設定について

設定する

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
			ユーサ	۴ID	abc012@A.ne.jp
			パスワ	ード	Apass
		PPPoE2	名称		Bprovider
			ユーサ	۴ID	abc012@B.ne.jp
			パスワ	ード	Bpass
		PPPoE3	名称		Cprovider
			ユーサ	۴ID	abc012@C.ne.jp
			パスワ	エード	Cpass
		PPPoE4 名称	名称		Dprovider
			ユーサ	۴ID	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	ス	192.168.0.1
		サブネッ	ットマス	くク	255.255.255.0
		DHCPサ	ーバ機能	נע	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 ⁺

<Webブラウザ操作>

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。

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。

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

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

5



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。

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。



<コマンド操作>

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 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 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 DHCPサーバ機能を設定します。 conf#dhcpserver on 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



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	192.168.0.1
		サブネットマスク	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>

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





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。

	簡単語	役定
現在Iは、WAN運用	形態の設定が <u>DH</u>	<u>CPクライアント</u> になっています。
(現在のIPアドレス:		アドレスを取得しなおす
WAN側 運用形態	PPP over Ethernet 9 手動設定 9	
MTU長	-9	
ホスト名		9
LAN側 IPアドレス🂡	IPアドレス サブネットマスク DHCPサーバ機能	192]. 168]. 0. 1 255]. 255]. 255]. 0 © 使用する ○ 使用しない
DNSサーバ	プライマリ セカンダリ 簡易DNS機能 ®	
NAT動作モード 💡	O OFF C NA	T+

設定内容を登録します。

h

設定項目を入力して、[登録する]をクリックします。

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。



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。



<コマンド操作>

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 簡易DNS機能を設定します。 4 conf#proxydns on DHCPサーバ機能を設定します。 conf#dhcpserver on NAT動作モードを設定します。 conf# nat wan natp 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)	158.xxx.xxx.1
		(セカンダリ)	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>

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



5

h

1000

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。

手動設定の各種設定を入力します。

現在は、WAN	運用形態の設定が <u>手動設定</u> になっています。		
WAN側 運用形態	運用形態 <u>DHCPクライアント</u>		
мт∪長			
WAN側 IPアドレス	IPアドレス		
LAN側 IPアドレス🂡	IPアドレス 192. 168. 0. 1 サブネットマスク 255. 255. 255. 0 DHCPサーバ機能 © 使用する C 使用しない		
デフォルトゲートウェイ			
DNSサーバ	プライマリ セカンダリ 簡易DNS機能 ☉ 使用する ○ 使用しない 💡		
NAT動作モード 💡	© OFF C NAT+		

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。

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

2-12

設定する

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プラウザ 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)



設定例1

VPN**の設定**

Pre-shared key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。



< 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。

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。

パスワードを入力します。

Z

3

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。

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。

│ 画面左側のメニューから[便利な設定]をク │ リックします。

[VPNの設定]をクリックします。

	使利な設定
スタティックルーティング	スタティックルーティングを整装します
<u>IPパケットフィルタリング</u>	Ⅰ ₽ パケットフィルタリングデータを登録します 🌳
学習フィルタリング	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)する場合に設定します 🌳
SNHPI-Sit	SNMPエージェント機能を使用する場合に設定します 🂡
NAT機能	LAN⇔VANで、NATを使用する場合に設定します
DHCPサーバ機能	DHCPで配布する内容を設定します 💡
syslogの通信	本装置のログ情報を、外部のSYSL06サーバに送信する場合に設定します 🌳
船県DNS	本装置を簡易DNSサーバとして運用する場合に設定します🌳
電子メール通知	不正アクセス時に電子メールにて情報を運知する場合に設定します 🌳
SNTP	現在時刻の傍報を、外部のSNTPサーバに問い合わせる場合に設定します 🌳
アクセス制御	不正アクセスに対処するための設定をします 💡
送受信ログの設定	送受信ログとして取得したいパケットを登録します 🌳
VPNの設定	VPN(IPsec)を使用する場合に設定します 🌳
冗長炭龍	FITELnet-E30と組み合わせて、ADSL回線の除害をISONでパックアップする場合に設定します 💡
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、VAN側にリレーし、VAN側のDHCPサーバから割り当ててもらう場合に設定します 🌳
マルチルーティング機能	PCのアドレスや、使用するアプリケーションにより、接続するプロバイダを実更したい場合に設定します。 💡

次ページへ続く

設定する

6 VPN動作モードの [ON]を選択して、[送信] をクリックします。



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。

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。

│ 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。

ポリシー識別子を設定します。



•[ポリシー識別子] ポリシー識別子を1~32の間で入力します。

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(拡張認証なし)		
C Pre-shared Key(拡張認証あり)		
C RSA signature (拡張認証なし)		
CRSA signature(拡張認証あり)		

•[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。)



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。

[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)

│ 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。

ポリシー識別子を設定します。



•[ポリシー識別子] ポリシー識別子を1~64の間で入力します。

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

2-20

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。



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。)



↓ 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)

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

5



h

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。

压缩	圧縮ネゴシエーション
○ 圧縮する	C する
● 圧縮しない	● しない

•[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。

[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。

│ VPNの設定画面(●P2-17)で、[VPNピア │ の登録]をクリックします。

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 方式を選択します。



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。

拉張謬証
 相手を認証しない 相手を認証する
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。



FQDNタイプ(●P5-17)

次ページへ続く





∨03.00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。

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

2-25



「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。

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。



「使用しない」を選択します。

NAT-Traversal
〇 使用する
④ 使用しない
KeerAlive送信間隔 <mark>5</mark> 秒

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。

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。



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。



[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。

次ページへ続く

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。

2-27



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	DN (Distinguished Name)
domainname 💌	

