MUCHO-EV/PK X.509（RSA signaturese）機能に関する補足資料

このたびは、MUCHO-EV/PK をお買い上げいただき、まことにありがとうございます。
MUCHO-EV/PK では、X.509 機能をサポートしておりますが、取扱説明書には記載がありません。
本資料を参考に設定を行ってください。

電子証明機能に関する設定

RSA signatures 機能で使用する鍵と電子証明書の登録

RSA signatures による認証方式では、鍵と電子証明書を使用します。

IKE Policy で RSA signatures を選択した場合、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 RSA signatures 機能を使用するには、はじめに鍵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リセットを行ってください。

証明書を取得するための準備

鍵ペアの生成 ..... RSA signatures に必要な鍵ペアの生成
パラメータの設定 ..... CA センターからの証明書を使用する設定

※上記の設定が終了したら装置のリセットを行ってください

証明書の取得および登録

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リセットを行ってください

電子証明機能を使用するための設定

IKE 方式に関する設定..... IKE の認証方式の選択
ピアルータの登録 ..... IPsec トンネルを確立するための設定
暗号方式の設定 ..... 相手ルータとの暗号化方式の登録
VPN パケットの登録..... VPN の対象とするパケットの登録

※上記の設定が終了したら装置のリセットを行ってください

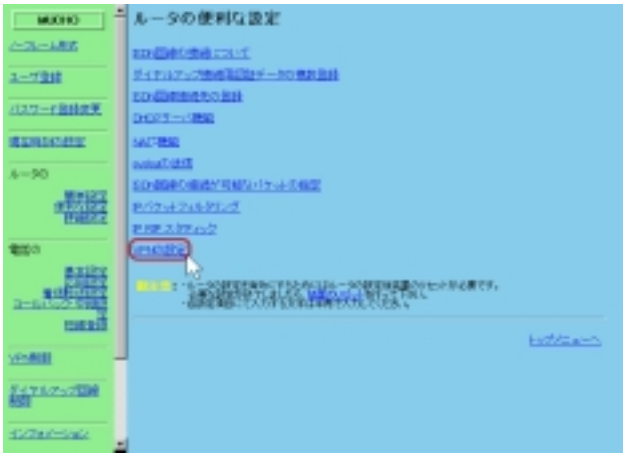
＜Web ブラウザ操作＞

1　鍵の生成と登録

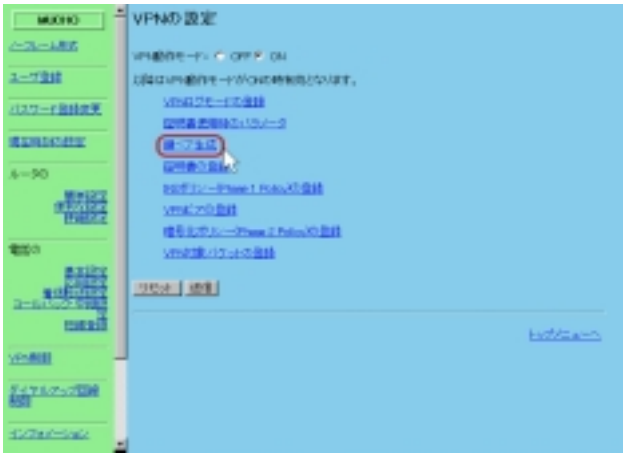
RSA signatures 機能で使用する鍵の生成、登録を行います。

2　「便利な設定」をクリックします。

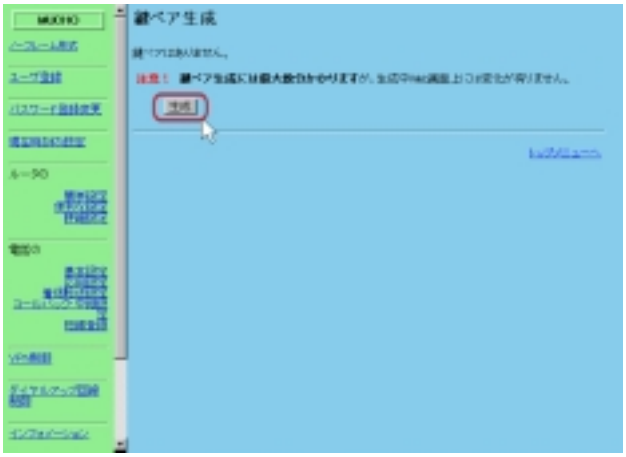
3　「VPN の設定」をクリックします。



4　VPN の設定画面で、VPN 動作モード"ON"を送信後、鍵ペアの生成を選択します。



5　鍵ペア生成画面で、"生成"ボタンをクリックして鍵ペアを生成します。



6　"生成"ボタンをクリック後、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。

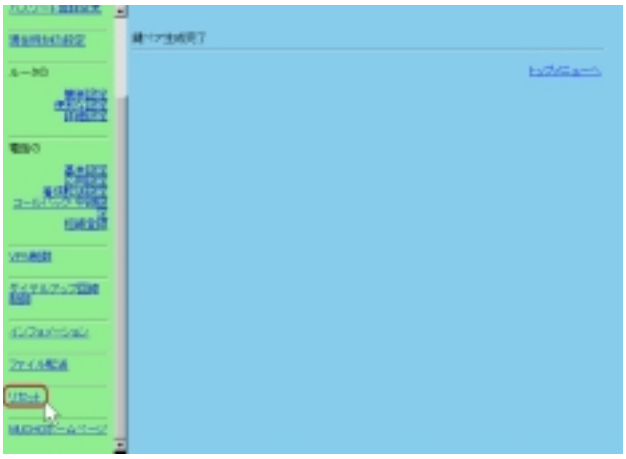
