ルート CA 証明書・中間 CA 証明書

インストールマニュアル

（ローカルコンピューター環境へのインストール用）

Ver.1.04

AMANO

アマノセキュアジャパン株式会社

目次

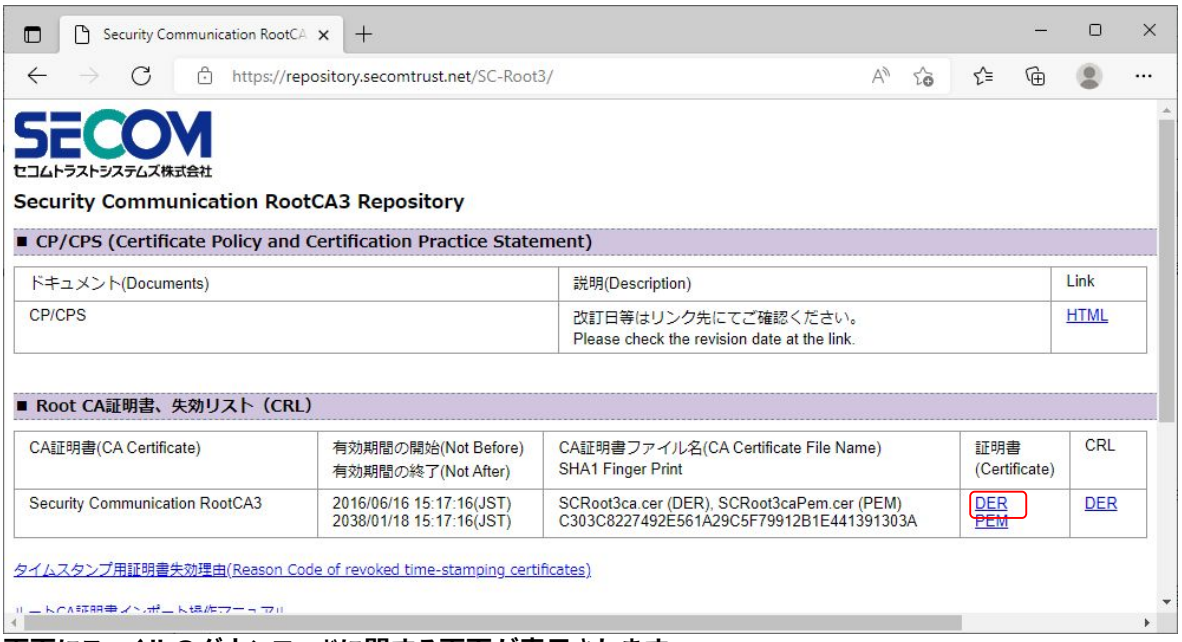
1. ルート CA 証明書・中間 CA 証明書の設定

タイムスタンプを生成･検証するためには、セコムトラストシステムズ株式会社が発行する電子証明書（ルート CA 証明書及び中間 CA 証明書）を対象の環境にインストールしておく必要があります。ここでは、Windows の証明書ストアに対するルート CA 証明書及び中間 CA 証明書のインストール方法、確認方法について説明します。なお、各証明書がすでにインストールされている環境では、インストール作業は不要です。各証明書が対象の環境にインストールされているかどうかの確認方法については、『1.3 ルート CA 証明書の確認』『1.4 中間 CA 証明書』を参照してください。

1.1 ルート CA 証明書のインストール

1 ブラウザを起動し、アドレスに「https://repository.secomtrust.net/SC-Root3/」と入力します。
ルート CA 証明書のダウンロードページが表示されます。

2 Security Communication RootCA3 の「DER」をクリックします。

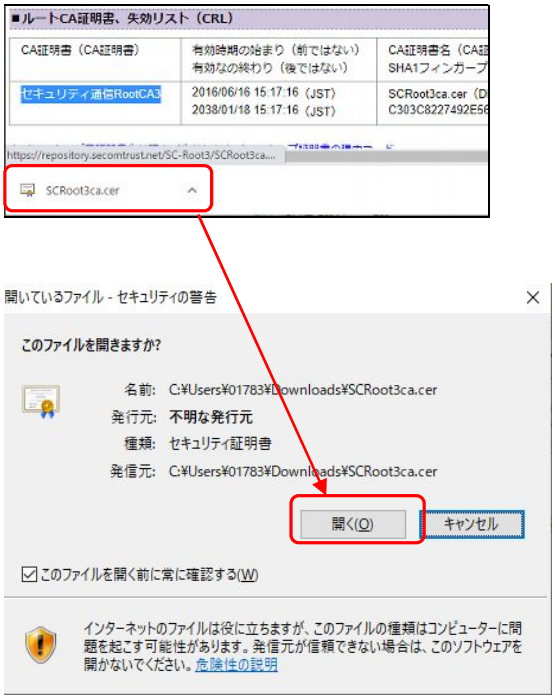


画面にファイルのダウンロードに関する画面が表示されます。

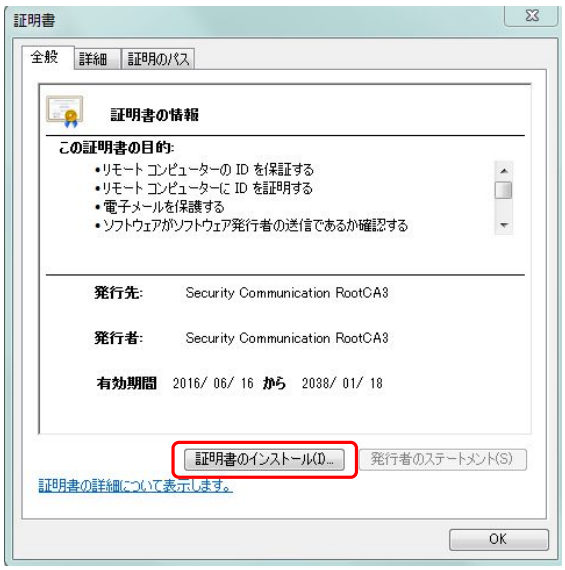
3 ［ファイルを開く］ボタンをクリックします。

［証明書］画面が表示されます。

※．Google Chrome をご利用の場合左下に表示されるダウンロードの案内をクリックした上でファイルを開いてください。

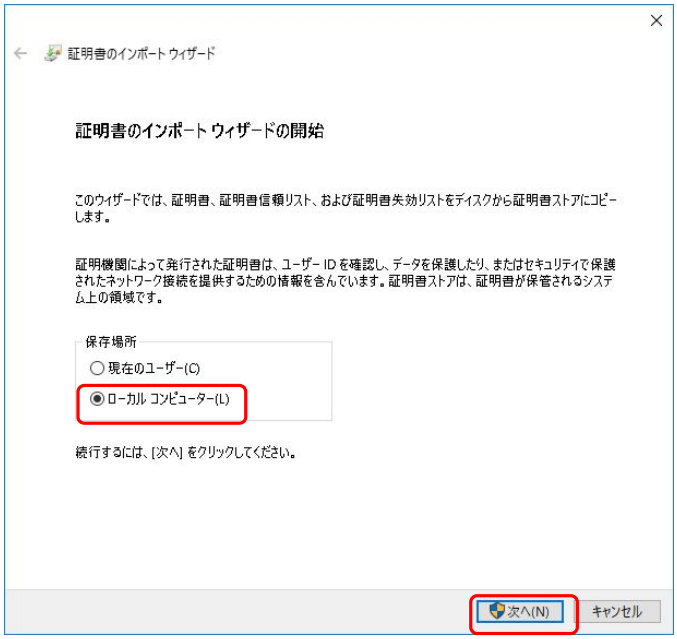


4 [証明書のインストール] ボタンをクリックします。



インポートウィザードの開始画面が表示されます。

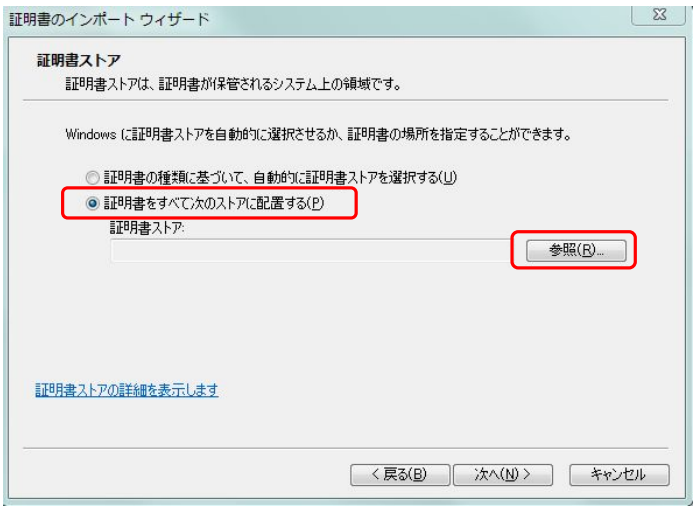
5 [保存場所]で[ローカルコンピューター]を選択し、[次へ]ボタンをクリックします。ユーザーアカウント制御の画面が表示された場合は、[はい]ボタンをクリックしてください。



証明書ストアの選択画面が表示されます。

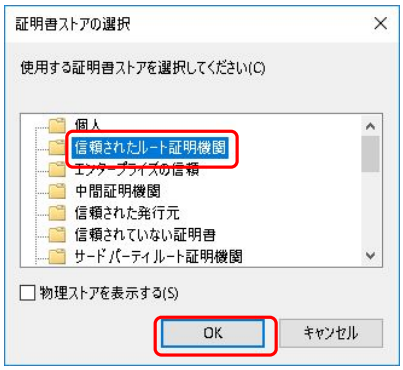
※. ローカルコンピュータの選択ができない場合は 1.1.1 管理コンソールからのインストールに従いインストールを行ってください。

