BROADBAND GATE

インターネットVPN対応ブロードバンドルータ

FutureNet XR シリーズ

IPSec設定ガイド

センチュリー・システムズ 株式会社

本ガイドについて

本設定ガイドは、以下の製品に対応しています。

- XR-380、XR-380/DES Ver 1.2.0 以降
- XR-410 シリーズ　Ver 1.2.1 以降
- XR-440/C
- XR-640/CD
- XR-1000 シリーズ Ver.2.0 以降

XR シリーズの IPsec 機能について

◆鍵交換について
IKE を使用しています。IKE フェーズ 1 ではメインモード、アグレッシブモードの両方をサポートしています。フェーズ 2 ではクイックモードをサポートしています。
固定 IP アドレス同士の接続はメインモード、固定 IP アドレスと動的 IP アドレスの接続はアグレッシブモードで設定してください。

◆認証方式について
「共通鍵方式」と「RSA 公開鍵方式」、さらに「X.509」による認証に対応しています。ただしアグレッシブモードは「共通鍵方式」にのみ対応しています。

◆暗号化アルゴリズム
シングル DES とトリプル DES、AES をサポートしています。暗号化処理は以下のようになっています。
ハードウェア処理
　XR-380/DES、XR-410/TX2DES、XR-440/C
　XR-640/CD
ソフトウェア処理
　XR-380、XR-410/TX2、XR-410/TX4、XR-1000

◆ハッシュアルゴリズム
SHA1 と MD-5 を使用しています。

◆認証ヘッダ
ESP の認証機能を利用しています。AH での認証はおこなっていません。

◆DH 鍵共有アルゴリズムで使用するグループ
group1、group2、group5 をサポートしています。

◆ IPsec 使用時の接続可能拠点数
XR-380・XR-410 シリーズは最大 64 拠点(128 セッション)、XR-380/DES・XR-440/C・XR-640/CD は最大 128 拠点(256 セッション)、XR-1000 は 512 拠点(1024 セッション)まで接続可能です。

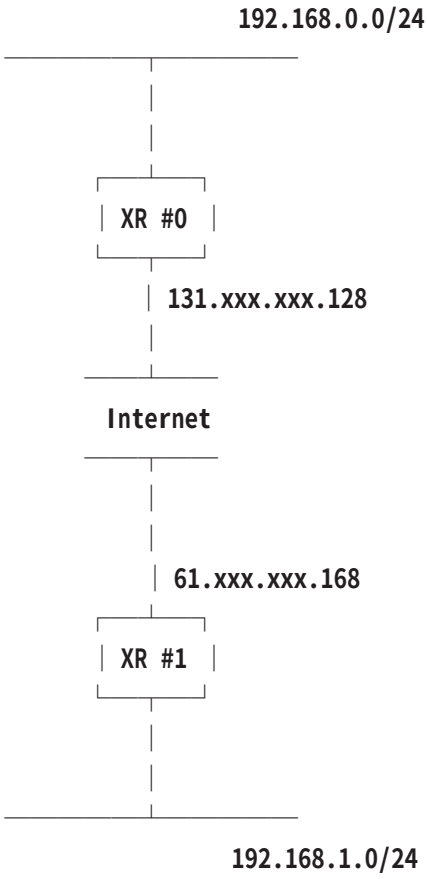
◆ IPsec とインターネット接続
IPsec 通信をおこなっている場合でも、その設定以外のネットワークへは、通常通りインターネットアクセスが可能です。

他の機器との接続実績について
他機種との接続実績につきましては、各製品のユーザーズガイドまたは弊社ホームページをご参照下さい。

XR シリーズ固定 IP 同士の IPSec 通信

ネットワーク構成

XR #0 と XR # 1 との間で IPsec トンネルを生成し、192.168.0.0/24 と 192.168.1.0/24 のネットワークをセキュアに通信可能とします。



接続条件

・RSA 公開鍵方式で認証します。

・main モードで接続します。

・XR #0 は PPPoE で接続します。

・XR #1 は、Ethernet 接続とします。

・XR #0、XR #1 ともに固定的に IP アドレスが割り当てられるものとします。

・XR #1 の上位ルータの IP アドレスは「61.xxx.xxx.160」とします

・その他の IP アドレスは図中の表記を使うものとします。

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「RSA 鍵の作成」で作成した公開鍵が表示されます。この鍵を対向側に通知します。

「本装置側の設定 1」

○インタフェースの IP アドレス 「131.xxx.xxx.128」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

インターフェースのIPアドレス	131.xxx.xxx.128
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 ポリシーの設定」

「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「61.xxx.xxx.168」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○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」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「RSA を使用する」を選択し、対向側から通知された公開鍵を入力します。

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	61.xxx.xxx.168
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	
○ PSKを使用する ◉ RSAを使用する	0sAQOhEET6kw9mEOzZx7KOZDq/xksIK2NNmGeA5O idpow+A9G5YD1io79OIutbryY80JQNvotXLGQB/E tsBVCIDdRx

「IPsec ポリシーの設定」

「IPsec1」を選択します。

○「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
「192.168.1.0/24」
○ PH2 の Transform の設定 「すべてを送信する」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「指定しない」
○ SA のライフタイム 「任意で設定」

◉ 使用する ○ 使用しない ○ Responderとして使用する	
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	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.1.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	◉ 使用する ○ 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)

◆XR #1 の設定

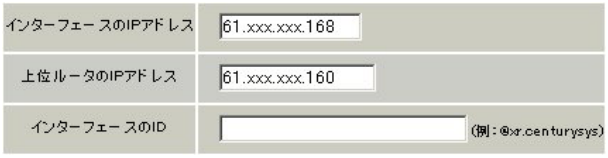
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「RSA 鍵の作成」で作成した公開鍵が表示されます。この鍵を対向側に通知します。

「本装置側の設定 1」

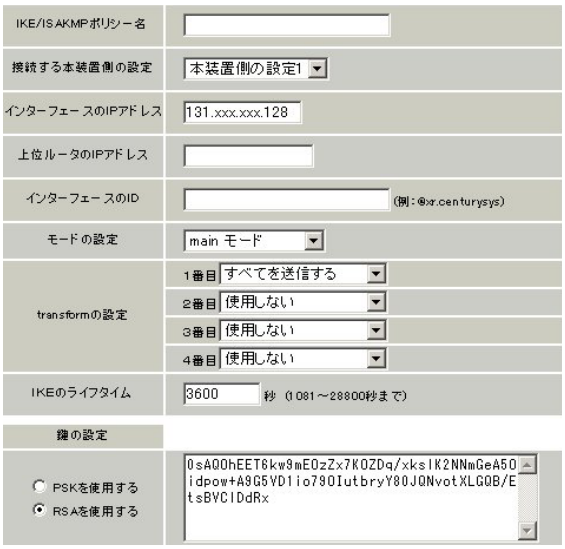
○インタフェースの IP アドレス 「61.xxx.xxx.168」
○上位ルーターの IP アドレス 「61.xxx.xxx.160」
○インタフェースの ID 「空欄」



「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

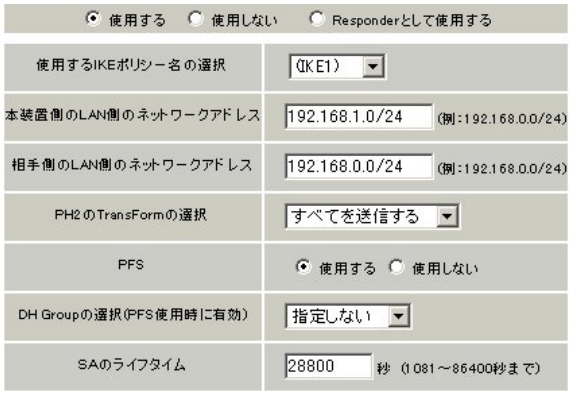
○IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「131.xxx.xxx.128」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「main モード」
○Transform の設定 1 番目「すべてを送信する」
2～4 番目は「使用しない」
○IKE のライフタイム 「任意で設定」
○鍵の表示 「RSA を使用する」を選択し、対向側から通知された公開鍵を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

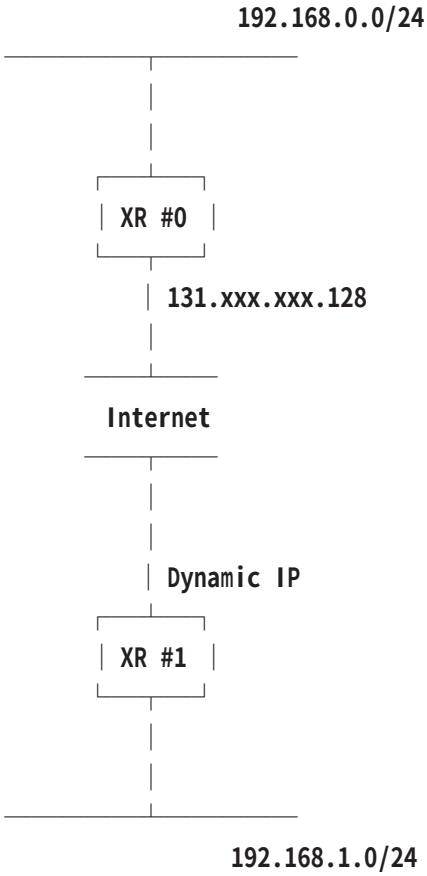
○「使用する」を選択
○使用する IKE ポリシー名の選択 「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○PH2 の Transform の設定 「すべてを送信する」
○PFS 「使用する」(推奨)
○DH Group の選択 「指定しない」
○SA のライフタイム 「任意で設定」



IPsec 設定ガイド
XR シリーズ固定 IP 1 ： XR シリーズ動的 IP 1 で IPSec 通信をおこなう (PPPoE 接続利用)

ネットワーク構成

XR #0 と XR # 1 との間で Ipsec トンネルを生成し、192.168.0.0/24 と 192.168.1.0/24 のネットワークをセキュアに通信可能とします。



接続環境(例)

・両 XR とも PPPoE で接続します。

・XR #0 には固定 IP アドレス、XR #1 には動的 IP アドレスが割り当てられるものとします。

・片側が動的 IP のため、aggressive モードで接続します。

・共通鍵方式で認証します。(aggressive モードは共通鍵方式のみ対応しています)

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

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
XR #1 の ID ： @ipsec

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

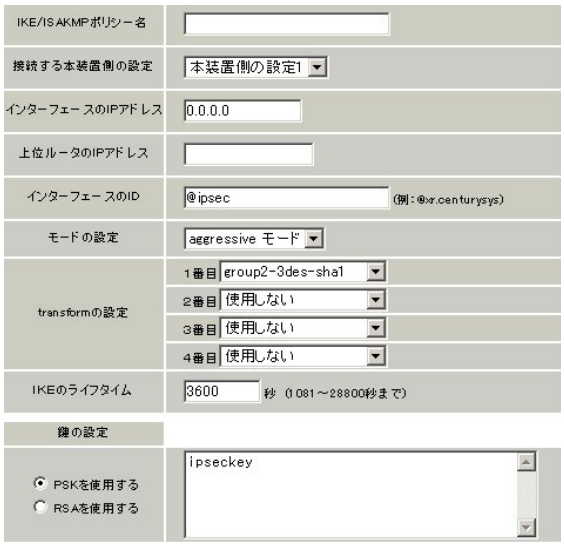
「本装置側の設定 1」

○インタフェースの IP アドレス 「131.xxx.xxx.128」
○上位ルーターの IP アドレス 「**%ppp0**」
○インタフェースの ID 「空欄」