上記の操作で、鍵ペアの生成が完了します。

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。

7　鍵を有効にするために、装置のリセットを行います。

※鍵生成後は、必ずリセットをしてください。



＜コマンド操作＞

１　鍵の生成と登録

コンソールまたは TELNET で本装置にログインし、RSA signatures 機能で使用する鍵の生成、登録を行います。

```
conf#vpngenkey size=1024                                    ①
generating a keypair…                                       ②
ok
conf#
```

①： 鍵の生成を行う際に、鍵のサイズを指定します。
サイズは、512bit～2048bit です。

②： 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 15 秒
1024bit	約 2 分
2048bit	約 15～25 分

鍵の生成が終了したら装置をリセットしてください。

メモ：既に鍵ペアが存在する場合は、②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。

以上で、鍵の登録が完了しました。

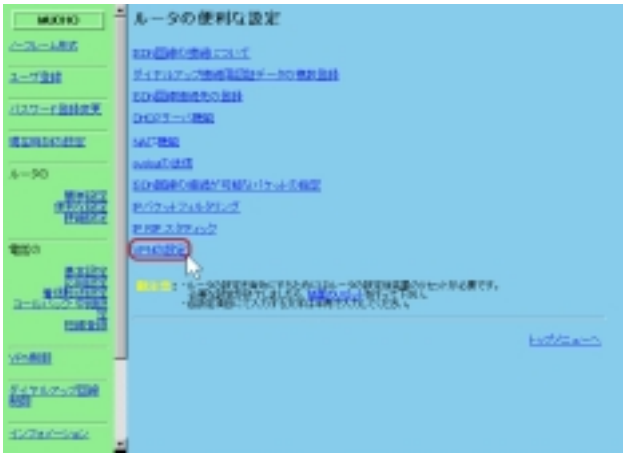
証明書使用時のパラメータの設定

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。

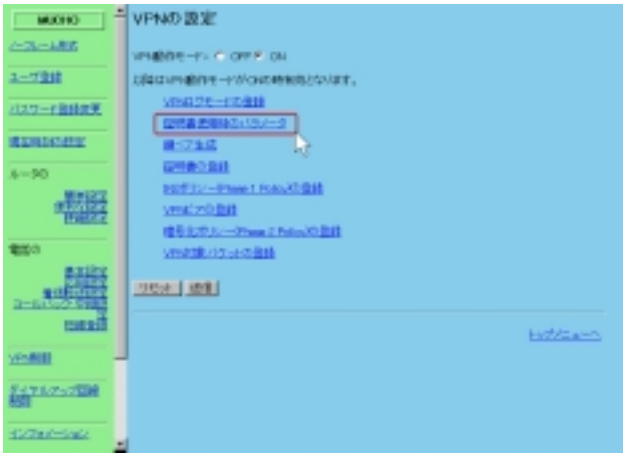
＜Web ブラウザ操作＞

1　「便利な設定」をクリックします。

2　ルータの便利な設定画面で「VPN の設定」をクリックします。



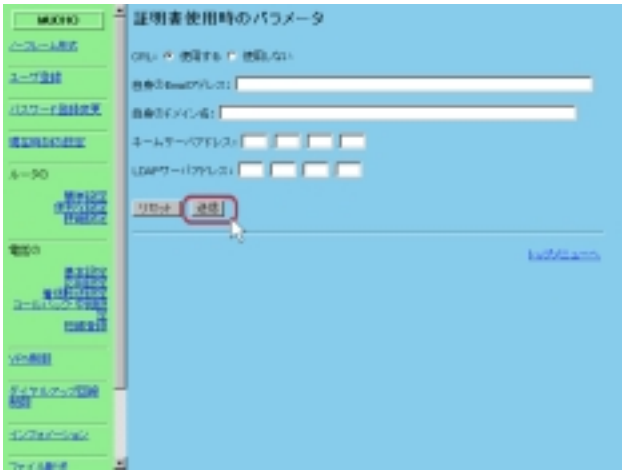
3　VPN の設定画面で、VPN 動作モード"ON"を送信後、証明書使用時のパラメータを選択します。



4　証明書使用時のパラメータ画面で、各種設定を行います。

各種設定入力後に"送信"をクリックして登録します。
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。

※登録が終了後、装置をリセットしてください。



【項目の説明】

CRL ・・・・・・・・・・・・・・・・・・・・・・ CRL を使用する/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 MUCHO-EV/PK がダイアルアップでインターネットに接続する場合に必要な設定です。

