

技術情報：Si-R Gシリーズ設定例

(NTT東日本 / NTT西日本フレッツ光ネクスト)

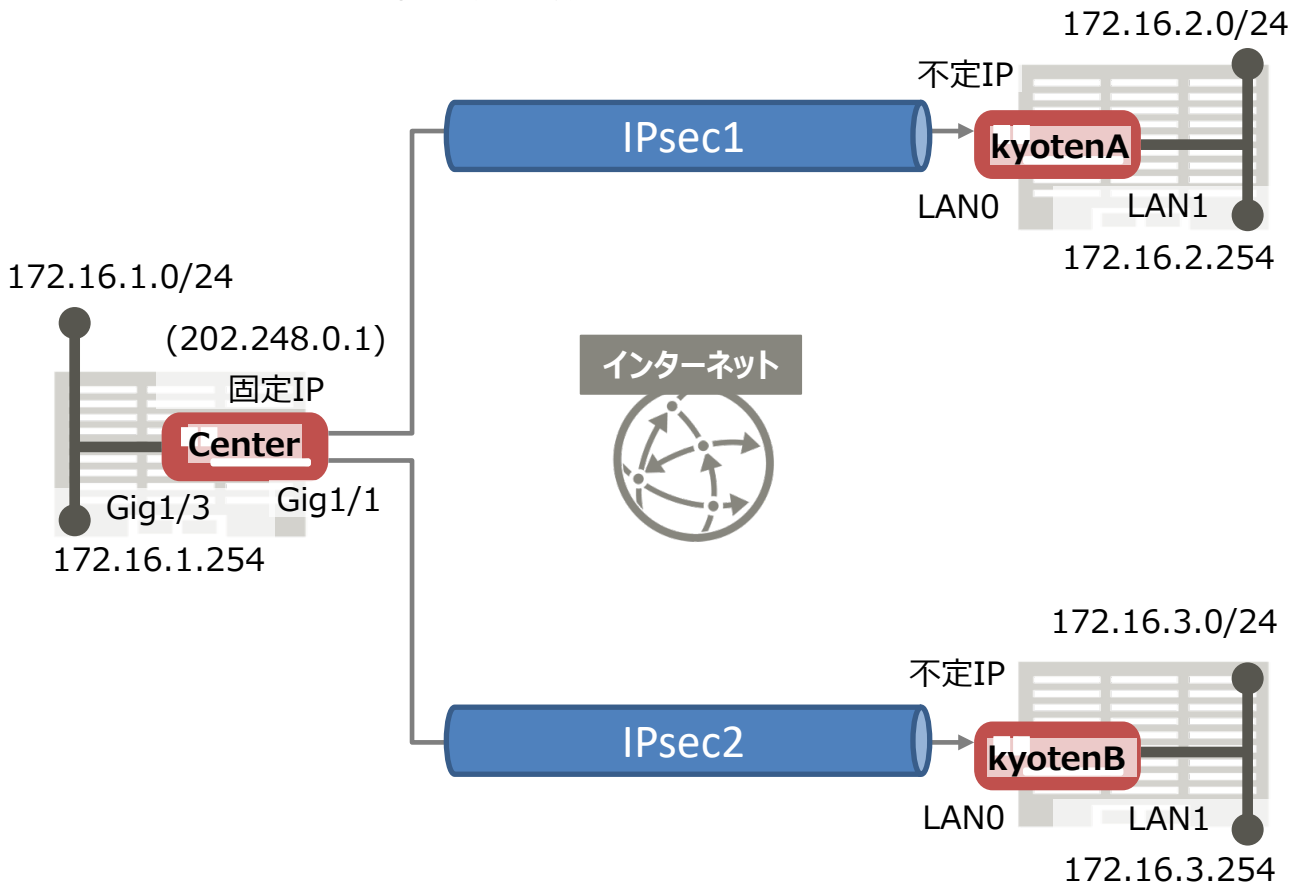
インターネットVPN（IPsecアグレッシブモード）で複数拠点を接続する設定例です。

[対象機種と版数]

- ・Si-RGX500 V01.14以降
- ・Si-R Gシリーズ V20.12以降

[設定内容]

- ・Si-RGX500(センター)のWAN側をGigabitethernet1/1、LAN側をGigabitethernet1/3とします。
- ・Si-R G(拠点)のWAN側をLAN0、LAN側をLAN1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でセンターと拠点間を接続します。
- ・インターネットVPN（アグレッシブモード）で拠点間を接続します。



[設定例]

