

IISにてOUなしのRSA用のCSR作成手順

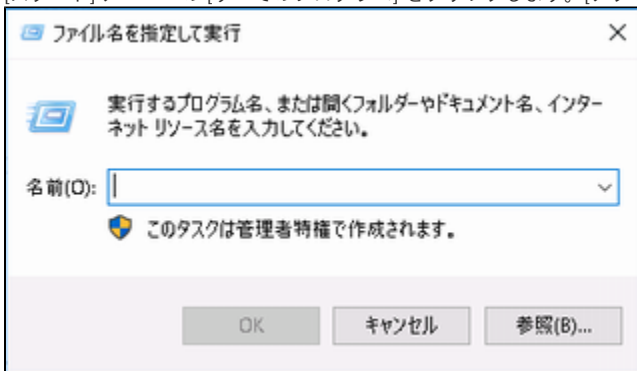
問題

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。
ペリオドを入力してもOUなしで作成することができない。

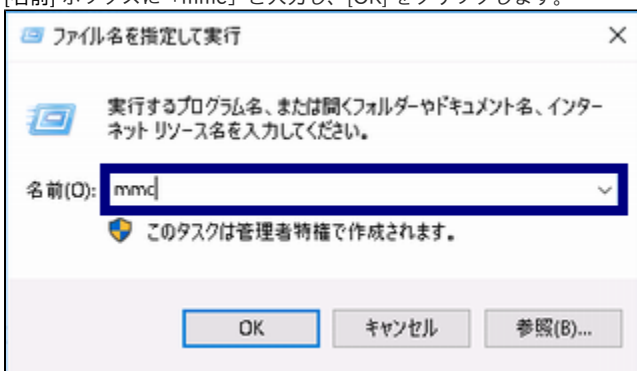
解決方法

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。

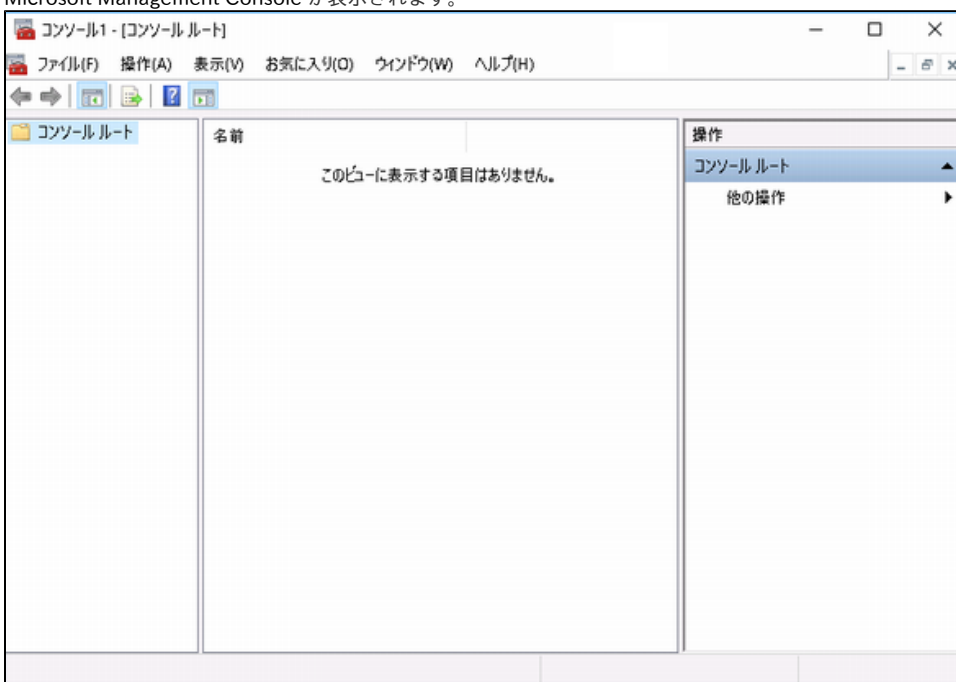
1. [スタート] メニューの [すべてのプログラム] をクリックします。[アクセサリ] をクリックして、[ファイル名を指定して実行] をクリックします。



