

# NRA

## マルチトラスト設定ガイド

(IIS10.0 編)

2024 年 09 月 06 日

Ver. 1.00

改訂履歴

| 版            | 日 付      | 内 容  | 備 考 |
|--------------|----------|------|-----|
| Ver.<br>1.00 | 2024/9/6 | 初版作成 |     |

## <目 次>

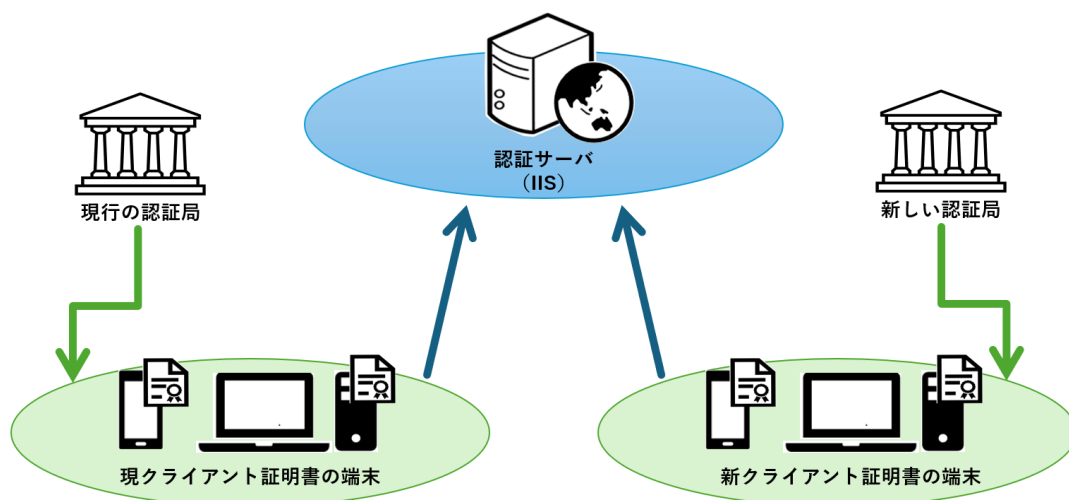
|                                          |    |
|------------------------------------------|----|
| 1. 概要.....                               | 3  |
| 1.1. はじめに .....                          | 3  |
| 1.2. 本書における注意事項 .....                    | 4  |
| 1.3. 失効リスト（CRL）について .....                | 4  |
| 2. マルチトラストの設定手順 .....                    | 5  |
| 2.1. 認証局証明書のインポート .....                  | 6  |
| 2.1.1. 新しい認証局のルート証明書および中間証明書の取得 .....    | 6  |
| 2.1.2. 新しい認証局のルート証明書および中間証明書のインポート ..... | 7  |
| 2.2. クライアント証明書認証の設定 .....                | 16 |
| 3. Appendix1（中間認証局の確認方法） .....           | 23 |
| 4. Appendix2（クライアント証明書情報の確認方法） .....     | 24 |

# 1. 概要

## 1.1. はじめに

本書は、NRA-PKI クライアント証明書の認証局（表 1）の世代交代（※1）に伴い、現行の認証局から発行したクライアント証明書と新しい認証局から発行したクライアント証明書の両方を従来と同様にご利用頂くための IIS におけるマルチトラスト設定の手順を記載したものです。

【構成図】



【表 1 NRA-PKI の認証局】

|          | 現行の認証局                                 | 新しい認証局                                    |
|----------|----------------------------------------|-------------------------------------------|
| ルート認証局   | Nippon RA Root Certification Authority | Nippon RA Root Certification Authority G2 |
| 中間認証局CA3 | Nippon RA Certification Authority 3    | Nippon RA Certification Authority 3 G2    |
| 中間認証局CA4 | Nippon RA Certification Authority 4    | Nippon RA Certification Authority 4 G2    |
| 中間認証局CA5 | Nippon RA Certification Authority 5    | Nippon RA Certification Authority 5 G2    |

※1 現行のルート認証局および中間認証局の有効期限により新しい認証局への移行

## 1.2. 本書における注意事項

本書は既存のクライアント証明書認証に追加して、新しい認証局のクライアント証明書を認証する設定手順を記載しております。

詳しいクライアント証明書認証の設定手順については、[Web サーバ設定ガイド](#)をご参照ください。

また、中間認証局 CA3 以外をご利用の場合は、本書における「Nippon RA Certification Authority 3」および「CA3」という記載をご利用の中間認証局に置き換えてください。

