IISにてOUなしのRSA用のCSR作成手順

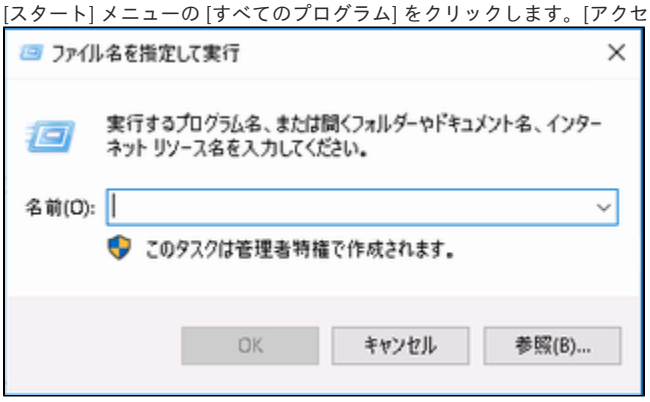
問題

IISにてOUなしのRSA用のCSRを作成時に、OUなしでは処理を進めることができない。
ピリオドを入力してもOUなしで作成することができない。

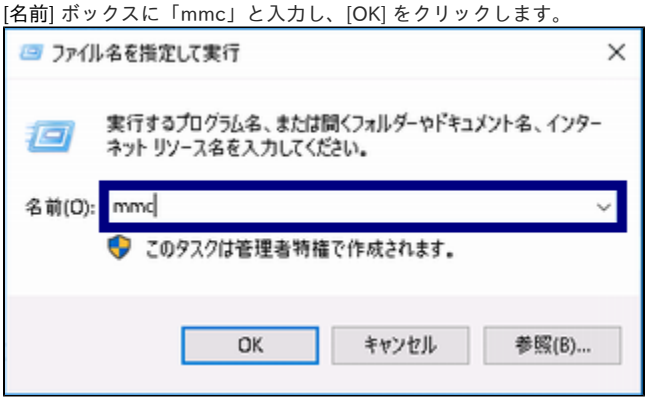
解決方法

OUなしにてRSA用のCSRを作成する手順について説明します。

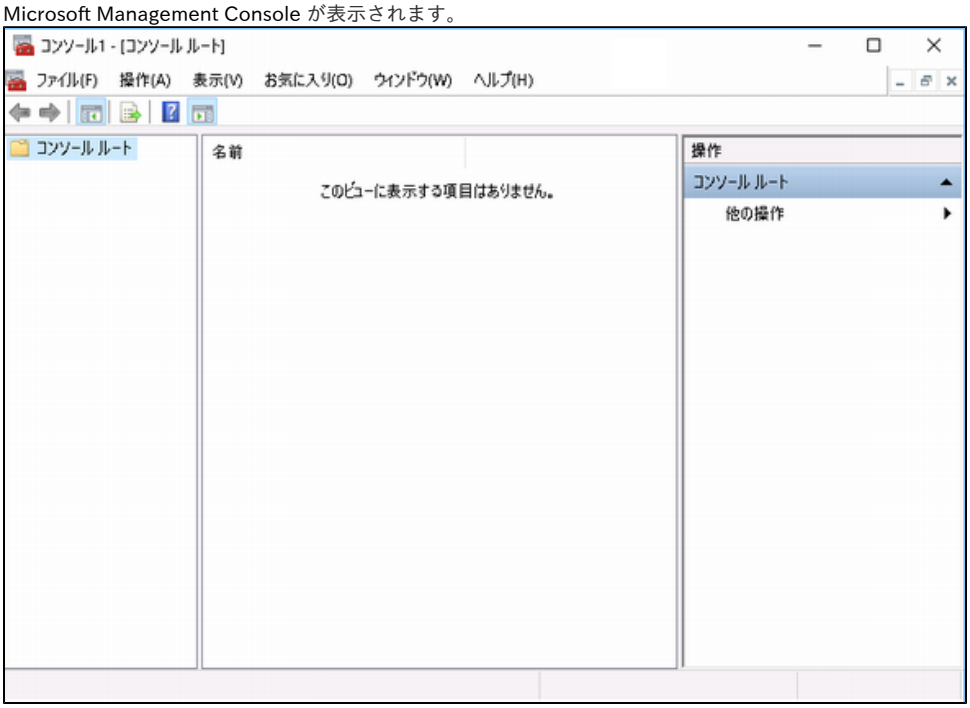
1. [スタート] メニューの [すべてのプログラム] をクリックします。[アクセサリ] をクリックして、[ファイル名を指定して実行] をクリックします。



