

2022.05.26 技術

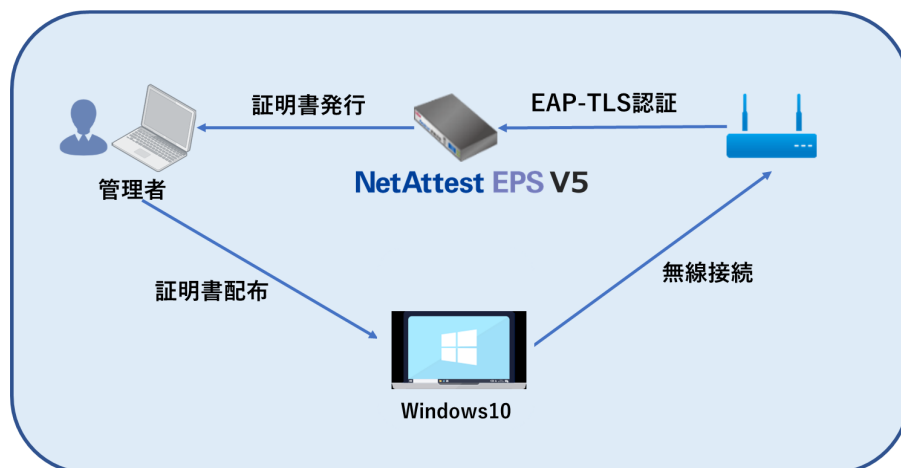
「Windows 10」で無線LANに接続する方法 ～ 電子証明書による認証（EAP-TLS）編 ～

ソリトンシステムズ・テクニカルチーム

この記事ではNetAttest EPSで発行したPKCS#12ファイルを**Windows 10** にインポートし、Wi-Fiに接続するまでの手順をご紹介します。