6 [証明書をすべて次のストアに配置する] を選択して、[参照] ボタンをクリックします。



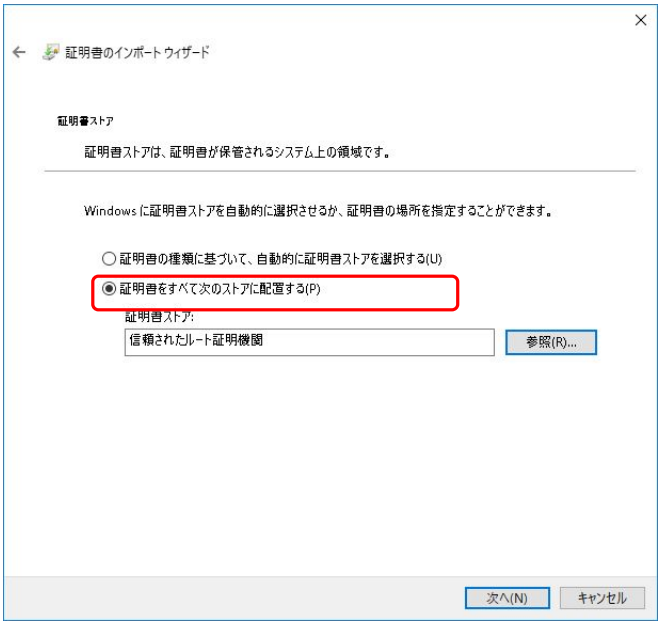
[証明書ストアの選択] 画面が表示されます。

7 [信頼されたルート証明機関]を選択し、[OK]ボタンをクリックします([物理ストアを表示する]の選択は不要)。



証明書のインポートウィザードが表示されます。

8 [証明書ストア]欄に[信頼されたルート証明機関]が表示されていることを確認し、[次へ]ボタンをクリックします。

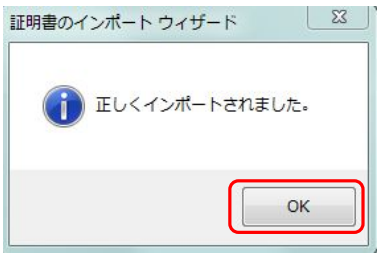


インポートウィザードの完了画面が表示されます。

9 [完了] ボタンをクリックします。

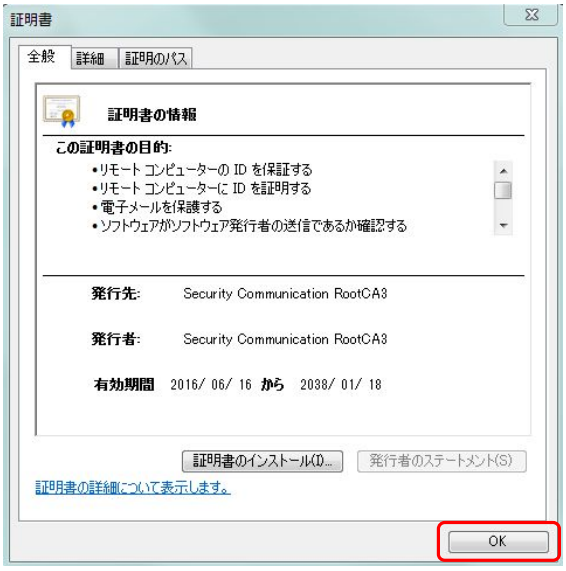
インポート完了のダイアログボックスが表示されます。

10 [OK] ボタンをクリックします。



ダイアログボックスが閉じます。

11 [OK] ボタンをクリックします。



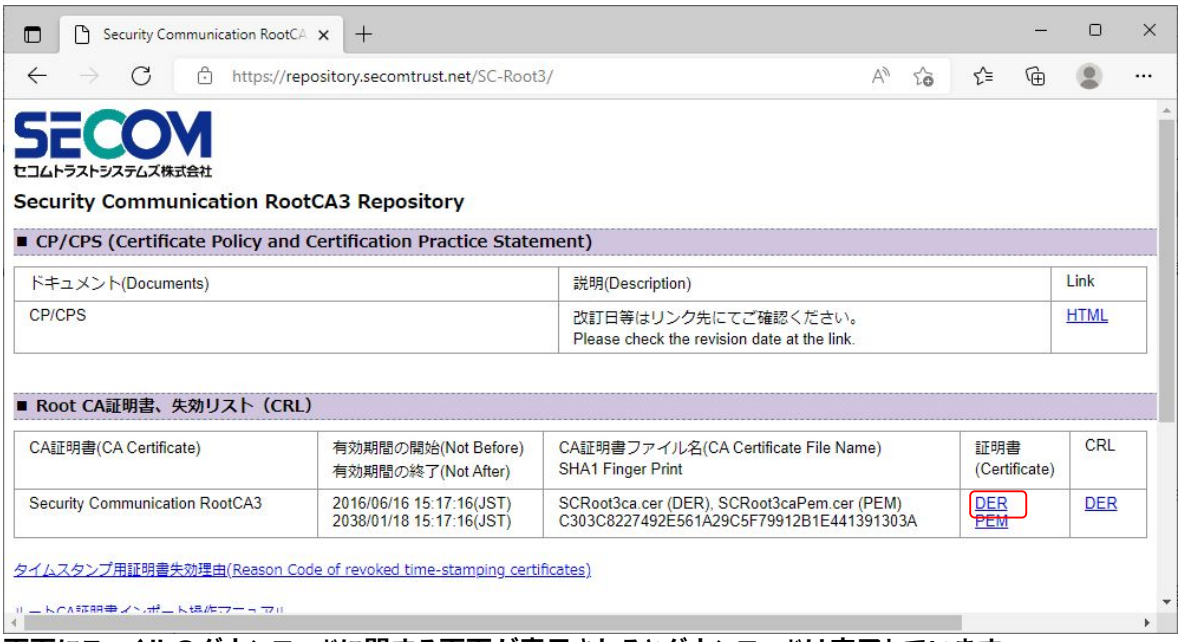
[証明書] 画面が閉じます。

1.1.1 ルート CA 証明書のインストール (管理コンソールからのインストール)

[証明書ストアの選択]画面に「ローカルコンピューター」が表示されない場合は、以下の手順で、ルート証明書 (SCRoot3ca.cer) をパソコンに保存し、管理コンソールからルート証明書をインストールしてください。前項の手順でインストールが完了している場合、本項目の操作は不要です。

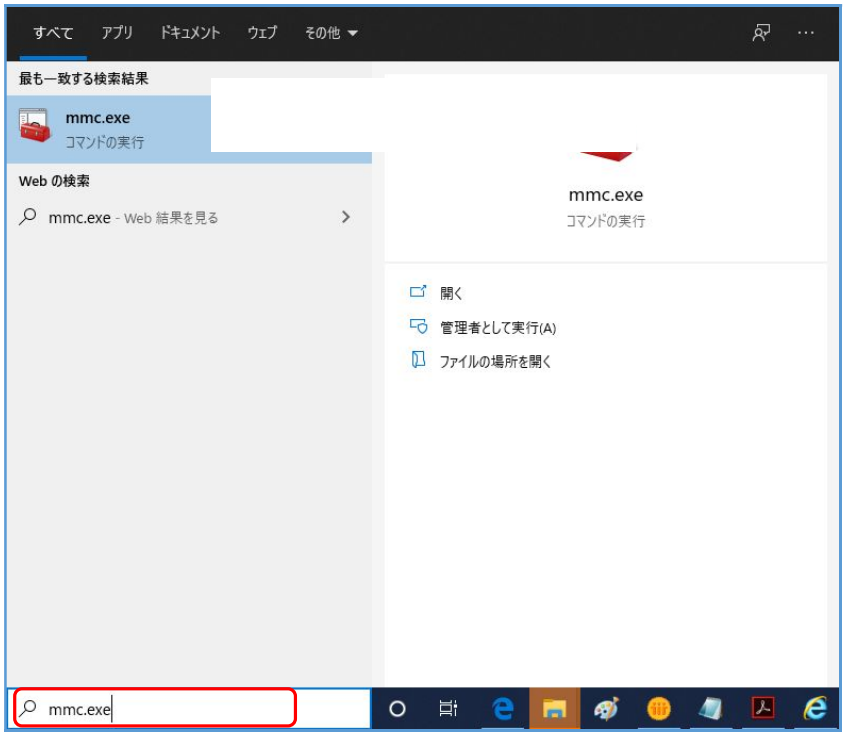
1 ブラウザを起動し、アドレスに「https://repository.secomtrust.net/SC-Root3/」と入力します。
ルート CA 証明書のダウンロードページが表示されます。

2 Security Communication RootCA3 の「DER」をクリックします。



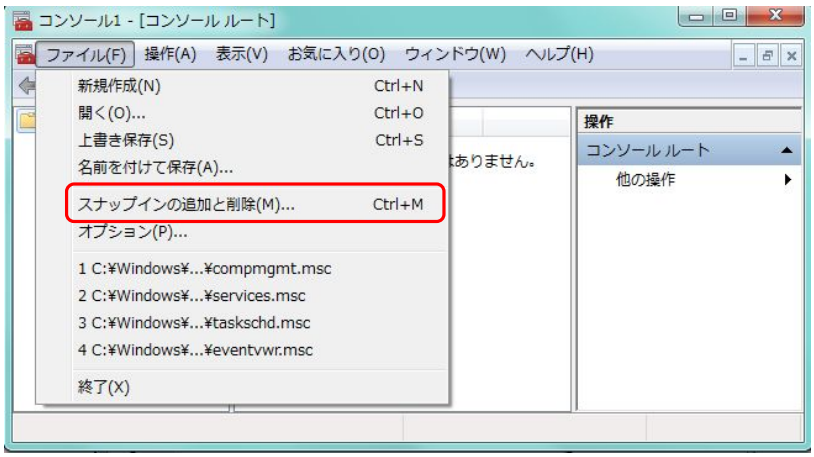
画面にファイルのダウンロードに関する画面が表示されるとダウンロードは完了しています。

3 **スタート画面で「mmc.exe」と入力し Enter キーを押します。**
ユーザーアカウント制御の画面が表示された場合は、[はい] ボタンをクリックしてください。



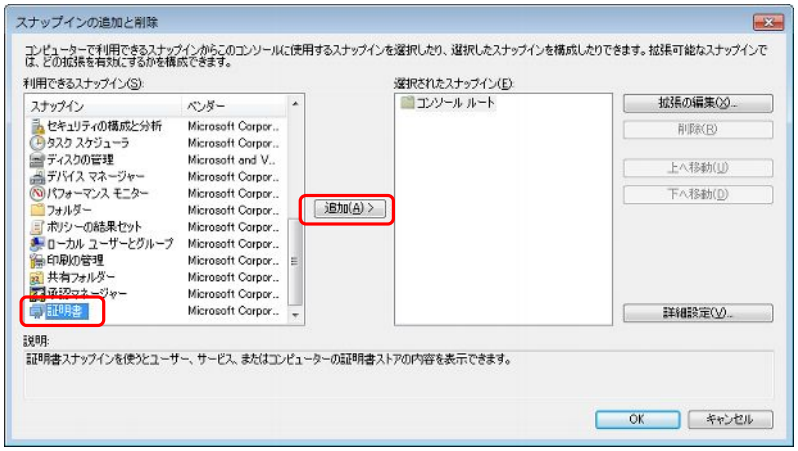
管理コンソールが起動します。

4 メニューバーから [ファイル] ― [スナップインの追加と削除] を選択します。



[スナップインの追加と削除] 画面が表示されます。

5 [利用できるスナップイン] の一覧で [証明書] を選択し、[追加] ボタンをクリックします。

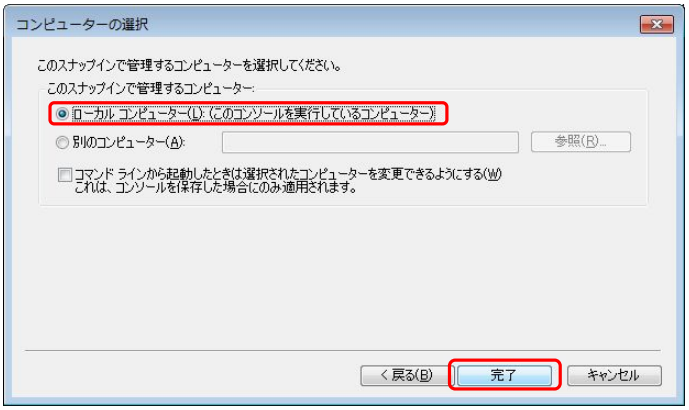


[証明書スナップイン] 画面が表示されます。

6 [このスナップインで管理する証明書] で、[コンピューターアカウント] を選択し、[次へ] ボタンをクリックします。

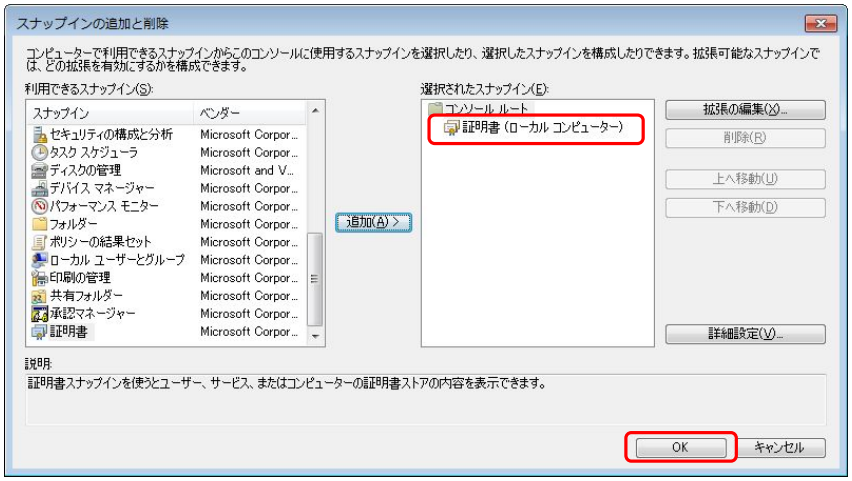
[コンピューターの選択] 画面が表示されます。

7 [このスナップインで管理するコンピューター] で、[ローカルコンピューター (このコンソールを実行しているコンピューター)] を選択し、[完了] ボタンをクリックします。



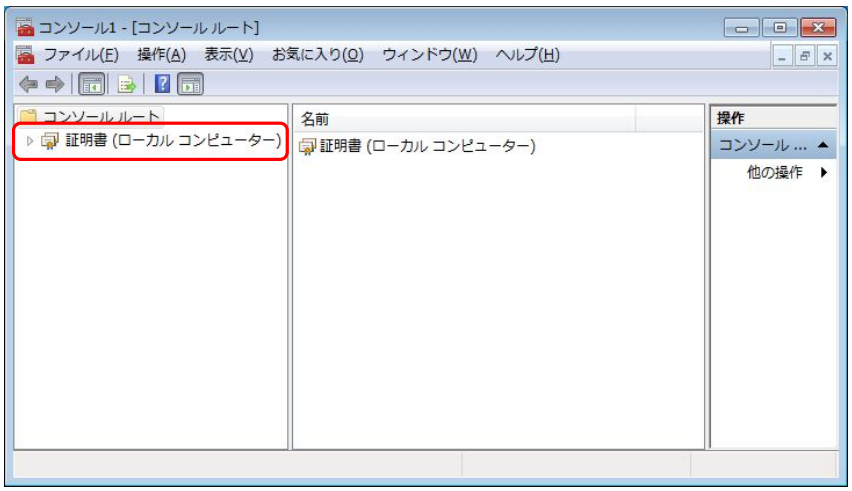
[スナップインの追加と削除] 画面が表示されます。

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) 」が追加されていることを確認し、[OK] ボタンをクリックします。

