3.3 PKI の利用

事前共有鍵の代わりに公開鍵証明書を利用して VPN 接続を行うことも可能です。

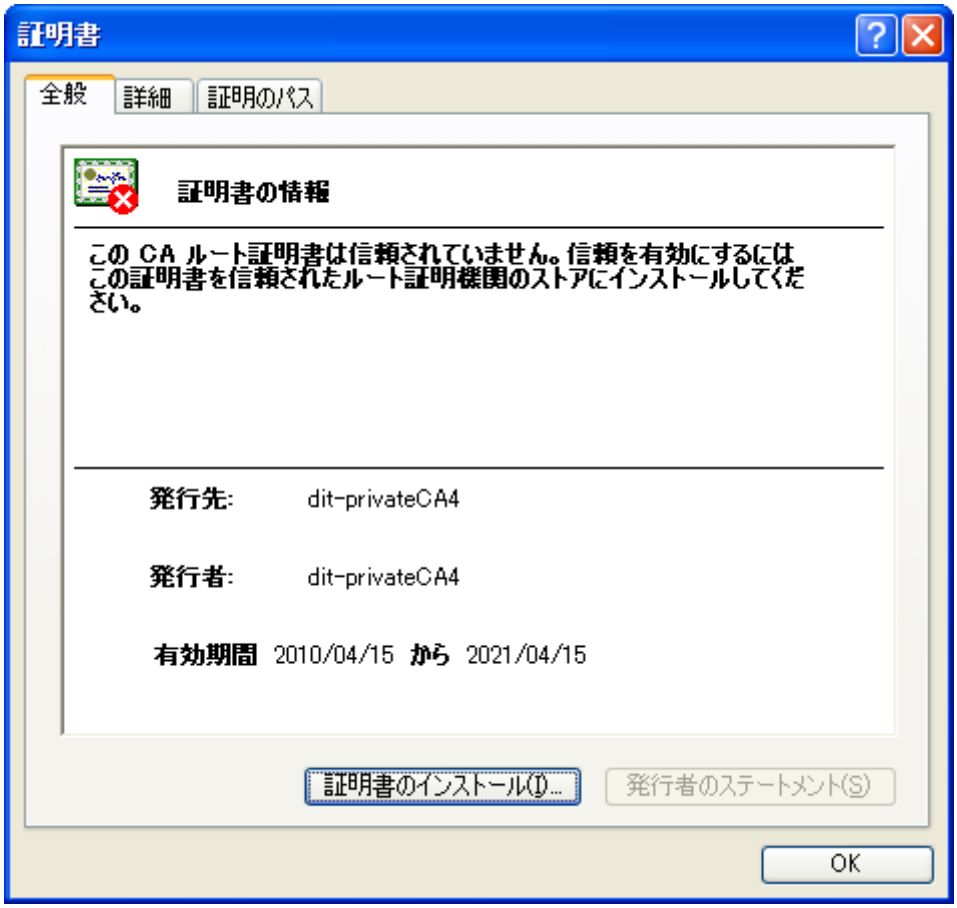
証明書には情報として有効期限や登録されている情報等が機関より正しいものと署名を受けたものとなるので、これらの情報を元に VPN 接続が行われることになりより安全な暗号化通信の環境を実現可能となります。

PKI の利用に際しては証明書を発行する機関である CA（認証局）が必要になります。公的（パブリック）にサービスとして利用できるものからプライベート目的で自社内で構築、利用されるものまで多種ありますが目的や環境等に従って適切なものを選択してください。ここではプライベート CA の場合について解説を行いますが発行される証明書の形式や設定方法については概ね同じとなります。

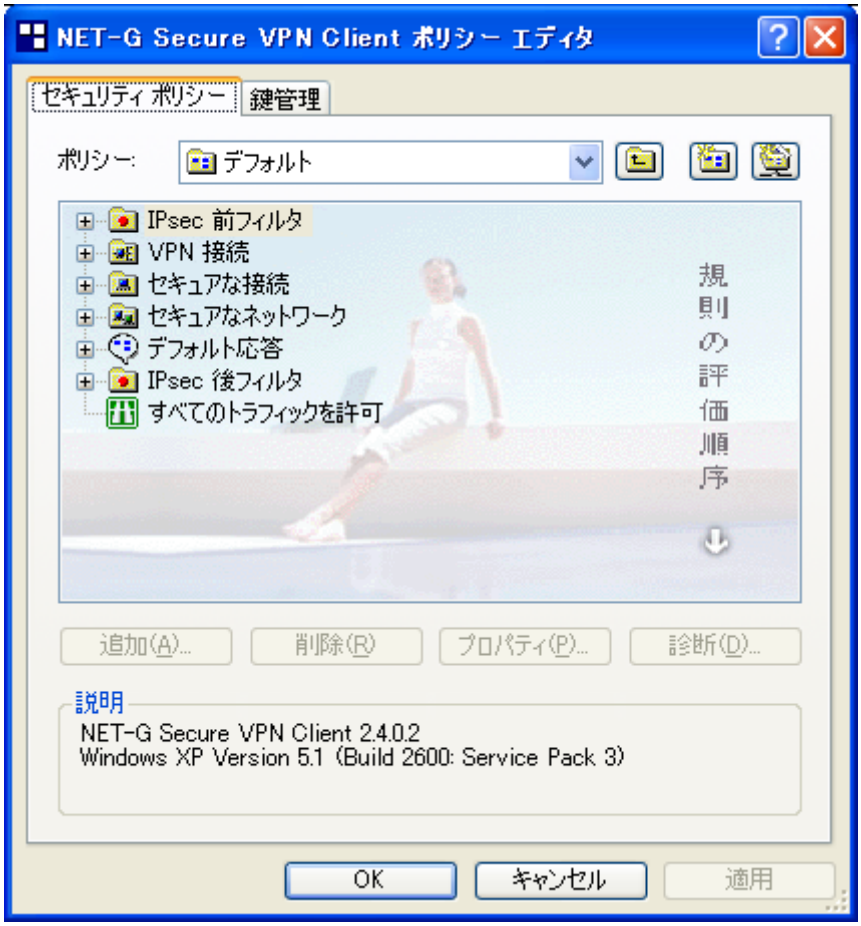
●Secure VPN Client の設定
基本的な流れとしては基礎編で行った設定をベースに認証鍵を事前共有鍵から証明書へと置き換えるだけです。

