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は、ログインIDに「root」と入力し、パスワードは空欄のままで［送信］をクリックします。

2 パスワードを入力します。

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

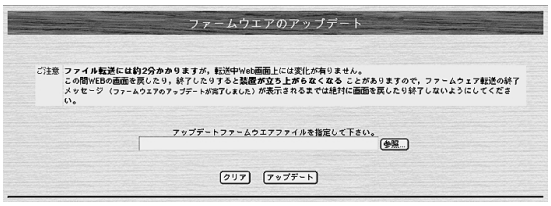
3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 ［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。



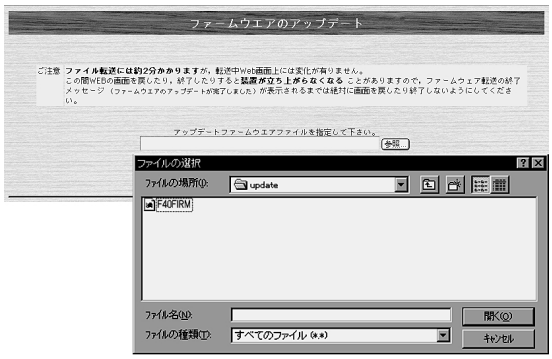
〈次ページへ続く〉

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 I.
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>
```

〈次ページへ続く〉

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

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で［送信］をクリックします。

2 パスワードを入力します。

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

3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 ［ファイル転送］をクリックします。

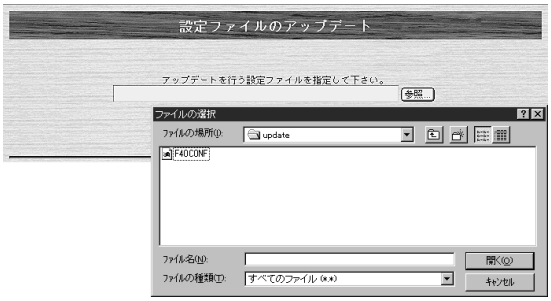
5 設定ファイルをアップデートする場合は［設定ファイルをアップデートする］、設定ファイルのバックアップをとる場合は［設定ファイルをダウンロードする］をクリックします。

（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〉

設定ファイルのアップデート/ダウンロード

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。

設定ファイルのアップデート/ダウンロード

＜コマンド操作＞

FTPを使い設定ファイルを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を本装置にバイナリでPUTします。

（例）装置から読込む

```
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
```

3 ログアウトします。

```
ftp> bye
```

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。

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で［送信］をクリックします。

2 パスワードを入力します。

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

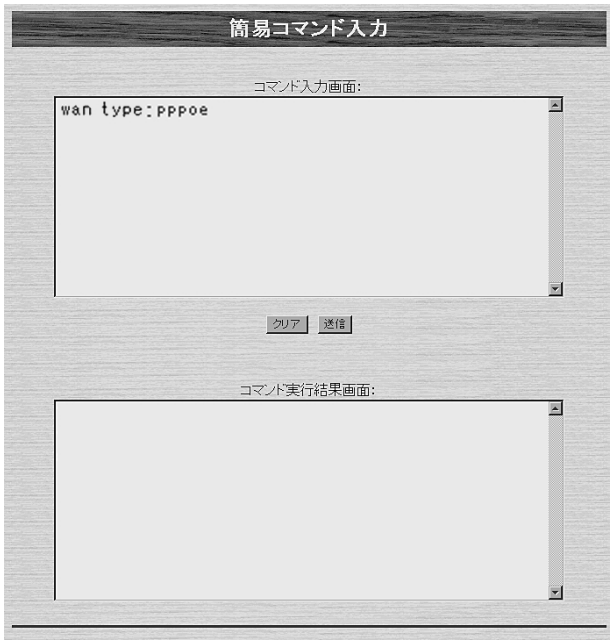
3 現在時刻を設定します。

変更しないときは、［次へ］をクリックしてください。

4 ［簡易コマンド入力］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す。



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、FITELnet-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。	• 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。	• 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。	• 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。	• 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ませんので、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えました。	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
                                          PPPoE Connect fail
```