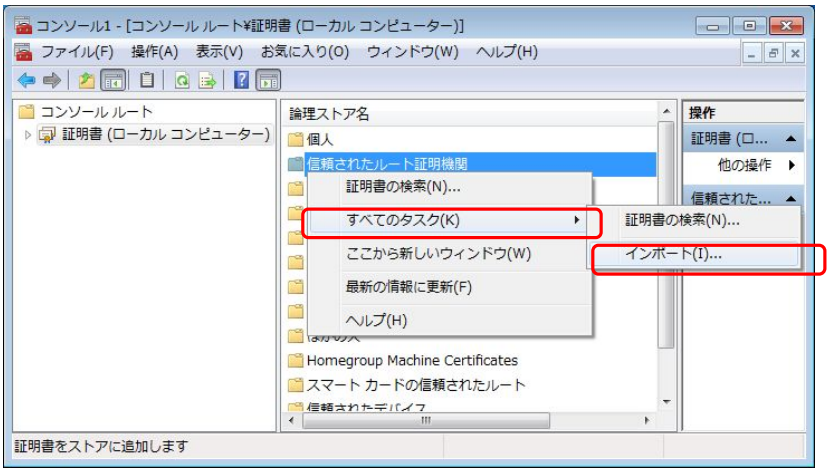


管理コンソールの画面が表示されます。

9 [コンソールルート] にある [証明書 (ローカルコンピューター)] をクリックします。

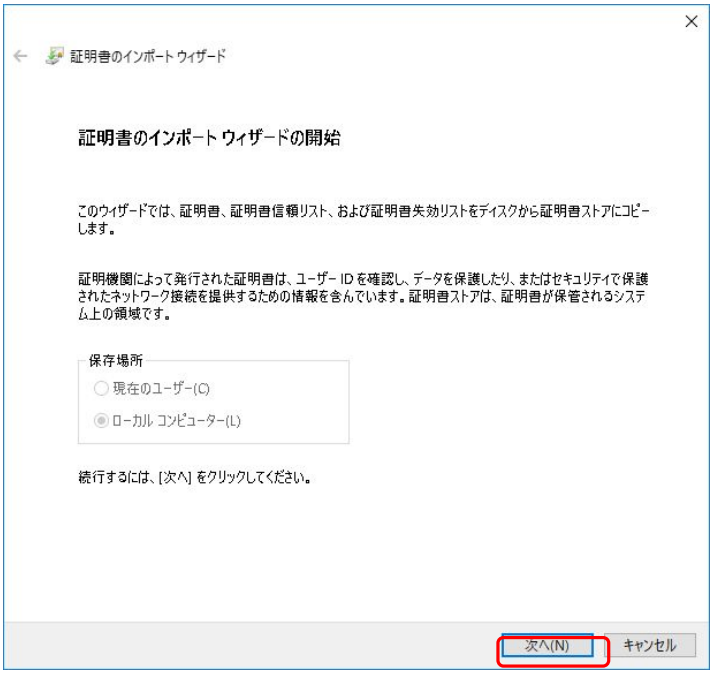


10 [論理ストア名] に表示された [信頼されたルート証明書機関] を右クリックし、[すべてのタスク] ー [インポート] を選択します。



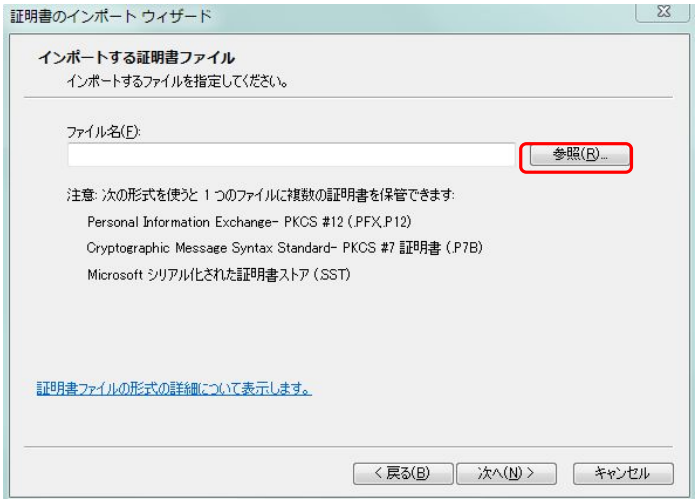
証明書のインポートウィザードの開始画面が表示されます。

11 [次へ] ボタンをクリックします。



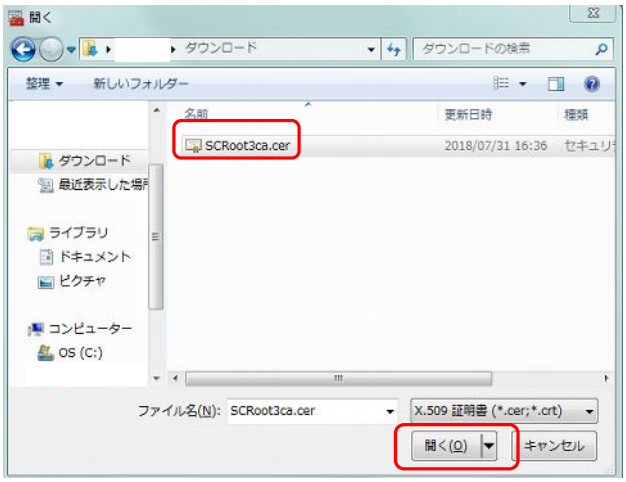
インポートする証明書ファイルの指定画面が表示されます。

12 [参照] ボタンをクリックします。



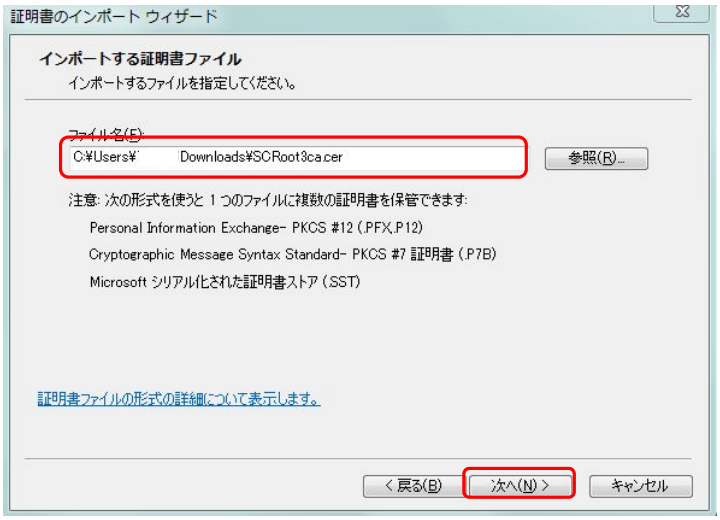
[開く] 画面が表示されます。

13 **手順 3 で保存したルート証明書 (SCRoot3ca.cer) の保存先を指定し、[SCRoot3ca.cer] を選択して [開く] ボタンをクリックします。**



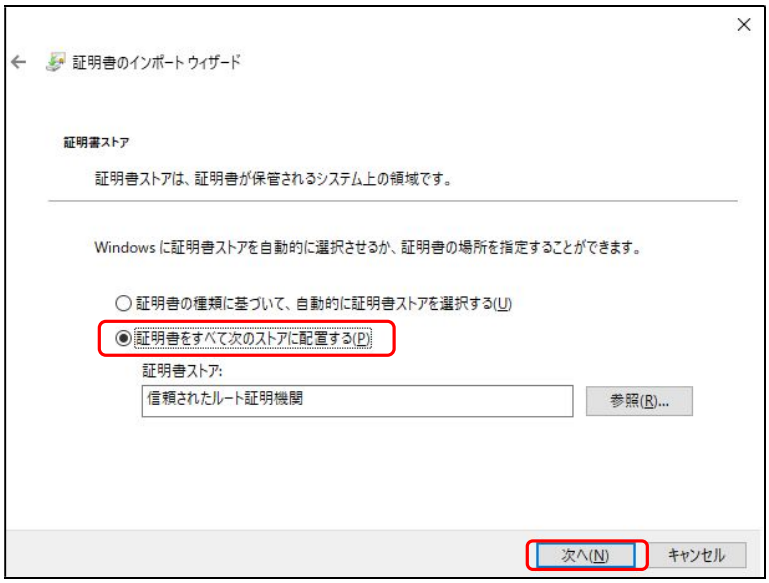
証明書のインポートウィザードが表示されます。

14 **[ファイル名] 欄にルート証明書 (SCRoot3ca.cer) のパス名が表示されていることを確認して、[次へ] ボタンをクリックします。**



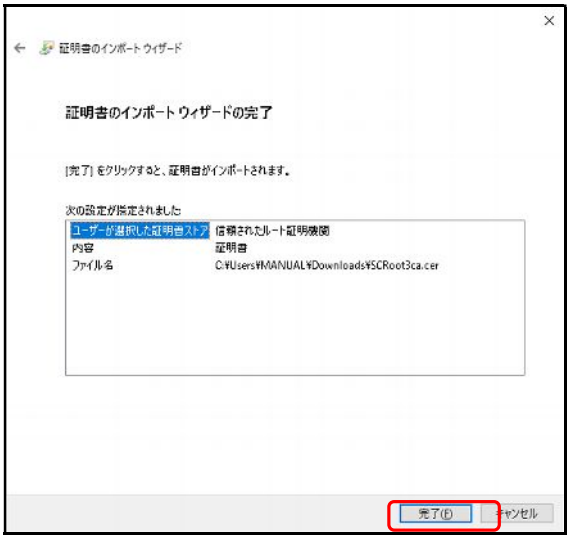
証明書ストアの選択画面が表示されます。

15 [証明書をすべて次のストアに配置する] が選択されていることを確認し、[次へ] ボタンをクリックします。



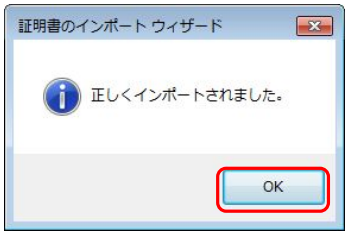
インポートウィザードの完了画面が表示されます。

16 [完了] ボタンをクリックします。



インポート完了のダイアログボックスが表示されます。

17 [OK] ボタンをクリックします。



ダイアログボックスが閉じます。

18 管理コンソール画面右上の [閉じる] ボタンをクリックします。

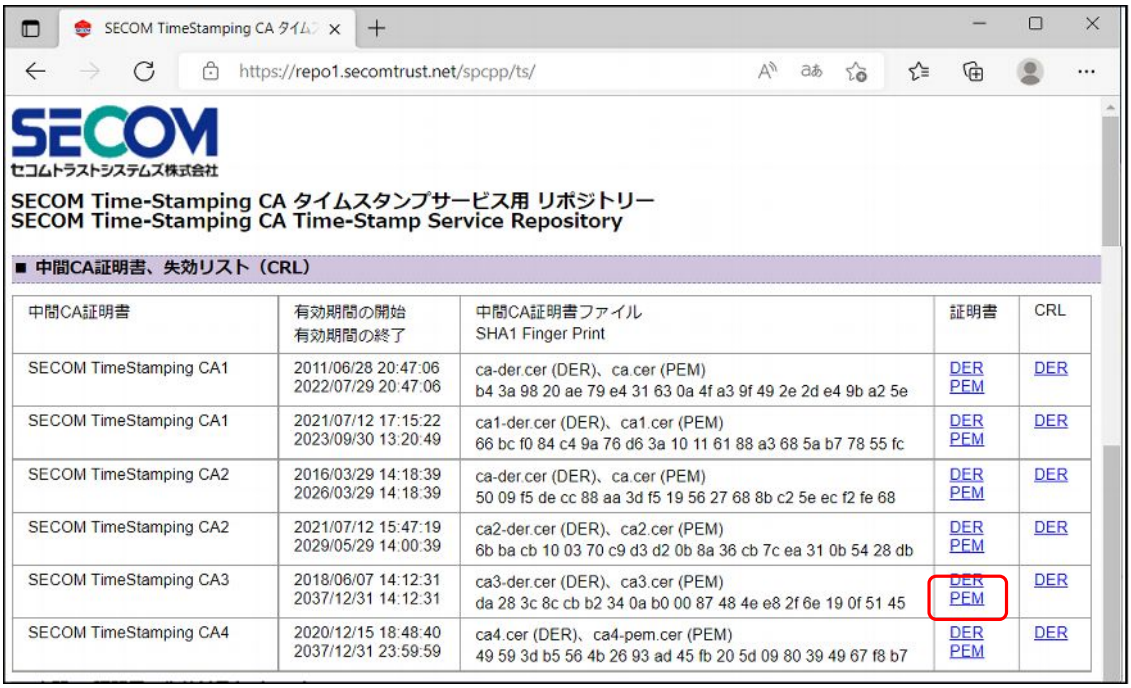
管理コンソール画面が閉じ、設定の保存を確認するダイアログボックスが表示されます。

29 [いいえ] ボタンをクリックします。

1.2 中間 CA 証明書のインストール

1 ブラウザを起動し、アドレスに「https://repo1.secomtrust.net/spcpp/ts/」と入力します。
中間 CA 証明書のダウンロードページが表示されます。

