

## PPPoE 接続環境における 3 点間 IPsecVPN (支社間通信は本社経由。1 支店のみアドレス不定)

PPPoE でインターネットに接続している3つの拠点を IPsec(ESP)トンネルで結ぶVPN構築例です。本社(ルーターA:AR550S)と各支社(ルーターB、C:AR260S V2)のみを接続する構成とし、支社間の通信は本社経由で行うものとします。また、1支社のみグローバルアドレス1個を動的に割り当てられ、その他の拠点はグローバルアドレス1個が固定で割り当てられていると仮定しています。

インターネットサービスプロバイダ(ISP)からは、次の情報が提供されているものとします。

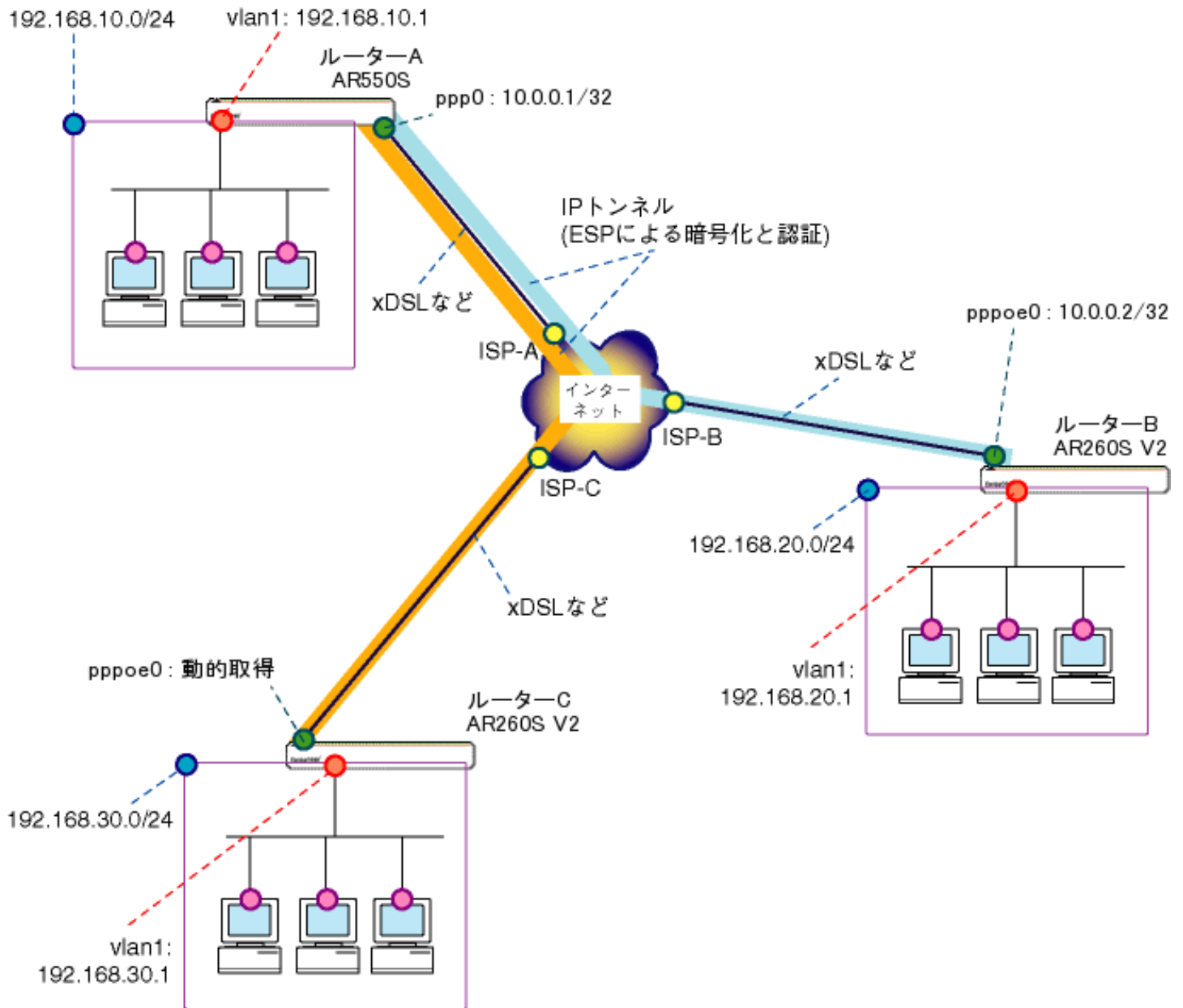
	ルーターA	ルーターB	ルーターC
ユーザーID (PPP ユーザー名)	user1@example	user2@example	user3@example
パスワード (PPP パスワード)	password	password	password
サービス名	指定なし	指定なし	指定なし
グローバル IP アドレス	10.0.0.1/32	10.0.0.2/32	不定(動的取得)