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

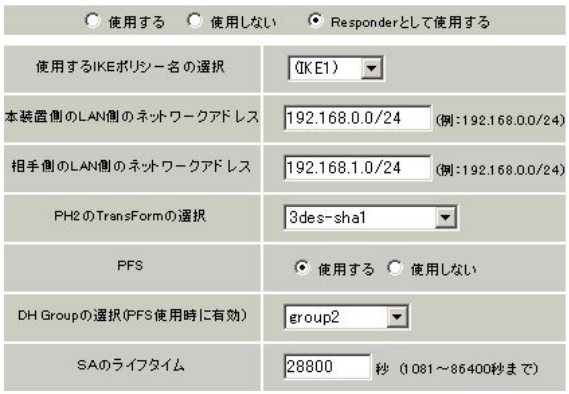
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「**本装置側の設定 1**」
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

○「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
「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



◆XR #1の設定

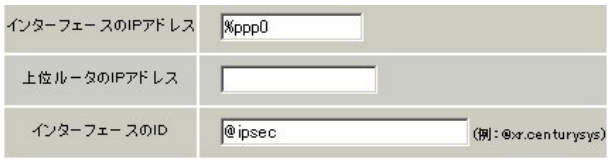
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTUの設定 必要に応じて設定します。
○NAT Traversalの設定 「使用しない」
○VirtualPrivate設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定1」

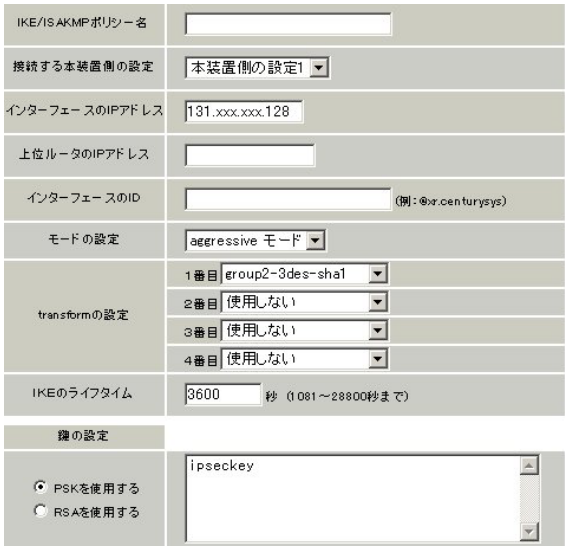
○インタフェースのIPアドレス 「%ppp0」
○上位ルーターのIPアドレス 「空欄」
○インタフェースのID 「@ipsec」



「IKE/ISAKMPポリシーの設定」

「IKE1」を選択します。

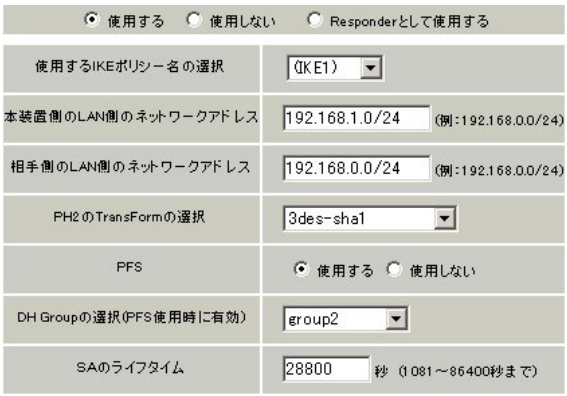
○ IKE/ISAKMPポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定1」
○インタフェースのIPアドレス 「131.xxx.xxx.128」
○上位ルーターのIPアドレス 「空欄」
○インタフェースのID 「空欄」
○モードの設定 「aggressiveモード」
○Transformの設定 1番目「group2-3des-sha1」
2～4番目は「使用しない」
○ IKEのライフタイム 「任意で設定」
○鍵の表示 「PSKを使用する」を選択し、「ipseckey」を入力します。



「IPsecポリシーの設定」

「IPsec1」を選択します。

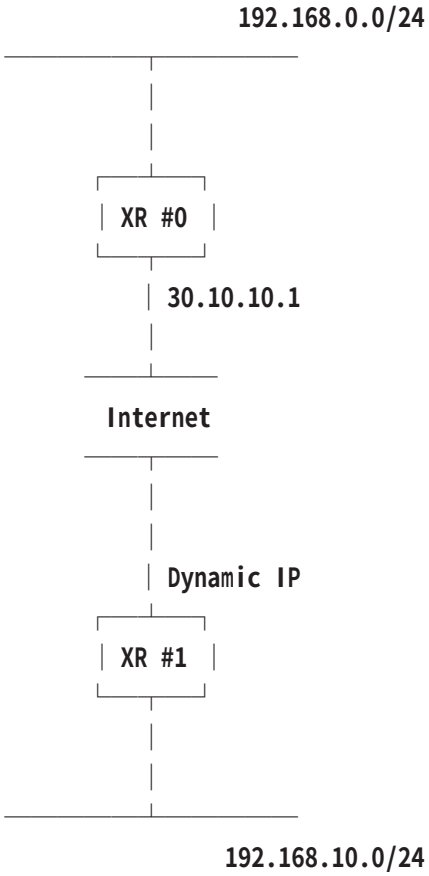
○「使用する」を選択
○使用するIKEポリシー名の選択 「IKE1」
○本装置側のLAN側のネットワークアドレス
「192.168.1.0/24」
○相手側のLAN側のネットワークアドレス
「192.168.0.0/24」
○PH2のTransformの設定 「3des-sha1」
○PFS 「使用する」(推奨)
○DH Groupの選択 「group2」
○SAのライフタイム 「任意で設定」



IPsec設定ガイド
XRシリーズ固定IP 1 ： XRシリーズ動的IP でIPSec通信をおこなう (Ethernet接続利用)

ネットワーク構成

XR #0 とXR # 1との間でIpsecトンネルを生成し、192.168.0.0/24 と192.168.1.0/24 のネットワークをセキュアに通信可能とします。



接続環境(例)

・XR #0 はPPPoE接続をおこないます。

・XR #1 はEthernet接続をおこないます。

・XR #0、#1 ともに、Ether1ポートをWAN側インタフェースとします。

・XR #0 には固定IPアドレス、XR #1 には動的IPアドレスが割り当てられるものとします。

・固定IP - 動的IP接続のため、aggressiveモードで接続します。

・共通鍵方式で認証します。(aggressiveモードは共通鍵方式のみ対応しています)

・IPアドレス等は図中の表記を使うものとします。

・IPsec設定で使用するパラメータ値は以下の通りとします。

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
XR #1のID ： @branch

◆XR #0 の設定

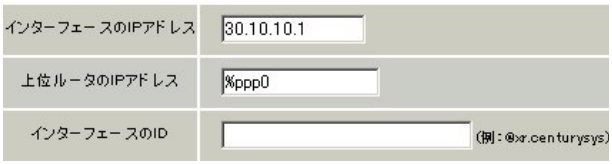
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

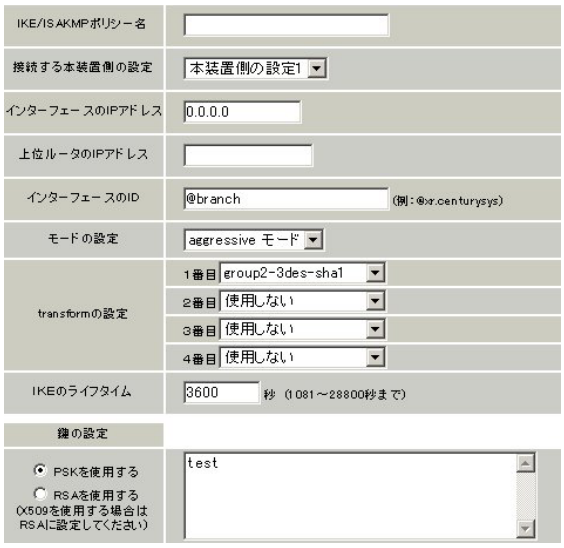
○インタフェースの IP アドレス 「30.10.10.1」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」



「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

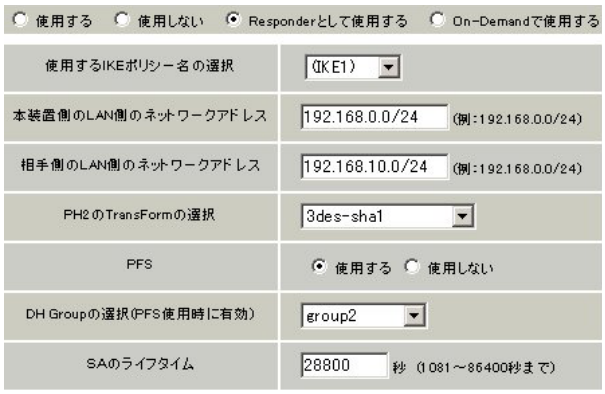
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@branch」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「test」
を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

○「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
「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.10.0/24」
○ PH2 の Transform の設定 「すべてを送信」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「指定しない」
○ SA のライフタイム 「任意で設定」



◆XR #1 の設定

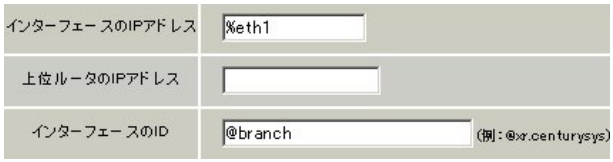
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

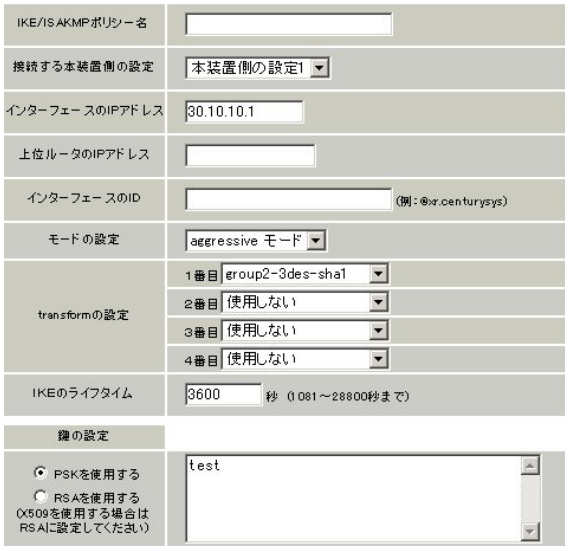
○インタフェースの IP アドレス 「**%eth1**」
○上位ルーターの IP アドレス 「**空欄**」
○インタフェースの ID 「@branch」



「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

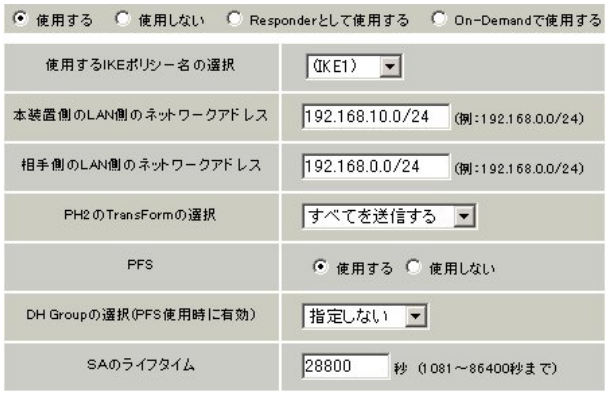
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「**本装置側の設定 1**」
○インタフェースの IP アドレス 「30.10.10.1」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「test」を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

