PPPoE 接続環境における2点間 IPsecVPN(片側アドレス不定)

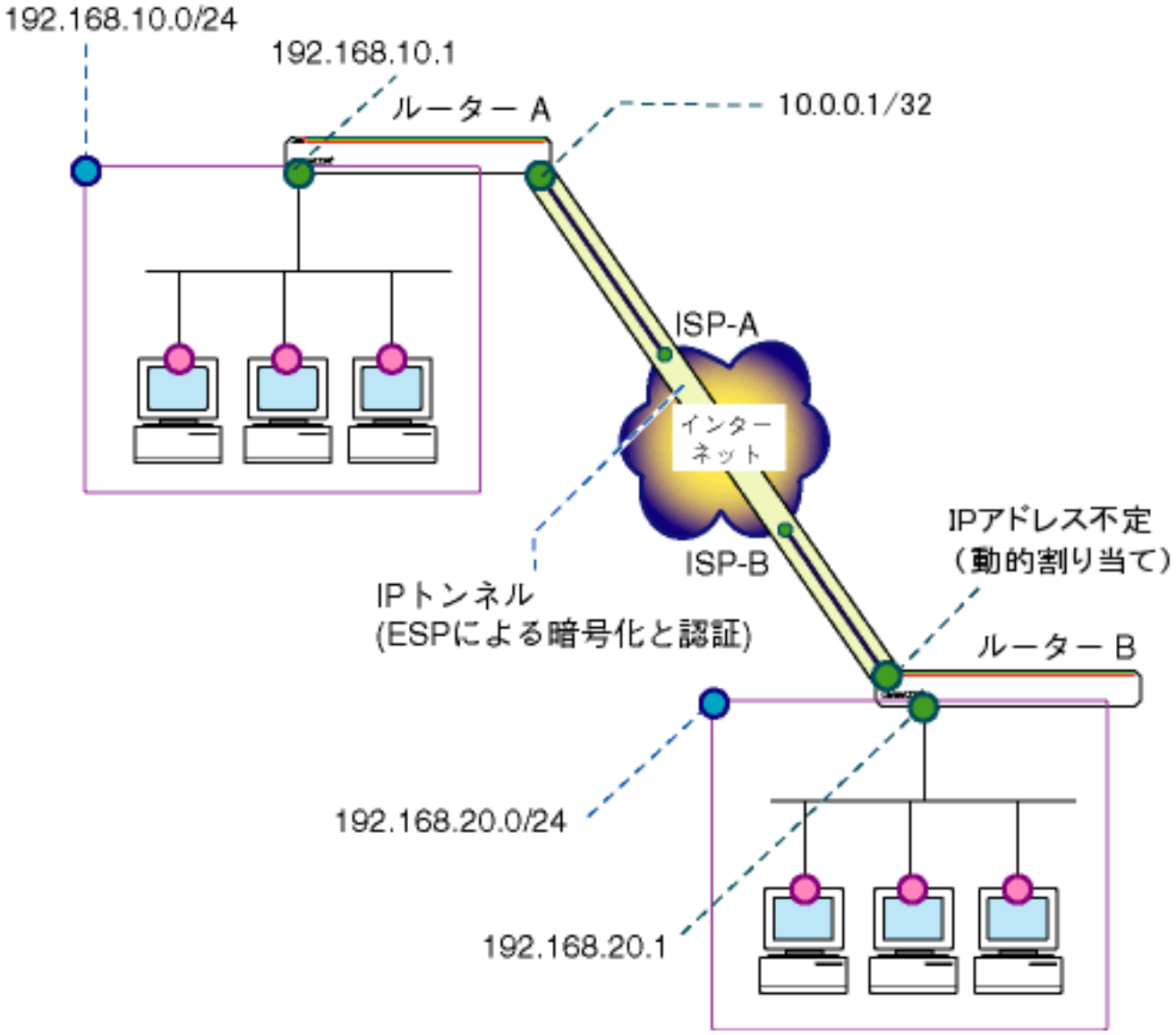
PPPoE でインターネットに接続している2つの拠点を IPsec で結ぶ VPN 構築例です。グローバルアドレス 1 個を固定的に割り当てられているサイト(ルーターA:AR260S V2)と、グローバルアドレス 1 個を動的に割り当てられるサイト(ルーターB:AR260S V2)の間を IPsec(ESP)トンネルで接続します。
また、各拠点からのインターネット向け通信を可能とします。