ルーターB、Cは、それぞれ以下のように設定するものとします。

	ルーターB	ルーターC
WAN 側 IP アドレス	自動取得 (10.0.0.2/32 を取得)	自動取得 (取得アドレスは不定)
LAN 側 IP アドレス	192.168.20.1/24	192.168.30.1/24
VPN 接続設定		
ローカルセキュアグループ ～リモートセキュアグループ	①192.168.20.0/24 ～ 192.168.10.0/24 ②192.168.20.0/24 ～ 192.168.30.0/24	①192.168.30.0/24 ～ 192.168.10.0/24 ②192.168.30.0/24 ～ 192.168.20.0/24
ローカルゲートウェイ	pppoe0	pppoe0
リモートゲートウェイ	10.0.0.1	10.0.0.1
IKE 設定		
交換モード	メイン	アグレッシブ
事前共有鍵	secret_ab	secret_ac
暗号化認証アルゴリズム	3DES & SHA1-DH2	3DES & SHA1-DH2
ローカル ID/リモート ID	なし/なし	vpn_ac/なし
IPsec 設定		
暗号化認証アルゴリズム	ESP 3DES HMAC SHA1	ESP 3DES HMAC SHA1
PFS グループ	なし	なし

# AR Series Configuration Example

## AR260S V2 設定例



本構成における設定のポイントは、次の通りです。

- ルーターA、B はアドレス固定のため、ルーターA、Bどちらからでも接続を開始できます。
- ルーターC はアドレス不定のため、ルーターA、Bからは接続を開始できません。常にルーターC から接続を開始することになります。

※ ルーターC の設定内容につきましては、文中の「ルーターC は～」をご参照ください。

## ルーターA(AR550S)の設定

※ 文中の「↓」は改行を表しています。

1. セキュリティモードで各種設定を行う事ができる Security Officer レベルのユーザー「secoff」を作成します。パスワードも「secoff」とします。

```
add user=secoff password=secoff priv=sec ↓
```

2. ISP へ接続するため、eth0 インターフェース上に ppp0 を作成します。

```
cre ppp=0 over=eth0-any ↓
```

3. ISP から通知されたユーザー名、パスワードを設定します。ISDN 回線向けの機能である BAP は無効化し、LCP ECHO による PPP セッション監視を有効化します。

```
set ppp=0 over=eth0-any user=user1@example password=password lqr=off bap=off echo=on ↓
```

4. IPルーティングを行うため、IP モジュールを有効化します。

```
ena ip ↓
```

5. IP インターフェース vlan1 に IP アドレス 192.168.10.1/24 を設定します。

```
add ip int=vlan1 ip=192.168.10.1 mask=255.255.255.0 ↓
```

6. ISP へ接続する ppp0 に、IP アドレス 10.0.0.1/32 を設定します。

```
add ip int=ppp0 ip=10.0.0.1 mask=255.255.255.255 ↓
```

7. デフォルトルートをも ppp0 に設定します。

```
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0 ↓
```

8. ppp0 が ISP に接続した際、通知された DNS サーバアドレスを使用するように設定します。

```
add ip dns int=ppp0 ↓
```

#### Note

ISP から DNS サーバアドレスが指定されている場合は、次のように設定します。

```
add ip dns primary=プライマリ DNS サーバ secondary=セカンダリ DNS サーバ ↓
```

9. DNS リレーを有効化します。

```
ena ip dnsrelay ↓
```

10. ファイアウォールを有効化します。

```
ena fire ↓
```

11. ファイアウォールの動作を規定するポリシー net を作成します。

ICMP は Unreachable、Echo/Echo replay(ping)のみ透過するよう設定し、ident プロキシ機能は無効化します。(メールサーバ等からの ident 要求に対して TCP RST を返します)

```
cre fire poli=net ↓  
ena fire poli=net icmp_f=unreach,ping ↓  
dis fire poli=net identproxy ↓
```

12. ファイアウォールポリシー net に、IP インターフェースを追加します。

ppp0 を public、vlan1 を private として設定し、ppp0 側から開始される通信は遮断しつつ、vlan1 側から開始される通信は透過します。

```
add fire poli=net int=vlan1 type=private ↓  
add fire poli=net int=ppp0 type=public ↓
```

13. インターネットアクセスを実現するため、vlan1～ppp0 間にダイナミック ENAT を設定します。

```
add fire poli=net nat=enhanced int=vlan1 gblint=ppp0 ↓
```

14. ルーターB、CからのIsakmp(UDP500番宛)を受信できるよう、透過ルールを設定します。

```
add fire poli=net ru=1 ac=allow int=ppp0 prot=udp po=500 gblpo=500 ip=10.0.0.1 gblip=10.0.0.1 ↓
```

