CentreCOM AR450S AR260S 設定例

PPPoE インターネット接続環境における 2 点間 IPsec VPN (両側アドレス固定)

PPPoE でインターネットに接続している 2 つの拠点を IPsec で結ぶ VPN 構築例です。この例では、グローバルアドレス 1 個を固定的に割り当てられているサイトの間を IPsec (ESP) のトンネルで接続します。

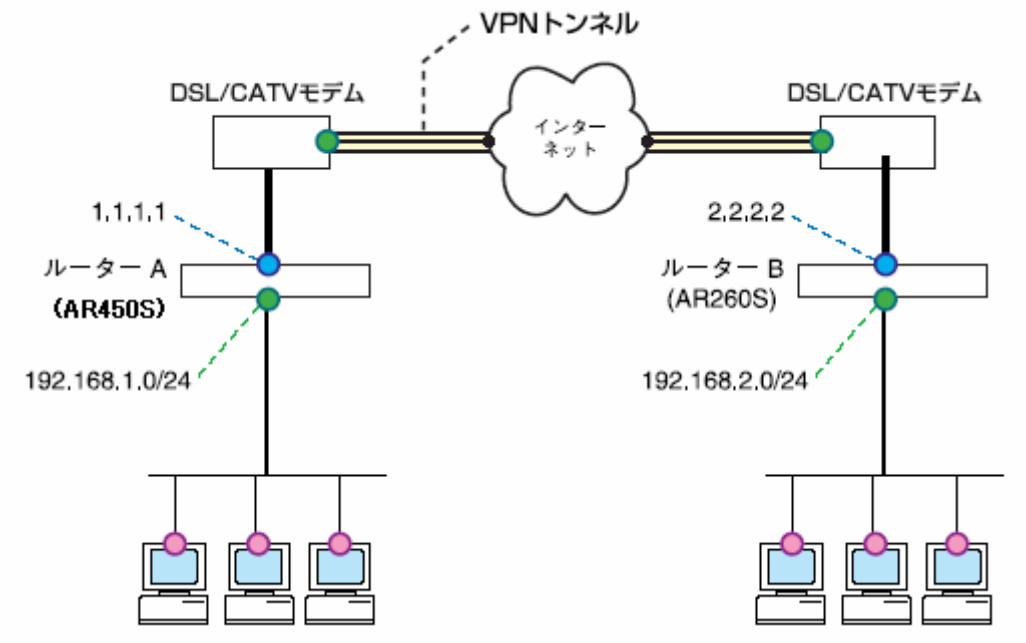
各拠点は、ISP から次の情報を提供されているものとします。

	ルーターA(AR450S)	ルーターB(AR260S)
PPP ユーザー名	userA@ispA	userB@ispB
PPP パスワード	isppasswdA	isppasswdB
PPPoE サービス名	指定なし	指定なし
使用できる IP アドレス	1.1.1.1/32	2.2.2.2/32
接続形態	端末型 (アドレス 1 個固定)	端末型 (アドレス 1 個固定)

ルーターA、ルーターB は、ダイナミック ENAT を使用した通常の端末型設定 (アドレス 1 個固定) です。

以下、ルーターA、B の基本設定についてまとめます。

	ルーターA(AR450S)	ルーターB(AR260S)
WAN 側物理インターフェース	eth0	pppoe0 (WAN)
WAN 側 IP アドレス (1)	1.1.1.1/32(ppp0)	2.2.2.2/32 (pppoe0)
LAN 側 IP アドレス	192.168.1.1/24 (vlan1)	192.168.2.1/24 (LAN 側)



この構成において IPsec VPN を構築するときのポイントは次のとおりです。

- IPsec 関連のパケット (IKE、ESP) がファイアウォールで遮断されないようにルールを設定します。(AR450S のみ)
- トンネリング対象のパケットに NAT が適用されないようファイアウォールルール (AR260S では Inbound/Outbound アクセス制御) を設定します。
- AR260S はハートビート機能に対応していないため、AR450S のハートビート機能は使用しません。