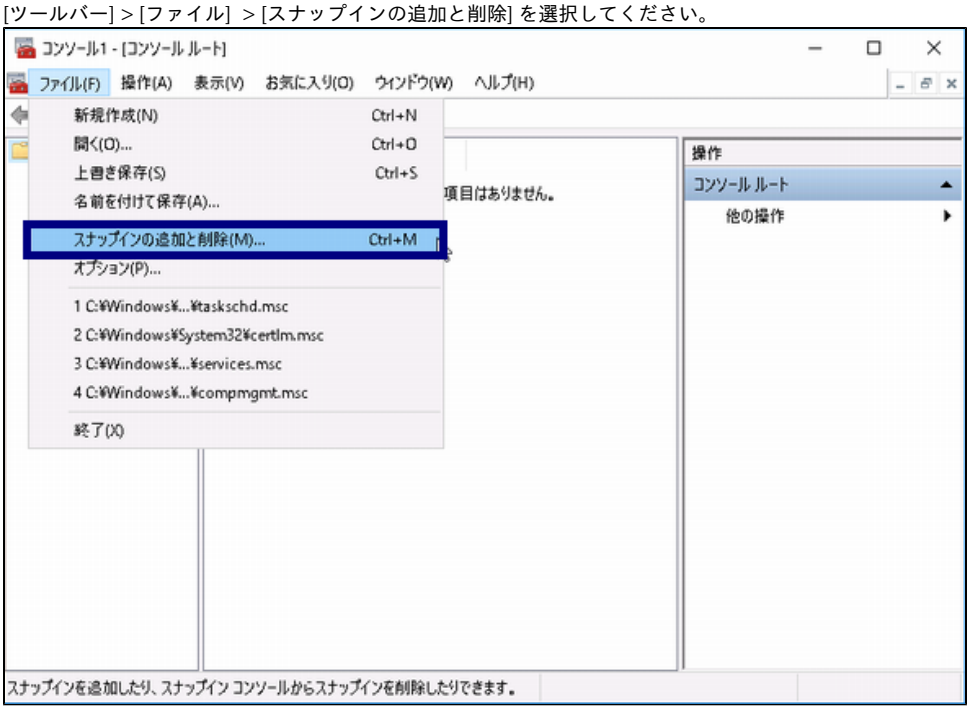
2. [名前] ボックスに「mmc」と入力し、[OK] をクリックします。



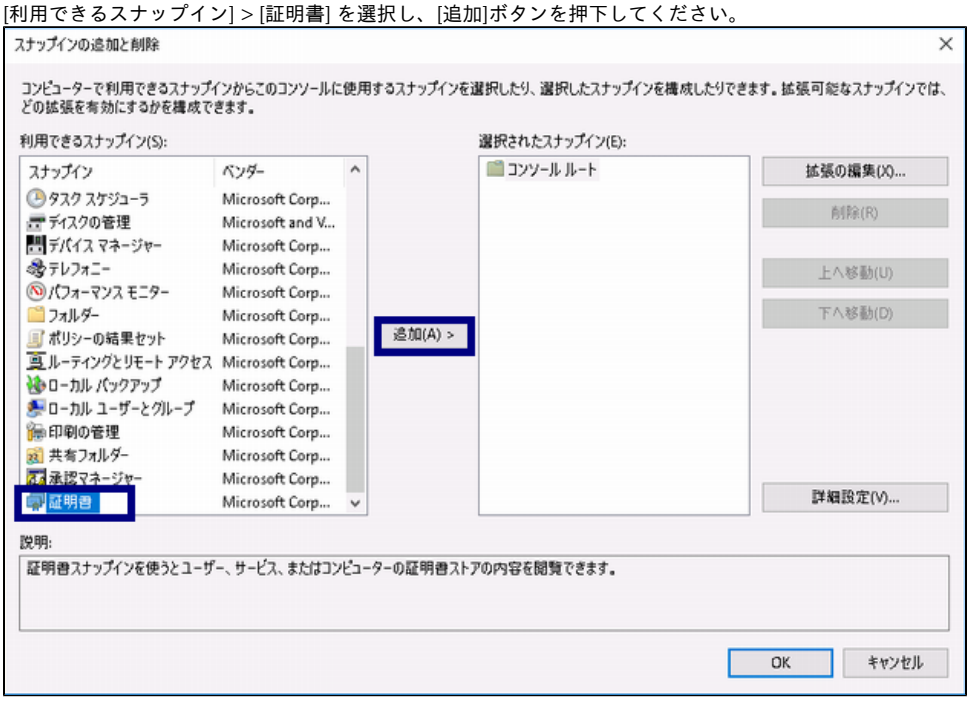
3. Microsoft Management Console が表示されます。



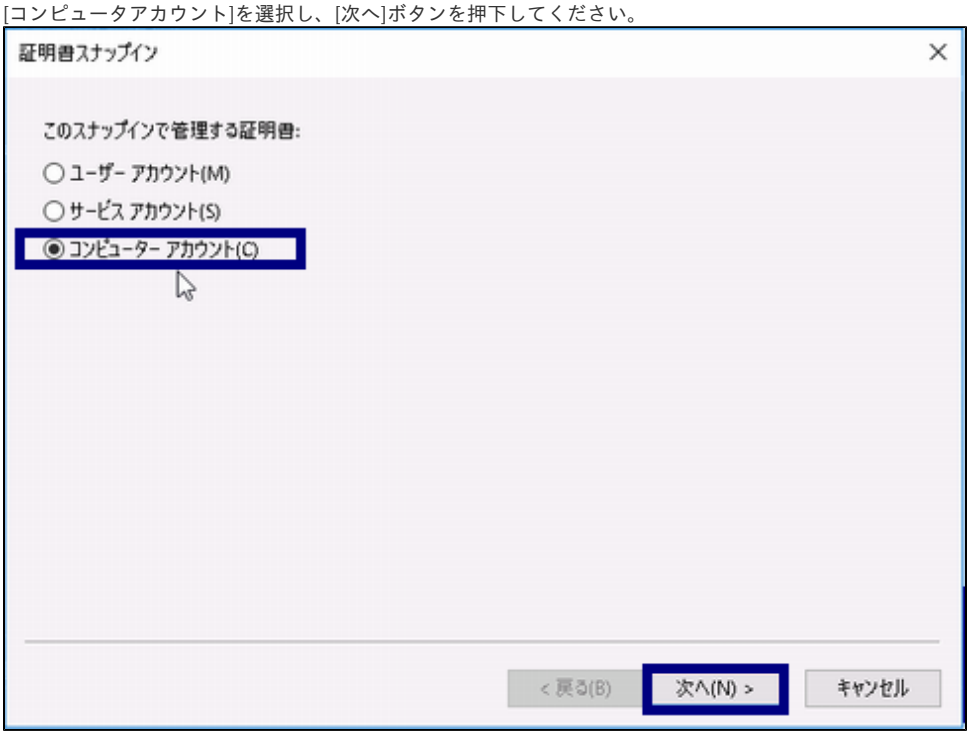
4. [ツールバー] > [ファイル] > [スナップインの追加と削除] を選択してください。



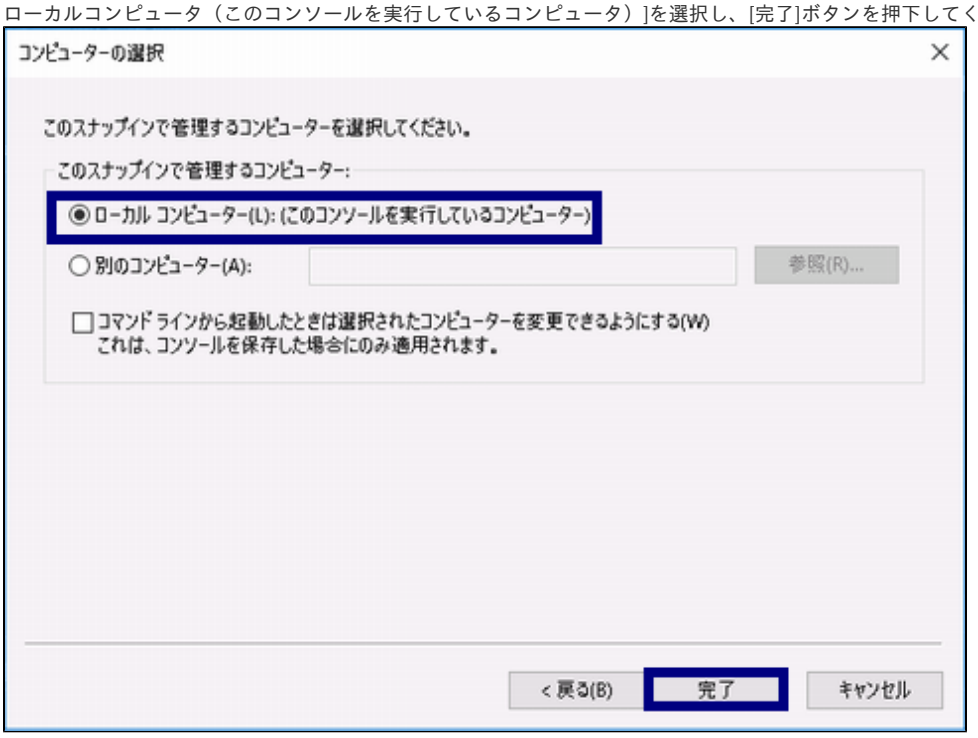
5. [利用できるスナップイン] > [証明書] を選択し、[追加]ボタンを押下してください。



