IISでSSL(https)を設定する方法

IISでセキュアサーバを構築する方法としてOpenSSLを使用した方法を実際の手順に沿って記述します。

１．はじめに
IISでSSL(https)を設定する方法を以下の手順で記述します。

（１）必要ソフトのダウンロード／インストールする
（２）CA局を作る
（３）IISでサーバー証明書を作る
（４）CA局でサーバー証明書へ署名する
（５）サーバー証明書をIISにインストールする
（６）CA証明書をブラウザにインポートする

今回はOpenSSLによりCA局を自作しサーバー証明書に署名しますが、本来はベリサイン等のCA局に署名して頂く事になります。その場合は（１）（２）（４）は不要です。

２．設定手順
（１）必要ソフトのダウンロード／インストールする
①OpenSSLのダウンロードとインストール
今回使用したOpenSSLのファイルは以下の通りです。
Win32OpenSSL_Light-0_9_8g.exe

C:¥OpenSSL にインストールします。

②ActivePerlのダウンロードとインストール
今回使用したＡｃｔｉｖｅＰｅｒｌのファイルは以下の通りです。
APi522e.exe

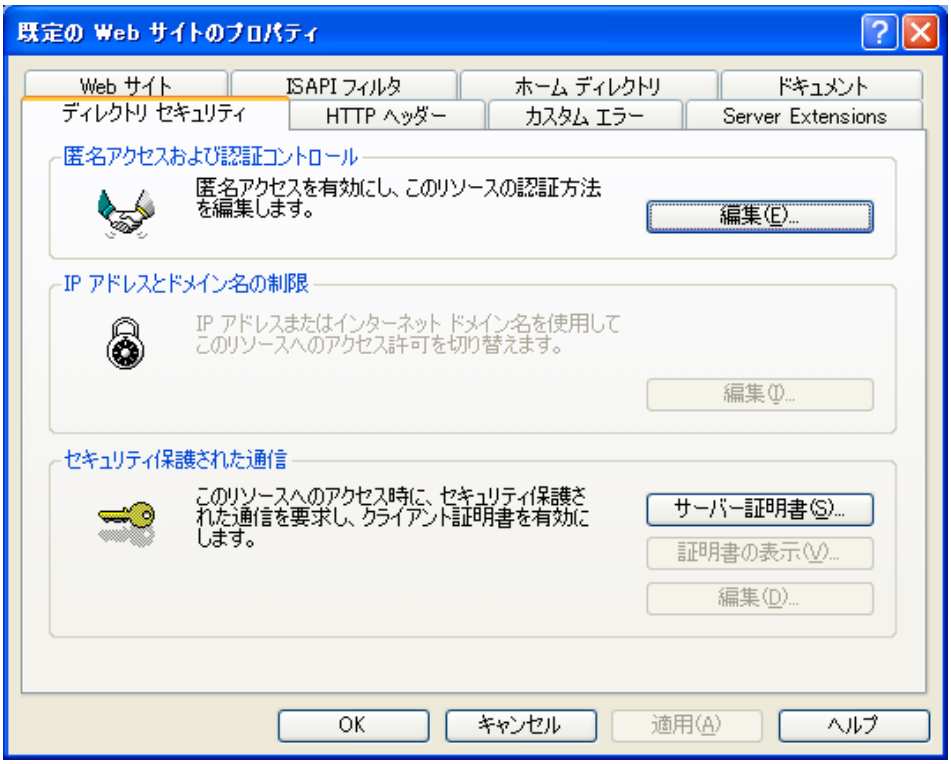
C:¥Perl にインストールします。

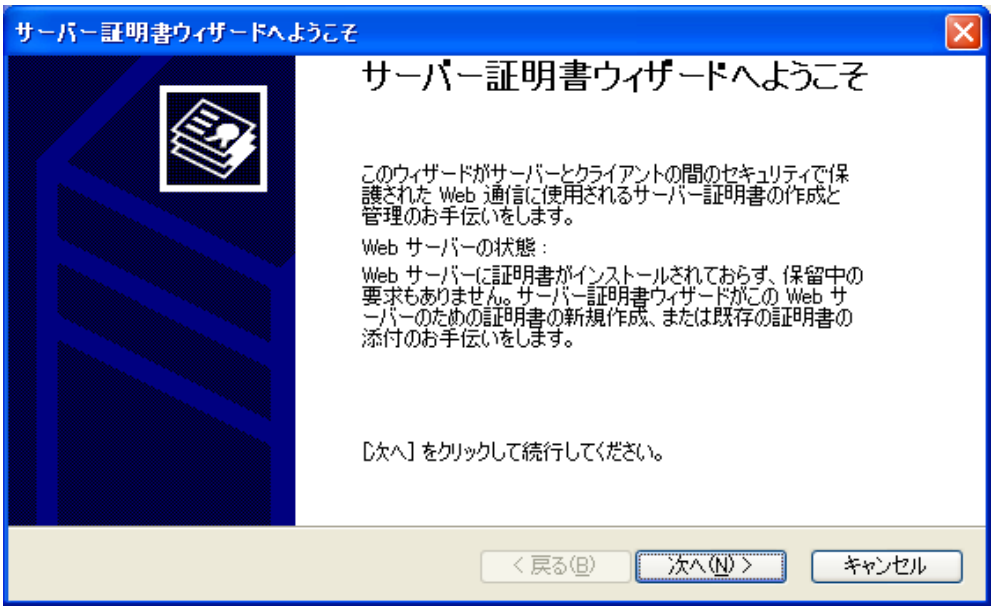
（２）CA局を作る
OpenSSLのCA.plを実行しCA局を作成します。(C:¥OpenSSL¥bin¥demoCAを作成します)
CA.plの実行方法はコマンドプロンプトで以下のコマンドを入力します。

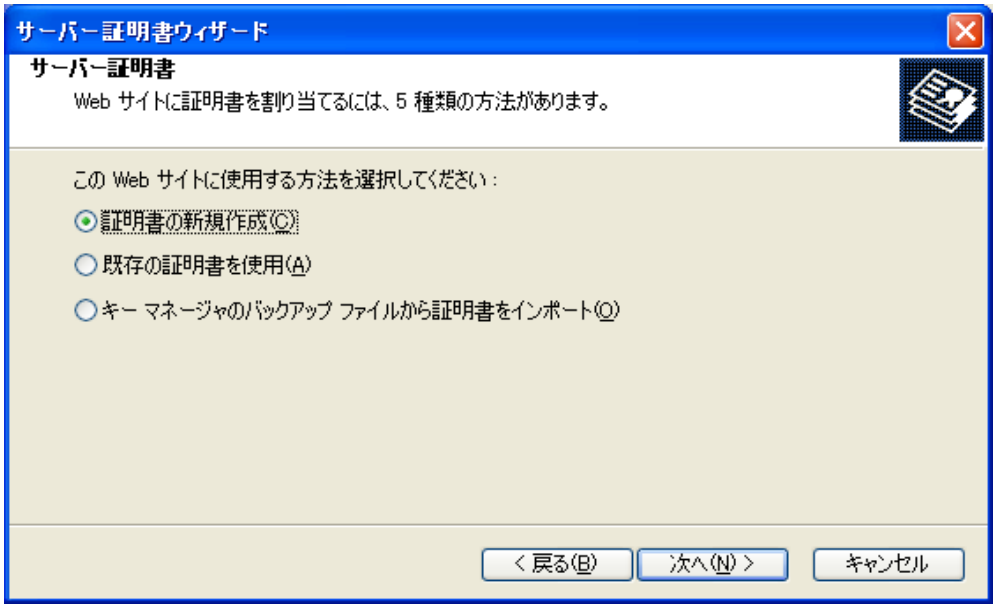
```
>cd C:¥OpenSSL¥bin
>CA.pl -newca
CA certificate filename (or enter to create)
                                                    ←「Enterを入力しました」
Making CA certificate ...
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
....++++++
.....................................................++++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:                              ←「pempassを入力しました」
Verifying - Enter PEM pass phrase:                  ←「pempassを入力しました」
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:OKINAWA
Locality Name (eg, city) []:NAHA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NONSOFT
Organizational Unit Name (eg, section) []:CA
Common Name (eg, YOUR name) []:NONCA
Email Address []:nonca@nonsoft.com
```

