FutureNet VPN Client/NET-G

接続設定ガイド　SEIL編

Ver1.0.0

CENTURY SYSTEMS

目次

1. 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。

■このソフトウェアは、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、NETG 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、製品 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、以下の FutureNet SEIL 製品に対応しております。

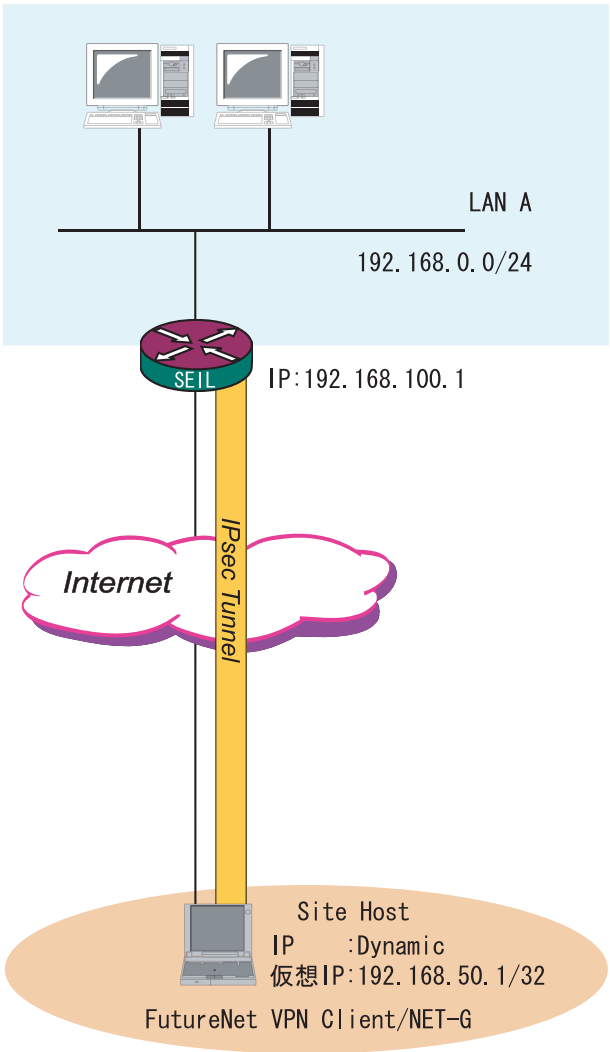
- CS-SEIL-510/C
- CS-SEIL/Turbo

■本ガイドは FutureNet VPN Client/NET-G Ver2.2.2.01, CS-SEIL-510/C Ver1.83, CS-SEIL/Turbo Ver1.83 をベースに作成しております。

2．接続設定例　～基本的な設定～

2-1. ネットワーク構成

SEIL をセンター、VPN Client を拠点とし、この間で IPsec トンネルを生成して 192.168.0.0/24 と拠点側ホストをセキュアに通信可能とします。



2-2. 接続条件

・PSK(共通鍵)方式で認証します。

・agressive モードで接続します。

・仮共通鍵は「ipseckey」とします。

・SEIL 側は固定 IP、NET-G 側は動的 IP とします。

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。

暗号方式 ： 3DES
整合性　 ： SHA-1
IKE で使用するグループ ： group2
拠点の ID ： netg.centurysys.co.jp

本ガイドではプライベート IP アドレスを用いた設定例としておりますが、実環境ではグローバルアドレスに置き換えて設定してください。

2-3.SEIL の設定

以下のように、IPsec の設定を行います。

[IKE の自動接続設定]

```
ike auto-initiation disable
```

常に responder となるため、自動接続を無効にします。

[事前共有鍵と識別子の設定]

```
ike preshared-key add netg.centurysys.co.jp "ipseckey"
```

VPN Client の識別子(netg.centurysys.co.jp)、および事前共有鍵(ipseckey)を設定します。

[IKE プロポーザルの設定]

```
ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group
modp1024 lifetime-of-time 08h
```

暗号アルゴリズムとして 3des を設定します。：　encryption 3des
hash sha1　認証アルゴリズムとして sha1 を設定します。：　hash sha1
Diffie-Hellman グループとして group2 を選択します。：　dh-group modp1024

[IKE Peer の設定]

```
ike peer add NET-G address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier
fqdn netg.centurysys.co.jp
```

フェーズ 1 で使用するモードとして、aggressive モードを設定します。：exchange-mode aggressive
相手識別子として FQDN を使用します。：　peers-identifier fqdn netg.centurysys.co.jp

[セキュリティアソシエーションプロポーザルの設定]

```
ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm
hmac-sha1 encryption-algorithm 3des lifetime-of-time 01h
```

Diffie-Hellman グループを設定します。：　pfs-group modp1024
AH で使用する認証アルゴリズムを設定します。：　authentication-algorithm hmac-sha1
ESP で使用する暗号アルゴリズムを設定します。：　encryption-algorithm 3des

[IKE を使ったセキュリティアソシエーションの設定]

```
ipsec security-association add DynamicSA tunnel dynamic ike PHASE2 esp enable
```

トンネルモードで IPsec を使用します。：　tunnel
IPsec トンネルの始点 / 終点 IP アドレスに動的アドレスを使用します。：　dynamic

[セキュリティポリシーの設定]

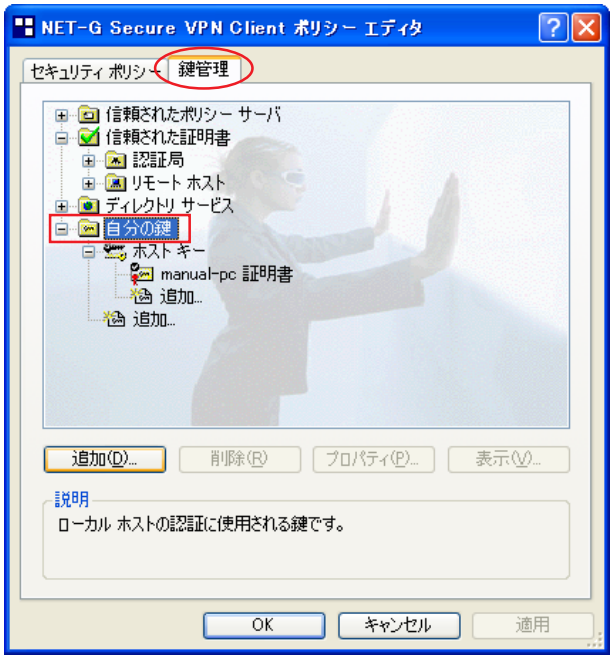
```
ipsec security-policy add SP01 security-association DynamicSA src 192.168.0.0/24 dst
192.168.50.1/32
```

送信元 IP アドレスとネットマスク長を指定します。：　src 192.168.0.0/24
送信先 IP アドレスとネットマスク長を指定します。：　dst 192.168.50.1/32
(※　VPN Client のネットマスク長は、/32 を指定してください)

