# FutureNet VPN Client/NET-G

# 接続設定ガイド NXR 編

Ver 1.0.0

センチュリー・システムズ株式会社

# 目次

# はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- FutureNet VPN Client/NET-G はセンチュリー・システムズ株式会社の商標です。
- FutureNet VPN Client/NET-G は国際著作権法によって保護されています。All rights reserved.
- ssh®は SSH Communications Security Corp の米国および一部の地域での登録商標です。
- SSH のロゴ、SSH Certifier、NET-G Secure VPN Client は、SSH Communications Security Corp の商標であり、一部の地域では登録されている場合もあります。その他の名前およびマークは各社の所有物です。
- 本書に記載されている会社名，製品名は、各社の商標および登録商標です。
- 本書の内容の正確性または有用性については、準拠法に従って要求された場合または書面で明示的に合意された場合を除き、一切の保証を致しません。
- FutureNet VPN Client/NET-G のインストール方法および詳細な操作方法につきましては、CD-ROM に収録されております「ユーザーマニュアル」をご覧ください。
- 本ガイドは FutureNet NXR 製品に対応しております。
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は FutureNet NXR-120/C，VPN Client/NET-G の以下のバージョンをベースに作成しております。

  FutureNet NXR シリーズ NXR-120/C Ver5.18.6

  FutureNet VPN Client/NET-G Ver2.4.2.1

  各種機能において、ご使用されている製品およびファームウェア，ソフトウェアのバージョンによっては一部機能，コマンドおよび設定画面が異なっている場合もございますので、その際は各製品のユーザーズガイドを参考に適宜読みかえてご参照および設定を行って下さい。
- NXR シリーズでは設定した内容の復帰（流し込み）を行う場合は、CLI では「copy」コマンド，GUI では設定の復帰を行う必要があります。
- モバイル通信端末をご利用頂く場合で契約内容が従量制またはそれに準ずる場合、大量のデータ通信を行うと利用料が高額になりますのでご注意下さい。
- 本書を利用し運用した結果発生した問題に関しましては、責任を負いかねますのでご了承下さい。

# 改版履歴

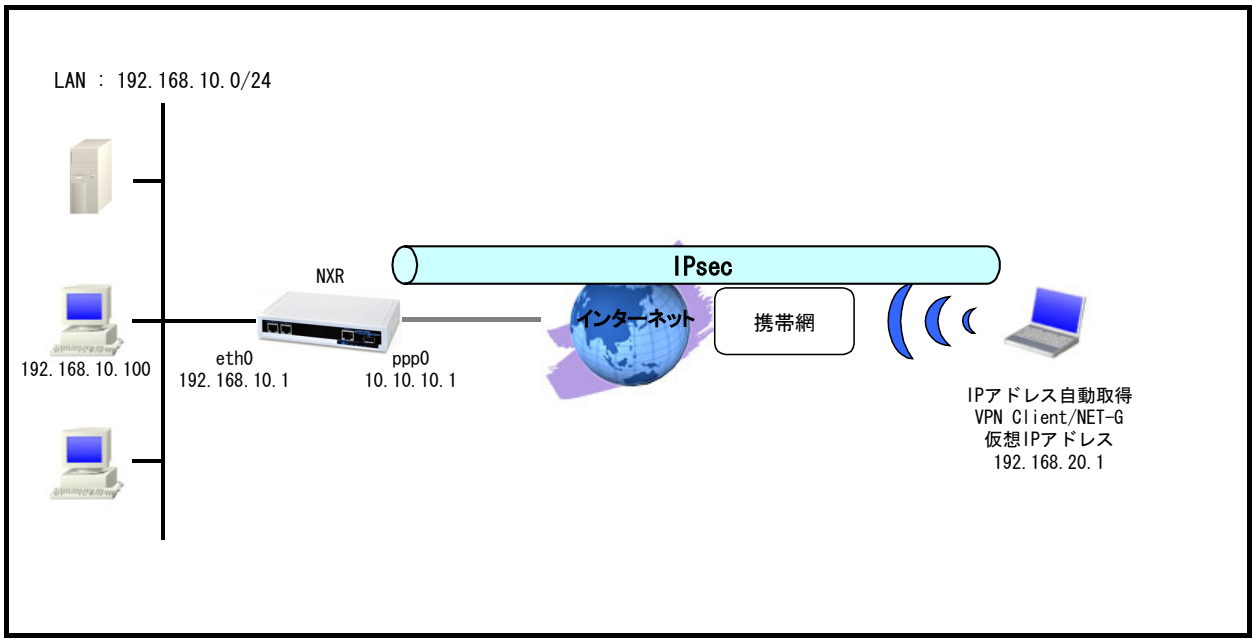
| Version | 更新内容 |
| --- | --- |
| 1.0.0 | 初版 |

# 1. VPN Client/NET-G 基本設定

# 1-1. 基本設定例1(仮想 IP アドレスを使用した設定)

VPN クライアント「FutureNet VPN Client/NET-G」をパソコンにインストールすることにより、外出先などリモートから IPsec によるインターネッ VPN が利用可能になります。

