Ver.1.8

証明書自動発行支援システム

サーバ証明書

インストールマニュアル

IIS6.0 編

2012/3/30

国立情報学研究所

改版履歴			
版数	日付	内容	担当
V.1.0	2009/5/15	初版	NII
V.1.1	2009/6/25	誤植修正 鍵ペアの作成手続き 2　rand1.txt→randfile1.txt rand2.txt→randfile2.txt rand3.txt→randfile3.txt	NII
V.1.2	2009/7/13	旧プロジェクトからの移行に伴う補足の追加 ルート CA 証明書インストール方法の修正 誤植の修正	NII
V.1.3	2009/8/6	誤植の修正	NII
V.1.4	2009/9/11	誤植の修正	NII
V.1.5	2009/10/13	DN 使用可能文字拡張 誤植の修正	NII
V.1.6	2011/2/28	サーバ証明書インストールマニュアルに IIS7.0・IIS7.5 を追加 DN のルール記載変更	NII
V.1.7	2011/6/3	文言を統一	NII
V.1.8	2012/03/30	暗号アルゴリズムのセキュリティ対応に伴いサーバ証明書および CSR の鍵長 1024 ビット記載削除	NII

目次

1.はじめに

証明書自動発行支援システムサーバ証明書インストールマニュアル IIS6.0 編（以下、[本マニュアル]）は、UPKI オープンドメイン証明書自動発行検証プロジェクト（以下、[本プロジェクト]）から発行された証明書を IIS6.0 で使用するための CSR の作成方法、発行したサーバ証明書をインストールする方法について記載します。

1-1.CSR とは

CSR（証明書発行要求：Certificate Signing Request）は証明書を作成するための元となる情報で、その内容には、加入者が管理する SSL/TLS サーバの組織名、Common Name（サーバの FQDN）、公開鍵などの情報が含まれています。NII では、加入者に作成いただいた CSR の内容を元に、証明書を作成します。

CSR の例

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBSTCB9AIBADCBjjELMAkGA1UEBhMCSlAxEDAOBgNVBAcTB0FjYWRlbWUxKjAo
BgNVBAoTIU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEiMCAGA1UE
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
lGu3rQIDAQABoAAwDQYJKoZIhvcNAQEEBQADQQCqpoKhuE6W4GpUhpSAJX51z/ze
BvHWjt2CBnDeyaIVNgr3+zdGKUpvWYG7ORkIss4ST6PDF+RQw+TRdkzl8TUF
-----END CERTIFICATE REQUEST-----
```

1-2.OpenSSL の利用について

証明書を申請する際に必要となる鍵の作成や CSR の生成には OpenSSL を利用することができます。

OpenSSL のインストール方法等は OpenSSL Project（http://www.openssl.org）等のインターネット上のサイトやダウンロードしたファイルに付属しているインストールマニュアルを参照してください。

OpenSSL は最新版を使用することを強く推奨致します。

1-3.他のサーバ証明書インストールマニュアルとの比較について

本マニュアルでは、各サーバで使用する鍵ペア、CSR生成ツールとして、【鍵ペア生成時に利用するツール】に記述したツールを使用して説明します。

また、各サーバへインストールする必要がある証明書を【サーバ証明書インストールに必要となる証明書一覧】に記述します。

【鍵ペア生成時に利用するツール】

○・・・該当する　　－・・・該当しない

	Openssl	JavaKeytool	iKeyman
Apache1.3 系+mod_ssl	○	－	－
Apache2.0 系+mod_ssl	○	－	－
Apache-SSL	○	－	－
Tomcat	－	○	－
IBM HTTP Server	－	－	○
IIS5.0	○	－	－
IIS6.0	○	－	－
IIS7.0	○	－	－
IIS7.5	○	－	－

【サーバ証明書インストールに必要となる証明書一覧】

○・・・該当する　　－・・・該当しない

	ルート CA 証明書	中間CA証明書	サーバ証明書
Apache1.3 系+mod_ssl	－	○	○
Apache2.0 系+mod_ssl	－	○	○
Apache-SSL	－	○	○
Tomcat	○	○	○
IBM HTTP Server	○	○	○
IIS5.0	○	○	○
IIS6.0	－	○	○
IIS7.0	－	○	○
IIS7.5	－	○	○

1-4.本書の範囲

本書では以下の(e、f)の作業について記述をします。

マニュアル名	内容
操作手順書（加入者用）	a. 加入者が実施する本システムへのサーバ証明書発行申請・取得について（2 章に記載） b. 加入者が実施する本システムへのサーバ証明書更新申請・取得について（3 章に記載） c. 加入者が実施する本システムへのサーバ証明書失効申請について（4 章に記載） d. 本システムへの証明書アップロードフォーマットについて(５章に記載)
サーバ証明書インストールマニュアル※1	e. ＣＳＲと鍵ペアの作成方法について f. サーバ証明書のインストール方法について

※1 以下のマニュアルを総称して[サーバ証明書インストールマニュアル]と呼びます。

- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　IBM HTTP Server 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　Tomcat(JavaKeytool)編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache-SSL 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache2.0 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　Apache1.3 系+mod_ssl 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS7.0・IIS7.5 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS6.0 編
- ・証明書自動発行支援システムサーバ証明書インストールマニュアル　IIS5.0 編

2.IIS6.0 によるサーバ証明書の利用

「サーバ証明書発行・導入における啓発・評価研究プロジェクト（以下、旧プロジェクト）」より発行したサーバ証明書を利用しているサーバに、UPKI オープンドメイン証明書自動発行検証プロジェクト（以下、本プロジェクト）から発行された証明書を使用する場合、事前の手続きとして、別冊「**証明書自動発行支援システム旧プロジェクトからの移行補足**」をご確認ください。

2-1.前提条件

IIS6.0 でサーバ証明書を使用する場合の前提条件について記載します。適時、サーバ証明書をインストールする加入者様の環境により、読み替えをお願いします。（本マニュアルでは Windows2003 Server、OpenSSL0.9.8k で CSR を作成し、Windows2003server へインストールする方法での実行例を記載しております）

前提条件
1.　鍵ペア及び CSR を生成する端末に OpenSSL がインストールされていること。
2.　証明書をインストールする端末に IIS6.0 がインストールされていること。

CSR 作成時は既存の鍵ペアは使わずに、必ず新たに CSR 作成用に生成した鍵ペアを利用してください。更新時も同様に、鍵ペアおよび CSR を新たに作成してください。鍵ペアの鍵長は 2048bit にしてください。

2-2.事前準備

鍵ペア・CSR を生成する前に、事前に以下の項目の準備をしてください。

事前準備
1.　乱数生成用ファイルの準備(200KB 程度のファイルであればどんなものでもかまいません) 本マニュアルではファイル名を randfile1.txt、randfile2.txt、randfile3.txt とします。
2.　サーバ鍵ペア用私有鍵パスフレーズ<*PassPhrase*>([2-3-1、2-3-2 で使用])
3.　サーバ DN（※サーバ DN については、本プロジェクト証明書ポリシまたは、下記 DN のルールをご確認ください）

CSR に記述する DN のルールは以下のとおりとなります。

DN のルール			
項目	指定内容の説明と注意	必須	文字数および注意点
Country(C)	本認証局では必ず「JP」と設定してください。 例） C=JP	○	JP 固定
State or Province Name(ST)	本認証局では使用しないでください。	×	
Locality Name(L)	本認証局では必ず「Academe2」と設定してください。 例)C=Academe2	○	Academe2 固定
Organization Name(O)	プロジェクト参加申請時の機関名英語表記を設定してください。この情報は各所属機関の登録担当者にお問い合わせください。 例)O=National Institute of Informatics	○	半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能)
Organizational Unit Name(OU)	証明書を使用する部局等の名前を設定してください。 （この値は省略可能です） （この値は複数設定することが可能です。複数指定する方法につきましては、CSR 作成時ご使用のアプリケーションのマニュアルをご確認ください。） 例)OU=Cyber Science Infrastructure Development Department	△	・半角の英数字 64 文字以内 (記号は「' (),-./:=」と半角スペースのみ使用可能) ・複数 OU を指定する場合は、全体で 64 文字以内
Common Name(CN)	サーバ証明書 URL に表示されるウェブ・サーバの名前を FQDN で設定してください。例えば SSL/TLS を行うサイトが https://www.nii.ac.jp の場合には、「www.nii.ac.jp」となります。FQDN にはプロジェクト参加申請時に登録いただいた対象ドメイン名を含む FQDN のみ、証明書発行が可能となります。 例)www.nii.ac.jp	○	証明書をインストールする対象サーバの FQDN で 64 文字以内 半角英数字、”．“、“-”のみ使用可能。 また、先頭と末尾に“.”と“-”は使用不可
Email	本認証局では使用しないでください。	×	
鍵長			

RSA 2048bit

○・・・必須　×・・・入力不可　△・・・省略可

注意：証明書の更新を行う場合は、先に 2-6 をご確認ください。

2-3.鍵ペアの生成と CSR の作成

2-3-1 鍵ペアの生成

以下に鍵ペアの生成方法を記述します。

鍵ペアの作成

1. 鍵ペアを生成するため、「2-2.事前準備」の手続き 1 で用意したファイル（200 KB 程度）を 3 つ選んでください。この手続きでは、 選択したファイルの名前を「randfile1.txt」、「randfile2.txt」、「randfile3.txt」として表記します。

2. 用意したファイルを、秘密鍵を保存するフォルダに移動してください。

