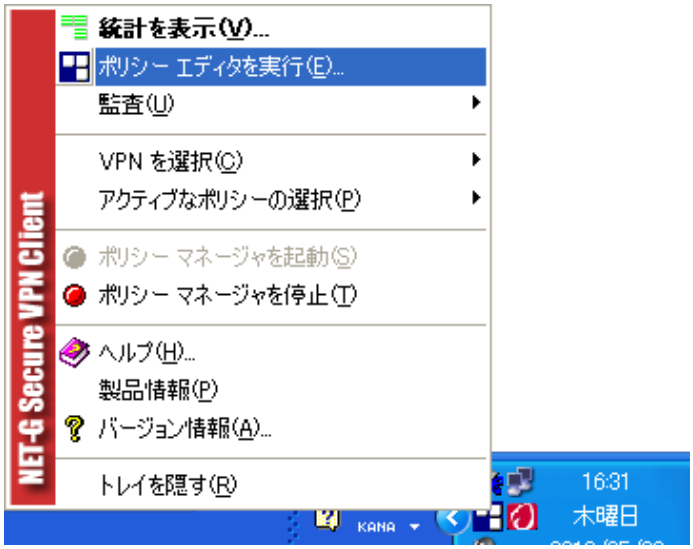
2-2. Secure VPN Client 側の設定

前提：既にソフトウェアがインストール済みであること

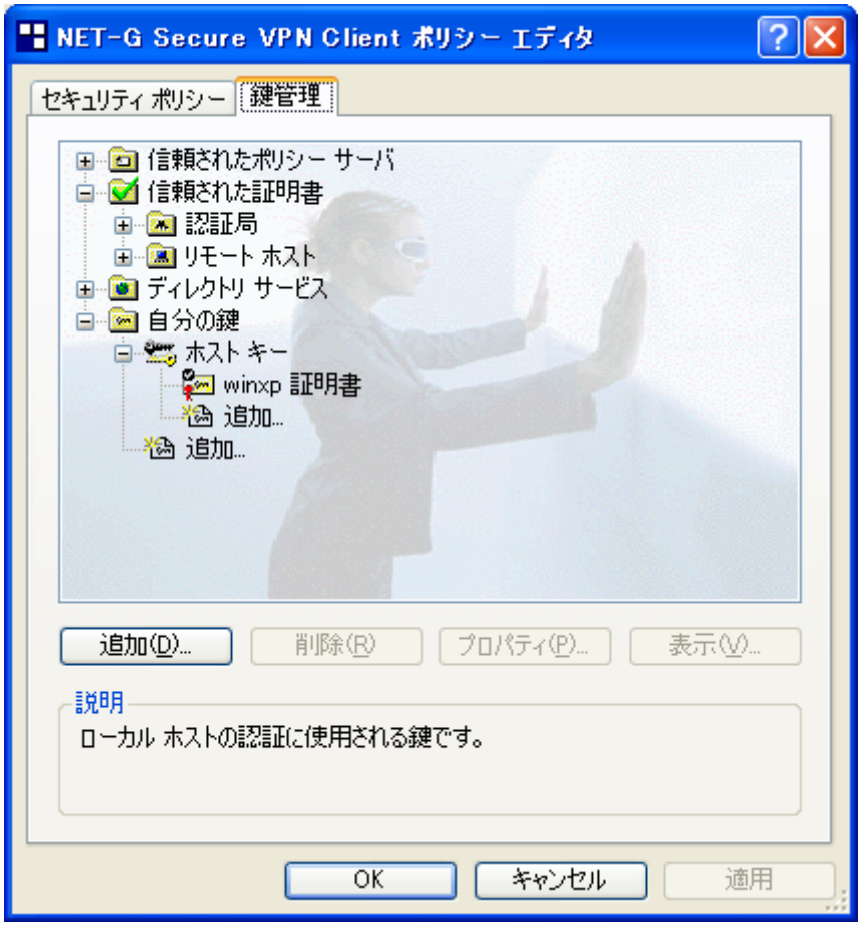
また、Secure VPN Client を設定するにあたり SSG 側で設定した以下の内容が必要となりますので事前に準備をお願いします。

1. ユーザ作成の際に設定した IKE Identity のメールアドレス
2. フェーズ 1 設定で設定した Preshared Key（事前共有鍵）
3. フェーズ 1/フェーズ 2 設定で設定した暗号アルゴリズムとハッシュ値