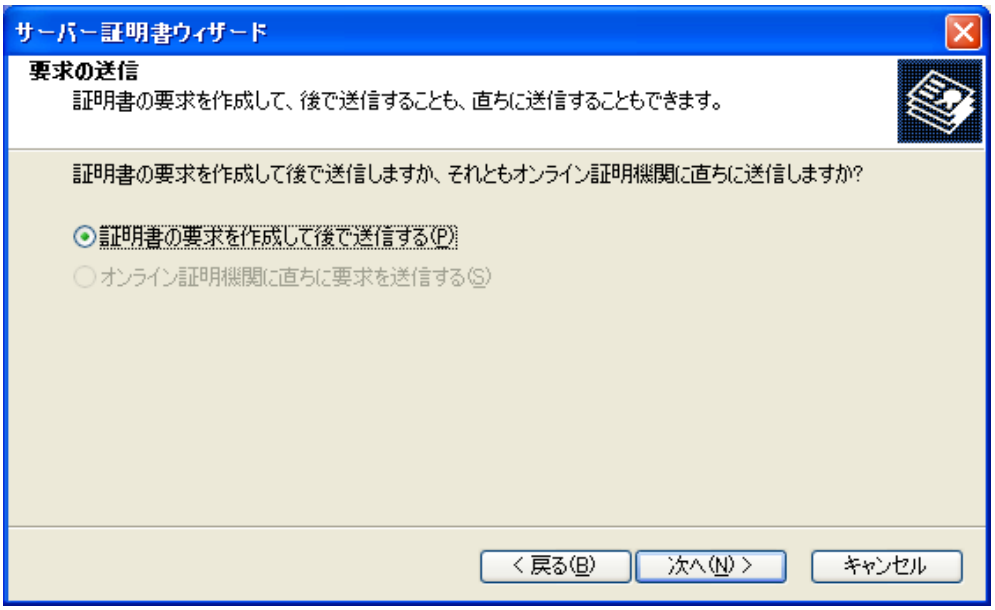
```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:                                ←「Enterを入力しました」
An optional company name []:                            ←「Enterを入力しました」
Using configuration from C:¥OpenSSL¥bin¥openssl.cnf
Loading 'screen' into random state - done
Enter pass phrase for ./demoCA/private/cakey.pem:       ←「pempassを入力しました」
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            9e:eb:c9:43:a0:5e:dc:cc
        Validity
            Not Before: Mar 26 01:18:11 2008 GMT
            Not After : Mar 26 01:18:11 2011 GMT
        Subject:
            countryName               = JP
            stateOrProvinceName       = OKINAWA
            organizationName          = NONSOFT
            organizationalUnitName    = CA
            commonName                = NONCA
            emailAddress              = nonca@nonsoft.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                02:BB:99:4F:61:09:B9:09:D7:5C:3D:F2:F1:68:53:2E:9D:DA:E0:B7
            X509v3 Authority Key Identifier:
                keyid:02:BB:99:4F:61:09:B9:09:D7:5C:3D:F2:F1:68:53:2E:9D:DA:E0:B7
                DirName:/C=JP/ST=OKINAWA/O=NONSOFT/OU=CA/CN=NONCA/emailAddress=nonca@nonsoft.com
                serial:9E:EB:C9:43:A0:5E:DC:CC

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Mar 26 01:18:11 2011 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
```

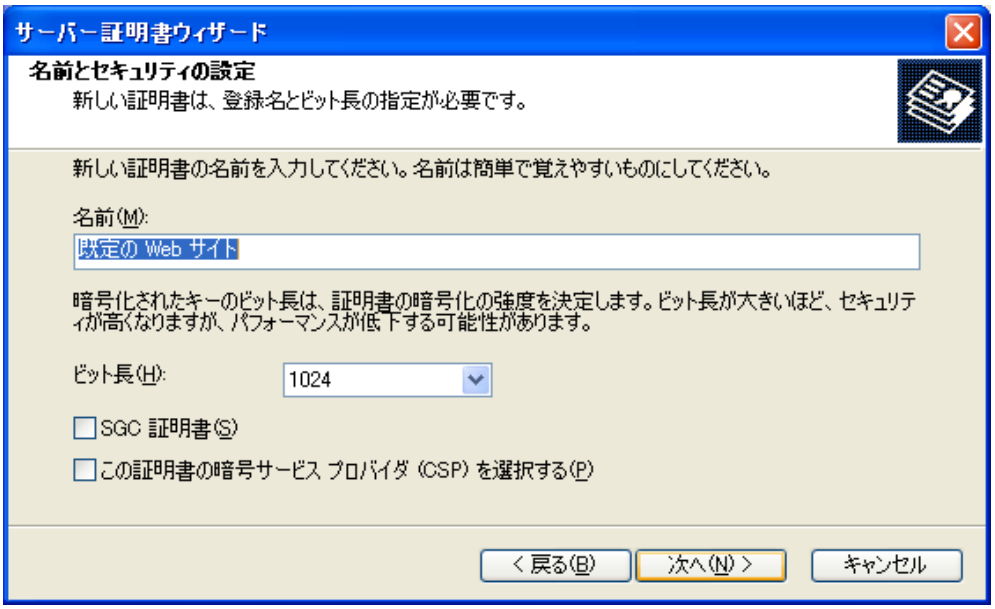
（３）IISでサーバー証明書を作る
IISの「既定のWebサイト」のプロパティで「ディレクトリ セキュリティ」タブを選択し、
サーバー証明書を作成します。(C:¥OpenSSL¥bin¥server¥certreq.txtを作成します)
以下に画面入力の流れの例を示します。