2 中間 CA 証明書、失効リストの SECOM TimeStamping CA3 の [DER] をクリックします。



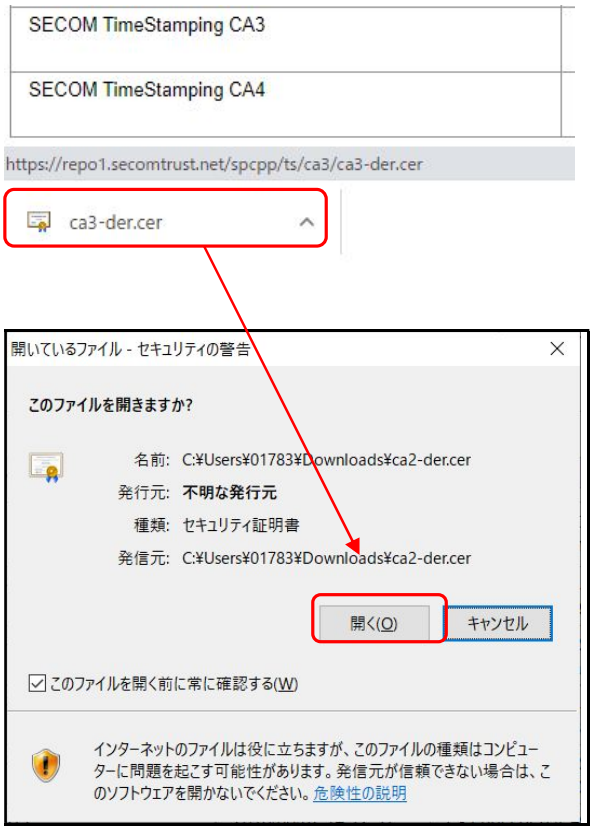
中間CA証明書	有効期間の開始 有効期間の終了	中間CA証明書ファイル SHA1 Finger Print	証明書	CRL
SECOM TimeStamping CA1	2011/06/28 20:47:06 2022/07/29 20:47:06	ca-der.cer (DER)、ca.cer (PEM) b4 3a 98 20 ae 79 e4 31 63 0a 4f a3 9f 49 2e 2d e4 9b a2 5e	DER PEM	DER
SECOM TimeStamping CA1	2021/07/12 17:15:22 2023/09/30 13:20:49	ca1-der.cer (DER)、ca1.cer (PEM) 66 bc f0 84 c4 9a 76 d6 3a 10 11 61 88 a3 68 5a b7 78 55 fc	DER PEM	DER
SECOM TimeStamping CA2	2016/03/29 14:18:39 2026/03/29 14:18:39	ca-der.cer (DER)、ca.cer (PEM) 50 09 f5 de cc 88 aa 3d f5 19 56 27 68 8b c2 5e ec f2 fe 68	DER PEM	DER
SECOM TimeStamping CA2	2021/07/12 15:47:19 2029/05/29 14:00:39	ca2-der.cer (DER)、ca2.cer (PEM) 6b ba cb 10 03 70 c9 d3 d2 0b 8a 36 cb 7c ea 31 0b 54 28 db	DER PEM	DER
SECOM TimeStamping CA3	2018/06/07 14:12:31 2037/12/31 14:12:31	ca3-der.cer (DER)、ca3.cer (PEM) da 28 3c 8c cb b2 34 0a b0 00 87 48 4e e8 2f 6e 19 0f 51 45	DER PEM	DER
SECOM TimeStamping CA4	2020/12/15 18:48:40 2037/12/31 23:59:59	ca4.cer (DER)、ca4-pem.cer (PEM) 49 59 3d b5 56 4b 26 93 ad 45 fb 20 5d 09 80 39 49 67 f8 b7	DER PEM	DER

※画面は途中省略しています。下へスクロールすると中間 CA 証明書、失効リストが表示されます。

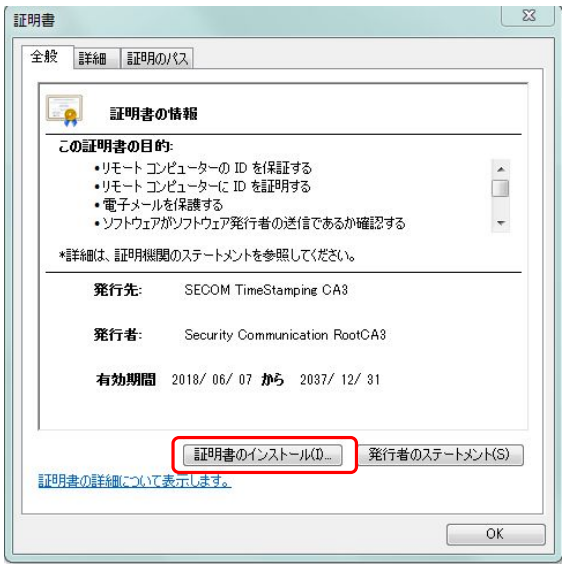
3 ［ファイルを開く］ボタンをクリックします。

［証明書］画面が表示されます。

※．Google Chrome をご利用の場合左下に表示されるダウンロードの案内をクリックした上でファイルを開いてください。

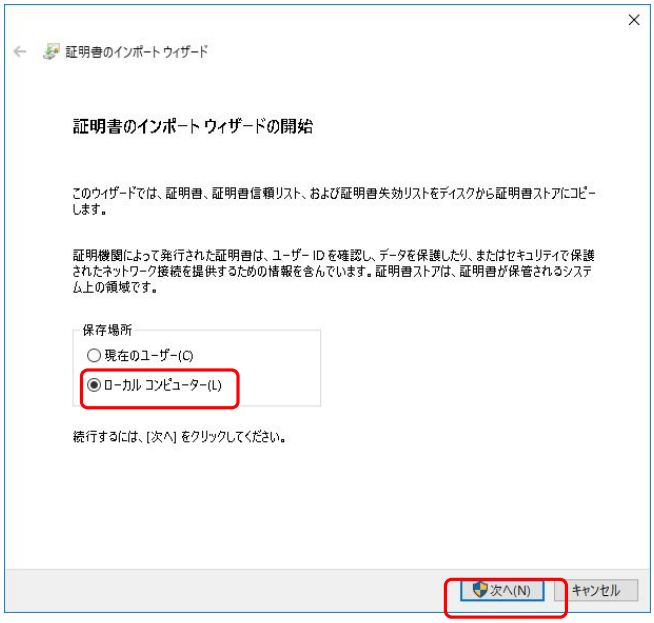


4 [証明書のインストール] ボタンをクリックします。



インポートウィザードの開始画面が表示されます。

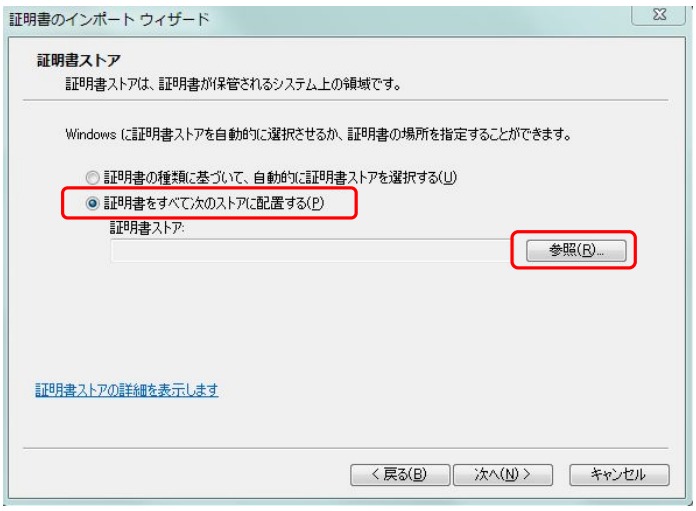
5 [保存場所]で[ローカルコンピューター]を選択し、[次へ]ボタンをクリックします。
ユーザーアカウント制御の画面が表示された場合は、[はい]ボタンをクリックしてください。



証明書ストアの選択画面が表示されます。

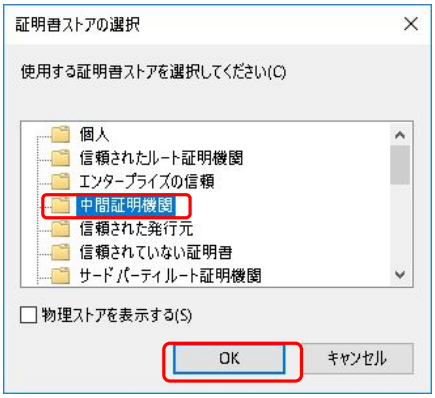
※ ローカルコンピュータが指定できない場合は 1.2.1 管理コンソールからのインストールに従いインストールを行ってください。

