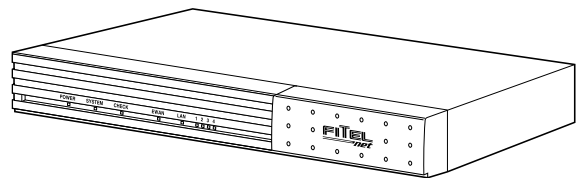
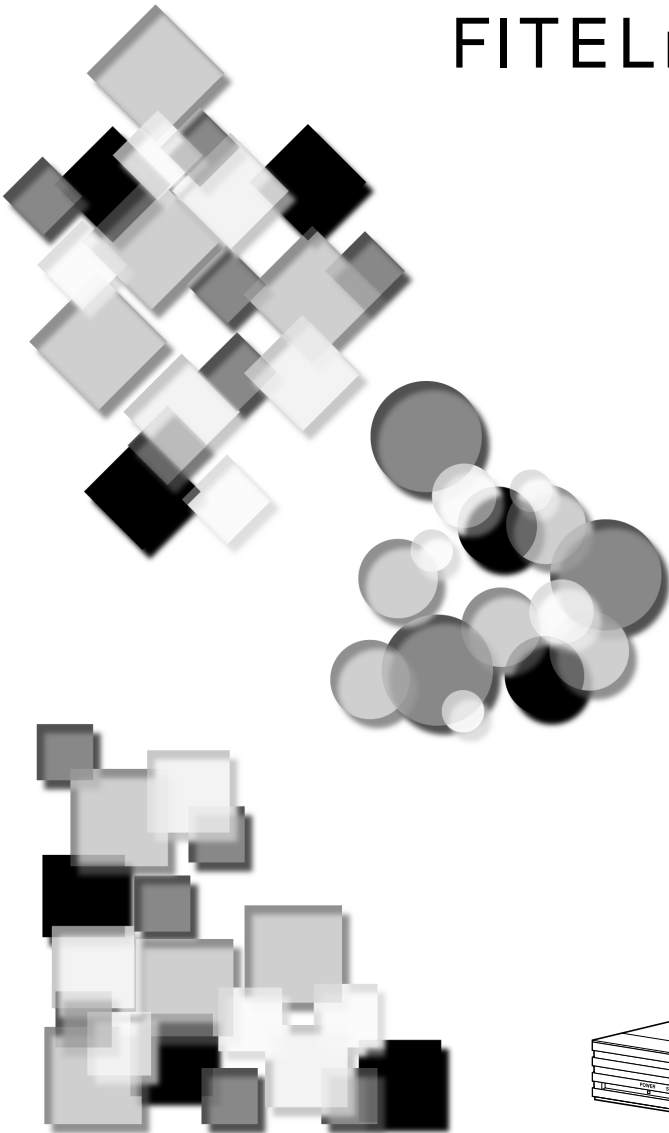


FITEL *net*

ブロードバンドアクセスマルタ

FITELnet-F40

取扱説明書



古河電工

この取扱説明書のみかた

《この取扱説明書の構成》

- 1 設定の準備**
Webブラウザやコマンドを使って本装置を設定するまでの準備について説明しています。
- 2 設定する**
本装置の設定方法と設定例を説明しています。
- 3 オペレーション**
PPPoEの接続/切断手順やVPN制御について説明しています。
- 4 インフォメーション**
本装置の運用やメンテナンスに必要な情報の閲覧方法を説明しています。
- 5 ご参考に**
エラーメッセージ、回線ログの一覧や、故障かな?と思ったときの確認方法などをご参考として説明しています。

《取扱説明書のページの構成》

章タイトル

章ごとにタイトルが付けられています。

タイトル

目的ごとにタイトルが付けられています。

ワンポイント

知っておくと便利な事項、操作へのアドバイスなどの補足説明です。

お願い

この表示を無視して、誤った取り扱いをすると、本装置の本来の性能を発揮できなかったり、機能停止を招く内容を示します。

お知らせ

この表示は、本装置を取り扱ううえでの注意事項を示します。

この取扱説明書のみかた

著作権及び商標について

Windows[®] は、米国Microsoft Corporationの米国及びその他の国における登録商標です。
Windows[®] 98の正式名称はMicrosoft[®] windows[®] 98 operating systemです。
Windows[®] Meは、Microsoft[®] Windows[®] Millennium Edition operating systemの略です。
Windows[®] 2000は、Microsoft[®] Windows[®] 2000 operating systemの略です。
Windows[®] XPは、Microsoft[®] Windows[®] XP operating systemの略です。
Microsoft Internet Explorerは、米国Microsoft Corporationの製品です。
画面の使用に際して米国Microsoft Corporationの許諾を得ています。
Macintoshは米国アップルコンピュータ社の商標です。
Mac OSは米国アップルコンピュータ社の登録商標です。
その他、本文中での記載の製品名や品名は各社の商標または登録商標です。
本書に、他社製品の記載がある場合、これは参考を目的にしたものであり、記載製品の使用を強制するものではありません。
本文中では、TMおよび[®]マークは記載していません。



StackerはStac Electronics社の登録商標です。
LZSはStac Electronics社の商標です。



Contains SSH IPSEC technology (pat,pending)
SSH is a registered trademark of SSH Communications Security Ltd
(<http://www.ssh.fi>)

目次

この取扱説明書のみかた	1-1
機能概要	1-6

1 設定の準備

設定する前に	1-8
動作環境	1-8
設定するまでの手順	1-8
Webブラウザの基本操作	1-9
Telnetの基本操作	1-11
モードの移行	1-13
コマンドの基本操作	1-14
パソコンのターミナルソフトを用意する	1-16
ログインIDを設定する	1-19
パスワードを登録、変更する	1-22
ログインパスワードを登録、変更する	1-22
コンフィグレーションパスワードを登録、変更する	1-25
現在時刻の設定	1-28
再起動	1-32
設定を初期化するには	1-34
設定画面の一般的な操作方法とみかた	1-39

2 設定する

設定について	2-1
簡単設定	2-2
設定例1 フレッツADSL接続設定	2-2
設定例2 DHCP接続設定	2-7
設定例3 手動接続設定	2-10
VPNの設定	2-13
設定例1 Pre-shared keyの設定	2-14
VPN動作モード	2-16
Phase1ポリシーの登録	2-18
Phase2ポリシーの登録	2-20
VPNピアの登録	2-23

VPN対象バケットの登録	2-29
設定例2 拡張認証の設定	2-35
VPN動作モード	2-37
Phase1ポリシーの登録	2-39
Phase2ポリシーの登録	2-41
VPNピアの登録	2-44
VPN対象バケットの登録	2-50
VPNを使用したNATスタティック機能	2-57
簡易ファイアウォール機能	2-58
設定例1 外部からの接続抑制	2-58
設定例2 IPパケットフィルタリング	2-61
中継するIPパケットの登録を行う	2-62
中継しないIPパケットの登録を行う	2-63
設定例3 学習フィルタリング	2-64
冗長機能	2-66
ルータグループ化機能	2-67
Layer3監視機能	2-69
マルチルーティング機能	2-71
マルチルーティング機能の設定	2-71
発信端末 / 宛先ポート番号の指定	2-72
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	2-73
SNMPエージェント機能	2-75
NAT機能	2-77
NATモードの場合の必須設定	2-77
設定例1 NAT ⁺ を使用してWebサーバを公開する	2-79
設定例2 NATを使用してWebサーバ / FTPサーバを公開する	2-82
DHCPリレーエージェント機能	2-85
DHCPサーバ機能	2-87
Syslogの送信	2-90
簡易DNS機能	2-92
設定例1 簡易DNS	2-92
設定例2 ドメイン名によるDNSの振り分け	2-94

目次

設定例3 ホスト名称とDNS IPアドレスの登録	2-96
電子メール通知機能.....	2-98
SNTP機能.....	2-100
送受信ログの設定.....	2-102
スタティックルーティング.....	2-104
Proxy ARP.....	2-106
RIPの制御.....	2-107
設定例1 RIP送受信制御.....	2-107
設定例2 RIPフィルタリング.....	2-109
受信RIPフィルタリングテーブル.....	2-109
送信RIPフィルタリングテーブル.....	2-111
設定例3 ユニキャスト宛RIP制御.....	2-113
設定例4 ルート情報提供ルータの指定.....	2-115
BGP機能.....	2-117
設定の流れ.....	2-117
BGPの一般設定.....	2-118
BGPピアの登録.....	2-119
BGPフィルタリング(受信)の設定.....	2-121
BGPフィルタリング(送信)の設定.....	2-123
Aggregate機能.....	2-125
設定の流れ.....	2-125
Aggregateの一般設定.....	2-126
Aggregateテーブルの登録.....	2-128
TCP MSSの設定.....	2-130

3 オペレーション

PPPoEの接続/切断手順.....	3-1
VPN制御.....	3-2
IKE SA/IPsec SAの消去.....	3-2
電子証明書リクエストデータの作成.....	3-5
CRL (Certificate Revocation List : 証明書失効リスト) の取得.....	3-5

4 インフォメーション

インフォメーション画面を表示する.....	4-1
装置情報を表示する.....	4-2
hereisコマンド、dateコマンド.....	4-2
通信状態を表示する.....	4-4
lineisコマンド.....	4-4
統計情報を表示する.....	4-6
stchannelコマンド、stipコマンド、vpnstatコマンド	4-6
ルーティングインタフェースを表示する.....	4-11
ipinterfaceコマンド.....	4-11
ルーティング状態を表示する.....	4-13
iprouteコマンド.....	4-13
BGPに関する情報を表示する.....	4-15
bgprouteコマンド、bgpstateコマンド.....	4-15
マルチルーティングに関する情報を表示する.....	4-17
multirouteisコマンド.....	4-17
DHCPサーバの状態を表示する.....	4-19
dhcpstatコマンド.....	4-19
NAT+の状態を表示する.....	4-21
natinfoコマンド.....	4-21
エラーログを表示する.....	4-22
elogコマンド.....	4-22
回線ログを表示する.....	4-23
llogコマンド.....	4-23
イベントログを表示する.....	4-25
vlogコマンド.....	4-25
送受信ログを表示する.....	4-26
clogコマンド.....	4-26
フィルタリングログを表示する.....	4-27
flogコマンド.....	4-27
電子メール通知統計を表示する.....	4-28
mailinfoコマンド.....	4-28

目次

VPNログを表示する	4-29	索引	5-24
vpnlogコマンド	4-29	仕様	5-27
VPN SAの状態を表示する	4-30		
vpnsainfoコマンド	4-30		
簡易DNSの情報を表示する	4-33		
proxydnstisコマンド	4-33		
DHCPクライアントの情報を表示する	4-34		
dhcpcinfoコマンド	4-34		
冗長機能に関する情報表示を表示する	4-36		
rgroupingisコマンド、pathchkisコマンド	4-36		
学習フィルタリングに関する情報表示を			
表示する	4-38		
sealedinfoコマンド	4-38		
DHCPリレーエージェントに関する情報表示を			
表示する	4-40		
stdhcprコマンド、dhcprdiscardコマンド	4-40		
電子証明書の情報を表示する	4-42		
vpncertinfoコマンド	4-42		
設定情報を確認する	4-43		
displayコマンド	4-43		

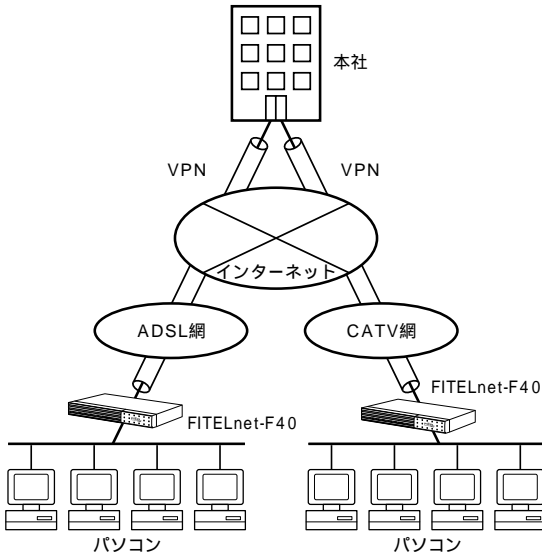
5 ご参考に

ファームウェアのアップデート	5-1
設定ファイルのアップデート/ダウンロード	5-5
設定ファイルのファイル転送	5-5
簡易コマンド入力	5-8
故障かな?と思ったら	5-9
エラーメッセージ一覧	5-10
コマンドによるping実行時のエラーメッセージ	5-10
コマンド入力時のエラーメッセージ	5-10
PPPoE使用時の回線ログ	5-11
VPN機能について	5-12
VPNの通信手順	5-12
BGP4について	5-14
PKI (公開鍵基盤) について	5-15
用語集	5-16

機能概要

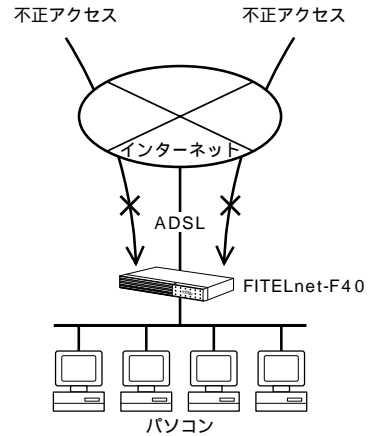
VPN機能

インターネットのようなオープンなネットワークを、専用線のように利用できます。



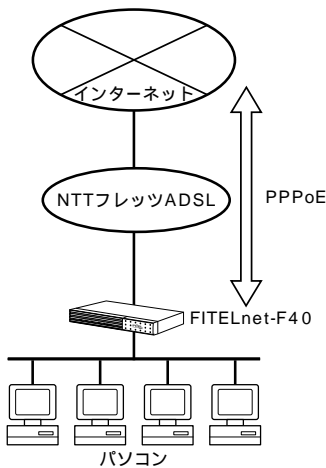
簡易ファイアウォール機能

不正なアクセスをシャットアウトできます。



PPPoE機能

PPPoEをサポート、NTTのフレッツADSLでも使用できます。



Webブラウザ設定

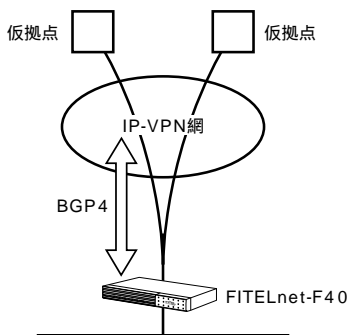
Microsoft Internet Explorer や Netscape Navigator などの Webブラウザを使った簡単設定ですから、初めてルータを使う方でも、ルータを使いこなしている方でも、簡単に素早く目的の機能を使いこなせます。



機能概要

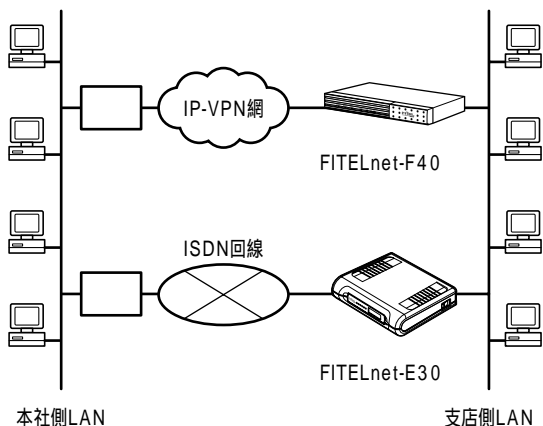
BGP4

IP-VPN網とBGP4の送受信を行い、IP-VPN網を含めたダイナミックルーティングを行うことができます。



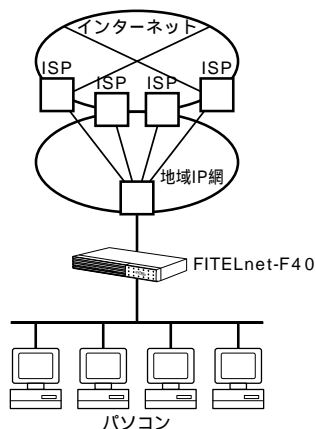
冗長機能

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、運用することができます。



PPPoE 4セッション

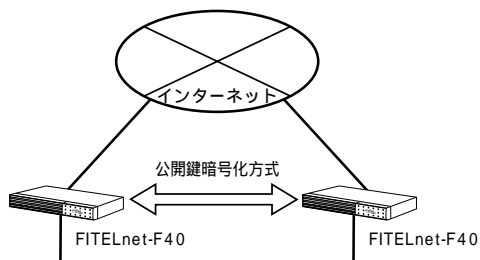
PPPoEを同時に4セッションまで接続することができます。4箇所のプロバイダと契約し、メールはこのプロバイダ、Webは別のプロバイダのような運用ができます。



PKI (公開鍵基盤) - X.509

電子証明書を利用した、公開鍵基盤に基づいたVPN通信を行うことができます。

PKI機能はオプションです。



設定する前に

本装置を設定するための動作環境や、設定する前に必要な手順を説明します。

動作環境

Windows[®] 98、Windows[®] 95、Windows[®] Me、Windows NT[®] 4.0、Windows[®] 2000、Windows[®] XP、Macintoshが動作しているパソコン
3Mバイト以上の空きがあるハードディスク

設定するまでの手順

以下の手順で、設定を行うための準備を行ってください。

1 パソコンに各ソフトウェアをインストールする

TCP/IPソフトウェア、Webブラウザなど設定に必要な各ソフトウェアの取扱説明書などを参照し、端末にインストールしてください。お使いの端末によってはあらかじめインストールされている場合もあります。詳しくは、ソフトウェアメーカーにお問い合わせください。

パソコンのIPアドレスを自動取得できるよう設定します。

2 パソコンのネットワークの設定を行う

お使いのパソコンの取扱説明書を参照してください。

3 パソコンの電源を切る

4 本装置とパソコンを接続する

本装置のLAN（1～4）ポートとパソコンを接続します。WANポートは接続しないでください。

5 本装置の電源を入れる

6 パソコンの電源を入れる

お使いのパソコンの取扱説明書を参照してください。

お知らせ

パソコンの詳細設定については『クイックスタートガイド』を参照してください。

お願い

本装置のLAN側ポートには、あらかじめIPアドレス（192.168.0.1）が設定されています。本装置の設定を行う前に、既存のLANへの接続は絶対にしないでください。

Webブラウザの基本操作

本装置はWWWサーバ機能を持っています。Webブラウザ（Netscape Navigator、Internet Explorerなど）を使って本装置にアクセスし、設定を行います。

1 Webブラウザを起動します。

2 URLに「http://192.168.0.1（本装置のIPアドレス）」と入力します。



3 ログインID/パスワードを入力します。

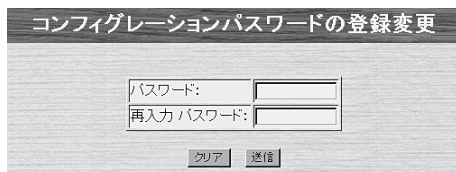
設定オープニング画面「ようこそ FITELnet-F40 設定画面」でログインID/パスワード（コンフィグレーションパスワード）を入力します。

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す。[送信]をクリックします。



4 パスワードの設定

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変更して、[次へ]をクリックします。



次ページへ続く

お知らせ

Webブラウザは一度アクセスした画面の内容を一定の期間記憶しておくことができます。再度同じ画面を表示しようとするとう記憶している画面を表示するため、最新の設定内容が表示されないことがあります。最新の設定内容を表示するには、Webブラウザの履歴（キャッシュ）をクリアするか、再読み込みをしてください。

モデムを使ってインターネットに接続していた場合は、Webブラウザの接続設定をLANを使った接続に変更してから、本装置にアクセスしてください。本装置のお買い求め時（工場出荷時）のIPアドレスは「192.168.0.1」に設定されています。はじめて本装置にアクセスするときは、URLに「http://192.168.0.1」と入力してください。

設定画面が表示されない場合は、次の内容を確認してください。

- ケーブルの接続（●クイックスタートガイド）
- 端末の設定（●クイックスタートガイド）

Webブラウザの操作に関しては、ソフトウェアメーカーにお問い合わせください。

推奨ブラウザ

Internet Explorer 5.0以上

Netscape Navigator 4.7以上

5 現在時刻の設定

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。

現在時刻の設定

現在の時刻は 2001年09月28日 08時46分20秒 となっています。変更する場合は、以下で変更します。
変更しない場合は、[次へ]

タイムサーバから現在時刻を取得する	タイムサーバのIPアドレス: 現在時刻を取得
手動で設定	2001年 09月 28日 08時 46分 装置に設定

6 画面左側のメニューから設定したい項目をクリックし、設定を行います。

- ログインID/パスワードの登録変更 (☛P1-19, 1-22)
- 現在時刻の設定 (☛P1-28)
- 簡単設定 (☛P2-1)
- 便利な設定 (☛P2-1)
- 詳細設定 (☛P2-1)
- 全設定情報を取得 (☛P4-43)
- PPPoE制御 (☛P3-1)
- VPN制御 (☛P3-2)
- インフォメーション (☛P4-1)
- 簡易コマンド入力 (☛P5-8)
- ファイル転送 (☛P5-5)
- 再起動 (☛P1-32)

7 設定が終わったら [送信] をクリックします。

設定した情報が装置に送られます。

8 再起動します。

設定を有効にするために、装置を再起動します。(☛P1-32)

Telnetの基本操作

本装置は、コマンドを入力しても機能設定を行うことができます。

設定する場合は、ログインパスワードを登録し(●P1-24) telnetでログインしてから設定を行います。

ここではMS-DOS画面からtelnetを起動して設定する方法を説明します。その他の方法で起動する場合はパソコンの取扱説明書などを参照してください。

1 MS-DOS画面を起動します。

2 「telnet LAN側IPアドレス」を入力します。

以下では、本装置のLAN側IPアドレスに「192.168.0.1」を例としています。お使いの本装置のLAN側IPアドレスを入力してください。

```
c:¥WINDOWS>telnet 192.168.0.1
```

↓ telnetが起動し、画面に次のように表示されます。

```
Login
```

3 ログインIDを入力します。

ログインIDの設定方法はP1-21を参照してください。

ログインIDが設定されていない場合は、ログインIDの問い合わせがありません。工場出荷時は、ログインIDは設定されていません。

```
Login: x x x x
```

4 ログインパスワードを入力します。

入力するパスワードは表示されません。また、カーソルも動きません。はじめてお使いになるときは、パスワードは設定されていません。[Enter]キーを押してください。

パスワードの設定方法は、P1-24を参照してください。

本装置にログインします。

```
Login password:
```

5 プロンプトが表示され、コマンド入力待ち状態になります。

```
#
```

6 設定したい機能のコマンドを入力し、設定を行います。

- パスワードの登録変更(●P1-24)
- 現在時刻の設定(●P1-29)
- 再起動(●P1-33)

7 設定する場合はコンフィグレーションモードに移行します。(●P1-13)

8 設定を保存します。(●P1-33)
コンフィグレーションモードで設定を変更した場合は、本装置を再起動します。(●P1-33)