## 【 構成図 】




- この設定例では NXR の IPsec 設定として Route Based IPsec を使用します。(Policy Based IPsec を利用することも可能です)
- NXR 配下の端末は NXR 経由でインターネットアクセスを行います。
- この設定例では NXR のシステム LED 設定で ppp0 インタフェースアップ時, トンネルインタフェースアップ時に LED が点灯するよう設定します。
- VPN Client/NET-G がインストールされたパソコンはインターネット経由での通信ができることおよび IPsec 関連のパケットの送受信ができることを前提とします。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 192.168.20.1/32 tunnel 1
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec access-list NETG ip 192.168.10.0/24 192.168.20.1/32
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description NETG
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode aggressive
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity fqdn netg
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description NETG
NXR(config-ipsec-tunnel)#negotiation-mode responder
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address NETG
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#system led aux 1 interface ppp 0
NXR(config)#system led aux 2 interface tunnel 1
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
```

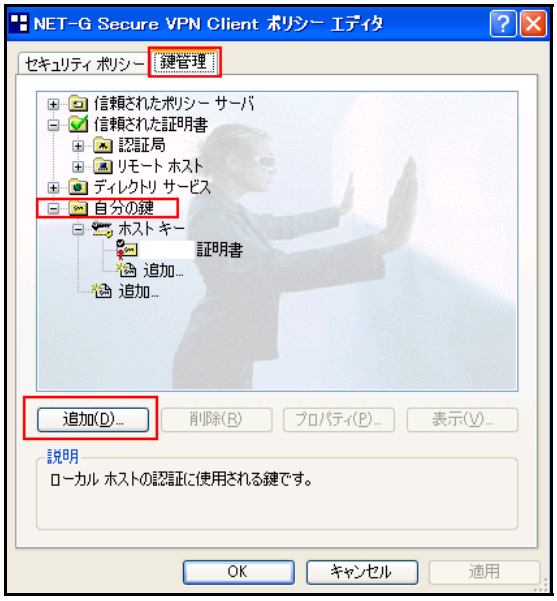
```
NXR(config)#exit
NXR#save config
```

NXR の設定およびコマンドの解説に関しましては、ご利用頂いている NXR 製品のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

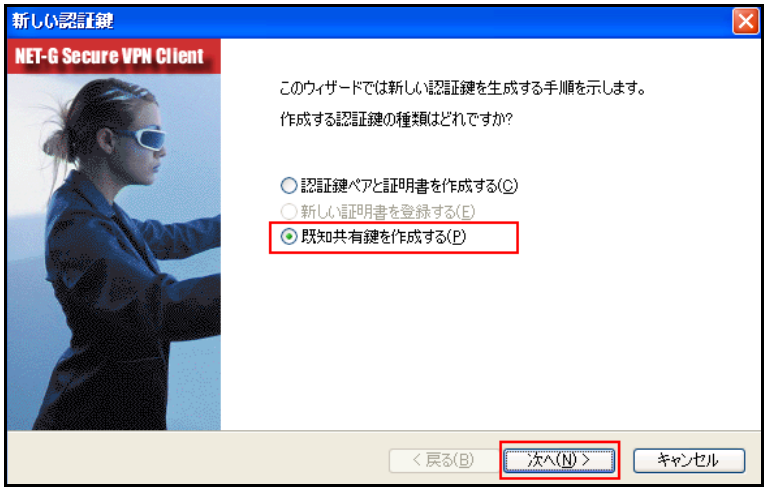
〔VPN Client/NET-G の設定〕

**1. ＜既知共有鍵(Pre Shared Key)の設定＞**

「鍵管理」タブをクリックし、「自分の鍵」を選択し、「追加」ボタンをクリックします。

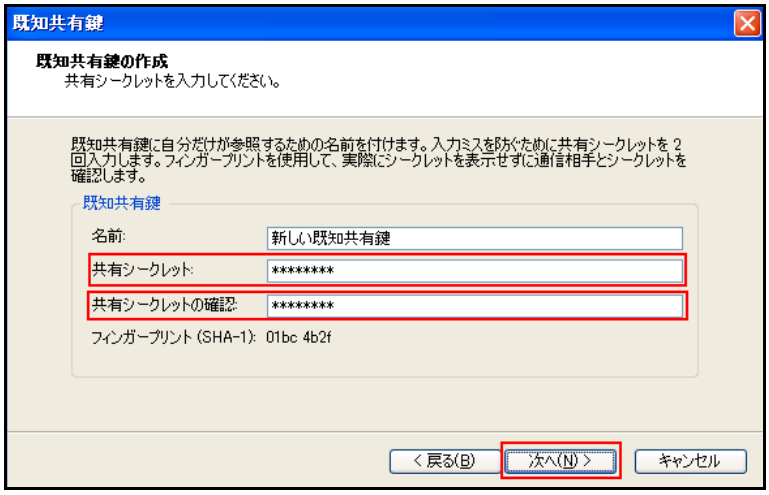



「新しい認証鍵」ウィンドウが開きますので、「既知共有鍵を作成する」を選択し、「次へ」ボタンをクリックして下さい。




「既知共有鍵の作成」画面が開きます。ここで既知共有鍵(PSK)を作成します。「名前」には任意の名称を入力します。「共有シークレット」、「共有シークレットの確認」項目には既知共有鍵を入力し、「次へ」ボタンをクリックします。このとき入力した鍵は“＊”, “●”等で表示されます。

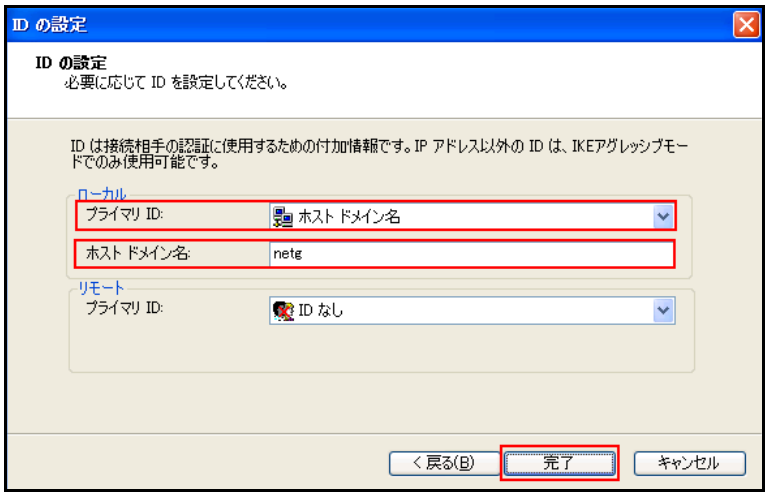
この例では共有シークレットとして「ipseckey」を設定します。




## 2. ＜ID の設定＞

既知共有鍵の作成後、「ID の設定」画面の「ローカル」側項目を設定します。

ここには NXR シリーズの IPsec 設定「ipsec isakmp policy 1」における「remote identity」と同じ ID を設定します。

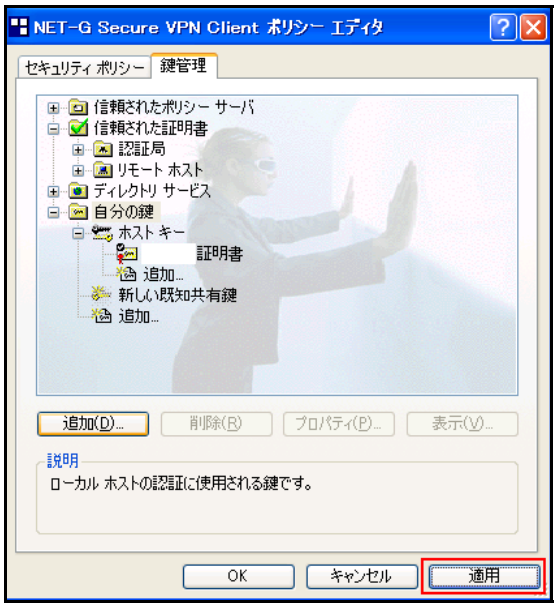



ID の設定(ローカル)では以下の項目を設定・選択します。

- [プライマリ ID]　　ホスト ドメイン名
- [ホストドメイン名]　　netg

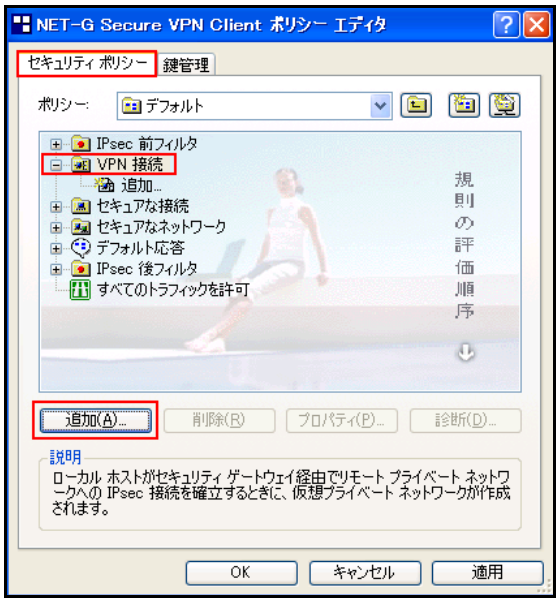
「完了」ボタンをクリックすると「鍵管理」画面に戻ります。

ここまでの設定が終わりましたら、必ず「適用」ボタンをクリックして下さい。「適用」ボタンをクリックしないと適切に設定されない場合があります。

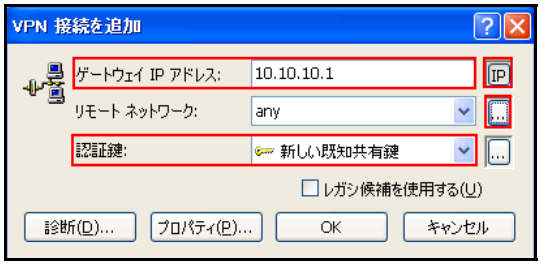



### 3. ＜セキュリティポリシーの設定＞

ポリシーエディタの「セキュリティポリシー」タブをクリックします。「VPN 接続」を選択し「追加」をクリックします。




「VPN 接続を追加」画面が開きます。「ゲートウェイ名」の右端の”IP”をクリックし、対向 NXR の WAN 側 IP アドレスを設定します。「認証鍵」は、既知共有鍵の設定で登録した既知共有鍵の名称を選択します。

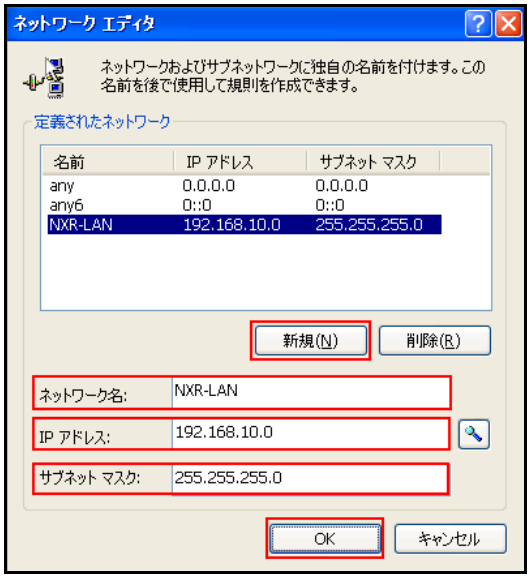


VPN 接続を追加では以下の項目を設定・選択します。

- [ゲートウェイ IP アドレス]　10.10.10.1
- [認証鍵]　新しい既知共有鍵

そして「リモートネットワーク」については右端にある"・・・"をクリックします。

「ネットワークエディタ」画面が開きますので、「新規」をクリックし新しいネットワーク(IPsec 接続先のネットワーク)を登録します。

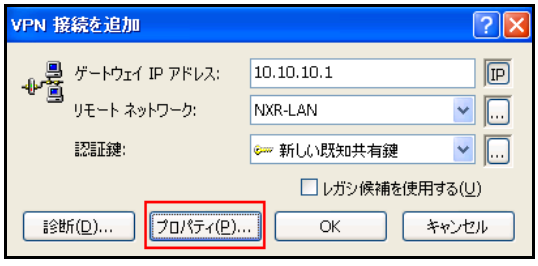



ネットワークエディタでは以下の項目を設定します。

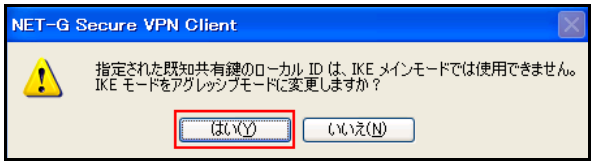
- [ネットワーク名]　NXR-LAN
- [IP アドレス]　192.168.10.0
- [サブネットマスク]　255.255.255.0

設定後、「OK」をクリックします。

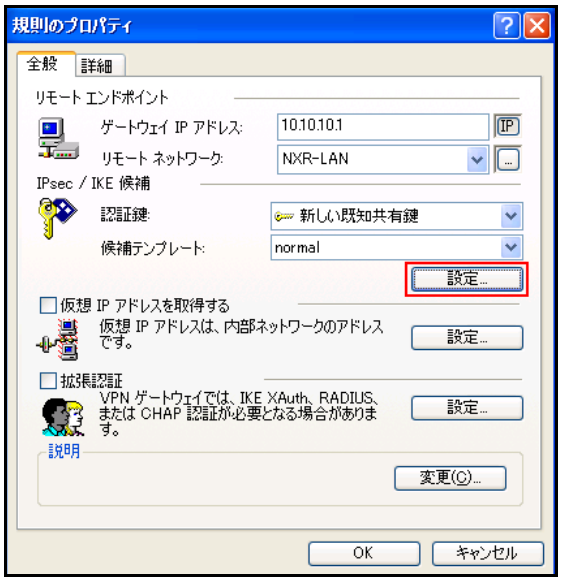
リモートネットワーク設定後、「VPN 接続を追加」画面が開きますので、続いてプロパティをクリックします。



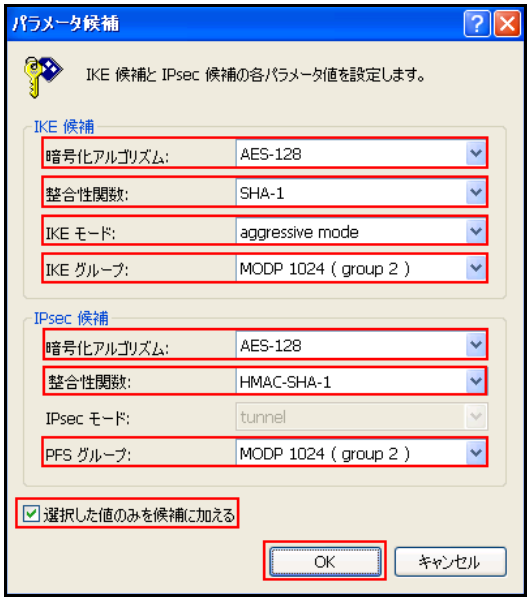

既知共有鍵のローカル ID は IKE アグレッシブモードでのみ利用可能なため、「IKE モードをアグレッシブモードに変更しますか？」と表示されますので、「はい」をクリックします。



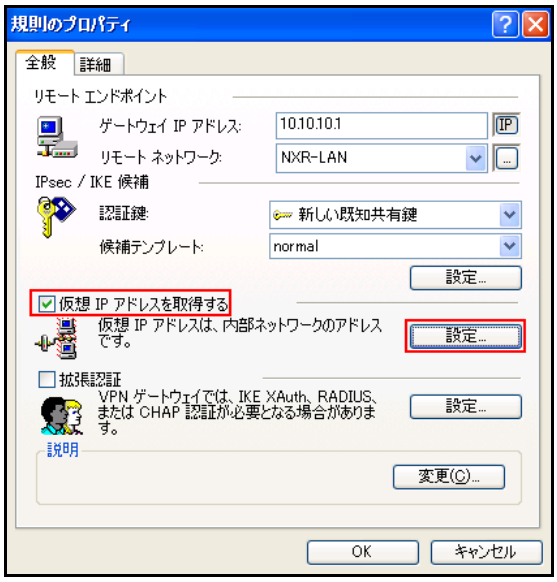

「規則のプロパティ」画面が開きます。ここで IPsec/IKE 候補の「設定」ボタンをクリックします。




「パラメータ候補画面」が開きます。ここでは暗号化方式などを設定します。またこの設定例では「選択した値のみを候補に加える」にチェックを入れています。

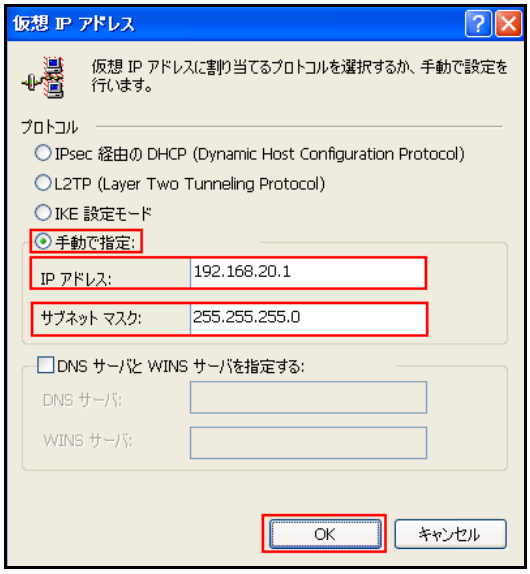



設定後、「OK」ボタンをクリックして「規則のプロパティ」画面に戻ります。
