【データコネクト拠点間接続（双方向NAT）】

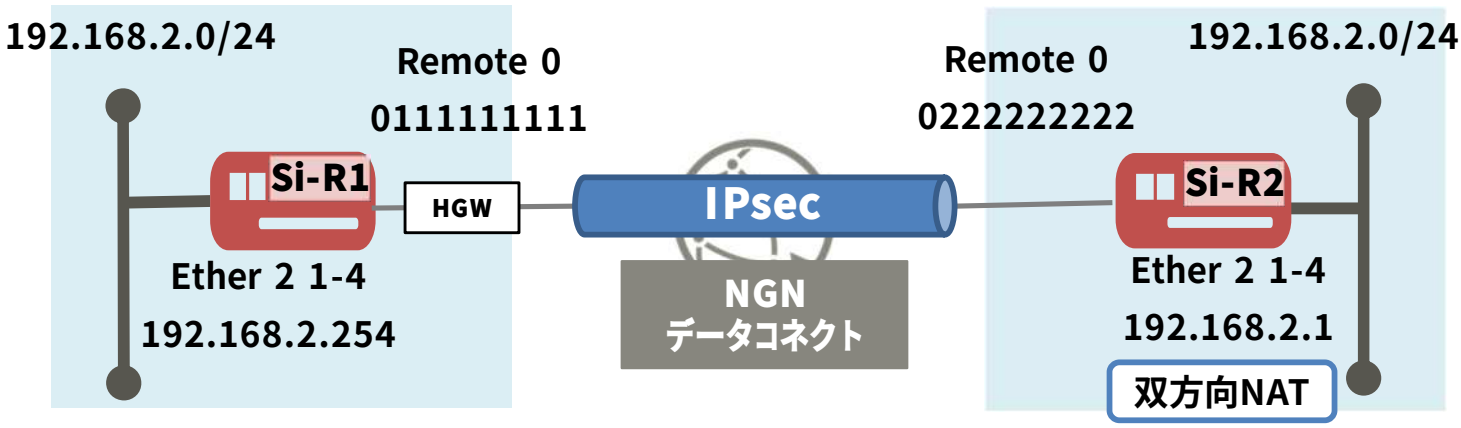
データコネクトで拠点間を接続する設定例です。
フレッツ 光ネクストのデータコネクトを利用して、拠点間をVPN（※）接続します。
データコネクトは、03等の市外局番から始まる電話番号を利用して、セキュアで安定したデータ通信を実現するサービスです。データコネクトの利用にあたっては、ひかり電話サービスの契約、およびナンバーディスプレイの契約が必要です。Si-R1はONU一体型ホームゲートウェイ(HGW)配下とし、Si-R2はONU直結とします。
※IPv4パケットをIPv6ヘッダでカプセリング(IPv4 over IPv6 IPsec tunnel)

[対象機種と版数]

Si-R Gシリーズ V20.50以降

[設定内容]

- Si-Rのether 1 1をWAN側、ether 2 1-4をLAN側とします。
- WAN側でDHCPクライアント（IPv4/IPv6）機能を有効にします。
- LAN側に192.168.2.254/24、192.168.2.1/24を割り当てるとします。
- IPv4 over IPv6 IPsec tunnelで拠点間を接続します。
- データコネクトの利用帯域を64Kとします。
- IPsec暗号化後にシェーピングを行うため、QoSを併用します。
- 重複したネットワーク同士の通信を実現するため、Si-R2のremoteインタフェースに双方向NATを設定します。
- Si-R2の拠点のアドレスを172.16.1.0/24に見せかけます。
  変換IPアドレス1 ： 192.168.2.1-192.168.2.254 ⇔ 172.16.1.1-172.16.1.254
- Si-R1の拠点のアドレスを172.16.2.0/24に見せかけます。
  変換IPアドレス2 ： 192.168.2.1-192.168.2.254 ⇔ 172.16.2.1-172.16.2.254



[設定]

