# 【拠点間接続+インターネット接続(IPsec)】

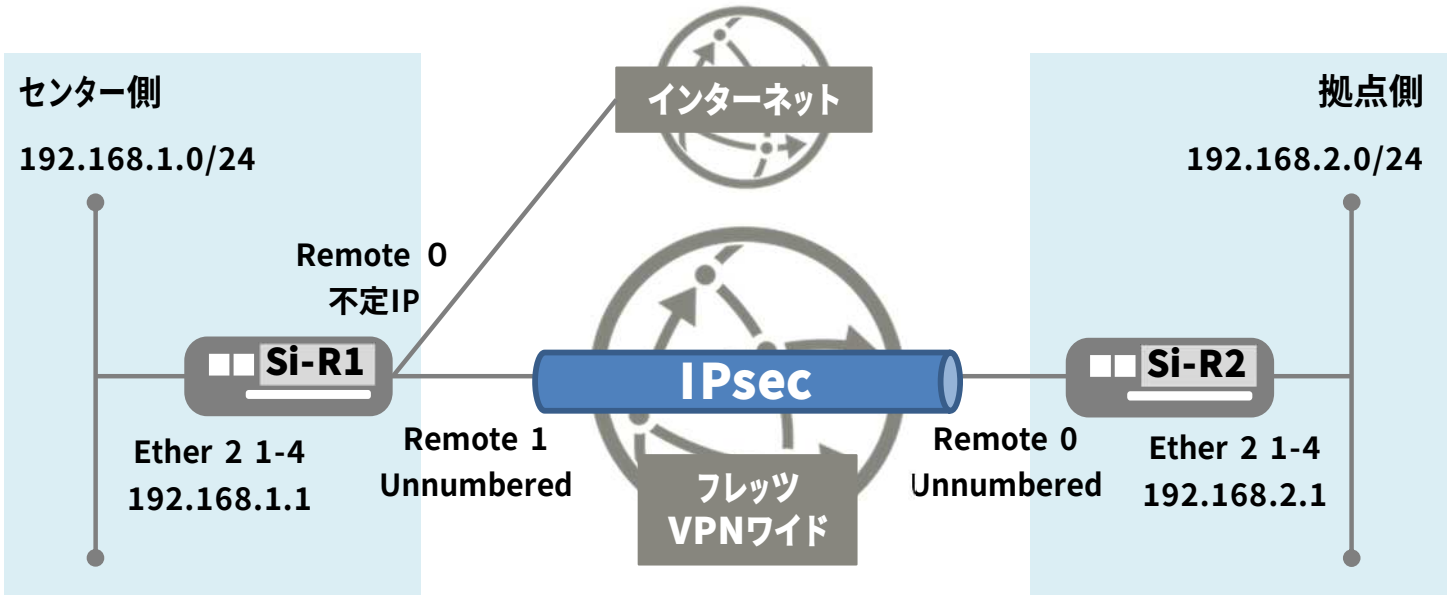
「フレッツ・VPNワイド」のLAN型払い出しタイプで拠点間を接続し、拠点からのインターネット接続のみ
センターとのIPsecトンネル経由で通信する設定例です。

## [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。
- インターネット側は不定IP設定とします。
- フレッツVPN側はUnnumbered設定とします。
- 拠点側からのインターネット接続のみIPsecトンネル経由でセンターから出て行きます。
- Si-R1のLAN側に192.168.1.1/24、Si-R2のLAN側に192.168.2.1/24を割り当てるとします。
- プロキシDNSを有効にします。



# [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Si-R1のインターネット接続のためのIDを設定してください。
- pwd-a@isp にはSi-R1のインターネット接続のためのパスワードを設定してください。
- id-a@flets にはSi-R1のフレッツ・VPNワイドのIDを設定してください。
- pwd-a@flets にはSi-R1のフレッツ・VPNワイドのパスワードを設定してください。
- id-b@flets にはSi-R2のフレッツ・VPNワイドのIDを設定してください。
- pwd-b@flets にはSi-R2のフレッツ・VPNワイドのパスワードを設定してください。
- sir-key にはIPsec 共有鍵を設定してください。

## ■ Si-R1設定

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 1 ip address 192.168.1.1/24 3
lan 1 ip dhcp service server
lan 1 ip dhcp info dns 192.168.1.1
lan 1 ip dhcp info address 192.168.1.2/24 253
lan 1 ip dhcp info time 1d
lan 1 ip dhcp info gateway 192.168.1.1
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 filter 0 reject acl 0 out
remote 0 ip filter 1 reject acl 1 out
remote 0 ip filter 2 reject acl 2 out
remote 0 ip filter 3 reject acl 3 out
remote 0 ip msschange 1414
remote 1 name fletsvpn
remote 1 mtu 1454
remote 1 ap 0 name PPPoE
remote 1 ap 0 datalink bind vlan 1
remote 1 ap 0 ppp auth send id-a@flets pwd-a@flets
remote 1 ap 0 keep connect
remote 1 ppp ipcp vjcomp disable
remote 1 ip msschange 1414
remote 2 name Si-R2
remote 2 ap 0 name ipsec
remote 2 ap 0 datalink type ipsec
remote 2 ap 0 ipsec type ike
```