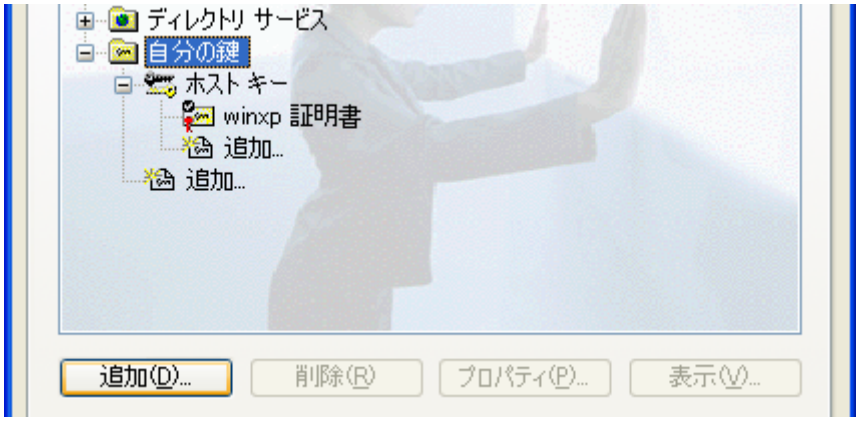
・タスクトレイにある Secure VPN Client のアイコンを右クリックし、”ポリシーエディタを実行”を選択します。

