

## CUG サービス(端末型)における 3 点間 IPsecVPN (インターネットアクセス・支社間通信は本社経由)

本社(ルーターA:AR550S)と支社(ルーターB、C:AR260S V2)を CUG(Closed Users Group)サービス(NTT 東日本のフレッツ・グループアクセス(ライト)および NTT 西日本のフレッツ・グループ(ベーシックメニュー))の「端末型払い出し」に接続します。本社～拠点間に IPsec(ESP)トンネルを構築して拠点間通信を実現しつつ、本社(ルーターA)経由でインターネットアクセスも行います。

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

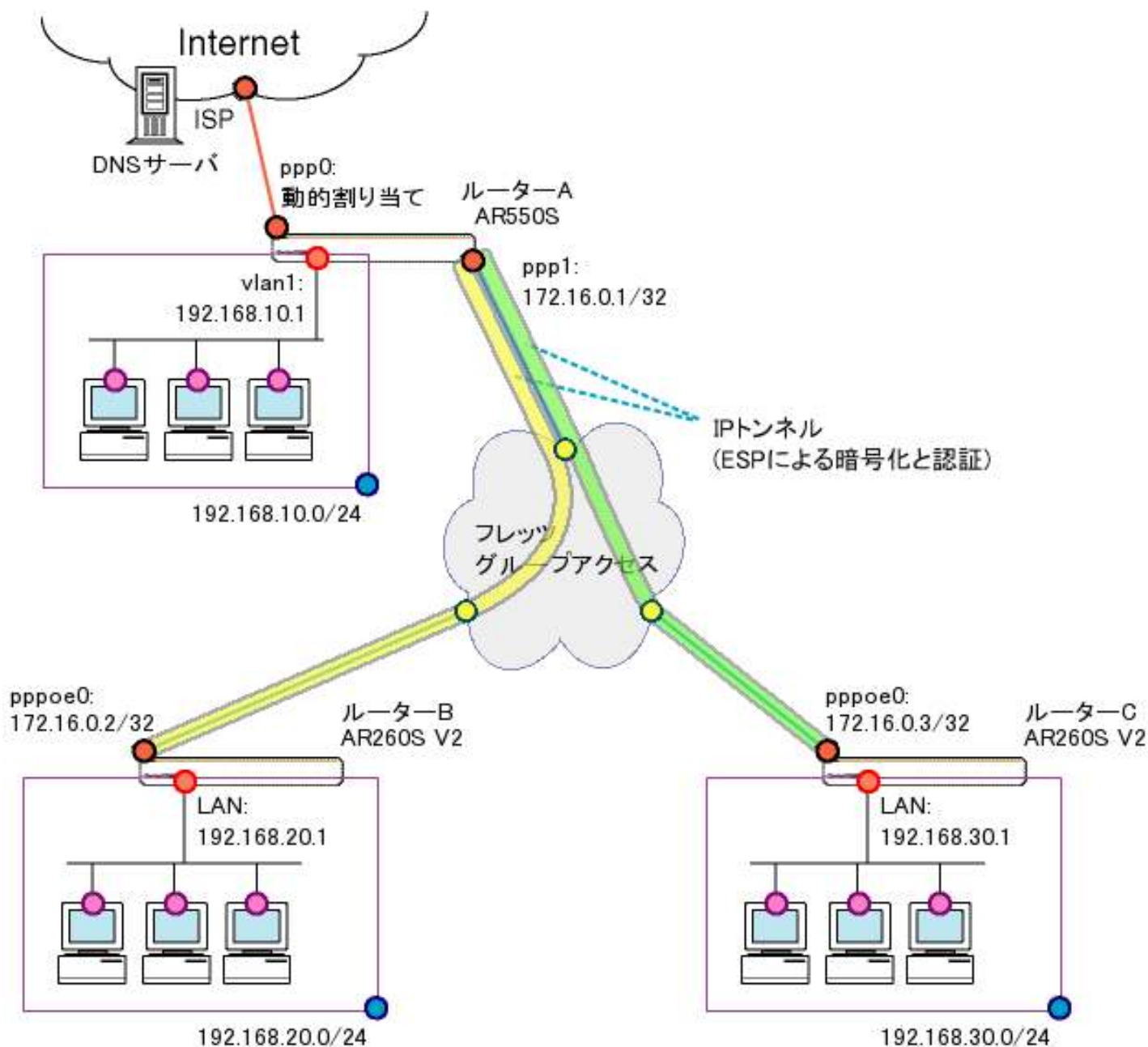
ルーターA	
PPP ユーザー名	user1@example
PPP パスワード	password
サービス名	指定なし
IP アドレス	グローバルアドレス 1 個 (動的割り当て)
DNS サーバー	接続時に通知される