続いて「仮想 IP アドレスを取得する」にチェックを入れ、「設定」ボタンをクリックします。




「仮想 IP アドレス」画面が開きます。

ここでは NXR に接続する際に使用する VPN Client/NET-G の仮想的な IP アドレスを設定します。



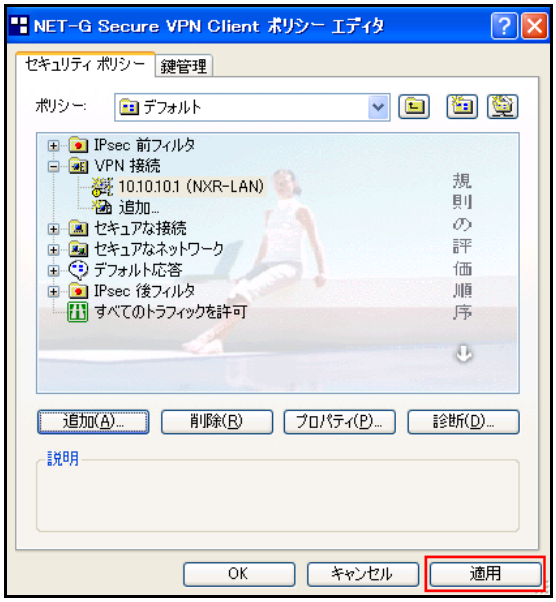

仮想 IP アドレスでは以下の項目を設定します。

- [プロトコル]　　手動で指定
- [IP アドレス]　　192.168.20.1
- [サブネットマスク]　　255.255.255.0

※NXR の IPsec ポリシーで設定したサブネットと異なるので注意して下さい。(32 ビットマスクは設定することができません。)

設定後、「OK」ボタンをクリックして「規則のプロパティ」画面に戻り、「規則のプロパティ」画面で「OK」ボタンをクリックして「VPN 接続を追加」画面に戻り、「OK」ボタンをクリックしてポリシーエディタに戻ります。

そしてポリシーエディタで「適用」をクリックし、設定は完了です。

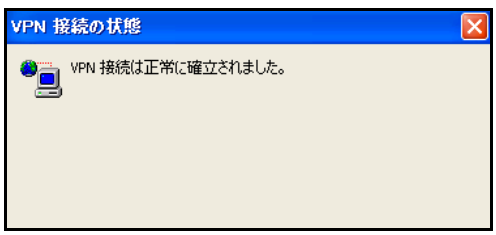



**4. ＜IPsec 接続＞**

タスクバーの中にある VPN Client/NET-G のアイコンを右クリックします。そして「VPN を選択」の指定し、作成した IPsec ポリシーを選択します。


選択後、IKE のネゴシエーションを行う画面が表示されます。


IPsec が正常に確立した場合、「VPN 接続は正常に確立しました」という画面が表示されます。




これで IPsec 接続は完了です。

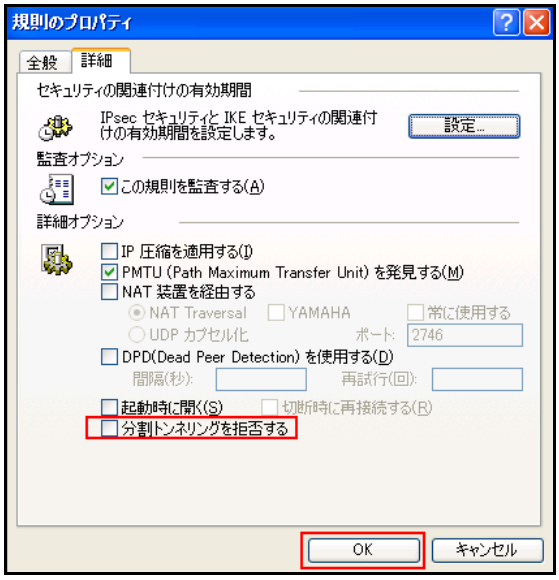
**＜補足1：VPN クライアントでの IPsec 通信とインターネット通信の同時利用について＞**

この設定例では、IPsec 接続時のインターネット通信は拒否になっています。

IPsec 接続時に IPsec 通信とインターネット通信を両方同時に利用する場合は、以下の設定を行って下さい。

「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「分割トンネリングを拒否する」のチェックボックスでチェックを外して「OK」ボタンをクリックし、ポリシーエディタに戻ります。

そしてポリシーエディタで「適用」をクリックします。

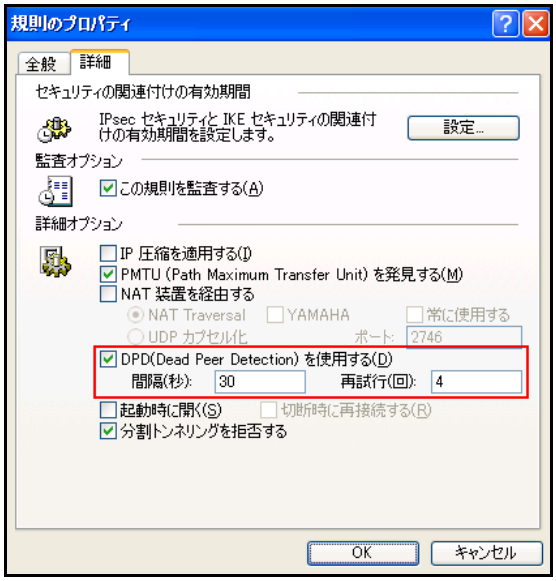



**＜補足 2：DPD の利用について＞**

NXR シリーズは DPD に対応しています。そのため VPN Client/NET-G でも DPD を使用することで DPD による監視を行うことができます。

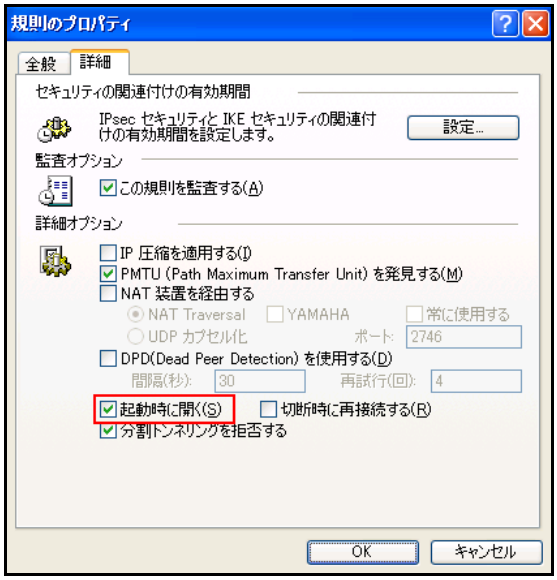
DPD を利用する場合は、以下の設定を行って下さい。

「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「DPD(Dead Peer Detection)を使用する」のチェックボックスでチェックを入れて、間隔および再試行回数を設定して「OK」ボタンをクリックして下さい。



**＜補足 3:起動時の IPsec 接続について＞**

VPN Client/NET-G のポリシーマネージャ起動時に VPN 接続を自動的に開くことができます。

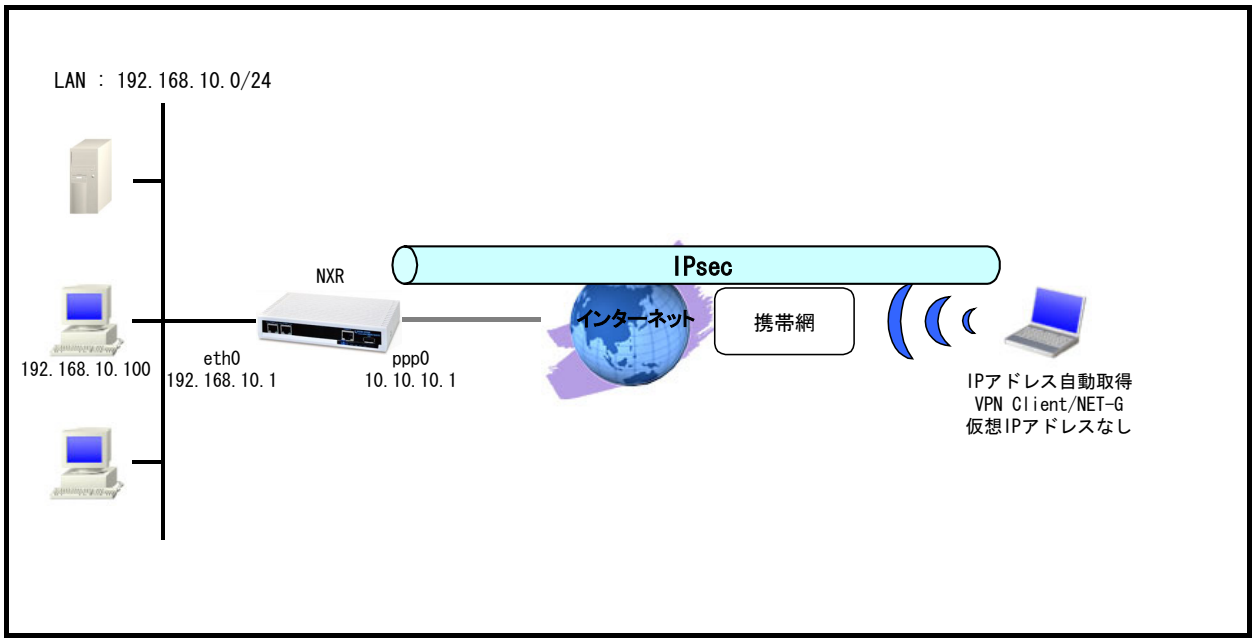



また「起動時に開く」のオプションとして「切断時に再接続する」があり、これを選択すると、何らかの問題で VPN 接続が切断された場合に自動的に再接続を行います。

## 1-2. 基本設定例2(仮想 IP アドレスを使用しない設定)

基本設定例1では、VPN クライアント側で IPsec 接続時に使用する IP アドレスとして「仮想 IP アドレス」を設定しました。このとき NXR の LAN 側からは VPN クライアントに設定した仮想 IP アドレスに対して IPsec 経由で通信を行います。この設定以外に、「仮想 IP アドレス」を使わずに VPN クライアントと NXR を IPsec 接続して通信することも可能です。「仮想 IP アドレス」を使用しないときは NXR の LAN 側から VPN クライアントが動作しているパソコン自身が持つ IP アドレスに対して IPsec 通信を行います。
なお下記設定例は、基本設定例1からの差分のみ記載しておりますので、その他の設定に関しましては基本設定例1をご参照下さい。

### 【 構成図 】




- この設定例では NXR の IPsec 設定として Policy Based IPsec を使用します。
  (☞) Route Based IPsec を使用することも可能ですが、VPN Client/NET-G の IP アドレスが固定 IP アドレスである必要があります。理由は Route Based IPsec では対向 VPN Client/NET-G の IP アドレス宛に IPsec トンネルのルートを設定する必要があるためです。よって VPN Client/NET-G で仮想 IP アドレスを使用しない場合で、かつ VPN Client/NET-G の IP アドレスが動的 IP アドレスの場合は Policy Based IPsec をご利用下さい。
- NXR 配下の端末は NXR 経由でインターネットアクセスを行います。
- この設定例では NXR のシステム LED 設定で ppp0 インタフェースアップ時に LED が点灯するよう設定します。
- VPN Client/NET-G がインストールされたパソコンはインターネット経由での通信ができることおよび IPsec 関連のパケットの送受信ができることを前提とします。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 50
NXR(config)#ipsec access-list NETG ip 192.168.10.0/24 host
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description NETG
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode aggressive
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity fqdn netg
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description NETG
NXR(config-ipsec-tunnel)#negotiation-mode responder
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address NETG
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#system led aux 1 interface ppp 0
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

