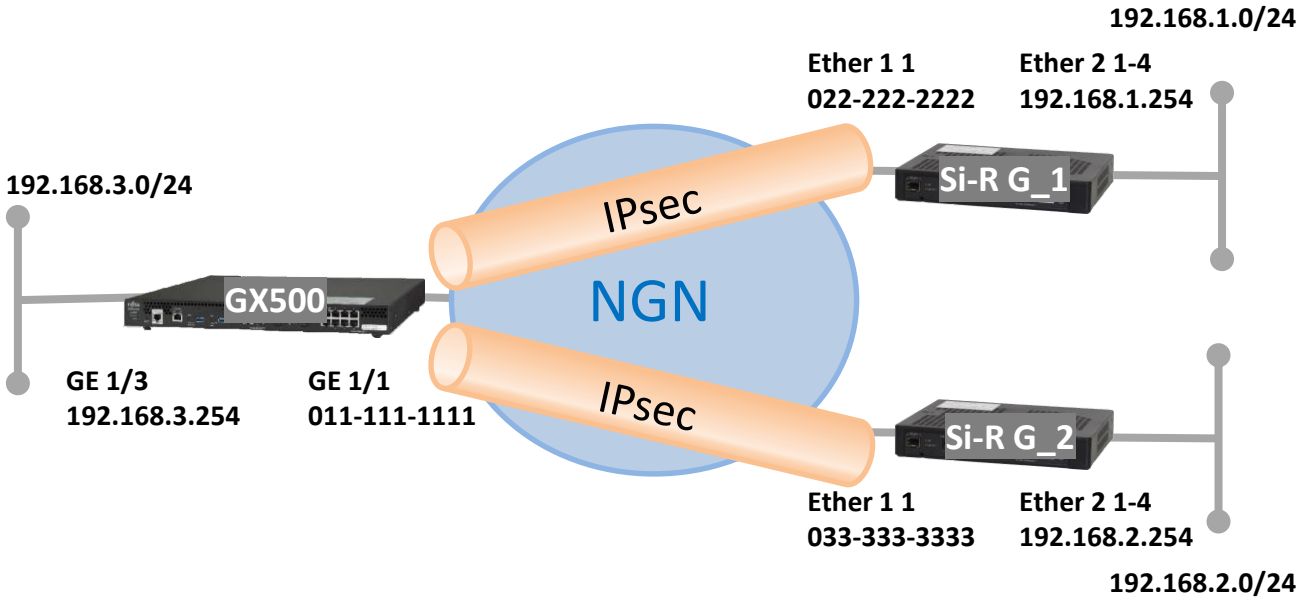
技術情報：Si-R/Si-R brinシリーズ設定例
（NTT東日本 / NTT西日本フレッツ光ネクスト）

データコネクトで、センター(Si-R GX500)と拠点間(Si-R Gシリーズ)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。
※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 V4.06以降
Si-R GX500 V1.05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。
・Si-R GXのGigaEthernet 1/1をWAN側、GigaEthernet 1/3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192.168.1.254/24、192.168.2.254/24、 192.168.3.254/24を割り当てます。
・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、512Kとします。
・Si-R GはIPsec暗号化後にシェーピングを行うため、QoSを併用します。