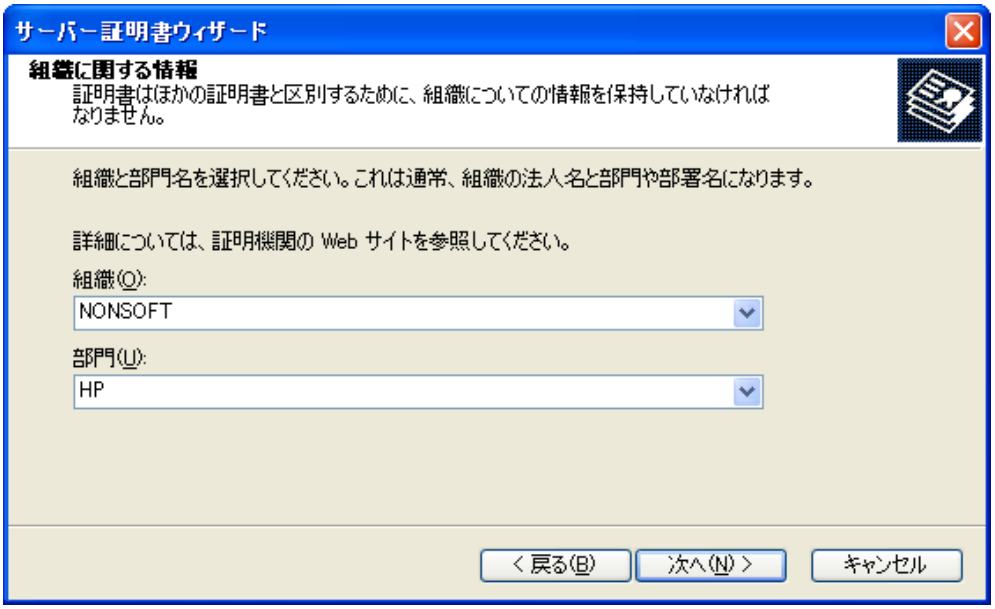


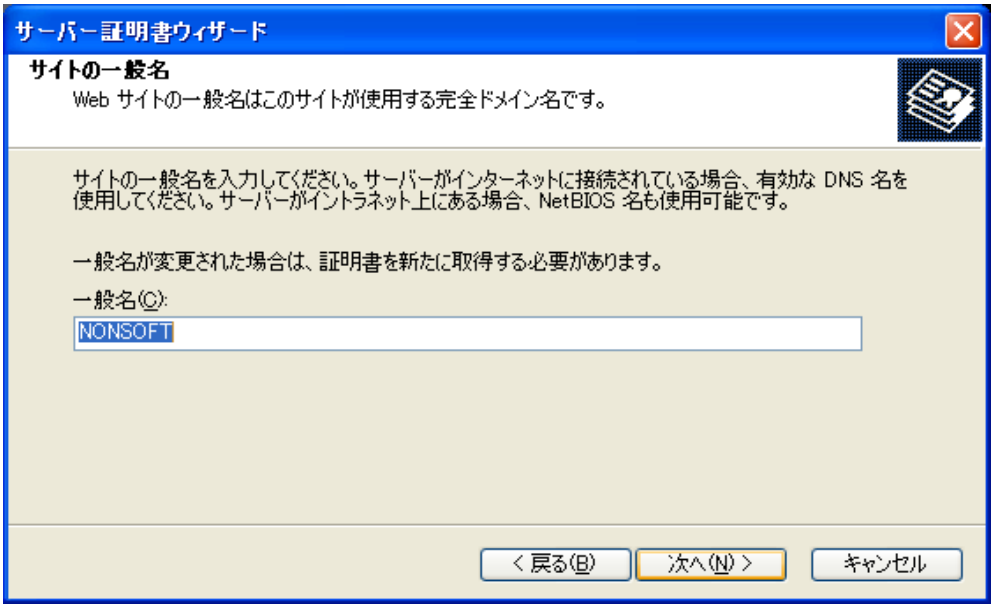


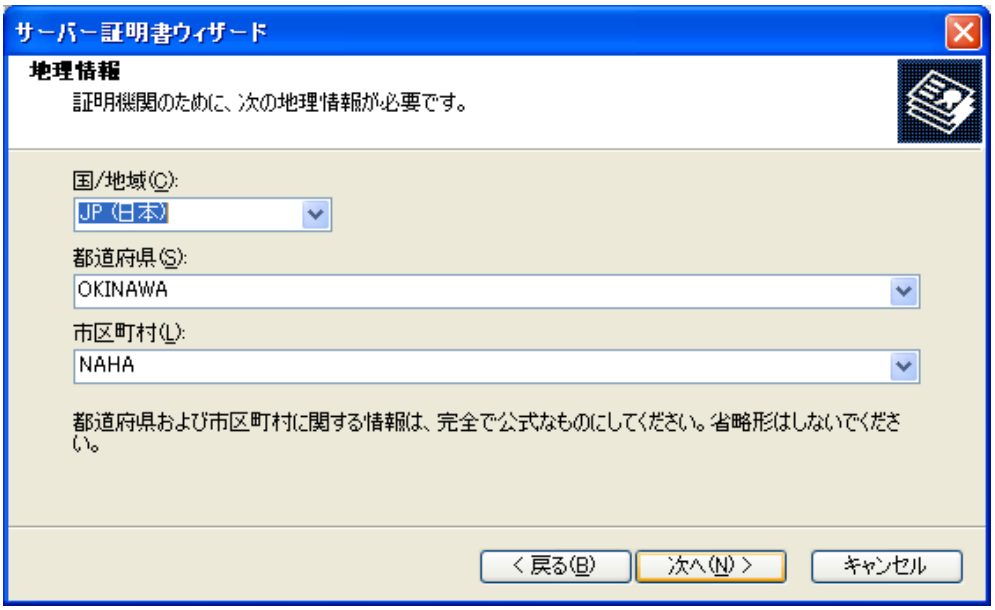

サーバー証明書ウィザード
サーバー証明書
Web サイトに証明書を割り当てるには、5 種類の方法があります。
この Web サイトに使用する方法を選択してください:
証明書の新規作成(C)
既存の証明書を使用(A)
キー マネージャのバックアップ ファイルから証明書をインポート(O)
< 戻る(B)
次へ(N) >
キャンセル

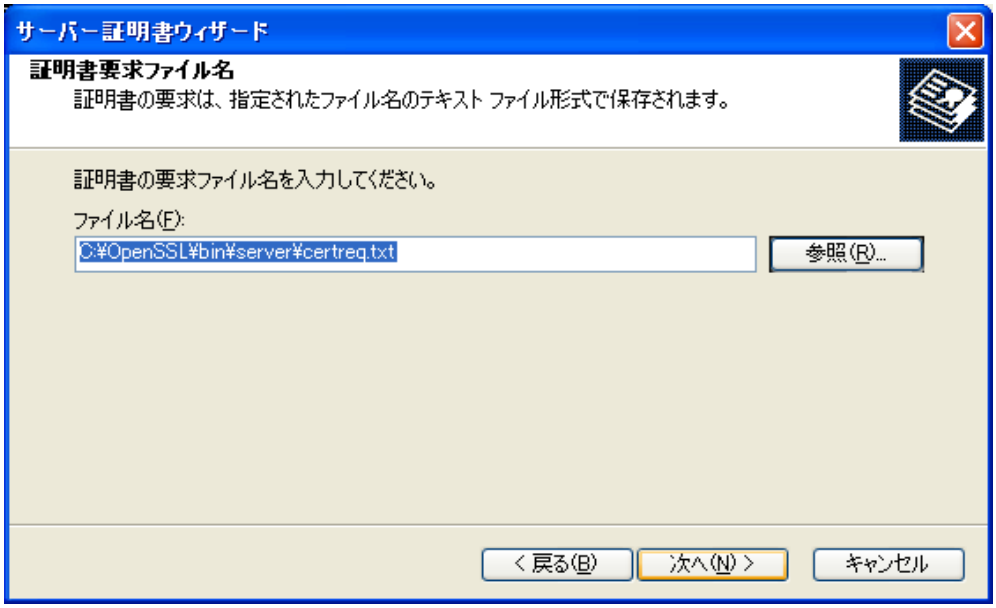

サーバー証明書ウィザード
要求の送信
証明書の要求を作成して、後で送信することも、直ちに送信することもできます。
証明書の要求を作成して後で送信しますか、それともオンライン証明機関に直ちに送信しますか?
証明書の要求を作成して後で送信する(P)
オンライン証明機関に直ちに要求を送信する(S)
< 戻る(B)
次へ(N) >
キャンセル


サーバー証明書ウィザード
名前とセキュリティの設定
新しい証明書は、登録名とビット長の指定が必要です。
新しい証明書の名前を入力してください。名前は簡単で覚えやすいものにしてください。
名前(M):
既定の Web サイト
暗号化されたキーのビット長は、証明書の暗号化の強度を決定します。ビット長が大きいほど、セキュリティが高くなりますが、パフォーマンスが低下する可能性があります。
ビット長(H):
1024
SGC 証明書(S)
この証明書の暗号サービス プロバイダ (CSP) を選択する(P)
< 戻る(B)
次へ(N) >
キャンセル

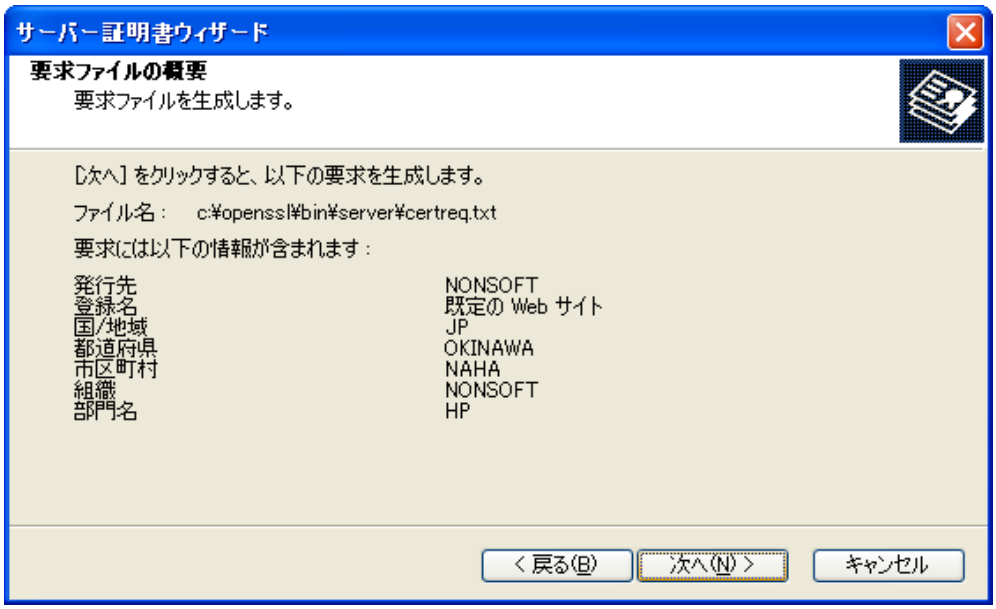

サーバー証明書ウィザード
組織に関する情報
証明書はほかの証明書と区別するために、組織についての情報を保持していなければなりません。
組織と部門名を選択してください。これは通常、組織の法人名と部門や部署名になります。
詳細については、証明機関の Web サイトを参照してください。
組織(O):
NONSOFT
部門(U):
HP
< 戻る(B)
次へ(N) >
キャンセル