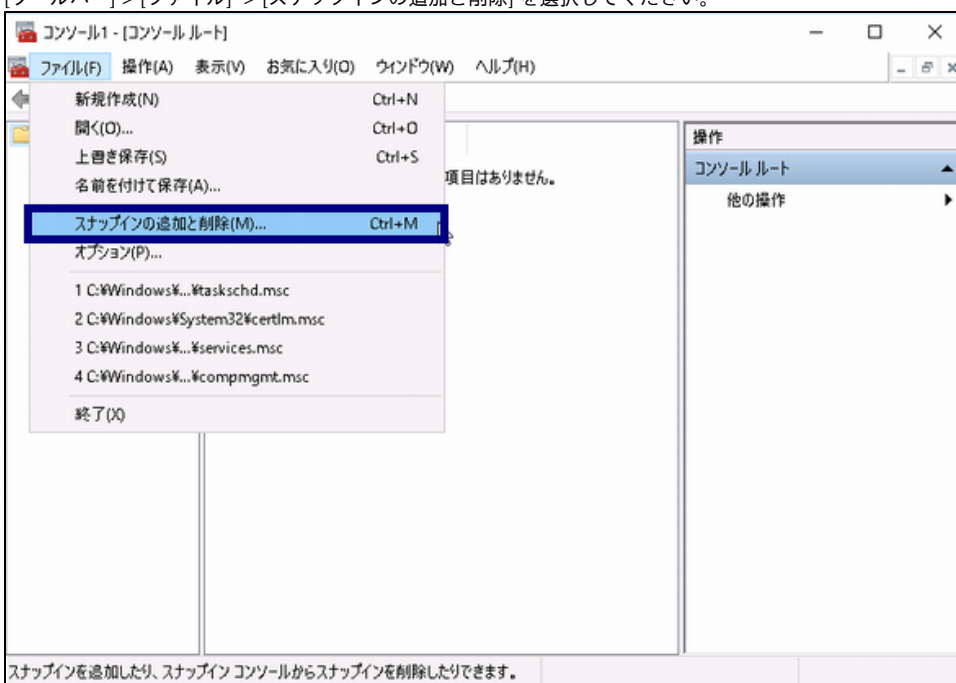
2. [名前] ボックスに「mmc」と入力し、[OK] をクリックします。



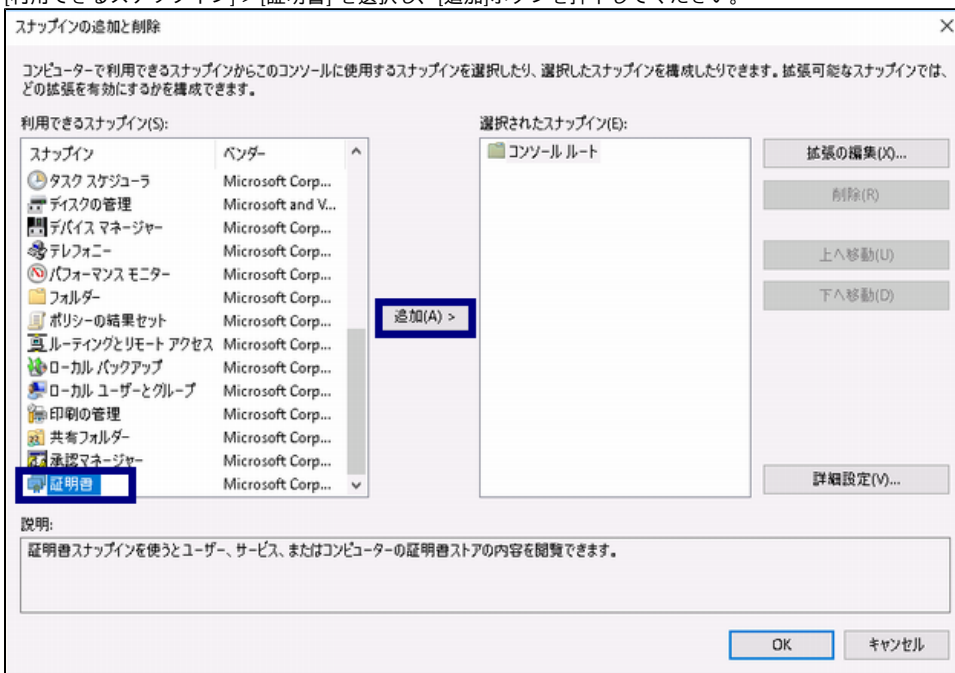
3. Microsoft Management Console が表示されます。



