

PPPoE マルチセッション用の設定手順

フレッツグループアクセス 端末型払い出しでの接続方法 6
~ IPsec トンネルを利用した接続例 2(センター経由の接続) ~

センチュリー・システムズ(株)

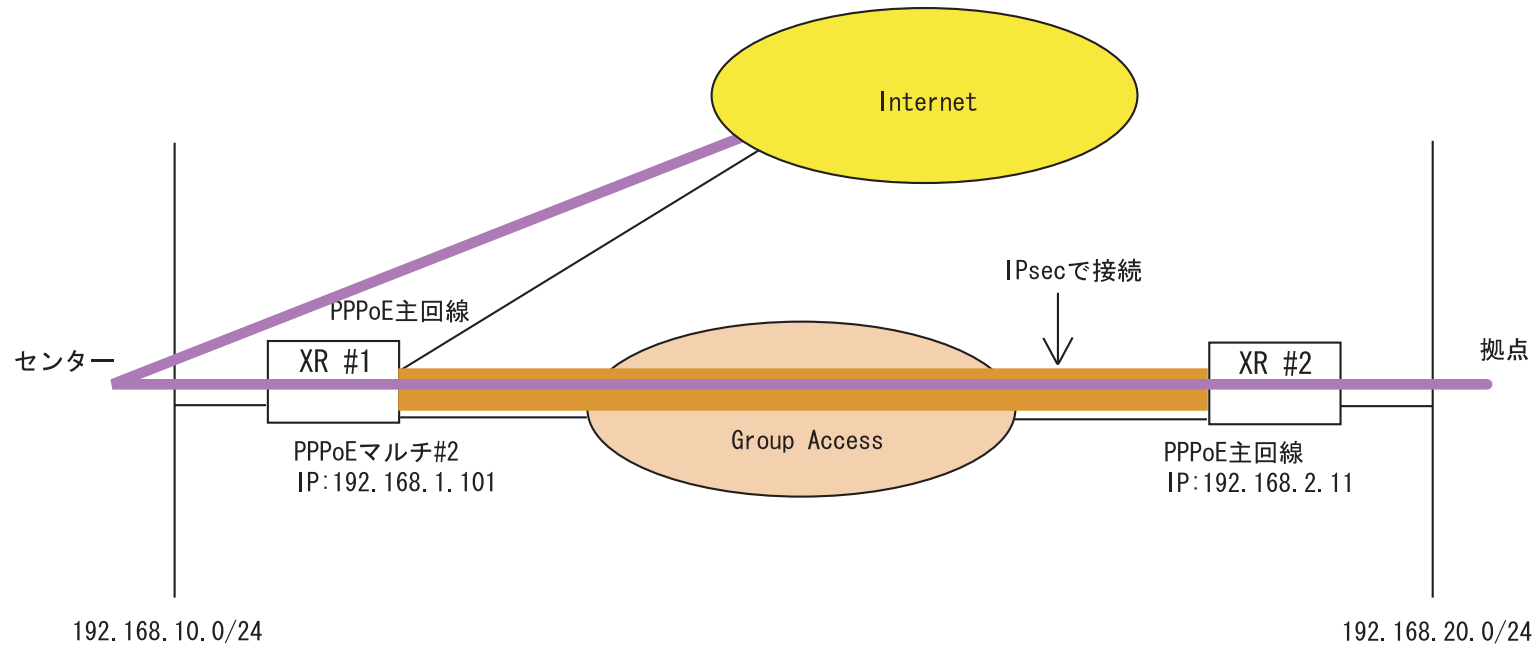
はじめに

この設定ガイドは、以下の機種に対応しています。

- XR-380/DES
- XR-410 シリーズ各製品
- XR-440/C
- XR-640/CD
- XR-1000 ファームウェア ver 2.0 以降
- XR-1000/TX4

この設定例は、インターネットへの接続とフレッツ・グループアクセス の利用を同時におこなう場合に必要な設定例です。フレッツ・グループアクセス プロ 端末型アドレス払い出しとフレッツ・グループアクセスライトでの利用にお使いいただける設定例となります。