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	ルーターB
PPP ユーザー名	user1@example	user2@example
PPP パスワード	password	password
IP アドレス	10.0.0.1/32 (固定)	不定 (動的割り当て)
DNS サーバー	接続時に通知される	接続時に通知される

各ルーターは以下のように設定するものとします。

	ルーターA	ルーターB
WAN 側 IP アドレス	自動取得 (10.0.0.1/32 を取得)	自動取得 (取得アドレスは不定)
LAN 側 IP アドレス	192.168.10.1/24	192.168.20.1/24
VPN 接続設定		
ローカルセキュアグループ	192.168.10.0/24	192.168.20.0/24
リモートセキュアグループ	192.168.20.0/24	192.168.10.0/24
ローカルゲートウェイ	pppoe0	pppoe0
リモートゲートウェイ	任意	10.0.0.1
IKE 設定		
交換モード	アグレッシブ	アグレッシブ
事前共有鍵	secret	secret
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/vpn	vpn/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



本構成における設定のポイントは、次の通りです。

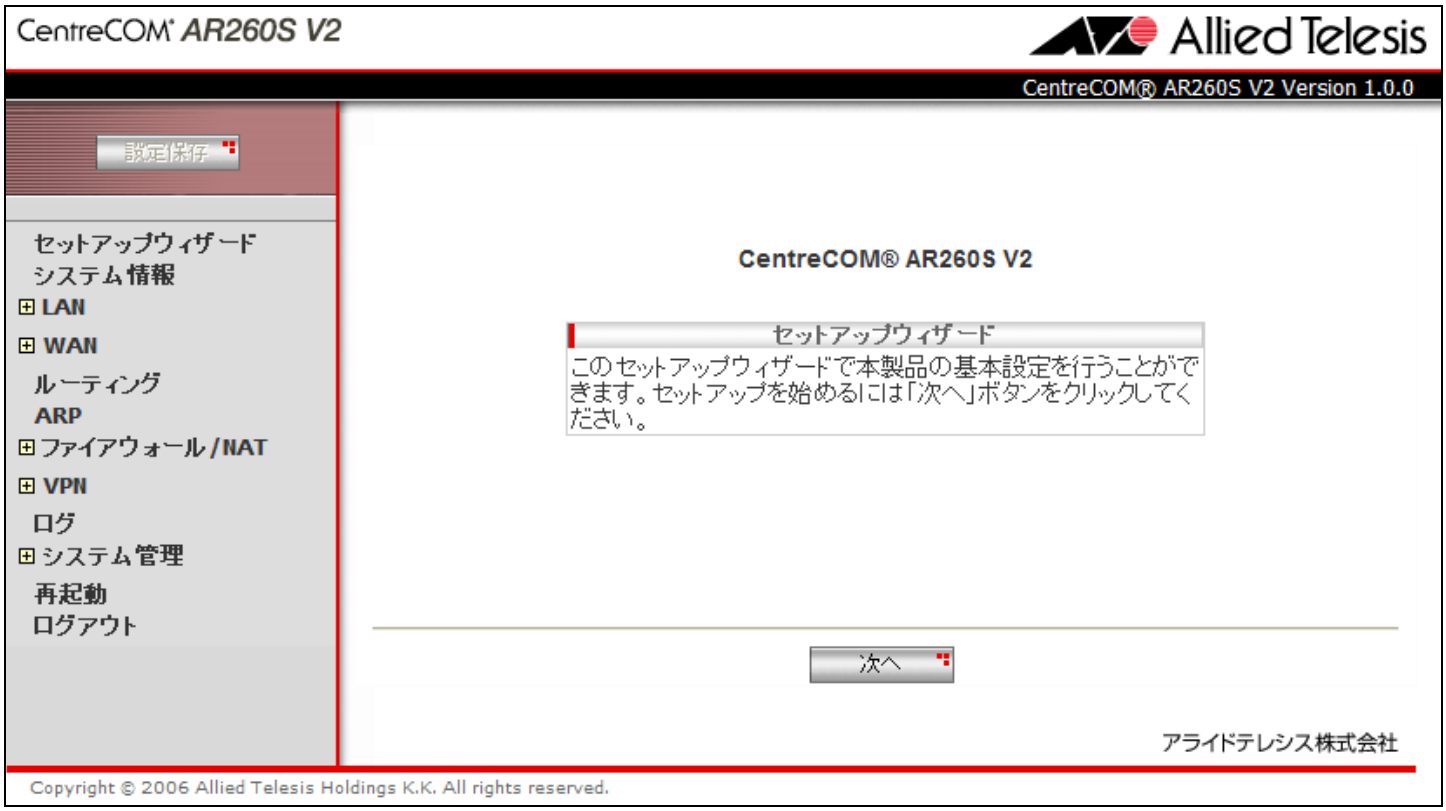
- ルーターBのアドレスが不定のため、ルーターAからルーターBに接続することはできません。
  常にルーターBから接続を開始することになります。