 [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。

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。



12

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)

│ 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。

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。

^{完先指定} ♥
IPアドレスとポート番号
(IPアドレス指定 😫
IPアドレス指定のとき 158 - xxx - 0 - 0 / 16
 ● すべてのボート ● ボート番号の指定

次ページへ続く

3

2-29



- •[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。

|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。

次ページへ続く

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]

[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。

インタフェースを選択します。

[pppoe1]を選択します。

ん	971-2 ⁸
宛先	オンタフェース
	WAN pppoe1 pppoe2 pppoe3 pppoe4

5

h

•[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。

NAT変換後のアドレスを設定します。

NAT変換後のアドレス
IPアドレスとマスク

•[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



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。

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 SA確立契機
起動時確立しない ▼ データ通信時 ▼
回線がダウンした場合の制御 回線が確立してもSA確立動作を行わない 💌
リトライ リトライしない ▼

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。

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。

[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。



<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

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 鍵データ	相手を認証しない * 空欄 admin-FITELnet-F40 secret-F40 「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。

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。

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。

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。

3

画面左側のメニューから「便利な設定]をク リックします。

[VPNの設定]をクリックします。

	使利な設定
スタティックルーティング	スタティックルーティングを登録します 🌳
ロパケットフィルタリング	19パケットフィルタリングデータを登録します 🌳
学習フィルタリング	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(廣棄)する場合に設定します 🍄
SNHPI-Sit	SHMPエージェント機能を使用する場合に設定します🂡
NAT 炭脸	LAN⇔VANで、NATを使用する場合に設定します 🂡
DHCPサーバ機能	DHCP एஸிக்ச தேலை பக்ச 💡
syslogの通信	本装蔵のログ博報を、外部のSYSLOGサーバに送信する場合に設定します
簡具DNS	本装置を簡易DNSサーバとして適用する場合に設定します 🍄
電子メール通知	不正アクセス時にモチメールにて情報を通知する場合に設定します
SNTP	現在時刻の情報を、外部のSNTPサーバに問い合わせる場合に設定します 🌳
アクセス制御	不正アクセスに対処するための設定をします 💡
送受信日グの設定	迷愛信ログとして取得したいパケットを登録します 🂡
VPNの設定	VPN(IPsee)を使用する場合に設定します
冗長機能	FITELnet-ESOと組み合わせて、ADSL回線の障害をISDNでバックアップする場合に改定します 💡
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、VAX側にリレーし、VAX側のDHCPサーバから割り当ててもらう場合に設定します 💡
マルチルーティング核能	pcのアドレスや、使用するアプリケーションにより、接続するプロバイダを変更したい場合に設定します。 🍄

次ページへ続く 2 - 37

6 VPN動作モードの [ON]を選択し、[送信] をクリックします。



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



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。

│ 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。

ポリシー識別子を設定します。



•[ポリシー識別子] ポリシー識別子を1~32の間で入力します。

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
O Pre-shared Key (拡張認証なし)
● Pre-shared Key(拡張認証あり)
C RSA signature(拡張認証なし)
CRSA signature(拡張認証あり)

•[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。

お知らせ

をクリックします。

るときは

ワンポイント

登録済みのPhase1ポリシーを削除す

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]

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。)

次ページへ続く

3



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。

[送信]をクリックします。

5

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)

│ 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。

′│ポリシー識別子を設定します。



[ポリシー識別子]
 ポリシー識別子を1~64の間で入力します。

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。

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。)

次ページへ続く 2-41





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)

│ 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



h

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。

正縮	圧縮ネゴシエーション
○ 圧縮する	0する
● 圧縮しない	© しない

•[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。

[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。

│ VPNの設定画面(●P2-38)で、[VPNピア │ の登録] をクリックします。

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。)





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。



Δ

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。

±₹37
● 相手を認証しない
●相手を認証する 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。



FQDNタイプ(●P5-17)

```
次ページへ続く
```





∨03.00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]

h

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。

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。

KeepAlive機能を選択します。

「OFF」を選択します。

IKE C VPNビア C VPNビア C (C) C (の KeepAlive 🖁 (送信元アドレス 🗑)
	C ICMP C ICMP C VPNビア C ICMP C ICMP 送信元IPアドレス: 通常の送信パケットと同じアドレスを使用する

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。

NAT-Traversal機能を選択します。

「使用しない」を選択します。

NAT-Traversal	
○ 使用する ● 使用しない KeerAlive送信間隔 <mark>5</mark>	秒

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。



[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。



1 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	DN (Distinguished Name)
domainname 💌	

 [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。

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。



12

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。 [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。(64件)

│ 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。

優先度を設定します。



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。



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。

^{寬先指定}
IPアドレスとポート番号
(IPアドレス指定 🚖
IPアドレス指定のとき 158 - xxx - 0 - 0 / 16
 ● すべてのボート ● ボート番号の指定

次ページへ続く

3

2-50



- •[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。

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。



•[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	\$71-2
宛先	ミインタフェース
	WAN pppoe1 pppoe2 pppoe3 pppoe4

6

[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。

NAT変換後のアドレスを設定します。

NAT変換後のアドレス
IPアドレスとマスク

•[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



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。

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。

SA確立契機 SA確立契機
起動時確立しない ▼ データ通信時 ▼
回線がダウンした場合の制御 回線が確立してもSA確立動作を行わない 💌
リトライ リトライしない ▼