CUG サービスからは、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)	router1	router2	router3
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
IP アドレス	172.16.0.1/32	172.16.0.2/32	172.16.0.3/32

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 (172.16.0.2/32 を取得)	自動取得 (172.16.0.3/32 を取得)
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	192.168.20.0/24 ～ すべて	192.168.30.0/24 ～ すべて
ローカルゲートウェイ	pppoe0	pppoe0
リモートゲートウェイ	172.16.0.1	172.16.0.1
IKE 設定		
交換モード	メイン	メイン
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
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



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は PPPoE マルチセッションで ISP と CUG サービスに同時接続します。
- ルーターB～A 間、C～A 間の IPsec ポリシーにて、リモートセキュアグループを「すべて」とすることでインターネット宛パケットもカプセル化対象になります。

※ ルーターB、C の設定手順は同一です。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。  
(2 行に分かれておりますが、1 行でまとめて入力します)

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

4. CUG サービスに接続するため、eth0 インターフェース上に ppp1 を作成します。

```
cre ppp=1 over=eth0-any ↓
```

5. CUG サービスから提供されたユーザー名、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=1 over=eth0-any user=router1 password=password lqr=off bap=off echo=on ↓
```

6. 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。  
また、IP インターフェースが IP アドレスを自動取得できるよう、リモートアサインも有効化します。

```
ena ip ↓  
ena ip remote ↓
```

7. 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 ↓
```

8. ISP に接続する ppp0 はIPアドレスを自動取得するので、IP アドレスに 0.0.0.0 を設定します。

```
add ip int=ppp0 ip=0.0.0.0 ↓
```

9. CUG サービスへ接続する ppp1 には、CUG サービスから提供された 172.16.0.1/32 を設定します。

```
add ip int=ppp1 ip=172.16.0.1 mask=255.255.255.255 ↓
```

10. デフォルトルートを 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 ↓
```

11. 対向ルータの IP アドレスと、対向拠点サブネット向けのルートを ppp1 に設定します。

```
add ip rou=172.16.0.2 mask=255.255.255.255 int=ppp1 next=0.0.0.0 ↓
```

```
add ip rou=172.16.0.3 mask=255.255.255.255 int=ppp1 next=0.0.0.0 ↓
```

```
add ip rou=192.168.20.0 mask=255.255.255.0 int=ppp1 next=0.0.0.0 ↓
```

```
add ip rou=192.168.30.0 mask=255.255.255.0 int=ppp1 next=0.0.0.0 ↓
```

12. 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 ↓
```

13. DNS リレーを有効化します。

```
ena ip dnsrelay ↓
```

14. ファイアウォールを有効化します。

```
ena fire ↓
```

15. 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 ↓
```

16. 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、ppp1/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 ppp1/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 ↓  
add fire poli=net int=ppp1 type=private ↓
```

17. インターネットアクセスを実現するため、vlan1～ppp0 間と ppp1～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 ↓  
add fire poli=net nat=enhanced int=ppp1 gblint=ppp0 ↓
```

18. DHCP サーバ機能を有効化します。

```
ena dhcp
```

19. 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 ↓
```

