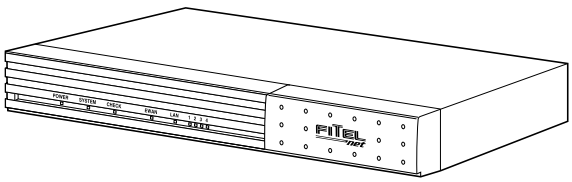
FITEL net

ブロードバンドアクセスルータ

FITELnet-F40

PKI（公開鍵基盤）-X.509機能に関する資料



古河電工

この取扱説明書のみかた

はじめに

このたびは、ブロードバンドアクセスルータFITELnet-F40のPKI（公開鍵基盤）-X.509（オプション）をお買い求めいただきまして、まことにありがとうございます。
本書は、ブロードバンドアクセスルータFITELnet-F40のPKI（公開鍵基盤）-X.509機能の取り扱いについて説明しています。
なお、ブロードバンドアクセスルータFITELnet-F40の基本的な取扱いについては「クイックスタートガイド」を、詳細な取扱いについては「取扱説明書」をご参照ください。

《この取扱説明書の構成》

1 **機能について**

2 **設定する**
本装置の設定方法を説明しています。

《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 機能について

電子証明機能に関する設定 ……4

2 設定する

証明書を取得するための準備 ……5

鍵の生成と登録……5

証明書使用時のパラメータの設定……9

証明書の取得および登録……12

電子証明書リクエストの作成 ……12

証明書の登録 ……17

CRL（Certificate Revocation List：証明書失効リスト）の取得……20

設定例……22

電子証明機能に関する設定

PKI-X.509機能で使用する鍵と電子証明書の登録

PKI-X.509による認証方式では、鍵と電子証明書を使用します。
PKI-X.509機能を使用する場合、この章の手順に従い証明書を登録する必要があります。
鍵には秘密鍵と公開鍵の２種類があり、電子証明書についても自身の証明とCAセンターの証明書があります。
本装置でPKI-X.509機能を使用するには、はじめに秘密鍵と公開鍵のペアを生成し、その後電子証明書を取得、登録します。手順は以下の通りです。
また、個々の設定を行う場合は、設定内容を有効にするために装置を再起動してください。

1　証明書を取得するための準備（☛P5）

鍵ペアの生成 ……PKI-X.509機能に必要な鍵ペアの生成
パラメータの設定 ……証明書に含める情報の設定

※上記の設定が終了したら装置の再起動をしてください。

2　証明書の取得および登録（☛P12）

電子証明書リクエストの生成、取得 ……CAセンターから証明書を入手するために必要なリクエストの生成、その後CAセンターから証明書を入手します
証明書の登録 ……入手したCAセンターからの証明書の登録

※上記の設定が終了したら装置の再起動をしてください。

お知らせ

PKI-X.509機能はオプションです、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。（☛取扱説明書P4-2参照）PKIキーがインストールされていない装置で、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いただく必要があります。下記のホームページもしくはお買い求めの販売店までお問い合わせください。
http://www.furukawa.co.jp/fitelnet/f/pki-upgrade.html

証明書を取得するための準備

鍵の生成と登録

RSA signatures機能で使用する鍵の生成、登録を行います。

＜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。

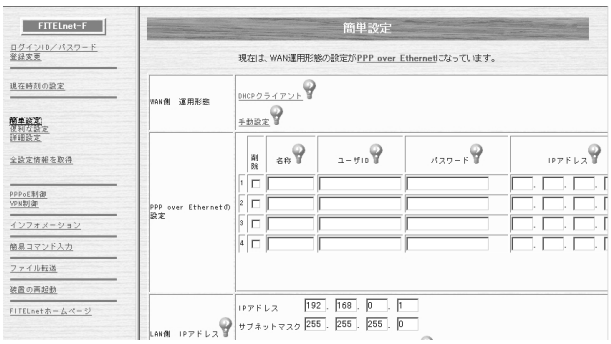
2 パスワードを入力します。

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。
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。