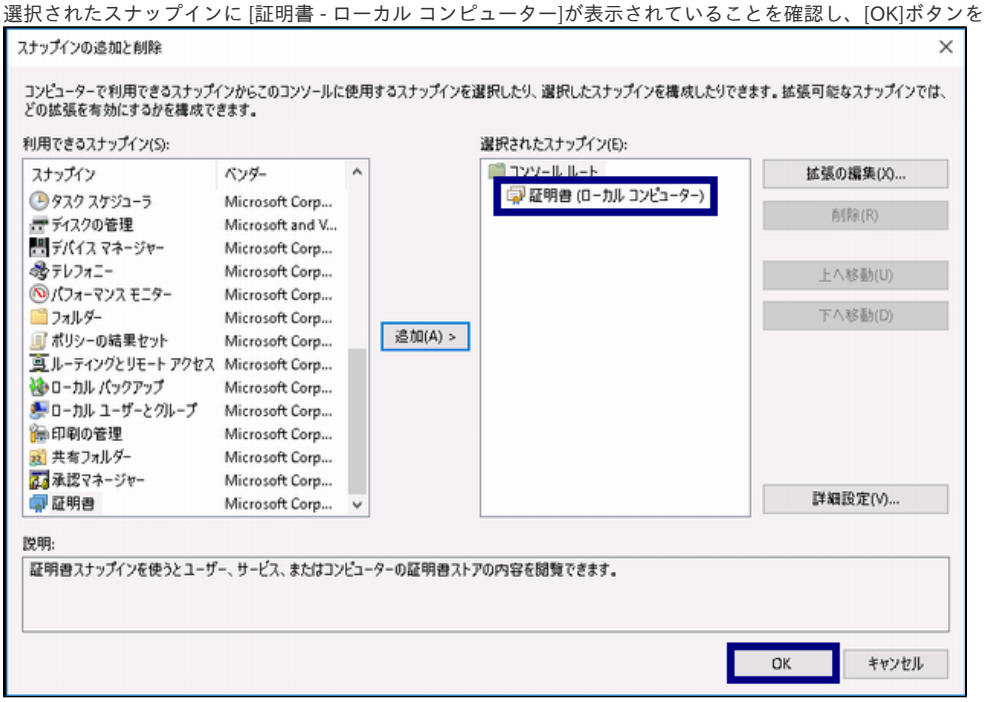
6. [コンピュータアカウント]を選択し、[次へ]ボタンを押下してください。



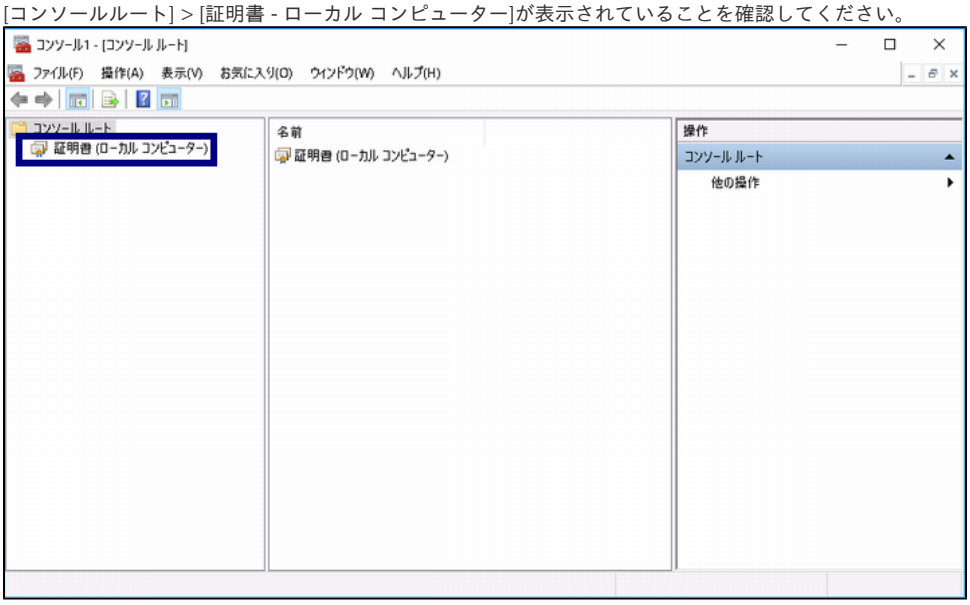
7. ローカルコンピュータ（このコンソールを実行しているコンピュータ）]を選択し、[完了]ボタンを押下してください。



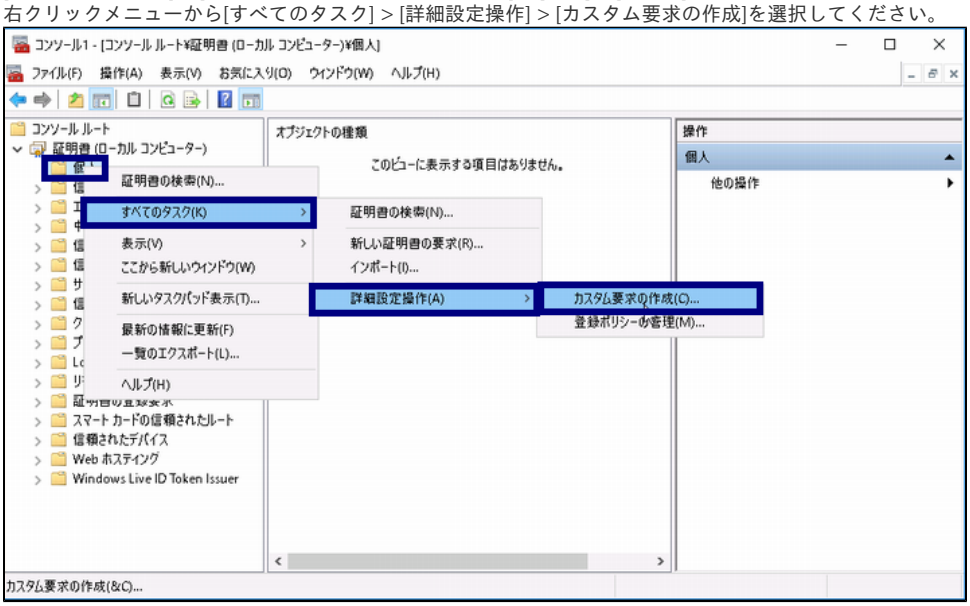
8. 選択されたスナップインに [証明書 - ローカル コンピューター]が表示されていることを確認し、[OK]ボタンを押下してください。