15. ルーターB、Cからの通信を受信できるよう、透過ルールを設定します。192.168.10.0/24宛に加え、ルーターB、C間の通信を実現するため 192.168.20.0/24、30.0/24宛も受信できるように設定します。

```
add fire poli=net ru=2 ac=nonat int=ppp0 prot=all ip=192.168.10.1-192.168.10.254 encap=ipsec ↓  
add fire poli=net ru=3 ac=nonat int=ppp0 prot=all ip=192.168.20.1-192.168.20.254 encap=ipsec ↓  
add fire poli=net ru=4 ac=nonat int=ppp0 prot=all ip=192.168.30.1-192.168.30.254 encap=ipsec ↓
```

16. 192.168.10.0/24に所属するホストから、192.168.20.0/24、30.0/24宛の通信に対して透過ルールを設定します。これらの通信にはNATを適用する必要が無いいため、ac=nonatとします。

```
add fire poli=net ru=5 ac=nonat int=vlan1 prot=all ip=192.168.10.1-192.168.10.254 ↓  
set fire poli=net ru=5 remoteip=192.168.20.1-192.168.20.254 ↓  
add fire poli=net ru=6 ac=nonat int=vlan1 prot=all ip=192.168.10.1-192.168.10.254 ↓  
set fire poli=net ru=6 remoteip=192.168.30.1-192.168.30.254 ↓
```

17. DHCPサーバ機能を有効化します。

```
ena dhcp ↓
```

18. DHCPポリシー baseを作成します。オプションとしてサブネット:255.255.255.0、ゲートウェイ:192.168.10.1、DNSサーバアドレス:192.168.10.1を配布するよう設定します。

```
cre dhcp poli=base lease=7200 ↓  
add dhcp poli=base subnet=255.255.255.0 ↓  
add dhcp poli=base router=192.168.10.1 dnss=192.168.10.1 ↓
```

19. DHCPレンジ lanを作成します。192.168.10.10から254までの245個を配布するよう設定します。

```
cre dhcp range=lan poli=base ip=192.168.10.10 num=245 ↓
```

20. ルータ間の鍵交換に使用される事前共有鍵を設定します。

```
cre enco key=1 type=gene value="secret-ab" ↓  
cre enco key=2 type=gene value="secret-ac" ↓
```

### Note

create enco key コマンドはコンフィグファイルには保存されず、装置内に別途保存されます。

21. ルータ間で鍵交換を行うための Isakmp ポリシーを定義します。暗号化プロトコルには 3DES を指定しています。(それぞれ 2 行に分かれていますが、1 行で入力します)

```
cre isakmp poli="ike_ab" peer=10.0.0.2 key=1 sendn=true encalg=3desouter hashalg=sha  
group=2 ↓  
cre isakmp poli="ike_ac" peer=any key=2 sendn=true encalg=3desouter hashalg=sha  
group=2 mode=aggressive remoteid="vpn_ac" ↓
```

### Note

3DES ではなく DES を使用する場合は、encalg パラメータの値を des に変更します。

22. IPsecSA を生成するための SA スペックとバンドル SA スペックを定義します。  
暗号化プロトコルには 3DES を指定しています。

```
cre ipsec sas=1 keyman=isakmp prot=esp encalg=3desouter hashalg=sha ↓  
cre ipsec bundle=1 keyman=isakmp string="1" ↓
```

### Note

3DES ではなく DES を使用する場合は、encalg パラメータの値を des に変更します。

23. Isakmp パケットを透過するための IPsec ポリシー isa を定義します。

```
cre ipsec poli="isa" int=ppp0 ac=permit lport=500 rport=500 transport=udp ↓
```

24. ルーターA～B 間で拠点間通信を実現するための IPsec ポリシー vpn\_ab を定義します。

```
cre ipsec poli="vpn_ab" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=10.0.0.2 ↓  
set ipsec poli="vpn_ab" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.20.0 rma=255.255.255.0 ↓
```

25. ルーターC～B間で拠点間通信を実現するためのIPsecポリシー vpn\_cb を定義します。

```
cre ipsec poli="vpn_cb" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=10.0.0.2 ↓  
set ipsec poli="vpn_cb" lad=192.168.30.0 lma=255.255.255.0 rad=192.168.20.0 rma=255.255.255.0 ↓
```

26. ルーターA～C間で拠点間通信を実現するためのIPsecポリシー vpn\_ac を定義します。

```
cre ipsec poli="vpn_ac" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=dynamic ↓  
set ipsec poli="vpn_ac" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.30.0 rma=255.255.255.0 ↓
```

27. ルーターB～C間で拠点間通信を実現するためのIPsecポリシー vpn\_bc を定義します。

```
cre ipsec poli="vpn_bc" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=dynamic ↓  
set ipsec poli="vpn_bc" lad=192.168.20.0 lma=255.255.255.0 rad=192.168.30.0 rma=255.255.255.0 ↓
```

28. インターネット向け通信を平文で透過するためのIPsecポリシー inet を定義します。

```
cre ipsec poli="inet" int=ppp0 ac=permit ↓
```