・ルート CA 証明書のインストール
事前に CA の証明書をファイルの形式で入手しておき、VPN Client がインストールされている端末のデスクトップ等に置いておきます。

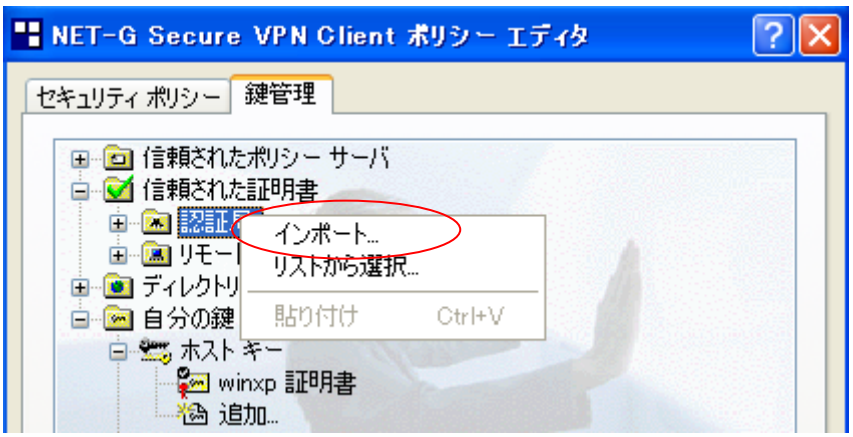
証明書ファイル（dit-privateCA4.crt を開いた時）



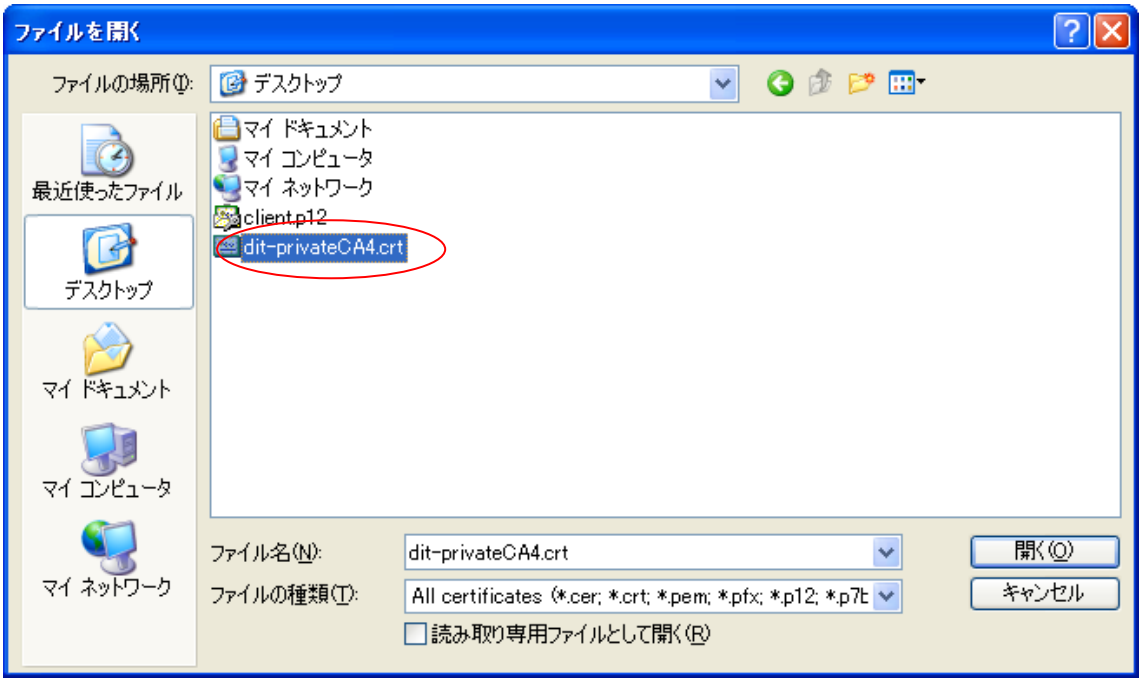
・タスクマネージャよりポリシーエディタを実行し、ウィンドウを開きます。



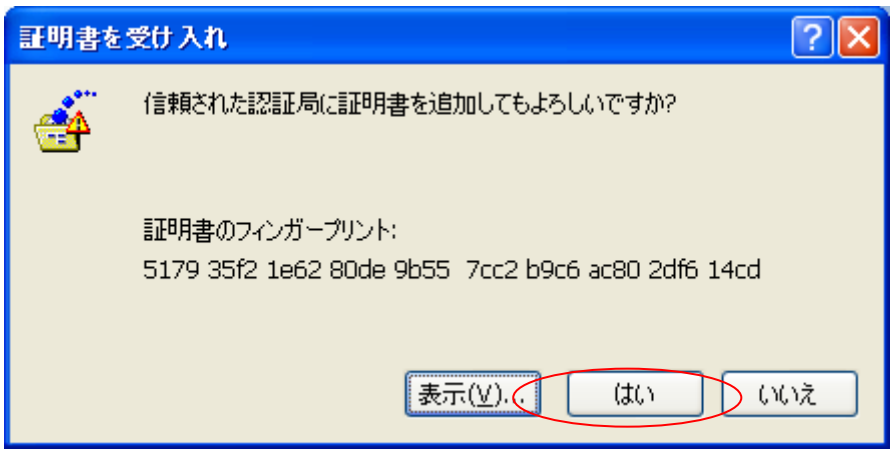
・鍵管理タブより、信頼された証明書 -> 認証局を選択し右クリックしてインポートを選択します。