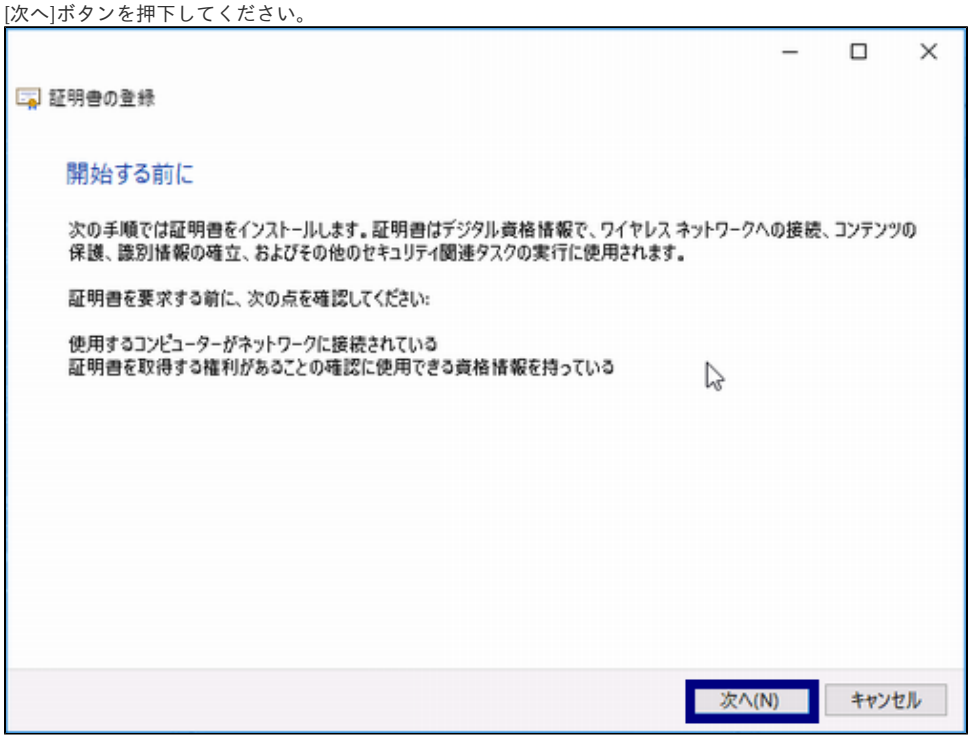
9. [コンソールルート] > [証明書 - ローカル コンピューター]が表示されていることを確認してください。



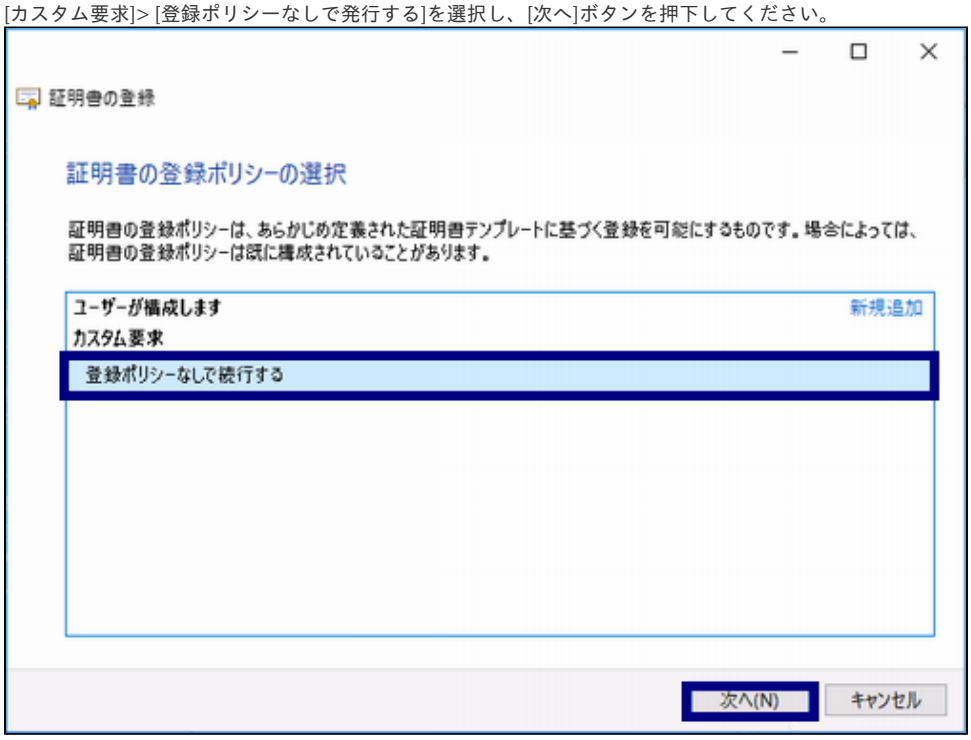
10. [コンソールルート] > [証明書 - ローカル コンピューター] > [個人] > [証明書]を選択し、
右クリックメニューから[すべてのタスク] > [詳細設定操作] > [カスタム要求の作成]を選択してください。