IPsec 関連の設定は次のようになります。

表 3:IKE フェーズ 1 (IKE 設定)

ルーター間の認証方式	事前共有鍵 (pre-shared key)
IKE 交換モード	Main モード
事前共有鍵	secret (文字列)
Oakley グループ	1 (デフォルト)
ISAKMP メッセージの暗号化方式	DES (デフォルト)
ISAKMP メッセージの認証方式	SHA1 (デフォルト)
ISAKMP SA の有効期限 (時間)	デフォルト値を使用
ISAKMP SA の有効期限 (Kbyte 数)	なし (デフォルト)
起動時の ISAKMP ネゴシエーション	行わない

表 4:IKE フェーズ 2 (IPsec SA 設定)

SA モード	Main モード
セキュリティープロトコル	ESP (暗号化＋認証)
暗号化方式	DES
認証方式	SHA1
IPComp	使用しない
IPsec SA の有効期限 (時間)	デフォルト値を使用
IPsec SA の有効期限 (Kbyte 数)	なし (デフォルト)
トンネリング対象 IP アドレス	192.168.1.0/24 ←→ 192.168.2.0/24
トンネル終端アドレス	1.1.1.1 (A) ・2.2.2.2 (B)
インターネットとの平文通信	行う
PFS グループ	使用しない

ルーターA (AR450S) の設定

Note -本設定例は、AR450S F/W Ver.2.6.4 PL0 を元にしています。F/W Ver.2.7.3-05 以降をお使いの場合、PPPoE セッションキープアライブ機能が追加されておりますので、(※) がついた項の設定は不要です。トリガーの設定を行われる場合は、以下の設定コマンドはルーターの WAN 側インターフェース (eth0) にケーブルを接続していない状態 (PPP インターフェースがリンクアップしない状態) で入力してください。詳細については章末の「メモ」をご覧ください。

1. セキュリティーモードで各種設定を行なうことのできる Security Officer レベルのユーザー「secoff」を作成します。パスワードは「PasswordS」とします。

   ADD USER=secoff PASSWORD=PasswordS PRIVILEGE=SECURITYOFFICER ↓

   Note - Security Officer レベルのユーザーを作成しておかないと、セキュリティーモードに移行できませんのでご注意ください。

2. WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、ISP から通知された PPPoE の「サービス名」を記述します。ISP から指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

   CREATE PPP=0 OVER=eth0-any ↓

3. ISP から通知された PPP ユーザー名とパスワードを指定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

   SET PPP=0 OVER=eth0-any USER=userA@ispA PASSWORD=isppasswdA LQR=OFF BAP=OFF ECHO=ON ↓

4. IP モジュールを有効にします。

   ENABLE IP ↓

5. LAN 側 (vlan1) インターフェースに IP アドレスを設定します。

   ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0 ↓

6. WAN 側 (ppp0) インターフェースに ISP から割り当てられた IP アドレスを設定します。

   ADD IP INT=ppp0 IP=1.1.1.1 MASK=255.255.255.255 ↓

7. デフォルトルートを設定します。

   ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0 ↓

8. (※) PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。

   - ppp0 をリセットするスクリプト reset.scp を作成します。

     ADD SCRIPT=reset.scp TEXT="RESET PPP=0" ↓

   - トリガー「1」を無効状態にするスクリプト up.scp を作成します。

     ADD SCRIPT=up.scp TEXT="DISABLE TRIGGER=1" ↓

   - トリガー「1」を有効状態にするスクリプト down.scp を作成します。

     ADD SCRIPT=down.scp TEXT="ENABLE TRIGGER=1" ↓

   Note - ADD SCRIPT コマンドは、コンソールなどからログインした状態で、コマンドラインから実行するコマンドです。そのため、EDIT コマンド（内蔵フルスクリーンエディター）等を使って設定スクリプトファイル（.CFG）にこのコマンドを記述しても意図した結果にならない場合がありますのでご注意ください。