```
c:¥>COPY randfile1.txt c:¥work¥randfile1.txt
c:¥>COPY randfile2.txt c:¥work¥randfile2.txt
c:¥>COPY randfile3.txt c:¥work¥randfile3.txt
```

3. 鍵ペアの作成を始めるため、次のコマンドを入力してください。(お使いのブラウザによっては 2 行以上で表示、印字されるかもしれませんが、実際は 1 行です) 今回のコマンド例では、 2048 bit の RSA 鍵ペアを生成し、[servername.key]という名前のファイルに保存することを示しています。

```
c:¥>cd c:¥work    ←作業フォルダへ移動してください
C:¥work>openssl  genrsa  -des3  -rand  randfile1.txt;randfile2.txt;randfile3.txt  2048  >
servername.key
Generating RSA private key, 2048 bit long modulus
..............................++++++
..............++++++
unable to write 'random state'
e is 65537 (0x10001)
Enter pass phrase: <PassPhrase>                    ←私有鍵パスフレーズ入力
Verifying - Enter pass phrase: <PassPhrase>        ←私有鍵パスフレーズ再入力
```

重要： この鍵ペア用私有鍵パスフレーズは、証明書のインストール時に必要となる重要な情報です。鍵ペア利用期間中は忘れることがないよう、また、情報が他人に漏れることがないよう、安全な方法で管理してください。証明書のインストール後、サーバ停止・起動時にパスフレーズは求められません。

4. 作成した鍵ペアのファイルを保存します。バックアップはフロッピーディスク等に保存し、安全な場所に保存してください。鍵ペアの中の私有鍵を利用すれば、お使いのウェブ・サーバが SSL/TLS で保護して送受信したデータを、解読することができてしまいます。従って保存する鍵ペアファイルへのアクセス権は加入者自身と SSL/TLS サーバのプロセス等必要最小限になるよう設定してください。またバックアップを保存したフロッピーディスク等も加入者のみまたは同じ権限のある方のみ利用できる場所へ保管してください。また、鍵ペア用私有鍵パスフレーズの管理も、確実に行ってください。鍵ペアファイルの紛失、鍵ペア用私有鍵パスフレーズ忘れ等が発生した場合、証明書のインストールが行えなくなります。この場合、新たに証明書を申請しなおしていただくことになりますので、ご注意ください。

2-3-2 CSR の生成

鍵ペアが作成されたことを確認後、CSR を生成します。

CSR の作成

1. 次のコマンドを入力し、CSR の作成を開始してください。パスフレーズの入力が求められますので、[2-3-1 鍵ペアの生成]の手続き 3 で作成した私有鍵のパスフレーズを入力してください。

```
C:¥work>openssl req -new -key servername.key -sha1 -out servername.csr←CSR ファイル名
Enter pass phrase for servername.key: <PassPhrase>  ←私有鍵パスフレーズ入力
```

2. パスフレーズの入力に成功すると DN 情報の問い合わせが行われますので、[2-2. 事前準備]の[DN ルール]に従い、DN 情報を入力してください。

```
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  ←“JP”を入力
State or Province Name (full name) [Some-State]:.  ←[.]ドットを入力
Locality Name (eg, city) []:Academe2 ←“Academe2”を入力
Organization Name (eg, company) [Internet Widgits Pty Ltd]:National Institute of
Informatics  ←組織名を入力
Organizational Unit Name (eg, section) []:Cyber Science Infrastructure Development
Department ←部局名を入力
Common Name (eg, YOUR name) []:www.nii.ac.jp ←サーバ名 FQDN を入力
Email Address []:.  ←[.]ドットを入力
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.  ←[.]ドットを入力
An optional company name []:.  ←[.]ドットを入力
```

3. 要求された情報の入力が完了すると CSR が生成され、-out 引数で指定した名前のファイル（今回の例では、[servername.csr]）に保存されます。[-----BEGIN CERTIFICATE REQUEST-----]から[-----END CERTIFICATE REQUEST-----]で囲まれた部分が CSR となります。なお、このファイルも、バックアップをとって、証明書を受領するまでは別途保管することをお勧めします。

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhDCB7gIBADBFMQswCQYDVQQGEwJKUDEQMA4GA1UEBxMHQWNhZGVtZTEMMAoG
                                        例
UmOE3vq8Ajg=
-----END CERTIFICATE REQUEST-----
```

4. 以下のコマンドを入力することにより、CSR の内容を確認することができます。

```
C:¥work>openssl req -noout -text -in servername.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, L=Academe2, O=National Institute of Informatics, OU=Cyber Science
Infrastructure Development Department, CN=www.nii.ac.jp          ←CSR 生成時に入力した DN
と一致していることを確認してください
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit) ←鍵長が 2048bit であることを確認してください
                Modulus (2048 bit):
                    00:c9:0e:99:5c:8a:4a:e3:b2:e2:0d:3d:60:4d:30:
                                    :
                                   例
                                    :
                    ca:2e:56:f7:66:bd:01:44:ea:f3:ca:d2:f6:e0:5e:
                    6c:57:4b:65:e4:e7:f7:ca:dd
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption←署名アルゴリズムは sha1 であることを確認し
                                                てください

        88:44:e5:27:06:02:ec:85:6c:29:6a:0f:a3:92:87:4e:e2:f1:
                                :
                               例
                                :
        9c:3c:0b:7e:1c:55:3d:c3:b3:7a:3a:36:d1:f6:3a:97:78:1a:
```

2-4.証明書の申請から取得まで

CSR を作成しましたら、登録担当者へ送付する証明書発行申請 TSV ファイルを作成し申請します。発行申請 TSV ファイルの作成方法、申請方法等につきましては、[**証明書自動発行支援システム操作手順書(加入者用)**]をご確認ください。

証明書の発行が完了すると、本システムより以下のメールが送信されます。メール本文に記載された証明書取得 URL にアクセスし、証明書の取得を実施してください。このメールは、電子署名されています。

証明書取得 URL の通知

【件名】

Web サーバ証明書発行受付通知

・・・・・

#以下に証明書の取得先が記述されています。

貴機関の登録担当者経由で発行申請をいただきましたサーバ証明書を配付いたします。

本日から 1 ヶ月以内に以下の証明書取得 URL へアクセスし、サーバ証明書の取得を行ってください。

証明書取得 URL:https://scia.nii.ac.jp/～　**←左記 URL にアクセスし証明書の取得を行ってください。**

・・・・・

2-5.証明書のインストール

本章では IIS6.0 へのサーバ証明書のインストール方法について記述します。

※サーバ証明書発行・導入における啓発・評価研究プロジェクト(以下、旧プロジェクト)より発行したサーバ証明書を利用しているサーバへ導入する場合は、事前に、別冊「証明書自動発行支援システム旧プロジェクトからの移行補足」を読み、設定の変更をお願いします。

2-5-1 事前準備

事前準備として、サーバ証明書、中間 CA 証明書を取得してください。また、ルート CA 証明書がインストールされているか確認を行ってください。

※別冊「証明書自動発行支援システム旧プロジェクトからの移行補足」で、ルート CA 証明書のインストールを終えている場合は、ルート CA 証明書の確認、ルート CA 証明書のインストールは不要となります。

事前準備

1. [2-4.証明書の申請から取得まで]で受領したサーバ証明書を server.cer という名前で任意の場所に保存してください。(本マニュアルではローカルディスクの work ディレクトリ[C:¥work]に保存しています。)