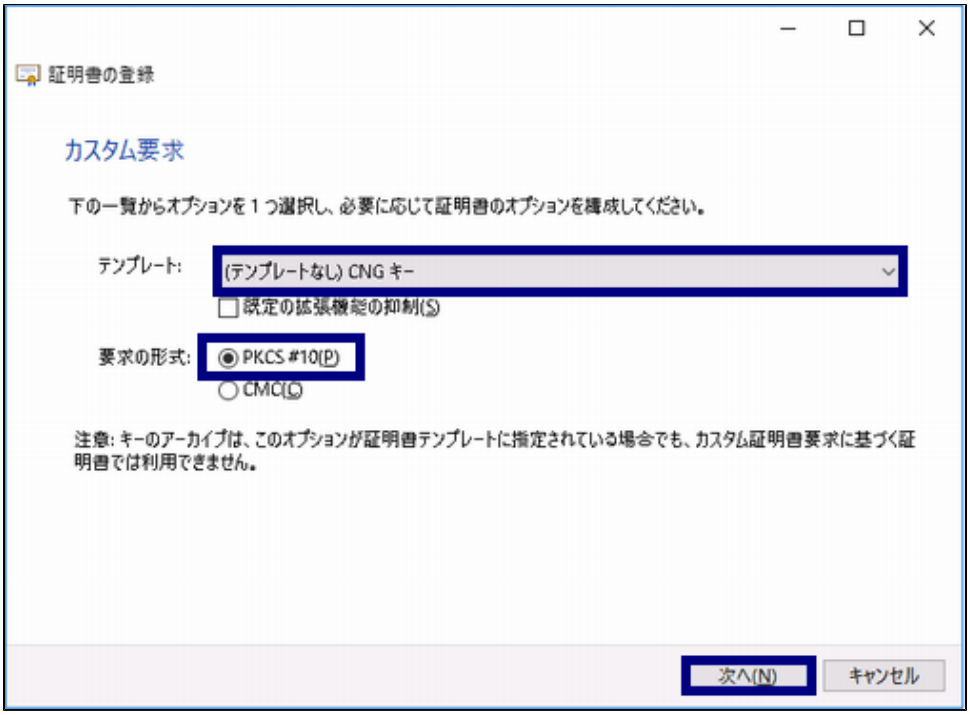
11. [次へ]ボタンを押下してください。



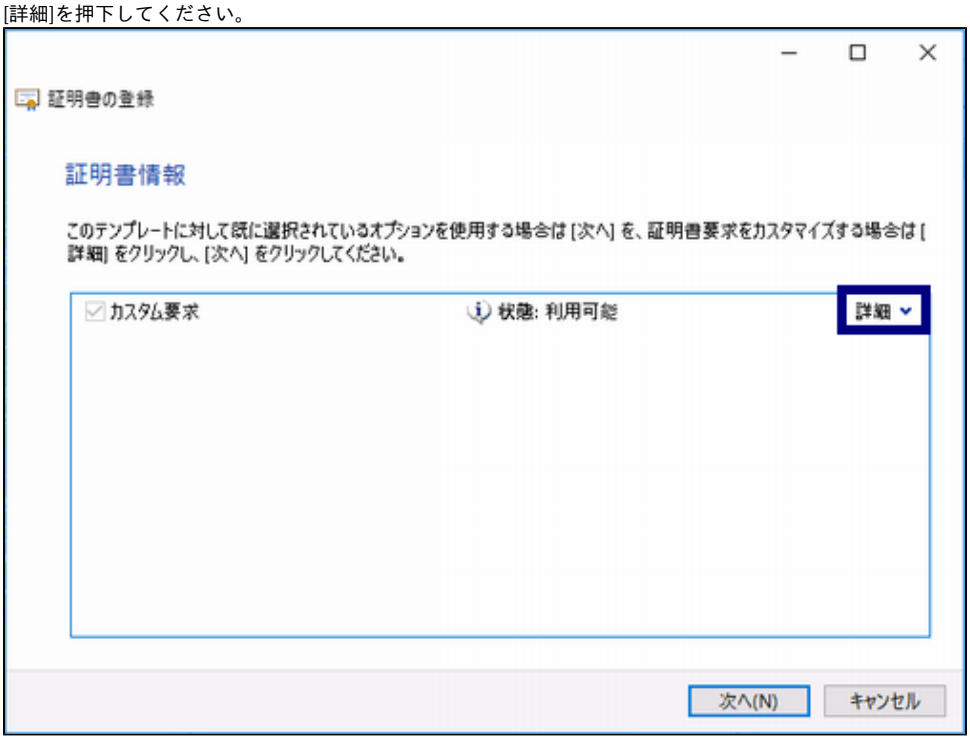
12. [カスタム要求]> [登録ポリシーなしで発行する]を選択し、[次へ]ボタンを押下してください。



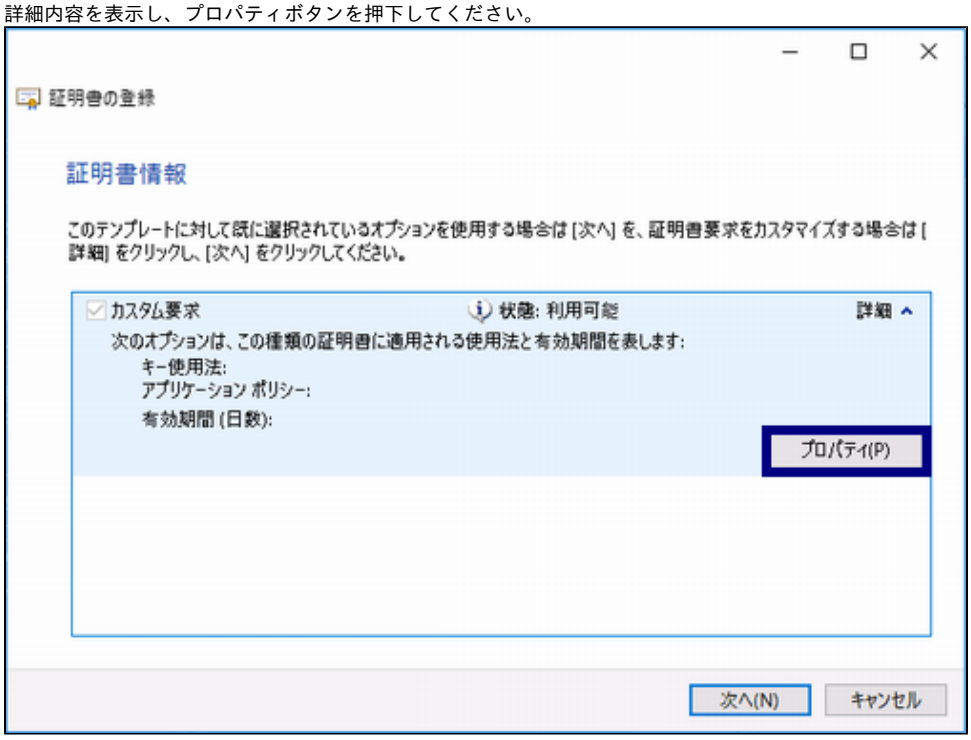
13. 以下を選択し、[次へ]ボタンを押下してください。
テンプレート：[（テンプレートなし）CNGキー]
要求の形式　：PKCS#10