〈次ページへ続く〉

証明書を取得するための準備

5 ［VPNの設定］をクリックします。

6 VPN動作モードの［ON］を選択して、［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。）

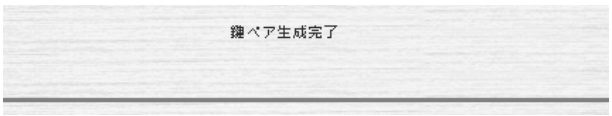
〈次ページへ続く〉

証明書を取得するための準備

7 鍵ペアの生成を選択します。

8 [生成] をクリックします。鍵ペアを生成します。

[生成] をクリック後、約2分ほどで “ 鍵ペア生成完了 ” のメッセージが表示されます。
上記の操作で、鍵ペアの生成が完了します。



証明書使用時のパラメータの設定に進みます。

ワンポイント

Web設定では、鍵のサイズは1024bit固定となります。
他のサイズの生成の必要がある場合は、コマンドにて設定を行ってください。

証明書を取得するための準備

＜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。(☛「取扱説明書」P1-13)

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

2 鍵のサイズを設定します。

サイズは、512bit～2048bitです。

鍵の生成が行われています。okの表示が出るまでしばらくお待ちください。
なお、サイズによる鍵の生成時間は以下の通りです。

512bit	約10秒
1024bit	約45秒
2048bit	約15分

```
conf#vpngenkey size=1024
generating a keypair...                                    ①
ok
conf#
```

証明書使用時のパラメータの設定に進みます。

ワンポイント

●既に鍵ペアが存在する場合

手順2の①の箇所でExist. New key pair create OK?(y/n)のメッセージが表示されますので、新しく鍵ペアを生成する場合は“y”を選択します。

証明書を取得するための準備

証明書使用時のパラメータの設定

Webブラウザで、証明書使用時のパラメータの設定を行います。

＜Webブラウザ操作＞

1 証明書使用時のパラメータを選択します。

2 証明書使用時の各種設定を入力します。

登録が終了すると、“ 証明書使用時のパラメータを以下の内容で登録しました。” と表示されます。

- **[CRL]**
  CRLを使用する（必ず使用/取得できたときだけ使用）/しないの選択をします。
- **[自身のEmailアドレス]**
  自身のEmailアドレスを設定します。この設定はFITELnet-F40がAggressive Modeで接続する場合に必要な設定です。
- **[自身のドメイン名]**
  自身のドメイン名を設定します。この設定はFITELnet-F40がMain Modeで接続する場合に必要な設定項目です。
- **[IPアドレス]**
  RSA signatures認証使用時の自身のIDとなります。
- **[ネームサーバアドレス]**
  証明書にCRLのURLが含まれていてHTTPでCRLを取得する場合、URLからIPアドレスを求めるためにネームサーバを使用します。
- **[LDAPサーバアドレス]**
  CRLがLDAPサーバにおかれている場合設定します。

〈次ページへ続く〉

証明書を取得するための準備

3 [送信] をクリックします。

設定内容が本装置に送信され、確認画面が表示されます。

4 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。

証明書を取得するための準備

＜コマンド操作＞

1 自身のEmailアドレス、ドメイン名を設定します。

```
conf# vpncertparam crl=use emailaddr=yyy@xxxx.co.jp
domainname=www.xxx.co.jp nameserver=x.x.x.x. ldapserver=y.y.y.y
```

2 設定を保存し、再起動します。

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

以上で、証明書使用時のパラメータの登録が完了しました。
次に、証明書リクエストの生成方法を説明します。

証明書の取得および登録

電子証明書リクエストの作成

Webブラウザで、電子証明書リクエストの作成を行います。

＜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。

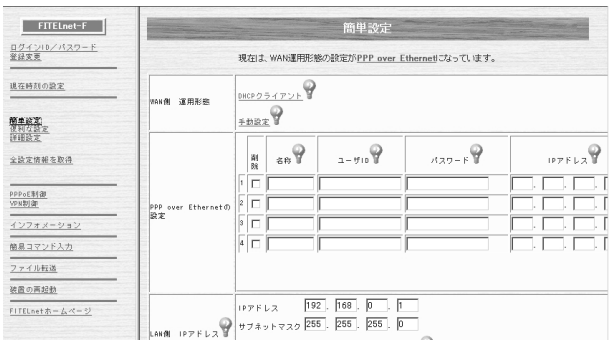
2 パスワードを入力します。

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。
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。