NXRの設定およびコマンドの解説に関しましては、ご利用頂いているNXR製品のユーザーズガイド(CLI版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

〔VPN Client/NET-G の設定〕

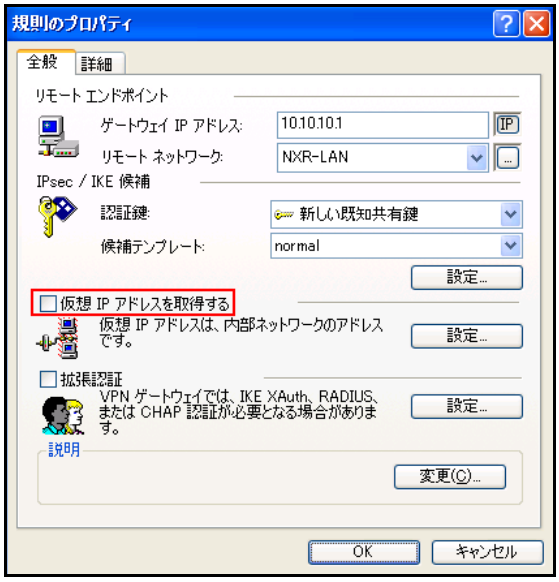
設定の大部分は 1-1.基本設定例1(仮想 IP アドレスを使用した設定)の VPN Client/NET-G の各設定が参考になりますので、そちらをご参照下さい。

1. **＜既知共有鍵(Pre Shared Key)の設定＞**
2. **＜ID の設定＞**
3. **＜セキュリティポリシーの設定＞**

ここでは上記設定以外に必要となる設定を記載します。

**＜セキュリティポリシーの設定＞**

「規則のプロパティ」画面を開き、「仮想 IP アドレスを取得する」にチェックを入れずに設定します。

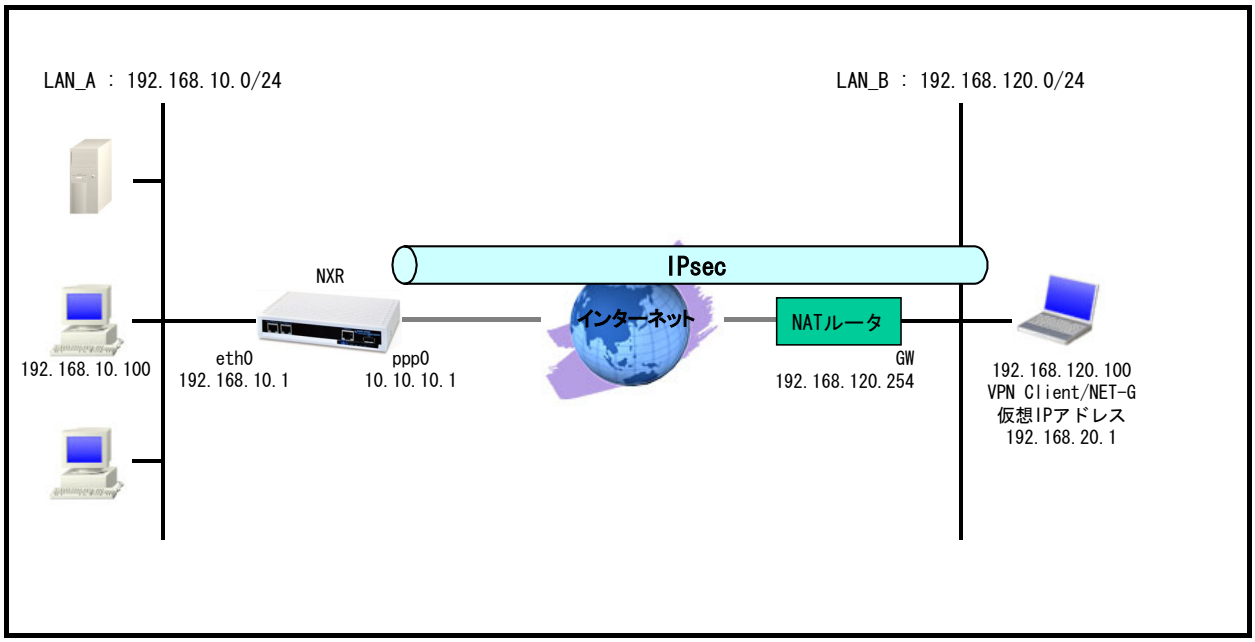


# 2. VPN Client/NET-G 応用設定

# 2-1. IPsec NAT トラバーサル設定(仮想 IP アドレスを使用した設定)

この設定例は、IPsec NAT トラバーサルを利用した IPsec 接続の設定例です。拠点側にインターネットアクセス用の NAT ルータがあり、その配下に VPN Client/NET-G をインストールしたパソコンがある構成です。

## 【 構成図 】




- この設定例では NXR の IPsec 設定として Route Based IPsec を使用します。(Policy Based IPsec を利用することも可能です)
- NXR 配下の端末は NXR 経由でインターネットアクセスを行います。
- この設定例では NXR のシステム LED 設定で ppp0 インタフェースアップ時, トンネルインタフェースアップ時に LED が点灯するよう設定します。
- VPN Client/NET-G がインストールされたパソコンはインターネット経由での通信ができることおよび IPsec 関連のパケットの送受信ができることを前提とします。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 192.168.20.1/32 tunnel 1
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR(config)#ipsec access-list NETG ip 192.168.10.0/24 192.168.20.1/32
NXR(config)#ipsec nat-traversal enable
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description NETG
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode aggressive
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity fqdn netg
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description NETG
NXR(config-ipsec-tunnel)#negotiation-mode responder
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address NETG
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface tunnel 1
NXR(config-tunnel)#tunnel mode ipsec ipv4
NXR(config-tunnel)#tunnel protection ipsec policy 1
NXR(config-tunnel)#ip tcp adjust-mss auto
NXR(config-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#system led aux 1 interface ppp 0
NXR(config)#system led aux 2 interface tunnel 1
NXR(config)#dns
NXR(config-dns)#service enable
```

```
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

NXR の設定およびコマンドの解説に関しましては、ご利用頂いている NXR 製品のユーザーズガイド(CLI 版)および FutureNetNXR 設定例集 IPsec 編をご参照ください。

〔VPN Client/NET-G の設定〕

設定の大部分は 1-1.基本設定例 1(仮想 IP アドレスを使用した設定)の VPN Client/NET-G の各設定が参考になりますので、そちらをご参照下さい。

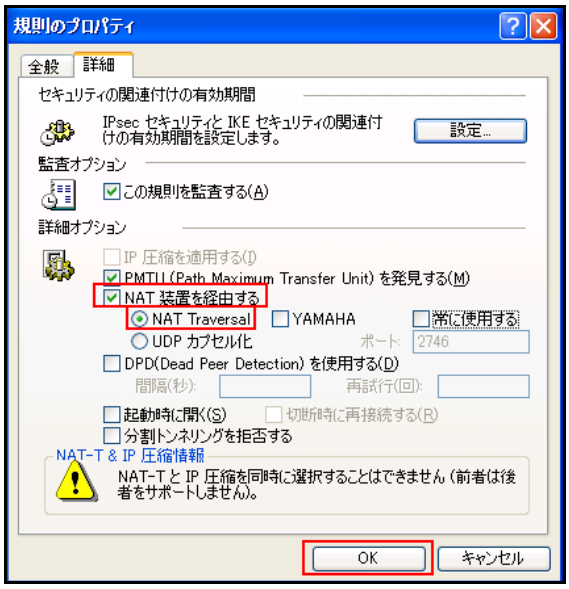
**1. ＜既知共有鍵(Pre Shared Key)の設定＞**

**2. ＜ID の設定＞**

**3. ＜セキュリティポリシーの設定＞**

ここでは上記設定以外に必要となる設定を記載します。

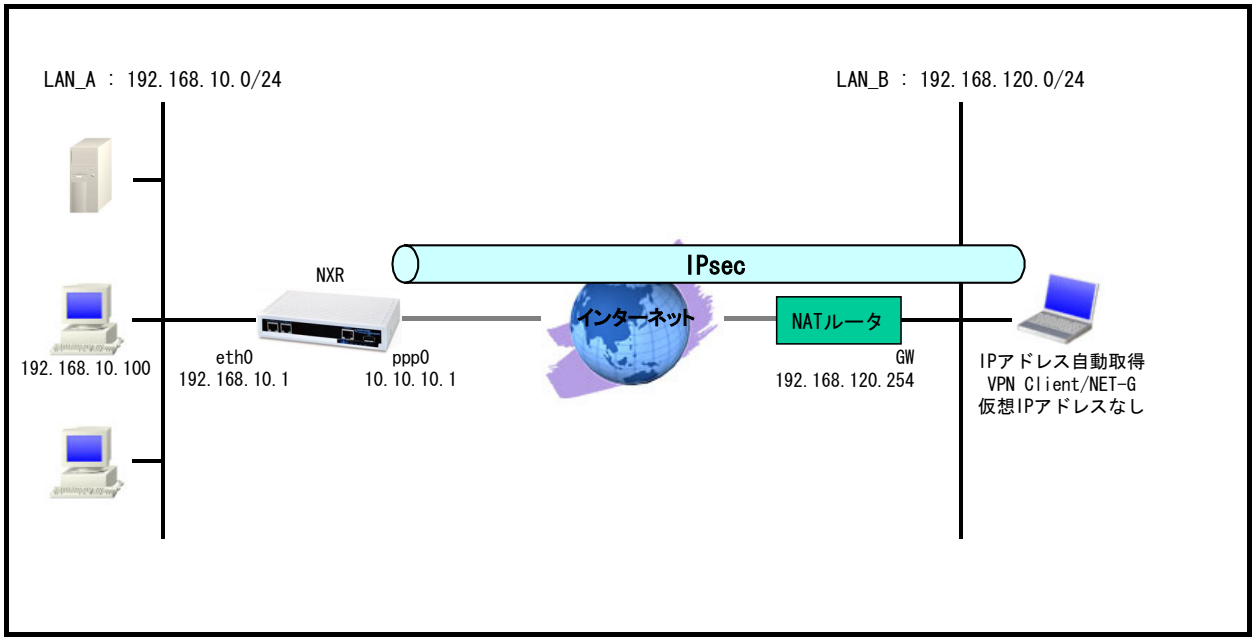
「規則のプロパティ」画面を開き、「詳細タブ」をクリックします。ここで詳細オプションにある「NAT 装置を経由する」のチェックボックスにチェックを入れて、「NAT Traversal」を選択し「OK」ボタンをクリックして下さい。



# 2-2. IPsec NAT トラバーサル設定(仮想 IP アドレスを使用しない設定)

この設定例は、「仮想 IP アドレス」を使用せずに IPsec NAT トラバーサルを利用する設定例です。NAT ルータから DHCP により IP アドレスが自動で割り当てられ、その割り当てられた IP アドレスを IPsec の通信に利用するようなケースが該当します。

## 【 構成図 】




- この設定例では NXR の IPsec 設定として Policy Based IPsec を使用します。
  (☞) Route Based IPsec を使用することも可能ですが、VPN Client/NET-G の IP アドレスが固定 IP アドレスである必要があります。理由は Route Based IPsec では対向 VPN Client/NET-G の IP アドレス宛に IPsec トンネルのルートを設定する必要があるためです。よって VPN Client/NET-G で仮想 IP アドレスを使用しない場合で、かつ VPN Client/NET-G の IP アドレスが動的 IP アドレスの場合は Policy Based IPsec をご利用下さい。
- NXR 配下の端末は NXR 経由でインターネットアクセスを行います。
- この設定例では NXR のシステム LED 設定で ppp0 インタフェースアップ時に LED が点灯するよう設定します。
- VPN Client/NET-G がインストールされたパソコンはインターネット経由での通信ができることおよび IPsec 関連のパケットの送受信ができることを前提とします。

## 【 設定例 】

〔NXR の設定〕