マルチセッション利用時におけるIPsecを利用した接続構成例 2



運用の条件

- (a) 双方のLAN は任意のプライベートアドレス環境で運用します。
- (b) XR #1 は PPPoE 主回線側でインターネットに、PPPoE マルチ #2 回線側でフレッツ・グループアクセスに同時接続します。XR #2はPPPoE主回線側でグループアクセスに接続します。グループアクセスは IP アドレス端末型払い出しでの接続とします。
- (c) XR #1 と XR #2 間を IPsec で接続します。
- (d) 拠点がインターネットアクセスするときは、IPsec トンネルでセンター側を経由してアクセスするものとします。

[a-1] インターフェース設定

<XR #1 の設定>

Ether 0ポート	<input checked="" type="radio"/> 固定アドレスで使用 IPアドレス <input type="text" value="192.168.10.254"/> ネットマスク <input type="text" value="255.255.255.0"/> MTU <input type="text" value="1500"/> <input type="radio"/> DHCPサーバから取得 ホスト名 <input type="text"/> MACアドレス <input type="text"/> <input type="checkbox"/> IPマスカレード (このポートで使用するIPアドレスに変換して通信を行います) <input type="checkbox"/> ステートフルパケットインスペクション <input type="checkbox"/> Proxy ARP ポートの通信モード <input checked="" type="radio"/> 自動 <input type="radio"/> full-100M <input type="radio"/> half-100M <input type="radio"/> full-10M <input type="radio"/> half-10M
	<input checked="" type="radio"/> 固定アドレスで使用 IPアドレス <input type="text" value="192.168.100.254"/> ネットマスク <input type="text" value="255.255.255.0"/> MTU <input type="text" value="1500"/> <input type="radio"/> DHCPサーバから取得 ホスト名 <input type="text"/> MACアドレス <input type="text"/> <input type="checkbox"/> IPマスカレード (このポートで使用するIPアドレスに変換して通信を行います) <input checked="" type="checkbox"/> ステートフルパケットインスペクション <input type="checkbox"/> Proxy ARP ポートの通信モード <input checked="" type="radio"/> 自動 <input type="radio"/> full-100M <input type="radio"/> half-100M <input type="radio"/> full-10M <input type="radio"/> half-10M
デフォルトゲートウェイ	<input type="text"/>

<XR #2 の設定>

Ether 0ポート	<input checked="" type="radio"/> 固定アドレスで使用 IPアドレス <input type="text" value="192.168.20.254"/> ネットマスク <input type="text" value="255.255.255.0"/> MTU <input type="text" value="1500"/> <input type="radio"/> DHCPサーバから取得 ホスト名 <input type="text"/> MACアドレス <input type="text"/> <input type="checkbox"/> IPマスカレード (このポートで使用するIPアドレスに変換して通信を行います) <input type="checkbox"/> ステートフルパケットインスペクション <input type="checkbox"/> Proxy ARP ポートの通信モード <input checked="" type="radio"/> 自動 <input type="radio"/> full-100M <input type="radio"/> half-100M <input type="radio"/> full-10M <input type="radio"/> half-10M
	<input checked="" type="radio"/> 固定アドレスで使用 IPアドレス <input type="text" value="192.168.110.254"/> ネットマスク <input type="text" value="255.255.255.0"/> MTU <input type="text" value="1500"/> <input type="radio"/> DHCPサーバから取得 ホスト名 <input type="text"/> MACアドレス <input type="text"/> <input type="checkbox"/> IPマスカレード (このポートで使用するIPアドレスに変換して通信を行います) <input checked="" type="checkbox"/> ステートフルパケットインスペクション <input type="checkbox"/> Proxy ARP ポートの通信モード <input checked="" type="radio"/> 自動 <input type="radio"/> full-100M <input type="radio"/> half-100M <input type="radio"/> full-10M <input type="radio"/> half-10M
デフォルトゲートウェイ	<input type="text"/>

それぞれのLANに合わせて、Ether0ポートのIPアドレス、ネットマスクを設定してください。

またEther1ポートは、運用環境において他で使われていないIPアドレスを設定してください。重複しているIPアドレス設定があると正常に通信できない場合があります。