自身のドメイン名 ‥‥‥‥‥ 本装置が組み込まれている環境のドメイン名を設定します。

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。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　証明書使用時のパラメータの設定を行います。

```
conf# vpncertparam emailaddr=yyy@xxxx.co.jp        ①
domainname=www.xxx.co.jp                           ②
conf#
```

①：証明書使用時のパラメータとして **Email** アドレスを登録します。

②：証明書使用時のパラメータとしてドメイン名を登録します。
ドメイン名の登録が終了したら、装置をリセットしてください。

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。

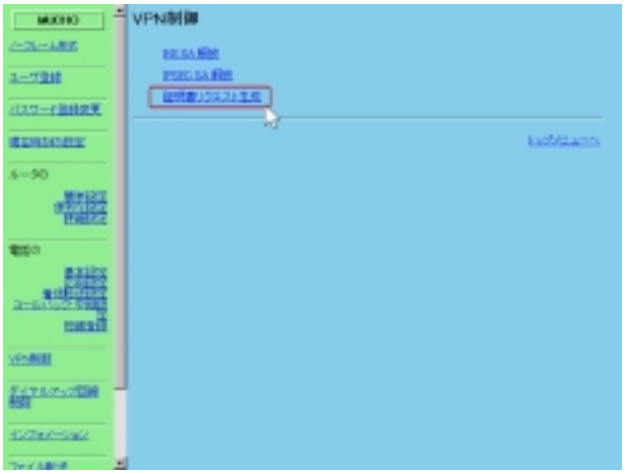
証明書リクエストの生成

Web ブラウザで、証明書リクエストの生成を行います。

＜Web ブラウザ操作＞

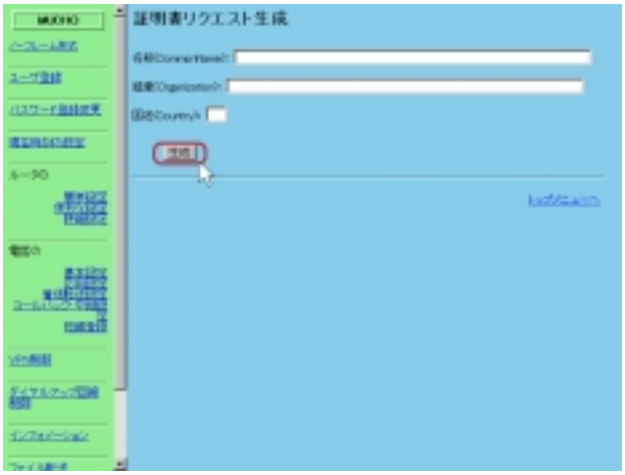
1　「VPN 制御」をクリックします。

2　VPN 制御画面で、証明書リクエスト生成を選択します。



３　証明書リクエスト生成画面で、各種設定を行います。

設定が終了したら、生成をクリックします。



【項目の説明】

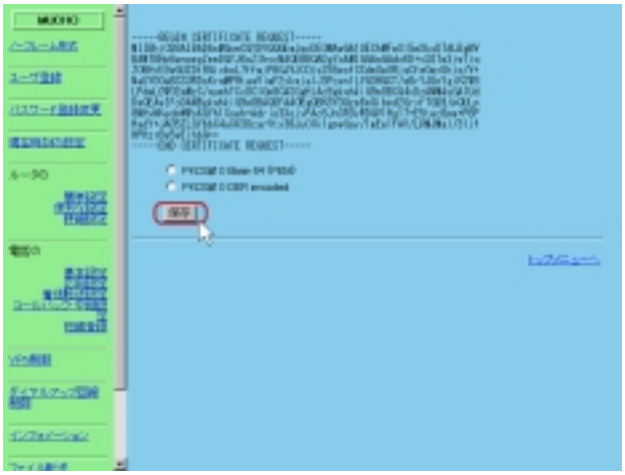
名前(CommonName)・・・・・・・・・・ 一般名を登録します。最大６４文字

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）

４　PEM 形式の証明書リクエストが表示

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。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　証明書リクエストの生成を行います。

```
conf#vpncertreq CN=XXX O=YYY C=jp                                    ①
-----BEGIN CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwLTELMAkGA1UEBhMCanAxDzANBgNVBAoTBmRlbmtvdTENMAsG
A1UEAxMEZnVydTCBnTANBgkqhkiG9w0BAQEFAAOBiwAwgYcCgYEAiUXsnMDkEK0B
V4I78L/XjCjhMF+U49AinRrvBt2jPxTmlwlXH2AnnKPoFjXOY9MBv1aeTrdKXlNL
H3Ysan4HmcKQAR/iSSGybKrq809GSBmqGiKzv2PyZX45PXwIqSuui+Q7jHQBZC0F
thfXeL69etZK3SIeaP3zQWlACTkMSHcCASGgQjBABgkqhkiG9w0BCQ4xMzAxMAsG
A1UdDwQEAwIFoDAiBgNVHREEGzAZghdqYWNrbWlnaS5mdXJ1a2F3YS5jby5qcDAN
BgkqgkiG9w0BAQUFAAOBgQBRsKfc7Bwh0nQL5YsxSfNCBm+ujvxpy1ASYvnEL54K
BeYMKvCop/PgIESGL3XJ+Au30VXVCJ6gM3zQkXKYj0AuvRyS+IQ3pa1L1aSbb4xm
HMjL5wOdmzuhHbok870i4y/T2/FdBAyV0sxNQxAGSejG7QzuqwSBfa62UMRQgCmq
tg==
-----END CERTIFICATE REQUEST-----
conf#
```

