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）

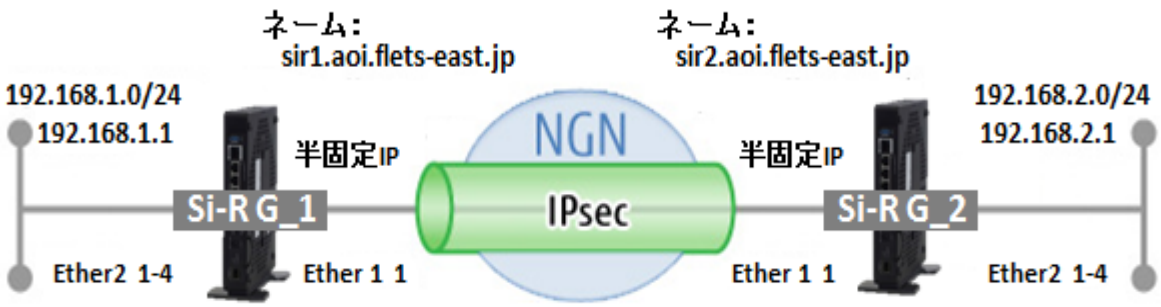
IPv6 IPoE方式（ひかり電話契約なし）で拠点間を接続する設定例です。

フレッツ 光ネクストのフレッツ・v6オプションを利用して、拠点間をVPN（※）接続します。
IPv6 IPoE方式（ひかり電話契約なし）の場合、/64のプレフィックスをひとつ配布されますが、このプレフィックスは半固定になります。フレッツ・v6オプションの「ネーム」設定を行うことで、配布されるプレフィックスが変更されても、自動でIPsecを再接続することが可能です。
なお、フレッツ・v6オプションの「ネーム」は、あらかじめサービス情報サイト(NGN IPv6)にて、登録が必要です。

※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 V3.00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側は、IPoEで/64のアドレス空間が割り当てられるとします。
・WAN側でDHCPクライアント機能を有効にします。
・LAN側に192.168.1.1/24、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。



[設定例]
・sir2-keyにはIPsec鍵を設定してください。

Si-R G_1設定例

```
ether 1 1 flowctl off off
ether 1 1 vlan untag 1
ether 2 1-4 flowctl off off
ether 2 1-4 vlan untag 2
lan 0 ipv6 use on
lan 0 ipv6 ifid 0:0:0:1
lan 0 ipv6 address 0 auto
lan 0 ipv6 ra mode recv
lan 0 ipv6 ra recv prefix-mode routers
lan 0 ipv6 filter 0 pass acl 0 reverse
lan 0 ipv6 filter 1 pass acl 1 reverse
lan 0 ipv6 filter 2 pass acl 2 reverse
lan 0 ipv6 filter 3 pass acl 3 reverse
lan 0 ipv6 filter 4 pass acl 4 reverse
lan 0 ipv6 filter default reject
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 vlan 1
lan 1 ip address 192.168.1.1/24 3
lan 1 vlan 2
remote 0 name vpn-hon
remote 0 ap 0 name honsya
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike encrypt aes-cbc-256
remote 0 ap 0 ipsec ike auth hmac-sha256
remote 0 ap 0 ipsec ike pfs modp1536
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text sir2-key
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 0 ap 0 ike proposal 0 hash hmac-sha256
remote 0 ap 0 ike proposal 0 pfs modp1536
remote 0 ap 0 tunnel local sir1.aoi.flets-east.jp
remote 0 ap 0 tunnel remote sir2.aoi.flets-east.jp
remote 0 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
remote 0 ip route 0 192.168.2.0/24 1 1
remote 0 ip msschange 1350
syslog facility 23
time zone 0900
proxydns source-port any
resource system vlan 4084-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
acl 0 ipv6 any any 17 any
acl 0 udp 500 500
acl 1 ipv6 any any 50 any
acl 2 ipv6 fe80::/16 any 17 any
acl 2 udp 546 547
acl 3 ipv6 any any 58 any
acl 4 ipv6 any any 17 any
acl 4 udp any 53
terminal charset SJIS
```

```
ether 1 1 flowctl off off
ether 1 1 vlan untag 1
ether 2 1-4 flowctl off off
ether 2 1-4 vlan untag 2
lan 0 ipv6 use on
lan 0 ipv6 ifid 0:0:0:1
lan 0 ipv6 address 0 auto
lan 0 ipv6 ra mode recv
lan 0 ipv6 ra recv prefix-mode routers
lan 0 ipv6 filter 0 pass acl 0 reverse
lan 0 ipv6 filter 1 pass acl 1 reverse
lan 0 ipv6 filter 2 pass acl 2 reverse
lan 0 ipv6 filter 3 pass acl 3 reverse
lan 0 ipv6 filter 4 pass acl 4 reverse
lan 0 ipv6 filter default reject
lan 0 ipv6 dhcp service client
lan 0 ipv6 dhcp client option na off
lan 0 vlan 1
lan 1 ip address 192.168.2.1/24 3
lan 1 vlan 2
remote 0 name vpn-hon
remote 0 ap 0 name honsya
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike encrypt aes-cbc-256
remote 0 ap 0 ipsec ike auth hmac-sha256
remote 0 ap 0 ipsec ike pfs modp1536
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text sir2-key
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 0 ap 0 ike proposal 0 hash hmac-sha256
remote 0 ap 0 ike proposal 0 pfs modp1536
remote 0 ap 0 tunnel local sir2.aoi.flets-east.jp
remote 0 ap 0 tunnel remote sir1.aoi.flets-east.jp
remote 0 ap 0 sessionwatch address 192.168.2.1 192.168.1.1
remote 0 ip route 0 192.168.1.0/24 1 1
remote 0 ip msschange 1350
syslog facility 23
time zone 0900
proxydns source-port any
resource system vlan 4084-4094
consoleinfo autologout 8h
telnetinfo autologout 5m
acl 0 ipv6 any any 17 any
acl 0 udp 500 500
acl 1 ipv6 any any 50 any
acl 2 ipv6 fe80::/16 any 17 any
acl 2 udp 546 547
acl 3 ipv6 any any 58 any
acl 4 ipv6 any any 17 any
acl 4 udp any 53
terminal charset SJIS
```