14. [詳細]を押下してください。

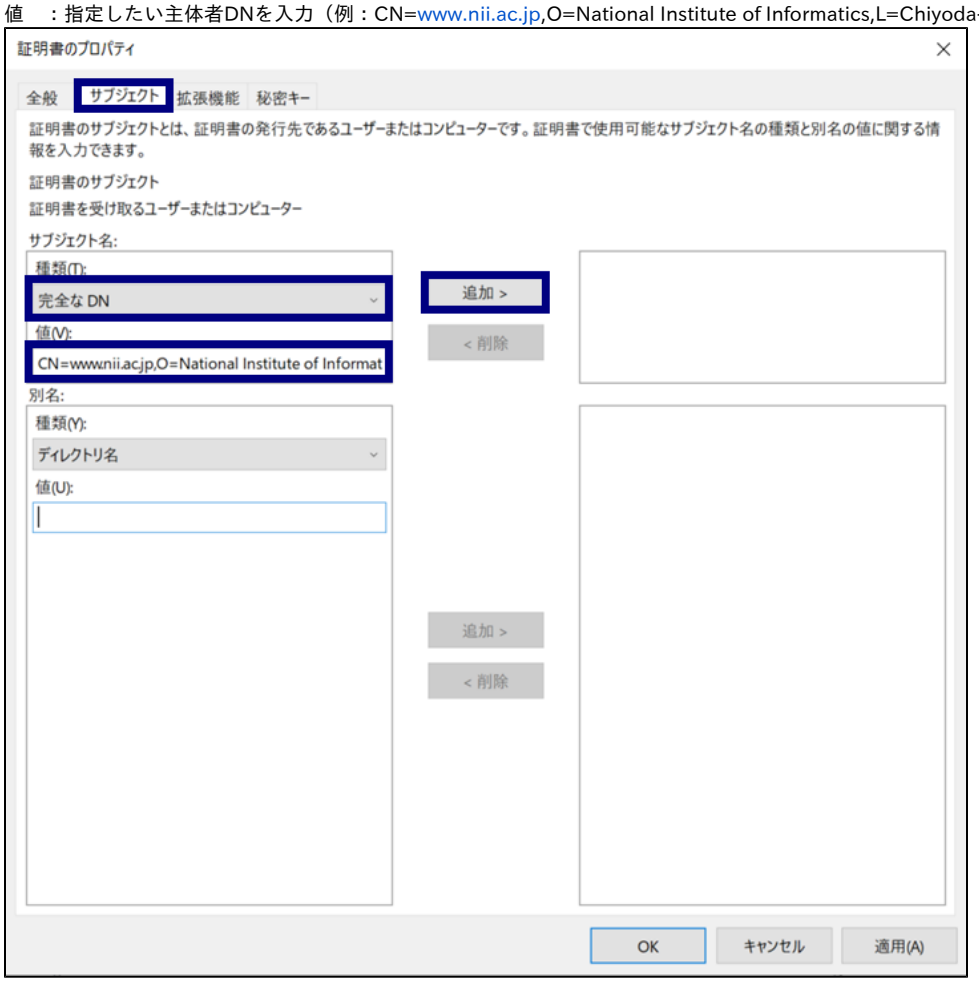


15. 詳細内容を表示し、プロパティボタンを押下してください。

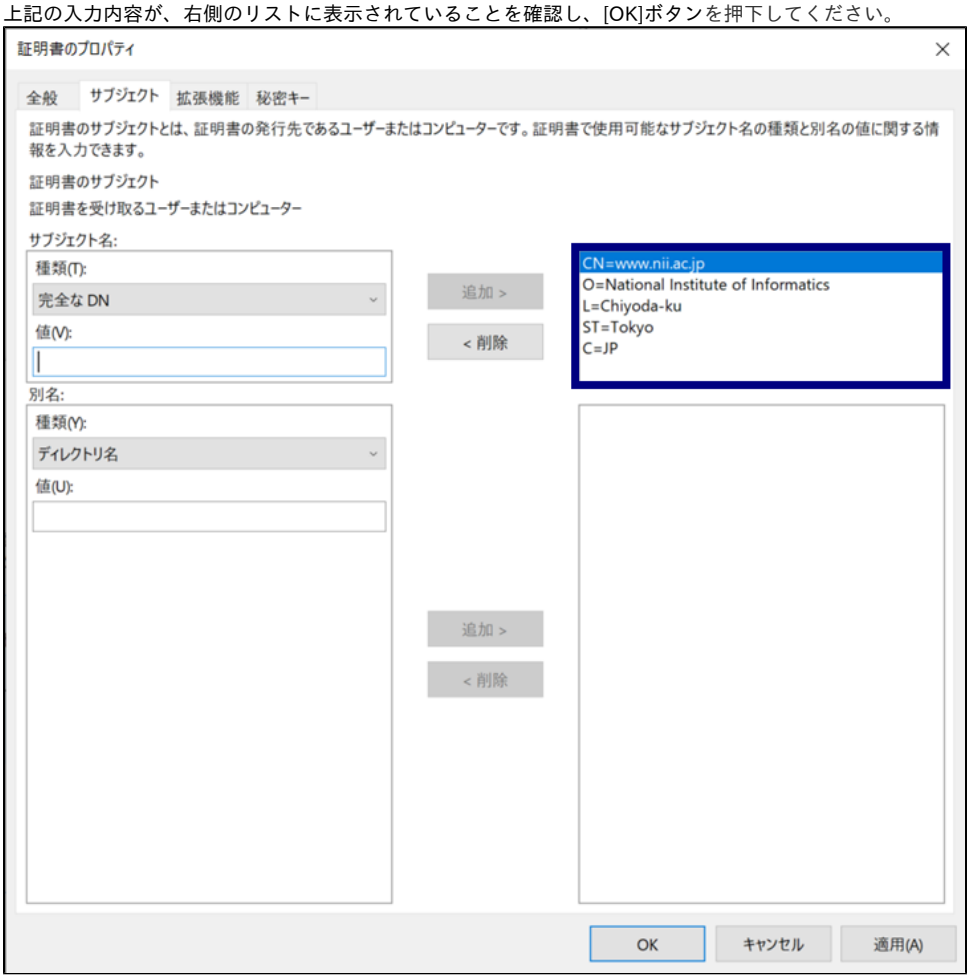


16. サブジェクトタブを選択後、以下を選択し、[追加]ボタンを押下してください。

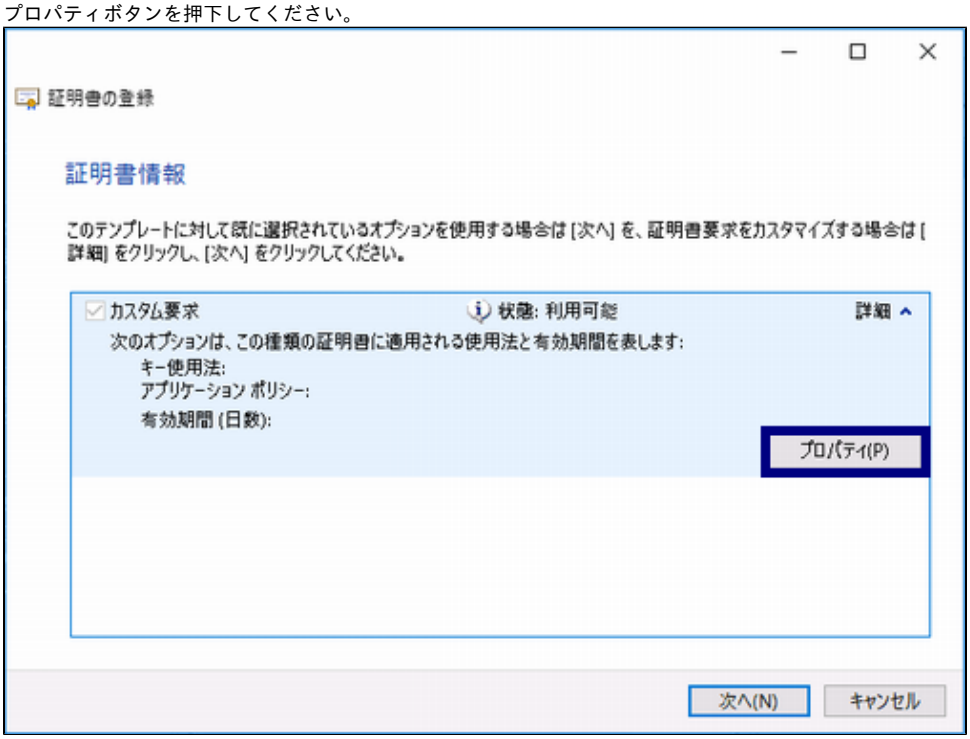
種類：「完全なDN」
値　：指定したい主体者DNを入力（例：CN=www.nii.ac.jp,O=National Institute of Informatics,L=Chiyoda-ku,ST=Tokyo,C=JP）