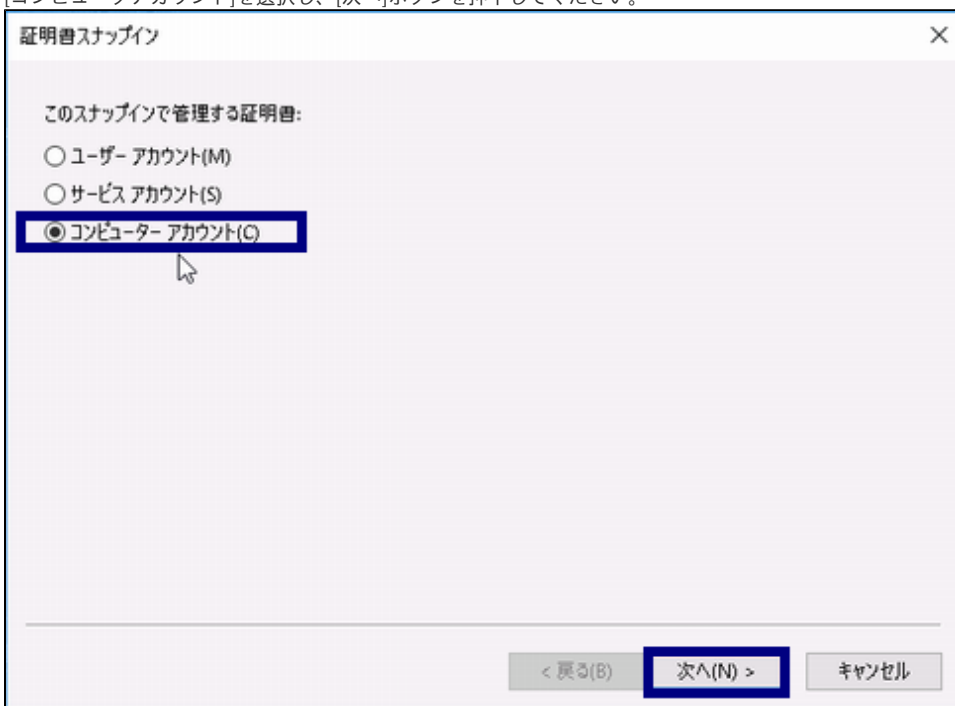
4. [ツールバー] > [ファイル] > [スナップインの追加と削除] を選択してください。



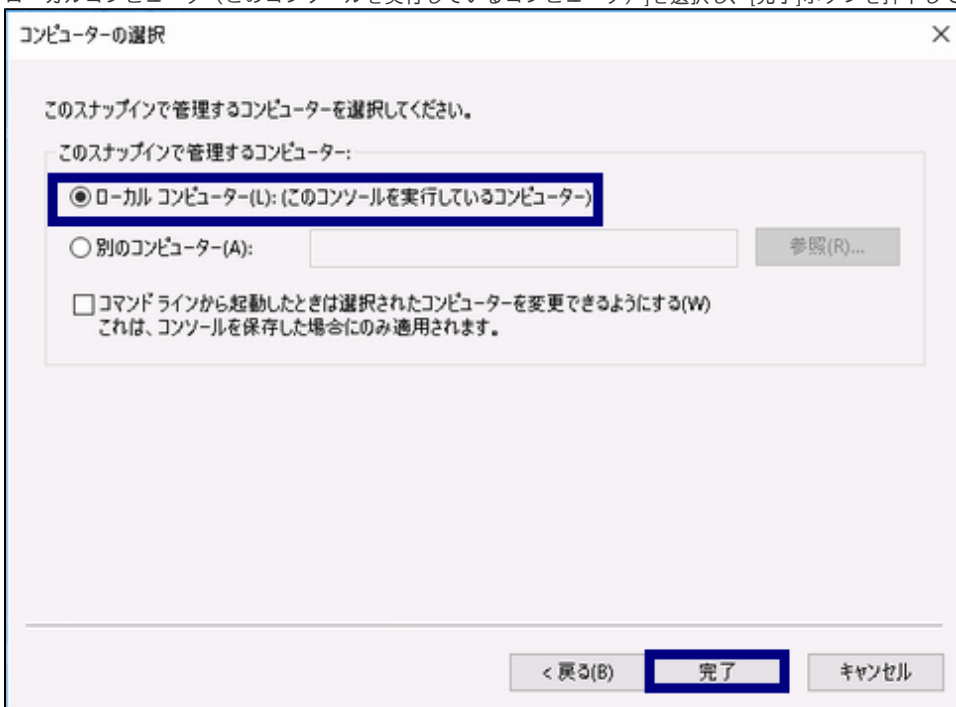
5. [利用できるスナップイン] > [証明書] を選択し、[追加]ボタンを押下してください。



