NRA

Web サーバ設定ガイド

（IIS10.0 クライアント証明書マッピング認証編）

2023 年 10 月 25 日

Ver. 1.50

改訂履歴

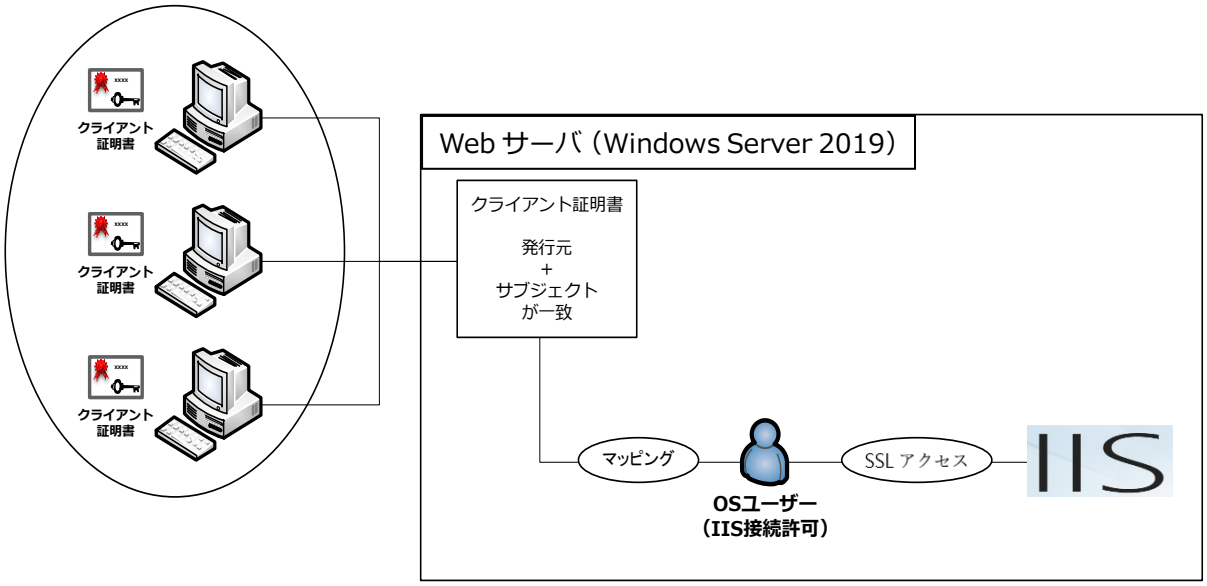
版	日　付	内　容	備　考
Ver. 1.10	--	初版作成	
Ver. 1.20	2020/10/12	3.5 サーバ証明書のインポートを追加 設定不要箇所の削除	
Ver. 1.30	2020/11/10	CA4 に関する記載の追加	
Ver. 1.40	2023/3/17	Windows Server 2022 に関する記載の追加	
Ver. 1.50	2023/10/25	CRL の更新間隔の変更手順に関する記載の追加	

<目　次>

1. 本書の目的

本書は、Windows Server 2019 環境で動作するインターネット インフォメーション サービス バージョン 10.0（以降 IIS 10.0）で構築された Web アプリケーションに SSL クライアント認証を実装し、プログラムを介さずクライアント証明書の発行元、サブジェクトでフィルタリングする手順を記述します。

以下が、SSL クライアント認証の概要図です。



2. 注意点

本書では、Windows Server 2019 環境に IIS10.0 をインストールした環境で検証した結果を記述します。

稼働中の IIS の設定状況や、バージョン等、環境に依存して、本手順だけでは網羅できない場合がございます。

※Windows Server 2022 環境でも動作確認ができております。

3. 設定手順

3.1. 手順の流れ

■OS（Windows）の設定

・IIS のインストール ※本手順では割愛

3.2 IIS クライアント証明書マッピング認証の役割追加

3.3 IIS へのアクセス許可ユーザーの作成

3.4 クライアント証明書と紐づく、ルート証明書、中間証明書のインポート

■IIS の設定

3.5 サーバ証明書のインポート

3.6 サイトのバインド編集（https のポートとサーバ証明書のバインド設定）

3.7 認証の設定

3.8 多対 1 マッピング規則の設定

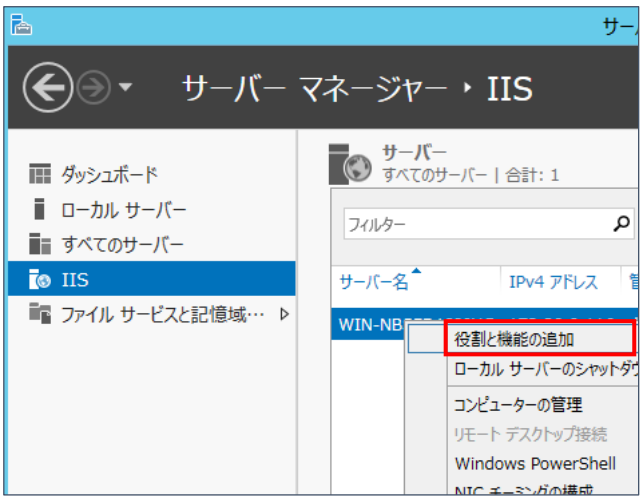
3.9 SSL 設定

■クライアントの設定

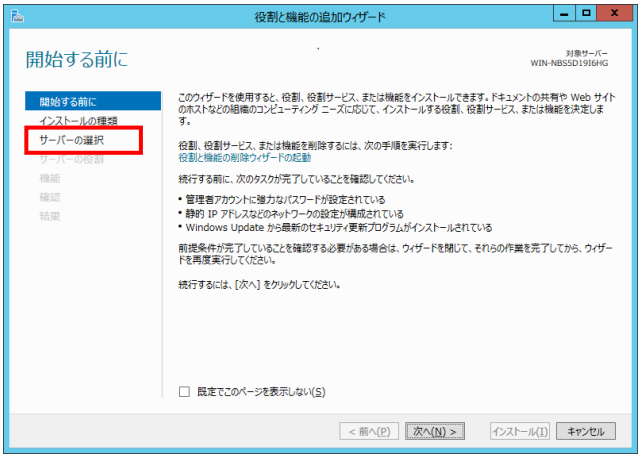
3.10 クライアント証明書の情報参照（クライアント側）

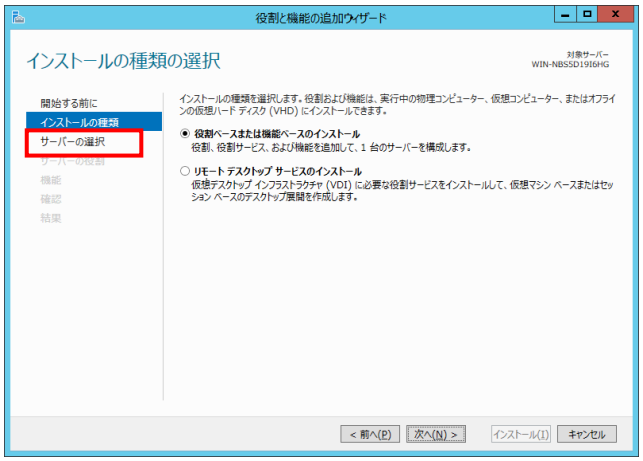
3.2. IIS クライアント証明書マッピング認証の役割追加

① Web サーバのサーバーマネージャを起動し、”IIS”→”Web サーバ”を選択。
右クリックで”役割と機能の追加”を選択します。

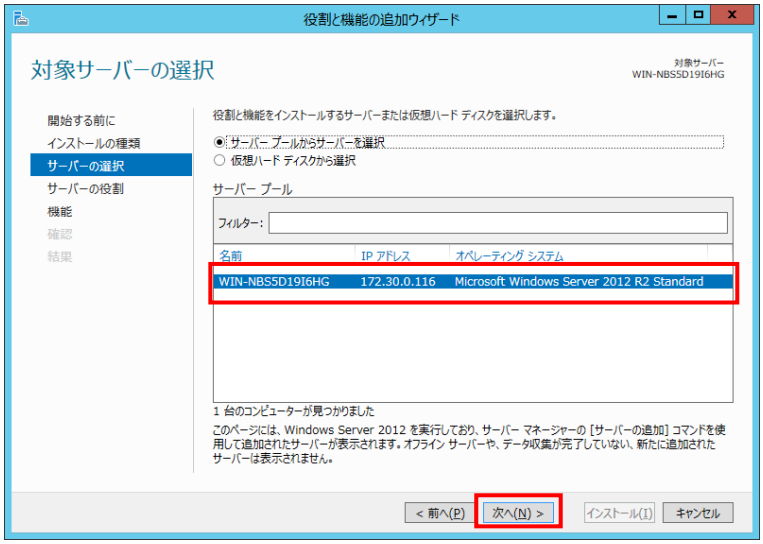


② 下記の画面のどちらかが表示されたら、いずれの場合も”サーバの選択”をクリックします。





③ Web サーバが選択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。



④ 役割の“Web Server（IIS）”→“Web Server”→”Security”に含まれる、“IIS Client Certificate Mapping Authentication”がインストールされていることを確認。（クライアント証明書のマッピング認証は本手順では使用しません。）

未インストールの場合は、チェックを入れて”次へ”ボタンをクリックしてインストールします。

3.3. IIS へのアクセス許可ユーザーの作成（OS の設定）

”スタート”→ ”管理ツール”→”コンピューターの管理”→ ”ローカルユーザとグループ”を開き、
”ユーザー”を選択し任意のユーザー（本手順では、”inetUsr”とします。）を作成します。

