事前準備 ～ 証明書の申請から取得まで

改版履歴			
版数	日付	内容	担当
V.1.1	2014/12/22	初版	NII
V.1.2	2015/5/15	中間CA証明書のファイル名を修正	NII
V.1.3	2015/12/11	サーバ証明書設定について注釈を追加	NII
V.2.0	2018/2/26	SHA1の記載内容の削除	NII
V.2.1	2018/7/9	DNのルールの修正 ECDSA対応を追加 IISにおけるCSR作成手順を追加	NII
V.2.5	2019/6/10	DNのルール(Locality Name)の修正	NII
V2.6	2020/1/30	誤植のある画像の差し替え	NII
V.2.7	2020/4/13	DNのルール(State or Province Name、Locality Name)の修正	NII
V.2.8	2020/7/15	DNのルール、TSVファイル形式のSTおよびLの値の説明、リンクの変更	NII
V.2.9	2020/12/22	サーバー証明書L、STを必須に修正 サーバー証明書OUの利用条件を修正	NII
V.2.10	2022/08/02	CSR作成からOUを削除	NII

目次

- 1.事前準備
- 2.鍵ペアの生成とCSRの作成(openssl)
  - 2-1 鍵ペアの生成
  - 2-2 CSRの生成
- 3.IISを利用したCSRの作成
  - 3-1 CSRの生成
    - RSAの場合
    - ECDSAの場合
- 4.証明書の申請から取得まで

1.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*>**(「**2-1、2-2**で使用」)
3. サーバ DN（※サーバDNについては、本サービス証明書ポリシまたは、下記DNのルールをご確認ください）
4. CSRファイル名は　**servername.csr**　としています。

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)	「都道府県」（ST）は利用管理者及び利用者が所属する組織の所在地の都道府県名としサービス窓口に事前に届出したとおりの所在地の都道府県名をローマ字表記で指定してください。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）ST=Tokyo	○	STとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）

Locality Name(L)	「場所」（L）は利用管理者及び利用者が所属する組織の所在地の市区町村名とし、サービス窓口に事前に届出したとおりの所在地の市区町村名をローマ字表記で指定してください。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)L=Chiyoda-ku	○	Lとして指定できる値は下記リンクを参照してください。機関ごとに固定となります。 UPKI証明書 主体者DNにおける ST および L の値一覧 ※STおよびLが必須。（2020年12月22日以降）
Organization Name (O)	サービス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)
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にはサービス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 ECDSA 384bit			

○・・・必須　×・・・入力不可　△・・・省略可

注意：証明書の更新を行う場合は、先に各手順の「サーバ証明書の置き換えインストール」をご確認ください。

2.鍵ペアの生成とCSRの作成(openssl)

2-1 鍵ペアの生成

以下にopensslを使用した場合の鍵ペアの生成方法を記述します。

鍵ペアの作成

RSA鍵の場合

1. 鍵ペアを生成するため、「1.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、作業ディレクトリに移動してください。

```
$mv <randfile1.txt> <randfile2.txt> <randfile3.txt> /etc/httpd/conf/ssl.key/
```

3. 鍵ペアの作成を行うため、次のコマンドを入力してください。今回のコマンド例では、 作業ディレクトリに移動し、2048 bitの RSA 鍵ペアを生成し、「servername.key」という名前で保存することを示しています。

```
$cd /etc/httpd/conf/ssl.key/ ←作業ディレクトリへ移動してください
$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、サーバの再起動時および証明書のインストール等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。

4. 作成した鍵ペアのファイルを保存します。バックアップは外部媒体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利用管理者自身と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外部媒体ディスク等も利用管理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。

ECDSA鍵の場合

1. 鍵ペアの作成を行うため、次のコマンドを入力してください。今回のコマンド例では、 作業ディレクトリに移動し、384 bitの ECDSA 鍵ペアを生成し、「servername.key」という名前で保存することを示しています。

```
$openssl ecparam -name secp384r1 -genkey | openssl ec -out servername.key -des3
read EC key
writing EC key
Enter PEM pass phrase:<PassPhrase>                 ←私有鍵パスフレーズ入力
Verifying - Enter PEM 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、サーバの再起動時および証明書のインストール等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。

2. 作成した鍵ペアのファイルを保存します。バックアップは外部媒体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利用管理者自身と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外部媒体ディスク等も利用管理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。

2-2 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、「2-1 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。

   RSA鍵の場合
   コマンドでは、署名アルゴリズムSHA2でCSRを作成し、「servername.csr」（ファイル名は任意）というファイル名で保存することを示しています。

   ```
   $openssl req -new -key servername.key -sha256 -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
   ```

   「**-sha256**」:署名アルゴリズムを示すオプション。
   署名アルゴリズムSHA1でCSRを作成する場合は、「-sha1」に置き換えてください。

   ECDSA鍵の場合
   コマンドでは、署名アルゴリズムecdsa-with-SHA256でCSRを作成し、「servername.csr」（ファイル名は任意）というファイル名で保存することを示しています。

   ```
   $openssl req -new -key servername.key -sha256 -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
   ```

   「**-sha256**」:署名アルゴリズムを示すオプション。
   署名アルゴリズムecdsa-with-SHA384でCSRを作成する場合は、「-sha384」に置き換えてください。

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、「1. 事前準備」の「DNルール」に従い、DN情報を入力してください。

   OpenSSLでは必要ない項目を「.」ドットを入力することにより、省略することができます。

   ```
   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) []:Tokyo ←都道府県名を入力
       Locality Name (eg, city) []:Chiyoda-ku ←市町村名を入力
       Organization Name (eg, company) [Default Company Ltd]:National Institute of Informatics← 組織名を入力

       Organizational Unit Name (eg, section) []:. ← 「.」ドットを入力
       Common Name (eg, your name or your server's hostname) []: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、servername.csrに保存されます。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
   Um0E3vq8Ajg=
   ----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。

RSA鍵で作成したCSRの場合

```
$ openssl req -noout -text -in servername.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, L=Chiyoda-ku,ST=Tokyo, O=National Institute of Informatics,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
            Public Key: (2048 bit)←鍵長が2048bitであることを確認してください。
                Modulus:
                    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: sha256WithRSAEncryption← CSR生成時に指定した署名アルゴリズムで あることを確認してください。
                                                 署名アルゴリズムにsha1を指定した場合は「sha1WithRSAEncryption」と表示されます。

         88:44:e5:27:06:02:ec:85:6c:29:6a:0f:a3:92:87:4e:e2:f1:
                                :
                               例
```

ECDSA鍵で作成したCSRの場合

```
$ openssl req -noout -text -in servername.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP, ST=Tokyo, L=Chiyoda-ku, O=National Institute of Informatics,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: id-ecPublicKey
            Public Key: (384 bit)←鍵長が384bitであることを確認してください。
            pub:
                04:6c:66:6a:98:01:63:ed:b8:36:fe:d9:bd:54:f7:
                                :
                               例
                                :
                c2:7e:92:20:93:e6:29
            ASN1 OID: secp384r1
            NIST CURVE: P-384
    Attributes:
    Requested Extensions:
        X509v3 Subject Key Identifier:
            98:5A:D9:7B:3C:5D:4E:C1:62:8C:5F:2D:89:1A:B3:DC:F7:6C:1C:E2
    Signature Algorithm: ecdsa-with-SHA256← CSR生成時に指定した署名アルゴリズムであることを確認してください。
                                           署名アルゴリズムにsha384を指定した場合は「ecdsa-with-SHA384」と表示されます。