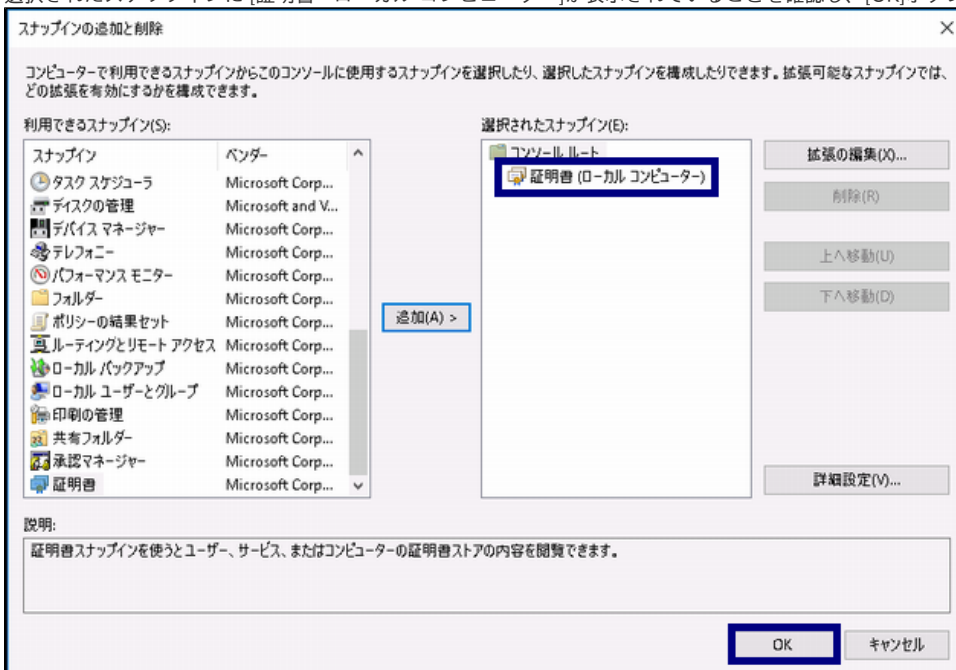
6. [コンピュータアカウント]を選択し、[次へ]ボタンを押下してください。



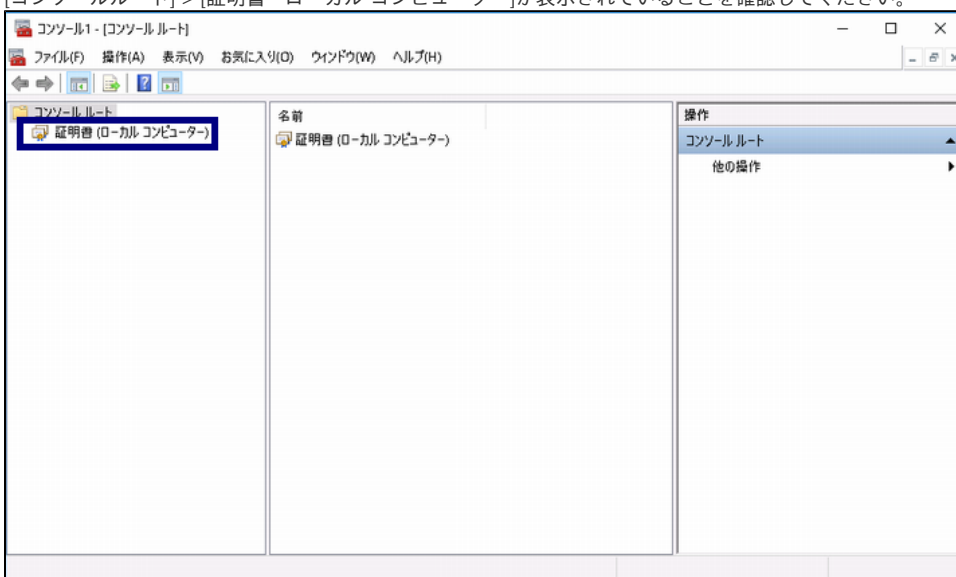
7. ローカルコンピュータ（このコンソールを実行しているコンピュータ）を選択し、[完了]ボタンを押下してください。



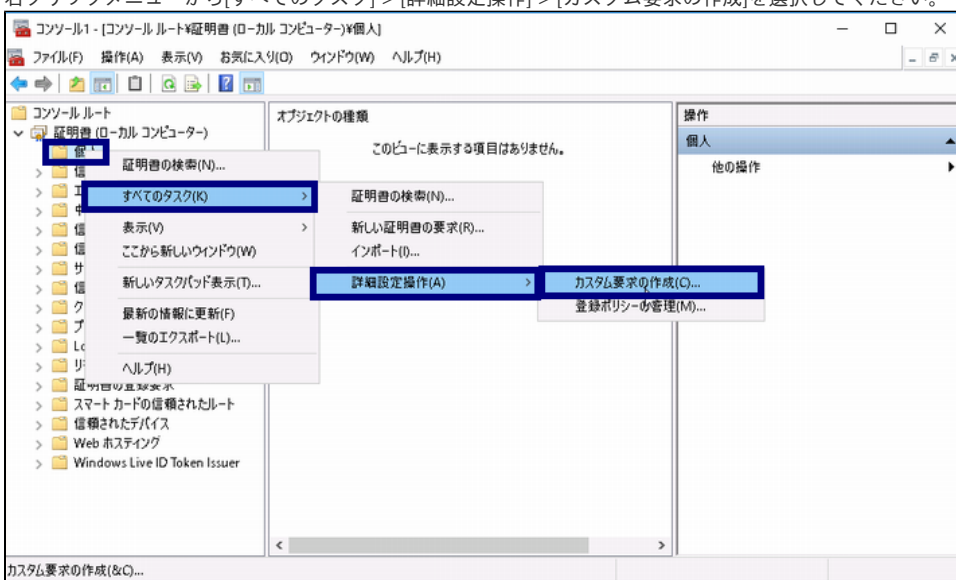
8. 選択されたスナップインに [証明書 - ローカル コンピューター] が表示されていることを確認し、[OK]ボタンを押下してください。