[設定例]
・sir2-keyにはIPsec鍵を設定してください。

GX500設定例

```
ip route 192.168.1.0 255.255.255.0 tunnel 1
ip route 192.168.2.0 255.255.255.0 tunnel 2
!
ip dhcp client-profile DHCPv4
 retries infinity
 ngn enable
exit
!
ipv6 route ::/0 dhcp port-channel 1
!
ipv6 dhcp client-profile DHCPv6
 option-request prefix-delegation
 option-request sip-server
 option-request sip-server-domain
 retries infinity
 ngn enable
exit
!
snmp-server source-interface port-channel 3
!
logging console level informational
!
hostname GX500
!
crypto ipsec udp-encapsulation nat-t
crypto ipsec udp-encapsulation-force
!
crypto ipsec policy P2
 set pfs group5
 set security-association lifetime seconds 3600
 set security-association transform-keysize aes 256 256 256
 set security-association transform esp-aes esp-sha256-hmac
exit
!
crypto ipsec selector SELECTOR
 src 1 ipv4 any
 dst 1 ipv4 any
exit
!
crypto isakmp log sa
crypto isakmp log session
crypto isakmp log negotiation-fail detail
crypto isakmp negotiation retry timer 5 limit 2 timer-max 5 guard-time 0
crypto isakmp security-association softlimit initiate seconds 90
crypto isakmp security-association softlimit respond seconds 30
!
```

```
crypto isakmp policy P1
 authentication pre-share
 encryption aes
 encryption-keysize aes 256 256 256
 group 5
 hash sha-256
exit
!
crypto isakmp profile 0222222222
 match identity tel-key-id 0222222222 sha-256
 self-identity tel-key-id 0111111111 sha-256
 set isakmp-policy P1
 set ipsec-policy P2
 set peer sip-profile 0222222222
 ike-version 2
 local-key sir2-key
exit
!
crypto isakmp profile 0333333333
 match identity tel-key-id 0333333333 sha-256
 self-identity tel-key-id 0111111111 sha-256
 set isakmp-policy P1
 set ipsec-policy P2
 set peer sip-profile 0333333333
 ike-version 2
 local-key sir2-key
exit
!
crypto session release idle-time 60
!
crypto map 0222222222 ipsec-isakmp
 match address SELECTOR
 set isakmp-profile 0222222222
exit
!
crypto map 0333333333 ipsec-isakmp
 match address SELECTOR
 set isakmp-profile 0333333333
exit
!
ngn sip use enable
ngn sip log session
ngn sip log registrar
ngn sip log session-fail
ngn sip log limit
ngn sip agent 0 bind port-channel 1
!
```

```
ngn sip profile 0222222222
 remote dial 0 number 0222222222
 remote dial 0 speed 64k
exit
!
ngn sip profile 0333333333
 remote dial 0 number 0333333333
 remote dial 0 speed 64k
exit
!
interface GigaEthernet 1/1
 channel-group 1
exit
!
interface GigaEthernet 1/3
 channel-group 3
exit
!
interface Port-channel 1
 ip dhcp service client
 ip dhcp client-profile DHCPv4
 ipv6 enable
 ipv6 address dhcp port-channel 1 ::1/64
 ipv6 nd receive-ra
 ipv6 dhcp service client
 ipv6 dhcp client-profile DHCPv6
exit
!
interface Port-channel 3
 ip address 192.168.3.254 255.255.255.0
exit
!
interface Tunnel 1
 ip unnumbered port-channel 3
 tunnel mode ipsec map 0222222222
exit
!
interface Tunnel 2
 ip unnumbered port-channel 3
 tunnel mode ipsec map 0333333333
exit
!
line console
 exec-timeout 0
exit
!
line telnet
 exec-timeout 0
exit
!
end
```

[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 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 192.168.1.254/24 3
lan 1 vlan 1002
remote 1 name GX500
remote 1 shaping on 512k
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 512K
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 modp1536
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 modp1536
remote 1 ap 0 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike nat-traversal use on
remote 1 ip route 0 192.168.3.0/24 1 60
remote 1 ip priority 0 any any any any any any express
remote 1 ip msschange 1280
loopback ip address 0 192.168.1.254
ngn sip use on
ngn sip bind lan 0
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
terminal charset SJIS
```

[設定例]
・sir2-keyにはIPsec鍵を設定してください。

Si-R G_2設定例