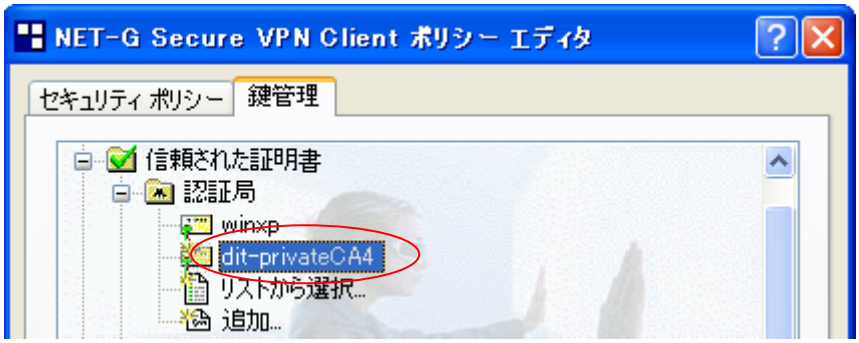
・”ファイルを開く”ウィンドウより CA 証明書のファイルを選択します。



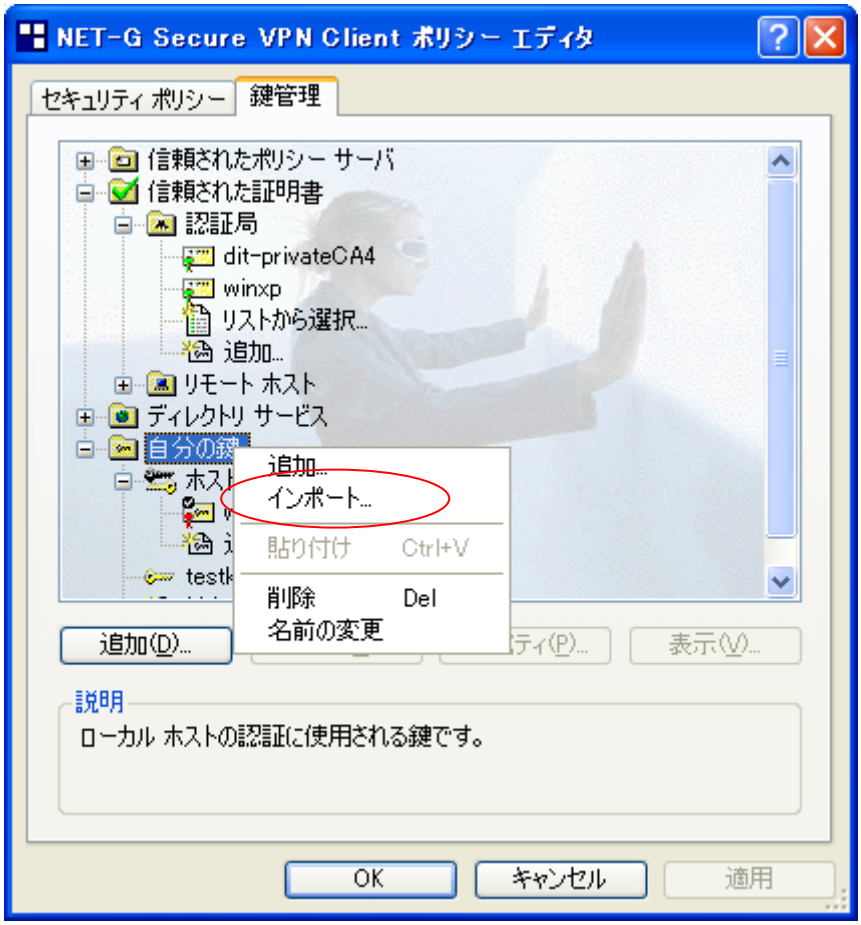
・以下のようなウィンドウが表示されますので、”はい”を選択します。



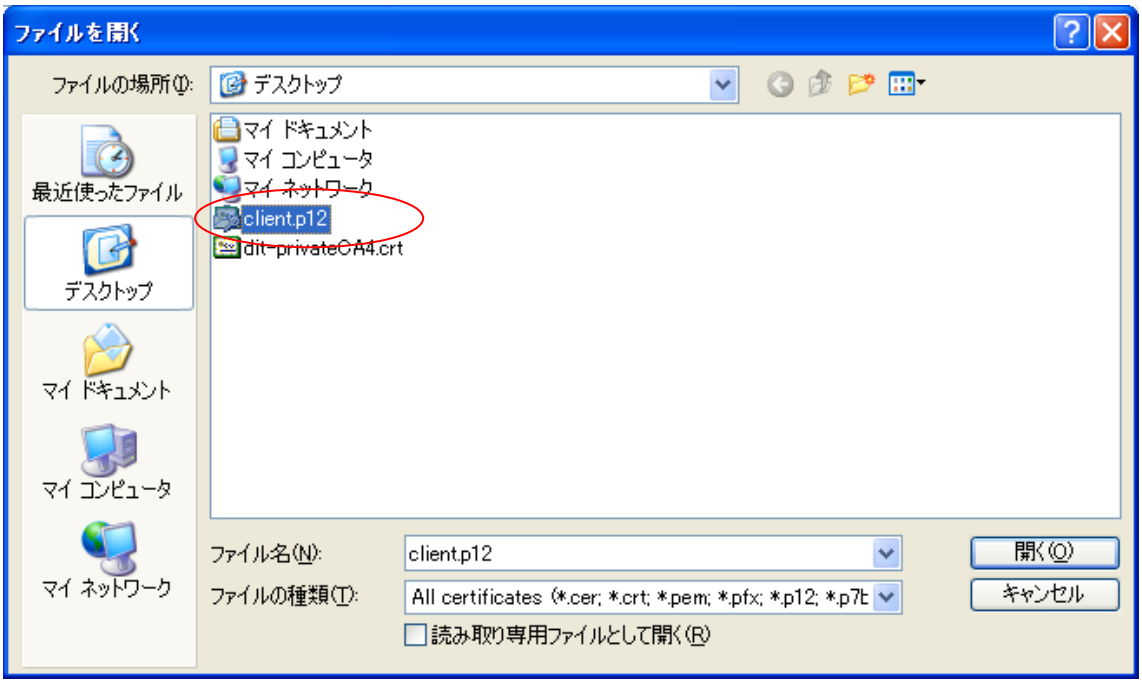
・下記のように認証局の項目の中に新しく CA 証明書が追加されますので、適用で反映させます。