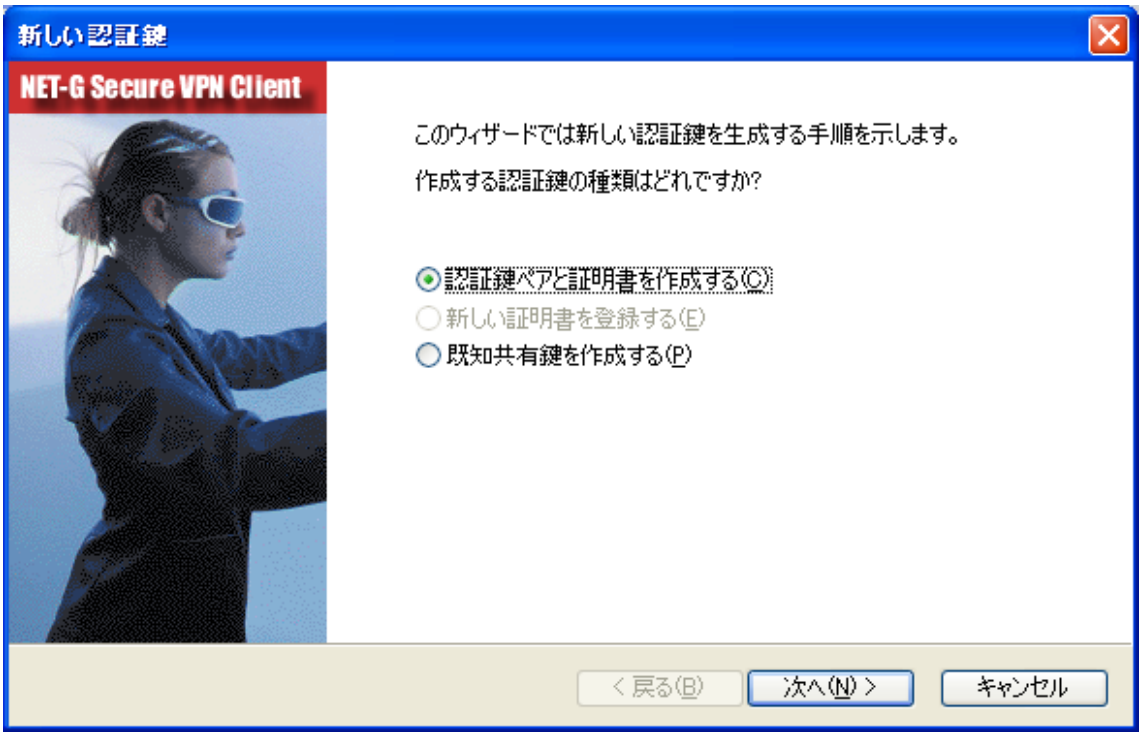


・はじめに共有鍵を設定します。鍵管理タブを選択してください。

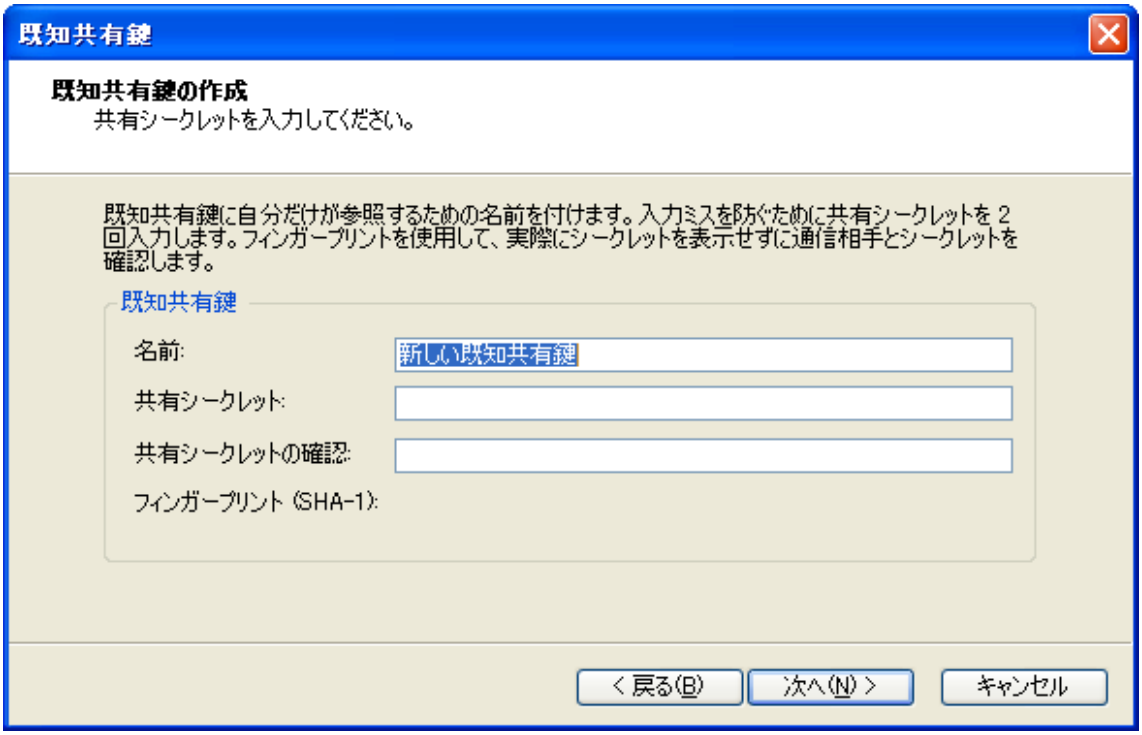


・下の方にある”自分の鍵”を選択し、追加を選択して新しい認証鍵ウィザードを表示させます。





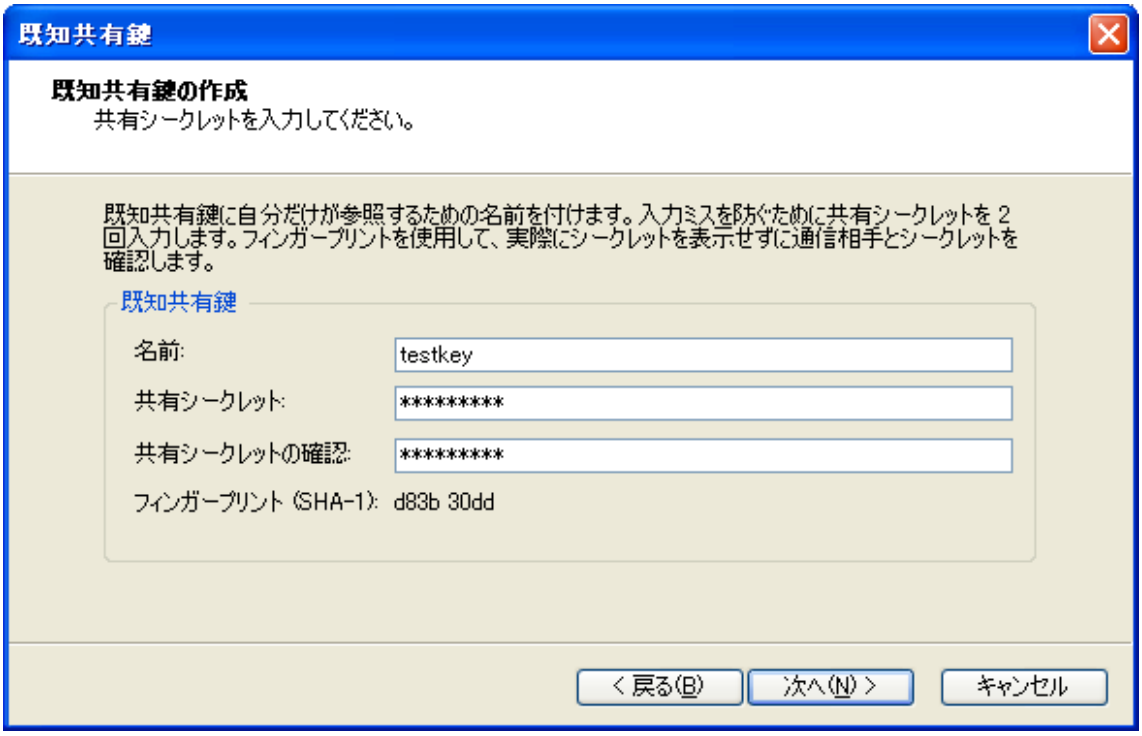