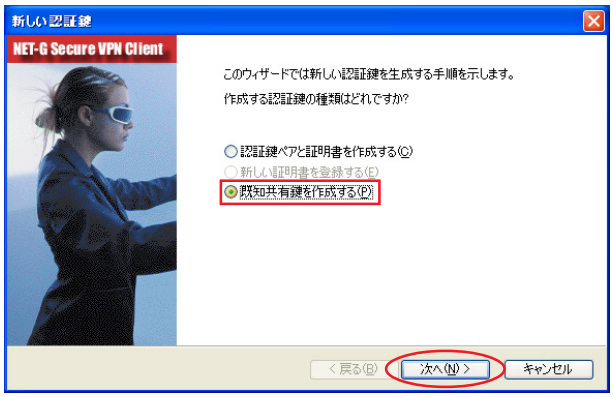
2-4.VPN Client の設定

Windows のタスクトレイから、VPN Client の“ ポリシーエディタ ”を開いて設定します。

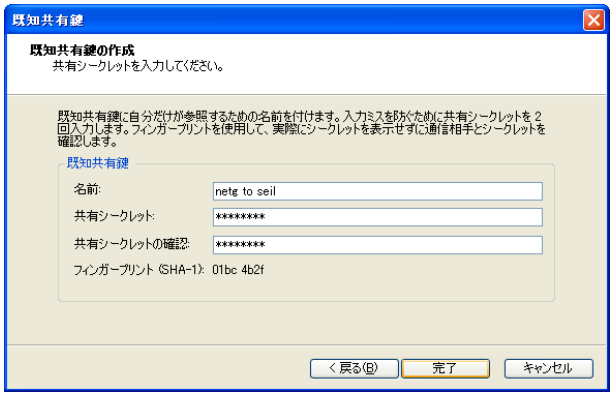
2-4-1. 仮共有鍵の設定



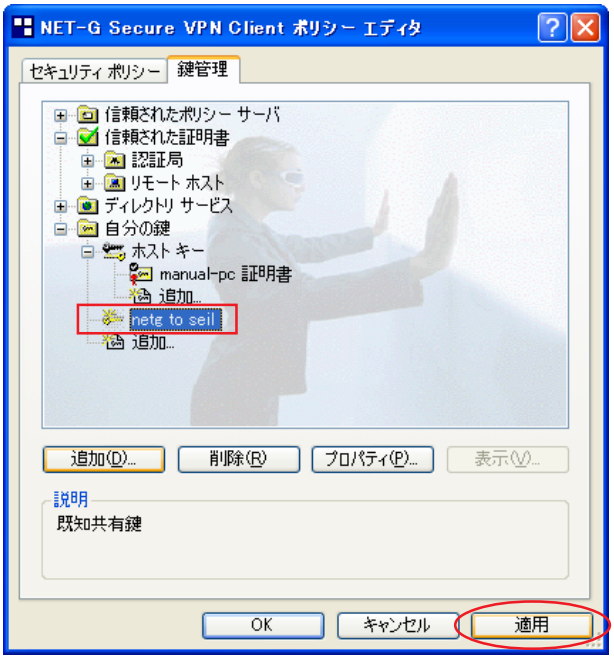
「鍵管理」タブをクリックします。
「自分の鍵」を選択し、「追加」ボタンをクリックします。



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



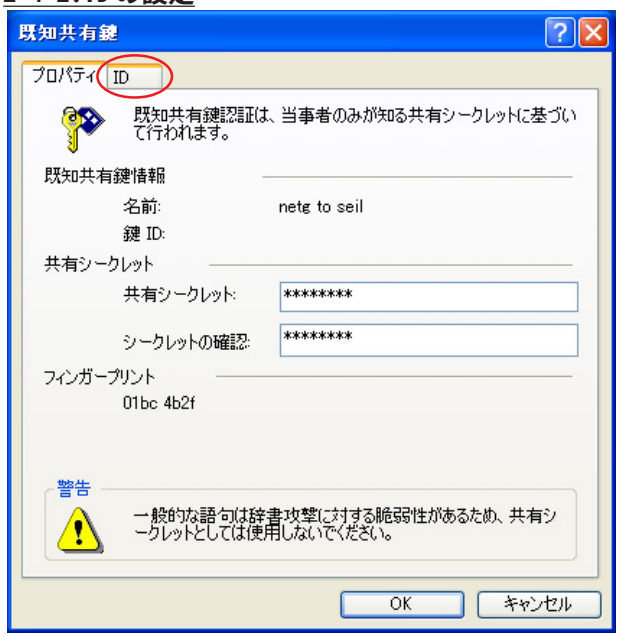
「事前共有鍵情報」画面が開きます。ここで事前共有鍵を設定します。
「名前」項目には任意の設定名を入力します。
「共有シークレット」「共有シークレットの確認」項目には、事前共有鍵(PSK)を入力して「完了」をクリックします。このとき、入力した鍵は“ ＊ ”や“ ● ”等で表示されます。



「鍵管理」画面に戻ります。事前共有鍵情報が登録されていることを確認したら、「適用」ボタンをクリックしてください。

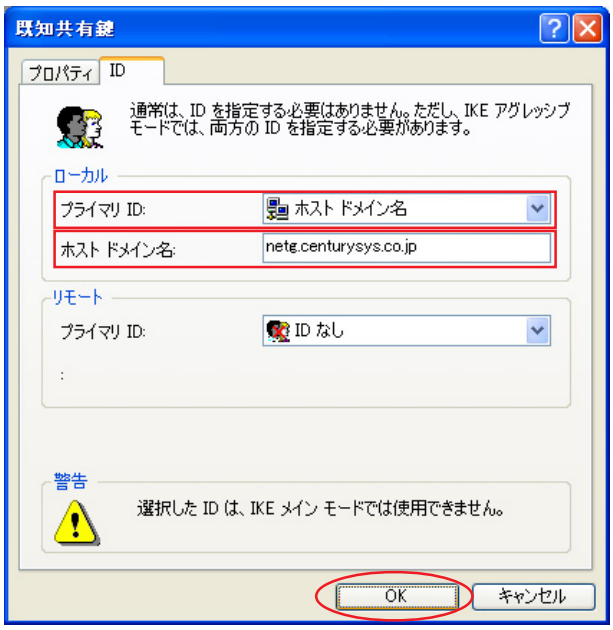
「適用」ボタンをクリックしないと適切に設定されない場合があります。

2-4-2.IDの設定



引き続き「鍵管理」画面で、登録した事前共有鍵情報を選択して「プロパティ」ボタンをクリックします。

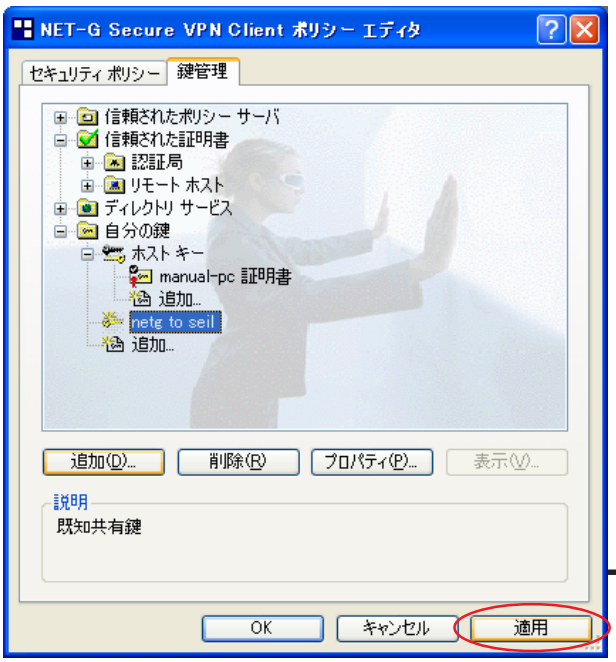
「事前共有鍵」画面が開きますので、「ID」タブをクリックします。
(この画面では仮共有鍵を変更できます。)