2. 中間 CA 証明書を準備します。以下の中間 CA 証明書の[-----BEGIN CERTIFICATE----- から -----END CERTIFICATE-----]までをコピーして、nii-odca2.cer という名前で保存してください。(次の URL にアクセスすることでリポジトリにアクセスすることが可能です)
   リポジトリ:https://repo1.secomtrust.net/sppca/nii/odca2/

```
-----BEGIN CERTIFICATE-----
MIIEVDCCAzygAwIBAgIEErmwxzANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJK
UDEYMBYGA1UEChMPU0VDTO0gVHJ1c3QubmV0MScwJQYDVQQLEx5TZWN1cmlOeSBD
b21tdW5pY2FOaW9uIFJvb3RDQTEwHhcNMDkwMzI3MDMxMzUxWhcNMTkwMzI3MDMx
MzUxWjB9MQswCQYDVQQGEwJKUDERMA8GA1UEBxMIQWNhZGVtZTIxKjAoBgNVBAoT
IU5hdGlvbmFsIEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczENMAsGA1UECxMEVVBL
STEgMB4GA1UECxMXTklJE9wZW4gRG9tYWluIENBIC0gRzIwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDgFG0JGEjnMbJg14iOOKK4qPNr1gwOIZwJRIdh
4L3cYh6+sKhn/lSvliCcbKFsGas9bj27d9N4dnzhyQaaurVmLFyFYtYdv8feyKcm
SN7UYUM4SoeAeq699OCPTLIQw2aehkPSGHy7ecH1JX6UYw/4OpmFNc+ITIDjqf0+
mwJTRM8CtTwvegL7k5fZYinXXtXnh0aiho91/mqDErWOw+AIpPTCDoQBnq1BJzSJ
h+9eMBqj1BrjcXULOpqBvzVz5lBXgrUq3zmVg3yjTGNErLnBg3xGxRwxgfCSo6vZ
e6MpUePb7YarCGJ99L2ENGdOp53AOm8rXyWOK9WSLdbQ9h4jAgMBAAGjggEHMIIB
AzAdBgNVHQ4EFgQUewoH9xjKjA7W2rxQgGwsRwLRDfswHwYDVR0jBBgwFoAUoHNJ
```

mWjchVtl45soL1efvTO8BOgwEgYDVROTAQH/BAgwBgEB/wIBADAOBgNVHQ8BAf8E
BAMCAQYwSQYDVROfBEIwQDA+oDygOoY4aHROcDovL3JlcG9zaXRvcnkuc2Vjb210
cnVzdC5uZXQvUOMtUm9vdDEvUONSb29OMUNSTC5jcmwwUgYDVROgBEswSTBHBgoq
gwiMmxtkhwUBMDkwNwYIKwYBBQUHAgEWK2h0dHBzOi8vcmVwb3NpdG9yeS5zZWNv
bXRydXNOLm5ldC9TQy1Sb29OMS8wDQYJKoZIhvcNAQEFBQADggEBAKoqogcGLHdD
lkXmNjCkI9kXn9I8zHNn7xO3YdMYkgsIkYSAic9+HwWHJPV12/baOxigpGKkY2vc
SEDwAiHqSsVTHrzY6QyERVSaalk+C74+sxjxw1JG5LcH+wgt+ExA4mZPAS7vOfgD
kni+7lP9YrlLR19E6K2AQW6G3Df8zhnkOf2+kl+lavDvT74KrhOFojYZTGF6DFIo
kBFfvNBdrux4CkIsKhpYQXCAIEuy12CFZUXEtHB5XxeBkntbs2lfP/rWbg2J1Ige
zZc6shCn3VdrL2douVFjaAXlc8zwys/KIpLzNSxOOGwJdKxFTaIzH/emcqKj93Jd
DC1rrFMhoPE=
-----END CERTIFICATE-----

3. ルート CA 証明書を確認します。Internet Explorer を立ち上げ、[ツール(T)]→[インターネットオプション(O)]で表示されるインターネットオプション画面より[コンテンツタブ]を選択し、[証明書(C)]ボタンを押して証明書ストアを表示してください。証明書画面で[信頼されたルート証明機関]のタブを選択し、発行先[Security Communication RootCA1]、発行者[Security Communication RootCA1]の証明書がある場合は、ルート CA 証明書の取得は不要となります。無い場合は、以下、「2-5-2 ルート CA 証明書のインストール手続き」に従い、ルート CA 証明書の取得、インストールを実施してください。

2-5-2 ルート CA 証明書のインストール

以下の手続きに従って、ルート CA 証明書のインストールを行ってください。

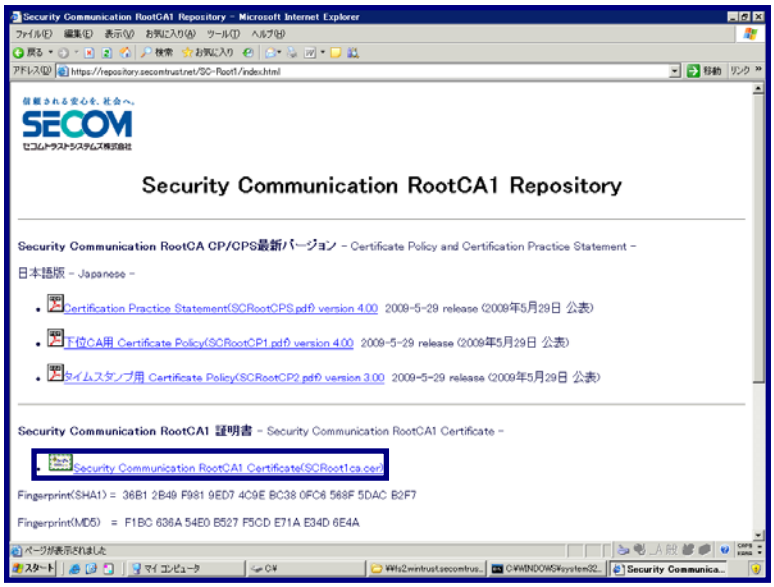
※別冊「証明書自動発行支援システム旧プロジェクトからの移行補足」で、ルート CA 証明書のインストールを終えている場合、また[2-5-1 事前準備]でルート CA 証明書が存在した場合は、本手続きは不要となります。次の「2-5-3 中間 CA 証明書のインストール」へ進んでください。

ルート CA 証明書のインストール

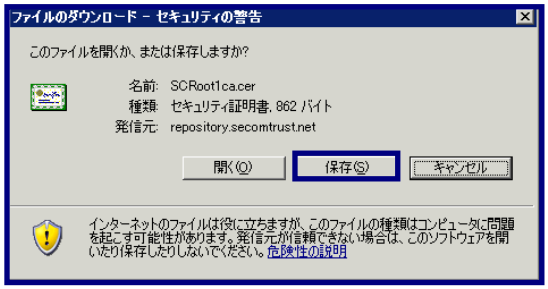
1. InternetExprorerを開始して、次のサイトに接続してください。

   URL：https://repository.secomtrust.net/SC-Root1/index.html

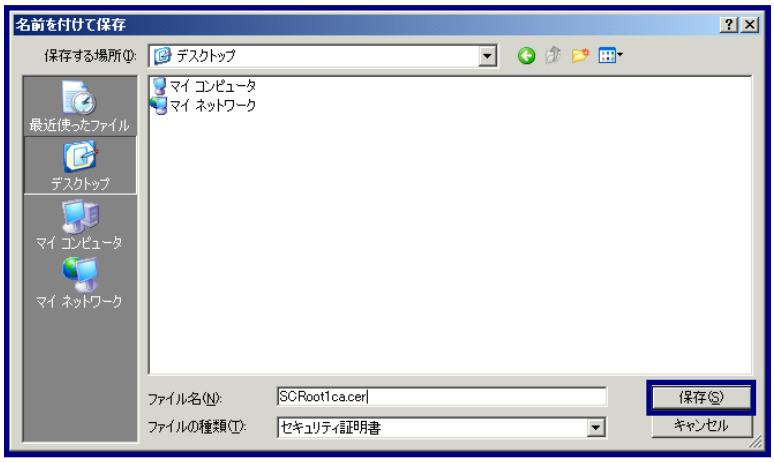
   「Security Communication RootCA1 Certificate(SCRoot1ca.cer)」と記述されたリンクを選択してください。