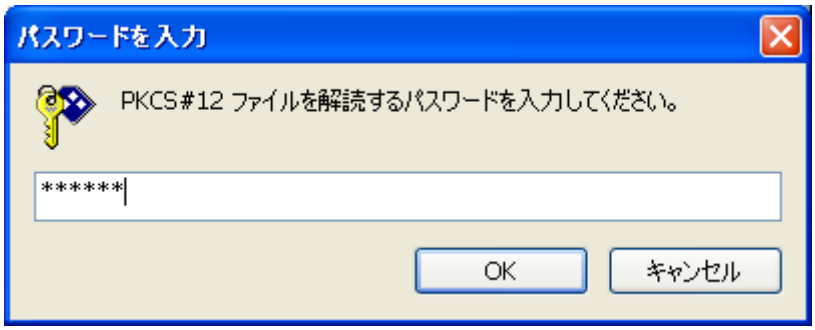
・ついで同じウィンドウの下の方の自分の鍵を選択し、右クリックでインポートを選びます。



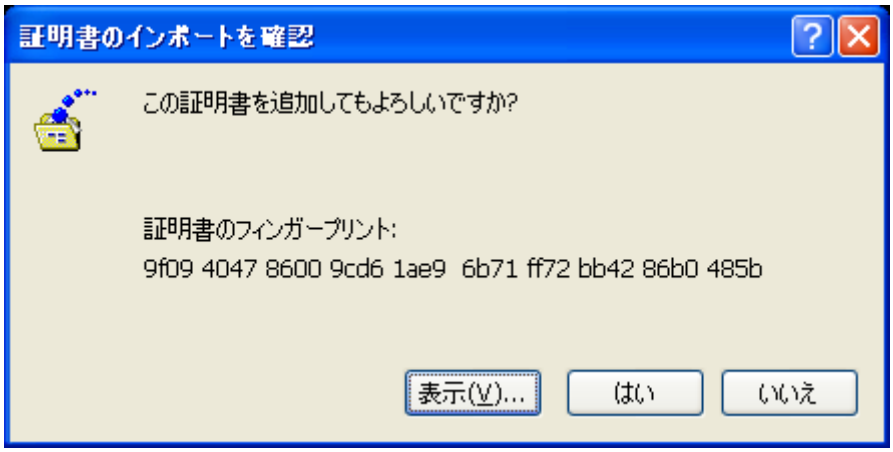
・事前に発行、入手しておいた自身の証明書（PKCS#12 形式）を選びます。



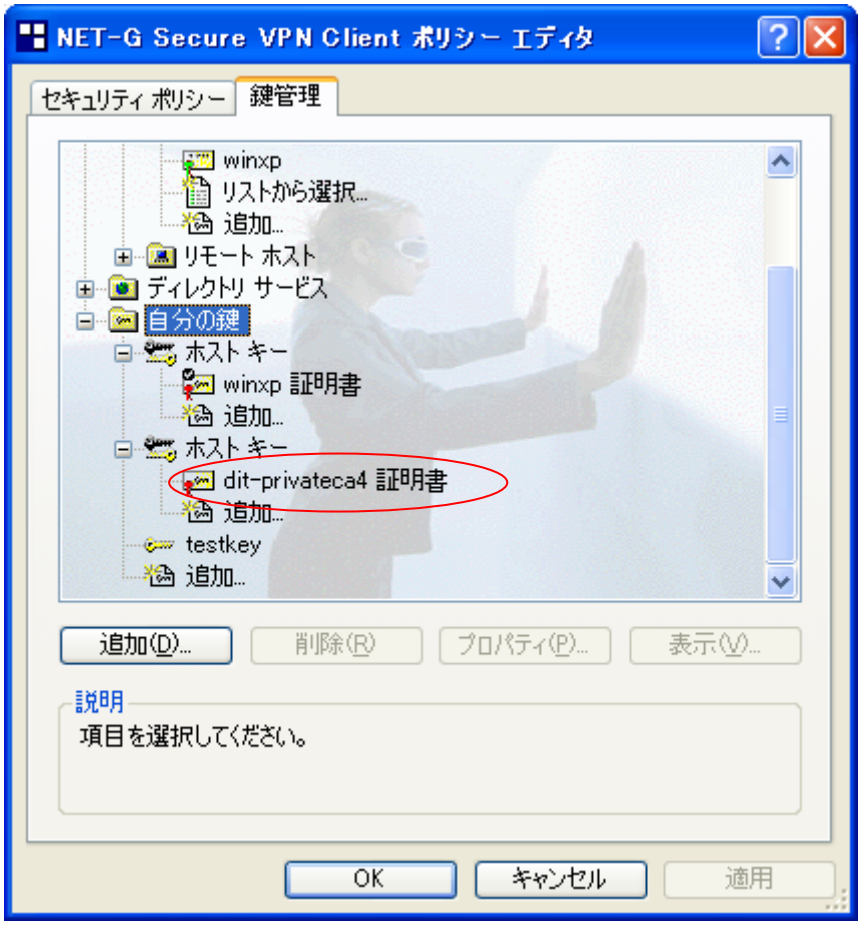
・パスワードが設定されている場合はパスワードを入力します。



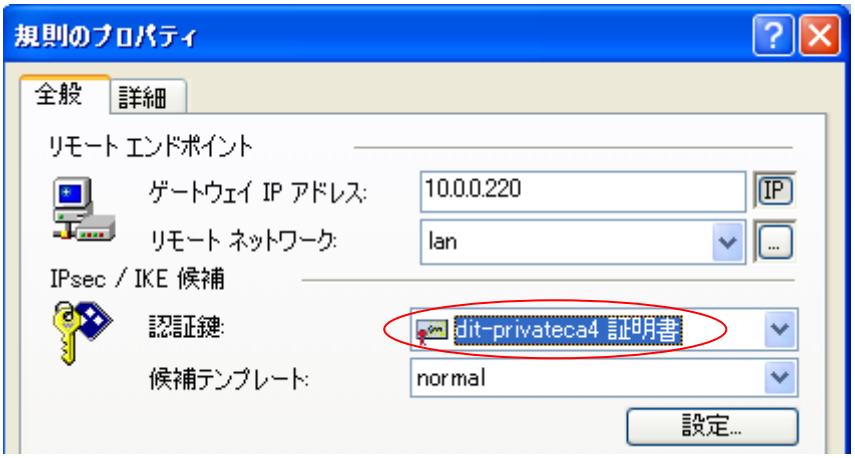
・確認が求められるので、”はい”を選択します。



・適用を選択して反映させます。



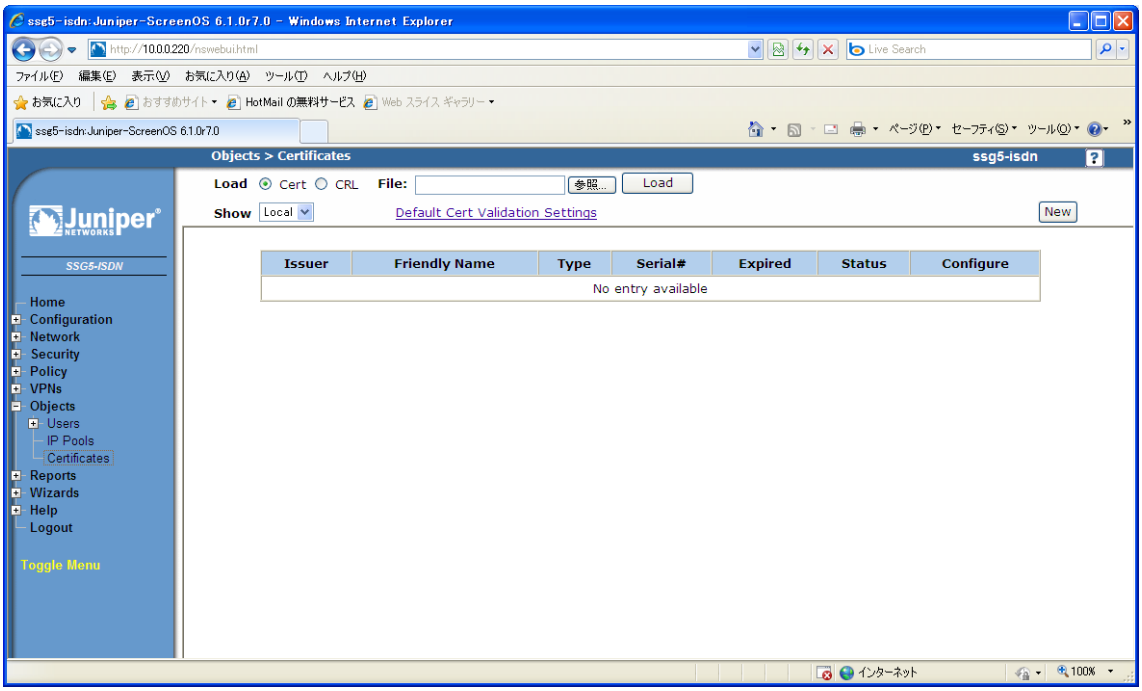