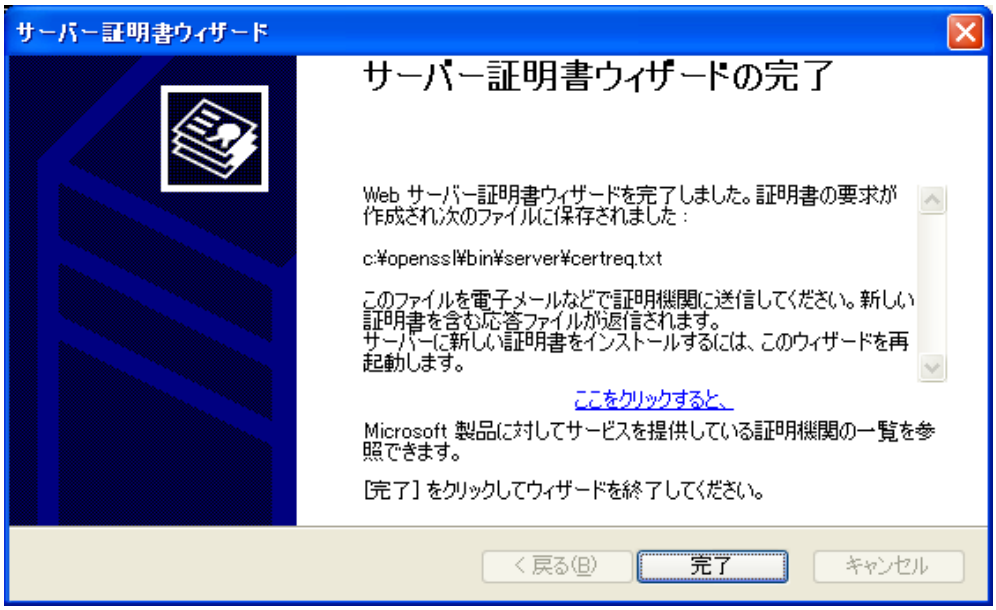

サーバー証明書ウィザード
サイトの一般名
Web サイトの一般名はこのサイトが使用する完全ドメイン名です。
サイトの一般名を入力してください。サーバーがインターネットに接続されている場合、有効な DNS 名を使用してください。サーバーがイントラネット上にある場合、NetBIOS 名も使用可能です。
一般名が変更された場合は、証明書を新たに取得する必要があります。
一般名(C):
NONSOFT
< 戻る(B)
次へ(N) >
キャンセル


サーバー証明書ウィザード
地理情報
証明機関のために、次の地理情報が必要です。
国/地域(C):
JP (日本)
都道府県(S):
OKINAWA
市区町村(L):
NAHA
都道府県および市区町村に関する情報は、完全で公式なものにしてください。省略形はしないでください。
< 戻る(B)
次へ(N) >
キャンセル