20. 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 ↓
```

21. 暗号化に使用す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。

22. 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=172.16.0.2 key=1 sendn=true encalg=3desouter hashalg=sha  
group=2 ↓  
cre isakmp poli="ike_ac" peer=172.16.0.3 key=2 sendn=true encalg=3desouter hashalg=sha  
group=2 ↓
```

### 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. 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。

24. 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=ppp1 ac=permit lport=500 rport=500 transport=udp ↓
```

25. ルーターB の LAN と VPN を行うため、ルーターB 向けの IPsec ポリシー vpn\_ab を定義します。  
lad を 0.0.0.0 とする事で 送信元 IP にかかわらず、宛先 IP アドレスのみを条件にポリシーが  
適用されます。

```
cre ipsec poli="vpn_ab" int=ppp1 ac=ipsec keyman=isakmp bundle=1 peer=172.16.0.2 ↓  
set ipsec poli="vpn_ab" lad=0.0.0.0 rad=192.168.20.0 rma=255.255.255.0 ↓
```

26. ルーターC の LAN と VPN を行うため、ルーターC 向けの IPsec ポリシー vpn\_ac を定義します。lad を 0.0.0.0 とする事で 送信元 IP にかかわらず、宛先 IP アドレスのみを条件にポリシーが適用されます。

```
cre ipsec poli="vpn_ac" int=ppp1 ac=ipsec keyman=isakmp bundle=1 peer=172.16.0.3 ↓  
set ipsec poli="vpn_ac" lad=0.0.0.0 rad=192.168.30.0 rma=255.255.255.0 ↓
```

27. 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 ↓
```

28. IPsec モジュール、Isakmp モジュールを有効化します。

```
ena ipsec ↓  
ena isakmp ↓
```

29. 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 ↓
```

30. セキュリティモードへ移行します。