2. ファイルのダウンロード -セキュリティ警告ウィンドウが表示されますので、[保存(S)]を選択してください。

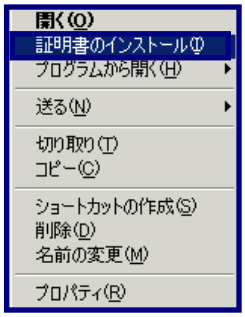


3.　ファイルの保存場所にデスクトップを選択し、保存をしてください。

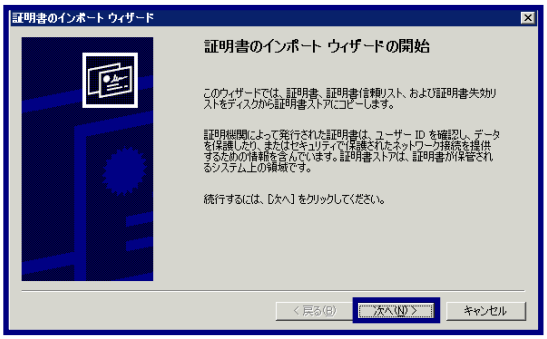


4.　デスクトップに移動し、先ほど保存した証明書を右クリックで選択してください。

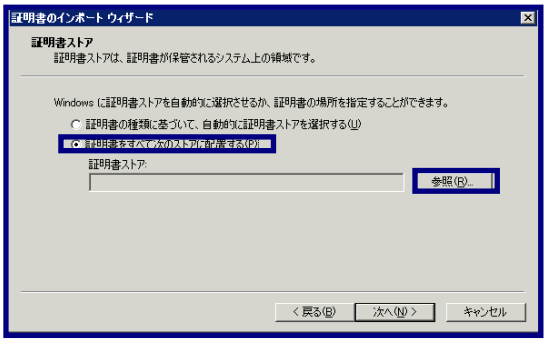
5.　一覧より、[証明書のインストール(I)]を選択してください。



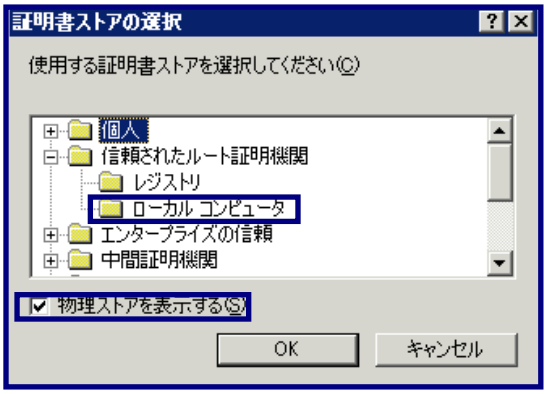
6.　証明書インポートウィザードが開始されますので、[次へ(N)]を選択してください。



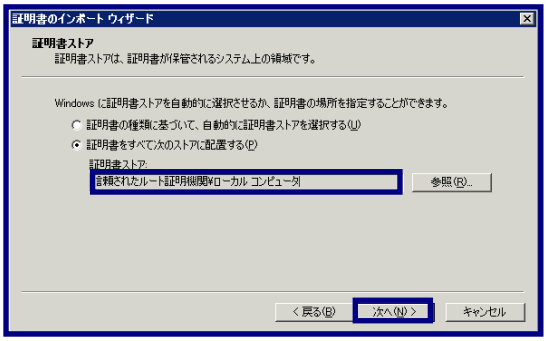
7.　[証明書をすべてのストアに配置する(P)]を選択し、[参照(R)]を選択してください。



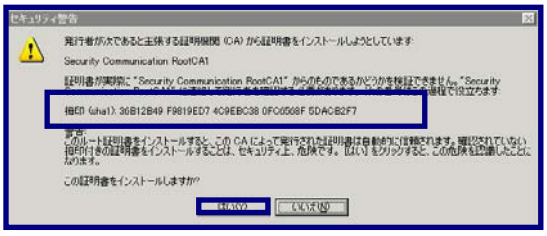
8.　証明書ストアの選択画面で、[物理ストアを表示する(S)]にチェックを入れ、「信頼されたルート証明機関」を選択し、[ローカル　コンピュータ]のフォルダを選択してください。



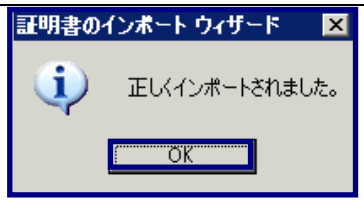
9. 証明書ストアが[信頼されたルート証明機関¥ローカルコンピュータ]であることを確認し、[次へ(N)]を選択してください。



10. セキュリティ警告画面が表示されますので、拇印が「Fingerprint (SHA-1) = 36 b1 2b 49 f9 81 9e d7 4c 9e bc 38 0f c6 56 8f 5d ac b2 f7]であることを確認して、[はい(Y)]を選択してください。

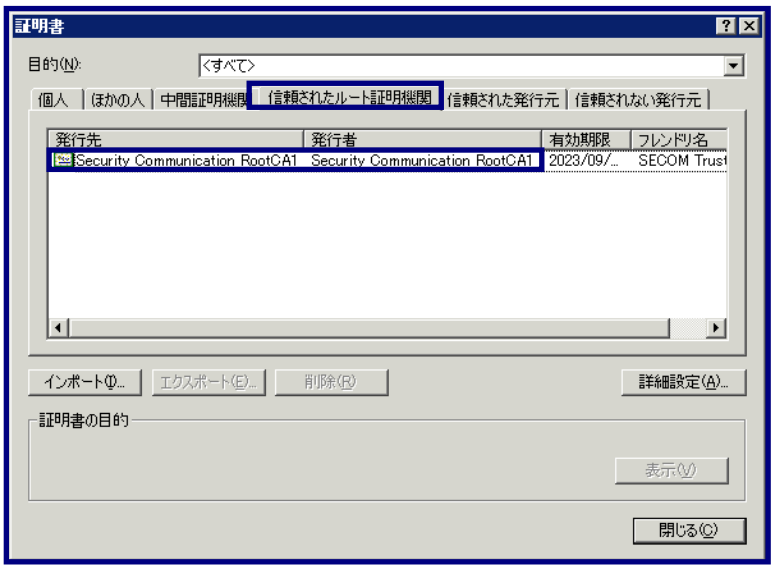


11. [正しくインポートされました]が表示されたら、インストールが終了です。[OK]を選択し、証明書インポートウィザードを終了してください。

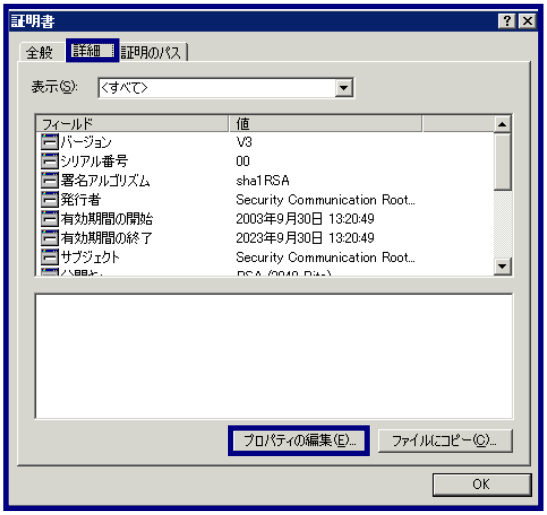


12. インストールされた証明書を確認するために、事前準備と同様の方法で発行先「Security Communication RootCA1」、発行者「Security Communication RootCA1」、「Fingerprint (SHA-1) = 36 b1 2b 49 f9 81 9e d7 4c 9e bc 38 0f c6 56 8f 5d ac b2 f7」であることを確認してください。

13. 上記を確認後、証明書の利用方法の変更を実施します。証明書画面より、当該の証明書を選択しダブルクリックしてください。



14. 証明書詳細画面が表示されますので、[詳細]のタブを選択し、[プロパティの編集(E)]を選択してください。



15. 証明書プロパティ画面で[全般]タブを選択してください。

[次の目的だけを有効にする(O)]のラジオボタンにチェックを入れると、下部の証明書の目的部分のチェックボックスの編集が可能となります。**以下の項目以外のチェックボックスをすべて外してください。**