〈次ページへ続く〉

証明書の取得および登録

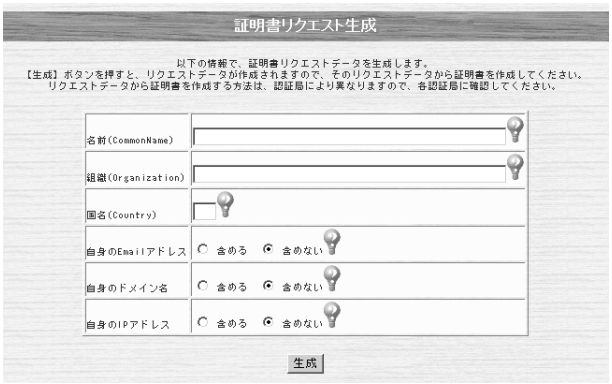
5 [VPNの設定] をクリックします。

6 [証明書リクエストデータの生成] を選択します。

〈次ページへ続く〉

証明書の取得および登録

7 各種設定を行います。



- **[名前(CommonName)]**
  一般名を登録します。最大64文字
- **[組織(Organization)]**
  組織名を登録します。最大64文字
- **[国名(Country)]**
  国名を登録します。（2文字の国コード）日本はJPです。
- **[自身のEmailアドレス]**
  証明書パラメータ（vpncertparam）で設定したemailaddressを証明書リクエストに入れます。
- **[自身のドメイン名]**
  証明書パラメータ（vpncertparam）で設定したdomainnameを証明書リクエストに入れます。
- **[自身のIPアドレス]**
  証明書パラメータ（vpncertparam）で設定したipaddrを証明書リクエストに入れます。

〈次ページへ続く〉

証明書の取得および登録

8 [生成] をクリックします。

PEM形式の証明書リクエストが表示されます。
PKCS#10 Base 64 (PEM)形式、PKCS#10 DER encoded 形式どちらかを選択して保存ボタンをクリックする事により、各形式でPCにファイルが保存されます。

本装置で作成した証明書のリクエストを使用して、CAセンターから証明書を取得します。
CAセンターでの証明書の取得方法は、各CAセンターの指示に従って行ってください。

以上で、証明書リクエストの生成が完了しました。
次に、取得した証明書の登録方法を説明します。

証明書の取得および登録

＜コマンド操作＞

1 証明書リクエストの生成に必要な、名前（CN）、組織（O）、国名（C）を設定します。

```
#vpncertreq CN=XXX O=YYY C=jp email domainname ip
```

入力が終了すると、画面のようにPEM形式の証明書リクエストが表示されます。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwLTELMAkGA1UEBhMCanAxDzANBgNVB
AoTBmRlbmtvdTENMAsGA1UEAxMEZnVydTCBnTANBgkqhkiG
9w0BAQEFAAOBiwAwgYcCgYEAiUXsnMDkEK0BV4l78L/XjCj
hMF+U49AinRrvBt2jPxTmlwlXH2AnnKPoFjXOY9MBv1aeTrdK
XlNLH3Ysan4HmcKQAR/iSSGybKrq809GSBmqGiKzv2PyZX4
5PXwlqSuui+Q7jHQBZC0FthfXeL69etZK3SleaP3zQWlACTkM
SHcCASGgQjBABgkqhkiG9w0BCQ4xMzAxMAsGA1UdDwQEA
wIFoDAiBgNVHREEGzAZghdqYWNrbWlnaS5mdXJ1a2F3YS5j
by5qcDANBgkqgkiG9w0BAQUFAAOBgQBRsKfc7Bwh0nQL5Y
sxSfNCBm+ujvxpy1ASYvnEL54KBeYMKvCop/PgIESGL3XJ+A
u30VXVCJ6gM3zQkXKYj0AuvRyS+lQ3pa1L1aSbb4xmHMjL5
wOdmzuhHbok870i4y/T2/FdBAyV0sxNQxAGSejG7QzuqwSBf
a62UMRQgCmqtg==
-----END CERTIFICATE REQUEST-----
#
```

本装置で作成した証明書のリクエストを使用して、CAセンターから証明書を取得します。
CAセンターでの証明書の取得方法は、各CAセンターの指示に従って行ってください。

以上で、証明書リクエストの生成が完了しました。
次に、取得した証明書の登録方法を説明します。

証明書の取得および登録

証明書の登録

Webブラウザで、PKI-X.509機能で使用する証明書の登録を行います。
証明書の登録には、自身の証明書と、CAの証明書共に登録する必要があります。

＜Webブラウザ操作＞

1 証明書の登録を選択します。

2 証明書の登録を行います。

新しく証明書を登録する場合は、［新規に登録］をクリックします。既に、登録してある証明書を削除する場合は、対象とするエントリの削除ボックスをチェックして［送信］をクリックします。

〈次ページへ続く〉

証明書の取得および登録

3 証明書の各種設定を入力します。

画面中央のウィンドウに自身または、CAセンターで取得した証明書をペーストします。
証明書の登録後は設定内容を有効にするためにリセットを行ってください。

- **[信頼できるroot CAの証明書である]**
  CAからの証明書を登録する場合はチェックします。自身の証明書を登録する場合は、チェックをしないでください。
- **[PEM format]**
  PEM formatの証明書をペーストして登録する場合に選択してください。
- **[ファイル]**
  PCに保存してある証明書を参照して登録する場合に選択します。

4 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。

5 装置を再起動します。

設定内容を有効にするために、FITELnet-F-40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。

以上の操作で証明書の登録は終了です。
以降の設定は、共通鍵方式（Pre-Shared Key）の設定方法と共通になりますので、「取扱説明書（☛P2-14）」を参照してください。

証明書の取得および登録

＜コマンド操作＞

1 証明書の登録を行います。

自身の証明書を登録する場合は、"vpncert add"と入力します。