・”既知共有鍵を作成する”を選択し、次へ進みます。



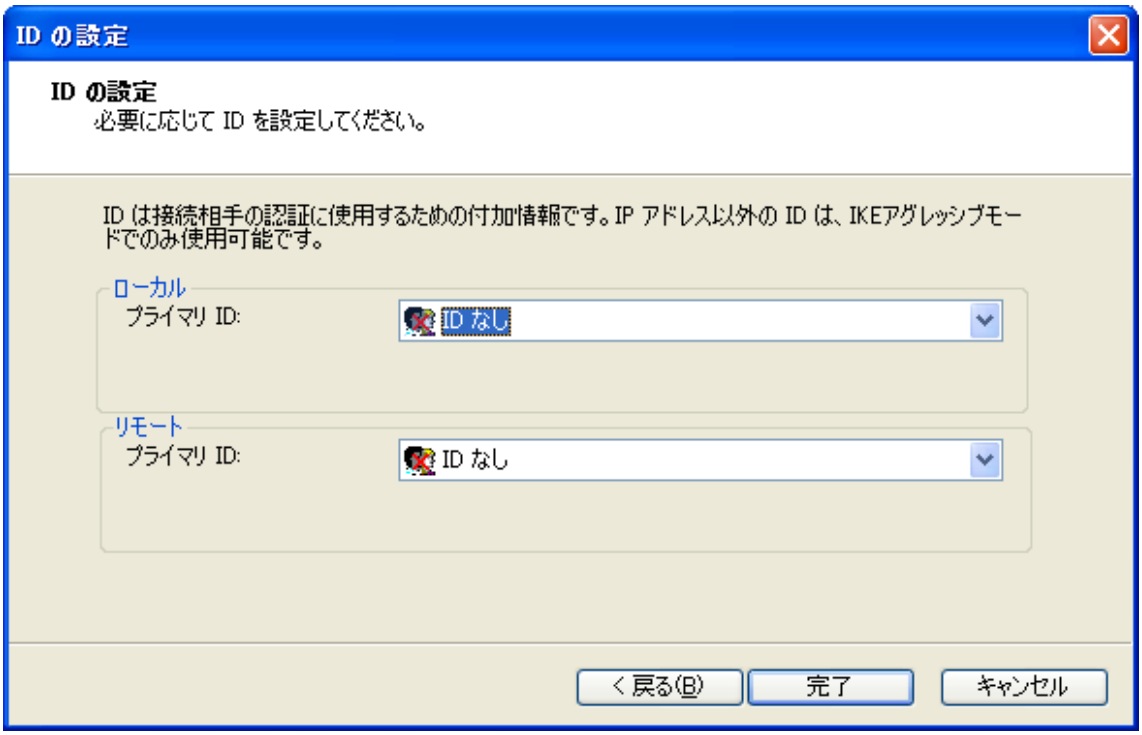
鍵として設定する内容は以下になります。

名前：任意の名前
共有シークレット：任意の値

ここではサンプルとして以下のように設定します。ただし、共有シークレットの値は SSG で設定したものと同じにする必要があります。



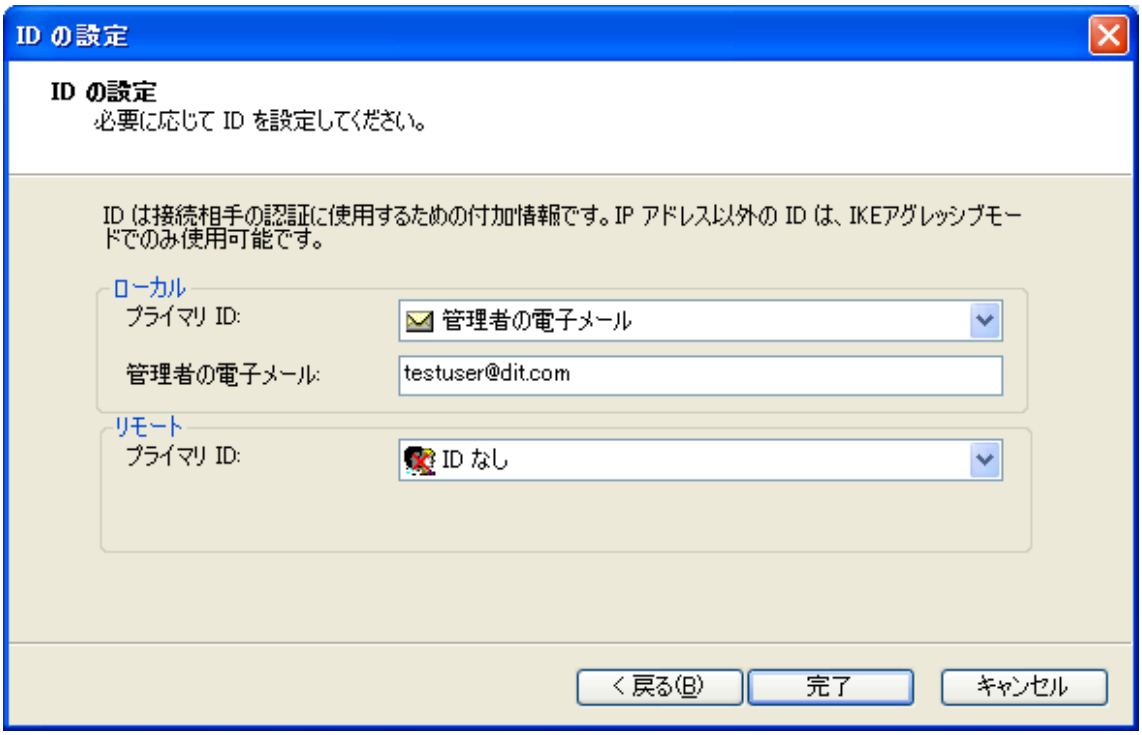
