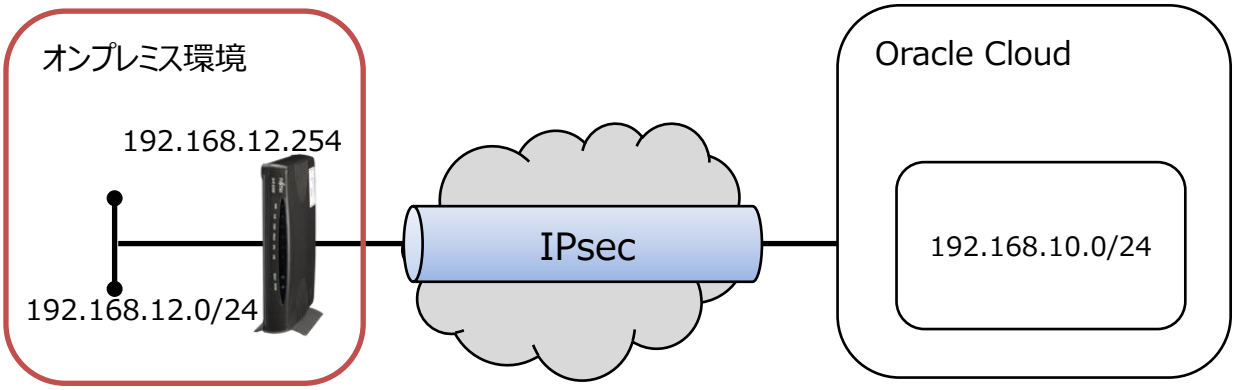
技術情報：Si-R/Si-R brinシリーズ設定例

「Oracle Cloud Infrastructure Classic」との接続

Si-R Gシリーズで「Oracle Cloud Infrastructure Classic」にIPsec接続する場合の設定例です。

本設定例は、弊社で独自に接続試験（2018年7月）を行った結果を元に作成しております。今後、仕様変更などの可能性もありますので、ご注意ください。



[対象機種と版数]
Si-R Gシリーズ　V04.04

[設定内容]
・Si-R Gのether 1 1をWAN側、ether 2 1-4をLAN側とする。
・WAN側は、専用線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のLAN側に192.168.12.254/24を割り当てます。
・Oracle側では、192.168.10.0/24を割り当てます。
・IPv4 over IPv4 IPsec tunnelで拠点間を接続します。

オンプレミス側ネットワーク

オンプレミス側ネットワークでは、Si-Rで専用線を使用します。
固定のアドレスを使用して、Oracleネットワークに対して、IPsec接続を動作させます。

項目	環境情報
接続メディア	FTTH(専用線)
WAN（固定グローバルIPアドレス）	xxx.xxx.xxx.xxx
LAN	192.168.12.254/24

Oracle Cloud側ネットワーク

オンプレミス側とOracle Cloud側でのIPsecにより、IPsecトンネルを介して、オンプレミスからOracle側のサブネットに対して通信をすることが可能となります。

項目	環境情報
Oracle Cloud側のプライベートIP範囲	192.168.10.0/24
WAN（固定グローバルIPアドレス）	yyy.yyy.yyy.yyy

[Oracle Cloudでの設定]

本章ではオンプレミス側とのIPsec接続をするためのOracleの設定について説明します。
IPsec接続するための簡易的な設定のため、セキュリティ・ルールなどは、別途設定ください。

［設定例］

IPネットワーク作成(Compute Classic > ネットワーク > IPネットワーク> IPネットワーク)
名前　　：nsc3 [任意文字列]
IPアドレス接頭辞　　：192.168.10.0/24 [Oracle Cloud側のプライベートIP範囲(CIDR)]
IP交換　　：未設定

