【NECルーターとのインターネットVPN(IPsec IKEv2)】

インターネットVPN(IPsec IKEv2)でセンター(NEC IX2207) ― 拠点(Si-R G)間を接続する設定例です。

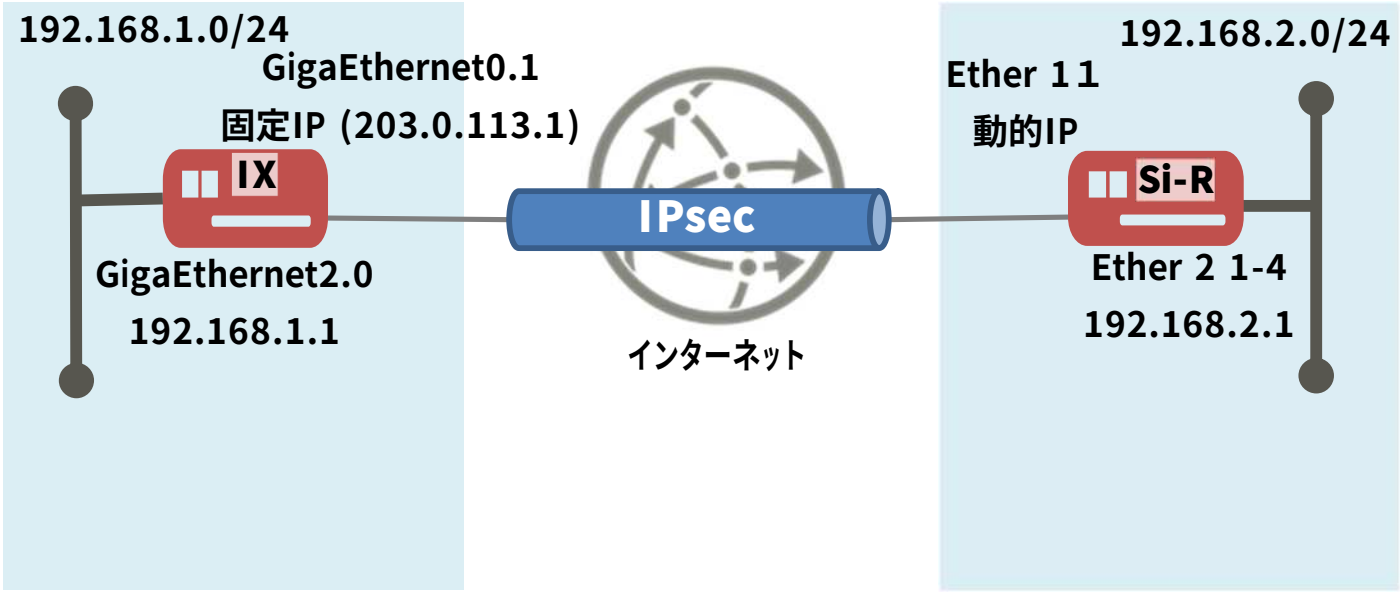
センター(IX2207)はPPPoE 固定1IP回線、拠点(Si-R G120)はPPPoE 動的IP回線を使用し、センター拠点間をIPsec(IKEv2)で接続します。
※本設定例は、弊社で独自に接続試験を行った結果を元に作成しております。

[対象機種と版数]

- Si-R Gシリーズ V20.52以降
- NEC IX2207 Version 10.8.21

[設定内容]

- IX2207のGigaEthernet0.1をWAN側、GigaEthernet2.0をLAN側とします。
- Si-R G120のether 1 1をWAN側、ether 2 1-8をLAN側とします。
- IX2207のLAN側に192.168.1.1/24を割り当てます。
- Si-RのLAN側に192.168.2.1/24を割り当てます。
- IX2207にはプロバイダより203.0.113.1の固定IPアドレスが割りてられるものとします。
- インターネットVPN(IPsec IKEv2)でセンター拠点間を接続します。



[設定]

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IXのISPのIDを設定してください。
- pwd-a@ispにはIXのISPのパスワードを設定してください。
- id-b@ispにはSi-RのISPのIDを設定してください。
- pwd-b@ispにはSi-RのISPのパスワードを設定してください。
- kyoten1にはSi-RのIPsecのID（装置識別情報）を設定してください。
- testにはIPsec共通鍵を設定してください。