29. IPsec モジュール、Isakmp モジュールを有効化します。

```
ena ipsec ↓  
ena isakmp ↓
```

30. Security Officer レベルのユーザーで再ログインを行います。login コマンドを実行するとパスワード入力を求められますので、1 で設定したパスワードを入力します。

```
login secoff ↓
```

31. セキュリティモードへ移行します。

```
ena sys sec ↓
```

32. 設定内容を router.cfg という名前で保存し、起動時に読み込まれるよう設定します。


```
cre con=router.cfg ↓  
set con=router.cfg ↓
```

ルーターAの設定は以上です。

## ルーターB、ルーターC (AR260S V2) の設定

### <手順1>

IP アドレスを自動取得するよう設定したPCを接続し、Webブラウザを起動します。  
Web ブラウザから「<http://192.168.1.1/>」を開くとユーザー名、パスワードを求められますのでユーザー名「manager」、パスワード「friend」を入力すると、次の画面が表示されます。



The screenshot shows the web interface for CentreCOM AR260S V2. The title bar indicates "CentreCOM® AR260S V2 Version 1.0.0". On the left is a navigation menu with options like "設定保存", "セットアップウィザード", "システム情報", "LAN", "WAN", "ルーティング", "ARP", "ファイアウォール/NAT", "VPN", "ログ", "システム管理", "再起動", and "ログアウト". The main content area displays "CentreCOM® AR260S V2" and a "セットアップウィザード" (Setup Wizard) dialog box with the text: "このセットアップウィザードで本製品の基本設定を行うことができます。セットアップを始めるには「次へ」ボタンをクリックしてください。" Below the dialog is a "次へ" (Next) button. The footer contains "アライドテレスिस株式会社" and "Copyright © 2006 Allied Telesis Holdings K.K. All rights reserved."

次に、左側のメニューから[LAN]-[IP]を選択します。

[IP アドレス]を 192.168.20.1 (ルーターC は 192.168.30.1)に変更して[適用]を押します。



The screenshot shows the "LAN側IP設定" (LAN Side IP Configuration) page. It has three input fields: "IPアドレス" (IP Address) with the value "192.168.20.1" circled in red, "サブネットマスク" (Subnet Mask) with "255.255.255.0", and "ダイレクトブロードキャスト転送" (Direct Broadcast Forwarding) with radio buttons for "有効" (Enabled) and "無効" (Disabled). Below these are "適用" (Apply) and "ヘルプ" (Help) buttons. At the bottom, a table titled "現在の設定" (Current Settings) shows the current IP address as "192.168.1.1" and the subnet mask as "255.255.255.0".

[適用]を押した後 1 分ほどお待ち頂き、PC を再起動します。PC が起動完了したら、再度 Web ブラウザを起動して「<http://192.168.20.1/>」(ルーターC は <http://192.168.30.1/>)を開きます。



## &lt;手順2&gt;

左側のメニューから[LAN]-[DHCP]を選択します。

[開始 IP アドレス]を 192.168.20.223 から 192.168.20.10(ルーターC は 192.168.30.10)に変更して [適用]を押します。

DHCPサーバ設定			
IPアドレスプール	始点IPアドレス	終点IPアドレス	
	<input type="text" value="192.168.20.10"/>	<input type="text" value="192.168.20.254"/>	
サブネットマスク	デフォルトゲートウェイ	リース期限	
<input type="text" value="255.255.255.0"/>	<input type="text" value="192.168.20.1"/>	<input type="text" value="00:12:00"/> (dd 日: hh 時間: mm 分)	
プライマリDNSサーバ		セカンダリDNSサーバ	
<input type="text" value="192.168.20.1"/> (オプション)		<input type="text"/> (オプション)	
プライマリWINSサーバ		セカンダリWINSサーバ	
<input type="text"/> (オプション)		<input type="text"/> (オプション)	
<input type="button" value="適用"/>		<input type="button" value="ヘルプ"/>	

## &lt;手順3&gt;

左側のメニューから[WAN]-[WAN]を選択します。

[WAN 設定]の[接続モード]に PPPoE を選択し、[デフォルトゲートウェイ]を pppoe0 とします。

pppoe0 の[ユーザ名][パスワード]に、ISP から提供された内容を入力します。

[クランプ値]を 40 から 120 に変更して[適用]を押します。

セッションID pppoe0	<input type="button" value="接続"/>	<input type="button" value="切断"/>
アンナバード PPPoE <input type="radio"/> 有効 <input checked="" type="radio"/> 無効	IPアドレス <input type="text"/> (オプション)	
<b>ユーザ名</b> <input type="text" value="user2@example"/>	<b>パスワード</b> <input type="password" value="●●●●●●●●"/>	
サービス名 <input type="text"/> (オプション)	AC(アクセスコンセントレータ名) <input type="text"/> (オプション)	
DNSオプション <input type="radio"/> 固定設定 <input checked="" type="radio"/> 自動取得	DNS問い合わせドメイン <input type="text"/> (オプション)	
MSSクランプ <input checked="" type="radio"/> 有効 <input type="radio"/> 無効	<b>クランプ値</b> <input type="text" value="120"/> バイト	MSS値 <input type="text" value="1334"/> バイト
接続オプション <input type="radio"/> ダイアルオンデマンド <input checked="" type="radio"/> キーブアライブ <input type="radio"/> 無効	エコー送信間隔 <input type="text" value="60"/> 秒	
<input type="button" value="適用"/>		