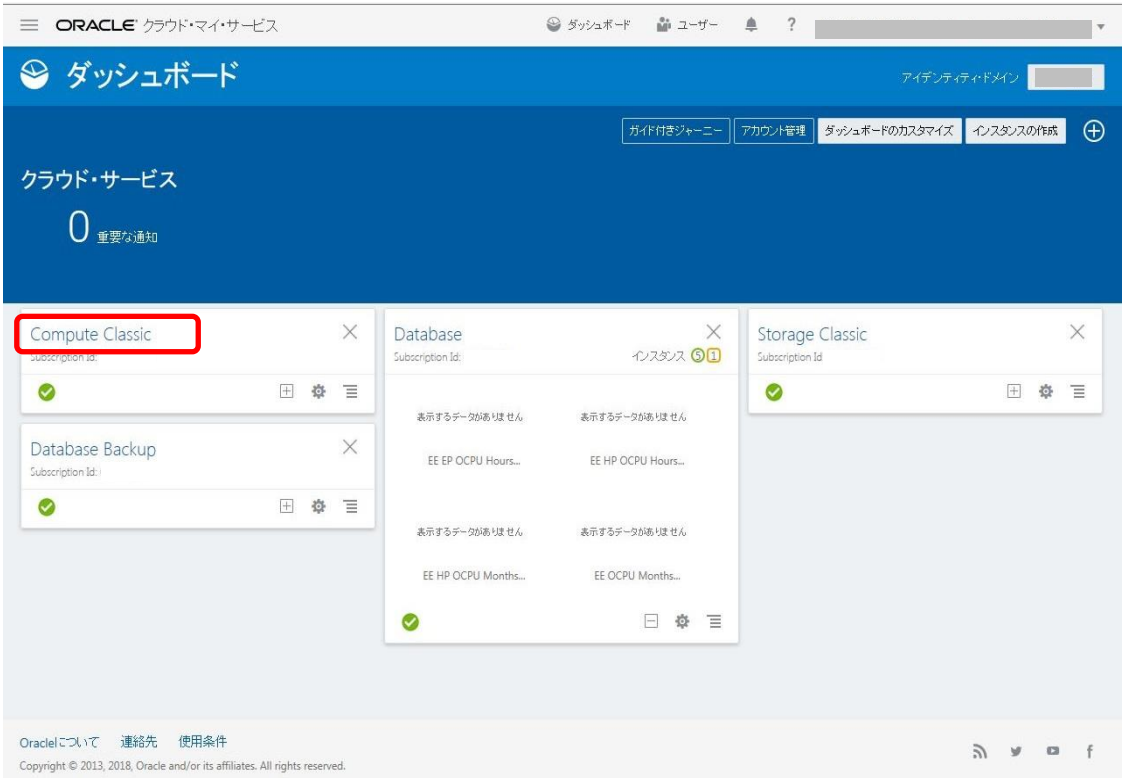
仮想NICセット作成(Compute Classic > ネットワーク > IPネットワーク> 仮想NICセット)
名前　　：nsc [任意文字列]

アクセス制御リスト作成(Compute Classic > ネットワーク > IPネットワーク> アクセス制御リスト)
名前　　：xxxx [任意文字列]