・ sir2-keyにはIPsec鍵を設定してください。

■ Si-R1設定

```
ether 1 1 vlan untag 1001
ether 2 1-4 vlan untag 1002
lan 0 ip dhcp service client
lan 0 ip route 0 default dhcp 1 1
lan 0 ipv6 use on
lan 0 ipv6 address 0 dhcp@lan0::/64
lan 0 ipv6 route 0 default dhcp 1 1
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 ipv6 dhcp client option pd on
lan 0 vlan 1001
lan 1 ip address 192.168.2.254/24 3
lan 1 vlan 1002
remote 1 name dataconn
remote 1 shaping on 64k
remote 1 ap 0 name IPsec
remote 1 ap 0 datalink type dataconnect
remote 1 ap 0 dial 0 number 0222222222
remote 1 ap 0 dial 0 speed 64K
remote 1 ap 0 idle 1m
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 tel_key_id on
remote 1 ap 0 ike remote-idtype tel_key_id on
remote 1 ap 0 ike name local 0111111111
remote 1 ap 0 ike name remote 0222222222
remote 1 ap 0 ike shared key text sir2-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 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike nat-traversal use on
remote 1 ip route 0 172.16.1.0/24 1 1
remote 1 ip priority 0 any any any any any any express
remote 1 ip msschange 1280
syslog pri error,warn,info
syslog facility 23
```

time auto server 0.0.0.0 dhcp
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
loopback ip address 0 192.168.2.254
ngn sip use on
ngn sip bind lan 0
terminal charset SJIS

■Si-R2設定

```
ether 1 1 vlan untag 1001
ether 2 1-4 vlan untag 1002
lan 0 ip dhcp service client
lan 0 ip dhcp client option router off
lan 0 ipv6 use on
lan 0 ipv6 address 0 dhcp@lan0::/64
lan 0 ipv6 route 0 default dhcp 1 1
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 ipv6 dhcp client option pd on
lan 0 vlan 1001
lan 1 ip address 192.168.2.1/24 3
lan 1 vlan 1002
remote 1 name dataconn
remote 1 shaping on 64k
remote 1 ap 0 name IPsec
remote 1 ap 0 datalink type dataconnect
remote 1 ap 0 dial 0 number 0111111111
remote 1 ap 0 dial 0 speed 64K
remote 1 ap 0 idle 1m
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 tel_key_id on
remote 1 ap 0 ike remote-idtype tel_key_id on
remote 1 ap 0 ike name local 0222222222
remote 1 ap 0 ike name remote 0111111111
remote 1 ap 0 ike shared key text sir2-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 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike nat-traversal use on
remote 1 ip route 0 172.16.2.0/24 1 1
remote 1 ip nat mode static 10.1.1.1 1 5m
remote 1 ip nat static 0 192.168.2.1 any 172.16.1.1-172.16.1.254 any any
remote 1 ip nat destination 0 172.16.2.1 192.168.2.1-192.168.2.254
remote 1 ip priority 0 any any any any any any express
remote 1 ip msschange 1280
syslog pri error,warn,info
syslog facility 23
```

time auto server 0.0.0.0 dhcp
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
loopback ip address 0 192.168.2.1
ngn sip use on
ngn sip bind lan 0
terminal charset SJIS

[解説]

■ Si-R1設定解説

ether 1 1 vlan untag 1001
Ether 1 1インタフェースにVLAN1001を割り当てます。

ether 2 1-4 vlan untag 1002
Ether 2 1-4インタフェースにVLAN1002を割り当てます。

lan 0 ip dhcp service client
WAN側インターフェースに対して、IPv4 DHCPクライアント機能を有効にします。

lan 0 ip route 0 default dhcp 1 1
WAN側インタフェースでDHCP サーバから受け取ったREPLYの送信元をデフォルトルートに設定します。

lan 0 ipv6 use on
WAN側インタフェースでIPv6機能を有効にします。

lan 0 ipv6 address 0 dhcp@lan0::/64
WAN側インタフェースでIPv6 DHCP クライアントが取得したIPv6アドレスを設定します。

lan 0 ipv6 route 0 default dhcp 1 1
WAN側インタフェースでDHCP サーバから受け取ったREPLYの送信元をデフォルトルートに設定します。

lan 0 ipv6 dhcp service client
WAN側インターフェースに対して、IPv6 DHCPクライアント機能を有効にします。

lan 0 ipv6 dhcp client option na off
IPv6 DHCP クライアントのIPv6 アドレス要求を無効にします。

lan 0 ipv6 dhcp client option pd on
IPv6 DHCP クライアントのIPv6 アドレス要求をonに設定します。

lan 0 vlan 1001
VLAN ID とlan 定義番号の関連付けを行います。

lan 1 ip address 192.168.2.254/24 3
LAN1側にIPアドレスを設定します。

・192.168.2.254/24 ：lan1 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 1002
VLAN ID とlan 定義番号の関連付けを行います。

remote 1 name dataconn
Si-R2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 shaping on 64k
シェーピングを設定します。

