# IIS10.0編

| 改版履歴 | | | |
|---|---|---|---|
| 版数 | 日付 | 内容 | 担当 |
| V.1.0 | 2018/2/26 | 初版 | NII |
| V.1.1 | 2018/3/26 | CT対応版の中間CA証明書について説明を追加 | NII |
| V.1.2 | 2018/7/9 | ECDSA対応版のルート証明書、中間CA証明書について説明を追加 | NII |
| V.2.4 | 2019/4/22 | ECC認証局 中間CA証明書の名称を変更 | NII |
| V2.5 | 2020/1/31 | 画像と文字の位置を修正 | NII |
| V.2.6 | 2020/4/13 | 中間CA証明書のファイル名を修正 | NII |
| V.2.7 | 2020/8/25 | 中間CA証明書の記載内容を修正 | NII |
| V.2.8 | 2020/12/22 | 中間CA証明書を修正 | NII |

**目次**

**1. IIS10.0 によるサーバ証明書の利用**
1-1. 前提条件
1-2. 証明書のインストール
1-2-1. 事前準備
1-2-2. ルートCA証明書のインストール
1-2-3. 中間CA証明書のインストール
1-2-4. サーバ証明書のインストール
1-3. サーバ証明書の置き換えインストール
1-4. 起動確認

# 1. IIS10.0 によるサーバ証明書の利用

## 1-1. 前提条件

IIS10.0 (以下IIS)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。
適宜、サーバ証明書をインストールする利用管理者様の環境により、読み替えをお願いします。
（本マニュアルではWindows Server2016、OpenSSL1.0.1eでCSRを作成し、IIS10.0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<br>2. 証明書をインストールする端末にIIS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
RSA鍵の場合、2048bit
ECDSA鍵の場合、384bit
にしてください。

## 1-2. 証明書のインストール

本章ではIIS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。

### 1-2-1. 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。

| **事前準備** |
|---|

1. [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。
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（証明書の発行日時が2020年12月25日0時以降の場合）：https://repo1.secomtrust.net/sppca/nii/odca4/index.html
サーバー証明書 RSA認証局　中間CA証明書
「NII Open Domain CA - G7 RSA(SC Organization Validation CA) CA証明書(nii-odca4g7rsa.cer)」
サーバー証明書 ECC認証局　中間CA証明書
「NII Open Domain CA - G7 ECC(SC Organization Validation CA) CA証明書(nii-odca4g7ecc.cer)」

●リポジトリ（証明書の発行日時が2020年12月25日0時以前の場合）：https://repo1.secomtrust.net/sppca/nii/odca3/index.html
SHA-2認証局CT対応版サーバ証明書
「国立情報学研究所 オープンドメイン SHA-2認証局 CT対応版 CA証明書(nii-odca3sha2ct.cer)」
ECC認証局サーバ証明書
「国立情報学研究所 オープンドメイン ECC認証局 CA証明書(nii-odca3ecdsa201903.cer)」

【サーバー証明書(ecdsa-with-SHA384)をインストールする場合】
ECC認証局 中間CA証明書 をnii-odca3ecdsa.cerという名前で保存したと仮定して以降記載します。

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]のタブを選択します。

発行先[Security Communication RootCA2]、発行者[Security Communication RootCA2]の証明書、または
発行先[Security Communication ECC RootCA1]、発行者[Security Communication ECC RootCA1]の証明書がある場合は、ルートCA証明書の取得は不要です。
無い場合は、以下、「1-2-2 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、インストールを行ってください。

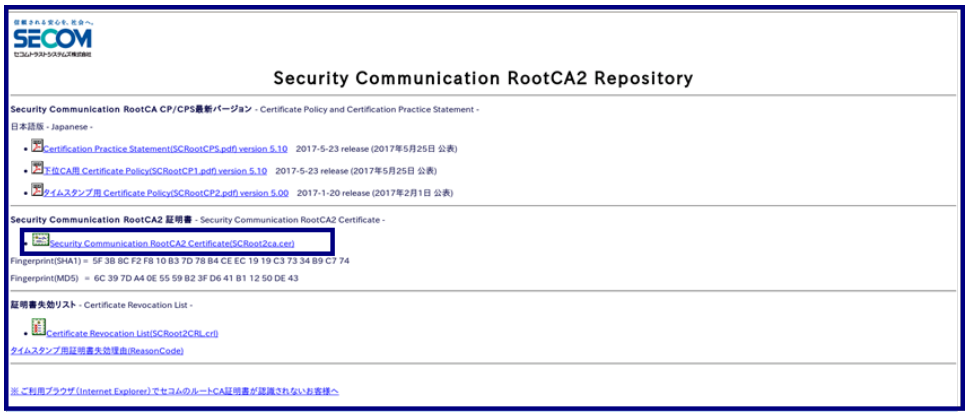
## 1-2-2. ルートCA証明書のインストール

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。
※ [1-2-1 事前準備]でルートCA証明書が存在した場合は、本手続きは不要です。次の「1-2-3 中間CA証明書のインストール」へ進んでください。

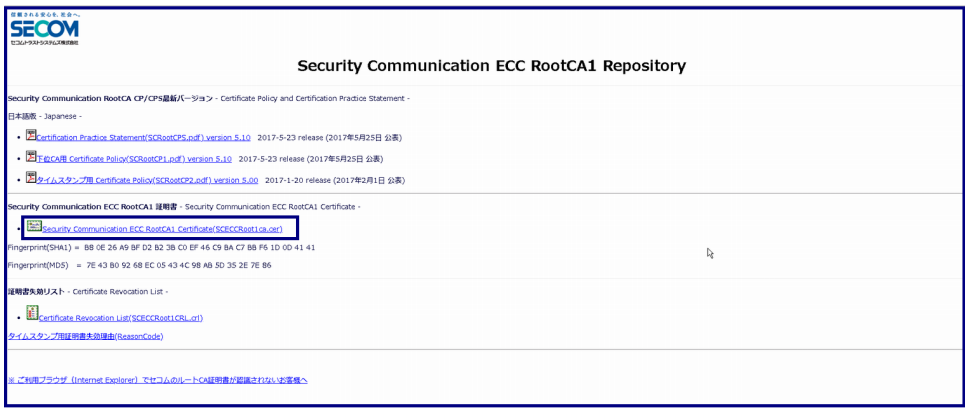
**ルートCA証明書のインストール**

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

【サーバー証明書(sha256WithRSAEncryption)利用の場合】
URL：https://repository.secomtrust.net/SC-Root2/index.html
「Security Communication RootCA2 Certificate(SCRoot2ca.cer)」と記述されたリンクを選択してください。

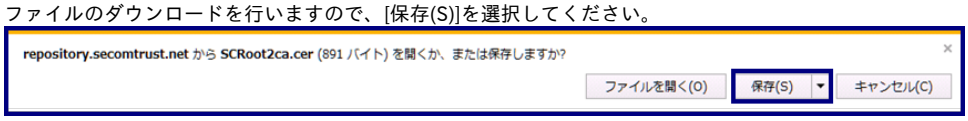



【サーバー証明書(ecdsa-with-SHA384)利用の場合】
URL：https://repository.secomtrust.net/SC-ECC-Root1/index.html
「Security Communication ECC RootCA1 Certificate(SCECCRoot1ca.cer)」と記述されたリンクを選択してください。




2.以降の説明はSCRoot2ca.cerを利用した場合の説明になります。
SCECCRoot1ca.cerを利用する場合もファイル名以外は同様の手順となります。

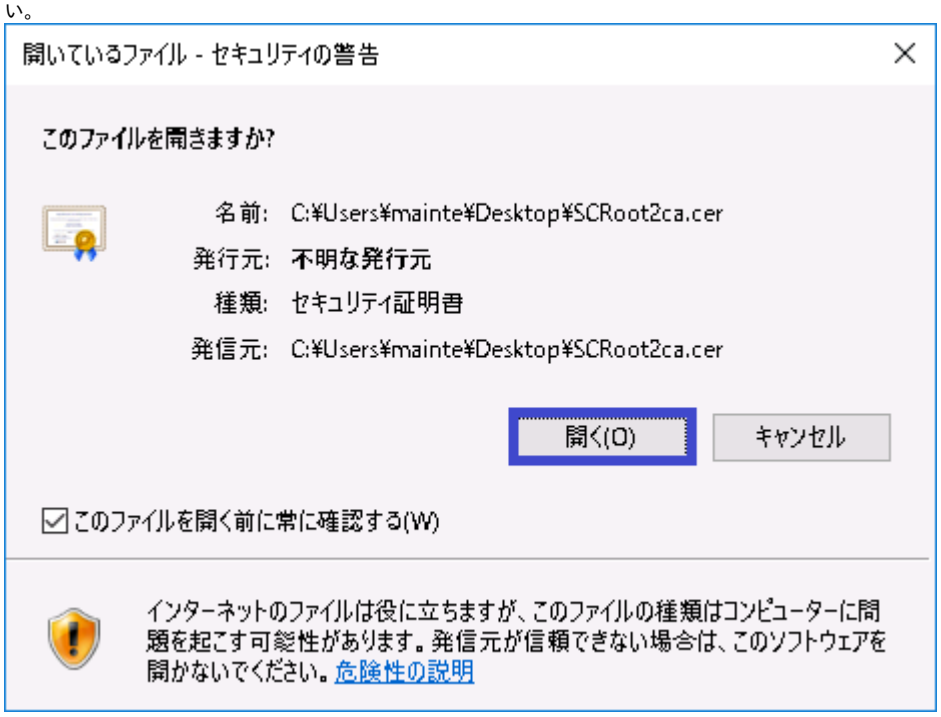
2. ファイルのダウンロードを行いますので、[保存(S)]を選択してください。



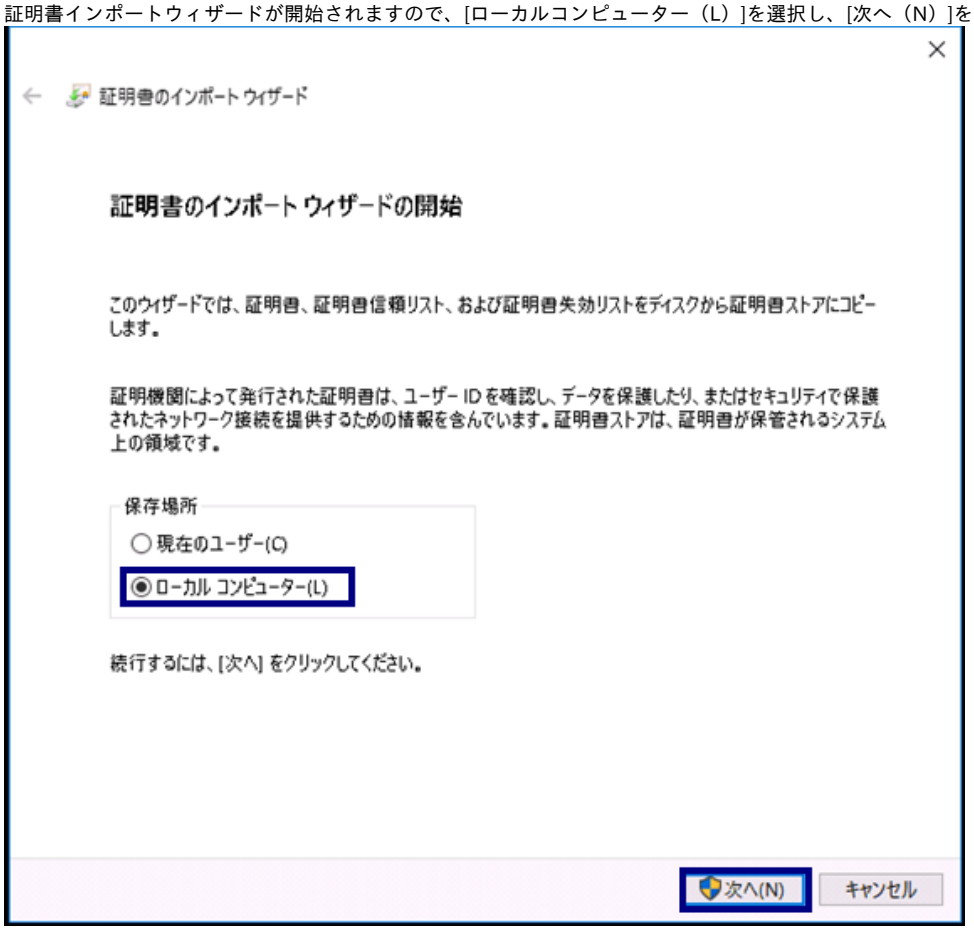

3. [ファイルを開く（O）]を選択してください。



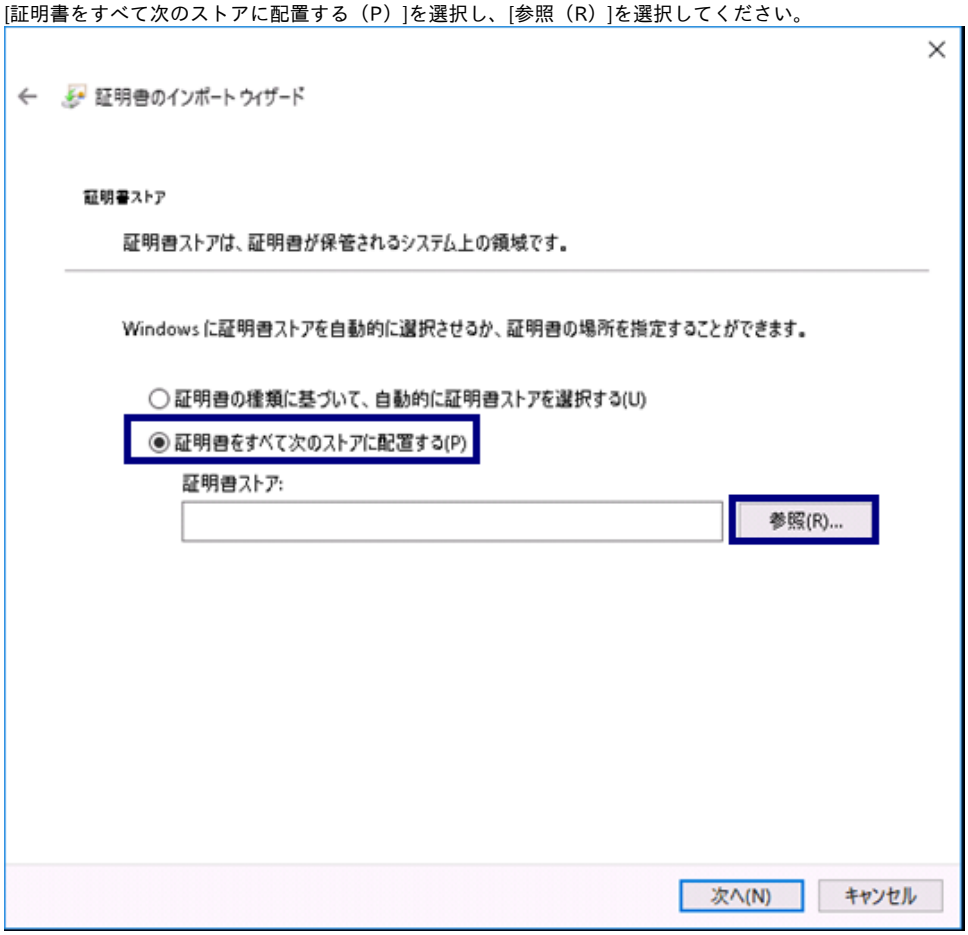
4. 開いているファイル – セキュリティ警告ウィンドウが表示されますので、[開く（O）]を選択し、[証明書のインストール（I）]を選択してください。