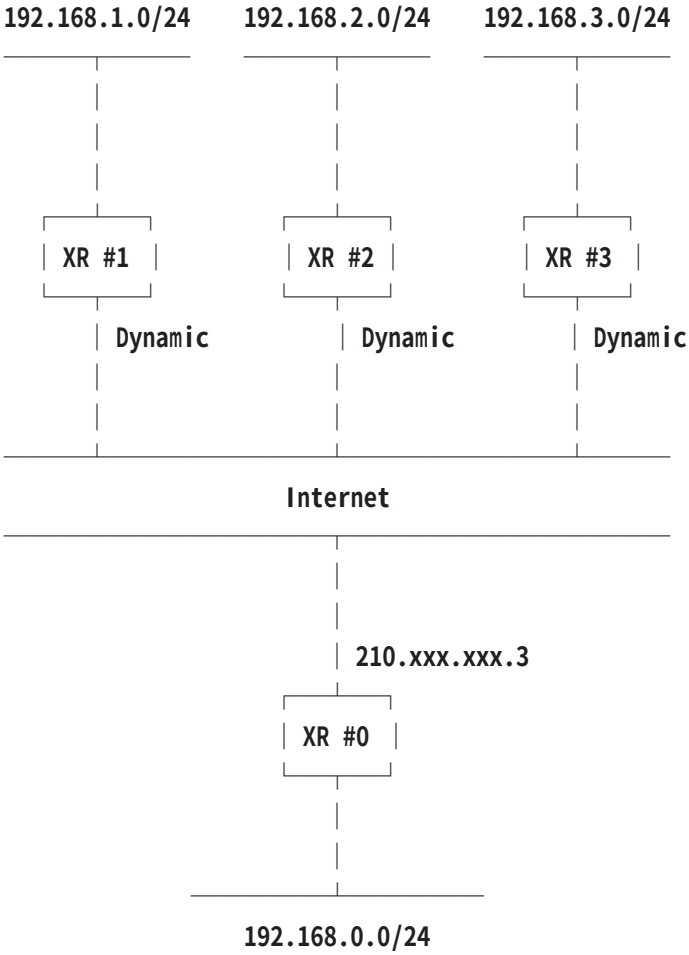
○「使用する」を選択
○使用する IKE ポリシー名の選択 「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.10.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



IPsec 設定ガイド
XR シリーズ固定 IP 1 ： XR シリーズ動的 IP 3 で IPSec 通信をおこなう (PPPoE 接続利用)

ネットワーク構成

XR #0 と XR # 1、# 2、# 3 との間で Ipsec トンネルを生成し、192.168.0.0/24 と 192.168.1.0/24、.2.0/24、.3.0/24 のネットワークをセキュアに通信可能とします。



接続環境(例)

・両 XR とも PPPoE で接続します。

・XR #0 には固定 IP アドレス、XR #1～#3 には動的 IP アドレスが割り当てられるものとします。

・片側が動的 IP のため、aggressive モードで接続します。

・共通鍵方式で認証します。(aggressive モードは共通鍵方式のみ対応しています)

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

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
XR #1 の ID ： @ipsec1
XR #2 の ID ： @ipsec2
XR #3 の ID ： @ipsec3

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

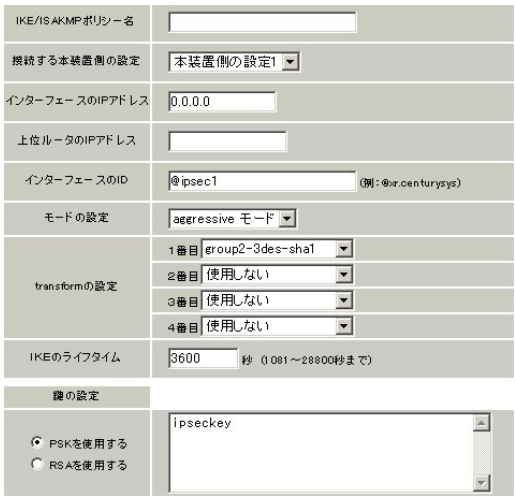
「本装置側の設定 1」

○インタフェースの IP アドレス 「210.xxx.xxx.3」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

「IKE/ISAKMP ポリシーの設定」(XR #1 向けの設定)

「IKE1」を選択します。

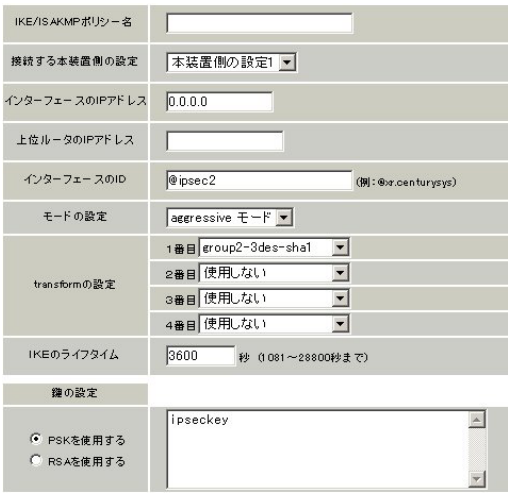
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec1」
○モードの設定 「aggressive モード」
○Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



「IKE/ISAKMP ポリシーの設定」(XR #2 向けの設定)

「IKE2」を選択します。

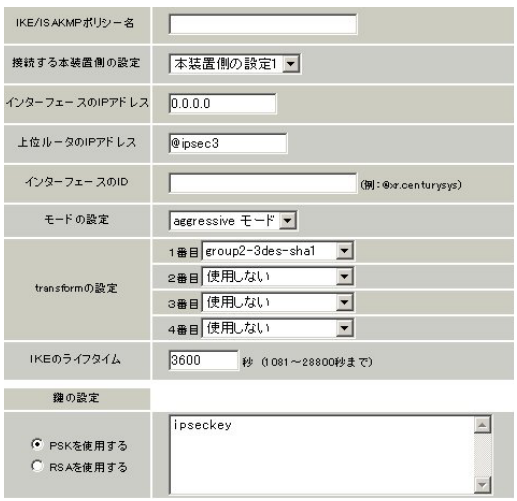
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec2」
○モードの設定 「aggressive モード」
○Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



「IKE/ISAKMP ポリシーの設定」(XR #3 向けの設定)

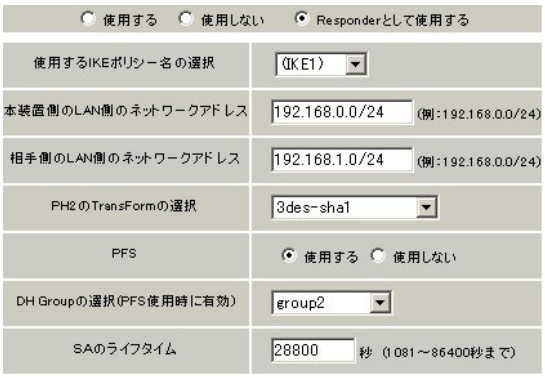
「IKE3」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec3」
○モードの設定 「aggressive モード」
○Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



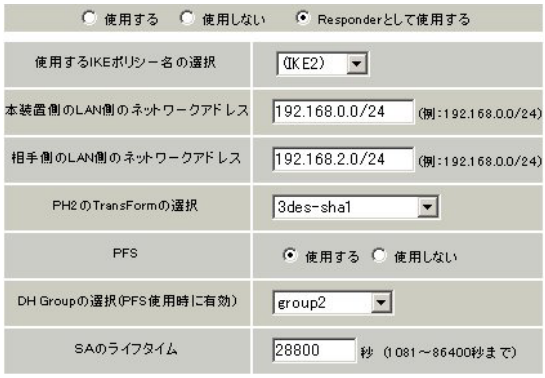
「IPsec ポリシーの設定」(XR　#1 向け設定)
「IPsec1」を選択します。

○「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
「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



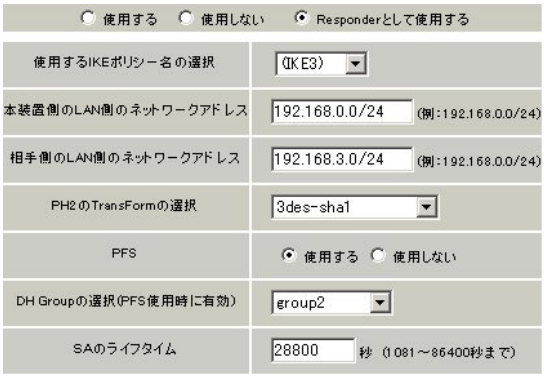
「IPsec ポリシーの設定」(XR　#2 向け設定)
「IPsec2」を選択します。

○「Responder として使用する」を選択
○使用する IKE ポリシー名の選択　「IKE2」
○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
「192.168.2.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



「IPsec ポリシーの設定」(XR　#3 向け設定)
「IPsec1」を選択します。

○「Responder として使用する」を選択
○使用する IKE ポリシー名の選択　「IKE3」
○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
「192.168.3.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



◆XR #1 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

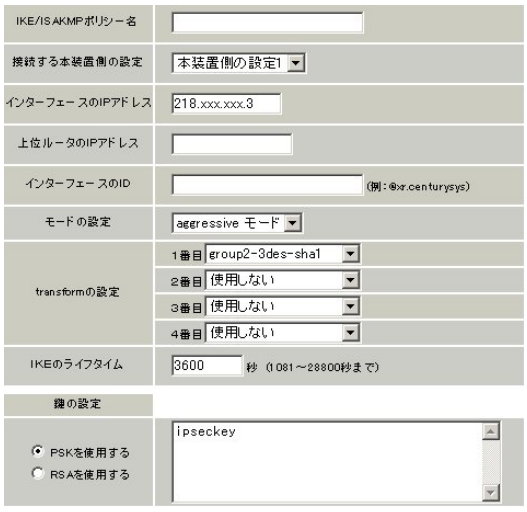
○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

○インタフェースの IP アドレス 「%ppp0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec1」

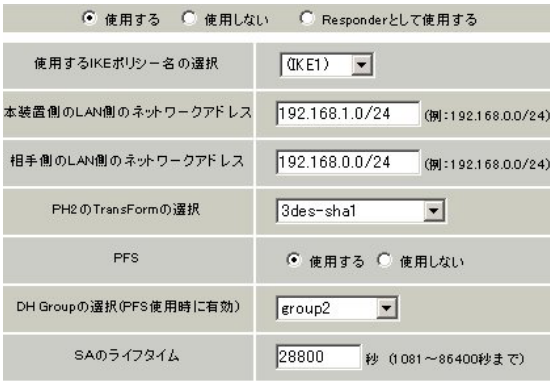
「IKE/ISAKMP ポリシーの設定」(XR #0 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「**本装置側の設定 1**」
○インタフェースの IP アドレス 「218.xxx.xxx.3」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」(XR #0 向けの設定)
「IPsec1」を選択します。

○「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
「192.168.1.0/24」
○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 の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



◆XR #2 の設定

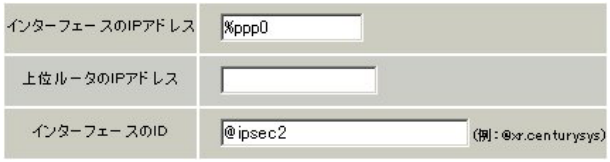
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

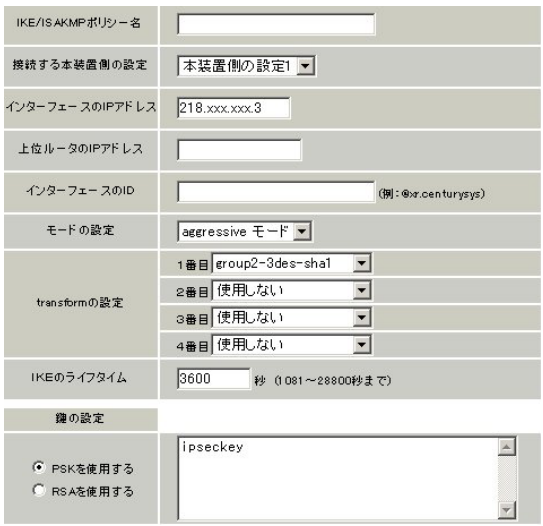
「本装置側の設定 1」

○インタフェースの IP アドレス **「%ppp0」**
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec2」