ここで「C:¥OpenSSL¥bin¥server¥certreq.txt」を指定します。

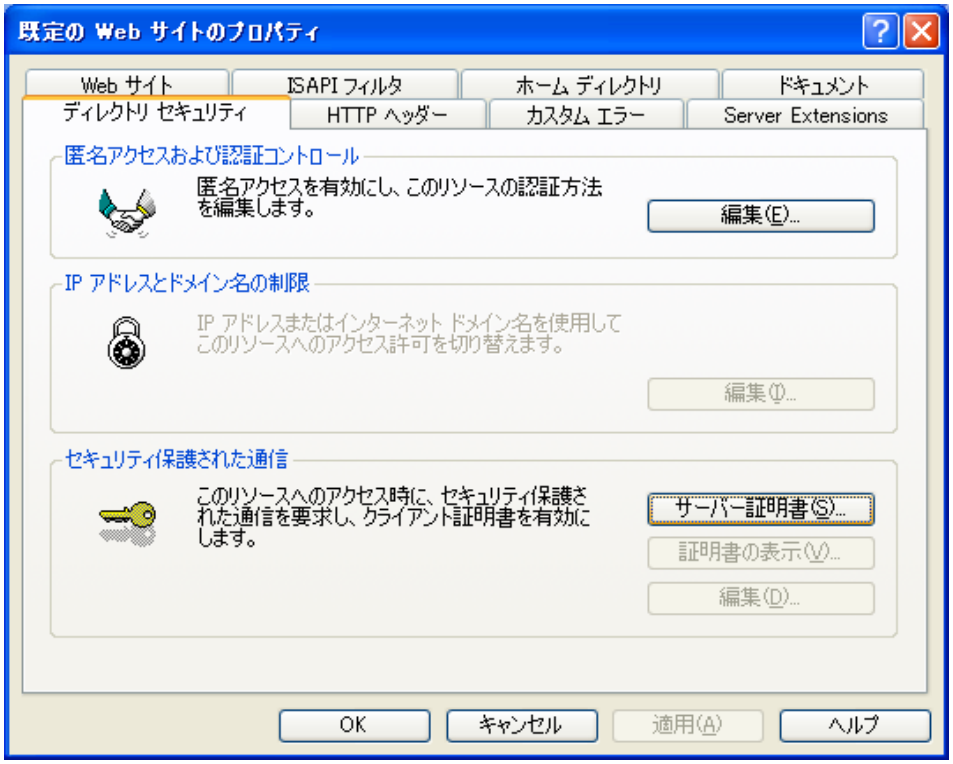


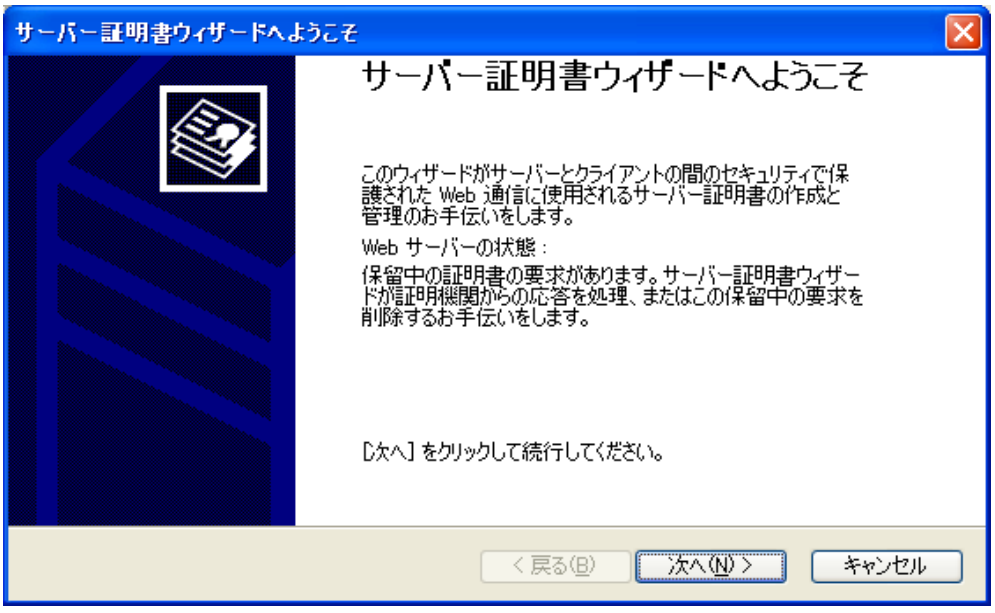


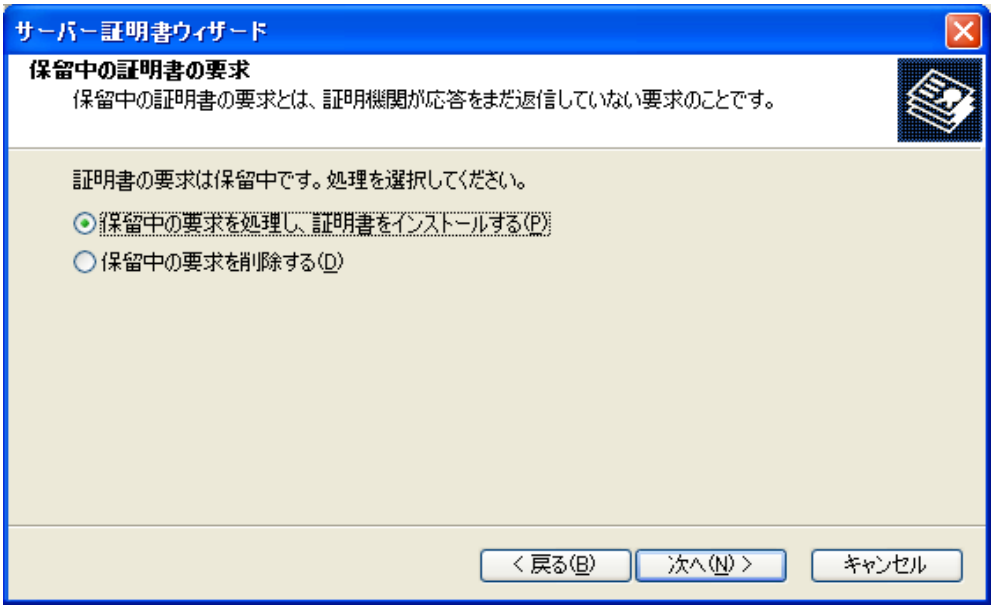
（４）CA局でサーバー証明書へ署名する
OpenSSLを実行しサーバー証明書に署名します。
(C:¥OpenSSL¥bin¥server¥certreq.cerを作成します)
OpenSSLの実行方法はコマンドプロンプトで以下のコマンドを入力します。