以下の設定例を、コピー&ペーストでご利用いただくことができます。

- ・ **id-a@isp**にはISPのIDを設定してください。
- ・ **pwd-a@isp**にはISPのパスワードを設定してください。
- ・ **id-b@isp**にはISPのIDを設定してください。
- ・ **pwd-b@isp**にはISPのパスワードを設定してください。
- ・ **sir-key**にはkyotenA用のIPsec鍵を設定してください。
- ・ **sir-key2**にはkyotenB用のIPsec鍵を設定してください。

Center設定事例

```
ip route 0.0.0.0 0.0.0.0 202.248.0.2
ip route 172.16.2.0 255.255.255.0 tunnel 1
ip route 172.16.3.0 255.255.255.0 tunnel 2
!
survey 172.16.2.254 survey-map SURVEY_IPsec source port-channel 3 nexthop
tunnel 1 interworking
survey 172.16.3.254 survey-map SURVEY_IPsec source port-channel 3 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 pfs group14
set security-association lifetime seconds 28800
set security-association transform esp-aes esp-sha256-hmac
set mtu 1454
set mss auto
set ip tos copy
set ip df-bit 0
set ip fragment post
exit
!
crypto ipsec selector SELECTOR
src 1 ipv4 any
dst 1 ipv4 any
exit
!
```

```
crypto isakmp log sa
crypto isakmp log session
crypto isakmp log negotiation-fail
!
crypto isakmp policy phase1
authentication pre-share
encryption aes
encryption-keysize aes 256 256 256
group 14
lifetime 86400
hash sha-256
initiate-mode aggressive
exit
!
crypto isakmp profile ISAKMP_PROF_1
match identity host kyotenA
local-address 202.248.0.1
set isakmp-policy phase1
set ipsec-policy phase2
ike-version 1
local-key ascii sir-key
exit
!
crypto isakmp profile ISAKMP_PROF_2
match identity host kyotenB
local-address 202.248.0.1
set isakmp-policy phase1
set ipsec-policy phase2
ike-version 1
local-key ascii sir-key2
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 1/1
 channel-group 1
 exit
!
interface GigaEthernet 1/3
 channel-group 3
 speed-duplex auto
 media auto
 exit
!
interface Management 1
 ip address 192.168.1.1 255.255.255.0
 exit
!
interface Port-channel 1
 ip address 202.248.0.1 255.255.255.252
 exit
!
interface Port-channel 3
 ip address 172.16.1.254 255.255.255.0
 exit
!
interface Tunnel 1
 ip unnumbered port-channel 1
 tunnel mode ipsec map IPsec_MAP_1
 exit
!
interface Tunnel 2
 ip unnumbered port-channel 1
 tunnel mode ipsec map IPsec_MAP_2
 exit
!
```

kyotenA設定事例

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 172.16.2.254/24 3
lan 1 vlan 2
remote 0 name internet
remote 0 mtu 1454
remote 0 ap 0 name pppoe
remote 0 ap 0 datalink bind vlan 1
remote 0 ap 0 ppp auth send id-a@isp pwd-a@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 default 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 172.16.2.254 500 any 500 17
remote 0 ip nat static 1 172.16.2.254 any any any 50
remote 0 ip msschange 1414
remote 1 name Center
remote 1 ap 0 name ipsec
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-256
remote 1 ap 0 ipsec ike auth hmac-sha256
remote 1 ap 0 ipsec ike pfs modp2048
remote 1 ap 0 ike mode aggressive
remote 1 ap 0 ike name local kyotenA
remote 1 ap 0 ike shared key text sir-key
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 1 ap 0 ike proposal 0 hash hmac-sha256
remote 1 ap 0 ike proposal 0 pfs modp2048
remote 1 ap 0 tunnel remote 202.248.0.1
remote 1 ap 0 sessionwatch address 172.16.2.254 172.16.1.254
remote 1 ip route 0 172.16.1.0/24 1 1
remote 1 ip msschange 1300
syslog facility 23
time zone 0900
consoleinfo autologout 1h
telnetinfo autologout 10m
terminal charset SJIS
```

kyotenB設定事例

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 172.16.3.254/24 3
lan 1 vlan 2
remote 0 name internet
remote 0 mtu 1454
remote 0 ap 0 name pppoe
remote 0 ap 0 datalink bind vlan 1
remote 0 ap 0 ppp auth send id-b@isp pwd-b@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 default 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 172.16.3.254 500 any 500 17
remote 0 ip nat static 1 172.16.3.254 any any any 50
remote 0 ip msschange 1414
remote 1 name Center
remote 1 ap 0 name ipsec
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-256
remote 1 ap 0 ipsec ike auth hmac-sha256
remote 1 ap 0 ipsec ike pfs modp2048
remote 1 ap 0 ike mode aggressive
remote 1 ap 0 ike name local kyotenB
remote 1 ap 0 ike shared key text sir-key2
remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 1 ap 0 ike proposal 0 hash hmac-sha256
remote 1 ap 0 ike proposal 0 pfs modp2048
remote 1 ap 0 tunnel remote 202.248.0.1
remote 1 ap 0 sessionwatch address 172.16.3.254 172.16.1.254
remote 1 ip route 0 172.16.1.0/24 1 1
remote 1 ip msschange 1300
syslog facility 23
time zone 0900
consoleinfo autologout 1h
telnetinfo autologout 10m
terminal charset SJIS
```