- ルーターBのアドレスが不定なため、IKEフェーズ1ではAggressiveモードを使い、
  ルーターBのIDとして文字列（名前）を使用します。

※ 本設定例は ルーターAへの設定内容を想定しています。ルーターBの設定を行う場合は
※ 文中の「ルーターBは～」をご参照ください。

＜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。

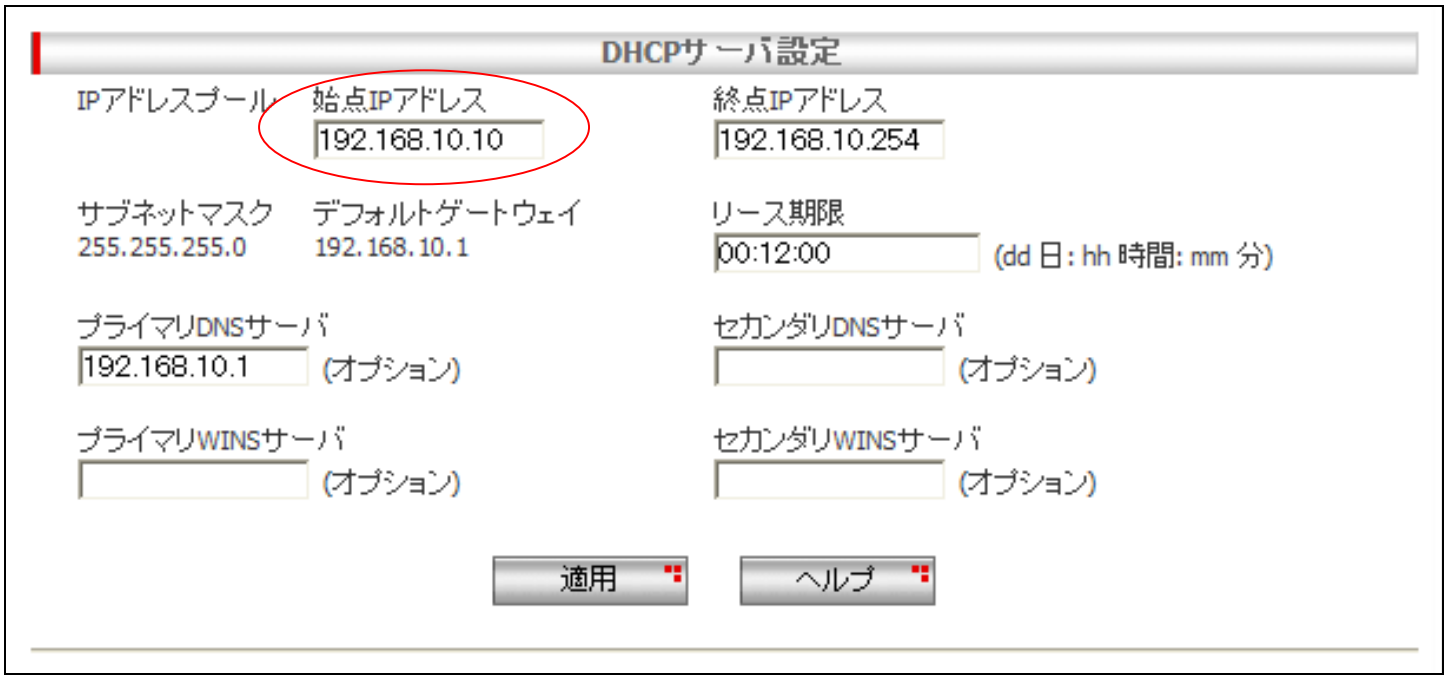


次に、左側のメニューから[LAN]-[IP]を選択します。
[IP アドレス]を 192.168.10.1 (ルーターBは 192.168.20.1)に変更して[適用]を押します。

[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://192.168.10.1/」(ルーターBは http://192.168.20.1/)を開きます。

＜手順2＞

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 192.168.10.223 から 192.168.10.10（ルーターBは 192.168.20.10）に変更して
[適用]を押します。