```
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 192.168.2.254/24 3
lan 1 vlan 1002
remote 1 name GX500
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 modp1536
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 0333333333
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 modp1536
remote 1 ap 0 ike proposal 0 prf hmac-sha256
remote 1 ap 0 ike nat-traversal use on
remote 1 ip route 0 192.168.3.0/24 1 60
remote 1 ip priority 0 any any any any any any express
remote 1 ip msschange 1280
loopback ip address 0 192.168.2.254
ngn sip use on
ngn sip bind lan 0
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
terminal charset SJIS
```

解説
Si-R_GX500設定解説

```
ip route 192.168.1.0 255.255.255.0 tunnel 1
ip route 192.168.2.0 255.255.255.0 tunnel 2
#Si-R G_1のLAN向けのStatic経路を設定します。
#・192.168.1.0 : 宛先ネットワークです。
#・255.255.255.0 : マスクです。
#・tunnel 1: ネクストホップです。
# Si-R G_2のLAN向けのStatic経路を設定します。
#・192.168.2.0 : 宛先ネットワークです。
#・255.255.255.0 : マスクです。
#・tunnel 2: ネクストホップです。
!

ip dhcp client-profile DHCPv4
#DHCPクライアント機能のプロファイルを設定します。

 retries infinity
#DHCPメッセージの返信があるまで再送します。

 ngn enable
#NGN網を介してSIP情報を取得します。
exit
!

ipv6 route ::/0 dhcp port-channel 1
#DHCPv6サーバアドレスをゲートウェイアドレスとして登録するデフォルトルートの設定をします。
!

ipv6 dhcp client-profile DHCPv6
#DHCPv6クライアント機能のプロファイルを設定します。

 option-request prefix-delegation
#取得したプレフィックスをリジェクト経路として登録します。

 option-request sip-server
#DHCP v 6サーバにSIPサーバの情報を要求します。

 option-request sip-server-domain
#DHCP v 6サーバにSIPサーバドメイン名の情報を要求します。

 retries infinity
#DHCPメッセージの返信があるまで再送します。

 ngn enable
#NGN網を介してSIP情報を取得します。
exit
!

snmp-server source-interface port-channel 3
#SNMP TRAPの送信元IPアドレスとして使用するインタフェースの設定をします。
!
```

```
crypto ipsec udp-encapsulation nat-t
#NATトラバーサルを有効にします。

crypto ipsec udp-encapsulation-force
#強制的にUDPカプセル化を行う設定をする。
#SIPを使用してIPsec通信する場合有効とする。
!

crypto ipsec policy P2
#IPsecポリシーのエントリの設定をします。

 set pfs group5
#Diffie-Hellmanの設定をします。

 set security-association lifetime seconds 3600
#IPsec-SA/Child-SAの生存時間を3600秒に設定します。

 set security-association transform-keysize aes 256 256 256
#ネゴシエーションで使用するAESの鍵長の設定をします。

 set security-association transform esp-aes esp-sha256-hmac
#暗号化アルゴリズム、認証アルゴリズムの設定をします。
#・esp-aes：暗号化アルゴリズムにAESを設定します。
#・esp-sha-hmac：認証アルゴリズムにHMAC-SHA-1を設定します。
exit
!

crypto ipsec selector SELECTOR
#IPSEC-SA/CHILD SA用のセレクタのエントリの設定をします。

 src 1 ipv4 any
 dst 1 ipv4 any
#送信元および送信先にIPv4のすべてのアドレスを指定します。
exit
!

crypto isakmp log sa
#SA確率/解放をログに出力します。

crypto isakmp log session
#セッション確率/解放をログに出力します。

crypto isakmp log negotiation-fail detail
#ネゴシエーション失敗をログに出力します。

crypto isakmp negotiation retry timer 5 limit 2 timer-max 5 guard-time 0
#ISAKMPネゴシエーションの再送パラメータの設定をします。
#・retry timer：再送間隔に5を設定します。
#・limit：再送回数に2を設定します。
#・timer-max：最大送信間隔に5を設定します。
#・guard-time：再送ガード時間に0を設定します。

crypto isakmp security-association softlimit initiate seconds 90
#イニシエーターとして確立したISAKMP/IKE SAの生存時間満了する90秒前に新しいSAの接続を開始します。
```