9. (※) トリガー機能を有効にします。

   ENABLE TRIGGER ↓

10. (※) PPPoE セッションを自動再接続するためのトリガーを作成します。

    - 3 分ごとに reset.scp を実行する定期トリガー「1」を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり（トリガー「3」による）、アップすると無効になります（トリガー「2」による）。

      CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp ↓

    - ppp0 のアップ時に up.scp を実行するインターフェーストリガー「2」を作成します。

      CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp ↓

    - ppp0 のダウン時に down.scp を実行するインターフェーストリガー「3」を作成します。

      CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓

11. ファイアウォール機能を有効にします。

    ENABLE FIREWALL ↓

12. ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。

```
CREATE FIREWALL POLICY=net ↓
```

13. ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。

```
ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH ↓
```

Note - デフォルト設定では、ICMP はファイアウォールを通過できません。

14. ルーターの ident プロキシー機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
DISABLE FIREWALL POLICY=net IDENTPROXY ↓
```

15. ファイアウォールポリシーの適用対象となるインターフェースを指定します。

- LAN 側インターフェース (vlan1) を PRIVATE (内部) に設定します。

```
ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE ↓
```

- WAN 側インターフェース (ppp0) を PUBLIC (外部) に設定します。

```
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC ↓
```

16. LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスには、ppp0 の IP アドレスを使用します。

```
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↓
```

17. 相手ルーターから受信した IKE パケット (UDP500 番) がファイアウォールを通過できるように設定します。

```
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500 GBLIP=1.1.1.1
PO=500 IP=1.1.1.1 ↓
```

18. ローカル LAN からリモート LAN へのパケットには NAT をかけないように設定します。

```
ADD FIREWALL POLICY=net RULE=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1-192.168.1.254 ↓
SET FIREWALL POLICY=net RULE=2 REMOTEIP=192.168.2.1-192.168.2.254 ↓
```

19. 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルー

ルを適用することを示します。以下のコマンドは、「取り出したパケットの終点が 192.168.1.1～192.168.1.254、つまり、ローカル側 LAN ならば NAT の対象外とする」の意味になります。

```
ADD FIREWALL POLICY=net RULE=3 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-192.168.1.254
ENCAP=IPSEC ↓
```

20. ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。ここでは鍵番号を「1」番とし、鍵の値は「secret」という文字列で指定します (ルーターB と同じに設定)。

```
CREATE ENCO KEY=1 TYPE=GENERAL VALUE="secret" ↓
```

Note - CREATE ENCO KEY コマンドは、コンソール上でログインしている場合のみ有効なコマンドです。そのため、EDIT コマンド (内蔵スクリーンエディター) 等で設定スクリプトファイル (.CFG) にこのコマンドを記述しても無効になりますのでご注意ください。

21. ルーターA との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「i」を作成します。KEY には、前の手順で作成した事前共有鍵 (鍵番号「1」) を、PEER には対向ルーターの IP アドレスを指定します。

```
CREATE ISAKMP POLICY="i" PEER=2.2.2.2 KEY=1 SENDN=TRUE ↓
```

22. IPsec 通信の仕様を定義する SA スペック「1」を作成します。トンネルモード (デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTO=ESP ENCALG=DES HASHALG=SHA ↓
```

23. SA スペック「1」だけからなる SA バンドルスペック「1」を作成します。鍵管理方式は「ISAKMP」を指定します。

```
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1" ↓
```

24. ISAKMP メッセージを素通しさせる IPsec ポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの 500 番ポート宛の UDP パケット (ISAKMP) に設定します。

```
CREATE  IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↓
```

Note - ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMP メッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は SHOW IPSEC POLICY コマンドで確認できます。また、検索順を変更するには、SET IPSEC POLICY コマンドの POSITION パラメーターを使用します。

25. 実際の IPsec 通信に使用する IPsec ポリシー「vpn」を、PPP インターフェース「0」に対して作成します。鍵管理方式には「ISAKMP」を、PEER にはルーターA の IP アドレスを、BUNDLE には SA バンドルスペック「1」を指定します。

```
CREATE IPSEC POLICY="vpn" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=2.2.2.2 ↓
```