1. 構成

本記事では、下記の環境での利用を想定しています。



無線APのSSID：soliton_wireless

2. Windows 10への証明書インポート

NetAttest EPSで発行したPKCS#12ファイルをダブルクリックし、インポートウィザードを起動します。

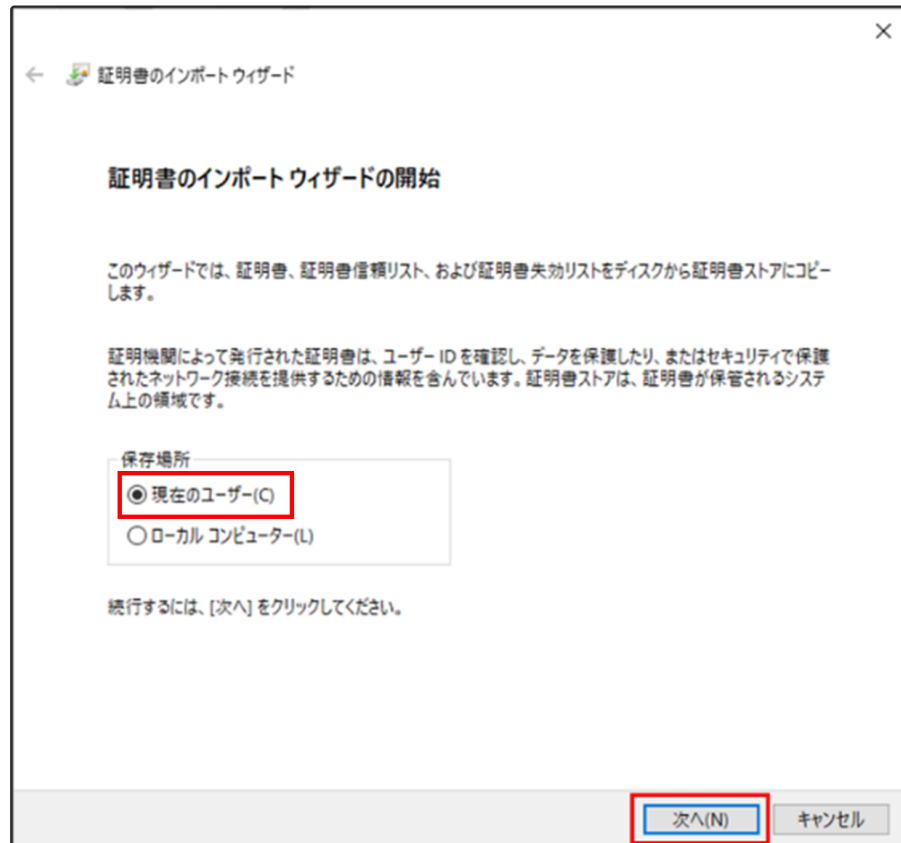
今回は**ユーザー認証**を前提とした手順を記載します。

1. 証明書の保存場所の指定

保存先は**ユーザーストア**と**コンピュータストア**の2種類があります。

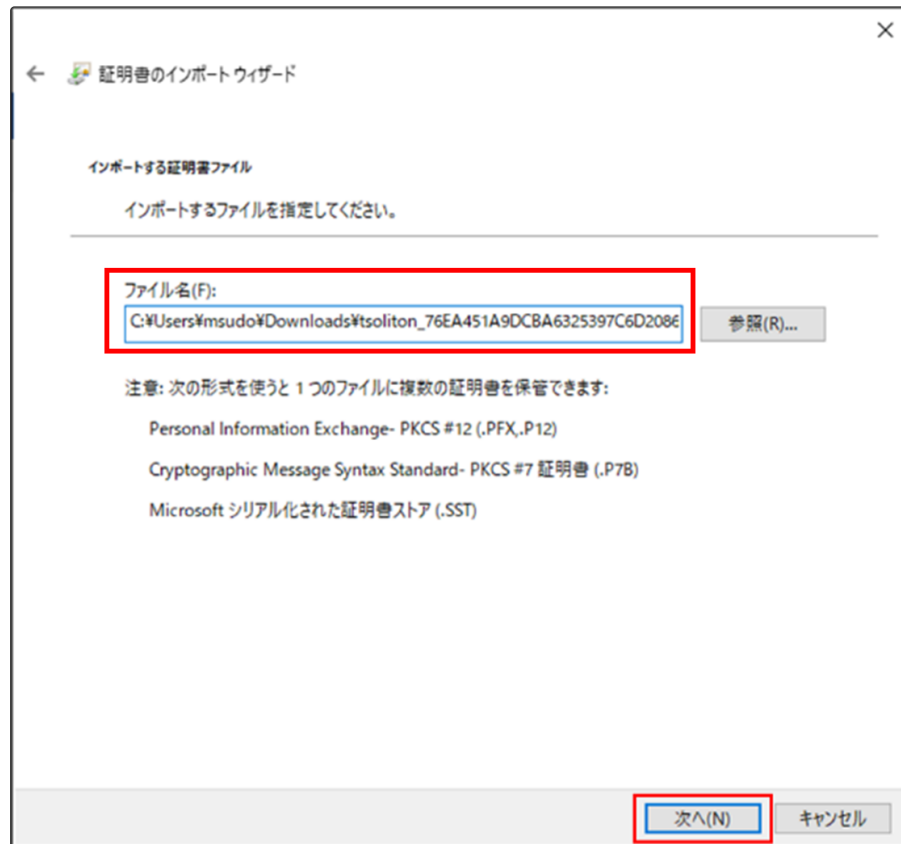
今回は**ユーザー認証**を行うため、**ユーザーストア**を指定します。

※コンピュータストアへ証明書をインポートする場合には、端末の管理者権限が必要です。



2. インポートする証明書ファイルを選択

証明書ファイルをダブルクリックし、ウィザードを起動した場合はそのファイルのパスが指定されます。



3. 秘密キーのパスワード入力

秘密キーのパスワード入力画面にパスワードを入力します。

#パスワードは大文字・小文字を区別します。

#下記のインポートオプションはオフのままにしておきます。

- 秘密キーの保護を強力にする
- このキーをエクスポート可能にする

⇒秘密キーが出力・流出すると、この証明書の信頼性が失われます。

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):

●●●●●●●●●●

☐ パスワードの表示(D)

インポート オプション(O):

☐ 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

☐ このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

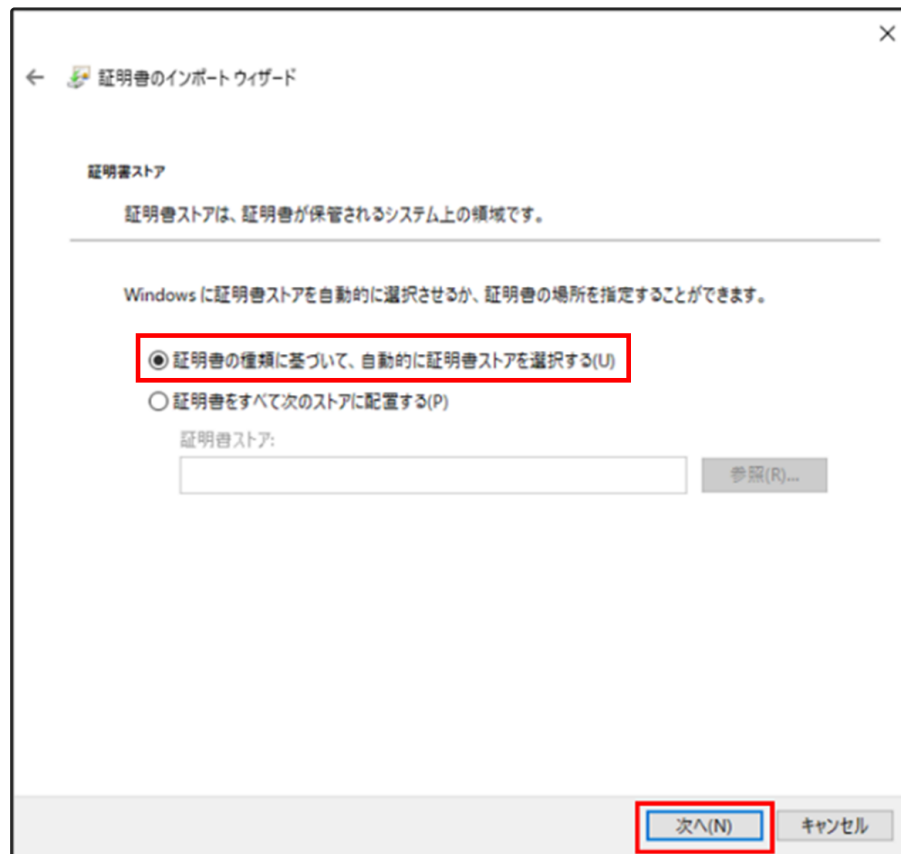
☐ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)

☒ すべての拡張プロパティを含める(A)

