化機能の設定も併せて行ってください。
(☛P2-67)

4 Layer3監視機能の各項目を設定します。

- **[Layer3監視を行う宛先IPアドレス（必須)]**
  監視する宛先のIPアドレスを設定します。目的のサーバのIPアドレスなどを設定します。(ルータである必要はありません)
- **[Layer3監視パケットの定期送信間隔]**
  監視パケットを送信する間隔を設定します。(秒単位)
- **[経路異常時の、Layer3監視パケット送信間隔]**
  監視パケットが戻ってこないため経路異常と判断している場合の、監視パケットの送信間隔を設定します。(秒単位)
- **[障害と判断するまでの時間]**
  監視パケットの戻りがない場合に経路異常と判断するまでの時間を設定します。
- **[障害復旧と判断するまでの時間]**
  経路異常中に監視パケットの戻りがあり経路復旧と判断するまでの時間を設定します。
- **[経路が異常となった場合の接続先IPアドレス]**
  バックアップルータがISDN回線を接続する際の接続先ルータのIPアドレスを設定します。
- **[Layer3監視パケットの送信元IPアドレス]**
  Layer3監視パケットを送信するときに送信元アドレスとしてLAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するWANインタフェースのIPアドレス）をつけて送信するかを選択します。
- **[バックアップ対象パケット（必須)]**
  この経路監視において経路異常と判断された場合に、FITELnet-E30でバックアップすべきパケットの宛先アドレスを指定します。IPアドレス、サブネットマスクにそれぞれ0.0.0.0を入力した場合は全てのパケットが対象となります。

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。

6 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

マルチルーティング機能

本装置では、PPPoEのセッションを同時に4セッション確立することができます。したがって、4つのプロバイダを同時に利用することができます。
※契約しているPPPoEが、複数セッション接続に対応している必要があります。
FITELnet-F40では、電子メールはこのプロバイダ／Webはこのプロバイダのように、アプリケーションによりプロバイダ（PPPoE）を分けたり、LAN上のこの端末はこのプロバイダ／別の端末は別のプロバイダのように、発信端末ごとにプロバイダ（PPPoE）を分けてルーティングすることができます（マルチルーティング機能）

マルチルーティング機能を使用するためには、
（1）発信端末のIPアドレスもしくは宛先ポート番号（アプリケーション）と、中継先を指定
（2）（1）で指定した中で、特別に通常ルーティングする発信端末のIPアドレスもしくは宛先ポート番号（アプリケーション）を指定
の2項目を設定する必要があります。

マルチルーティング機能の設定

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［マルチルーティング機能］をクリックします。

6 マルチルーティング機能で［ON］を選択し、［送信］をクリックします。

マルチルーティング機能

発信端末／宛先ポート番号の指定

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 ［マルチルーティング機能］をクリックします。

3 ［マルチルーティングするデータの登録］をクリックします。

4 マルチルーティングするデータを登録します。

- **［送信元指定（必須）］**
  発信端末のIPアドレスもしくは宛先ポート番号（アプリケーション）を指定します。
- **［宛先指定］**
  パケットの宛先IPアドレスまたはURLを指定します。
- **［中継先指定（必須）］**
  指定した送信元指定のデータの中継先を指定します。
- **［プリファレンス］**
  データが複数のエントリにマッチした場合に、どのマルチルーティングテーブルを使用するかの優先度を指定します。数値の小さいほうが優先度が高くなります。

5 ［送信］をクリックします。

お知らせ

宛先指定（URL）でマルチルーティングを行う場合、簡易DNSを必ず使用する設定にしてください。（☛P2-92）

マルチルーティングしない発信端末／宛先ポート番号の指定

発信端末／宛先ポート番号の指定（☛P2-72）で、マルチルーティングするデータとして登録した中で、特別に通常ルーティングさせたいデータを登録します。
例）端末Aからのデータはマルチルーティングするが、Aからのメールだけは通常ルーティングしたい
→Aからのメールというエントリを登録

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 ［マルチルーティング機能］をクリックします。

3 ［マルチルーティング適応外データの登録］をクリックします。

- **［送信元アドレス］**
  マルチルーティングを適応しない発信端末のIPアドレスもしくは宛先ポート番号（アプリケーション）を指定します。
- **［宛先指定］**
  マルチルーティングを適応しないパケットの宛先IPアドレスまたはURLを指定します。

〈次ページへ続く〉

お知らせ

宛先指定（URL）でマルチルーティングを行う場合、簡易DNSを必ず使用する設定にしてください。（☛P2-92）

4 ［送信］をクリックします。

5 装置を再起動します。

SNMPエージェント機能

ネットワークに接続されたSNMPエージェント（SNMP Agent）の状態を、SNMP（Simple Network Management Protocol）マネージャがネットワーク経由で監視するためのプロトコルです。
LAN上のSNMPマネージャから、本装置の状態を監視することができます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［SNMPエージェント］をクリックします。

〈次ページへ続く〉

SNMPエージェント機能

6 SNMPエージェント機能を設定します。

- **[SNMPエージェント機能]**
  SNMPエージェント機能を使用するかどうかの設定です。
- **[認証失敗トラップ]**
  コミュニティ名が正しくなかったり、登録していないマネージャからのSNMP要求があった場合、それをトラップとしてマネージャに通知するかどうかを設定します。
- **[SNMPマネージャのIPアドレス]**
  SNMPマネージャのIPアドレスを登録します。
- **[コミュニティ名]**
  SNMPマネージャと通信する場合のコミュニティ名を、最大32文字で設定します。
- **[トラップ]**
  SNMPマネージャにトラップを送信するための設定です。
- **[送信元IPアドレス]**
  送信元アドレスとして、LAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。

7 [送信] をクリックします。

8 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みのSNMPマネージャのIPアドレスを削除するときは

手順6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。

NAT機能

NAT（Network Address Translation）は、ネットワーク内のプライベートIPアドレスと、インターネット接続できる本来のIPアドレスを相互に変換します。これにより、ネットワーク内でローカルなIPアドレスが割り当てられているコンピュータから、直接インターネットに接続することができる機能です。
FITELnet-F40では、NAT（1対1変換）と、NAT+（1対多）変換をサポートしています。
NAT+では、複数のLAN端末を、1つのアドレスに変換して通信します。この機能により、ADSL／CATVインターネットに、複数のパソコンから接続することができます。
NATの各種設定は、WAN（DHCP）およびPPPoE4セッション毎に設定します。
設定時はまず設定するインタフェースを選択してから各種設定を行ってください。

NATモードの場合の必須設定

NATモードで使用する場合は、NAT変換範囲を必ず設定してください。以下に設定方法を説明します。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそFITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

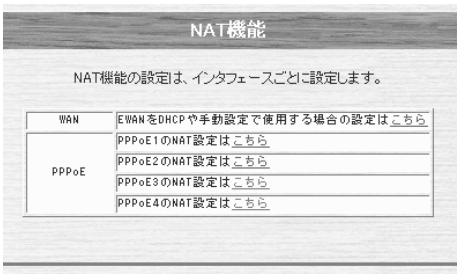
3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［NAT機能］をクリックします。

