

# 技術情報：Si-R Gシリーズ設定例

「Microsoft Azure」との接続 複数セグメントからの接続（ポリシーベースIPsec）

Si-R Gシリーズで「Microsoft Azure」と複数セグメント（オンプレミス側）からポリシーベースIPsec接続する場合の設定例です。

Azure VPNゲートウェイ接続用のVPNデバイスとして、Microsoft社様と富士通共同でSi-R Gシリーズの検証を実施いたしました。

検証済みのVPNデバイスとデバイス構成ガイド

<https://docs.microsoft.com/ja-jp/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

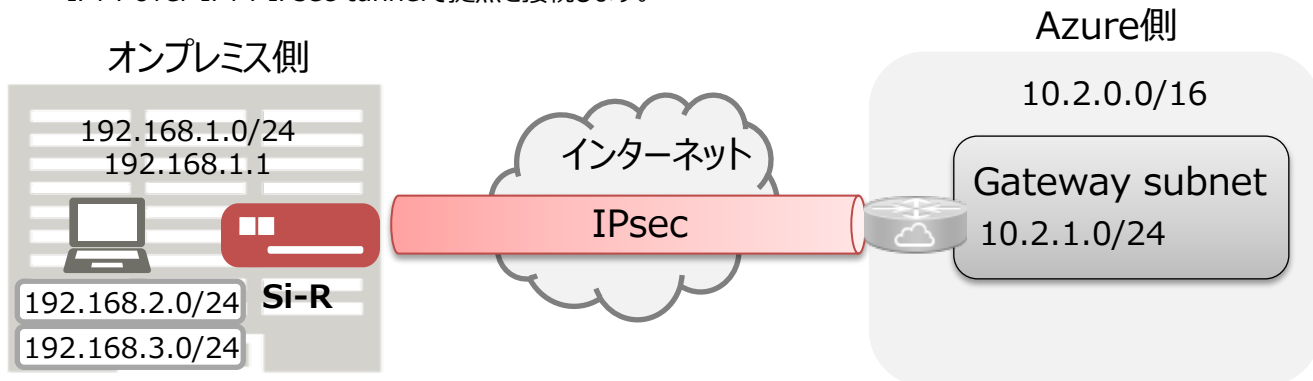
## [対象機種と版数]

Si-R Gシリーズ V20.14以降

Si-R Gシリーズ V04.12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、PPPoEで固定グローバルアドレスが1つ割り当てられるとします。
- ・Si-R LAN側に192.168.1.1/24を割り当てるとします。
- ・オンプレミス側では、192.168.1.0/24の他に、192.168.2.0/24、192.168.3.0/24のローカルネットワークが存在するとします（192.168.2.0/24、192.168.3.0/24のゲートウェイアドレスは、192.168.1.254を割り当て）。
- ・Azure側では、10.2.0.0/16の仮想ネットワークの中に、ゲートウェイサブネット10.2.1.0/24が存在するとします。
- ・IPv4 over IPv4 IPsec tunnelで拠点を接続します。



## オンプレミス側ネットワーク

項目	環境情報
接続メディア	FTTHなど
接続プロトコル	PPPoE
WAN	固定グローバルアドレス(XXX.XXX.XXX.XXX)
LAN	192.168.1.0/24 192.168.2.0/24 192.168.3.0/24

オンプレミス側ネットワークでは、Si-RでPPPoE(アドレス固定)を行います。  
固定のアドレスを使用して、Azureネットワークに対して、IPsec接続を動作させます。

## Microsoft Azure側ネットワーク

サブネット名	アドレス範囲
Gateway subnet	10.2.1.0/24

Microsoft Azure 仮想ネットワークでは、10.2.0.0/16のアドレス空間の中に、1つのサブネットが存在します。

## オンプレミス(Si-R)での設定

本章では、Microsoft AzureとIPsec接続するためのSi-Rの設定について解説します。

Azure側の設定については以下を参照ください。

<https://docs.microsoft.com/ja-jp/azure/vpn-gateway/tutorial-site-to-site-portal>