次へ(N) キャンセル

4. 証明書ストアの選択

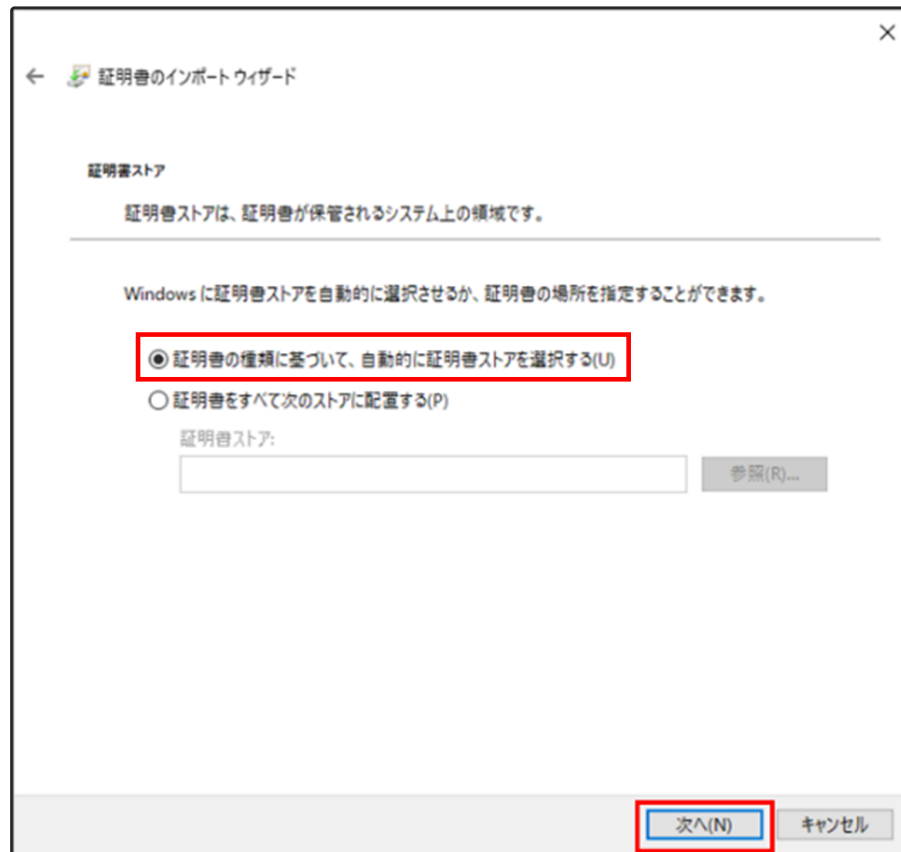
証明書をインポートするストアを選択します。



5. 証明書のインポートウィザードの完了

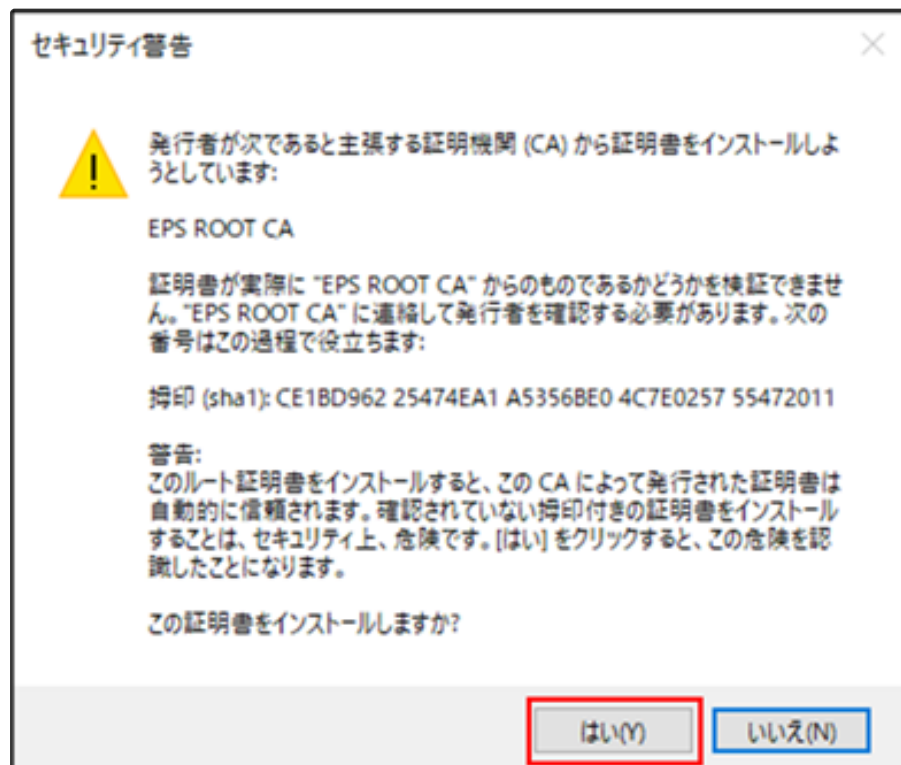
これでクライアント証明書のインポートは完了です。

次に、証明書機関の証明書（CA証明書）のインポートを行います。



6. CA証明書のインポート

[セキュリティ警告]ダイアログが表示されますが、
そのまま[はい]をクリックし[正しくインポートされました]と表示されれば完了です。
※既にCA証明書がインポートされている場合には表示されません。



