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。

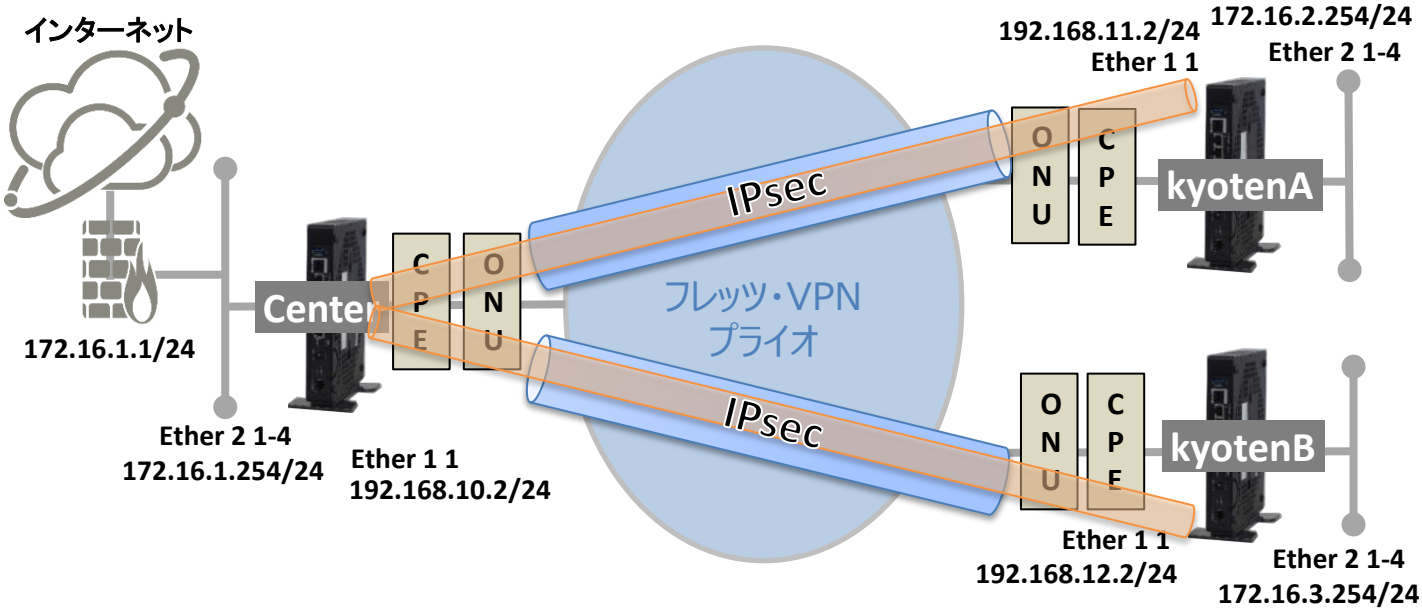
フレッツ・VPNプライオを利用して、拠点間をVPN（※）接続します。

※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 Gシリーズ V4.05以降

[設定内容]
・Si-R G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

```
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 192.168.10.2/24 3
lan 0 ip route 0 192.168.11.0/24 192.168.10.1 1 1
lan 0 ip route 1 192.168.12.0/24 192.168.10.1 1 1
lan 0 vlan 1
lan 1 ip address 172.16.1.254/24 3
lan 1 ip route 0 default 172.16.1.1 1 1
lan 1 vlan 2
remote 0 name kyotenA
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 192.168.10.2
remote 0 ap 0 tunnel remote 192.168.11.2
remote 0 ap 0 sessionwatch address 172.16.1.254 172.16.2.254
remote 0 ip route 0 172.16.2.0/24 1 60
remote 0 ip msschange 1334
remote 1 name kyotenB
remote 1 mtu 1374
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 keep connect
remote 1 ap 0 ipsec type ike
remote 1 ap 0 ipsec ike protocol esp
remote 1 ap 0 ipsec ike encrypt aes-cbc-128
remote 1 ap 0 ipsec ike auth hmac-sha1
remote 1 ap 0 ike shared key text sir-key
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-128
remote 1 ap 0 ike proposal 0 hash hmac-sha1
remote 1 ap 0 tunnel local 192.168.10.2
remote 1 ap 0 tunnel remote 192.168.12.2
remote 1 ap 0 sessionwatch address 172.16.1.254 172.16.3.254
remote 1 ip route 0 172.16.3.0/24 1 60
remote 1 ip msschange 1334
time zone 0900
consoleinfo autologout 1h
telnetinfo autologout 10m
```

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

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 192.168.10.2/24 3
#WAN側IPアドレスを設定します。
#・192.168.10.2/24 : 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 0 192.168.11.0/24 192.168.10.1 1 1
lan 0 ip route 1 192.168.12.0/24 192.168.10.1 1 1
#kyotenA向けのStatic経路を設定します。
#・192.168.11.0/24 : 宛先ネットワーク/マスクです。
#・192.168.10.1 : 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。
#kyotenB向けのStatic経路を設定します。
#・192.168.12.0/24 : 宛先ネットワーク/マスクです。
#・192.168.10.1 : 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 172.16.1.254/24 3
#LAN側IPアドレスを設定します。
#・172.16.1.254/24 : 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 ip route 0 default 172.16.1.1 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。
#・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 1 vlan 2
#VLAN ID とlan 定義番号の関連付けを行います。

remote 0 name kyotenA
#kyotenA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 192.168.10.2
remote 0 ap 0 tunnel remote 192.168.11.2
#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 172.16.1.254 172.16.2.254
#接続先セッション監視の設定をします。
#・172.168.1.254 : ICMP ECHOパケットの送信元IPアドレスです。
#・172.168.2.254 : ICMP ECHOパケットの宛先IPアドレスです。

remote 0 ip route 0 172.16.2.0/24 1 60
#kyotenA向きにStatic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。

remote 1 name kyotenB
#kyotenA向けのIPsecインターフェースの名前（任意）を設定します。

remote 1 mtu 1374
#MTU長を1374byteに設定します。

remote 1 ap 0 datalink type ipsec
#パケット転送方法としてIPsecを設定します。

remote 1 ap 0 keep connect
#インターネットへ常時接続します。
```

remote 1 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 1 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 1 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 1 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 1 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 1 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 1 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 1 ap 0 tunnel local 192.168.10.2
remote 1 ap 0 tunnel remote 192.168.12.2
#IPsecトンネルの送信元/送信先アドレスの設定をします。

remote 1 ap 0 sessionwatch address 172.16.1.254 172.16.3.254
#接続先セッション監視の設定をします。
#・172.168.1.254：ICMP ECHOパケットの送信元IPアドレスです。
#・172.168.3.254：ICMP ECHOパケットの宛先IPアドレスです。

remote 1 ip route 0 172.16.3.0/24 1 60
#kyotenB向きにStaticルートを設定します。

remote 1 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
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
#インターネットへ常時接続します。

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
#インターネットへ常時接続します。

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。