Center設定解説

```
ip route 0.0.0.0 0.0.0.0 202.248.0.2
ip route 172.16.2.0 255.255.255.0 tunnel 1
ip route 172.16.3.0 255.255.255.0 tunnel 2
#デフォルトルートをWAN側に向けて設定します。
#・0.0.0.0 : 宛先ネットワークです。
#・0.0.0.0 : マスクです。
#・202.248.0.2: ネクストホップです。
#Si-R_2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。
#Si-R_3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。

!
survey 172.16.2.254 survey-map SURVEY_IPsec source port-channel 3 nexthop
tunnel 1 interworking
survey 172.16.3.254 survey-map SURVEY_IPsec source port-channel 3 nexthop
tunnel 2 interworking
#Si-R_1宛のSURVEYを設定します。
#・172.16.2.254 : Si-R_1のLAN側アドレスを指定します。
#・SURVEY_IPsec : サーベイマップを指定します。
#・Port-channel 3 : 送信元のインタフェースを指定します。
#・tunnel 1 : 送信インタフェースを指定します。
#・interworking : IPsecトンネルの状態を同期させます。
#Si-R_2宛のSURVEYを設定します。
#・172.16.3.254 : Si-R_3のLAN側アドレスを指定します。
#・SURVEY_IPsec : サーベイマップを指定します。
#・Port-channel 3 : 送信元のインタフェースを指定します。
#・tunnel 2 : 送信インタフェースを指定します。
#・interworking : IPsecトンネルの状態を同期させます。

!
survey-map SURVEY_IPsec
#Survey-map名を指定します。

ttl 255
#ICMP echoパケットのTTL値を設定します。

timeout 1000
#応答待ち時間の設定をします。

retry 4
#再送回数の設定をします。

frequency every 10000
#定期監視間隔の設定をします。
```

```
stability 5 interval 10000
#相手の復旧を確認するための再送回数と送信間隔の設定をします。
#・5：再送回数
#・10000：送信間隔
exit
!
```

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

```
set pfs group14
#Diffie-Hellmanの設定をします。
```

```
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-sha256-hmac
#ネゴシエーションで使用するAESの鍵長の設定をします。
```

```
set mtu 1454
#MTU長の設定をする。
```

```
set mss auto
#MSS値を書き換える設定をします。
```

```
set ip tos copy
#TOSフィールド値、およびトラフィッククラス値の設定をします。
```

```
set ip df-bit 0
#DFビット値の設定をします。
```

```
set ip fragment post
#Post-Fragmentを行う設定をします。
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 log sa
#SA確率/解放をログに出力します。
```

```
crypto isakmp log session
#セッション確率/解放をログに出力します。
```

```
crypto isakmp log negotiation-fail
#ネゴシエーション失敗をログに出力します。
!
```



```
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。
```

```
encryption-keysize aes 256 256 256
#ISAKMP-SA/IKE SAのネゴシエーションで使用するAESの鍵長の設定します。
```

```
group 14
#Diffie-Hellmanグループ番号の設定をします。
```

```
lifetime 86400
#ライフタイムを設定します。
```

```
hash sha-256
#ISAKMP-SA/IKE SAのハッシュアルゴリズムをSHA-2に設定します
```

```
initiate-mode aggressive
#アグレッシブモードに設定します。
```

```
exit
!
```

```
crypto isakmp profile ISAKMP_PROF_1
# Si-R_1宛のISAKMPプロファイル設定を設定します。
```

```
match identity host kyotenA
#接続先の拠点名を設定します。
```

```
local-address 202.248.0.1
#自装置のIPアドレスを設定します。
```

```
set isakmp-policy phase1
#ISAKMPポリシー名を設定します。
```

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

```
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
# Si-R_2宛のISAKMPプロファイル設定を設定します。
```

```
match identity host kyotenB
#接続先の拠点名を設定します。
```

```
local-address 202.248.0.1
#自装置のIPアドレスを設定します。
```

```
set isakmp-policy phase1
#ISAKMPポリシー名を設定します。
```