以上で、「証明書のインポートウィザード」を使用した証明書のインポートは完了です。

3. Wi-Fiとサブリカントの設定

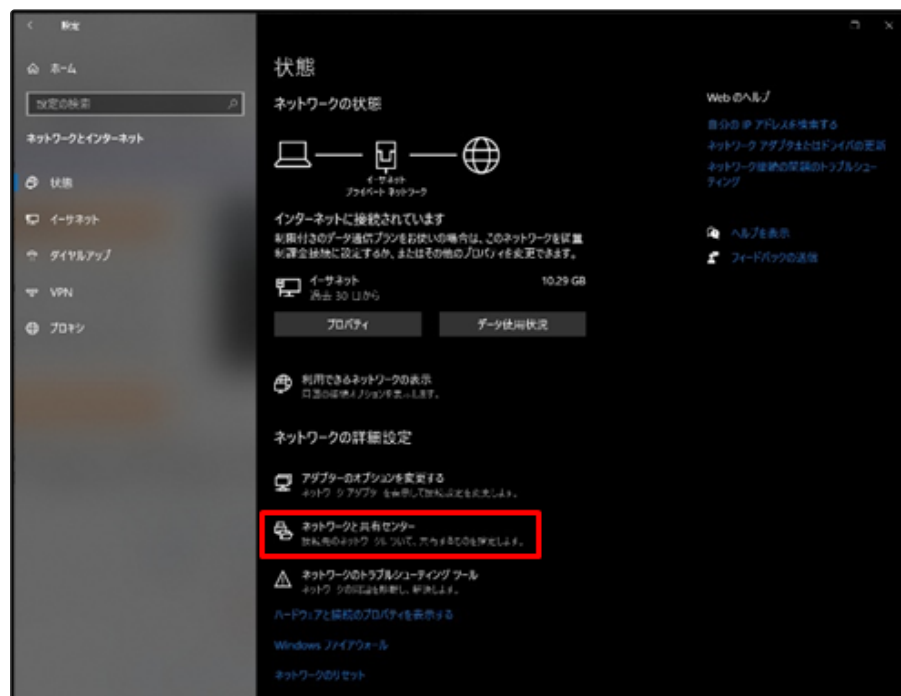
Wi-Fiとサブリカントの設定を行います。

今回はSSID：「soliton_wireless」を使用します。

1. ネットワークと共有センターを開く

「設定」-「ネットワークとインターネット」より

「ネットワークと共有センター」をクリックします。



2. ネットワーク設定の変更

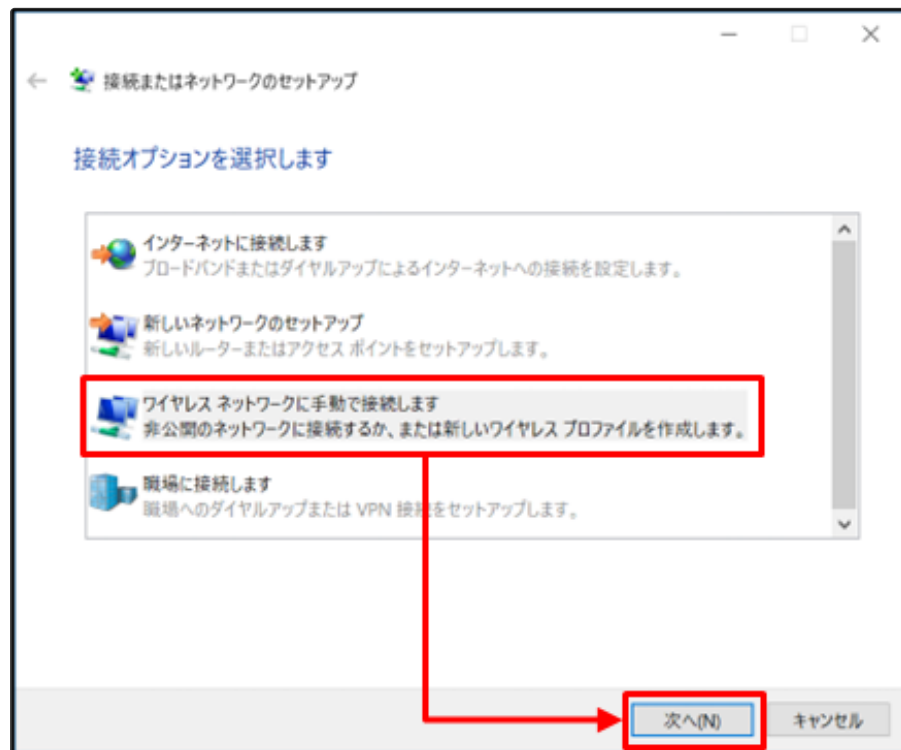
「新しい接続またはネットワークのセットアップ」をクリックします。



3. 接続オプションの選択

接続オプション選択画面にて

「ワイヤレスネットワークに手動で接続します」を選択します。