     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:
    c1:cc
```

3.IISを利用したCSRの作成

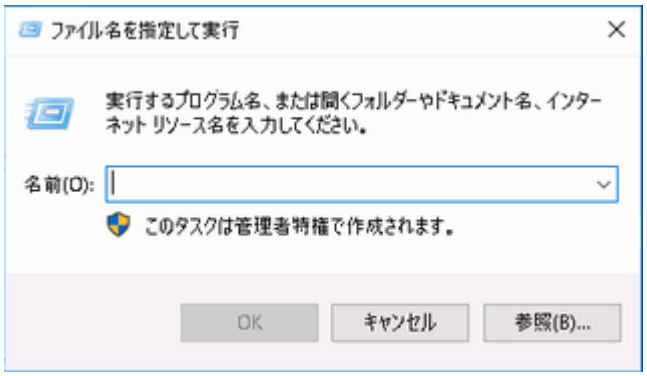
3-1 CSRの生成

以下にIISを使用した場合のCSRの作成を記述します。

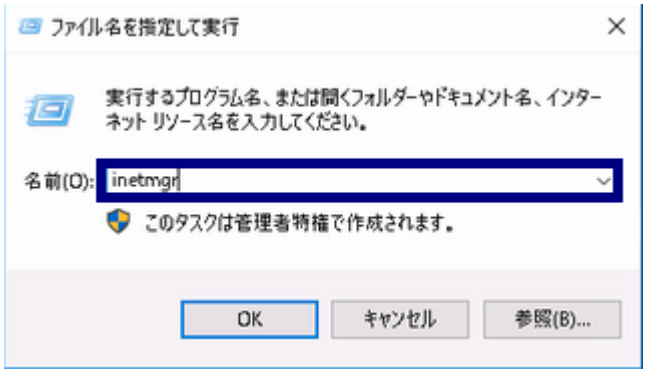
CSRの作成

RSAの場合

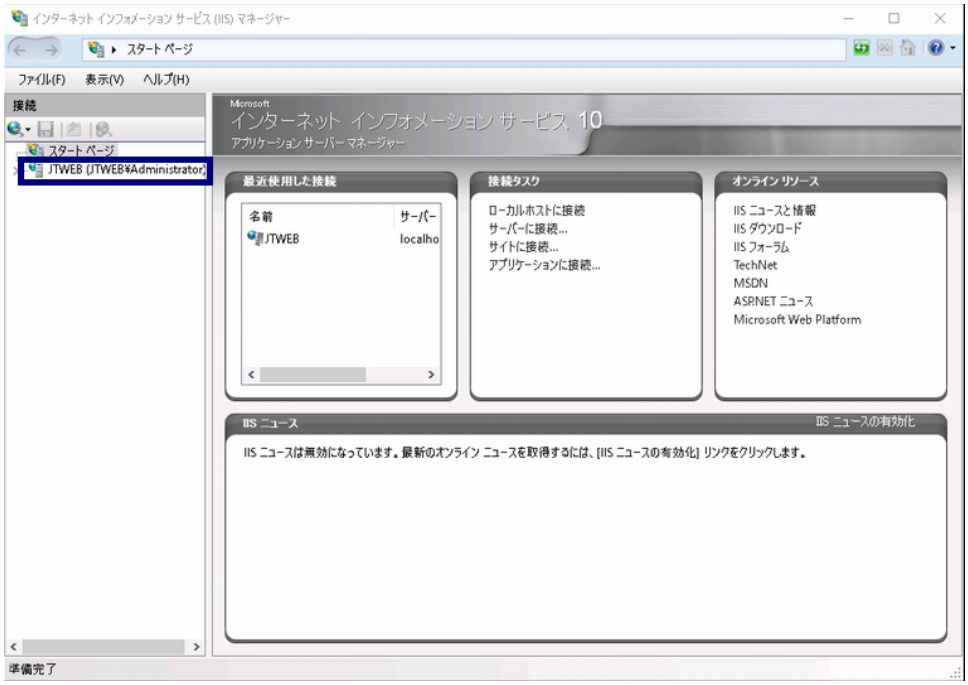
1. [スタート] メニューの [すべてのプログラム] をクリックします。[アクセサリ] をクリックして、[ファイル名を指定して実行] をクリックします。



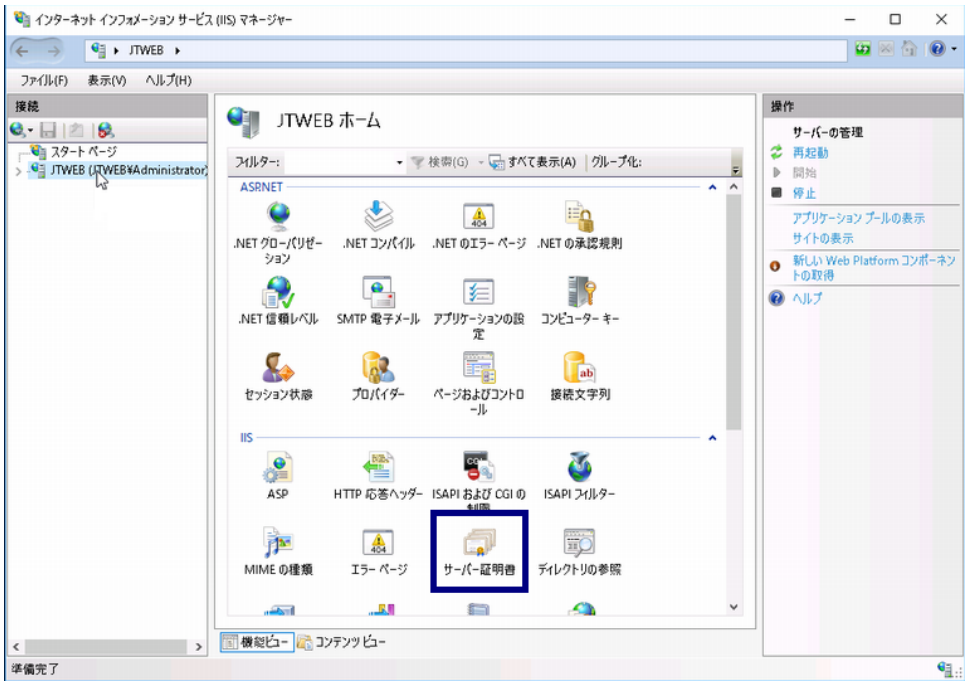
2. [名前] ボックスに「inetmgr」と入力し、[OK] をクリックします。



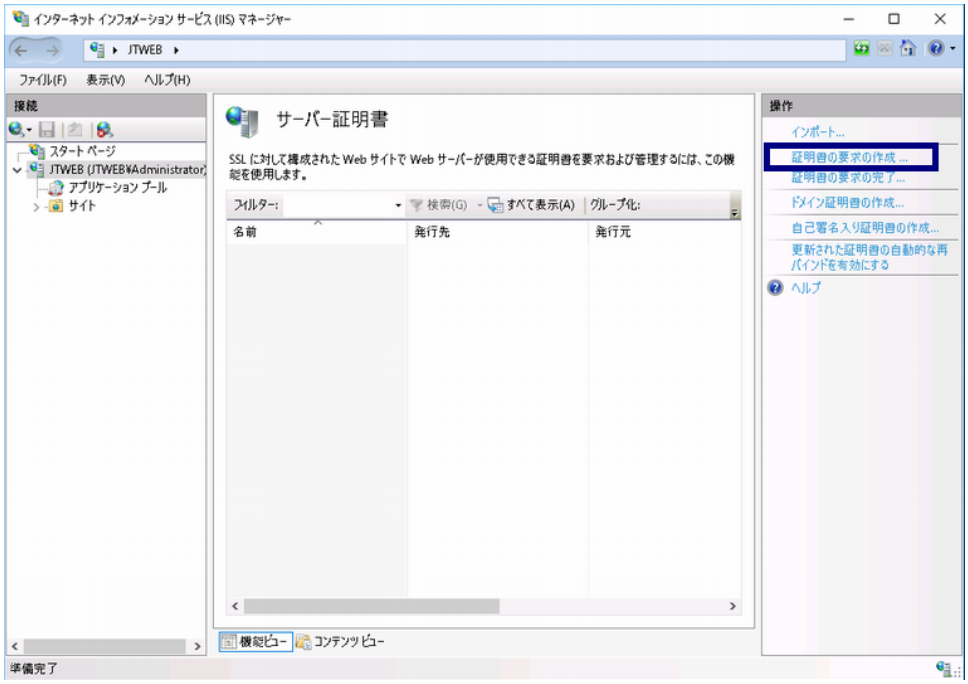
3. インターネットインフォメーションサービス（IIS）マネージャーが表示されます。
画面左側の[接続]メニューよりサーバー名をクリックしてください。