```
crypto isakmp security-association softlimit respond seconds 30
#レスポンダーとして確立したISAKMP/IKE SAの生存時間満了する90秒前に新しいSAの接続を開始します。
!

crypto isakmp policy P1
#ISAKMPポリシー設定をします。

 authentication pre-share
 #認証方式をPre-shared key方式に設定します。

 encryption aes
#ISAKMP-SA/IKE SAの暗号化アルゴリズムにAESを設定します。

 encryption-keysize aes 256 256 256
#ISAKMP-SA/IKE SAのネゴシエーションで使用するAESの鍵長の設定します。

 group 5
#Diffie-Hellmanグループ番号の設定をします。

 hash sha-256
#ISAKMP-SA/IKE SAのハッシュアルゴリズムをSHA-2に設定します
exit
!

crypto isakmp profile 0222222222
# Si-R G_1宛のISAKMPプロファイル設定を設定します。

 match identity tel-key-id 0222222222 sha-256
#接続先の電話番号を設定します。

 self-identity tel-key-id 0111111111 sha-256
#接続元の電話番号を設定します。

 set isakmp-policy P1
#ISAKMPポリシー名を設定します。

 set ipsec-policy P2
#このISAKMPプロファイルで使用するIPSECポリシー名を設定します。

 set peer sip-profile 0111111111
#接続先の電話番号を設定します。

 ike-version 2
#IKEv2を設定します。

 local-key sir2-key
#Pre-shared keyを設定します。
exit
!
```

```
crypto isakmp profile 0333333333
#Si-R G_2宛のISAKMPプロファイル設定を設定します。

 match identity tel-key-id 0333333333 sha-256
#接続先の電話番号を設定します。

 self-identity tel-key-id 0111111111 sha-256
#接続元の電話番号を設定します。

 set isakmp-policy P1
#ISAKMPポリシー名を設定する。

 set ipsec-policy P2
#このISAKMPプロファイルで使用するIPSECポリシー名を設定します。

 set peer sip-profile 0333333333
#接続先の電話番号を設定します。

 ike-version 2
#IKEv2を設定します。

 local-key sir2-key
#Pre-shared keyを設定します。
exit
!

crypto session release idle-time 60
#セッションが一定時間ESP通信を行わない場合にセッションを解放する時間を設定します。
!

crypto map 0222222222 ipsec-isakmp
#VPNセレクタ設定モードへの移行します。

 match address SELECTOR
#暗号化するパケットとしてIPSEC セレクタ名を設定します。

 set isakmp-profile 0222222222
#使用するISAKMPプロファイル名の設定します。
exit
!

crypto map 0333333333 ipsec-isakmp
#VPNセレクタ設定モードへの移行します。

 match address SELECTOR
#暗号化するパケットとしてIPSEC セレクタ名を設定します。

 set isakmp-profile 0333333333
#使用するISAKMPプロファイル名の設定します。
exit
!
```

```
ngn sip use enable
#NGN網への接続とデータコネクト機能を有効にします。

ngn sip log session
#データコネクト機能処理のsyslogにSIPセッションの接続/切断情報を出力させます。

ngn sip log registrar
#データコネクト機能処理のsyslogにSIPレジストラ情報を出力させます。

ngn sip log session-fail
#データコネクト機能処理のsyslogにSIPセッションの接続失敗を出力させます。

ngn sip log limit
#データコネクト機能処理のsyslogにSIPの課金制御情報を出力させます。

ngn sip agent 0 bind port-channel 1
#ポートチャネル1でSIPコントロールパケット、メディアストリームパケットの送受信を行う設定をします。
!