① ユーザー情報の入力。

・"ユーザー名(U)" →任意で入力
・"パスワード(P)" →任意で入力
・"パスワードの確認入力(C)" →任意で入力
・"ユーザーは次回ログオン時にパスワードの変更が必要(M)" →チェックをはずす
・"ユーザーはパスワードを変更できない(S) " →チェックする
・"パスワードを無期限にする(W) " →チェックする
・"アカウントを無効にする(B) " →チェックをはずす

② 作成したユーザーの"プロパティ"確認。

・"全般" タブ内で、"アカウントのロックアウト"にチェックが入っていないこと
・"全般" タブ内で、"ユーザーはパスワードを変更できない"にチェックが入っていること
・"全般" タブ内で、"パスワードを無期限にする" にチェックが入っていること

3.4. クライアント証明書と紐づく ルート証明書、中間証明書のインポート

日本 RA の管理する、ルート証明機関、中間証明機関の証明書のインポートをします。
証明書は下記の URL からダウンロードしてください。中間証明機関の証明書についてはご利用中の中間証明機関の証明書をインポートしてください。
※ご利用中の中間証明機関の確認方法については補足をご確認ください。

・中間証明機関(CA3)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3.crt
・中間証明機関(CA4)
https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4.crt
・ルート証明機関
https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthority.crt

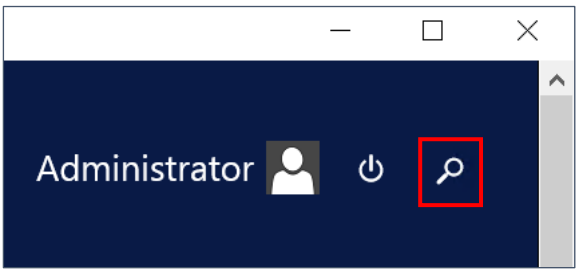
インポート対象のファイルは、中間証明機関→ルート証明機関の順にインポートします。
・NipponRACertificationAuthority3.crt→ 中間証明機関(CA3)
・NipponRACertificationAuthority4.crt→ 中間証明機関(CA4)
・NipponRARootCertificationAuthority.crt→ ルート証明機関

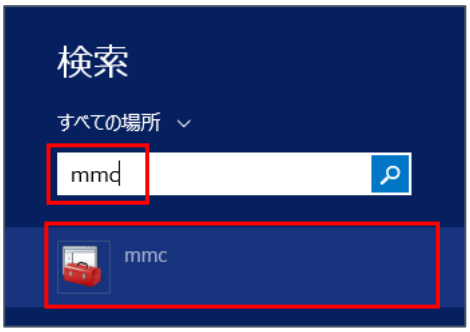
【補足】
下図の NRA-PKI システム管理画面にて、[利用者メンテナンス]をクリックしていただくと、適用されているサービス名が表示されます。サービス名の後に**（CA4）**という表記があれば CA4、なければ CA3 をご利用いただいております。

次ページから中間証明機関とルート証明機関の証明書をインポートする手順を記載します。

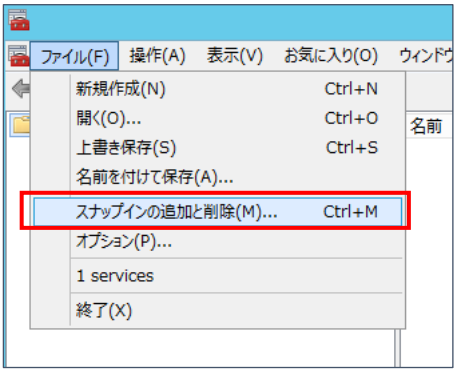
① mmc（管理コンソール）の起動。

画面左下の検索アイコン（または Windows キー）を押下し、“mmc” と入力して、検索結果に表示された mmc を選択します。

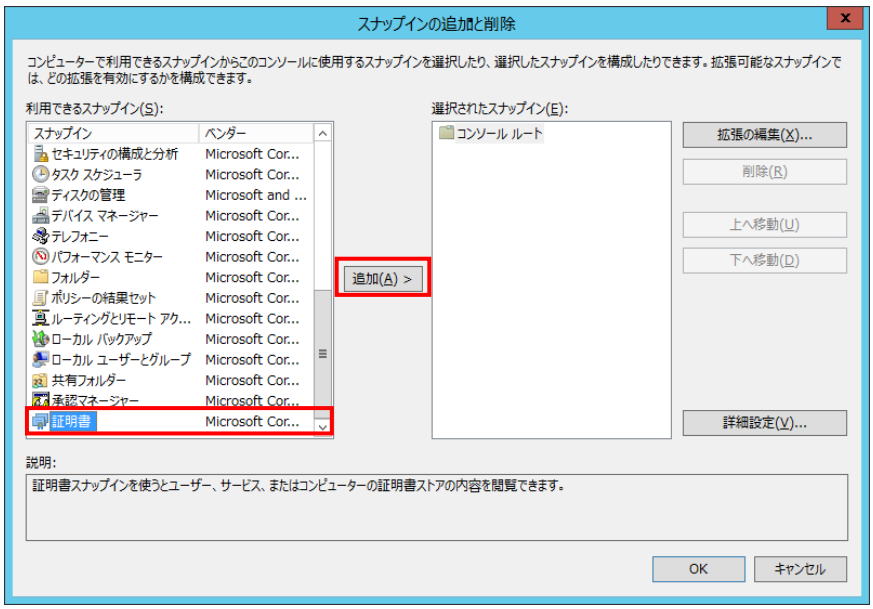




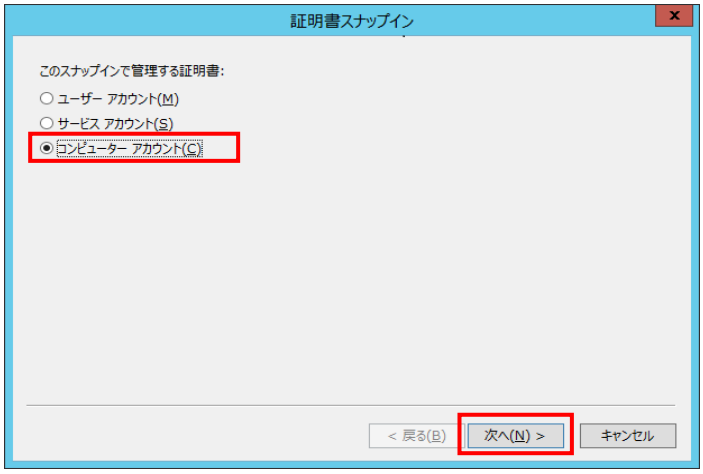
② “ファイル（F）”→”スナップインの追加と削除”を選択。



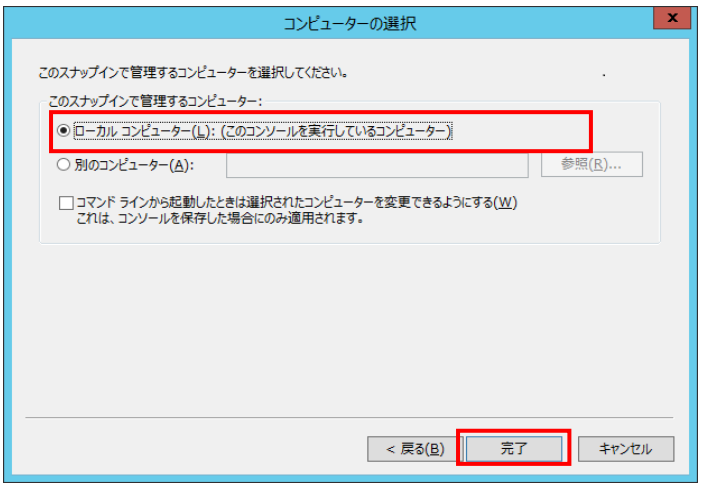
③ 左画面の下方にある証明書を選択し、”追加”ボタンをクリック。



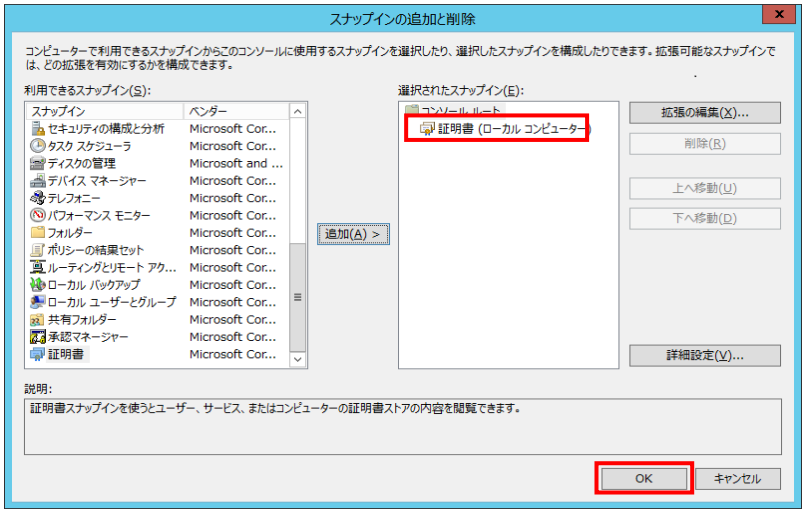
④ 証明書スナップイン画面にて”コンピューター アカウント”を選択し、”次へ”ボタンをクリック。