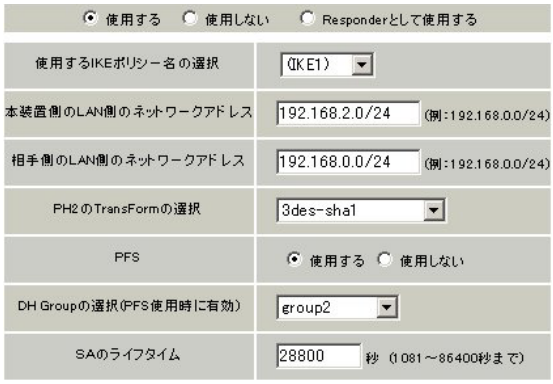
「IKE/ISAKMP ポリシーの設定」(XR #0 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「218.xxx.xxx.3」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」(XR #0 向けの設定)
「IPsec1」を選択します。

○「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
「192.168.2.0/24」
○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 の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



◆XR #3 の設定

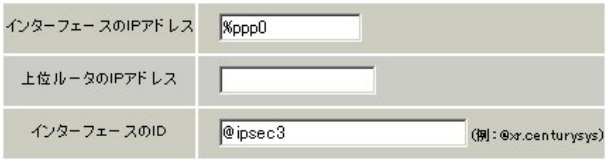
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

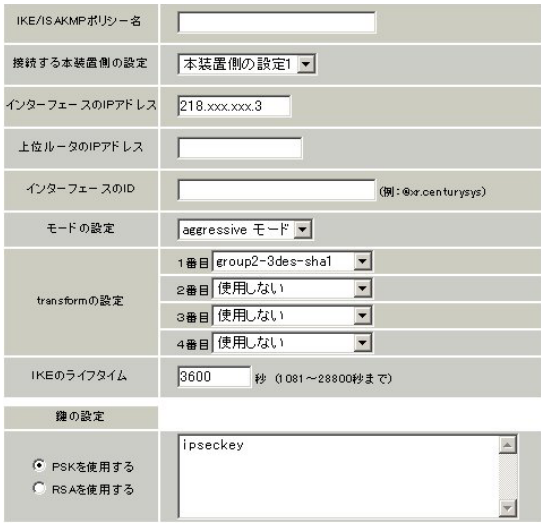
「本装置側の設定 1」

○インタフェースの IP アドレス 「%ppp0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec3」



「IKE/ISAKMP ポリシーの設定」(XR #0 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「218.xxx.xxx.3」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



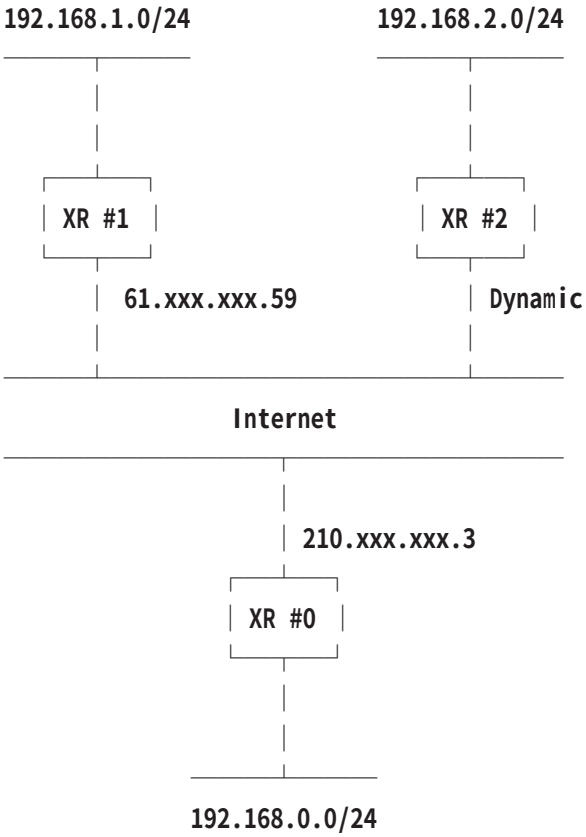
「IPsec ポリシーの設定」(XR #0 向けの設定)
「IPsec1」を選択します。

○「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
「192.168.3.0/24」
○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 の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」

IPsec 設定ガイド
XR シリーズ固定 IP 1 ： XR シリーズ固定 IP 1 ： XR シリーズ動的 IP 1 で IPSec 通信をおこなう(Mesh 接続)

ネットワーク構成

すべての XR 間で IPsec トンネルを生成して、192.168.0.0/24、.1.0/24、.2.0/24 のネットワーク同士がセキュアに通信可能とします。



接続環境(例)

・全ての XR とも PPPoE で接続します。

・XR #0、#1 には固定 IP アドレス、XR #2 には動的 IP アドレスが割り当てられるものとします。

・XR #0 - XR #1 間は main モード、XR #0 - XR #2 間は aggressive モードで接続します。

・全て共通鍵方式で認証します。(aggressive モードは共通鍵方式のみ対応しています)

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

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
XR #2 の ID ： @ipsec

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

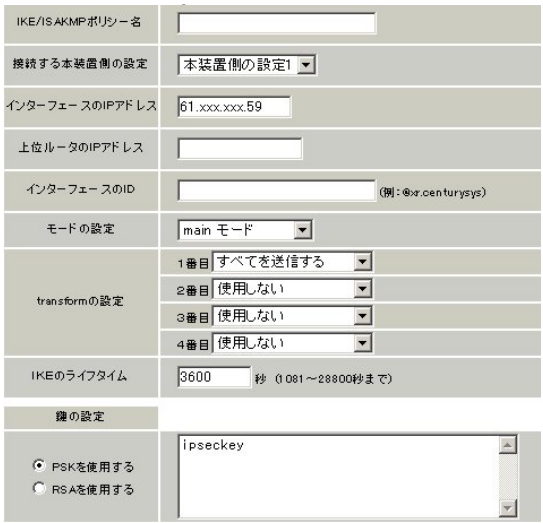
○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

○インタフェースの IP アドレス 「210.xxx.xxx.3」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

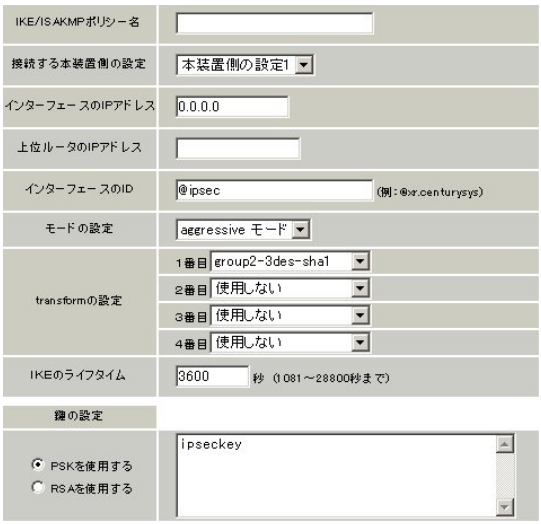
「IKE/ISAKMP ポリシーの設定」(XR #1 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「61.xxx.xxx.59」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○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」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」



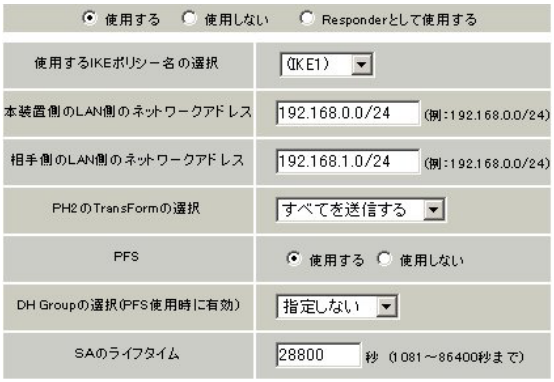
「IKE/ISAKMP ポリシーの設定」(XR #2 向けの設定)
「IKE2」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



「IPsec ポリシーの設定」(XR　#1 向け設定)
「IPsec1」を選択します。

○「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
「192.168.1.0/24」
○ PH2 の Transform の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」



「IPsec ポリシーの設定」(XR #2 向け設定)
「IPsec2」を選択します。

○「Responder として使用する」を選択
○使用する IKE ポリシー名の選択　「IKE2」
○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
「192.168.2.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」

◆XR #1 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

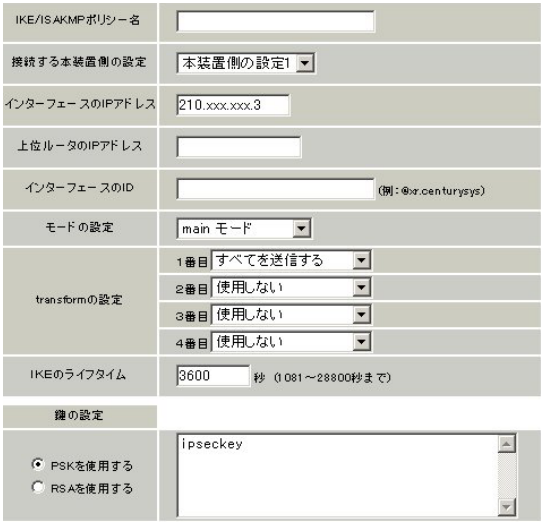
○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

○インタフェースの IP アドレス 「61.xxx.xxx.59」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

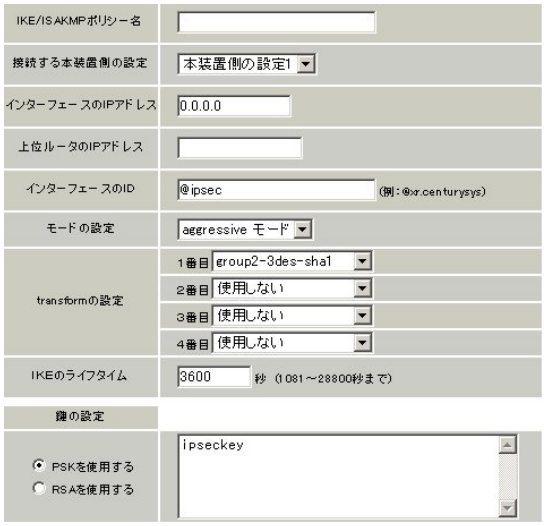
「IKE/ISAKMP ポリシーの設定」(XR #0 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「210.xxx.xxx.3」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○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」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



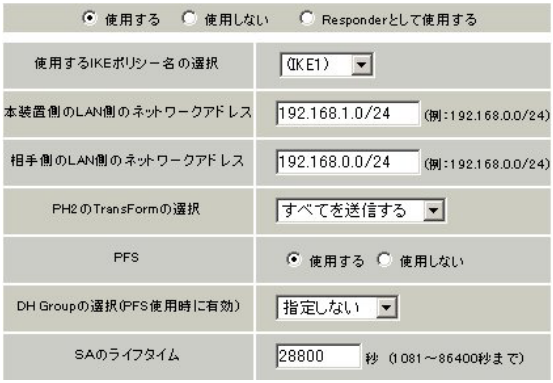
「IKE/ISAKMP ポリシーの設定」(XR #2 向けの設定)
「IKE2」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」
を入力します。



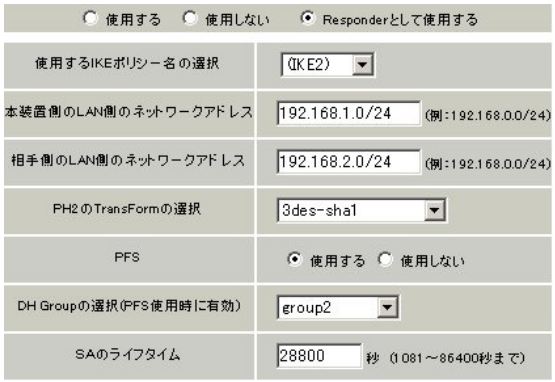
「IPsec ポリシーの設定」(XR　#0 向け設定)
「IPsec1」を選択します。