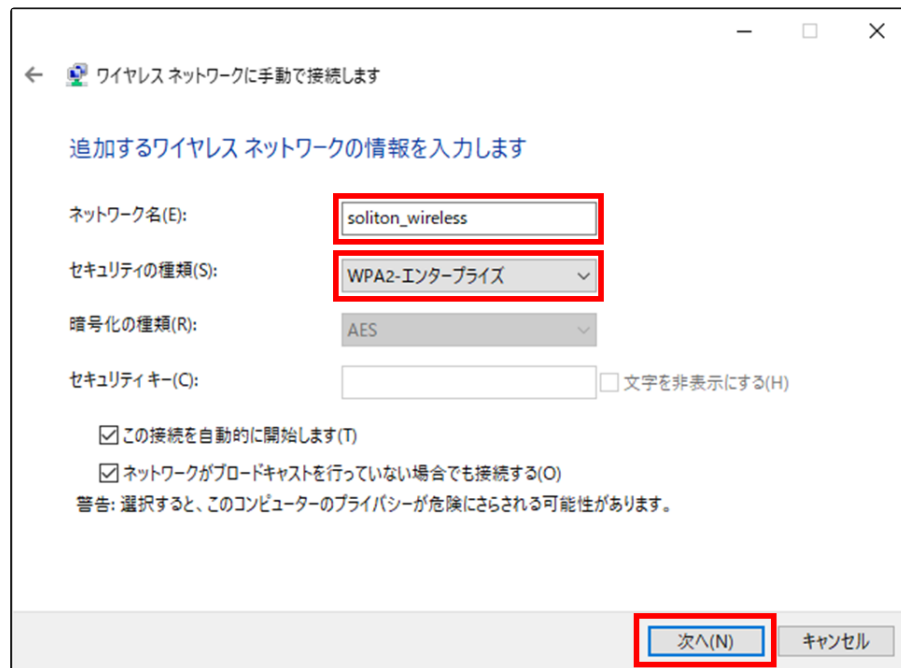


4. 追加するワイヤレスネットワーク情報の入力

SSIDやセキュリティの種類を指定し、「次へ」ボタンをクリックします。

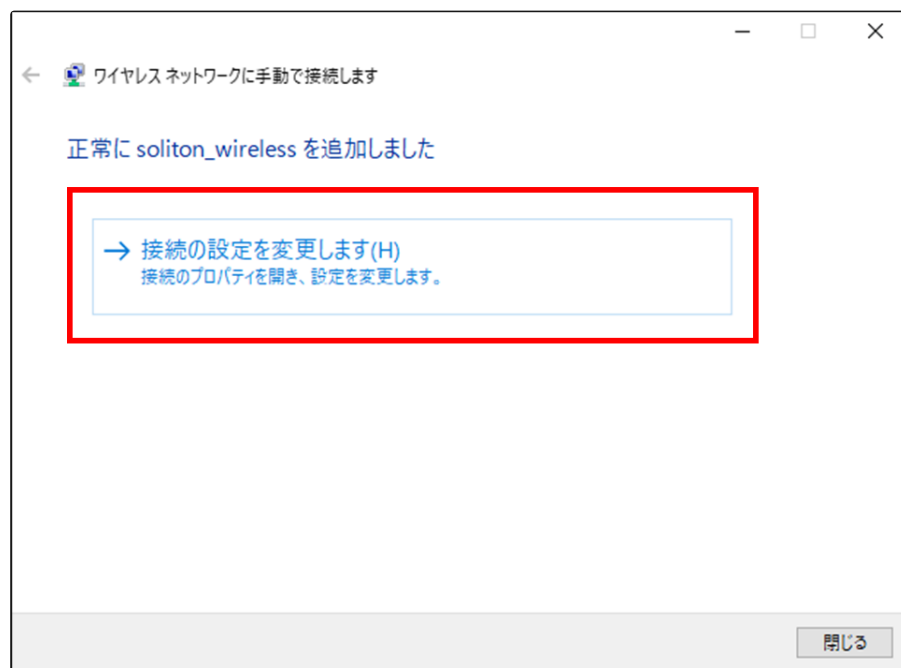
ネットワーク名：soliton_wireless

セキュリティの種類：WPA2-エンタープライズ



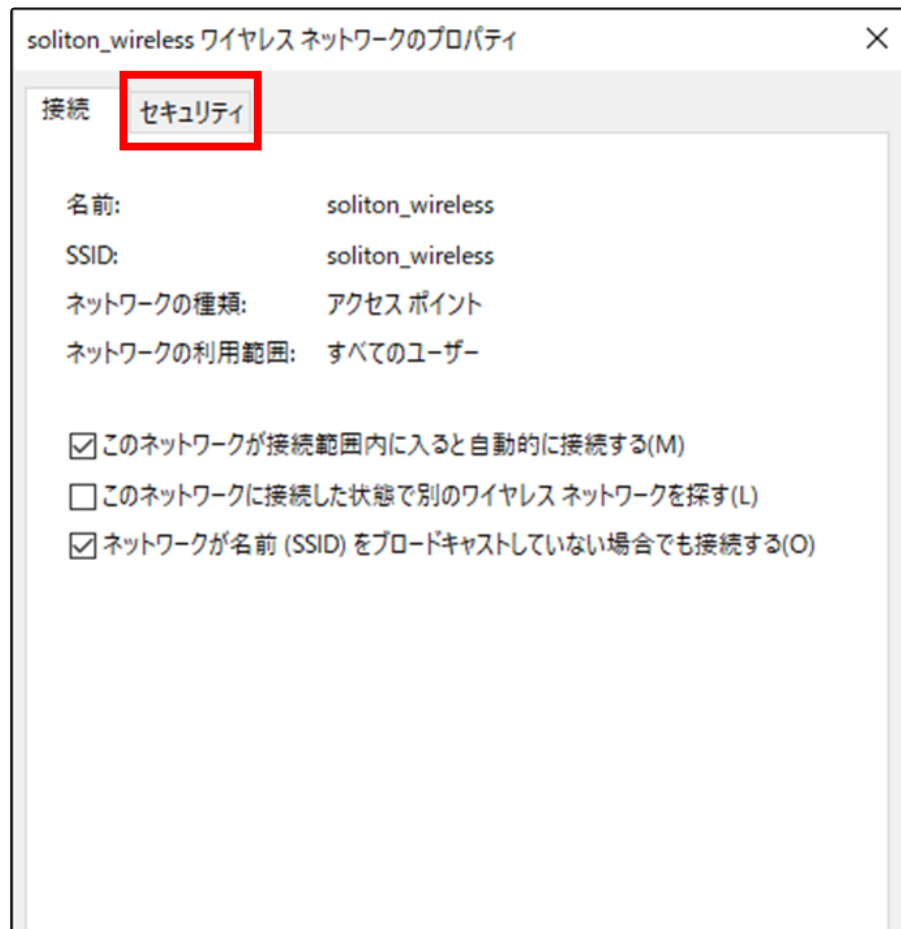
5. 接続の設定の変更

「接続の設定を変更します」をクリックします。



6. ワイヤレスネットワークのプロパティ

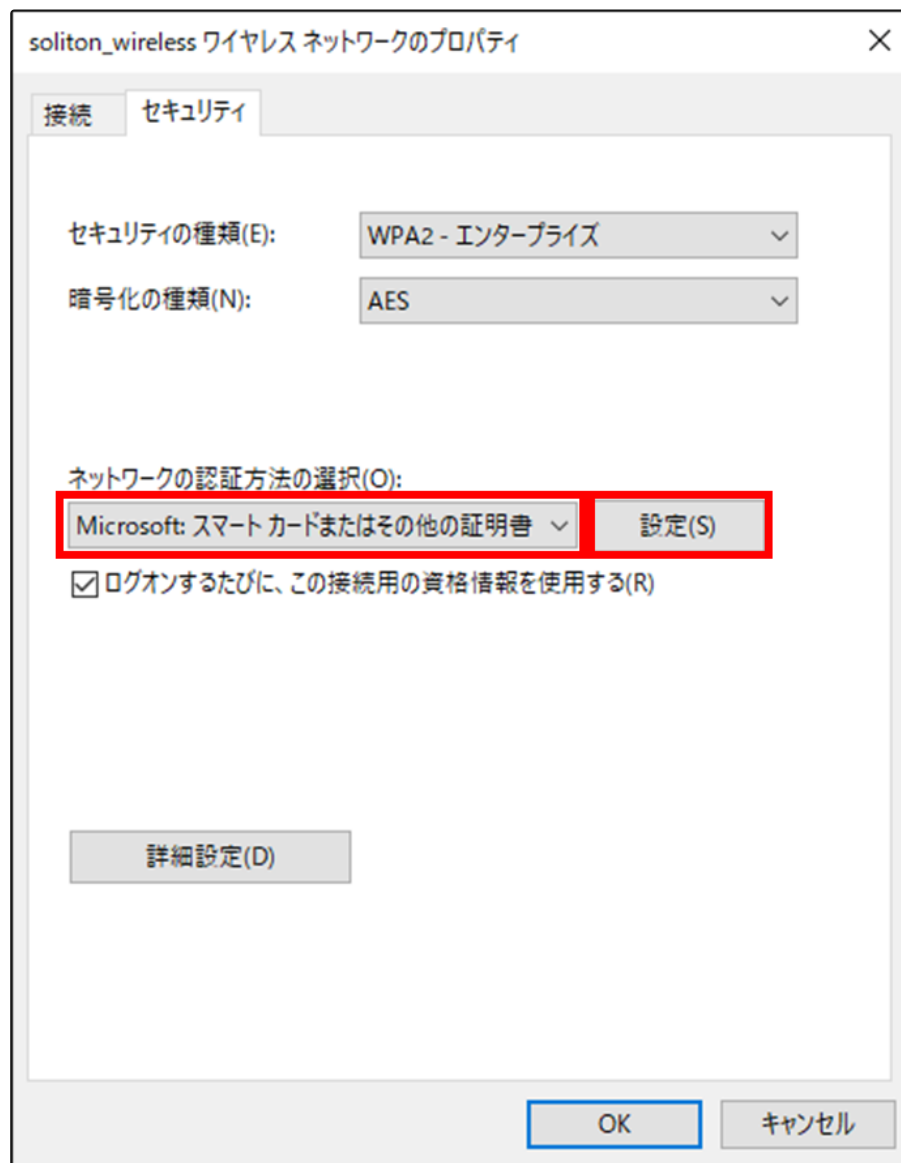
「ワイヤレスネットワークのプロパティ」画面の
「セキュリティ」タブをクリックします。