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。

│ 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。

[〕

[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。



<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

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 1

設定する

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。

│NATスタティックを使用するVPNピアを選択 │します。

VI	PN N	IATスタティ	ック登録、	VPNピア選択	
	No.	アドレス	相手名称	VPNNATモード	
選択	1	158.202.236.17		nat ⁺	
選択	2				
12240	_				

2 NATスタティック設定をします。

		VPN NAT	スタティ	ック登録		
	No. 1 15	アドレス 8.202.236.17	相手名	f¥ VP nat	NNAT E-F	
翻脫	LAN上の編末 IPァドレス	前定 外書	に見えるい	アドレス	73	スク指定
1	192 . 168 . 100	. 0 192	. 168 . 0	. 0	255 . 255	5 . 255 . 0
2						
3 🗖						
4]			
5 🗖						

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。

簡易ファイアウォール機能

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>

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。

ログインID/パスワードを入力します。

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。

↓ 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。

[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。

アクセ	スを許可する端末/イン	タフェースの指定
<装置^	のFTP、TELNET、Web謬	定のログイン制御>
装置へのアクセスを許可する線 定がある場合は、指定されたIPアドレス	まのIPアドレス、もしくは- Rまたはインタフェース経由(インタフェースを指定することができます。 のアクセスは許可しますが、その他のアクセス
© アクセスインタフェース指定	✓ LAN ✓ VAN (VPN) ✓ VAN ✓ PPP001 ○ PPP002 ○ pPp003 ○ PPP004	
○ 端末の1₽アドレスを指定	開録 IPアドレス 1 □ □ · □ · □ · □ · □ · □ · □ · □ · □ ·	
○ アクセス許可しない		
また、ping0 ここに指定しない	くping応答制御)リクエストに応答するイン: インタフェースからのpingの	■> タフェースを選択します。 リクエストにはた答しません。 ↓ LAN
,	ing応告インタフェース 🌱	INAN (VPH) WAN pppoe1 pppoe2 pppoe3 pppoe4
端意へのFIP、TELNET、WANDERのの	ing応答インタフェース ア パスワード送り時の アクセス時に、パスワードの	♥ wax(vpa) ■ wax ■ ppool ■ ppool
装置へのFTP、TELNET、Vo5設定の: パスフー FigU を計断する国家と	ing応等インタフェース バスワード 遣り時の ククをス緒に、バスワードの 、バスワード試りが発見した	▼ Wat(v(P)) ■ Wat ■ ppco1 ■ ppco2 ■ ppco2 ■ ppco2 ■ ppco2 ■ ppco4 ■ ppco4
構造へのFIP5、TELNET、Web設定の パスワード試りを評答する国家と パスワード試りを評答する国家と	ins応等インタフェース パスワード記り時の アクセス時に、パスワードの 、パスワード試りが発現した スワード試りを許容する語数	Wax(vpp) Wax Papeat

<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。

次ページへ続く

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



< 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。

[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。

設定する

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。

	┃ 画面左側のメニューから [便利な設定] をクリックします。	שי ש
	2 [IPパケットフィルタリング]をクリックしま す。	_ ŧ
	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。	一、ン沢
	IPバケットフィルタリング	
	この設定は、【送信】ボタンを押した直後に有効となります。(再起動の必要はありません)	
	IPパケットフィルタリング機能 C OFF C ON フィルタリングログを取得するかどうか C 取得する アイルタリングログを取得するかどうか C 取得する	
	クリア 送信	
	以降は1Pパケットフィルタリング機能が0Nの時有効となります。 中語する1Pパケットの登録を行う 上記登録中から中語したくない1Pパケットの登録を行う 中語を許可するパケットを登録します 中語を許可しないパケットを登録します	
	特定のIPバケットを中継したくない場合は、中継するIPパケットとして「全て」を登録してから、 中継したくないないIPパケットの登録に特定のIPパケットを登録して下さい。	
	 「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 するログを表示するかどうかを選択します。 	関
は(<i>●</i> P4-	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	
リクした直	(# P 2-63)	
かの必要は 送信]をク きなくなる	5 中継または遮断するIPパケットの登録が約 わったら、[送信]をクリックします。	_ 冬
ださい。	設定内容が本装置に送信され、確認画面が表示されます。	

2-61



フィルタリングログを見るには (*P4 27)

お知らせ

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)

┃ 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。

中継するIPパケットを設定します。

2



- 「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。

)ワンポイント

設定する

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。



簡易ファイアウォール機能

中継しなNIP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。

│ 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

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。

|[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

簡易ファイアウォール機能

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。

画面左側のメニューから [便利な設定]をクリッ クします。 [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 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IPフィルタリング機能 🂡 O OFF C ON VAN VAN PPPoE1 PPPoE2 用するインタフェ PPPoE3 学習データのエージアウト時間 🌳 🚺 (0~1440) クリア 送信