⑤ コンピューターの選択画面にて”ローカルコンピュータ”が選択されていることを確認し”完了”をクリック。

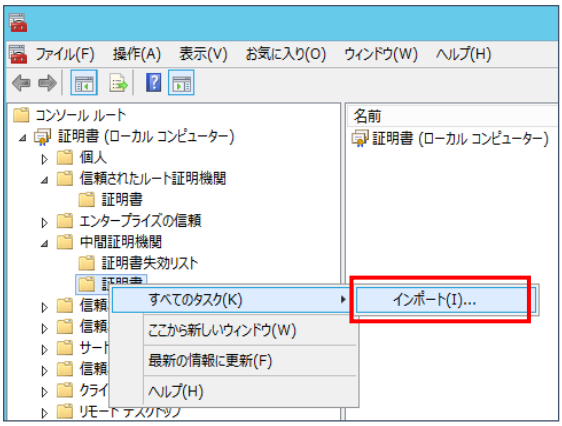


⑥ 手順③の”スナップインの追加と削除”画面の右側に”証明書”が追加されたことを確認し”OK”をクリック。

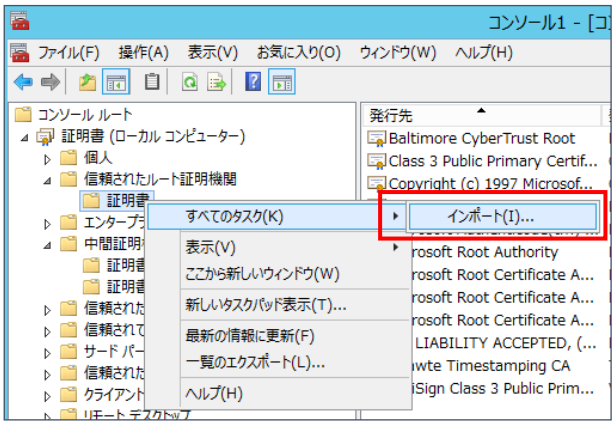


⑦ 証明書のインポートを実行。

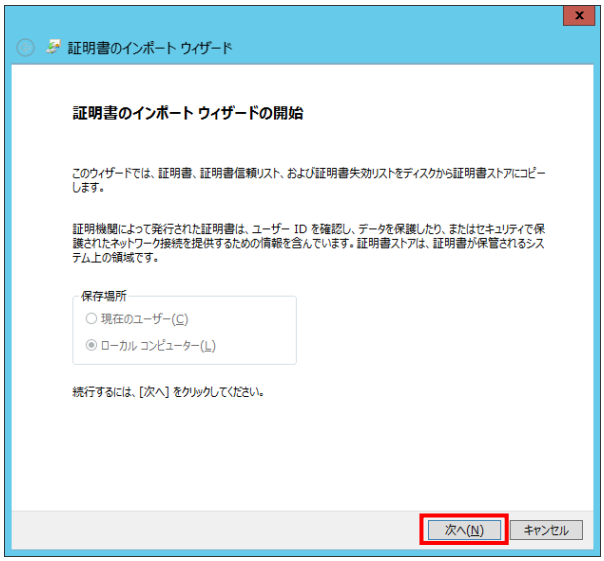
中間証明機関の場合



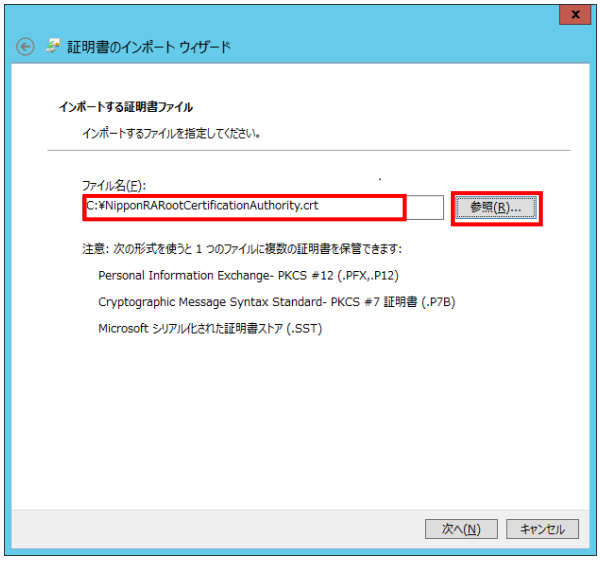
ルート証明機関の場合



⑧ 証明書のインポートウィザードの開始を確認し、”次へ”をクリック。

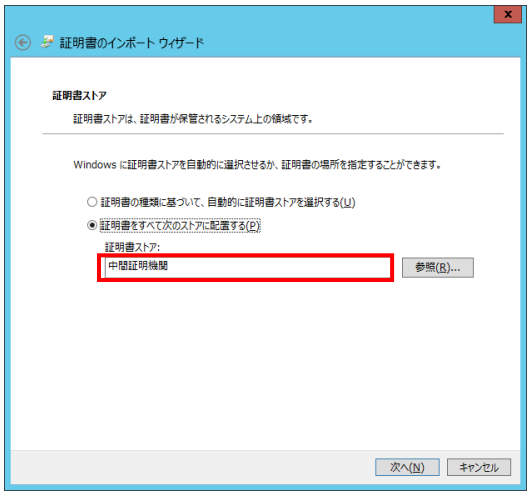


⑨ インポートする証明書ファイルは”参照”をクリックし、手順 3.4 でダウンロードした証明機関の XXX.crt を選択。

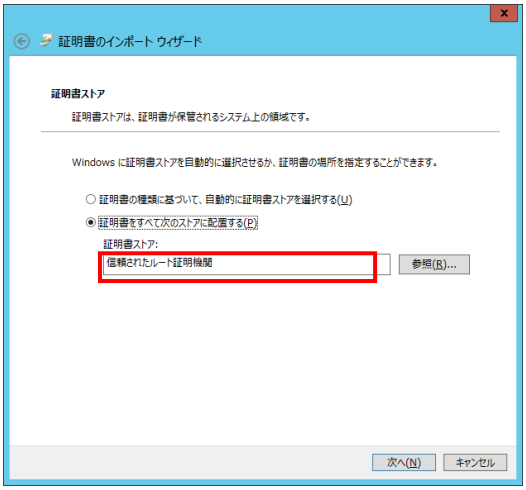


⑩ 証明書ストアが”中間証明機関”または“信頼されたルート証明機関”であることを確認し”次へ”をクリック。

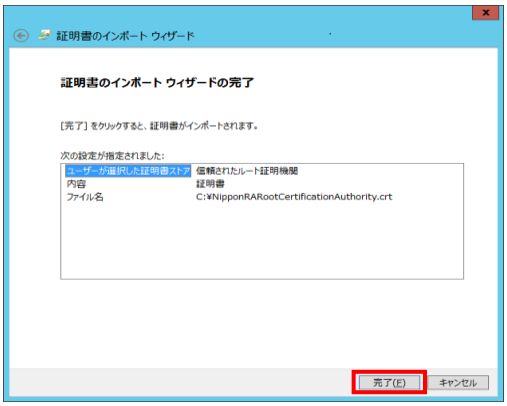
中間証明機関の場合



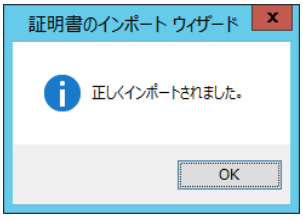
ルート証明機関の場合



⑪ “完了”をクリックして証明書インポートウィザードを完了。

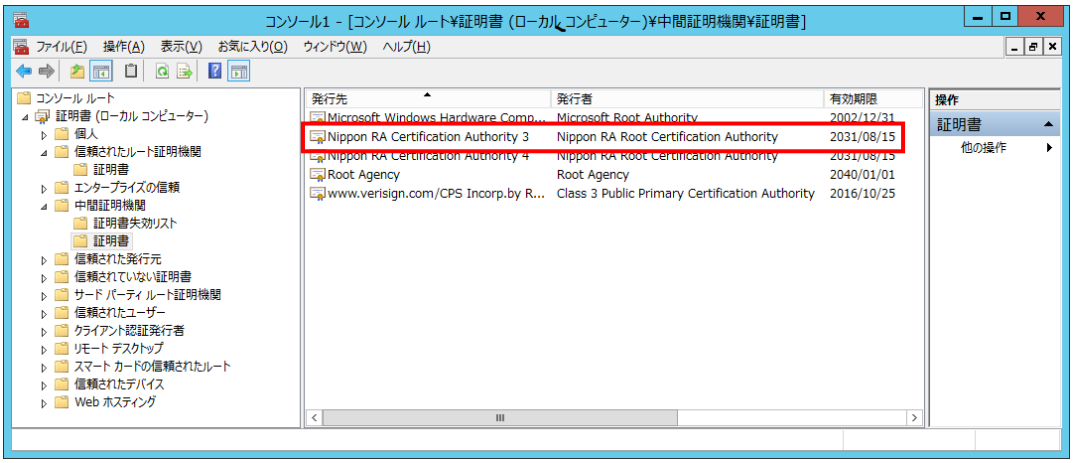


⑫ 正しくインポートされたことを確認し”OK”をクリック。手順⑦～⑫までを繰り返します。

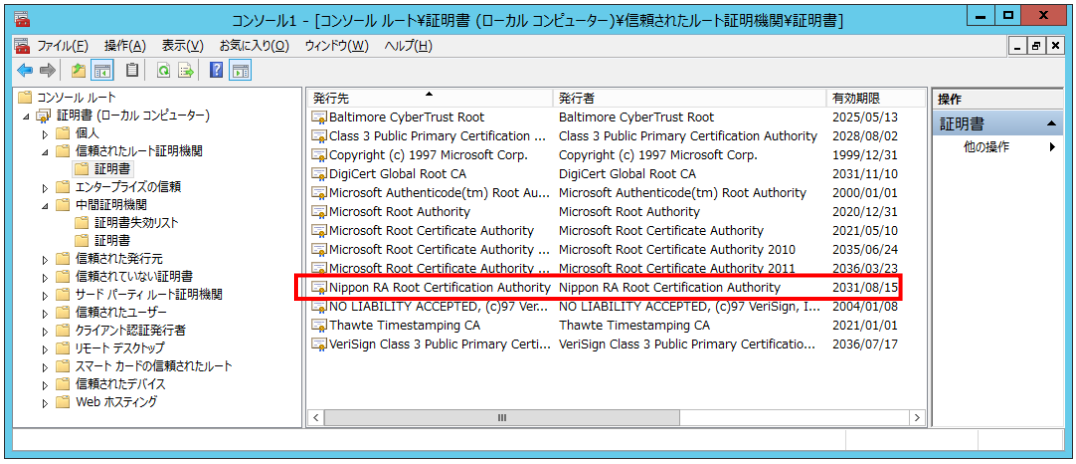


⑬ インポートされた証明機関の証明書を確認。

中間証明機関(画像は CA3)