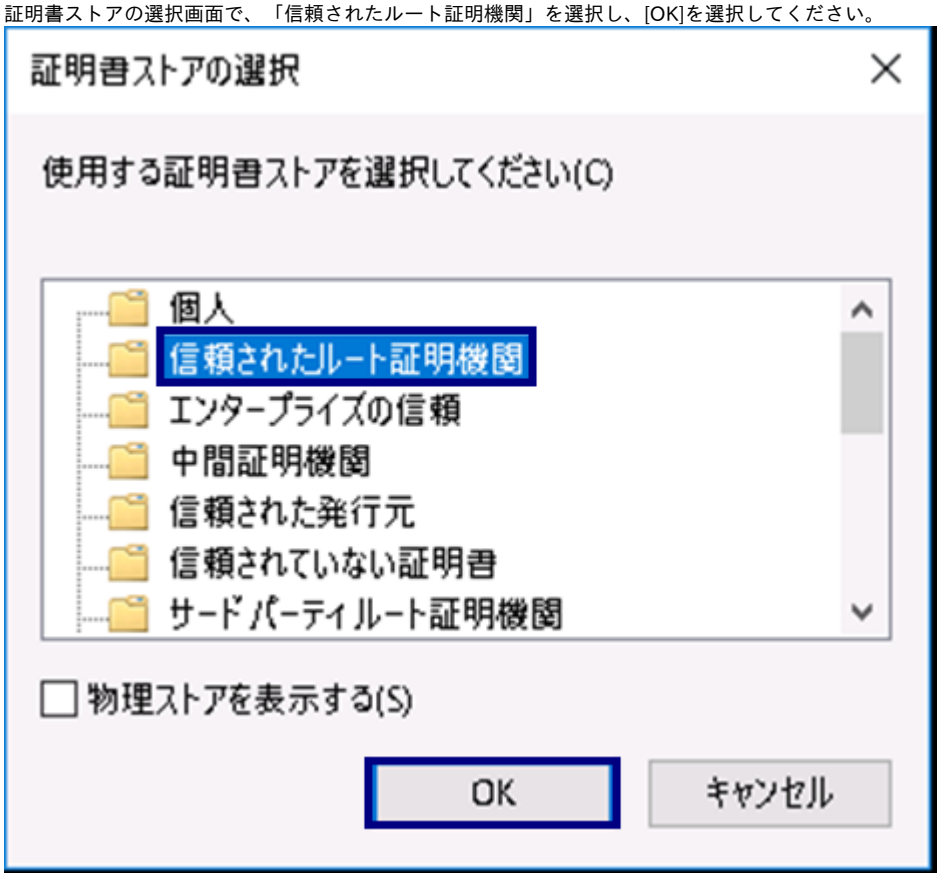

5. 証明書インポートウィザードが開始されますので、[ローカルコンピューター（L）]を選択し、[次へ（N）]を選択してください。



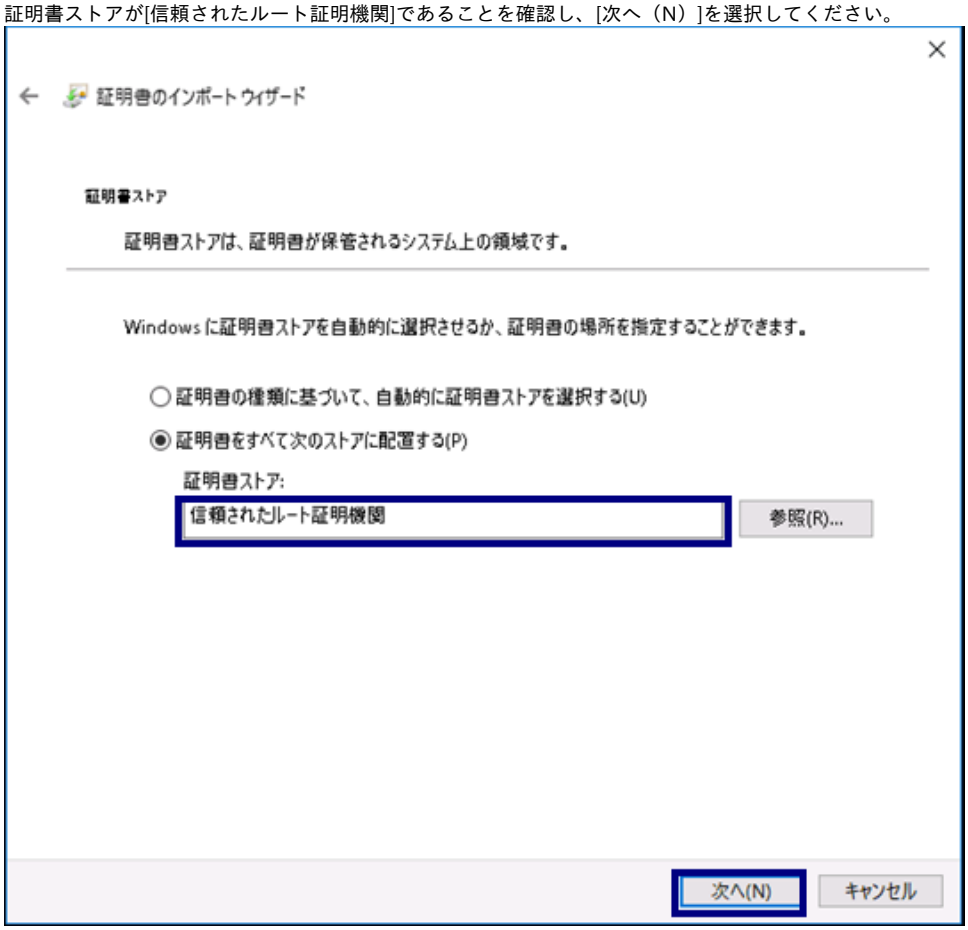
6. [証明書をすべて次のストアに配置する（P）]を選択し、[参照（R）]を選択してください。



7. 証明書ストアの選択画面で、「信頼されたルート証明機関」を選択し、[OK]を選択してください。



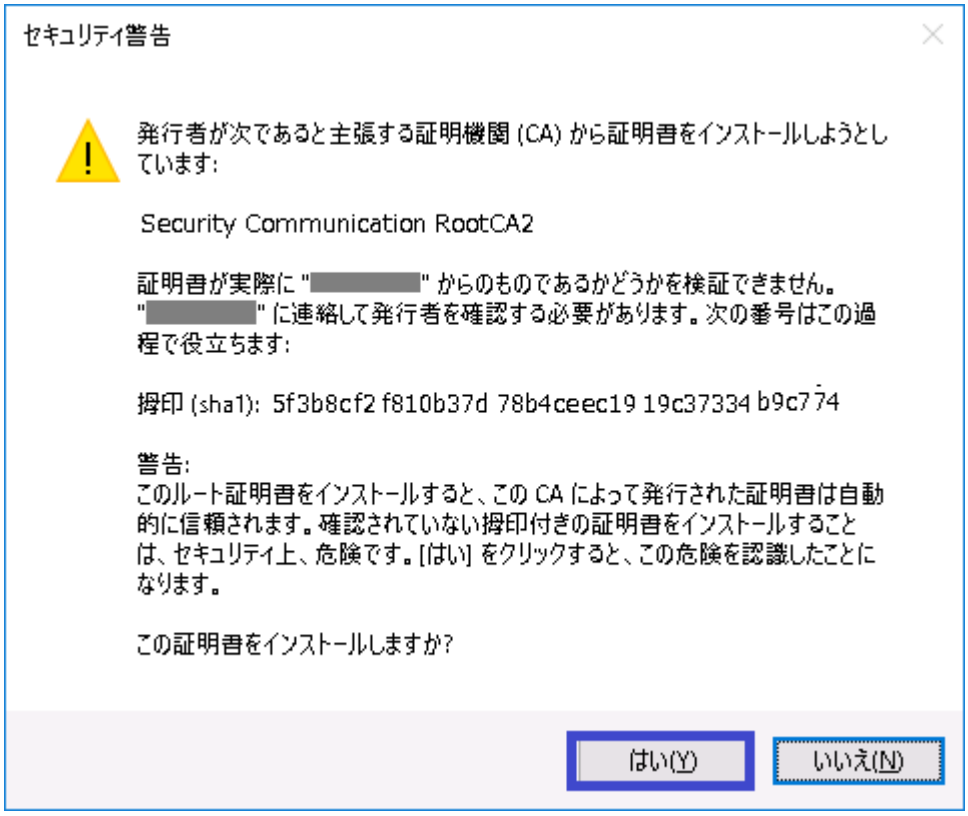
8. 証明書ストアが[信頼されたルート証明機関]であることを確認し、[次へ（N）]を選択してください。



9. セキュリティ警告画面が表示された場合、下の情報を確認してください。

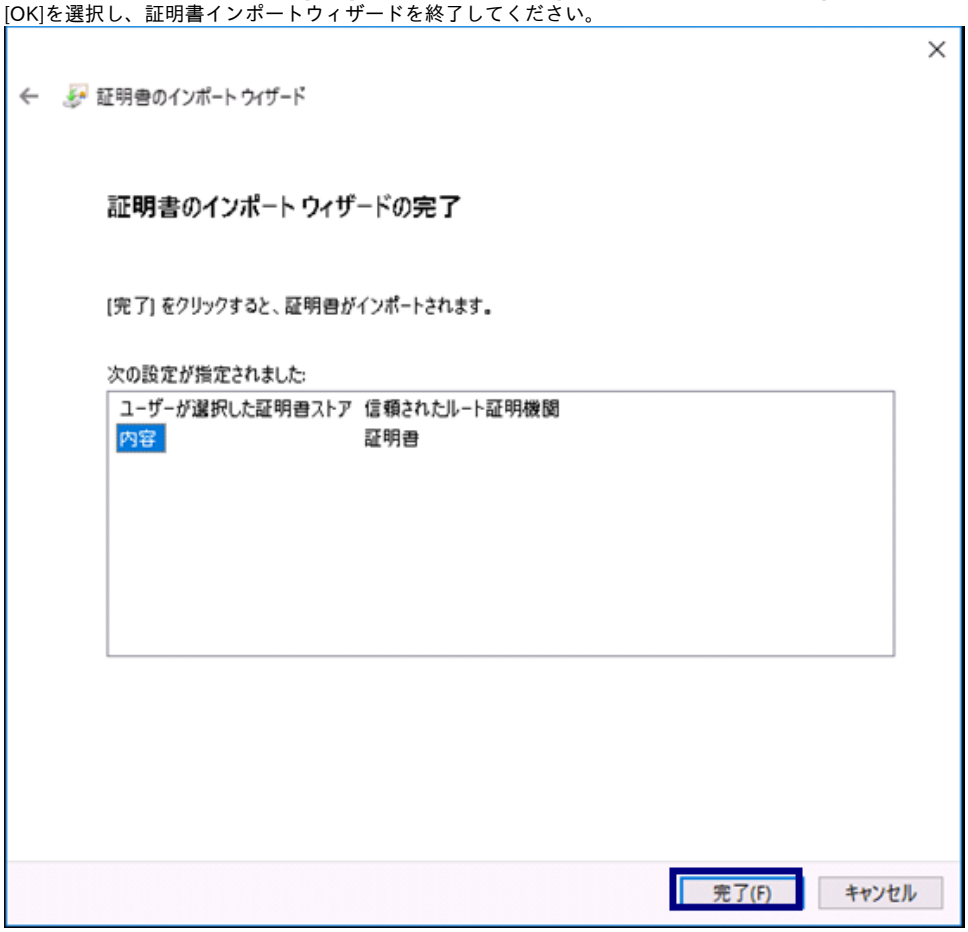
【ルート証明書がSCRoot2ca.cerの場合】
拇印が「Fingerprint (SHA-1) = 5f 3b 8c f2 f8 10 b3 7d 78 b4 ce ec 19 19 c3 73 34 b9 c7 74]

【ルート証明書がSCECCRoot1ca.cerの場合】
拇印が「Fingerprint (SHA-1) = b8 0e 26 a9 bf d2 b2 3b c0 ef 46 c9 ba c7 bb f6 1d 0d 41 41]

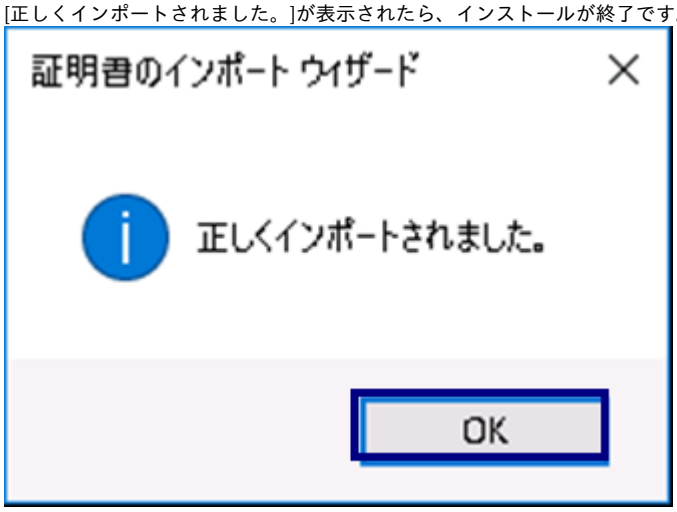



であることを確認して、[はい（Y）]を選択してください。

10. 以下の確認画面が表示されたら、[完了]を選択してください。[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。




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。

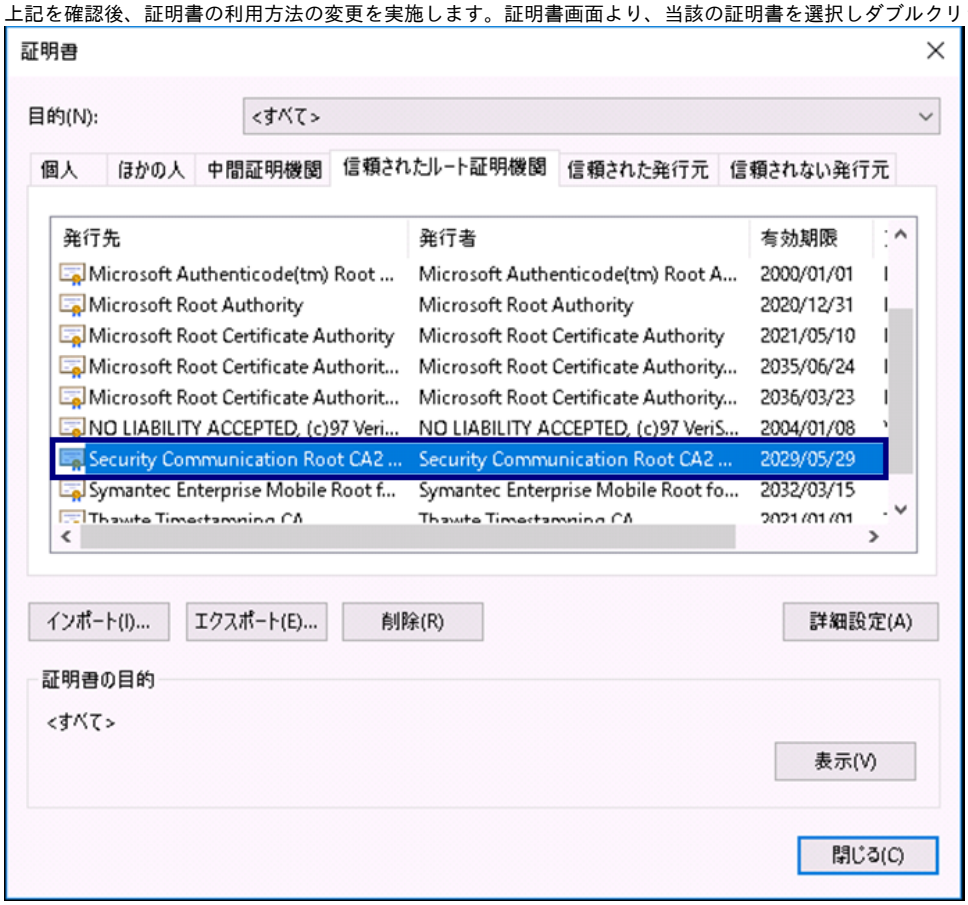



12. インストールされた証明書を確認するために、事前準備と同様の方法で発行先、発行者を確認してください。

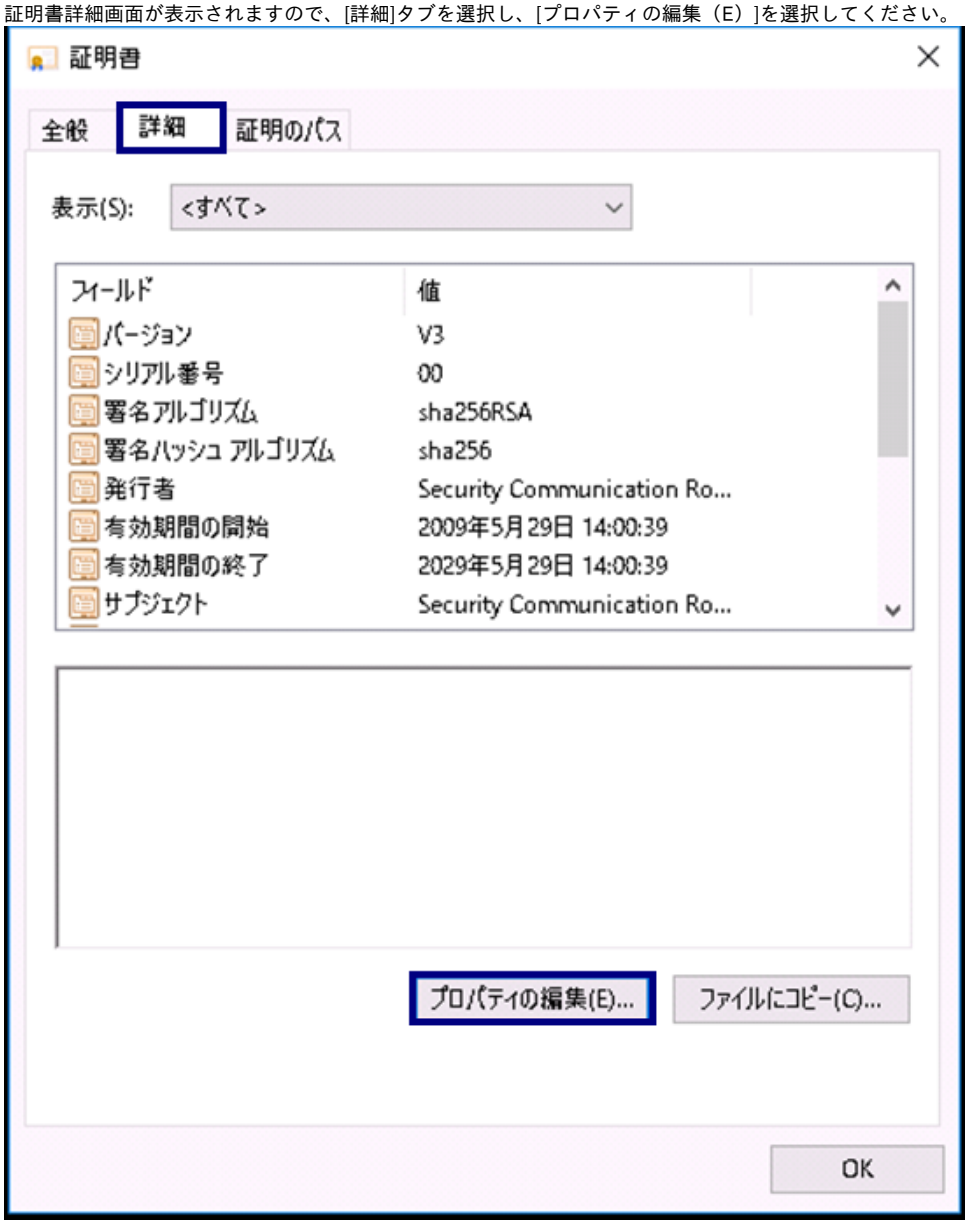
【ルート証明書がSCRoot2ca.cerの場合】
発行先「Security Communication RootCA2」、発行者「Security Communication RootCA2」、
「Fingerprint (SHA-1) =5f 3b 8c f2 f8 10 b3 7d 78 b4 ce ec 19 19 c3 73 34 b9 c7 74」であることを確認してください。