モードの移行

機能を設定する場合はコンフィグレーションモードに移行してから設定を行います。

コンフィグレーションモードに移行する

1 コマンド入力待ち状態で「conf」と入力します。

```
#conf
```

2 コンフィグレーションパスワードを入力します。

入力するパスワードは表示されません。また、カーソルも動きません。ログインの際にコンフィグレーションパスワードを入力した場合は、パスワードの問い合わせはありません。

```
#conf  
Configuration password:
```

3 コンフィグレーションパスワードが正しいと、コンフィグレーションモードに移行し、confプロンプトが表示されます。

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

ワンポイント

コンフィグレーションモードを終了するには(●P1-33)

お願い

コンフィグレーションパスワードが設定されていない場合は、コンフィグレーションモードへ移行できません。先にコンフィグレーションパスワードを設定してください。(●P1-25)

コマンドの基本操作

本装置は、コマンドを入力しても機能設定を行うことができます。設定する場合は、ターミナルソフトを使って設定を行います。ここではWindows[®] 98に付属されているハイパーターミナルを使って設定する方法を説明します。(●P1-16) その他のターミナルソフトを使う場合は、パソコンの取扱説明書などを参照してください。

1 パソコンでハイパーターミナルを起動します。

2 本装置の電源を入れます。

3 ログインIDを入力します。

ログインIDの設定方法はP1-21を参照してください。
ログインIDが設定されていない場合は、ログインIDの問い合わせがありません。工場出荷時には、ログインIDは設定されていません。

Login: x x x x

4 ログインパスワードを入力します。

入力するパスワードは表示されません。また、カーソルも動きません。はじめてお使いになるときは、パスワードは設定されていません。[Enter]キーを押してください。

パスワードの設定方法は、P1-24を参照してください。

本装置にログインします。

Login password:

5 プロンプトが表示され、コマンド入力待ち状態になります。

#

次ページへ続く

コマンドの基本操作

6 設定する場合はコンフィグレーションモードに移行します。(●P1-13)

7 設定したい機能のコマンドを入力し、設定を行います。

- 各種設定 (●P2-1)

8 設定を保存します。(●P1-33)

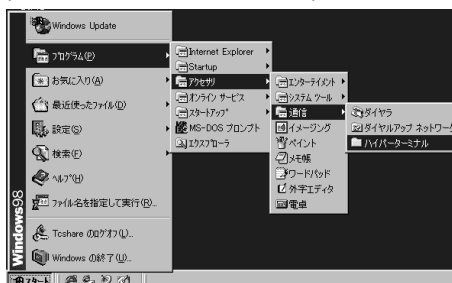
コンフィグレーションモードで設定を変更した場合は、本装置を再起動します。(●P1-33)

コマンドの基本操作

パソコンのターミナルソフトを用意する

- 1 [スタート]から、[プログラム][アクセサリ][通信]を経て、[ハイパーターミナル]を選択します。

(Windows® 98メニュー画面)



- 2 ハイパーターミナルのアイコン ([Hypertrm.exe]) をダブルクリックします。



- 3 [名前] に任意の名前を入力し、[OK] をクリックします。



次ページへ続く

コマンドの基本操作

- 4 [接続方法] に [Com 1ヘダイレクト] (コンソールケーブルをCom 1に接続した場合) を指定し、[OK] をクリックします。

(例) Com 1に接続したとき



- 5 COMポートのプロパティを入力し、[OK] をクリックします。

ビット/秒 : 9600
 データビット : 8
 パリティ : なし
 ストップビット : 1
 フロー制御 : Xon/Xoff



次ページへ続く

6 「新しい接続」ウィンドウが表示されます。



これでターミナルソフトの用意ができました。

ログインIDを設定する

ログインIDを設定します。ログインIDは、下記の場合に必要です。

- Webから装置の設定 / 運用を行う場合
- ファームウェアのアップデート / 設定ファイルを転送する場合

ログインIDは忘れないようにしてください。

< 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 FITEInet-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に [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 [ログインID / パスワード登録変更] をクリックします。



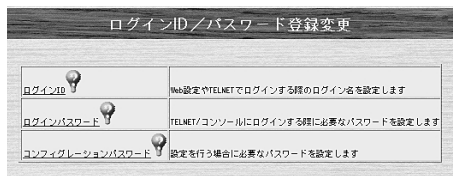
次ページへ続く

お願い

ログインIDを忘れた場合は、設定を初期化してください。(●P1-36)

ログインIDを設定する

5 「ログインID」をクリックします。



ログインID/パスワード登録変更	
ログインID	Web設定やTELNETでログインする際のログイン名を設定します
ログインパスワード	TELNET/コンソールにログインする際に必要なパスワードを設定します
コンフィグレーションパスワード	設定を行う場合に必要なパスワードを設定します

6 「ログインID」を入力します。
ログインIDは半角31文字以内で入力します。

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。

ログインIDを設定する

<コマンド操作>

1 コマンド入力待ち状態で「login」と入力します。

ログインIDをFITELとする場合

```
# login FITEL
```

2 ログインIDが設定され、入力待ち状態になります。

```
#
```

パスワードを登録、変更する

パスワードにはログインパスワードとコンフィグレーションパスワードがあります。ログインパスワードは本装置へログインする場合に、コンフィグレーションパスワードはコンフィグレーションモードに移行して設定する場合に入力します。コンフィグレーションパスワードが設定されていないと設定できません。

またコンフィグレーションパスワードが設定されていないと、ファームウェアのアップデートや設定ファイルの転送ができません。(●P5-1、5-5)

Webブラウザから設定する場合は、コンフィグレーションパスワードを入力します。

ログインパスワードを登録、変更する

< 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に[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 [ログインID / パスワード登録変更] をクリックします。

5 [ログインパスワード] をクリックします。

ログインパスワードの登録変更画面が表示されます。



6 旧パスワードを入力します。

はじめてログインパスワードを登録するときは、旧パスワードの入力は不要です。

お願い

パスワードを忘れた場合は、設定を初期化してください。(●P1-36)

次ページへ続く

パスワードを登録、変更する

7 新パスワードを入力します。
パスワードは、半角15文字以内で入力します。

8 確認のため、新パスワードをもう一度入力します。



ログインパスワードの登録変更

旧パスワード:	●●●●●●
新パスワード:	●●●●●●
再入力 新パスワード:	●●●●●●

クリア 送信

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

パスワードを登録、変更する

<コマンド操作>

- 1 コマンド入力待ち状態で「password」と入力します。

```
#password
```

- 2 現在設定されているパスワードを入力します。
入力するパスワードは表示されません。また、カーソルも動きません。パスワードが設定されていない場合は「old password」は表示されませんので、手順3に進んでください。

```
#password  
old password:
```

- 3 新しいパスワードを入力します。確認のためもう一度新しいパスワードを入力します。

```
#password  
old password:  
new password:  
retype password:
```

- 4 パスワードが更新され、入力待ち状態になります。

```
#
```

お知らせ

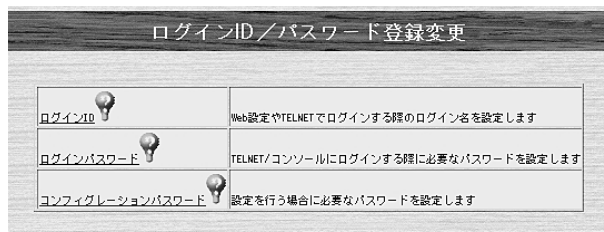
コマンドでパスワードを設定する場合、LANポート経由、CONSOLEポート経由ともに操作手順は同じです。

パスワードを登録、変更する

コンフィグレーションパスワードを登録、変更する

< 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に [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 [ログインID / パスワード登録変更] をクリックします。
- 5** [コンフィグレーションパスワード] をクリックします。
コンフィグレーションパスワードの登録変更画面が表示されます。



- 6** 旧パスワードを入力します。
初めてコンフィグレーションパスワードを登録するときは、旧パスワードの入力は不要です。

お願い

パスワードを忘れた場合は、設定を初期化してください。(P1-36)

次ページへ続く

パスワードを登録、変更する

7 新パスワードを入力します。
パスワードは、半角15文字以内で入力します。

8 確認のため、新パスワードをもう一度入力します。



The screenshot shows a web interface for changing the configuration password. The title is 'コンフィグレーションパスワードの登録変更'. There are three input fields: '旧パスワード:' (Old Password), '新パスワード:' (New Password), and '再入力 新パスワード:' (Re-enter New Password). Each field contains a series of dots representing masked characters. Below the fields are two buttons: 'クリア' (Clear) and '送信' (Send).

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

パスワードを登録、変更する

<コマンド操作>

- 1 コマンド入力待ち状態で「password -c」と入力します。

```
#password -c
```

- 2 現在設定されているパスワードを入力します。
入力するパスワードは表示されません。また、カーソルも動きません。パスワードが設定されていない場合は「old password」は表示されませんので、手順3に進んでください。

```
#password -c  
old password:
```

- 3 新しいパスワードを入力します。確認のためもう一度新しいパスワードを入力します。

```
#password -c  
old password:  
new password:  
retype password:
```

- 4 パスワードが更新され、入力待ち状態になります。

```
#
```

お知らせ

コマンドでパスワードを設定する場合、LANポート経由、CONSOLEポート経由ともに操作手順は同じです。

現在時刻の設定

設定には、タイムサーバを指定して設定する方法と、手動で入力する方法があります。また設定操作は、パスワード入力後に表示される設定画面と、画面左側のメニューから選択できる設定画面で入力できます。

1. 手動で設定する場合

< 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 [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 「手動で設定」の項目で年（西暦）、月、日、時刻を設定します。

◆ をクリックすると一覧が表示されて、その中から設定する項目を選択することができます。

現在時刻の設定

現在の時刻は 2001年09月28日 08時46分20秒 となっています。変更する場合は、以下で変更します。
変更しない場合は、[次へ](#)

タイムサーバから現在時刻を取得する タイムサーバのIPアドレス:

手動で設定 現在時刻を取得

2001 年 09 月 28 日 08 時 46 分

[装置に設定](#)

4 設定が終わったら、[装置に設定] をクリックします。

設定内容が本装置に送信されます。

お願い

お買い求め直後や、しばらく電源をOFFにした場合は、内蔵の時計が遅れることがありますので、必ず時刻の設定を行ってください。

<コマンド操作>

1 コマンド入力待ち状態で「date」と入力し、続けて年（西暦）、月、日、時刻を入力します。

年は西暦の下2桁を入力します。

（例）2001年10月30日12時0分0秒を設定する場合

```
#date 011030.120000
```

2 時刻が設定され、入力待ち状態になります。

```
#
```

現在時刻の設定

2. タイムサーバから時刻を取得する場合

< Webブラウザ操作 >

タイムサーバとは、現在時刻の情報を供給してくれるサーバです。タイムサーバを指定して、[現在時刻を取得] をクリックすることで、FITELnet-F40の時刻を設定することができます。

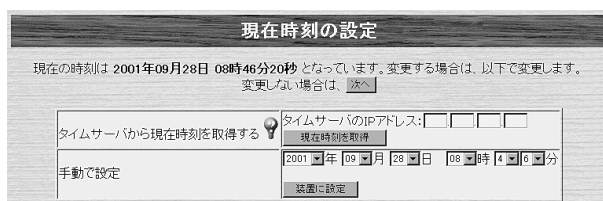
1 設定画面を起動し、本装置にログインします。
(P1-9)

2 画面左側のメニューから [現在時刻の設定] をクリックします。

現在時刻の設定画面が表示されます。



3 タイムサーバに指定したパソコンのIPアドレスを入力します。



4 [現在時刻を取得] をクリックします。

<コマンド操作>

- 1 コマンド入力待ち状態で「syncclock」と入力し、続けてタイムサーバのIPアドレスを入力します。

```
#syncclock xxx.xxx.xxx.xxx
```

- 2 タイムサーバに接続し、時刻が設定されます。

```
#
```


再起動

更新された設定項目によっては、本装置が再起動されない限り本装置に対して有効になりません。設定を有効にするには本装置を再起動してください。

< Webブラウザ操作 >

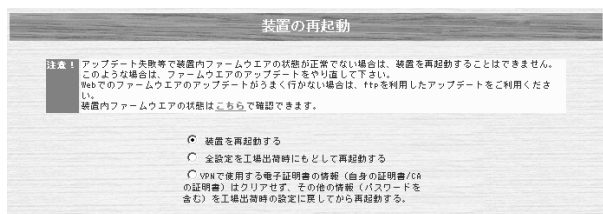
1 設定画面を起動し、本装置にログインします。
(☛P1-9)

2 画面左側のメニューから [装置の再起動] をクリックします。

[装置の再起動] 画面が表示されます。



3 [装置を再起動する] をチェックします。



4 [送信] をクリックします。

本装置が再起動され、設定が本装置に対して有効になります。

< コマンド操作 >

- 1 コンフィグレーションモードのコマンド入力待ち状態で「exit」と入力します。

```
conf#exit
```

- 2 次のように表示されたら「y」と入力します。
コンフィグレーションモードが終了し、設定が保存されます。

```
conf#exit  
configuration modified. save OK? (y/n) :y
```

- 3 設定が更新されているときは、「please reset#」が表示されます。

```
conf#exit  
configuration modified. save OK? (y/n) :y  
please reset#
```

- 4 「reset」と入力します。

```
please reset#reset
```

- 5 次のように表示されたら「y」と入力します。
本装置が再起動されます。しばらくするとログイン画面が表示され、設定が本装置に対して有効になります。

```
please reset#reset  
Do you want to continue (y/n)? :y
```

設定を初期化するには

本装置を初期値（工場出荷時の値）に戻すことができます。初期化すると、ログインパスワード、コンフィグレーションパスワードもクリアされます。

FITELnet-F40では、設定を初期値に戻す方法に2種類の方法があります。

1. 全設定を初期値に戻す（●P1-34）
2. 電子証明書以外の情報を初期値に戻す（●P1-37）

1. 全設定を工場出荷時設定に戻すには

< Webブラウザ操作 >

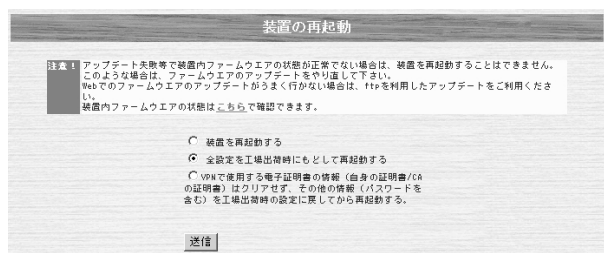
1 設定画面を起動し、本装置にログインします。
（●P1-9）

2 画面左側のメニューから [装置の再起動] をクリックします。

[装置の再起動] 画面が表示されます。



3 [全設定を工場出荷時に戻して再起動する] をチェックします。



4 [送信] をクリックします。

本装置が再起動され、設定が工場出荷時の状態に戻ります。

設定を初期化するには

<コマンド操作>

- 1 本装置の電源を入れ、ログインします。
(●P1-11、1-14)

```
#
```

- 2 「reset -d」と入力します。

```
#reset -d
```

- 3 コンフィグレーションパスワードを入力します。

入力するパスワードは表示されません。またカーソルも動きませ

```
#reset -d  
Configuration password:
```

- 4 確認の画面が表示されますので、再起動してよければ「y」を入力します。

```
Do you want to continue (y/n)? : y
```

- 5 設定が工場出荷時の状態に戻り、本装置が再起動します。

お知らせ

ログインの際にコンフィグレーションパスワードを入力した場合は、パスワードの問い合わせはありません。

お願い

「設定を初期化するには」の手順3で、コンフィグレーションパスワードが設定されていない場合は、「not yet password」と表示されますので、まずコンフィグレーションパスワードを設定してください。
(●P1-27)

設定を初期化するには

<ディップSWの操作>

- 1 本装置の電源を切ります。
- 2 背面のディップSW5を [ON] 側にします。
- 3 本装置の電源を入れます。
設定が初期化され、工場出荷時の状態に戻ります。
- 4 ディップスイッチを戻します。
ディップSW5を [OFF] 側に戻します。

設定を初期化するには

2. 電子証明書以外の情報を工場出荷時設定に戻すには
PKI（公開鍵基盤）- X.509機能で使用する電子証明書以外の
情報を工場出荷状態にして再起動します。

< Webブラウザ操作 >

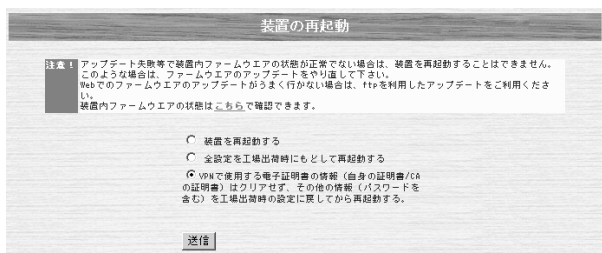
- 1 設定画面を起動し、本装置にログインします。
(P1-9)

- 2 画面左側のメニューから [装置の再起動] をクリックします。

[装置の再起動] 画面が表示されます。



- 3 [VPNで使用する電子証明書の情報（自身の証明書 / CAの証明書）はクリアせず、その他の情報（パスワードを含む）を工場出荷時の設定に戻してから再起動する] をチェックします。



- 4 [送信] をクリックします。

本装置が再起動され、電子証明書以外の情報が工場出荷時の状態に戻ります。

お知らせ

PKI機能は、オプションです。

設定を初期化するには

<コマンド操作>

- 1 本装置の電源を入れ、ログインします。
(●P1-11、1-14)

#

- 2 「reset -1」と入力します。

#reset -1

- 3 コンフィグレーションパスワードを入力します。

入力するパスワードは表示されません。またカーソルも動きませ

#reset -1
Configuration password:

- 4 確認の画面が表示されますので、再起動してよければ「y」を入力します。

Do you want to continue (y/n)?: y

- 5 電子証明書の情報以外が工場出荷時の状態に戻り、本装置が再起動します。

お知らせ

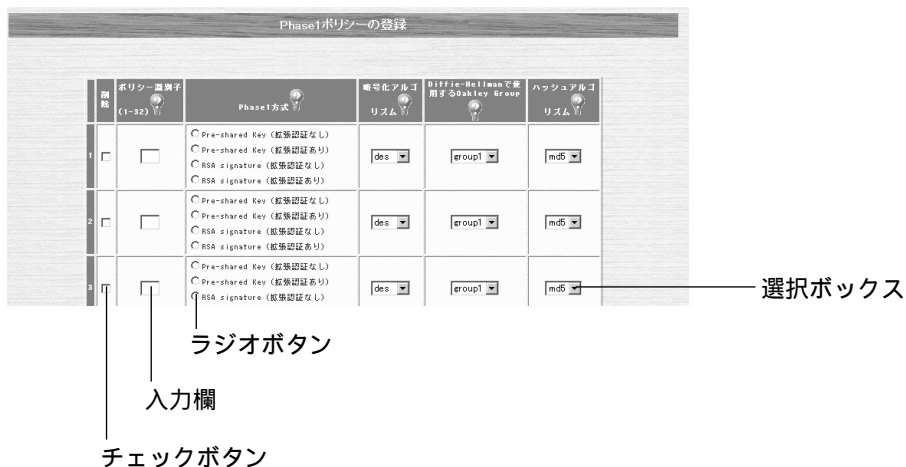
ログインの際にコンフィグレーションパスワードを入力した場合は、パスワードの問い合わせはありません。

お願い

「設定を初期化するには」の手順3で、コンフィグレーションパスワードが設定されていない場合は、「not yet password」と表示されますので、まずコンフィグレーションパスワードを設定してください。
(●P1-27)

設定画面の一般的な操作方法とみかた

(例) Phase1ポリシー登録画面



チェックボタン

画面の項目の左にある のボタンです。チェックボタンがついている設定項目は、複数選択することができます。また、どれか一つを選択する、またはどれも選択しない設定ができます。クリックするとチェックマーク✓になります。チェックマークがつくと選択されたことになります。

入力欄

画面の入力欄があり、数値やアドレスを入力するときは、入力欄をクリックします。カーソルが表示されて、数値が入力できるようになります。

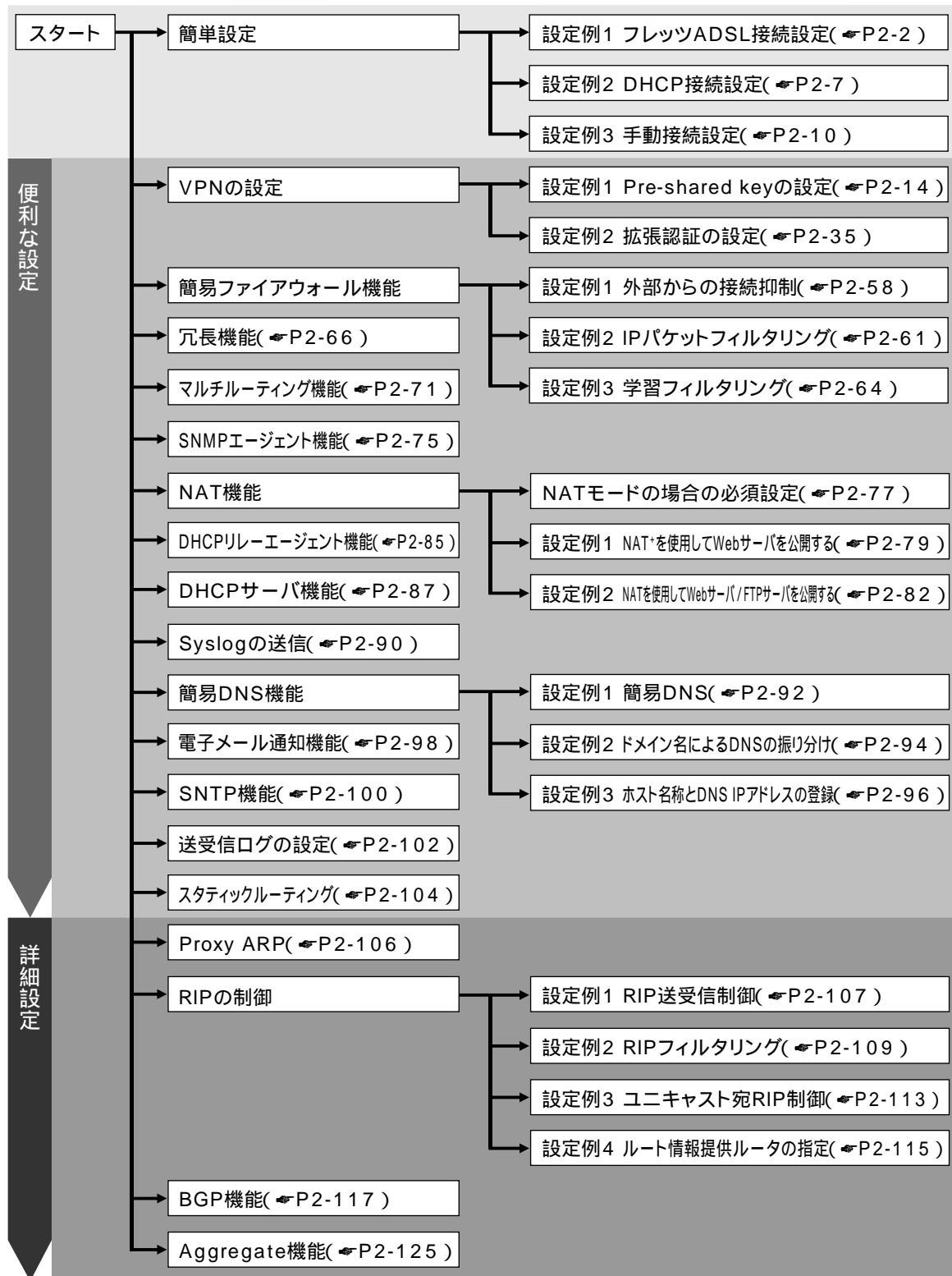
ラジオボタン

画面の項目の左にある や のボタンです。ラジオボタンがついている設定項目は、どれか1つしか選択できません。 が現在の設定値です。変更するときは をクリックして にします。