・次に ID を設定します。



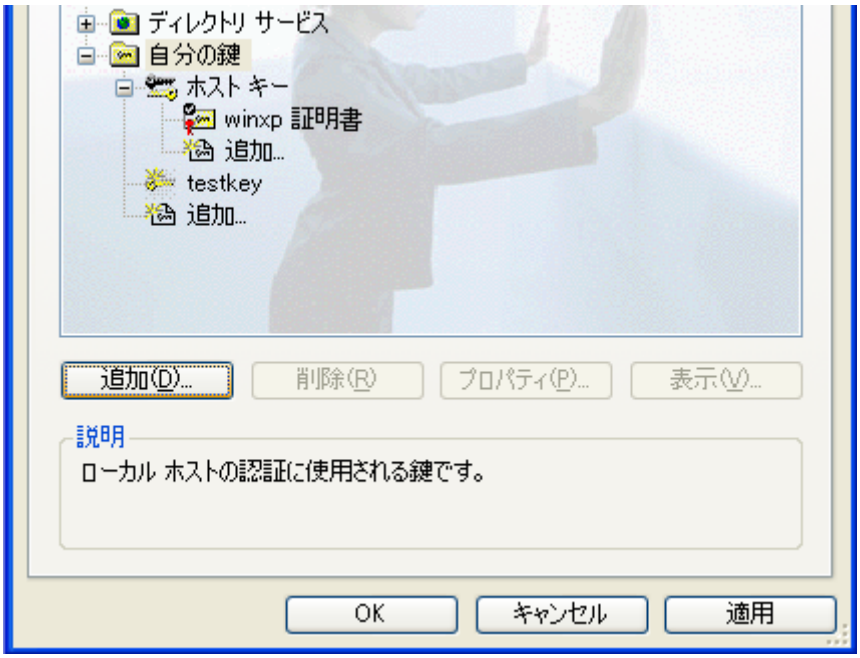
ここで設定を行うのはローカル側となり、選択支として以下があります。

・ホスト ID アドレス：端末の IP アドレス
・ホストドメイン名：端末のホスト名
・管理者の電子メール：メールアドレス
・ベンダ固有（CISCO Group ID）：接続先が Cisco の場合