（ア） サーバー認証

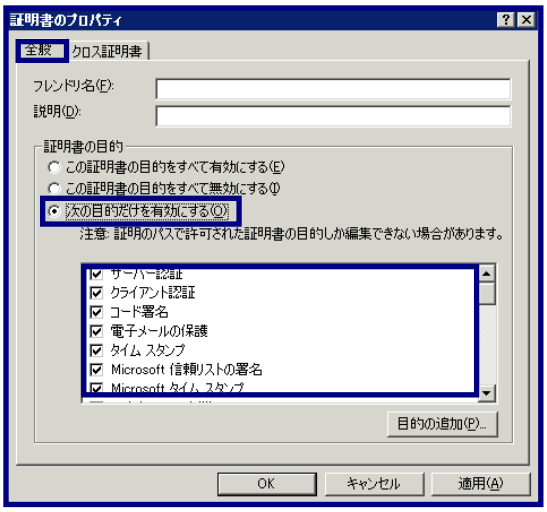
（イ） クライアント認証

（ウ） 電子メールの保護

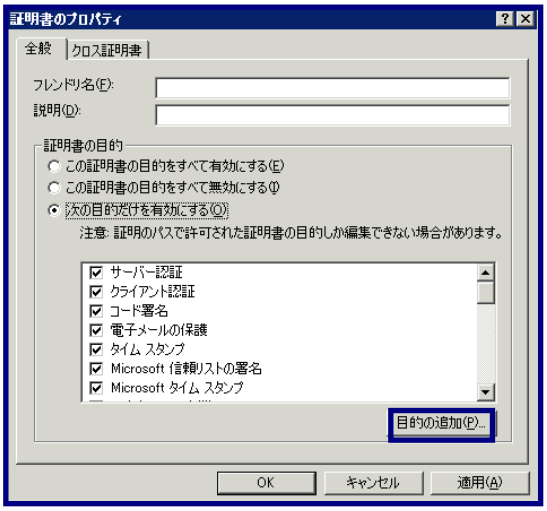
（エ） コード署名

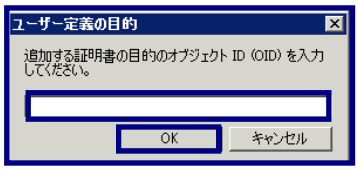
（オ） タイムスタンプ

（カ） 1.3.6.1.5.5.7.3.9



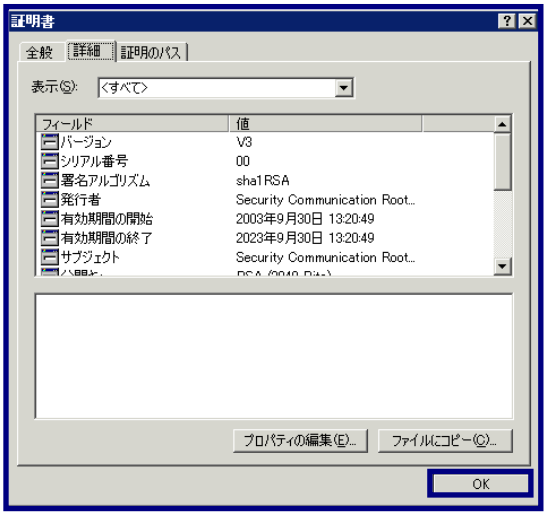
16.（手続き 15　項目(カ)）が利用目的の一覧に表示されていない場合は、[目的の追加(P)]を選択し、[ユーザ定義の目的]画面に「1.3.6.1.5.5.7.3.9」の値を入力し、[OK]を選択してください。





17. 証明書プロパティ画面に戻り[適用(A)]を選択後、[OK]を選択してください。

18. 証明書詳細画面に戻るので、[OK]を選択し、画面を閉じてください。



19. 証明書画面に戻るので、証明書の目的の欄に以下の項目が表示されていることを確認し[閉じる(C)]を選択してください。

(ア) サーバー認証

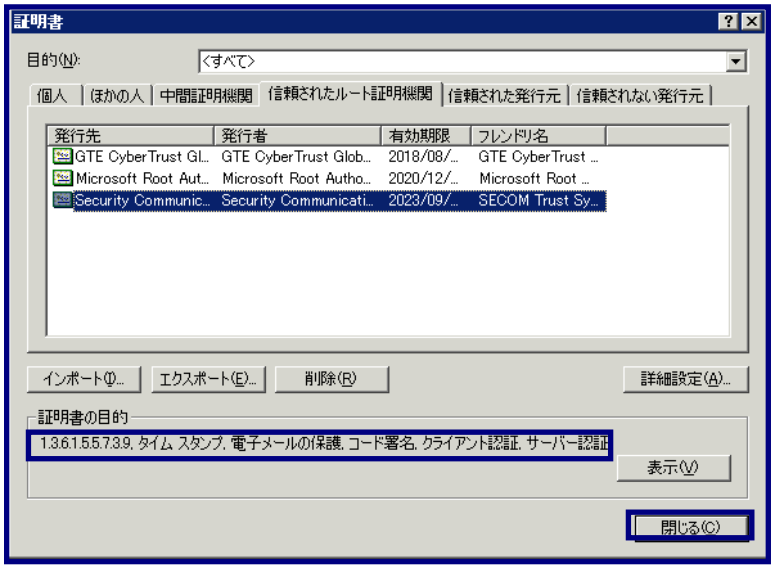
(イ) クライアント認証

(ウ) 電子メールの保護

(エ) コード署名

(オ) タイムスタンプ

（カ） 1.3.6.1.5.5.7.3.9



以上で、ルートCA証明書のインストールは終了となります。

2-5-3 中間 CA 証明書のインストール

以下の手続きに従って、中間 CA 証明書のインストールを行ってください。

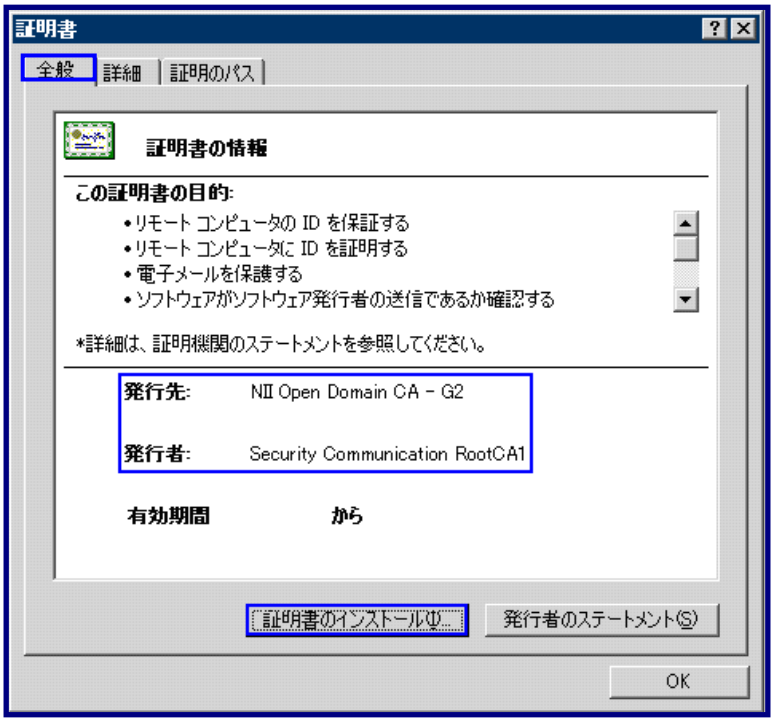
中間 CA 証明書のインストール

1. [2-5-1.事前準備]で取得した中間CA証明書をダブルクリックしてください。

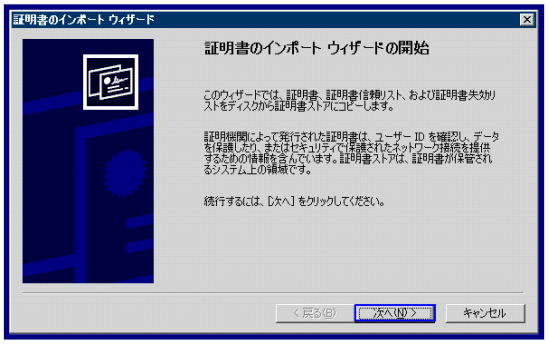
2. [証明書]ダイアログが表示されます。発行先と発行者を確認した後、[全般]タブの[証明書のインストール(I)...]ボタンをクリックします。