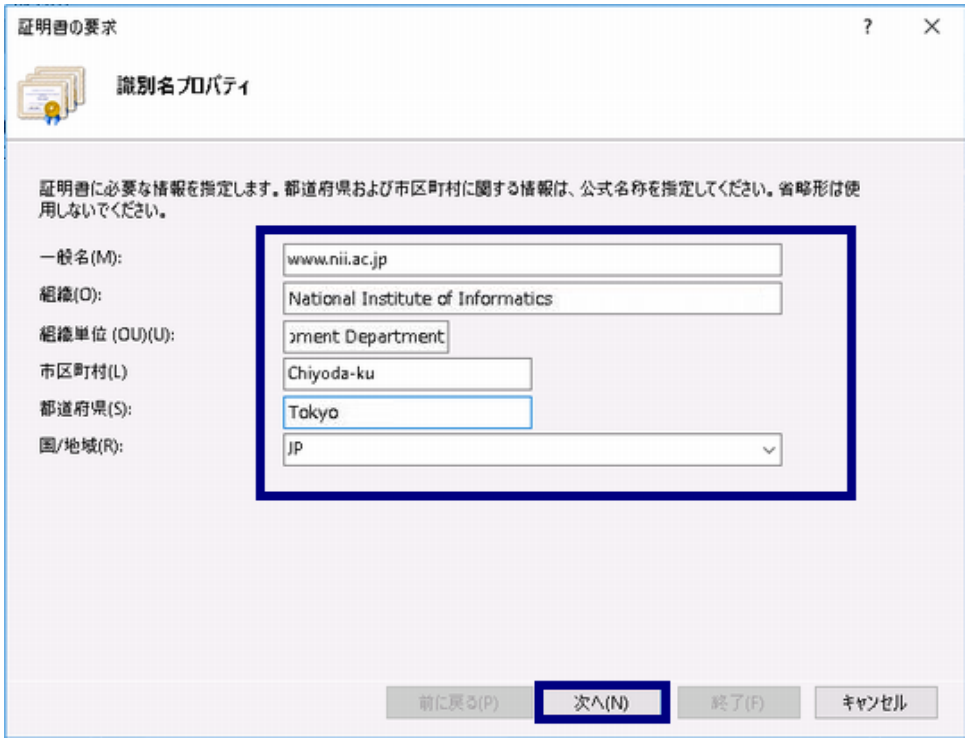
4. [サーバー証明書]をダブルクリックしてください。



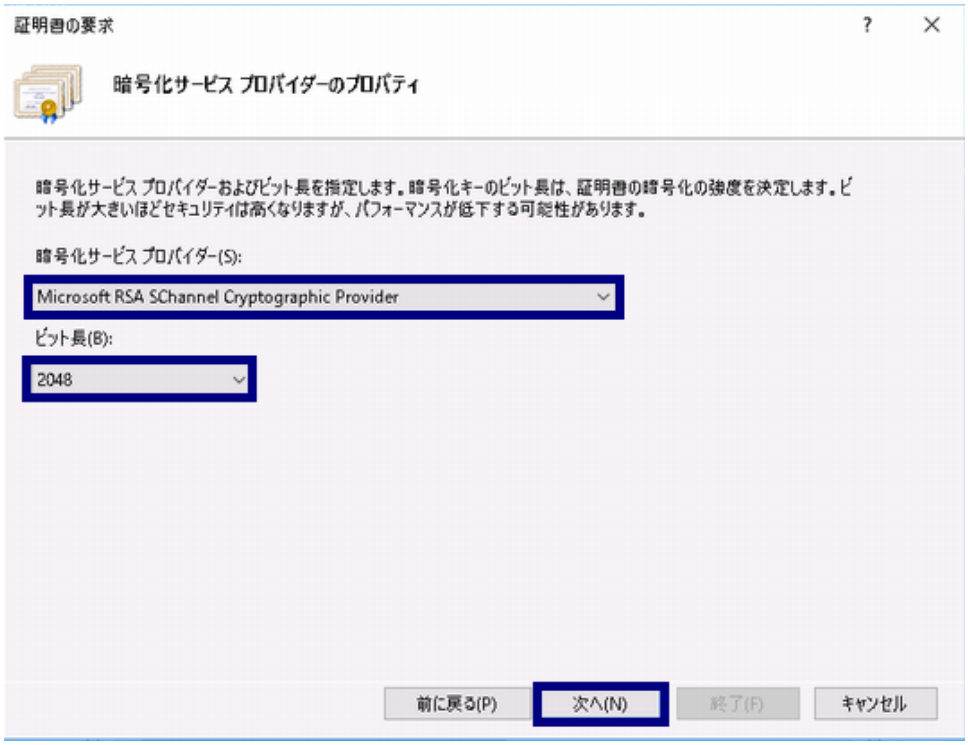
5. [操作]ペインの[証明書の要求の作成]を選択してください。



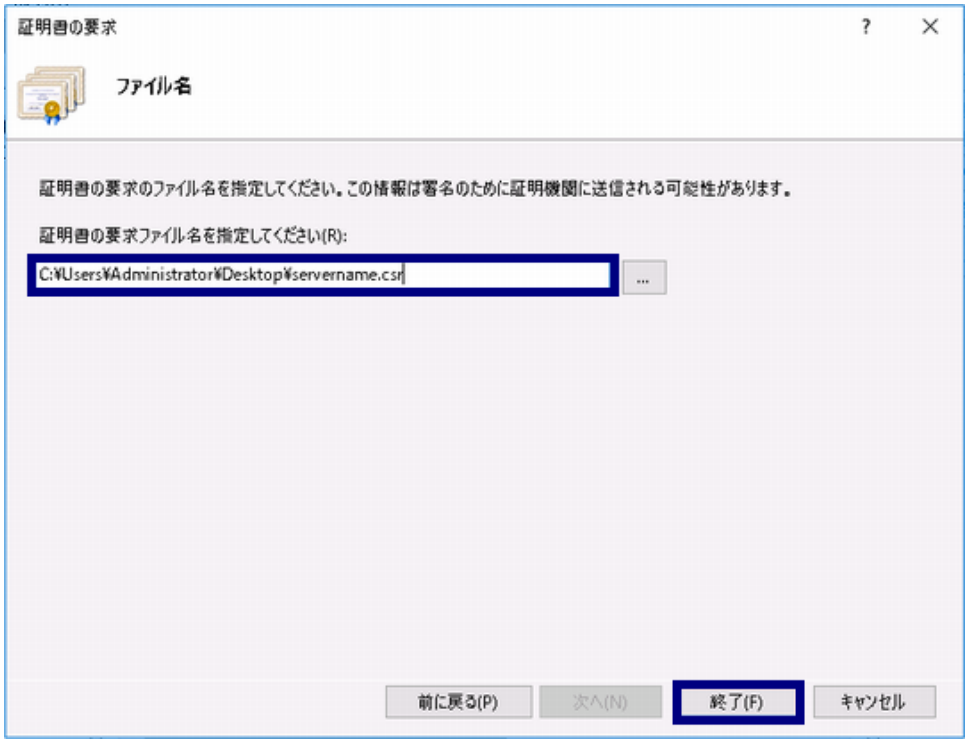
6. [証明書の要求]画面で[識別名プロパティ]が表示されますので、[2-2. 事前準備]の[DNルール]に従い、DN情報を入力して[次へ(N)]を押してください。



7. [暗号化サービス プロバイダーのプロパティ]が表示されますので、
[暗号化サービス プロバイダー(S)]の欄は[Microsoft RSA Schannel Cryptographic Provider]を選択し、
[ビット長(B)]の欄は[2048]を選択して[次へ(N)]を押してください。



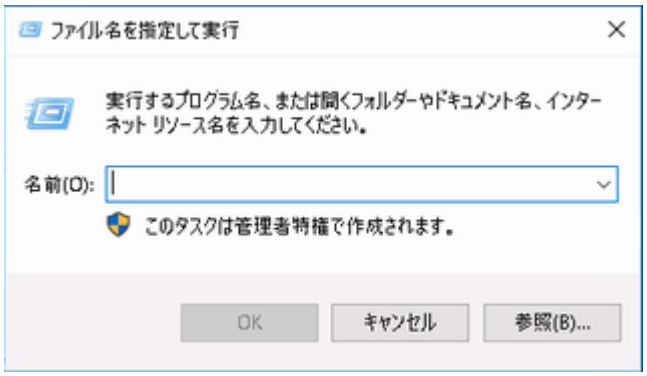
8. [ファイル名]が表示されますので、
[証明書の要求ファイル名を指定してください(R)]の欄に任意の保存場所を選択して[終了(F)]を押してください。