・後は定義してある VPN 接続の設定を開き、認証鍵としてインポートした CA の証明書を選択して Secure VPN Client の方の設定は終了となります。



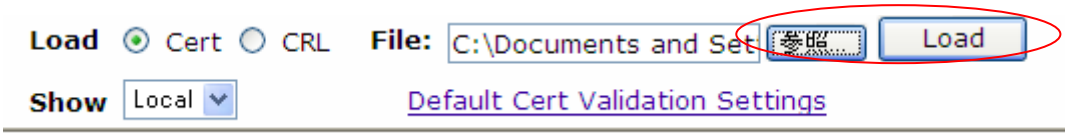
●SSG の設定

Secure VPN Client と同じようにまずは CA 証明書のインポートを行います。

・WebUI にログイン後、左欄のメニューの Objects から Certificates を選択します。



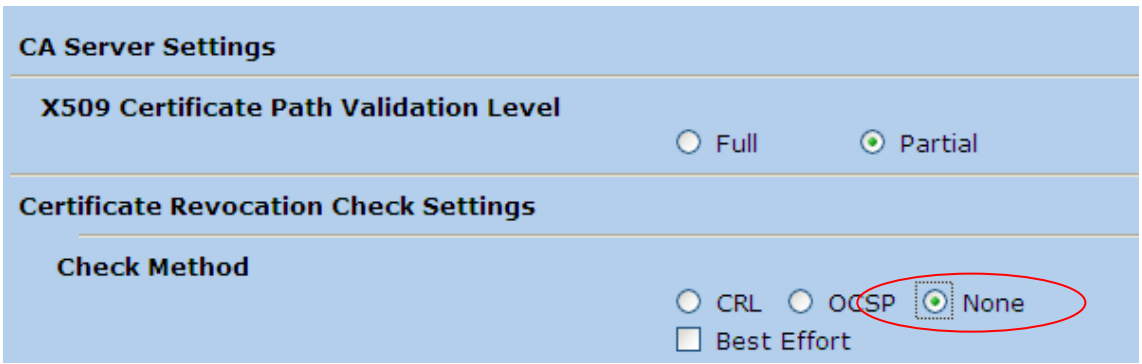
・ページ上段の”参照”を選択し、CA の証明書ファイルを指定して、Load ボタンでインポートを行います。