※ その他のパラメータは、初期状態のままで問題ございません。

## &lt;手順 4&gt;

左側のメニューから[ファイアウォール/NAT]-[ファイアウォール]を選択します。  
 [pppoe0(WAN)] タブを開き、[アクセスリスト設定]に次の設定を行います。

[方向] Inbound

[動作] 通過

[優先度] 1

[送信元]-[タイプ] サブネット

[サブネット] 192.168.10.0 [マスク] 255.255.255.0

[宛先]-[タイプ] サブネット

[サブネット] 192.168.20.0(ルーターC の場合 192.168.30.0) [マスク] 255.255.255.0

[送信元ポート] すべて

[宛先ポート] すべて

[プロトコル] すべて

[ログ] 無効

設定が完了したら、[追加]を押します。

アクセスリスト設定			
ID	新規作成		
方向	動作	優先度	
Inbound ▼	通過 ▼	1 ▼	
送信元	タイプ	サブネット	マスク
	サブネット ▼	192.168.10.0	255.255.255.0
宛先	タイプ	サブネット	マスク
	サブネット ▼	192.168.20.0	255.255.255.0
送信元ポート	タイプ		
	すべて ▼		
宛先ポート	タイプ		
	すべて ▼		
プロトコル	プロトコル		
	すべて ▼		
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		
追加		変更	ヘルプ

引き続き、[\[アクセスリスト設定\]](#)に次の設定を行います。

[\[方向\]](#) Inbound

[\[動作\]](#) 通過

[\[優先度\]](#) 1

[\[送信元\]-\[タイプ\]](#) サブネット

[\[サブネット\]](#) 192.168.30.0(ルーターC の場合 192.168.20.0) [\[マスク\]](#) 255.255.255.0

[\[宛先\]-\[タイプ\]](#) サブネット

[\[サブネット\]](#) 192.168.20.0(ルーターC の場合 192.168.30.0) [\[マスク\]](#) 255.255.255.0

[\[送信元ポート\]](#) すべて

[\[宛先ポート\]](#) すべて

[\[プロトコル\]](#) すべて

[\[ログ\]](#) 無効

設定が完了したら、[\[追加\]](#)を押します。

### アクセスリスト設定

ID	新規作成		
方向	動作	優先度	
<input type="text" value="Inbound"/>	<input type="text" value="通過"/>	<input type="text" value="1"/>	
送信元	タイプ	サブネット	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.30.0"/>	<input type="text" value="255.255.255.0"/>
宛先	タイプ	サブネット	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.20.0"/>	<input type="text" value="255.255.255.0"/>
送信元ポート	タイプ		
	<input type="text" value="すべて"/>		
宛先ポート	タイプ		
	<input type="text" value="すべて"/>		
プロトコル	プロトコル		
	<input type="text" value="すべて"/>		
ログ	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		
<input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="ヘルプ"/>			

### <手順5>

左側のメニューから[VPN]-[VPN 接続]を選択します。

[VPN 接続設定]に、一つ目の VPN ポリシーとして次の内容を設定します。

[ポリシー名] vpn\_ab(ルーターC の場合 vpn\_ac) 、有効

[キープ SA] 無効

[DF ビット設定] クリア

[ローカルセキュアグループ]-[種類] サブネット

[アドレス] 192.168.20.0(ルーターC の場合は 192.168.30.0) [マスク] 255.255.255.0

[リモートセキュアグループ]-[種類] サブネット

[アドレス] 192.168.10.0 [マスク] 255.255.255.0

[ローカルゲートウェイ] pppoe0

[リモートゲートウェイ]-[種類] IP アドレス

[IP アドレス] 10.0.0.1

[内部 NAT] 無効 [フェーズ 2 ローカル ID] 空欄

VPN接続設定

ID 新規作成

ポリシー名   有効  無効

キープSA  有効  無効      DFビット設定  コピー  セット  クリア

ローカルセキュアグループ	種類 <input type="text" value="サブネット"/>	アドレス <input type="text" value="192.168.20.0"/>	マスク <input type="text" value="255.255.255.0"/>
リモートセキュアグループ	種類 <input type="text" value="サブネット"/>	アドレス <input type="text" value="192.168.10.0"/>	マスク <input type="text" value="255.255.255.0"/>
ローカルゲートウェイ	インターフェース <input type="text" value="pppoe0"/>		
リモートゲートウェイ	種類 <input type="text" value="IPアドレス"/>	IPアドレス <input type="text" value="10.0.0.1"/>	
内部NAT <input type="radio"/> 有効 <input checked="" type="radio"/> 無効	フェーズ2ローカルID <input type="text"/>	例: 192.168.1.1/32	