- ・[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。

	削除]	Pアド	レス			サブ	ネッ	トマス:	ク		削除	IP71	× <i>ν</i>	ζ		サ	ブネッ	トマスク	
				-]. Г	[17				. [. [□ . [. [_ . [
]. []. [<u></u> .[18				F	E		. [. [. [
3				- F			Ъ. Г	<u> </u>		19				□. □	П. Г	T	□ . [□ . [. [
1			Γ]. []. [<u></u> .[20			Γ	F	□. □		_ . [□. [. [
5				Т. Г]. Г	. [21				□. □	П. Г		Π. Γ	□ . [. [
3			Γ]. []. [[22			Γ	. [□. □		. [□. [. [
7				Т. Г			1. [. [23				□. □	□. □	T	□ . [□ . [. [
3			Γ	. []. [. [24			Γ	. [□. □		. [□. [. [
9]. [1. [<u> </u>		25				□. □	□. □		□. [□. [<u> </u>
0			Γ	. []. [<u></u> .[26			Γ	□. □	□. □		. [□. [. [
11]. []. [<u> </u>		27				. [□. □		<u> </u>	. [<u> </u>
12			Γ	. [Ъ. Г	<u></u> .[28			Γ	□. □	□. □		. [□. [□ . [
13]. []. [. [29				. [□. □		□. [□. [<u> </u>
4				Т. Г]. Г	. [30			Г	. [□. □	ΠE	□ . [. [. [
15]. []. [<u> </u>		31				. [□. [□. [□. [<u> </u>
16			Γ	Т. Г			1. [□ . [32			Γ	. [. [ΠĒ	<u>.</u> .Г	. [. [

- ・[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。

┣ 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。

設定する



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

設定する

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。

Constant and	冗長機能	
ルータグループ化機能	ルータグルーブ化機能: C OFF @ ON	➡_ルータグルーブ化機能の設定
Layer3監視機能	Layer3監視機能	➡ <u>経路監視先の登録(Layer3監視機能</u>

次ページへ続く

グループ内の優先度	1 (1~99)
宛先UDPポート番号🂡	55555 (1024~65535)
代表IPアドレス	0.0.0
グループ内共有データの送信間隔	5 (5~45)
グルーブ内のルータを異常と見なすまでの	0時間 15 (15~100)

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 サプネットに属し、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。

[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。

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。

2-68

5

h

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。

│ 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。

- Carrier	冗長機能	
ルータグループ化機能	ルータグループ化機能: C OFF © ON	➡_ルータグループ化機能の設定
Layer3監視機能	Layer3監視機能	➡_経路監視先の登録(Laver3監視機能

次ページへ続く



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。 (*ー*P2-67)

	経路監視機能の登録(Layer3監視機能)
71 12	きや通日の商曲1-146世
	Layer3監視を行う宛先PTアドレス :
・[監ド」に、「「「」」」、「「」」、「」」、「「」」、「「」」、「「」」、「「」」、	yer3監視を行う宛先IPアドレス(必須)] むする宛先のIPアドレスを設定します。目的のサーバのI シスなどを設定します。(ルータである必要はありません yer3監視パケットの定期送信間隔] パケットを送信する間隔を設定します。(秒単位) 路異常時の、Layer3監視パケット送信間隔] パケットが戻ってこないため経路異常と判断している 監視パケットの送信間隔を設定します。(秒単位) 書と判断するまでの時間] 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 設定します。 書復旧と判断するまでの時間] 各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 ま復にと判断するまでの時間] 各が異常となった場合の接続先IPアドレス] から時間を設定します。 路が異常となった場合の接続先IPアドレス] クアップルータがISDN回線を接続する際の接続先ルー アドレスを設定します。 yer3監視パケットの送信元IPアドレス] rer3監視パケットの送信するときに送信元アドレスとし、 例のアドレスをつけて送信するか、通常のIPアドレス こるWANインタフェースのIPアドレス)をつけて送信す ご選択します。 ックアップ対象パケット(必須)] D経路監視において経路異常と判断された場合に、FITELr の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 IPアドレス、サブネットマスクにそれぞれ0.0.0.0を入た 合は全てのパケットが対象となります。
[送イ _{設定内}	言]をクリックします。 回容が本装置に送信され、確認画面が表示されます。
装置	を再起動します。

設定する

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



設定する

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

- │ | 画面左側のメニューから [便利な設定] をクリッ │ クします。
- 🔰 [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。

	送信元相3	ż	宛先指定	*****	プリファレ
3	IPアドレスとマスク長	宛失ポート番号			ンス
		€ FTP • C 0 ~ 65535	C1P7FL2882	C IP7FL2502:	1
		© FTP × C 0 ~ 65535	C 197F L 2882	C IPアドレス施定: , , , , , , , , , , , , C インタフェース施定: pppce1 💌	1
		€ FTP ■ C 0 ~ (65535	CIP7FU282	C IPアドレス指定:	1
-		 ● FTP ● ● ○ ● ●	C IP7F L 2802	C 07FL282:	1

• [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機能

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

> ┃ | 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。

マルチ	ルーティング適応外デー	一夕の登録
※信元アド		宛先指定
107FCXE7X9&	現先ホート番号	
	C 0 ~ 65535	C IPアドレス指定
2		
	 ● FTP ● ○ 0 ~ 05535 	CIP7FLZHIZ
	 ● FTP ● ○ 0 ~ 65535 	CIP7Fレ2指定
5 🗖 🗖, 🔂, 🗖, 🗍 / 🗖	 € FTP C 0 ~ 65535 	С IP7F L 2推定
	 ● FTP ▼ ○ 0 ~ 65535 	С IP7F L 2推定
	 ● FTP ▼ ● 0 ~ 65535 	Сіртғі і дійд
8 🗖 🗖, 🗍, 🗍, 🗍 / 🗖	 ● FTP ● 0 ~ 65535 	С IP7F U 2推定 / / / / / / / / / / / / / / / / / / /
現在	の登録件数/最大登録件数:0/1 	61~9~