■ NEC IX2207設定例

```
timezone +09 00
!
ip ufs-cache enable
ip route default GigaEthernet0.1
ip route 192.168.2.0/24 Tunnel0.0
!
ikev2 authentication psk id fqdn kyoten1 key char test
!
ppp profile isp
  authentication myname id-a@isp
  authentication password id-a@isp pwd-a@isp
!
interface GigaEthernet0.0
  no ip address
  shutdown
!
interface GigaEthernet1.0
  no ip address
  shutdown
!
interface GigaEthernet2.0
  ip address 192.168.1.1/24
  no shutdown
!
interface GigaEthernet0.1
  encapsulation pppoe
  auto-connect
  ppp binding isp
  ip address 203.0.113.1/32
  ip tcp adjust-mss auto
  ip napt enable
  ip napt static GigaEthernet0.1 udp 500
  ip napt static GigaEthernet0.1 50
  no shutdown
!
```

```
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet2.0
  ip tcp adjust-mss auto
  ikev2 child-lifetime 3600
  ikev2 dpd interval 10
  ikev2 local-authentication psk id ipv4 203.0.113.1
  ikev2 negotiation-direction responder
  ikev2 outgoing-interface GigaEthernet0.1
  ikev2 sa-lifetime 28800
  ikev2 peer any authentication psk id fqdn kyoten1
  no shutdown
```

■ Si-R G120設定

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 192.168.2.1/24 3
lan 1 vlan 2
remote 0 name PPPoE
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 0 203.0.113.1/32 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 192.168.2.1 500 any 500 17
remote 0 ip nat static 1 192.168.2.1 any any any 50
remote 0 ip msschange 1414
remote 1 name IX
remote 1 ap 0 name IX
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 ipsec type ikev2
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 ipsec ike lifetime 1h
remote 1 ap 0 ipsec ike esn disable
remote 1 ap 0 ike local-idtype fqdn
remote 1 ap 0 ike remote-idtype address
remote 1 ap 0 ike name local kyoten1
remote 1 ap 0 ike shared key text test
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 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike initial connect
remote 1 ap 0 ike dpd use on
remote 1 ap 0 tunnel remote 203.0.113.1
remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
remote 1 ip route 0 default 1 1
remote 1 ip msschange 1350
syslog facility 23
time zone 0900
resource system vlan 4089-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

[解説]

■ IX2207設定解説

timezone +09 00
タイムゾーンを設定します。

ip ufs-cache enable
UFSキャッシュを使用するように設定します。

ip route default GigaEthernet0.1
デフォルトルートをインターネット向きに設定します。

ip route 192.168.2.0/24 Tunnel0.0
拠点側LANへのルートをIPsecトンネル向きに設定します。

ikev2 authentication psk id fqdn kyoten1 key char test
IKEv2情報の相手装置IDと共有鍵(Pre-shared key)を設定します。

ppp profile isp
pppプロファイルを作成します。

authentication myname id-a@isp
authentication password 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。

interface GigaEthernet2.0
LAN側インターフェースを設定します。

ip address 192.168.1.1/24
IPアドレスを設定します。

no shutdown
インターフェースを有効にします。

interface GigaEthernet0.1
WAN側インターフェースの設定をします。

encapsulation pppoe
データリンク種別をPPPoEに設定します。

auto-connect
装置起動直後に自動接続するように設定します。

ppp binding isp
pppプロファイルを割り当てます。

ip address 203.0.113.1/32
プロバイダから割り当てられたIPアドレスを設定します。

ip tcp adjust-mss auto
MSS書き換えを設定します。

ip napt enable
NAPTを有効にします。

ip napt static GigaEthernet0.1 udp 500
ip napt static GigaEthernet0.1 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。