※ ファームウェアバージョンが 2.0.0 の場合は[キープアライブ(DPD)]という項目も表示されますが、  
※ 「無効」に設定してください。

次に、[IKE 設定]を設定します。

### Note

[IKE 暗号化/認証アルゴリズム]に 3DES ではなく DES を使用する場合、DES & SHA1-DH2 を選択します。

[IKE 交換モード] メイン(ルーターC の場合 アグレッシブ)

[事前共有鍵] secret-ab(ルーターC の場合 secret-ac)

[IKE 暗号化/認証アルゴリズム] 3DES & SHA1-DH2

[有効期限] 3600 秒(1 時間)

ルーターC の場合は、上記に加えて[ローカル ID]-[種類]を FQDN に、[FQDN]を vpn\_ac とします。

ルーターB の設定内容:

IKE設定	
IKE交換モード	
<input checked="" type="radio"/> メイン <input type="radio"/> アグレッシブ	
事前共有鍵	IKE暗号化/認証アルゴリズム
●●●●●●●●●●	3DES & SHA1-DH2 ▼
有効期限	
3600	秒 ▼

ルーターC の設定内容:

IKE設定	
IKE交換モード	
<input type="radio"/> メイン <input checked="" type="radio"/> アグレッシブ	
事前共有鍵	IKE暗号化/認証アルゴリズム
●●●●●●●●●●	3DES & SHA1-DH2 ▼
ローカルID	種類
	FQDN ▼
	vpn_ac
リモートID	種類
	未定義 ▼
有効期限	
3600	秒 ▼

続いて、[IPsec 設定]を設定します。

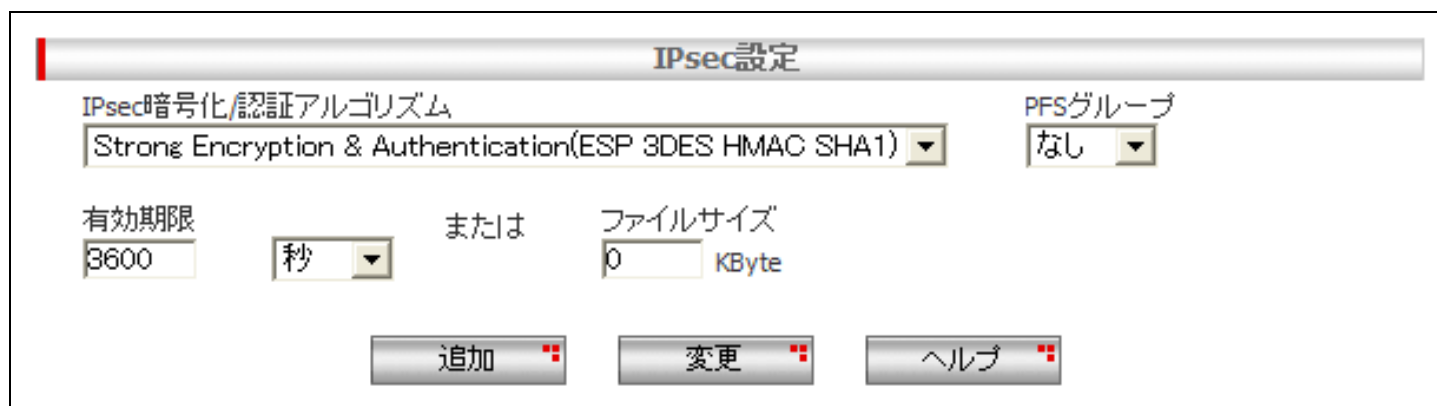
[IPsec 暗号化/認証アルゴリズム] Strong Encryption & Authentication(ESP 3DES HMAC SHA1)

[PFS グループ] なし

[有効期限] 3600 秒(1 時間)

### Note

IPsec 暗号化/認証アルゴリズムに 3DES ではなく DES を使用する場合、Encryption & Authentication(ESP DES HMAC SHA1) を選択します。