・Show の項目にて CA を選択して表示させると下記のよう追加されているのが分かります。

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
Class 3 Public Primary Certificatio Server Settings	5	CA	70bae41d10d92934b638ca7b03ccbabf	08-01-2028 23:59	Active	Detail,Remove
dit-privateCA4 Server Settings	10	CA	00028b71	04-15-2021 08:04	Active	Detail,Remove
Secure Server Certification Authori Server Settings	2	CA	02ad667e4e45fe5e576f3c98195eddc0	01-07-2010 23:59	Active	Detail
Class 3 Public Primary Certificatio Server Settings	7	CA	75337d9ab0e1233bae2d7de4469162d4	01-18-2015 23:59	Active	Detail,Remove

追加された CA（ここでは dit-privateCA4）の Server Settings を選択し、CRL 確認を無効にします。証明書の失効確認をきちんと行う場合は CRL のままとし、関連するパラメータも正しく設定するようにしてください。

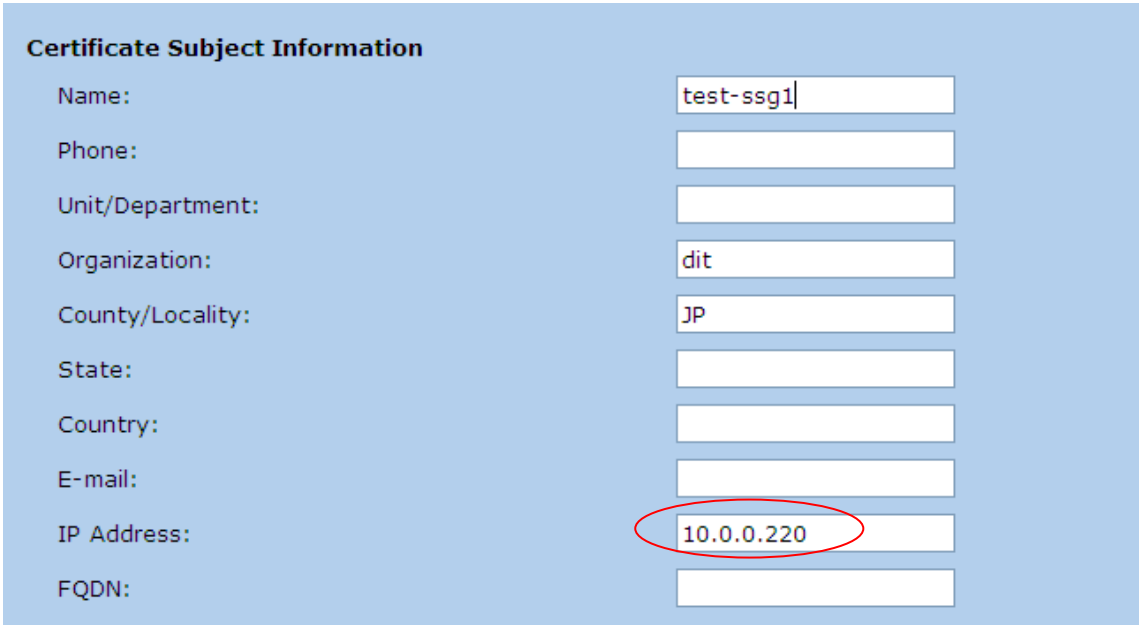


OK で終了します。

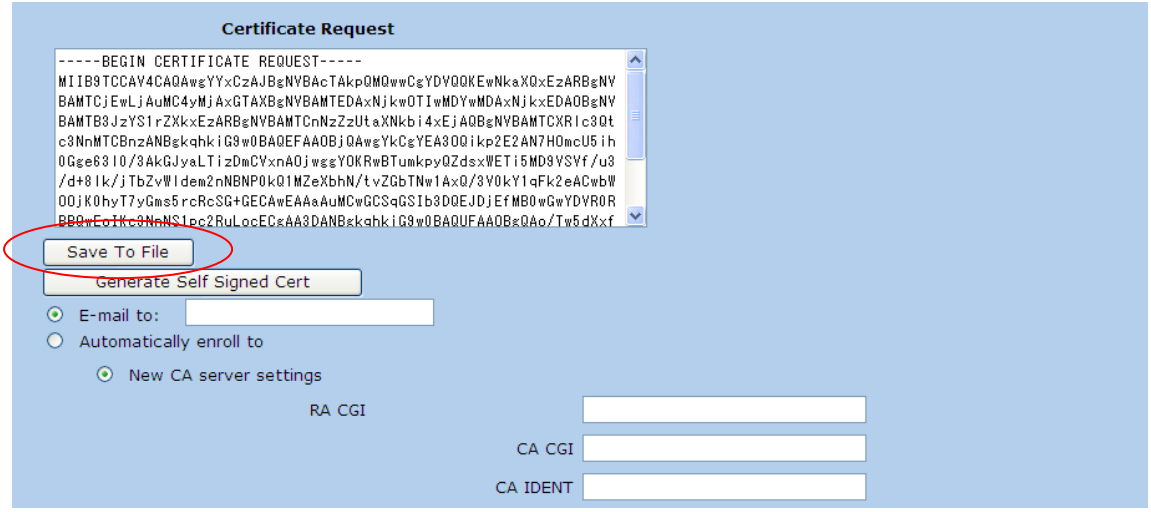
・SSG では PKCS#12 形式の証明書インポートができないので、新しくリクエストファイルを作成します。