選択ボックス

選択されている項目は、選択ボックスに表示されています。 をクリックすると、選択項目の一覧が表示されて、その中から設定する項目をクリックして選択することができます。

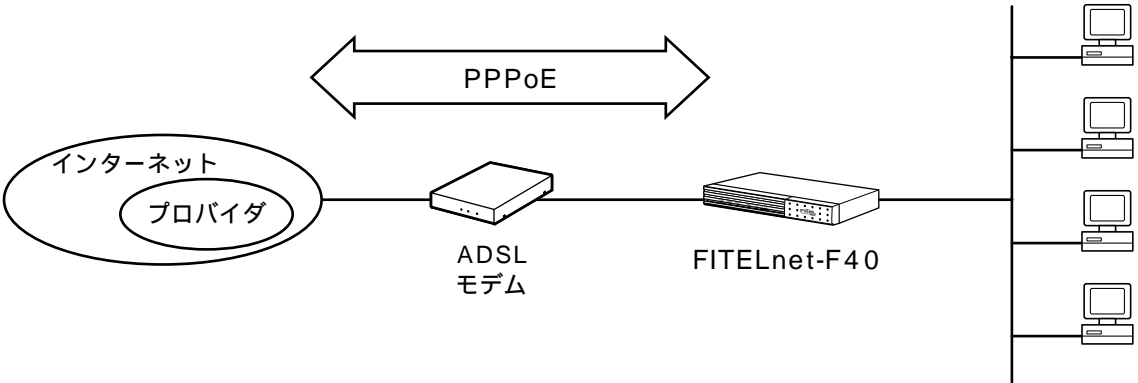
接続例と設定方法を説明しています。
 具体的な操作方法は、P2-2～P2-128をご覧ください。



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		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	
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 >

- 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

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。

< 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
```

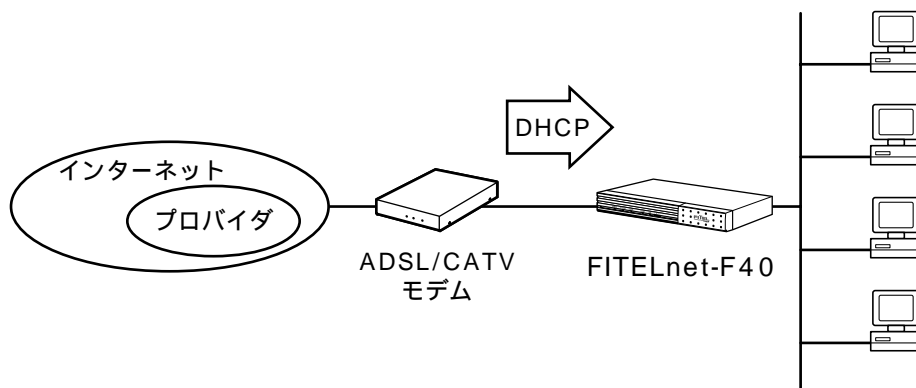
次ページへ続く

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
```

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には、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

- 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。

簡単設定

現在は、WAN運用形態の設定がDHCPクライアントになっています。

〈現在のIPアドレス:xxxxxx.xxxx.xxxx〉 アドレスを取得しなおす

WAN側 運用形態	PPP over Ethernet 手動設定
MTU長	
ホスト名	
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 <input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DNSサーバ	プライマリ
	セカンダリ
	簡易DNS機能 <input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
NAT動作モード	<input checked="" type="radio"/> OFF <input type="radio"/> NAT+

登録する 変更前に戻す

- 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。

<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。

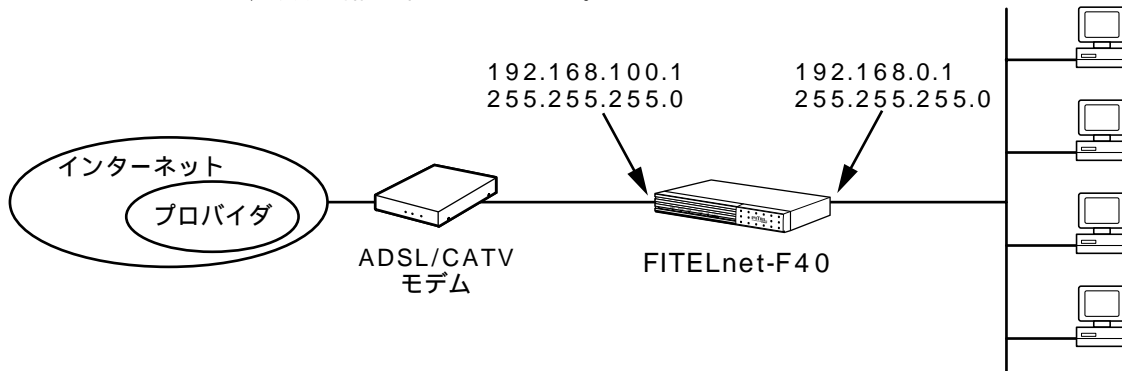
```
conf# nat wan natp
```

- 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
```

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には、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

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。

簡単設定

現在は、WAN運用形態の設定が手動設定になっています。

WAN側 運用形態	<input type="radio"/> PPP over Ethernet <input type="radio"/> DHCPクライアント
MTU長	<input type="text"/>
WAN側 IPアドレス	IPアドレス <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> サブネットマスク <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
LAN側 IPアドレス	IPアドレス <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> サブネットマスク <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> . <input type="text"/> <input type="text"/> DHCPサーバ機能 <input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
デフォルトゲートウェイ	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
DNSサーバ	プライマリ <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> セカンダリ <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 船尾DNS機能 <input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
NAT動作モード	<input checked="" type="radio"/> OFF <input type="radio"/> NAT+

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。

<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#ipipstatic delete default
conf#ipipstatic 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）

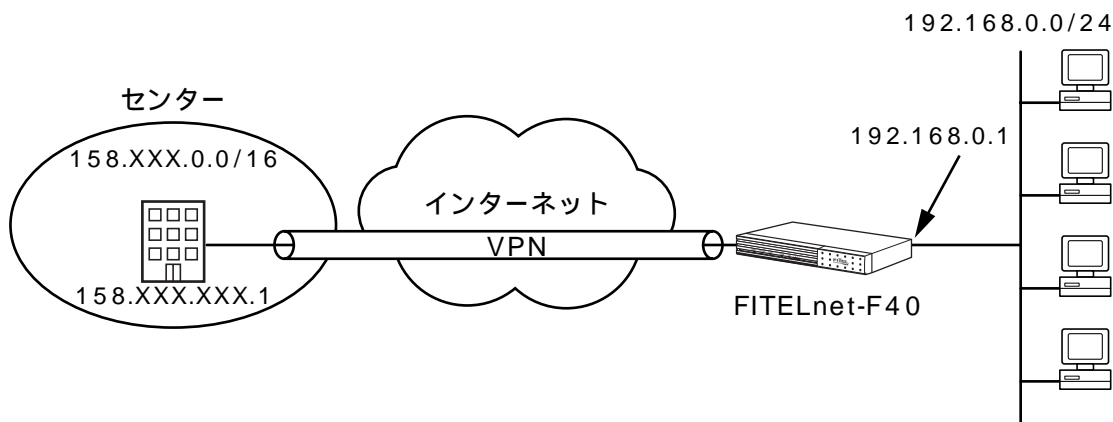
ワンポイント

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	158.xxx.xxx.1
		相手名称指定	空欄
		こちらの名前	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。

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[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。

便利な設定	
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
IPパケットフィルタリング	IP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をフィルタリング(遮断)する場合に設定します
BMPエージェント	BMP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⇄WAN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の送信	本装置のログ情報を、外部のSYSLOGサーバに送信する場合に設定します
簡易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通知する場合に設定します
SMTP	現在時刻の情報を、外部のSMTP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 (Phase) を使用する場合に設定します
冗長機能	FITElnet-E30と組み合わせて、ADSL回線の障害を150Wでバックアップする場合に設定します
DHCPクライアントエージェント機能	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った場合に設定します
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変更したい場合に設定します。

次ページへ続く

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の設定

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)

VPN動作モード OFF ON

以下はVPN動作モードがONの特有効となります。

鍵ペアの生成	公開鍵と秘密鍵のペアを生成します。電子証明書を使用 (RSA signature) する場合は、必ず行ってください。
証明書登録用パラメータ	自身の証明書を作成するためのパラメータ値を設定します
ここで装置を再起動してください	
証明書リクエストデータの生成	証明書を生成するためのリクエストデータを生成します
証明書の登録	自身の証明書およびCAの証明書を登録/削除します
ここで装置を再起動してください	
Phase1ポリシーの登録	IPsec Phase1のポリシーエントリを登録します
Phase2ポリシーの登録	IPsec Phase2のポリシーエントリを登録します
VPNピアの登録	IPsecトンネルを確立する相手の登録をします
VPN対象パケットの登録	VPN対象データを登録します
VPN NATスタティック登録	VPN NATのスタティック情報を設定します

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。

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。

削除		ポリシー識別子	
		(1-32)	
1	<input type="checkbox"/>	1	

- [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
<input checked="" type="radio"/> Pre-shared Key（拡張認証なし）
<input type="radio"/> Pre-shared Key（拡張認証あり）
<input type="radio"/> RSA signature（拡張認証なし）
<input type="radio"/> RSA 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。）

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	Diffie-Hellmanで使用するOakley Group	ハッシュアルゴリズム
des	group1	md5

- [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。

鍵データ (PFS) の再生成	PFSで使用するOakley Group
<input type="radio"/> する <input checked="" type="radio"/> しない	group1

- [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	認証アルゴリズム
des	hmac-md5

- [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	圧縮ネゴシエーション
<input type="radio"/> 圧縮する <input checked="" type="radio"/> 圧縮しない	<input type="radio"/> する <input checked="" type="radio"/> 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。

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。

削除	VPNピア識別 
1 <input type="checkbox"/>	相手IPアドレス指定: 158 - xxx - xxx - 1 相手名称指定: _____ こちらの名前: FITElnet-F40

- [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。

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。)

次ページへ続く

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。

FQDNタイプ

FQDN

UserFQDN

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。

拡張認証

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。

ワンポイント

FQDNタイプ (●P5-17)

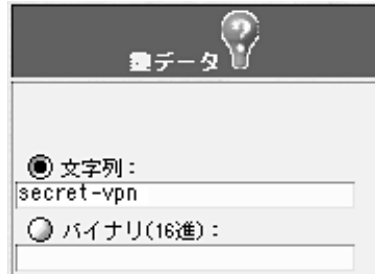
次ページへ続く

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 	DN (Distinguished Name) 
<input type="text"/>	<input type="text"/>
domainname 	<input type="text"/>

- [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。

Phase1ポリシー 

識別子 

1 

- 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)

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。

削除	優先度(1-64)
1	<input type="text"/>

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。)

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。

宛先指定

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

すべてのポート
 ポート番号の指定

次ページへ続く

• [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。

The screenshot shows two adjacent dropdown menus. The left menu is titled 'プロトコル' (Protocol) and has '全て' (All) selected. The right menu is titled 'IPsec処理タイプ' (IPsec Processing Type) and has 'IPsec処理して中継' (IPsec processing and relay) selected.

- [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。

The screenshot shows the 'SA確立契機' (SA Establishment Trigger) configuration screen. It contains several dropdown menus: '起動時確立しない' (Do not establish at startup), 'データ通信時' (During data communication), '回線がダウンした場合の制御' (Control when the line goes down) with '回線が確立してもSA確立動作を行わない' (Do not perform SA establishment action even if the line is established) selected, and 'リトライ' (Retry) with 'リトライしない' (Do not retry) selected.

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。

<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
```

ワンポイント

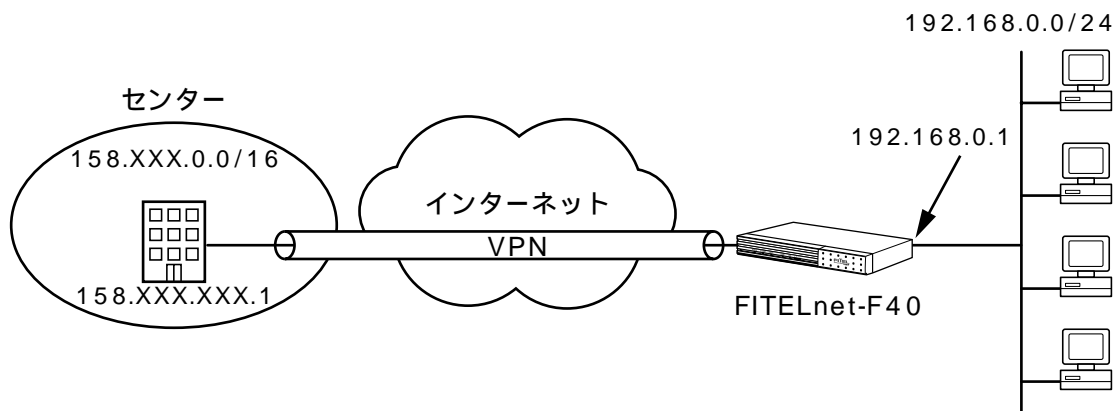
VPN以外はインターネット接続を行うためには手順6で、以下のコマンドを設定します。

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

7 設定を保存します。

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

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	158.xxx.xxx.1
		相手名称指定	空欄
		こちらの名前	FITELnet-F40
		FQDNタイプ	User FQDN
		拡張認証	相手を認証しない *
		相手のパスワード	空欄
		ユーザ管理用名称	admin-FITELnet-F40
		こちらのパスワード	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 [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。

便利な設定	
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
IPパケットフィルタリング	IP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
SNMPエージェント	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側WAN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の送信	本装置のログ情報を、外部のSYSLOGサーバに送信する場合に設定します
簡易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通知する場合に設定します
SMTP	現在時刻の情報を、外部のSMTP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
遠端ログの設定	遠端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
冗長機能	FITELnet-E30と組み合わせて、4054回路の障害を150kでバ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、WAN側にリレーし、WAN側のDHCPサーバから割り当ててもらった場合に設定します
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変更したい場合に設定します。

次ページへ続く

6 VPN動作モードの [ON] を選択し、[送信] をクリックします。

VPNの設定

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)

VPN動作モード OFF ON

以降はVPN動作モードがONの特有効となります。

鍵ペアの生成	公開鍵と秘密鍵のペアを生成します。電子証明書を使用 (RSA signature) する場合は、必ず行ってください。
証明書登録用パラメータ	自身の証明書を作成するためのパラメータ値を設定します ここで装置を再起動してください
証明書リクエストデータの生成	証明書を生成するためのリクエストデータを生成します
証明書の登録	自身の証明書およびCAの証明書を登録/削除します ここで装置を再起動してください
Phase1ポリシーの登録	IPsec Phase1のポリシーエントリを登録します
Phase2ポリシーの登録	IPsec Phase2のポリシーエントリを登録します
VPNピアの登録	IPsecトンネルを確立する相手の登録をします
VPN対象パケットの登録	VPN対象データを登録します
VPN_NATスタティック登録	VPN NATのスタティック情報を設定します

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。

削除		ポリシー識別子	
		(1-32)	
1	<input type="checkbox"/>	1	<input type="text"/>

- [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	
<input type="radio"/>	Pre-shared Key（拡張認証なし）
<input checked="" type="radio"/>	Pre-shared Key（拡張認証あり）
<input type="radio"/>	RSA signature（拡張認証なし）
<input type="radio"/>	RSA 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。

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。）

次ページへ続く

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	Diffie-Hellmanで使用するOakley Group	ハッシュアルゴリズム
des	group1	md5

- [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。

削除		ポリシー識別子 (1-64)
1	<input type="checkbox"/>	1

- [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。

SAライフタイム
時間(秒: 60以上からの指定): 600
転送サイズ(kbytes: 1000以上からの指定): 0

- [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。

鍵データ (PFS) の再生成	PFSで使用するOakley Group
<input type="radio"/> する <input checked="" type="radio"/> しない	group1

- [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	認証アルゴリズム
des	hmac-md5

- [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 	圧縮ネゴシエーション 
<input type="radio"/> 圧縮する	<input type="radio"/> する
<input checked="" type="radio"/> 圧縮しない	<input checked="" type="radio"/> 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。

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。

削除	VPNピア識別 
1 <input type="checkbox"/>	相手IPアドレス指定: 158 - .xxx - .xxx - 1 相手名称指定: _____ こちらの名前: FITELnet-F40

- [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。

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。)

次ページへ続く

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。

FQDNタイプ

FQDN

UserFQDN

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。

拡張認証

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。

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	DN (Distinguished Name)
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

- [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。

**Phase1ポ
リシー選
別子**

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。

- 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)

- 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。)

- 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

- [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。

[ppoe1] 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。

The screenshot shows two adjacent configuration panels. The left panel is titled 'プロトコル' (Protocol) and has a dropdown menu set to '全て' (All). The right panel is titled 'IPsec処理タイプ' (IPsec Processing Type) and has a dropdown menu set to 'IPsec処理して中継' (IPsec processing and relay).

- [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：セレクト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。

The screenshot shows the 'SA確立契機' (SA Establishment Trigger) configuration page. It contains several dropdown menus: '起動時確立しない' (Do not establish at startup), 'データ通信時' (During data communication), '回線がダウンした場合の制御' (Control when the line goes down) with the option '回線が確立してもSA確立動作を行わない' (Do not perform SA establishment action even if the line is established), and 'リトライ' (Retry) with the option 'リトライしない' (Do not retry).

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。

<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#vpnpolicy 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。

VPN NATスタティック登録 VPNピア選択

	No.	アドレス	相手名称	VPN NATモード
選択	1	158.202.236.17		nat+
選択	2			

- 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.	アドレス	相手名称	VPN NATモード
1	158.202.236.17		nat

種別	LAN上の端末指定 IPアドレス	外側に見えるIPアドレス	マスク指定
1	<input type="checkbox"/> 192 . 168 . 100 . 0	192 . 168 . 0 . 0	255 . 255 . 255 . 0
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		

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 [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。

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。

<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

<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。

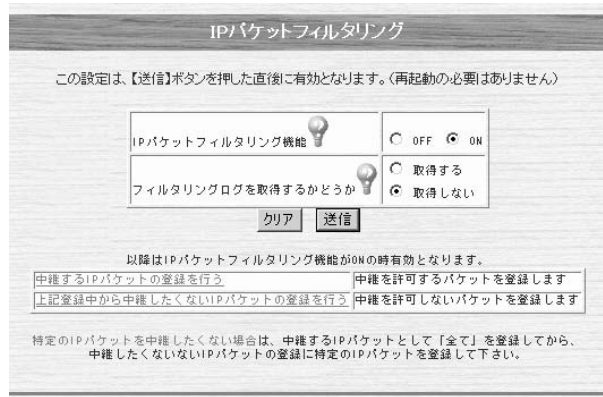
7 [送信] をクリックします。

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 (← P 2-62)
- 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 (← P 2-63)

- 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 (← P 4-27)

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。

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。

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。

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。

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。

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。

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。

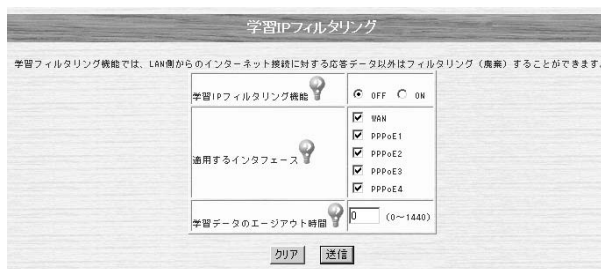
学習フィルタリング機能を使用する場合は、外部からのアクセス（Web等）はできなくなります。（アクセスを許可するアドレスを限定することはできません）

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。

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。〈オプション設定〉

削除	IPアドレス	サブネットマスク	削除	IPアドレス	サブネットマスク	
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	17	<input type="checkbox"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	18	<input type="checkbox"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	19	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	20	<input type="checkbox"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	21	<input type="checkbox"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	22	<input type="checkbox"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	23	<input type="checkbox"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	24	<input type="checkbox"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	25	<input type="checkbox"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	26	<input type="checkbox"/>	<input type="text"/>
11	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	27	<input type="checkbox"/>	<input type="text"/>
12	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	28	<input type="checkbox"/>	<input type="text"/>
13	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	29	<input type="checkbox"/>	<input type="text"/>
14	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	30	<input type="checkbox"/>	<input type="text"/>
15	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	31	<input type="checkbox"/>	<input type="text"/>
16	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	32	<input type="checkbox"/>	<input type="text"/>

クリア 送信

- [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。

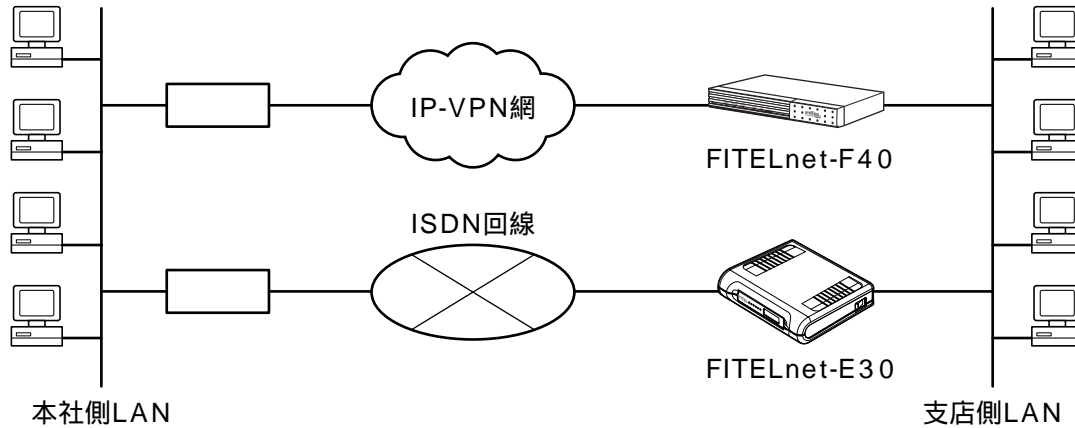
設定内容を有効にするために、FITELnet-F40を再起動します。画面左側のメニューの中から、[装置の再起動] をクリックします。
[装置を再起動する] をチェックしてから、[送信] をクリックします。