ルート証明機関

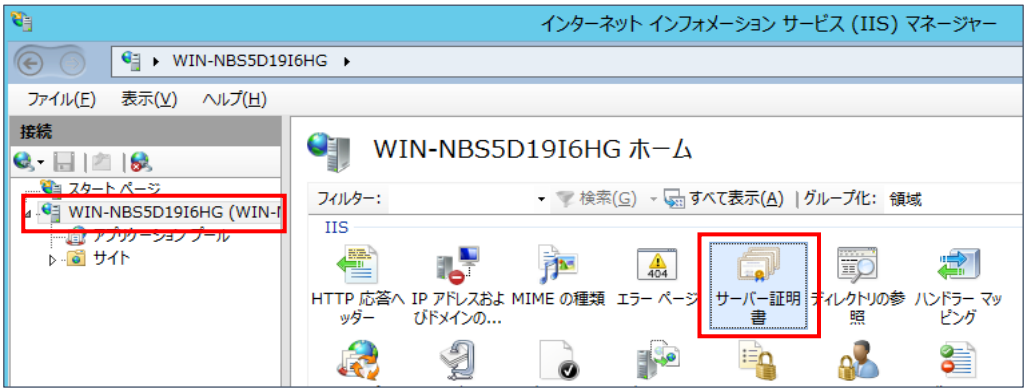


3.5. サーバ証明書のインポート

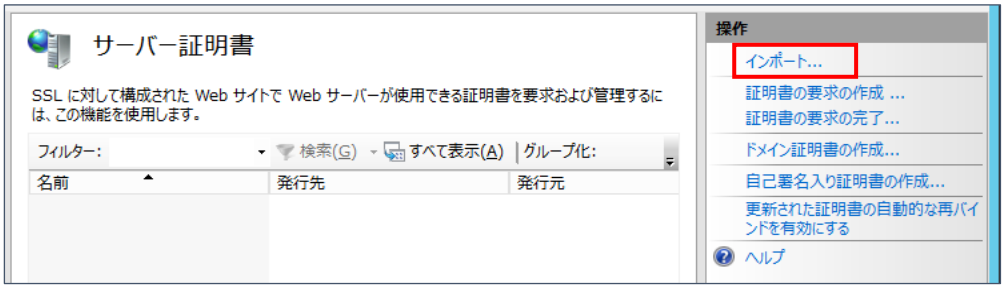
① インターネット インフォメーション サービス（IIS）マネージャを実行。
"スタート"→"管理ツール"→" インターネット インフォメーション サービス（IIS）マネージャ"
を選択。

※以降、手順 3.10 まで、インターネット インフォメーション サービス（IIS）マネージャで設定します。

② Web サーバのホームを選択し、"サーバ証明書"をダブルクリック。

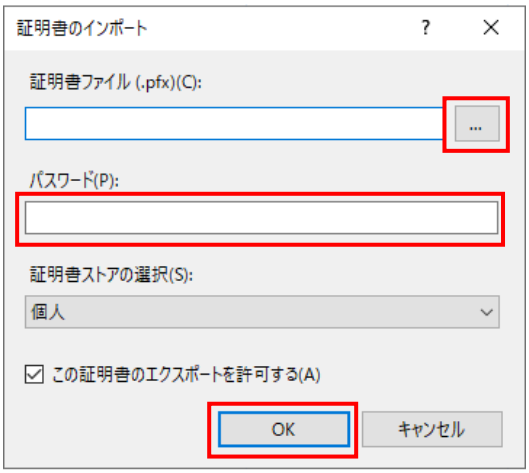


③ "インポート"をクリック。



④ サーバ証明書ファイルを選択し、パスワードを入力後 OK"をクリック。

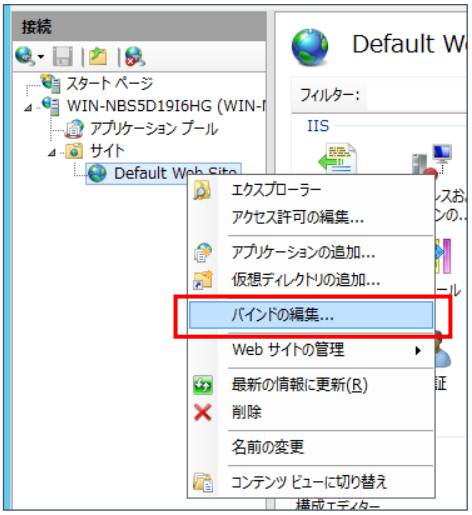
＊ファイルの形式は「.p12」



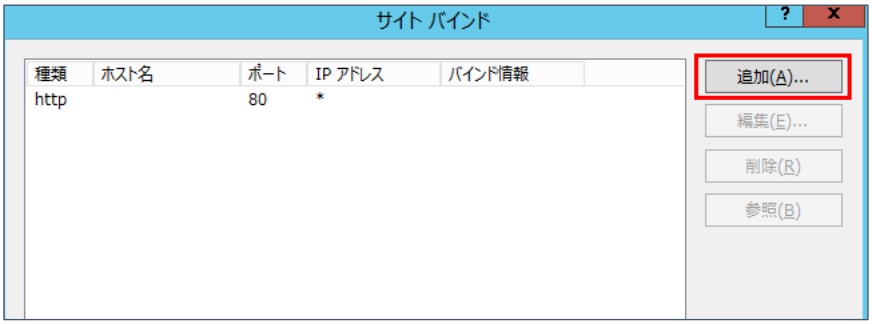
3.6. サイトのバインド編集

バインド編集を実行し、手順 3.5 でインポートしたサーバ証明書を https のポートに設定します。

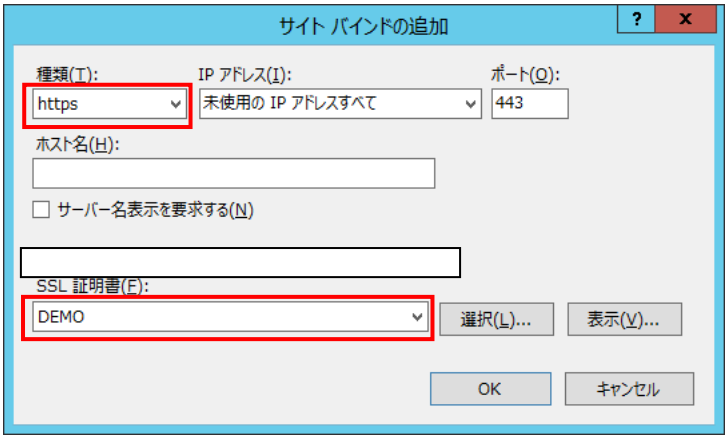
① “Default Web Site”を選択し、右クリックから”バインドの編集”を選択。