ecode

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

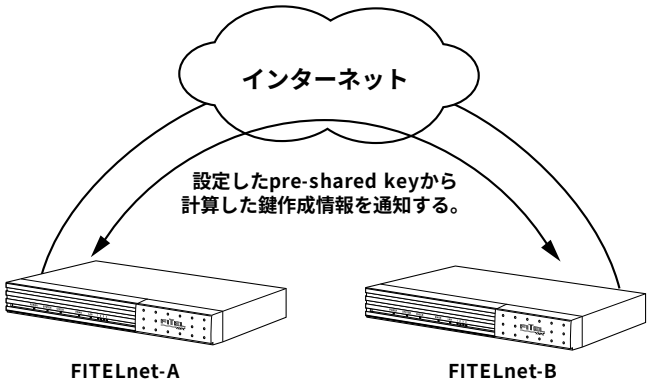
VPN機能について

VPNの通信手順

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

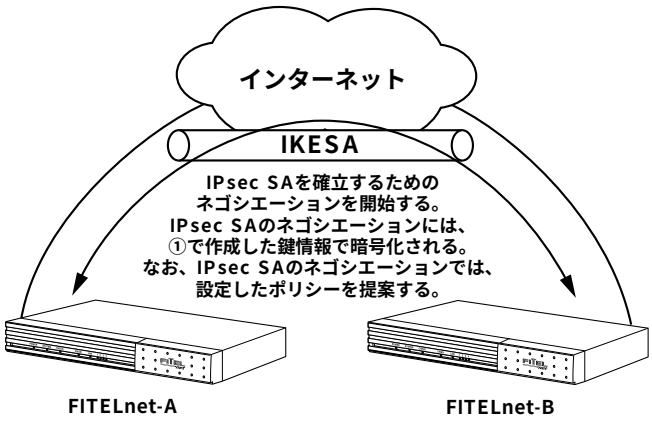
①IKE SAの確立

共通鍵方式の場合は、設定した鍵データ（pre-shared key）から計算した鍵作成情報をお互いに通知します。設定する鍵データは、VPNを確立するルータ同士（FITELnet-AとFITELnet-B）で同じでなくてはいけません。鍵作成情報／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。



②IPsec SAの確立

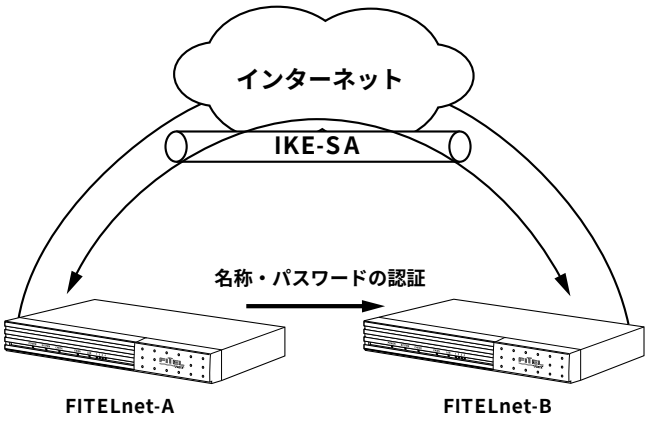
設定したVPN対象パケットに一致するパケットをLANから受信した場合、VPN対象パケットで設定してある相手に対して、IPsec SAを確立するためのネゴシエーションを開始します。IPsec SAのためのネゴシエーションには、①で作成された鍵を使用します。IPsec SA通信では、指定したポリシーで提案します。指定したポリシーでネゴシエーションが拒否された場合、通信はできません。IPsec SAを確立した際は、確立したIPsec SAを使用して通信する際の中継データを暗号化・認証するために使用する鍵が作成されます。
IPsec SAは、設定したLifetime間後に消滅します。消滅したあとにデー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