チュートリアル: Azure Portal でサイト間接続を作成する

## IPsec設定項目

IPsec設定値については、以下のような内容になります。

Azure側のIPsec/IKEポリシーで設定される最優先パラメータ、かつSi-Rがサポートしているパラメータを指定しています。

### IKEフェーズ1

項目	設定値
自側トンネルエンドポイントアドレス	xxx.xxx.xxx.xxx
相手側トンネルエンドポイントアドレス	yyy.yyy.yyy.yyy ポータルサイトより確認
lan側ローカルアドレス	192.168.1.1/24
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha256
DHグループ	group 2(modp1024)
PRF(疑似乱数関数)	hmac-sha1
IKE SA有効時間	8h
NAT-TRAVERSAL	on
DPD	off
IKEセッション共有鍵	test ポータルサイトに設定した値を使用

### IKEフェーズ2

項目	設定値
IPsec情報のセキュリティプロトコル	esp
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha256
IPsec SA 有効時間	1h
IPsec SA 有効パケット量	100000m
DHグループ	off
IPsec対象範囲(送信元)	192.168.1.0/24 192.168.2.0/24 192.168.3.0/24
IPsec対象範囲(宛先)	10.2.0.0/16

## config

configの全体像としては以下のような内容になります。

configは大きく分けて、etherポート定義、lan定義、PPPoE定義、IPsec定義に分けられます。それぞれについて順を追って説明していきます。

```
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 route 0 192.168.2.0/24 192.168.1.254 1 1
lan 1 ip route 1 192.168.3.0/24 192.168.1.254 1 1
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@isp pass@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip address local xxx.xxx.xxx.xxx
remote 0 ip route 0 default 1 1
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
remote 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
remote 0 ip nat static 2 xxx.xxx.xxx.xxx 4500 xxx.xxx.xxx.xxx 4500 17
remote 0 ip msschange 1414
remote 1 name Azure
remote 1 ap 0 name IPsec1
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 multiroute pattern 0 use 192.168.1.0/24 any 10.2.0.0/16 any any any
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 range 192.168.1.0/24 10.2.0.0/16
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 lifetime 1h
remote 1 ap 0 ipsec ike lifebyte 100000m
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 modp1024
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike nat-traversal use on
remote 1 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 1 ap 0 tunnel remote yyy.yyy.yyy.yyy
```

```
remote 1 ap 1 name IPsec2
remote 1 ap 1 datalink type ipsec
remote 1 ap 1 multiroute pattern 0 use 192.168.2.0/24 any 10.2.0.0/16 any any any
remote 1 ap 1 keep connect
remote 1 ap 1 ipsec type ike
remote 1 ap 1 ipsec ike protocol esp
remote 1 ap 1 ipsec ike range 192.168.2.0/24 10.2.0.0/16
remote 1 ap 1 ipsec ike encrypt aes-cbc-256
remote 1 ap 1 ipsec ike auth hmac-sha256
remote 1 ap 1 ipsec ike lifetime 1h
remote 1 ap 1 ipsec ike lifebyte 100000m
remote 1 ap 1 ike bind ap 0
remote 1 ap 2 name IPsec3
remote 1 ap 2 datalink type ipsec
remote 1 ap 2 multiroute pattern 0 use 192.168.3.0/24 any 10.2.0.0/16 any any any
remote 1 ap 2 keep connect
remote 1 ap 2 ipsec type ike
remote 1 ap 2 ipsec ike protocol esp
remote 1 ap 2 ipsec ike range 192.168.3.0/24 10.2.0.0/16
remote 1 ap 2 ipsec ike encrypt aes-cbc-256
remote 1 ap 2 ipsec ike auth hmac-sha256
remote 1 ap 2 ipsec ike lifetime 1h
remote 1 ap 2 ipsec ike lifebyte 100000m
remote 1 ap 2 ike bind ap 0
remote 1 ip route 0 10.2.0.0/16 1 1
remote 1 ip msschange 1350
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
terminal charset SJIS
```