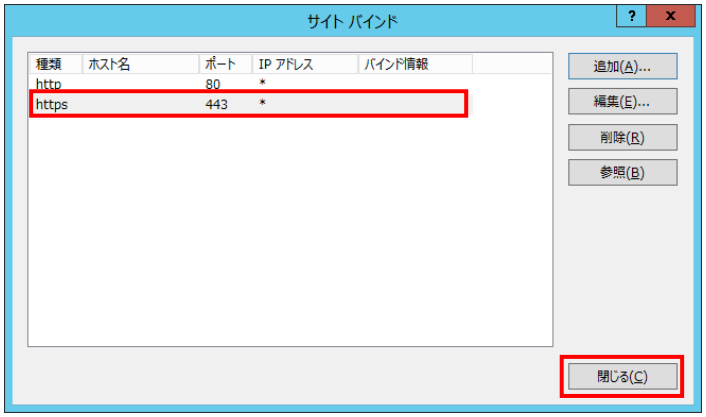
② サイトバインドから”追加”をクリック。



③ “種類”のリストから”https”を選択し、次に手順 3.5 でインポートしたサーバ証明書をリストから選択。”OK”をクリック。

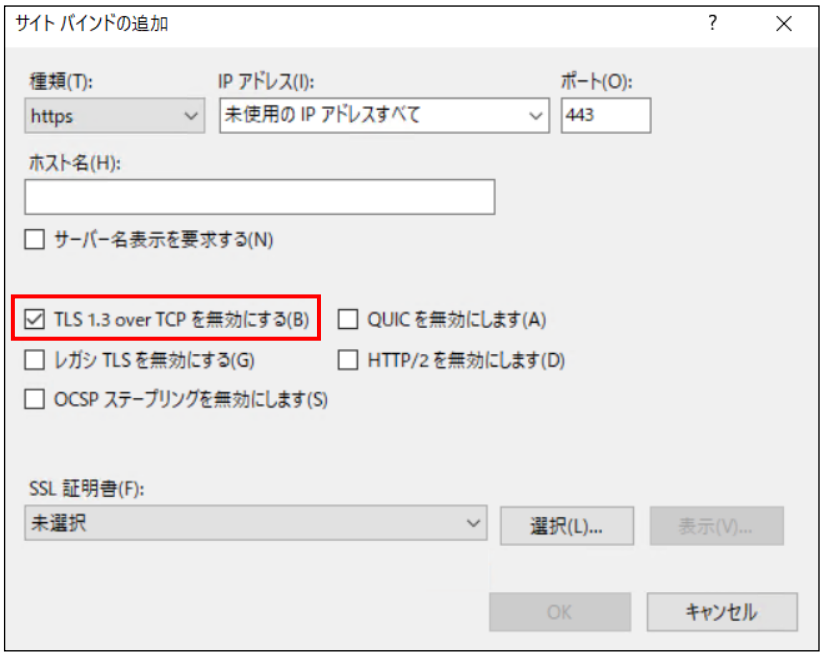


④ https が追加されたことを確認し”閉じる”をクリック。



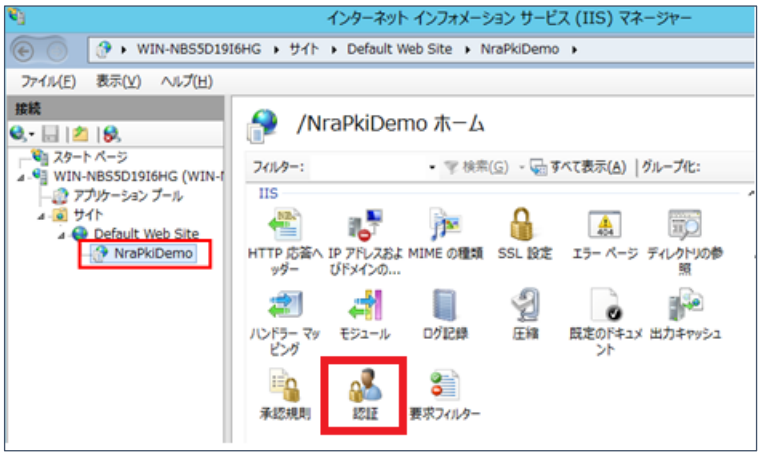
【補足】

Windows Server 2022 の IIS においてクライアント証明書認証でうまく接続できない場合は、バインド編集から「TLS 1.3 over TCP を無効にする」にチェックを入れてお試しください。

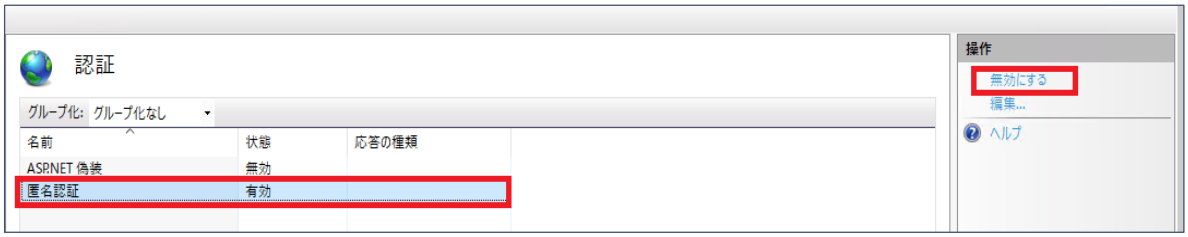


3.7. 認証の設定

① 本手順対象の Web アプリケーションを選択し、/<アプリケーション> ホーム→”認証”をダブルクリック。

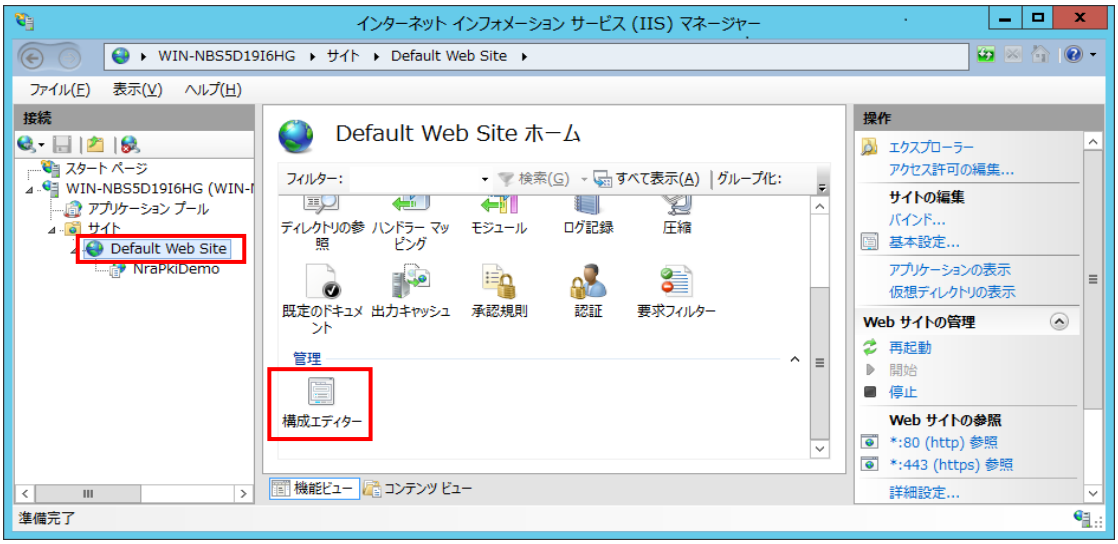


② “匿名認証“を選択し、”無効にする“をクリック。

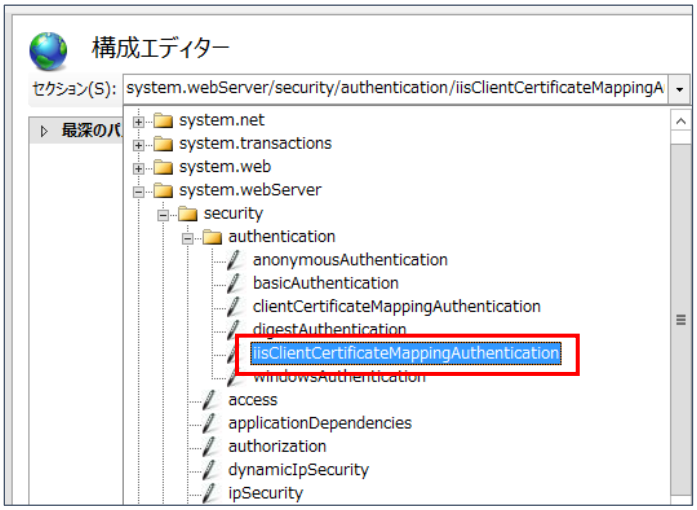


3.8. IIS 多対 1 マッピング規則（ルール）の設定

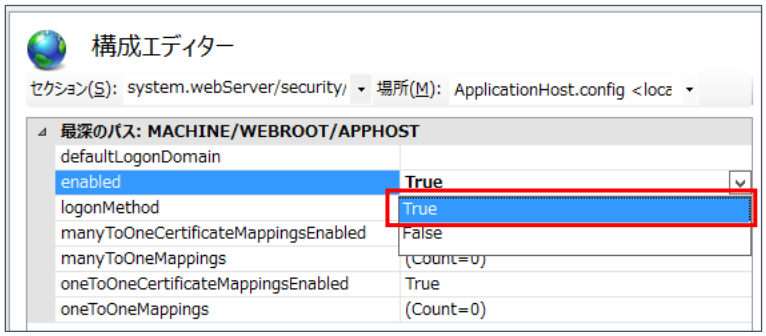
① 本手順対象の Web アプリケーションを選択し、Default Web Site ホーム→”構成エディター”をダブルクリック。



② セクションのリストから” iisClientCertificateMappingAuthentication”を選択。
system.webServer/security/authentication/iisClientCertificateMappingAuthentication を選択

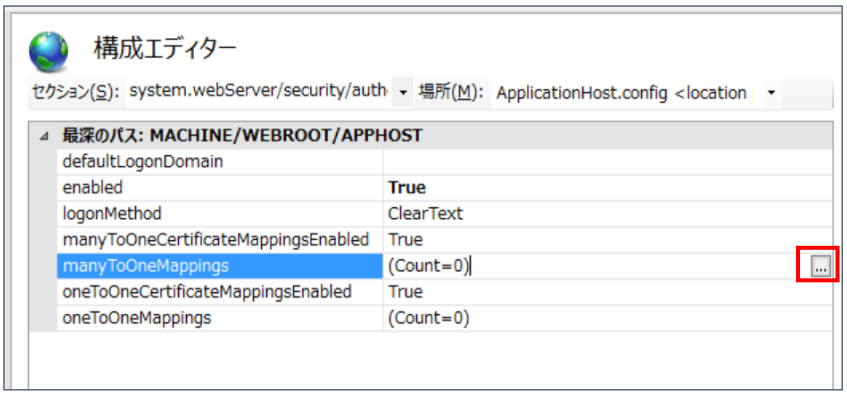


③ ”enabled” のプルダウンメニューから”True” を選択。

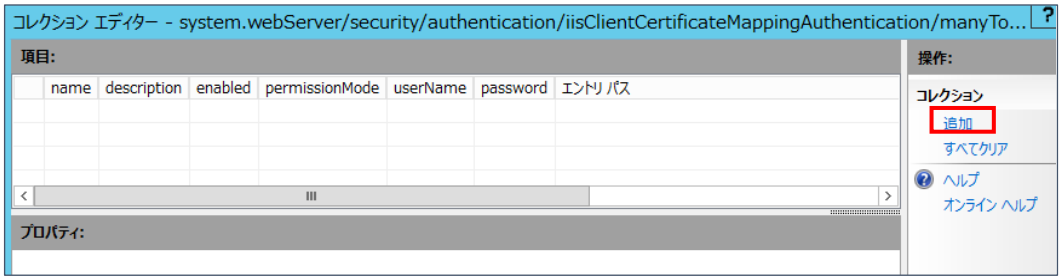


④ 多対 1 マッピング規則（ルール）を設定。

ManyToOneMappings のリストボタンをクリック。



⑤ コレクションエディターの “追加“をクリック。



⑥ “ManyToOneMappings”のプロパティを設定。(”rules“の設定は⑦以降で行います。)