IPsec設定

IPsec暗号化/認証アルゴリズム  
Strong Encryption & Authentication(ESP 3DES HMAC SHA1) ▼

PFSグループ  
なし ▼

有効期限  
3600 秒 ▼

または ファイルサイズ  
0 KByte

追加 ▼ 変更 ▼ ヘルプ ▼

設定が完了したら、[追加]を押します。

次に、[VPN 接続設定]に 2 つ目の VPN ポリシーを設定します。

[ポリシー名] vpn\_cb(ルーターC の場合 vpn\_bc) 、有効

[キープ SA] 無効

[DF ビット設定] クリア

[ローカルセキュアグループ]-[種類] サブネット

[アドレス] 192.168.20.0(ルーターC の場合は 192.168.30.0) [マスク] 255.255.255.0

[リモートセキュアグループ]-[種類] サブネット

[アドレス] 192.168.30.0(ルーターC の場合は 192.168.20.0) [マスク] 255.255.255.0

[ローカルゲートウェイ] pppoe0

[リモートゲートウェイ]-[種類] IP アドレス

[IP アドレス] 10.0.0.1

[内部 NAT] 無効 [フェーズ 2 ローカル ID] 空欄

VPN接続設定			
ID	新規作成		
ポリシー名	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 <input type="text" value="vpn_cb"/>		
キープSA	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効		
	DFビット設定	<input type="radio"/> コピー <input type="radio"/> セット <input checked="" type="radio"/> クリア	
ローカルセキュアグループ	種類	アドレス	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.20.0"/>	<input type="text" value="255.255.255.0"/>
リモートセキュアグループ	種類	アドレス	マスク
	<input type="text" value="サブネット"/>	<input type="text" value="192.168.30.0"/>	<input type="text" value="255.255.255.0"/>
ローカルゲートウェイ	インターフェース		
	<input type="text" value="pppoe0"/>		
リモートゲートウェイ	種類	IPアドレス	
	<input type="text" value="IPアドレス"/>	<input type="text" value="10.0.0.1"/>	
内部NAT	フェーズ2ローカルID		
<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	<input type="text"/> 例: 192.168.1.1/32		

※ ファームウェアバージョンが 2.0.0 の場合は[キープアライブ(DPD)]という項目も表示されますが、  
 ※ 「無効」に設定してください。



## AR260S V2 設定例

次に、[IKE 設定]を設定します。

**Note**

[IKE 暗号化/認証アルゴリズム]に 3DES ではなく DES を使用する場合、DES & SHA1-DH2 を選択します。

[IKE 交換モード] メイン(ルーターC の場合 アグレッシブ)

[事前共有鍵] secret-ab(ルーターC の場合 secret-ac)

[IKE 暗号化/認証アルゴリズム] 3DES & SHA1-DH2

[有効期限] 3600 秒(1 時間)

ルーターC の場合は、上記に加えて[ローカル ID]-[種類]を FQDN に、[FQDN]を vpn\_ac とします。

**ルーターB の設定内容:**

IKE設定	
IKE交換モード	
<input checked="" type="radio"/> メイン	<input type="radio"/> アグレッシブ
事前共有鍵	IKE暗号化/認証アルゴリズム
●●●●●●●●●●	3DES & SHA1-DH2 ▼
有効期限	
3600	秒 ▼

**ルーターC の設定内容:**

IKE設定	
IKE交換モード	
<input type="radio"/> メイン	<input checked="" type="radio"/> アグレッシブ
事前共有鍵	IKE暗号化/認証アルゴリズム
●●●●●●●●●●	3DES & SHA1-DH2 ▼
ローカルID	種類
	FQDN
	vpn_ac
リモートID	種類
	未定義 ▼
有効期限	
3600	秒 ▼

続いて、[IPsec 設定]を設定します。

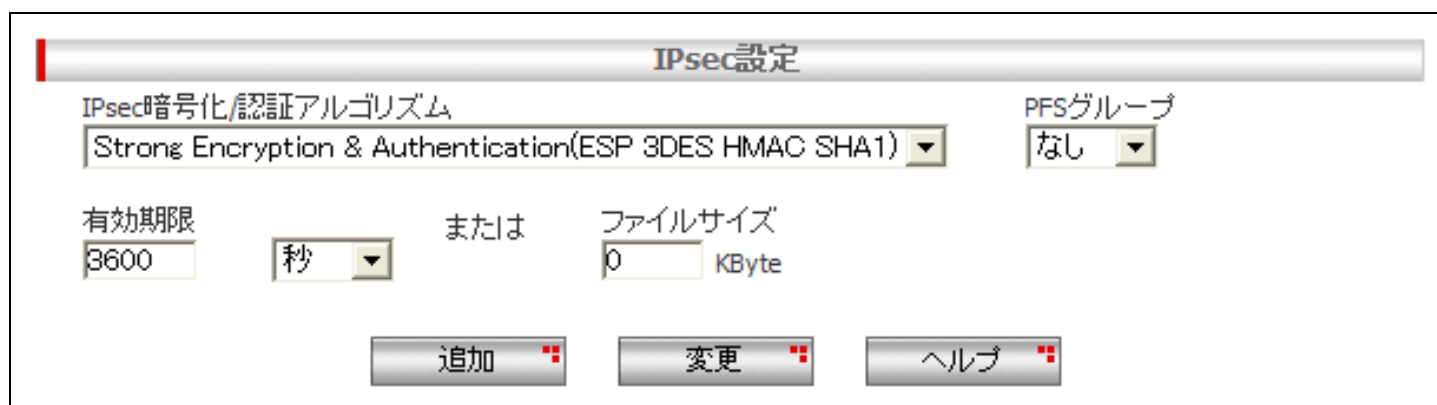
[IPsec 暗号化/認証アルゴリズム] Strong Encryption & Authentication(ESP 3DES HMAC SHA1)