- ・[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

設定する

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機能

4 [送信]をクリックします。

5 装置を再起動します。

設定する

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。

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。



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。

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。

[SNMPエージェント]をクリックします。



SNMPエージェント機能

SNMPエージェント機能を設定します。

		101.000	SNM	Pエーシ	エント	
			SNMPエージェント機能	C off @	on 9	
			認証失敗トラップ	 通信す 	る C 通信しない	9
			以移動はSNMPエージェン	小機能がの	Nの時有効とない	lます。
副 敗	SNMPマネージャの	IP7FL2	コミュニティ名 (最大32)	\$\$)	トラップ 🖗	送信元 IPアドレス 🕅
	0 0 0	0	public		 ● 送信しない C 送信する 	通常の送信パケットと同じアドレスを使用する 💌
					 ● 送信しない ○ 送信する 	通常の送信パケットと同じアドレスを使用する 💌
					 ● 送信しない ○ 送信する 	「通常の送信パケットと同じアドレスを使用する ▼
					 通信しない C 送信する 	通常の送信パケットと同じアドレスを使用する 💌

- •[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。

[送信]をクリックします。

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 リ、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	ンID/パスワードを入力します。
-	 設定オーフ グインID/ 初めて設う ワードはS	プニング画面「ようこそFITELnet-F40 設定画面」でロ パスワードを入力してください。 定するときは、ログインIDに「root」と入力し、パス 2欄のままで [送信]をクリックします。
2	パスワ・	 − ドを入力します。
	 初めてロ? されます。 ます。	ブインした場合は、新しいパスワードの入力画面が表示 ここでパスワードを入力して、[次へ] をクリックし
3	現在時刻	
	 変更しない 簡単設定の	\ときは、[次へ] をクリックしてください。 D設定画面が表示されます。
4	画面左 リック	側のメニューから[便利な設定]をク します。
5	[NAT樹	幾能]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。
		NAT機能
	NAT	機能の設定は、インタフェースごとに設定します。
	WAN	EWANをDHCPや手動設定で使用する場合の設定は <u>こちら</u>
	PPPoE	PPPoE1のNAT設定は <u>こちら</u> PPPoE2のNAT設定は <u>こちら</u> PPPoE3のNAT設定は <u>こちら</u> PPPoE4のNAT設定は <u>こちら</u>

次ページへ続く

┃ NAT機能の [NAT] を選択し、[送信] をクリッ クします。

	NAT機能 C OFF C NAT ● NAT+
	クリア 送信
以降はNA	NT機能が"NAT"または"NAT+"の時有効となります。
NAT変換範囲の登録	変換を許可するアドレスの範囲を設定します。 NAT機能を"NAT"で使用する場合は、必ず登録してください
<u>NAT変換範囲の登録</u> NAT+スタティック登録	変換を計可するアドレスの範囲を設定します。 NAT機能を「NATで使用する場合は、必ず登録してくたれ。 NAT+のスタティック情報を設定します。

[NAT変換範囲の登録]をクリックします。

•[NAT変換範囲の登録]

8

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。

R. I.		11112	NA	T変換	範囲の	登録	(WAI	小用)		2.54
			ວຫຮ	登録はNAT	機能がON	の時有刻	カとなり	ます。		
	耐 般 変 換 す る 先 語 の IP アドレス			変換する最後の IPアドレス						
1	П	Γ	<u> </u>	—. r	∟		<u> </u>	<u> </u>	<u> </u>	
2	П	Γ	<u>- Г</u>	—. r			. [—. r	— . [
3	П	Г	- . [<u> </u>	∟		Τ. Γ	<u> </u>	<u> </u>	
4	Г	Γ	Т. Г	—. r			. [—. r	— . Г	
5	П	Γ	<u> </u>	—. r	∟		Τ. Γ	<u> </u>	<u> </u>	
6	Г		Т. Г		. [- . [—. r	□.	
7	Π	Γ	Т. Г	<u> </u>	<u> </u>		Т. Г	<u> </u>	<u> </u>	
8	Г	Γ	Т. Г	[. [—. r		

[送信]をクリックします。

|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

設定する

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	ンID/パスワードを入力します。
-	設定オーフ ログインII	プニング画面「ようこそ FITELnet-F40 設定画面」で D/パスワードを入力してください。
	初めて設た ワードはS	દするときは、ログインIDに「root」と入力し、パス ≧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。
	「初めてロク されます。 ます。	ブインした場合は、新しいパスワードの入力画面が表示 ここでパスワードを入力して、[次へ] をクリックし
3	現在時刻	
	を 変更しない 簡単設定の	≀ときは、[次へ]をクリックしてください。 D設定画面が表示されます。
4	画面左 リック	側のメニューから[便利な設定]をク します。
5	[NAT桥	幾能]をクリックします。
6	設定する	るインタフェースを指定します。
		NAT機能
	NAT	機能の設定は、インタフェースごとに設定します。
	WAN	EWANをDHCPや手動設定で使用する場合の設定は <u>こちら</u>
		PPPoELONAT BOCK 555
	PPPoE	PPPoE3のNAT設定は <u>こちら</u>
		PPPoE4のNAT設定は <u>こちら</u>

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。



Inor	
<u> </u>	COFF C NAT C NAT
	クリア 送信
LURS ITNAT #	能が"NAT"またけ"NAT+"の結石効とかります。
以降はNAT機	能が"NAT"または"NAT+"の時有効となります。
以降はNAT機 NAT変換範囲の登録	能が"NAT"または"NAT+"の時有効となります。 変換を許可するアドレスの範囲を設定します。 NAT機能を"NAT"で使用する場合は、必ず登録してください。
以降はNAT機 <u>NAT変換範囲の登録</u> の	能が"NAT"または"NAT"の時有効となります。 実施を計可するアドレスの範囲を設定します。 NAT機能を"NAT"で使用する場合は、必ず登録してください。
以降はNAT機 NAT変換範囲の登録 NAT・スタティック登録	能が『NAF"または"NAF"の時有効となります。 実施を許可するアドレスの範囲を設定します。 NAT機能を"NAF"で使用する場合は、必ず登録してくだれ、