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。

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）

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。

設定項目	設定値	範囲
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	0.0.0.0	
グループ内共有データの送信間隔	5	(5~45)
グループ内のルータを異常と見なすまでの時間	15	(15~100)

クリア 送信

- ・[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て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ては、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ては、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。

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。

経路監視機能の登録 (Layer3監視機能)

設定項目の意味はこちら

Layer3監視を行う宛先IPアドレス	:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Layer3監視パケットの定期送信間隔	:	<input type="text"/>	秒 (30~1800)		
経路異常時の、Layer3監視パケット送信間隔	:	<input type="text"/>	秒 (30~1800)		
障害と判断するまでの時間	:	<input type="text"/>	秒 (60~3600)		
障害復旧と判断するまでの時間	:	<input type="text"/>	秒 (90~5400)		
経路が異常となった場合の接続先IPアドレス	:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Layer3監視パケットの送信元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			
バックアップ対象パケット (宛先IPアドレス)					
1. IPアドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	サブネットマスク	<input type="text"/>
2. IPアドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	サブネットマスク	<input type="text"/>
3. IPアドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	サブネットマスク	<input type="text"/>
4. IPアドレス	<input type="text"/>	<input type="text"/>	<input type="text"/>	サブネットマスク	<input type="text"/>

- [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無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 [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。



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ー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。

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)

- 5 [送信] をクリックします。

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。

別注	送信元アドレス		宛先ポート番号	宛先指定	
	IPアドレスとマスク			IPアドレス指定	URL指定
1	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
2	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
3	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
4	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
5	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
6	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
7	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
8	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定
9	<input type="checkbox"/>	<input type="text"/>	FTP <input type="radio"/> 0 ~ 65535	<input type="radio"/> IPアドレス指定	<input type="radio"/> URL指定

現在の登録件数/最大登録件数: 0/161~9

クリア 送信

- [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 FITEInet-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 [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

6 SNMPエージェント機能を設定します。

No.	SNMPマネージャのIPアドレス	コミュニティ名 (最大32文字)	トラップ	送信元IPアドレス
1	0.0.0.0	public	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	通常 of 送信元IPアドレスを使用する
2			<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	通常 of 送信元IPアドレスを使用する
3			<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	通常 of 送信元IPアドレスを使用する
4			<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	通常 of 送信元IP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。

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 (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

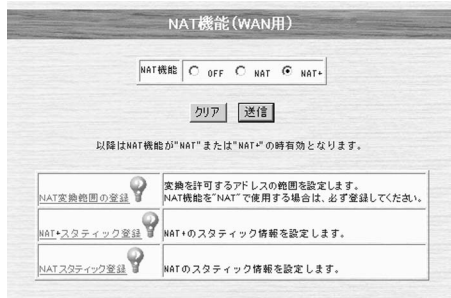
NATモードで使用する場合は、NAT変換範囲を必ず設定してください。以下に設定方法を説明します。

- 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 [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

- 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。



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。

- 9 [送信] をクリックします。

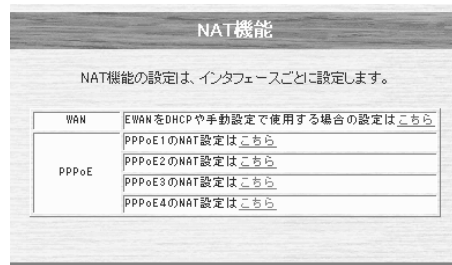
- 10 装置を再起動します。

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。

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 FTELnet-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 [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。

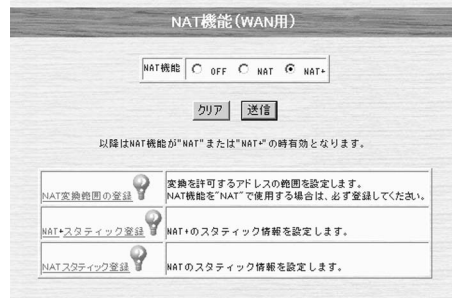


お願い

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、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。

次ページへ続く

- 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。

The screenshot shows a configuration window titled '外部に見えるIPアドレスとポート番号' (External IP and Port). It has two main sections: 'WAN側から配付されたIPアドレスを' (WAN side assigned IP address) and 'ポート番号範囲' (Port number range). Under the IP section, there are two radio buttons: '● 使用する' (Use) which is selected, and '○ 使用しない' (Do not use). To the right of the radio buttons are four empty input boxes for the IP address. Under the port range section, there are two input boxes, both containing '80', with a tilde '~' between them.

• [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 [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。

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。



次ページへ続く

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。

	削除	LAN上の端末指定 IPアドレス	外部に見えるIPアドレス	マスク指定
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			
5	<input type="checkbox"/>			
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			
8	<input type="checkbox"/>			
9	<input type="checkbox"/>			
10	<input type="checkbox"/>			
11	<input type="checkbox"/>			
12	<input type="checkbox"/>			
13	<input type="checkbox"/>			
14	<input type="checkbox"/>			
15	<input type="checkbox"/>			
16	<input type="checkbox"/>			

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える機能です。
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に [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

6 DHCPリレーエージェント機能を設定します。

削除	IPアドレス	送信元IPアドレス
<input type="checkbox"/>	0.0.0.0	通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	0.0.0.0	通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	0.0.0.0	通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	0.0.0.0	通常の送信パケットと同じアドレスを使用する

DHCPサーバまでの最大ホップ数: 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。

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 [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

- 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。

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せん。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。

- 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

- 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。

配布アドレスのスタティック登録 (オプション設定) 

	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.	<input type="checkbox"/>	: : : : : :
2.	<input type="checkbox"/>	: : : : : :
3.	<input type="checkbox"/>	: : : : : :
4.	<input type="checkbox"/>	: : : : : :
5.	<input type="checkbox"/>	: : : : : :
6.	<input type="checkbox"/>	: : : : : :
7.	<input type="checkbox"/>	: : : : : :
8.	<input type="checkbox"/>	: : : : : :
9.	<input type="checkbox"/>	: : : : : :
10.	<input type="checkbox"/>	: : : : : :
11.	<input type="checkbox"/>	: : : : : :
12.	<input type="checkbox"/>	: : : : : :
13.	<input type="checkbox"/>	: : : : : :
14.	<input type="checkbox"/>	: : : : : :
15.	<input type="checkbox"/>	: : : : : :
16.	<input type="checkbox"/>	: : : : : :

- [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には
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に [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。

syslogの送信	
syslogの送信	<input checked="" type="radio"/> しない <input type="radio"/> する 
syslogを受け取る端末のIPアドレス	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> 
tlog (errレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
elog (warningレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
llog (infoレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
vlog (infoレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
vpnlog (infoレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
clog (noticeレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
flog (noticeレベル) で送信	<input checked="" type="radio"/> しない <input type="radio"/> する
ファシリティ値	LOCAL0 
送信元アドレス	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 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どうかを選択します。

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。

DNSサーバ機能は、数字の羅列で表されていて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に [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。

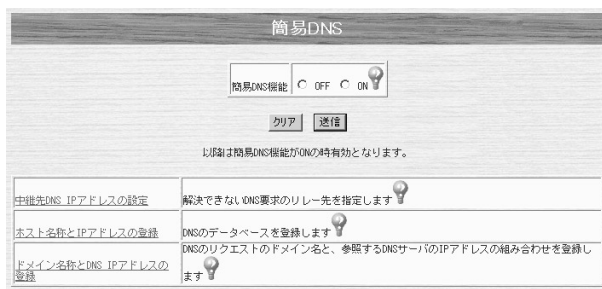
5 [登録する] をクリックします。

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。

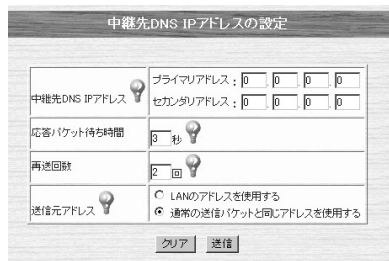
次ページへ続く

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

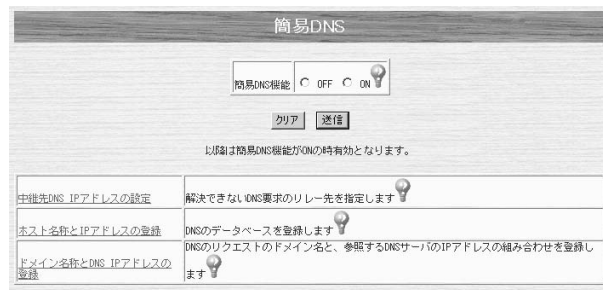
DNSのリクエスト内のドメインにより、リクエストし直すDNSを振り分けることができます。

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索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 FTELnet-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に [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

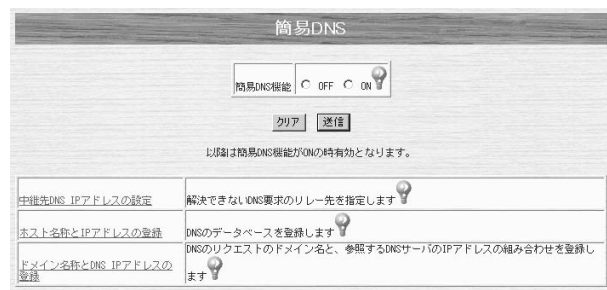
登録済みのドメイン名称を削除するときは
手順7で、削除するレコードのチェックボックスをチェックして、[送信] をクリックします。

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 FITEInet-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[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。

ホスト名称とIPアドレスの登録

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

クリア 送信

- 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 [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

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] SMTP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 (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 FTELnet-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 [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バ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に [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)

- [自局送信]
プロトコル欄にかかっ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っ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っ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 [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

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。

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。

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。

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に [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 (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 [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

6 RIPを設定します。

インタフェース	RIPの受信	RIPの送信	RIP2パスワード	定期送信 (RIP送信「する」で有効)	RIPエージアウト	メトリック
LAN	<input type="radio"/> RIP1のみ <input type="radio"/> RIP2のみ <input checked="" type="radio"/> RIP1,2両方 <input type="radio"/> 変更しない	<input type="radio"/> RIP1 <input type="radio"/> RIP2 <input checked="" type="radio"/> 送信しない	<input type="text"/>	<input type="radio"/> しない <input checked="" type="radio"/> 30 秒毎に送信	<input type="radio"/> しない <input checked="" type="radio"/> 180 秒で削除	<input type="text" value="0"/>
WAN	<input type="radio"/> RIP1のみ <input type="radio"/> RIP2のみ <input checked="" type="radio"/> RIP1,2両方 <input type="radio"/> 変更しない	<input type="radio"/> RIP1 <input type="radio"/> RIP2 <input checked="" type="radio"/> 送信しない	<input type="text"/>	<input type="radio"/> しない <input checked="" type="radio"/> 30 秒毎に送信	<input type="radio"/> しない <input checked="" type="radio"/> 180 秒で削除	<input type="text" value="0"/>
PPPoE1	<input type="radio"/> RIP1のみ <input type="radio"/> RIP2のみ <input checked="" type="radio"/> RIP1,2両方 <input type="radio"/> 変更しない	<input type="radio"/> RIP1 <input type="radio"/> RIP2 <input checked="" type="radio"/> 送信しない	<input type="text"/>	<input type="radio"/> しない <input checked="" type="radio"/> 30 秒毎に送信	<input type="radio"/> しない <input checked="" type="radio"/> 180 秒で削除	<input type="text" value="0"/>

- [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 FTELnet-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 [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

受信RIPフィルタリングテーブル

フィルタリング属性 テーブルに一致しないRIP情報を有効にする
 テーブルに一致したRIP情報を有効にする

削除	RIPの宛先IPアドレスとマスク長	受信インタフェース
1 <input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> PPPoe1 <input type="checkbox"/> PPPoe2 <input type="checkbox"/> PPPoe3 <input type="checkbox"/> PPPoe4
2 <input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> PPPoe1 <input type="checkbox"/> PPPoe2 <input type="checkbox"/> PPPoe3 <input type="checkbox"/> PPPoe4
3 <input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> PPPoe1 <input type="checkbox"/> PPPoe2 <input type="checkbox"/> PPPoe3 <input type="checkbox"/> PPPoe4
4 <input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> PPPoe1 <input type="checkbox"/> PPPoe2 <input type="checkbox"/> PPPoe3 <input type="checkbox"/> PPPoe4
5 <input type="checkbox"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> PPPoe1 <input type="checkbox"/> PPPoe2 <input type="checkbox"/> PPPoe3 <input type="checkbox"/> PPPoe4

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 [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

送信RIPフィルタリングテーブル

フィルタリング機能 テーブルに一致しないRIP情報を有効にする
 テーブルに一致したRIP情報を有効にする

別 名	RIPの宛先IPアドレスとマスク長	送信インタフェース	ルーティングプロトコル	AS番号	ASパス
1	<input type="checkbox"/> / <input type="checkbox"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> pppoe1 <input type="checkbox"/> pppoe2 <input type="checkbox"/> pppoe3 <input type="checkbox"/> pppoe4	<input checked="" type="radio"/> 全てのルーティングプロトコル <input type="radio"/> RIP <input type="radio"/> BGP <input type="radio"/> Aggregate <input type="radio"/> スタティック <input type="radio"/> ダイレクト	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/> / <input type="checkbox"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> pppoe1 <input type="checkbox"/> pppoe2 <input type="checkbox"/> pppoe3 <input type="checkbox"/> pppoe4	<input checked="" type="radio"/> 全てのルーティングプロトコル <input type="radio"/> RIP <input type="radio"/> BGP <input type="radio"/> Aggregate <input type="radio"/> スタティック <input type="radio"/> ダイレクト	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/> / <input type="checkbox"/>	<input type="checkbox"/> LAN <input type="checkbox"/> WAN <input type="checkbox"/> pppoe1 <input type="checkbox"/> pppoe2 <input type="checkbox"/> pppoe3 <input type="checkbox"/> pppoe4	<input checked="" type="radio"/> 全てのルーティングプロトコル <input type="radio"/> RIP <input type="radio"/> BGP <input type="radio"/> Aggregate <input type="radio"/> スタティック <input type="radio"/> ダイレクト	<input type="text"/>	<input type="text"/>

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 FTELnet-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 [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ース（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。

6 ユニキャスト宛RIP制御を設定します。

No.	宛先IPアドレス	送信インタフェース	送信元アドレス
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 通常の送信パケットと同じアドレスを使用する
<input type="checkbox"/>	[.] [.] [.] [.]	<input type="radio"/> WAN <input type="radio"/> PPPoe1 <input type="radio"/> PPPoe2 <input type="radio"/> PPPoe3 <input type="radio"/> PPPoe4	<input type="radio"/> LANのアドレスを使用する <input checked="" type="radio"/> 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、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。

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。

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 FTELnet-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に [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指定

	削除	ルート情報提供ルータのIPアドレス	削除	ルート情報提供ルータのIPアドレス	
1.	<input type="checkbox"/>	11.	<input type="checkbox"/>
2.	<input type="checkbox"/>	12.	<input type="checkbox"/>
3.	<input type="checkbox"/>	13.	<input type="checkbox"/>
4.	<input type="checkbox"/>	14.	<input type="checkbox"/>
5.	<input type="checkbox"/>	15.	<input type="checkbox"/>
6.	<input type="checkbox"/>	16.	<input type="checkbox"/>
7.	<input type="checkbox"/>	17.	<input type="checkbox"/>
8.	<input type="checkbox"/>	18.	<input type="checkbox"/>
9.	<input type="checkbox"/>	19.	<input type="checkbox"/>
10.	<input type="checkbox"/>	20.	<input type="checkbox"/>

- [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。

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網に新規拠点が増加された場合や、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 [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の一般設定	
BGP動作モード	<input type="radio"/> on <input checked="" type="radio"/> off
AS番号 (1~65534)	<input type="text"/>
ルータID (自IPアドレス)	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="button" value="クリア"/> <input type="button" value="送信"/>	

- [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[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。

種別	Internal type	ピアアドレス	ローカルアドレス	プロリット	優先度1	hold time	ゲートウェイアドレス
<input type="checkbox"/>	ゲートウェイアドレスを参照 ルーティングテーブルを参照	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on
<input type="checkbox"/>	ゲートウェイアドレスを参照 ルーティングテーブルを参照	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on
<input type="checkbox"/>	ゲートウェイアドレスを参照 ルーティングテーブルを参照	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on	<input type="checkbox"/> off <input type="checkbox"/> on

<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 [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

受信BGPフィルタリング

フィルタリング属性

- テーブルに一致したBGP情報を掲載する
- テーブルに一致したBGP情報を非表示にする
- 受信BGPフィルタリングを適用しない

種別	シーケンス番号 1~50	IPアドレス	マスク	優先度 0~255	AS番号 1~65534	ASパス番号
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	170		

最大登録件数 11~20, 21~30, 31~40, 41~50

- [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 [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。

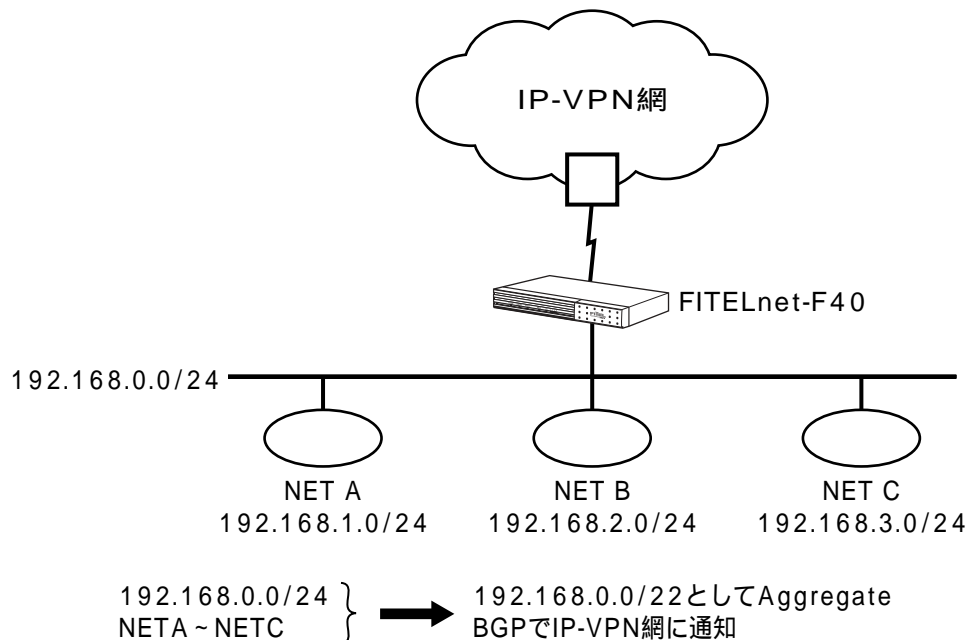
設定内容が本装置に送信され、確認画面が表示されます。

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。

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 FITEInet-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 [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 FITEInet-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 [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 [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、送信インター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。各インターフェースの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、送信インターフェースの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 [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

- ① 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。
- 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。

PPPoE制御		
名称	状況	制御
Provider A	接続	切断します
Provider B	接続	切断します
Provider C	接続	切断します
Provider D	接続	切断します

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[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。

<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)
```

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。

インフォメーション画面を表示する

通信ログなど本装置の運用やメンテナンスに必要な情報をインフォメーションで表示することができます。[インフォメーション]画面を表示し、メニューの中から使用する機能を選択してください。

< 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す[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[インフォメーション]をクリックします。
[インフォメーション]画面が表示されます。
- 5 表示したい項目をクリックします。

ワンポイント

- 装置情報の表示 (●P4-2)
- 通信状態の表示 (●P4-4)
- 統計情報の表示 (●P4-6)
- ルーティングインタフェースの表示 (●P4-11)
- ルーティング状態の表示 (●P4-13)
- BGP情報の表示 (●P4-15)
- マルチルーティング情報の表示 (●P4-17)
- DHCPサーバの状態表示 (●P4-19)
- NATの状態表示 (●P4-21)
- エラーログの表示 (●P4-22)
- 回線ログの表示 (●P4-23)
- イベントログの表示 (●P4-25)
- 送受信ログの表示 (●P4-26)
- フィルタリングログの表示 (●P4-27)
- 電子メール通知統計表示 (●P4-28)
- VPNログの表示 (●P4-29)
- VPN SAの状態表示 (●P4-30)
- 簡易DNSに関する情報表示 (●P4-33)
- DHCPクライアントの情報表示 (●P4-34)
- 冗長機能に関する情報表示 (●P4-36)
- 学習フィルタリングに関する情報表示 (●P4-38)
- DHCPリレーエージェントに関する情報表示 (●P4-40)
- 電子証明書情報の表示 (●P4-42)
- 設定情報の確認 (●P4-43)

インフォメーション	
装置について	本装置のバージョン等の情報を表示します。
通信状態の表示	LAN/WANの接続状態や、PPPoEの接続を表示します。
統計情報の表示	回線幅/プロトコル/VPNに関する、各種統計情報を表示します。
ルーティングインタフェースの表示	LAN/WAN/PPPoEの、IPアドレス等の情報を表示します。
ルーティング情報の表示	ルーティングテーブルの情報を表示します。
DHCPサーバの状態表示	DHCPサーバ機能により、パソコンに割り当てたアドレスの情報を表示します。
NATの状態表示	NAT/NAT機能の変換テーブルの情報を表示します。
エラーログの表示	装置のエラーログ情報を表示します。
回線ログの表示	LAN/WAN/PPPoEの、回線ログ情報を表示します。
イベントログの表示	本装置へのログイン情報を表示します。
送受信ログの表示	送受信ログ情報を表示します。
フィルタリングログの表示	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の情報を表示します。
電子メール通知統計表示	電子メール通知機能により、電子メールを送信する際の、各種統計情報を表示します。
VPNログの表示	VPNに関するログの情報を表示します。
VPN SAの状態表示	Phase1およびPhase2のSAの情報を表示します。
簡易DNSに関する情報表示	本装置のDNSキャッシュ情報を表示します。
DHCPクライアントの情報表示	WAN側でDHCPクライアント機能を使用している場合に、DHCPで取得した情報を表示します。
冗長機能に関する情報表示	FITELnet-E30と連携して、バックアップを実行している場合の、各種情報を表示します。
学習フィルタリングに関する情報表示	WAN→LANへの中継を許可する通信元アドレスの情報を表示します。
DHCPリレーエージェントに関する情報表示	DHCPリレーエージェント機能使用時の各種情報を表示します。
マルチルーティングに関する情報表示	マルチルーティングの運用状態を表示します。
BGPに関する情報	BGPでの経路情報/邻居ピアの状態を表示します。
電子証明書に関する表示	取得した電子証明書の情報を表示します。

hereisコマンド、dateコマンド

本装置のID、システムアップ時間、現在時刻を表示することができます。

< Webブラウザ操作 >

1 [インフォメーション]画面で、[装置について]をクリックします。

[装置について]画面が表示されます。
ブラウザで再読み込み操作を行うと、最新の状態が表示されます。



画面のみかた

項目	説明
装置IDの表示	装置を識別する内容として次を表示します。 装置名/装置版数/ファームウェア版数と作成日/装置のMACアドレス
装置現在時刻	現在時刻として、年月日時分秒を表示します。

お知らせ

PKIキーがインストールされている場合は、装置IDの表示に“With PKI”の文字が追加されます。

装置情報を表示する

< コマンド操作 >

1 装置IDを表示する場合は「hereis」、現在時刻を表示する場合は「date」と入力します。

(例) 本装置のIDを表示する。