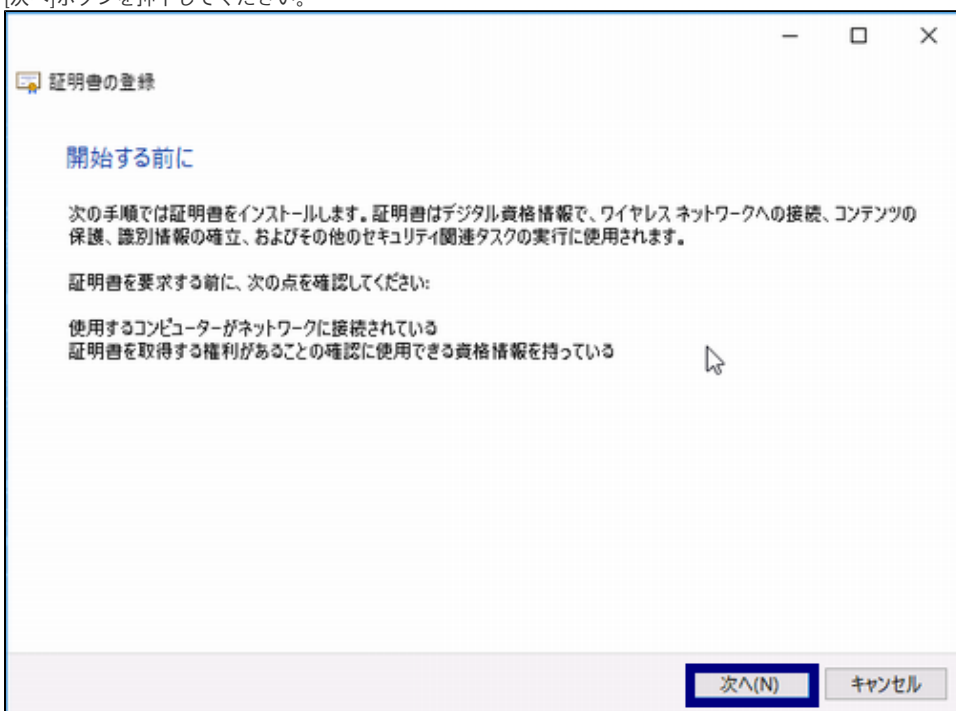
9. [コンソールルート] > [証明書 - ローカル コンピューター]が表示されていることを確認してください。



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。



証明書登録

開始する前に

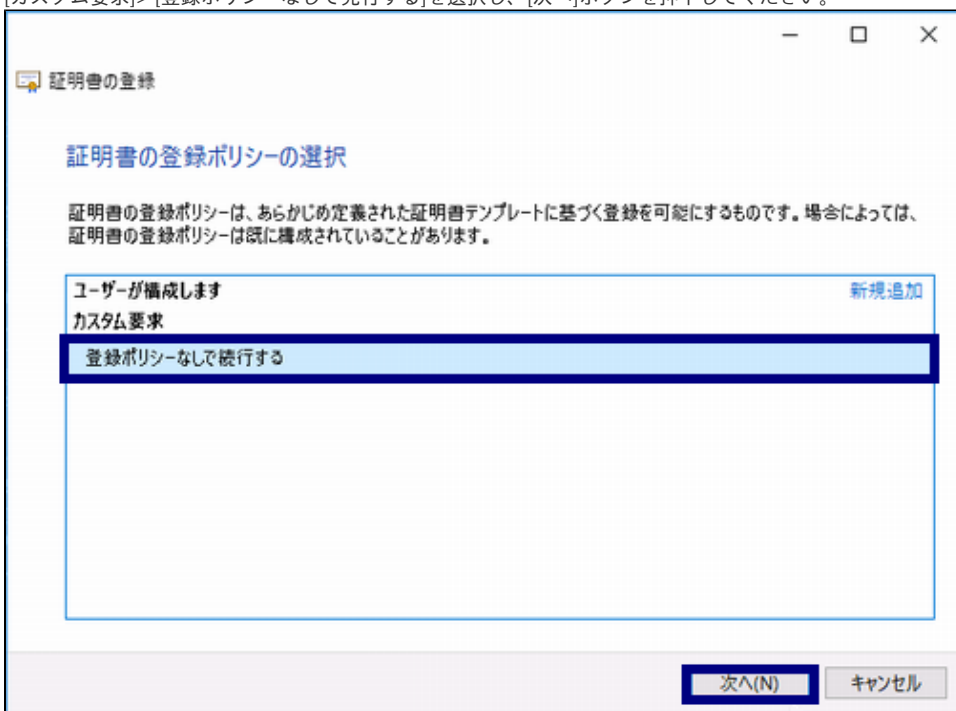
次の手順では証明書をインストールします。証明書はデジタル資格情報で、ワイヤレス ネットワークへの接続、コンテンツの保護、識別情報の確立、およびその他のセキュリティ関連タスクの実行に使用されます。

証明書を要求する前に、次の点を確認してください:

- 使用するコンピューターがネットワークに接続されている
- 証明書を取得する権利があることの確認に使用できる資格情報を持っている

次へ(N) キャンセル

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。



証明書登録

証明書の登録ポリシーの選択

証明書の登録ポリシーは、あらかじめ定義された証明書テンプレートに基づく登録を可能にするものです。場合によっては、証明書の登録ポリシーは既に構成されていることがあります。

ユーザーが構成します 新規追加

カスタム要求

- 登録ポリシーなしで発行する

次へ(N) キャンセル

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

証明書登録

カスタム要求

下の一覧からオプションを1つ選択し、必要に応じて証明書のオプションを構成してください。

テンプレート: (テンプレートなし) CNG キー

☐ 既定の拡張機能の抑制(S)

要求の形式: ☒ PKCS #10(P) ☐ CMC(Q)

注意: キーのアーカイブは、このオプションが証明書テンプレートに指定されている場合でも、カスタム証明書要求に基づく証明書では利用できません。

次へ(N) キャンセル

14. [詳細]を押下してください。

証明書登録

証明書情報

このテンプレートに対して既に選択されているオプションを使用する場合は [次へ] を、証明書要求をカスタマイズする場合は [詳細] をクリックし、[次へ] をクリックしてください。

☒ カスタム要求	状態: 利用可能	詳細
--	----------	----

次へ(N) キャンセル

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。

証明書登録

証明書情報

このテンプレートに対して既に選択されているオプションを使用する場合は [次へ] を、証明書要求をカスタマイズする場合は [詳細] をクリックし、[次へ] をクリックしてください。

☒ カスタム要求 状態: 利用可能 詳細 ^

次のオプションは、この種類の証明書に適用される使用法と有効期間を表します:

- キー使用法:
- アプリケーション ポリシー:
- 有効期間 (日数):

プロパティ(P)

次へ(N) キャンセル

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)

証明書のプロパティ

全般 **サブジェクト** 拡張機能 秘密キー

証明書のサブジェクトとは、証明書の発行先であるユーザーまたはコンピューターです。証明書で使用可能なサブジェクト名の種類と別名の値に関する情報を入力できます。

証明書のサブジェクト

証明書を受け取るユーザーまたはコンピューター

サブジェクト名:

種類(T): **完全な DN** 追加 >

値(V): **CN=www.nii.ac.jp,O=National Institute of Informatics** < 削除

別名:

種類(Y): **ディレクトリ名**

値(U):

追加 >
< 削除

OK キャンセル 適用(A)

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。

証明書のプロパティ

全般 サブジェクト 拡張機能 秘密キー

証明書のサブジェクトとは、証明書の発行先であるユーザーまたはコンピューターです。証明書で使用可能なサブジェクト名の種類と別名の値に関する情報を入力できます。

証明書のサブジェクト
証明書を受け取るユーザーまたはコンピューター

サブジェクト名:

種類(T):
完全な DN

追加 >

< 削除

値(V):

別名:

種類(Y):
ディレクトリ名

追加 >

< 削除

値(U):

CN=www.nii.ac.jp
O=National Institute of Informatics
L=Chiyoda-ku
ST=Tokyo
C=JP

OK キャンセル 適用(A)

18. プロパティボタンを押下してください。

証明書の登録

証明書情報

このテンプレートに対して既に選択されているオプションを使用する場合は [次へ] を、証明書要求をカスタマイズする場合は [詳細] をクリックし、[次へ] をクリックしてください。

☒ カスタム要求 状態: 利用可能 詳細 ^

次のオプションは、この種類の証明書に適用される使用法と有効期間を表します:

キー使用法:
アプリケーション ポリシー:
有効期間 (日数):

プロパティ(P)

次へ(N) キャンセル

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

証明書のプロパティ

全般 サブジェクト 拡張機能 **秘密キー**

暗号化サービス プロバイダー(C) [v]

CSP は、多数の証明書関連プロセスで使用する公開キーと秘密キーの組を生成するプログラムです。

暗号化サービス プロバイダー (CSP) を選択してください:

☒ RSA,Microsoft Software Key Storage Provider

☐ DH,Microsoft Software Key Storage Provider

☐ DSA,Microsoft Software Key Storage Provider

☐ ECDH,Microsoft Software Key Storage Provider

☐ ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider

☐ ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider

☐ すべての CSP の表示(S)

キーのオプション(O) [v]

ハッシュ アルゴリズムの選択(H) [v]

署名の形式の選択(F) [v]

キーのアクセス許可(P) [v]

OK キャンセル 適用(A)

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

証明書のプロパティ

全般 サブジェクト 拡張機能 秘密キー

暗号化サービス プロバイダー (CSP) を選択してください:

- ☒ RSA,Microsoft Software Key Storage Provider
- ☐ DH,Microsoft Software Key Storage Provider
- ☐ DSA,Microsoft Software Key Storage Provider
- ☐ ECDH,Microsoft Software Key Storage Provider
- ☐ ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider
- ☐ ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider

☐ すべての CSP の表示(S)

キーのオプション(O)

キーの長さを設定し、秘密キーのオプションをエクスポートします。

キーのサイズ: 2048

☒ 秘密キーをエクスポート可能にする

☐ 秘密キーのアーカイブを許可する

☐ 強力な秘密キーの保護

ハッシュ アルゴリズムの選択(H)

sha256

OK キャンセル 適用(A)

21. [OK]ボタンを押下してください。

証明書の登録

証明書情報

このテンプレートに対して既に選択されているオプションを使用する場合は [次へ] を、証明書要求をカスタマイズする場合は [詳細] をクリックし、[次へ] をクリックしてください。

☒ カスタム要求 状態: 利用可能 詳細 ^

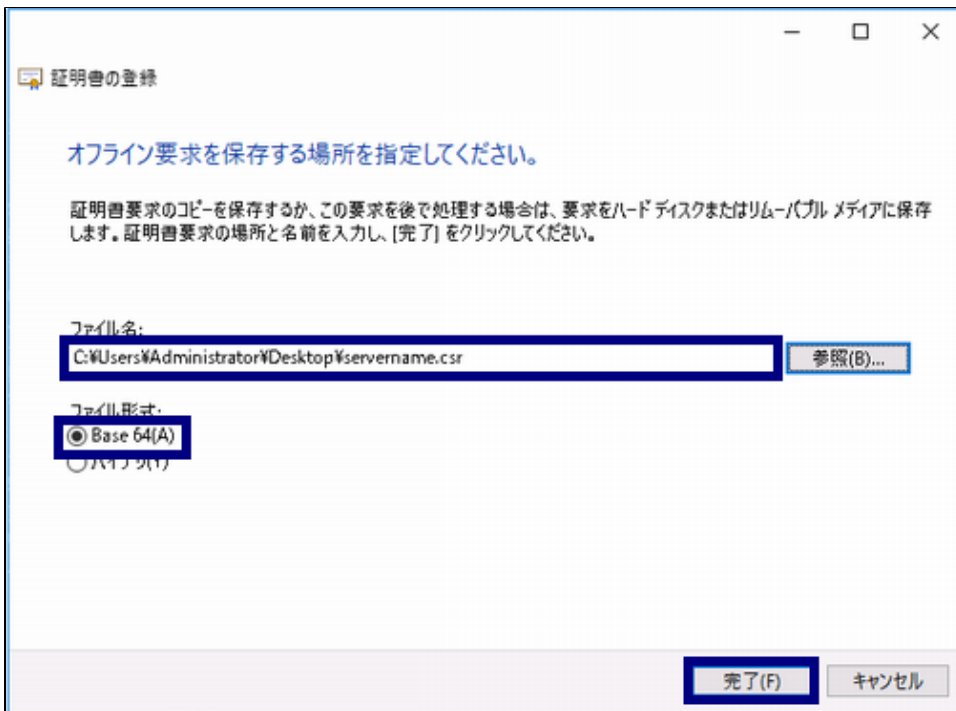
次のオプションは、この種類の証明書に適用される使用法と有効期間を表します:

キー使用法:
アプリケーション ポリシー:
有効期間 (日数):

プロパティ(P)

次へ(N) キャンセル

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(shash256WithRSAEncryption)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。