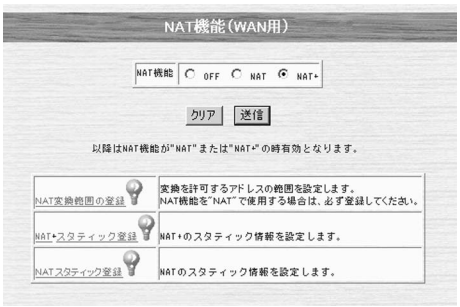
6 設定するインタフェースを指定します。



〈次ページへ続く〉

NAT機能

7 NAT機能の［NAT］を選択し、［送信］をクリックします。



8 [NAT変換範囲の登録]をクリックします。

- **［NAT変換範囲の登録］**
  NAT機能でNATを選択した場合、NATで変換するWAN側アドレス（グローバルアドレス）の範囲を設定します。先頭のグローバルアドレスは、NAT+変換用に保持され、変換用のIPアドレスが残り１つになった場合に使用します。

9 ［送信］をクリックします。

10 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、［装置の再起動］をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

ワンポイント

●登録済みのNAT変換範囲を削除するときは

手順8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。

お知らせ

グローバルアドレスの個数より、LAN側の端末数が多い場合は、ＮＡＴ変換とNAT+変換を併用します。

例）LAN側の端末数：254台

取得したグローバルアドレスの個数：8（うち2個は使用できない）のケースでは、1～5番目に外部へアクセスしようとした端末はNAT変換（1対1変換）されます。6台目以降の端末から、外部へのアクセス要求があった場合は、残り1つのグローバルアドレスでNAT+変換（1対多変換）されます。

設定例1　NAT+を使用してWebサーバを公開する

例）ここでは、グローバルアドレスを1つだけ取得して内部の192.168.0.100のWebサーバを外部に公開する場合の設定を説明しています。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［NAT機能］をクリックします。

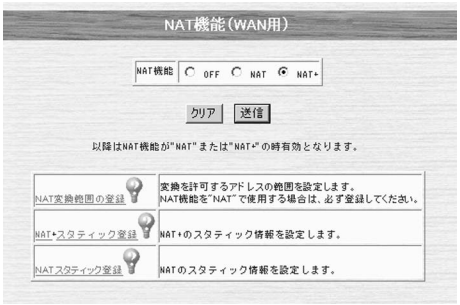
6 設定するインタフェースを指定します。

〈次ページへ続く〉

お願い

内部のサーバを公開することは、同時にセキュリティホールをつくることになりますので、本装置およびサーバのセキュリティには十分にご注意ください。

7 NAT機能の［NAT］を選択し、［送信］をクリックします。



8 ［NAT⁺スタティック登録］をクリックします。

- **［NAT⁺スタティック登録］**
  内部にあるサーバを、外部に公開するような場合に指定します。例えば、内部のWebサーバ（192.168.0.100）を公開する場合に、LAN上の端末指定：192.168.0.100/80、外部に見えるIPアドレスとポート番号：WAN側から配布されたIPアドレスを使用する/80　と設定することにより、公開することができます。

9 LAN上の端末を指定します。

IPアドレス「192.168.0.100」、ポート番号「80」と入力します。

- **［LAN上の端末指定］**
  NAT⁺変換する際の、プライベート側（LAN側）のIPアドレス／ポート番号を指定します。

〈次ページへ続く〉

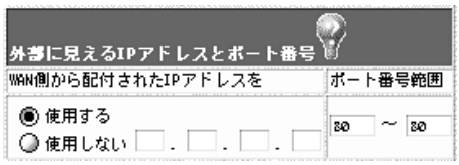
ワンポイント

●登録済みのNAT⁺スタティック登録を削除するときは

手順8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。

10 外部に見えるIPアドレスとポート番号を指定します。

外部に見えるIPアドレスは［使用する］をチェックし、ポート番号範囲を［80～80］と入力します。



- **［外部に見えるIPアドレス］**
  NAT+変換する際の、パブリック側（WAN側）のIPアドレス／ポート番号を指定します。PPPoEやDHCPで、自動的に割り当てられたIPアドレスに変換するかどうか、および変換後のポート番号を指定してください。

11 ［送信］をクリックします。

12 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、［装置の再起動］をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

設定例2　NATを使用してWebサーバ／FTPサーバを公開する

例）ここでは、グローバルアドレスを8つ（xxx.xxx.xxx.0～xxx.xxx.xxx.7）取得して、内部の192.168.0.100のWebサーバ／192.168.0.200のFTPサーバを公開する場合の設定を説明しています。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそFITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。
簡単設定の設定画面が表示されます。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［NAT機能］をクリックします。

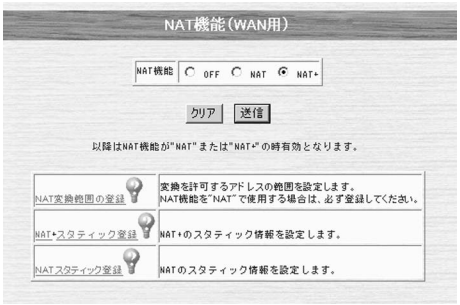
6 設定するインタフェースを指定します。

〈次ページへ続く〉

お願い

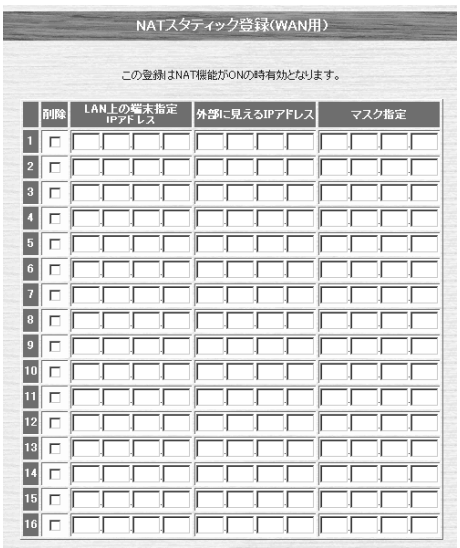
NATスタティック登録を使用する場合、登録した端末は、外部からのアクセスを完全に許可しますので、セキュリティには充分にご注意ください。

7 NAT機能の［NAT］を選択し、［送信］をクリックします。



8 ［NATスタティック登録］をクリックします。

- **［NATスタティック登録］**
  複数のグローバルアドレスが割り当てられている形態で、内部にあるサーバを、外部に公開するような場合に指定します。
  例えば、内部のWebサーバ（192.168.0.100）を公開する場合に、LAN上の端末指定：192.168.0.100、外部に見えるIPアドレス：xxx.xxx.xxx.1 と設定することにより、xxx.xxx.xxx.1のアクセスは、192.168.0.100に変換します。



〈次ページへ続く〉

この例では、
　LAN側：192.168.0.100、外部に見えるIPアドレス：xxx.xxx.xxx.1、マスク指定：255.255.255.255
　LAN側：192.168.0.200、外部に見えるIPアドレス：xxx.xxx.xxx.2、マスク指定：255.255.255.255
と設定することで、Webサーバ、FTPサーバを公開することができます。
マスク指定を利用すると、複数のNATスタティックエントリを1つのエントリで指定することができます。
　LAN側：192.168.0.0／255.255..255.0
　　↓
外部に見えるIPアドレス：XXX.XXX.XXX.0／255.255.255.0
（192.168.0.0→XXX.XXX.XXX.0、192.168.0.2→XXX.XXX.XXX.2 ‥‥192.168.0.255→XXX.XXX.XXX.255）

9 ［送信］をクリックします。

10 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、［装置の再起動］をクリックします。
［装置を再起動する］をチェックしてから、［送信］をクリックします。

ワンポイント

●登録済みのNATスタティック登録を削除するときは
手順8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。

DHCPリレーエージェント機能

LAN上のDHCPクライアントからの要求を、WAN側にリレーし、WAN側のDHCPサーバから割り当ててもらう機能です。
本社側で、支店のLAN側のIPアドレスを一括で管理する場合に有効な機能です。
DHCPリレーエージェント機能と、DHCPサーバ機能を併用することはできません。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから[便利な設定］をクリックします。