```
#hereis
```

2 本装置のIDが以下のように表示されます。

```
#hereis
description : FITELnet-F40 A V01.00 2001.09.19 (00:80:bd:f0:09:fd)
node       : FITELnet-F40
manager    : admin@FITELnet-F40
location   : Honsha
```

3 コマンド入力待ち状態になります。

```
#
```

お知らせ

PKIキーがインストールされている場合は、“hereis”コマンドのdescriptionに“With PKI”の文字列が追加されます。

lineisコマンド

通信状態の表示では、回線情報を表示することができます。

< Webブラウザ操作 >

1 [インフォメーション]画面で、[通信状態の表示]をクリックします。

課金情報と回線情報が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

```

通信状態の表示

回線情報:

<LAN>
interface:IS08802-3

<WAN>
interface:IS08802-3
Speed:10M Duplex:half MDI,MDI-X:MDI

<pppoe-1>
name      :ProviderA
line      :connected
servicename :
connect time:xxxxxxxxxxxx
address   :aaa.aaa.aaa.aaa
MTU       :1454(bytes)

<pppoe-2>
name      :ProviderB
line      :connected
servicename :
connect time:xxxxxxxxxxxx
address   :bbb.bbb.bbb.bbb
MTU       :1454(bytes)

<pppoe-3>
name      :ProviderC
line      :connected
servicename :
connect time:xxxxxxxxxxxx
address   :ccc.ccc.ccc.ccc
MTU       :1454(bytes)

<pppoe-4>
name      :ProviderD
line      :connected
servicename :
connect time:xxxxxxxxxxxx
address   :ddd.ddd.ddd.ddd
MTU       :1454(bytes)

```

回線情報のみかた

接続形態	説明
LAN回線	<ul style="list-style-type: none"> 回線インタフェース名
WAN回線	<ul style="list-style-type: none"> 回線インタフェース名 接続状態（回線速度・Duplexモード・MDI or MID-X） MTU 長 (PPPoE使用時) PPPoE接続相手の名称 接続の状態 接続中かどうか サービス名称 PPPoEで学習したIP アドレス

通信状態を表示する

<コマンド操作>

1 回線情報を表示するには「lineis」と入力します。

(例) 回線情報を表示する。

```
#lineis
```

2 本装置の持つ回線情報が、以下のように表示されます。

```
#lineis
<LAN>
interface:ISO8802-3
<WAN>
interface:ISO8802-3
Speed:10M Duplex:half MDI,MDI-X:MDI
<pppoe-1>
name           :ProviderA
line           :connected
servicename    :
connect time   :XXXXXXXXXXXX
address        :aaa.aaa.aaa.aaa
MTU            :1454(bytes)
<pppoe-2>
name           :ProviderB
line           :connected
servicename    :
connect time   :XXXXXXXXXXXX
address        :bbb.bbb.bbb.bbb
MTU            :1454(bytes)
<pppoe-3>
name           :ProviderC
line           :connected
servicename    :
connect time   :XXXXXXXXXXXX
address        :ccc.ccc.ccc.ccc
MTU            :1454(bytes)
<pppoe-4>
name           :ProviderD
line           :connected
servicename    :
connect time   :XXXXXXXXXXXX
address        :ddd.ddd.ddd.ddd
MTU            :1454(bytes)
#
```

3 コマンド入力待ち状態になります。

```
#
```

統計情報を表示する

stchannelコマンド、stipコマンド、vpnstatコマンド

統計情報の表示では、回線統計情報とルーティング統計情報を表示することができます。
回線統計情報として、現在、ルーティングで使用しているチャンネルの統計を表示します。
IPルーティングの統計情報では次の項目を表示します。

- IPパケット統計情報
- ICMPパケット統計情報
- UDPパケット統計情報
- TCPパケット統計情報
- RIPパケット統計情報

< Webブラウザ操作 >

1 [インフォメーション]画面で、[統計情報の表示]をクリックします。

回線統計情報とルーティング統計情報、VPN統計情報が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

```

IP統計情報の表示

回線統計情報:
<lan>
alignment error frames:      0
FCS error frames           :  0
collision count             :  0
<wan>
alignment error frames:      0
FCS error frames           :  0
collision count             :  0
<pppoe1>
connect count               :  0
connected count             :  0
connect fail count          :  0
<pppoe2>
connect count               :  0
connected count             :  0
connect fail count          :  0
<pppoe3>
connect count               :  0
connected count             :  0
connect fail count          :  0
<pppoe4>
connect count               :  0
connected count             :  0
connect fail count          :  0

ルーティング統計情報:
<IP>
in packet                   :  0  in discard packet       :  0
in header error packet      :  0  in address error packet:  0
out request packet          :  0  out discard packet      :  0
forward packet              :  0  no route packet         :  0
<ICMP>
in message packet           :  0  in error packet         :  0
out message packet          :  0  out error packet        :  0
<UDP>
in datagram packet          :  0  in error packet         :  0
no port packet              :  0  out datagram packet     :  0
<TCP>
in segment packet           :  0  out segment packet      :  0
in error packet             :  0  passive open count      :  0
<RIP>
in packet                   :  0  sent packet             :  0
out request packet          :  0  in reply packet         :  0
flash update packet         :  0  send error packet       :  0
bad receive packet          :  0

VPN統計情報:

```

次ページへ続く

統計情報を表示する

回数統計情報のみかた

LAN/WAN

項目	意味
alignment error frames	フレーム長がオクテット整数でなく、FCSチェックにもエラーした受信フレーム数
FCS error frames	フレーム長はオクテット整数だがFCSエラーで廃棄された受信フレーム総数
collision count	コリジョン発生回数

PPPoE

項目	意味
connect count	接続回数
connected count	接続成功回数
connected fail count	接続失敗回数

ルーティング統計情報のみかた

IP

項目	意味
in packet	総入力IPパケット数
in discard packet	廃棄された入力パケット数
in header errors packet	IPヘッダエラー受信パケット数
in address error packet	IPアドレスエラー受信パケット数
out request packet	送信要求パケット数
out discard packet	内部資源不足のため廃棄された送信要求パケット数
forward packet	フォワーディングの必要のある受信パケット数
no route packet	送信経路がないため廃棄された送信要求パケット数

ICMP

項目	意味
in message packet	受信ICMPパケット数（エラー含む）
in error packet	受信ICMPエラーパケット数
out message packet	送信ICMPパケット数（エラー含む）
out error packet	送信ICMPエラーパケット数

次ページへ続く

統計情報を表示する

UDP

項目	意味
in datagram packet	受信UDPデータグラム数
in error packet	受信エラーUDPデータグラム数（チェックサムエラー等）
no port packet	受信エラーUDPデータグラム数（不正宛先ポート）
out datagram packet	送信UDPデータグラム数

TCP

項目	意味
in segment packet	受信TCPセグメント数
out segment packet	送信TCPセグメント数
in error packet	受信エラーTCPセグメント数（チェックサムエラー等）
passive open count	受動オープンした回数

RIP

項目	意味
in packet	受信RIPパケット数
sent packet	送信RIPパケット数
out request packet	送信RIP要求パケット数
in reply packet	受信RIPリプライパケット数
flash update packet	「triggered update」した回数
send error packet	送信エラーパケット数
bad receive packet	受信エラーパケット数

[次ページへ続く](#)

統計情報を表示する

VPN統計情報のみかた

項目	意味
PI send packet	Phase I 送信パケット数
PI receive packet	Phase I 受信パケット数
PI discard packet	Phase I 廃棄パケット数
PI decrypt error packet	Phase I 復号化エラーパケット数
PI hash error packet	Phase I ハッシュエラーパケット数
PI exchange fail	IKE SA 確立エラー数
PI exchange success	IKE SA 確立数
config send packet	transaction exchange 送信パケット数
config receive packet	transaction exchange 受信パケット数
config discard packet	transaction exchange 廃棄パケット数
mcfg send packet	mode-config 送信パケット数
mcfg receive packet	mode-config 受信パケット数
xauth send packet	拡張認証送信パケット数
xauth receive packet	拡張認証受信パケット数
xauth exchange error	拡張認証失敗数
xauth exchange success	拡張認証成功数
Pll send packet	Phase II 送信パケット数
Pll receive packet	Phase II 受信パケット数
Pll discard packet	Phase II 廃棄パケット数
Pll decrypt error packet	Phase II 復号化エラーパケット数
Pll hash error packet	Phase II ハッシュエラーパケット数
Pll exchange fail	IPsec SA 確立エラー数
Pll exchange success	IPsec SA 確立数
notify send packet	Notify メッセージ送信数
notify receive packet	Notify メッセージ受信数
other ISAKMP send packet	その他のISAKMP パケット送信数
other ISAKMP receive packet	その他のISAKMP パケット受信数
VPN discard packet	VPN 廃棄対象パケットとして廃棄したパケット数
ESP send packet	ESP 送信パケット数
ESP receive packet	ESP 受信パケット数
ESP discard packet	ESP 廃棄パケット数
ESP replay error packet	ESP リプレイアタックされたパケット数
ESP auth error packet	ESP 認証エラーパケット数
ESP send error	ESP 送信失敗数
IPCOMP send packet	圧縮したパケット送信数
IPCOMP receive packet	圧縮したパケット受信数
IPCOMP send error	圧縮に失敗した送信パケット数
IPCOMP compress error	圧縮するとパケットサイズが大きくなってしまふパケット数(圧縮効果なし)

統計情報を表示する

<コマンド操作>

- 1 回線の統計情報を表示する場合は「stchannel」、ルーティングの統計情報を表示する場合は「stip」、VPN統計情報を表示する場合は、「vpnstat」と入力します。

(例) 回線の統計情報を表示する。

```
#stchannel
```

- 2 回線の統計情報が以下のように表示されます。

```
#stchannel
<lan>
alignment error frames      :      0
FCS error frames           :      0
collision count             :      4
<wan>
alignment error frames      :      0
FCS error frames           :      0
collision count             :      2
<ppoe1>
connect count              :      0
connected count            :      0
connect fail count         :      0
                            :
```

- 3 コマンド入力待ち状態になります。

```
#
```

ipinterfaceコマンド

IPインタフェースの情報として次の内容をインタフェースごとに表示します。ただし、ダウンしているインタフェースに対しては表示を行いません。

- インタフェースのステータス
- インタフェースタイプ
- インタフェースアドレス
- インタフェースのIPアドレスサブネットマスク
- ブロードキャストアドレス
- リモートアドレス
- リモートサブネットマスク

NAT*を利用しているとき、ISDN回線のインタフェースアドレスが「0.0.0.0」と表示される場合があります。これは一度も接続が行われていないことを表します。

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[ルーティングインタフェースの表示]をクリックします。

ルーティングインタフェースに関する情報が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

```
ルーティングインタフェースの表示

<LAN>
up broadcast
address:192.128.128.122 subnet:255.255.255.0 broadcast:192.52.128.255
<WAN>
down broadcast
<PPPoE1>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPoE2>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPoE3>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPoE4>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
```

ルーティングインタフェースを表示する

<コマンド操作>

1 「ipinterface」と入力します。

```
#ipinterface
```

2 ルーティングインタフェースが以下のように表示されます。

```
#ipinterface
<LAN>
up broadcast
address:192.52.128.122 subnet:255.255.255.0 broadcast:192.52.128.255
<WAN>
down broadcast
<PPPOE1>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPOE2>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPOE3>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
<PPPOE4>
up pointToPoint
address:xxx.xxx.xxx.xxx remote:yyy.yyy.yyy.yyy remotesubnet:0.0.0.0
#
```

3 コマンド入力待ち状態になります。

```
#
```

iprouteコマンド

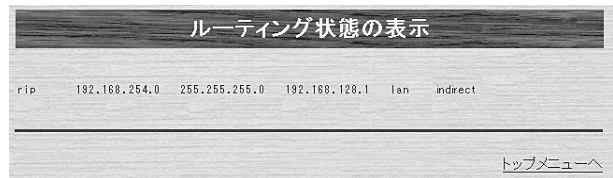
IPルーティングテーブルとして次の内容を表示します。

- ルーティング情報を得た手段
- 宛先IPアドレスIPアドレスマスク
- 宛先に到達するために送信するゲートウェイのIPアドレス
- 経由するインタフェース経路タイプ

< Webブラウザ操作 >

1 [インフォメーション]画面で、[ルーティング状態の表示]をクリックします。

ルーティング状態が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。



ルーティング状態のみかた

画面例では、以下の情報がわかります。

- 192.168.254.0ネットワークへは、LAN側の192.168.128.1ゲートウェイを通過して通信を行うことができる。
- この情報はRIPにより受信した。

項目		意味
ルーティング情報を得た手段	local	スタティック登録
	rip	RIPで学習
	bgp	BGP4で学習
	other	localとrip以外
宛先IPアドレスIPアドレスマスク		-
宛先に到達するために送信するゲートウェイのIPアドレス		-
経由するインタフェース経路タイプ	direct	直接ルート等の自装置内の経路
経由するインタフェース経路タイプ	indirect	自装置以外の経路

ルーティング状態を表示する

<コマンド操作>

1 「iproute」と入力します。

```
#iproute
```

2 ルーティング状態が以下のように表示されます。

```
rip 192.168.254.0 255.255.255.0 192.168.128.1 lan indirect
```

3 コマンド入力待ち状態になります。

```
#
```

bgprouteコマンド、bgpstateコマンド

BGPで取得した経路情報や、BGPピアの情報を表示します。

BGPに関する情報では、次の項目が表示されます。

[BGPで取得した経路情報]

- 宛先アドレス/マスク
- ゲートウェイアドレス
- 他のプロトコルに対する優先度
- メトリック値
- 相手から受信したローカルプリファレンス
- インタフェース名

[BGPピアの情報]

- BGPピアのアドレス/ポート番号
- 自身のIPアドレス/ポート番号
- AS番号
- 接続形態
- 接続ステータス
- 受信メッセージ / アップデート数
- 送信メッセージ / アップデート数

< Webブラウザ操作 >

1 [インフォメーション] 画面で、[BGPに関する表示] をクリックします。

取得した電子証明書の情報が表示されます。

```

BGPに関する情報表示

BGP経路情報:
Destination/Masklen Gateway Pref Metric LPref Interface
0/0 192.52.138.201 -170 10 100 lan
AS Path:
(65002) 16P (Id 2)
*192.52.119/24 192.52.138.201 170 10 100 lan
AS Path:
(65002) 16P (Id 2)
192.52.121/24 192.52.138.201 -170 10 100 lan
AS Path:
(65002) 16P (Id 2)

BGPピアの状態:
BGP_200.192.168.213.10:
Peer : 192.168.213.10+179 AS(200)
Local: 192.168.211.210+1026 AS(100)
Type : External State: Established
Input messages: Total 0 Updates 0
Output messages: Total 0 Updates 0

BGP_100.192.52.138.2:
Peer : 192.52.138.2+179 AS(100)
Local: 192.52.138.252 AS(100)
Type : Internal State: Active
  
```

BGPに関する情報を表示する

<コマンド操作>

- 1 BGPで取得した経路情報を表示する場合は「bgproute」、BGPピアの情報を表示する場合は「bgpstate」と入力します。

(例) BGPで取得した経路情報を表示する場合

```
#bgproute
```

- 2 BGPで取得した経路情報が、以下のように表示されます。

Destination/Masklen	Gateway	Pref	Metric	LPref	Interface
0/0	192.52.138.201	-170	10	100	lan
AS Path: (65002) IGP (ld 2)					
*192.52.119/24	192.52.138.201	170	10	100	lan
AS Path: (65002) IGP (ld 2)					
192.52.121/24	192.52.138.201	-170	10	100	lan
AS Path: (65002) IGP (ld 2)					

- 3 コマンド入力待ち状態になります。

```
#
```



multirouteisコマンド

マルチルーティングの設定内容を表示します。各項目の説明は、P2-68を参照してください。

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[マルチルーティングに関する表示]をクリックします。

取得した電子証明書の情報が表示されます。



```
マルチルーティングに関する情報表示

status:on

route data:
<seq: 1>
src=1.1.1.1,255.255.255.255
dst=NOT_RESOLVED
url=www.lets
dns_timer[sec]=27
dstport=0,65535
nextif=pppoe1
preference=31

exclusive route data:

src=2.2.2.2,255.255.255.255
dst=0.0.0.0,0.0.0.0
dstport=0,65535
```

<コマンド操作>

1 「multirouteis」と入力します。

```
#multirouteis
```

2 マルチルーティングに関する情報が、以下のように表示されます。

```
status:on

route data:
<seq: 1>
  src=1.1.1.1,255.255.255.255
  dst=NOT RESOLVED
  url=www.flets
  dns_timer [ sec ] =27
  dstport=0,65535
  nextif=pppoe1
  preference=31

exclusive route data:

  src=2.2.2.2,255.255.255.255
  dst=0.0.0.0,0.0.0.0
  dstport=0,65535
```

3 コマンド入力待ち状態になります。

```
#
```

dhcpstatコマンド

DHCPサーバ機能がARPにより認識した（すでに利用済みの）IPアドレス、IP端末からのIPアドレス取得要求に対してDHCPサーバ機能が自動配付したIPアドレス、設定（hosttableコマンド）により割り付けが決められているIPアドレスおよびリース残り時間を表示します。

< Webブラウザ操作 >

1 [インフォメーション]画面で、[DHCPサーバの状態表示]をクリックします。

ルーティング状態が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。



MAC	IP	リース残り時間
a 08:00:20:0f:83:54	192.168.128.1	
a 00:80:bd:f0:06:f4	192.168.128.8	
a 00:80:bd:f0:06:6b	192.168.128.9	
a 08:00:20:7b:4d:3a	192.168.128.13	
a 00:80:bd:f0:04:9a	192.168.128.22	
a 00:80:bd:f0:05:77	192.168.128.97	
s 00:80:bd:f0:01:33	192.168.128.200	0:54

DHCPサーバの状態表示のみかた表示はIP端末とのペアで表示し、IP端末はIPアドレスで表わします。

DHCPサーバの状態を表示する

<コマンド操作>

1 「dhcpstat」と入力します。

```
# dhcpstat
```

2 DHCPサーバの状態が以下のように表示されます。

```
a 08:00:20:0f:83:54 192.168.128.1
a 00:80:bd:f0:06:f4 192.168.128.8
a 00:80:bd:f0:06:6b 192.168.128.9
a 08:00:20:7b:4d:3a 192.168.128.13
a 00:80:bd:f0:04:9a 192.168.128.22
a 00:80:bd:f0:05:77 192.168.128.97
s 00:80:bd:f0:01:33 192.168.128.200 0:54
```

3 コマンド入力待ち状態になります。

```
#
```

NAT⁺の状態を表示する

natinfoコマンド

アドレス変換状況を取得して、NAT⁺の状態を表示します。

- LAN側の送信元IPアドレスとWAN側の変換後IPアドレスの組
- LAN側の送信元IPアドレスとWAN側の変換後IPアドレスの組に対応する宛先IPアドレス
- LAN側の送信元ポートとWAN側の変換後ポートの組

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[NAT⁺の状態表示]をクリックします。

NAT⁺の状態が表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

NAT ⁺ の状態表示							
< NAT >							
< NATP >							
wan	private		global	remote			
no	(IP address	port)	port	(IP address	port)	protocol	timer(sec)
1	192.168.0.2	3543	3543	158.202.232.7	53	UDP	210
2	192.168.0.2	3544	3544	158.202.232.7	23	TCP	3540

表示フォーマット

- LAN側送信元IPアドレス (WAN側変換後IPアドレス) 宛先IPアドレス
- LAN側送信元ポート (WAN側変換後ポート) 宛先ポート

< コマンド操作 >

- 1 「natinfo natp」と入力します。

NAT使用時はnatinfo natと入力します。

```
# natinfo natp
```

- 2 NAT⁺の状態が以下のように表示されます。

wan	private		global	remote			
no	(IP address	port)	port	(IP address	port)	protocol	timer(sec)
1	192.168.0.2	3543	3543	158.202.232.7	53	UDP	210
2	192.168.0.2	3544	3544	158.202.232.7	23	TCP	3540

- 3 コマンド入力待ち状態になります。

```
#
```

エラーログを表示する

elogコマンド

エラーに関するロギングとして次の項目を表示します。

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

< Webブラウザ操作 >

1 [インフォメーション]画面で、[エラーログ表示]をクリックします。

エラーログが表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

seq	uptime	date	tid	logid	ecode
000	0000:00:00.00	01/09/24 (mon) 13:17:09	0	00000000	00000000
				#P_ON[V00.04-091901]	
001	0000:00:00.00	01/09/24 (mon) 13:19:33	0	00000000	00000000
				#Reset[V00.04-091901]	

< コマンド操作 >

1 「elog」と入力します。

```
# elog
```

2 エラーログが以下のように表示されます。

seq	uptime	date	tid	logid	ecode
000	0000:00:00.00	01/09/24 (mon) 13:17:09	0	00000000	00000000
				#P_ON[V01.00-091901]	
001	0000:00:00.00	01/09/24 (mon) 13:19:33	0	00000000	00000000
				#Reset[V01.00-091901]	

3 コマンド入力待ち状態になります。

```
#
```

llogコマンド

回線に関するロギングとして次の項目を表示します。

- 通し番号
- ロギング時刻
- 回線種別
- エラーコード
- ログメッセージ

切断時や接続が失敗した時などは網からその原因が通知されます。その内容は切断時のログ（ログメッセージが「Disconnected」）や接続失敗時のログ（ログメッセージが「Connect fail」）の「エラーコード」に16進値で記録されています。PPPでの認証失敗時やデータリンクレベルでの接続失敗時の原因も記録されます。

< Webブラウザ操作 >

1 [インフォメーション]画面で、[回線ログの表示]をクリックします。

回線ログが表示されます。ブラウザで再読み込み操作を行うと、最新の状態が表示されます。

```

回線ログの表示

LAN:
seq uptime      date                channel  ecode
-----
000 0000:00:00.00 01/09/24 (mon) 18:17:09 LAN      00000000
                                #P_ON[V00,04-091901]
001 0000:00:00.00 01/09/24 (mon) 18:19:33 LAN      00000000
                                #Reset[V00,04-091901]