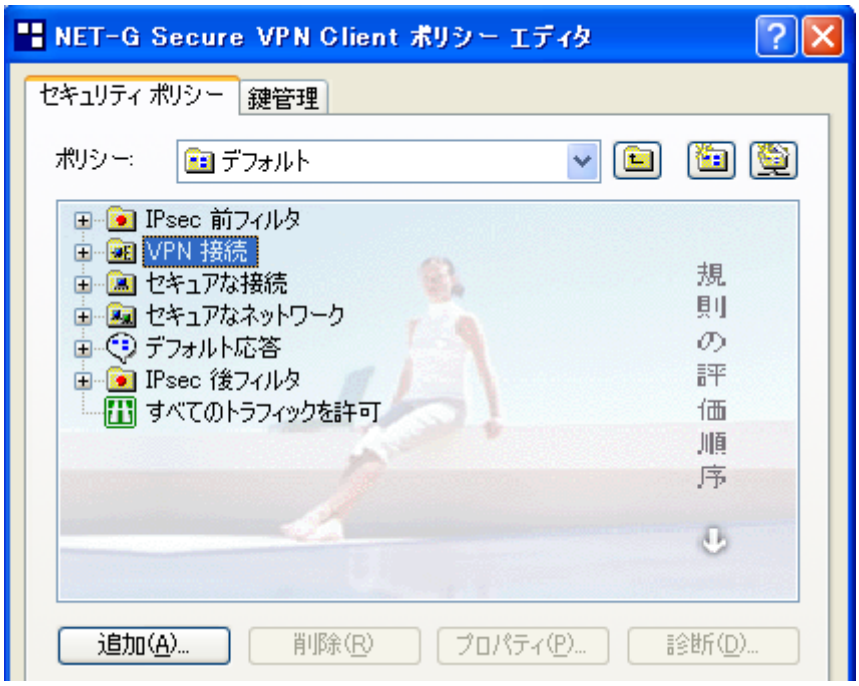
今回はメールアドレスを設定します。ただし、メールアドレスの値は SSG で設定したものと同じにする必要があります。