```
ena sys sec ↓
```

31. 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。

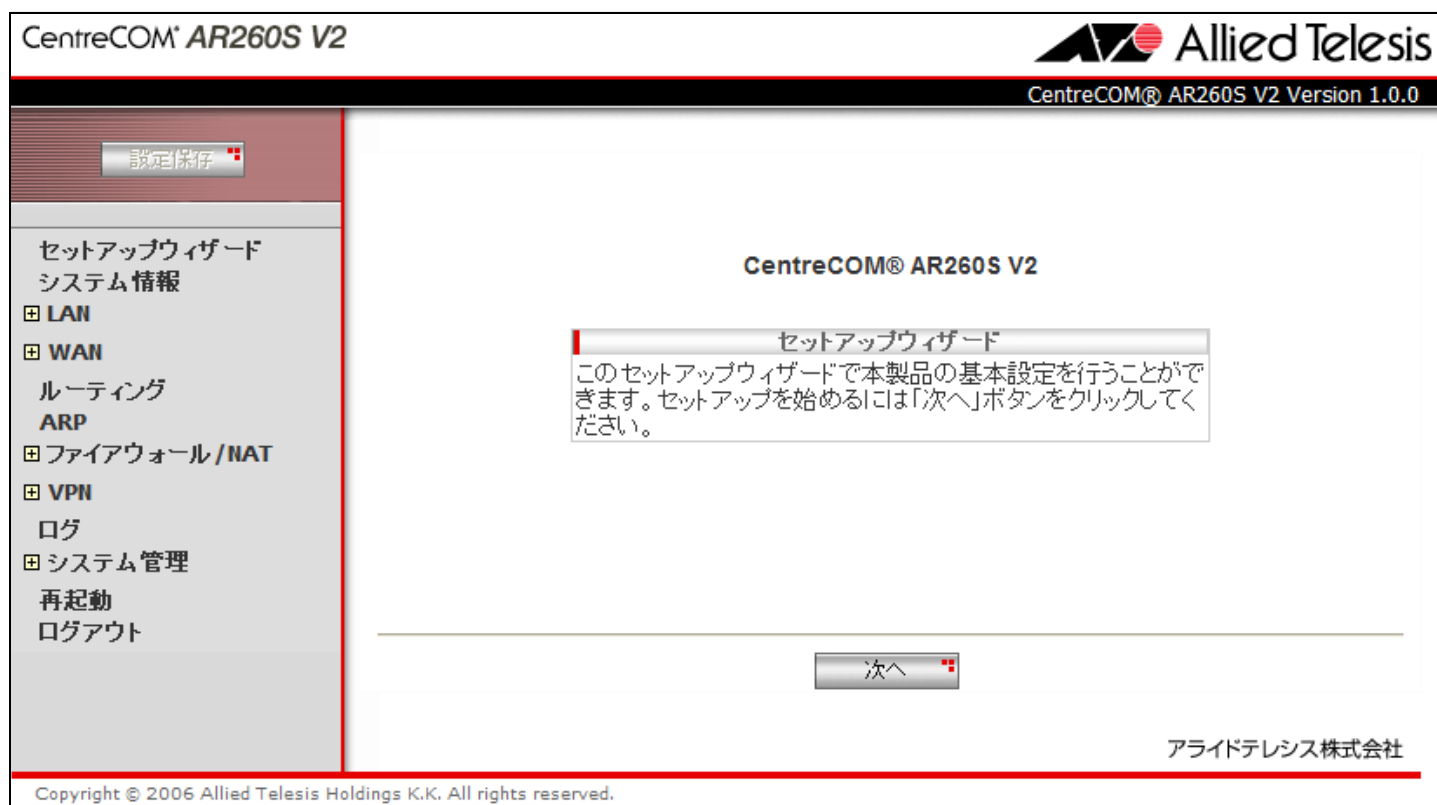
```
cre con=router.cfg ↓  
set con=router.cfg ↓
```

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 includes the Allied Telesis logo and the version number "CentreCOM® AR260S V2 Version 1.0.0". On the left, there 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 the "セットアップウィザード" (Setup Wizard) screen with a message: "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。" (You can perform the basic settings of this product using this setup wizard. To start the setup, click the "Next" button.) Below the message is a "次へ" (Next) button. At the bottom right, the text "アライドテレシス株式会社" (Allied Telesis Co., Ltd.) and "Copyright © 2006 Allied Telesis Holdings K.K. All rights reserved." are visible.

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 features 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), where "無効" is selected. Below these fields 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 configuration: IPアドレス: 192.168.1.1 and サブネットマスク: 255.255.255.0.

現在の設定	
IPアドレス	192.168.1.1
サブネットマスク	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。

## <手順2>

左側のメニューから[LAN]-[DHCP]を選択し、  
[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)に変更します。  
[プライマリ DNS サーバ]を 192.168.10.1 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	
255.255.255.0	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="192.168.10.1"/> (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、CUGサービス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="router2"/>	<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"/> キープアライブ <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] すべて

[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		
	すべて		
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		
<input type="button" value="追加"/> <input type="button" value="変更"/> <input type="button" value="ヘルプ"/>			

## &lt;手順5&gt;

左側のメニューから[VPN]-[VPN 接続]を選択し、[VPN 接続設定]を次の内容で設定します。

[ポリシー名] vpn 、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] すべて

[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] 172.16.0.1

[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"/>			
キープSA	DFビット設定		