【ルート証明書がSCECCRoot1ca.cerの場合】
発行先「Security Communication ECC RootCA1」、発行者「Security Communication ECC RootCA1」、
「Fingerprint (SHA-1) = b8 0e 26 a9 bf d2 b2 3b c0 ef 46 c9 ba c7 bb f6 1d 0d 41 41」であることを確認してください。

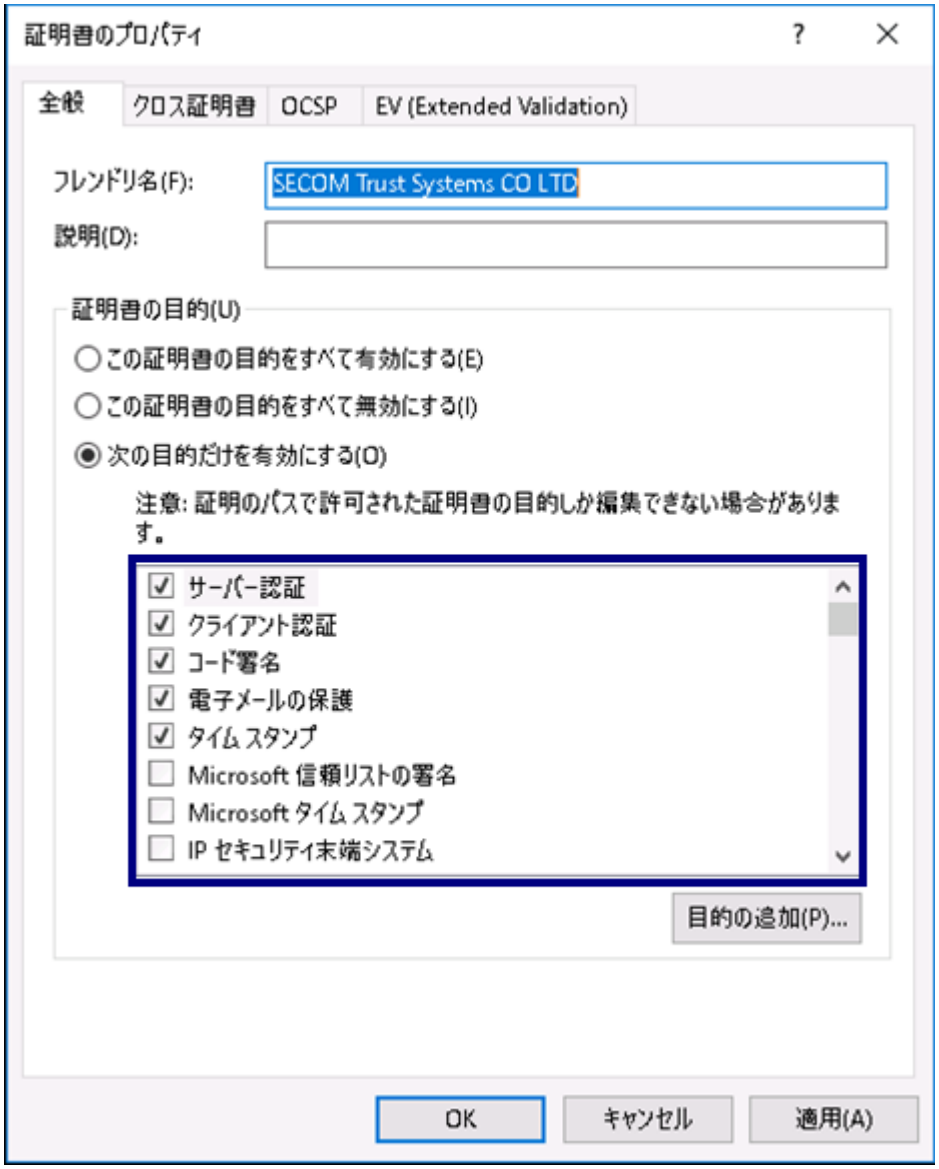
13. 上記を確認後、証明書の利用方法の変更を実施します。証明書画面より、当該の証明書を選択しダブルクリックしてください。



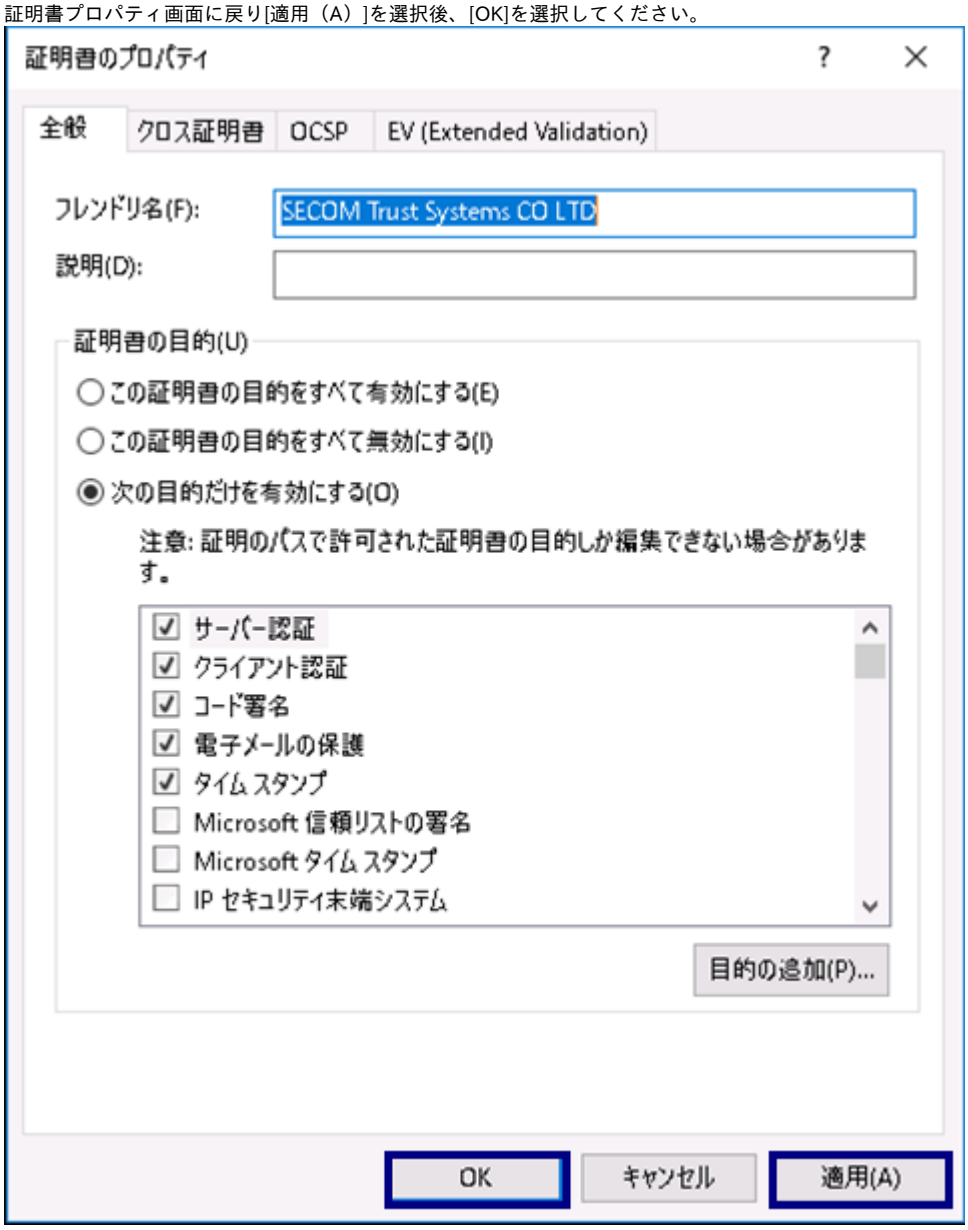
14. 証明書詳細画面が表示されますので、[詳細]タブを選択し、[プロパティの編集（E）]を選択してください。



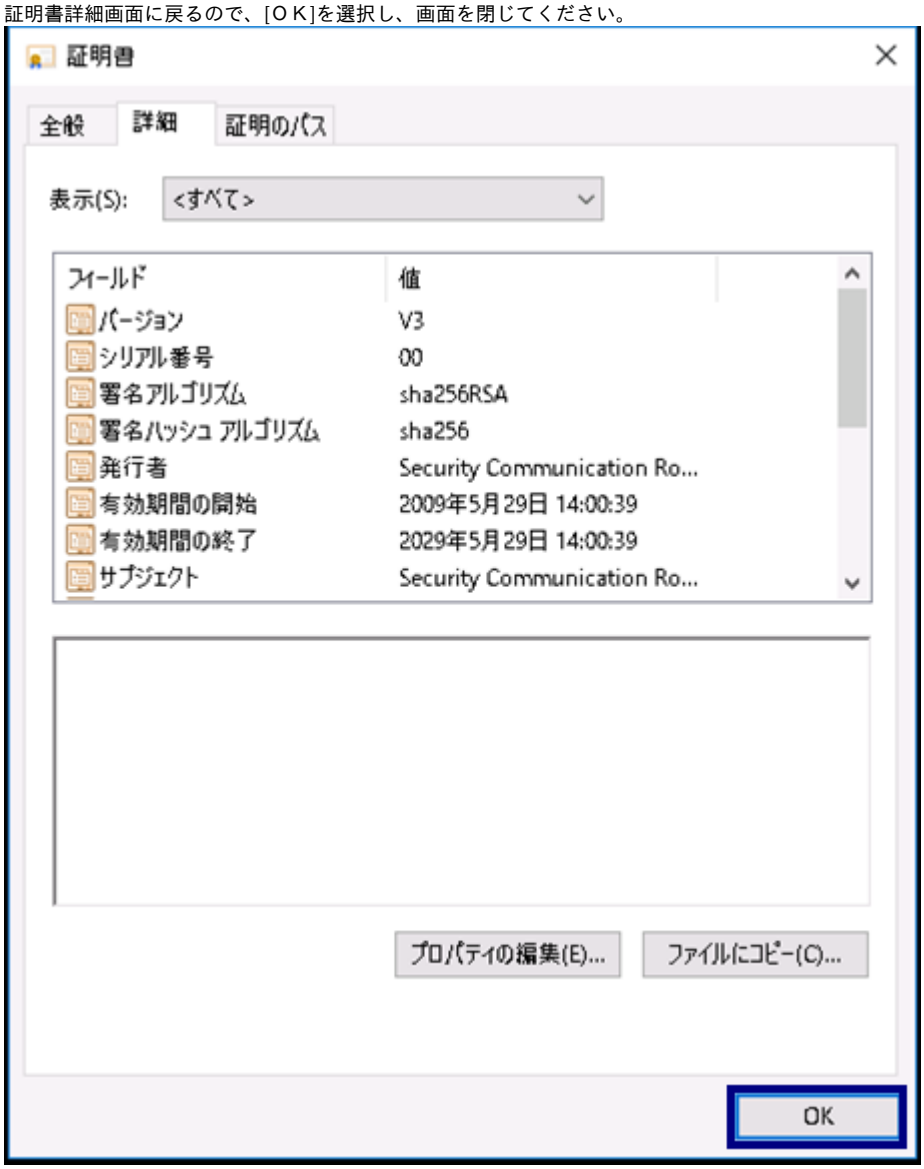
15. 証明書プロパティ画面で[全般]タブを選択してください。 [次の目的だけを有効にする（O）]のラジオボタンにチェックを入れると、下部の証明書の目的部分のチェックボックスの編集が可能となります。**以下の項目以外のチェックボックスをすべて外してください。**
    a. サーバー認証
    b. クライアント認証
    c. コード署名
    d. 電子メールの保護
    e. タイムスタンプ



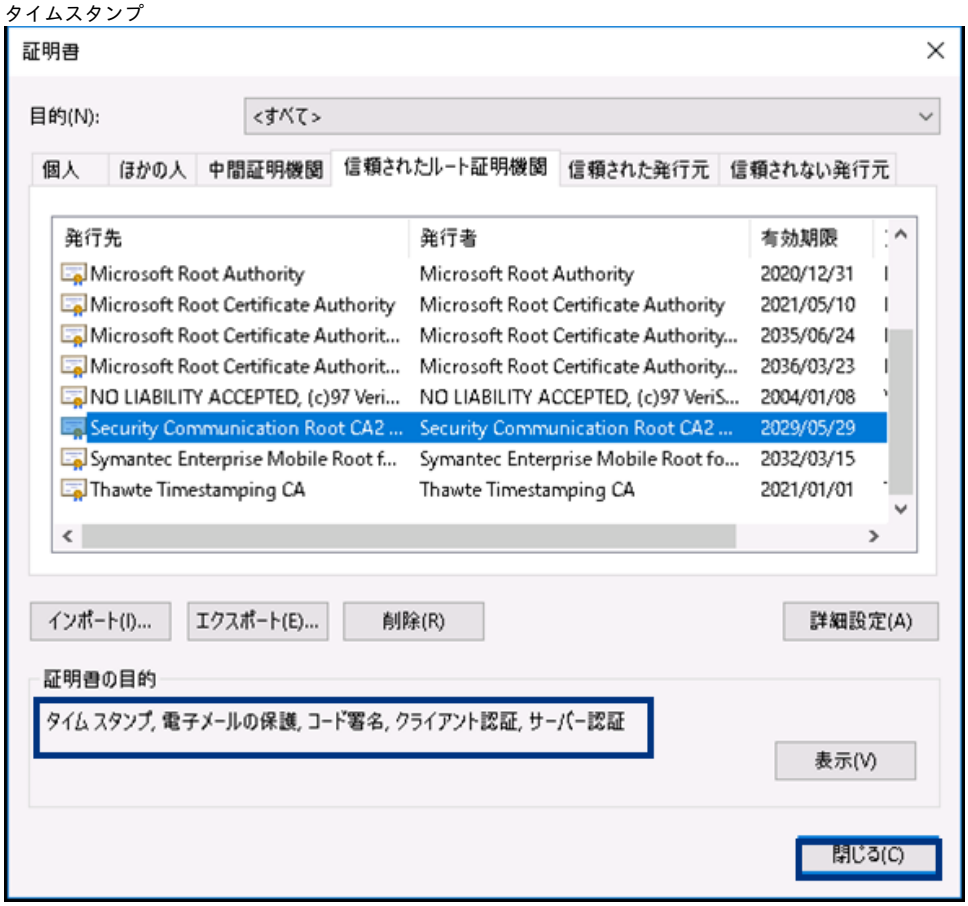
16. 証明書プロパティ画面に戻り[適用（A）]を選択後、[OK]を選択してください。



17. 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。



18. 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。
    a. サーバー認証
    b. クライアント認証
    c. コード署名
    d. 電子メールの保護
    e. タイムスタンプ




以上で、ルートＣＡ証明書のインストールは終了です。

## 1-2-3. 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. [1-2-1.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)...]を選択してください。

●証明書の発行日時が2020年12月25日0時以降の場合

【RSA認証局　中間CA証明書をインストールする場合】
発行先：NII Open Domain CA - G7 RSA
発行者：Security Communication RootCA2