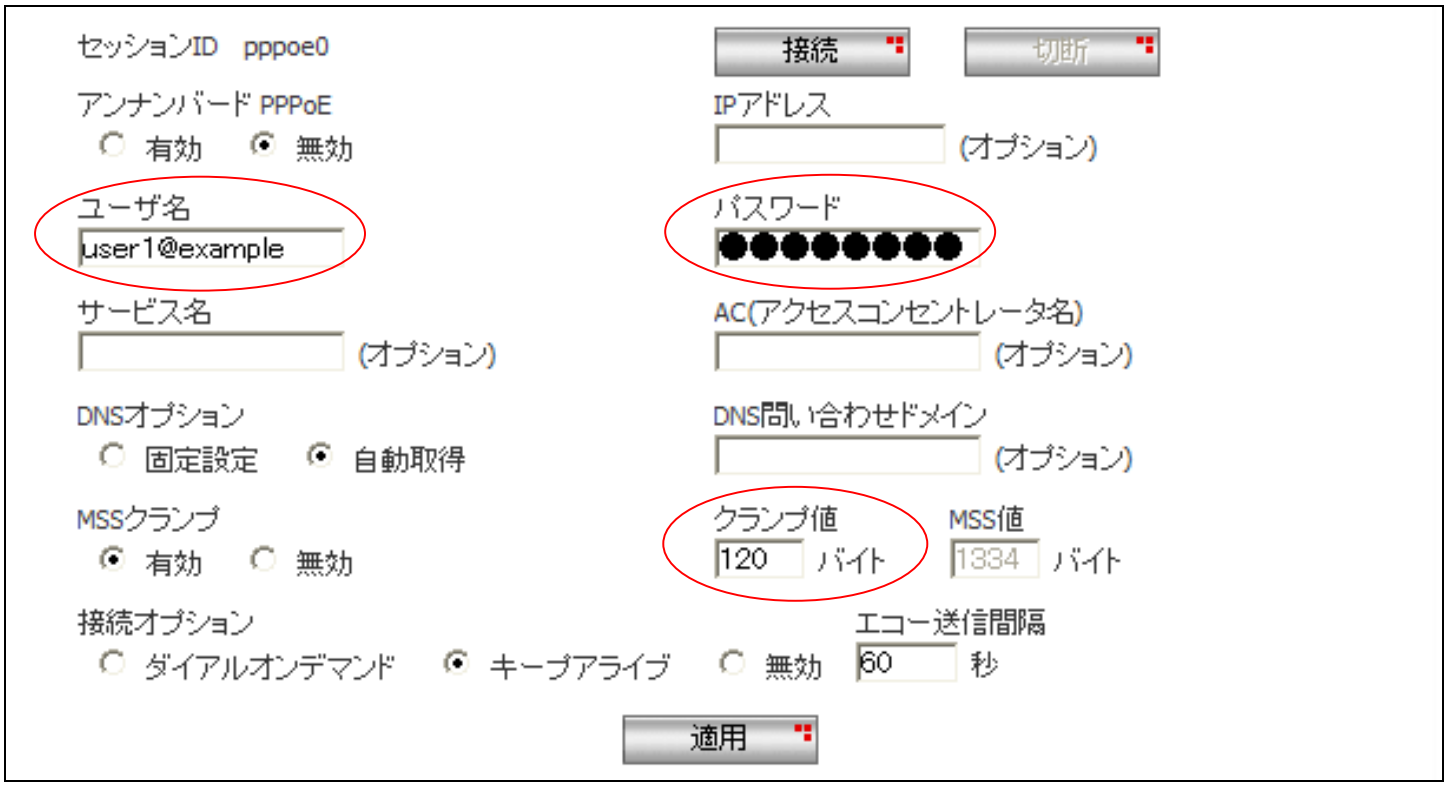


＜手順3＞

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 の設定

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。



※ 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。

＜手順 4＞

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] 192.168.20.0（ルーターB の場合 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] 192.168.10.0（ルーターB の場合 192.168.20.0） [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