5 [DHCPリレーエージェント機能］をクリックします。

〈次ページへ続く〉

DHCPリレーエージェント機能

6 DHCPリレーエージェント機能を設定します。

- **[DHCPリレーエージェント機能]**
  DHCPリレーエージェント機能を使用するかどうかを設定します。DHCPサーバ機能も使用すると設定されていた場合は、DHCPリレーエージェント機能が優先になります。（DHCPサーバ機能は動作しない）
- **[DHCPサーバリスト]**
  DHCPサーバを登録します。
- **[送信元IPアドレス]**
  DHCPリレーエージェント機能を使用する際に、送信元アドレスとしてLAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するWANインターフェースのIPアドレス）をつけて送信するかを選択します。
- **[DHCPサーバまでの最大ホップ数]**
  DHCPリレーエージェント機能を使用する場合に、リレーを許可する最大ホップ数を設定します。登録しているDHCPサーバが、このホップ数以上のネットワークに存在する場合は、有効になりません。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みのDHCPサーバリストを削除するには

手順6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。

DHCPサーバ機能

本装置に接続している端末に対して、自動的にIPアドレスを割り付けるかどうかを設定します。自動的にIPアドレスを割り付けない場合は、各端末それぞれに手動でIPアドレスを割り付けてください。
DHCPサーバ機能が「on」の時、DHCPアロケート開始アドレス（配布先端末の指定で指定されたIPアドレス）から始まり、DHCPアロケート数（割り付け可能なIPアドレスの個数）分のIPホストアドレスを割り付けます。
DHCPアロケートアドレスが 0.0.0.0 の場合は、LANインタフェースに設定されたIPアドレスが属するネットワーク番号内の最初のホストアドレスからDHCPアロケート数で示される分のIPホストアドレスを割り付けます。
「IPアドレス」が割り付け可能かどうかはARPによりチェックします。（ARPの応答がタイムアウトした内容を配信可能アドレスとします。）

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから[便利な設定］をクリックします。

5 [DHCPサーバ機能］をクリックします。

〈次ページへ続く〉

DHCPサーバ機能

6 本装置のDHCPサーバ機能を使用する場合は、[ON]をチェックします。

7 DHCPサーバの動作と配信データの設定をします。

- **[配付IPアドレスの開始値]**
  配付IPアドレスの開始値を、LANインタフェースのIPアドレスの次から開始するのか、または指定したIPアドレスから開始するのかを選択します。指定したIPアドレスから開始するときは、IPアドレスを入力してください。
- **[割り当てるIPアドレスの個数]**
  IPアドレスを割り当てる個数を、1～255の範囲で指定します。この個数が、同時に使用できるDHCPクライアント端末の個数となります。
- **[デフォルトゲートウェイの通知]**
  DHCPサーバを利用する時、LANインタフェースのアドレスをデフォルトゲートウェイとして通知するかどうかを選択します。
- **[ドメイン名称の通知]**
  ドメイン名称を通知するかどうかを選択します。通知するときは、ドメイン名称を半角英数字40文字以内で入力してください。
- **[WINSアドレスの通知]**
  WINSアドレスを通知するかどうかを選択します。通知するときは、NetBIOSサーバのIPアドレスを入力します。最大2件まで登録できます。
- **[リース期限]**
  IPアドレスの貸出し期限を設定します。
- **[ネームサーバアドレスの通知]**
  ネームサーバアドレスを通知するかどうかを選択します。通知する場合は、通知するIPアドレス（プライマリ・セカンダリ）を入力します。しないを選択した場合でProxyDNS機能を使用する場合は本装置のLAN側アドレスを通知します。

8 [送信]をクリックします。

DHCPサーバ機能の設定はこれで完了ですが、MACアドレスとIPアドレスの組み合わせを設定する場合は、次の手順にすすんでください。

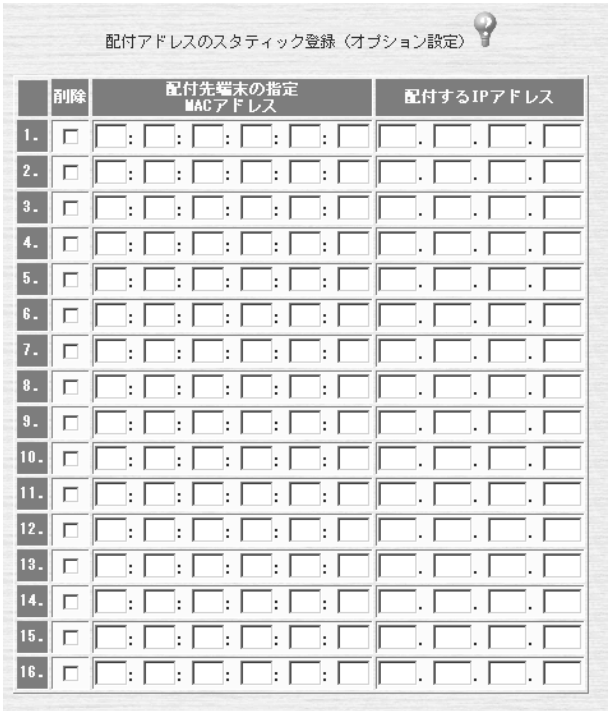
〈次ページへ続く〉

お知らせ

- ●DHCPにより、DNS（ドメインネームサーバ)のIPアドレスを配布できます。DNSのアドレスは、簡単設定で設定してください。
- ●DHCPサーバを使用するにはサーバからIPアドレスを取得する設定が、クライアント側に必要です。

9 配布アドレスのスタティック登録をします。

最大16件まで登録することができます。



- **[配付先端末の指定]**
  配付先の端末を指定するためにMACアドレスを入力します。
- **[配付するIPアドレス]**
  端末に対して割り付けるIPアドレスを入力します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みの配布アドレスリストを削除するときは

手順9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。

Syslogの送信

Syslogを指定先に送信するかどうかを設定します。Syslogサーバと送信するログの種類を設定することができます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［syslogの送信］をクリックします。

6 syslogの送信を設定します。

〈次ページへ続く〉

Syslogの送信

- **[syslogの送信]**
  syslogを送信するかどうかを選択します。
- **[syslogを受け取る端末のIPアドレス]**
  本装置が送信するsyslogを受信するsyslogサーバのIPアドレスを設定します。
- **[tlog(errレベル)で送信]**
  syslog機能を使用して、errレベルでtlogを送信するかどうかを選択します。
- **[elog(warningレベル)で送信]**
  syslog機能を使用して、warningレベルでelog(エラーログ)を送信するかどうかを選択します。
- **[llog(infoレベル)で送信]**
  syslog機能を使用して、infoレベルでllog(LAN・WAN回線の状況)を送信するかどうかを選択します。
- **[vlog(infoレベル)で送信]**
  syslog機能を使用して、infoレベルでvlog（イベントログ）を送信するかどうかを選択します。
- **[vpnlog（infoレベル）で送信]**
  syslog機能を使用して、infoレベルでvpnlog（VPN情報）を送信するかどうかを選択します。
- **[clog（noticeレベル）で送信]**
  syslog機能を使用して、noticeレベルでclog（送受信ログ）を送信するかどうかを選択します。
- **[flog（noticeレベル）で送信]**
  syslog機能を使用して、noticeレベルでflog（フィルタリングログ）を送信するかどうかを選択します。
- **[ファシリティ値]**
  syslogで通知する場合のファシリティ値を設定します。この設定は、受信するサーバ側と設定があっている必要があります。
- **[送信元アドレス]**
  syslogを送信するときに、送信元アドレスとしてLAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