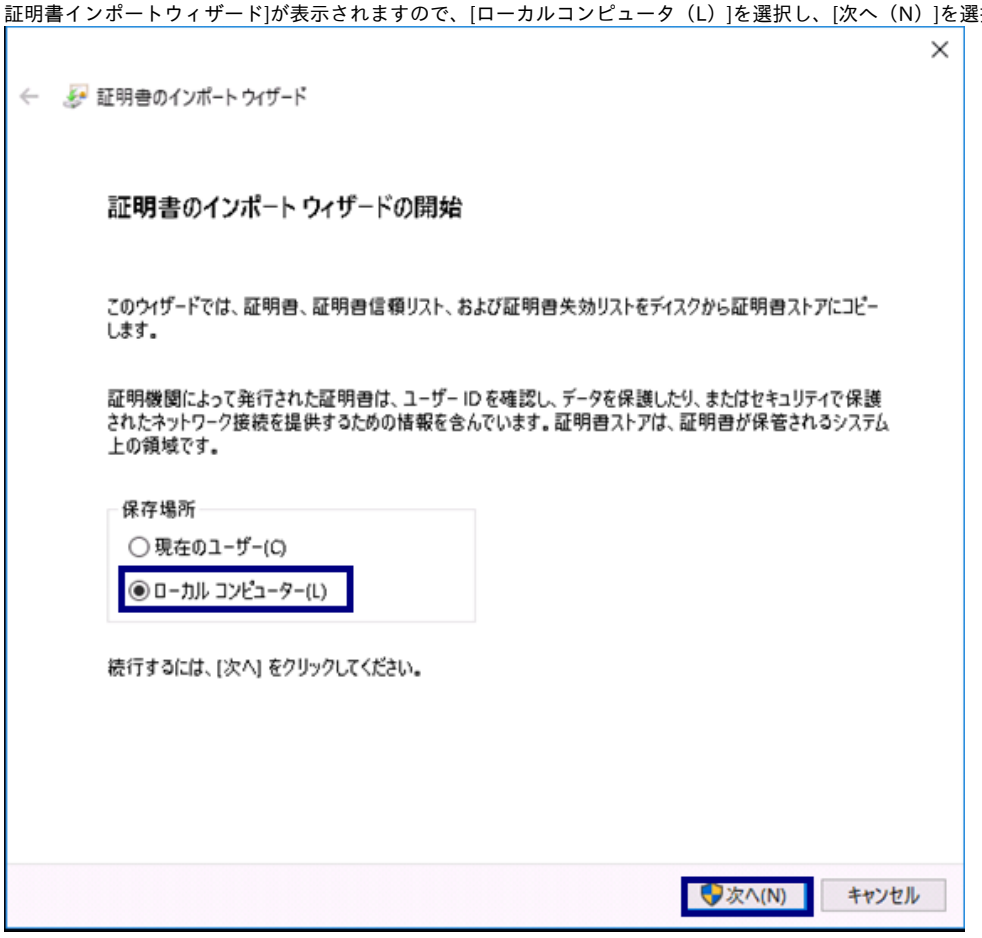
【ECC認証局　中間CA証明書をインストールする場合】
発行先：NII Open Domain CA - G7 ECC
発行者：Security Communication ECC RootCA1

●証明書の発行日時が2020年12月25日0時以前の場合

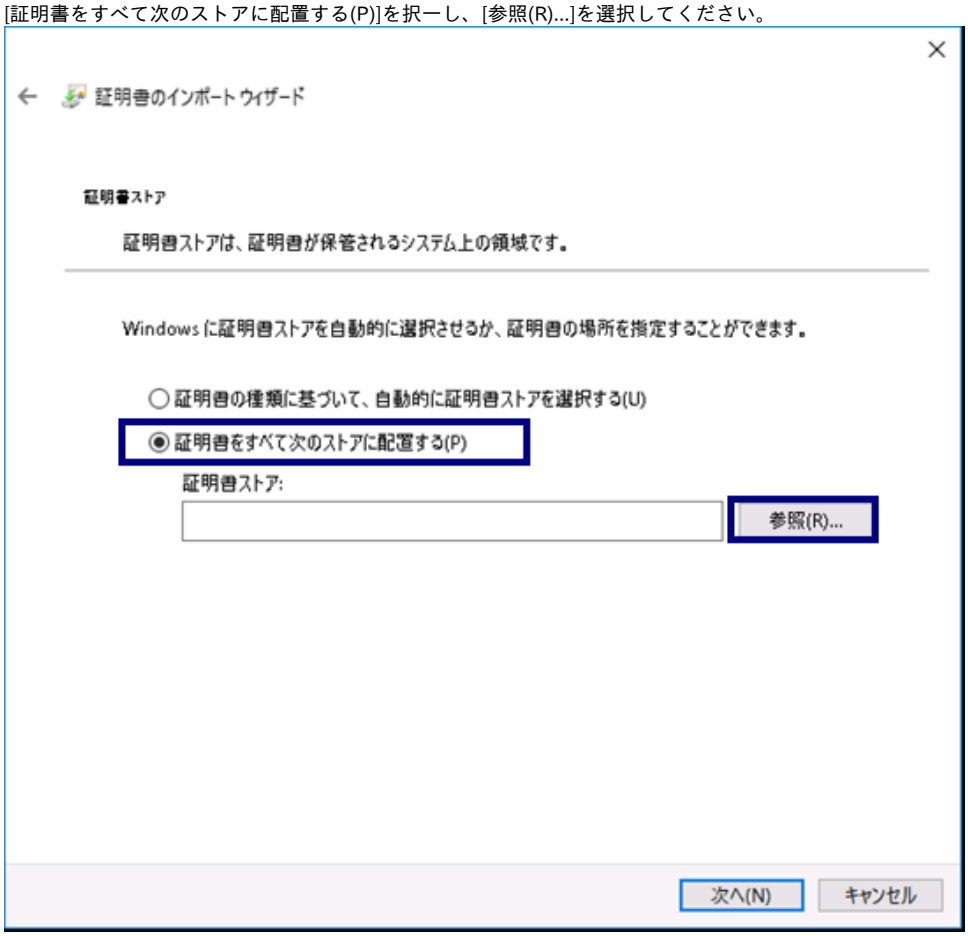
【SHA-2認証局 CA証明書 CT対応版をインストールする場合】
発行先：NII Open Domain CA - G5
発行者：Security Communication RootCA2

【ECC認証局 CA証明書をインストールする場合】
発行先：NII Open Domain CA - G6
発行者：Security Communication ECC RootCA1

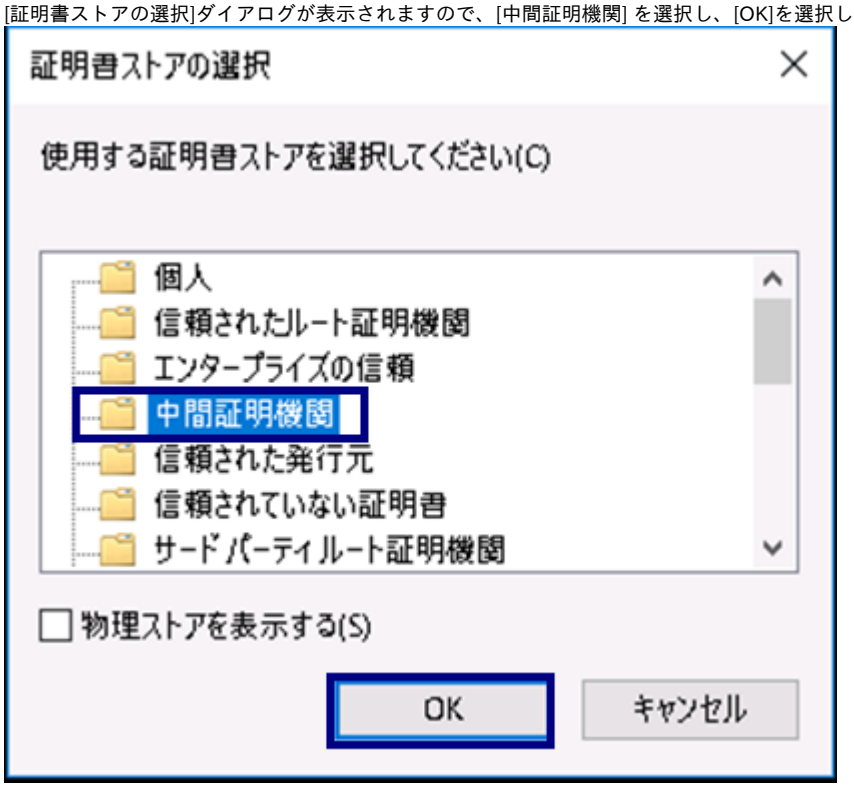
3. 証明書インポートウィザード]が表示されますので、[ローカルコンピュータ（L）]を選択し、[次へ（N）]を選択してください。



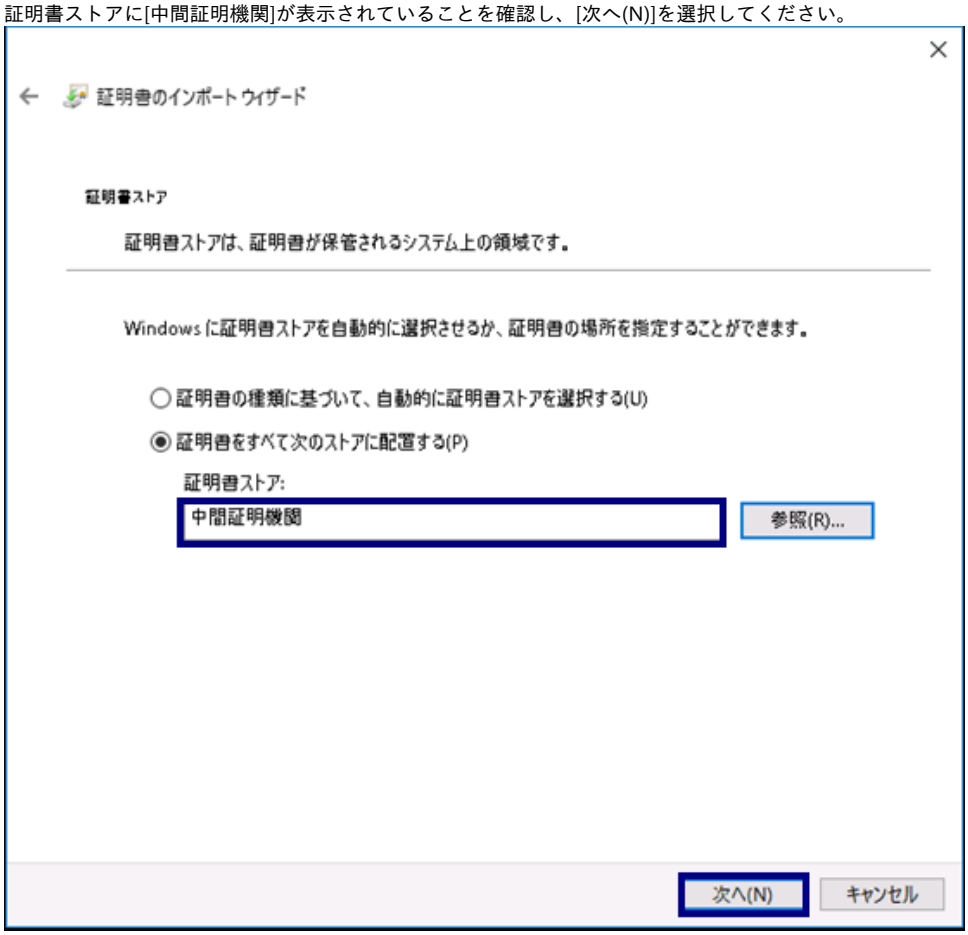
4. [証明書をすべて次のストアに配置する(P)]を択一し、[参照(R)...]を選択してください。



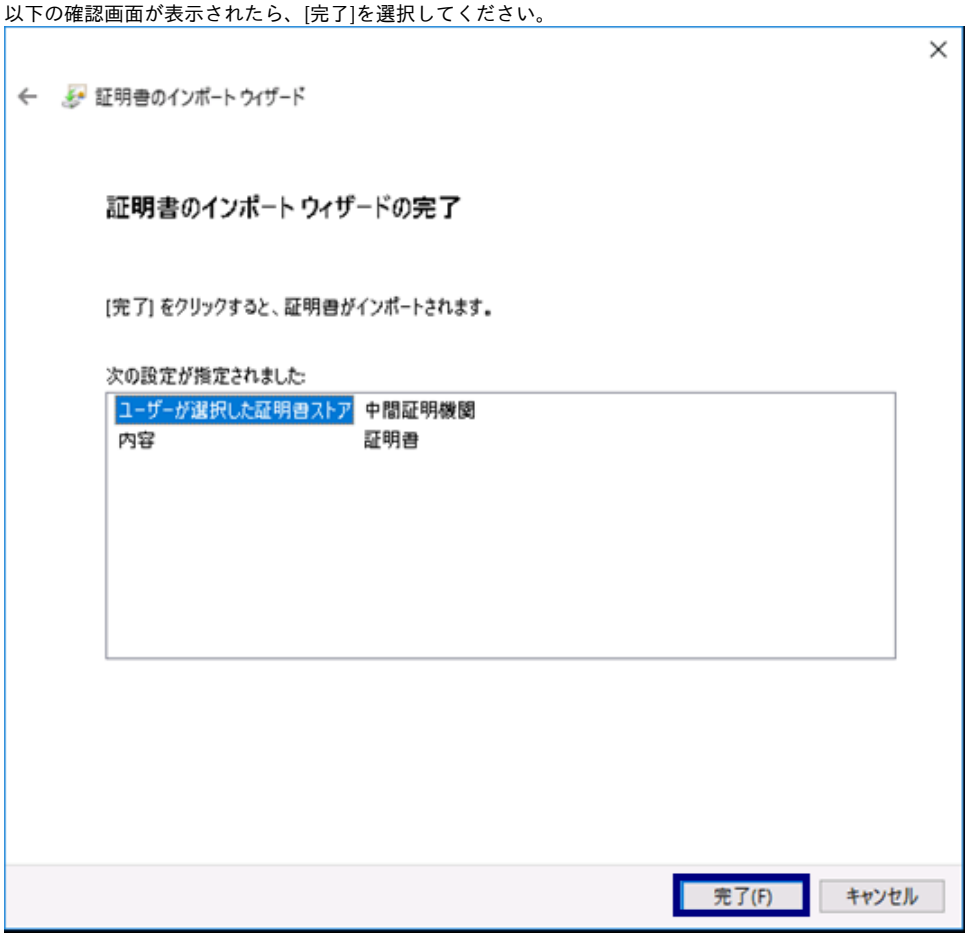

5. [証明書ストアの選択]ダイアログが表示されますので、[中間証明機関] を選択し、[OK]を選択してください。



6. 証明書ストアに[中間証明機関]が表示されていることを確認し、[次へ(N)]を選択してください。



7. 以下の確認画面が表示されたら、[完了]を選択してください。




## 1-2-4. 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を実施してください。

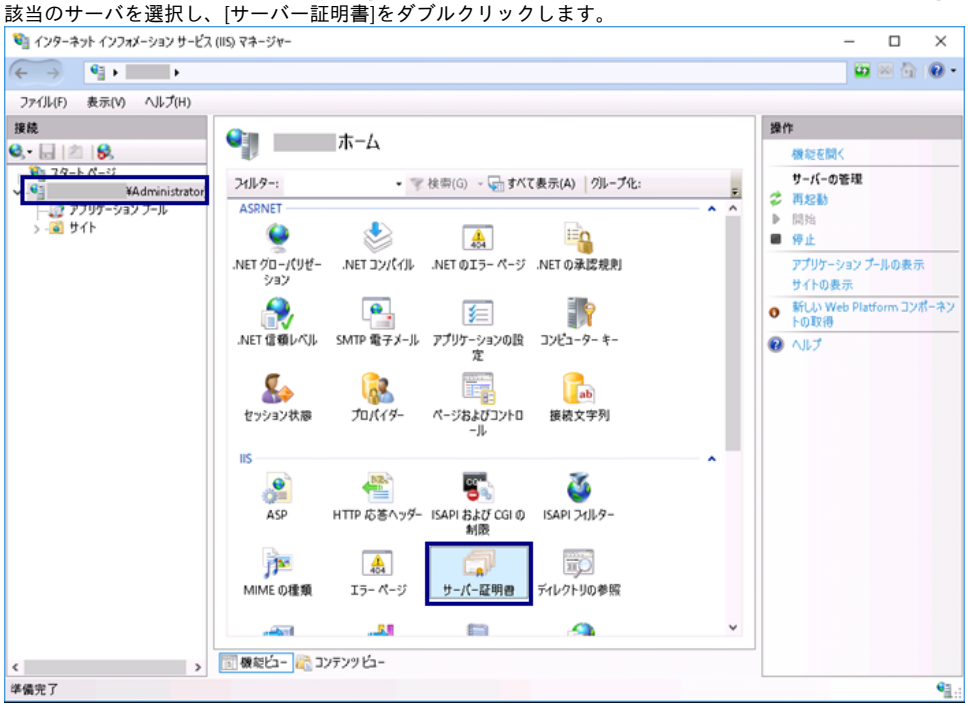
**サーバ証明書のインストール**

1. [1-2-1.事前準備]で取得したサーバ証明書と[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。

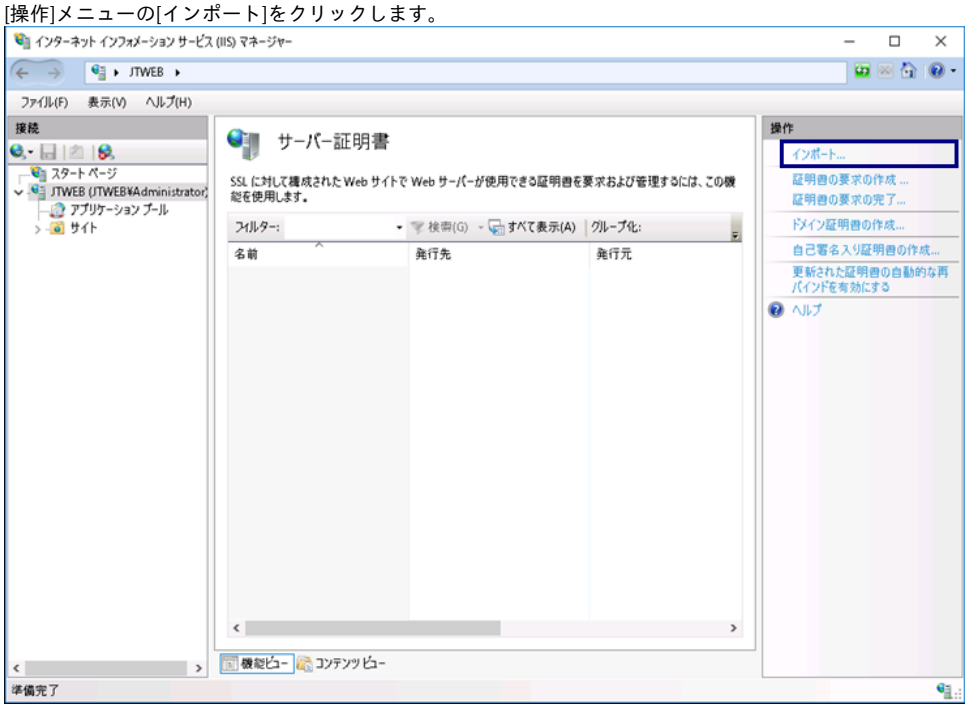
```
C:\work> openssl pkcs12 -export -inkey servername.key -in server.cer -out servername.pfx

Enter pass phrase for servername.key: ←[鍵ペアの生成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
```