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。
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。

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。

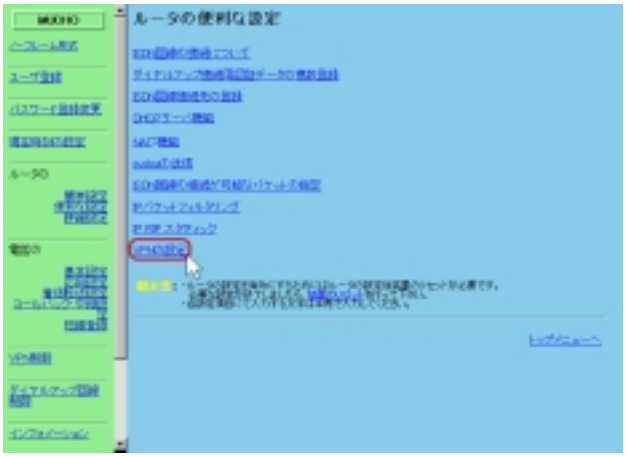
証明書の登録

Web ブラウザで、RSA signatures 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。

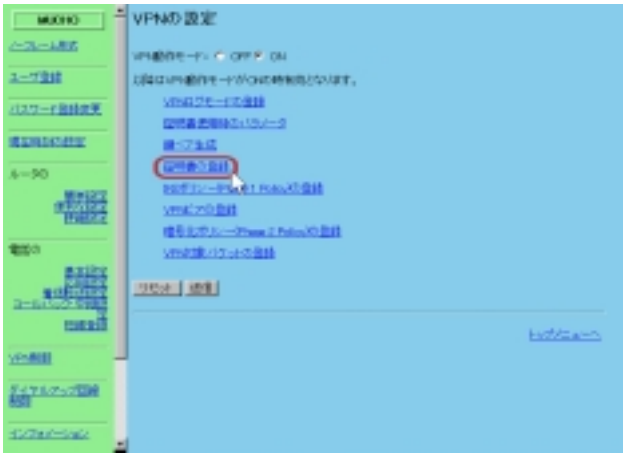
＜Web ブラウザ操作＞

1　「便利な設定」をクリックします。

2　「VPN の設定」をクリックします。



3　VPN 動作モード"ON"を送信後、証明書の登録を選択します。



4　証明書の登録を行います。

証明書の登録画面で、新しく証明書を登録する場合は、新規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、対象とする番号を入力して送信をクリックする事により削除ができます。

5　証明書の各種設定

証明書の登録画面で、各種設定を行います。
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。
設定が終了後、登録をクリックします。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。

【項目の説明】

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 の証明書をペースと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。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　証明書の登録を行います。

```
conf#vpncert add                                    ①
"Input certificate"
```

①： vpncert add と入力すると"Input certificate" と表示されるので、CA センターで取得した自信の証明書を登録します。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。