簡易DNS機能

DNSサーバ機能は、数字の羅列で表されていつIPアドレスを、覚えやすいドメイン名に置き換えることができる機能です。ユーザーは、本装置を経由することにより、ドメイン名でIPアドレスを持つサーバにアクセスできるようになります。
FITELnet-F40は、DNSサーバ機能をサポートしていませんが、DNS簡易サーバ機能により、DNSサーバのように動作させることができます。
LAN上のパソコンに、あたかも本装置がDNSサーバであるかのように動作し、パソコンからのDNSのリクエストを、最適なDNSサーバへリクエストし直します。

設定例1　簡易DNS

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 簡単設定のDNSサーバで簡易DNS機能の［使用する］をチェックします。

DNSサーバのプライマリ、セカンダリには、プロバイダから通知されたアドレスを入力してください。通知がない場合には、空欄のままにしてください。
PPPoEやDHCPでDNSサーバのアドレスを学習した場合は、そちらを優先します。

5 ［登録する］をクリックします。

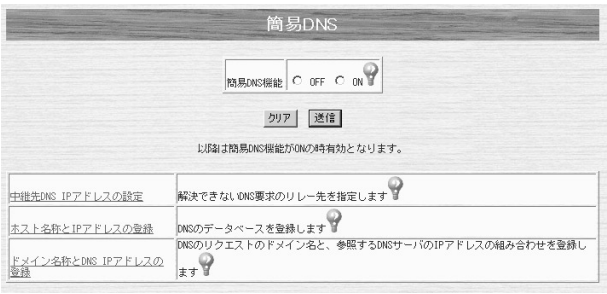
6 画面左側のメニューから［便利な設定］をクリックします。

7 ［簡易DNS］をクリックします。

〈次ページへ続く〉

簡易DNS機能

8 [中継先DNS IPアドレスの設定] をクリックします。



- **[中継先DNS IPアドレスの設定]**
  簡易DNSを使用する場合、通常はPPPoEやDHCPで学習したDNSへリクエストしなおしますが、学習できなかった場合、ここで設定したDNSアドレスにリクエストしなおします。

9 中継先DNS IPアドレスを設定します。

- **[応答パケット待ち時間]**
  DNSのリクエストをしなおしてから、応答パケットを受信するまでの待ち時間を設定します。ここで設定した時間応答パケットを受信しなかった場合は、設定した再送回数再送した後、セカンダリDNSサーバにリクエストしなおします。セカンダリDNSサーバでもタイムアウトした場合は、ホストに解決できないことを通知します。
- **[再送回数]**
  DNSのリクエストをしなおした後、応答パケット待ち時間応答がなかった場合、ここに設定した回数再送します。
- **[送信元アドレス]**
  送信元アドレスとして、LAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

設定例2　ドメイン名によるDNSの振り分け

DNSのリクエスト内のドメインにより、リクエストし直すDNSを振り分けることができます。

例）「*.furukawa.co.jp」のリクエストは「158.xxx.xxx.100（セカンダリ　158.xxx.xxx.101）」のDNSサーバに問い合わせる。また、「www.furukawa.co.jp」や「ftp.furukawa.co.jp」のような端末のアドレスを探すDNSのリクエストに対しては「158.xxx.xxx.100」にリクエストし直すケースの設定例です。**

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

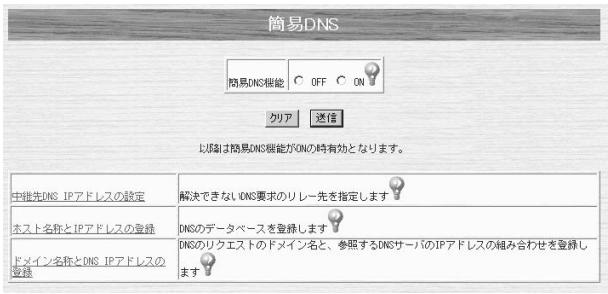
変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［簡易DNS］をクリックします。

〈次ページへ続く〉

6 [ドメイン名称とDNS IPアドレスの登録] をクリックします。



- **[ドメイン名称とDNS IPアドレスの登録]**
  リクエスト中のドメイン名により、どのDNSサーバに問い合わせるかのエントリを登録します。
  例えば、furukawa.co.jp／xxx.xxx.xxx.xxxというエントリを登録した場合、host.furukawa.co.jpのリクエストがあった場合は、xxx.xxx.xxx.xxxにリクエストしなおします。

7 ドメイン名称とDNS IPアドレスを登録します。

ドメイン名称［furukawa.co.jp］、DNS IPアドレス（プライマリ）［158.xxx.xxx.100］を入力します。

8 [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。

9 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

ワンポイント

●登録済みのドメイン名称を削除するときは

手順7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。

設定例3　ホスト名称とDNS IPアドレスの登録

DNSのデータベースを登録することができます。頻繁にアクセスするホームページのURLとIPアドレスを登録しておくと便利です。
例）ここでは、URL「www.furukawa.co.jp」、IPアドレス「203.192.162.36」を登録します。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

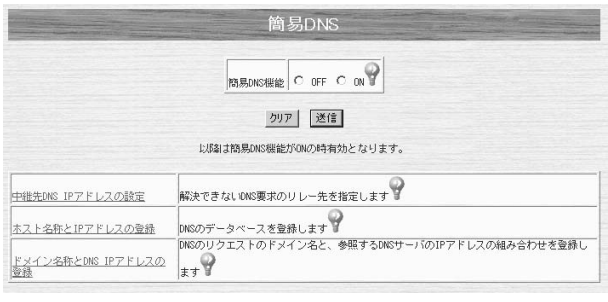
3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［簡易DNS］をクリックします。

6 ［ホスト名称とDNS IPアドレスの登録］をクリックします。



〈次ページへ続く〉

7 ホスト名称とDNS IPアドレスを登録します。

ホスト名称［www.furukawa.co.jp］、IPアドレス（プライマリ）［203.192.162.36］を入力します。

8 ［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。

9 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、［装置の再起動］をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

ワンポイント

●登録済みのドメイン名称を削除するときは

手順7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。

電子メール通知機能

FITELnet-F40は、不正アクセスがあった場合およびLayer3監視機能で監視先がエラー／復旧した場合に、管理者宛てに電子メールを利用して通知する機能をサポートしています。

例）不正アクセスを、「admin@home.ne.jp」に電子メールで通知する場合の設定です。メールサーバは「xxx.xxx.xxx.xxx」で、差出人はFITELnet-F40とし、電子メールが届けられない場合には「error@home.ne.jp」にエラーメールを送らせます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［電子メール通知］をクリックします。

〈次ページへ続く〉

電子メール通知機能

6 電子メールの通知を設定します。

［送信先メールアドレス］に電子メールが送られ、失敗したときには［エラーメール送信先メールアドレス］に送られます。

送信先メールアドレス［admin@home.ne.jp］、エラーメール送信先アドレス［error@home.ne.jp］、SNTPサーバのIPアドレス［xxx.xxx.xxx.xxx］を入力します。