7. ネットワーク認証方法の選択

「ネットワークの認証方法の選択」のプルダウン設定にて

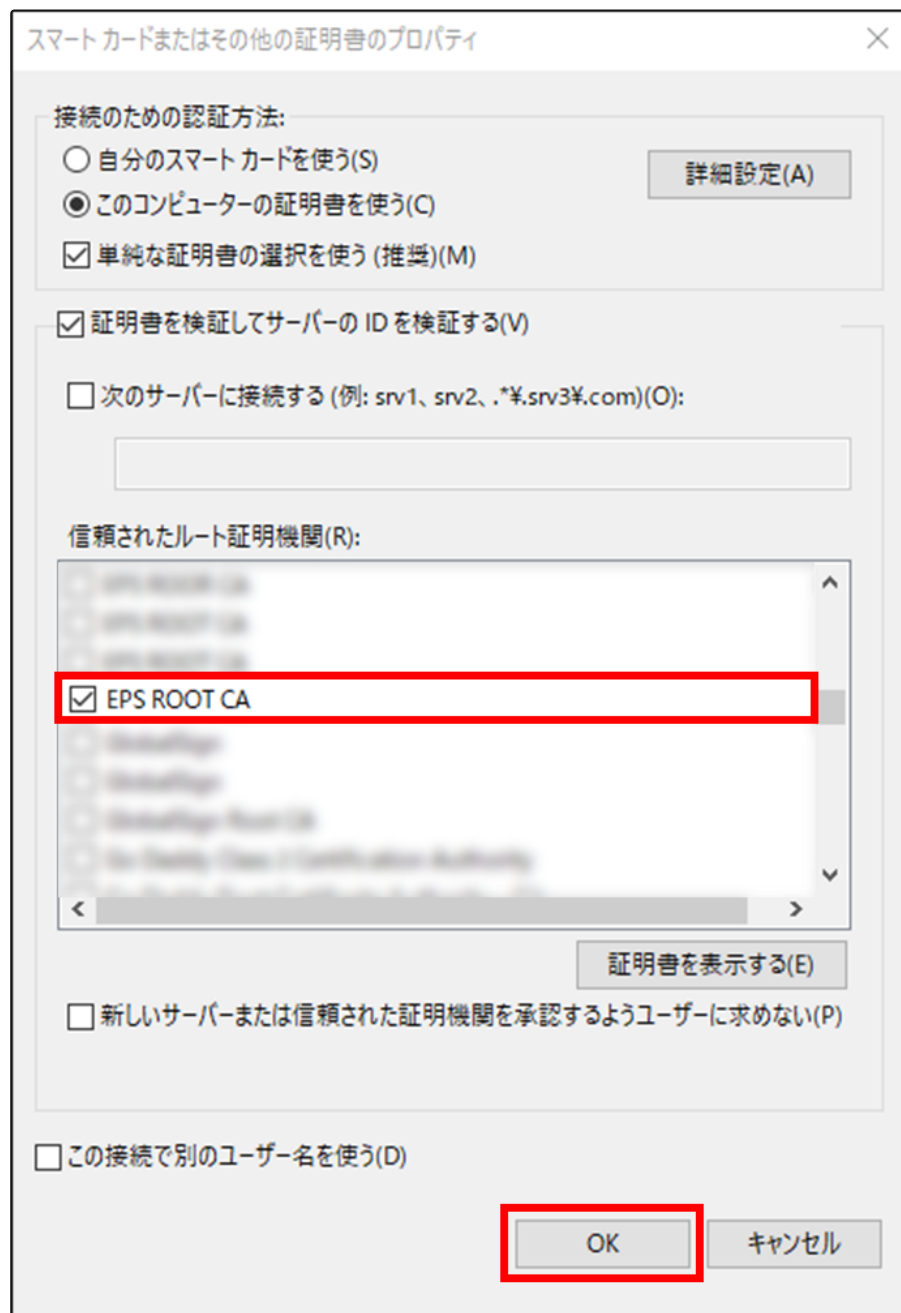
「Microsoft: スマートカードまたはその他の証明書」を選択し、[設定]ボタンをクリックします。



8. プロパティ設定

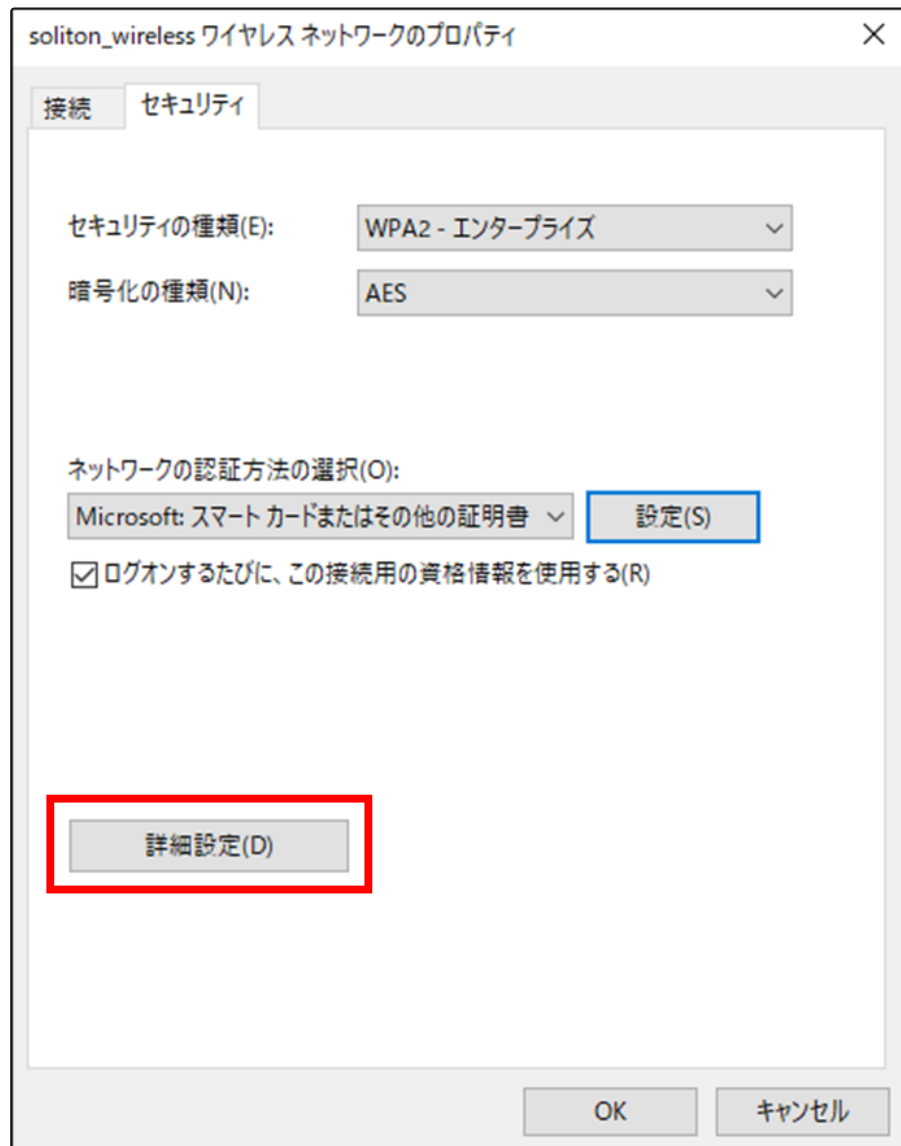
クライアント証明書認証の設定を行います。

ここではインポートしたCA証明書を選択します。設定後「OK」ボタンをクリックします。



9. 詳細設定

「ワイヤレスネットワークのプロパティ画面」に戻り、
「詳細設定」ボタンをクリックします。



10. 認証モードの指定

「802.1Xの設定」タブの「認証モードを指定する」をチェックし、プルダウンメニューを「ユーザー認証」にセットします。画面下部の「OK」ボタンをクリックし設定完了です。