ngn sip profile 0222222222
#SIP プロファイル設定モードに移行します。

 remote dial 0 number 0222222222
#接続相手を指定します。

 remote dial 0 speed 64k
#発進時の帯域を64kに指定します。
exit
!

ngn sip profile 0333333333
#SIP プロファイル設定モードに移行します。

 remote dial 0 number 0333333333
#接続相手を指定します。

 remote dial 0 speed 64k
#発進時の帯域を64kに指定します。
exit

interface GigaEthernet 1/1
#WAN側のインタフェース設定をします。

 channel-group 1
#チャネルグループ1を割り当てます。
exit
!

interface GigaEthernet 1/3
#LAN側のインタフェース設定をします。

 channel-group 3
#チャネルグループ5を割り当てます。
exit
!
```

```
interface Port-channel 1
#WAN側のポートチャネルの設定をします。

 ip dhcp service client
#DHCPv4クライアント機能を有効にします。

 ip dhcp client-profile DHCPv4
#使用するプロファイル名を指定します。

 ipv6 enable
#IPv6アドレスを有効にします。

 ipv6 address dhcp port-channel 1 ::1/64
#IPv6クライアント機能で取得したプレフィックスをポートチャネル1に設定します。

 ipv6 nd receive-ra
#RAを受信します。

 ipv6 dhcp service client
#DHCPv6 クライアント機能を有効にします。

 ipv6 dhcp client-profile DHCPv6
#使用するプロファイル名を指定します。
exit
!

interface Port-channel 3
#LAN側のポートチャネルの設定をします。

 ip address 192.168.3.254 255.255.255.0
#LAN側のIPアドレスを設定します。
#・192.168.3.254 : LAN側のIPアドレスです。
#・255.255.255.0 : LAN側のマスクです。
exit
!

interface Tunnel 1
# Si-R G_1側のトンネル設定をします。

 ip unnumbered port-channel 3
#送信元としてポートチャネル3を使用します。

 tunnel mode ipsec map 0222222222
#Tunnnlで使用するVPNセレクタの設定をします。
exit
!

interface Tunnel 2
# Si-R G_2側のトンネル設定をします。

 ip unnumbered port-channel 3
#送信元としてポートチャネル3を使用します。

 tunnel mode ipsec map 0333333333
#Tunnnlで使用するVPNセレクタの設定をします。
exit
!
```

ether 1 1 vlan untag 1001
#ether1 1ポートをTag なしVLAN1001に設定します。

ether 2 1-4 vlan untag 1002
#ether2 1-4ポートをTag なしVLAN1002に設定します。

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 192.168.1.254/24 3
#LAN側IPアドレスを設定します。
#・192.168.1.254/24 : 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 1002
#VLAN ID とlan 定義番号の関連付けを行います。

remote 1 name GX500
#GX500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 512k
#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 512K
#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 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 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 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 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 0 192.168.3.0/24 1 60
#対向装置GX500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。
#・192.168.3.0/24 : 対向装置GX500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。
#・60 : distance値です。

remote 1 ip priority 0 any any any any any any express
#帯域制御の設定をします。
#シェーピング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 0 192.168.1.254
#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。

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。

ether 1 1 vlan untag 1001
#ether1 1ポートをTag なしVLAN1001に設定します。

ether 2 1-4 vlan untag 1002
#ether2 1-4ポートをTag なしVLAN1002に設定します。

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 192.168.2.254/24 3
#LAN側IPアドレスを設定します。
#・192.168.2.254/24 : 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 1002
#VLAN ID とlan 定義番号の関連付けを行います。

remote 1 name GX500
#GX500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 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 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 0333333333
#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 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 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 0 192.168.3.0/24 1 60
#対向装置GX500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。
#・192.168.3.0/24 : 対向装置GX500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。
#・60 : distance値です。

remote 1 ip priority 0 any any any any any any express
#帯域制御の設定をします。
#シェーピング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 0 192.168.2.254
#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。

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。