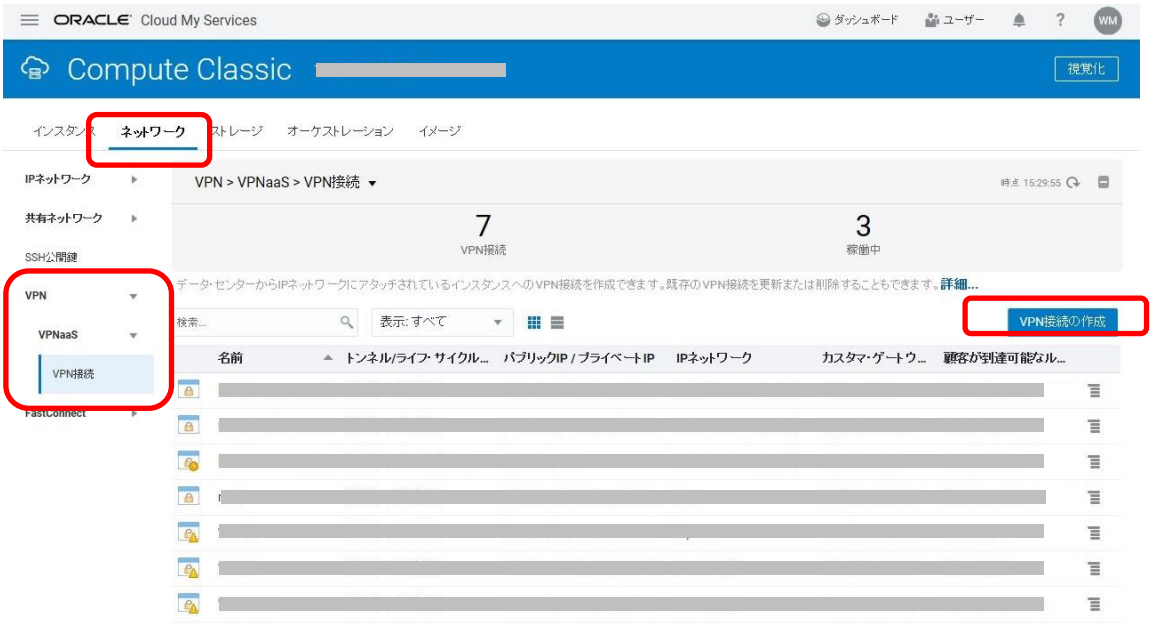
セキュリティ・ルール作成(Compute Classic > ネットワーク > IPネットワーク> セキュリティ・ルール)
名前　　：yyyy [任意文字列]
タイプ　　：送信
アクセス制御リスト　：xxxx [前項で作成したアクセス制御リスト]
ソースvNICセット　：nsc [前項で作成した仮想NICセット]
宛先vNICset　：未設定
名前　　：zzzz [任意文字列]
タイプ　　：受信
アクセス制御リスト　：xxxx [前項で作成したアクセス制御リスト]
ソースvNICセット　：nsc [前項で作成した仮想NICセット]
宛先vNICset　：nsc [前項で作成した仮想NICセット]

VPN接続の作成

Oracle Cloud ポータルサイトにログインし、[Compute Classic]を選択します。



タブの[ネットワーク]を選択、[VPN]-[VPNaaS]-[VPN接続]を選択し、
[VPN接続の作成]を押下します。



IPsecの設定をします。

設定内容	設定値
名前	nsc3
IPネットワーク	nsc(192.168.10.0/24)
vNICset	nsc
カスタマ・ゲートウェイ	xxx.xxx.xxx.xxx Si-R側のグローバルアドレス
顧客が到達可能なルート	192.168.12.0/24
事前共有鍵	任意(Si-R側でも同一設定を使用)
IKE ID	空欄

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。

IKEフェーズ1

設定内容	設定値
IKE暗号化	AES 256
IKEハッシュ	SHA2 256
IKE DHグループ	14
IKE存在期間	28800

IKEフェーズ2

設定内容	設定値
ESP暗号化	AES 256
ESPハッシュ	SHA2 256
IPSEC存在期間	3600

以上で仮想ネットワークの作成が完了します。

[オンプレミス(Si-R)の設定]

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

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。

IKEフェーズ1

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	8h
DHグループ	14
IPsec対象範囲(送信元)	192.168.12.0/24
IPsec対象範囲(宛先)	192.168.10.0/24

IKEフェーズ2

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 Si-R側グローバルアドレス
相手側トンネルエンドポイントアドレス	yyy.yyy.yyy.yyy Oracle側グローバルアドレス
lan側ローカルアドレス	192.168.12.254/24
暗号情報	aes-cbc-256
認証(ハッシュ)情報	hmac-sha256
DHグループ	off
PRF(疑似乱数関数)	hmac-sha254
IKE SA有効時間	1h
IKEセッション共有鍵	Oracle側と同じ値を使用