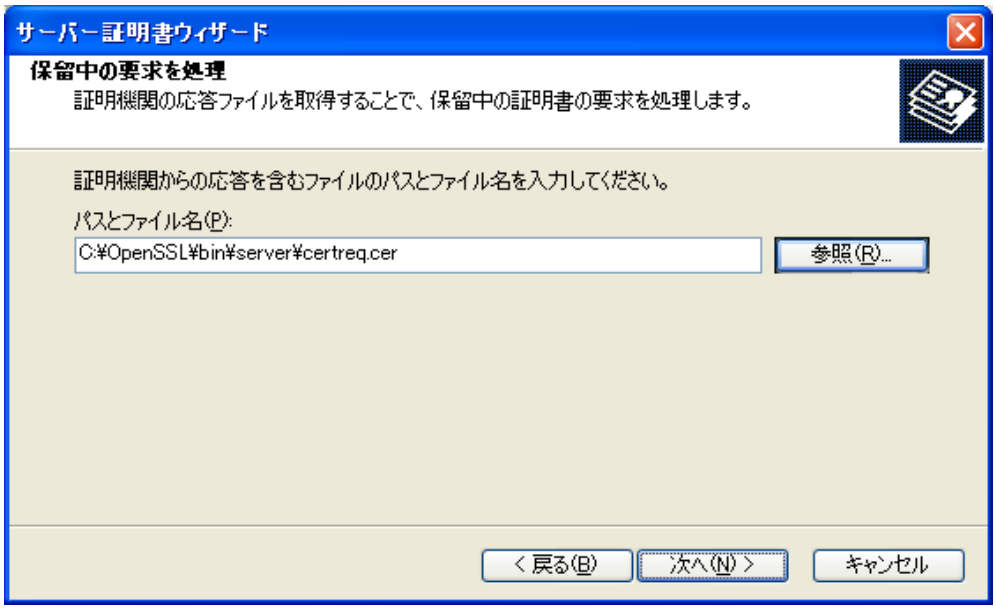
```
>openssl ca -config openssl.cnf -days 365 -out server¥certreq.cer -infiles server¥certreq.txt
Using configuration from openssl.cnf
Loading 'screen' into random state - done
Enter pass phrase for ./demoCA/private/cakey.pem:              ←「pempassを入力しました」
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            9e:eb:c9:43:a0:5e:dc:ce
        Validity
            Not Before: Mar 26 01:22:39 2008 GMT
            Not After : Mar 26 01:22:39 2009 GMT
        Subject:
            countryName               = JP
            stateOrProvinceName       = OKINAWA
            organizationName          = NONSOFT
            organizationalUnitName    = HP
            commonName                = NONSOFT
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                3B:D5:B6:6D:EF:0E:F3:24:63:08:49:7D:BD:DB:C9:A2:44:8E:E6:51
            X509v3 Authority Key Identifier:
                keyid:02:BB:99:4F:61:09:B9:09:D7:5C:3D:F2:F1:68:53:2E:9D:DA:E0:B7

Certificate is to be certified until Mar 26 01:22:39 2009 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

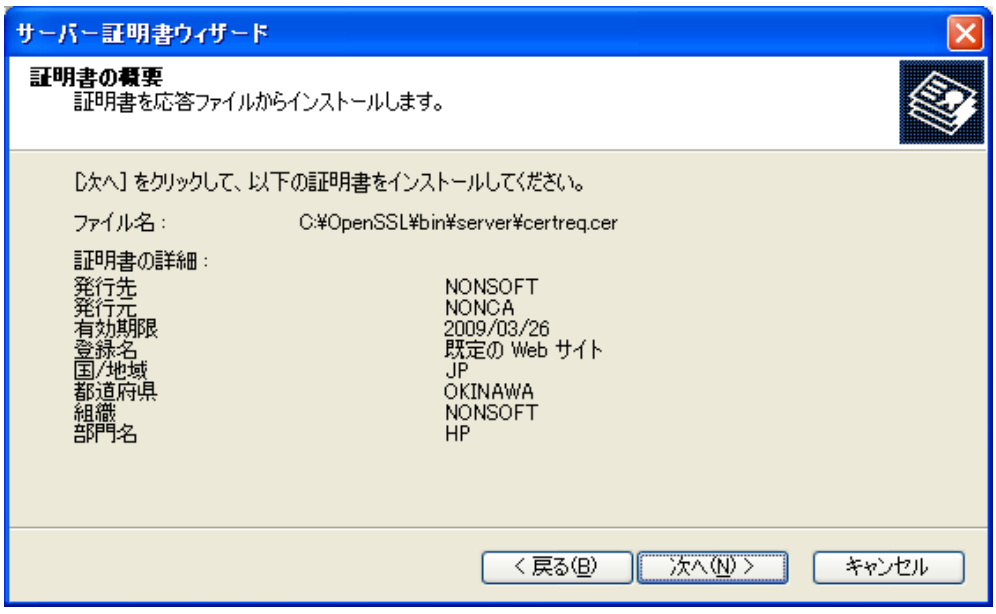
（５）サーバー証明書をIISにインストールする
IISの「既定のWebサイト」のプロパティで「ディレクトリ セキュリティ」タブを選択し、