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

```
ike-version 1
#IKEv1を設定します。
```

```
local-key ascii sir-key2
#Pre-shared keyを設定します。
```

```
exit
!
```

```
crypto map IPsec_MAP_1 ipsec-isakmp
#VPNセクタ設定モードへ移行します。
```

```
match address SELECTOR
#IPsecセクタ名を設定します。
```

```
set isakmp-profile ISAKMP_PROF_1
#使用するISAKMPプロファイル名の設定をします。
```

```
exit
!
```

```
crypto map IPsec_MAP_2 ipsec-isakmp
#VPNセクタ設定モードへ移行します。
```

```
match address SELECTOR
#IPsecセクタ名を設定します。
```

```
set isakmp-profile ISAKMP_PROF_2
#使用するISAKMPプロファイル名の設定をします。
```

```
exit
!
```

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

```
channel-group 1
#チャンネルグループ1を割り当てます。
```

```
exit
!
```

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

channel-group 3
#チャンネルグループ3を割り当てます。

speed-duplex auto
#Speed/Duplexをオートに設定します。

media auto
#メディアタイプをオートに設定します。
exit
!
interface Management 1
#マネージメントインタフェースの設定をします。

ip address 192.168.1.1 255.255.255.0
#IPアドレスを設定します。
exit
!

interface Port-channel 1
#WAN側のポートチャネルの設定をします。

ip address 202.248.0.1 255.255.255.252
#WAN側のIPアドレスを設定します。
#・202.248.0.1 : WAN側のIPアドレスです。
#・255.255.255.252 : WAN側のマスクです。
exit
!
interface Port-channel 3
#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
# Si-R_1側のトンネル設定をします。

ip unnumbered port-channel 1
#送信元としてポートチャンネル1を使用します。

tunnel mode ipsec map IPsec_MAP_1
#Tunnel1で使用するVPNセクタの設定をします。
exit
!
interface Tunnel 2
# Si-R_2側のトンネル設定をします。

ip unnumbered port-channel 1
#送信元としてポートチャンネル1を使用します。

tunnel mode ipsec map IPsec_MAP_2
#Tunnel1で使用するVPNセクタの設定をします。
exit
!
```

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 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です。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 internet
```

#PPPoEインターフェースの名前（任意）を設定します。

```
remote 0 mtu 1454
```

#Bフレッツ・フレッツADSLでは、MTU長を1454byteに設定します。

```
remote 0 ap 0 name pppoe
```

#アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

```
remote 0 ap 0 datalink bind vlan 1
```

#インターネット向けパケットの転送先をvlan1設定します。

```
remote 0 ap 0 ppp auth send id-a@isp pwd-a@isp
```

#インターネット用プロバイダーの認証ID、パスワードを設定します。

```
remote 0 ap 0 keep connect
```

#インターネットへ常時接続します。

```
remote 0 ppp ipcp vjcomp disable
```

#VJヘッダー圧縮を使用しない設定にします。

```
remote 0 ip route 0 default 1 1
```

#default : 対向装置にデフォルトルート向けます。

- ・ 1 : metric値です。通常は1で構いません。
- ・ 1 : distance値です。通常は0で構いません。

```
remote 0 ip nat mode multi any 1 5m
```

#マルチNATの設定をします。

```
remote 0 ip nat static 0 172.16.2.254 500 any 500 17
```

```
remote 0 ip nat static 1 172.16.2.254 any any any 50
```

#スタティックNATにより、IKE,ESPパケットを通す設定をします。

```
remote 0 ip msschange 1414
```

#MSS値です。1414byte (1454 (MTU長) - 40 (TCP/IPヘッダー長)) を設定します。

remote 1 name Center

#Center向けIPsecインターフェースの名前（任意）を設定します。

remote 1 ap 0 name ipsec

#アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

remote 1 ap 0 datalink type ipsec

#データリンクタイプをIpsecに設定します。

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

#パケット転送方法としてIPsec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-256

#自動鍵交換用IPsec情報の暗号情報にAES256ビットを設定します。

remote 1 ap 0 ipsec ike auth hmac-sha256

#自動鍵交換用IPsec情報の認証情報に設定SHA256を設定します。

remote 1 ap 0 ipsec ike pfs modp2048

#自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループにmodp2048を設定します。

remote 1 ap 0 ike mode aggressive

#アグレッシブモードに設定します。

remote 1 ap 0 ike name local kyotenA

#IKE情報の自側装置識別情報を設定します。

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-256

#IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha256

#IKEセッション用の認証情報にSHA2を設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048

#IKE情報のPFS使用時のDH（Diffie-Hellman）グループにmodp2048を設定します。

remote 1 ap 0 tunnel remote 202.248.0.1

#IPsecトンネルの宛先アドレスの設定をします。

remote 1 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。

- ・ 172.16.2.254 : ICMP ECHOパケットの送信元IPアドレスです。
- ・ 172.16.1.254 : ICMP ECHOパケットの宛先IPアドレスです。

```
remote 1 ip route 0 172.16.1.0/24 1 1
```