- **［電子メール通知機能］**
  電子メール通知機能を使用するかどうかを選択します。
- **［送信先メールアドレス］**
  電子メールの宛先アドレスを指定します。
- **［エラーメール送信先アドレス］**
  電子メールが送信先メールアドレスに届かなかった場合のエラーメールの送信先アドレスを指定します。
- **［通知内容］**
  電子メールを通知する契機として、「不正アクセスが発覚したとき」「Layer3監視機能で監視先がエラー／エラー復旧したとき」の中から選択します。
- **［SMTPサーバのIPアドレス］**
  SMTPサーバのIPアドレスを指定します。SMTPサーバは2エントリ登録できます。FITELnet-F40は、まず1エントリ目のSMTPサーバにメールを送信し、失敗したら2エントリ目のSMTPサーバにメールを送信します。
- **［送信元メールアドレス］**
  メールのFormに入るアドレスを指定します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、［装置の再起動］をクリックします。［装置を再起動する］をチェックしてから、［送信］をクリックします。

SNTP機能

SNTP（Simple Network Time Protocol）は、NTPプロトコル（インターネットで標準的に利用されている、時刻情報プロトコル）を単純化した時刻情報の転送プロトコルで、本製品は、正確な時刻情報を容易に利用できるSNTPクライアント機能を備えています。

例）タイムサーバ「xxx.xxx.xxx.xxx」に、起動時に時刻を問い合わせ、その後12時間おきに問い合わせる設定をします。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

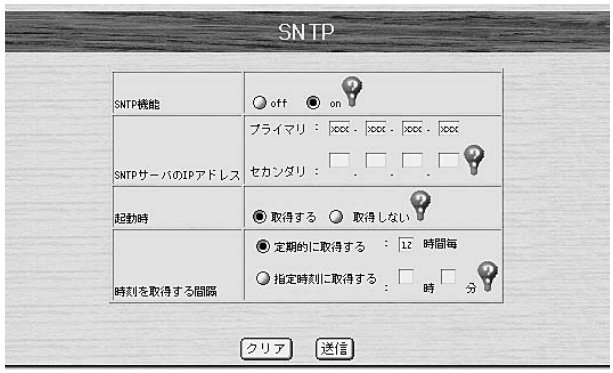
4 画面左側のメニューから［便利な設定］をクリックします。

5 ［SNTP］をクリックします。

〈次ページへ続く〉

6 SNTPを設定します。

SNTP機能の［ON］をチェックし、SNTPサーバのIPアドレス［xxx.xxx.xxx.xxx］、時刻を取得する間隔［12時間毎］を入力します。



- **［SNTP機能］**
  ［ON］をクリックすると、外部のSNTPサーバから現在時刻を取得することができます。
- **［SNTPサーバのIPアドレス］**
  SNTPサーバのIPアドレスを設定します。
- **［起動時］**
  起動時にSNTPサーバに、現在時刻取得の要求を行うかどうかを選択します。
- **［時刻を取得する間隔］**
  SNTPサーバに、現在時刻の要求を行う間隔を設定します。間隔の指定方法は、何時間毎／何時何分のように指定ができます。定期的に時刻の設定を行わない場合は、0時間毎と設定します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、［装置の再起動］をクリックします。
［装置を再起動する］をチェックしてから、［送信］をクリックします。

送受信ログの設定

指定したプロトコル／送信インタフェース（自局送信）／受信インタフェース（自局宛）／中継のデータをログに残すかどうかを設定します。
また、フィルタリングしたパケットをログに残すかどうかを設定します。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［送受信ログの設定］をクリックします。

6 「送受信ログを取得する」を選択し、送受信ログの登録を設定します。

〈次ページへ続く〉

ワンポイント

●送受信ログを見るには（☛P4-26）

送受信ログの設定

- **[自局送信]**
  プロトコル欄にかかれているプロトコルに関して、ログに残す自局からの送信を指定します。例えば、TCPに関して、WANへの送信パケットをログに残す場合は、「WAN」をチェックします。
- **[自局受信]**
  プロトコル欄にかかれているプロトコルに関して、ログに残す自局宛の受信を指定します。例えば、TCPに関して、LANからの受信パケットをログに残す場合は、「LAN」をチェックします。
- **[中継]**
  プロトコル欄にかかれているプロトコルに関して、ログに残す中継インタフェースを指定します。例えば、TCPに関して、LANからWANへの中継パケットをログに残す場合は、「LAN→WAN」をチェックします。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

スタティックルーティング

スタティックルーティングは、パケットを各接続機器へ伝達する制御情報をあらかじめルータに設定しておき、常に固定的なルートを選択する機能です。

ご利用になるLAN環境に複数のネットワークがあるときは、経路情報を設定することができます。WAN側またはLAN側で中継したいパケットを受け取った場合、そのパケットを送り出す先の情報を設定することができます。64件まで登録できます。中継先にはIPアドレス指定の他に、インタフェース指定ができます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［便利な設定］をクリックします。

5 ［スタティックルーティング］をクリックします。

〈次ページへ続く〉

スタティックルーティング

6 スタティックルーティングのルート情報を設定します。

- **[通信先指定]**
  スタティックルーティングの宛先のIPアドレスを入力します。
- **[中継先指定]**
  スタティックルーティングの中継先を指定します。IPアドレス、ISDN接続先指定、インタフェースの指定の中から選択します。
  - **IPアドレス指定**
    IPアドレスを入力することにより、中継先を指定します。
  - **インタフェース指定**
    インタフェースを選択し、中継先インタフェースを選択します。
- **[メトリック]**
  宛先へのメトリック値を設定します。
- **[プリファレンス]**
  他のルーティング情報との優先順位を設定します。プリファレンス値の小さい方が優先順位が高くなります。デフォルト値は、RIP＝100、E-BGP＝70、I-BGP＝170、Aggregateルート＝130です。

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。

ワンポイント

●登録済みのスタティックルーティングを削除するときは
手順6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。

お知らせ

この設定は、[送信]をクリックした直後に有効となります。(再起動の必要はありません。)したがって、[送信]をクリックした瞬間Web設定ができなくなることがありますので注意してください。

Proxy ARP

IPルーティングを使用する場合のProxyARP動作モードに関する設定を行います。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［ProxyARPの設定］をクリックします。

6 ProxyARPの動作モードを選択します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する]をチェックしてから、[送信]をクリックします。

RIPの制御

RIP（Routing Information Protocol）は、データベースに登録された情報により、通信先までの最短経路を選択する機能です。これまでの登録情報（IPアドレス、次のホップ先、ホップ数など）に、RIP2では認証パスワード、サブネットマスクの指定、マルチキャストアドレッシングなどもデータベースに加えられます。

設定例1　RIP送受信制御

IPルーティングを使用する場合のRIPの動作モードに関する設定を行います。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［RIPの制御］をクリックします。

〈次ページへ続く〉

RIPの制御

6 RIPを設定します。

- **[ルーティング方法]**
  RIPを利用したルーティング（ダイナミックルーティング）の動作を選択します。

＜RIP送受信制御＞

- **[RIPの受信]**
  受信するRIPのバージョンを設定します。
- **[RIPの送信]**
  送信するRIPのバージョンを設定します。
- **[RIP2パスワード]**
  RIP2を使用する場合のパスワードを登録します。
- **[定期送信]**
  RIPを定期的に送信する設定です。定期的に送信する場合は、送信間隔を設定します。PPPoEはユニキャスト宛RIP以外送信できません。
- **[RIPエージアウト]**
  学習したRIPを、テーブルから削除する設定です。削除する場合は、削除するまでの時間を設定します。
- **[メトリック]**
  インタフェースのメトリック値を設定します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信]をクリックします。

設定例2　RIPフィルタリング

受信RIPフィルタリングテーブル

RIPフィルタリング機能のフィルタリングを設定します。RIPパケット受信時に有効にする情報を受信インタフェースごとに限定することができます。40件まで設定できます。事前にRIPの制御の設定が必要です。（☞P 2-107）