no shutdown
インターフェースを有効にします。

interface Tunnel0.0
IPsecトンネル用インターフェースの設定をします。

tunnel mode ipsec-ikev2
トンネルモードにIPsec(IKEv2)を設定します。

ip unnumbered GigaEthernet2.0
Unnumbered接続を設定します。

ip tcp adjust-mss auto
MSS書き換えを設定します。

ikev2 child-lifetime 3600
自動鍵交換用IPsec情報のSA 有効時間を3600秒(1時間)に設定します。

ikev2 dpd interval 10
DPD(Dead Pear Detection)を有効/送信間隔を10秒に設定します。

ikev2 local-authentication psk id ipv4 203.0.113.1
IKEv2情報の自装置識IDを設定します。

ikev2 negotiation-direction responder
ネゴシエーションをレスポンダ動作のみに設定します。

ikev2 outgoing-interface GigaEthernet0.1
IKEv2パケットの出力インターフェースを設定します。

ikev2 sa-lifetime 28800
IKEv2情報のSA 有効時間を28800秒(8時間)に設定します。

ikev2 peer any authentication psk id fqdn kyoten1
IKEv2情報の相手装置IDを設定します。

no shutdown
インターフェースを有効にします。

■ Si-R G120設定解説

ether 1 1 vlan untag 1
Ether 1 1インタフェースにVLAN1を割り当てます。

ether 2 1-4 vlan untag 2
Ether 2 1-4インタフェースにVLAN1を割り当てます。

lan 1 ip address 192.168.2.1/24 3
LAN1側にIPアドレスを設定します。

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 PPPoE
インターネット接続用インターフェースに名前(任意)を設定します。

remote 0 mtu 1454
フレッツ光ネクストでは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
VLAN IDとremote定義番号の関連付けを行います。

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 0 203.0.113.1/32 1 1
センターへのスタティックルートを設定します。

remote 0 ip nat mode multi any 1 5m
マルチNATを設定します。

remote 0 ip nat static 0 192.168.2.1 500 any 500 17
スタティックNATにより、IKEパケットを通す設定をします。

remote 0 ip nat static 1 192.168.2.1 any any any 50
スタティックNATにより、ESPパケットを通す設定をします。

remote 0 ip msschange 1414
MSS書き換えを設定します。

remote 1 name IX
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 IX
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
パケット転送方法としてIPsecを設定します。

remote 1 ap 0 ipsec type ikev2
IPsec情報のタイプにIPsec自動鍵交換(IKE Version2)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 ipsec ike lifetime 1h
自動鍵交換用IPsec情報のSA 有効時間を1時間に設定します。

remote 1 ap 0 ipsec ike esn disable
ENS(拡張シーケンス番号）を使用しないように設定します。

remote 1 ap 0 ike local-idtype fqdn
IKEv2情報の自装置IDタイプをFQDNに設定します。

remote 1 ap 0 ike remote-idtype address
IKEv2情報の相手装置IDタイプをアドレスに設定します。

remote 1 ap 0 ike name local kyoten1
IKEv2情報の自装置識IDを設定します。

remote 1 ap 0 ike shared key text test
IKEv2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
IKEv2セッション用暗号情報の暗号アルゴリズムにAES256を設定します。

remote 1 ap 0 ike proposal 0 hash hmac-sha256
IKEv2セッション用認証(ハッシュ)情報をSHA256に設定します。

remote 1 ap 0 ike proposal 0 pfs modp2048
IKEv2セッション用DH(Diffie-Hellman)グループにmodp2048を設定します。

remote 1 ap 0 ike proposal 0 prf hmac-sha256
IKEv2セッション用PRF(Pseudo Random Function)にSHA256を設定します。

remote 1 ap 0 ike proposal 0 lifetime 8h
IKEv2情報のSA 有効時間を8時間に設定します。

remote 1 ap 0 ike initial connect
対象回線の接続またはIPsec 対象パケットの送信を契機として、IPsec/IKE SAの確立動作を開始しするように設定します。

remote 1 ap 0 ike dpd use on
DPD(Dead Pear Detection)を有効に設定します。

remote 1 ap 0 tunnel remote 203.0.113.1
IPsecトンネルの送信先アドレスとしてセンターのアドレスを設定します。

remote 1 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
接続先セッション監視の設定をします。
192.168.2.1 : ICMP ECHOパケットの送信元IPアドレスです。
192.168.1.1 : ICMP ECHOパケットの宛先IPアドレスです。

remote 1 ip route 0 default 1 1
センター向きにデフォルトルートを設定します。

remote 1 ip msschange 1350
MSS書き換えの設定をします。

syslog facility 23
システムログ情報の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。

resource system vlan 4089-4094
装置内部資源として予約するVLAN IDを設定します。通常はこのままで構いません。

consoleinfo autologout 8h
telnetinfo autologout 5m
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。

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。