技術情報：Si-R/Si-R brinシリーズ設定例
（NTT東日本 / NTT西日本フレッツ光ネクスト）

フレッツ・VPNプライオで拠点間を接続する設定例です。

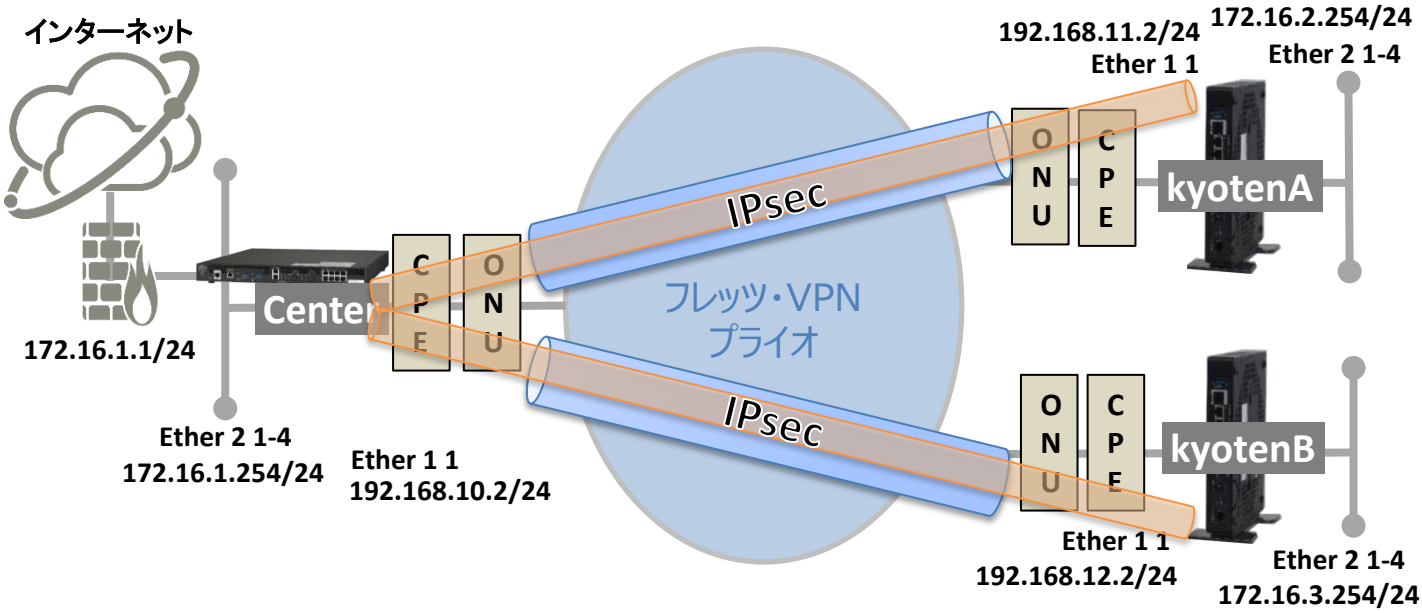
フレッツ・VPNプライオを利用して、拠点間をVPN（※）接続します。

※IPv4パケットをIPv4ヘッダでカプセリング(IPv4 over IPv4 IPsec tunnel)

Si-Rでトンネリングすることで以下の構成が可能になります。
・拠点からフレッツ・VPNプライオを経由して、センターから一元的にインターネットアクセスする
・拠点からフレッツ・VPNプライオを経由して、センターの複数セグメントと通信を行う

[対象機種と版数]
Si-R GX500 V1.05以降
Si-R Gシリーズ V4.05以降

[設定内容]
・Si-R GX（センター）のGigaEthernet 1/3をWAN側、GigeEthernet 1/5をLAN側とします。
・Si-R G（拠点）のether 1 1をWAN側、ether 2 1-4をLAN側とします。
・WAN（Si-R）側に192.168.10.2/24 、192.168.11.2/24 、192.168.12.2/24を割り当てるとします。
・WAN（CPE）側に192.168.10.1/24 、192.168.11.1/24 、192.168.12.1/24を割り当てるとします。
・LAN側に172.16.1.254/24、172.16.2.254/24、172.16.3.254/24を割り当てるとします。
・IPsec tunnelで拠点間を接続します。
・WAN側のMTUを1444とします。



