

# ***BROADBAND GATE***

---

Linux エンジン搭載ブロードバンドルータ

***FutureNet XR series***

unnumbered 接続時の IPsec 設定ガイド

## 本ガイドについて

本ガイドは、以下の製品・ファームウェアバージョンに対応しています。

**XR-380**

**XR-410**

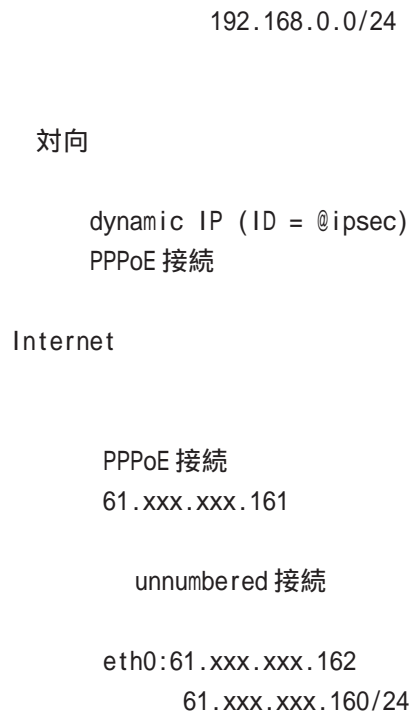
**XR-1000 Ver2.0.0 以降**

**XR-1000/TX4**

## unnumbered と IPsec の同時接続

PPPoE を用いた unnumbered 接続と同時に、DMZ 側にあるサーバ / ホストが IPsec 通信をおこなうための設定例です。

### 構成図(例)



### ISP から提供された情報(例)

- ・ユーザー ID  
*user@unnumbered*
- ・パスワード  
*password*
- ・提供された IP アドレス群  
*61.xxx.xxx.160 ~ 61.xxx.xxx.167*  
(29 ビットマスク)
- ・各インターフェースの接続  
WAN側インターフェース : Ether1ポート  
LAN側インターフェース : Ether0ポート
- ・対向側の装置は PPPoE 接続、動的 IP アドレスとします。対向側装置の ID は「@ipsec1」とします。
- ・IPsec 設定で使用するパラメータ値は以下の通りとします。  
**transform** : aggressive  
**共通鍵** : ipseckey  
**暗号方式** : 3DES  
**整合性** : SHA-1  
**IKEで使用するグループ** : group2  
**対向の ID** : @ipsec
- ・IP アドレス等は、構成図(例)の表記に従います。

## unnumbered 接続の設定

### STEP 1 Ethernet ポートの設定

はじめに Ethernet ポートの設定をおこないます。  
「インターフェース設定」画面で設定します。

#### [Ether0ポートについて]

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="61.xxx.xxx.162"/> ネットマスク <input type="text" value="255.255.255.248"/> 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
Ether 1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="192.168.1.254"/> 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"/>

「固定アドレスで使用」を選択し、以下のように入力します。

「IPアドレス」 **61.xxx.xxx.162**

「ネットマスク」 **255.255.255.248**

IPマスカレード **チェックを入れません。**

「ステートフルパケットインスペクション」  
**チェックを入れません。**

「Proxy ARP」 **任意でチェックしてください。**

**Ether1ポートは初期設定のままにします。**  
**デフォルトゲートウェイは空欄にしておきます。**

入力後に「設定の保存」をクリックします。

「設定の保存」をクリックした後は、変更した値がすぐに反映されます。

設定画面やインターネットへのアクセスするために、各ホストやサーバの IP アドレスを再設定してください。本ガイドでは、61.xxx.xxx.163 ~ 61.xxx.xxx.166 のいずれかの IP アドレスを設定します。

その後、**http://61.xxx.xxx.162:880** にアクセスし、再度設定画面にログインします。

## unnumbered 接続時の IPsec 設定ガイド

### PPPoE 接続と Ethernet ポートの設定

#### STEP 2 ISP アカウント設定をおこなう

「PPP/PPPoE 設定」画面の「接続先設定」(1 ~ 5のいずれか)をクリックします。そして、設定画面で以下のように入力します(ここでは「接続先設定1」での設定例とします)。

プロバイダ名	<input type="text"/>
ユーザID	<input type="text" value="user@unnumbered"/>
パスワード	<input type="text" value="password"/>
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 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PIP-Gatewayに発行します
<b>UnNumbered-PPP回線使用時に設定できません</b>	
IPアドレス	<input type="text" value="61.xxx.xxx.161"/> 回線接続時に割り付けるグローバルIPアドレスです
<b>PPPoE回線使用時に設定して下さい</b>	
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text" value="0"/> Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