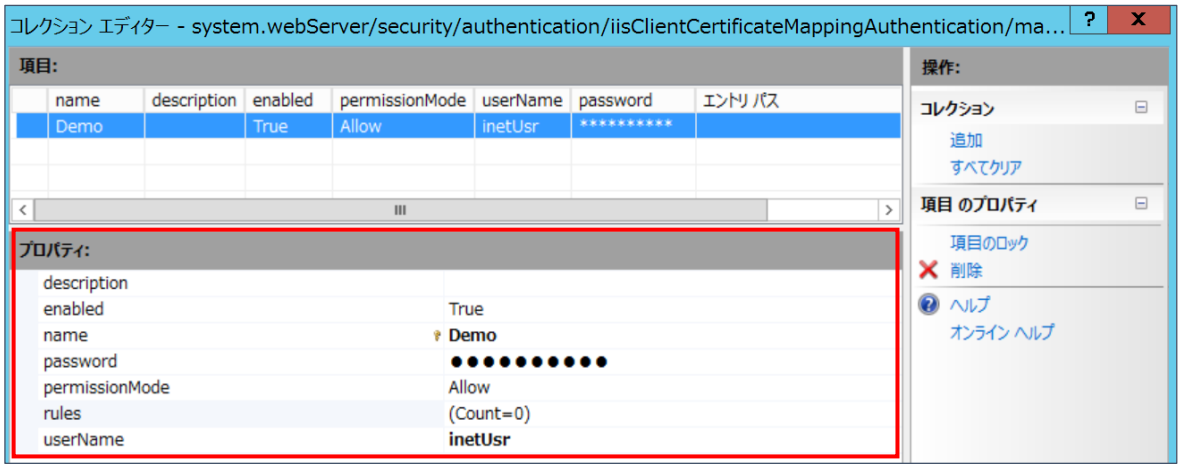
(1)enabled → “True”

(2)name → 任意で指定

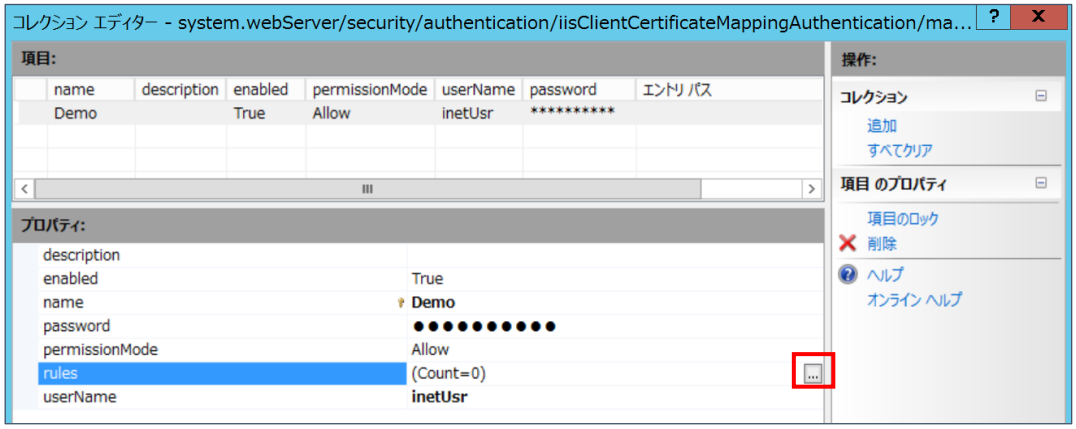
(3)password → 手順 3.3 で作成した OS ユーザーのパスワードを設定

(4)permissionMode → “Allow”

(5)userName → 手順 3.3 で作成した OS ユーザーを設定



⑦ プロパティの“rules”を選択しリストボタンをクリック。



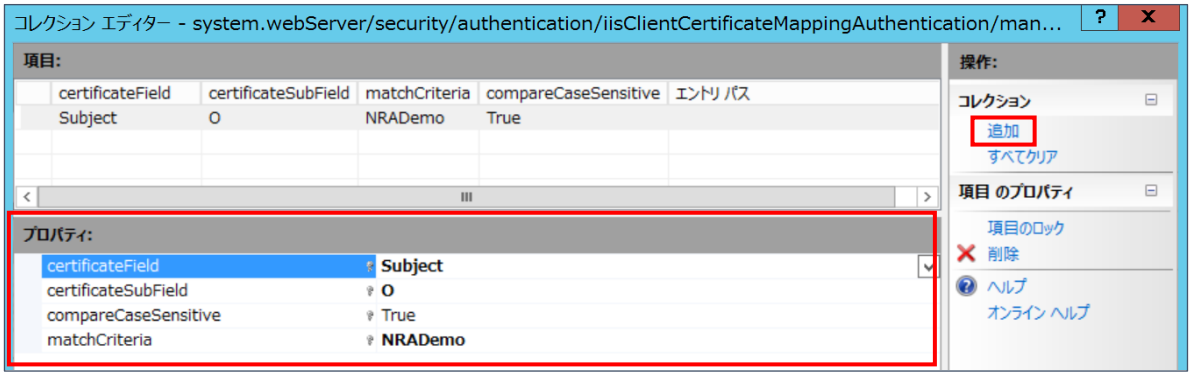
⑧ 新たに表示されたコレクションエディターの”追加“をクリックして、”Rules”（サブジェクト）のプロパティを設定

(1)certificateField → “Subject”

(2)certificateSubField → “O”

(3)compareCaseSensitive → “True”

(4)matchCriteria → クライアント証明書のサブジェクトを指定



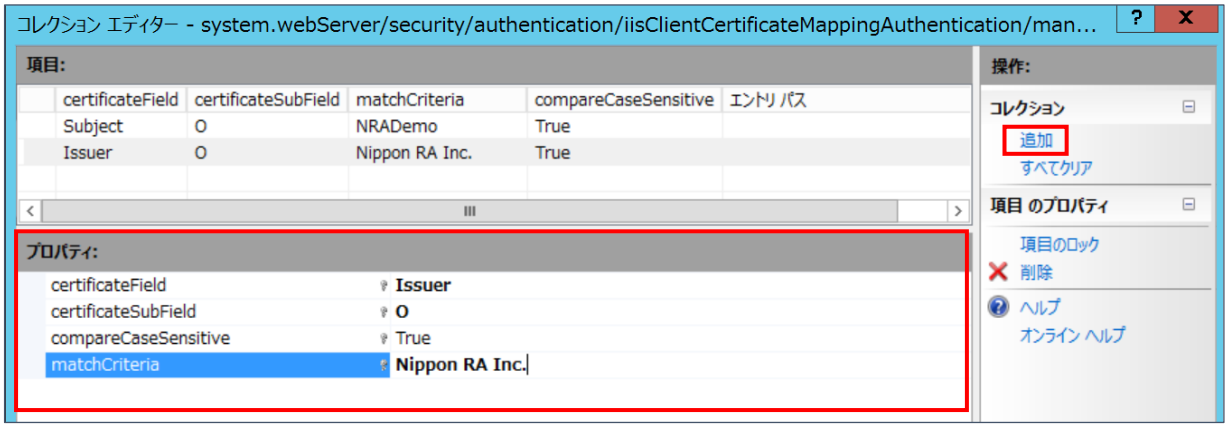
⑨ 再度、“追加”をクリックして、”rules”（発行元）のプロパティを設定

(1)certificateField → “Issure”

(2)certificateSubField → “O”

(3)compareCaseSensitive → “True”