○「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
「192.168.1.0/24」
○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 の設定　「すべてを送信する」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「指定しない」
○ SA のライフタイム　「任意で設定」



「IPsec ポリシーの設定」(XR #2 向け設定)
「IPsec2」を選択します。

○「Responder として使用する」を選択
○使用する IKE ポリシー名の選択　「IKE2」
○本装置側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.2.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



◆XR #2 の設定

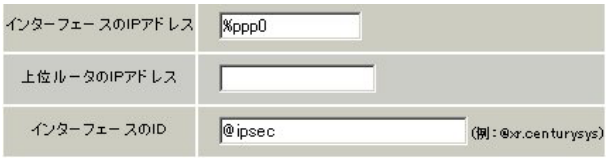
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

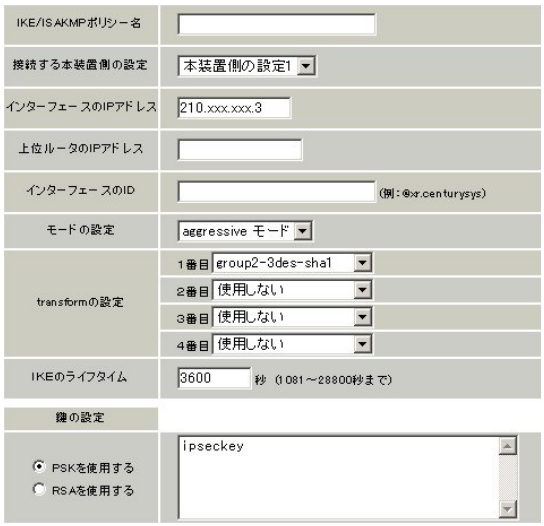
「本装置側の設定 1」

○インタフェースの IP アドレス 「%ppp0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」



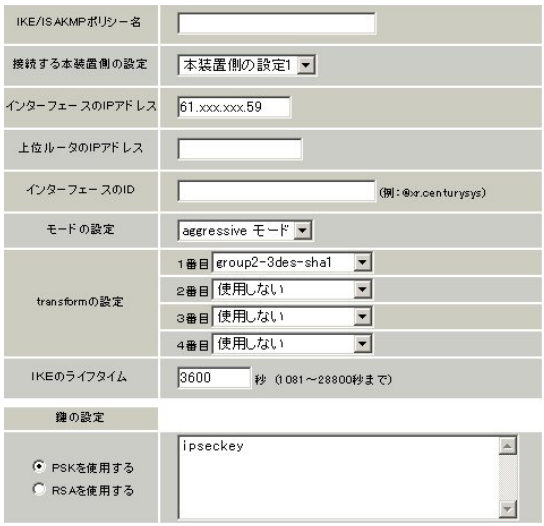
「IKE/ISAKMP ポリシーの設定」(XR #0 向けの設定)
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「210.xxx.xxx.3」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



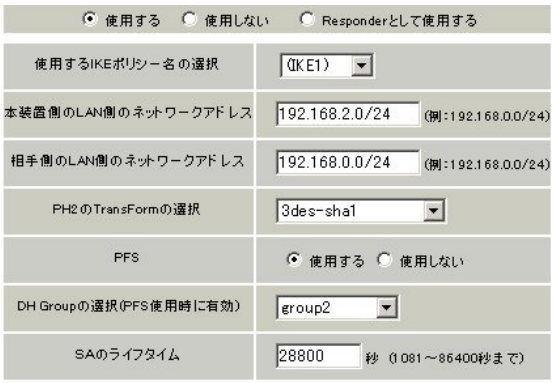
「IKE/ISAKMP ポリシーの設定」(XR #1 向けの設定)
「IKE2」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「61.xxx.xxx.59」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



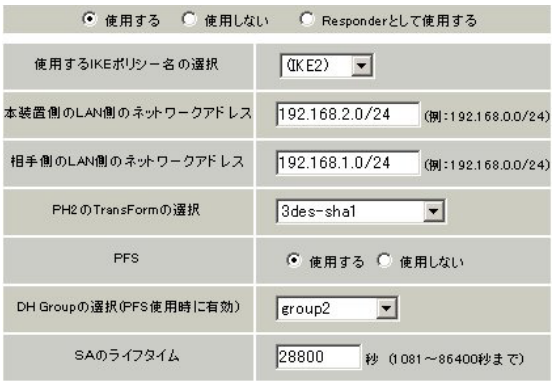
「IPsec ポリシーの設定」(XR　#0 向け設定)
「IPsec1」を選択します。

○「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
「192.168.2.0/24」
○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 の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



「IPsec ポリシーの設定」(XR #1 向け設定)
「IPsec2」を選択します。

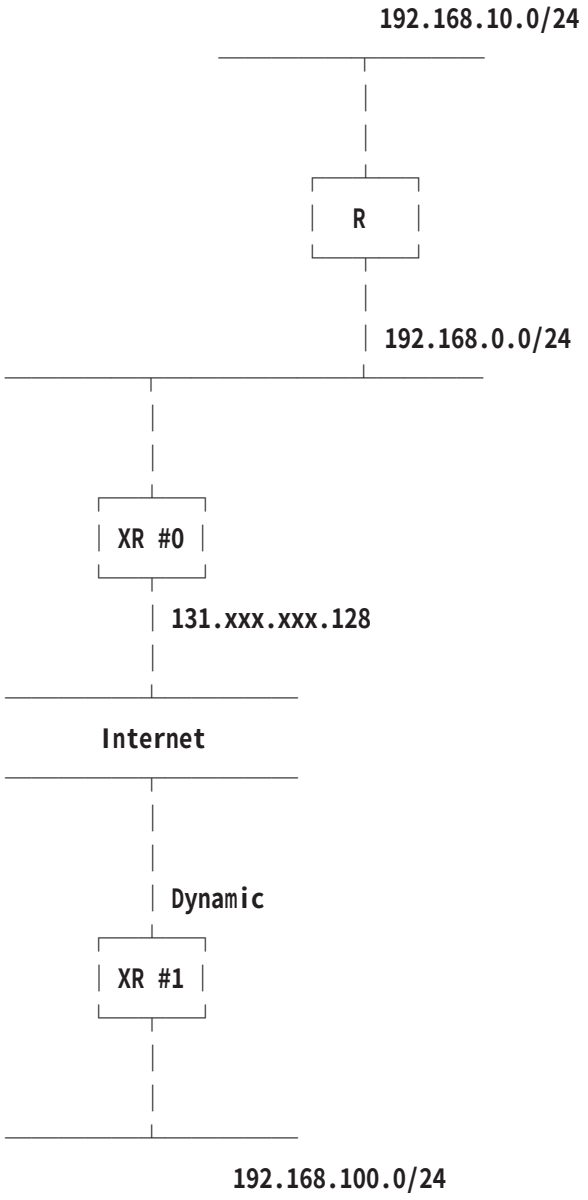
○「使用する」を選択
○使用する IKE ポリシー名の選択　「IKE2」
○本装置側の LAN 側のネットワークアドレス
「192.168.2.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○ PH2 の Transform の設定　「3des-sha1」
○ PFS　「使用する」(推奨)
○ DH Group の選択　「group2」
○ SA のライフタイム　「任意で設定」



複数セグメントを持つ拠点間での IPsec 接続

ネットワーク構成

すべての XR シリーズ間で Ipsec トンネルを生成し、192.168.0.0/24、.10.0/24 のネットワークと .100.0/24のネットワーク同士がセキュアに通信可能とします。



接続環境(例)

・XR #0 には固定 IP アドレス、XR #1 には動的 IP アドレスが割り当てられるものとします。

・片側が動的 IP のため、aggressive モードで接続します。

・共通鍵方式で認証します。(aggressive モードは共通鍵方式のみ対応しています)

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

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
XR #1 の ID ： @ipsec

・「192.168.0.0/24」と「192.168.10.0/24」間ではあらかじめルーティング設定をしておきます。

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

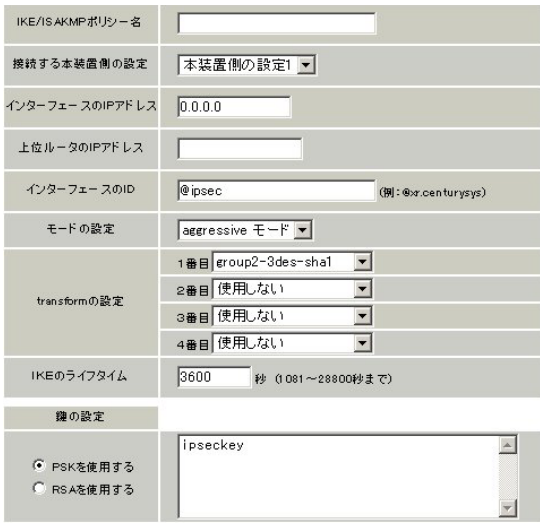
「本装置側の設定 1」

○インタフェースの IP アドレス 「131.xxx.xxx.128」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

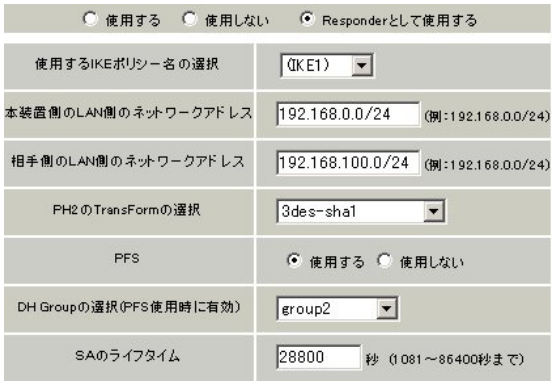
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

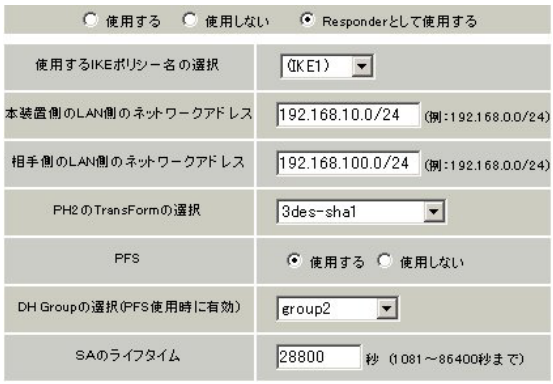
○「Responder として使用する」を選択
○使用する IKE ポリシー名の選択 「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.100.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



「IPsec ポリシーの設定」(XR #2 向け設定)

「IPsec2」を選択します。

○「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
「192.168.10.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.100.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



◆XR #1 の設定

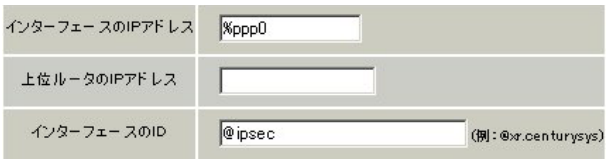
各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「空欄」

「本装置側の設定 1」

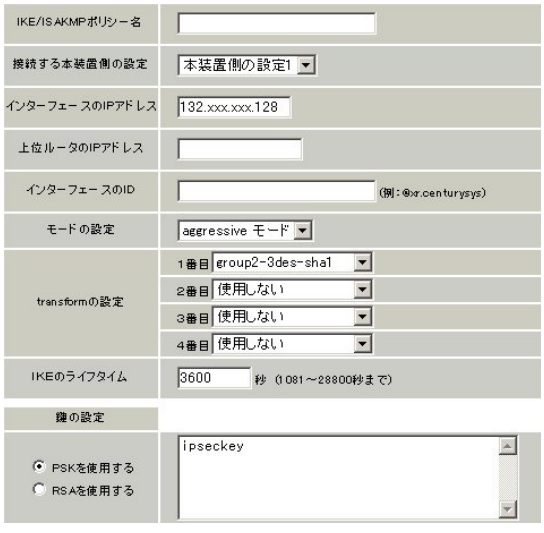
○インタフェースの IP アドレス 「%ppp0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」