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、IPsec定義に分けられます。
それぞれについて説明します。

```
ether 1 1 vlan untag 1
ether 2 1-4 vlan untag 2
lan 0 ip address xxx.xxx.xxx.xxx/xx 3
lan 0 ip route 0 default <Si-Rグローバル側ゲートウェイ> 1 1
lan 0 ip nat mode multi xxx.xxx.xxx.xxx 1 5m
lan 0 ip nat static 0 xxx.xxx.xxx.xxx 500 xxx.xxx.xxx.xxx 500 17
lan 0 ip nat static 1 xxx.xxx.xxx.xxx any xxx.xxx.xxx.xxx any 50
lan 0 vlan 1
lan 1 ip address 192.168.12.254/24 3
lan 1 vlan 2
remote 0 name Oracle
remote 0 ap 0 name ipsec
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 keep connect
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range 192.168.12.0/24 192.168.10.0/24
remote 0 ap 0 ipsec ike encrypt aes-cbc-256
remote 0 ap 0 ipsec ike auth hmac-sha256
remote 0 ap 0 ike shared key text erfELAyPBMAMsPeIX encrypted
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 0 ap 0 ike proposal 0 pfs modp2048
remote 0 ap 0 ike proposal 0 lifetime 1h
remote 0 ap 0 ike initial connect
remote 0 ap 0 ike dpd use on
remote 0 ap 0 tunnel local xxx.xxx.xxx.xxx
remote 0 ap 0 tunnel remote yyy.yyy.yyy.yyy
remote 0 ip route 0 192.168.10.0/24 1 1
remote 0 ip msschange 1350
syslog facility 23
time zone 0900
resource system vlan 4089-4094
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。

lan側アドレスの設定
lan側のアドレスを192.168.12.254/24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 1 ip address 192.168.12.125424 3
lan 1 vlan 2
```

IPsecの設定
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。

```
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 ipsec type ike
```

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 0 ap 0 ike shared key text erfELAyPBMAMsPeIX encrypted
remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
remote 0 ap 0 ike proposal 0 pfs modp2048
remote 0 ap 0 ike proposal 0 lifetime 1h
remote 0 ap 0 ike initial connect
remote 0 ap 0 ike dpd use on
remote 0 ap 0 tunnel local <Si-R側グローバルIPアドレス>
remote 0 ap 0 tunnel remote <Oracle側グローバルIPアドレス>
```

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、Oracle Cloudサイトにて確認した内容を設定します。
lifetimeは、Oracle側の値を超えないように設定してください。

IKEフェーズ2
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 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range 192.168.12.0/24 192.168.10.0/24
remote 0 ap 0 ipsec ike encrypt aes-cbc-256
remote 0 ap 0 ipsec ike auth hmac-sha256
```

ike range設定の対向側のセグメントについては注意が必要です。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。
lifetimeは、Oracle側の値を超えないように設定してください。

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 10.0.0.0/8 1 1
remote 1 ip msschange 1350
```

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
```

[Oracle Cloudの状態確認]

[VPN]-[VPNaaS]-[VPN接続]に画面に表示される項目を確認します。

[トンネル]：オンプレミスとIPSecが確立している場合、[稼働中]と表示されます。
[パブリックIP]：Oracle側のグローバルアドレスが表示されます。

[IPsec確立確認方法]

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 0 ap 0          : Oracle.ipsec
  status               : connected
    since              : Jul 17 13:38:04 2018
  speed                : not available
    send traffic       : not available
    receive traffic    : not available
  type                 : IPsec/IKE
    IKE Version        : 1
    exchange type      : main
    IKE SA             : established
    IPsec SA           : established
```

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