(4)matchCriteria → 発行元証明書のサブジェクトを指定

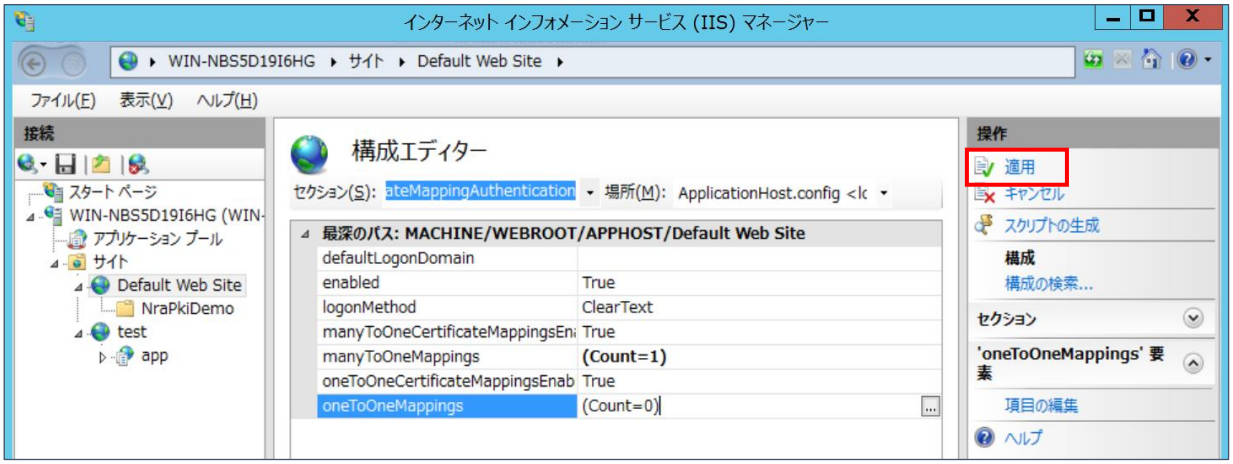


※以下、(1)、(2)が AND で合致した場合、認証を許可するルールとなります。

(1)Subject：クライアント証明書のサブジェクト情報の”O”が、”matchCriteria”で指定された法人の英字表記であること

(2)Issuer：発行元の”O”が、”matchCriteria”で指定された日本 RA の英字表記であること

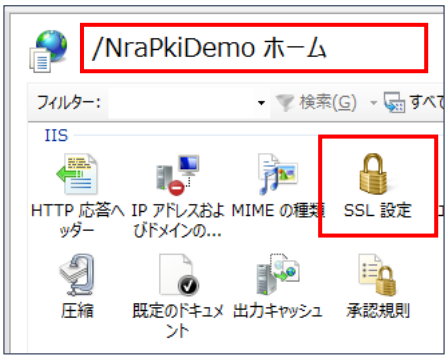
⑩ コレクションエディターをすべて閉じて、インターネット インフォメーション サービス (IIS) マネージャの”適用“をクリックして変更内容を保存



3.9. SSL 設定

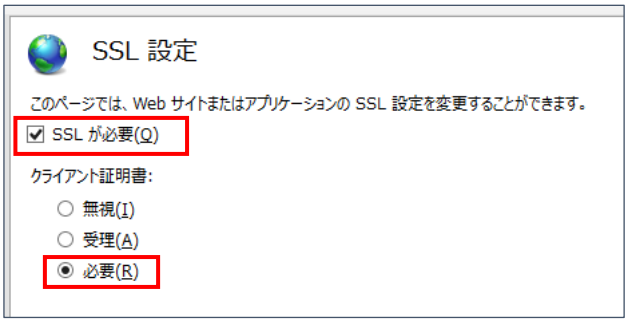
クライアント証明書を必要とする SSL クライアント認証を実装する。

① 本手順対象の Web アプリケーションを選択し、/<アプリケーション> ホーム→”SSL 設定”をダブルクリック。



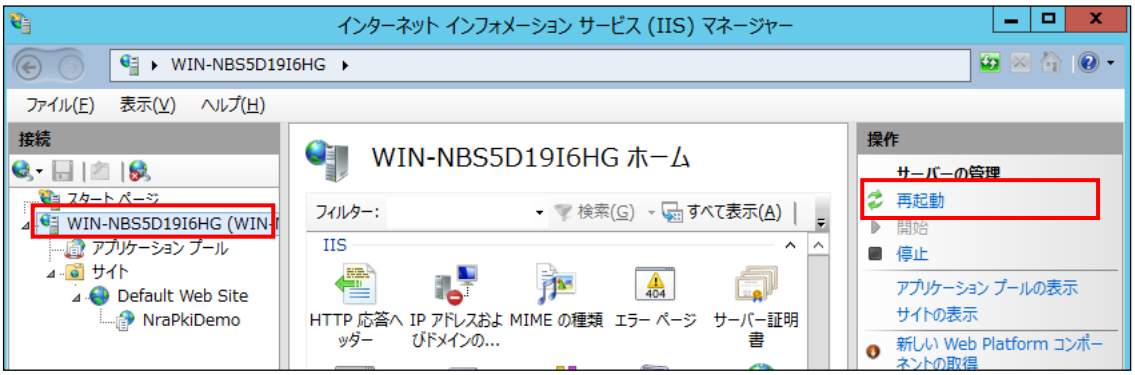
② SSL 設定

“SSL が必要”にチェックし、クライアント証明書の箇所で”必要”を選択。



③ Web サーバの IIS 再起動。

Web サーバ ホームを選択し、再起動をクリック。



【補足】CRL の更新間隔の変更手順について

① ご利用のサーバにて cmd.exe(コマンドプロンプト)を管理者として実行してください。

② 以下コマンドにて証明書のバインドを確認し、結果をメモ帳などに保存します。

netsh http show sslcert

```
C:\Users\Administrator>netsh http show sslcert

SSL Certificate bindings:
-------------------------



    IP:port                      : 0.0.0.0:443
    Certificate Hash             : c03c505301f4d329f494b52425585bc4015675d4
    Application ID               : {4dc3e181-e14b-4a21-b022-59fc669b0914}
    Certificate Store Name       : My
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Disabled
    Reject Connections           : Disabled
    Disable HTTP2                : Not Set
    Disable QUIC                 : Not Set
    Disable TLS1.2               : Not Set
    Disable TLS1.3               : Set
    Disable OCSP Stapling        : Not Set
    Enable Token Binding         : Not Set
    Log Extended Events          : Not Set
    Disable Legacy TLS Versions  : Not Set
    Enable Session Ticket        : Not Set
 Extended Properties:
    PropertyId                   : 0
    Receive Window               : 1048576
 Extended Properties:
    PropertyId                   : 1
    Max Settings Per Frame       : 2796202
    Max Settings Per Minute      : 4294967295
 Extended Properties:
    PropertyId                   : 2
 Extended Properties:
    PropertyId                   : 3
 Extended Properties:
    PropertyId                   : 4
```

③ 以下コマンドにて証明書のバインドを削除してください（②で確認した IP:port の値を指定します。）

netsh http delete sslcert ipport= x.x.x.x:xxx

④ 以下コマンドにてバインドの再作成をします。

netsh http add sslcert ipport=x.x.x.x:xxx certhash=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
appid={xxxxxx-xxxx-xxxx-xxxx-xxxx} certstorename=xxx verifyclientcertrevocation=enable
verifyrevocationwithcachedclientcertonly=disable usagecheck=enable
revocationfreshnesstime=任意の数値 urlretrievaltimeout=任意の数値

x の部分には②で確認した内容を以下の箇所に代入し実行してください。

ipport = IP:port の値
certhash = Certificate Hash の値
appid = Application ID の値
certstorename = Certificate Store Name の値
verifyclientcertrevocation = enable
verifyrevocationwithcachedclientcertonly = disable
usagecheck = enable
revocationfreshnesstime = 任意の数値※
(更新版の CRL をチェックする間隔 (秒))
urlretrievaltimeout = 任意の数値※
(証明書失効一覧の取得試行がタイムアウトになる時間 (ミリ秒))

※本手順で変更となる箇所です。数値が小さすぎるとうまく動作しない可能性がございます。
revocationfreshnesstime=3600、urlretrievaltimeout=300000 での動作確認はできております。

以上で CRL の更新間隔の変更は完了です。

3.10. クライアント証明書の情報参照（クライアント側）

Web アプリケーションの認証で使用するクライアント証明書がインポートされていることを前提に、証明書の内容を確認する手順を記載します。

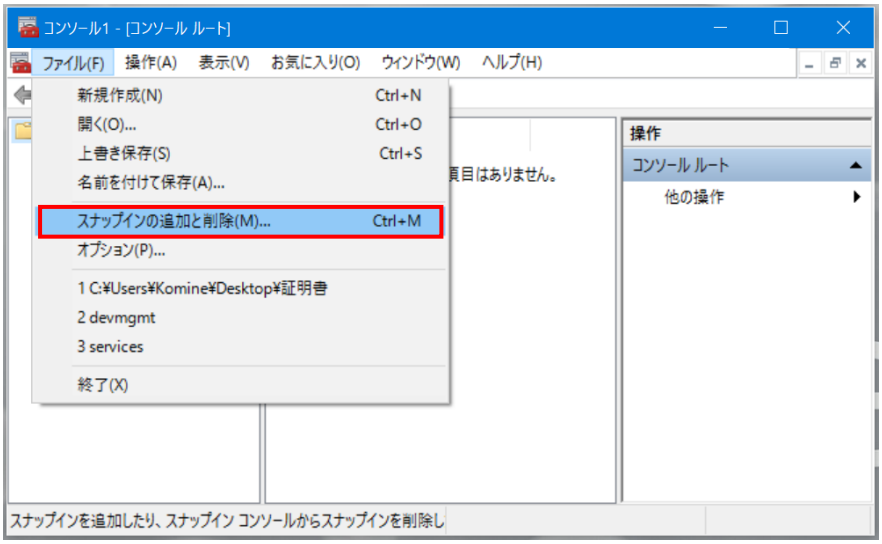
（本手順の画面キャプチャは Windows10 環境で取得しております。）

① mmc の起動

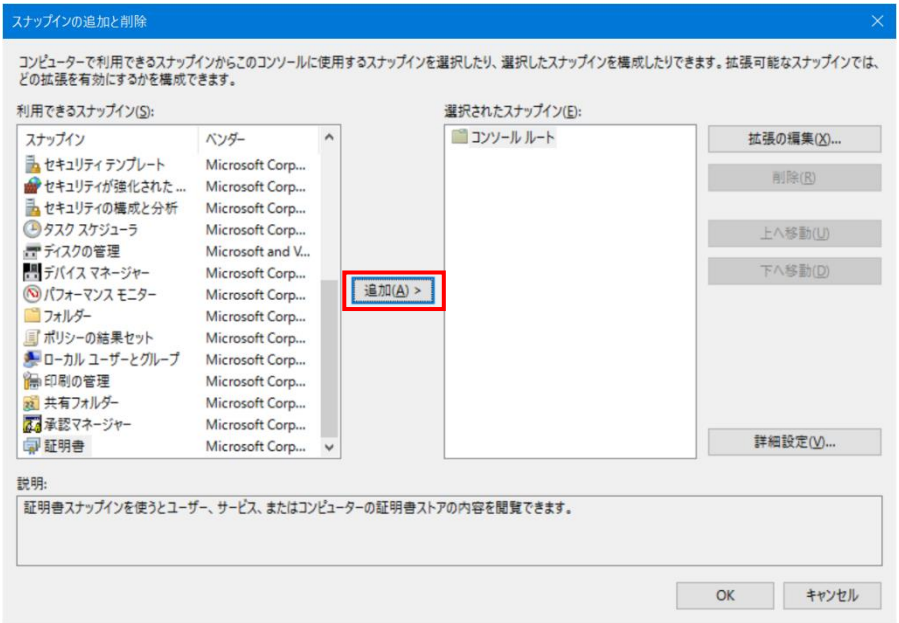
Windows キーを押下し、検索 で“mmc” と入力し、”Enter”を押下します。