解説
Si-R_G_1設定解説

Si-R G1
ether 1 1 flowctl off off
#ether1 1ポートでフロー制御機能を無効にします。

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 flowctl off off
#ether2 1-4ポートでフロー制御機能を無効にします。

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 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 ifid 0:0:0:1
#WAN側インタフェースでインタフェースIDの設定を行います。
#v6オプションでname登録したインタフェースID(v6アドレスの後半部)を設定します。

lan 0 ipv6 address 0 auto
#WAN側インタフェースでIPv6アドレスを設定します。

lan 0 ipv6 ra mode recv
#RAメッセージの受信機能を有効にします。

lan 0 ipv6 ra recv prefix-mode routers
#RAメッセージ受信によりプレフィックスが変更された場合、アドレス切替を行うように設定します。

lan 0 ipv6 filter 0 pass acl 0 reverse
lan 0 ipv6 filter 1 pass acl 1 reverse
lan 0 ipv6 filter 2 pass acl 2 reverse
lan 0 ipv6 filter 3 pass acl 3 reverse
lan 0 ipv6 filter 4 pass acl 4 reverse
lan 0 ipv6 filter default reject
#IPv6フィルタリングにより、ACLに該当する通信を許可し、それ以外の通信を遮断する設定をします。

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offに設定します。

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 192.168.1.1/24 3
#LAN側IPアドレスを設定します。
#・192.168.1.1/24 : 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 vpn-hon
#Si-R G2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 ap 0 name honsya
#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 type ipsec
#パケット転送方法としてIPsecを設定します。

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

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-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 0 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 0 ap 0 ipsec ike pfs modp1536
#自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループにmodp1536を設定します。

remote 0 ap 0 ike mode main
#IKE 情報の交換モードをMain Modeに設定します。

remote 0 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 0 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 0 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 0 ap 0 ike proposal 0 pfs modp1536
#IKE情報のPFS使用時のDH（Diffie-Hellman）グループにmodp1536を設定します。

remote 0 ap 0 tunnel local sir1.aoi.flets-east.jp
#IPsecトンネルの送信元アドレスの設定をします。
#v6オプションにて設定した「ネーム」の値を記載します。

remote 0 ap 0 tunnel remote sir2.aoi.flets-east.jp
#IPsecトンネルの宛先アドレスの設定をします。
#v6オプションにて設定した「ネーム」の値を記載します。