6 [証明書をすべて次のストアに配置する] を選択して、[参照] ボタンをクリックします。



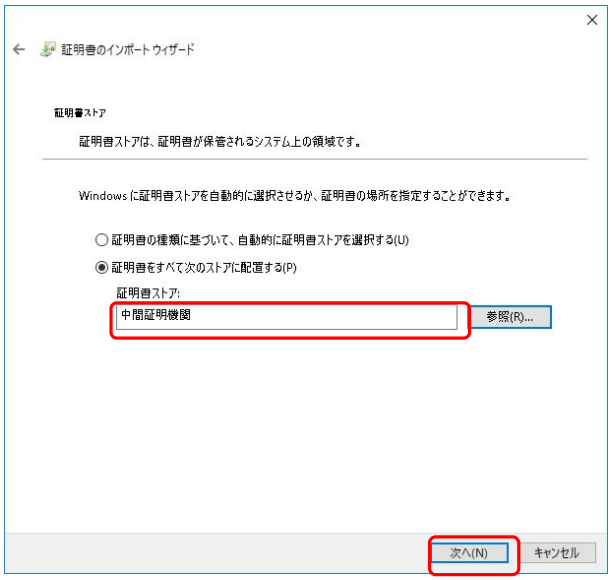
[証明書ストアの選択] 画面が表示されます。

7 [中間証明機関]を選択し、[OK]ボタンをクリックします。



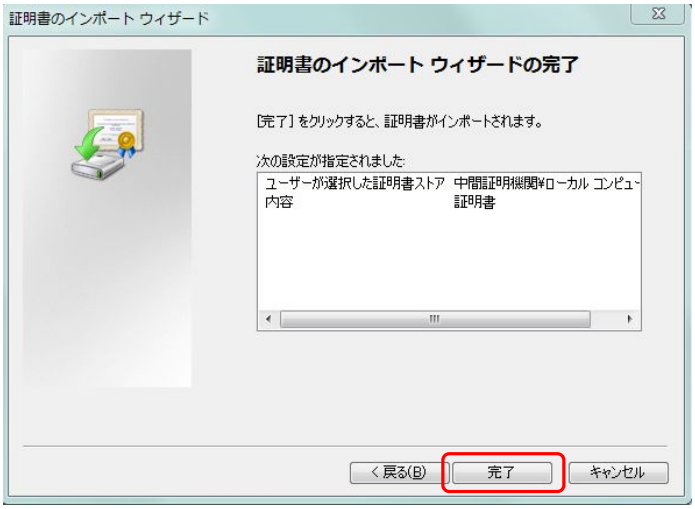
証明書のインポートウィザードが表示されます。

8 [証明書ストア]欄に[中間証明機関]が表示されていることを確認し、[次へ]ボタンをクリックします。



インポートウィザードの完了画面が表示されます。

9 [完了] ボタンをクリックします。

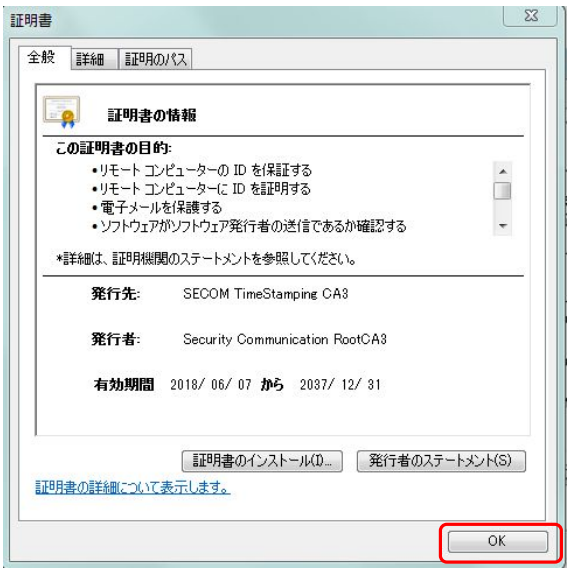


インポート完了のダイアログボックスが表示されます。

10 [OK] ボタンをクリックします。

ダイアログボックスが閉じます。

11 [OK] ボタンをクリックします。



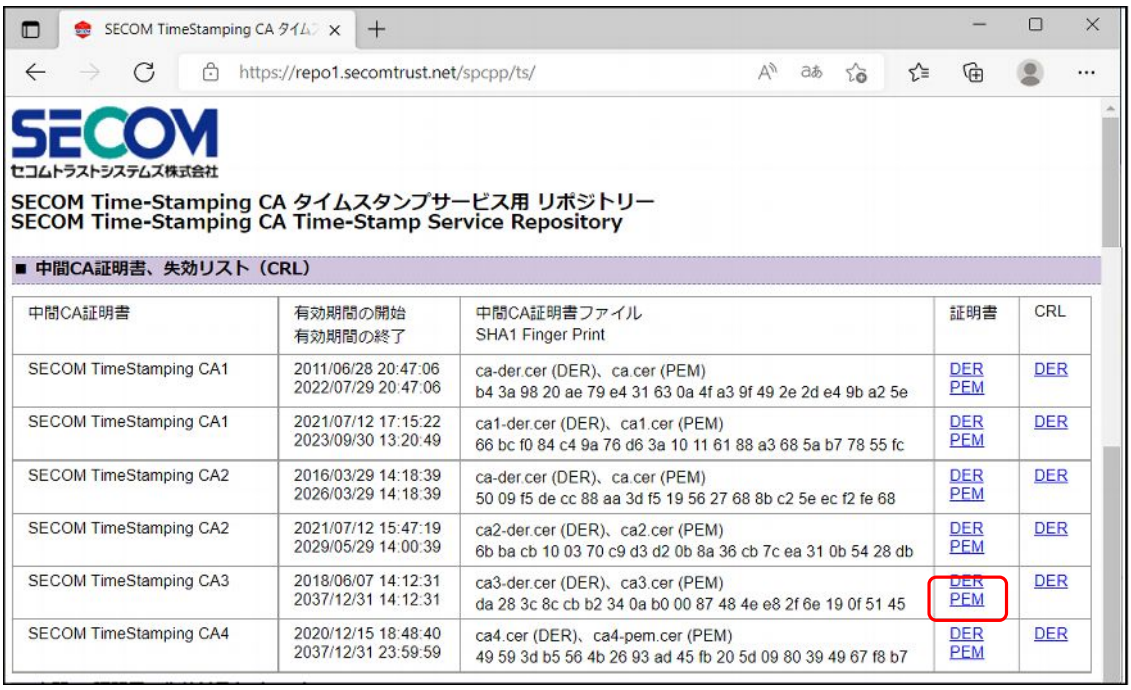
[証明書] 画面が閉じます。

1.2.1 中間 CA 証明書のインストール (管理コンソールからのインストール)

[証明書ストアの選択]画面に「ローカルコンピューター」が表示されない場合は、以下の手順で、中間 CA 証明書 (ca3.cer) をパソコンに保存し、管理コンソールから中間証明書をインストールしてください。前項の手順でインストールが完了している場合、本項目の操作は不要です。

1 ブラウザを起動し、アドレスに「https://repo1.secomtrust.net/spcpp/ts/」と入力します。
中間 CA 証明書のダウンロードページが表示されます。

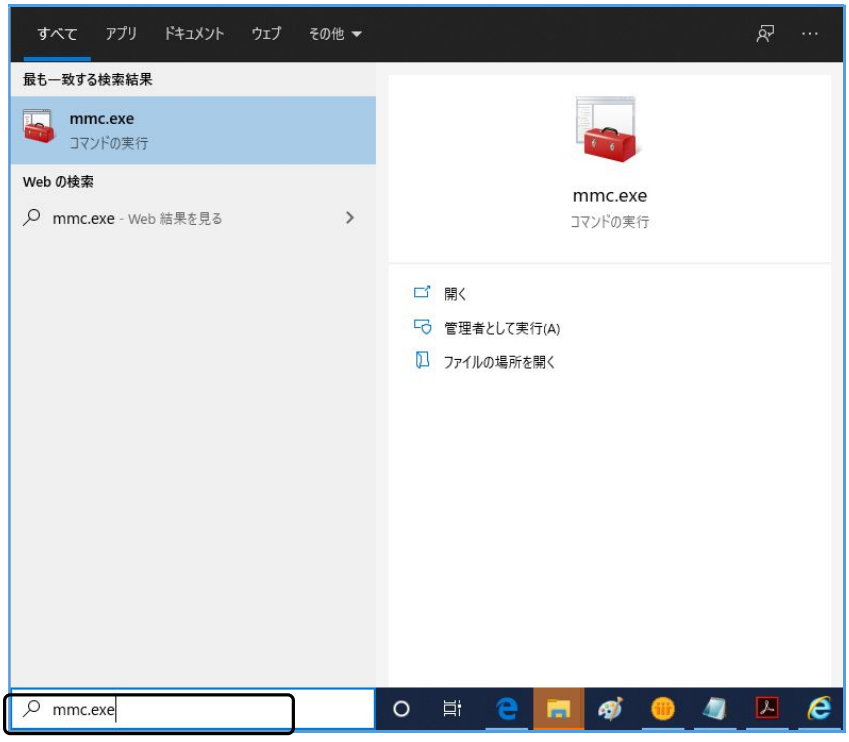
2 **中間 CA 証明書、失効リストの SECOM TimeStamping CA3 の [DER] をクリックします。**



中間CA証明書	有効期間の開始 有効期間の終了	中間CA証明書ファイル SHA1 Finger Print	証明書	CRL
SECOM TimeStamping CA1	2011/06/28 20:47:06 2022/07/29 20:47:06	ca-der.cer (DER)、ca.cer (PEM) b4 3a 98 20 ae 79 e4 31 63 0a 4f a3 9f 49 2e 2d e4 9b a2 5e	DER PEM	DER
SECOM TimeStamping CA1	2021/07/12 17:15:22 2023/09/30 13:20:49	ca1-der.cer (DER)、ca1.cer (PEM) 66 bc f0 84 c4 9a 76 d6 3a 10 11 61 88 a3 68 5a b7 78 55 fc	DER PEM	DER
SECOM TimeStamping CA2	2016/03/29 14:18:39 2026/03/29 14:18:39	ca-der.cer (DER)、ca.cer (PEM) 50 09 f5 de cc 88 aa 3d f5 19 56 27 68 8b c2 5e ec f2 fe 68	DER PEM	DER
SECOM TimeStamping CA2	2021/07/12 15:47:19 2029/05/29 14:00:39	ca2-der.cer (DER)、ca2.cer (PEM) 6b ba cb 10 03 70 c9 d3 d2 0b 8a 36 cb 7c ea 31 0b 54 28 db	DER PEM	DER
SECOM TimeStamping CA3	2018/06/07 14:12:31 2037/12/31 14:12:31	ca3-der.cer (DER)、ca3.cer (PEM) da 28 3c 8c cb b2 34 0a b0 00 87 48 4e e8 2f 6e 19 0f 51 45	DER PEM	DER
SECOM TimeStamping CA4	2020/12/15 18:48:40 2037/12/31 23:59:59	ca4.cer (DER)、ca4-pem.cer (PEM) 49 59 3d b5 56 4b 26 93 ad 45 fb 20 5d 09 80 39 49 67 f8 b7	DER PEM	DER

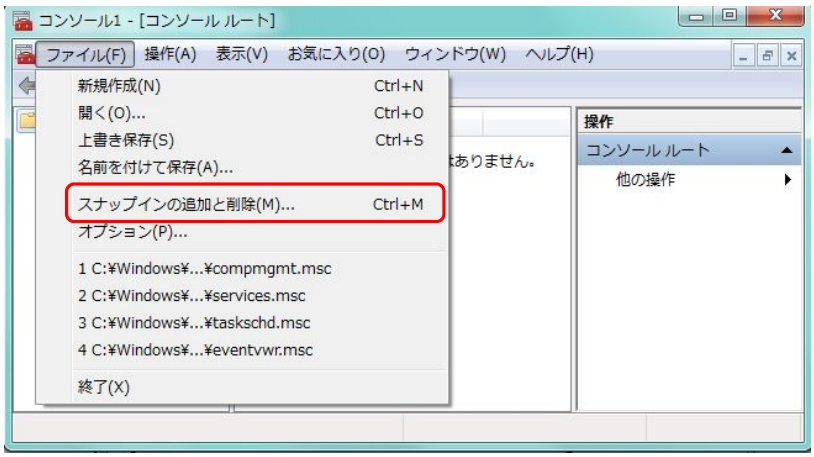
画面にファイルのダウンロードに関する画面が表示されるとダウンロードは完了しています。

3 **スタート画面で「mmc.exe」と入力し Enter キーを押します。**
ユーザーアカウント制御の画面が表示された場合は、[はい] ボタンをクリックしてください。



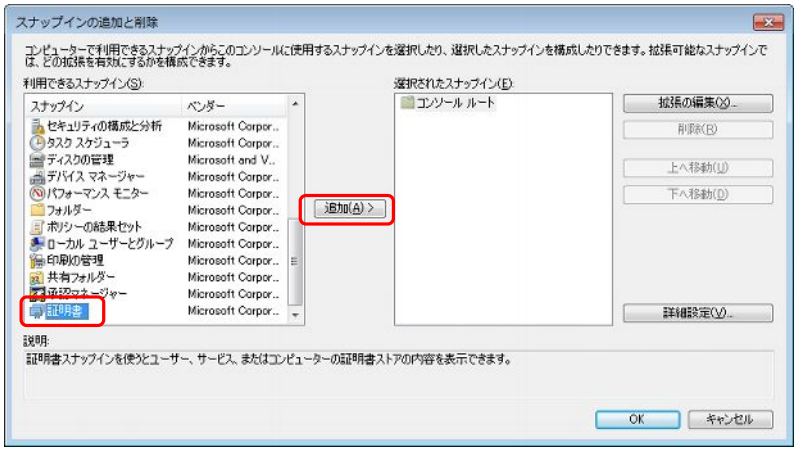
管理コンソールが起動します。

4 メニューバーから [ファイル] ― [スナップインの追加と削除] を選択します。



[スナップインの追加と削除] 画面が表示されます。

5 [利用できるスナップイン] の一覧で [証明書] を選択し、[追加] ボタンをクリックします。

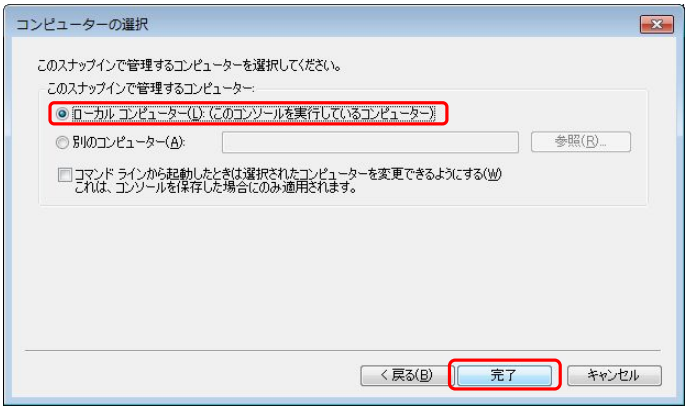


[証明書スナップイン] 画面が表示されます。

6 [このスナップインで管理する証明書] で、[コンピューターアカウント] を選択し、[次へ] ボタンをクリックします。

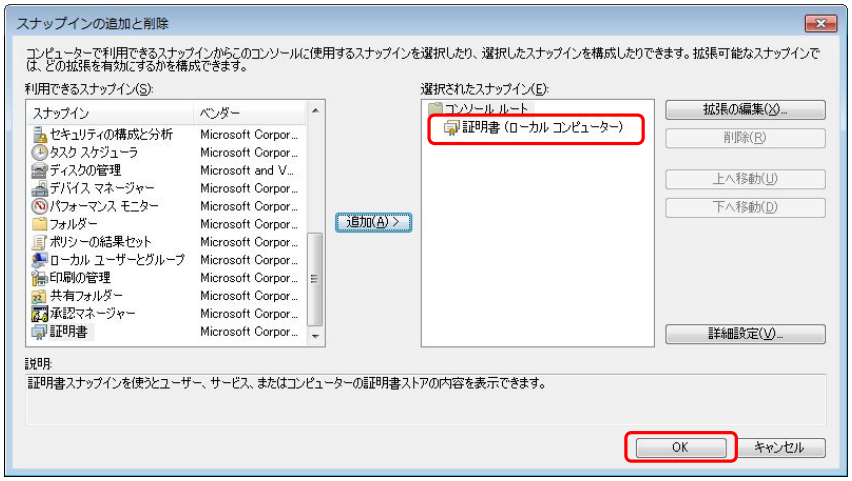
[コンピューターの選択] 画面が表示されます。

7 [このスナップインで管理するコンピューター] で、[ローカルコンピューター (このコンソールを実行しているコンピューター)] を選択し、[完了] ボタンをクリックします。