[設定例]
・sir-keyにはIPsec鍵を設定してください。

Center設定例

```
ip route 172.16.2.0 255.255.255.0 tunnel 1
ip route 172.16.3.0 255.255.255.0 tunnel 2
ip route 192.168.11.0 255.255.255.0 192.168.10.1
ip route 192.168.12.0 255.255.255.0 192.168.10.1
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
survey 172.16.2.254 survey-map SURVEY_IPsec source port-channel 5 nexthop
tunnel 1 interworking
survey 172.16.3.254 survey-map SURVEY_IPsec source port-channel 5 nexthop
tunnel 2 interworking
!
survey-map SURVEY_IPsec
 ttl 255
 timeout 1000
 retry 4
 frequency every 10000
 stability 5 interval 10000
exit
!
crypto ipsec policy phase2
 set security-association always-up
 set security-association lifetime seconds 28800
 set security-association transform esp-aes esp-sha-hmac
 set mtu 1444
 set mss auto
 set ip tos copy
exit
!
crypto ipsec selector SELECTOR
 src 1 ipv4 any
 dst 1 ipv4 any
exit
!
crypto isakmp policy phase1
 authentication pre-share
 encryption aes
 group 1
 lifetime 86400
 hash sha
 initiate-mode main
exit
!
crypto isakmp profile ISAKMP_PROF_1
 local-address 192.168.10.2
 set isakmp-policy phase1
 set ipsec-policy phase2
 set peer 192.168.11.2
 ike-version 1
 local-key ascii sir-key
exit
!
```

```
crypto isakmp profile ISAKMP_PROF_2
 local-address 192.168.10.2
 set isakmp-policy phase1
 set ipsec-policy phase2
 set peer 192.168.12.2
 ike-version 1
 local-key ascii sir-key
exit
!
crypto map IPsec_MAP_1 ipsec-isakmp
 match address SELECTOR
 set isakmp-profile ISAKMP_PROF_1
exit
!
crypto map IPsec_MAP_2 ipsec-isakmp
 match address SELECTOR
 set isakmp-profile ISAKMP_PROF_2
exit
!
interface GigaEthernet 1/3
 channel-group 3
exit
!
interface GigaEthernet 1/5
 channel-group 5
exit
!
interface Port-channel 3
 ip address 192.168.10.2 255.255.255.0
 mtu 1444
exit
!
interface Port-channel 5
 ip address 172.16.1.254 255.255.255.0
exit
!
interface Tunnel 1
 ip unnumbered port-channel 5
 tunnel mode ipsec map IPsec_MAP_1
exit
!
interface Tunnel 2
 ip unnumbered port-channel 5
 tunnel mode ipsec map IPsec_MAP_2
exit
!
end
```