```
nxr120#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
nxr120(config)#hostname NXR
NXR(config)#interface ethernet 0
NXR(config-if)#ip address 192.168.10.1/24
NXR(config-if)#exit
NXR(config)#ip route 0.0.0.0/0 ppp 0
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 500
NXR(config)#ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
NXR(config)#ipsec access-list NETG ip 192.168.10.0/24 host
NXR(config)#ipsec nat-traversal enable
NXR(config)#ipsec local policy 1
NXR(config-ipsec-local)#address ip
NXR(config-ipsec-local)#exit
NXR(config)#ipsec isakmp policy 1
NXR(config-ipsec-isakmp)#description NETG
NXR(config-ipsec-isakmp)#authentication pre-share ipseckey
NXR(config-ipsec-isakmp)#hash sha1
NXR(config-ipsec-isakmp)#encryption aes128
NXR(config-ipsec-isakmp)#group 2
NXR(config-ipsec-isakmp)#lifetime 10800
NXR(config-ipsec-isakmp)#isakmp-mode aggressive
NXR(config-ipsec-isakmp)#remote address ip any
NXR(config-ipsec-isakmp)#remote identity fqdn netg
NXR(config-ipsec-isakmp)#keepalive 30 3 periodic clear
NXR(config-ipsec-isakmp)#local policy 1
NXR(config-ipsec-isakmp)#exit
NXR(config)#ipsec tunnel policy 1
NXR(config-ipsec-tunnel)#description NETG
NXR(config-ipsec-tunnel)#negotiation-mode responder
NXR(config-ipsec-tunnel)#set transform esp-aes128 esp-sha1-hmac
NXR(config-ipsec-tunnel)#set pfs group2
NXR(config-ipsec-tunnel)#set sa lifetime 3600
NXR(config-ipsec-tunnel)#set key-exchange isakmp 1
NXR(config-ipsec-tunnel)#match address NETG nat-traversal
NXR(config-ipsec-tunnel)#exit
NXR(config)#interface ppp 0
NXR(config-ppp)#ip address 10.10.10.1/32
NXR(config-ppp)#ip masquerade
NXR(config-ppp)#ip access-group in ppp0_in
NXR(config-ppp)#ip spi-filter
NXR(config-ppp)#ip tcp adjust-mss auto
NXR(config-ppp)#no ip redirects
NXR(config-ppp)#ppp username test1@centurysys password test1pass
NXR(config-ppp)#ipsec policy 1
NXR(config-ppp)#exit
NXR(config)#interface ethernet 1
NXR(config-if)#no ip address
NXR(config-if)#pppoe-client ppp 0
NXR(config-if)#exit
NXR(config)#system led aux 1 interface ppp 0
NXR(config)#dns
NXR(config-dns)#service enable
NXR(config-dns)#exit
NXR(config)#exit
NXR#save config
```

NXRの設定およびコマンドの解説に関しましては、ご利用頂いているNXR製品のユーザーズガイド(CLI版)およ

び FutureNetNXR 設定例集 IPsec 編をご参照ください。

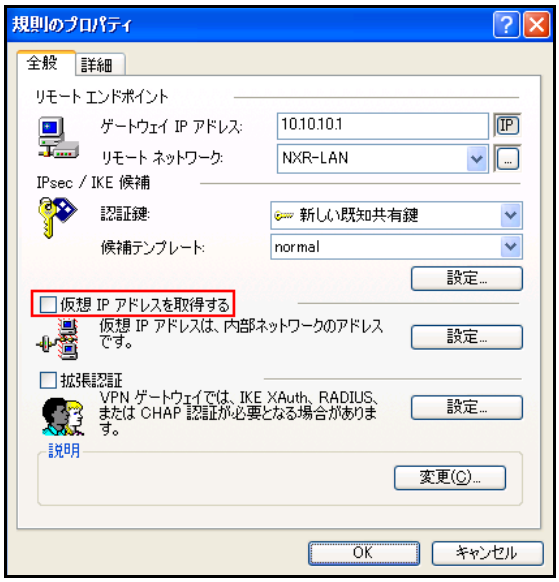
〔VPN Client/NET-G の設定〕

設定の大部分は 1-1.基本設定例1(仮想 IP アドレスを使用した設定)の VPN Client/NET-G の各設定が参考になりますので、そちらをご参照下さい。

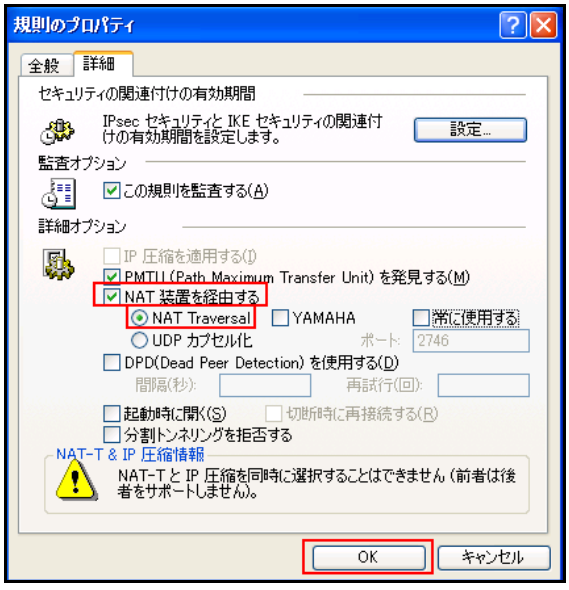
1. **＜既知共有鍵(Pre Shared Key)の設定＞**
2. **＜ID の設定＞**
3. **＜セキュリティポリシーの設定＞**

ここでは上記設定以外に必要となる設定を記載します。

「規則のプロパティ」画面を開き、「仮想 IP アドレスを取得する」にチェックを入れずに設定します。




「規則のプロパティ」画面で「詳細タブ」をクリックします。ここで詳細オプションにある「NAT 装置を経由する」のチェックボックスにチェックを入れて、「NAT Traversal」を選択し「OK」ボタンをクリックして下さい。



# 付録

# IPsec 状態確認方法

〔NXR〕

## ● ステータスの確認

IPsec の各トンネル状況を一覧で確認する場合は、show ipsec status brief コマンドを使用します。

<実行例>