```
remote 2 ap 0 ipsec ike protocol esp
remote 2 ap 0 ipsec ike encrypt aes-cbc-256
remote 2 ap 0 ipsec ike auth hmac-sha1
remote 2 ap 0 ipsec ike pfs modp1536
remote 2 ap 0 ike shared key text sir-key
remote 2 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 2 ap 0 tunnel local 192.168.1.1
remote 2 ap 0 tunnel remote 192.168.2.1
remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
remote 2 ip msschange 1300
remote 3 name policy
remote 3 mtu 1454
remote 3 ap 0 name fletsvpn
remote 3 ap 0 datalink type overlap
remote 3 ap 0 multiroute pattern 0 use 192.168.1.0/24 any any any any any
remote 3 ap 0 overlap to remote 1
remote 3 ap 1 name ipsec
remote 3 ap 1 datalink type overlap
remote 3 ap 1 overlap to remote 2
remote 3 ip route 0 192.168.2.0/24 1 1
acl 0 ip any any 6 any
acl 0 tcp any 137-139 yes
acl 1 ip any any 17 any
acl 1 udp any 137-139
acl 2 ip any any 6 any
acl 2 tcp any 445 yes
acl 3 ip any any 17 any
acl 3 udp any 445
syslog facility 23
time zone 0900
proxydns domain 0 any * any to 0
proxydns address 0 any to 0
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal pager enable
terminal charset SJIS
```

## ■ Si-R2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 ip dhcp service server
lan 1 ip dhcp info dns 192.168.1.1
lan 1 ip dhcp info address 192.168.2.2/24 253
lan 1 ip dhcp info time 1d
lan 1 ip dhcp info gateway 192.168.2.1
lan 1 vlan 2
remote 0 name fletsvpn
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@flets pwd-b@flets
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 192.168.1.0/24 1 1
remote 0 ip msschange 1414
remote 1 name Si-R1
remote 1 ap 0 name ipsec
remote 1 ap 0 datalink type ipsec
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-sha1
remote 1 ap 0 ipsec ike pfs modp1536
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 tunnel local 192.168.2.1
remote 1 ap 0 tunnel remote 192.168.1.1
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 1300
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal pager enable
terminal charset SJIS
```

# [解説]

## ■ Si-R1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VLAN2を割り当てます。

**lan 1 ip address 192.168.1.1/24 3**
LAN1側にIPアドレスを設定します。

・192.168.1.1/24：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 ip dhcp service server**
IPv4 DHCP サーバ機能を使用します。

**lan 1 ip dhcp info dns 192.168.1.1**
DHCP クライアントに配布する、DNS サーバの IP アドレスを指定します。

**lan 1 ip dhcp info address 192.168.1.2/24 253**
DHCP クライアントにリースする先頭アドレスと割り当てアドレス数を指定します。

**lan 1 ip dhcp info time 1d**
DHCP クライアントに配布する情報の有効時間を設定します。

**lan 1 ip dhcp info gateway 192.168.1.1**
DHCP クライアントに配布する、デフォルトルータの 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 internet**
インターネット接続用インターフェースの名前(任意)を設定します。

**remote 0 mtu 1454**
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インターフェースに設定します。

**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**
インターネット向けにデフォルトルートを設定します。

・1：metric値です。通常は1のままで構いません。
・1：distance値です。通常は1のままで構いません。

**remote 0 ip nat mode multi any 1 5m**
マルチNATの設定をします。

**remote 0 ip filter 0 reject acl 0 out**
**remote 0 ip filter 1 reject acl 1 out**
**remote 0 ip filter 2 reject acl 2 out**
**remote 0 ip filter 3 reject acl 3 out**
IPフィルタリングでアクセスリスト（acl定義）の条件に該当する通信を遮断する設定をします。

**remote 0 ip msschange 1414**
MSS値です。1414byte（注1）を設定します。
（注1）1454（MTU長）-40（TCP/IPヘッダー長）

**remote 1 name fletsvpn**
フレッツ・VPNワイドインターフェースの名前(任意)を設定します。

**remote 1 mtu 1454**
MTU長を1454byteに設定します。

**remote 1 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 1 ap 0 datalink bind vlan 1**
フレッツ・VPNワイド向けパケットの転送先をvlan1インターフェースに設定します。