「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

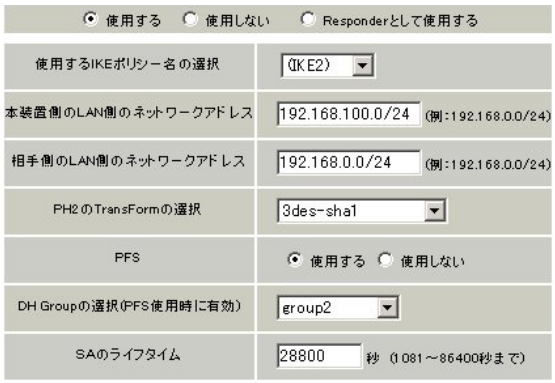
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 **「本装置側の設定 1」**
○インタフェースの IP アドレス 「132.xxx.xxx.128」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

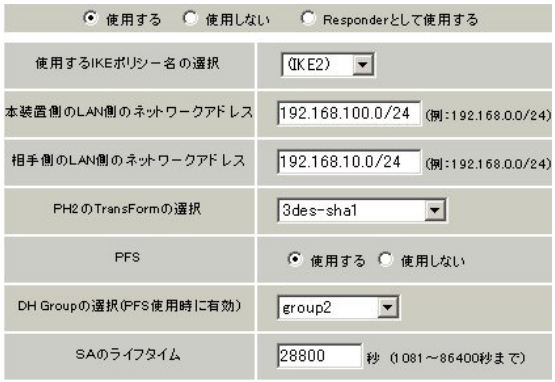
○「使用する」を選択
○使用する IKE ポリシー名の選択 「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.100.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



「IPsec ポリシーの設定」(XR #2 向け設定)

「IPsec2」を選択します。

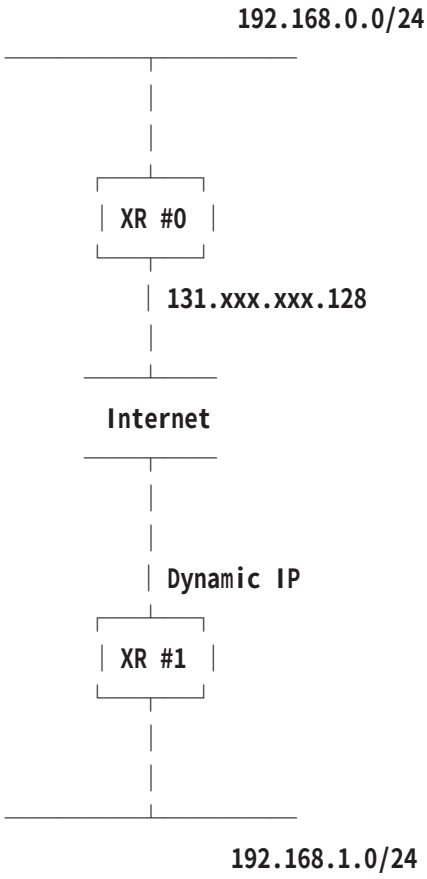
○「使用する」を選択
○使用する IKE ポリシー名の選択 「IKE1」
○本装置側の LAN 側のネットワークアドレス
「192.168.100.0/24」
○相手側の LAN 側のネットワークアドレス
「192.168.10.0/24」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」



すべてのアクセスをセンター経由でおこなう IPsec 接続

ネットワーク構成

XR 間で Ipsec トンネルを生成し、192.168.0.0/24、.10.0/24 と 192.168.10.0/24 のネットワーク同士がセキュアに通信可能とします。
さらに、192.168.1.0/24 のネットワークからのインターネットアクセスはすべて、センター側 XR を経由するようにします。



※192.168.1.0/24 からの通常のインターネットアクセスは、IPsec -> センター側 XR を経由しておこなわれます。

接続環境(例)

・XR #0 には固定 IP アドレス、XR #1 には動的 IP アドレスが割り当てられるものとします。

・片側が動的 IP のため、aggressive モードで接続します。

・共通鍵方式で認証します。(aggressive モードは共通鍵方式のみ対応しています)

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

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
XR #1 の ID ： @ipsec

◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○MTU の設定 必要に応じて設定します。
○NAT Traversal の設定 「使用しない」
○VirtualPrivate 設定 「空欄」
○鍵の表示 「RSA 鍵の作成」で作成した公開鍵が表示されます。この鍵を対向側に通知します。

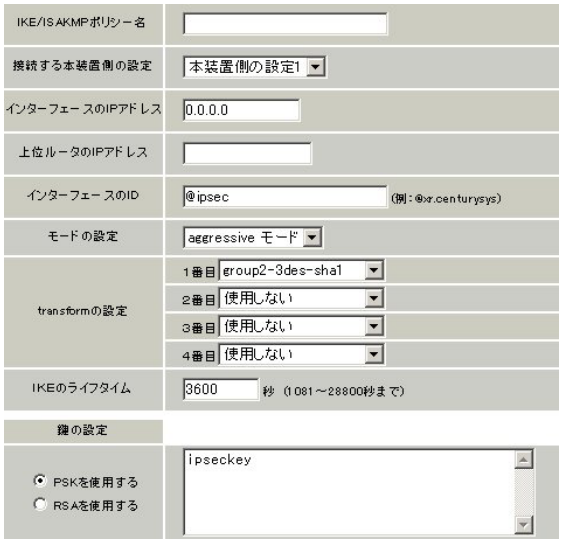
「本装置側の設定 1」

○インタフェースの IP アドレス 「131.xxx.xxx.128」
○上位ルーターの IP アドレス 「%ppp0」
○インタフェースの ID 「空欄」

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

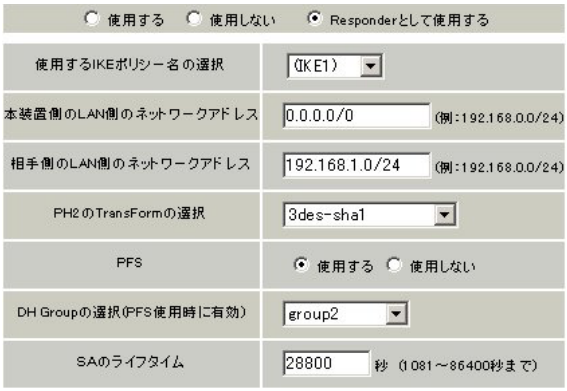
○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「本装置側の設定 1」
○インタフェースの IP アドレス 「0.0.0.0」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」
○モードの設定 「aggressive モード」
○Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。



「IPsec ポリシーの設定」

「IPsec1」を選択します。

○「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
「0.0.0.0/0」
○相手側の LAN 側のネットワークアドレス
「192.168.1.0/24」
○PH2 の Transform の設定 「3des-sha1」
○PFS 「使用する」(推奨)
○DH Group の選択 「group2」
○SA のライフタイム 「任意で設定」



◆XR #0 の設定

各設定画面で、以下のように入力・設定します。

「本装置の設定」

○ MTU の設定 必要に応じて設定します。
○ NAT Traversal の設定 「使用しない」
○ VirtualPrivate 設定 「空欄」
○鍵の表示 「RSA 鍵の作成」で作成した公開鍵が表示されます。この鍵を対向側に通知します。

「本装置側の設定 1」

○インタフェースの IP アドレス 「**%ppp0**」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「@ipsec」

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	
インターフェースのID	@ipsec (例：@xr.centurysys)

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「任意で入力」
○接続する本装置側の設定 「**本装置側の設定 1**」
○インタフェースの IP アドレス 「**131.xxx.xxx.128**」
○上位ルーターの IP アドレス 「空欄」
○インタフェースの ID 「空欄」
○モードの設定 「aggressive モード」
○ Transform の設定 1 番目「group2-3des-sha1」
2～4 番目は「使用しない」
○ IKE のライフタイム 「任意で設定」
○鍵の表示 「PSK を使用する」を選択し、「ipseckey」を入力します。

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	131.xxx.xxx.128
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	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	
○ PSKを使用する ○ RSAを使用する	ipseckey

「IPsec ポリシーの設定」

「IPsec1」を選択します。

○「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
「192.168.1.0/24」
○相手側の LAN 側のネットワークアドレス
「**0.0.0.0/0**」
○ PH2 の Transform の設定 「3des-sha1」
○ PFS 「使用する」(推奨)
○ DH Group の選択 「group2」
○ SA のライフタイム 「任意で設定」

○ 使用する ○ 使用しない ○ Responderとして使用する	
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	192.168.1.0/24 (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	3des-sha1
PFS	○ 使用する ○ 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)

「X.509 デジタル証明書」を用いた電子認証

XR-380、410 は X.509 デジタル証明書を用いた電子認証方式に対応しています。

ただし XR-380、410 は証明書署名要求の発行や証明書の発行ができませんので、あらかじめ CA 局から証明書の発行を受けておく必要があります。

電子証明の仕組みや証明書発行の詳しい手順につきましては関連書籍等をご参考下さい。

情報処理振興事業協会セキュリティセンター
http://www.ipa.go.jp/security/pki/

設定は、IPsec 設定画面内の「X.509 の設定」から行います。

[X.509 の設定]
「X.509 の設定」画面→「X.509 の設定」を開きます。

○ X509 の設定
X.509 の使用 / 不使用を選択します。

○証明書のパスワード
証明書のパスワードを入力します。

[CA の設定]
ここには、CA 局自身のデジタル証明書の内容をコピーして貼り付けます(「cacert.pem」ファイル等)。

[本装置側の証明書の設定]
ここには、本装置に対して発行されたデジタル証明書の内容をコピーして貼り付けます。

[本装置側の鍵の設定]
ここにはデジタル証明書と同時に発行された、本装置の秘密鍵の内容をコピーして貼り付けます(「cakey.pem」ファイル等)。

[接続先側の設定]
ここには、IPsec 接続先の装置に対して発行された証明書の内容をコピーして貼り付けます。接続先から証明書を入手してください。

[失効リストの設定]
失効リストを作成している場合は、その内容をコピーして貼り付けます(「crl.pem」ファイル等)。

[その他の設定について]
その他の設定については、通常の IPsec 設定と同様にしてください。

その際、「IKE/ISAKMAP ポリシーの設定」画面内の鍵の設定項目は「RSA を使用する」にチェックします。鍵は空欄のままにします(「本装置の設定」画面の鍵表示も空欄のままです)。

以上で X.509 の設定は完了です。

◆設定のバックアップ保存について
設定のバックアップを作成しても、X.509 関連の設定は含まれません。またパラメータによる設定にも反映されません。

バックアップファイルから設定を復帰させる場合でも、X.509 関連の設定は再度おこなってください。

IPsec Keep-Alive 機能

通常の IPsec 通信では、たとえ対向側の回線に障害が発生して IPsec 通信が出来なくなったとしても、それを判断することが出来ずに IPsec トンネルをそのまま保持し続けてしまいます。

このため見かけ上では IPsec が確立しているように見えていますが、実際には IPsec 通信は不可能となります。さらに IPsec が再接続するためには、SA のライフタイムが切れるまで待たなければなりません。