詳細設定

802.1X の設定 802.11 の設定

☒ 認証モードを指定する(P):

ユーザー-認証

資格情報の保存(C)

☐ すべてのユーザーの資格情報を削除する(D)

☐ このネットワークに対するシングル サインオンを有効にする(S)

☒ ユーザー ログオンの直前に実行する(E)

☐ ユーザー ログオンの直後に実行する(F)

最大待ち時間 (秒)(M): 10

☒ シングル サインオン中に追加のダイアログの表示を許可する(L)

☐ このネットワークでは、コンピューターとユーザーの認証に別の仮想 LAN を使用する(V)

OK キャンセル

4. Wi-Fiに接続

SSID：「soliton_wireless」に接続できることを確認してください。

証明書の選択には、インポートしたクライアント証明書を選択してください。

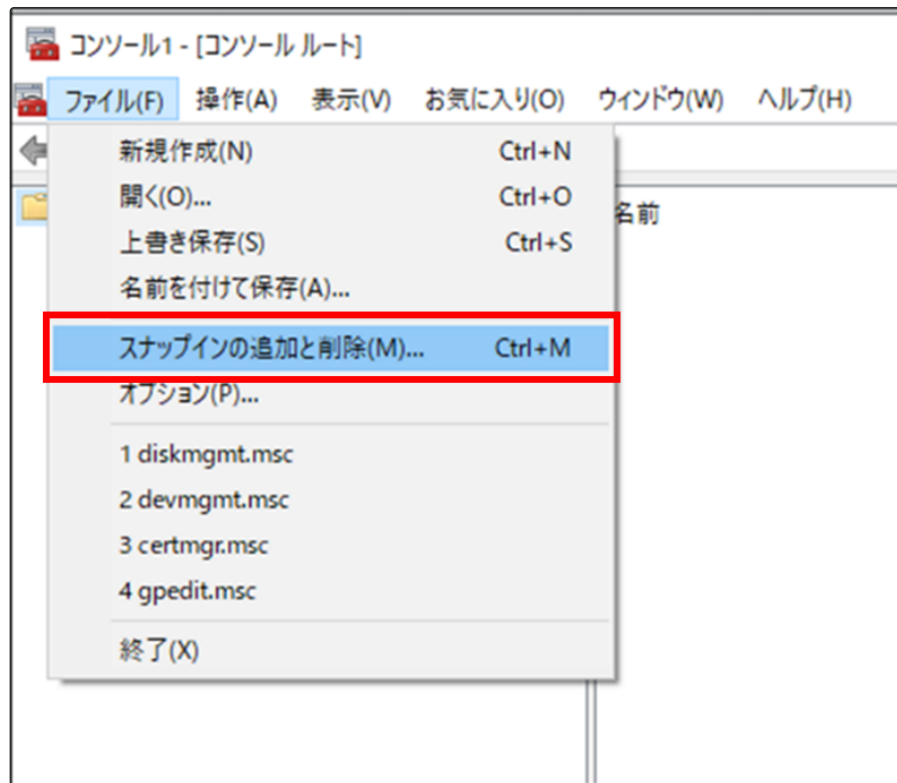
以上で、Wi-Fiへの接続完了です。



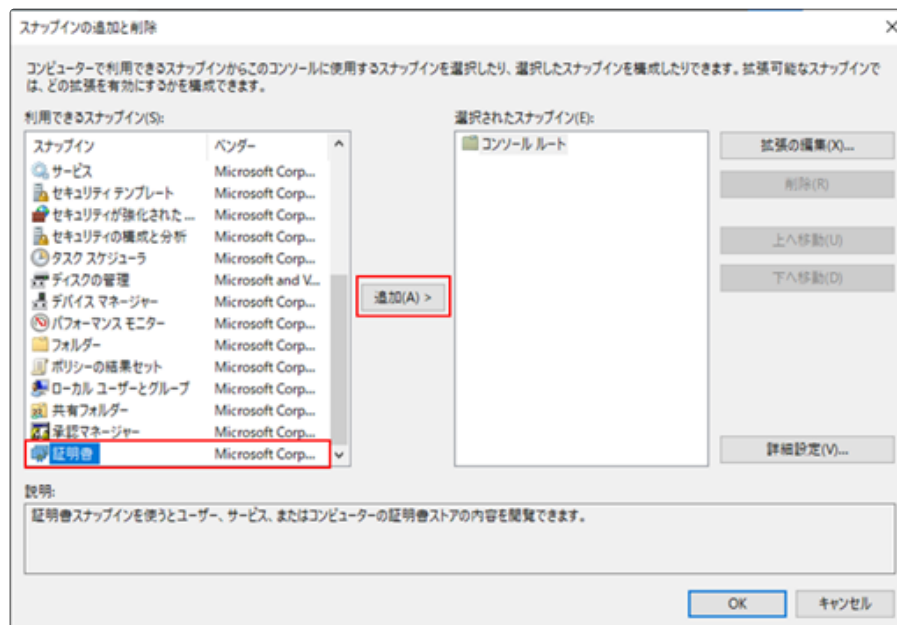
5.(参考情報)インポートした証明書の確認方法

Windows 10へインポートしたクライアント証明書とCA証明書を確認する方法をご紹介します。

- 01 Microsoft管理コンソール(MMC)をコマンドから起動し「ファイル」から「スナップインの追加と削除」をクリックします。

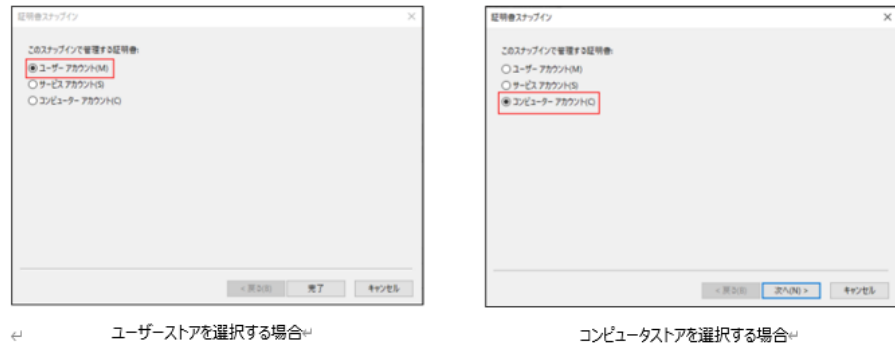


- 02 「スナップインの追加と削除」が表示されます。
「証明書」を選択し、「追加」をクリックします。



03 「証明書スナップイン」が表示されます。

ユーザーアカウント（コンピュータアカウント）を選択し、「完了」をクリックします。



[図を拡大して表示](#)