“ローカル”側項目について、プライマリ ID は「ホスト ドメイン名」を選択し、ホストドメイン名に ID を入力します。
ここには、2-3.SEIL の設定の[事前共有鍵と識別子の設定]で指定した識別子を入力します。

[事前共有鍵と識別子の設定]
ike preshared-key add **netg.centurysys.co.jp** "ipseckey"

「OK」ボタンをクリックすると「鍵管理」画面に戻ります。

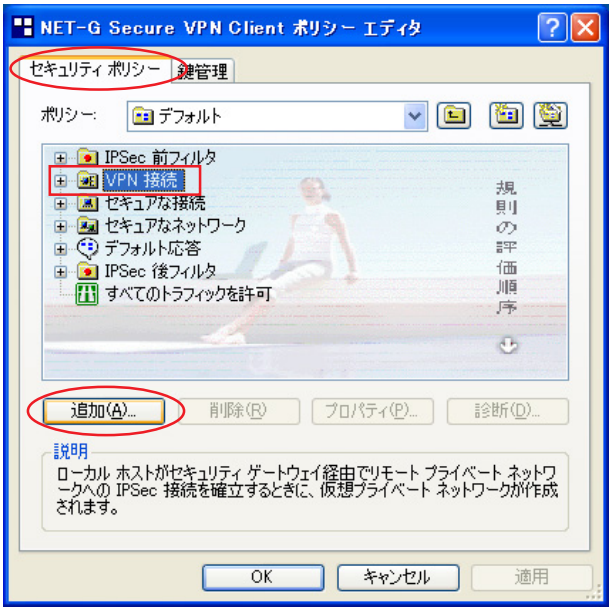


ここまでの設定が終わったら、必ず「適用」ボタンをクリックしてください。

「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。

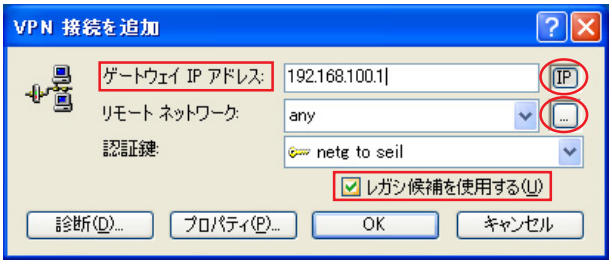
続いて SEIL への IPsec 接続設定を行ないます。

2-4-3. セキュリティポリシーの設定



ポリシーエディタの「セキュリティーポリシー」タブをクリックします。

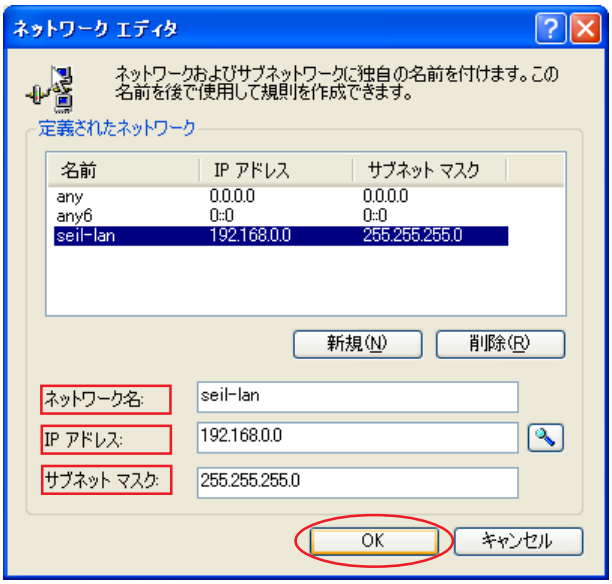
「VPN 接続」を選択し「追加」ボタンをクリックします。



「VPN 接続を追加」画面が開きます。

「ゲートウェイ名」は、右端の“ IP ”をクリックして「ゲートウェイ IP アドレス」とし、SEIL の WAN 側 IP アドレスを入力します。
「認証鍵」は 2-4-1. 仮共有鍵の設定で登録した仮共有鍵の設定名を選択します。
「レガシ候補を使用する」にはチェックを入れます。

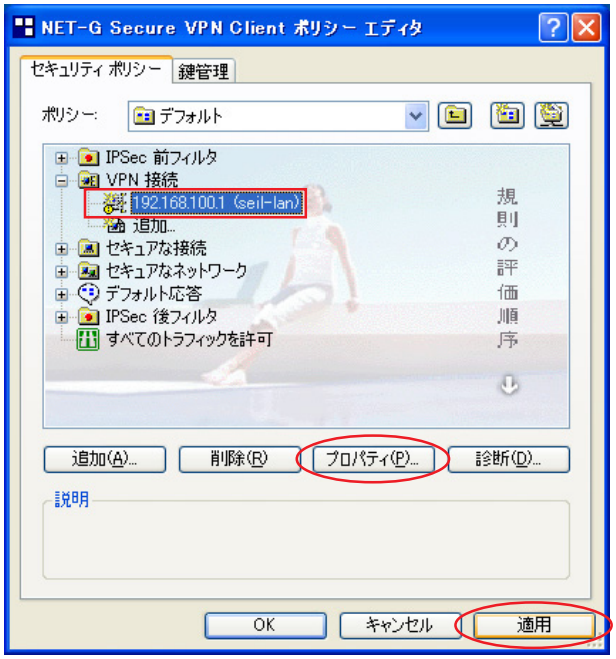
さらに、「リモートネットワーク」については、右端にある“ ... ”をクリックしてください。



“ ... ”をクリックすると、「ネットワークエディタ」画面が開きます。

「ネットワークエディタ」画面では、「ネットワーク名」は任意の設定名を付けます。
「IP アドレス」「サブネットマスク」は、SEIL に接続している LAN について入力します。