## etherポートの設定

各etherポートにVLAN(untag)を割り当てます。これは、後のlan定義や、PPPoEの定義と結びつきます。

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
```

wan側のポートに対してvlan 1を、lan側のポートに対してvlan 2を設定します。

## PPPoEの設定

WAN側にPPPoEの設定をします。PPPoEの送出先としてvlan 1(ether 1 1)を指定します。

```
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@isp pass@isp
remote 0 ap 0 keep connect
remote 0 ppp ipcp vjcomp disable
remote 0 ip address local xxx.xxx.xxx.xxx
remote 0 ip msschange 1414
```

項目	設定値
ID(PPPoE)	id@isp
PASS(PPPoE)	pass@isp

mtu値、mss値については回線により異なります。回線側にご確認ください。

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

PPPoEのインタフェースに対してデフォルトルートを設定します。

## ファイアウォールの設定

PPPoEの定義にファイアウォールの設定を追加します。

```
remote 0 ip nat mode multi any 1 5m
remote 0 ip nat static 0 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
remote 0 ip nat static 1 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
remote 0 ip nat static 2 xxx.xxx.xxx.xxx 4500 xxx.xxx.xxx.xxx 4500 17
```

mode multiの設定により、NAPTの設定が有効になります。  
IPsec/IKEパススルーの設定を行います。

## lan側アドレスの設定

lan側のアドレスを192.168.1.1/24に設定します。このlanインタフェースはvlan 2の物理ポートと結びつきます。

lan側のスタティックルートを設定します。

```
lan 1 ip address 192.168.1.1/24 3
lan 1 ip route 0 192.168.2.0/24 192.168.1.254 1 1
lan 1 ip route 1 192.168.3.0/24 192.168.1.254 1 1
lan 1 vlan 2
```

## IPsecの設定（送信元：192.168.1.0/24）

まず、設定するインタフェースをIPsecができるようにするため、インタフェースの転送方式、IPsecタイプを設定します。

multiroute patternで、このap定義を利用して送信するネットワークを設定します。

IPsecを常時接続に設定します。

```
remote 1 ap 0 name IPsec1
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 multiroute pattern 0 use 192.168.1.0/24 any 10.2.0.0/16 any any any
remote 1 ap 0 keep connect
```

## IKEフェーズ1

[IPsec設定項目](#)：IKEフェーズ1表にて提示した内容を設定します。

```
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 modp1024
remote 1 ap 0 ike proposal 0 lifetime 8h
remote 1 ap 0 ike nat-traversal use on
remote 1 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 1 ap 0 tunnel remote yyy.yyy.yyy.yyy
```

事前共有鍵(ike shared key)、相手側トンネルエンドポイント(tunnel remote)については、Microsoft Azureポータルサイトにて確認した内容を設定します。

## IKEフェーズ2（送信元：192.168.1.0/24）

[IPsec設定項目](#)：IKEフェーズ2表にて提示した内容を設定します。

```
remote 1 ap 0 ipsec type ike
remote 1 ap 0 ipsec ike protocol esp
remote 1 ap 0 ipsec ike range 192.168.1.0/24 10.2.0.0/16
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 lifetime 1h
remote 1 ap 0 ipsec ike lifebyte 100000m
```

ike range設定の対向セグメントは、ゲートウェイサブネットではなく、仮想ネットワークのセグメントを設定してください。

### IPsecの設定（送信元：192.168.2.0/24）

まず、設定するインタフェースをIPsecができるようにするため、インタフェースの転送方式、IPsecタイプを設定します。

multiroute patternで、このap定義を利用して送信するネットワークを設定します。  
IPsecを常時接続に設定します。

```
remote 1 ap 1 name IPsec2
remote 1 ap 1 datalink type ipsec
remote 1 ap 1 multiroute pattern 0 use 192.168.2.0/24 any 10.2.0.0/16 any any any
remote 1 ap 1 keep connect
```

### IKEフェーズ2（送信元：192.168.2.0/24）

[IPsec設定項目](#)：IKEフェーズ2表にて提示した内容を設定します。