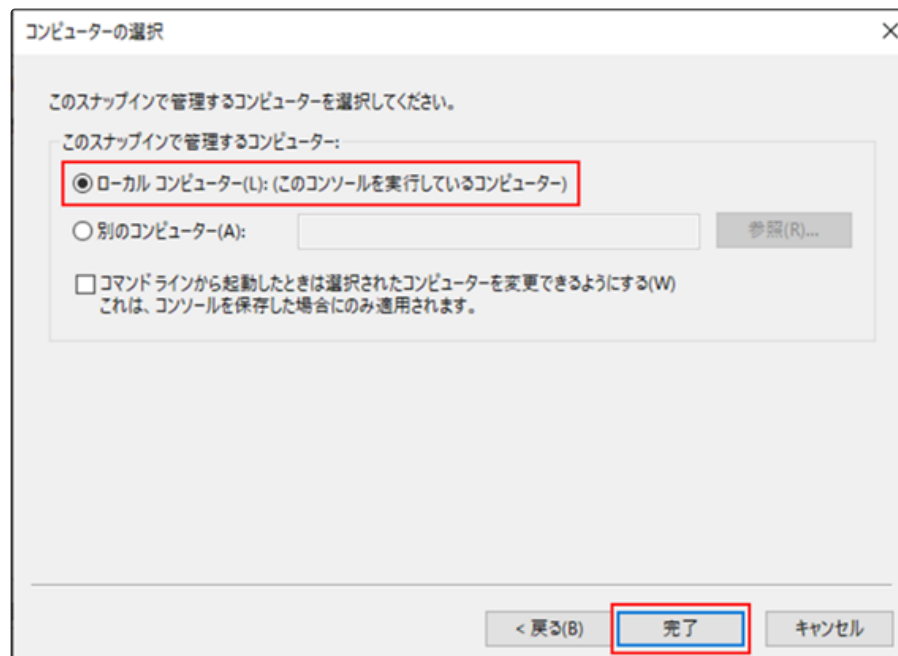
※画像（証明書ストアの選択）は、管理者権限のあるユーザーのみ表示されます。

※管理者権限がある場合、ユーザーストアとコンピュータストアの証明書確認が可能です。

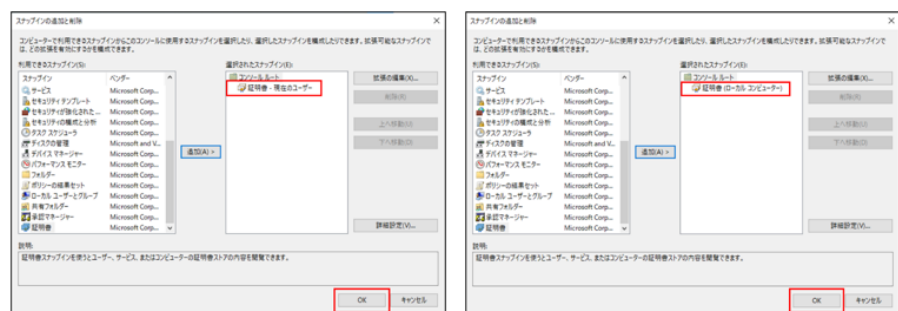
※管理者権限がない場合、証明書ストアの確認はユーザーストアのみとなります。⇒5へ進んでください。

04 コンピュータストアを選択した場合、「コンピューターの選択」が表示されます。

「ローカルコンピュータ」を選択し、「完了」をクリックします。



- 05 「選択されたスナップイン」画面に証明書が表示されていることを確認し、「OK」をクリックします。

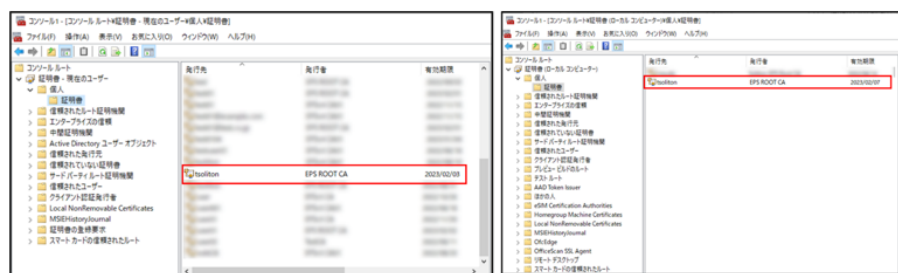


ユーザーストアを選択した場合

コンピュータストアを選択した場合

[図を拡大して表示](#)

- 06 ユーザーストアを選択した場合、「証明書 - 現在のユーザー」⇒「個人」⇒「証明書」を選択し、クライアント証明書がインポートされていることを確認します。
(コンピュータストアを選択した場合は、「証明書(ローカルコンピュータ)」⇒「個人」⇒「証明書」を選択します。)

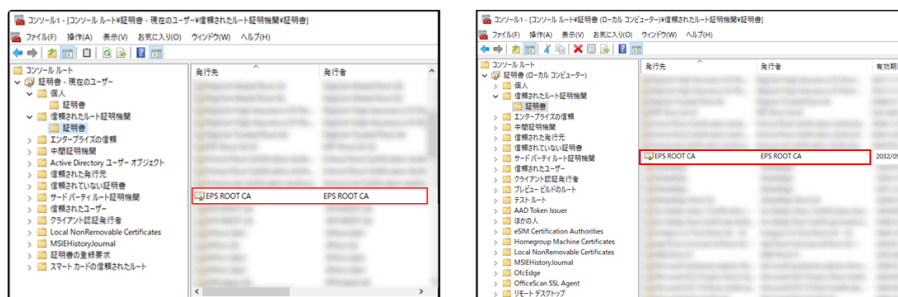


ユーザーストア

コンピュータストア

[図を拡大して表示](#)

- 07 「証明書 - 現在のユーザー」⇒「信頼されたルート証明機関」⇒「証明書」を選択し、CA証明書がインポートされていることを確認します。



ユーザーストア

コンピュータストア

[図を拡大して表示](#)