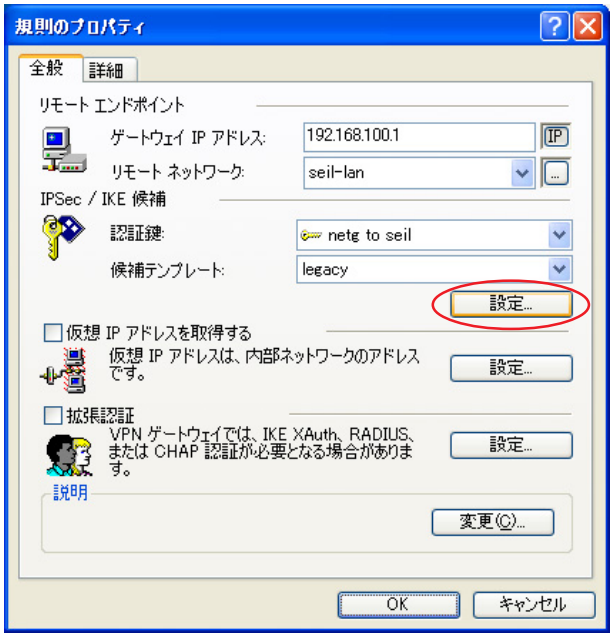
設定後に「OK」をクリックすると「セキュリティーポリシー」画面に戻ります。



「セキュリティーポリシー」画面で、これまでのセキュリティーポリシー設定が登録されていることを確認したら、「適用」ボタンをクリックしてください。

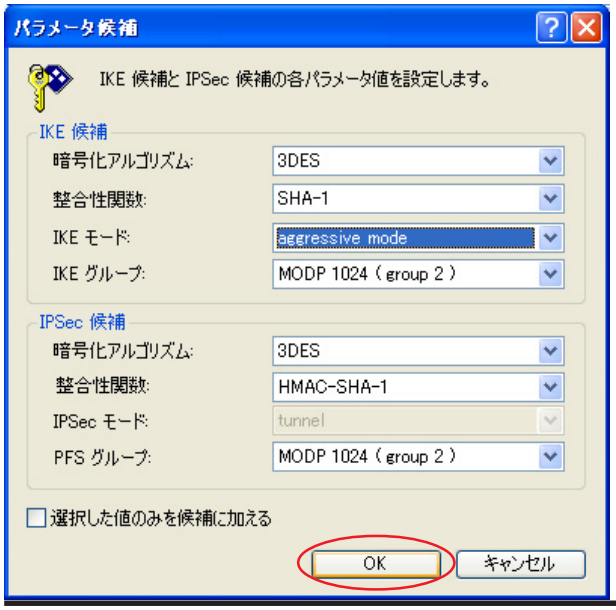
「適用」ボタンをクリックしないと適切に設定されない場合があります。

引き続いて、登録した設定を選択し、「プロパティ」ボタンをクリックしてください。



「規則のプロパティ」画面が開きます。

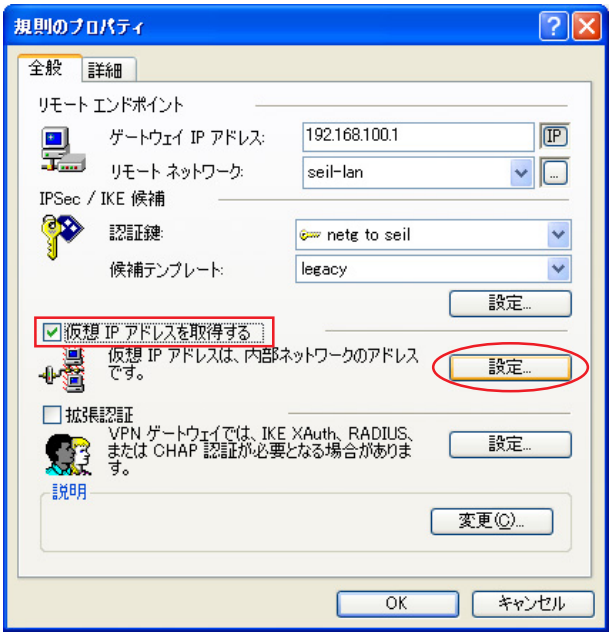
3つある「設定」ボタンのうち、一番上の「IPsec / IKE 候補」の「設定」ボタンをクリックします。



「パラメータ候補」画面が開きます。ここで暗号化方式などについて設定します。

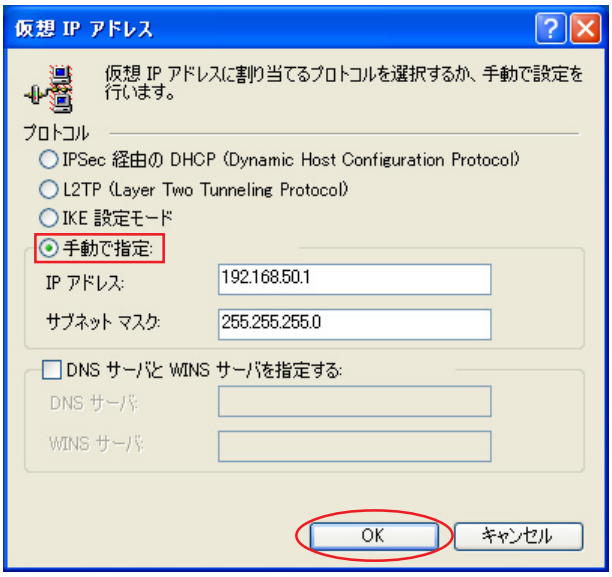
「IKE モード」は“ agressive mode ”に設定してください。

設定後に「OK」ボタンをクリックしてください。「規則のプロパティ」画面に戻ります。



「規則のプロパティ」画面に戻りましたら、続いて「仮想 IP アドレスを取得する」にチェックを入れ、2 つ目の「設定」ボタンをクリックしてください。

「仮想 IP アドレス」画面が開きます。



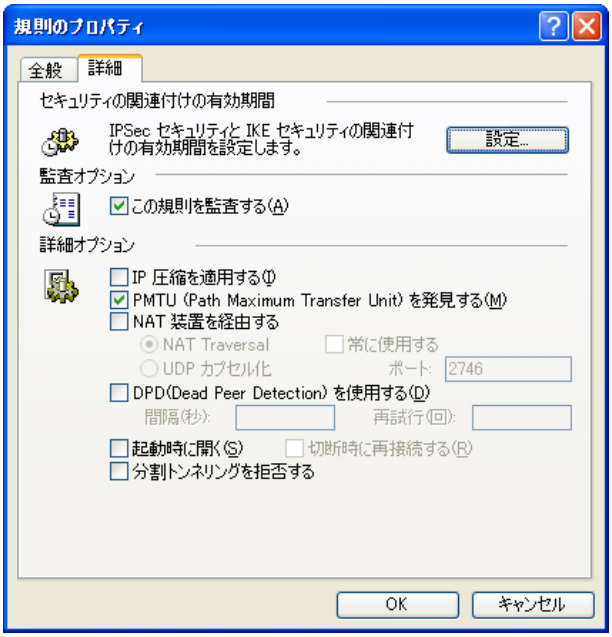
「仮想 IP アドレス」画面では、ホストが SEIL に IPsec 接続する際に使用する仮想的な IP アドレスを設定します。
SEIL から見たときには、仮想 IP アドレスが IPsec 対向のホストということになります。

「プロトコル」は“ 手動で指定 ”を選択し、任意のプライベート IP アドレスとサブネットマスクを入力します。
ここで入力する IP アドレスは、2-3.SEIL の設定の[セキュリティポリシーの設定]で指定した送信先 IP アドレスと一致させます。
ただしサブネットマスクは 24 ビットマスクとしてください。