【 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。

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。

	削脫	LAM上の編末指定				
		IPアドレス	ポート番号			
1		197 - 168 - 0 - 100	80			

・[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

Q

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。

【 】 [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。 NAT機能

設定する

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.xx.0~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。

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。 画面左側のメニューから「便利な設定]をク リックします。 [NAT機能]をクリックします。 設定するインタフェースを指定します。 h NAT機能 NAT機能の設定は、インタフェースごとに設定します。 WAN EWANをDHCPや手動設定で使用する場合の設定はこちら PPPoE1のNAT設定は<u>こちら</u> . PPPoE2のNAT設定は<u>こちら</u> PPPoE , PPPoE3のNAT設定はこちら PPPoE4のNAT設定は<u>こちら</u>

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。





┠ [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.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.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.xx.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)

|[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。

設定する

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。

> 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。

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。

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

1

3

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	 C 使用する © 使用しない 	
DHCPサーバリスト	開降 IPアドレス 送信元Pアドレス 1 0	ক • ক • ক • ক •
DHCPサーバまでの最大ホッブ数	4 -	

•[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。

[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。

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。

設定する

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。)

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。

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。

│ [DHCPサーバ機能]をクリックします。

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。

	DHCPサーバ機能
DHCPサーバ機能	C OFF C ON
配付IPアドレスの開始値	 C LANインタフェースIPアドレスの次から開始する C の値から開始する
割り当てるIPアドレスの個数	(範囲:1~255)
デフォルトゲートウェイの通知	○ しない ○ する デフォルトゲートウェイのIPアドレス:
ドメイン名称の通知	C しない C する 通知するドメイン名称:
WINSアドレスの通知	○ しない ○ する VINSプライマリアドレス: ○ . ○ . ○ . ○ VINSセカンダリアドレス: ○ . ○ . ○ . ○
リース期限	 ● 無期限リース ○ 期限付きリース □ 時間 □ 分 (範囲:0時間1分~9999時間59分)
ネームサーバアドレスの通知 💡	◎ しない、もしくは簡易DNS機能を利用 ○ する プライマリアドレス:
ネームサーバアドレスの通知 💡	Pomoriteシス

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。

[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

8

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。

		配付アドレスのスタティック登録(才)	ブション設定) 💡
	削除	配付先端末の指定 MACアドレス	配付するIPアドレス
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			

・[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。

【 ┃ [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。

装置を再起動します。

11

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

設定する

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。

設定する

Syslog**の送信**

1

3

h

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。

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。

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。

[syslogの送信]をクリックします。

syslogの送信を設定します。

S	syslogの送信			
syslogの送信	Cutal C #3			
syslogを受け取る端末のIPアドレス	0 0 0			
tlog(errレベル)で送信	●しない C する			
elog(warningレベル)で送信	●しない ○ する			
llog(infoレベル)で送信	●しない C する			
vlog(infoレベル)で送信	©しない C する			
vpnlog(infoレベル)で送信	●しない C する			
clog(noticeレベル)で送信	●しない C する			
flog(noticeレベル)で送信	©しない C する			
ファシリティ値				
送信元アドレス	 LANのアドレスを使用する 通常の送信パケットと同じアドレスを使用する 			

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。

[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。

装置を再起動します。

8

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。

設定する

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

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DNSサーバで簡易DNS機能の「使 4 用する1をチェックします。 אר או או או או セカンダリ 🔄 - 🔄 - 📃 簡易DNS機能 ® 使用する C 使用しない 💡 PPPoE1 PPPoE2 PPPoE3 PPPoE4 NAT動作モード 💡 © OFF C NAT+ ⊙ OFF C NAT+ ⊙ OFF C NAT+ ⊙ OFF C NAT+ 登録する 変更前に戻す 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。 「登録する」をクリックします。 画面左側のメニューから「便利な設定」をク h リックします。 [簡易DNS]をクリックします。 次ページへ続く



簡易DNS機能

【 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。

中継先DNS IPアドレスを設定します。

中継先DNS IPアドレス	セカンダリアドレス:000000000000000000000000000000000000
応答バケット待ち時間	3 10 9
再送回数	2 0 9
送信元アドレス 💡	 ○ LANのアドレスを使用する ○ 通常の送信パケットと同じアドレスを使用する

•[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。

[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。

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

設定する

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。

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。 [簡易DNS]をクリックします。

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。

	簡易DNS
	問馬DNS機能 C OFF C ON
	クリア 送信
中枢元DNS IF / F レスの設定 ホスト名称とIP アドレスの登録	
<u>ドメイン名称とDNS IPアドレスの</u> 登録	DNSのリクエストのドメイン名と、参照するDNSサーバのIPアドレスの組み合わせを登録し 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。

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。

	副院	ドメイン名称	DNS IPアドレス(プライマリ)	DNS IPアドレス(セカンダリ)
1		furukawa.co.jp	158 , poor , xxx , 100	158 , xxx , boot , 101
2				
3				
4				
5		1		
6				
7		1		
8		1		

8 [送

[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。

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。



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。

3

4

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。 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。 画面左側のメニューから [便利な設定]をク