   発行先：NII Open Domain CA-G2

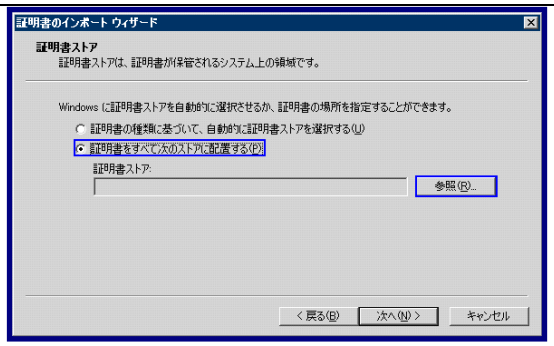
   発行者：Security Communication RootCA1



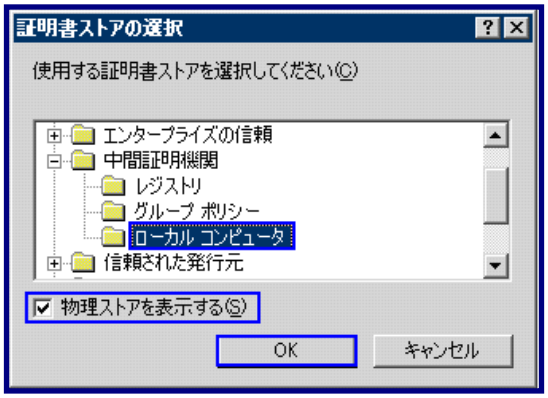
3. [証明書インポートウィザード]が表示されますので、[次へ(N)]ボタンをクリックします。



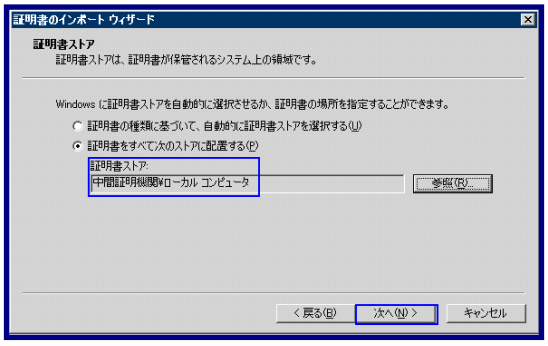
4. [証明書をすべて次のストアに配置する(P)]を択一し、[参照(R)...]ボタンをクリックします。



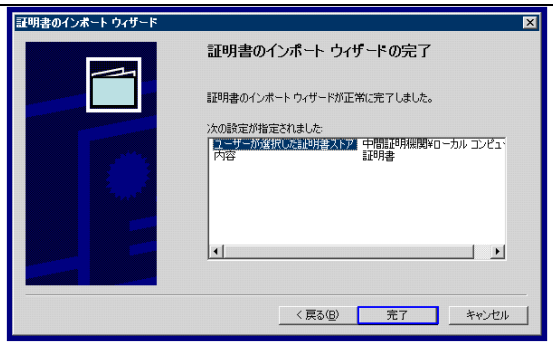
5. [証明書ストアの選択]ダイアログが表示されますので、[物理ストアを表示する(S)]をチェックしてください。
ダイアログ・ボックス内の項目［中間証明機関］のそばにある［+］マークをクリックして拡張し、［ローカル コンピュータ］を選択し、[OK]ボタンをクリックしてください。



6. 証明書ストアに[中間証明機関¥ローカル コンピュータ]が表示されていることを確認し、[次へ(N)>]ボタンをクリックします。



7. 以下の確認画面が表示されたら、[完了]ボタンをクリックしてください。証明書のインポートウィザードが表示されます。[OK]ボタンをクリックします。



8.　証明書のインポートウィザードが表示されます。[OK]ボタンをクリックします。

2-5-4 サーバ証明書のインストール

新規でサーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

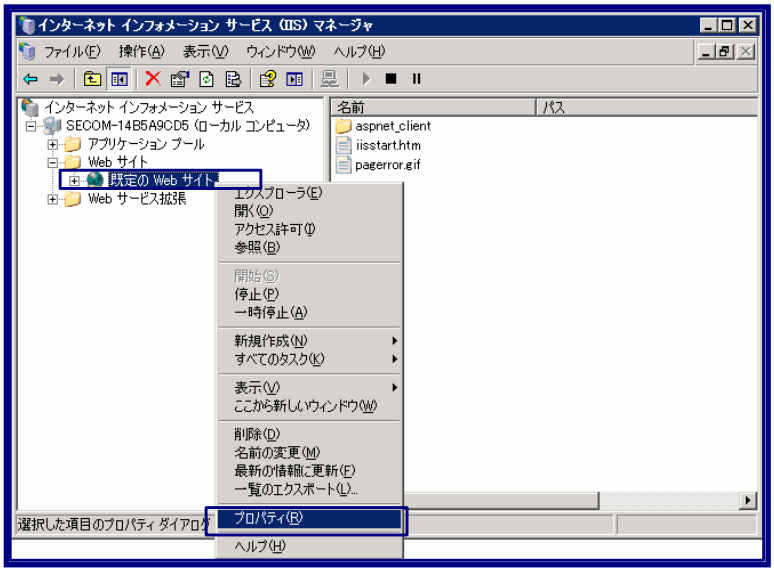
サーバ証明書のインストール

1. [2-5-1.事前準備]で取得したサーバ証明書と[2-3-1.鍵ペアの生成]で生成した私有鍵を PKCS#12 ファイルにします。サーバ証明書と私有鍵を同じフォルダ内に配置し、以下のコマンドを実行してください。カレントフォルダ内に、鍵ペアとサイト証明書(SSL/TLS 証明書)を連結した PKCS#12 の[servername.pfx]が作成されます。

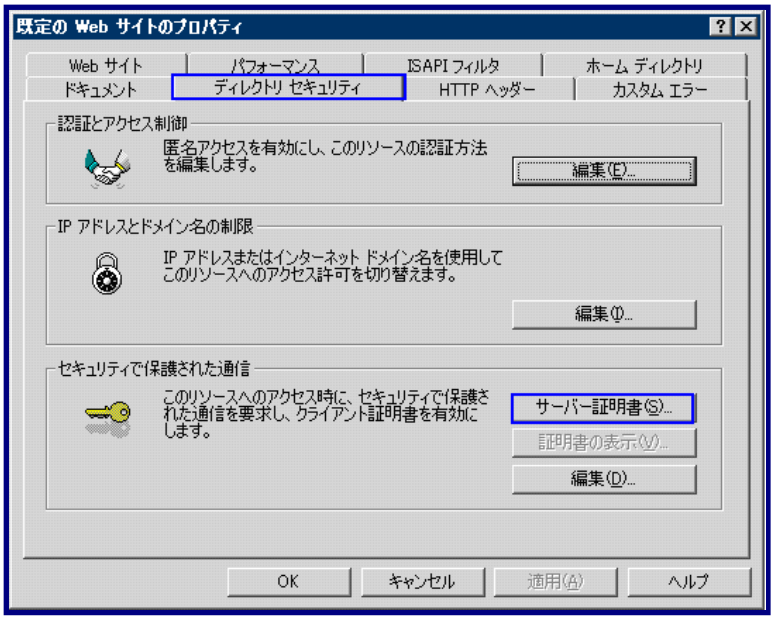
```
C:¥work> openssl pkcs12 -export -inkey servername.key -in server.cer -out servername.pfx

Enter pass phrase for servername.key:  ←[2-3-1 で入力したパスフレーズを入力]
Enter Export Password:                 ←PKCS#12 保護パスワード入力
Verifying - Enter Export Password:     ←PKCS#12 保護パスワード再入力
```

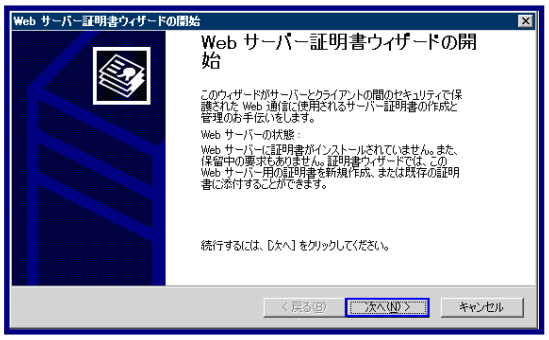
2. 次に、サーバ証明書を IIS6.0 に設定します。[インターネットインフォメーションサービス(IIS)マネージャ]を起動し、Web サイトのプロパティを開きます。