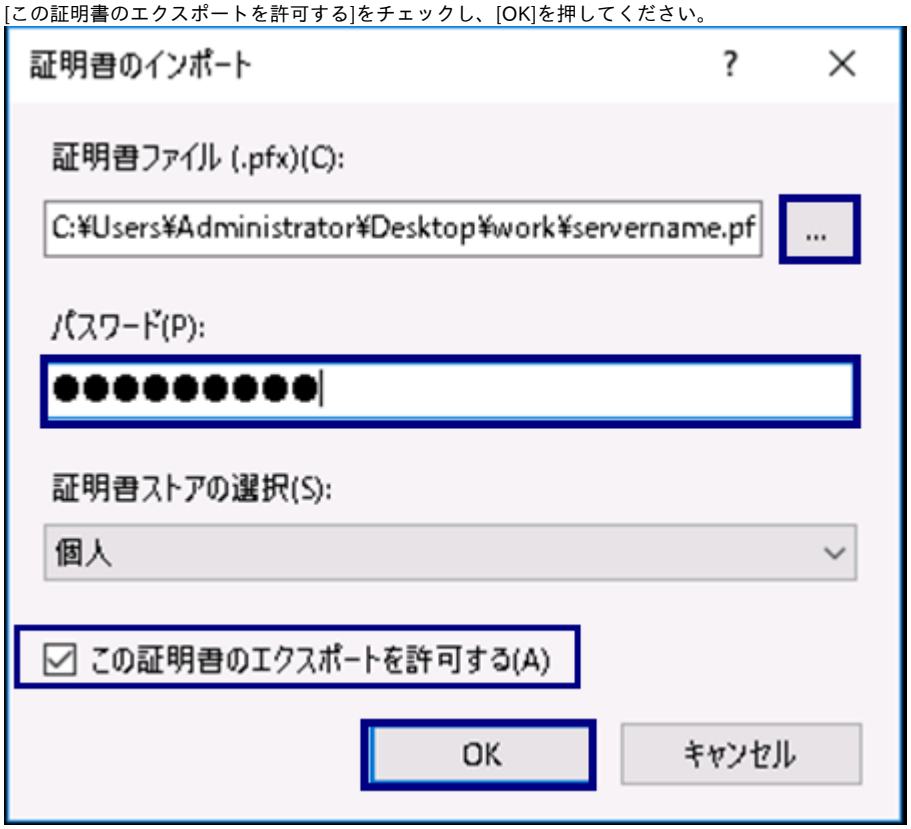
2. 次に、サーバ証明書をIISに設定します。[インターネットインフォメーションサービス（IIS）マネージャ]を 起動し、該当のサーバを選択し、[サーバー証明書]をダブルクリックします。



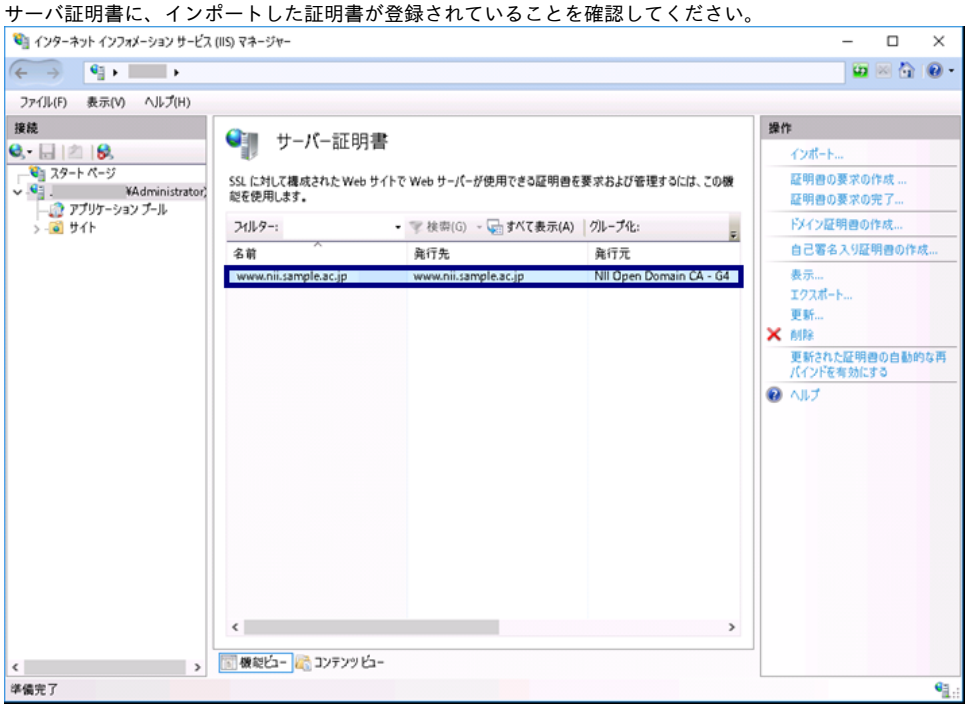

3. [操作]メニューの[インポート]をクリックします。



4. [. . . ]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。
パスワード欄にPKCS#12ファイルを作る際に指定したPKCS#12保護パスワードを入力します。
[この証明書のエクスポートを許可する]をチェックし、[OK]を押してください。

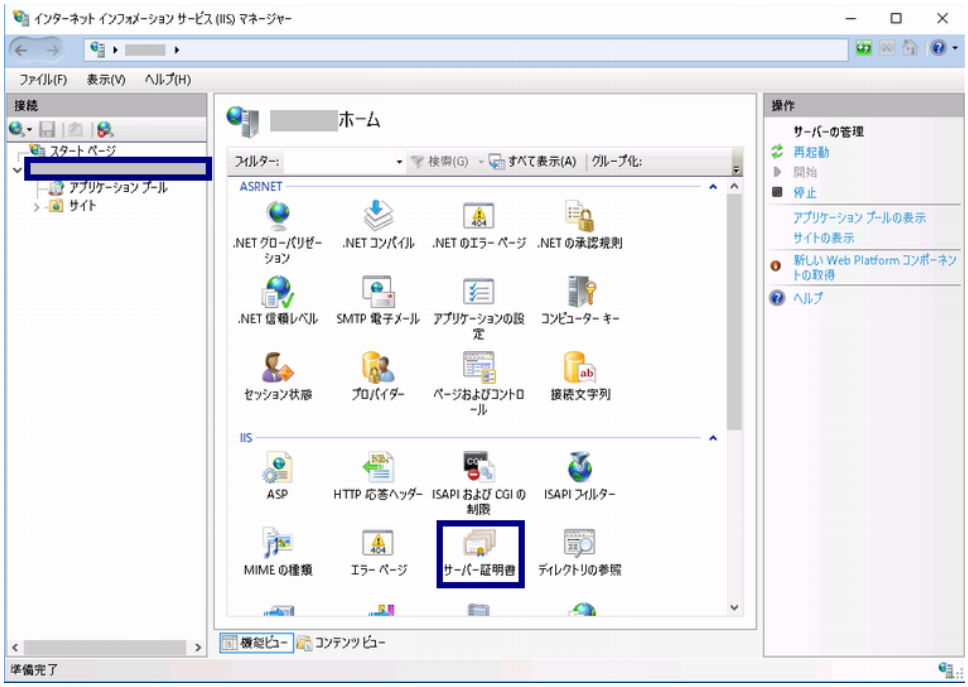



5. サーバ証明書に、インポートした証明書が登録されていることを確認してください。

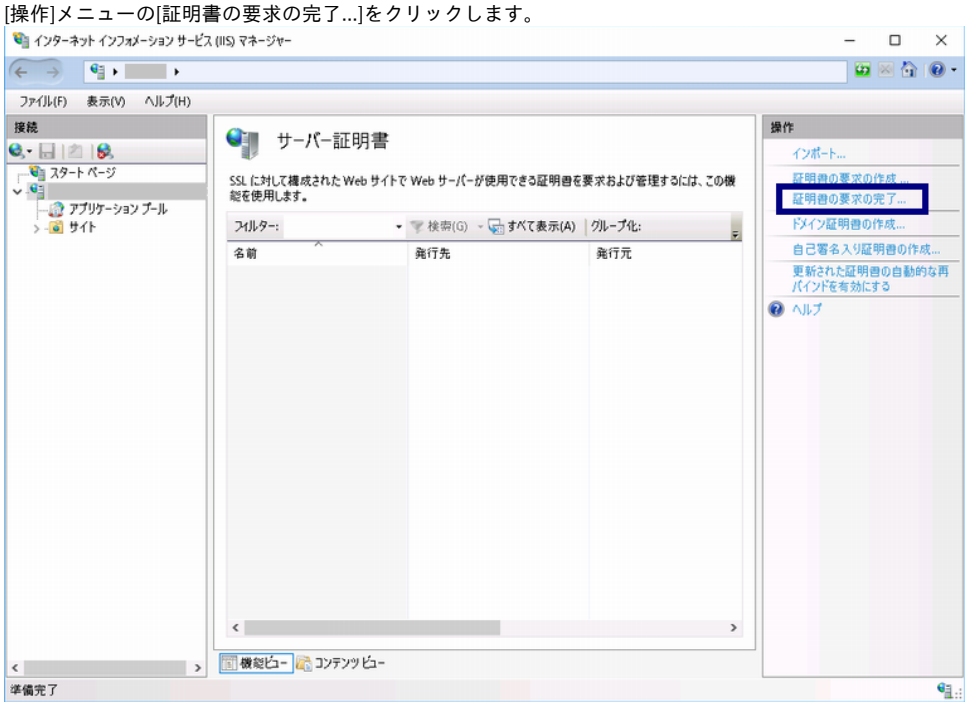



**CSRをIISで作成した場合(RSA)**

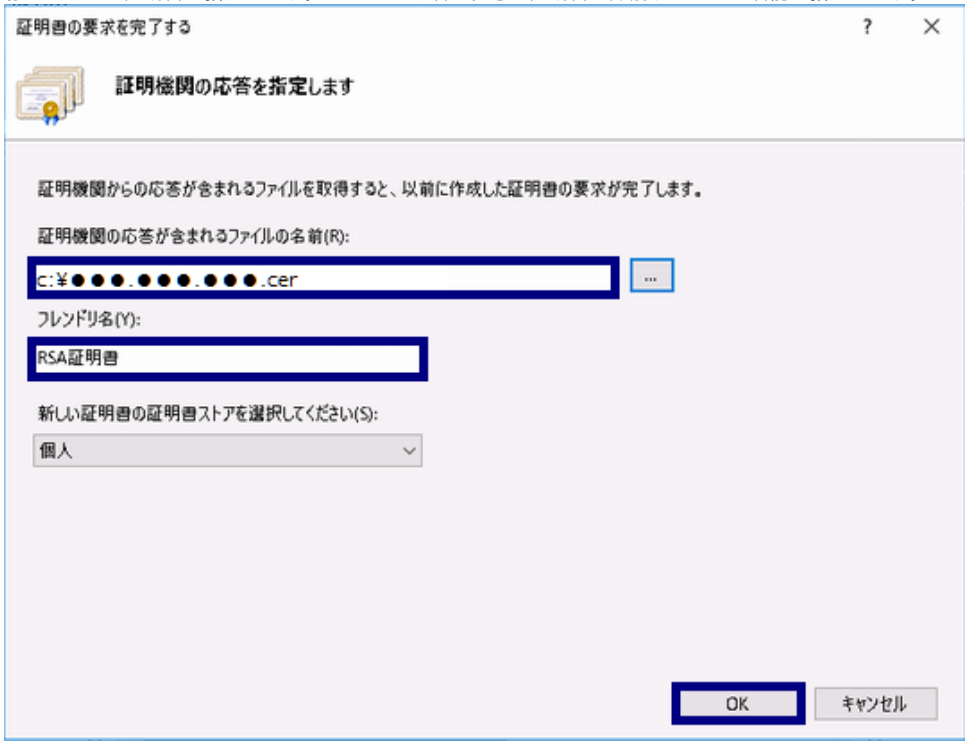
1. サーバ証明書をIISに設定します。[インターネットインフォメーションサービス（IIS）マネージャ]を起動し、該当のサーバを選択し、[サーバー証明書]をダブルクリックします。



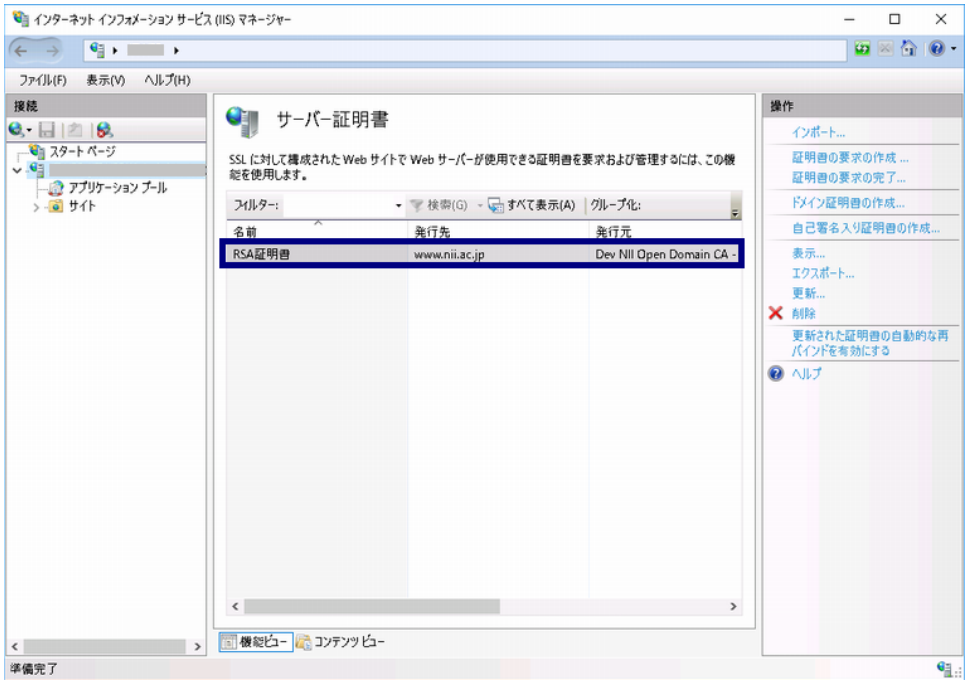

2. [操作]メニューの[証明書の要求の完了...]をクリックします。



3. [証明書の要求を完了する]ウィザードが起動します。[OK]ボタンを押下します。 証明機関の応答が含まれるファイルの名前：【...】ボタンより保存したサーバ証明書を指定します。 フレンドリ名：任意で証明書を識別するための名前を指定します。

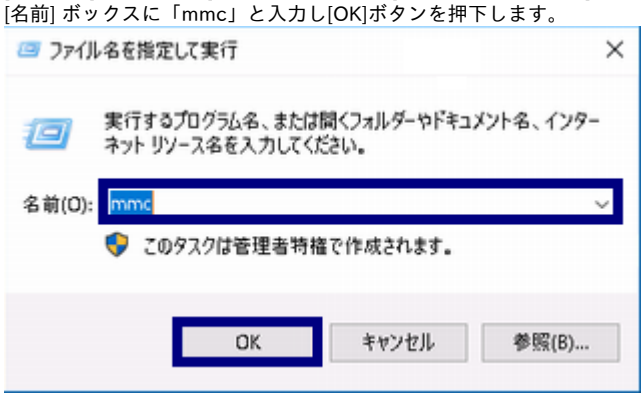



4. サーバ証明書に、インポートした証明書が登録されていることを確認してください。




**CSRをIISで作成した場合(ECDSA)**

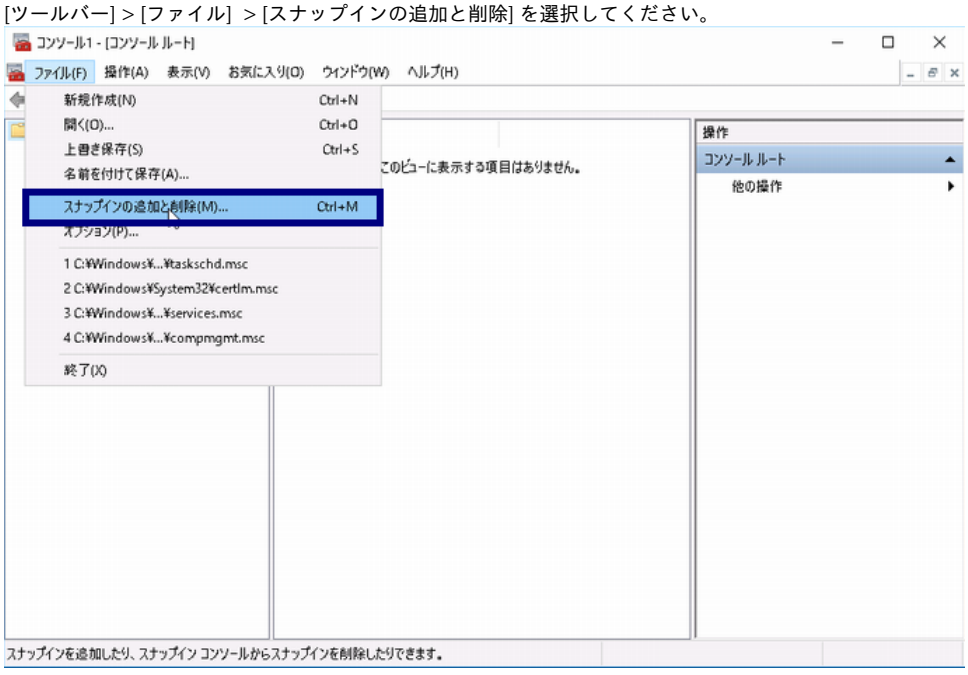
1. [スタート] メニューの [すべてのプログラム] をクリックします。[アクセサリ] をクリックして、[ファイル名を指定して実行] をクリックします。[名前] ボックスに「mmc」と入力し[OK]ボタンを押下します。