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"
```

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。

IKE 認証方式に関する設定

MUCHO-EV/PK は、IKE の認証方式に Pre-Shared key を使用する方式と、RSA signatures を使用する方法があります。Pre-Shared key を使用する場合は、MUCHO-EV 取扱説明書を参照してください。

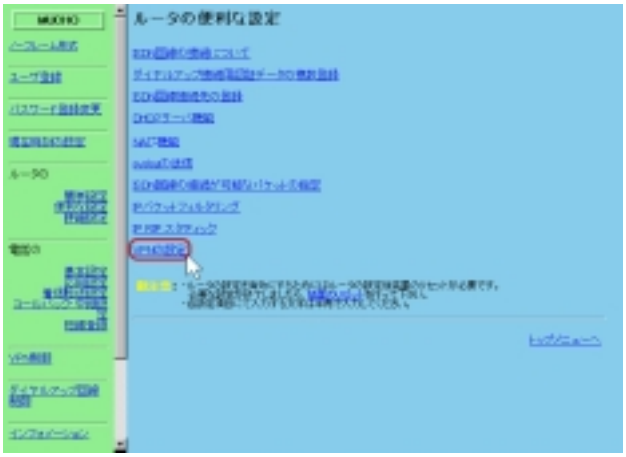
＜Web ブラウザ操作＞

1　IKE ポリシーの登録

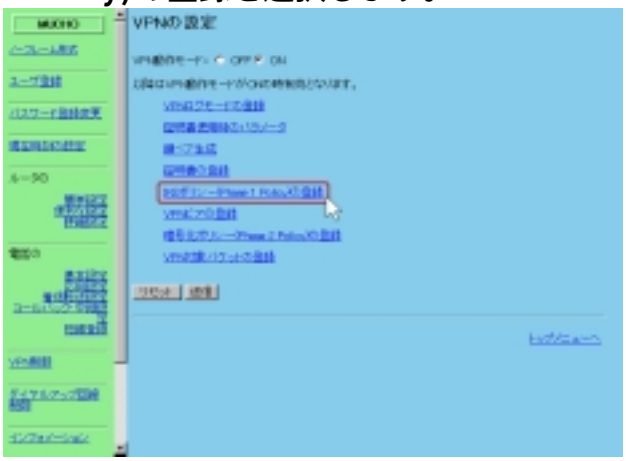
IKE ポリシーの登録時に、使用する認証方式を選択することができます。

2　「便利な設定」をクリックします。

3　「VPN の設定」をクリックします。



4　VPN 動作モード"ON"を送信後、IKE ポリシー(Phase 1 Policy)の登録を選択します。

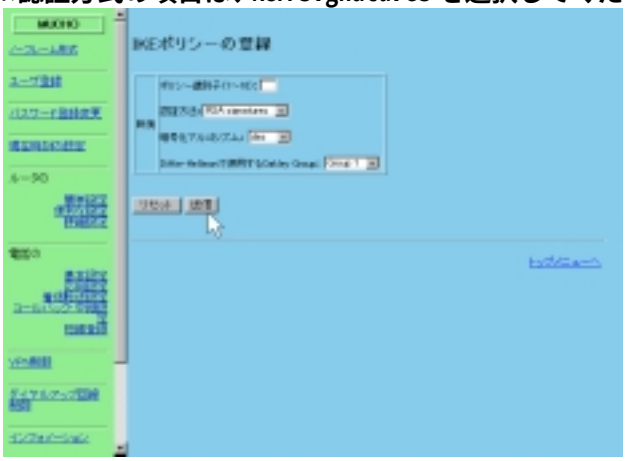


5　新規登録または、変更を行いたい番号を選択します。

6　新規登録画面

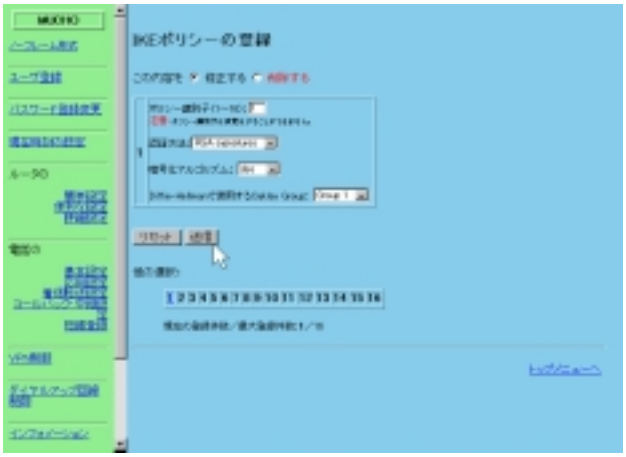
各種設定を入力した後に送信ボタンをクリックします。
既に登録してある内容を変更する場合は、次項を参照してください。

※認証方式の項目は、RSA signatures を選択してください。



7　登録変更画面

各種設定を入力した後に送信ボタンをクリックします。



【項目の説明】

この内容を‥‥‥‥‥‥‥‥‥‥‥‥‥‥ 登録内容を修正する、または削除するかを選択します。
この項目は、登録変更画面のみ表示されます。

ポリシー識別子（1～16）‥ ポリシーエントリの識別子を設定します。

認証方法…… IKE の認証方式を Pre-Shared key または、RSA signatures から選択します。X.509 を使用する場合は、RSA signatures を選択します。
Pre-Shared key を選択する場合は、MUCHO-EV 取扱説明書を参照してください。

暗号化アルゴリズム…… 暗号化アルゴリズムを des または、3des から選択します。

Diffie-Hellman で使用する Oakley Group
…… 鍵計算に使用する Diffie-Hellman Group を 1 または、2 から選択します。

他の選択…… 他の登録内容を変更する場合、変更したい登録の番号を選択します。この項目は、登録変更画面のみ表示されます。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　証明書の登録を行います。

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

①：X.509 を使用する場合は、method=prekey としてください。