26. IPsec ポリシー「vpn」に対して実際に IPsec 通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
SET IPSEC POLICY="vpn" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0 ↓
```

27. インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPP インターフェース「0」に対して作成します。

```
CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT ↓
```

Note - インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーですべてのパケットを通過させる設定を行ってください。いずれの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないと VPN 以外の通信ができなくなります。

28. IPsec モジュールを有効にします。

```
ENABLE IPSEC ↓
```

29. ISAKMP モジュールを有効にします。

```
ENABLE ISAKMP ↓
```

30. Security Officer レベルのユーザーでログインしなおします。

```
LOGIN secoff ↓
```

31. 動作モードをセキュリティーモードに切り替えます。

```
ENABLE SYSTEM SECURITY_MODE ↓
```

Note - セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO (Remote Security Officer) の設定を行っておいてください (本章末尾のメモを参照)。

32. 設定は以上です。設定内容をファイルに保存し、SET CONFIG コマンドで起動時設定ファイルに指定します。

```
CREATE CONFIG=router.cfg ↓
SET CONFIG=router.cfg ↓
```

Note - WAN 側のケーブルを抜いた状態でここまでの設定を行った場合は、ファイル保存後にケーブルを接続してください。

ルーターB (AR260S) の設定

1.メニューから「LAN」→「LAN」の順にクリックし、LAN 側 IP アドレスの設定を行います。

LAN側IP設定	
IPアドレス	192.168.2.1
サブネットマスク	255.255.255.0
適用	ヘルプ

現在の設定	
IPアドレス	192.168.2.1
サブネットマスク	255.255.255.0

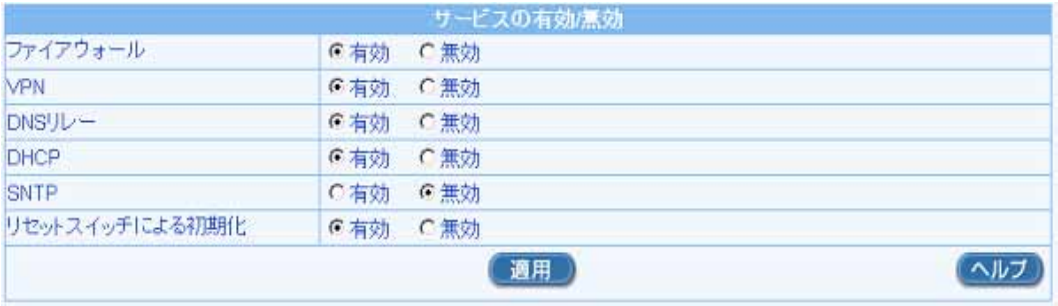
以下のメッセージが表示されますので、「OK」ボタンをクリックし、端末の IP アドレスを取得しなおしてから、AR260S の変更後のアドレスに接続します。

2.メニューから「WAN」→「WAN」の順にクリックします。

セッション ID：PPPoE0 を選択し、インターネット接続の設定を行います。

WAN設定	
接続モード	PPPoE
セッションID	PPPoE:0 切断
デフォルトゲートウェイ	PPPoE:0
Unnumbered PPPoE	○ 有効 ◉ 無効
ホスト名	AR260S (オプション)
ユーザー名	userB@ispB
パスワード	••••••••••
サービス名	(オプション)
AC(アクセスコンセントレーター)名	(オプション)
DNSオプション	○ 固定設定 ◉ 自動取得
プライマリDNSサーバー	(オプション)
セカンダリDNSサーバー	(オプション)
MSSクランプ	○ 無効 ◉ 有効 MSSの値: 40 Bytes
接続オプション	○ ダイアルオンデマンド ◉ キープアライブ ○ 無効 エコー送信間隔 60 秒
適用	ヘルプ

3.メニューから「システム管理」→「サービスの有効／無効」の順にクリックし、VPN を有効にします。VPN 機能を使用する場合、「サービスの有効／無効」にて VPN を有効にしてから、VPN 接続設定を行う必要があります。



4.メニューから「VPN」→「VPN 接続」の順にクリックし、VPN 接続設定を行います。VPN 接続設定にてポリシーを作成する前に、「サービスの有効／無効」にて VPN サービスを有効にしておいてください。各パラメーターについて以下に説明いたします。