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

remote 0 ip route 0 192.168.2.0/24 1 1
#対向装置Si-R_2のLAN側ネットワークへのスタティックルートを設定します。
#・192.168.2.0/24 : 対向装置Si-R G2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 0 ip msschange 1350
#トンネルインタフェースのMSS値を1350に書き換えます。

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 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。

proxydns source-port any
#DNSの送信元ポートを不定に設定します。

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。

acl 0 ipv6 any any 17 any
acl 0 udp 500 500
acl 1 ipv6 any any 50 any
#アクセスリストで、IPsecの設定をします。

acl 2 ipv6 fe80::/16 any 17 any
acl 2 udp 546 547
#アクセスリストでDHCPv6の設定をします。

acl 3 ipv6 any any 58 any
#アクセスリストで、ICMPv6の設定をします。

acl 4 ipv6 any any 17 any
acl 4 udp any 53
#アクセスリストでDNSの設定をします。

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。

解説
Si-R_G_2設定解説

ether 1 1 flowctl off off
#ether1 1ポートでフロー制御機能を無効にします。

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 flowctl off off
#ether2 1-4ポートでフロー制御機能を無効にします。

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 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 ifid 0:0:0:1
#WAN側インタフェースでインタフェースIDの設定を行います。
#v6オプションでname登録したインタフェースID(v6アドレスの後半部)を設定します。

lan 0 ipv6 address 0 auto
#WAN側インタフェースでIPv6アドレスを設定します。

lan 0 ipv6 ra mode recv
#RAメッセージの受信機能を有効にします。

lan 0 ipv6 ra recv prefix-mode routers
#RAメッセージ受信によりプレフィックスが変更された場合、アドレス切替を行うように設定します。

lan 0 ipv6 filter 0 pass acl 0 reverse
lan 0 ipv6 filter 1 pass acl 1 reverse
lan 0 ipv6 filter 2 pass acl 2 reverse
lan 0 ipv6 filter 3 pass acl 3 reverse
lan 0 ipv6 filter 4 pass acl 4 reverse
lan 0 ipv6 filter default reject
#IPv6フィルタリングにより、ACLに該当する通信を許可し、それ以外の通信を遮断する設定をします。

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offに設定します。

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 192.168.2.1/24 3
#LAN側IPアドレスを設定します。
#・192.168.2.1/24 : 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 vpn-shi
#Si-R G1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 ap 0 name shisya
#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 type ipsec
#パケット転送方法としてIPsecを設定します。

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

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-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 0 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 0 ap 0 ipsec ike pfs modp1536
#自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループにmodp1536を設定します。

remote 0 ap 0 ike mode main
#IKE 情報の交換モードをMain Modeに設定します。

remote 0 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 0 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 0 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 0 ap 0 ike proposal 0 pfs modp1536
#IKE情報のPFS使用時のDH（Diffie-Hellman）グループにmodp1536を設定します。

remote 0 ap 0 tunnel local sir2.aoi.flets-east.jp
#IPsecトンネルの送信元アドレスの設定をします。
#v6オプションにて設定した「ネーム」の値を記載します。

remote 0 ap 0 tunnel remote sir1.aoi.flets-east.jp
#IPsecトンネルの宛先アドレスの設定をします。
#v6オプションにて設定した「ネーム」の値を記載します。

remote 0 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 0 ip route 0 192.168.1.0/24 1 1
#対向装置Si-R_2のLAN側ネットワークへのスタティックルートを設定します。
#・192.168.1.0/24 : 対向装置Si-R G2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 0 ip msschange 1350
#トンネルインタフェースのMSS値を1350に書き換えます。

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 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。

proxydns source-port any
#DNSの送信元ポートを不定に設定します。

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。

acl 0 ipv6 any any 17 any
acl 0 udp 500 500
acl 1 ipv6 any any 50 any
#アクセスリストで、IPsecの設定をします。

acl 2 ipv6 fe80::/16 any 17 any
acl 2 udp 546 547
#アクセスリストでDHCPv6の設定をします。

acl 3 ipv6 any any 58 any
#アクセスリストで、ICMPv6の設定をします。

acl 4 ipv6 any any 17 any
acl 4 udp any 53
#アクセスリストでDNSの設定をします。

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。