5 [簡易DNS]をクリックします。

リックします。

h [ホスト名称とDNS IPアドレスの登録]をクリッ クします。

	簡易DNS
	簡易DNS機能 C OFF C DN
	クリア 送信
	以降は簡易DNS機能がONの時有効となります。
中継先DNS IPアドレスの設定	解決できないIONS要求のリレー先を指定します
ホスト名称とIPアドレスの登録	- DNSのデータベースを登録します
<u>ドメイン名称とDNS IPアドレスの</u> 登録	DNSのリクエストのドメイン名と、参照するDNSサーバのIPアドレスの組み合わせを登録し ます

次ページへ続く

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。

削除		ホスト名称	IPアドレス
1		www.furukawa.co.jp	203 . 192 . 162 . 36
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

8

g

[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。

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。

設定する

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。

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。 [電子メール通知]をクリックします。 次ページへ続く

2-98

6

設定する

| 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	● 使用しない C 使用する
差信先 义	ールアドレス	
[∋-x	ール递信先メールアドレス	
直知内容		□ 不正アクセス発覚時 □ Layer3監視エラー/復旧時 💡
17112		SMTPサーバのIPアドレス登録
	SMTPサーバのIPアドレス 送信元メールアドレス	swrpサーハのIPアドレス望立

•[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。

[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。

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。

設定する

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。

> 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。 画面左側のメニューから [便利な設定]をク Δ リックします。 [SNTP]をクリックします。

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。

[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。

装置を再起動します。

8

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。

設定する

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。

> 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。 Ζ 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。 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。 画面左側のメニューから [便利な設定]をク 4 リックします。 「送受信ログの設定」をクリックします。 「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。 送受信ログの設定 送受信ログを取得するかどうか C 取得する ● 取得しない ここへ変建されたデータをログに務します。 フロトコル 白島逆信 白島受信
> LM
> LM
> LM-LM
> LM-HA
> P99021
> L 07942 L 07942 L 04499762 L 04499762 099541 04499762 U 04499762 U 04499762 U 04499762 U 0449762 U 04497
> Image: Section 2016
> Image: Section 2016
> E
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999421
> 1999

クリア 送信

次ページへ続く

送受信ログを見るには (~ P4-26)



•[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]

8

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。

[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。

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。

設定する

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。





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。

離 通信先指定 ■ 10 アドレスとマスク長	中推先指定 [®]	x+U>0	プリファレンス
	© 1975 ↓ 2H2		

•[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。

|[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

設定する

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。

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。 画面左側のメニューから [詳細設定]をクリッ クします。 [ProxyARPの設定]をクリックします。 ProxyARPの動作モードを選択します。 h ProxyARPの設定 ♀ ○ しない ● 中継すべきアドレスのARPに答える ④全てのアドレスのARPに答える クリア 送信 [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。 X 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。



6 RIPを設定します。

a dia in			RIPの制	司御		
	-		ルーティン・	グ方法		-
		ルーティン	ノグ方法 🖓 C スタ © スタ	ティックのみ ティックとRIPを併用する		
			RIP送受信	制御		
インタフェース	RIPの受信	RIPの送信 🖗	RIP2パスワー F 🖗) 定明送信 🕅 (RIP送信「する」で有効)	RIPエージアウト	メトリック
LAN	C RIP1のみ C RIP2のみ © RIP1.2双方 C 受信しない	C RIP1 C RIP2 © 送信しない		C しない © 30 秒毎に送信	C しない © 180 秒で削除	0
TAN	C RIP1のみ C RIP2のみ C RIP1,2双方 C 受信しない	C RIP1 C RIP2 C 送信しない		C しない C 30 秒毎に送信	C しない C 180 秒で削除	D
PPPoE1	C RIP1のみ C RIP2のみ © RIP1,2双方 C 受信しない	C RIP1 C RIP2 ® 送信しない		C しない © 30 秒毎に送信	C しない © 180 秒で削除	D

- ・[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。

[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。

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。

8
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) 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。 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。 画面左側のメニューから [詳細設定]をクリッ 4 クします。 「受信RIPフィルタリングテーブル」をク リックします。 h 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

	受信RIPフィルタリングテ	ーブル
5	マィルタリング属性 🌍 デーブルに一致した ウィルタリング属性 🖓 デーブルに一致した	CURIP情報を有効にする -RIP情報を有効にする
	剤 隆 RIPの寬先IPアドレスとマスク長 前	● 受信インタフェース 🕅
1		LAN WAN pppoe1 pppoe2 pppoe3 pppoe4
2		LAN WAN pppoel pppoe2 pppoe3 pppoe4
3		LAN WAN pppoe1 pppoe2 pppoe3 pppoe4
4		LAN WAN pppoe1 pppoe2 pppoe3 pppoe4
5		LAN WAN pppoe1 pppoe2 pppoe3 pppoe4

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。

[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。

装置を再起動します。

8

Q

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。

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。
- **|**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

送(信RIPフィルタリ	リン グテーブル		
フィルタリン	ジ馬性 (*) [©] テーブル ク馬性 (*) ウ テーブル	こ一致しないRIP情報を有効にする こ一致したRIP情報を有効にする		
剤 降 RIPの宛先IPアドレスとマスク長	送信インタフェース	ルーティングブロトコル	AS#5	ASITZ
	LAN VAN PPPoel Pppoe2 pppoe3 Pppoe4	 全てのルーティングブロトコル C RIP C BGP C Asspreate C スタティック C ダイレクト 		
2	LAN VAN PPPOel PPPoel PPPoel PPPoel	 金てのルーティングブロトコル C RIP BDP Asgregate C スタティック ダイレクト 		
3	LAN VAN pppoel pppoe2 pppoe3 pppoe4	 全てのルーティングブロトコル C RIP C BGP C Apperente C スタティック C ダイレクト 		