```
conf#vpncert add
"Input certificate"
```

"Input certificate"と表示されるので、自身の証明書を登録します。

CAセンター証明書を登録する場合は、"vpncert add root"と入力します。

```
conf#vpncert add root
"Input certificate"
```

"Input certificate"と表示されるので、CAセンター証明書を登録します。
証明書を追加する場合、証明書の入力が終了した後^d（Controlキー＋d）を入力します。
^d（Controlキー＋d）入力後OKが表示された場合は、証明書は正しく登録されています。エラーになった場合は、再度登録操作を見直してください。

自身の証明書およびCAセンターの証明書を登録後は、設定内容を有効にするためにリセットを行ってください。

2 設定を保存します。

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

以上の操作で証明書の登録は終了です。
以降の設定は、共通鍵方式（Pre-Shared Key）の設定方法と共通になりますので、「取扱説明書（☛P2-14）」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を取得する命令です。通常は証明書に書かれているCRL Dest Pointに対して自動でCRLを取得しますが、手動で取得する際にこのオペレーションを行います。

＜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。

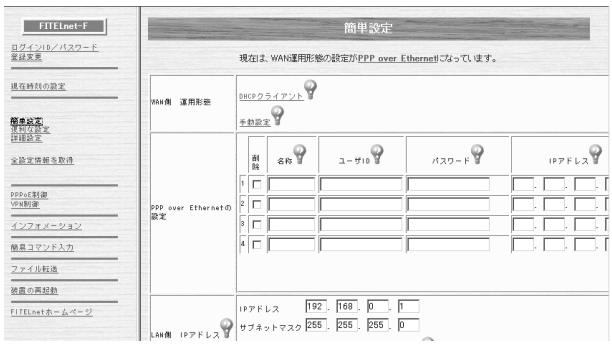
2 パスワードを入力します。

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。
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［VPN制御］をクリックします。



〈次ページへ続く〉

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

5 ［CRLの取得］をクリックします。

6 取得するCRL Dist Pointを選択し、［取得］をクリックします。

設定例

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

＜VPN動作モード＞

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

＜証明書登録用パラメータ設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPNの設定	CRL	取得できた場合のみ使用する
		自身のEmailアドレス	aaa@xxxxxx.ne.jp
		自身のドメイン名	aaa.xxxxxx.ne.jp
		自身のIPアドレス	なし
		ネームサーバアドレス	yyy.yyy.yyy.yyy
		LDAPサーバアドレス	zzz.zzz.zzz.zzz

＜証明書リクエストデータの生成設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPNの設定	名前（CommonName）	FITELnet-F40
		組織（Organization）	FURUKAWA
		国名（Country）	JP
		自身のEmailアドレス	含める
		自身のドメイン名	含める
		自身のIPアドレス	含めない

＜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	RSA Signature
		暗号化アルゴリズム	des
		ハッシュアルゴリズム	md5

設定例

＜Phase2ポリシーの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPNの設定	ポリシー識別子	1
		SAライフタイム	600秒 1000kbytes
		鍵データの再生成	しない
		暗号化アルゴリズム	des
		認証アルゴリズム	hmac-md5

＜VPNピアの設定例＞

分類	画面名	設定項目	入力値
便利な設定	VPNの設定	VPNピア識別 相手IPアドレス指定 相手名称指定 こちらの名前	 158.xxx.xxx.1 空欄 FITELnet-F40
		拡張認証	相手を認証しない
		鍵データ	(空欄)
		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
		RSA signatures 認証使用時の自身のID	email
		DN	(空欄)

設定例

＜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
		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

設定例

＜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。（☛取扱説明書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 鍵ペアを生成します。作成には約45秒程度かかります。