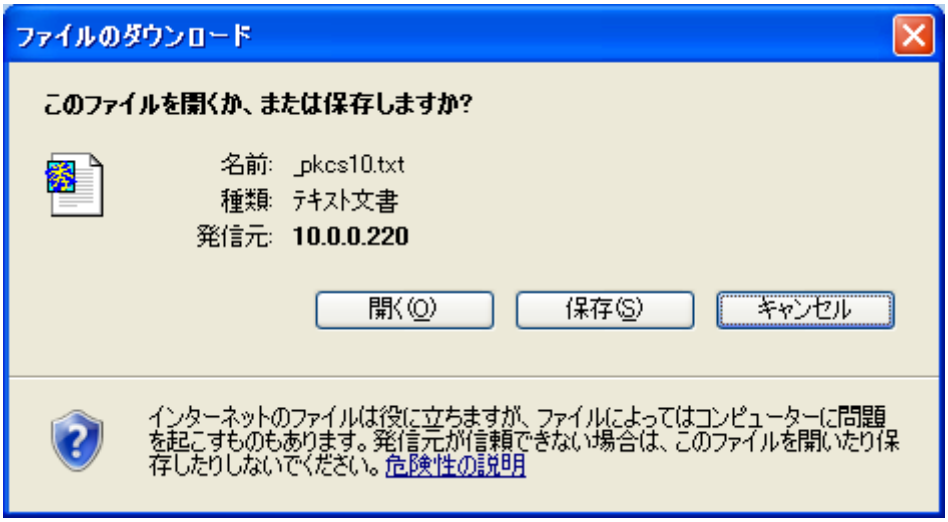
・Objects -> Certificates ページの右上の New を選択します。

・環境に応じて値（ここでは IP Address）を入力し、下欄の Generate ボタンをクリックします。



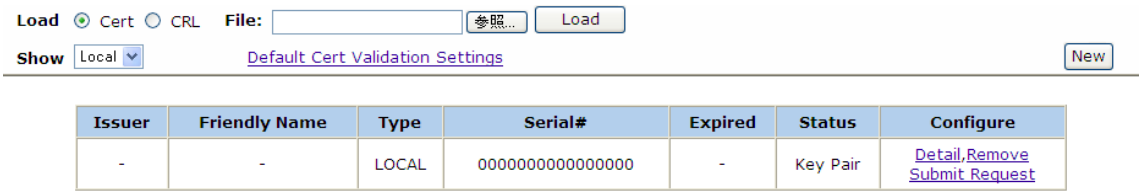
・しばらくした後、以下のような画面になったら、”Save To File”でデスクトップにファイルとして保存します。





SSG の画面はそのままでも一度閉じても問題ありません。保存したファイルを認証局の管理者に渡し証明書を発行してもらい、再度証明書のファイルをもらいデスクトップ等に同じく保存しておきます。

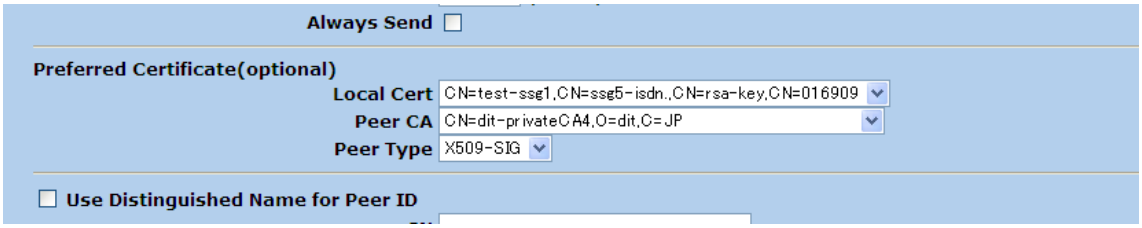
・Objects -> Certificates を選択すると下記のようになっています。



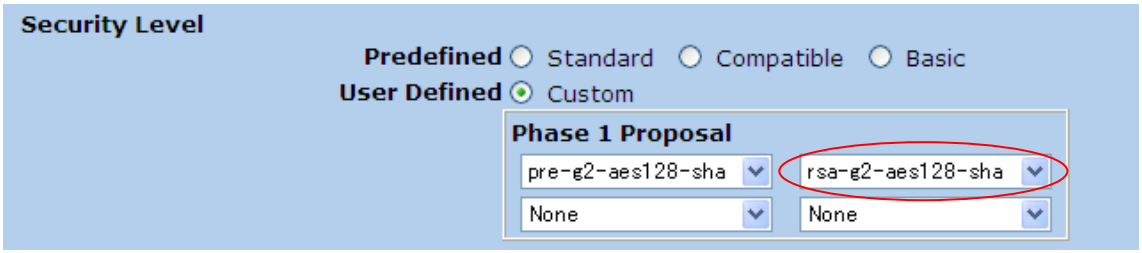
・上段の File から保存した証明書ファイルを参照で選択し、Load でインポートすると下記のように変わります。Show 項目が Local となっている箇所に SSG 自身の証明書が、CA となっている箇所で CA の証明書が確認できます。