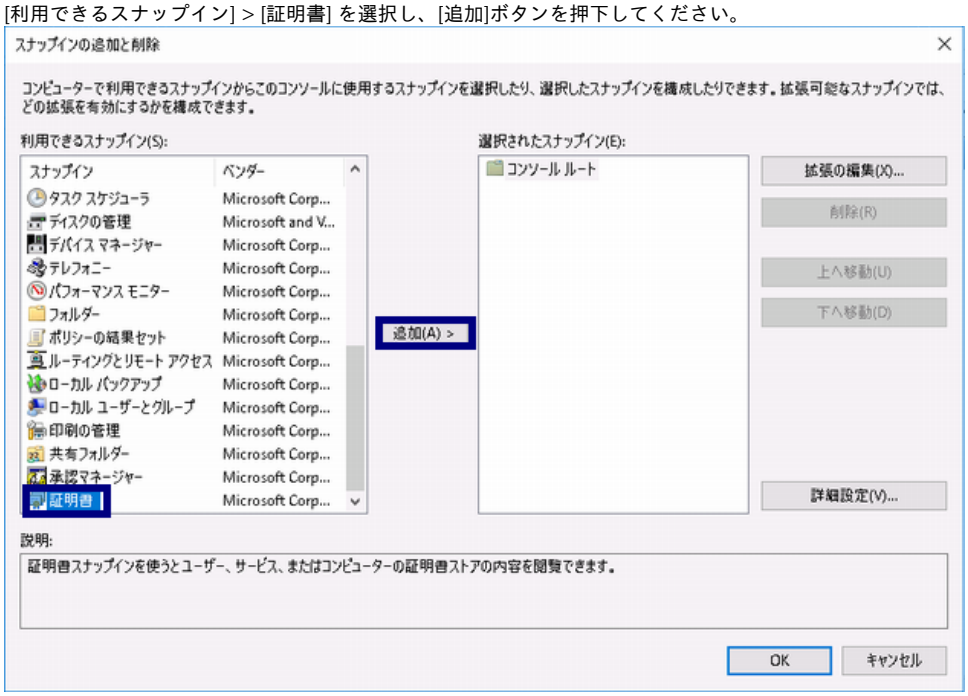

2. Microsoft Management Console が表示されます。



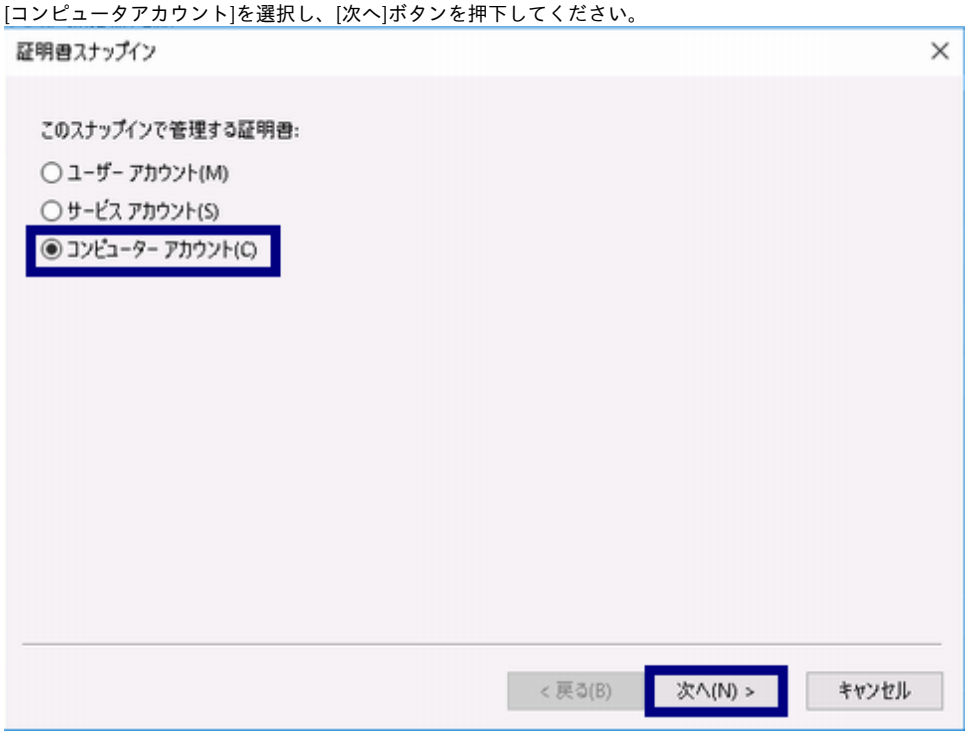

3. [ツールバー] > [ファイル] > [スナップインの追加と削除] を選択してください。



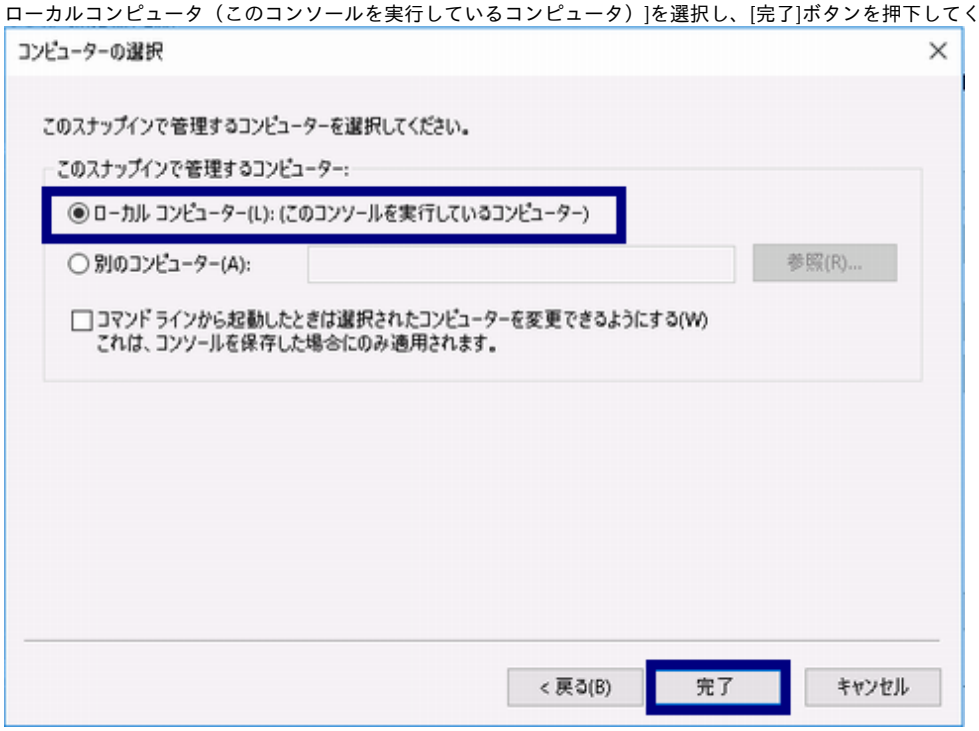
4. [利用できるスナップイン] > [証明書] を選択し、[追加]ボタンを押下してください。



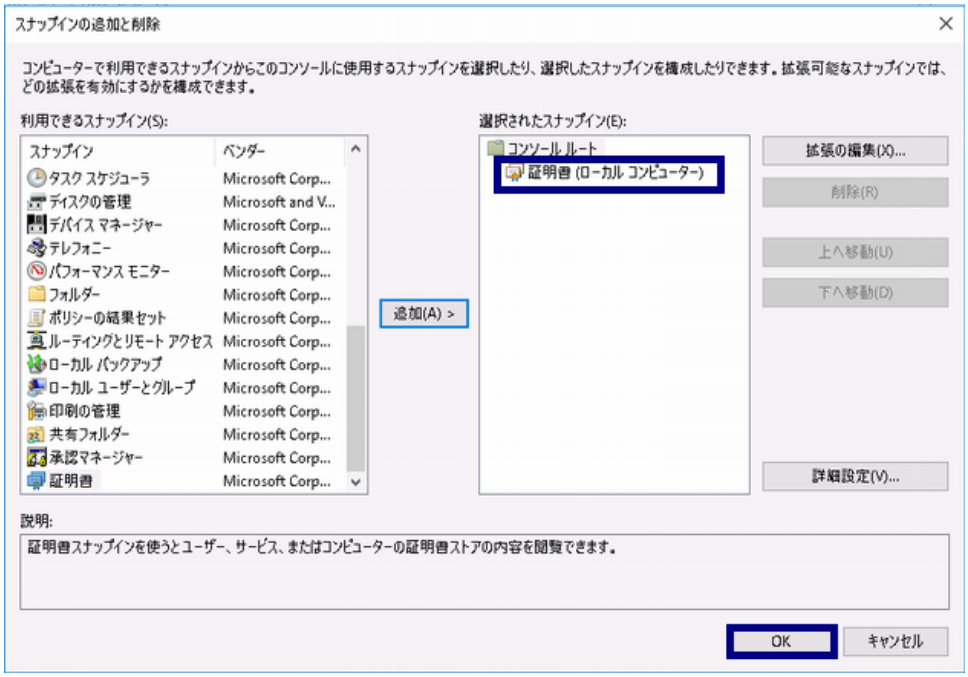

5. [コンピュータアカウント]を選択し、[次へ]ボタンを押下してください。



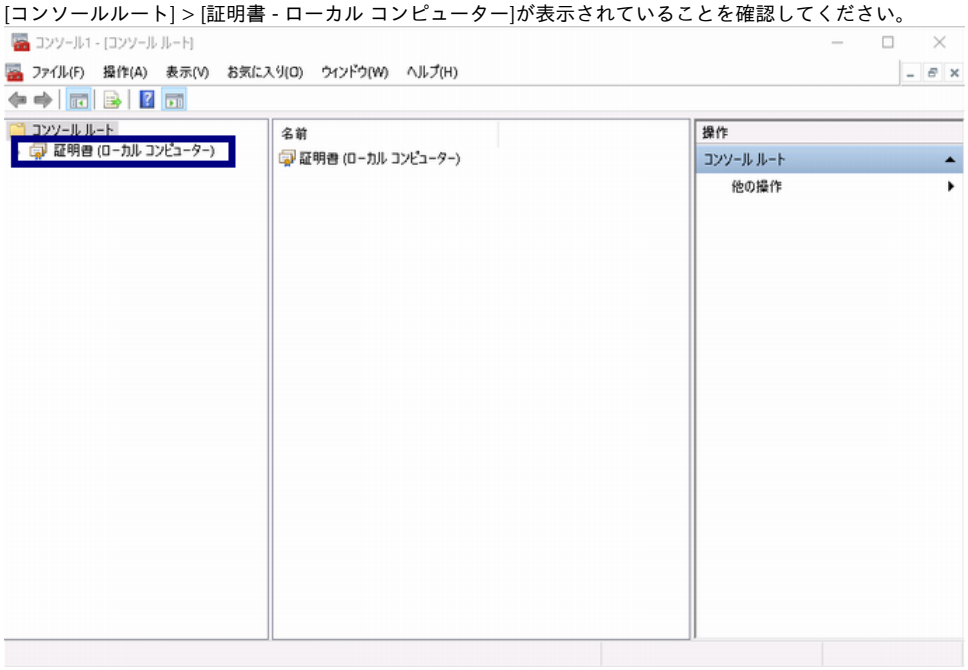
6. ローカルコンピュータ（このコンソールを実行しているコンピュータ）]を選択し、[完了]ボタンを押下してください。



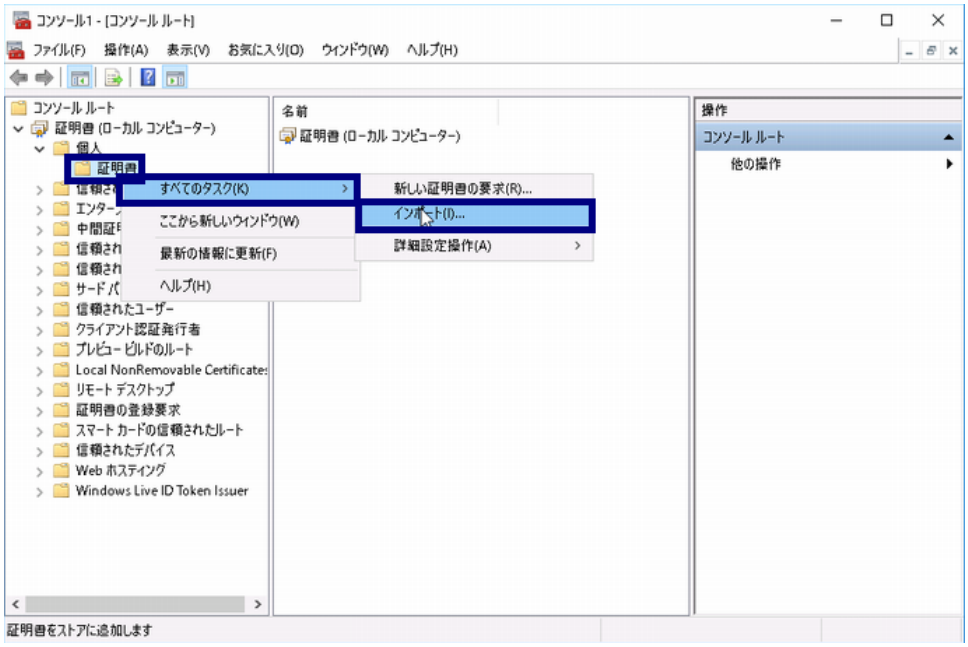

7. 選択されたスナップインに [証明書 - ローカル コンピューター]が表示されていることを確認し、[OK]ボタンを押下してください。



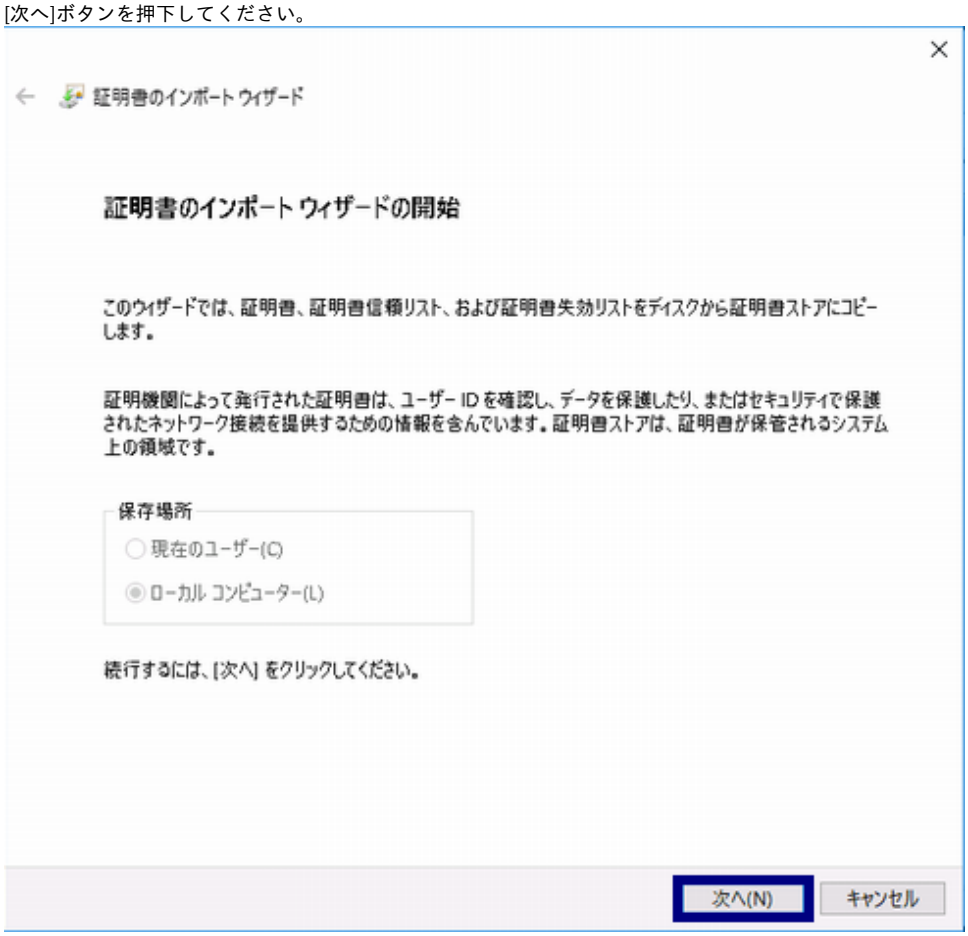
8. [コンソールルート] > [証明書 - ローカル コンピューター]が表示されていることを確認してください。