#172.16.1.0/24：対向装置CenterのLAN側ネットワークです。

- ・ 1：metric値です。通常は1で構いません。
- ・ 1：distance値です。通常は1で構いません。

```
remote 1 ip msschange 1300
```

#MSS値に1300byteを設定します。

```
syslog facility 23
```

#システムログ情報の出力情報／出力対象ファシリティの設定をします。通常はこのままで構いません。

```
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。

```
terminal charset SJIS
```

#ターミナルで使用する漢字コードをShift JISコードに設定します。

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 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です。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 internet
```

#PPPoEインターフェースの名前（任意）を設定します。

```
remote 0 mtu 1454
```

#Bフレッツ・フレッツADSLでは、MTU長を1454byteに設定します。

```
remote 0 ap 0 name pppoe
```

#アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

```
remote 0 ap 0 datalink bind vlan 1
```

#インターネット向けパケットの転送先をvlan1設定します。

```
remote 0 ap 0 ppp auth send id-b@isp pwd-b@isp
```

#インターネット用プロバイダーの認証ID、パスワードを設定します。

```
remote 0 ap 0 keep connect
```

#インターネットへ常時接続します。

```
remote 0 ppp ipcp vjcomp disable
```

#VJヘッダー圧縮を使用しない設定にします。

```
remote 0 ip route 0 default 1 1
```

#default : 対向装置にデフォルトルート向けます。

- ・ 1 : metric値です。通常は1で構いません。
- ・ 1 : distance値です。通常は0で構いません。

```
remote 0 ip nat mode multi any 1 5m
```

#マルチNATの設定をします。

```
remote 0 ip nat static 0 172.16.3.254 500 any 500 17
```

```
remote 0 ip nat static 1 172.16.3.254 any any any 50
```

#スタティックNATにより、IKE,ESPパケットを通す設定をします。

```
remote 0 ip msschange 1414
```

#MSS値です。1414byte (1454 (MTU長) - 40 (TCP/IPヘッダー長)) を設定します。


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

remote 1 ap 0 name ipsec
#アクセスポイントの名前（任意、remote nameと同じでも可）を設定します。

remote 1 ap 0 datalink type ipsec
#データリンクタイプをIpsecに設定します。

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
#パケット転送方法としてIPsec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-256
#自動鍵交換用IPsec情報の暗号情報にAES256ビットを設定します。

remote 1 ap 0 ipsec ike auth hmac-sha256
#自動鍵交換用IPsec情報の認証情報に設定SHA256を設定します。

remote 1 ap 0 ipsec ike pfs modp2048
#自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループにmodp2048を設定します。

remote 1 ap 0 ike mode aggressive
#アグレッシブモードに設定します。

remote 1 ap 0 ike name local kyotenB
#IKE情報の自側装置識別情報を設定します。

remote 1 ap 0 ike shared key text sir-key2
#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-256
#IKEセッション用暗号情報の暗号アルゴリズムにAES256ビットを設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha256
#IKEセッション用の認証情報にSHA2を設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048
#IKE情報のPFS使用時のDH（Diffie-Hellman）グループにmodp2048を設定します。

remote 1 ap 0 tunnel remote 202.248.0.1
#IPsecトンネルの宛先アドレスの設定をします。

remote 1 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。


- ・ 172.16.3.254 : ICMP ECHOパケットの送信元IPアドレスです。
- ・ 172.16.1.254 : ICMP ECHOパケットの宛先IPアドレスです。

```

```
remote 1 ip route 0 172.16.1.0/24 1 1  
#172.16.1.0/24：対向装置CenterのLAN側ネットワークです。
```

- ・ 1：metric値です。通常は1で構いません。
- ・ 1：distance値です。通常は1で構いません。

```
remote 1 ip msschange 1300  
#MSS値に1300byteを設定します。
```

```
syslog facility 23  
#システムログ情報の出力情報／出力対象ファシリティの設定をします。通常はこのままで構いません。
```

```
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。
```

```
terminal charset SJIS  
#ターミナルで使用する漢字コードをShift JISコードに設定します。
```