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 dataconnect
パケット転送方法としてデータコネクトを設定します。

remote 1 ap 0 dial 0 number 0222222222
接続先の電話番号を設定します。

remote 1 ap 0 dial 0 speed 64K
接続時の通信速度を設定します。

remote 1 ap 0 idle 1m
無通信監視タイマを設定します。

remote 1 ap 0 ipsec type ikev2
IPsec情報のタイプにIPsec自動鍵交換(IKE Version2/IPsec Version3)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SHA2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 有効時間を設定します。

remote 1 ap 0 ipsec ike esn disable
IPsecV3情報のESN(拡張シーケンス番号)を要求なしに設定します。

remote 1 ap 0 ike local-idtype tel_key_id on
IKE Version2情報の自装置ID タイプを任意の文字列(NGN 網電話番号)に設定します。

remote 1 ap 0 ike remote-idtype tel_key_id on
IKE Version2情報の相手装置ID タイプを任意の文字列(NGN 網電話番号)に設定します。

remote 1 ap 0 ike name local 0111111111
IKE情報の自装置識別情報を設定します。

remote 1 ap 0 ike name remote 0222222222
IKE情報の相手装置識別情報を設定します。

remote 1 ap 0 ike shared key text sir2-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 ike proposal 0 prf hmac-sha256
IKE Version2ｾｯｼｮﾝ用prf(Pseudo Random Function)の設定にSHA2を設定します。

remote 1 ap 0 ike nat-traversal use on
IKE情報のNAT トラバーサルを利用する設定をします。

remote 1 ip route 0 172.16.1.0/24 1 1
ｽﾀﾃｨｯｸルートを設定します。

・172.16.1.0/24 ：対向装置Si-R2のLAN側ﾈｯﾄﾜｰｸ（宛先ｱﾄﾞﾚｽ変換前）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 priority 0 any any any any any any express
帯域制御の設定をします。ｼｪｰﾋﾟﾝｸﾞを使用する際に必要となります。

remote 1 ip msschange 1280
MSS書き換えの設定をします。

syslog pri error,warn,info
syslog facility 23
ｼｽﾃﾑﾛｸﾞ情報の出力情報 / 出力対象ﾌｧｼﾘﾃｨの設定をします。通常はこの値で構いません。

time auto server 0.0.0.0 dhcp
time zone 0900
DHCP サーバが広報する時刻提供サーバに従います。
ﾀｲﾑｿﾞｰﾝを設定します。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。

loopback ip address 0 192.168.2.254
loopbackのｱﾄﾞﾚｽを設定します。

ngn sip use on
ngn sip bind lan 0
SIPﾌﾟﾛﾄｺﾙを利用可否 / 利用するｲﾝﾀﾌｪｰｽを設定します。

terminal charset SJIS
ﾀｰﾐﾅﾙで使用する漢字ｺｰﾄﾞをShift JISｺｰﾄﾞに設定します。

■Si-R2設定解説

ether 1 1 vlan untag 1001
Ether 1 1インタフェースにVLAN1001を割り当てます。

ether 2 1-4 vlan untag 1002
Ether 2 1-4インタフェースにVLAN1002を割り当てます。

lan 0 ip dhcp service client
WAN側インターフェースに対して、IPv4 DHCPクライアント機能を有効にします。

lan 0 ip dhcp client option router off
IPv4 DHCP クライアントのRouter オプションを無効に設定します。

lan 0 ipv6 use on
WAN側インタフェースでIPv6機能を有効にします。

lan 0 ipv6 address 0 dhcp@lan0::/64
WAN側インタフェースでIPv6 DHCP クライアントが取得したIPv6アドレスを設定します。

lan 0 ipv6 route 0 default dhcp 1 1
WAN側インタフェースでDHCP サーバから受け取ったREPLYの送信元をデフォルトルートに設定します。

lan 0 ipv6 dhcp service client
WAN側インターフェースに対して、IPv6 DHCPクライアント機能を有効にします。

lan 0 ipv6 dhcp client option na off
IPv6 DHCP クライアントのIPv6 アドレス要求を無効にします。

lan 0 ipv6 dhcp client option pd on
IPv6 DHCP クライアントのIPv6 アドレス要求をonに設定します。

lan 0 vlan 1001
VLAN ID とlan 定義番号の関連付けを行います。

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

・192.168.2.1/24 ：lan1 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 1002
VLAN ID とlan 定義番号の関連付けを行います。

remote 1 name dataconn
Si-R1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 shaping on 64k
シェーピングを設定します。