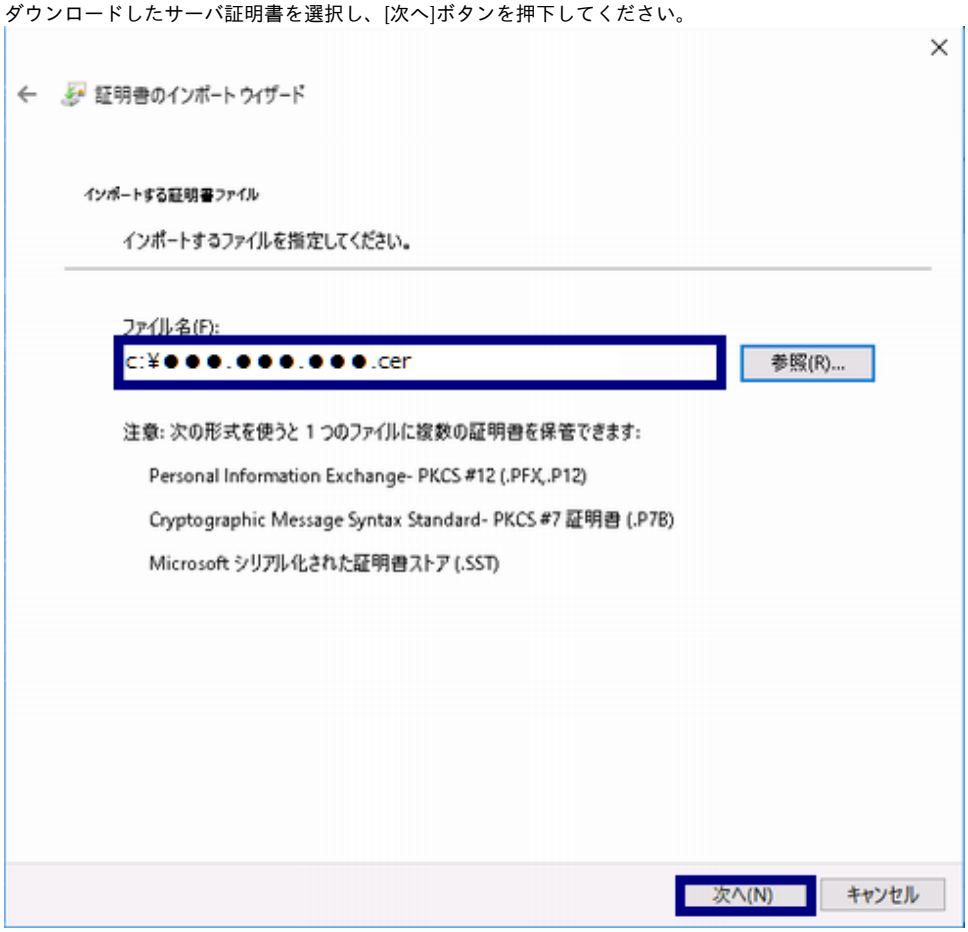

9. [コンソールルート] > [証明書 - ローカル コンピューター] > [個人] > [証明書]を選択し、
右クリックメニューから[すべてのタスク] > [インポート]を選択してください。



10. [次へ]ボタンを押下してください。

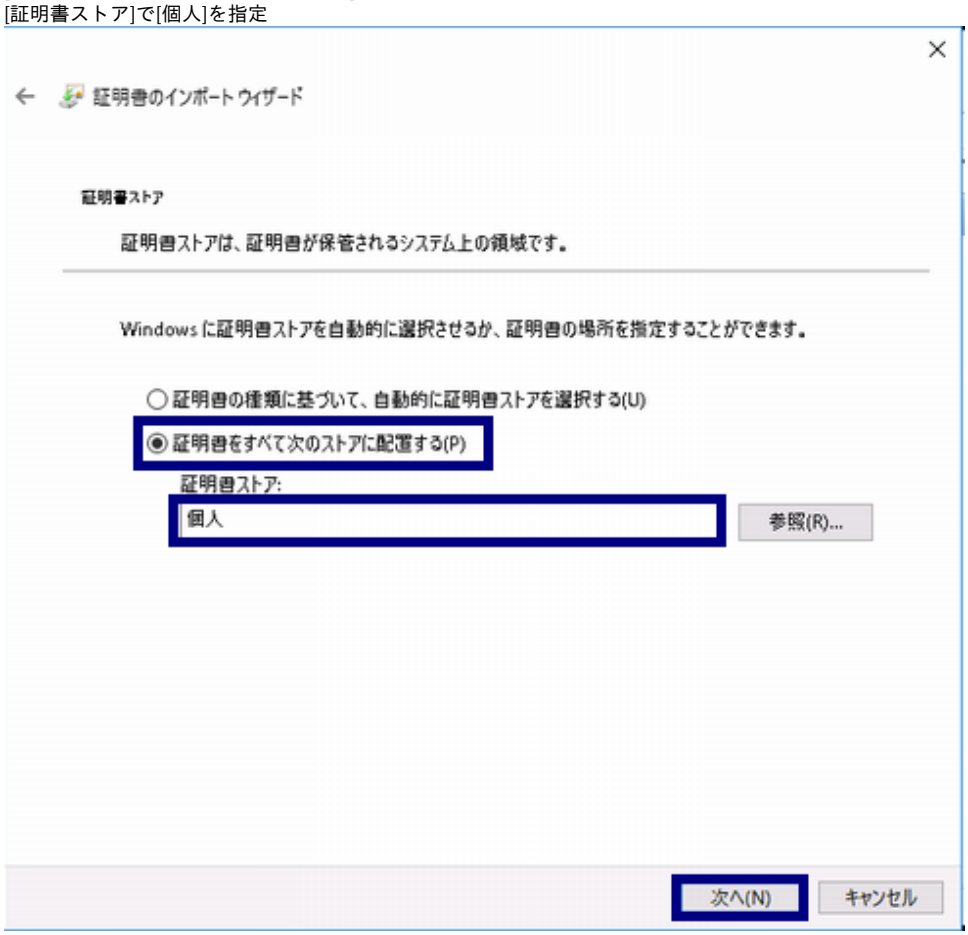


11. ダウンロードしたサーバ証明書を選択し、[次へ]ボタンを押下してください。

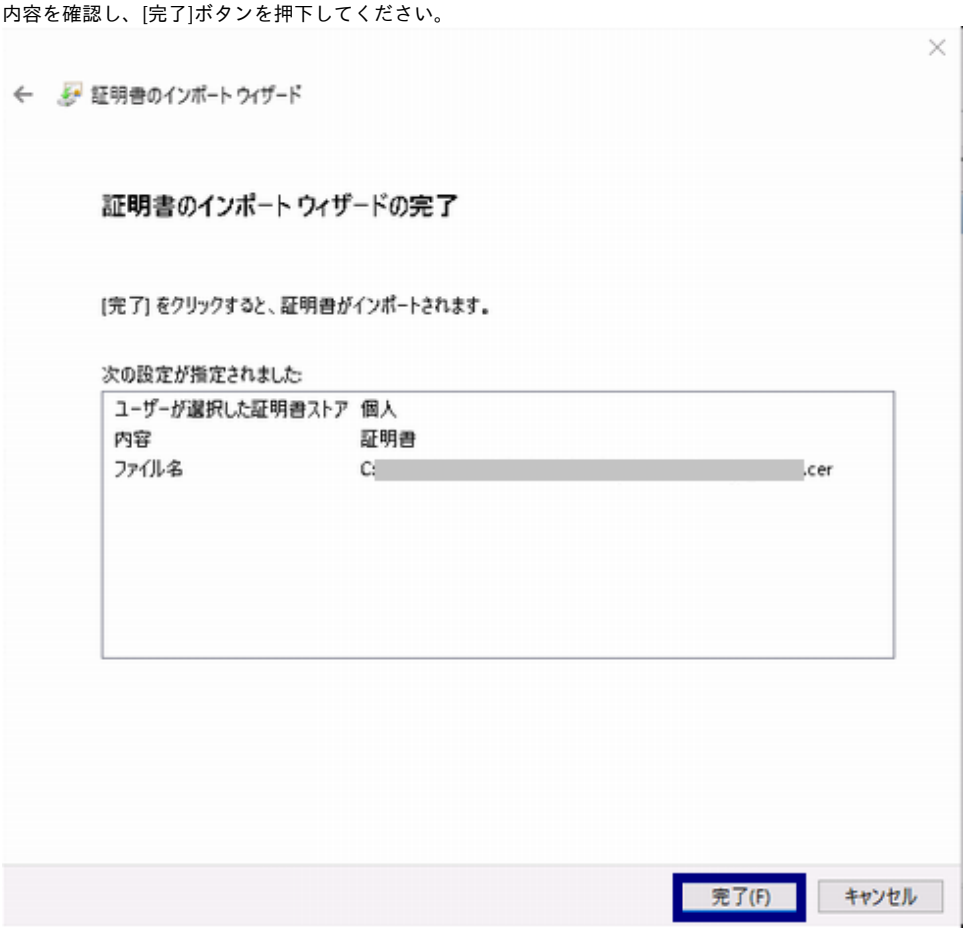


12. 以下の設定になっていることを確認し、[次へ]ボタンを押下してください。

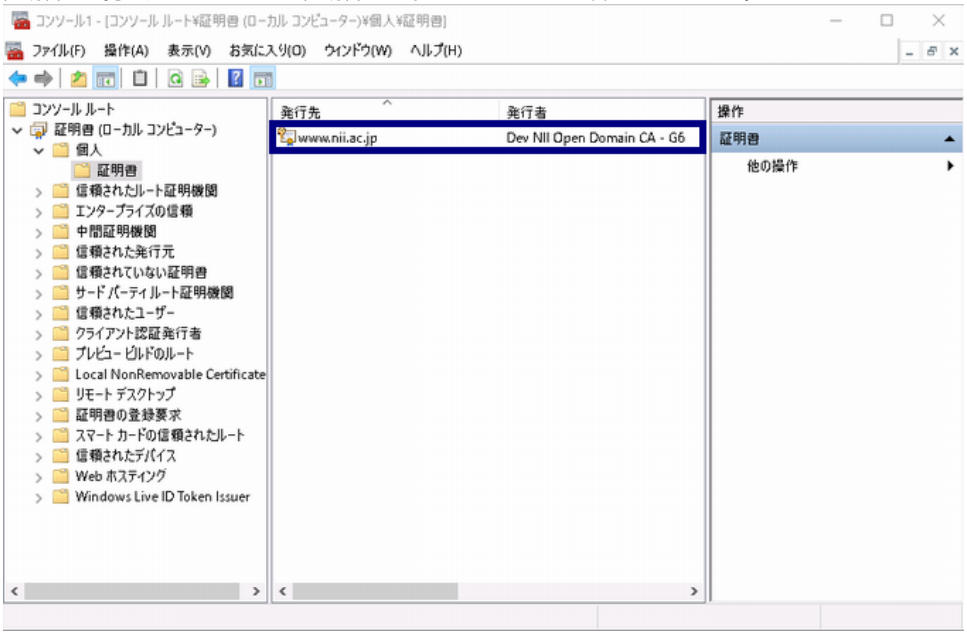
[証明書をすべて次のストアに配置する]を選択
[証明書ストア]で[個人]を指定



13. 内容を確認し、[完了]ボタンを押下してください。




14. 証明書の一覧に、インポートした証明書が登録されていることを確認してください。



# 1-3. サーバ証明書の置き換えインストール

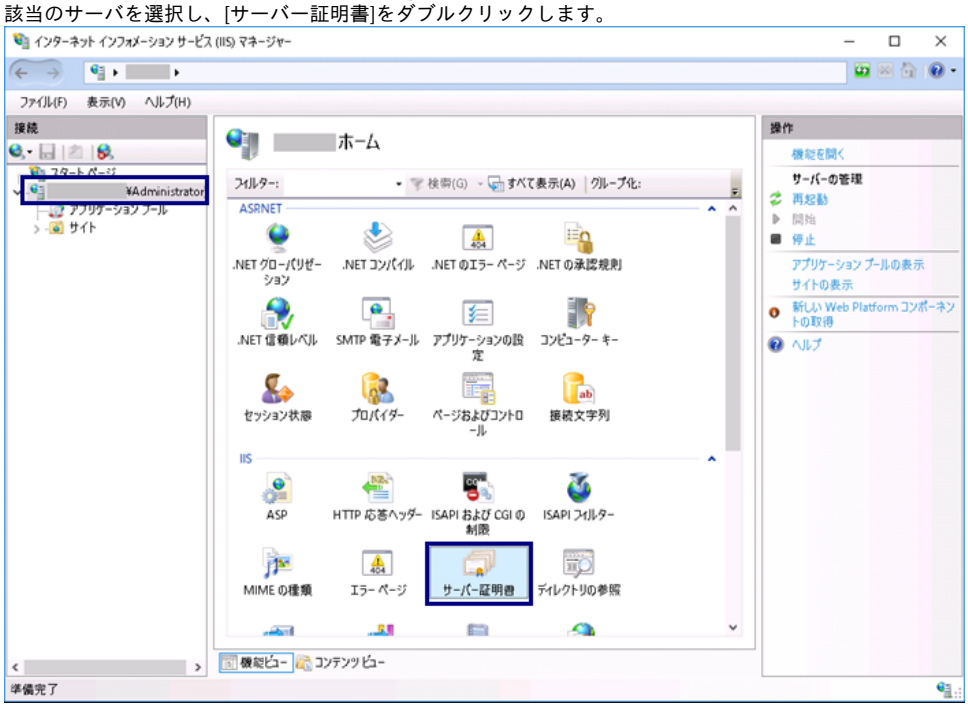
更新したサーバ証明書をインストールする場合は以下の手続きを実施してください。
既に対象のサーバに証明書をインストールしている場合は、事前にインストールしている証明書の削除が必要です。

**サーバ証明書の置き換えインストール**

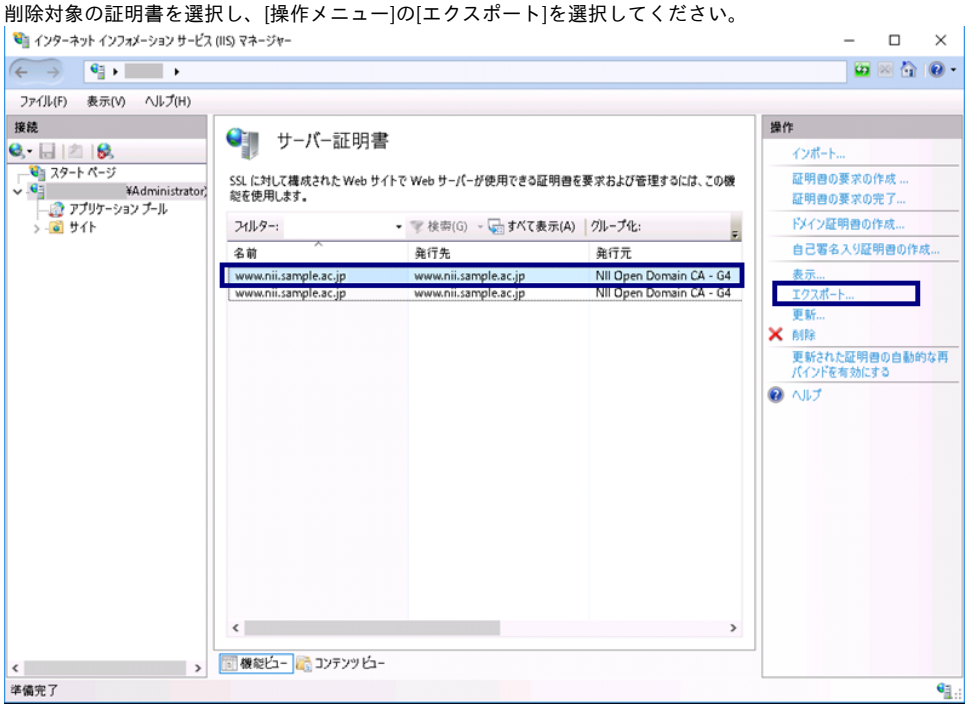
1. 手続き「1-2-1 事前準備」で取得した中間CA証明書を、手続き「1-2-3 中間CA証明書のインストール」に従ってインストールしてください。