<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	<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		
	<input type="text" value="すべて"/>		
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="172.16.0.1"/>	
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。

次に、[\[IKE 設定\]](#)の設定を行います。

[\[IKE 交換モード\]](#) メイン

[\[事前共有鍵\]](#) 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)

### 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設定**

IKE交換モード  
 メイン    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 ▼

次に、[\[IPsec 設定\]](#)を設定して[\[追加\]](#)を押します。

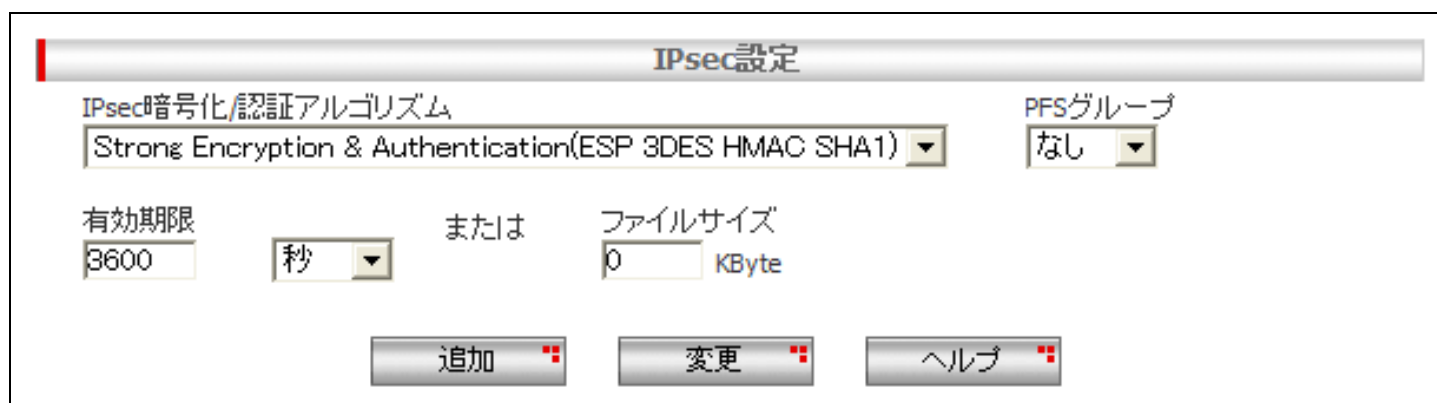
[\[IPsec 暗号化/認証アルゴリズム\]](#) Strong Encryption & Authentication(ESP 3DES HMAC SHA1)

[\[PFS グループ\]](#) 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 PFSグループ  
 Strong Encryption & Authentication(ESP 3DES HMAC SHA1) ▼ なし ▼

有効期限 秒 ▼ または ファイルサイズ  
 3600 秒 ▼ 0 KByte

#### <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 iprequest=on lqr=off bap=off echo=on
cre ppp=1 over=eth0-any
set ppp=1 over=eth0-any user=router1 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=0.0.0.0
add ip int=ppp1 ip=172.16.0.1 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 rou=172.16.0.2 mask=255.255.255.255 int=ppp1 next=0.0.0.0
add ip rou=172.16.0.3 mask=255.255.255.255 int=ppp1 next=0.0.0.0
add ip rou=192.168.20.0 mask=255.255.255.0 int=ppp1 next=0.0.0.0
add ip rou=192.168.30.0 mask=255.255.255.0 int=ppp1 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 int=ppp1 type=private
add fire poli=net nat=enhanced int=vlan1 gblint=ppp0
add fire poli=net nat=enhanced int=ppp1 gblint=ppp0
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=172.16.0.2 key=1 sendn=true encalg=3desouter hashalg=sha group=2
cre isakmp poli="ike_ac" peer=172.16.0.3 key=2 sendn=true encalg=3desouter hashalg=sha group=2
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=ppp1 ac=permit lport=500 rport=500 transport=udp
cre ipsec poli="vpn_ab" int=ppp1 ac=ipsec keyman=isakmp bundle=1 peer=172.16.0.2
set ipsec poli="vpn_ab" lad=0.0.0.0 rad=192.168.20.0 rma=255.255.255.0
cre ipsec poli="vpn_ac" int=ppp1 ac=ipsec keyman=isakmp bundle=1 peer=172.16.0.3
set ipsec poli="vpn_ac" lad=0.0.0.0 rad=192.168.30.0 rma=255.255.255.0
cre ipsec poli="inet" int=ppp0 ac=permit
ena ipsec
ena isakmp
# login secoff
# ena sys sec
```