[b-1] PPPoE 接続先設定 1

<XR #1 の設定>

プロバイダ名	<input type="text"/>
ユーザID	<input type="text" value="<インターネット接続用のユーザID>"/>
パスワード	<input type="text" value="<インターネット接続用のパスワード>"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LCPキープアライブ	チェック間隔 <input type="text" value="30"/> 秒 ☑ 回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はP4P-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できません	
IPアドレス	<input type="text" value="<適宜設定します>"/> 回線接続時に割り付けるグローバルIPアドレスです

接続先設定 1 にインターネット接続のための設定をします。

ユーザ ID とパスワード、DNS 設定など。

また IP アドレスが固定割り当ての場合は、「IP アドレス」欄に値を設定してください。

<XR #2 の設定>

プロバイダ名	<input type="text"/>
ユーザID	<input type="text" value="<グループアクセス接続用のユーザID>"/>
パスワード	<input type="text" value="<グループアクセス接続用のパスワード>"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LCPキープアライブ	チェック間隔 <input type="text" value="30"/> 秒 ☑ 回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はP4P-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できません	
IPアドレス	<input type="text" value="192.168.2.1"/> 回線接続時に割り付けるグローバルIPアドレスです

接続先設定 1 にフレッツグループアクセス接続のための設定をします。ユーザ ID とパスワードを設定します。

さらに「IP アドレス」欄に、フレッツグループアクセス接続で割り当てられる IP アドレスを設定してください。

[b-2] PPPoE 接続先設定 2

<XR #1 の設定 >

プロバイダ名	<input type="text"/>
ユーザID	<input type="text" value="<グループアクセス 接続用のユーザID>"/>
パスワード	<input type="text" value="<グループアクセス 接続用のパスワード>"/>
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>
LOPキーアライブ	チェック間隔 <input type="text" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPTP-Gate wayに発行します
UnNumbered-PPP回線使用時に設定できません	
IPアドレス	<input type="text" value="192.168.1.1"/> 回線接続時に割り付けるグローバルIPアドレスです

接続先設定 2 にフレッツグループアクセス接続のための設定をします。ユーザ ID とパスワードを設定します。

さらに「IP アドレス」欄に、フレッツグループアクセス接続で割り当てられる IP アドレスを設定してください。

[b-3] PPPoE 接続設定

<XR #1 の設定>

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステートフルパケット インスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

主回線が自動的にデフォルトゲートウェイに設定されますので、ISP 接続を主回線、グループアクセス接続をマルチ接続に設定します。
接続先は「接続先1」を選択し、IP マスカレードは[有効]に設定してください。

(画面は XR-410/TX2 の表示例です)

<XR #2 の設定>

回線状態	回線は接続されていません
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケット インスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

接続先は「接続先1」を選択します。端末型接続ですが IPsec を使用しますので、IP マスカレードは[無効]にします。
また閉域網を介しての接続となりますので、ステートフルインスペクションは無効としています。

(画面は XR-410/TX2 の表示例です)

[b-4] PPPoE 接続設定 マルチ接続回線

<XR #1 の設定>

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい	
マルチ接続 #2	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
接続先の選択	<input type="radio"/> 接続先1 <input checked="" type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケット インスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

マルチ接続 #2 を「有効」に設定して、接続先は「接続先2」を選択して下さい。

端末型接続ですが IPsec を使用しますので、IP マスカレードは[無効]にします。

また閉域網を介しての接続となりますので、ステートフルインスペクションは無効としています。

(画面は XR-410/TX2 の表示例です)

[c-1] IPsec 設定 <XR #1 の設定>

本装置側の設定 1

IKE/ISAKMPの設定1	
インターフェースのIPアドレス	192.168.1.1
上位ルータのIPアドレス	%ppp2
インターフェースのID	(例:@xr.centurysys)

IKE/ISAKMP ポリシー設定 1

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	192.168.2.1
上位ルータのIPアドレス	
インターフェースのID	(例:@xr.centurysys)
モードの設定	main モード
transformの設定	1番目 すべてを送信する
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<input checked="" type="radio"/> PSKを使用する	ipsec
<input type="radio"/> RSAを使用する (X509を使用する場合はRSAに設定してください)	