・VPN 無通信監視

VPN 通信が「無通信時間」指定した時間発生しなかった場合に、IPsec SA を削除する機能です。

・キープ SA

PPPoEセッションが切断されたときに、確立中のIPsec SA 保持する機能です。有効時は、PPPoE セッションが切断されても有効期限がくるまでSA を保持します。

・ローカルセキュアグループ：

ポリシーの適用対象となるパケットのローカル側 IP アドレスを指定します。

・リモートセキュアグループ：

ポリシーの適用対象となるパケットのリモート側 IP アドレスを指定します。

・ローカルゲートウェイ：

VPN 通信パケットを送受信するローカルのインターフェースを指定します。

・リモートゲートウェイ：

VPN 接続先ルーター（対向ルーターの WAN 側）の IP を指定します。

・IKE交換モード：

両側IPアドレス固定の場合、通常「Main」を選択します。Mainモードは、両側IPが固定の場合に使用することが可能です。

・IKE暗号化/認証アルゴリズム：

対向のARルーターとIKE 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。

・IPsec 暗号化/認証アルゴリズム：

対向のARルーターとIPsec 暗号化/認証アルゴリズムを合わせて設定する必要があります。「全て」を選択することも可能です。

・PFS グループ：

PFS 機能を使用するかどうかを指定します。未定義は使用しません。

4-1.IKE 暗号化/認証アルゴリズム、IPsec 暗号化/認証アルゴリズムを固定にする場合は、以下の組み合わせを選択します。

5.メニューから「ファイアウォール」→「Inbound アクセス」の順にクリックします。

ファイアウォールを有効にしている場合は、ファイアウォールで ISAKMP/IPsec のパケットが遮断されないように、Inbound/Outbound アクセス制御設定にて、アクセスを透過する設定が必要になります。

6.メニューから「ファイアウォール」→「Outbound アクセス」の順にクリックします。
ファイアウォールを有効にしている場合は、ファイアウォールで ISAKMP/IPsec のパケットが遮断されないように、Inbound/Outbound アクセス制御設定にて、アクセスを透過する設定が必要になります。

※Outboundアクセスルールにはデフォルトでポリシーが設定されています。(ID:2 の設定がデフォルトポリシーになります。) このポリシーが設定されていることで、LAN側からインターネットへ向けたパケットのIPアドレスは全てpppoe0インターフェースのIP アドレスに変換され、インターネット通信が可能になります。VPNパケットを透過するアクセスルールはデフォルトポリシーより優先度を高く設定する必要があります。

以上

メモ (AR450S)

■本構成例にて、トリガーの設定をされている場合には、以下の点に注意してください。PPP リンクのアップ･ダウンによってトリガー「1」の状態 (有効･無効) が動的に変化します。そのため、WAN 側インターフェースにケーブルを接続したまま設定を行うと、コマンド入力時と設定保存時でトリガー「1」の状態が変わってしまうことがあります。その場合、PPP の自動再接続機能が働かなくなりますので、必ず次のいずれかの方法で設定を行ってください。

- WAN 側インターフェースのケーブルを抜いた状態でコマンドを入力し、設定保存後にケーブルを接続する。
- PC 上で設定ファイルを作成し、ZMODEM か TFTP でルーターに転送する。
- ルーターの EDIT コマンドで設定ファイルを作成する。

設定が正しく保存されているかどうかを確認するには、SHOW FILE コマンドか SHOW SCRIPT コマンドで設定ファイルを表示し、トリガー「1」の設定内容を確認してください。正しく保存されている場合、トリガー「1」の設定は次のようになります。

```
create trigger=1 periodic=3 script=reset.scp
```

手順が正しくなかった場合は、次のように「state=disabled」というパラメーターが付きます。この設定では、ルーター起動直後に再接続機能が働きません。