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［受信RIPフィルタリングテーブル］をクリックします。

6 フィルタリング属性を選択します。

- **［フィルタリング属性］**
  指定したテーブルに一致した情報を有効とするか／一致しない情報を有効とするかを設定します。
  例えば、テーブルに［x.x.x.x］という情報を登録した場合
  …「テーブルに一致した情報を有効とする」と設定した場合は、「x.x.x.x」のみが有効となり、それ以外の情報は無効となります。
  …「テーブルに一致しない情報を有効とする」と設定した場合は、「x.x.x.x」以外の情報が有効となり、「x.x.x.x」の情報は無効となります。

〈次ページへ続く〉

RIPの制御

7 受信RIPフィルタリングテーブルを設定します。

- **[RIPの宛先IPアドレス]**
  受信ルーティング情報のフィルタリングの対象とする宛先IPアドレスを入力します。
- **[アドレスマスク長]**
  宛先IPアドレスに対するマスクパターンを入力します。
- **[受信インタフェース]**
  受信インタフェースを選択します。

8 [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。

9 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する]をチェックしてから、[送信]をクリックします。

ワンポイント

●登録済みの受信フィルタリングテーブルを削除するときは
手順6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。

送信RIPフィルタリングテーブル

RIPフィルタリング機能のフィルタリングを設定します。RIPパケット送信時に有効にする情報を送信インタフェースごとに限定することができます。40件まで設定できます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

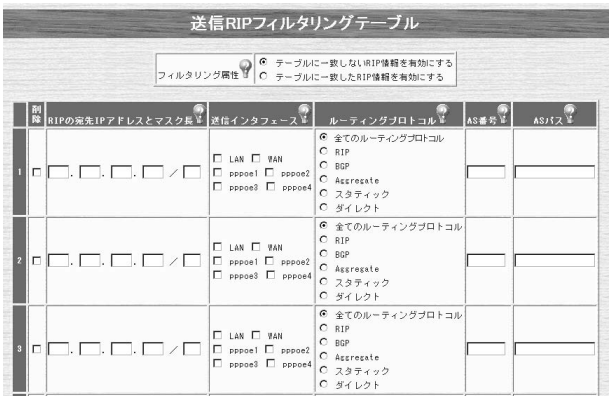
5 ［送信RIPフィルタリングテーブル］をクリックします。

6 フィルタリング属性を選択します。

- **［フィルタリング属性］**
  指定したテーブルに一致した情報を有効とするか／一致しない情報を有効とするかを設定します。
  例えば、テーブルに［x.x.x.x］という情報を登録した場合
  …「テーブルに一致した情報を有効とする」と設定した場合は、「x.x.x.x」のみが有効となり、それ以外の情報は無効となります。
  …「テーブルに一致しない情報を有効とする」と設定した場合は、「x.x.x.x」以外の情報が有効となり、「x.x.x.x」の情報は無効となります。

〈次ページへ続く〉

RIPの制御



7 送信RIPフィルタリングテーブルを設定します。

- **[RIPの宛先IPアドレスとマスク長]**
  - **RIPの宛先IPアドレス**
    送信ルーティング情報のフィルタリングの対象とする宛先IPアドレスを入力します。
  - **アドレスマスク長**
    宛先IPアドレスに対するマスクパターンを入力します。
- **[送信インタフェース]**
  送信インタフェースを選択します。
- **[ルーティングプロトコル]**
  この情報を取得した手段（プロトコル）を選択します。
- **[AS番号]**
  BGPで取得した場合、RIPフィルタの対象とする情報のAS番号を指定します。ASパスを同時に設定することはできません。
- **[ASパス]**
  BGPで取得した場合、RIPフィルタの対象とする情報のASパスを指定します。AS番号を同時に設定することはできません。
  ASパスの入力方法は、通過するASパスを「スペース」で区切った書式となります。
  例）ASパスが、「10→100→25」の場合は、"10 100 25"と入力します。

8 [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。

9 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みの受信フィルタリングテーブルを削除するときは
手順6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。

設定例3　ユニキャスト宛RIP制御

IP-VPN網などの、管理外のネットワークを介している場合、インターネットを介した先のネットワーク情報（経路情報）は、通常わかりませんが、ユニキャスト宛RIP制御機能を使用すると、管理外のネットワークを介した先のネットワーク情報も知ることができます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［RIPの制御］をクリックします。

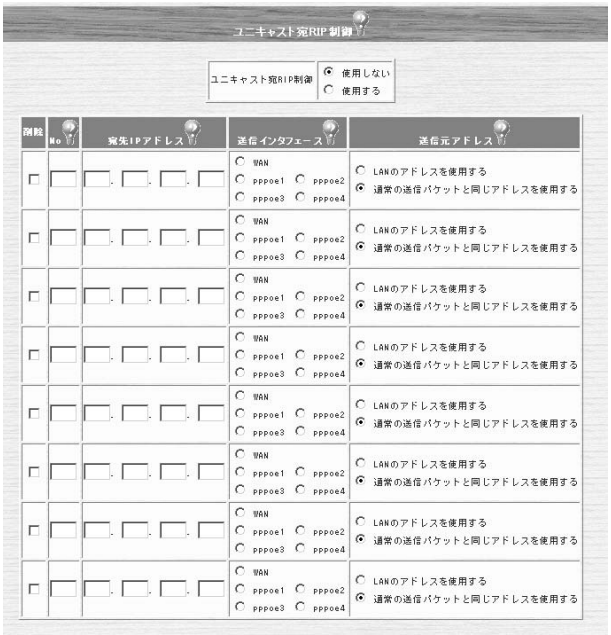
〈次ページへ続く〉

お知らせ

RIPの制御（☛P2-107）で送受信したいインターフェス（LANを除く）を設定することでユニキャスト宛RIPが送受信できます。

RIPの制御

6 ユニキャスト宛RIP制御を設定します。



- **[ユニキャスト宛RIP制御]**
  ユニキャスト宛RIP機能を使用するかどうかを設定します。
- **[No.]**
  番号を指定します。
- **[宛先IPアドレス]**
  RIPを送信する宛先のIPアドレスを設定します。
- **[送信インタフェース]**
  ユニキャスト宛のRIPを送信するインタフェースを指定します。ここで指定したインタフェースには、ブロードキャストもしくはマルチキャスト宛のRIPは送信されません。
- **[送信元アドレス]**
  ユニキャスト宛RIPを送信するときに、送信元アドレスとしてLAN側のアドレスをつけて送信するか、通常のIPアドレス（送信するWANインタフェースのIPアドレス）をつけて送信するかを選択します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みのユニキャストRIP制御を削除するときは

手順6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。

設定例4　ルート情報提供ルータの指定

有効なルーティング情報を提供してくれるゲートウェイのIPアドレスを設定します。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［ルート情報提供ルータの指定］をクリックします。

〈次ページへ続く〉

6 有効なルーティング情報を提供してくれるゲートウェイのIPアドレスを登録または削除します。

装置導入時は未設定です。

- **[ルート情報提供ルータのIPアドレス]**
  有効な情報を提供してくれるゲートウェイのIPアドレスを入力します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

ワンポイント

●登録済みのルート情報提供ルータを削除するときは

手順6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。

BGP機能

本装置では、IP-VPN網と接続する場合に、IP-VPN網を含めた経路情報をダイナミックに制御することができる、BGP Version 4（BGP4）をサポートしています。IP-VPN網に新規拠点が追加された場合や、拠点が削除された場合等に、FITELnet-F40の設定を変更することなく、柔軟に経路変更を行うことができます。