kyotenA設定例

```
ether 1 1 vlan untag 1
ether 2 1 vlan untag 2
ether 2 2 vlan untag 2
ether 2 3 vlan untag 2
ether 2 4 vlan untag 2
lan 0 mtu 1444
lan 0 ip address 192.168.11.2/24 3
lan 0 ip route 0 192.168.10.0/24 192.168.11.1 1 1
lan 0 vlan 1
lan 1 ip address 172.16.2.254/24 3
lan 1 vlan 2
remote 0 name Center
remote 0 mtu 1374
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 keep connect
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike encrypt aes-cbc-128
remote 0 ap 0 ipsec ike auth hmac-sha1
remote 0 ap 0 ike shared key text sir-key
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
remote 0 ap 0 ike proposal 0 hash hmac-sha1
remote 0 ap 0 tunnel local 192.168.11.2
remote 0 ap 0 tunnel remote 192.168.10.2
remote 0 ap 0 sessionwatch address 172.16.2.254 172.16.1.254
remote 0 ip route 0 default 1 60
remote 0 ip msschange 1334
time zone 0900
consoleinfo autologout 1h
telnetinfo autologout 10m
```

```
ether 1 1 vlan untag 1
ether 2 1 vlan untag 2
ether 2 2 vlan untag 2
ether 2 3 vlan untag 2
ether 2 4 vlan untag 2
lan 0 mtu 1444
lan 0 ip address 192.168.12.2/24 3
lan 0 ip route 0 192.168.10.0/24 192.168.12.1 1 1
lan 0 vlan 1
lan 1 ip address 172.16.3.254/24 3
lan 1 vlan 2
remote 0 name Center
remote 0 mtu 1374
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 keep connect
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike encrypt aes-cbc-128
remote 0 ap 0 ipsec ike auth hmac-sha1
remote 0 ap 0 ike shared key text sir-key
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
remote 0 ap 0 ike proposal 0 hash hmac-sha1
remote 0 ap 0 tunnel local 192.168.12.2
remote 0 ap 0 tunnel remote 192.168.10.2
remote 0 ap 0 sessionwatch address 172.16.3.254 172.16.1.254
remote 0 ip route 0 default 1 60
remote 0 ip msschange 1334
time zone 0900
consoleinfo autologout 1h
telnetinfo autologout 10m
```