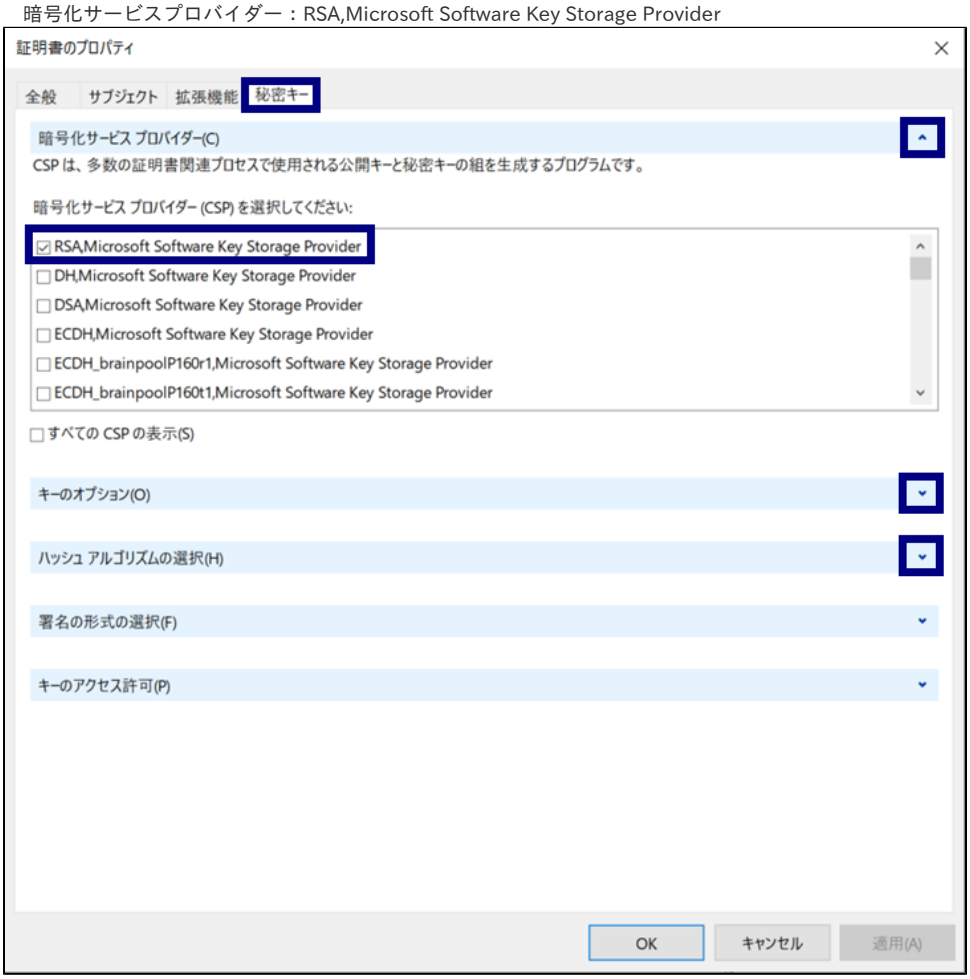
17. 上記の入力内容が、右側のリストに表示されていることを確認し、[OK]ボタンを押下してください。



18. プロパティボタンを押下してください。



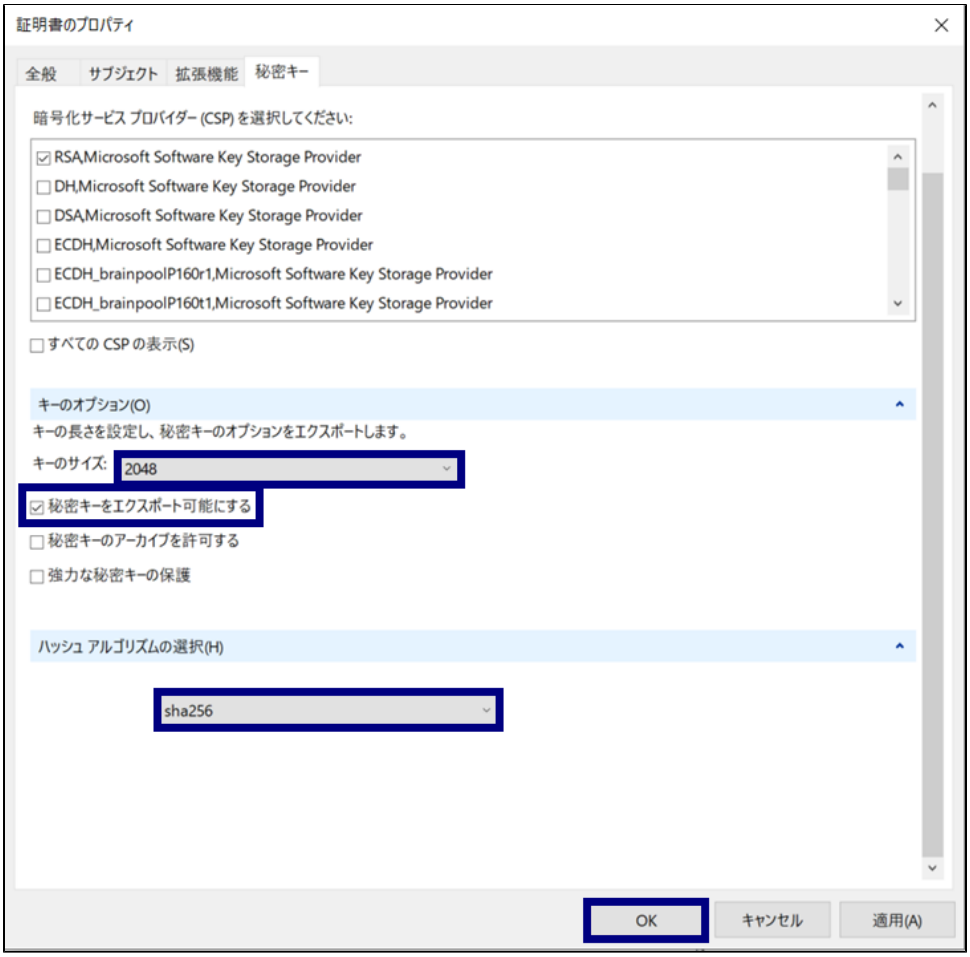
19. 秘密キータブを選択してください。
暗号化サービスプロバイダーとハッシュアルゴリズムの選択の詳細を表示してください。
以下の暗号化サービスプロバイダーにチェックを入れてください。
暗号化サービスプロバイダー：RSA,Microsoft Software Key Storage Provider