IPsec ポリシー設定 1

<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransformの選択	すべてを送信する
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	(1~255まで)

本装置側の設定では、インターフェースの IP アドレスにフレッツグループアクセス接続で払い出される IP アドレスを、上位ルータの IP アドレスには「%ppp2」を設定します(ppp2 は ” マルチ接続 #2 ” のインターフェース名です)。

IKE/ISAKMP ポリシー設定のインターフェースの IP アドレスには、相手側装置の IP アドレスを設定します。

IPsec ポリシー設定には、IPsec で接続する LAN アドレスを設定します。また拠点側はすべてセンター経由の通信となりますので、本装置側の LAN 側アドレスには「0.0.0.0/0」を設定します。

[c-2] IPsec 設定 <XR #2 の設定>

本装置側の設定 1

IKE/ISAKMP の設定 1	
インターフェースの IP アドレス	192.168.2.1
上位ルータの IP アドレス	%ppp0
インターフェースの ID	(例: @xr.centurysys)

IKE/ISAKMP ポリシー設定 1

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	
接続する本装置側の設定	本装置側の設定 1
インターフェースの IP アドレス	192.168.1.1
上位ルータの IP アドレス	
インターフェースの ID	(例: @xr.centurysys)
モードの設定	main モード
transform の設定	1 番目: すべてを送信する
	2 番目: 使用しない
	3 番目: 使用しない
	4 番目: 使用しない
IKE のライフタイム	3600 秒 (1081 ~ 28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する	ipsec
<input type="radio"/> RSA を使用する (X509 を使用する場合は RSA に設定してください)	

IPsec ポリシー設定 1

<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> Responder として使用する <input type="radio"/> On-Demand で使用する	
使用する IKE ポリシー名の選択	(IKE1)
本装置側の LAN 側のネットワークアドレス	192.168.20.0/24 (例: 192.168.0.0/24)
相手側の LAN 側のネットワークアドレス	0.0.0.0/0 (例: 192.168.0.0/24)
PH2 の Transform の選択	すべてを送信する
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Group の選択 (PFS 使用時に有効)	指定しない
SA のライフタイム	28800 秒 (1081 ~ 86400 秒まで)
DISTANCE	(1 ~ 255 まで)

本装置側の設定では、上位ルータの IP アドレスには「%ppp0」を設定します (ppp2 は「PPP/PPPoE 主回線 #1」のインタフェース名です)。

IPsec ポリシー設定では「本装置側」と「相手側」の LAN 側アドレス設定が逆になっているところに注意してください。

[c-3] IPsec サービスの起動

<XR #1 の設定>

DNSサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
IPsecサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい	停止中
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
帯域制御(QoS)サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
VRRPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中

<XR #2 の設定>

DNSサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
IPsecサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい	停止中
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
帯域制御(QoS)サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
VRRPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中

「各種サービス」設定画面の IPsec サーバを、「起動」状態に動作変更してください。また PPPoE 接続を開始してください。

これですべての設定が完了です。

[補足1]入力フィルタ設定について

<XR #1 の設定>

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE-マルチ #2		パケット受信時	許可	udp				500
PPP/PPPoE-マルチ #2		パケット受信時	許可	esp				

<XR #2 の設定>

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE-マルチ #2		パケット受信時	許可	udp				500
PPP/PPPoE-マルチ #2		パケット受信時	許可	esp				

マルチ接続側でステートフルインスペクションを有効にしているときは、IPsec用の入力フィルタを設定してください。

インターフェースは「PPP/PPPoE - マルチ #2」を選択します。

[補足2]MTUについて

センター経由の通信で運用する場合に正常な通信ができないときには、MTU 値を調整する必要があります。

PPPoE 上の IPsec 接続をおこなう場合の理論上の最大 MTU 値は「1397byte」となります。

フレッツグループアクセス 端末型払い出しでの接続方法 6
～ IPsec トンネルを利用した接続例 2(センター経由の接続)～

2004 年 1 月版

発行 センチュリー・システムズ株式会社

2001-2004 CENTURYSYSTEMS, INC. All rights reserved.