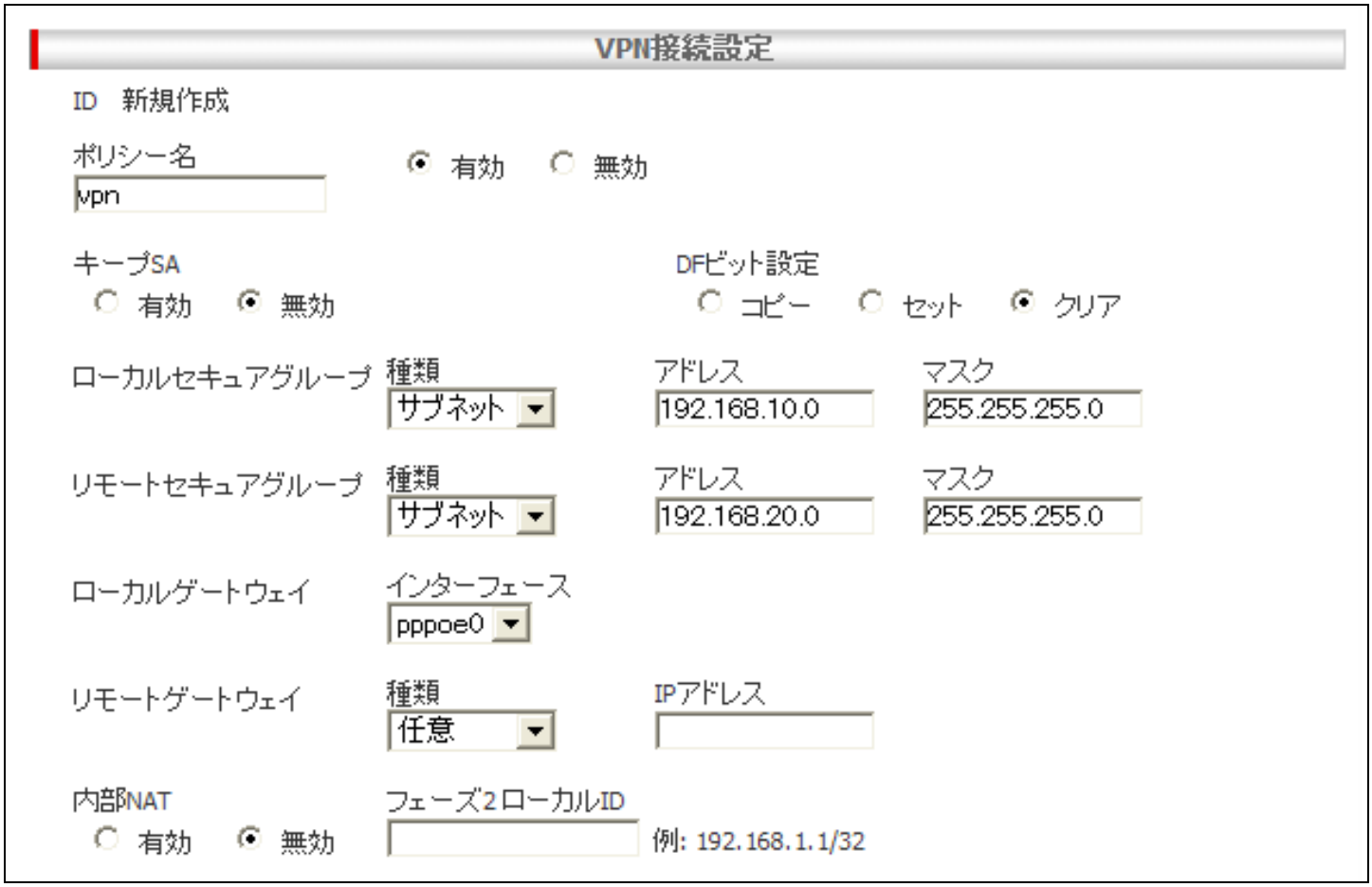
設定が完了したら、[追加]を押します。

＜手順 5＞

左側のメニューから[VPN]-[VPN 接続]を選択し、[VPN 接続設定]をそれぞれ以下の内容で設定します。

ルーターAの場合：

[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] 192.168.10.0
[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] 192.168.20.0
[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] 任意
[IP アドレス] 空欄
[内部 NAT] 無効 [フェーズ 2 ローカル ID] 空欄



※ 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ので、
※「有効」に設定してください。

次に、[IKE 設定]を設定します。

[IKE 交換モード] アグレッシブ
[事前共有鍵] secret
[IKE 暗号化/認証アルゴリズム] 3DES & SHA1-DH2
[有効期限] 3600 秒(1 時間)
[リモート ID]-[種類] FQDN
[FQDN] vpn

次に、[IPsec 設定]を設定し[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)

ルーターBの場合：

[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
[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

※ 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ので、
※「有効」に設定してください。

次に、[IKE 設定]を設定します。

[IKE 交換モード] アグレッシブ
[事前共有鍵] secret
[IKE 暗号化/認証アルゴリズム] 3DES & SHA1-DH2
[有効期限] 3600 秒(1 時間)
[ローカル ID]-[種類] FQDN
[FQDN] vpn

次に、[IPsec 設定]を設定し[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)

＜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。