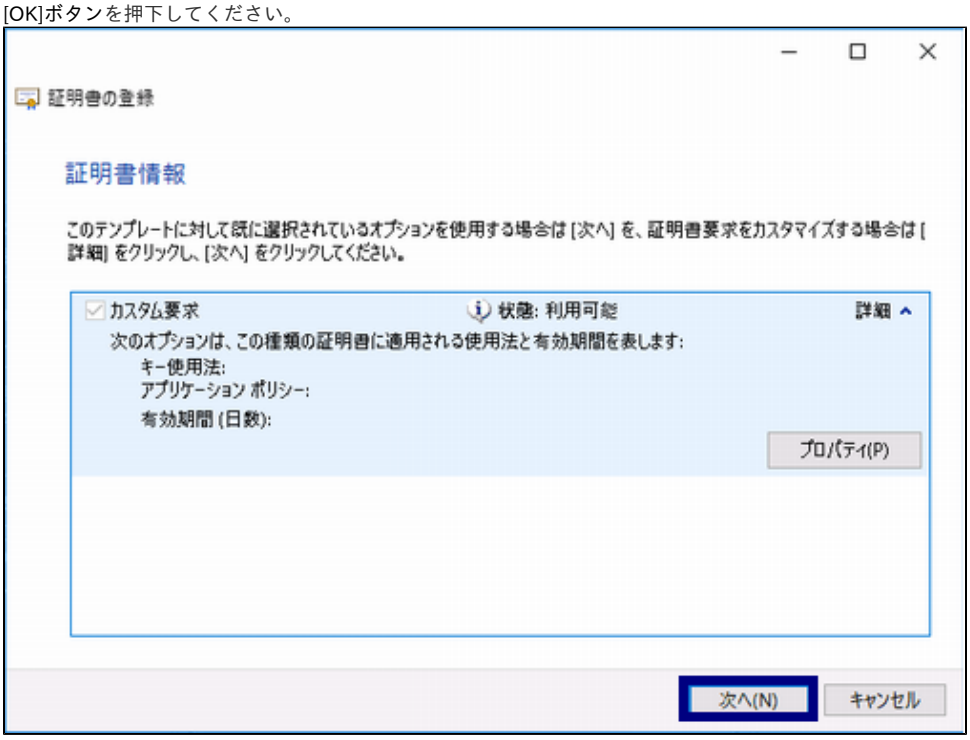
20. 以下を選択し、[OK]ボタンを押下してください。

キーのオプション（O）
キーサイズ：2048
秘密キーにエクスポートを可能にするにチェック

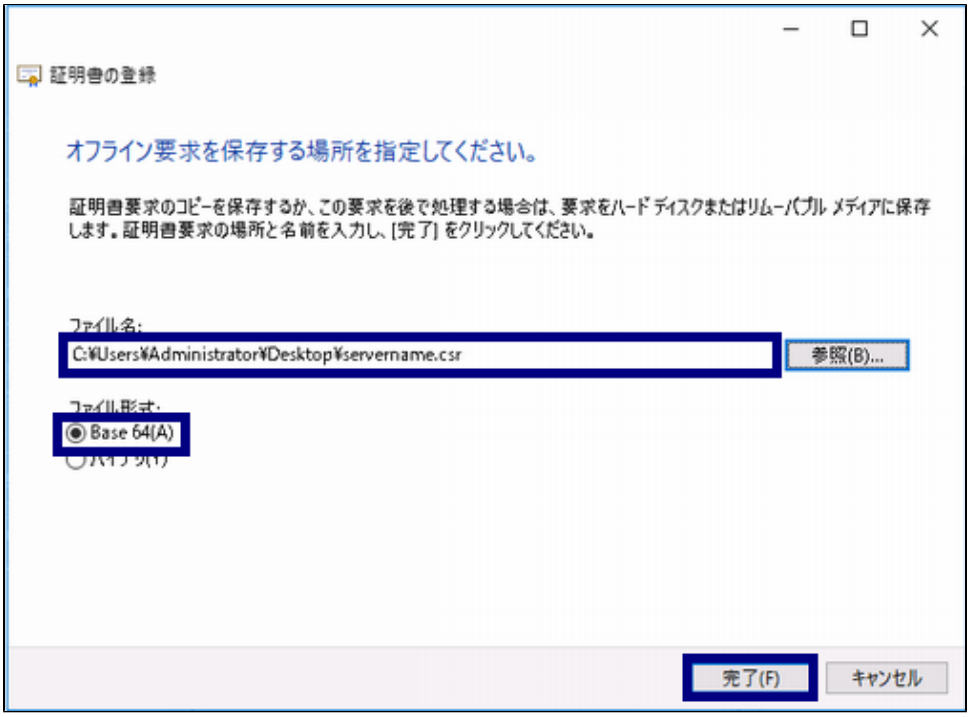
ハッシュアルゴリズムの選択（H）
sha256



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。

証明書のインストールは下記マニュアルより行うことができます。
IIS8.0・IIS8.5編：https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26192405
IIS10.0編：https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=26192446

参照箇所としましては
・「1-2-2. ルートCA証明書のインストール」では【サーバー証明書(sha256WithRSAEncryption)利用の場合】
・「1-2-3. 中間CA証明書のインストール」では【RSA認証局　中間CA証明書をインストールする場合】
・「1-2-4. サーバ証明書のインストール」では「CSRをIISで作成した場合(ECDSA)」
を参照してください。