```
conf# vpngenkey
generation a keypair
ok
conf#
```

4 証明書使用時のパラメータを設定します。

```
conf# vpncertparam crl=use emailaddr=aaa@xxxxxx.ne.jp
domainname=aaa.xxxxxx.ne.jp nameserver=yyy.yyy.yyy.yyy
ldapserver=zzz.zzz.zzz.zzz
conf#
```

5 設定を保存し、再起動します。

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

〈次ページへ続く〉

設定例

6 ログイン後、電子証明書リクエストを作成します。

```
Login password:
# vpncertreq CN=FITELnet-F40 O=FURUKAWA C=jp email domainname
-----BEGIN CERTIFICATE REQUEST-----
MIIBoDCCAQkCAQAwJjERMA8GA1UECh4IU+Rss5b7XeUxETAPBgNVBAMeCGWJheR5
wE4AMIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgFLsbKpzM+OHFwYlUxu7g7XH
vlWPuJjEcZWlkczhhcZHVpxmauUFYylNTwb6RrYYQxeZNmw8uBTPA+iJO9Wt16KH
0aOVH2FUhszyX8D5k1mGjq8ziv7DvQsREuPOvYqb4f7Cfbju+JTJQZdlbQdXyU+t
n5H7fXv4vHeI8jdrAoDzAgMBAAGgOzA5BgkqhkiG9w0BCQ4xLDAqMCgGA1UdEQQh
MB+HBJ7K6oCBF3NodXVAaW5mLmZ2cnVrYXdhLmNvLmpwMA0GCSqGSIb3DQEBBAUA
A4GBACz6tGA2WOjH/mN2zqKltTyLMTMxyOi/5AtEhF6cPmBYKgPo9sjssDePwUpH
fOzncUhXrjT/bwPLTGswfD3/b6ISML39innKN9SqCQZCP+l+AEvrCoae5/qxTfV2
OgI979vliZJAevk+u95GzDzkr8bMttqQeiajEDGHsjQ27E0b
-----END CERTIFICATE REQUEST-----
#
```

---BEGIN CERTIFICATE REQUEST--- から
---END CERTIFICATE REQUEST--- までが、
証明書リクエストデータになります。
信頼できるCAセンターで、このリクエストデータから自身の電子証明書を発行してもらい、同時にCAセンターの証明書も取得してください。

7 証明書が取得できたら、証明書を登録します。

証明書を登録するために、コンフィグレーションモードに移行します。（☛取扱説明書P1-13）

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

〈次ページへ続く〉

設定例

8 自身の証明書を登録します。

```
conf# vpncert add
"Input certificate"
-----BEGIN CERTIFICATE-----
MIIEGwYJKoZIhvcNAQcCoIIEDDCCBAgCAQExADALBgkqhkiG9w0BBwGgggPwMIID
7DCCA1WgAwIBAgIEO5lYFjANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJVUzEQ
MA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25zdHJh
dGlvbiBDZXJ0aWZpY2F0ZXMwHhcNMDExMjA1MDMzMjM0WhcNMDQxMjA1MDQwMjM0
WjCBxjELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VudHJ1c3QxLzAtBgNVBAsTJkVu
dHJ1c3QgUEtJIERlbW9uc3RyYXRpb24gQ2VydGlmaWNhdGVzMUUwQwYDVQQLEzxO
byBvMaWFiaWxpdHkgYXMgcGVyIGh0dHA6Ly9mcmVlY2VydHMuZW50cnVzdC5jb20v
bGljZW5zZS5odG0xHjAcBgNVBAsTFUVudHJ1c3QvVlBOIENvbm5lY3RvcjENMAsG
A1UEAxMEU0hVVTCBnjANBgkqhkiG9w0BAQEFAAOBjAAwgYgCgYBfChu54wuv5V7a
kt8/eeapTYppB2JgO2S+JHLRLBKsf+YMoe9lVLMe1uTsaA60UMsCv2QUaGrb6jwC
/V3fM0y9t/1LRWtH4DFB3GnZtS3tG+/hxHUBuTxVL1pzR0im3M7PV202ro7rebMY
bh7BU5MrgR2Zoqbr75vE83slTsDBlQlDAQABo4IBWzCCAVcwQQYDVR0RBDowOIcE
nsrqglEXc2h1dUBpbmYuZnVydWthd2EuY28uanCCF3NodXUuaW5mLmZ1cnVrYXdh
LmNvLmpwMAsGA1UdDwQEAwIAoDArBgNVHRAEJDAigA8yMDAxMTIwNTA0MDIzNFqB
DzIwMDQwMTExMDgwMjM0WjByBgNVHR8EazBpMGegZaBjpGEwXzELMAkGA1UEBhMC
VVMxEDAOBgNVBAoTB0VudHJ1c3QxLzAtBgNVBAsTJkVudHJ1c3QgUEtJIERlbW9u
c3RyYXRpb24gQ2VydGlmaWNhdGVzMQ0wCwYDVQQDEwRDUkw5MB8GA1UdIwQYMBaA
FHNSsvL8PTcMqhffaMAOOpbtViW6MB0GA1UdDgQWBBQGCxSN7wwl3XnsFStJ/v8t
B1z3VzAJBgNVHRMEAjAAMBkGCSqGSIb2fQdBAAQMMAobBFY0LjADAgSwMA0GCSqG
SIb3DQEBBQUAA4GBAGQ5muCpRg/lyX/eKNY3AcSDSPHeDxQKFlCMlTm6LA6emKRi
6gkvtPq0btxilzkMEw8Ob9MYRvrWiXYsggc6TuuyywFmr2SUWpcqkl0WFytwAm8m
ULPK9sVTWPpjhrvDfnCndscuv1t1Nl1qpVNf/CU4/rEsTIFpPqTFawHOXe7YMQA=
-----END CERTIFICATE-----
Ctrl+Dを入力
conf#
```

〈次ページへ続く〉

設定例

9 CAセンターの証明書を登録します。