```
remote 1 ap 1 ipsec type ike
remote 1 ap 1 ipsec ike protocol esp
remote 1 ap 1 ipsec ike range 192.168.2.0/24 10.2.0.0/16
remote 1 ap 1 ipsec ike encrypt aes-cbc-256
remote 1 ap 1 ipsec ike auth hmac-sha256
remote 1 ap 1 ipsec ike lifetime 1h
remote 1 ap 1 ipsec ike lifebyte 100000m
remote 1 ap 1 ike bind ap 0
```

ike range設定の対向セグメントは、ゲートウェイサブネットではなく、仮想ネットワークのセグメントを設定してください。

### IPsecの設定（送信元：192.168.2.0/24）

まず、設定するインタフェースをIPsecができるようにするため、インタフェースの転送方式、IPsecタイプを設定します。

multiroute patternで、このap定義を利用して送信するネットワークを設定します。  
IPsecを常時接続に設定します。

```
remote 1 ap 2 name IPsec3
remote 1 ap 2 datalink type ipsec
remote 1 ap 2 multiroute pattern 0 use 192.168.3.0/24 any 10.2.0.0/16 any any any
remote 1 ap 2 keep connect
```

### IKEフェーズ2（送信元：192.168.3.0/24）

[IPsec設定項目](#)：IKEフェーズ2表にて提示した内容を設定します。

```
remote 1 ap 2 ipsec type ike
remote 1 ap 2 ipsec ike protocol esp
remote 1 ap 2 ipsec ike range 192.168.3.0/24 10.2.0.0/16
remote 1 ap 2 ipsec ike encrypt aes-cbc-256
remote 1 ap 2 ipsec ike auth hmac-sha256
remote 1 ap 2 ipsec ike lifetime 1h
remote 1 ap 2 ipsec ike lifebyte 100000m
remote 1 ap 2 ike bind ap 0
```

ike range設定の対向セグメントは、ゲートウェイサブネットではなく、仮想ネットワークのセグメントを設定してください。

## その他

ルート設定、MSS値の設定をします。このMSS値はカプセル化の方式によって変わります。今回は1350を設定します。

```
remote 1 ip route 0 10.2.0.0/16 1 1
remote 1 ip msschange 1350
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
```

ポリシーベースでは、DPDがサポートされてません。そのため、Azure GWとSi-R間で、IPsecSAの不一致が生じ、通信が行えない事象が発生した場合もすぐに検知することができません。

Azure GWは、トンネル経由のトラフィックが5分以上アイドル状態になると、トンネルを破棄します。どちらかの方向のトラフィック フローが開始されると再確立されますが、この間通信を行うことができません。

上記事象を回避するために、Azure内の仮想サーバ等、ICMPに応答する装置（Azureの仮想ネットワークゲートウェイ宛は不可）がある場合は、接続先セッション監視の設定を追加することを推奨します。

例) remote 1 ap 0 sessionwatch address 192.168.1.1 a.a.a.a  
(a.a.a.a→仮想サーバなど)

以上で設定が完了です。

最後に設定をsaveして再起動します。

```
save
reset
```



Si-Rを接続し、少し時間がたってからshow access-pointコマンドを実行して確認してください。正常にIPsecが確立できていれば下記のような結果が得られます。

```
#show access-point
remote 1 ap 0          : Azure.IPsec
  status               : connected
  since                : Jul 8 09:45:24 2022
  speed                : not available
  send traffic         : not available
  receive traffic      : not available
  type                 : IPsec/IKE
  IKE Version          : 1
  IKE SA               : established
  IPsec SA             : established

remote 1 ap 1          : Azure.IPsec2
  status               : connected
  since                : Jul 8 09:45:27 2022
  speed                : not available
  send traffic         : not available
  receive traffic      : not available
  type                 : IPsec/IKE
  IKE Version          : 1
  IKE SA               : established
  IPsec SA             : established

remote 1 ap 2          : Azure.IPsec3
  status               : connected
  since                : Jul 8 09:45:27 2022
  speed                : not available
  send traffic         : not available
  receive traffic      : not available
  type                 : IPsec/IKE
  IKE Version          : 1
  IKE SA               : established
  IPsec SA             : established
```

IKE SA,IPsec SAともにestablished、status connectedとなっていれば接続ができています。