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]

R

Q

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。

[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**

登録済みの受信フィルタリングテープ 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。

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**

設定例3 ユニキャスト宛RIP制御

設定する

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。

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。 [RIPの制御]をクリックします。

次ページへ続く



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。



		ユニキャスト宛RIP 制筆	, ?
	-	Lニキャスト宛RIP制御 C 値 C 値	8月しない 8月する
74 Bž	- 宛先IPアドレス 10	送信インタフェース 🕅	送信元アドレス
		C WAN C pppoel C pppoe2 C pppoe3 C pppoe4	 C LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	 C LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	 ○ LANのアドレスを使用する ◎ 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoel C pppoe2 C pppoe3 C pppoe4	 ○ LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	 ○ LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	 ○ LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	○ LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する
		C WAN C pppoe1 C pppoe2 C pppoe3 C pppoe4	 C LANのアドレスを使用する ● 通常の送信パケットと同じアドレスを使用する

•[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。

[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。

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。 Х

RIP**の制御**

設定例4 ルート情報提供ルータの指定

設定する

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。

|[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。

| 装置を再起動します。

8

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

設定する

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。



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**機能**



次ページへ続く

BGP機能

設定する

•[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。

	10000			I-BGPの登録	A Providence of the owner.	and the second se		
I	MR	internal type	877FL2	11-242F628	メトリック (0~65525) 🕅	原先表 1 (0~255) 省	held time (6-65535) 🖗	ダートウェイアドレス
•		グートウェイアドレスを参照 Cルーティングテーフルを参照		€ off ○,,,,			C ett C 90	C off C
2	-	ダートウェイアドレスを参照 Cルーティングテーフルを参照		e.,,,			C etr C 90	C off C
3	-	ダートウェイアドレスを参照 ベルーティングラーブルを参照		€ off ○,,,,			C ett @ 90	C off C
1000				597 送信				

- <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。

┃ |[送信]をクリックします。

▶ 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。



				フィルタ	リング席性	テーフ テーフ 受信B	ブルに・ ブルに・ GPフィ	- 歌した - 歌した ルタリ:	BGP情報をJ BGP情報をT ノグを使用	乾棄する 言効にする しない		
1	74 M2	シーケンス番号 1~50	1	Pアドレ	2			マスク	8	優先唐 0~~255	AS番号 1~65534	ASバス番号
١						-				170		
2			Ъ.Г				1.			170		
3			1.				1.			170		
4			Т. Г				1.	-		170		
5			1.				1.			170		
•]			Ъ. Г	— . [. [1.	- F	-	170		
1			1.				ЪГ			170		
•			Т. Г				1.			170		
•			1.				1.			170		
0			Т. Г				1. [-	_ . [170		

・[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。

[送信]をクリックします。





・[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"

1例) AS/XX/X、10 100 25」の場合は、10 100 25° と入力します。

|[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。

再起動します。

8

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。

設定する

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。





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。





8

設定する

Aggregate(7)	一般設	定
Aggregate動作モード	9	Con €off
Aggregate経路情報のM	_{憂先度}	130
לעל	送信	

- •[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。

/ [送信]をクリックします。

Aggregateテーブルを登録します。

Aggregateテーブルの登録
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。

Aggregateテーブルの登録							
Ri I	*yトワーク	7+142	#-ティングブロ - -=#₩	AS BER	45/L2 V		
• • 🗆 🗆		C マスクをがけて、IPアドレスと一致した情報をAggregate C IPアドレス、マスクとも一致する情報をAggregate C 上記の双力を満足する情報をAggregate	C スタティック C RIP C BBP C Apprepate C タイレクト		[
		C マスクをがけて、IPアドレスと一致した情報をAppregate C IPアドレス、マスクとも一致する情報をAppregate C LIDの対応調査で高級をAppregate	C 227492 C BIP C BSP C Apprepate C S4425		[
		C マスクをがけて、IPアドレスと一致した情報をAggregate C マスクをかけて、IPアドレスと一致した情報をAggregate C IPアドレス、マスクとも一致する情報をAggregate C レビの元力を満足する情報をAggregate	C 227172 C RIP C BBP C Apprepate C S14225				
•		C マスクを約りて、IPアドレスと一致した情報をAggregate C IPアドレス、マスクとも一致する情報をAggregate C 上記の方を満足する情報をAggregate	C 229472 C BIP C BIP C Appropriate C S4L21		[

・[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。

[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。

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。

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。

】 [TCP MSSの設定]をクリックします。

次ページへ続く

┣ TCP MSSの動作モードを選択します。

MSSの設定					
送信インタフェース	MSSE				
	C off				
LAN	 auto 				
	○ 設定値 (1240 ~ 1460)				
	C off				
EWAN	 auto 				
	○ 設定値 (1240 ~ 1460)				
	C off				
PPPoE1	 auto 				
	C 設定値 (1240 ~ 1452)				

• [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。

۰off

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。

[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。

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。

オペレーション

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。

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。

ログインID/パスワードを入力します。

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。

↓ 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。

P

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

 PPPoE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。
 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。

-	PPPoE和	御
名称	状況	制御
ProvederA	接続	切断します
ProvederB	接続	切断します
ProvederC	接続	切断します
ProvederD	接統	切断します

オペレーション

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>





3 オペレーション

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。

	IKE SA 解放
O全てのIN Osaid:[E SA を解放する を解放する SAIDの確認は <u>こちら</u>
	リセット 送信

IPsec SAの消去でも、同様の手順で消去できます。

オペレーション

<コマンド操作>

│ 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)

子 オペレーション

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。