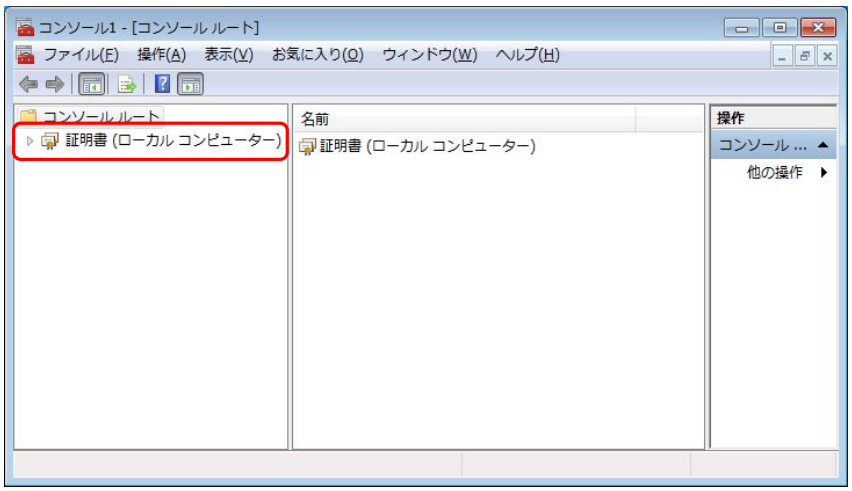
[スナップインの追加と削除] 画面が表示されます。

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) 」が追加されていることを確認し、[OK] ボタンをクリックします。

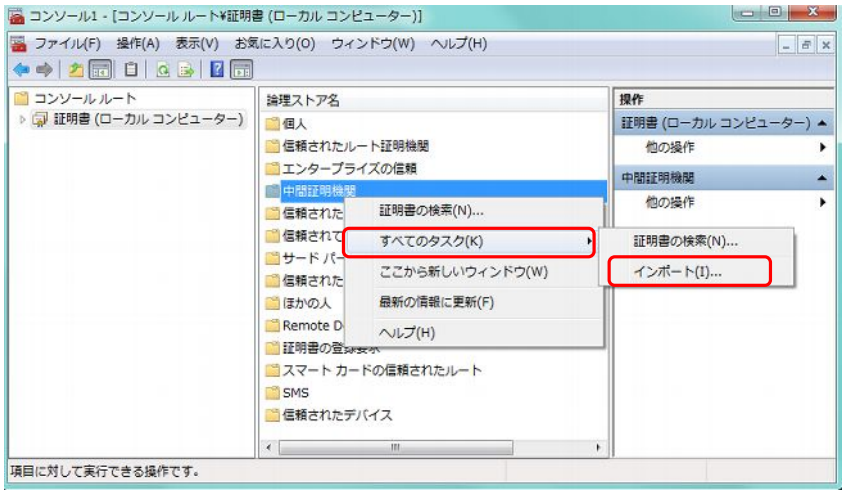


管理コンソールの画面が表示されます。

9 [コンソールルート] にある [証明書 (ローカルコンピューター)] をクリックします。

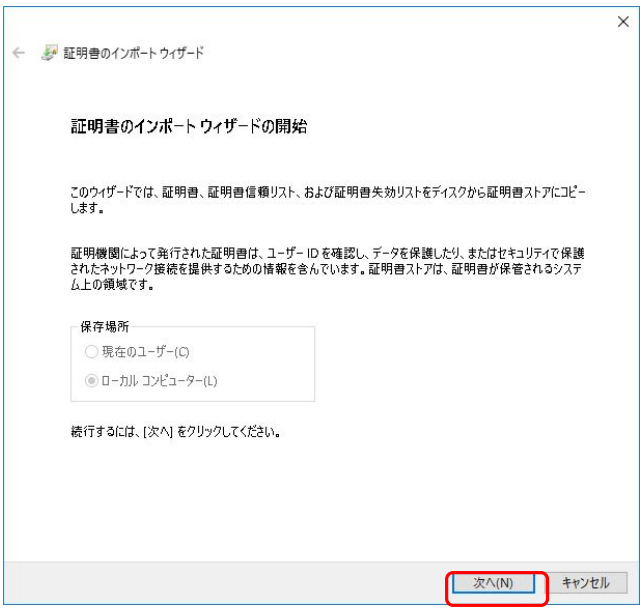


10 [論理ストア名] に表示された [中間証明機関] を右クリックし、[すべてのタスク] ― [インポート] を選択します。



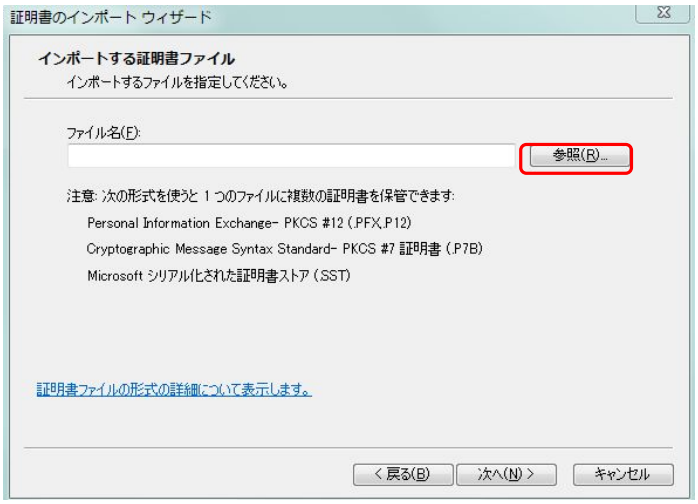
証明書のインポートウィザードの開始画面が表示されます。

11 [次へ] ボタンをクリックします。



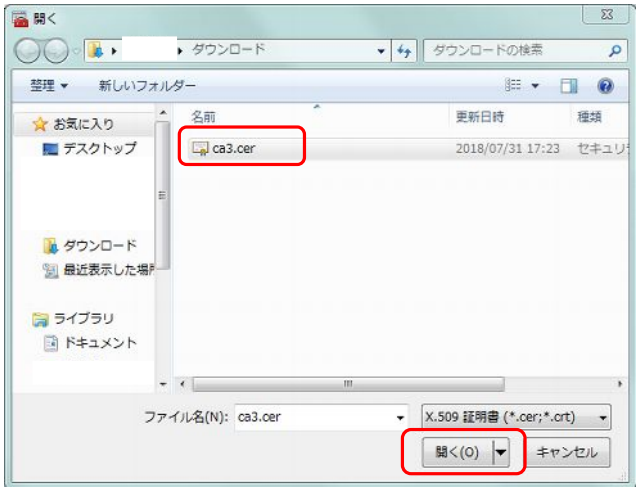
インポートする証明書ファイルの指定画面が表示されます。

12 [参照] ボタンをクリックします。



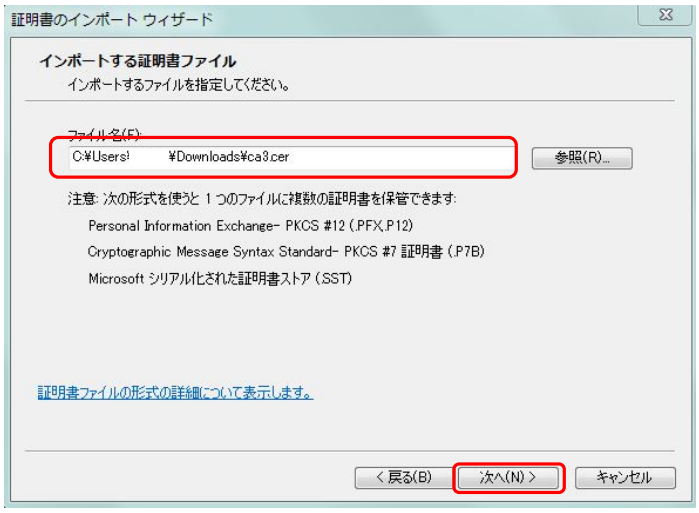
[開く] 画面が表示されます。

13 **手順 3 で保存したルート証明書 (ca3-der.cer) の保存先を指定し、[ca3-der.cer)] を選択して [開く] ボタンをクリックします。(手順3で「DER」を指定した場合は「ca3-der.cer」となります。)**



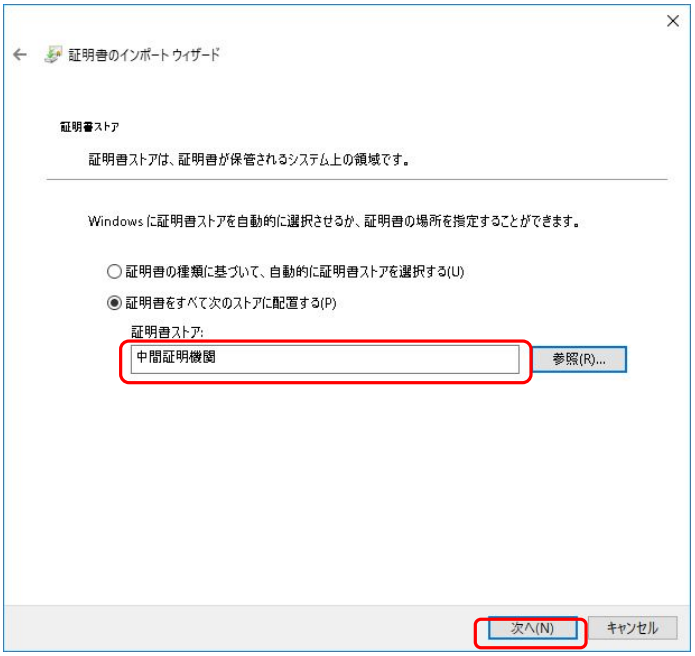
証明書のインポートウィザードが表示されます。

14 **[ファイル名] 欄に中間証明書 (ca3-der.cer)) のパス名が表示されていることを確認して、[次へ] ボタンをクリックします。**



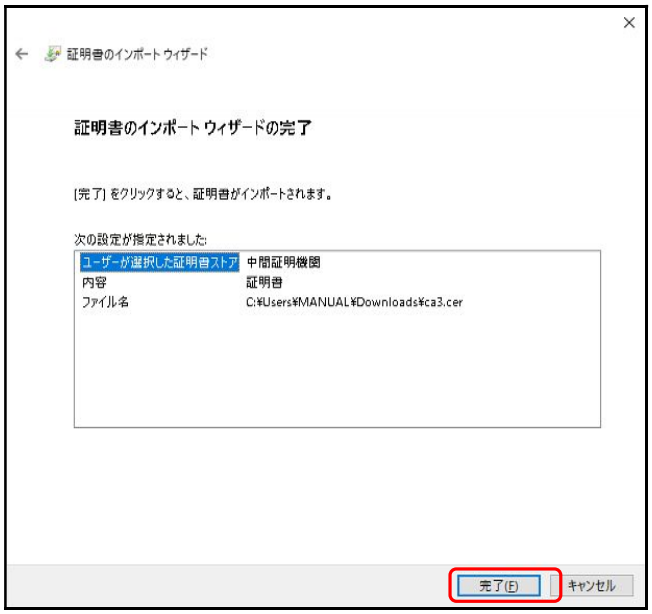
証明書ストアの選択画面が表示されます。

15 [証明書ストア]欄に[中間証明機関]が表示されていることを確認し、[次へ]ボタンをクリックします。



インポートウィザードの完了画面が表示されます。

16 [完了] ボタンをクリックします。



インポート完了のダイアログボックスが表示されます。

17 [OK] ボタンをクリックします。

ダイアログボックスが閉じます。

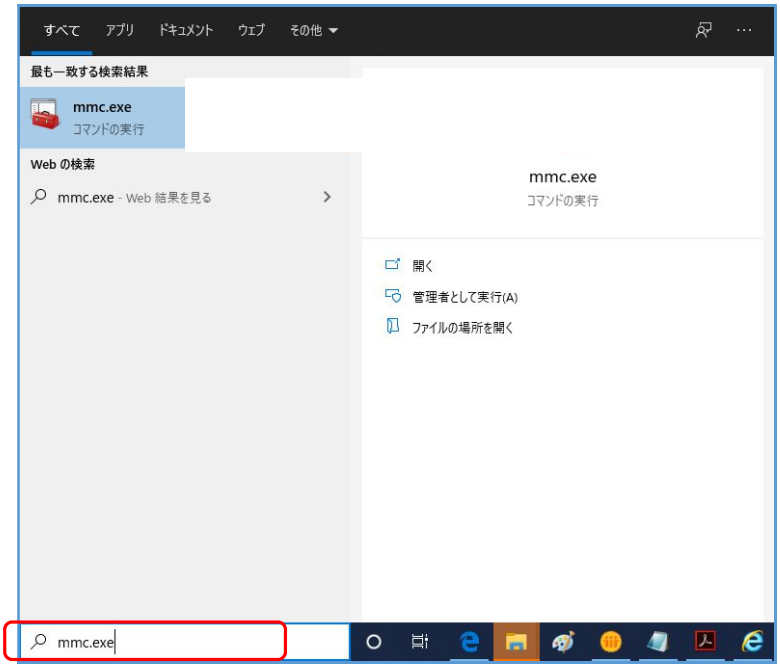
18 管理コンソール画面右上の [閉じる] ボタンをクリックします。

管理コンソール画面が閉じ、設定の保存を確認するダイアログボックスが表示されます。

19 [いいえ] ボタンをクリックします。

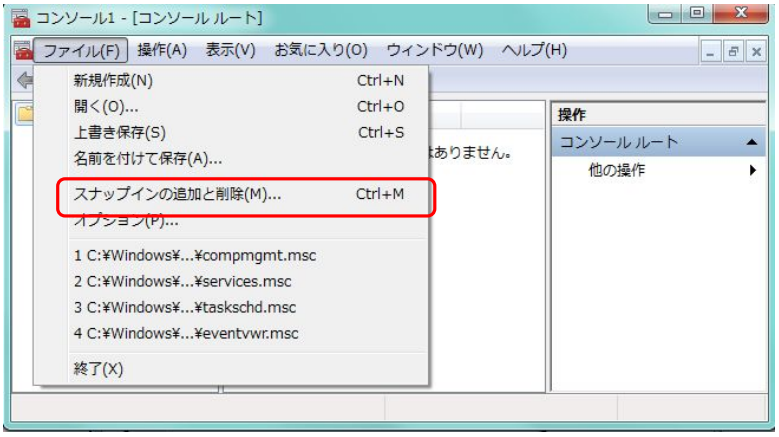
1.3 ルート CA 証明書の確認

1 スタート画面で「mmc.exe」と入力し Enter キーを押します。
ユーザーアカウント制御の画面が表示された場合は、[はい] ボタンをクリックしてください。