サーバー証明書をインストールします。以下に画面入力の流れの例を示します。

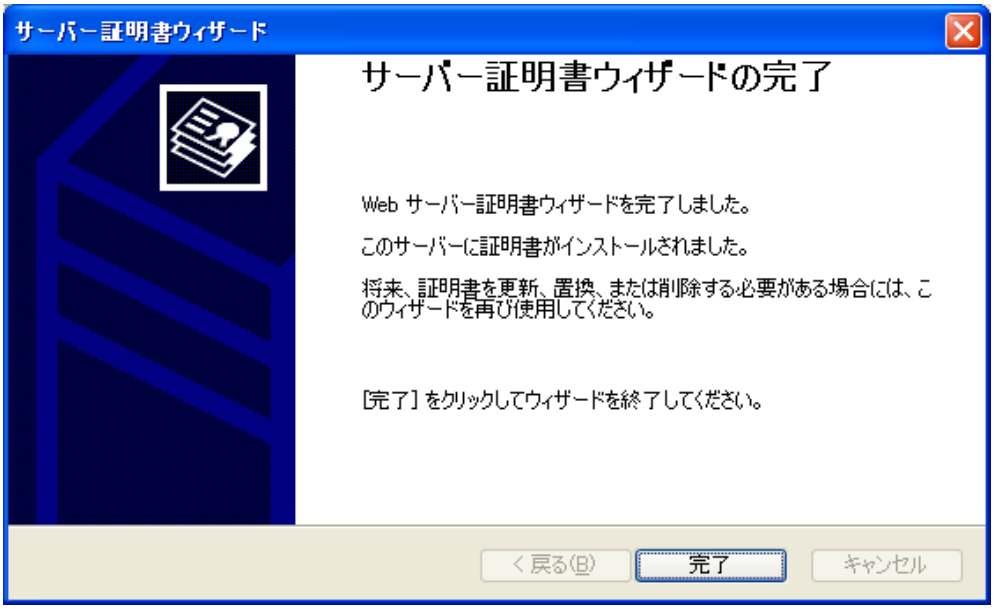




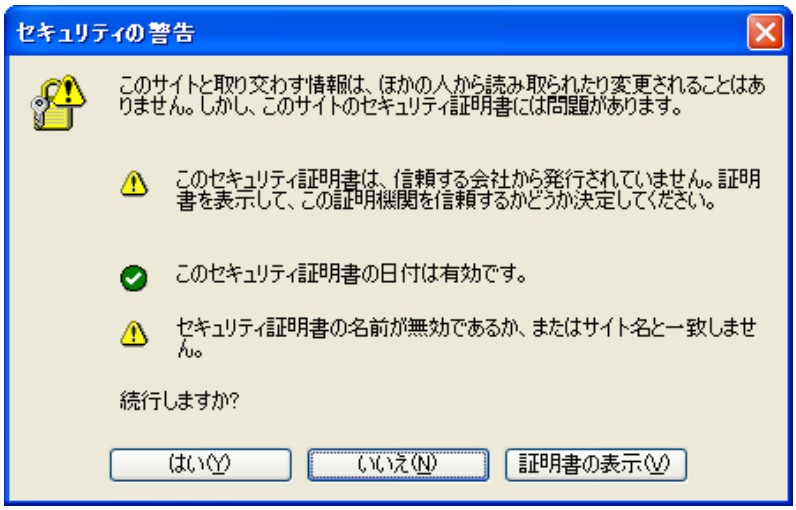

サーバー証明書ウィザード
保留中の証明書の要求
保留中の証明書の要求とは、証明機関が応答をまだ返信していない要求のことです。
証明書の要求は保留中です。処理を選択してください。
保留中の要求を処理し、証明書をインストールする(P)
保留中の要求を削除する(D)
< 戻る(B)
次へ(N) >
キャンセル


サーバー証明書ウィザード
保留中の要求を処理
証明機関の応答ファイルを取得することで、保留中の証明書の要求を処理します。
証明機関からの応答を含むファイルのパスとファイル名を入力してください。
パスとファイル名(P):
C:¥OpenSSL¥bin¥server¥certreq.cer
参照(R)...
< 戻る(B)
次へ(N) >
キャンセル


サーバー証明書ウィザード
証明書の概要
証明書を応答ファイルからインストールします。
[次へ] をクリックして、以下の証明書をインストールしてください。
ファイル名 :
C:¥OpenSSL¥bin¥server¥certreq.cer
証明書の詳細 :
発行先
NONSOFT
発行元
NONCA
有効期限
2009/03/26
登録名
既定の Web サイト
国/地域
JP
都道府県
OKINAWA
組織
NONSOFT
部門名
HP
< 戻る(B)
次へ(N) >
キャンセル

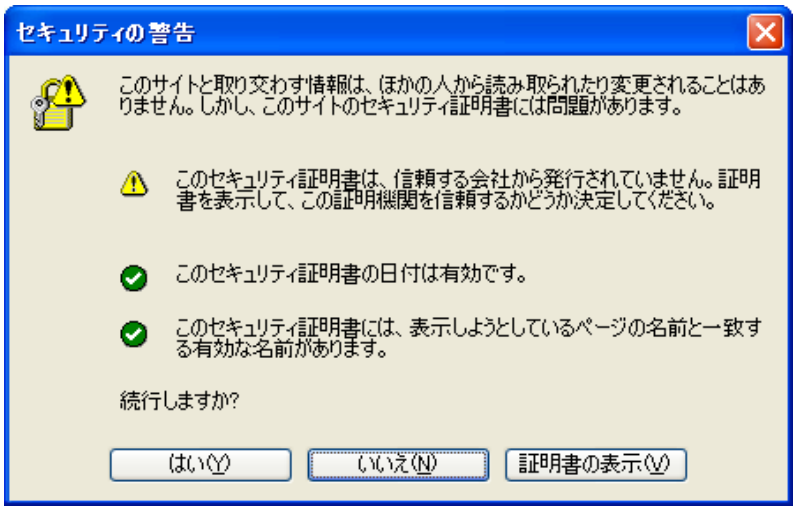

サーバー証明書ウィザード
サーバー証明書ウィザードの完了
Web サーバー証明書ウィザードを完了しました。
このサーバーに証明書がインストールされました。
将来、証明書を更新、置換、または削除する必要がある場合には、このウィザードを再び使用してください。
[完了] をクリックしてウィザードを終了してください。
< 戻る(B)
完了
キャンセル

（６）CA証明書をブラウザにインポートする
ここまでの設定でサーバーに「https://localhost/index.html」でアクセスすると以下のような警告が表示されます。

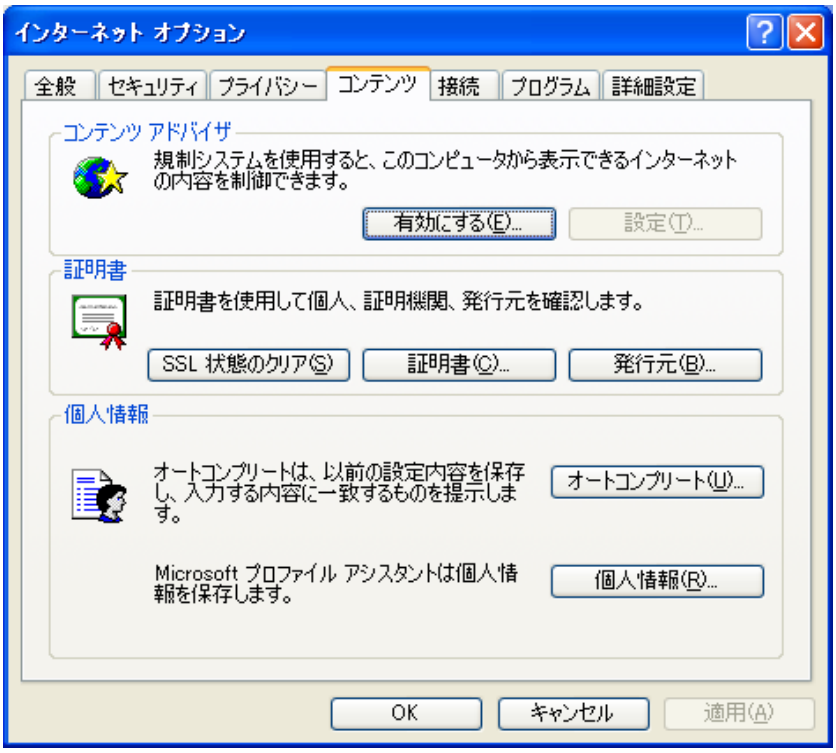


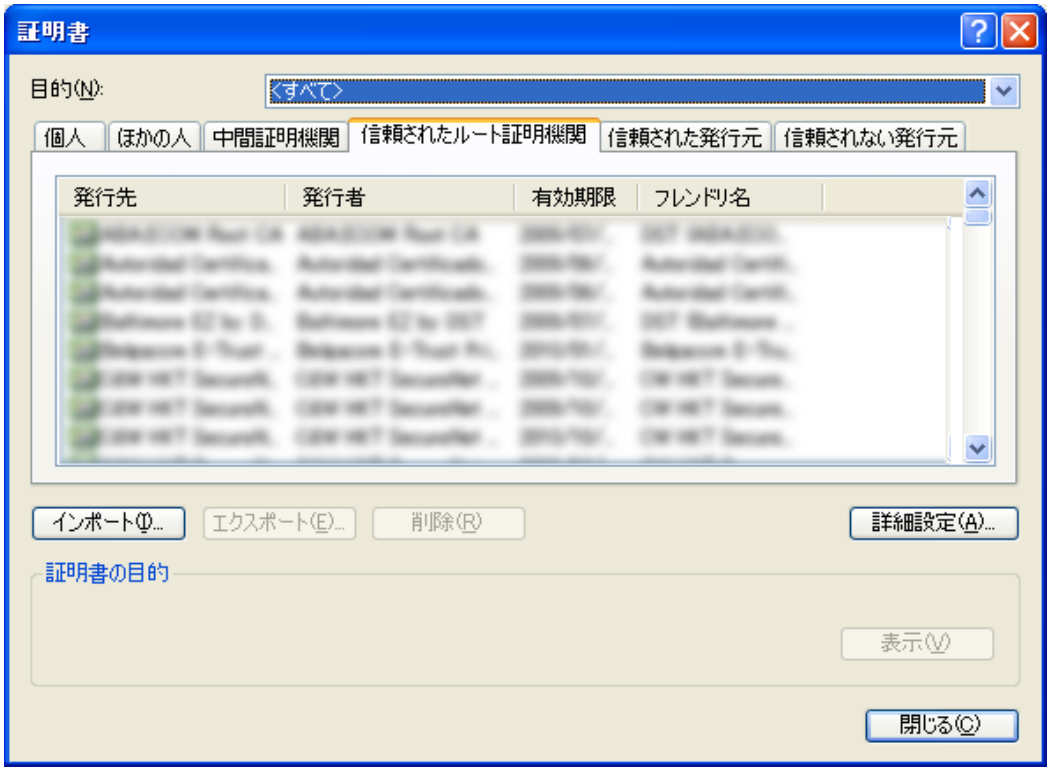
そこで、C:¥WINDOWS¥system32¥drivers¥etc¥hostsに以下を追加します。
　127.0.0.1　　NONSOFT

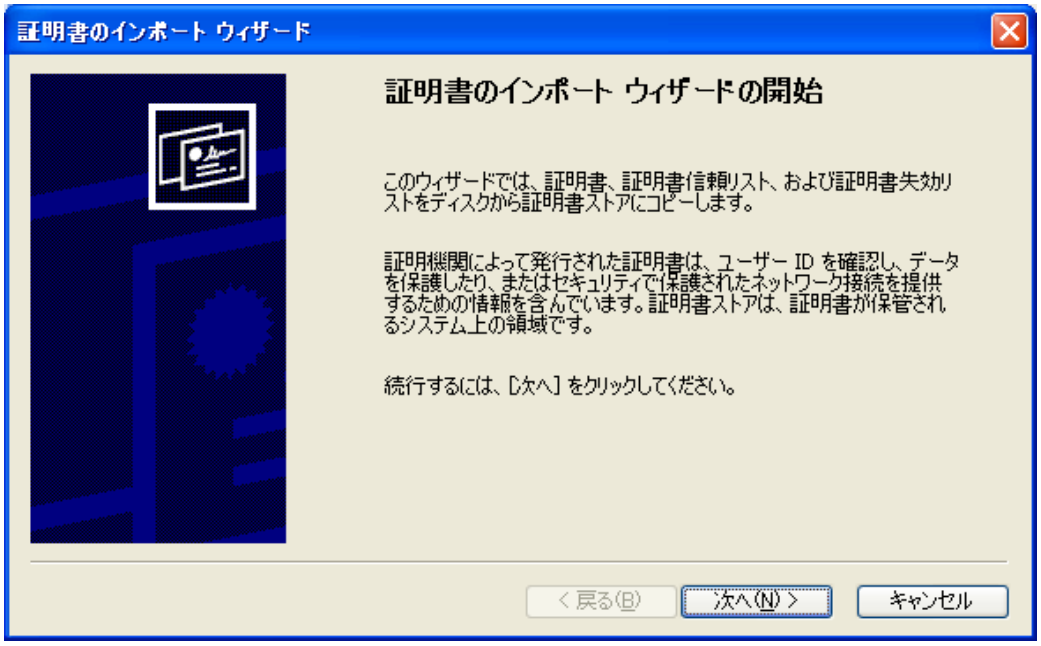