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 dataconnect
パケット転送方法としてデータコネクトを設定します。

remote 1 ap 0 dial 0 number 0111111111
接続先の電話番号を設定します。

remote 1 ap 0 dial 0 speed 64K
接続時の通信速度を設定します。

remote 1 ap 0 idle 1m
無通信監視タイマを設定します。

remote 1 ap 0 ipsec type ikev2
IPsec情報のタイプにIPsec自動鍵交換(IKE Version2/IPsec Version3)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SHA2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 有効時間を設定します。

remote 1 ap 0 ipsec ike esn disable
IPsecV3情報のESN(拡張シーケンス番号)を要求なしに設定します。

remote 1 ap 0 ike local-idtype tel_key_id on
IKE Version2情報の自装置ID タイプを任意の文字列(NGN 網電話番号)に設定します。

remote 1 ap 0 ike remote-idtype tel_key_id on
IKE Version2情報の相手装置ID タイプを任意の文字列(NGN 網電話番号)に設定します。

remote 1 ap 0 ike name local 0222222222
IKE情報の自装置識別情報を設定します。

remote 1 ap 0 ike name remote 0111111111
IKE情報の相手装置識別情報を設定します。

remote 1 ap 0 ike shared key text sir2-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 ike proposal 0 prf hmac-sha256
IKE Version2ｾｯｼｮﾝ用prf(Pseudo Random Function)の設定にSHA2を設定します。

remote 1 ap 0 ike nat-traversal use on
IKE情報のNAT トラバーサルを利用する設定をします。

remote 1 ip route 0 172.16.2.0/24 1 1
ｽﾀﾃｨｯｸルートを設定します。

・172.16.2.0/24 ：対向装置Si-R1のLAN側ﾈｯﾄﾜｰｸ（宛先ｱﾄﾞﾚｽ変換前）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 nat mode static 10.1.1.1 1 5m
Remote1でNATを設定します。

・static ：静的NATです。
・10.1.1.1 ：NAT動作用のｱﾄﾞﾚｽです。
・1 ：変換後ｱﾄﾞﾚｽの個数です。
・5m ：NATﾃｰﾌﾞﾙの保持時間です。

remote 1 ip nat static 0 192.168.2.1 any 172.16.1.1-172.16.1.254 any any
static NATの設定をします。

・192.168.2.1 ：変換前の送信元IPｱﾄﾞﾚｽを指定します。
・any ：変換前のﾎﾟｰﾄ番号を設定します。
・172.16.1.1-172.16.1.254 ：変換後の送信元IPｱﾄﾞﾚｽの範囲を設定します。
・any ：変換後のﾎﾟｰﾄ番号を設定します。
・any ：ﾌﾟﾛﾄｺﾙ番号を設定します。

remote 1 ip nat destination 0 172.16.2.1 192.168.2.1-192.168.2.254
宛先NATの設定をします。

・172.16.2.1 ：変換前の宛先IPｱﾄﾞﾚｽを指定します。
・192.168.2.1-192.168.2.254 ：変換後の宛先IPｱﾄﾞﾚｽの範囲を設定します。

remote 1 ip priority 0 any any any any any any express
帯域制御の設定をします。ｼｪｰﾋﾟﾝｸﾞを使用する際に必要となります。

remote 1 ip msschange 1280
MSS書き換えの設定をします。

loopback ip address 0 192.168.2.1
loopbackのアドレスを設定します。

syslog pri error,warn,info
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。通常はこの値で構いません。

time auto server 0.0.0.0 dhcp
time zone 0900
DHCP サーバが広報する時刻提供サーバに従います。
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 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。

loopback ip address 0 192.168.2.1
loopbackのアドレスを設定します。

ngn sip use on
ngn sip bind lan 0
SIPプロトコルを利用可否 / 利用するインタフェースを設定します。

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。