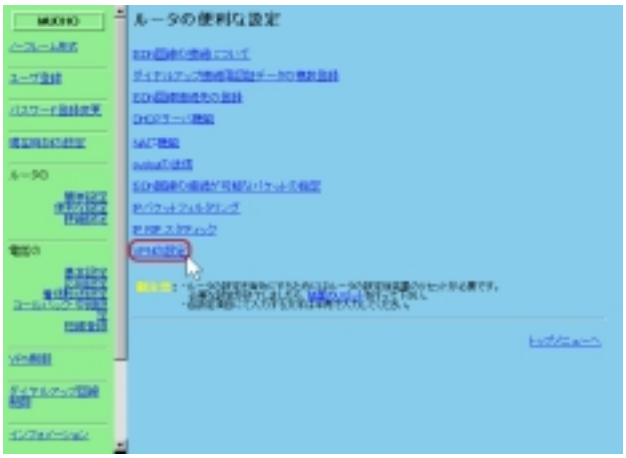
IPsec トンネルを確立する相手ルータ（ピアルータ）の登録

IPsec 機能を使用する場合は、論理的な IPsec トンネルを確立する必要があり、IPsec トンネルを確立する相手ルータを登録しておく必要があります。本書では、IPsec トンネルを確立する相手ルータをピアルータと記述する場合もあります。

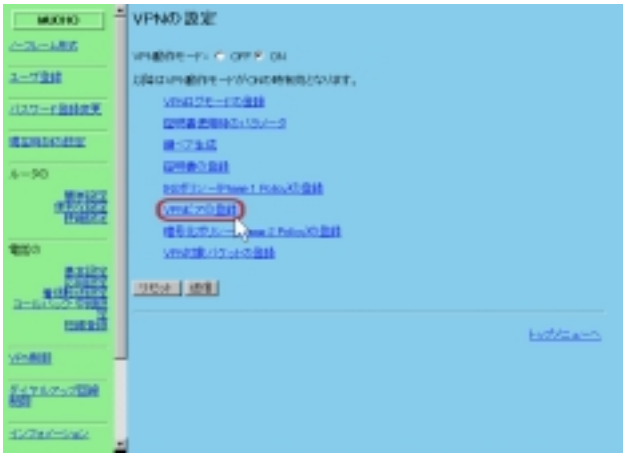
＜Web ブラウザ操作＞

1　「便利な設定」をクリックします。

2　「VPN の設定」をクリックします。



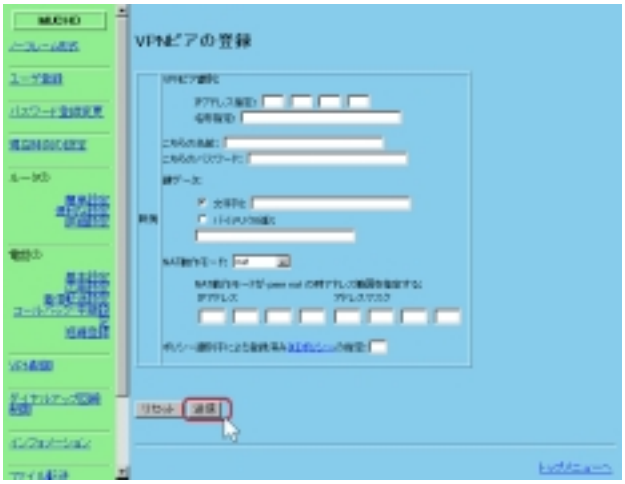
3　VPN 動作モード"ON"を送信後、VPN ピアの登録を選択します。



4　VPN ピアの登録画面で、新規登録または、変更を行いたい番号を選択します。

※登録データが無い場合、登録リスト選択できません。

5　各種設定を入力した後に送信ボタンをクリックします。



【項目の説明】

VPN 識別：

IP アドレス ･･･････････････ VPN ピアの IP アドレスを設定します。

名称指定･･･････････････････ VPN ピアの名前を設定します。
VPN ピアが Dial-up 接続して IP アドレスを取得する場合等で、IP アドレスが固定ではない場合、IP アドレスではなく相手装置の任意の名前で指定できます。RSA signatures の場合は、VPN ピアの ID を（証明書の Email アドレスやドメイン名）を指定します。

こちらの名前･･･････････････ 本装置側の名前を設定します。
将来拡張用のため、特に設定する必要はありません。

こちらのパスワード･･･････ 本装置側のパスワードを設定します。
将来拡張用のため、特に設定する必要はありません。

鍵データ：**※この設定項目は、X.509 の認証方式では必要ありません。**

文字列･･･････････････････ VPN ピアに依存する鍵データを ASCII データで設定します。

バイナリ（16 進） ･･･････ VPN ピアに依存する鍵データをバイナリ（16 進数）データで設定します。

※VPN ピアが MUCHO の場合は、RSA signatures 使用時の自身の ID は IP アドレスが固定の場合はドメイン名になるので、「名称指定」で VPN ピアのドメイン名を指定します。

NAT 動作モード…… VPN ピア毎の NAT 動作モードを指定します。
off…… NAT 変換しません。

nat…… NAT のモード、変換アドレス等、装置としての NAT の設定に従います。

nat+…… NAT+モードとして動作します。

peer nat…… 指定したアドレスを使用して NAT+モードとして動作します。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　IPsec トンネルを確立するピアルータの登録を行います。

設定はコンフィグレーションモードで行います。