```
create trigger=1 periodic=3 state=disabled script=reset.scp
```

この場合は、EDIT コマンドで設定ファイルを開き、「state=disabled」を削除して上書き保存してください。

■ セキュリティーモードに移行すると、Security Officer レベルでルーターに Telnet ログインすることができなくなります。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO (Remote Security Officer) コマンドを使ってログインを許可するホストの IP アドレスを指定しておく必要があります。たとえば、ネットワーク 192.168.1.0/24、192.168.2.0/24 上のすべてのホストから Security Officer レベルでの Telnet ログインを許可する場合は、次のようにします。

```
ENABLE USER RSO ↓
ADD USER RSO IP=192.168.1.0 MASK=255.255.255.0 ↓
ADD USER RSO IP=192.168.2.0 MASK=255.255.255.0 ↓
```

■ セキュリティーモードでは、たとえ Security Officer でログインした場合であっても、セキュリティーコマンドを一定期間入力しないでいると、次回セキュリティーコマンドを入力したときにパスワードの再入力を求められます。このタイムアウト値は、下記コマンドによって変更できますが、IPsec の設定を行うときは、ノーマルモードで設定を行った後、セキュリティーモードに変更することをおすすめします。

■ セキュリティー関連コマンドのタイムアウトは、次のコマンドで変更できます。SECUREDELAY パラメーターには、10～600 (秒) を指定します。デフォルトは 60 秒です。

```
SET USER SECUREDELAY=300 ↓
```

まとめ

ルーターA のコンフィグ

※「#」で始まる行は、コンソールから入力しないと意味を持たないコマンドか、設定ファイル（.cfg）に記述しても無効なコマンドを示しています。詳細は本文の説明をご覧ください。 F/W Ver.2.7.3-05 以降の場合は（※）の項の設定は必要ありません。F/W Ver.2.6.4 PL0 以前の場合は必要です。

```
ADD USER=secoff PASSWORD=PasswordS PRIVILEGE=SECURITYOFFICER ↓
CREATE PPP=0 OVER=eth0-any ↓
SET PPP=0 OVER=eth0-any USER=userA@ispA PASSWORD=isppasswdA LQR=OFF BAP=OFF ECHO=ON ↓
ENABLE IP ↓
ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0 ↓
ADD IP INT=ppp0 IP=1.1.1.1 MASK=255.255.255.255 ↓
ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0 ↓
※ ENABLE TRIGGER ↓
※ CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp ↓
※ CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp ↓
※ CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓
ENABLE FIREWALL ↓
CREATE FIREWALL POLICY=net ↓
ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH ↓
DISABLE FIREWALL POLICY=net IDENTPROXY ↓
ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE ↓
ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC ↓
ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↓
ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500 GBLIP=1.1.1.1 PO=500 IP=1.1.1.1 ↓
ADD FIREWALL POLICY=net RULE=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1-192.168.1.254 ↓
SET FIREWALL POLICY=net RULE=2 REMOTEIP=192.168.2.1-192.168.2.254 ↓
ADD FIREWALL POLICY=net RULE=3 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC ↓
# CREATE ENCO KEY=1 TYPE=GENERAL VALUE="secret" ↓
CREATE ISAKMP POLICY="i" PEER=2.2.2.2 KEY=1 SENDN=TRUE ↓
CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↓
CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1" ↓
CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP ↓
CREATE IPSEC POLICY="vpn" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=2.2.2.2 ↓
SET IPSEC POLICY="vpn" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0 ↓
CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT ↓
ENABLE IPSEC ↓
```

ENABLE ISAKMP ↓

LOGIN secoff ↓

ENABLE SYSTEM SECURITY_MODE ↓

※スクリプト「reset.scp」

※ RESET PPP=0 ↓

※スクリプト「up.scp」

※ DISABLE TRIGGER=1 ↓

※スクリプト「down.scp」

※ ENABLE TRIGGER=1 ↓

更新日 2005 年 10 月 26 日