設定の流れ

BGPを使用する場合は、以下の手順で設定を行っていきます。

1 BGPの一般設定

BGPを使用するかどうか、FITELnet-F40が属するASの番号など、BGPを使用する場合に必要なFITELnet-F40側の情報を設定します。

↓

2 BGPピアの登録

BGPで接続する相手の情報を設定します。I-BGPで使用する場合は、フルメッシュのネットワーク形態である必要がありますので、全てのBGPピアを登録します。

↓

3 BGPフィルタリングの設定

BGPを受信あるいは送信する際に、どのような情報を有効とする／提供するかを登録します。

ワンポイント

●PPPoEやDHCPで良く使われるIPアドレスを自動で取得する方法では

BGPを使用することはできません。自動で割り当てられる方法でなく、固定的にIPアドレスを取得するようにしてください。固定的に割り当てる方法については、各プロバイダ／CATVインターネット業者にご確認ください。

BGPの一般設定

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［BGPの設定］をクリックします。

6 ［BGPの一般設定］をクリックします。

- **［BGP動作モード］**
  BGPを動作させるかどうかを選択します。
- **［AS番号］**
  FITELnet-F40が属するASのAS番号を設定します。
- **［ルータID］**
  BGPを確立するためのFITELnet-F40のIPアドレスを設定します。

BGPピアの登録

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［BGPの設定］をクリックします。

6 ［BGPピアの登録］をクリックします。

＜E-BGPの登録＞

- **［ピアAS番号］**
  BGPピアの属するAS番号を設定します。
- **［ピアアドレス］**
  BGPピアを確立する相手のIPアドレスを設定します。
- **［ローカルアドレス］**
  送信元アドレスとして、指定したIPアドレスをつけて送信するか、通常のIPアドレス（送信するインタフェースのIPアドレス）をつけて送信するかを選択します。
- **［メトリック］**
  BGPの経路情報が重複した場合、どちらを優先するかを指定します。数値の小さい方が優先されます。

〈次ページへ続く〉

- **[優先度１]**
  指定している宛先に対して、複数の経路が存在した場合の優先度を設定します。デフォルト値は、RIP=100、E-BGP=70、I-EGP=170、Aggregateルート=130、スタティック=50です。
- **[hold time]**
  BGPコネクションを保持しておく時間を設定します。BGPコネクションを切断しない場合は「off」を選択してください。
- **[ゲートウェイアドレス]**
  指定しているBGPピアと通信するためのゲートウェイアドレスを設定します。ゲートウェイを介さない場合は「off」を選択します。

＜I-BGPの登録＞

- **[internal type]**
  BGPピアまでの経路情報を、ルーティングテーブルを参照するか、この画面で設定するゲートウェイアドレスを利用するかを選択します。
- **[ローカルアドレス]**
  BGPを接続する自身のIPアドレスを設定します。offを指定した場合は、LANのIPアドレスを使用します。
- **[メトリック]**
  BGPの経路情報が重複した場合、どちらを優先するかを指定します。数値の小さい方が優先されます。
- **[優先度１]**
  指定している宛先に対して、複数の経路が存在した場合の優先度を設定します。デフォルト値は、RIP=100、E-BGP=70、I-EGP=170、Aggregateルート=130、スタティック=50です。
- **[hold time]**
  BGPコネクションを保持しておく時間を設定します。BGPコネクションを切断しない場合は「off」を選択してください。
- **[ゲートウェイアドレス]**
  指定しているBGPピアと通信するためのゲートウェイアドレスを設定します。ゲートウェイを介さない場合は「off」を選択します。プロバイダ経由の場合等、gatewayがわからない場合は、インタフェースを選択します。

7 [送信] をクリックします。

8 フィルタリングの設定をしない場合は、再起動します。

フィルタリングの設定を行う場合は、このまま設定を続けます。

BGPフィルタリング（受信）の設定

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［BGPの設定］をクリックします。

6 ［BGPフィルタリング（受信）］をクリックします。

〈次ページへ続く〉

- **[フィルタリング属性]**
  設定するテーブルの属性を指定します。
- **[シーケンス番号]**
  エントリの番号を設定します。
- **[IPアドレス・マスク]**
  フィルタリングの対象とする宛先IPアドレス／マスクを入力します。
- **[優先度]**
  フィルタリングの対象とする優先度を設定します。
- **[AS番号]**
  フィルタタイプに「AS」を指定した場合、フィルタリングの対象とするAS番号を設定します。ASパスを同時に設定することはできません。
- **[ASパス番号]**
  フィルタタイプに「as-path」を指定した場合、フィルタリングの対象とするASパス番号を設定します。AS番号を同時に設定することはできません。ASパスの入力方法は、通過するASパスを「スペース」で区切った書式となります。
  例）ASパスが、「10→100→25」の場合は、"10 100 25"と入力します。

7 [送信] をクリックします。

BGPフィルタリング（送信）の設定

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

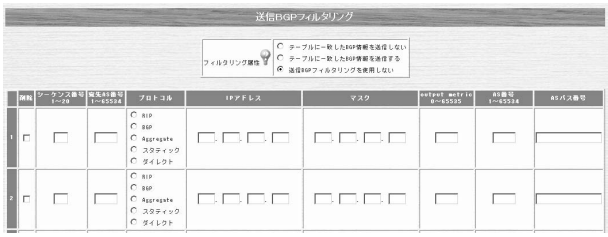
変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［BGPの設定］をクリックします。

6 ［BGPフィルタリング（送信）］をクリックします。

〈次ページへ続く〉



- **[フィルタリング属性]**
  設定するテーブルの属性を指定します。
- **[シーケンス番号]**
  エントリの番号を設定します。
- **[宛先AS番号]**
  フィルタリングの対象とする宛先AS番号を設定します。
- **[プロトコル]**
  フィルタリングの対象とするプロトコルを選択します。"ダイレクト"はFITELnet-F40が直接接続しているネットワークの情報、"スタティック"はFITELnet-F40に設定された経路情報、"RIP"はRIPで取得した経路情報、"BGP"はBGPで取得した経路情報を示します。
- **[IPアドレス・マスク]**
  フィルタリングの対象とする宛先IPアドレス／マスクを入力します。
- **[output metric]**
  フィルタリングの対象とするメトリック値を設定します。
- **[AS番号]**
  フィルタタイプに「AS」を指定した場合、フィルタリングの対象とするAS番号を設定します。ASパスを同時に設定することはできません。
- **[ASパス番号]**
  フィルタタイプに「as-path」を指定した場合、フィルタリングの対象とするASパス番号を設定します。AS番号を同時に設定することはできません。ASパスの入力方法は、通過するASパスを「スペース」で区切った書式となります。
  例）ASパスが、「10→100→25」の場合は、"10 100 25"と入力します。