解説
Center設定解説

```
ip route 172.16.2.0 255.255.255.0 tunnel 1
ip route 172.16.3.0 255.255.255.0 tunnel 2
#kyotenAのLAN向けのStatic経路を設定します。
#・172.16.2.0：宛先ネットワークです。
#・255.255.255.0：マスクです。
#・tunnel 1: ネクストホップです。
#kyotenBのLAN向けのStatic経路を設定します。
#・172.16.3.0：宛先ネットワークです。
#・255.255.255.0：マスクです。
#・tunnel 2: ネクストホップです。

ip route 192.168.11.0 255.255.255.0 192.168.10.1
ip route 192.168.12.0 255.255.255.0 192.168.10.1
#kyotenA向けのStatic経路を設定します。
#・192.168.11.0：宛先ネットワークです。
#・255.255.255.0：マスクです。
#・192.168.10.1: ネクストホップです。
#kyotenB向けのStatic経路を設定します。
#・192.168.12.0：宛先ネットワークです。
#・255.255.255.0：マスクです。
#・192.168.10.1: ネクストホップです。

ip route 0.0.0.0 0.0.0.0 172.16.1.1
#インターネット向けのStatic経路を設定します。
#・172.16.1.1：ネクストホップです。
!

survey 172.16.2.254 survey-map SURVEY_IPsec source port-channel 5 nexthop tunnel
1 interworking
survey 172.16.3.254 survey-map SURVEY_IPsec source port-channel 5 nexthop tunnel
2 interworking
#kyotenA宛に接続監視設定をする。
#・172.16.2.254：kyotenAのLAN側IPアドレスです。
#・SURVEY_IPsec：使用するsurvey-map名を指定します。
#・port-channel 5：送信元インタフェースを使用します。
#・tunnel 1：Tunnnel使用するインタフェースを指定します。
#・interworking：IPsec tunnelの状態を同期します。
#kyotenB宛に接続監視設定をする。
#・172.16.3.254：kyotenBのLAN側IPアドレスです。
#・SURVEY_IPsec：使用するsurvey-map名を指定します。
#・port-channel 5：送信元インタフェースを使用します。
#・tunnel 2：Tunnnel使用するインタフェースを指定します。
#・interworking：IPsec tunnelの状態を同期します。

!
```

```
survey-map SURVEY_IPsec
#接続監視の設定をします。

 ttl 255
#TTLを255に設定します。

 timeout 1000
#タイムアウトを1000ミリ秒に設定します。

 retry 4
#再送回数を4回に設定します。

 frequency every 10000
#定期監視感覚を10000ミリ秒に設定します。

 stability 5 interval 10000
#相手装置の復旧確認時の設定をします。
#・5：連続受信回数を設定します。
#・10000：送信間隔を設定します。

exit
!

crypto ipsec policy phase2
#IPsecポリシーのエントリの設定をします。

 set security-association always-up
#SAを常に確立する設定をします。

 set security-association lifetime seconds 28800
#IPsec-SA/Child-SAの生存時間を28800秒に設定します。

 set security-association transform esp-aes esp-sha-hmac
#暗号化アルゴリズム、認証アルゴリズムの設定をします。
#・esp-aes：暗号化アルゴリズムにAESを設定します。
#・esp-sha-hmac：認証アルゴリズムにHMAC-SHA-1を設定します。

 set mtu 1444
#MTU長を1444に設定します。

 set mss auto
#MSS値をオートに設定します。

 set ip tos copy
#ESPパケットにIPv4ヘッダのTOSフィールド値、IPv6ヘッダのトラフィッククラス値をそのまま使用する。

exit
!
crypto ipsec selector SELECTOR
#IPSEC-SA/CHILD SA用のセレクタのエントリの設定をします。

 src 1 ipv4 any
 dst 1 ipv4 any
#送信元および送信先にIPv4のすべてのアドレスを指定します。

exit
!
```

```
crypto isakmp policy phase1
#ISAKMPポリシー設定をします。

 authentication pre-share
#認証方式をPre-shared key方式に設定します。

 encryption aes
#ISAKMP-SA/IKE SAの暗号化アルゴリズムにAESを設定します。

 group 1
#Diffie-Hellmanグループ番号の設定をします。

 lifetime 86400
#ISAKMP-SA/IKE SAの生存時間を86400秒に設定します。

 hash sha
#ISAKMP-SA/IKE SAのハッシュアルゴリズムをSHA-1に設定します

 initiate-mode main
#IKEv1のPhase1のネゴシエーションモードをMainモードに設定します。

exit
!
crypto isakmp profile ISAKMP_PROF_1
#kyotenA宛のISAKMPプロファイル設定を設定します。

 local-address 192.168.10.2
#送信元アドレスを設定します。

 set isakmp-policy phase1
#ISAKMPポリシー名を設定する。

 set ipsec-policy phase2
#このISAKMPプロファイルで使用するIPSECポリシー名を設定する。

 set peer 192.168.11.2
#kyotenAのWAN側IPアドレスを指定する。

 ike-version 1
#IKEv1を設定します。

 local-key ascii sir-key
#Pre-shared keyを設定します。

exit
!
```

```
crypto isakmp profile ISAKMP_PROF_2
#kyotenB宛のISAKMPプロファイル設定を設定します。

 local-address 192.168.10.2
#送信元アドレスを設定します。

 set isakmp-policy phase1
#ISAKMPポリシー名を設定する。

 set ipsec-policy phase2
#このISAKMPプロファイルで使用するIPSECポリシー名を設定する。

 set peer 192.168.12.2
#kyotenBのWAN側IPアドレスを指定する。

 ike-version 1
#IKEv1を設定します。

 local-key ascii sir-key
#Pre-shared keyを設定します。

exit
!

crypto map IPsec_MAP_1 ipsec-isakmp
#kyotenA宛のVPNセレクタを設定する。

 match address SELECTOR
#暗号化するパケットとしてIPSECセレクタを設定する。

 set isakmp-profile ISAKMP_PROF_1
#kyotenA宛のISAKMPプロファイルを使用する。

exit
!

crypto map IPsec_MAP_2 ipsec-isakmp
#kyotenB宛のVPNセレクタを設定する。

 match address SELECTOR
#暗号化するパケットとしてIPSECセレクタを設定する。

 set isakmp-profile ISAKMP_PROF_2
#kyotenB宛のISAKMPプロファイルを使用する。

exit
!

interface GigaEthernet 1/3
#WAN側のインタフェース設定をします。

 channel-group 3
#チャネルグループ3を割り当てます。

exit
!
```

```
interface GigaEthernet 1/5
#LAN側のインタフェース設定をします。

 channel-group 5
#チャネルグループ5を割り当てます。

exit
!

interface Port-channel 3
#WAN側のポートチャネルの設定をします。

 ip address 192.168.10.2 255.255.255.0
#WAN側のIPアドレスを設定します。
#・192.168.10.2 : WAN側のIPアドレスです。
#・255.255.  255.0 : WAN側のマスクです。

 mtu 1444
#MTU長を1444byteに設定します。

exit
!

interface Port-channel 5
#LAN側のポートチャネルの設定をします。

 ip address 172.16.1.254 255.255.255.0
#LAN側のIPアドレスを設定します。
#・172.16.1.254 : LAN側のIPアドレスです。
#・255.255.  255.0 : LAN側のマスクです。

exit
!

interface Tunnel 1
#kyotenA側のトンネル設定をします。

 ip unnumbered port-channel 5
#送信元としてポートチャネル5を使用します。

 tunnel mode ipsec map IPsec_MAP_1
#Tunnnlで使用するVPNセレクタの設定をします。

exit
!

interface Tunnel 2
#kyotenB側のトンネル設定をします。

 ip unnumbered port-channel 5
#送信元としてポートチャネル5を使用します。

 tunnel mode ipsec map IPsec_MAP_2
#Tunnnlで使用するVPNセレクタの設定をします。

exit
!
end
```