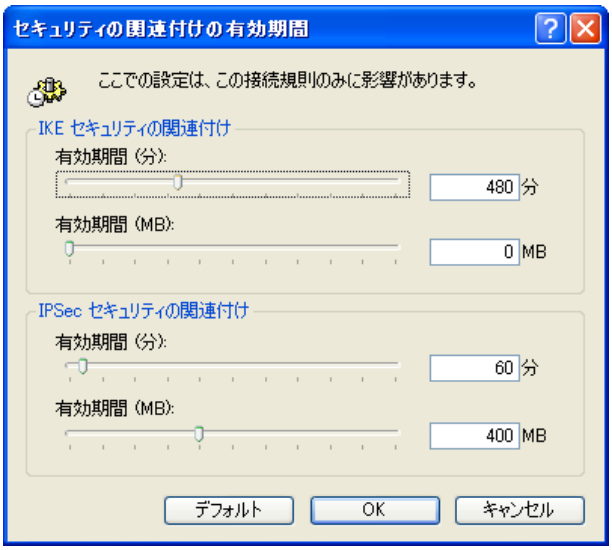
設定後に「OK」ボタンをクリックしてください。

[セキュリティポリシーの設定]

```
ipsec security-policy add SP01 security-association DynamicSA src 192.168.0.0/24 dst
192.168.50.1/32
```



「規則のプロパティ」の「詳細」画面で、[設定]をクリックします。



有効期間を設定します。2-3.SEIL の設定の[IKE プロポーザルの設定]、および[セキュリティアソシエーションプロポーザルの設定]で指定した lifetime-of-time の値に合わせます。

設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

IPsec 接続を開始してください。
(操作方法につきましては、製品マニュアルをご参照ください。)

[IKE プロポーザルの設定]
ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group modp1024 **lifetime-of-time 08h**

[セキュリティアソシエーションプロポーザルの設定]
ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm hmac-sha1 encryption-algorithm 3des **lifetime-of-time 01h**

3．接続設定例　～仮想 IP アドレスを使わない設定～

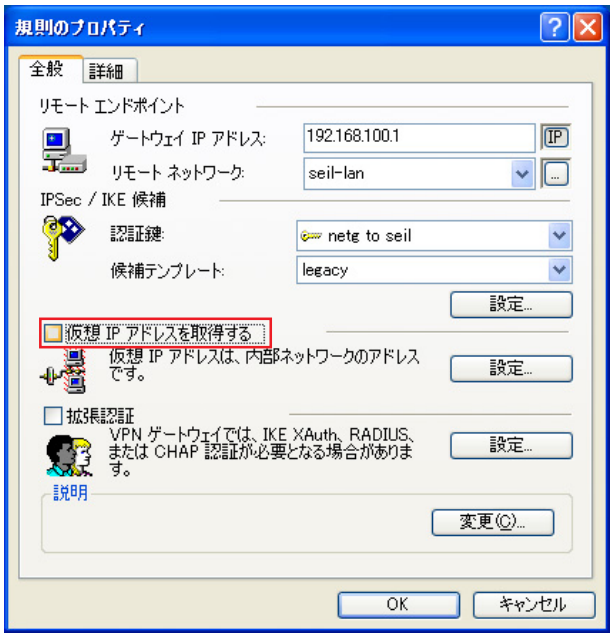
前セクションの基本設定例では、VPN Clinet 側で IPsec 接続時に使われる「仮想 IP アドレス」を設定しました。このとき SEIL 側の LAN からは、VPN Client に設定した「仮想 IP アドレス」に対して IPsec 経由での通信を行います。

この設定以外に、「仮想 IP アドレス」を使わずに、VPN Client と SEIL シリーズを IPsec 接続することもできます。

「仮想 IP アドレス」を使わないときは、SEIL 側の LAN からは、VPN Clinet が動作しているホスト自身が持つ IP アドレスに対して IPsec 通信を行います。

3-1.VPN Clinet の設定

「規則のプロパティ」画面の「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。



設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

3-2.SEIL の設定

2-3.SEIL の設定からの変更点を記します。

[変更前]
```
ipsec security-association add DynamicSA tunnel dynamic ike PHASE2 esp enable
ipsec security-policy add SPO1 security-association DynamicSA src 192.168.0.0/24 dst
192.168.50.1/32
```

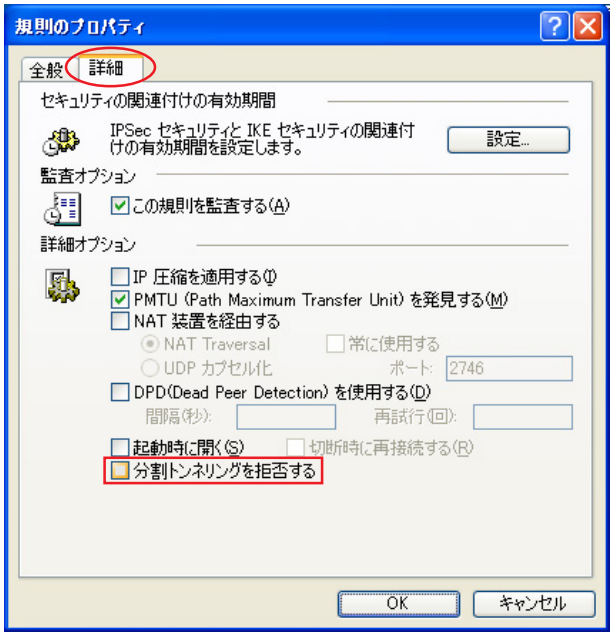
[変更後]　IPsec トンネルに動的アドレスを使用し、対応するセキュリティポリシを自動生成します。
```
ipsec security-association add AUTO tunnel auto ike PHASE2 esp enable
```

＜この設定での注意点＞
VPN Client 側が動的 IP 側の場合、IPsec 接続中に VPN Client 側の IP アドレスが何らかの理由で変わってしまうと、一時的に通信できない状態となります。
もしこのような状況になったときは、VPN Client を操作して IPsec 接続を再確立してください。

基本設定例にしたがって設定したときは、IPsec 通信とインターネットの同時アクセスができません。IPsec とインターネットを同時に利用するときは、次の設定を行ってください。

4-1.VPN Client の設定 1

「規則のプロパティ」画面の「詳細」タブをクリックし、「分割トンネリングを拒否する」のチェックを外します。



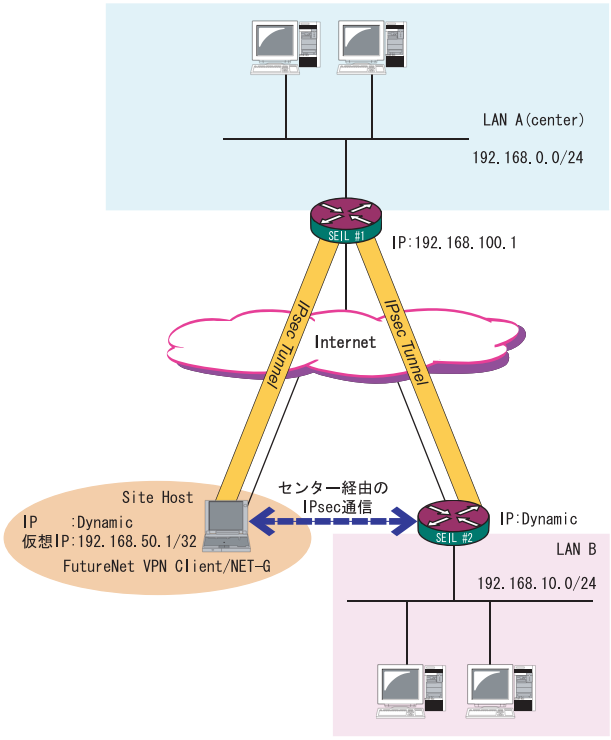
設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