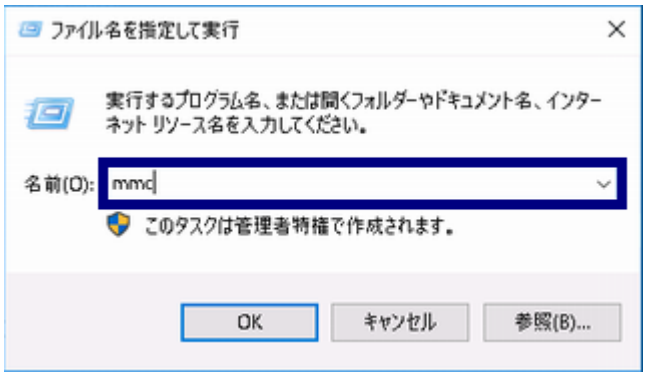
9. 指定した保存場所に生成したCSRが保存されます。

ECDSAの場合

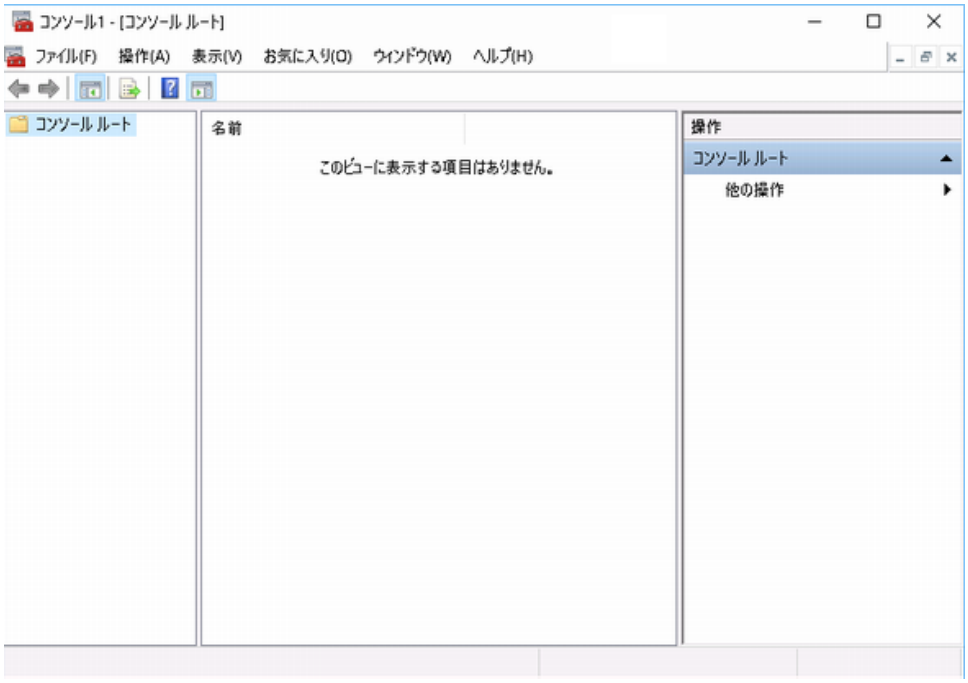
1. [スタート] メニューの [すべてのプログラム] をクリックします。[アクセサリ] をクリックして、[ファイル名を指定して実行] をクリックします。



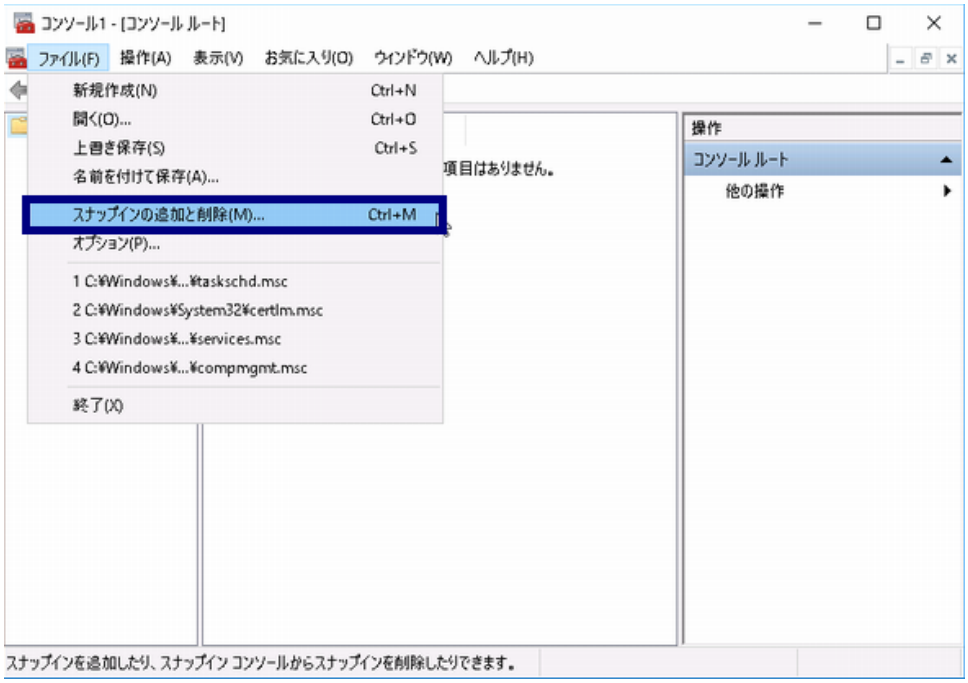
2. [名前] ボックスに「mmc」と入力し、[OK] をクリックします。



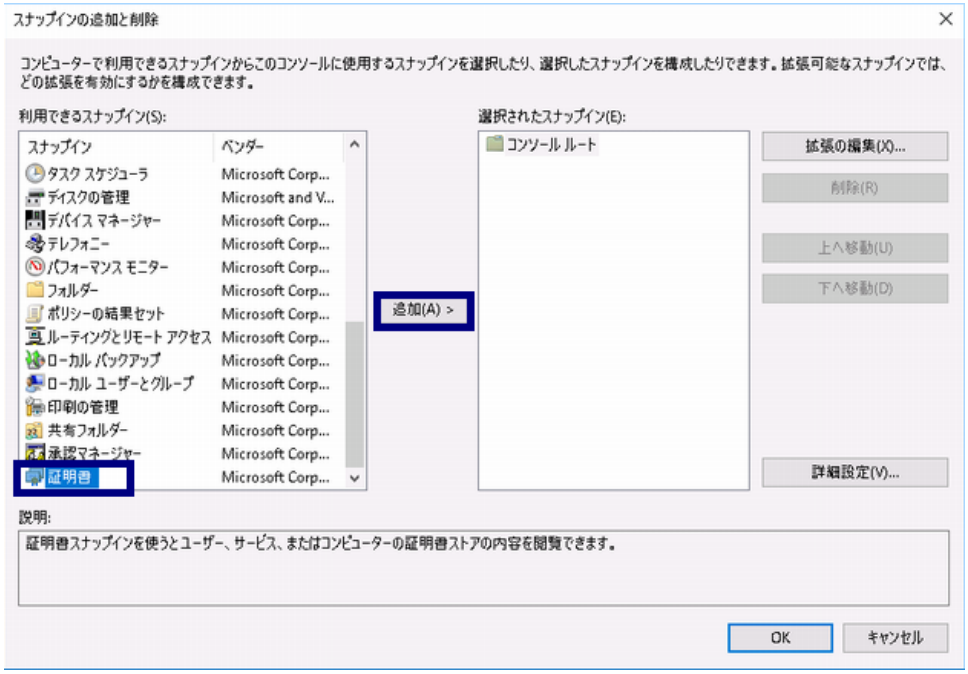
3. Microsoft Management Console が表示されます。



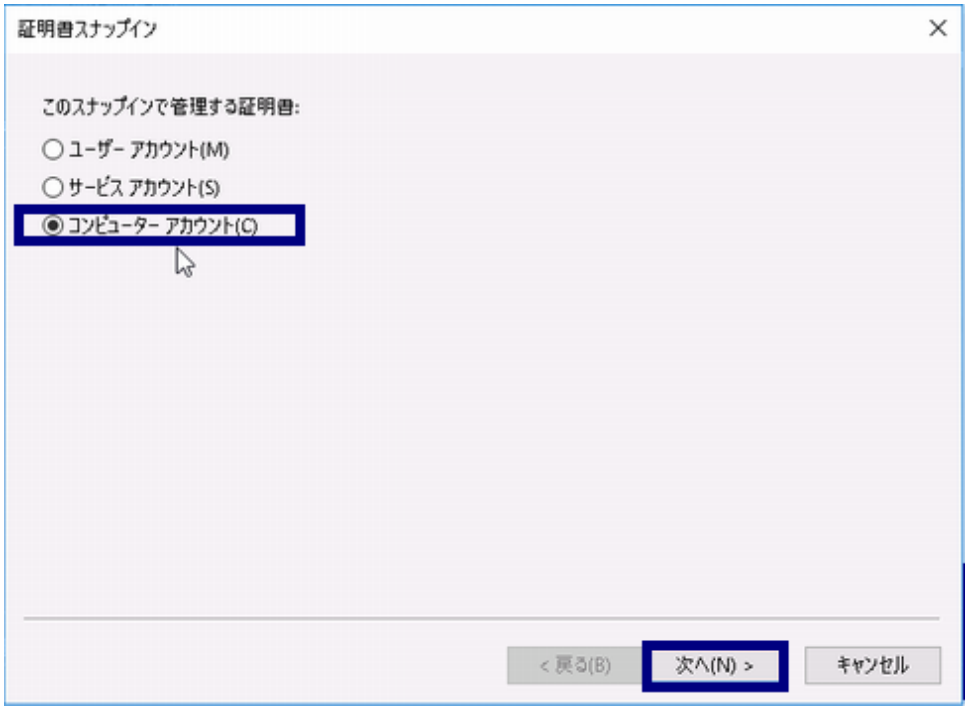
4. [ツールバー] > [ファイル] > [スナップインの追加と削除] を選択してください。



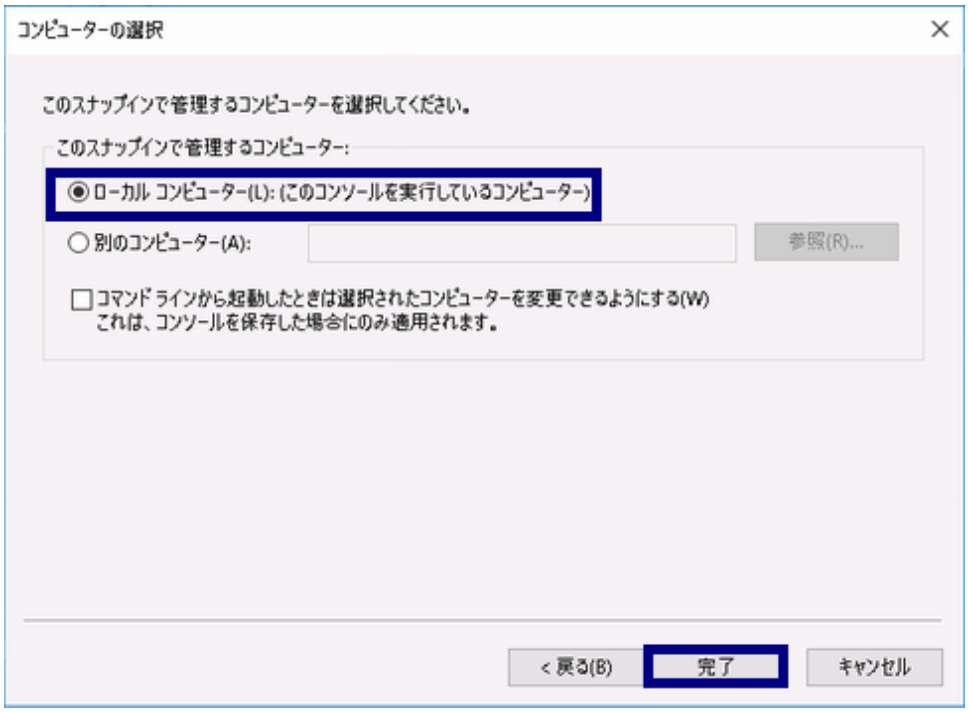
5. [利用できるスナップイン] > [証明書] を選択し、[追加]ボタンを押下してください。