解説
kyotenA設定解説

ether 1 1 vlan untag 1
#ether1 1ポートをTag なしVLAN1に設定します。

ether 2 1-4 vlan untag 2
#ether2 1-4ポートをTag なしVLAN2に設定します。

lan 0 mtu 1444
#MTU長を1444に設定します。

lan 0 ip address 192.168.11.2/24 3
#WAN側IPアドレスを設定します。
#・192.168.11.2/24 : WAN側のIPアドレス/マスクです。
#・3 : ブロードキャストアドレスのタイプ。通常は3で構いません。

lan 0 ip route 0 192.168.10.0/24 192.168.11.1 1 1
#Center拠点向けのStatic経路を設定します。
#・192.168.10.0/24 : 宛先ネットワーク/マスクです。
#・192.168.11.1 : ネクストホップです。
#・1 : metric値。通常は1で構いません。
#・1 : distance値。通常は1で構いません。

lan 0 vlan 1
#VLAN ID とlan 定義番号の関連付けを行います。

lan 1 ip address 172.16.2.254/24 3
#LAN側IPアドレスを設定します。
#・172.16.2.254/24 : LAN側のIPアドレス/マスクです。
#・3 : ブロードキャストアドレスのタイプ。通常は3で構いません。

lan 1 vlan 2
#VLAN ID とlan 定義番号の関連付けを行います。

remote 0 name Center
#Center向けのIPsecインターフェースの名前（任意）を設定します。

remote 0 mtu 1374
#MTU長を1374byteに設定します。

remote 0 ap 0 datalink type ipsec
#パケット転送方法としてIPsecを設定します。

remote 0 ap 0 keep connect
#常時接続します。

remote 0 ap 0 ipsec type ike
#IPsec情報のタイプにIPsec自動鍵交換(IKE Version1)を設定します。

remote 0 ap 0 ipsec ike protocol esp
#自動鍵交換用IPsec情報のセキュリティプロトコルにESP（暗号）を設定します。

remote 0 ap 0 ipsec ike encrypt aes-cbc-128
#自動鍵交換用IPsec情報の暗号情報にAES128ビットを設定します。

remote 0 ap 0 ipsec ike auth hmac-sha1
#自動鍵交換用IPsec情報の認証情報にSHA1を設定します。

remote 0 ap 0 ike shared key text sir-key
#IKEセッション確立時の共有鍵（Pre-shared key）を設定します。

remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
#IKEセッション用暗号情報の暗号アルゴリズムにAES128ビットを設定します。

remote 0 ap 0 ike proposal 0 hash hmac-sha1
#IKEセッション用の認証情報にSHA1を設定します。

remote 0 ap 0 tunnel local 192.168.11.2
remote 0 ap 0 tunnel remote 192.168.10.2
#IPsecトンネルの送信元/送信先アドレスの設定をします。

remote 0 ap 0 sessionwatch address 172.16.2.254 172.16.1.254
#接続先セッション監視の設定をします。
#・172.168.2.254：ICMP ECHOパケットの送信元IPアドレスです。
#・172.168.1.254：ICMP ECHOパケットの宛先IPアドレスです。

remote 0 ip route 0 default 1 60
#Center拠点向きにデフォルトルートを設定します。

remote 0 ip msschange 1334
#MSS書き換えの設定をします。

time zone 0900
#タイムゾーンを設定します。通常はこのままで構いません。

consoleinfo autologout 1h
telnetinfo autologout 10m
#シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこの値で構いません。