WAN:
seq uptime      date                channel  ecode
-----
000 0000:00:00.00 01/09/24 (mon) 18:17:09 WAN      00000000
                                #P_ON[V00,04-091901]
001 0000:00:00.01 01/09/24 (mon) 18:17:10 WAN      08050200
                                Ethernet Tx error
002 0000:00:00.00 01/09/24 (mon) 18:19:33 WAN      00000000
                                #Reset[V00,04-091901]
003 0000:00:00.01 01/09/24 (mon) 18:19:34 WAN      08050200
                                Ethernet Tx error
  
```

回線ログのみかた

項目名	意味
seq	シーケンス番号
uptime	操作が起動してからの時間（時間・分・秒）
channel	選択した回線
ecode	回線の状況

お知らせ

PPPoE使用時の回線ログについては、P5-11も参照してください。

回線ログを表示する

< コマンド操作 >

1 「llog」と入力します。

LAN、WAN回線個別の状況を確認する場合は、「llog」のあとに以下のオプションをつけてください。

回線種別	パラメータ	説明
LAN	-l	
WAN	-w	WANの物理的内容のログ
PPPoE	-pppoe1	PPPoE1のログ
	-pppoe2	PPPoE2のログ
	-pppoe3	PPPoE3のログ
	-pppoe4	PPPoE4のログ

(例) LANの状況を確認する。

```
#llog -l
```

2 表示された内容により、LAN、WAN回線の状況を確認します。

```
#llog -l
seq  uptime          date                channel  ecode
---  -
000  0000:00:00.00    01/09/11 (Tue) 07:14:52  LAN     00000000
                                     #Reset[V01.00-091901]
```

3 コマンド入力待ち状態になります。

```
#
```

お知らせ

ラインログの最大ログ件数は回線ごとに20件です。20件以上のログは、最も古いログから上書きしていきます。

vlogコマンド

Telnet やFTP によるリモートログインに関するログを表示します。
次の項目が表示されます。

- 通し番号
- ログID
- ログイン時刻
- イベントコード
- タスクID
- ログメッセージ

< Webブラウザ操作 >

1 [インフォメーション]画面で、[イベントログの表示]をクリックします。

イベントログが表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。

イベントログの表示					
seq	uptime	date	tid	logid	ecode
000	0000:00:00.00	01/09/24 (mon) 13:17:09	0	00000000	00000000
				#P_ON[V00.04-091901]	
002	0000:21:14.65	01/09/24 (mon) 13:40:48	10	00000000	00000000
				telnet login success from 192.168.0.2	

< コマンド操作 >

1 「vlog」と入力します。

```
#vlog
```

2 イベントログが以下のように表示されます。

seq	uptime	date	tid	logid	ecode
000	0000:00:00.00	01/09/24 (mon) 13:17:09	0	00000000	00000000
				#P_ON[V00.04-091901]	
002	0000:21:14.65	01/09/24 (mon) 13:40:48	10	00000000	00000000
				telnet login success from 192.168.0.2	

3 コマンド入力待ち状態になります。

```
#
```

送受信ログを表示する

clogコマンド

本装置の送受信ログ機能により、送信/受信/中継したパケットのログを表示します。ログに残すパケットの種類は、送受信ログの設定で行います。

送受信ログの表示では、次の項目が表示されます。

- 受信時/送信時/中継時
- インタフェース
- プロトコル
- パケットの送信元アドレス
- パケットの宛先アドレス

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[送受信ログの表示]をクリックします。

送受信ログが表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。



< コマンド操作 >

- 1 「clog」と入力します。

```
#clog
```

- 2 送受信ログが以下のように表示されます。

```
SEND lan,UDP:xxx.xxx.xxx.xxx:1000 -> yyy.yyy.yyy.yyy:2000
RECV wan,ICMP:xxx.xxx.xxx.xxx-> yyy.yyy.yyy.yyy,type8,code0
FWD wan>lan,protocol2:zzz.zzz.zzz.zzz-> yyy.yyy.yyy.yyy
```

1行目は、xxx.xxx.xxx.xxx(port 1000) yyy.yyy.yyy.yyy (port 2000) のUDPパケットをLANに自局から送信したことを示しています。TCP/UDP以外の場合は、ポート番号の表示はありません。

- 3 コマンド入力待ち状態になります。

```
#
```

ワンポイント

送受信ログの設定 (P2-101)

フィルタリングログを表示する

flogコマンド

本装置の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のログを表示します。フィルタリングログを残すかどうかは、IPパケットフィルタリングの設定で行います。

フィルタリングログの表示では、次の項目が表示されます。

- 受信時/送信時/中継時
- インタフェース
- プロトコル
- パケットの送信元アドレス
- パケットの宛先アドレス

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[フィルタリングログの表示]をクリックします。

フィルタリングログが表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。



< コマンド操作 >

- 1 「flog」と入力します。

```
#flog
```

- 2 フィルタリングログが以下のように表示されます。

```

RECV recv from wan,UDP:xxx.xxx.xxx.xxx:1000 -> yyy.yyy.yyy.yyy:2000
FWD recv from wan,protocol2:xxx.xxx.xxx.xxx -> yyy.yyy.yyy.yyy
FWD send to lan,TCP(S):xxx.xxx.xxx.xxx:1000 -> zzz.zzz.zzz.zzz:2000
  
```

1行目は、192.52.150.1(port1000) 192.52.150.100 (port2000)のUDPパケットをWANから受信した際に廃棄したことを示しています。TCP/UDP以外の場合は、ポート番号の表示はありません。

- 3 コマンド入力待ち状態になります。

```
#
```

ワンポイント

フィルタリングログの設定(●P2-60)

電子メール通知統計を表示する

mailinfoコマンド

電子メールにより管理者に電子メールを送信する機能に関する統計情報を表示します。
次の項目が表示されます。

項目名	意味
event count	電子メールを送信するイベントが発生した回数
send success count	電子メールの送信が成功した回数
tcp connection error count	電子メール送信時にSMTP サーバとコネクションが張れなかった回数
smtp error count	電子メール送信時にSMTP サーバとのやり取りに失敗があった回数
send error count	電子メール送信が失敗した回数
event buffer full count	電子メールを送信するイベントがオーバーフローした回数

< Webブラウザ操作 >

- 1 [インフォメーション] 画面で、[電子メール通知統計表示] をクリックします。

電子メール通知機能に関する統計が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。

電子メール通知統計表示	
event count	: 6
send success count	: 0
tcp connection error count	: 0
smtp error count	: 6
send error count	: 0
event buffer full count	: 13

< コマンド操作 >

- 1 「mailinfo」と入力します。

```
#mailinfo
```

- 2 電子メール統計情報が以下のように表示されます。

```
event count          : 6
send success count   : 0
tcp connection error count : 0
smtp error count     : 6
send error count     : 0
event buffer full count : 13
```

ワンポイント

- 不正アクセスフィルタリング機能
(●P2-57)
- 電子メール通知機能の設定
(●P2-97)

- 3 コマンド入力待ち状態になります。

```
#
```

VPNログを表示する

vpnlogコマンド

VPNに関するログ情報を参照することができます。

- 通し番号
- ログID
- ログイン時刻
- エラーコード
- タスクID
- ログメッセージ

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[VPNログの表示]をクリックします。

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

seq	uptime	date	tid	logid	ecode
000	0000:00:00.00	02/01/13 (sun)	21:17:57	0	00000000 00000000
001	0000:00:00.32	02/01/13 (sun)	21:17:57	16	10000002 00000000 vpn enabled.

VPNログにSA確立の情報を載せるかどうかを、本画面で設定します。

< コマンド操作 >

- 1 「vpnlog」と入力します。

```
#vpnlog
```

- 2 VPNに関するログが以下のように表示されます。

seq	uptime	date	tid	logid	ecode
001	0000:05:17.55	01/09/24 (mon)	15:59:34	16	1000032 00000000 IKE SA XXX.XXX.XXX.XXX
002	0000:05:17.58	01/09/24 (mon)	15:59:34	16	10000221 00000000 IPSEC SA XXX.XXX.XXX.XXX

お知らせ

この設定は、[残す]あるいは[残さない]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 コマンド入力待ち状態になります。

```
#
```

vpnsainfoコマンド

IKE SAとIPsec SAの状態を表示することができます。

< Webブラウザ操作 >

1 [インフォメーション]画面で、[VPN SAの状態表示]をクリックします。

IKE SAとIPsec SAの状態が表示されます。

```

VPN SA の状態表示

IKE SA
[ 1 ] XXX.XXX.XXX.XXX
      <=> YYY.YYY.YYY.YYY
      <R> Main_Mode UP pre-shared key DES MD5
      Lifetime:120secs
      Current:20secs,1kbytes

IPSEC SA
[ 3 ] XXX.XXX.XXX.XXX,255.255.255.255 ALL ALL
      <=> YYY.YYY.YYY.YYY,255.255.255.255 ALL ALL
peer:YYY.YYY.YYY.YYY
<R> UP ESP DES HMAC-MD5 PFS:off
Lifetime: 600secs,1000kbytes
O-SPI:0x16485d8e Current:568secs,100kbytes
out_packet :258 error_packet :0
I-SPI:0x16485d8d Current:568secs,17kbytes
in_packet :222 auth_packet :222
decrypt_packet :222 discard_packet :0
reply_packet :0 auth_error_packet :0
  
```

VPN SAの状態画面のみかた

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

次ページへ続く

VPN SAの状態を表示する

<Outbound>

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

<Inbound>

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

VPN SAの状態を表示する

< コマンド操作 >

1 「vpnsainfo」と入力します。

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

パラメータ	表示種別
ike	IKE SA
ipsec	IPsec SA
省略	IPsec SA

(例) IKE SAの状態を表示する。

```
#vpnsainfo ike
```

2 VPN SAの状態を表示します。

(表示例)

```
#vpnsainfo ike
IKE SA
[ 1] XXX.XXX.XXX.XXX
    <-> YYY.YYY.YYY.YYY
    <R> Main Mode      UP    pre-shared key DES MD5
    Lifetime:120secs
    Current:6secs,1kbytes
    mcfg-addr:  ZZZ.ZZZ.ZZZ.ZZZ
#
#vpnsainfo ipsec
IPSEC SA
[ 5] XXX.XXX.XXX.XXX,255.255.255.255 ALL ALL
    <-> YYY.YYY.YYY.YYY,255.255.255.255 ALL ALL
peer:XXX.XXX.XXX.XXX
<R> UP ESP DES HMAC-MD5 PFS:off
Lifetime:        600secs,1000kbytes
O-SPI:0xd763a302  Current:7secs,1kbytes
  out packet    :2      error packet      :0
I-SPI:0xc447f4c   Current:7secs,1kbytes
  in packet     :2      auth packet      :2
  decrypt packet :2      discard packet   :0
  replay packet :0      auth error packet :0
#
```

3 コマンド入力待ち状態になります。

```
#
```


簡易DNSの情報を表示する

proxydnsisコマンド

本装置の簡易DNS機能により学習/設定した、DNSキャッシュ情報を表示します。
簡易DNS情報の表示では、次の項目が表示されます。

- dns server
- ホスト名
- キャッシュの残り時間
- IPアドレス

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[簡易DNSに関する情報表示]をクリックします。

DNSキャッシュ情報が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。

Proxy dns server	xxx.xxx.xxx.xxx	<min>	<IPAddress>
<hostname>			
0	setup.fitelnet	0	192.52.138.129
1	host.furukawa.co.jp	65	192.52.138.130

< コマンド操作 >

- 1 「proxydnsis」と入力します。

```
#proxydnsis
```

- 2 簡易DNSの情報が以下のように表示されます。

Proxy dns server	xxx.xxx.xxx.xxx	<min>	<IPAddress>
<hostname>			
0	setup.fitelnet	0	192.52.138.129
1	host.furukawa.co.jp	65	192.52.138.130

Proxy DNS Serverでは、設定または学習したDNSアドレスを表示します。表の1行目は、キャッシュ情報として、setup.fitelnetは、192.52.138.129であることを示しています。ProxyDNS機能で、本装置がこのホスト名のnameリクエストを受信した場合は、学習しているIPアドレスの情報を送信します。

- 3 コマンド入力待ち状態になります。

```
#
```

ワンポイント

簡易DNSの設定 (P2-91)

dhcpcinfoコマンド

WAN側でDHCPクライアント機能が動作している場合、DHCPで取得した情報等を表示します。次の項目が表示されます。

- 取得したIPアドレス/サブネットマスク
- DHCPサーバのIPアドレス
- リース残り時間
- クライアントID
- ホスト名
- 取得したDNSサーバのIPアドレス
- 取得したデフォルトゲートウェイのIPアドレス

< Webブラウザ操作 >

1 [インフォメーション]画面で、[DHCPクライアントの情報表示]をクリックします。

DHCPクライアント情報が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。



<コマンド操作>

1 「dhcpcinfo」と入力します。

```
#dhcpcinfo
```

2 DHCPクライアント情報が以下のように表示されます。

```
status          : BOUND
IP address      : xxx.xxx.xxx.xxx
subnetmask     : 255.255.255.0
DHCP server    : xxx.xxx.xxx.xxx
lease expires   : xx yy:yy:yy
client ID      :
host name      :
primary DNS    : xxx.xxx.xxx.xxx
secondary DNS  : xxx.xxx.xxx.xxx
default gateway : xxx.xxx.xxx.xxx
```

3 コマンド入力待ち状態になります。

```
#
```

冗長機能に関する情報表示を表示する

rgroupingisコマンド、pathchkisコマンド

冗長機能（ルーティンググループ化機能・Layer3監視機能）が動作している場合、ルーティンググループの情報、Layer3監視状態を表示します。

次の項目が表示されます。

- ルーティンググループを形成している全てのルーティングの情報
- Layer3監視を行っている相手の状態

< Webブラウザ操作 >

1 [インフォメーション]画面で、[冗長機能に関する情報表示]をクリックします。

ルーティンググループ化機能・Layer3監視機能に関する情報が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。

冗長機能に関する情報表示				
ルーティンググループ化機能に関する情報				
grouping-on	gipaddr=192.168.0.200			
no.	preference	IP address	MAC address	free ch connected IP address
0	88	192.168.0.2	00.80.bd.13.0e.6a 08	

Layer3監視機能に関する設定
<pathchkis>
on
PingTrial:2
pathchk paddr:158.xxx.xxx.1
pathfilter ncipaddr:
destipaddr:158.xxx.xxx.1
PathChkInterval:30[sec] RestChkInterval:30[sec]
PathChkTimer:120[sec] RestChkTimer:300[sec]
L3Status:Normal

冗長機能に関する情報表示を表示する

<コマンド操作>

1 「rgroupingis」, 「pathchkis」のいずれかを
入力します。

(例) ルータグループ化機能に関する統計情報を表示する

```
#rgroupingis
```

2 ルータグループを形成している全てのルータの
情報が、以下のように表示されます。

```
grouping=on gipaddr=192.168.0.200
no. preference IP address      MAC address      free ch  connected IP address
-----+-----+-----+-----+-----+-----
0. 99          192.168.0.2     00.80.bd.13.0e.6a 0B
```

1行目はルータグループ化を使用し、代表IPアドレスは
192.168.0.200であることを示しています。

表の1行目は、グループルータとして、preference:99、
MAC:00.80.bd.13.0e.6a/IP:192.168.0.2であるルータが存
在し、どことも接続していない (free ch=0B) ということを示
しています。

3 コマンド入力待ち状態になります。

```
#
```

sealedinfoコマンド

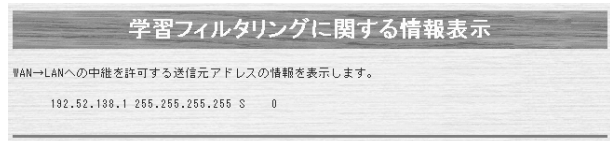
学習フィルタリング機能が動作している場合、WAN LANに中継を許可するIPアドレスを表示します。次の項目が表示されます。

- 中継を許可するIPアドレス/マスク
- タイプ
- エージアウト時間 (残り時間)

< Webブラウザ操作 >

1 [インフォメーション]画面で、[学習フィルタリングに関する情報表示]をクリックします。

学習フィルタリングに関する情報が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。



< コマンド操作 >

1 「sealedinfo」と入力します。

```
#sealedinfo
```

2 LAN WANに中継を許可するアドレスの情報が以下のように表示されます。

```
192.xxx.xxx.100 255.255.255.255 S 0  
158.xxx.xxx.1 255.255.255.255 S 0
```

3 コマンド入力待ち状態になります。

```
#
```

DHCPリレーエージェントに関する情報表示を表示する

stdhcprコマンド、dhcprdiscardコマンド

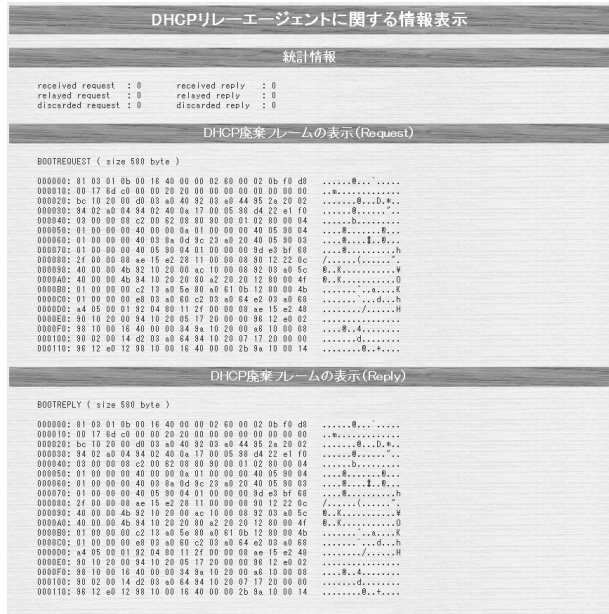
DHCPリレーエージェント機能が動作している場合、各種統計情報、廃棄されたパケット情報表示します。次の項目が表示されます。

- DHCPのリクエストを受信した回数
- DHCPのリクエストをリレーした回数
- 廃棄したDHCPリクエストパケット数
- 廃棄したDHCPリクエストのデータ
- DHCPのリプライを受信した回数
- DHCPのリプライをリレーした回数
- 廃棄したDHCPリプライパケット数
- 廃棄したDHCPリプライのデータ

< Webブラウザ操作 >

1 [インフォメーション]画面で、[DHCPリレーエージェントに関する情報表示]をクリックします。

DHCPリレーエージェントに関する情報が表示されます。ブラウザで再読み込み操作を行うと、最新の情報が表示されます。



DHCPリレーエージェントに関する 情報表示を表示する

<コマンド操作>

1 「stdhcpr」、「dhcprdiscard」のいずれかを入力します。

(例) DHCPリレーエージェントに関する統計情報を表示する

```
#stdhcpr
```

2 DHCPリレーエージェントに関する統計情報が、以下のように表示されます。

```
received request : 0    received reply  : 0
relayed request  : 0    relayed reply   : 0
discarded request : 0    discarded reply : 0
```

3 コマンド入力待ち状態になります。

```
#
```

電子証明書の情報を表示する

vpncertinfoコマンド

PKI（公開鍵基盤）で使用する、取得した電子証明書およびCRLの情報を表示します。

< Webブラウザ操作 >

- 1 [インフォメーション]画面で、[電子証明書に関する表示]をクリックします。

取得した電子証明書の情報が表示されます。



< コマンド操作 >

- 1 証明書の情報を表示する場合は「vpncertinfo」、CRLの情報を表示する場合は「vpncertinfo crl」と入力します。

```
#vpncertinfo
```

- 2 取得した電子証明書の情報が、以下のように表示されます。

```
[1] Subject:C=FI, O=xxxxxxxxxxxxxx, OU=Web, CN=CA1
Issuer:C=FI, O=xxxxxxxxxxxxxx, OU=Web, CN=CA1
Serial Number:c9
Validity: 2001.02.28 14:55:32 - 2002.12.31 23:59:59
Key Usage:DigitalSignature KeyCertSign CRLSign
[2] Subject:C=jp, O=YYY, CN=XXX
Issuer:C=FI, O=xxxxxxxxxxxxxx, OU=Web, CN=CA1
Serial Number:3c106275
Validity: 2001.12.07 00:00:00 - 2002.02.01 00:00:00
Email Address:xxx@xxxxxxxxxx.xx
CRL DistPoint:http://ldap.xxxxxxxxxxx
Key Usage:DigitalSignature KeyEncipherment
```

- 3 コマンド入力待ち状態になります。

```
#
```

設定情報を確認する

displayコマンド

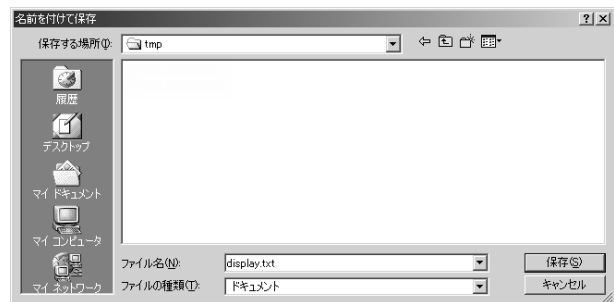
全設定情報を、コマンド入力形式で確認することができます。

< Webブラウザ操作 >

- 1 画面左側のメニューから [全設定情報を取得] を選択します。



- 2 設定情報を保存するファイルを指定します。



- 3 コマンドで入力した形式の全設定情報が、テキストファイルで保存されます。

設定情報を確認する

< コマンド操作 >

1 「display」と入力します。