5．接続設定例　～センター経由で IPsec 接続を行う設定～

5-1. ネットワーク構成

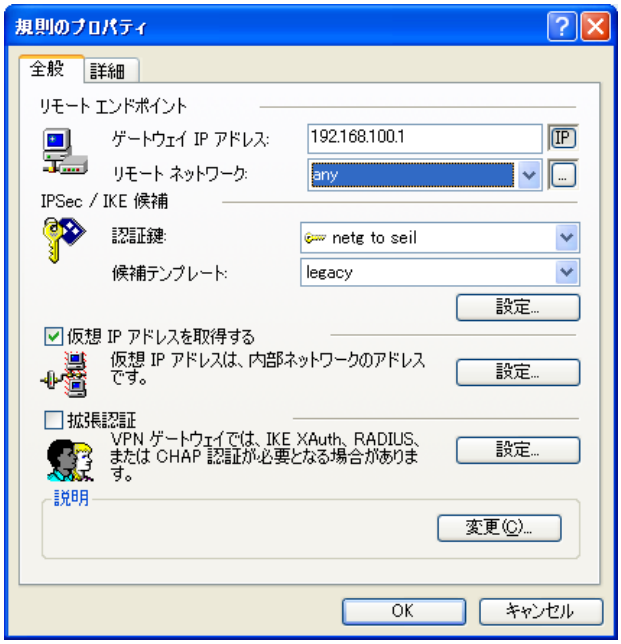
VPN Client は、センター側 LAN（LAN A(center)）と拠点側 LAN（LAN B）に IPsec で接続します。
拠点側にはセンター経由（SEIL #1）で IPsec 接続します。
IPsec トンネルは、VPN Client と SEIL #1 間、SEIL #2 と SEIL #1 間で生成します。



5-2.VPN Client の設定

基本設定については2-4. VPN Client の設定を参照してください。
ただし「規則のプロパティ」画面では、次のように設定してください。

・「リモートネットワーク」を指定する項目では、「any」を選択します。



設定後に「OK」ボタンをクリックしてください。

以上で VPN Client の設定は完了です。

5-3.SEIL の設定

5-3-1.SEIL #1(センター側)の設定

IPsec ポリシーについては、以下のような設定をしてください。

a.(VPN Client とセンター側 LAN を結ぶ設定)

本装置側の LAN 側のネットワークアドレス　any

相手側の LAN 側のネットワークアドレス　VPN Client の仮想 IP アドレス 192.168.50.1/32

b.(センター側 LAN と拠点側 LAN を結ぶ設定)

本装置側の LAN 側のネットワークアドレス　any

相手側の LAN 側のネットワークアドレス　192.168.10.0/24

```
ike auto-initiation disable
ike preshared-key add netg.centurysys.co.jp "ipseckey"
ike preshared-key add 510c.centurysys.co.jp "ipseckey"
ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group
modp1024 lifetime-of-time 08h
ike peer add 510C address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier
fqdn 510c.centurysys.co.jp
ike peer add NET-G address dynamic exchange-mode aggressive proposals PHASE1 peers-identifier
fqdn netg.centurysys.co.jp
ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm
hmac-md5,hmac-sha1 encryption-algorithm 3des,des,aes128 lifetime-of-time 01h
ipsec security-association add NET-G tunnel dynamic ike PHASE2 esp enable
ipsec security-association add 510C tunnel dynamic ike PHASE2 esp enable
```

[特殊なセキュリティアソシエーションの追加]

```
ipsec security-association add sapass pass
ipsec security-policy add sppass security-association sapass src 192.168.0.1/32 dst
192.168.0.0/24
```

配下の端末から SEIL #1 への Telnet 通信を許可するための設定です。

```
ipsec security-policy add SP01 security-association NET-G src any dst 192.168.50.1/32
ipsec security-policy add SP02 security-association 510C src any dst 192.168.10.0/24
```

5-3-2.SEIL #2(拠点側)の設定

IPsec ポリシーについては、以下のような設定をしてください。

a.(センター側 LAN と拠点側 LAN を結ぶ設定)

本装置側の LAN 側のネットワークアドレス　192.168.10.0/24

相手側の LAN 側のネットワークアドレス　any

```
ike preshared-key add 510c.centurysys.co.jp "ipseckey"
ike proposal add PHASE1 encryption 3des hash sha1 authentication preshared-key dh-group
modp1024
ike peer add Turbo address 192.168.100.1 exchange-mode aggressive proposals PHASE1 my-identi-
fier fqdn 510c.centurysys.co.jp
ipsec security-association proposal add PHASE2 pfs-group modp1024 authentication-algorithm
hmac-sha1 encryption-algorithm 3des
ipsec security-association add SA01 tunnel lan1 192.168.100.1 ike PHASE2 esp enable

[特殊なセキュリティアソシエーションの追加]
ipsec security-association add sapass pass
ipsec security-policy add sppass01 security-association sapass src 192.168.10.1/32 dst
192.168.10.0/24
```

配下の端末から SEIL #2 への Telnet 通信を許可するための設定です。

```
ipsec security-policy add SP01 security-association SA01 src 192.168.10.0/24 dst any
```