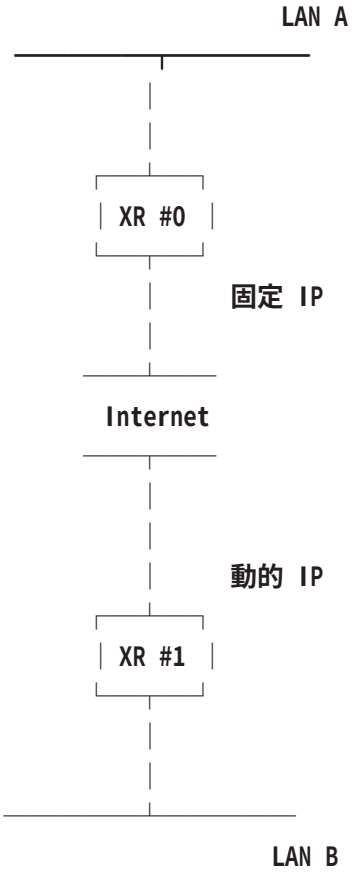
このような不都合を解消するために IPsec Keep-Alive 機能を使用します。

IPsec Keep-Alive 機能は、指定した宛先へ IPsec トンネル経由で ping パケットを発行して応答がない場合に IPsec トンネルに障害が発生したと判断し、その IPsec トンネルを自動的に削除する機能です。

不要な IPsec トンネルを自動的に削除することで、IPsec の再接続性を高めます。

この機能は固定 IP - 動的 IP の IPsec 接続環境において、動的 IP 側で設定・運用することで最も効果を発揮します。

動作の流れ



XR #1 で IPsec Keep-Alive 機能を有効にして IPsec 通信を行っているときに、XR #0 側の回線に障害が発生して通信不可に陥ったとします。

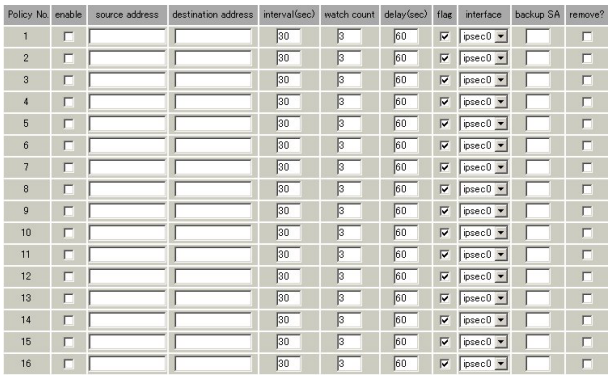
このとき XR #1 の Keep-Alive 機能が働き、XR #0 に対しての IPsec トンネルの保持が無効と判断します。

すると XR #1 は、自身が保持している XR #0 への IPsec トンネルを自動的に削除します。

IPsec トンネルが削除されると、XR #1 はただちに IPsec の再接続を試みます(XR #1 は動的 IP ＝ initiator になっているため)。

設定方法

IPsec 設定画面上部の「IPsecKeep-Alive 設定」をクリックして設定します。



Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
1	☐			30	3	60	☑	ipsec0		☐
2	☐			30	3	60	☑	ipsec0		☐
3	☐			30	3	60	☑	ipsec0		☐
4	☐			30	3	60	☑	ipsec0		☐
5	☐			30	3	60	☑	ipsec0		☐
6	☐			30	3	60	☑	ipsec0		☐
7	☐			30	3	60	☑	ipsec0		☐
8	☐			30	3	60	☑	ipsec0		☐
9	☐			30	3	60	☑	ipsec0		☐
10	☐			30	3	60	☑	ipsec0		☐
11	☐			30	3	60	☑	ipsec0		☐
12	☐			30	3	60	☑	ipsec0		☐
13	☐			30	3	60	☑	ipsec0		☐
14	☐			30	3	60	☑	ipsec0		☐
15	☐			30	3	60	☑	ipsec0		☐
16	☐			30	3	60	☑	ipsec0		☐

○ enable
設定を有効にする時にチェックします。IPsec Keep-Alive 機能を使いたい IPsec ポリシーと同じ番号にチェックを入れます。

○ source address
IPsec 通信を行う際の、XR の LAN 側インターフェースの IP アドレスを入力します。

○ destination address
IPsec 通信を行う際の、XR の対向側装置の LAN 側のインターフェースの IP アドレスを入力します。

source address、destination address ともに”0.0.0.0”を指定すると、本装置と対向側装置の WAN 側 IP アドレスを自動的に設定して動作するようになります。この設定により、本装置の WAN 側 IP アドレス - 対向側装置の WAN 側 IP アドレス間で IPsecKeepAlive 監視をおこなえるようになります。

○ interval(sec)
○ watch count
ping を発行する間隔を設定します。
「『interval(sec)』間に『watch count』回 ping を発行する」という設定になります。

○ delay(sec)
IPsec が起動してから ping を発行するまでの待ち時間を設定します。IPsec が確立するまでの時間を考慮して設定します。

○ flag
チェックを入れると、delay 後に ping を発行して、ping が失敗したら即座に指定された IPsec トンネルの削除、再折衝を開始します。また Keep-Alive によって SA 削除後は、毎回 delay 時間待ってから Keep-Alive が開始されます。
チェックはずすと、delay 後に最初に ping が成功(IPsec が確立)し、その後に ping が失敗してはじめて指定された IPsec トンネルの削除、再折衝を開始します。IPsec が最初に確立する前に ping が失敗してもなにもしません。また delay は初回のみ発生します。

○インタフェース
Keep-Alive 機能を使う、本装置の IPsec インタフェース名を選択もしくは入力します。

○ backup SA
ここに IPsec ポリシーの設定番号を指定しておくと、IPsec Keepalaive 機能で IPsec トンネルを削除した時に、ここで指定したポリシー設定を起動させます。

○ remove
設定を削除したいときにチェックします。

最後に「設定 / 削除の実行」をクリックしてください。remove 項目にチェックが入っているものについては、その設定が削除されます。

設定番号について

IPsec Keep-Alive 機能を使う際は、監視する IPsec のポリシー No. と Keepalive の No. は一致させてください。

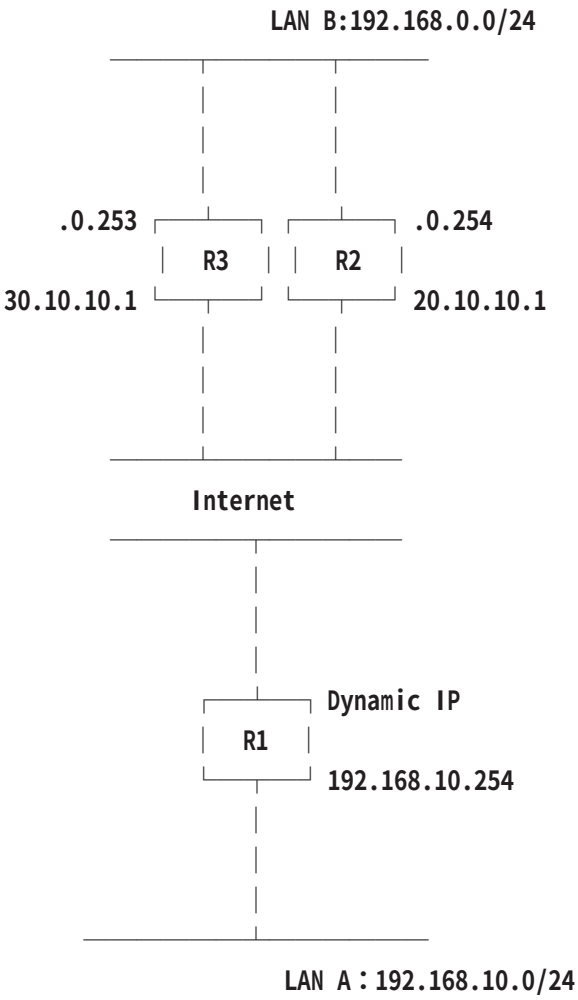
IPsec トンネルの障害を検知する条件

IPsec Keep-Alive 機能によって障害を検知するのは、「interval/watch count」に従って ping を発行して、一度も応答がなかったときです。
このとき本装置は、ping の応答がなかった IPsec トンネルを自動的に削除します。
反対に一度でも応答があったときは、本装置は IPsec トンネルを保持します。

IPsec KeepAlive を用いた IPsec の冗長化設定

IPsec KeepAlive 機能を用いて、IPsec の冗長化をおこないます。

ネットワーク構成



※R1、R2、R3 のいずれも XR-380 とします。

運用条件

1.R1-R2 間で IPsec 接続をおこないます。

2.R1-R2 間で IPsecKeepAlive 機能を動作させます。

3.R1 の IPsecKeepAlive 機能で、R1-R3 間の IPsec 接続設定を「backup SA」として指定しておきます。

4. すべて PPPoE 接続しているものとします。

5.R1 は動的 IP アドレス、R2 と R3 は図の固定 IP アドレスで接続しているものとします。

6. その他の IP アドレスについても図に従うものとします。

動作の概要

1.R1-R2 間で IPsec 接続をおこないます。

2.R2 側 PPPoE が切断してしまったとします。

3.R1 の IPsecKeepAlive 機能により、R1 は R2 への IPsecSA を削除します。

4. 同様に、R2 の IPsecKeepAlive 機能により、R2 は R1 への IPsecSA を削除します。

5.R1 の IPsecKeepAlive backup SA 設定によって、R1 は R3 との IPsec 接続を開始します。

6.R2 でのフローティングスタティックルート設定によって、LAN B から LAN A へのルーティングを R3 経由にします。

7.LAN A と LAN B は、R3-R1 間の IPsec を経由して通信が確立します。

8.R2 の回線接続が復旧したときに、R1-R2 間で IPsec を再確立します。また確立後に R1-R3 間の IPsecSA を削除し、LAN A と LAN B は、R1-R2 間の IPsec を経由して通信が確立します。

R1 の設定

[IPsec 本装置側の設定 1]

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	
インターフェースのID	@branch (例：@xr.centurysys)

[IKE/ISAKMP ポリシー設定 1]

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	20.10.10.1
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	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	
PSKを使用する 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)	test

・R2 と接続するための IKE/ISAKMP 設定です。

[IKE/ISAKMP ポリシー設定 2]

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	30.10.10.1
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	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	
PSKを使用する 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)	test2

・R3 と接続するための IKE/ISAKMP 設定です。

[IPsec ポリシー設定 1]

使用する / 使用しない / Responderとして使用する / 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	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 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 (1～255まで)

・LAN A - LAN B 間接続のための IPsec 設定です。

[IPsec ポリシー設定 2]

使用する / 使用しない / Responderとして使用する / 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	(例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	20.10.10.1/32 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 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 (1～255まで)

・R1 の WAN 側 I/F - R2 の WAN 側 I/F 間の IPsec 設定です。
・R1 の WAN 側 I/F - R2 の WAN 側 I/F 間で IPsecKeepAlive 監視を行うための設定です。

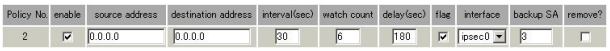
[IPsec ポリシー設定 3]

使用する / 使用しない / Responderとして使用する / On-Demandで使用する

使用するIKEポリシー名の選択	(IKE2)
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する / 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	2 (1～255まで)

・R3 を経由して LAN A - LAN B 間接続するための IPsec 設定です。
・**Responder 設定、distance は 2 にします。**
IPsecKeepAlive の backup SA として動作するときに、R3 へ向けて接続開始します。

[IPsec KeepAlive 設定]



Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	backup SA	remove?
2	☑	0.0.0.0	0.0.0.0	30	6	180	☑	ipsec0	3	☐

・「IPsec ポリシー設定 2」の接続で IPsecKeepAlive 監視を行いますので、設定番号 2 に設定します。
・source address、destination address ともに ”0.0.0.0 ”を指定し、本装置と対向側装置の WAN 側 IP アドレス間で IPsecKeepAlive 監視をおこなうようにします。
・R2 への IPsecSA を削除したときには、「IPsec ポリシー設定 3」を使って接続しますので、backup SA には「3」を指定します。

R2 の設定

[IPsec 本装置側の設定 1]