**remote 1 ap 0 ppp auth send id-a@flets pwd-a@flets**
フレッツ・VPNワイドの認証ID、パスワードを設定します。

**remote 1 ap 0 keep connect**
フレッツ・VPNワイドへ常時接続します。

**remote 1 ppp ipcp vjcomp disable**
VJヘッダー圧縮を使用しない設定にします。

**remote 1 ip msschange 1414**
MSS値です。1414byte（注1）を設定します。
（注1）1454（MTU長）-40（TCP/IPヘッダー長）

**remote 2 name Si-R2**
Si-R_2向けのIPsecインターフェースの名前（任意）を設定します。

**remote 2 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 2 ap 0 datalink type ipsec**
パケット転送方法としてIPsecを設定します。

**remote 2 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 2 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 2 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 2 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 2 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 2 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 2 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 2 ap 0 tunnel local 192.168.1.1**
IPsecトンネルの送信元アドレスの設定をします。

**remote 2 ap 0 tunnel remote 192.168.2.1**
IPsecトンネルの送信先アドレスの設定をします。

**remote 2 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 2 ip msschange 1300**
MSS値に1300byteを設定します。

**remote 3 name policy**
overlapインターフェースの名前（任意）を設定します。

**remote 3 mtu 1454**
MTU長を1454byteに設定します。

**remote 3 ap 0 name fletsvpn**
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 3 ap 0 datalink type overlap**
パケット転送方法としてoverlapを設定します。

**remote 3 ap 0 multiroute pattern 0 use 192.168.1.0/24 any any any any any**
マルチルーティングのパケット振り分けパターンを設定します。

・192.168.1.0/24 :対象とする送信元IPアドレスです。
・any:対象とする送信元ポート番号です。
・any:対象とするあて先IPアドレスです。
・any:対象とするあて先ポート番号です。
・any:対象とするプロトコル番号です。

**remote 3 ap 0 overlap to remote 1**
overlap ap の実際の送出先を設定します。

**remote 3 ap 1 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 3 ap 1 datalink type overlap**
パケット転送方法としてoverlapを設定します。

**remote 3 ap 1 overlap to remote 2**
overlap ap の実際の送出先を設定します。

**remote 3 ip route 0 192.168.2.0/24 1 1**
対向装置Si-R2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-R2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。

**acl 0 ip any any 6 any**
**acl 0 tcp any 137-139 yes**
**acl 1 ip any any 17 any**
**acl 1 udp any 137-139**
**acl 2 ip any any 6 any**
**acl 2 tcp any 445 yes**
**acl 3 ip any any 17 any**
**acl 3 udp any 445**
netbios&Microsoft-DSの通信を対象とするアクセスリストを設定します。

**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 domain 0 any * any to 0**
**proxydns address 0 any to 0**
プロキシDNSの（順引き/逆引き）動作条件の設定します。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。

**terminal pager enable**
ページャー機能を使用します。

**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。

## ■ Si-R2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VLAN2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。

・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 ip dhcp service server**
IPv4 DHCP サーバ機能を使用します。

**lan 1 ip dhcp info dns 192.168.1.1**
DHCP クライアントに配布する、DNS サーバの IP アドレスを指定します。

**lan 1 ip dhcp info address 192.168.2.2/24 253**
DHCP クライアントにリースする先頭アドレスと割り当てアドレス数を指定します。

**lan 1 ip dhcp info time 1d**
DHCP クライアントに配布する情報の有効時間を設定します。

**lan 1 ip dhcp info gateway 192.168.2.1**
DHCP クライアントに配布する、デフォルトルータの 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 fletsvpn**
フレッツ・VPNワイドインターフェースの名前(任意)を設定します。

**remote 0 mtu 1454**
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**
フレッツ・VPNワイド向けパケットの転送先をvlan1インターフェースに設定します。

**remote 0 ap 0 ppp auth send id-b@flets pwd-b@flets**
フレッツ・VPNワイドの認証ID、パスワードを設定します。

**remote 0 ap 0 keep connect**
フレッツ・VPNワイドへ常時接続します。

**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 0 192.168.1.0/24 1 1**
対向装置Si-R2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-R1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 1414**
MSS値です。1414byte（注1）を設定します。
（注1）1454（MTU長）-40（TCP/IPヘッダー長）

**remote 1 name Si-R1**
Si-R_1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 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**
パケット転送方法としてIPsecを設定します。

**remote 1 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 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-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 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 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 tunnel local 192.168.2.1**
IPsecトンネルの送信元アドレスの設定をします。

**remote 1 ap 0 tunnel remote 192.168.1.1**
IPsecトンネルの送信先アドレスの設定をします。

**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**
WAN側インターフェースにデフォルトルートを設定します。
・1：metric値です。通常は1のままで構いません。
・1：distance値です。通常は1のままで構いません。

**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。

**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。

**terminal pager enable**
ページャー機能を使用します。

**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。