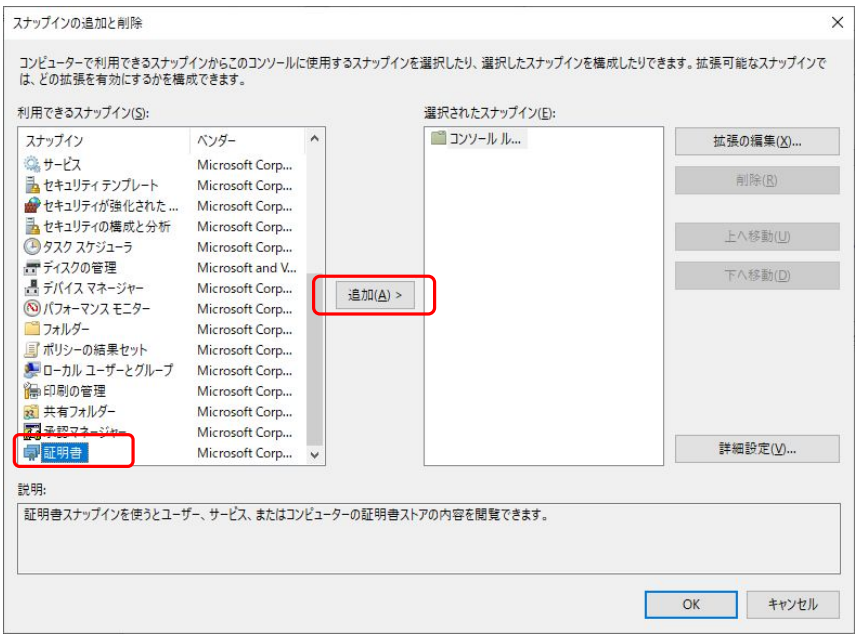
管理コンソールが起動します。

2 メニューバーから [ファイル] ー [スナップインの追加と削除] を選択します。



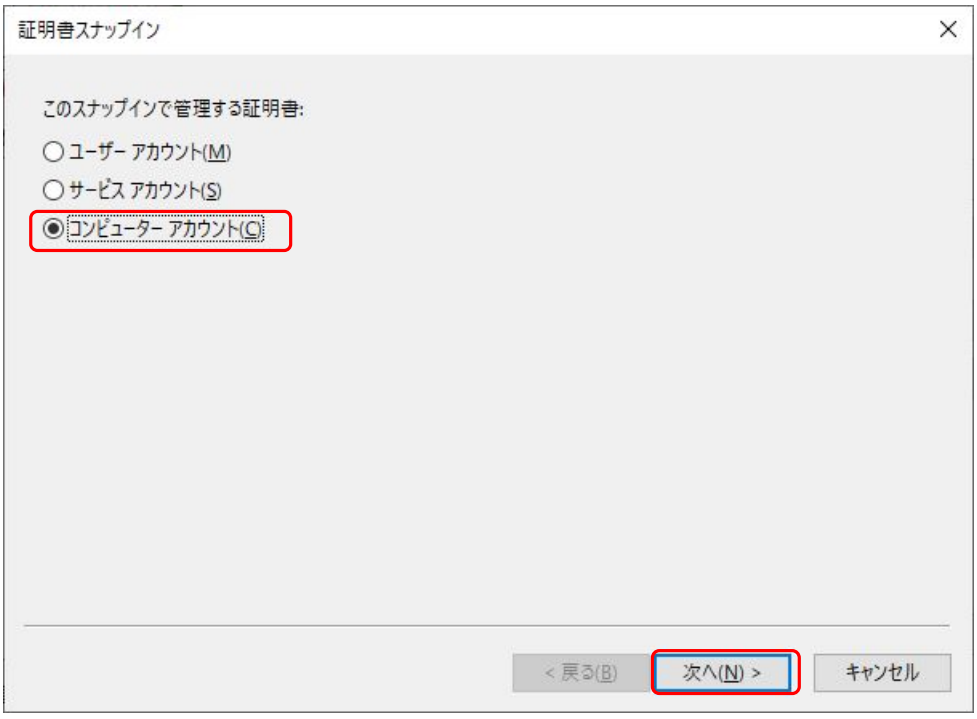
[スナップインの追加と削除] 画面が表示されます。

3 [利用できるスナップイン] の一覧で [証明書] を選択し、[追加] ボタンをクリックします。



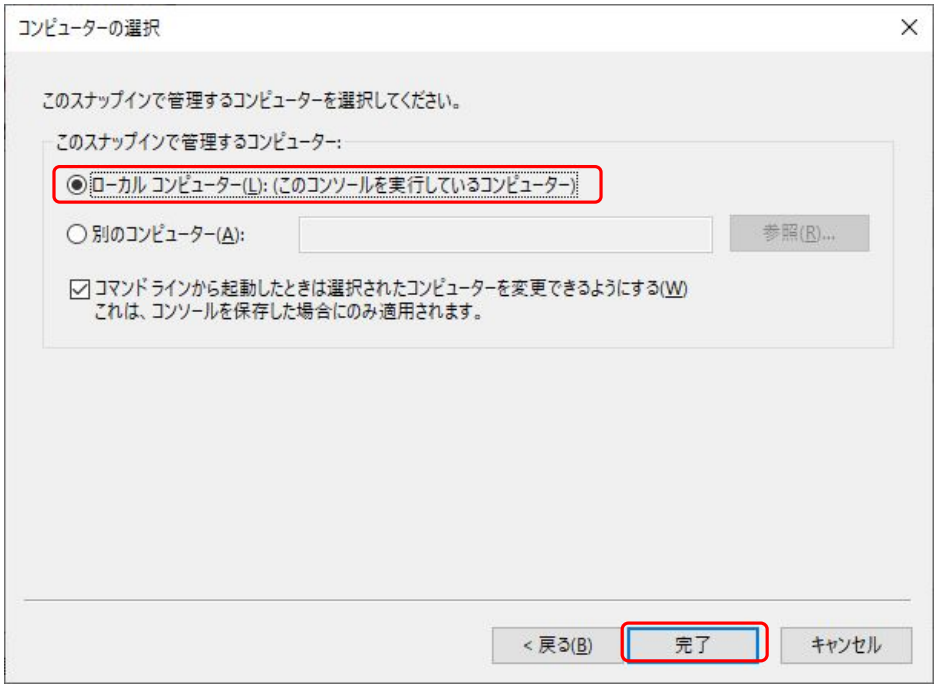
[証明書スナップイン] 画面が表示されます。

4 内容を確認し、[OK] ボタンをクリックします。



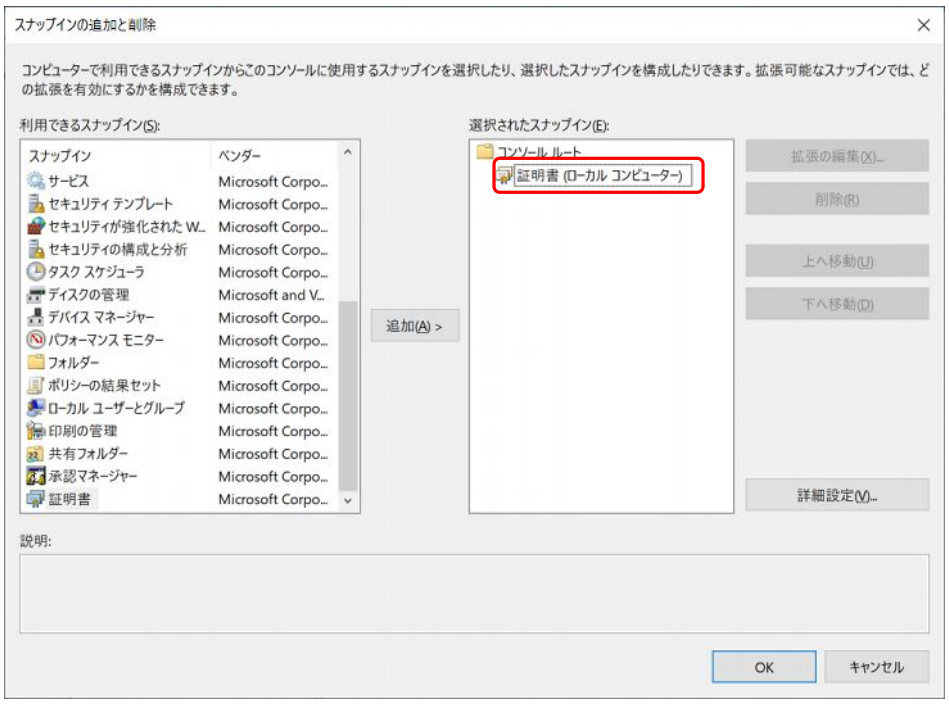
[コンピューターの選択] 画面が表示されます。

5 [このスナップインで管理するコンピューター] で、[ローカルコンピューター (このコンソールを実行しているコンピューター)] を選択し、[完了] ボタンをクリックします。



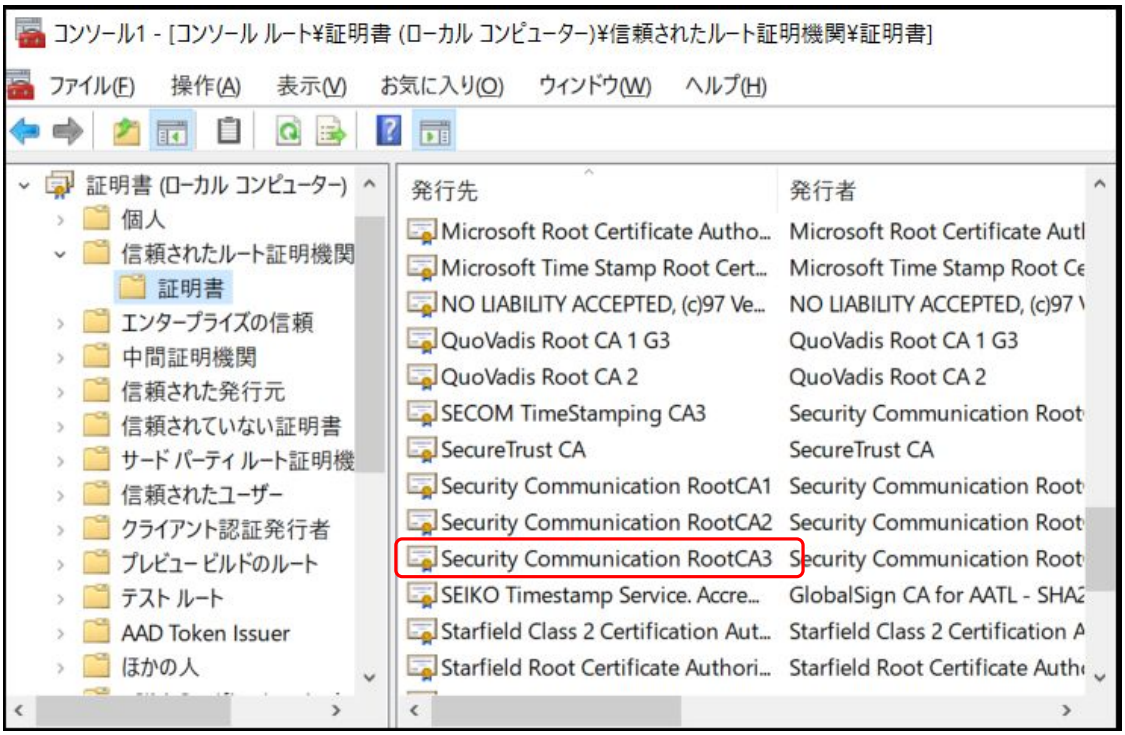
[スナップインの追加と削除] 画面が表示されます。

6 **[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)」が追加されていることを確認し、[OK] ボタンをクリックします。**