```
nxr120#show ipsec status brief
TunnelName              Status
tunnel1                  up
tunnel2                  down
```

IPsec SA が確立している(IPsec established)ものを up,それ以外を down として表示します。

IPsec の SA 確立状況等を確認する場合は、show ipsec status コマンドを使用します。

また show ipsec status コマンドの後に tunnel <ポリシー番号>を指定することにより tunnel ポリシー毎にステータスを表示させることができます。これは多拠点収容構成で個々のポリシーを確認するのに有効です。

<実行例>

```
nxr120#show ipsec status
000 "tunnel1":192.168.30.0/24===10.10.30.1[nxrc]...10.10.10.1[10.10.10.1]===192.168.10.0/24; erouted; eroute owner: #2
000 "tunnel1":     ike_life: 10800s; ipsec_life: 3600s; margin: 270s; inc_ratio: 100%
000 "tunnel1":     newest ISAKMP SA: #1; newest IPsec SA: #2;
000 "tunnel1":     IKE proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000 "tunnel1":     ESP proposal: AES_CBC_128/HMAC_SHA1/MODP_1536
000
000 #2: "tunnel1" STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 3212s; newest IPSEC; eroute owner
000 #2: "tunnel1" esp.7a5cb4c1@10.10.10.1 (0 bytes) esp.9867e772@10.10.30.1 (0 bytes); tunnel
000 #1: "tunnel1" STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 10291s; newest ISAKMP
000
Connections:
Security Associations:
   none
```

## ● ログの確認

ログは show syslog message コマンドで確認することができます。

(☞) ここで設定しているシスログのプライオリティは info(初期値)となります。このプライオリティを debug に変更することによりより多くのログが出力されます。

IPsec 接続完了時には以下のようなログが出力されます。

- イニシエータでメインモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0x14bd33f0 <0xf49c1f56 DPD}
```

- レスポンダでメインモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.10.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #3: responding to Main Mode
pluto[XXXX]: "tunnel1" #3: sent MR3, ISAKMP SA established
pluto[XXXX]: "tunnel1" #3: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #4: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #4: IPsec SA established {ESP=>0x9c4fb981 <0xc30f38e1 DPD}
```

- イニシエータでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [strongSwan]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [XAUTH]
pluto[XXXX]: "tunnel1" #1: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000
 {using isakmp#1}
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1" #2: sent QI2, IPsec SA established {ESP=>0xc5e28ab0 <0x899ed286 DPD}
```

- レスポンダでアグレッシブモード利用時

<出力例>

```
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [strongSwan]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.30.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1"[1] 10.10.30.1 #2: IPsec SA established {ESP=>0x899ed286 <0xc5e28ab0 DPD}
```

- レスポンダでアグレッシブモード＋NAT トラバーサル利用時(対向：VPN Client/NET-G)

<出力例>

```
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [SSH Sentinel 1.4.1]
pluto[XXXX]: packet from 10.10.40.1:500: received Vendor ID payload [RFC 3947]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-stenberg-ipsec-nat-traversal-02]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-stenberg-ipsec-nat-traversal-01]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-03]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02_n]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-02]
pluto[XXXX]: packet from 10.10.40.1:500: ignoring Vendor ID payload [draft-ietf-ipsec-nat-t-ike-00]
pluto[XXXX]: packet from 10.10.40.1:500: received Vendor ID payload [XAUTH]
pluto[XXXX]: packet from 10.10.40.1:500: received Vendor ID payload [Dead Peer Detection]
pluto[XXXX]: "tunnel1"[1] 10.10.40.1 #1: responding to Aggressive Mode from unknown peer 10.10.40.1
pluto[XXXX]: "tunnel1"[1] 10.10.40.1 #1: NAT-Traversal: Result using RFC 3947: both are NATed
pluto[XXXX]: "tunnel1"[1] 10.10.40.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel1"[1] 10.10.40.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: | NAT-T: new mapping 10.10.40.1:500/4500)
pluto[XXXX]: "tunnel1"[1] 10.10.40.1:4500 #2: responding to Quick Mode
charon: 03[KNL] interface tunnel1 activated
pluto[XXXX]: "tunnel1"[1] 10.10.40.1:4500 #2: IPsec SA established {ESP=>0x085012f6 <0x7df01563
 NATOA=0.0.0.0 DPD}
```

「ISAKMP SA established」が ISAKMP SA が確立したことを、「IPsec SA established」が IPsec SA が確立したことを示しています。

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

- 対向機器からの応答がない（メインモード）

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
・・・
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_MAIN_I1.  No response(or no
acceptable response) to our first IKE message
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Main Mode to replace #1
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ（UDP500）は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

- 対向機器からの応答がない（アグレッシブモード）

<イニシエータ側のログ出力例>

```
・luto[XXXX]: “tunnel1” #1: initiating Aggressive Mode #1, connection "tunnel1"
・・・
pluto[XXXX]: "tunnel1" #1: max number of retransmissions (20) reached STATE_AGGR_I1
pluto[XXXX]: "tunnel1" #1: starting keying attempt 2 of an unlimited number
pluto[XXXX]: "tunnel1" #2: initiating Aggressive Mode #2 to replace #1, connection "tunnel1"
```

(☞) 対向ルータの WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ（UDP500）は許可されているか、IPsec サービスが起動しているか、対向ルータで該当する IPsec 設定が正しく設定されているかなどを確認してください。

- 該当するポリシがない（イニシエータがメインモード）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Main Mode message received on 10.10.10.1:500 but no
connection has been authorized with policy=PSK
```

(☞) フェーズ１のモードは正しいか、対向のルータの IP アドレスの設定は正しいか、IPsec の設定の関連づけ

は正しいかなどを確認してください。

- 該当するポリシがない（イニシエータがアグレッシブモード）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: packet from 10.10.20.1:500: initial Aggressive Mode message received on 10.10.10.1:500 but no connection has been authorized with policy=PSK
```

(☞) フェーズ1のモードは正しいか、IPsec の設定の関連づけは正しいかなどを確認してください。

- 事前共有鍵の不一致（メインモード）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: responding to Main Mode
pluto[XXXX]: "tunnel1" #1:"tunnel1" #1: next payload type of ISAKMP Identification Payload has an unknown value
pluto[XXXX]: "tunnel1" #1: probable authentication failure (mismatch of preshared secrets?):
malformed payload in packet
```

(☞) お互いのルータで設定した事前共有鍵（PSK）の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Main Mode
pluto[XXXX]: "tunnel1" #1: next payload type of ISAKMP Hash Payload has an unknown value:
```

(☞) お互いのルータで設定した事前共有鍵（PSK）の値が正しいか確認してください。

- 事前共有鍵の不一致（アグレッシブモード）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
```

(☞) お互いのルータで設定した事前共有鍵（PSK）の値が正しいか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: received Hash Payload does not match computed value
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_HASH_INFORMATION to 10.10.10.1:500
```

(☞) お互いのルータで設定した事前共有鍵（PSK）の値が正しいか確認してください。

- フェーズ1の ID 不一致（イニシエータの self-identity 不一致）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: no suitable connection for peer 'nxr'
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: initial Aggressive Mode packet claiming to be from 10.10.30.1 but no connection has been authorized
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending notification INVALID_ID_INFORMATION to 10.10.30.1:500
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値（ID タイプを含む）が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: packet from 10.10.10.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値（ID タイプを含む）が対向機器の remote identity と一致しているか確認してください。