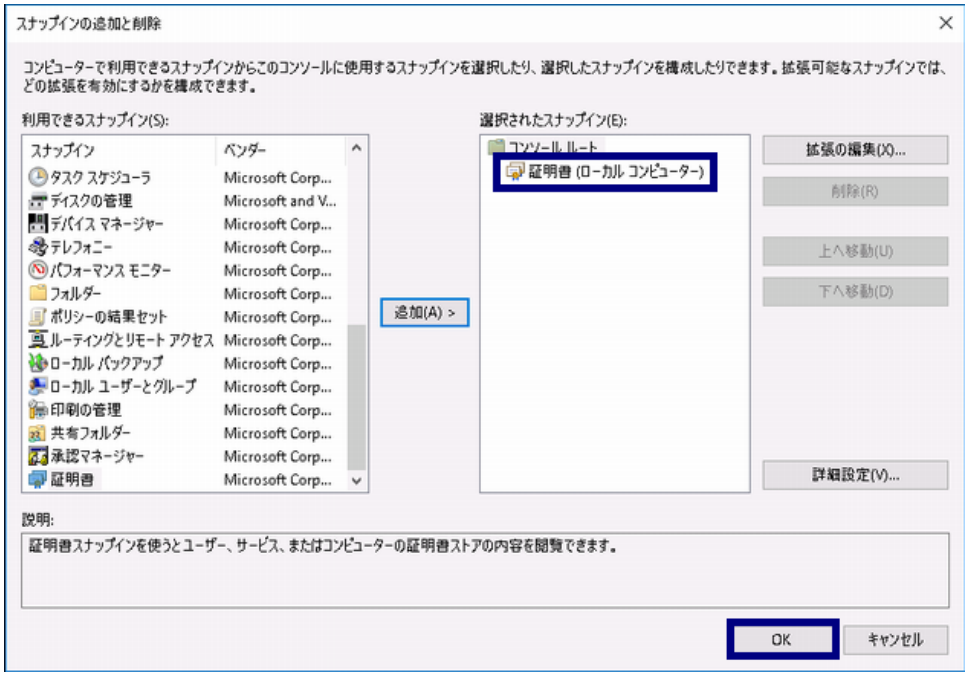
6. [コンピュータアカウント]を選択し、[次へ]ボタンを押下してください。



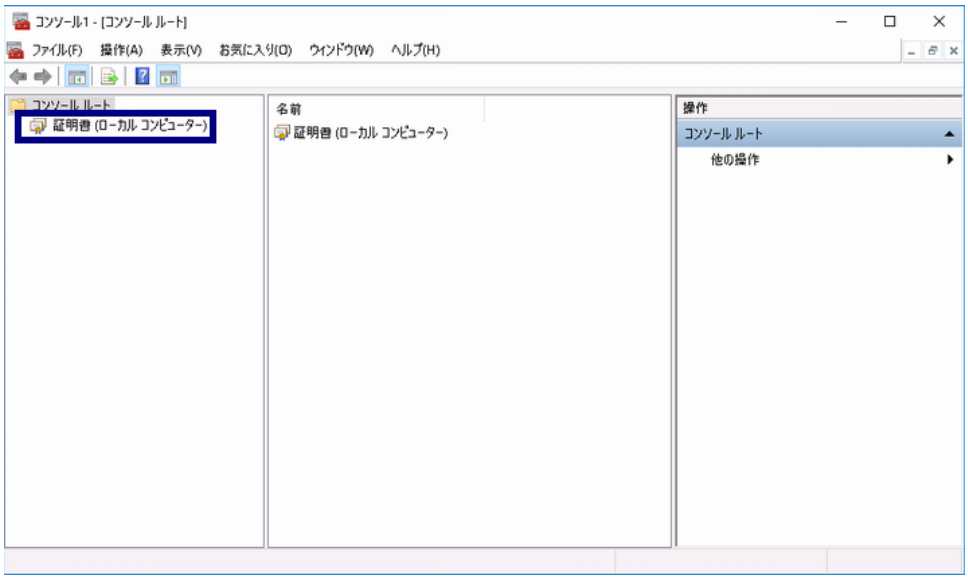
7. ローカルコンピュータ（このコンソールを実行しているコンピュータ）]を選択し、[完了]ボタンを押下してください。



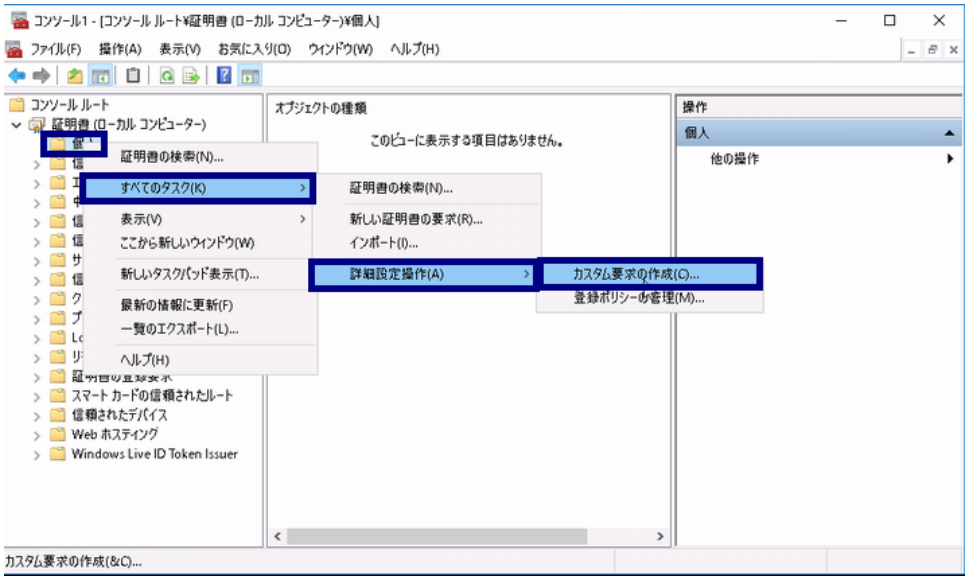
8. 選択されたスナップインに [証明書 - ローカル コンピューター]が表示されていることを確認し、[OK]ボタンを押下してください。



9. [コンソールルート] > [証明書 - ローカル コンピューター]が表示されていることを確認してください。

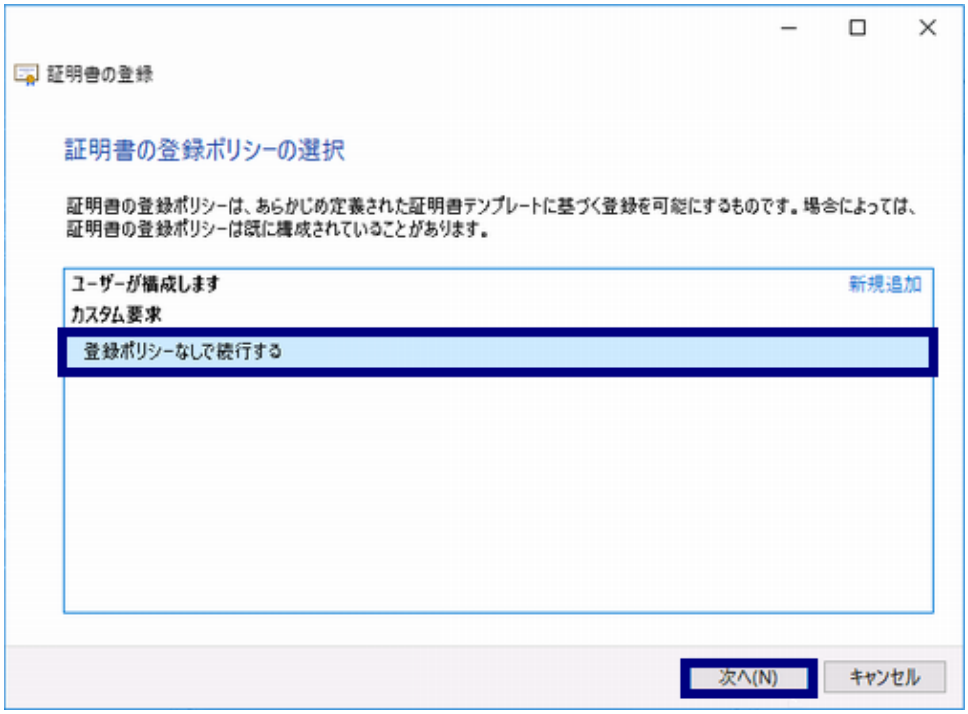


10. [コンソールルート] > [証明書 - ローカル コンピューター] > [個人] > [証明書]を選択し、
右クリックメニューから[すべてのタスク] > [詳細設定操作] > [カスタム要求の作成]を選択してください。

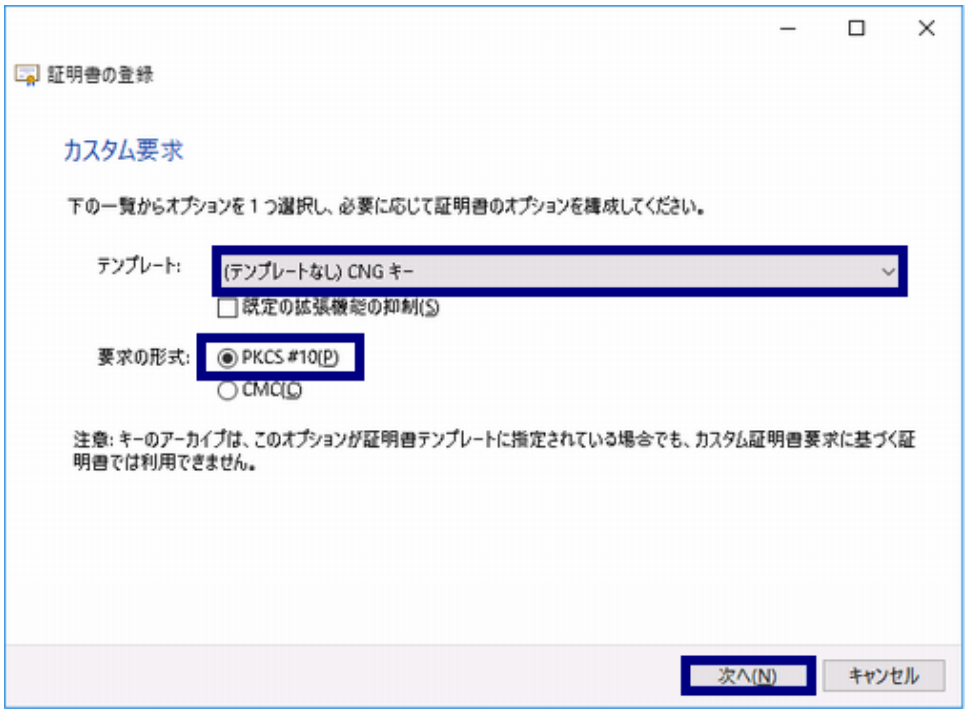