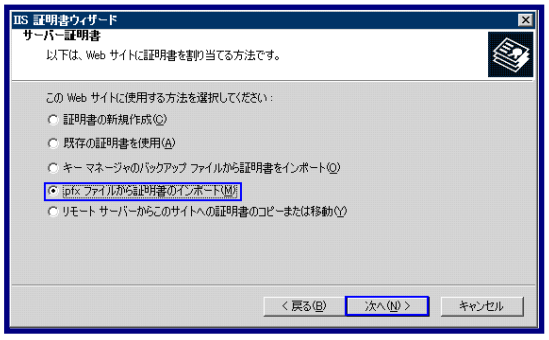
3. [ディレクトリ セキュリティ]タブより[セキュリティで保護された通信]の[サーバー証明書(S)...]を開きます。



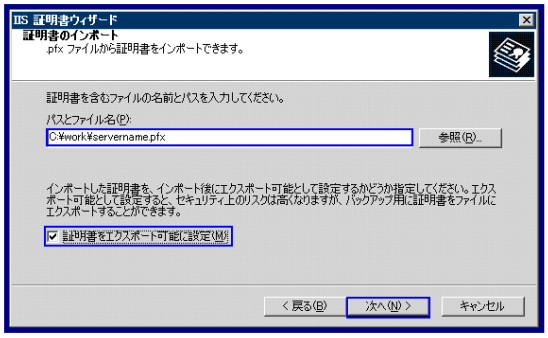
4.　[Web サーバー証明書ウィザードの開始]が起動します。[次へ(N)]ボタンをクリックします。



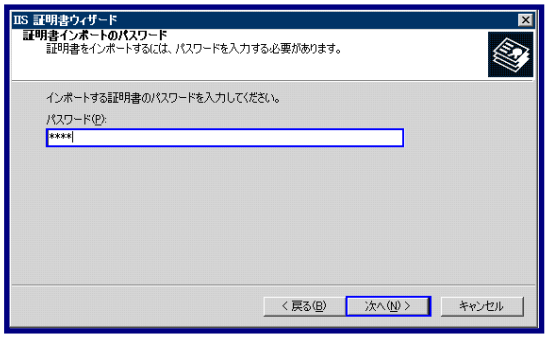
5.　[pfx ファイルから証明書のインポート]をチェックし、[次へ(N)]ボタンをクリックします。



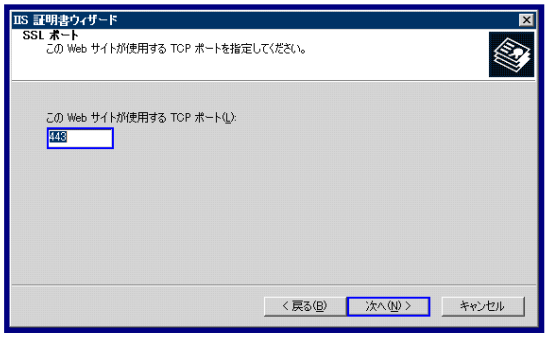
6. [参照(R)...]ボタンをクリックし、手続き 1.で準備した[servername.pfx]を指定します。[証明書をエクスポート可能に設定]をチェックし、[次へ(N)]ボタンをクリックします。



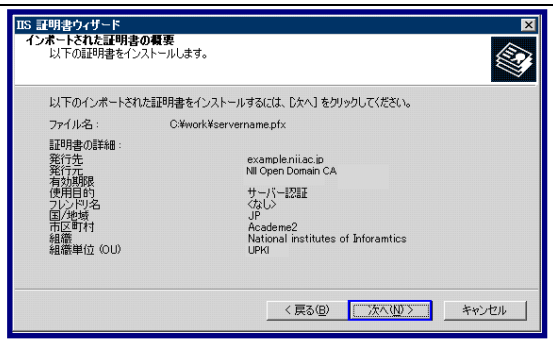
7. PKCS#12 ファイルを作る際に指定した PKCS#12 保護パスフレーズを入力し、[次へ(N)]ボタンをクリックします。



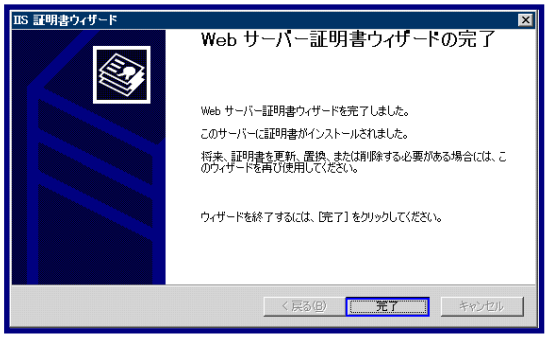
8. SSL/TLS サーバの TCP ポート番号を入力し[次へ(N)]ボタンをクリックします



9. サーバ証明書情報が表示されます。[次へ(N)]ボタンをクリックします。



10.　サーバ証明書がインストールされました。[完了]ボタンをクリックします。



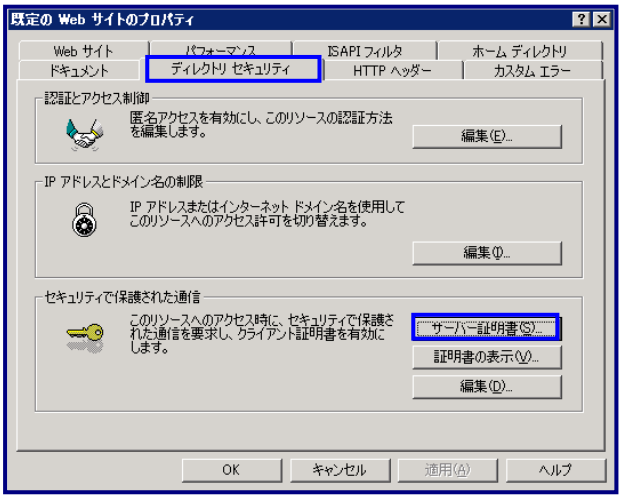
2-6.サーバ証明書の置き換えインストール

更新したサーバ証明書をインストールする場合は以下の手続きによりサーバ証明書のインストールを実施してください。

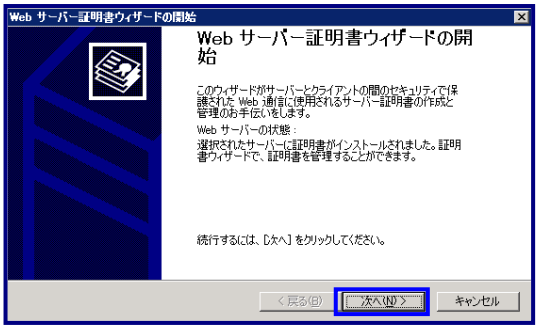
既に対象のサーバに証明書をインストールしている場合は，事前にインストールしている証明書の削除が必要となります。下記に登録された証明書の削除方法を記述します。

サーバ証明書の置き換えインストール

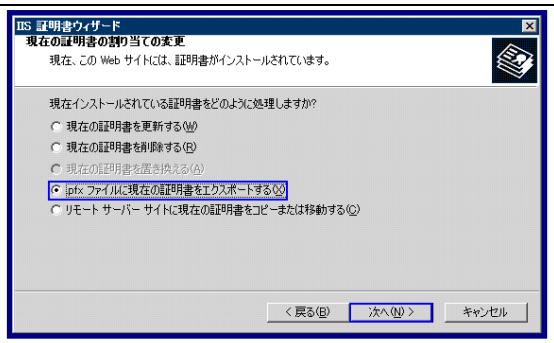
1. [インターネットインフォメーションサービス(IIS)マネージャ]を起動し、サイトのプロパティを開きます。
2. [ディレクトリ セキュリティ]のタブより[セキュリティで保護された通信]の[サーバー証明書(S)...]を開きます。



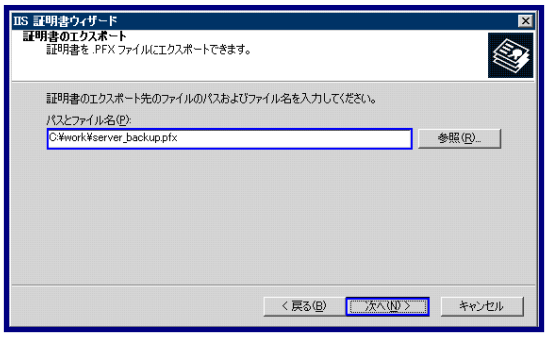
3. [サーバ証明書ウィザード]が起動します。[次へ(N)]ボタンをクリックします。