プロバイダ名 任意で名前を付けてください。

ユーザー名 user@unnumbered

パスワード password

DNSサーバ 任意で選択します。

LCP キープアライブ

ping による接続確認

基本的には初期設定のままかまいません。

IP アドレス 61.xxx.xxx.161

**STEP 1** で設定した Ether0 の IP アドレスとは異なる IP アドレスを入力します。同じアドレスを設定すると、IPsec 接続ができません。

MSS 設定

任意で設定できますが、特に 必要がない限り「有効」を選択し、「0」を指定しておきます。

入力が終わりましたら「設定の保存」をクリックして、PPPoE 接続先設定は完了です。

#### STEP 3 PPPoE 接続の設定

「PPP/PPPoE 設定」の「接続設定」をクリックして、PPPoE 接続のための設定をおこないます。以下の項目について設定します。

目標状態	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"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand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 checked="" type="radio"/> 無効 <input 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IP変更お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
お知らせメールの宛先	<input type="text"/>
お知らせメールのFromアドレス	<input type="text" value="xr380"/>
中継するメールサーバのアドレス	<input type="text"/>

接続先の選択 「接続先1」を選択します。

接続ポート 「Ether1」を選択します。

接続形態 任意で選択してください。

BRI 接続タイプ(XR-380)「通常」を選択します。

IP マスカレード 「無効」を選択します。

ステートフルパケットインスペクション  
「無効」を選択します。

デフォルトルートの設定

「有効」を選択します。

接続 IP 変更お知らせメール

「送信しない」を選択します。

上記設定後に「設定の保存」をクリックして PPPoE 接続設定は完了です。

## 各ホスト / サーバの設定と PPPoE の接続

### STEP 4 各ホスト / サーバの設定

各ホスト / サーバの IP アドレス設定をおこないません。

ISP から提供された IP アドレス群の中から、重複しないように IP アドレスをそれぞれのホスト / サーバに割り当てます。

DNS アドレスは、XR の DNS サーバ機能が起動していれば XR の IP アドレスを(この設定例では、61.xxx.xxx.162)、起動していない場合は ISP から指定されたものを設定します。

またデフォルトゲートウェイは、61.xxx.xxx.162 に設定します。

### STEP 5 PPPoE 接続の開始

「PPP/PPPoE」->「接続設定」を開き、画面最下部にある「接続」ボタンをクリックして、PPPoE 接続を開始します。

ここで通常のインターネットアクセスや、外部からのアクセスができることを確認してください。

正常にアクセスできることが確認できましたら、続いて IPsec の設定をおこないます。

## IPsec の設定

### STEP 6 本装置側の設定

設定画面「各種サービスの設定」 「IPsec サーバ」 画面左側上部の「本装置の設定」を開きます。各項目には、以下のように入力します。

#### [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	<input type="text" value="61.xxx.xxx.161"/>
上位ルータのIPアドレス	<input type="text" value="%ppp0"/>
インターフェースのID	<input type="text" value=""/> (例:@x.centurysys)

インターフェースの IP アドレス  
「61.xxx.xxx.161」  
上位ルータの IP アドレス 「%ppp0」  
インターフェースの ID 「空欄」

入力後に「設定の保存」をクリックします。

#### [本装置の設定]

主回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ#0回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ#1回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ#4回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
バックアップ回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
Ether 0ポート使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
Ether 1ポート使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
NAT Traversalの設定	
NAT Traversal	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private設定	<input type="text" value=""/>
鍵の表示	
本装置のRSA鍵 (PSKを使用する場合は必要ありません)	<input type="text" value=""/>

MTU の設定 初期設定のまま  
NAT Traversal 「使用しない」  
Virtual Private 設定 「空欄」  
本装置の RSA 鍵 「空欄」

入力後に「設定の保存」をクリックします。

### STEP 7 IKE/ISAKMP ポリシーの設定

設定画面の「各種サービスの設定」 「IPsec サーバ」 画面左側上部の「IKE/ISAKMP ポリシーの設定」を開きます。ここでは「IKE1」で設定するものとします。

各項目には、以下のように入力します。

IKE/ISAKMPポリシー名	<input type="text" value=""/>
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	<input type="text" value="0.0.0.0"/>
上位ルータのIPアドレス	<input type="text" value=""/>
インターフェースのID	<input type="text" value="@ipsec"/> (例:@x.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-3des-sha1
	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 <input type="radio"/> RSAを使用する (X.509を使用する場合はRSAに設定してください)	<input type="text" value="ipseckey"/>
X.509の設定	
接続先の証明書の設定 (X.509を使用しない場合は必要ありません)	<input type="text" value=""/>