11. [次へ]ボタンを押下してください。

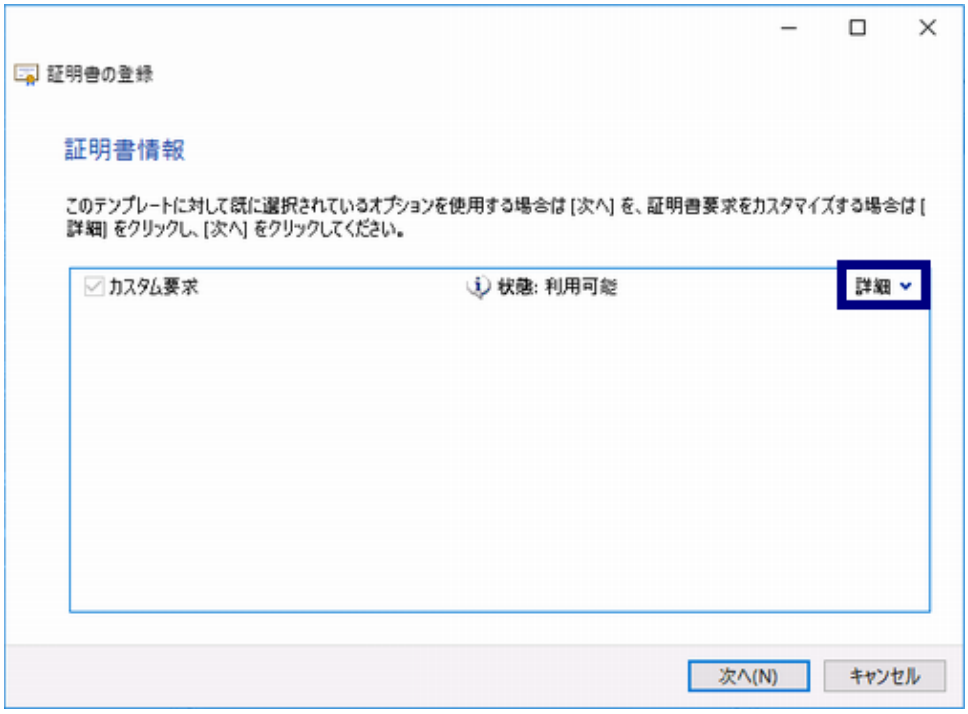
12. [カスタム要求]> [登録ポリシーなしで発行する]を選択し、[次へ]ボタンを押下してください。



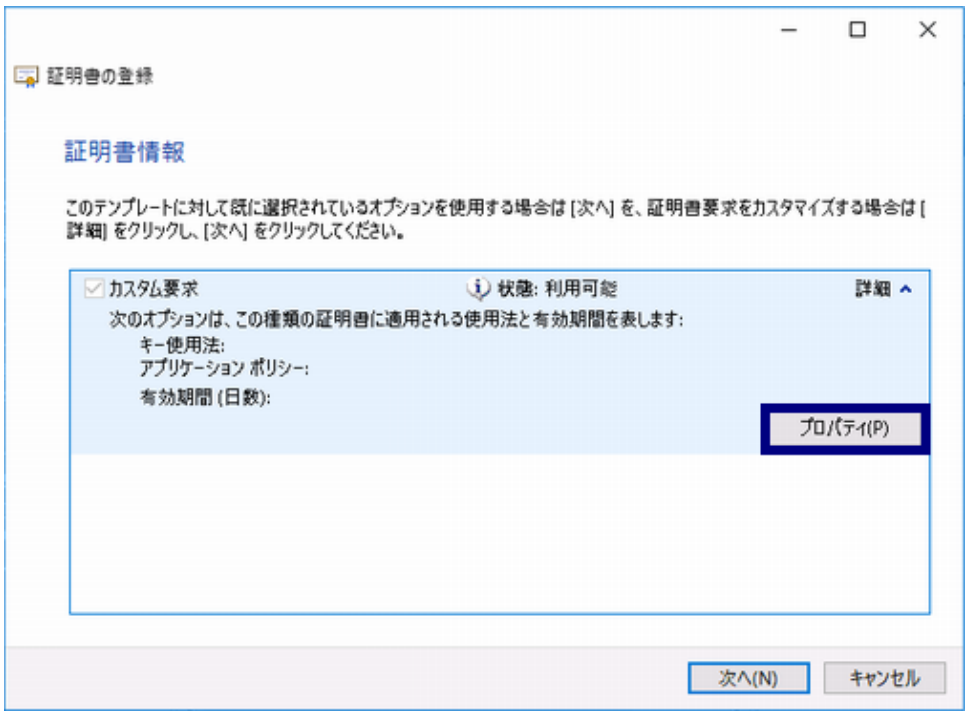
13. 以下を選択し、[次へ]ボタンを押下してください。
テンプレート：[（テンプレートなし）CNGキー]
要求の形式　：PKCS#10



14. [詳細]を押下してください。

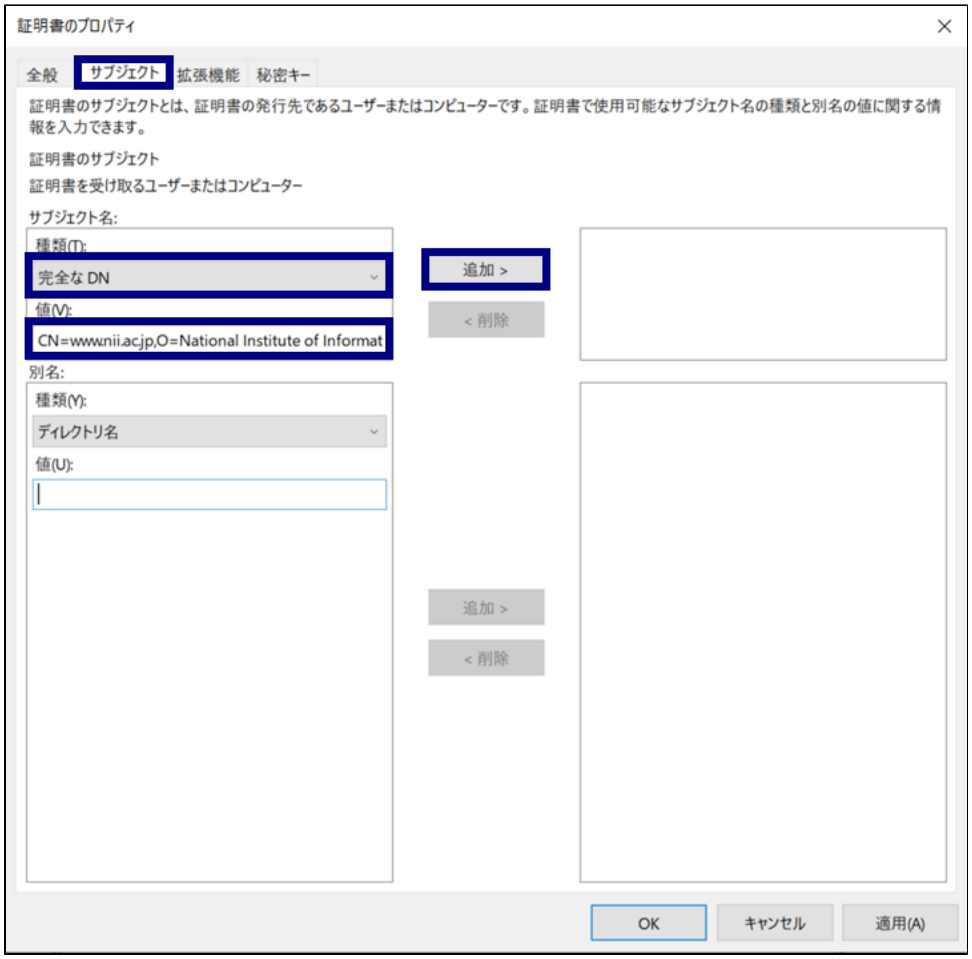


15. 詳細内容を表示し、プロパティボタンを押下してください。

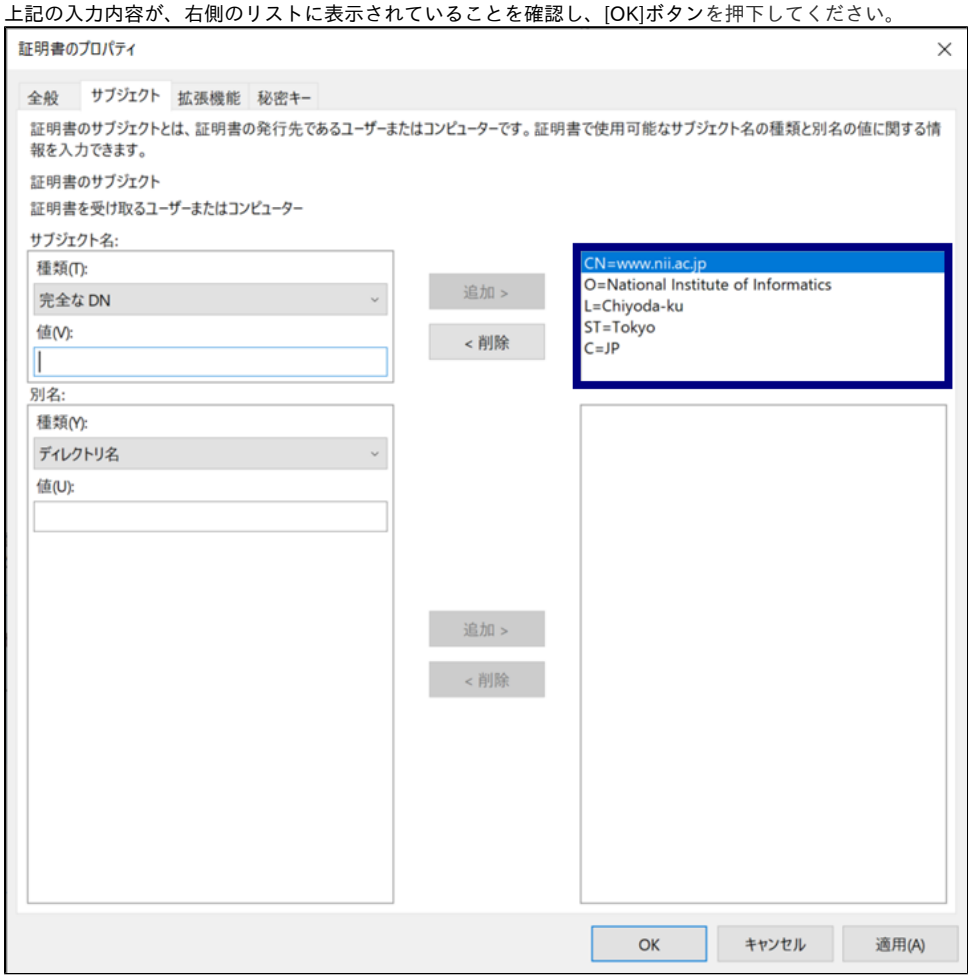


16. サブジェクトタブを選択後、以下を選択し、[追加]ボタンを押下してください。

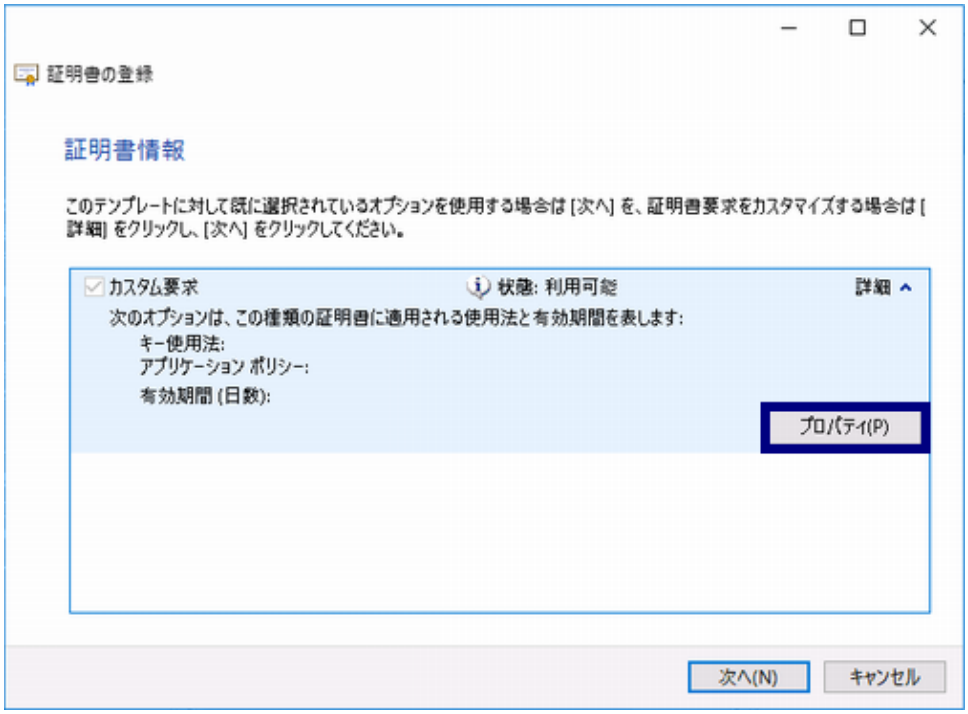
種類：「完全なDN」
値　：指定したい主体者DNを入力（例：CN=www.nii.ac.jp,O=National Institute of Informatics,L=Chiyoda-ku,ST=Tokyo,C=JP）