```
#display
```

2 コマンドで入力した形式の全設定情報が表示されます。

```
hereis
description:FITELnet-F40 A V01.02 2001.12.14 (00:80:bd:cf:f1:00)
node      :
manager   :
location  :

date
011210.041513 (0 00:35:05)

ipripstatic
:
:
:
```

3 コマンド入力待ち状態になります。

```
#
```

ファームウェアのアップデート

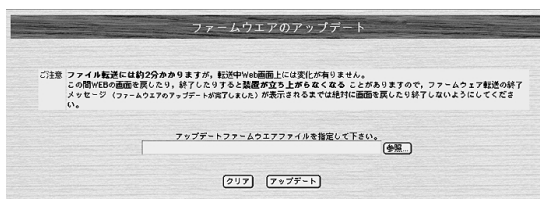
ファームウェアファイルを端末から本装置へ書き込み、設定情報を保存することができます。
(ファームウェアと設定ファイルの2種類のファイルがあります。)

< Webブラウザ操作 >

最新ファームウェアを本装置へ送信し、ファームウェアをアップデートします。まず、ホームページから最新のファームウェアを端末にダウンロードしてからアップデートしてください。

- 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、ログインIDに「root」と入力し、パスワードは空欄のまま[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 [ファイル転送]をクリックします。
- 5 [ファームウェアをアップデートする]をクリックします。

ファームウェアのアップデート画面が表示されます。



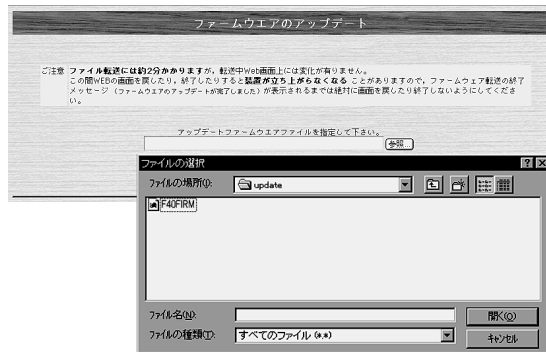
次ページへ続く

お知らせ

コンフィグレーションパスワードが設定されていない状態でファームウェアのアップデートを行おうとすると、「パスワードを設定してください」というメッセージが表示され、ファームウェアのアップデートはできません。先にコンフィグレーションパスワードを設定してください。(●P1-25)
最新のファームウェアは、FITElnet ホームページからダウンロードして、入手してください。
(●クイックスタートガイド)
ファームウェアのアップデート後は、本装置を再起動してください。
(●P1-32)

ファームウェアのアップデート

- 6 [参照] をクリックし、端末に保存されているファームウェアファイルを選択します。



- 7 [アップデート] をクリックします。
最新ファームウェアが本装置に送信されます。

- 8 ファームウェアのアップデート後は、本装置をリセットしてください。

ファームウェアのアップデート

⚠ 注意

「INVALID」が表示されているとき、端末および本装置の電源をOFFにしたり、再起動したりしないでください。本装置が動作しなくなる可能性があります。

<コマンド操作>

FTPを使ってファームウェアをアップデートすることができます。ログインに必要なデータは下記の通りです。出荷時の状態ではパスワードが設定されていません。パスワードを設定してから操作してください。

項目	説明
HOST	本装置のIPアドレス（工場出荷時は192.168.0.1）
ユーザID	ログインID（設定していない場合は"root"）
コンフィグレーションパスワード	本装置のコンフィグレーションパスワード
Directory	指定なし

SYSTEMランプ、CHECKランプの両方が点灯している場合もユーザIDは、" root "となる

1 FTPでログインします。

IPアドレス、ユーザID、コンフィグレーションパスワードを入力します。

```
ftp 192.168.0.1
Connected to 192.168.0.1.
220- Wait a moment. Now checking firmware.
220 FTP server ready.
Name (192.168.0.1): root ← ログインIDを入力
331 Password required for root.
Password: ← コンフィグレーションパスワードを入力
230 User root logged in.
```

2 端末に保存されているファームウェアファイルを本装置にバイナリでPUTします。

```
ftp>binary
200 Type set to l.
ftp>put F40FIRM
```

3 バージョンを確認します。

本装置の中にある「FIRMINFO」ファイルを確認します。

```
ftp> get FIRMINFO -
200 PORT command ok.
150 Opening data connection for FIRMINFO (192.52.150.2,1829).
SIDE-A: VALID
ID: WAKATO
EXTID: XAP4
FIRM VER: V01.00
FILE VER: 041099
226 Transfer complete.
remote: FIRMINFO
87 bytes received in 0.0036 seconds (24 Kbytes/s)
ftp>
```

お知らせ

SYSTEMランプ、CHECKランプの両方が点灯した状態では、EWAN側が使用できませんので、ホームページから新しいファームウェアを取得できません。ファームウェアはCD-ROMにも収録されていますので、一度そのファームウェアをインストールした後、ホームページから新しいファームウェアを取得してバージョンアップしてください。

格納場所：CD-ROM\FIRM\F40FIRM

次ページへ続く

ファームウェアのアップデート

「SIDE-A」という項目が「VALID」になっていることを確認してください。「INVALID」になっていた場合、再度PUTし直す必要があります。

4 ログアウトします。

```
ftp>bye
```

5 本装置を再起動します。

新しいファームウェアで動作するには本装置を再起動してください。(▶P1-32)

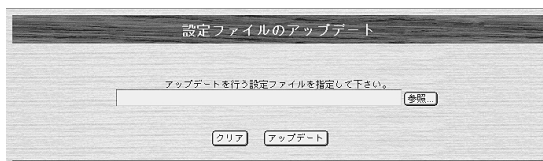
設定ファイルのアップデート/ダウンロード

本装置に設定されている設定情報を端末にダウンロードして保存することができます。また、保存した設定情報を本装置にアップデートすることもできます。

設定ファイルのファイル転送

< 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[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 [ファイル転送]をクリックします。
- 5 設定ファイルをアップデートする場合は[設定ファイルをアップデートする]、設定ファイルのバックアップをとる場合は[設定ファイルをダウンロードする]をクリックします。
(例)[設定ファイルをアップデートする]を選択した場合



次ページへ続く

- 6 アップデートする場合は、[参照] をクリックし、アップデートするファイルを選択します。



ダウンロードする場合は、[ダウンロード] をクリックします。

- 7 アップデートする場合は、[アップデート] をクリックして、設定ファイルをアップデートします。

ダウンロードする場合は、ファイルのダウンロード画面で [OK] をクリックすると、ダウンロードが開始されます。

<コマンド操作>

FTPを使い設定ファイルの本装置と端末の間でファイル転送することができます。ログインに必要なデータは下記の通りです。出荷時の状態ではパスワードが設定されていません。パスワードを設定してから操作してください。

項目	説明
HOST	本装置のIPアドレス（工場出荷時は192.168.0.1）
ユーザID	ログインID（設定していない場合は"root"）
コンフィグレーションパスワード	本装置のコンフィグレーションパスワード
Directory	指定なし

1 FTPでログインします。

IPアドレス、ユーザID、コンフィグレーションパスワードを入力します。

```
ftp 192.168.0.1
Connected to 192.168.0.1.
220- Wait a moment. Now checking firmware.
220 FTP server ready.
Name (192.168.0.1): root ← ログインIDを入力
331 Password required for root.
Password: ← コンフィグレーション
                パスワードを入力
230 User root logged in.
```

2 端末に保存されている設定ファイルの本装置にバイナリでPUTします。

(例) 装置から読む

```
ftp>binary
200 Type set to I.
ftp>get F40CONF
```

(例) 装置へ書き込む

```
ftp>binary
200 Type set to I.
ftp>put F40CONF
```

お知らせ

新しい設定ファイルで動作するには、本装置を再起動してください。

3 ログアウトします。

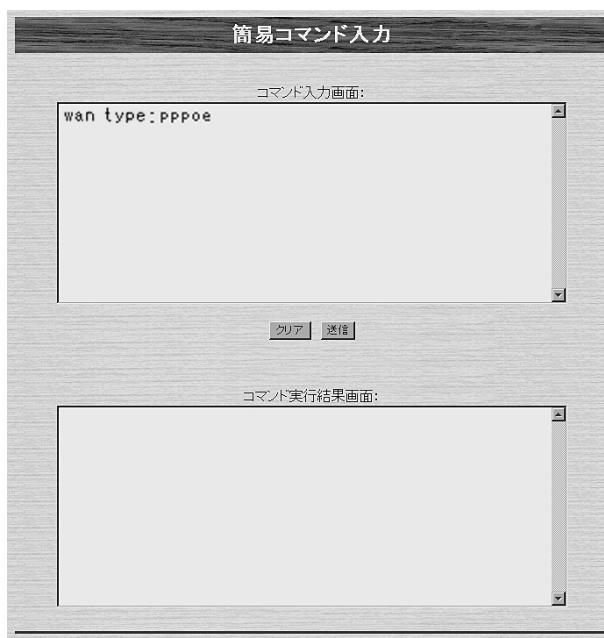
```
ftp> bye
```

簡易コマンド入力

本装置は、Webブラウザ操作の設定画面から、コマンドを入力して設定することもできます。

< 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[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** [簡易コマンド入力]をクリックします。
- 5** コマンド入力画面にコマンドを入力します。
コマンド実行結果画面に、コマンド入力の出力結果が表示されません。



お知らせ

簡易コマンド入力では、装置の設定に関するコマンドを入力できます。
各コマンドについては、コマンドリファレンスを参照してください。
コマンド操作で設定した場合は、装置を再起動してください

(●P1-32)

故障かな？と思ったら

こんなとき	確認してください	参照ページ
電源ケーブルを接続してもPOWERランプがつかない	電源スイッチがONになっていますか。	—
POWERランプがついているが、SYSTEMランプがつかない	装置異常です。弊社サポートデスクにご連絡ください。	●クイックスタートガイド P35
POWERランプがついているが、SYSTEMランプが点滅している	CHECKランプがついている場合は、装置異常です。弊社サポートデスクにご連絡ください。	●クイックスタートガイド P35
	CHECKランプが消えている場合は、装置起動中です。少しお待ちください。	—
CHECKランプが点灯し、SYSTEMランプも点灯している	起動するファームウェアが壊れて、バックアップファームウェアで起動しています。この状態では、FITEInet-F40の全ての機能を使用することができませんので、通常のファームウェアを入れなおしてください。	●P5-3
LANポートに端末、HUBを接続しているのにLANのランプがつかない	HUBのケーブルは、4番ポートに接続されていますか。 HUB接続時は、MDI/MDI-Xスイッチは「II」側になっていますか。 ケーブルの接続を確認してください。	●クイックスタートガイド P15
EWANポートとADSL/CATVモデムを接続しているのに、EWANのランプがつかない	速度・Duplex・MDIの設定が誤っている可能性があります。ディップスイッチで、接続しているADSL/CATVモデムの仕様に合わせてください。本装置は工場出荷状態では、10Mbps half Duplex MDIに設定されています。	●クイックスタートガイド P15

エラーメッセージ一覧

コマンドによるping実行時のエラーメッセージ

エラーメッセージ	原因	確認してください
[1011]Network is unreachable.	ネットワークに対するルート情報が見つからない。	<ul style="list-style-type: none"> • 入力を確認してください。 • ルーティング状態を確認してください。(▶P4-13) • LANまたはWANのケーブルが抜けていることが考えられます。ケーブルを見直してください。
[101d]No route to host.	ホストに対するルート情報が見つからない。	<ul style="list-style-type: none"> • 入力を確認してください。 • ルーティング状態を確認してください。(▶P4-13) • LANまたはWANのケーブルが抜けていることが考えられます。ケーブルを見直してください。
[1010]Network is down.	インタフェースがダウンしている。	<ul style="list-style-type: none"> • LANまたはWANのケーブルが抜けていることが考えられます。ケーブルを見直してください。
Ping Time Out.	相手からの応答がない。	<ul style="list-style-type: none"> • 相手端末が存在しないか、電源がOFFになっている可能性があります。

コマンド入力時のエラーメッセージ

コマンド入力時に表示されるエラーメッセージとその意味、対応方法を以下に記述します。

エラーメッセージ	意味	対応方法等
*** someone already login	多重ログインエラー	すでにログインされている装置にログインすることはできません。先のログインがログアウトされるのをお待ちください。あるいは、ログアウトしてもらってください。
*** permission denied	コマンドの実行レベルが違います。	コマンドには、ログイン状態（ログインモード）でしか実行できないもの、コンフィグレーションモードでしか実行できないものがそれぞれ存在します。コマンドが実行できるモードに変更してください。
*** illegal strings	入力された文字列はデータとして不正です。	正しい文字列を入力してください。
*** illegal password	入力したパスワードは登録されているパスワードあるいは登録しようとしているパスワードと違います。	正しいパスワードを入力してください。
*** illegal parameter <値等>	<値等>で示される入力はパラメータとして受け付けられません。	パラメータとして正しい内容を入力してください。
*** password too long	入力したパスワードが長すぎます。	パスワードは15文字以内で設定してください。
*** not yet password	コンフィグレーションパスワードの設定が行われていないので、コンフィグレーションモードには移れません。	コンフィグレーションパスワードの設定を行ってください。
*** parameter too long	入力したパラメータのデータは、長すぎて設定できません。	パラメータとして正しい内容を入力してください。

エラーメッセージ一覧

エラーメッセージ	意味	対応方法等
*** illegal address <アドレス値>	入力した<アドレス値>はアドレス値として不正です。	パラメータとして正しいアドレス値を入力してください。
*** parameter combination error	入力したパラメータの組み合わせが不正です。	正しい組み合わせで入力し直してください。
*** range error <値>	入力した<値>は設定できる範囲外にあります。	パラメータとして正しい範囲内の値を入力してください。
*** duplicate error	登録しようとしている内容は既に登録されています。	登録内容を見直すか、登録されている内容を削除してから登録してください。
*** registration overflow	登録できる件数を超過しました。	登録済みの内容を見直して不要な登録を削除してから、登録し直してください。
*** no entry	登録されているデータはありません。	必要ならばデータを登録してください。
*** no name	入力した名称は登録されていません。	登録されている名称を入力してください。
*** configuration busy	多重コンフィグレーションモードエラー	先に入っているコンフィグレーションモードが終了するのを待ってからコンフィグレーションモードに入ってください。FTPでログインされていたり、displayコマンドの表示がMOREで途中で止まっている場合でも同じ状態になります。
*** illegal socket <ソケット番号>	入力した<ソケット番号>が不正です。	正しいソケット番号を入力してください。
*** no entry <名称等>	入力した<名称等>は実行できるコマンドとして登録されていません。	コマンド名を見直してください。telnetにより非表示文字が入力された場合はその内容を16進値で<名称等>に表示します。

PPPoE使用時の回線ログ

回線ログの表示結果で、ecodeの部分の値により、PPPoEの状況を確認することができます。

【回線ログ結果】