管理コンソールの画面が表示されます。

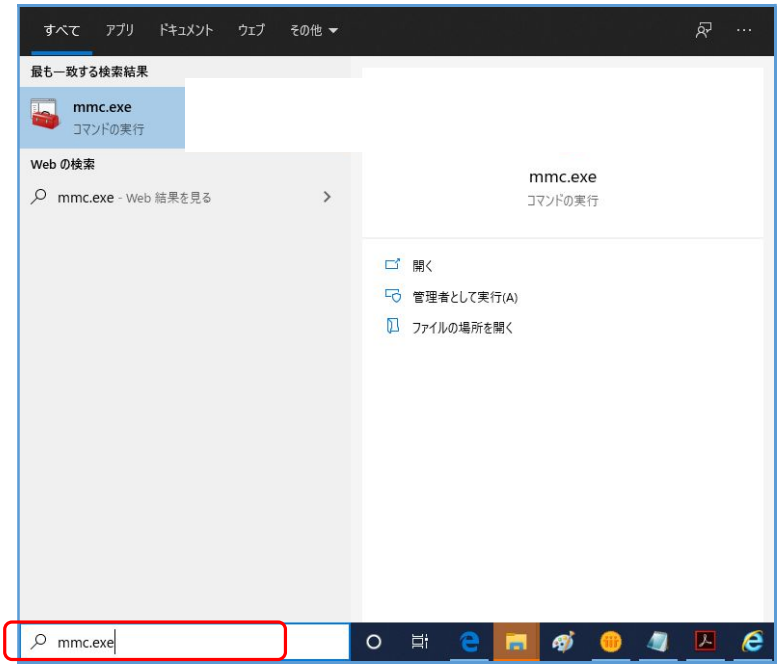
7 **[コンソールルート] にある [証明書 (ローカルコンピューター)]、信頼されたルート証明機関、証明書の順にクリックし開きます。**



Security Communication RootCA3 **が見つかれば証明書の登録はできています。**

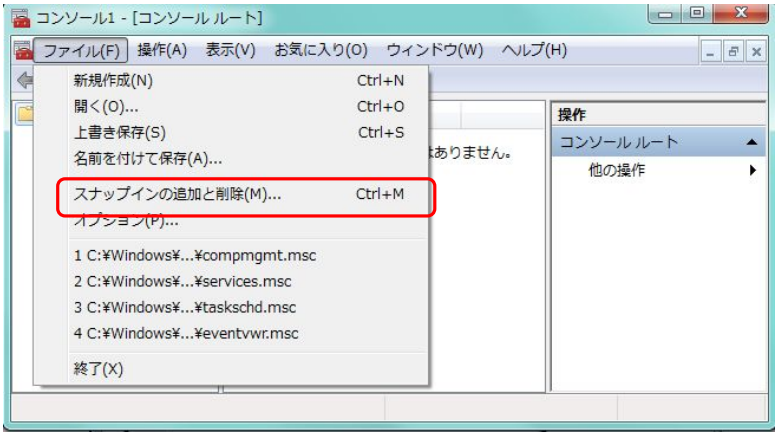
1.4 中間 CA 証明書の確認

1 スタート画面で「mmc.exe」と入力し Enter キーを押します。
ユーザーアカウント制御の画面が表示された場合は、[はい] ボタンをクリックしてください。



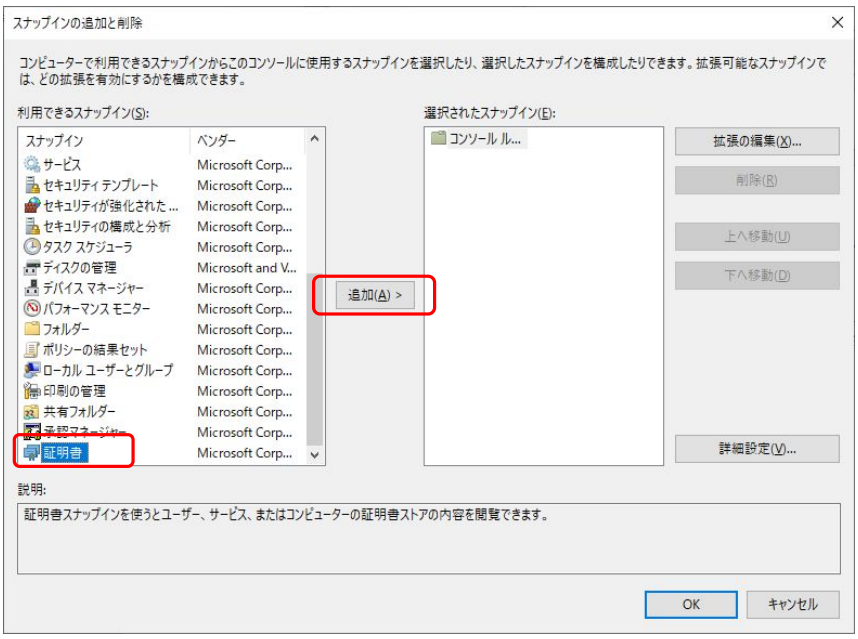
管理コンソールが起動します。

2 メニューバーから [ファイル] ー [スナップインの追加と削除] を選択します。



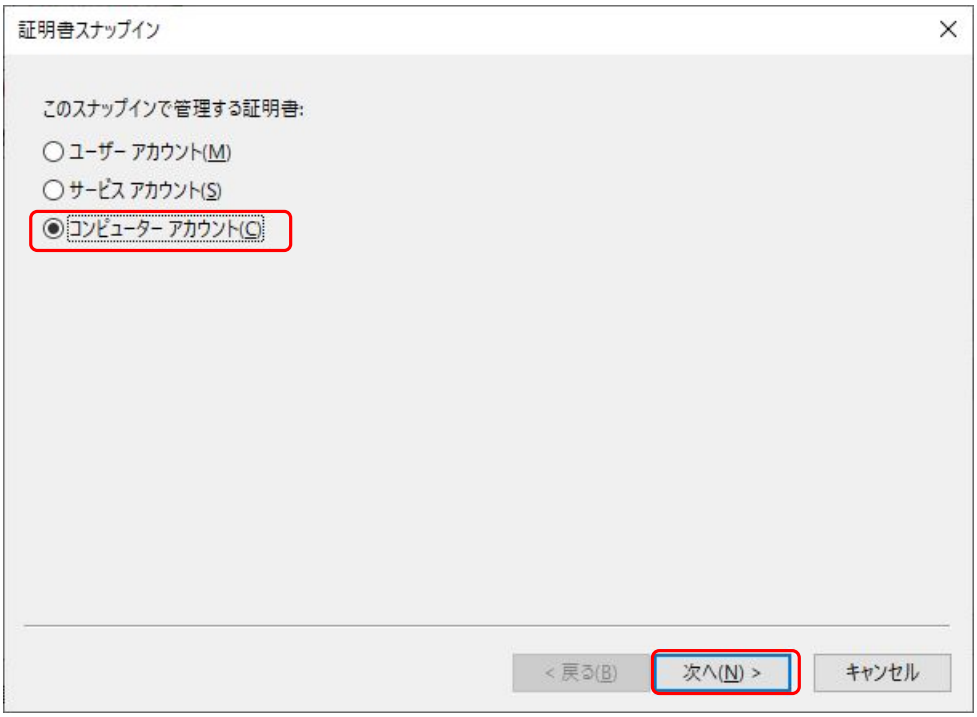
[スナップインの追加と削除] 画面が表示されます。

3 [利用できるスナップイン] の一覧で [証明書] を選択し、[追加] ボタンをクリックします。



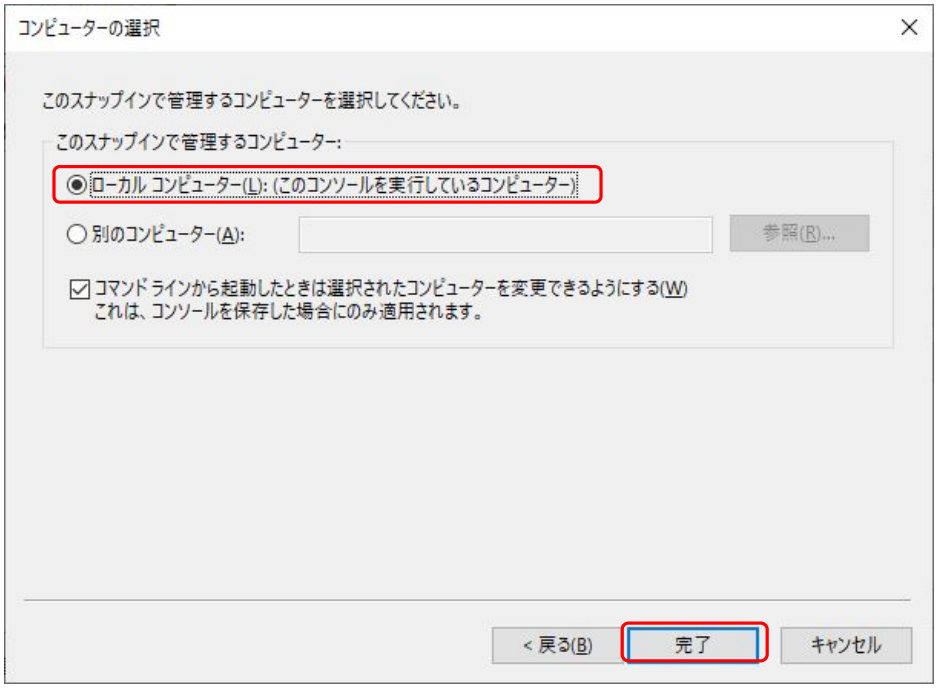
[証明書スナップイン] 画面が表示されます。

4 内容を確認し、[OK] ボタンをクリックします。



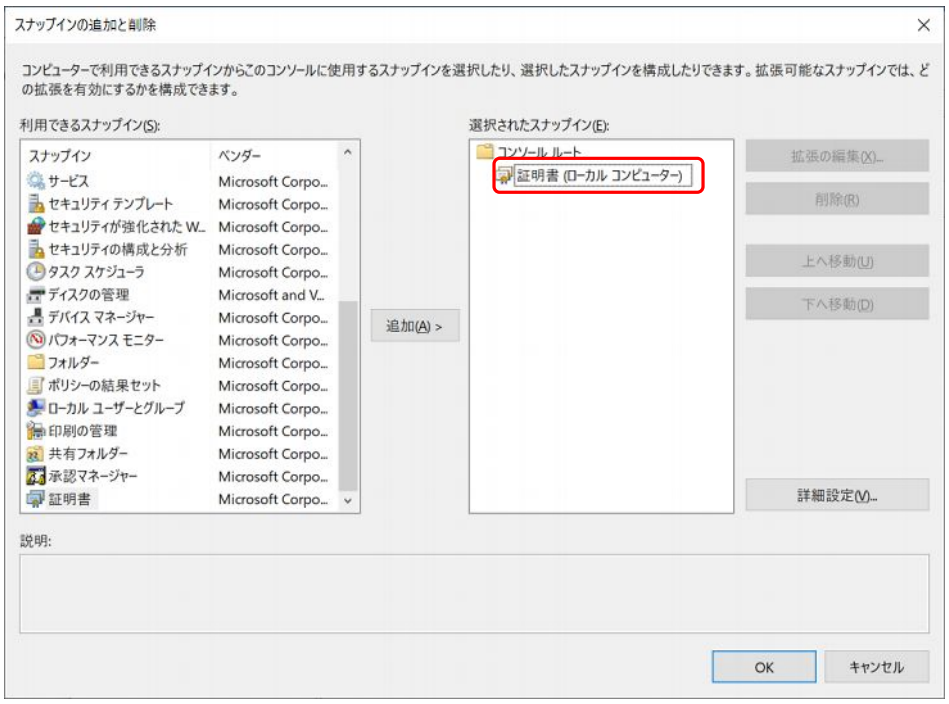
[コンピューターの選択] 画面が表示されます。

5 [このスナップインで管理するコンピューター] で、[ローカルコンピューター (このコンソールを実行しているコンピューター)] を選択し、[完了] ボタンをクリックします。



[スナップインの追加と削除] 画面が表示されます。

6 **[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)」が追加されていることを確認し、[OK] ボタンをクリックします。**



管理コンソールの画面が表示されます。

7 **[コンソールルート] にある [証明書 (ローカルコンピューター)]、中間明機関、証明書の順にクリックし開きます。**

SECOM TimeStamping CA3 **が見つかれば証明書の登録はできています。**