- フェーズ1の ID 不一致（レスポンダの self-identity 不一致）

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: packet from 10.10.30.1:500: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec isakmp policy 設定モードの remote identity コマンドで設定した値(ID タイプを含む)が対向機器の self-identity と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: no suitable connection for peer '10.10.10.1'
pluto[XXXX]: "tunnel1" #1: initial Aggressive Mode packet claiming to be from 10.10.10.1but no connection has been authorized
pluto[XXXX]: "tunnel1" #1: sending notification INVALID_ID_INFORMATION to 10.10.10.1:500
```

(☞) ipsec local policy 設定モードの self-identity コマンドで設定した値(ID タイプを含む)が対向機器の remoteidentity と一致しているか確認してください。

- フェーズ 2 の ID 不一致

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: cannot respond to IPsec SA request because no connectionis known for 192.168.10.0/24===10.10.10.1[10.10.10.1]...10.10.30.1[nxrc]===192.168.30.0/24
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: sending encrypted notification INVALID_ID_INFORMATION to10.10.30.1:500
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type INVALID_ID_INFORMATION
```

(☞) ipsec access-list コマンドで設定した値が対向機器と対になっているか確認してください。

- PFS 設定の不一致(レスポンダ側でのみ PFS を設定)

<レスポンダ側のログ出力例>

```
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: responding to Aggressive Mode from unknown peer 10.10.30.1
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: ISAKMP SA established
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: we require PFS but Quick I1 SA specifies no GROUP_DESCRIPTION
pluto[XXXX]: "tunnel2"[1] 10.10.30.1 #2: sending encrypted notification NO_PROPOSAL_CHOSEN to 10.10.30.1:500
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドで設定した値が対向機器と一致しているか確認してください。

<イニシエータ側のログ出力例>

```
pluto[XXXX]: "tunnel1" #1: initiating Aggressive Mode #1, connection "tunnel1"
pluto[XXXX]: "tunnel1" #1: sent AI2, ISAKMP SA established
pluto[XXXX]: "tunnel1" #1: Dead Peer Detection (RFC 3706): enabled
pluto[XXXX]: "tunnel1" #2: initiating Quick Mode PSK+ENCRYPT+TUNNEL+UP+0x4000000 {using isakmp#1}
pluto[XXXX]: "tunnel1" #1: ignoring informational payload, type NO_PROPOSAL_CHOSEN
```

(☞) ipsec tunnel policy 設定モードの set pfs コマンドを設定しているか確認してください。

## 〔VPN Client/NET-G〕

VPN Client/NET-G では、IPsec 接続時のログを取得することが可能です。

これにより IPsec が確立できない場合もログを確認することにより原因追及が可能です。

ログを取得するためには、VPN Client/NET-G のメインメニューから「監査」->「IKE ログウィンドウを表示」を選択します。※詳細は、VPN Client/NET-G のユーザーマニュアルをご参照下さい。

表示されているログのレベルは「Low」を想定しています。

(☞) 表示される情報量は、選択したレベルにより異なります。

IPsec 接続完了時には以下のようなログが出力されます。

- アグレッシブモード利用時(NAT トラバーサル未使用)

<出力例>

```
Security: Info: The remote server at 10.10.10.1:500 is '88 2f e5 6d 6f d2 0d bc 22 51 61 3b 2e be 5b eb'
Security: Info: The remote server at 10.10.10.1:500 is 'draft-beaulieu-ike-xauth-02.txt'
Security: Info: The remote server at 10.10.10.1:500 is 'RFC3706 Dead Peer Detection'
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 502966dd 9ab4ff3b - ddf1a62a 8393f65e [-1] / 0x00000000 } Aggr;
MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec,
key len = 128, group = 2
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..3]=netg) and ipv4(any:0,[0..3]=10.10.10.1) done.
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 502966dd 9ab4ff3b - ddf1a62a 8393f65e [0] / 0xfc394794 } QM;
MESSAGE: Phase 2 connection succeeded, Using PFS, group = 2
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 502966dd 9ab4ff3b - ddf1a62a 8393f65e [0] / 0xfc394794 } QM;
MESSAGE: SA[0][0] = ESP aes, life = 409600 kB/3600 sec, group = 2, tunnel, hmac-sha1-96, key len = 128, key rounds = 0
Auth: Info: Phase-2 [initiator] done bundle 11 with 2 SA's by rule 199:`ipsec
 ipv4(any:0,[0..3]=192.168.20.1)<->ipv4_subnet(any:0,[0..7]=192.168.10.0/24)(gw:ipv4(any:0,[0..3]=10.10.10.1))'
Auth: Info: SA ESP[10b9f3f4] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [11,0] pri 0 opts src=ipv4(any:0,[0..3]=192.168.20.1)
dst=ipv4_subnet(any:0,[0..7]=192.168.10.0/24)
Auth: Info: SA ESP[5da4a656] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [11,0] pri 0 opts
 src=ipv4_subnet(any:0,[0..7]=192.168.10.0/24) dst=ipv4(any:0,[0..3]=192.168.20.1)
```

- アグレッシブモード利用時(NAT トラバーサル使用時)

<出力例>

```
Security: Info: The remote server at 10.10.10.1:500 is '88 2f e5 6d 6f d2 0d bc 22 51 61 3b 2e be 5b eb'
Security: Info: The remote server at 10.10.10.1:500 is 'draft-beaulieu-ike-xauth-02.txt'
Security: Info: The remote server at 10.10.10.1:500 is 'RFC3706 Dead Peer Detection'
Security: Info: The remote server at 10.10.10.1:500 is 'RFC3947 NAT Traversal'
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:4500 { 7b70fdb2 70773115 - 937a8c44 a5ecc2b0 [-1] / 0x00000000 }
Aggr; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB /
14400 sec, key len = 128, group = 2
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..3]=netg) and ipv4(any:0,[0..3]=10.10.10.1) done.
DEBUG: *** SSH_IPADDR_ANY ***:4500 (Initiator) <-> 10.10.10.1:4500 { 7b70fdb2 70773115 - 937a8c44 a5ecc2b0 [0] / 0x0101c2cf } QM;
MESSAGE: Phase 2 connection succeeded, Using PFS, group = 2
DEBUG: *** SSH_IPADDR_ANY ***:4500 (Initiator) <-> 10.10.10.1:4500 { 7b70fdb2 70773115 - 937a8c44 a5ecc2b0 [0] / 0x0101c2cf } QM;
MESSAGE: SA[0][0] = ESP aes, life = 409600 kB/3600 sec, group = 2, udp-encap-tunnel, hmac-sha1-96, key len = 128, key rounds = 0
Auth: Info: Phase-2 [initiator] done bundle 4 with 2 SA's by rule 79:`ipsec
ipv4(any:0,[0..3]=192.168.20.1)<->ipv4_subnet(any:0,[0..7]=192.168.10.0/24)(gw:ipv4(any:0,[0..3]=10.10.10.1))'
Auth: Info: SA ESP[5fee317d] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [4,0] pri 0 opts udpencap src=ipv4(any:0,[0..3]=192.168.20.1)
dst=ipv4_subnet(any:0,[0..7]=192.168.10.0/24)
Auth: Info: SA ESP[c6b838a5] alg [aes-cbc/16]+hmac[hmac-sha1-96] bundle [4,0] pri 0 opts udpencap
src=ipv4_subnet(any:0,[0..7]=192.168.10.0/24) dst=ipv4(any:0,[0..3]=192.168.20.1)
```

IPsec 接続が失敗する時に出力されるログとして以下のようなものが挙げられます。

- 対向機器からの応答がない

<ログ出力例>

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.2:500 { 85430614 874bf810 - 00000000 00000000 [-1] / 0x00000000 } Aggr; **Connection timed out or error**, calling callback
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..3]=netg) and ipv4(udp:500,[0..3]=10.10.10.2) failed; Timeout.

(☞) NXR の WAN 回線が接続されているか、パケットが届いているか、IPsec のフィルタ(UDP500)は許可されているか、IPsec サービスが起動しているか、NXR で該当する IPsec 設定が正しく設定されているかなどを確認してください。

VPN Client/NET-G 側では以下の設定を確認してください。

「セキュリティポリシー」->「規則のプロパティ」->「ゲートウェイ IP アドレス」

- フェーズ1ID の不一致

<ログ出力例>

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 374e78d5 eaa19830 - 00000000 00000000 [-1] / 0x00000000 } Aggr; **Connection timed out or error**, calling callback
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..2]=**net**) and ipv4(udp:500,[0..3]=10.10.10.1) failed; Timeout.

(☞) VPN Client/NET-G と NXR で設定したフェーズ1の ID が一致しているか確認してください。

VPN Client/NET-G, NXR それぞれで以下の設定を確認してください。

VPN Client/NET-G 側:「既知共有鍵」->「ID」のホストドメイン名

NXR 側:ipsec isakmp policy 設定モード→ remote identity コマンド

- 事前共有鍵の不一致

<ログ出力例>

DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 251499cb fa741ae5 - 37e74116 1f9e0c81 [-1] / 0x00000000 } Aggr; Hash value mismatch
Auth: Info: Phase-1 [initiator] between fqdn(udp:500,[0..3]=netg) and ipv4(udp:500,[0..3]=10.10.10.1) failed; Authentication failed.
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 251499cb fa741ae5 - 37e74116 1f9e0c81 [-1] / 0x00000000 } Aggr; Error = **Authentication failed** (24)

(☞) VPN Client/NET-G と NXR で設定した事前共有鍵(PSK)の値が一致しているか確認してください。

VPN Client/NET-G, NXR それぞれで以下の設定を確認してください。

VPN Client/NET-G 側:「既知共有鍵」->「共有シークレット」

NXR 側:ipsec isakmp policy 設定モード→ authentication pre-share コマンド

- フェーズ 2 の ID 不一致

<ログ出力例>

Security: Info: The remote server at 10.10.10.1:500 is '88 2f e5 6d 6f d2 0d bc 22 51 61 3b 2e be 5b eb'
Security: Info: The remote server at 10.10.10.1:500 is 'draft-beaulieu-ike-xauth-02.txt'
Security: Info: The remote server at 10.10.10.1:500 is 'RFC3706 Dead Peer Detection'
DEBUG: *** SSH_IPADDR_ANY ***:500 (Initiator) <-> 10.10.10.1:500 { 81b43121 2d49f76d - caca254c 532dcef2 [-1] / 0x00000000 } Aggr; MESSAGE: Phase 1 version = 1.0, auth_method = Pre shared keys, cipher = aes-cbc, hash = sha1, prf = hmac-sha1, life = 0 kB / 14400 sec, key len = 128, group = 2
Auth: Info: **Phase-1** [initiator] between fqdn(udp:500,[0..3]=netg) and ipv4(any:0,[0..3]=10.10.10.1) **done**.
DEBUG: *** SSH_IPADDR_ANY ***:500 (Responder) <-> 10.10.10.1:500 { 81b43121 2d49f76d - caca254c 532dcef2 [1] / 0x1ee1633f } Info; **Received notify err = Invalid ID information** (18) to isakmp sa, delete it
Auth: Info: Phase-2 [initiator] for ipv4(icmp:0,[0..3]=192.168.20.10) and ipv4(icmp:0,[0..3]=192.168.10.1) failed; Aborted notification.

(☞) VPN Client/NET-G と NXR で設定したフェーズ2の ID が一致しているか確認してください。

VPN Client/NET-G, NXR それぞれで以下の設定を確認してください。

VPN Client/NET-G 側:「セキュリティポリシー」->「規則のプロパティ」->「仮想 IP アドレスを取得する」->
「仮想 IP アドレス」
「セキュリティポリシー」->「規則のプロパティ」->「リモートネットワーク」

NXR 側:ipsec access-list コマンド
ipsec tunnel policy 設定モード→ match address コマンド

# 設定例の show config 形式サンプル

## 1-1. 基本設定例1（仮想 IP アドレスを使用した設定）

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.18.6 (build 7/10:35 29 08 2012)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NETG
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 2
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn netg
 local policy 1
!
!
ipsec tunnel policy 1
 description NETG
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group2
 set key-exchange isakmp 1
 match address NETG
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
```

```
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
system led aux 2 interface tunnel 1
!
!
!
!
!
!
ip route 192.168.20.1/32 tunnel 1
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list NETG ip 192.168.10.0/24 192.168.20.1/32
!
!
end
```