VPN機能について

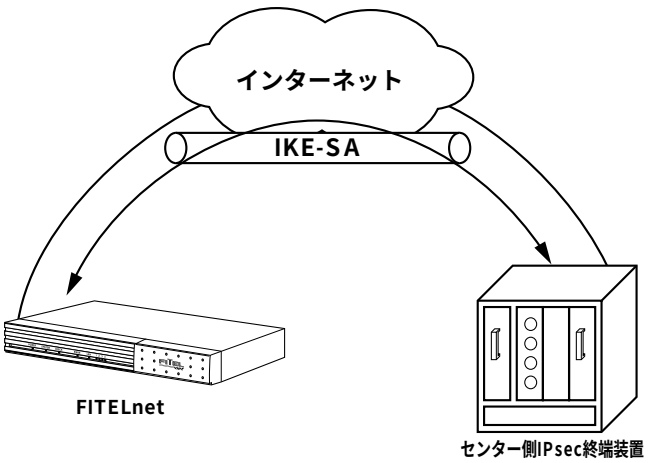
③拡張認証

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



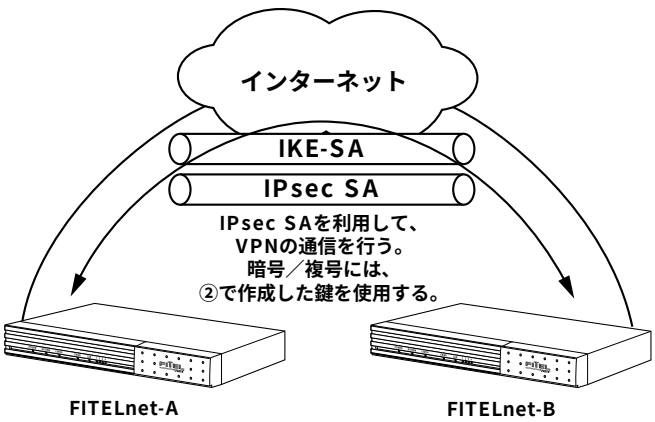
④mode-config

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。



⑤暗号化

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

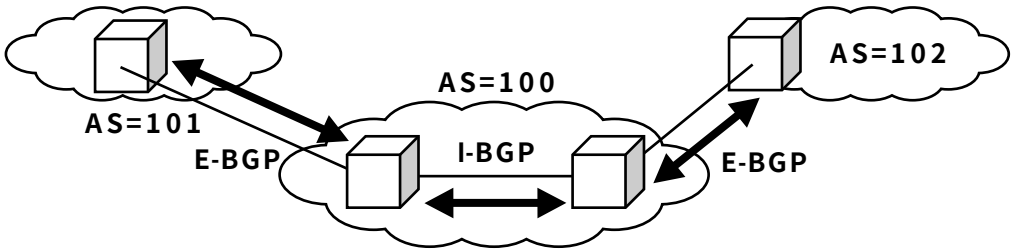


BGP4について

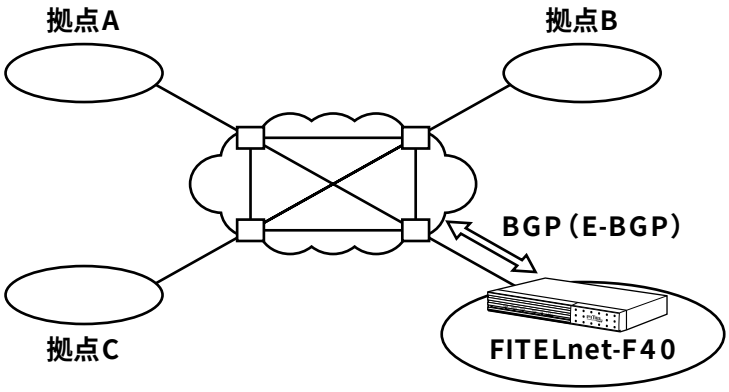
FITELnet-F40では、BGP Version 4（BGP4）をサポートしています。
ここでは、BGP4のしくみ・使用方法について説明します。

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

**FITELnet-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。

FITElnet-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。
①Initiatorは、CAの証明書を通知する。
②Responderは、そのCAが発行する自分の証明書を通知する。
③Initiator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。
④Responder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③・④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。

FILTEnet-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。

用語集

【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。

用語集

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。

用語集

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。

用語集

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ピアどうしで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。

用語集

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。

用語集

【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す。

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ピアどうしで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あっている必要があります。

用語集

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。

用語集

【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。

索　引

■アルファベット■

索　引

■五十音■

【あ行】

【か行】

【さ行】

【た行】

【な行】

【は行】

索　引

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

発行責任：古河電気工業株式会社

130-B0334-AH01-K
2003.1