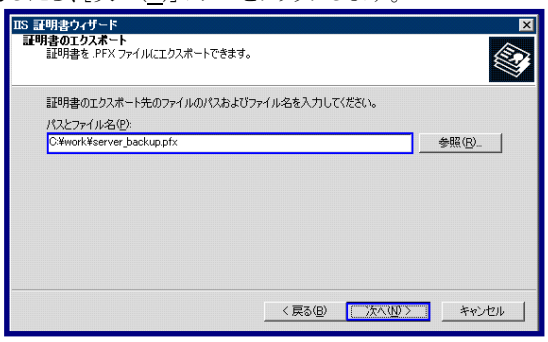
4. [.pfx ファイルに現在の証明書をエクスポートする(X)]をチェックし[次へ(N)]ボタンをクリックします。



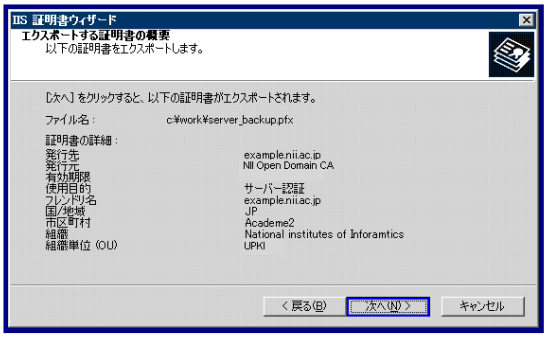
5. [参照(R)...]ボタンをクリックし、適当な名前を指定し、[次へ(N)]ボタンをクリックします。



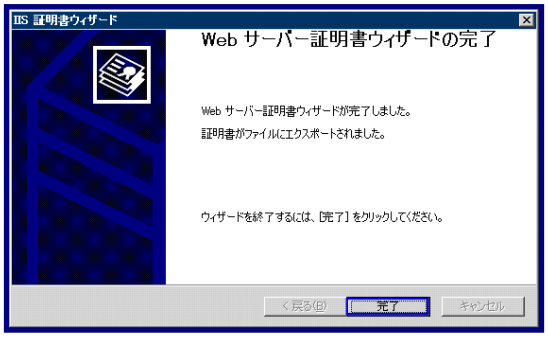
6. サーバ証明書を PKCS#12 にエクスポートします。PKCS#12 に保護パスフレーズを入力してください。
二度パスフレーズを入力したら、[次へ(N)]ボタンをクリックします。



7. エクスポートされるサーバ証明書情報が表示されます。[次へ(N)]ボタンをクリックします。

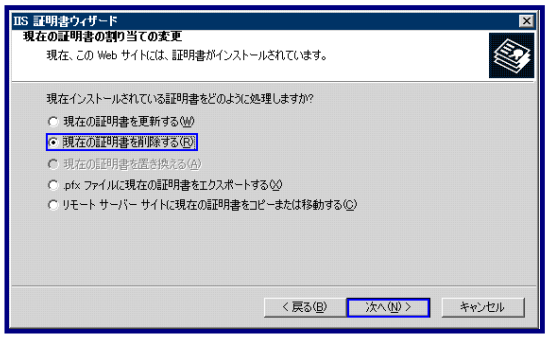


8. [完了]ボタンをクリックします。

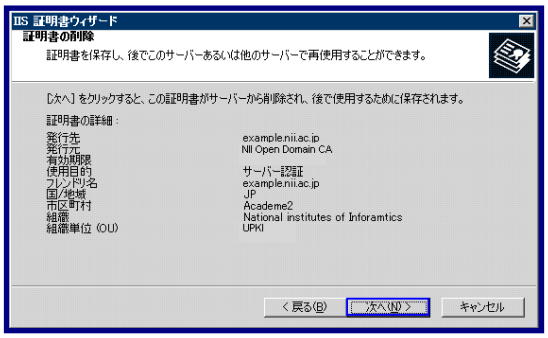


9. 再度、手続き 2. 3.を行ってください。

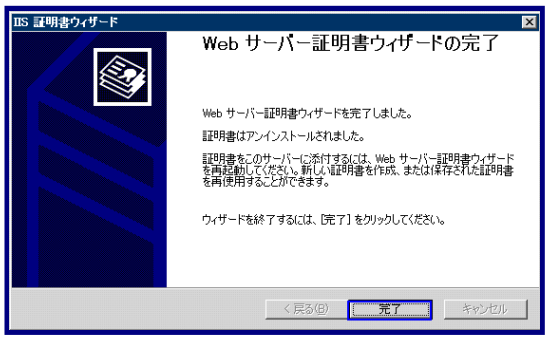
10. [現在の証明書を削除する(R)]をチェックし、[次へ(N)]ボタンをクリックします。



11. 現在インストールされている証明書を確認し、[次へ(N)]ボタンをクリックします。



12. [完了]をクリックします。



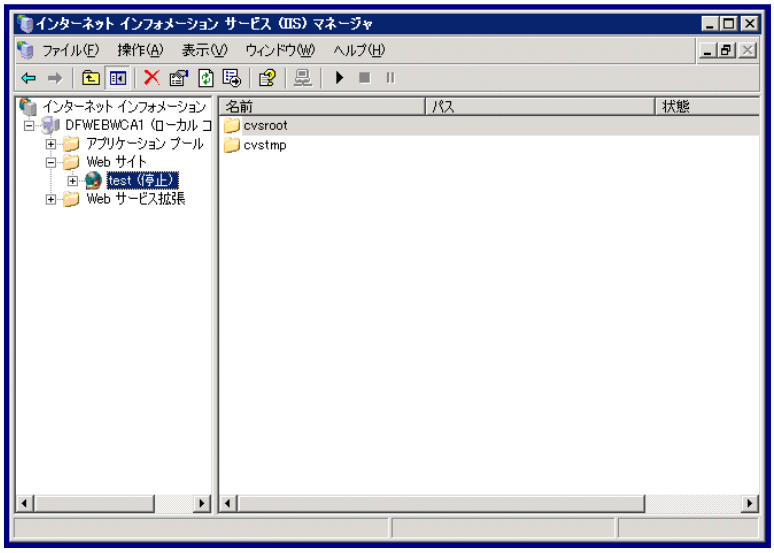
13. [2-5-3 サーバ証明書のインストール方法]の手続きに従い、新しい証明書をインストールしてください。

2-7.起動確認

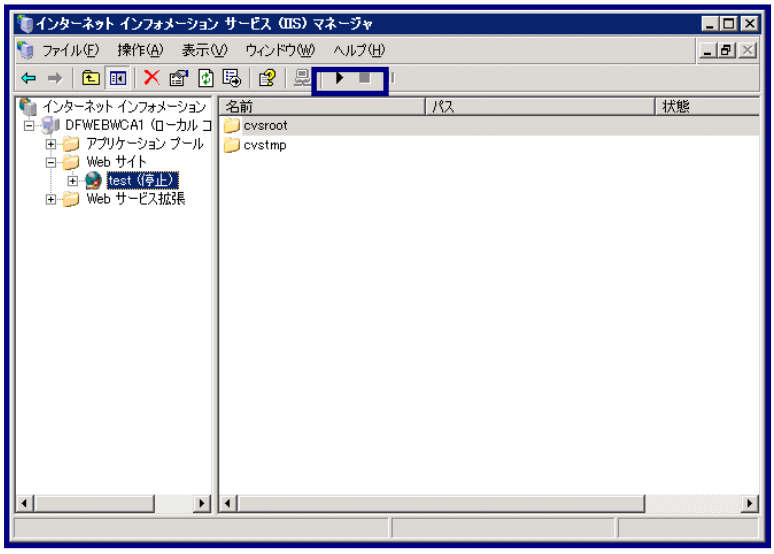
本章ではインストールした証明書による SSL 通信に問題がないか確認する方法を記述します。

証明書の反映・確認

1. [スタート]→[管理ツール]→[インターネットインフォメーションサービスマネージャ]を選択し、インターネットインフォメーションマネージャを開いてください。



2. [サービスの停止]→[サービスの開始]を実行し、IIS を再起動してください。



3. 当該のサーバに接続し、SSL 通信が行えることを確認してください。