```
conf#vpn on                                          ①
conf#vpnpeer add addr=1.1.1.1 key=secret             ②
```

①： VPN 機能を使用するために、使用するかどうかの設定を on にします。

②： VPN 機能を使用して確立したトンネルで接続する相手装置の IP アドレスを入力します。
次に VPN キー（pre-shared key）の入力をします。

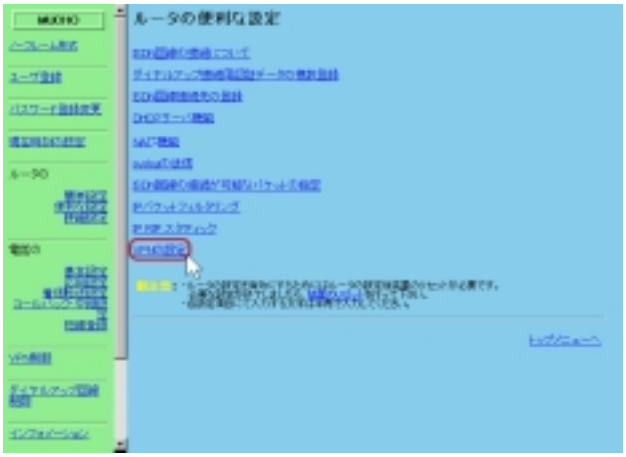
暗号化方式の登録

IPsec トンネルを確立する際に、相手ルータとの暗号化方式を登録しておく必要があります。

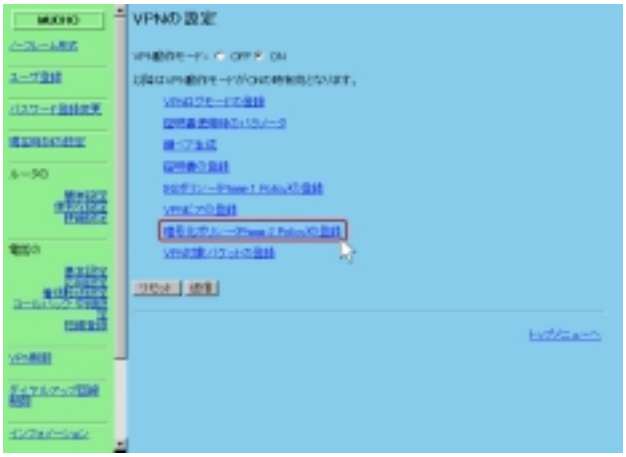
＜Web ブラウザ操作＞

1　「便利な設定」をクリックします。

2　「VPN の設定」をクリックします。



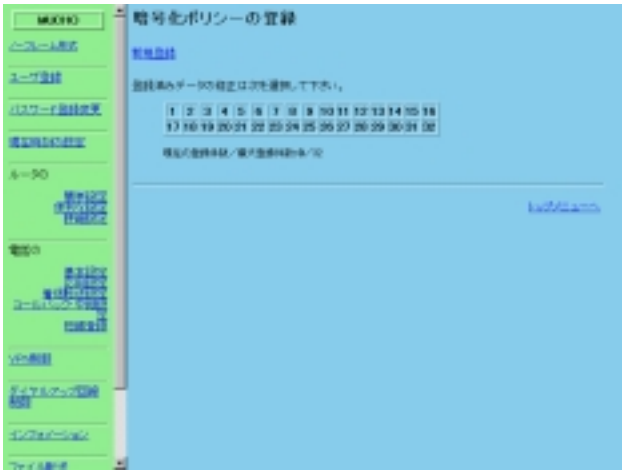
3　VPN 動作モード"ON"を送信後、暗号化ポリシーの登録を選択します。



4　登録方法を選択します。

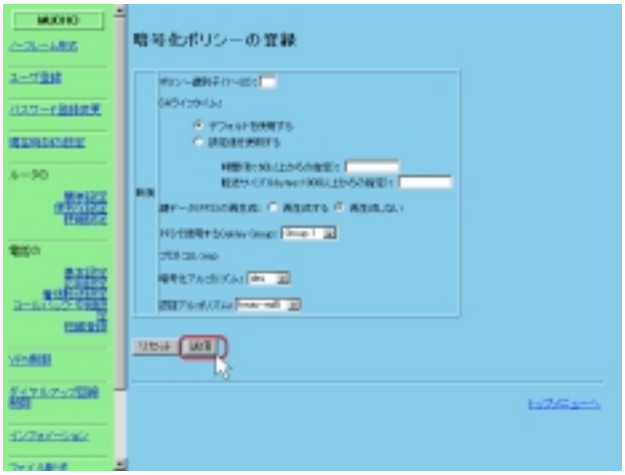
新規登録を選択します。

既に登録してある設定を変更する場合は、対象とする設定番号を選択してください。



5　登録画面で各種設定を行います。

各種設定を入力した後に送信ボタンをクリックします。



【項目の説明】

ポリシー識別子 ･･･････････ 暗号化ポリシーエントリの識別子。

SA ライフタイム：

　デフォルトを使用する････ 通常はこちらを選択してください。

　設定値を使用する･･･････ 変更する場合は、VPN ピアどうしで同じ値になるように設定してください。

鍵データ（PFS）の再生成：

　再生成する･･･････････････ SA 確立時に新たな鍵情報を指定します。

　再生成しない･･･････････ 鍵情報を再生成しない。

暗号化アルゴリズム ･･･････ null、des、3des のどれかを選択します。

認証アルゴリズム ･･･････････ null、hmac-md5、hmac-sha のどれかを選択します。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　IPsec トンネルを確立する際に、相手ルータとの暗号化方式を登録しておく必要があります。

設定はコンフィグレーションモードで行います。