IKE/ISAKMP ポリシー名  
任意で入力してください(省略可)。半角英数字のみで設定可能です。

インターフェースの IP アドレス 「0.0.0.0」  
上位ルータの IP アドレス 「空欄」  
インターフェースの ID 「@ipsec」  
モードの設定 「aggressive モード」  
transform の選択 「group2-3des-sha1」  
IKE のライフタイム 「任意で設定」

鍵の設定  
「PSK を使用する」を選択し、「ipseckey」を入力します。

X.509 の設定 「空欄」

入力後に「設定の保存」をクリックします。

## IPsec の設定

### STEP 8 IPsec ポリシーの設定

設定画面の「各種サービスの設定」 「IPsec サーバ」 画面左側上部の「IPsec ポリシーの設定」を開きます。ここでは「IPsec1」で設定するものとします。

各項目には、以下のように入力します。

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" 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	61.xxx.xxx.160/29 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransformの選択	3des-sha1
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)	group2
SAのライフタイム	28800 秒 (1081~86400秒まで)

「Responderとして使用する」を選択

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

「61.xxx.xxx.160/29」

相手側の LAN 側のネットワークアドレス

「192.168.0.0/24」

PH2 の Transform の選択 「3des-sha1」

PFS 「使用する」

DH Group の選択 「group2」

SA のライフタイム 「任意で設定」

入力後に「設定の保存」をクリックします。

ここまでで、IPsec の設定は完了です。

続いて IPsec サーバの起動をおこないます。

### STEP 9 IPsec サーバの起動

IPsec 設定の完了後は IPsec サーバを起動します。

設定画面の「各種サービスの設定」を開き、「IPsec サーバ」項目で「起動」を選択し、画面下部の「動作変更」をクリックすることで、IPsec が起動します。

**IPsec 設定の詳細につきましては、「IPsec 設定ガイド」をご参照ください。**



## unnumbered 接続時の IPsec 設定ガイド

### 補足：対向側装置が XR-380/410/1000 の場合の IPsec 設定例

#### [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	<input type="text" value="%ppp0"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text" value="@ipsec"/> (例: @xr.centurysys)

インターフェースの IP アドレス 「%ppp0」

上位ルータの IP アドレス 「空欄」

インターフェースの ID 「@ipsec」

入力後に「設定の保存」をクリックします。

#### [本装置の設定]

主回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
マルチ回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
バックアップ回線使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
Ether 0ポート使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
Ether 1ポート使用時のipsec-インターフェースのMTU値	<input type="text" value="1500"/>
NAT Traversalの設定	
NAT Traversal	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private設定	<input type="text"/>
鍵の表示	
本装置のRSA鍵 (PSKを使用する場合は 必要ありません)	<input type="text"/>

MTUの設定 初期設定のまま

NAT Traversal 「使用しない」

Virtual Private設定 「空欄」

本装置のRSA鍵 「空欄」

#### [IKE/ISAKMP ポリシーの設定]

IKE/ISAKMPポリシー名	<input type="text"/>
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	<input type="text" value="0.0.0.0"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text" value="@ipsec"/> (例: @xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 <input type="text" value="group2-3des-sha1"/>
	2番目 <input type="text" value="使用しない"/>
	3番目 <input type="text" value="使用しない"/>
	4番目 <input type="text" value="使用しない"/>
IKEのライフタイム	<input type="text" value="3600"/> 秒 (1001~28800秒まで)
鍵の設定	
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する (X.509を使用する場合は RSAに設定してください)	<input type="text" value="ipseckey"/>
X.509の設定	
接続先の証明書の設定 (X.509を使用しない場合は 必要ありません)	<input type="text"/>

IKE/ISAKMP ポリシー名

任意で入力してください(省略可)。半角英数字のみで設定可能です。

インターフェースの IP アドレス

「61.xxx.xxx.161」

上位ルータの IP アドレス 「空欄」

インターフェースの ID 「空欄」

モードの設定 「aggressive モード」

transformの選択 「group2-3des-sha1」

IKEのライフタイム 「任意で設定」

鍵の設定

「PSKを使用する」を選択し、「ipseckey」を入力します。

X.509 の設定 「空欄」

## [ Ipsecポリシーの設定 ]

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" 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	61.xxx.xxx.160/29 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransformの選択	3des-sha1
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)	group2
SAのライフタイム	28800 秒 (1081~86400秒まで)

**「使用する」**を選択

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  
「192.168.0.0/24」

相手側の LAN 側のネットワークアドレス  
「61.xxx.xxx.160/29」

PH2 の Transform の選択 「3des-sha1」

PFS 「使用する」

DH Group の選択 「group2」

SA のライフタイム 「任意で設定」

unnumbered 接続 + IPsec 設定ガイド v1981

---

2003年6月版

発行 センチュリー・システムズ株式会社

2001-2003 CENTURYSYSTEMS, INC. All rights reserved.

---