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。

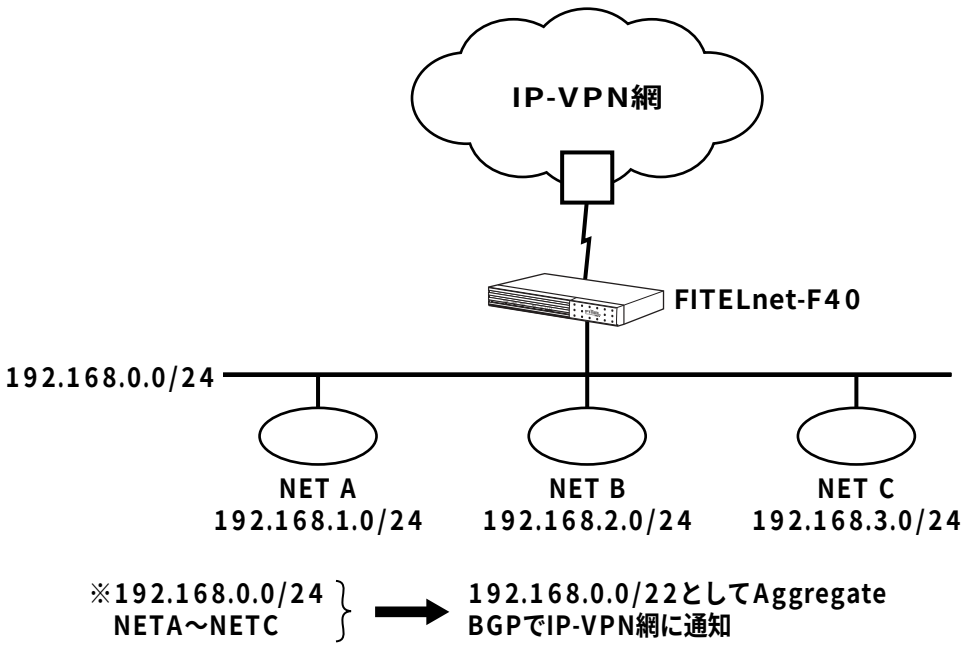
8 再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

Aggregate機能

本装置では、複数の経路情報を集約（Aggregate）して保持し、その情報をルーティングプロトコルにより通知する機能があります。この機能により、ネットワーク上を流れる経路情報の数が減るため、本来のデータ通信の効率が良くなります。
Aggregate機能は、以下のような形態で有効です。

〈4つのネットワークが1つの情報になる〉



設定の流れ

Aggregate機能を使用する場合は、以下の手順で設定を行っていきます。

1 Aggregateの一般設定

Aggregate機能を使用するかどうか、Aggregateルート情報の優先度を設定します。

↓

2 Aggregateテーブルの登録

どのような情報をAggregateするかを登録します。

Aggregateの一般設定

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［Aggregateの設定］をクリックします。

6 ［Aggregateの一般設定］をクリックします。

〈次ページへ続く〉

- **[Aggregate動作モード]**
  Aggregate機能を動作させるかどうかを選択します。
- **[Aggregate経路情報の優先度]**
  Aggregate経路情報を、他のルーティング情報に比較して優先とするかどうかの優先度を設定します。数値が小さい方が優先されます。デフォルト値は、E-BGP=70、I-BGP=170、RIP=100、スタティック=50、Aggregate=130です。

7 [送信] をクリックします。

8 Aggregateテーブルを登録します。

Aggregateテーブルの登録

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［Aggregateの設定］をクリックします。

6 ［Aggregateテーブルの登録］をクリックします。

〈次ページへ続く〉

- **[ネットワーク]**
  Aggregate後の宛先IPアドレスを設定します。PXXの例では、192.168.0.0/255.255.252.0になります。
- **[フィルタ]**
  Aggregateする元データおよびAggregateの条件を設定します。P2-122の例では、192.168.0.0/24～192.168.3.0/24が対象となります。
  ただし、P2-122の例では、192.168.0.0/24は自身が属するネットワーク、192.168.1.0/24～192.168.3.0/24はRIPで学習したネットワークのように、学習した手段が異なるため、2エントリ登録する必要があります。
- **[ルーティングプロトコル]**
  学習した手段（ルーティングプロトコル）を指定します。
- **[AS番号]**
  Aggregateした情報をBGPで送信する際のAS番号を指定します。ASパスを同時に設定することはできません。
- **[ASパス]**
  Aggregateした情報をBGPで送信する際のASパスを指定します。AS番号を同時に設定することはできません。ASパスの入力方法は、ASパスを「スペース」で区切った書式となります。ASパスが「10→100→25」の場合は、“10 100 25”と入力します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。[装置を再起動する] をチェックしてから、[送信] をクリックします。

TCP MSSの設定

TCPパケットを中継する際、TCPオプションのMSS（Max Segment Size）を変更することができます。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、[次へ]をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［詳細設定］をクリックします。

5 ［TCP MSSの設定］をクリックします。

〈次ページへ続く〉

6 TCP MSSの動作モードを選択します。

- **[MSS長]**
  パケットのMSSオプションが付加されている場合、送信インタフェース毎もしくはIPsec対象パケットに対し、MSS値を書き換えることができます。

・off
MSS値を変更しません。

・auto
各MTU値から40を引いた値と、MSSオプション値を比較して、小さい方を、MSS値として使用します。各インタフェースのMTU値は、以下の通りです。

- LAN：1500固定
- EWAN/PPPoE：基本設定画面で設定した値

IPsecの場合は、送信インタフェースのMTU値から72を引いた値と、MSSオプション値を比較して、小さい方をMSS値として使用します。(IPsecは、本装置が暗号化するパケットを対象)

・設定値
設定値とMSSオプション値を比較して、小さい方をMSS値として使用します。

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 装置を再起動します。

設定内容を有効にするために、FITELnet-F40を再起動します。
画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する]をチェックしてから、[送信]をクリックします。

PPPoEの接続/切断手順

PPPoE（Point to Point Protocol over Ethernet）は、ダイヤルアップ接続で使用するPPP（Point to Point Protocol）接続をEthernetで可能にした接続方法で、日本電信電話株式会社（以降NTT）のADSL接続サービス、フレッツADSLで採用されているプロトコルです。
ここでは、PPPoE接続した回線の接続/切断操作を説明しています。

1 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［PPPoE制御］をクリックします。

現在の接続ユーザーと接続状況が表示されます。

5 PPPoEの接続と切断を選択します。

お知らせ

● **本装置のPPPoEクライアント機能について**

①PPPoE接続ソフトが不要
本装置がクライアントとしてプロバイダとのPPPoEセッションを確立しますので、面倒なソフトウェアのインストールは必要ありません。

②常時接続
常にプロバイダと接続しています。

③複数のパソコンで同時にインターネット接続
NAT/IP マスカレード機能（NAT[+]）により、1契約（1セッション）で複数のパソコンを使った同時インターネット接続が可能です。

VPN制御

VPN制御機能として、以下の3機能をサポートしています。
・IKE SA/IPsec SAの消去
・電子証明書リクエストデータの作成
・CRL（Certificate Revocation List：証明書失効リスト）のクリア

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 ログインID/パスワードを入力します。

設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワードを入力してください。
初めて設定するときは、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

初めてログインした場合は、新しいパスワードの入力画面が表示されます。ここでパスワードを入力して、［次へ］をクリックします。

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 画面左側のメニューから［VPN制御］をクリックします。

5 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。

〈次ページへ続く〉

6 全てのIKE SAを消去する場合は［全てのIKE SA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。

SA番号は、「SAIDはこちら」をクリックすることにより確認できます。

IPsec SAの消去でも、同様の手順で消去できます。

VPN制御

＜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」を入力します。

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

VPN制御

電子証明書リクエストデータの作成

電子証明書リクエストデータは、PKI（公開鍵基盤）－X.509機能で使用します。
電子証明書が必要な場合は、別冊「PKI（公開鍵基盤）－X.509機能に関する資料」を参照してください。

CRL（Certificate Revocation List：証明書失効リスト）の取得

CRLは、PKI（公開鍵基盤）－X.509機能で使用します。
CRLについては、別冊「PKI（公開鍵基盤）－X.509機能に関する資料」を参照してください。