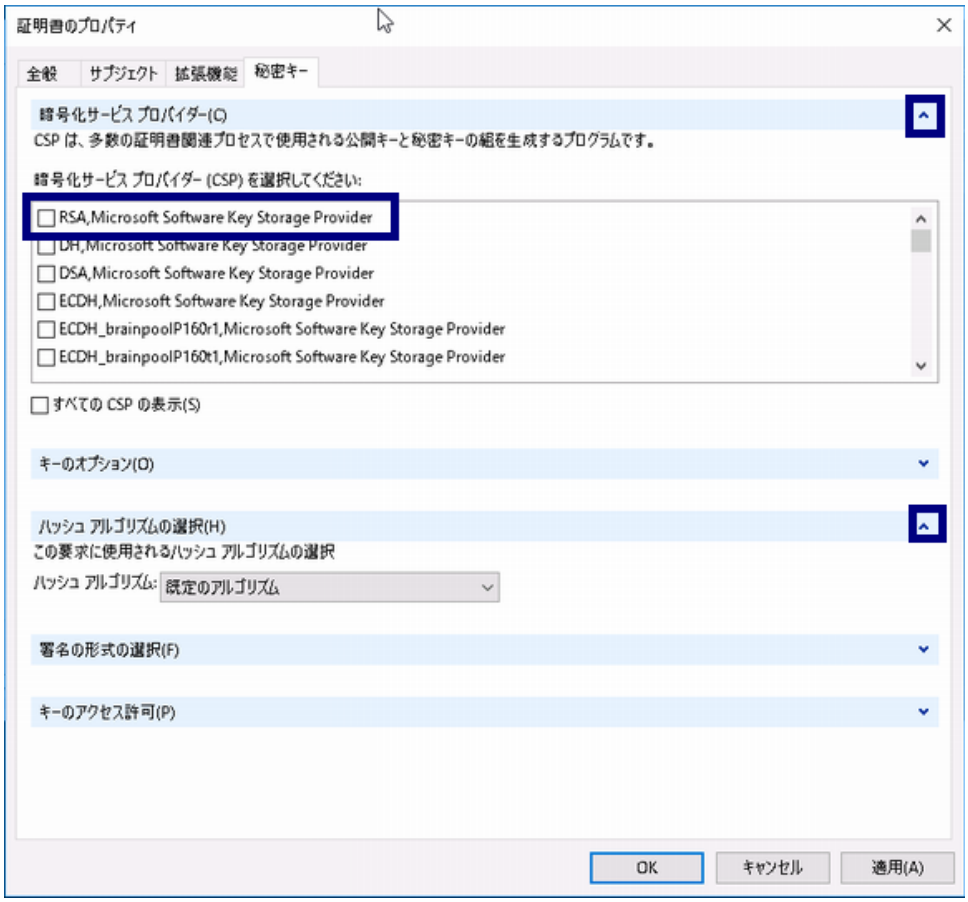
17. 上記の入力内容が、右側のリストに表示されていることを確認し、[OK]ボタンを押下してください。



18. プロパティボタンを押下してください。

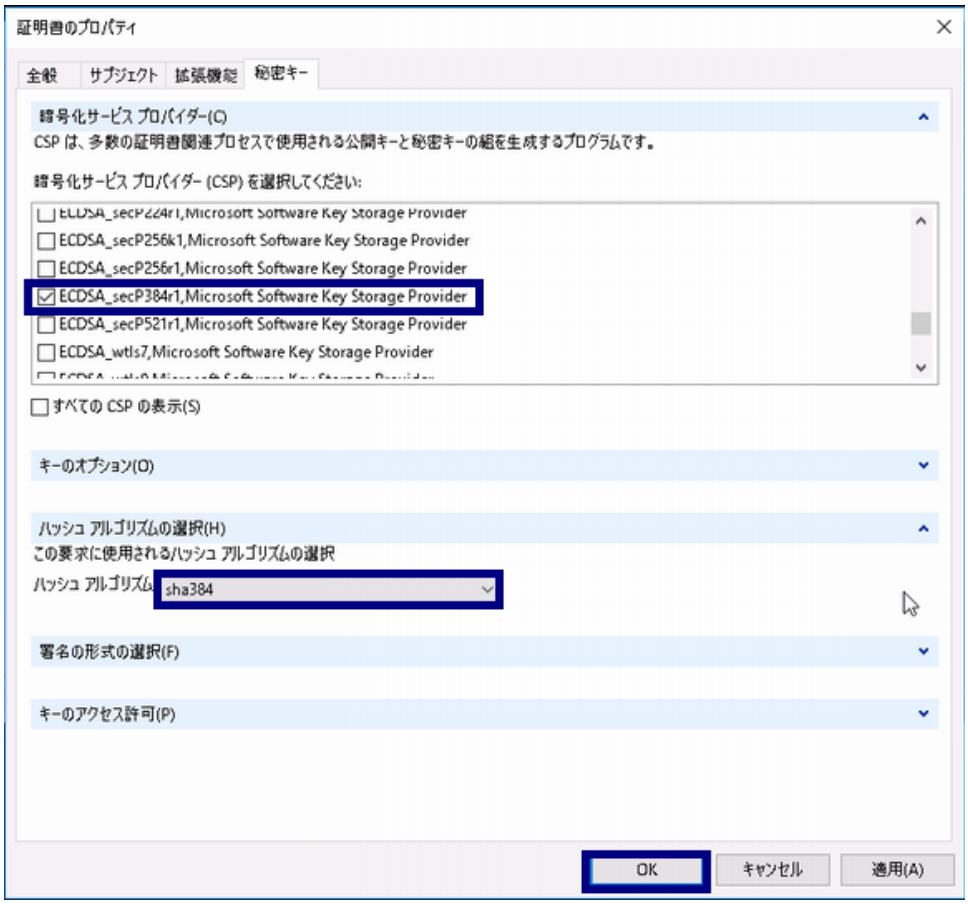


19. 秘密キータブを選択してください。
暗号化サービスプロバイダーとハッシュアルゴリズムの選択の詳細を表示してください。
以下が選択されていた場合、チェックを外してください。
暗号化サービスプロバイダー：RSA,Microsoft Software Key Storage Provider

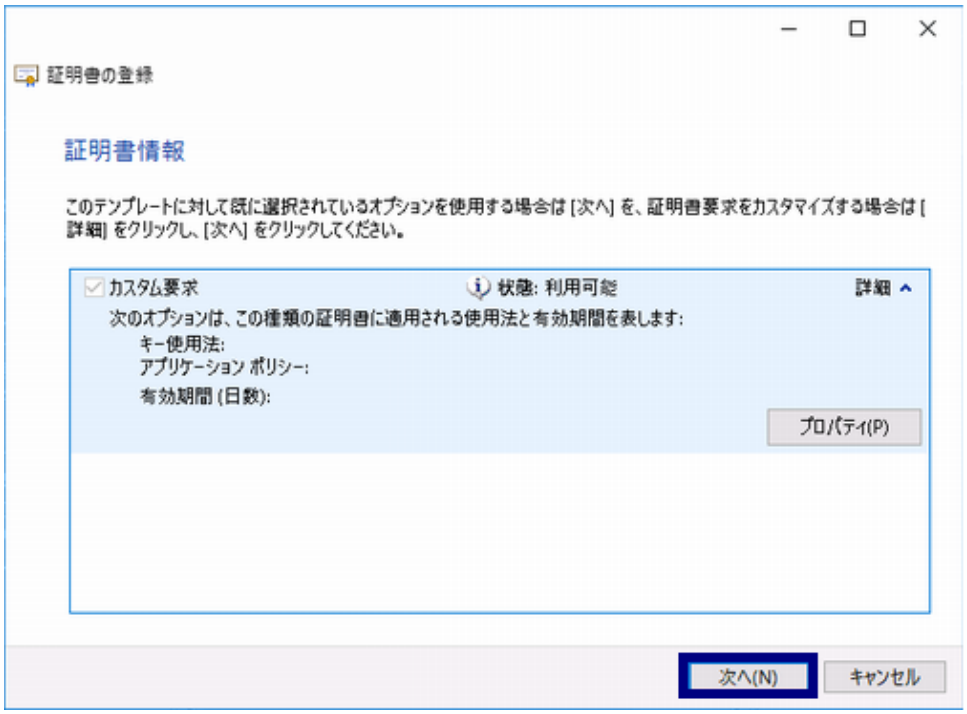


20. 以下を選択し、[OK]ボタンを押下してください。

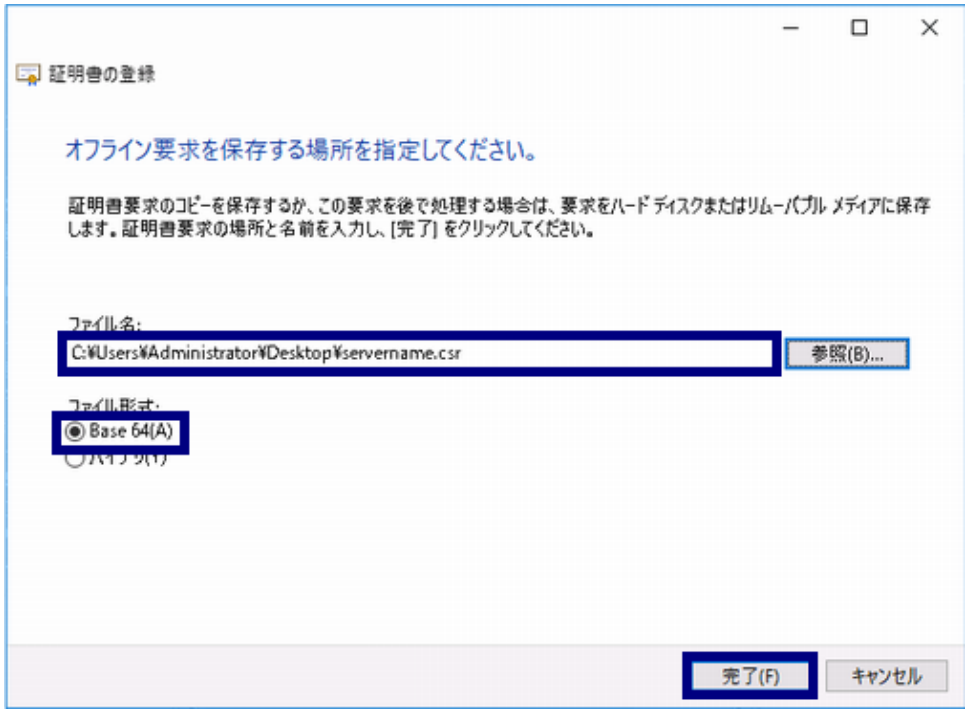
IIS10の場合
暗号化サービスプロバイダー：ECDSA_secp384r1,Microsoft Software Key Storage Provider
IIS7.5～8.5の場合
暗号化サービスプロバイダー：ECDSA_P384,Microsoft Software Key Storage Provider
ハッシュアルゴリズムの選択：sha384



21. [OK]ボタンを押下してください。



22. [ファイル名]に任意のファイル名を含む保存先のフルパスを入力します。
[ファイル形式]は[Base 64]を選択します。
[完了]ボタンを押下してください。



23. 指定した保存場所に生成したCSRが保存されます。

4.証明書の申請から取得まで

CSRを作成後、登録担当者へ送付するための証明書発行申請TSVファイルを作成し申請します。

証明書発行申請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(利用管理者用)**」をご確認ください。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
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。

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.secomtrust.net/～　**←左記URLにアクセスし証明書の取得を行ってください。**

・・・・・