下記のように追加がされますので、適用ボタンを押し反映させてください。

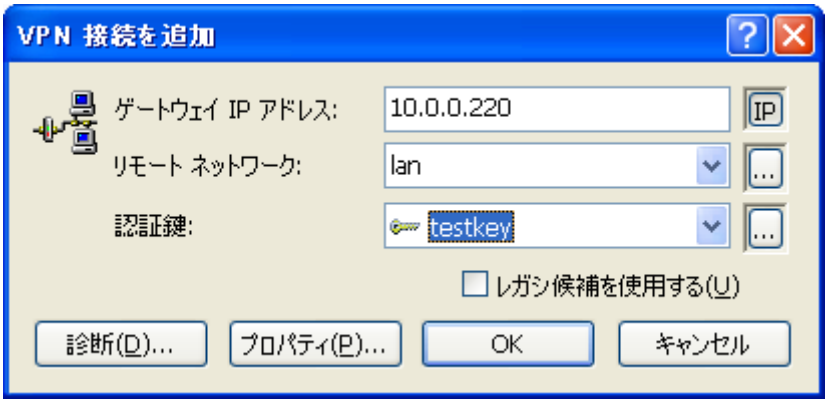


次にセキュリティポリシータブを選択し、VPN 接続を選んで追加を選択します。

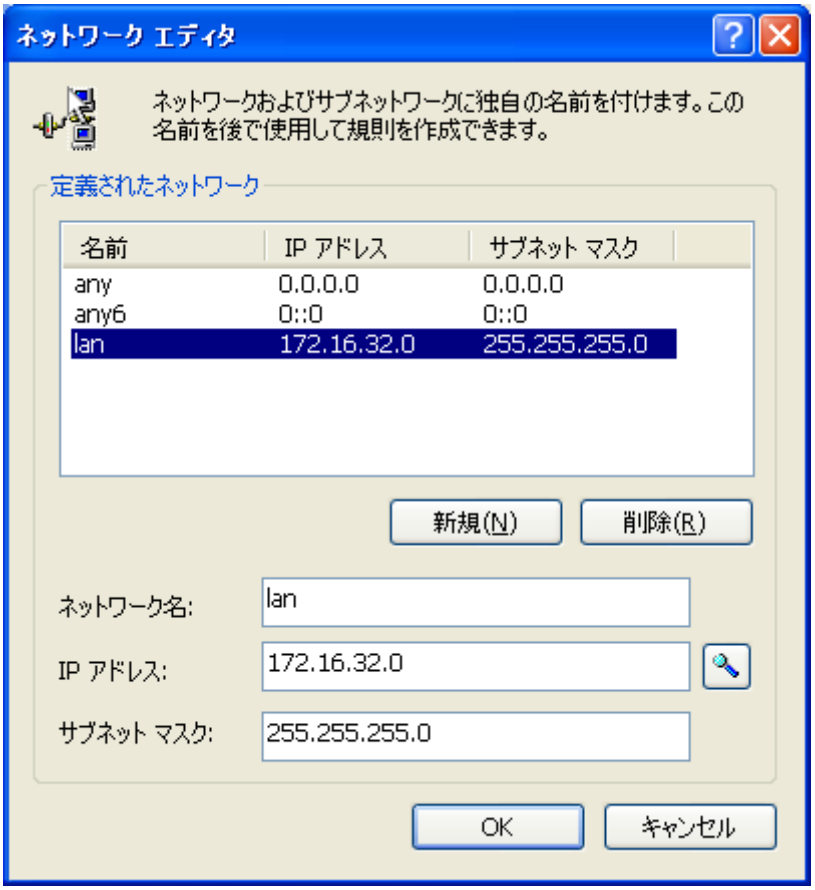


・接続先である SSG ルータの情報を入力します。

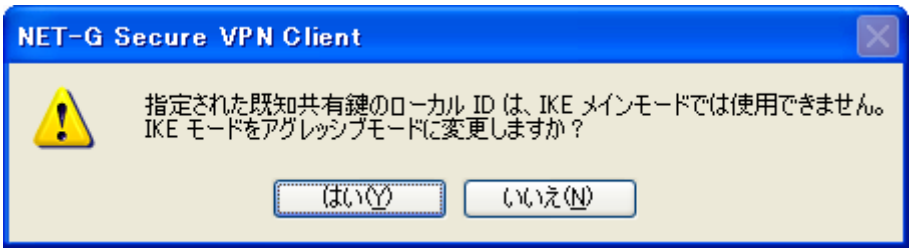
ゲートウェイ名 : SSG ルータの Untrust 側の IP アドレス（名前解決が出来ればホスト名）
リモートネットワーク：SSG ルータの Trust 側の IP アドレス
認証鍵：先に作成した共有鍵の名前



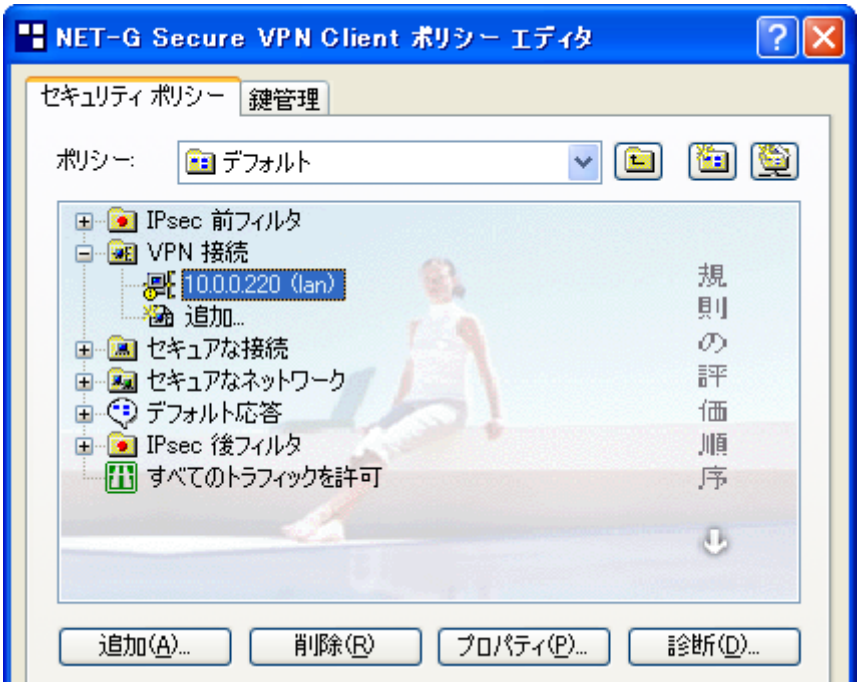
リモートネットワークの項目は下記のように事前にプロファイルとしてエントリーを作成し、後で選択するようにします。