```
000 0000:00:00.00 01/11/05 (mon) 10:49:08 PPPoE1 08050111 ecode
PPPoE Connect fail
```

ecode書式：0805xxyy

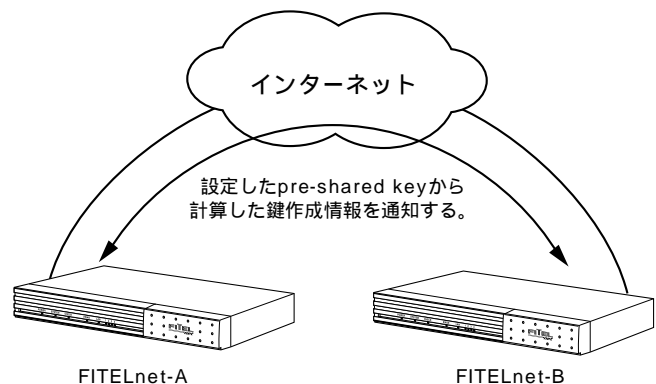
xx	0a : 接続 02 : 切断	01 : 接続失敗
yy	00 : 正常 01 : 無効セッション 02 : (既に) 接続中又は接続試行中 03 : (既に) 切断中 04 : (既に) 切断処理中 11 : ディスカバリ失敗	21 : PPP(LCP/AUTH/NCP) 折衝失敗 31 : 無通信による切断 32 : 手動による切断 (接続試行中の手動切断もこのモードとなる) 33 : PPP (LCP-TR受信、ECHO無応答等) による切断 34 : IF UPタイムアウトによる切断 35 : PADT受信による切断

VPNの通信手順

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

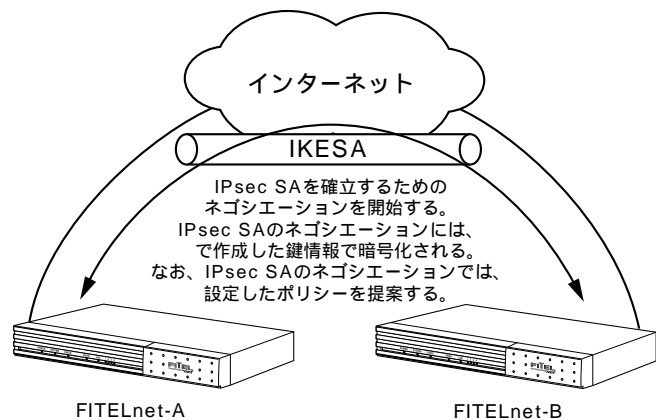
IKE SAの確立

共通鍵方式の場合は、設定した鍵データ (pre-shared key) から計算した鍵作成情報をお互いに通知します。設定する鍵データは、VPNを確立するルータ同士 (FITELnet-AとFITELnet-B) で同じでなくてはなりません。鍵作成情報 / 電子証明書が正しい場合 (公開鍵方式の場合は、お互いの電子証明書をやりとりします。) にVPN通信を開始することができます (IKE SA確立)。IKE SAを確立した際は、鍵作成情報から鍵を作成します。複数の相手とVPN接続する場合には、相手ごとの鍵が作成されます。



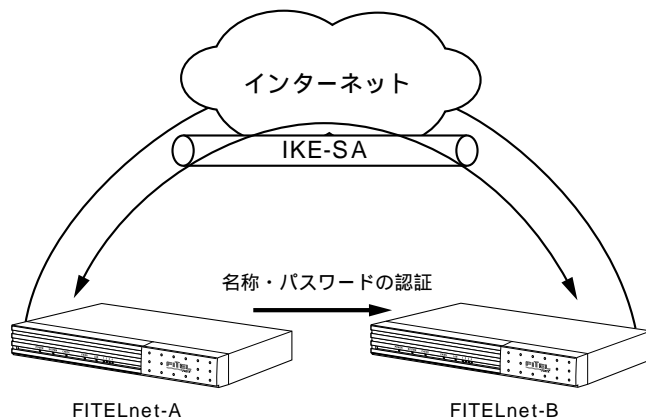
IPsec SAの確立

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



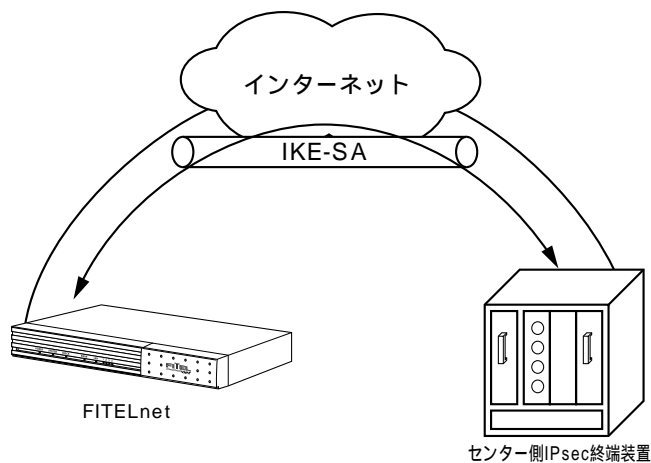
拡張認証

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



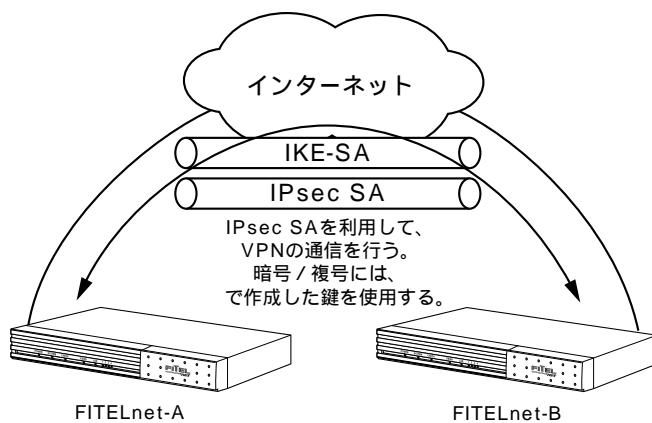
mode-config

VPN通信を行う相手から、VPNで使用するIPアドレスを指定してもらい動作します。センター側で、VPNのIPアドレスを一括管理するような場合に有効な機能です。FITELnet-F40は、IPアドレスを割り当てる機能はサポートしていません。



暗号化

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



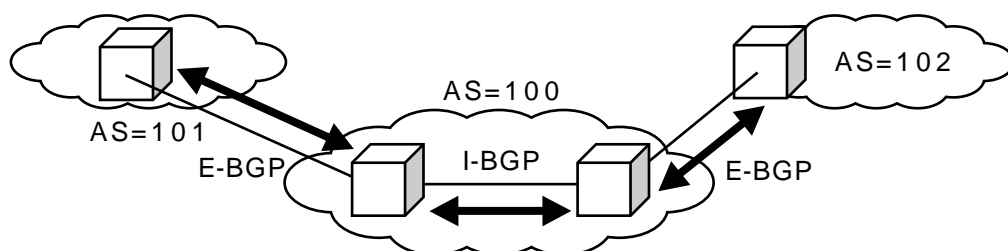
BGP 4 について

FITELnet-F40では、BGP Version 4 (BGP4)をサポートしています。
ここでは、BGP4のしくみ・使用方法について説明します。

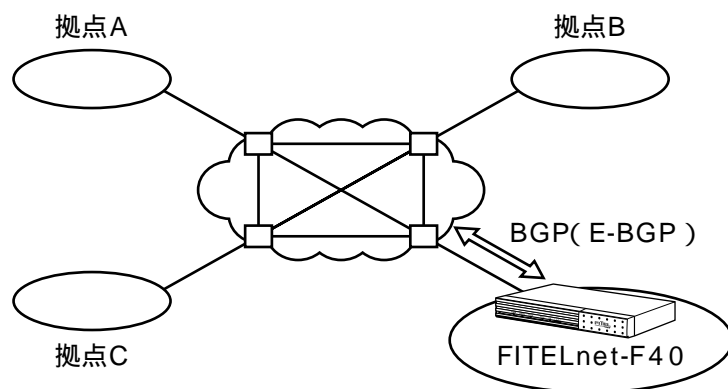
現在のインターネットを含めたTCP/IPのネットワークシステムは、AS (Autonomous System : 自律システム) と呼ばれるネットワーク単体が、互いに相互接続して、大規模なネットワークを形成しています。ASを識別するためには、AS番号があり、1~65535の範囲で割り振られています。このうち、1~64511はグローバルAS番号と呼ばれ、IANA (Internet Assigned Numbers Authority : IPアドレスやドメイン名等の割り当てを司る組織) からプロバイダ等で使用するよう予約されています。それに対し64512~65535はプライベートAS番号と呼ばれ、IP-VPN網やインターネットに接続する場合に使用するAS番号とされています。

AS内の経路情報をやり取りするルーティングプロトコルを「IGP : Interior Gateway Protocol」、AS間の経路情報をやり取りするルーティングプロトコルを「EGP : Exterior Gateway Protocol」と呼ばれています。IGPの代表的プロトコルにはRIP/OSPFがあり、EGPの代表的プロトコルにはBGPがあります。

ただし、BGPはIGPとしても使用でき、EGPとして使用するケースを「E-BGP」、IGPとして使用するケースを「I-BGP」と一般的には呼ばれています。FITELnet-F40では、「E-BGP」「I-BGP」のどちらもサポートしています。



FITELnet-F40で使用するケース (IP-VPN網のアクセスで使用する) を考えてみます。
多くのIP-VPN網は、IP-VPN網内の経路制御にBGPを利用しており、FITELnet-F40でBGP (E-BGP) を動作させることにより、IP-VPN網を含めたダイナミックな経路制御を行うことができます。



例えば、新規に拠点が追加された場合でも、設定を変更することなく、即座に経路を認識し通信を行うことができます。

IP-VPNの接続のみを考えた場合は、I-BGPは使用しませんので、設定は不要です。LAN側でBGPを使用する場合のみI-BGPの設定を行ってください。

PKI（公開鍵基盤）について

FITENet-F40では、共通鍵（Pre-shared Key）方式に基づいた方式と、公開鍵基盤（PKI）に基づいた方式の、2つのVPN通信方式をサポートしています。ここでは、公開鍵について説明します。

公開鍵基盤では、電子証明書がCA（Certificate Authority：電子証明書認証局）から発行され、その証明書を利用して、改ざん／なりすましを防ぐ方式を利用しています。

公開鍵基盤の特徴は、

- ・ 公開鍵・秘密鍵の2つの鍵のペアをもつ
- ・ 公開鍵で暗号化したデータは、秘密鍵でのみ復号できる。また、秘密鍵で暗号化したデータは公開鍵でのみ復号できる。
- ・ 電子証明書の中には、公開鍵・CAの情報が含まれている。

FITENet-F40での、公開鍵基盤を使用した鍵交換のしくみは、以下のようになります。

Initiatorは、CAの証明書を通知する。

Responderは、そのCAが発行する自分の証明書を通知する。

Initiatorは、通知された相手の証明書から公開鍵を取り出し、その鍵で暗号化した自分の証明書に、自身の秘密鍵で暗号化した署名をつけて通知する。

Responderは、自分の秘密鍵を使用して相手の証明書を復号できること／署名を相手の公開鍵で復号して相手であることに間違いがないことを確認し、認証OKとする。

この ・ の動作で、改ざん・盗聴防止（暗号化）／なりすまし防止（署名）の制御を行うことができます。

FITENet-F40では、

- ・ 鍵ペア（公開鍵・秘密鍵）の生成
- ・ 証明書を取得するためのリクエストデータの作成
- ・ 証明書の登録

を行い、PKI方式のVPN通信を行います。

各種設定方法については、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。

【アルファベット】**AH(Authentication Header)**

旧IPsecでは認証にはAHが必要でしたが、新仕様（RFC2406）からESPで認証が可能となり効率がよくなりました。FITELnet-F40ではサポートしていません。

AS番号

FITELnet-F40が属するAS（Autonomous System：自律システム）の番号を指定します。BGP4は、AS間のルーティングプロトコルとして知られています。

BGP4

IP-VPN網を含めたイントラネットの経路制御をダイナミックに行うためのプロトコルです。

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

証明書が有効かどうかを判定するリストです。CRLを使用する場合、相手の証明書が期限切れ等で無効になったかどうかを確認します。

DES-CBS

暗号化アルゴリズムの1つ。

DHCPクライアント

DHCP（Dynamic Host Configuration Protocol）は、LANに接続された端末に、IPアドレスやDNSアドレス等の情報を通知するプロトコルです。

FITELnet-F40では、WAN側にDHCPクライアント（割り当てられる側）の機能をサポートしています。

接続したADSLモデム/ケーブルモデムが、DHCPサーバ機能をサポートしている場合に、使用できます。

DHCPクライアントを使用する場合は、WANにアドレスを割り当てるなどの面倒な設定が不要になります。

DHCPサーバ

DHCP（Dynamic Host Configuration Protocol）は、LANに接続された端末に、IPアドレスやDNSアドレス等の情報を通知するプロトコルです。

FITELnet-E40では、LAN側及びWAN側にDHCPサーバ（割り当てる側）の機能をサポートしています。（WAN側では、DHCPサーバ機能とDHCPクライアント機能を併用することはできません）

LAN上の端末では、IPアドレス等の面倒な設定が不要になります。

（'IPアドレスを自動的に取得する'設定にしておいてください）

DHCP識別子

ADSLモデムやケーブルモデムから、DHCPでIPアドレスを割り当てられる形態で、ADSL/ケーブルTVインターネット事業者から通知された識別子を設定します。

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、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。

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。

Diffie-Hellman

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

ESP (Encapsulation Security Payload)

IPsecで規定されている認証・暗号のパケット方式。FITELnet-F40では、暗号アルゴリズムとしてDES (56bit)、3DES、NULL、ハッシュアルゴリズムとしてHMAC with MD5・HMAC with SHAをサポートしています (RFC2406)。

FQDNタイプ

FITELnet-F40がAggressiveモードで動作する場合に通知するnameの情報の送信形式を、FQDN or UserFQDNから選択します。

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

HMAC-MD5

認証アルゴリズムの一つ。

HMAC-SHA

認証アルゴリズムの一つ。

IKE (Internet Key Exchange)

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

Initiator

VPNネゴシエーションを行う側を指します。

IPsec

インターネットで暗号通信を行うための規格。

IPパケットフィルタリング

特定のパケットのみを中継させたり、特定のパケットを中継させずに廃棄したりする機能です。

FITELnet-F40では、ADSLやケーブルテレビインターネットの常時接続回線を利用するため、IPパケットフィルタリングを利用して、不正なアクセスを中継しないようにする必要があります。また、パケットフィルタリングにより廃棄されたパケットをログに残すことができます。

ISAKMP (Internet Security Association and Key Management Protocol)

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

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。

mode-config

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

FITELnet-F40は、IPアドレスを割り当てる機能はサポートしていません。

MTU長

PPPoEのMTU長を設定します。

フレッツADSLを使用している場合は、1454bytes以下に設定してください。

NAT機能

NAT (Network Address Transfer : アドレス変換) に関する設定をします。
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/
ケーブルテレビインターネットに、複数のパソコンから接続することができます

PFS

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

PKI

公開鍵基盤。信頼できる第三者機関から発行される電子証明書を使用してセキュアな通信を行うしくみ。

PKIキー

FITELnet-F40では、PKIを使用するために、PKIキーがインストールされている必要があります。PKI対応版FITELnet-F40をご購入いただいた場合は、すでにインストールされています。PKI未対応版をご購入いただいたお客様でPKI機能をご使用になる場合は、別途アップグレードキットをご購入ください。

PPPoE

PPP over Ethernet (略称PPPoE) の設定をします。
PPPoEは、フレッツADSLなど、ADSLを使用してインターネットに接続するためのプロトコルです。フレッツADSLなどのADSLインターネットに加入すると、PPPoEのソフトウェアフロッピーがADSL業者から提供されます。通常は、提供されたソフトウェアをパソコンにインストールしてインターネットに接続しますが、本装置のようにPPPoEをサポートしたルータを使用すると、パソコンにソフトウェアをインストールする必要はありません。
ADSLを使用する場合でも、PPPoEを使用しない場合がありますので、加入したADSL業者に確認してください。

Pre-Shared Key

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

ProxyARP

ProxyARPするかどうかを設定します。
FITELnet-F40のProxyARP機能は、FITELnet-F40が中継すべきパケットにのみ代理応答するモード (shortcut) と、FITELnet-F40が実際に中継しない場合でも代理応答するモード (any) の2種類があります。

RIPの制御

インタフェース毎にRIPを送受信する/しない、定期送信する/しないの設定をします。

Responder

VPNネゴシエーションを受ける側を指します。

SA(Security Association)

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

SNMPエージェント機能

SNMPマネージャから、FITELnet-F40を監視することができる機能です。

SNMPマネージャ

FITELnet-F40にアクセス可能/トラップを通知するSNMPマネージャのIPアドレスを登録します。
FITELnet-F40では、4件のSNMPマネージャを登録できます。

SNTP機能

現在時刻を取得するプロトコルです。

FITELnet-F40は、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サーバとしては動作しません。

syslog

FITELnet-F40のログ情報を、syslogサーバに通知することができます。

VPN

VPN(Virtual Private Network)は、インターネットのような開かれたネットワークを、あたかも専用線のような閉ざされたネットワークのように利用する技術です。FITELnet-F40はVPNの中の、ネットワーク層の暗号化/認証に特化したIPsec (IP Security) をサポートしており、専用線を用いなくても、安価にセキュリティの高いネットワークを構築できます。

さらに、FITELnet-F40では、暗号化/認証の処理をハードウェアで行っており、IPsecの性能に優れているという特徴があります。

VPNピア

VPNピアとは、IPsecのトンネルを確立する相手のことを指します。(SG: Security Gatewayということもある)

VPNを使用する場合、IPsecのトンネルを確立する相手を登録しておく必要があります。VPNピアは、相手のIPアドレスがわかっている場合はIPアドレスで指定しますが、相手のIPアドレスがわからない場合(プロバイダから動的に割り当てられるような場合)は名前で指定します。

【あ】

暗号化アルゴリズム

DESもしくは3DESより選択します。VPNピアどうして同じアルゴリズムである必要があります。

イベントログ

TELNETやFTPによるリモートログインに関するログを残すことができます。

【か】

鍵データ

鍵データ (Pre-shared Key) を設定します。鍵データは文字列もしくはバイナリで指定します。VPNピアと同じである必要があります。

学習フィルタリング機能

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。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。

拡張認証

FITELnet-F40では、IPsecの拡張認証(xauth)に対応しています。
拡張認証では、Phase1終了後にID/パスワードの認証を行います。

簡易DNS機能

FITELnet-F40が、DNSサーバとして動作します。
簡易DNS機能を使用する場合は、LAN側のPCのDNSの設定には、FITELnet-F40のIPアドレスを設定してください。LAN側でDHCPサーバ機能を使用する設定になっている場合は、FITELnet-F40のアドレスをDNSサーバとして通知します。
また、リクエストのドメイン名によりDNSサーバを振り分けたり、ホスト名とIPアドレスの組み合わせを設定しDNSサーバとして動作させることもできます。

コミュニティ名

SNMPマネージャとのコミュニティ名を設定します。
設定したコミュニティ名と、マネージャからの要求に含まれているコミュニティ名が異なる場合、SNMP機能が使用できません(認証失敗となります)。

コンフィグレーションパスワード

FITELnet-F40では、装置を扱うためのパスワードとして、「ログインパスワード」と「コンフィグレーションパスワード」の2つのパスワードがあります。
コンフィグレーションパスワードは、装置の設定を行う際に必要なパスワードです。また、Web設定にログインする際にも必要になります。
コンフィグレーションパスワードを忘れてしまった場合は、設定を初期化してください(▶P1-34)

【さ】

受信RIPフィルタリング

RIPパケットを受信するときに有効(あるいは無効)にするルーティング情報を設定することができます。

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。

FITELnet-F40の冗長機能は、

- ・ ルータグループ化機能
- ・ L3監視機能

の2種類があり、組み合わせて使用できます。

スタティックルーティング

経路情報を、静的にFITELnet-F40に設定します。

送受信ログ

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、およびフィルタリングしたパケットをログに残すことができます。

送信RIPフィルタリング

RIP情報を送信するかどうかを設定します。

【た】**ダイナミックルーティング**

経路情報を、動的にFITELnet-F40に設定します。

FITELnet-F40では、RIP1,RIP2及びRIP2bcastをサポートします。

タイムサーバ(SNTPサーバ)

現在時刻の情報を供給してくれるサーバです。タイムサーバを指定して、[現在時刻を取得] ボタンを押すことで、FITELnet-F40の時刻を設定することができます。また、指定した時刻(あるいは間隔)にタイムサーバに接続して、現在時刻を取得することができます。

デフォルトゲートウェイ

経路情報をもたない宛先に対して中継する場合のゲートウェイをデフォルトゲートウェイといいます。パソコン等は、経路情報をもたず、デフォルトゲートウェイの設定をするだけで、TCP/IPの通信ができるようになります。

FITELnet-F40では、DHCPサーバ機能で、デフォルトゲートウェイのアドレスも通知することができます。このことにより、パソコン等DCHPクライアントは、IPアドレスはもとより、デフォルトゲートウェイの設定も不要になります。

電子証明書

証明機関(CA: Certificate Authority)から取得した自身の証明書と、その機関の証明書がありません。

電子メール通知機能

不正アクセスがあった場合、管理者に電子メールを利用して通知する機能です。

ドメイン名

TCP/IPでは、IPアドレスとは別に、ドメイン名と呼ばれる名前で端末を管理しています。一般的なドメイン名の書式は、furukawa.co.jpなどです。通常、パソコンでは自身の属するドメイン名を設定する必要がありますが、FITELnet-F40にドメイン名を設定し、DHCPで配布することにより、パソコン等に設定する必要がなくなります。

トラストゲートウェイ

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を設定することができます。

トラップ

SNMPマネージャに対しての状態通知を、トラップといいます。

【な】**認証アルゴリズム**

HMAC-SHA1またはHMAC-MD5より選択します。VPNピアどうして同じアルゴリズムである必要があります。

【は】**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一致している必要があります。

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 [A] 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、「A」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、「A」以外の情報が有効となり、「A」の情報は無効となります。

フィルタリングログ (flog)

IPパケットフィルタリングにより廃棄されたパケットをログに残すことができます。

不正アクセス制御

FITELnet-F40では、不正アクセスを制御する機能として、以下の機能を備えています。

- TELNET/FTP/Webのアクセスを許可するインタフェースまたは端末を指定
- 不正アクセスと判断した場合は、アクセスを拒否

プリファレンス

経路情報の優先度を設定します。数値の小さいほうが優先度が高くなります。同じ宛先への情報が複数存在した場合、どの情報を採用するかのパラメータとして使用します。

【ま】

マルチルーティング機能

PPPoEを複数セッション（最大4セッション）確立するような形態で、送信元のパソコンや、使用するアプリケーションにより、利用するプロバイダをコントロールするような場合に使用する機能です。

メトリック

宛先へ到達するために経由するネットワークの数です。

【や】

ユーザID

フレッツADSLの加入時に、プロバイダから通知されたユーザIDを設定します。

ユニキャストRIP

通常のRIPは、ブロードキャスト宛またはマルチキャスト宛（RIP2）で、経路情報を通知しますが、FITELnet-F40は、特定のアドレス（ユニキャスト）宛のRIPを送信することができます。

この機能を使用すると、IP-VPN網のような、管理外の経路を通過する場合でも、遠隔拠点の経路情報を把握することができます。

【ら】

ルータグループ化機能

LAN上のFITELnet-E30と、冗長機能のためのグループを確立する機能を、ルータグループ化機能とといいます。

ルータグループ化機能では、実際にデータを中継するルータをマスタールータ、待機するルータをバックアップルータとといいます。

ルータグループ化機能を使用すると、マスタールータが動作できなくなった場合に、自動でバックアップルータに経路を切り替えて、通信を継続することができます。

ログインID

ログインIDは以下の場合に必要となります。

- (1) コンソールから装置のコマンドを使用する。
- (2) TELNETでログインして、装置のコマンドを使用する。
- (3) FTPでログインして、ファームウェアのアップデートや設定情報の保存などを行う。
- (4) Webブラウザで装置の設定・運用を行う。

ログインIDが設定されていない場合、以下となります。

- (1),(2)のケースではログインIDの問い合わせがありません。
- (3),(4)のケースでは、ログインIDには"root"を指定してください。

ログインパスワード

FITELnet-F40では、装置を扱うためのパスワードとして、「ログインパスワード」と「コンフィグレーションパスワード」の2つのパスワードがあります。

ログインパスワードは、コンソールやTELNETで装置にログインする際に必要なパスワードです。

ログインパスワードでログインした状態では、装置の設定を行うことはできません。

ログインパスワードを忘れてしまった場合は、コンフィグレーションパスワードで代用することができます。

アルファベット

Aggregate機能	2-125	NAT [*] の状態表示	4-21
BGP4について	5-14	NAT変換範囲の登録	2-78
bgpstateコマンド	4-15	pathchkisコマンド	4-36
bgprouteコマンド	4-15	Phase1方式	2-18、2-39
BGP機能	2-117	Phase1ポリシー	2-16、2-39
BGPピア	2-117、2-119	Phase2ポリシー	2-16、2-41
BGPフィルタリングの設定		ping応答制御	2-58
.....	2-117、2-121、2-123	PKI (公開鍵基盤) について	5-15
clogコマンド	4-26	PPPoEの接続	3-1
dateコマンド	4-2	PPPoEの切断	3-1
dhcpcinfoコマンド	4-34	pre-shared key	2-14、2-18、2-39
dhcpcstatコマンド	4-19	Proxy ARPの設定	2-106
DHCPクライアント	2-8	proxydnstisコマンド	4-33
DHCPクライアントの情報表示	4-34	rgroupingisコマンド	4-36
DHCPサーバ	2-85	RIP送受信制御	2-107
DHCPサーバの状態表示	4-19	SA確立契機	2-33、2-54
DHCPリレーエージェント	2-85	SAライフタイム	2-20、2-41
DHCPリレーエージェントの情報表示	4-40	sealedinfoコマンド	4-38
dhcprdiscardコマンド	4-40	SNMPエージェント	2-75
elogコマンド	4-22	SNMPマネージャ	2-76
flogコマンド	4-27	SNTP	2-100
hereisコマンド	4-2	stchannelコマンド	4-6
ikeclearコマンド	3-4	stdhcprコマンド	4-40
ipsecclearコマンド	3-4	stipコマンド	4-6
ipinterfaceコマンド	4-11	syslog	2-90
iprouteコマンド	4-13	TCP MSSの設定	2-130
IPsec処理タイプ	2-32、2-53	telnetを利用した設定	1-11
IPパケットフィルタリング	2-61	vlogコマンド	4-25
LAN上の端末指定	2-80	vpncertinfoコマンド	4-42
Layer3監視	2-70	vpnlogコマンド	4-29
lineisコマンド	4-4	VPN SAの状態表示	4-30
llogコマンド	4-23	vpnsainfoコマンド	4-30
mailinfoコマンド	4-28	vpnstatコマンド	4-6
mode-configモード	2-27、2-48	VPNを使用したNATスタティック機能	2-57
multirouteisコマンド	4-17	VPN制御	3-2
NAT	2-77	VPN対象パケット	2-29、2-50
natinfoコマンド	4-21	VPNで使用する電子証明書の情報 (自身の証明書 / CAの証明書) はクリアせずその他の情報 (パスワードを含む) を工場出荷時の設定に戻してから再起動	1-37
NATスタティック登録	2-83	VPN動作モード	2-16、2-37
NAT動作モード	2-27、2-48	VPNの設定	2-14、2-36
NAT [*] スタティック登録	2-80		

VPNピア	2-23、2-44
VPNピア識別	2-23、2-44
VPNログの表示	4-29
WAN側運用形態	2-3、2-8、2-11
Webサーバの公開	2-79
Webブラウザを利用した設定	1-9

五十音

【あ行】

宛先指定	2-29、2-50
暗号化アルゴリズム	2-19、2-21、2-40、2-42
アクセス制御	2-58
イベントログの表示	4-25
インフォメーション画面	4-1
エラーメッセージ	5-10
エラーログの表示	4-22

【か行】

回線ログの表示	4-23
外部からの接続抑制	2-58
外部に見えるIPアドレス	2-80
鍵データ	2-25、2-46
鍵データの再生成	2-21、2-42
学習フィルタリング	2-64
学習フィルタリングの情報表示	4-38
拡張認証	2-24、2-45
拡張認証の設定	2-35
簡易DNS	2-92
簡易DNSの情報表示	4-33
簡易コマンド入力	5-8
簡易ファイアウォール機能	2-58
簡単設定	2-1
現在時刻の取得	1-30
現在時刻の設定	1-28
故障かな?と思ったら	5-9
コマンドを利用した設定	1-14
コンフィグレーションパスワード	1-25

【さ行】

再起動	1-32
-----	------

時刻を手動で設定する	1-28
受信RIPフィルタリングテーブル	2-109
手動接続	2-10
詳細設定	2-1
冗長機能	2-66
冗長機能の情報表示	4-36
初期化	1-34
スタティックルーティング	2-104
設定情報を確認する	4-43
設定ファイル	5-5
全設定を工場出荷時に戻して再起動する	1-34
送受信ログ	2-102
送受信ログの表示	4-26
送信RIPフィルタリングテーブル	2-111
送信元指定	2-30、2-51
装置情報の表示	4-2
装置へのFTP、telnet、Web設定のログイン制御	2-59
装置を再起動する	1-32

【た行】

タイムサーバから時刻を取得する	1-30
中継先DNS IPアドレスの設定	2-93
中継しないIPパケットの登録	2-63
中継するIPパケットの登録	2-62
通信状態の表示	4-4
ディップスイッチによる初期化	1-36
電子メール通知統計の表示	4-28
電子メールで通知する	2-98
統計情報の表示	4-6
動作環境	1-8
ドメイン名称とDNS IPアドレスの登録	2-95

【な行】

認証アルゴリズム	2-21、2-42
----------	-----------

【は行】

ハイパーターミナル	1-16
配信データの設定	2-88
配布アドレスのスタティック登録	2-89
パスワード誤り時の動作	2-60
ハッシュアルゴリズム	2-19、2-40
ファームウェア	5-1

ファイル転送	5-5
フィルタリング属性	2-109、2-111
フィルタリングログの取得	2-61
フィルタリングログの表示	4-27
フレッツADSL	2-2
プロトコル	2-32、2-53
便利な設定	2-1
ホスト名称とDNS IPアドレスの登録	2-96
ポリシー識別子	2-18、2-20、2-39、2-41
マルチルーティング機能	2-71

【や行】

ユニキャスト宛RIP制御	2-113
--------------	-------

【ら行】

ルータグループ化	2-67
ルーティングインタフェースの表示	4-11
ルーティング状態の表示	4-13
ルーティング方法	2-108
ルート情報提供ルータの指定	2-115
ログインID	1-19
ログインパスワード	1-22

仕 様

項目		FITELnet-F40
LAN	10/100BASE-TX SWITCH	4ポート オートネゴ(内1ポートはMDI/MDI-X切り替え可)
WAN	10/100BASE-TX	1ポート オートネゴ、固定(10/100,full/half) MDI/MDI-X切り替え可
電源		内蔵
サポートプロトコル		IP
IPルーティングプロトコル		スタティック、RIP、RIP2、BGP
PPPoE		(4セッション)
パケットフィルタリング		アドレス、プロトコル、ポート番号、インタフェース
DHCP		DHCPサーバ、クライアント、リレーエージェント
アドレス変換		NAT、NAT+(plus)、NATスタティック
冗長構成		(FITELnet-E30との組み合わせ)
電子メール通知		
簡易ファイアウォール	学習IPフィルタリング	
マルチルーティング(PPPoE複数セッション)		
簡易DNS		
SNTP		
SNMP		
SYSLOG		
VPN (IPsec)	ESP	トンネルモード
	暗号	DES(56bit)、3DES
	認証	MD5、SHA-1
	鍵交換	IKE/ISAKMP Pre-shared Key
	PKI(オプション)	RSA Signature(X.509V3)、CRL
	IKE Mode	Main Mode, Aggressive Mode, Quick Mode
	圧縮	LZS、IPCAあり/なしは設定による
設定、運用		WWWサーバ、コマンド
外形寸法、重量		273(W)×203(D)×44.5(H)mm、約1.5kg

: サポート

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

発行責任：古河電気工業株式会社