[PFS グループ] なし

[有効期限] 3600 秒(1 時間)

### Note

IPsec 暗号化/認証アルゴリズムに 3DES ではなく DES を使用する場合、Encryption & Authentication(ESP DES HMAC SHA1) を選択します。



設定が完了したら、[追加]を押します。

### <手順6>

画面左上の[設定保存]を押します。

設定保存ボタン下の「設定が保存されていません」という表示が消えれば設定完了です。

設定例は以上です。

## AR550S の設定内容 まとめ

```
add user=secoff password=secoff priv=sec
cre ppp=0 over=eth0-any
set ppp=0 over=eth0-any user=user1@example password=password lqr=off bap=off echo=on
ena ip
ena ip remote
add ip int=vlan1 ip=192.168.10.1 mask=255.255.255.0
add ip int=ppp0 ip=10.0.0.1 mask=255.255.255.255
add ip rou=0.0.0.0 mask=0.0.0.0 int=ppp0 next=0.0.0.0
add ip dns int=ppp0
ena ip dnsrelay
ena fire
cre fire poli=net
ena fire poli=net icmp_f=unreach,ping
dis fire poli=net identproxy
add fire poli=net int=vlan1 type=private
add fire poli=net int=ppp0 type=public
add fire poli=net nat=enhanced int=vlan1 gblint=ppp0
add fire poli=net ru=1 ac=allow int=ppp0 prot=udp po=500 gblpo=500 ip=10.0.0.1 gblip=0.0.0.0
add fire poli=net ru=2 ac=nonat int=ppp0 prot=all ip=192.168.10.1-192.168.10.254 encaps=ipsec
add fire poli=net ru=3 ac=nonat int=ppp0 prot=all ip=192.168.20.1-192.168.20.254 encaps=ipsec
add fire poli=net ru=4 ac=nonat int=ppp0 prot=all ip=192.168.30.1-192.168.30.254 encaps=ipsec
add fire poli=net ru=5 ac=nonat int=vlan1 prot=all ip=192.168.10.1-192.168.10.254
set fire poli=net ru=5 remoteip=192.168.20.1-192.168.20.254
add fire poli=net ru=6 ac=nonat int=vlan1 prot=all ip=192.168.10.1-192.168.10.254
set fire poli=net ru=6 remoteip=192.168.30.1-192.168.30.254
ena dhcp
cre dhcp poli=base lease=7200
add dhcp poli=base subnet=255.255.255.0
add dhcp poli=base router=192.168.10.1 dnss=192.168.10.1
cre dhcp range=lan poli=base ip=192.168.10.10 num=245
# cre enco key=1 type=gene value="secret-ab"
# cre enco key=2 type=gene value="secret-ac"
cre isakmp poli="ike_ab" peer=10.0.0.2 key=1 sendn=true encalg=3desouter hashalg=sha group=2
cre isakmp poli="ike_ac" peer=any key=2 encalg=3desouter hashalg=sha group=2 mode=aggressive
set isakmp poli="ike_ac" sendn=true remoteid="vpn_ac"
cre ipsec sas=1 keyman=isakmp prot=esp encalg=3desouter hashalg=sha
cre ipsec bundle=1 keyman=isakmp string="1"
cre ipsec poli="isa" int=ppp0 ac=permit lport=500 rport=500 transport=udp
cre ipsec poli="vpn_ab" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=10.0.0.2
set ipsec poli="vpn_ab" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.20.0 rma=255.255.255.0
cre ipsec poli="vpn_cb" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=10.0.0.2
set ipsec poli="vpn_cb" lad=192.168.30.0 lma=255.255.255.0 rad=192.168.20.0 rma=255.255.255.0
cre ipsec poli="vpn_ac" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=dynamic
set ipsec poli="vpn_ac" lad=192.168.10.0 lma=255.255.255.0 rad=192.168.30.0 rma=255.255.255.0
cre ipsec poli="vpn_bc" int=ppp0 ac=ipsec keyman=isakmp bundle=1 peer=dynamic
set ipsec poli="vpn_bc" lad=192.168.20.0 lma=255.255.255.0 rad=192.168.30.0 rma=255.255.255.0
```

## AR Series Configuration Example

### AR260S V2 設定例

---

```
cre ipsec poli="inet" int=ppp0 ac=permit
ena ipsec
ena isakmp
# login seoff
# ena sys sec
```