```
conf# vpncert add root
"Input certificate"
-----BEGIN X509 CERTIFICATE-----
MIICTDCCAbWgAwIBAgICAMkwDQYJKoZIhvcNAQEFBQAwWjELMAkGA1UEBhMCRkkx
JDAiBgNVBAoTG1NTSCBDb21tdW5pY2F0aW9ucyBTZWN1cml0eTERMA8GA1UECxMI
V2VilHRlc3QxEjAQBgNVBAMTCVRlc3QgQ0EgMTAeFw0wMTAyMjgxNDU1MzJaFw0w
MjEyMzEyMzU5NTlaMFoxCzAJBgNVBAYTAkZJMSQwIgYDVQQKExtTU0ggQ29tbXVu
aWNhdGlvbnMgU2VjdXJpdHkxETAPBgNVBAsTCFdlYiB0ZXN0MRIwEAYDVQQDEwlU
ZXN0IENBIDEwgZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBAI3wb1DaZUvk7L+d
sQxr8hD7YFSqUlTy6xJFKj7DzgulhU9w5Jlt83qxeXp1aMcjhK//00feFhM4lEH+
JNi3Qk4Hbcwqtmz4jFW58ib0GSWq9LR7hFdakDVKQJtiCPLM9zZ8PY1REd04wwiH
lGCPKBZJdl/FjC3wyaw4CKgnJ6jTAgEloyMwlTALBgNVHQ8EBAMCAYYwEgYDVR0T
AQH/BAgwBgEB/wlBMjANBgkqhkiG9w0BAQUFAAOBgQAGfJNNvXRspfh6PZ45S+mD
1QJYmj8/j1sh6ipwOYHb4lBtAE4iPgywGE24Jk8MQdYzQ2J1lZTUVAqxU1pnyxAk
vTqpEdvMUxJd5mbHHZrUjSs5Mqsiq7rKfjU0eJEWeAAh7vBx1lBZ6KXR0jy6iETO
tgAK98NcY12kqB8BI+jroQ==
-----END X509 CERTIFICATE-----
Ctrl+Dを入力
conf#
```

10 Phase1ポリシーの設定をします。

```
conf# vpnikepolicy add id=1 method=rsasig encr=des hash=md5
```

11 Phase2ポリシーの設定をします。

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

〈次ページへ続く〉

設定例

12 VPNピアの設定をします。

```
conf# vpnpeer add addr=158.xxx.xxx.1 myname=FITELnet-F40
idtype-rsa=email ikepolicy=1
```

13 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
conf# vpnselector add id=32 dst=zzz.zzz.zzz.zzz src=all type=bypass
```

LDAPサーバを登録している場合は、LDAPサーバ宛のデータは暗号化されないように設定しておく必要があります。

14 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
```

発行責任：古河電気工業株式会社

130-B0334-AX01-A
2002.2