2. 手続き「1-2-4 サーバ証明書のインストール」を参照し、更新したサーバ証明書のインストールを実施してください。

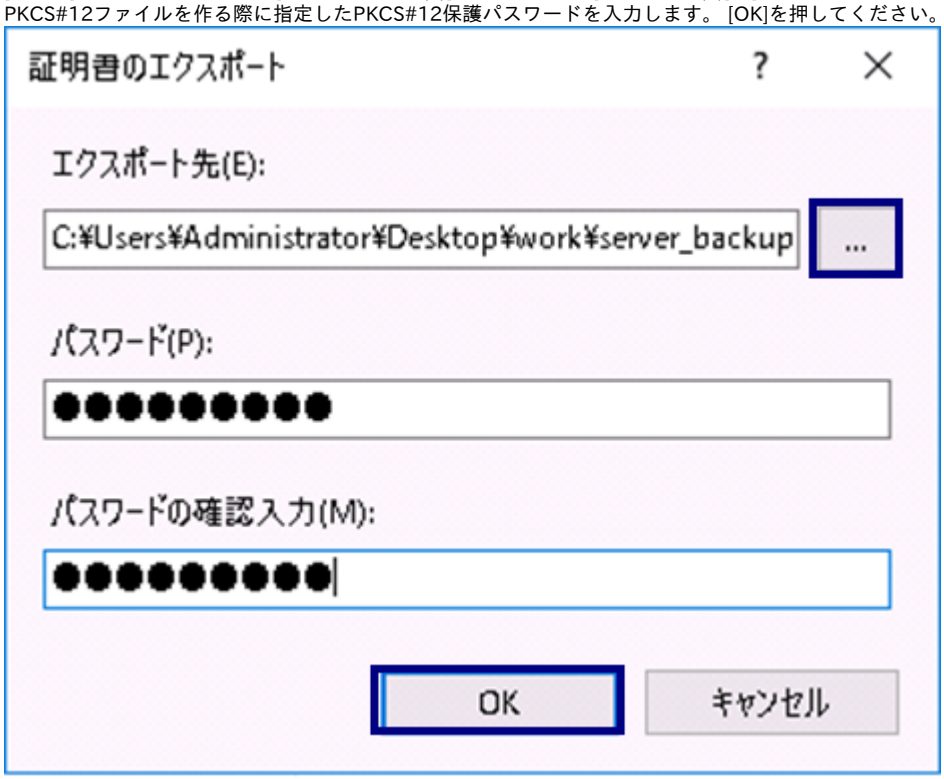
3. サーバ証明書をIISからエクスポートします。[インターネットインフォメーションサービス（IIS）マネージャ]を起動し、
該当のサーバを選択し、[サーバー証明書]をダブルクリックします。




4. 削除対象の証明書を選択し、[操作メニュー]の[エクスポート]を選択してください。



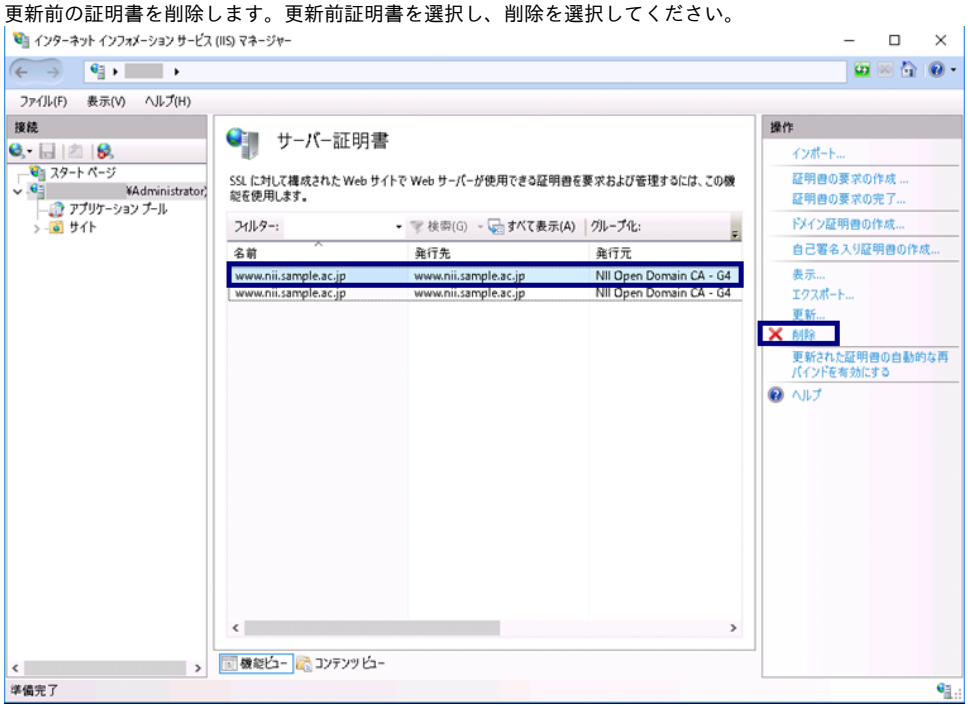
5. [. . . ]ボタンをクリックし、[エクスポート先(E)]を指定します。[パスワード(P)]と[パスワードの確認入力(M)]にPKCS#12ファイルを作る際に指定したPKCS#12保護パスワードを入力します。 [OK]を押してください。



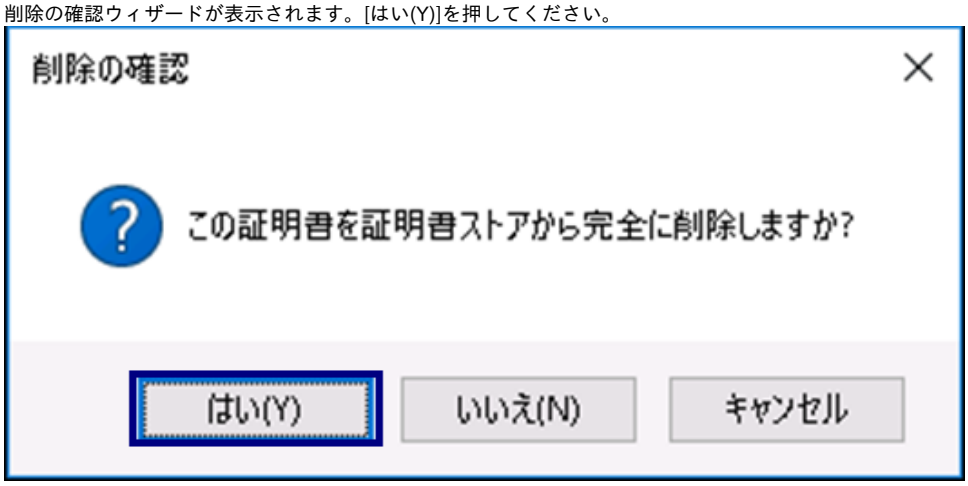

6. 指定したエクスポート先に、エクスポートした証明書が保存されていることを確認してください。



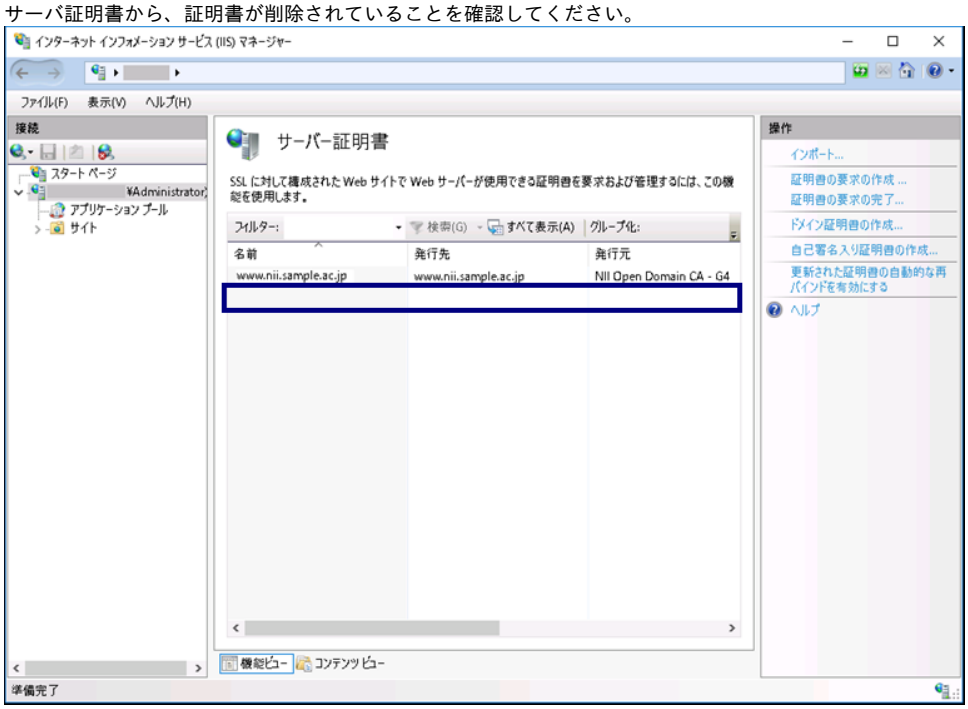

7. 更新前の証明書を削除します。更新前証明書を選択し、削除を選択してください。



8. 削除の確認ウィザードが表示されます。[はい(Y)]を押してください。




9. サーバ証明書から、証明書が削除されていることを確認してください。

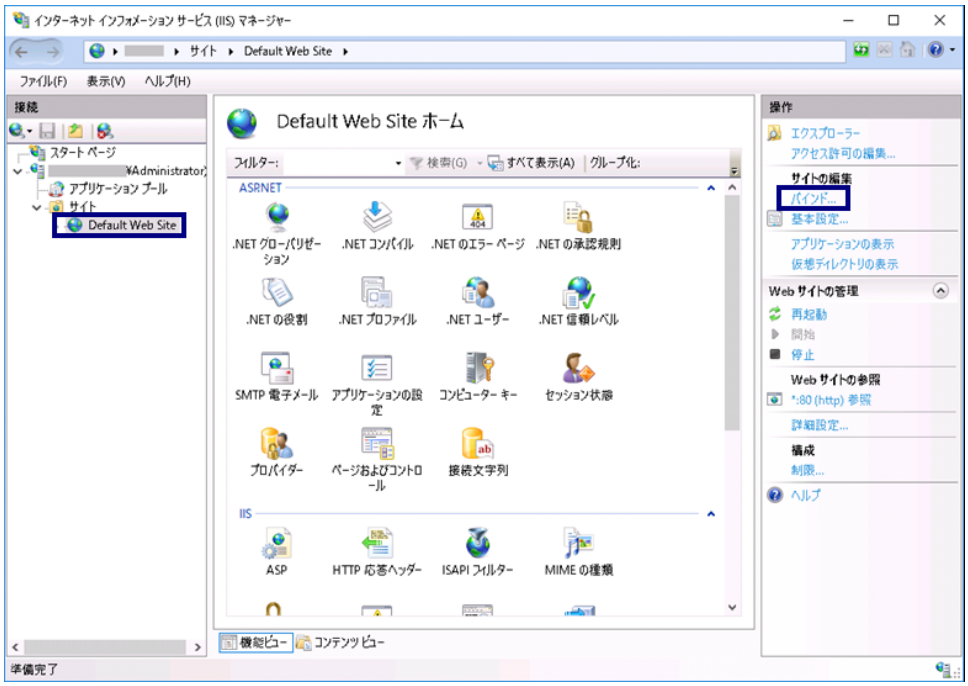



## 1-4. 起動確認

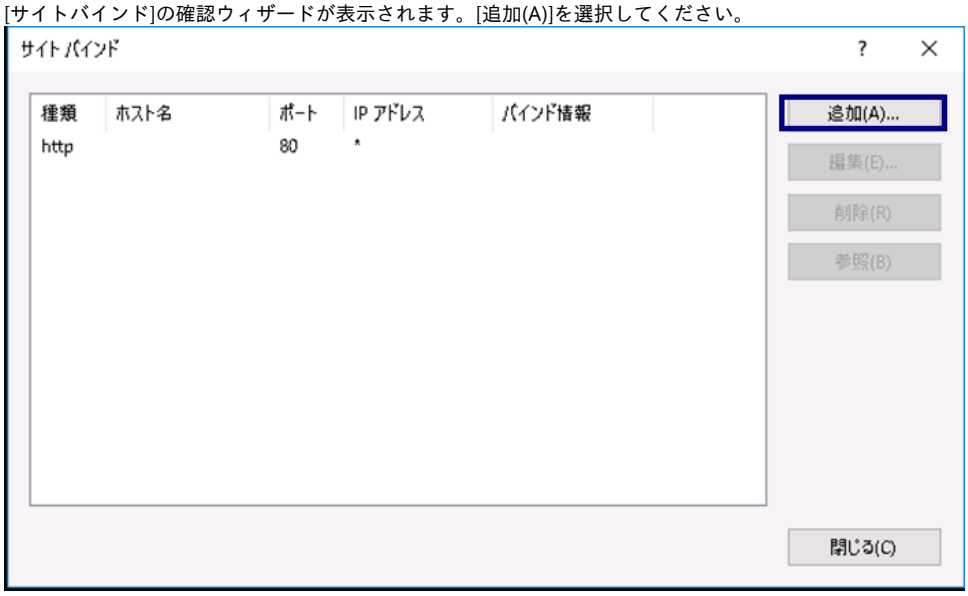
本章ではインストールした証明書によるSSL通信に問題がないか確認する方法を記述します。

| **証明書の反映・確認** |
| --- |
| |

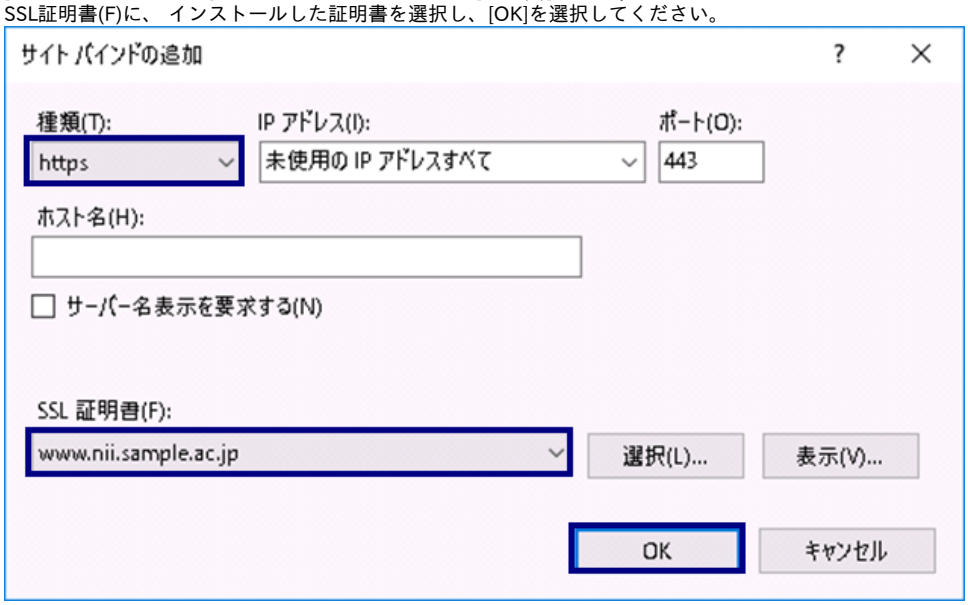
1. [インターネットインフォメーションサービス（IIS）マネージャ]を起動し、該当のサーバを選択し、 [バインド]を選択してください



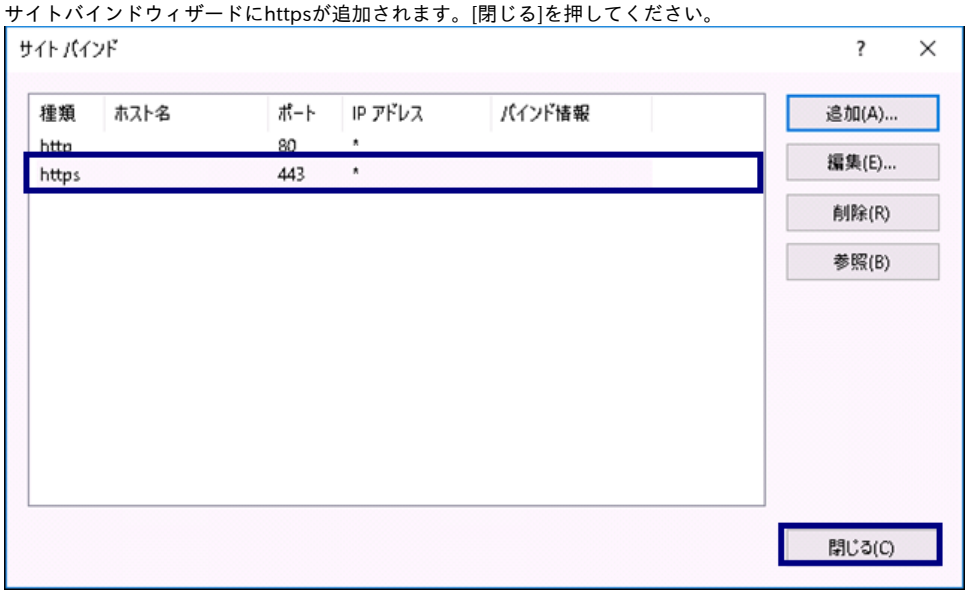

2. [サイトバインド]の確認ウィザードが表示されます。[追加(A)]を選択してください。



3. [サイトバインドの追加]ウィザードが表示されます。[種類(T)]に、httpsを選択します。
SSL証明書(F)に、 インストールした証明書を選択し、[OK]を選択してください。




4. サイトバインドウィザードにhttpsが追加されます。[閉じる]を押してください。




5. 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。

[操作]メニューの[証明書の要求の完了...]をクリックします