## 1-2. 基本設定例2（仮想 IP アドレスを使用しない設定）

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.18.6 (build 7/10:35 29 08 2012)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NETG
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
```

```
 encryption aes128
 group 2
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn netg
 local policy 1
!
!
ipsec tunnel policy 1
 description NETG
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group2
 set key-exchange isakmp 1
 match address NETG
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp 500 500
ip access-list ppp0_in permit any 10.10.10.1 50
!
ipsec access-list NETG ip 192.168.10.0/24 host
!
!
end
```

## 2-1. IPsec NAT トラバーサル設定（仮想 IP アドレスを使用した設定）

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.18.6 (build 7/10:35 29 08 2012)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NETG
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
 group 2
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn netg
 local policy 1
!
!
ipsec tunnel policy 1
 description NETG
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group2
 set key-exchange isakmp 1
 match address NETG
!
!
interface tunnel 1
 no ip address
 ip tcp adjust-mss auto
 tunnel mode ipsec ipv4
 tunnel protection ipsec policy 1
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
```

```
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
system led aux 2 interface tunnel 1
!
!
!
!
!
!
ip route 192.168.20.1/32 tunnel 1
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list NETG ip 192.168.10.0/24 192.168.20.1/32
!
!
end
```

## 2-2. IPsec NAT トラバーサル設定（仮想 IP アドレスを使用しない設定）

〔NXR の設定〕

```
!
! Century Systems NXR-120 Series ver 5.18.6 (build 7/10:35 29 08 2012)
!
hostname NXR
telnet-server enable
http-server enable
!
!
!
!
ipv6 forwarding
no fast-forwarding enable
!
!
ipsec nat-traversal enable
!
ipsec local policy 1
 address ip
!
!
ipsec isakmp policy 1
 description NETG
 authentication pre-share ipseckey
 keepalive 30 3 periodic clear
 hash sha1
 encryption aes128
```

```
 group 2
 isakmp-mode aggressive
 remote address ip any
 remote identity fqdn netg
 local policy 1
!
!
ipsec tunnel policy 1
 description NETG
 negotiation-mode responder
 set transform esp-aes128 esp-sha1-hmac
 set pfs group2
 set key-exchange isakmp 1
 match address NETG nat-traversal
!
!
interface ppp 0
 ip address 10.10.10.1/32
 no ip redirects
 ip tcp adjust-mss auto
 ip access-group in ppp0_in
 ip masquerade
 ip spi-filter
 ppp username test1@centurysys password test1pass
 ipsec policy 1
!
interface ethernet 0
 ip address 192.168.10.1/24
!
interface ethernet 1
 no ip address
 pppoe-client ppp 0
!
dns
 service enable
!
syslog
 local enable
!
!
!
no system led ext 0
system led aux 1 interface ppp 0
!
!
!
!
!
!
ip route 0.0.0.0/0 ppp 0
!
ip access-list ppp0_in permit any 10.10.10.1 udp any 500
ip access-list ppp0_in permit any 10.10.10.1 udp any 4500
!
ipsec access-list NETG ip 192.168.10.0/24 host
!
!
end
```

# FutureNet サポートデスクへのお問い合わせ

# FutureNet サポートデスクへのお問い合わせに関して

サポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させて頂くことが可能ですので、ご協力をお願い致します。

※FutureNet サポートデスク宛にご提供頂きました情報は、製品のお問合せなどサポート業務以外の目的には利用致しません。
なおご提供頂く情報の取り扱いについて制限等がある場合には、お問い合わせ時または事前にその旨ご連絡下さい。(設定ファイルのプロバイダ情報や IPsec の事前共有鍵情報を削除してお送り頂く場合など)
弊社のプライバシーポリシーについては下記 URL の内容をご確認下さい。
http://www.centurysys.co.jp/company/privacy.html

＜NXR,VPN Client/NET-G 共通＞

■ ご利用頂いている NXR 製品を含むネットワーク構成図
(ご利用頂いている回線やルータを含むネットワーク機器の IP アドレスを記載したもの)

■ 障害・不具合の内容およびその再現手順
(いつどこで何を行った場合にどのような問題が発生したのかをできるだけ具体的にお知らせ下さい)

□ 問い合わせ内容例1

〇月〇日〇〇時〇〇分頃より拠点 A と拠点 B の間で IPsec による通信ができなくなった。障害発生前までは問題なく利用可能だった。現在当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通は確認できたが、対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通は確認できない。障害発生前後で拠点 B のバックアップ回線としてモバイルカードを接続し、ppp1 インタフェースの設定を行った。設定を元に戻すと通信障害は解消する。
機器の内蔵時計は NTP で同期を行っている。

□ 問い合わせ内容例2

- 発生日時
  〇月〇日〇〇時〇〇分頃
- 発生拠点
  拠点 AB 間
- 障害内容
  IPsec による通信ができなくなった。
- 切り分け内容
  ルータ配下の端末から当該拠点のルータの LAN 側 IP アドレスに対して Ping による疎通確認可能。
  対向ルータの LAN 側 IP アドレス, 配下の端末に対しては Ping による疎通確認不可。
- 障害発生前後での作業
  ルータの設定変更やネットワークに影響する作業は行っていない。
- 備考
  障害発生前までは問題なく利用可能だった。
  機器の内蔵時計は拠点 A の機器で 10 分、拠点 B の機器で 5 分遅れている。

□ 問い合わせ内容例3

現在 IPsec の設定中だが、一度も IPsec SA の確立および IPsec の通信ができていない。IPsec を設定している拠点からのインターネットアクセスおよび該当拠点への Ping による疎通確認も可能。設定例集および設定例集内のログ一覧は未確認。

□ 良くない問い合わせ内容例1

VPN ができない。

→VPN として利用しているプロトコルは何か。VPN のトンネルが確立できないのか、通信ができないのかなど不明。

□ 良くない問い合わせ内容例2

通信ができない。

→どのような通信がいつどこでできない（またはできなくなった）のかが不明。

<NXR>

※情報を取得される前に

シリアル接続で情報を取得される場合は取得前に下記コマンドを実行してください。

#terminal width 180（初期値に戻す場合は terminal no width）

■ ご利用頂いている NXR 製品での不具合発生時のログ

ログは以下のコマンドで出力されます。

#show syslog message

■ ご利用頂いている NXR 製品のテクニカルサポート情報の結果

テクニカルサポート情報は以下のコマンドで出力されます。

# show tech-support

■ 障害発生時のモバイル関連コマンドの実行結果（モバイルカード利用時のみ）

#show mobile <N> ap

#show mobile <N> phone-number

#show mobile <N> signal-level

※<N>はモバイルデバイスナンバ

<VPN Client/NET-G>

■ FutureNet VPN Client/NET-G をインストールしている端末の OS 情報

■ ご利用頂いている FutureNet VPN Client/NET-G のバージョン番号

■ ご利用頂いている VPN クライアントでの不具合発生時のログ

ログを取得するためには、VPN Client/NET-G のメインメニューから「監査」->「IKE ログウィンドウを表示」を選択します。※詳細は、VPN Client/NET-G のユーザーマニュアルをご参照下さい。

（お問い合わせ頂く際に取得するログレベルは、「Detailed」でお願い致します）

# FutureNet サポートデスクのご利用に関して

電話サポート

電話番号:**0422－37－8926**

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 AM – 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail: support@centurysys.co.jp

FAXサポート

FAX 番号:**0422－55－3373**

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため停止する場合があります。 その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet VPN ClientNET-G 接続設定ガイド NXR 編

Ver 1.0.0

2012 年 11 月

発行 センチュリー・システムズ株式会社