・以上で証明書ファイルのインポートは終わりました。

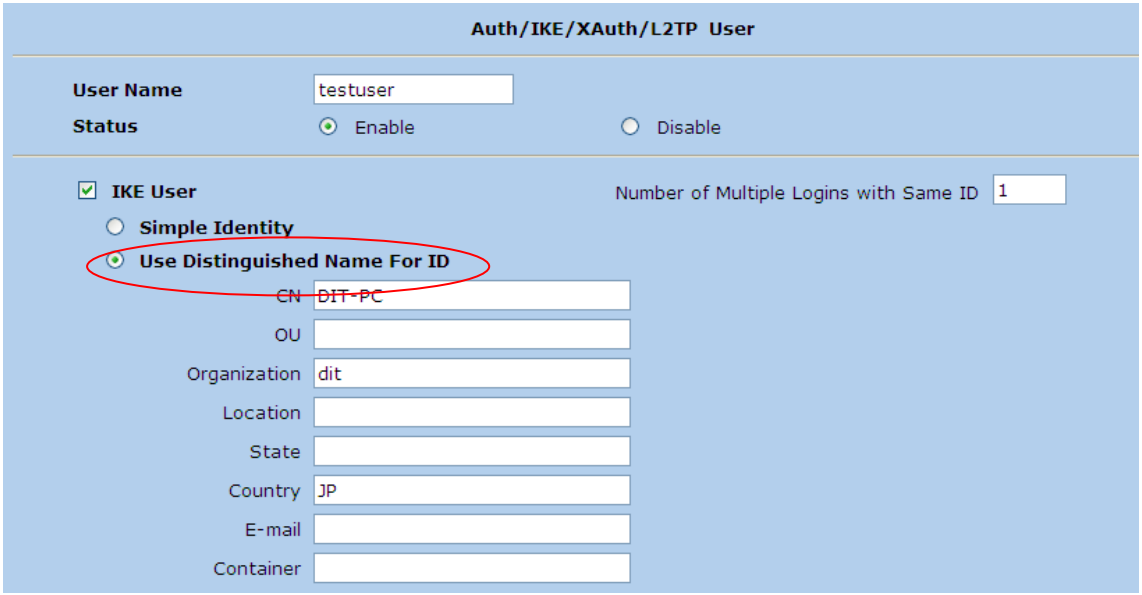
・VPNs -> AutoKey Advanced -> Gateway から該当するフェーズ 1 設定を Edit で開き、Advanced 項目から下記の証明書を指定する箇所で SSG 自身の証明書と CA 証明書を指定します。



また、セキュリティレベルにて暗号の設定は rsa-か dsa-で始まるものを選択します。

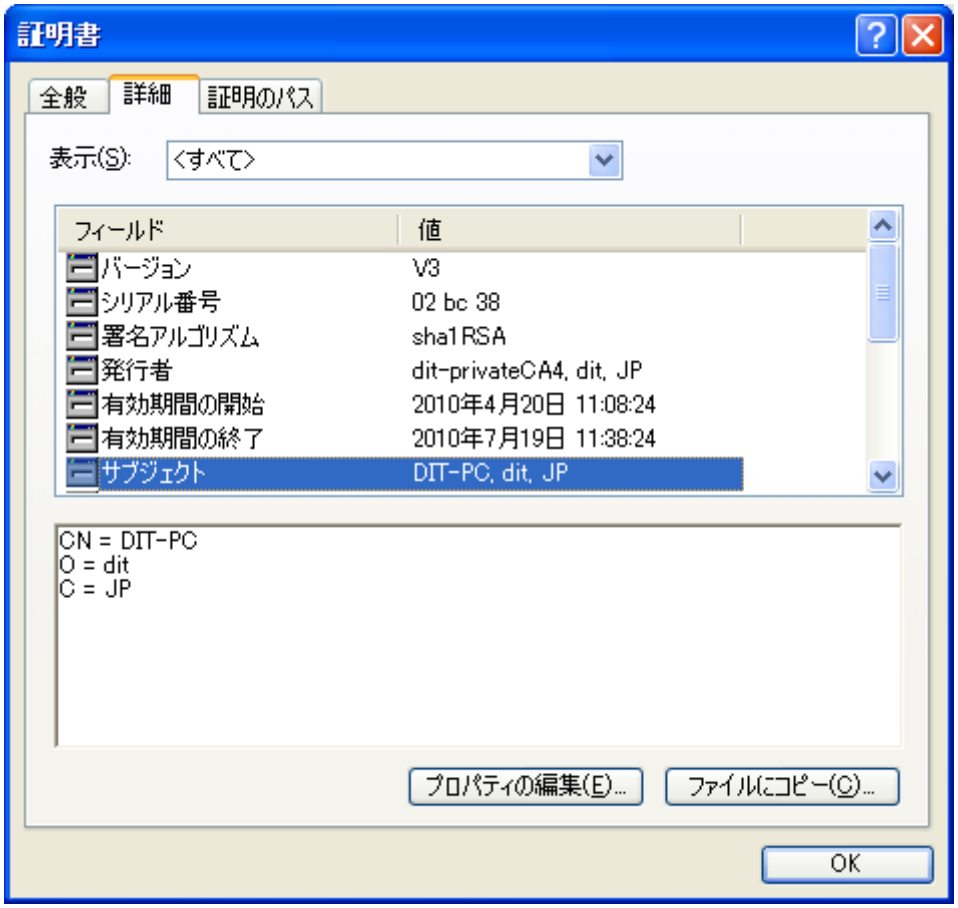


さらに、Objects -> Users からクライアント証明書とユーザを結び付ける設定を行います。
Local Groups から該当するユーザを一旦外した後で、ユーザを Edit で選択します。



ここで入力を行うのはクライアントの証明書の内容です。

参考：Internet Explore で証明書の中身を開いた時



・以上の設定を全て行い、Secure VPN Client から VPN 接続を行うと証明書の内容に基づいて接続が行われます。下記は証明書ベースで接続した場合の SSG のログになります。

Date / Time	Level	Description
2010-05-28 15:05:58	info	IKE 10.0.0.200 Phase 2 msg ID 7672a24c: Completed negotiations with SPI 5b6460b3, tunnel ID 32801, and lifetime 3600 seconds/409600 KB.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 2 msg ID 7672a24c: Responded to the peer's first message.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Completed for user testuser.
2010-05-28 15:05:57	notif	PKI: No revocation check, per config, for cert with subject name CN=DIT-PC,O=dit,C=JP,.
2010-05-28 15:05:57	info	IKE<10.0.0.200> Phase 1: IKE responder has detected NAT in front of the remote device.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2010-05-28 15:05:49	notif	All logged events or alarms were cleared by admin netscreen