これらの設定によって、VPN Client は全てのパケットをセンター側に送信し、センター側 LAN および拠点側 LAN に IPsec 接続可能となります。

この設定を用いると、動的 IP アドレスを持つ拠点 / クライアント同士を IPsec 接続できるようになります。

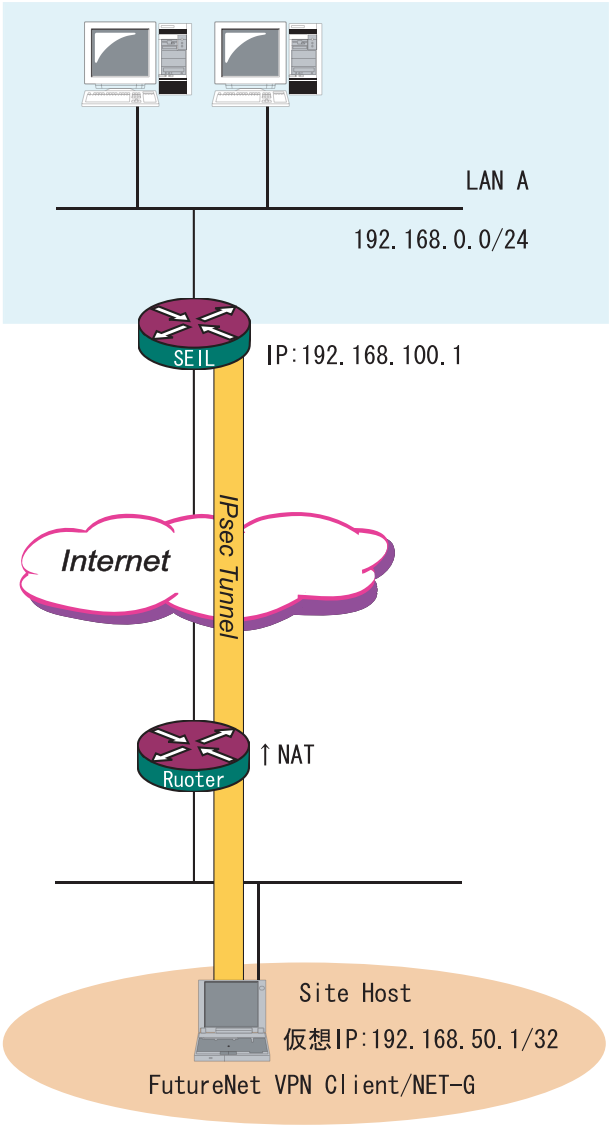
またこの運用においては、通常のインターネットアクセスもすべてセンター経由となります。

6. 接続設定例　～NAT 環境下での接続 1～

NAT ルータの配下にあるホストから IPsec 通信を行うための設定例です。

6-1. ネットワーク構成

SEIL をセンター側(LAN A)、VPN Client を拠点側とします。Router は NAT ルータとして機能します。この環境下で、VPN Client と LAN A 間でのセキュアな通信を確立させます。



6-2. 接続条件

・PSK(共通鍵)方式で認証します。

・agressive モードで接続します。

・SEIL 側は固定 IP とします。

・NET-G の上位ルータは、IP マスカレード処理だけをしているものとします。

・それぞれの LAN は以下の設定とします。
　LAN A ： 192.168.0.0/24
　LAN B ： 192.168.1.0/24

・NET-G の仮想 IP アドレスは以下のようにします。
　192.168.50.1/255.255.255.0

・IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。
　暗号方式 ： 3DES
　整合性　 ： SHA-1
　IKE で使用するグループ ： group2
　PSK　　：ipseckey
　拠点の ID ： netg.centurysys.co.jp

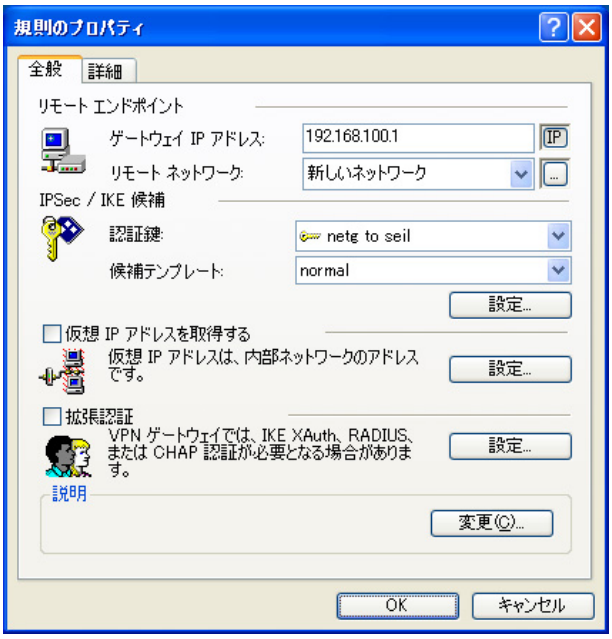
6-3.SEIL の設定

SEIL の設定は、2-3.SEIL の設定と同じにしてください。

SEIL は、NAT トラバーサル未対応のため、この条件下で IPsec 接続できる VPN Client 数は「1」です。

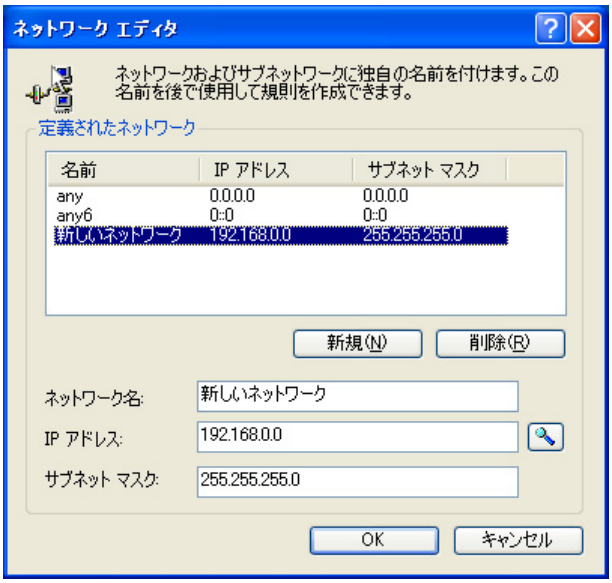
6-4.VPN Client の設定

[規則のプロパティ＜全般＞設定]



- ゲートウェイ IP アドレス
  「192.168.100.1」
- リモートネットワーク
  作成したリモートネットワーク設定を選択します(次項を参照ください)。
- 認証鍵：事前に作成した鍵を選択します。
- 候補テンプレート　「normal」
- 仮想 IP アドレスを使用する　「チェックなし」
- 拡張認証　「チェックなし」

[リモートネットワークの設定]



「新規」をクリックして以下のように設定してください。

- IP アドレス　「192.168.0.0」
- サブネットマス　「255.255.255.0」

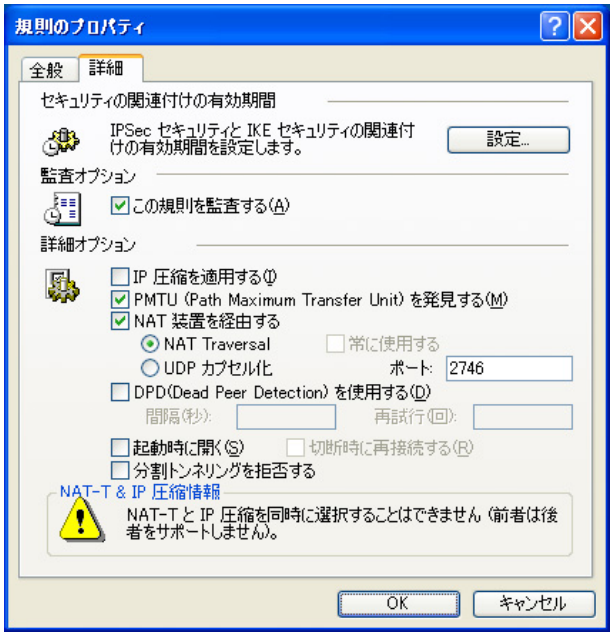
[パラメータの設定]