② スナップインの追加

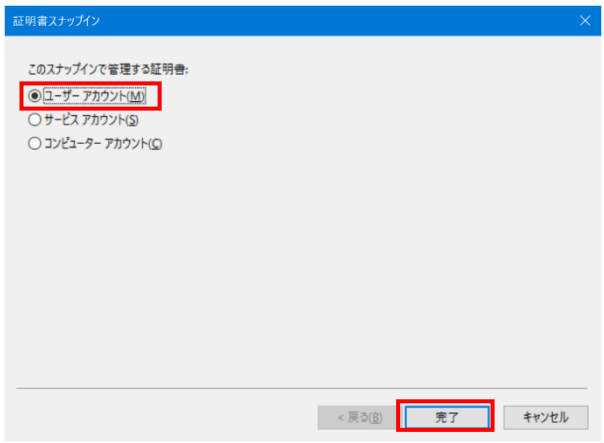
ファイル→スナップインの追加と削除を選択。



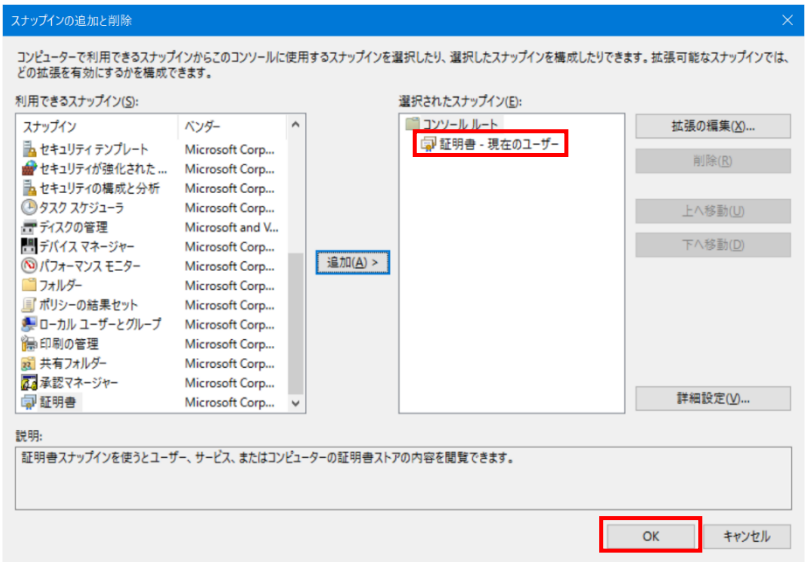
③ 左画面の下方にある証明書を選択、”追加”をクリック。



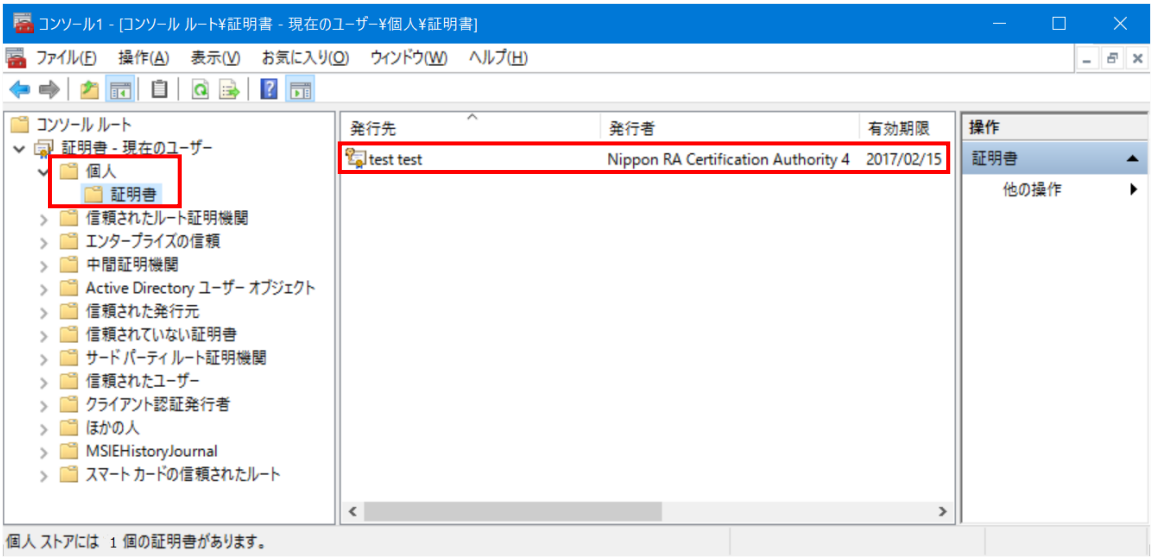
④ 証明書スナップイン画面にて”ユーザアカウント”を選択し、”完了”をクリック。



⑤ 右画面（選択されたスナップイン）に”証明書 – 現在のユーザー”が表示されたことを確認し、”OK”をクリック。



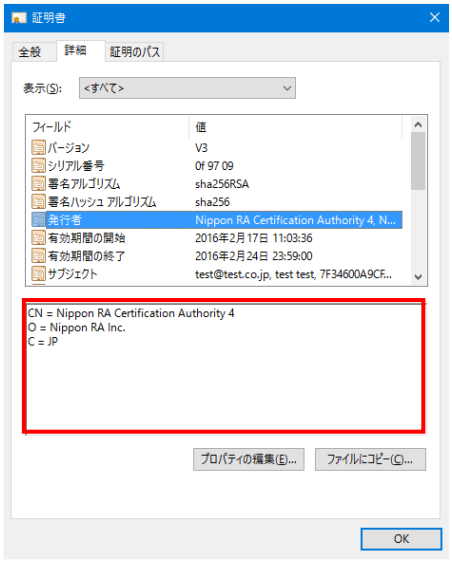
⑥ ”コンソールルート”→”証明書 – 現在のユーザー”→”個人”→”証明書”を選択し、証明書が右画面に表示されることを確認。



⑦ 表示された証明書をダブルクリックしプロパティを表示させる。

⑧ 上部、"詳細"タブを選択し、２つのフィールドを確認します。

(1) 発行者



"発行者"はクライアント証明書の証明機関を示します。

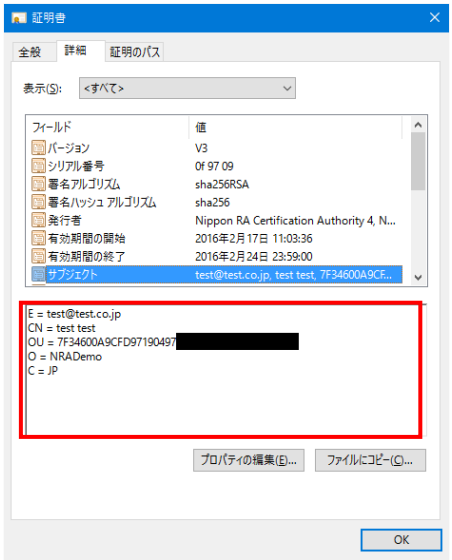
CN=証明機関（発行・認証局）

※NRA では、Nippon RA Certification Authority 3 または Nippon RA Certification Authority 4 が表示されます。

O=発行局を管理する日本 RA の英字表記

C=国

(2) サブジェクト



"サブジェクト"はクライアント証明書を配付されたユーザー

E= E メールアドレス

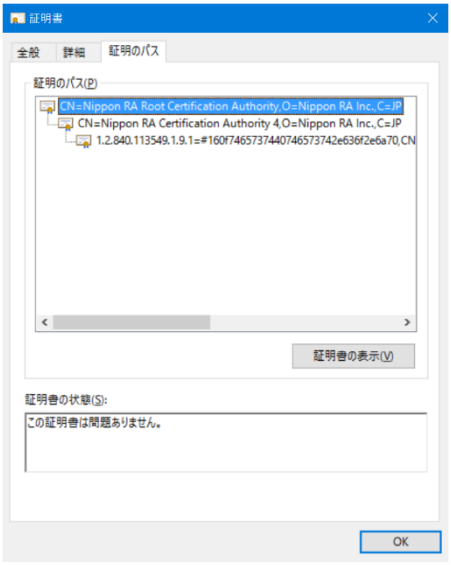
CN= 配布ユーザーの英字表記

OU=NRA-PKI システムのユーザーID

O=法人の英字表記

C=国

⑨ 上部、"証明のパス"タブを選択し、証明書のパスを確認。



"証明書のパス"はNRAがクライアント証明書の認証機関を示します。
ルート認証機関（Nippon RA Root Certification Authority）

※クライアント証明書のインポート時に、証明機関の証明書をインポートしなかった場合、
警告が表示され認証に使えない証明書となります。