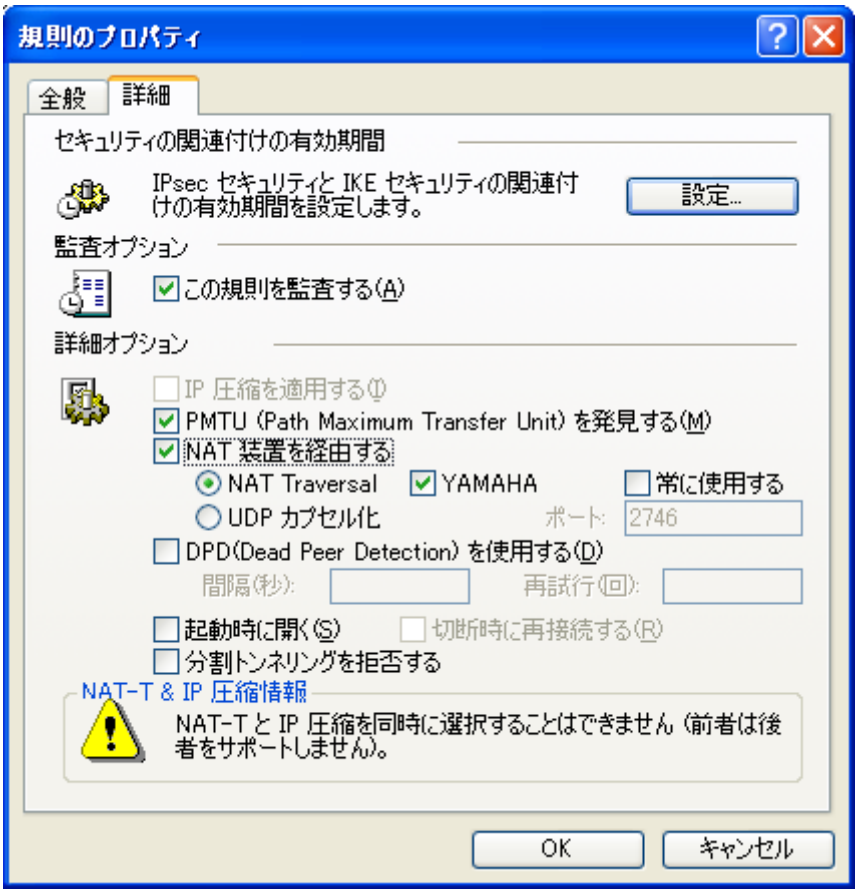
・ここで一度、OK を選択し、継続します。



・適用を押して、反映させます。

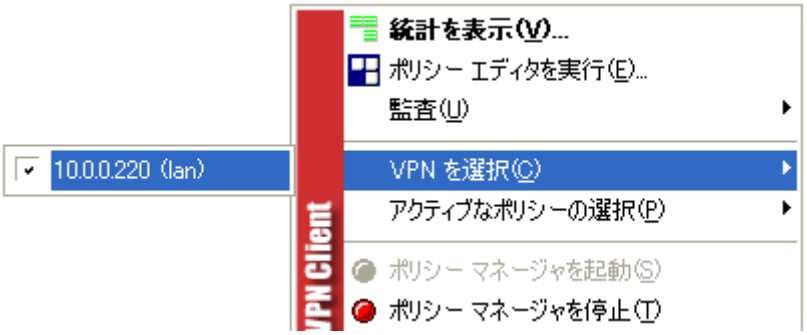


・プロパティを選択し、詳細タブより、NAT 装置を経由するにチェックを入れます。今回はクライアント端末が NAT ルータの配下にあるためこの設定を有効にします。チェックをつけない場合は VPN 接続が確立するものの実際の通信が出来ないことになります。

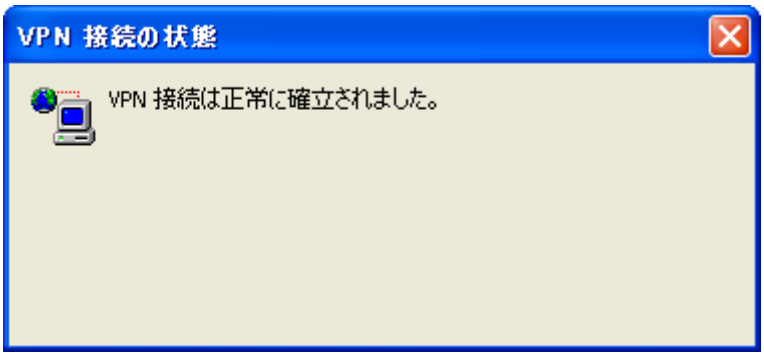


・OK を押して終了します。

・タスクトレイにある Secure VPN Client のアイコンを右クリックし、”VPN を選択”から作成した VPN 接続を選択し、VPN 接続を開始します。



正常に VPN 接続ができると下記のようなメッセージが表示されます。



後は普段利用しているアプリケーション等から社内にある Web サーバやメールサーバへ接続、又は Windows のファイル共有などを利用します。

※参考：接続が成功した場合の SSG には下記のようなログが記録されます。

Date / Time	Level	Description
2010-05-21 16:08:04	info	IKE 10.0.0.200 Phase 2 msg ID 2d5cffe6: Completed negotiations with SPI 5b646042, tunnel ID 32781, and lifetime 3600 seconds/409600 KB.
2010-05-21 16:08:04	info	IKE 10.0.0.200 Phase 2 msg ID 2d5cffe6: Responded to the peer's first message.
2010-05-21 16:08:04	info	IKE 10.0.0.200 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2010-05-21 16:08:04	info	IKE 10.0.0.200 Phase 1: Completed for user testuser.
2010-05-21 16:08:04	info	IKE<10.0.0.200> Phase 1: IKE responder has detected NAT in front of the remote device.
2010-05-21 16:08:04	info	IKE 10.0.0.200 Phase 1: Responder starts AGGRESSIVE mode negotiations.