「IKE/IPsec 候補」項目の「設定 ...」をクリックします。

IKE 候補
- 暗号化アルゴリズム　「3DES」
- 整合性関数　「SHA-1」
- IKE モード　「aggressive mode」
- IKE グループ　「MODP 1024 (group2)」

IPsec 候補
- 暗号化アルゴリズム　「3DES」
- 整合性関数　「HMAC SHA-1」
- PFS グループ　「MODP 1024 (group2)」

[規則のプロパティ＜詳細＞設定]



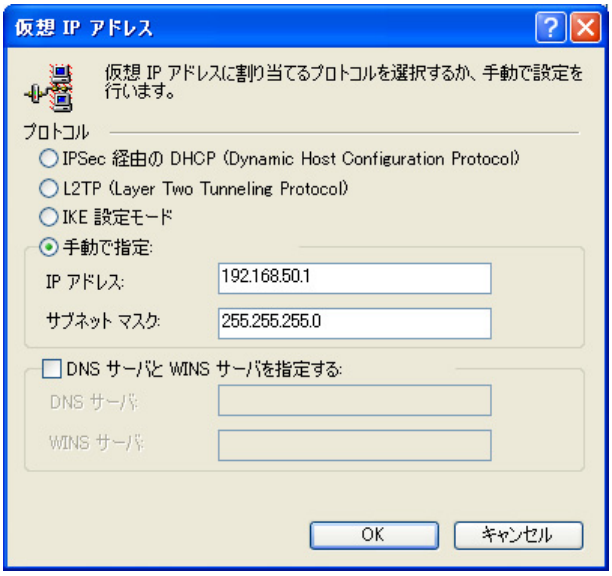
詳細オプション項目
下記のいずれかに設定してください。

- NAT 装置を経由する　チェックしない

- NAT 装置を経由する　チェックする
- NAT Traversal　チェックする
- 常に使用する　チェックしない

- NAT 装置を経由する　チェックする
- NAT Traversal　チェックする
- 常に使用する　チェックする

以上で VPN Client の設定は完了です。



[規則のプロパティ＜仮想 IP アドレス＞設定]
「規則のプロパティ」画面の「仮想 IP アドレスを取得する」にチェックを入れます。

続いて「設定」ボタンをクリックします。

仮想 IP アドレス画面では、次のように設定します。

- 手動で設定にチェック
- IP アドレス　「192.168.50.1」
- サブネットマスク　「255.255.255.0」

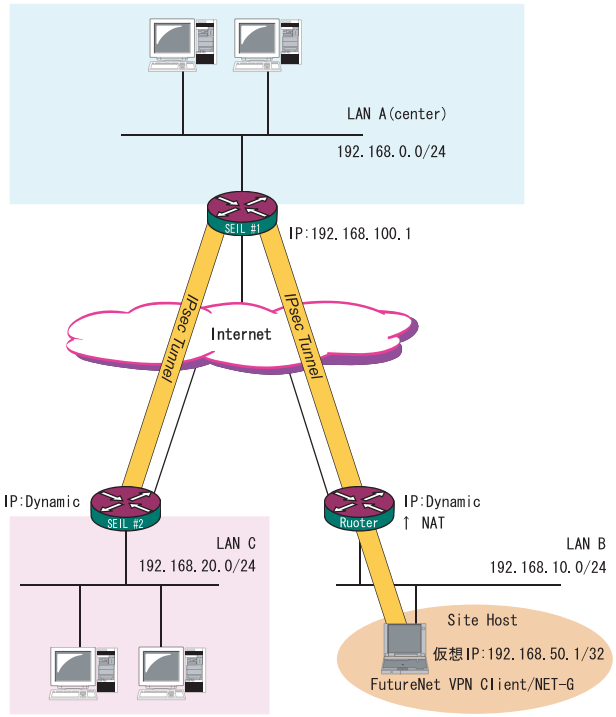
6-5. 複数の VPN Client を接続する場合

SEIL は、NAT トラバーサル未対応のため、複数の VPN Client を接続することはできません。この条件下で IPsec 接続できる VPN Client 数は「1」です。

7. 接続設定例　～NAT 環境下での接続 2～

NAT 環境下での IPsec 接続と、通常の IPsec 接続を同時に行うための設定です。

7-1. ネットワーク構成



7-2. 運用条件

・SEIL #1 は固定 IP アドレス、Router と SEIL #2 は動的 IP アドレスとします。

・Router は通常の NAT ルータとして動作します。

・SEIL #1 と PC は、NAT トラバーサルによって IPsec 接続を行います。

・SEIL #1 と SEIL #2 は aggressive モードで IPsec 接続を行います。

・それぞれの LAN は以下の設定とします。
　LAN A ： 192.168.0.0/24
　LAN B ： 192.168.10.0/24
　LAN C ： 192.168.20.0/24

・その他の IP アドレス等は図中の表記を使うものとします。

・IPsec 設定で使用するパラメータ値は以下の通りとします。
　暗号方式　　：3DES
　整合性　　：SHA-1
　IKE で使用するグループ ：group2

・VPN Client の仮想 IP アドレス設定は以下の通りとします。
　192.168.50.1/255.255.255.0

7-3.SEIL の設定

7-3-1.SEIL#1 の設定

5-3-1.SEIL #1(センター側)の設定を参照してください。

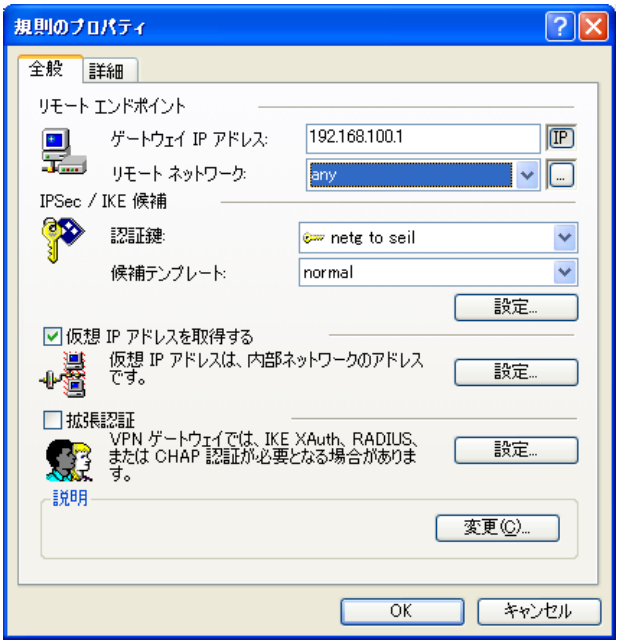
7-3-2.SEIL#2 の設定

5-3-2.SEIL #2(拠点側)の設定を参照してください。

SEIL は、NAT トラバーサル未対応のため、この条件下で IPsec 接続できる VPN Client 数は「1」です。

7-4.VPN Client の設定

[規則のプロパティ＜全般＞設定]



リモートネットワークとして、any を選択します。

その他の設定は、6-4.VPN Client の設定を参照してください。

FutureNet VPN Client/NET-G　接続設定ガイド　SEIL編　v1.0.0

2008年3月版

発行　センチュリー・システムズ株式会社