解説
kyotenB設定解説

ether 1 1 vlan untag 1
#ether1 1ポートをTag なしVLAN1に設定します。

ether 2 1-4 vlan untag 2
#ether2 1-4ポートをTag なしVLAN2に設定します。

lan 0 mtu 1444
#MTU長を1444に設定します。

lan 0 ip address 192.168.12.2/24 3
#WAN側IPアドレスを設定します。
#・192.168.12.2/24 : WAN側のIPアドレス/マスクです。
#・3 : ブロードキャストアドレスのタイプ。通常は3で構いません。

lan 0 ip route 0 192.168.10.0/24 192.168.12.1 1 1
#Center向けのStatic経路を設定します。
#・192.168.10.0/24 : 宛先ネットワーク/マスクです。
#・192.168.12.1 : ネクストホップです。
#・1 : metric値。通常は1で構いません。
#・1 : distance値。通常は1で構いません。

lan 0 vlan 1
#VLAN ID とlan 定義番号の関連付けを行います。

lan 1 ip address 172.16.3.254/24 3
#LAN側IPアドレスを設定します。
#・172.16.3.254/24 : LAN側のIPアドレス/マスクです。
#・3 : ブロードキャストアドレスのタイプ。通常は3で構いません。

lan 1 vlan 2
#VLAN ID とlan 定義番号の関連付けを行います。

remote 0 name Center
#Center向けのIPsecインターフェースの名前（任意）を設定します。

remote 0 mtu 1374
#MTU長を1374byteに設定します。

remote 0 ap 0 datalink type ipsec
#パケット転送方法としてIPsecを設定します。

remote 0 ap 0 keep connect
#常時接続します。

remote 0 ap 0 ipsec type ike
#IPsec情報のタイプにIPsec自動鍵交換(IKE Version1)を設定します。

remote 0 ap 0 ipsec ike protocol esp
#自動鍵交換用IPsec情報のセキュリティプロトコルにESP（暗号）を設定します。

remote 0 ap 0 ipsec ike encrypt aes-cbc-128
#自動鍵交換用IPsec情報の暗号情報にAES128ビットを設定します。

remote 0 ap 0 ipsec ike auth hmac-sha1
#自動鍵交換用IPsec情報の認証情報にSHA1を設定します。

remote 0 ap 0 ike shared key text xx sir-key
#IKEセッション確立時の共有鍵（Pre-shared key）を設定します。

remote 0 ap 0 ike proposal 0 encrypt aes-cbc-128
#IKEセッション用暗号情報の暗号アルゴリズムにAES128ビットを設定します。

remote 0 ap 0 ike proposal 0 hash hmac-sha1
#IKEセッション用の認証情報にSHA1を設定します。

remote 0 ap 0 tunnel local 192.168.12.2
remote 0 ap 0 tunnel remote 192.168.10.2
#IPsecトンネルの送信元/送信先アドレスの設定をします。

remote 0 ap 0 sessionwatch address 172.16.3.254 172.16.1.254
#接続先セッション監視の設定をします。
#・172.168.3.254：ICMP ECHOパケットの送信元IPアドレスです。
#・172.168.1.254：ICMP ECHOパケットの宛先IPアドレスです。

remote 0 ip route 0 default 1 60
#Center向きにデフォルトルートを設定します。

remote 0 ip msschange 1334
#MSS書き換えの設定をします。

time zone 0900
#タイムゾーンを設定します。通常はこのままで構いません。

consoleinfo autologout 1h
telnetinfo autologout 10m
#シリアルコンソール、TELNETコネクションの入出力がない場合のコネクション切断時間を設定します。通常はこの値で構いません。