```
conf#vpnpolicy add id=1                                    ①
```

①： ポリシー識別子を入力します。

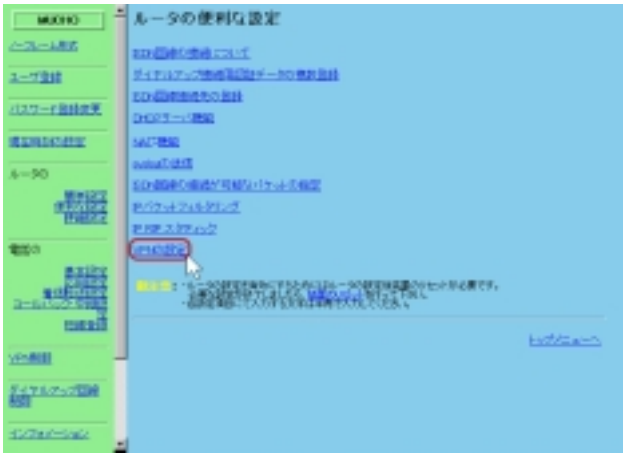
VPN 対象パケットの登録

VPN の対象とするパケットの登録方法を以下に示します。

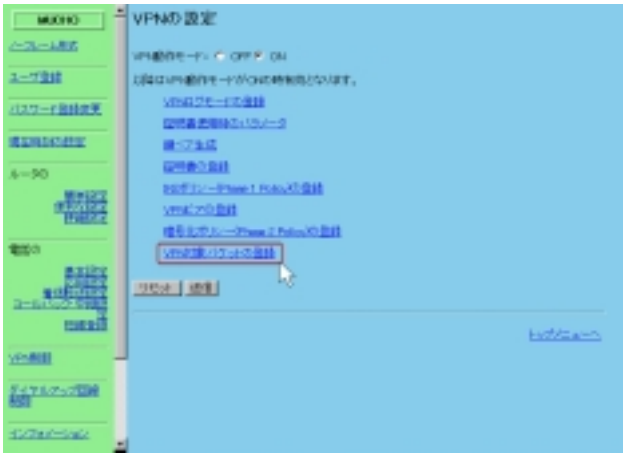
＜Web ブラウザ操作＞

1　「便利な設定」をクリックします。

2　「VPN の設定」をクリックします。



3　VPN 動作モード"ON"を送信後、VPN 対象パケットの登録を選択します。



4　対象パケットの登録を行います。

VPN 対象のパケットの登録画面で、新規登録を選択します。既に登録してある設定を変更する場合は、対象とする設定番号を選択してください。

※登録データが無い場合、登録リストは表示されません。

5　各種設定を入力した後に送信ボタンをクリックします。

【項目の説明】

パケット優先順位 ・・・・・・・・・・ VPN 対象データのエントリの識別子。

宛先指定：

全て・・・・・・・・・・・・・・・・・・・ 全てのパケットを対象とします。

宛先が VPN ピアの時・・・・・・ VPN ピアに登録してある IP アドレスを対象とします。

IP アドレス指定 ・・・・・・・・・ 対象とするパケットの IP アドレス、アドレスマスクを指定します。

宛先ポート指定 ・・・・・・・・・・・・ 全てのポートまたは、ポートを指定します。

送信元指定：

全て・・・・・・・・・・・・・・・・・・・ 全てのパケットを対象とします。

IP アドレス指定 ・・・・・・・・・ 対象とするパケットの IP アドレス、アドレスマスクを指定します。

送信元ポート指定 ····· 全てのポートまたは、ポートを指定します。

プロトコル指定 ····· icmp、tcp、udp または全てのいずれかを選択します。

任意指定時はプロトコル番号を設定
····· 該当するプロトコル番号を指定します。

IPsec 処理タイプ：
IPsec 処理して中継 ····· IPsec による VPN 通信を行います。

IPsec 処理しないで中継 ·· VPN 通信を行わず、通常の通信を行います。

廃棄····· 該当しないパケットは廃棄します。

以下の設定は「IPsec 処理タイプ」に「IPsec 処理して中継」を選択した時に有効となります。

SA 確立契機····· SA 確立契機を起動時に行うかどうかの指定後、データ通信時、ライフタイム満了時の指定を行います。

登録済み VPN ピア指定 ····· 登録済み VPN ピアから IP アドレス、または名称で指定します。

ポリシー識別子による登録済み暗号化ポリシーの指定
····· 登録してある暗号化ポリシーの中から指定します。

登録したパケット以外は全て廃棄されます。
登録したパケット以外を IPsec 処理せず、中継する場合は、パケット優先順位=32 のエントリに「全てのパケットを中継（Bypass）」というエントリを追加してください。

＜コマンド操作＞

1　コンソールまたは TELNET で本装置にログインします。

2　VPN の対象とするパケットの登録を行います。

設定はコンフィグレーションモードで行います。

```
conf#vpnselector add id=1 dst=192.52.128.0,255.255.255.0      ①
src=192.168.56.0,255.255.255.0 peeraddr=192.168.55.1 policy=1
```

①： パケット優先順位、対象とするパケットの送信元／先の IP アドレス、相手装置の IP アドレス、暗号化ポリシーの指定を行います。