再度、サーバーに「https://NONSOFT/index.html」でアクセスすると以下のような警告が表示されます。（警告がひとつ減りました）

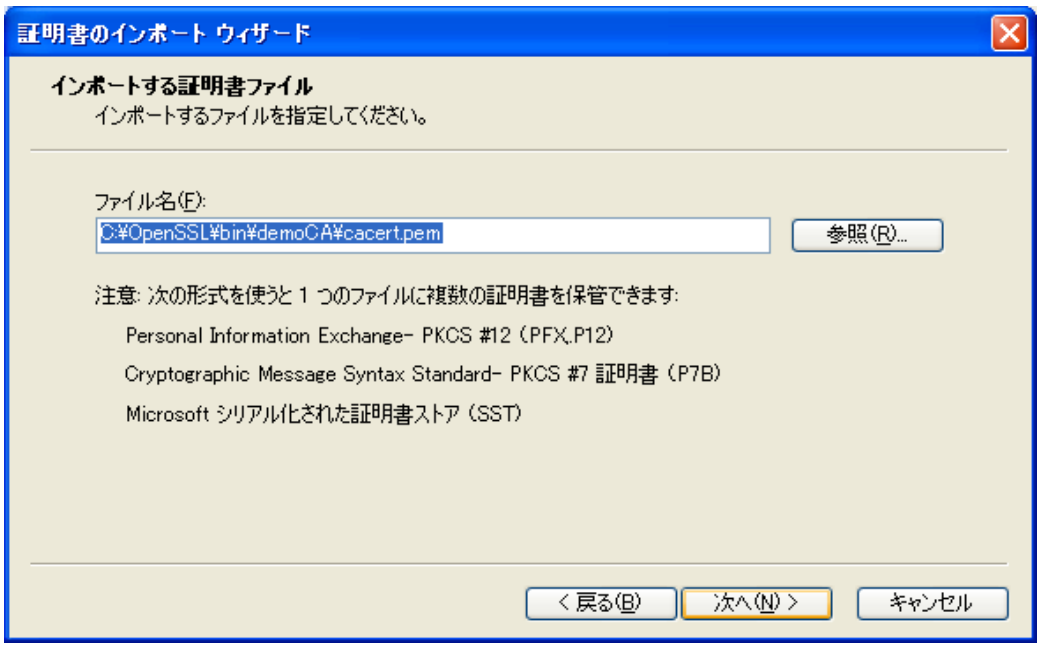


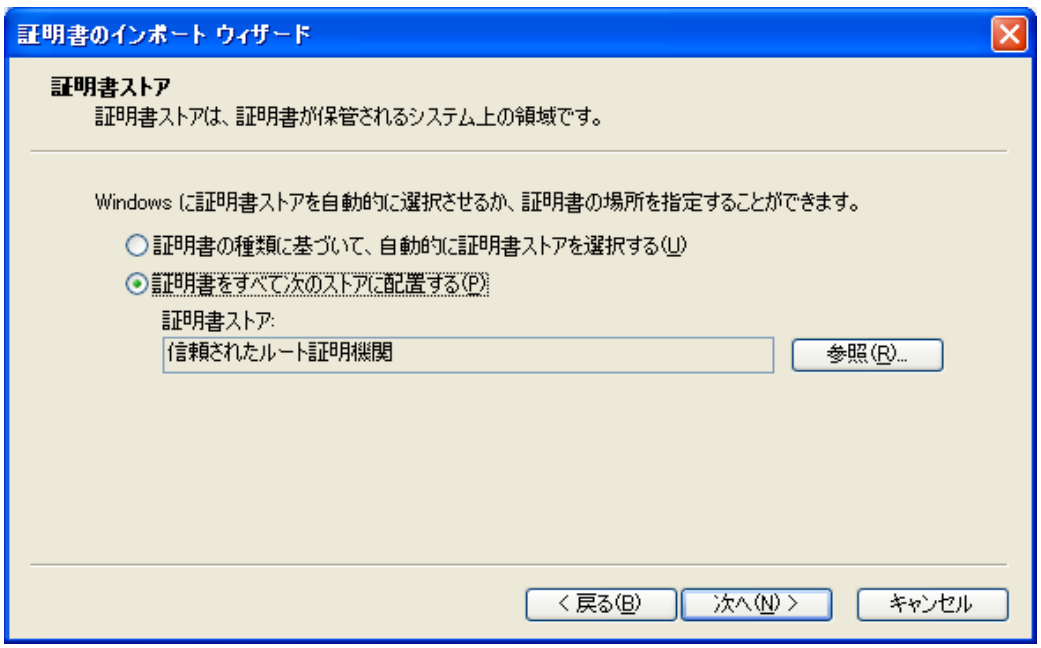
この警告を表示しないようにする為には、CA証明書をブラウザにインポートする必要があります。
（C:¥OpenSSL¥bin¥demoCA¥cacert.pemをブラウザにインストールします）
IEの「ツール」メニューの「インターネット オプション」でCA証明書をインポートします。
以下に画面入力の流れの例を示します。

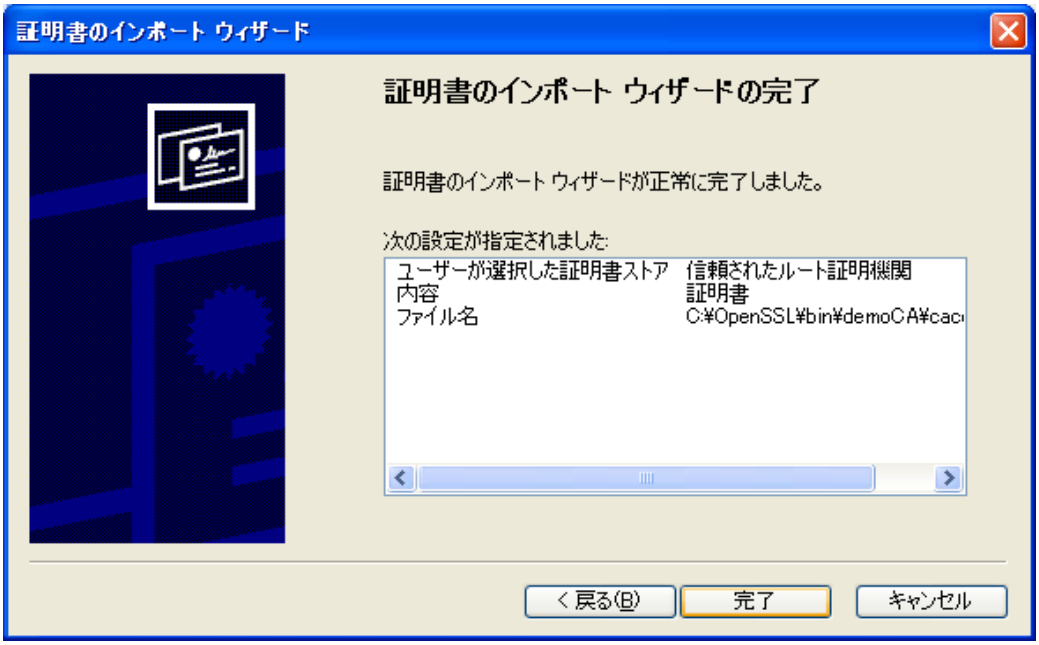


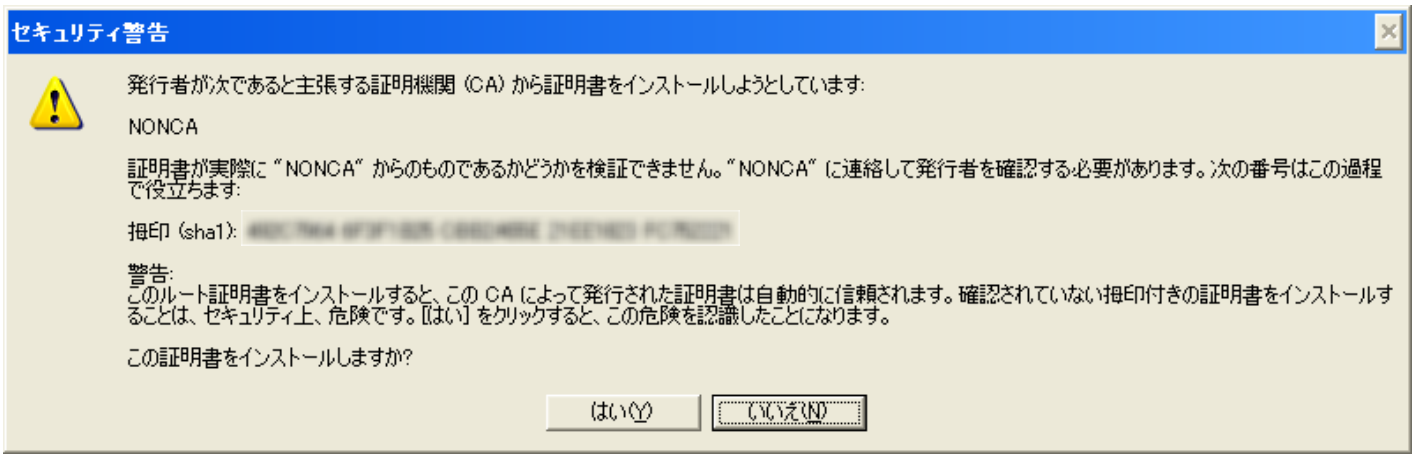


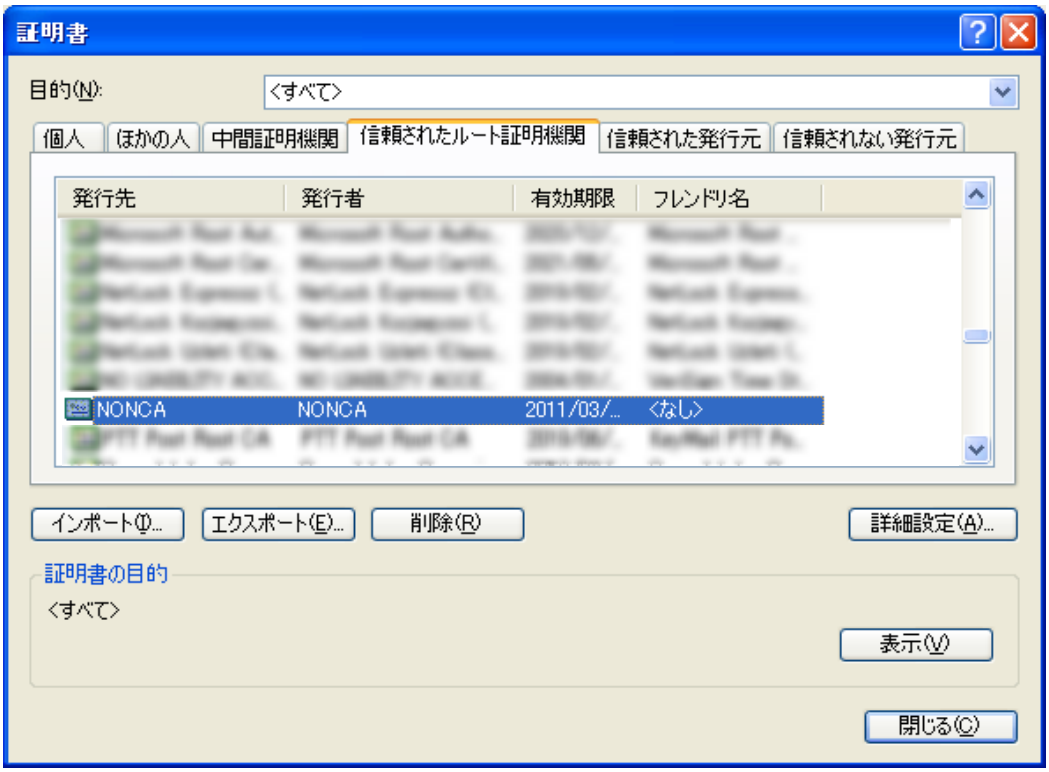

証明書のインポート ウィザード
証明書のインポート ウィザードの開始
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。
続行するには、[次へ] をクリックしてください。
< 戻る(B)
次へ(N) >
キャンセル


証明書のインポート ウィザード
インポートする証明書ファイル
インポートするファイルを指定してください。
ファイル名(F):
C:¥OpenSSL¥bin¥demoCA¥cacert.pem
参照(R)...
注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:
Personal Information Exchange- PKCS #12 (PFX,P12)
Cryptographic Message Syntax Standard- PKCS #7 証明書 (P7B)
Microsoft シリアル化された証明書ストア (SST)
< 戻る(B)
次へ(N) >
キャンセル


証明書のインポート ウィザード
証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。
証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
証明書をすべて次のストアに配置する(P)
証明書ストア:
信頼されたルート証明機関
参照(R)...
< 戻る(B)
次へ(N) >
キャンセル







以上で全ての設定が完了です。サーバーに「https://NONSOFT/index.html」でアクセスすると、
警告無く目的ののページが表示されます。