インターフェースのIPアドレス	20.10.10.1
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	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@branch (例：@xr.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	
PSKを使用する 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)	test

・R1 と接続するための IKE/ISAKMP 設定です。

[IPsec ポリシー設定 1]

使用する　使用しない　Responderとして使用する　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	192.168.0.0/24 (例：192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する　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 (1～255まで)

・LAN A - LAN B 間接続のための IPsec 設定です。
・Responder 設定にします。

[IPsec ポリシー設定 2]

使用する　使用しない　Responderとして使用する　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	20.10.10.1/32 (例：192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する　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 (1～255まで)

・R1 の WAN 側 I/F - R2 の WAN 側 I/F 間の IPsec 設定です。
・R1 の WAN 側 I/F - R2 の WAN 側 I/F 間で IPsecKeepAlive 監視を行うための設定です。

[IPsec KeepAlive 設定]

2	☑	192.168.0.254	192.168.10.254	30	6	180	☑	ipsec0		☐

・「IPsec ポリシー設定 2」の接続で IPsecKeepAlive 監視を行いますので、設定番号 2 に設定します。
・source address、destination address はそれぞれ、本装置の LAN 側 IP アドレス、対向側装置の LAN 側 IP アドレスを設定します。
・backup SA は使用しません。

[スタティックルーティング設定]

No.	ホスト/ネットワーク	アドレス	ネットマスク	インターフェース	pre No. (1～64)	ゲートウェイ	ディスタンス (1～255)	削除
1	ネットワーク	192.168.10.0	255.255.255.0	Ether0ポート		192.168.0.253	2	☐

・LAN A へのスタティックルート設定をおこないます。
・IPsec 接続時のルーティング設定と重複しますが、IPsec 接続時のルーティングを優先しますので、DISTANCE 値を「2」に設定します。
・これにより、IPsec 接続時は IPsec 側のルートが採用されるようになり、IPsec が非接続時にはスタティックルート設定でのルートが採用され、R3 から R1 を経由して LAN A - LAN B 間の通信を確立するようになります。

R3 の設定

[IPsec 本装置側の設定 1]

インターフェースのIPアドレス	30.10.10.1
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	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@branch (例：@xr.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	
PSKを使用する 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)	test2

・R1 と接続するための IKE/ISAKMP 設定です。

[IPsec ポリシー設定 1]

使用する　使用しない　Responderとして使用する　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	192.168.0.0/24 (例：192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.10.0/24 (例：192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	使用する　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 (1～255まで)

・LAN A - LAN B 間接続のための IPsec 設定です。
・Responder 設定にします。

IPsec 通信時のパケットフィルタ設定

ステートフルパケットインスペクション機能を使っていたり、パケットフィルタの設定によっては、IPsec 通信ができない場合があります。
このような場合は IPsec 通信でのデータをやりとりできるように、パケットフィルタの設定を追加する必要があります。

IPsec では、以下の 2 種類のプロトコル・ポートを使用します。

- **プロトコル「UDP」のポート「500」番**
  ->IKE(IPsec の鍵交換)のトラフィックに必要です

- **プロトコル「ESP」**
  ->ESP(暗号化ペイロード)のトラフィックに必要です

これらのパケットを通せるように、**「入力フィルタ」**に設定を追加してください。なお、「ESP」については、ポート番号の指定はしません。

< 設定例 >

インターフェース	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－主回線 #1	パケット受信時	許可	udp				500
PPP/PPPoE－主回線 #1	パケット受信時	許可	esp				

本装置の IPsec インタフェース名について

本装置は、通信インタフェースごとに IPsec のインタフェース名を設定しています。

ipsec0 ⇔ ppp0(PPPoE 主回線)
ipsec1 ⇔ ppp2(PPPoE マルチ回線 2)
ipsec2 ⇔ ppp3(PPPoE マルチ回線 3)
ipsec3 ⇔ ppp4(PPPoE マルチ回線 4)
ipsec4 ⇔ ppp5(バックアップ回線)
ipsec5 ⇔ eth0(ether0 ポート)
ipsec6 ⇔ eth1(ether1 ポート)

たとえば、PPPoE 主回線接続を使って IPsec 接続するときの ipsec インタフェース名は「ipsec0」となります。

「スタティックルート設定」や「フィルタ設定」などで ipsec インタフェースを選択するときは、上記を参照に選択またはインタフェース名を入力してください。

IPsec のログについて

IPsec で正常に通信できないときは本体ログを確認することで、どの段階で接続に失敗しているかを把握することができます。

本体ログは、「システム設定」内の「ログ表示」で確認します。

[正常に IPsec 接続できたときのログメッセージ]

メインモードの場合

```
Aug  3 12:00:14 localhost ipsec_setup:
 ...FreeS/WAN IPsec started

Aug  3 12:00:20 localhost ipsec__plutorun:
 104 "xripsec1" #1: STATE_MAIN_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 106 "xripsec1" #1: STATE_MAIN_I2: from
 STATE_MAIN_I1; sent MI2, expecting MR2

Aug  3 12:00:20 localhost ipsec__plutorun:
 108 "xripsec1" #1: STATE_MAIN_I3: from
 STATE_MAIN_I2; sent MI3, expecting MR3

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
 established

Aug  3 12:00:20 localhost ipsec__plutorun:
 112 "xripsec1" #2: STATE_QUICK_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #2: STATE_QUICK_I2: sent QI2,
 IPsec SA established
```

アグレッシブモードの場合

```
Apr 25 11:14:27 localhost ipsec_setup:
...FreeS/WAN IPsec started

Aug 3 11:14:34 localhost ipsec__plutorun:
whack:ph1_mode=aggressive whack:CD_ID=@home
whack:ID_FQDN=@home 112 "xripsec1" #1:
STATE_AGGR_I1: initiate

Aug 3 11:14:34 localhost ipsec__plutorun: 004
"xripsec1" #1: SAEST(e)=STATE_AGGR_I2: sent
AI2, ISAKMP SA established

Aug 3 12:14:34 localhost ipsec__plutorun: 117
"xripsec1" #2: STATE_QUICK_I1: initiate

Aug 3 12:14:34 localhost ipsec__plutorun: 004
"xripsec1" #2: SAEST(13)=STATE_QUICK_I2: sent
QI2, IPsec SA established
```

IPsec のログについて

「現在の状態」は IPsec 設定画面の「ステータス」から、画面中央下の「現在の状態」をクリックして表示します。

[正常に IPsec が確立したときの表示例]

```
000 interface ipsec0/eth1 218.xxx.xxx.xxx

000

000 "xripsec1": 192.168.xxx.xxx/24
===218.xxx.xxx.xxx[@<id>]---218.xxx.xxx.xxx...

000 "xripsec1": ...219.xxx.xxx.xxx
===192.168.xxx.xxx.xxx/24

000 "xripsec1":   ike_life: 3600s; ipsec_life:
28800s; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0

000 "xripsec1":   policy: PSK+ENCRYPT+TUNNEL+PFS;
interface: eth1; erouted

000 "xripsec1":   newest ISAKMP SA: #1; newest
IPsec SA: #2; eroute owner: #2

000

000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec
SA established); EVENT_SA_REPLACE in 27931s;
newest IPSEC; eroute owner

000 #2: "xripsec1" esp.32a406c4@219.xxx.xxx.xxx
esp.1be9611c@218.xxx.xxx.xxx
tun.1002@219.xxx.xxx.xxx tun.1001@218.xxx.xxx.xxx

000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA
established); EVENT_SA_REPLACE in 2489s; newest
ISAKMP
```

これらのログやメッセージ内に

- **ISAKMP SA established**
- **IPsec SA established**

のメッセージがない場合は IPsec が確立していません。設定を再確認して下さい。

IPsec がつながらないとき

○「 ...FreeS/WAN IPsec started」でメッセージが止まっています。

この場合は、接続相手との IKE 鍵交換が正常に行えていません。
IPsec 設定の「IKE/ISAKMP ポリシーの設定」項目で相手側機器についての設定を確認してください。

また、ステートフルパケットインスペクションを有効にしている場合、IPsec 通信のパケットを受信できるようにフィルタ設定を施す必要があります。IPsec のパケットを通すフィルタ設定は、「IPsec 通信時のパケットフィルタ設定」をご覧ください。

○「ISAKMP SA established」メッセージは表示されていますが「IPsec SA established」メッセージが表示されていません。

この場合は、IPsec SA が正常に確立できていません。IPsec 設定の「IPsec ポリシー設定」項目で、自分側と相手側のネットワークアドレスが正しいか、設定を確認してください。

○ Ipsec で接続できません。ログには

localhost ipsec__plutorun: whack: ph1_mode=main whack:CD_ID=@century1 whack:ID_FQDN=@century2 003 IP interfaces ppp0 and eth1 share address xx.xx.xx.xx!

というメッセージが出ています。

このログは PPPoE 接続で使用するアドレスと Ether1 ポートに割りあてられているアドレスが同一である為に表示されるエラーです。
これが原因で IPsec が正常に起動できません。
インタフェース設定において Ether1 ポートのアドレスを他のどの設定とも重複しないダミーのプライベートアドレスを設定してください。

固定 IP アドレスサービスで PPPoE 接続をする場合、固定 IP アドレスはインタフェース設定で設定するのではなく、PPP/PPPoE 設定の接続先設定において設定してください。

○「ISAKMP SA established」と「IPsec SA established」の両方のメッセージが表示されていますが、相手側と通信できません。

・ステートフルパケットインスペクションが有効になっていると、IPsec トンネルが生成されても通信ができない状況になってしまうことがあります。ステートフルパケットインスペクションを有効にしている場合は必ず、Ipsec 用のパケットフィルタ設定をおこなってください。詳細は本ガイド「IPsec 通信時のパケットフィルタ設定」をご覧ください。

○ IPsec 通信中に回線が一時的に切断してしまうと、回線が回復しても IPsec 接続がなかなか復帰しません。

相手が動的 IP アドレスの場合は相手側の IP アドレスが分からないために、固定 IP アドレス側からは IPsec 通信を開始することが出来ず、動的 IP アドレス側から IPsec 通信の再要求を受けるまでは IPsec 通信が復帰しなくなります。また動的側 IP アドレス側が IPsec 通信の再要求を出すのは IPsec SA のライフタイムが過ぎてからとなります。

このため IPsec 通信がなかなか復帰しない現象となります。

すぐに IPsec 通信を復帰させたいときは、動的 IP アドレス側の IPsec サービスも再起動してください。

動的 IP アドレス側の IPsec サービスの再起動が困難な環境でお使いの場合は、IPsec SA のライフタイムを短くして運用するか、IPsec Keep-Alive 機能を使用してください。

IPsec がつながらないとき

○相手の XR シリーズには IPsec のログが出ているのに、こちらの XR シリーズにはログが出ていません。IPsec は確立しているようなのですが、確認方法はありませんか？

固定 IP - 動的 IP 間での IPsec 接続を行なう場合、固定 IP 側(受信者側)の XR シリーズではログが表示されないことがあります。その場合は「各種サービスの設定」→「IPsec サーバ」→「ステータス」を開き、「現在の状態」をクリックして下さい。ここに現在の IPsec の状況が表示されます。

○新規に設定を追加したのですが、追加した設定については IPsec がつながりません。

設定を追加し、その設定を有効にする場合には IPsec 機能を再起動(本体の再起動)を行ってください。設定を追加しただけでは設定が有効になりません。

○ IPSec は確立していますが、Windows でファイル共有ができません。

XR シリーズは工場出荷設定において、NetBIOS を通さないフィルタリングが設定されています。Windows ファイル共有をする場合はこのフィルタ設定を削除もしくは変更してください。

FutureNet XR シリーズ　IPsec 設定ガイド v1985

2004 年 5 月版

発行 センチュリー・システムズ株式会社