ご利用の中間認証局の確認方法については、後記の [Appendix1](#) をご参照ください。

※Windows Server 2022 環境に IIS10.0 をインストールして動作確認をしております。

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。

## 1.3. 失効リスト（CRL）について

IIS では証明書の失効確認はデフォルトで有効になっています。失効リストで失効確認をされている場合は失効確認に関する設定は不要となります。独自に失効確認をしている場合は、別途対応をお願いいたします。

## 2. マルチトラストの設定手順

IIS における認証局世代交代に伴うマルチトラスト設定は以下の手順で行います。

### 2.1. 認証局証明書のインポート

新しい認証局の証明書をインポートします。

### 2.2. クライアント証明書認証の設定変更

クライアント認証で許可する条件を設定します。

## 2.1. 認証局証明書のインポート

---

クライアント認証で許可する認証局証明書に、新しい認証局の証明書を追加します。

### 2.1.1. 新しい認証局のルート証明書および中間証明書の取得

ルート認証局 G2 の証明書とご利用の中間認証局の証明書を以下の URL よりダウンロードしてください。

ご利用の中間認証局の確認方法については、[Appendix1](#) をご参照ください。

#### 【新しい認証局の証明書】

##### ■ルート認証局 G2（Nippon RA Root Certification Authority G2）

<https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt>

##### ■中間認証局 CA 3 G2（Nippon RA Certification Authority 3 G2）

<https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt>

##### ■中間認証局 CA 4 G2（Nippon RA Certification Authority 4 G2）

<https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt>

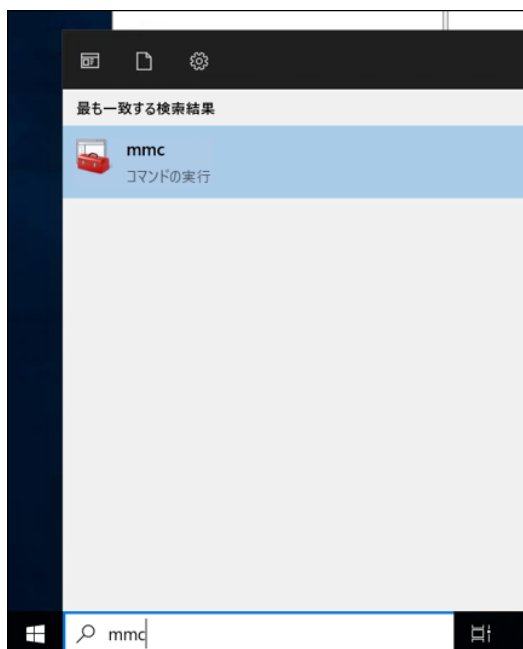
##### ■中間認証局 CA 5 G2（Nippon RA Certification Authority 5 G2）

<https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority5G2.crt>

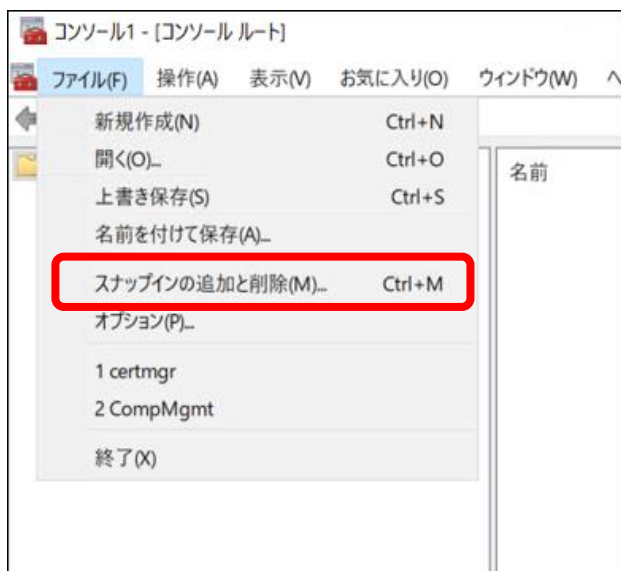
### 2.1.2. 新しい認証局のルート証明書および中間証明書のインポート

手順 2.1.1.で取得したルート証明書と中間証明書をインポートします。

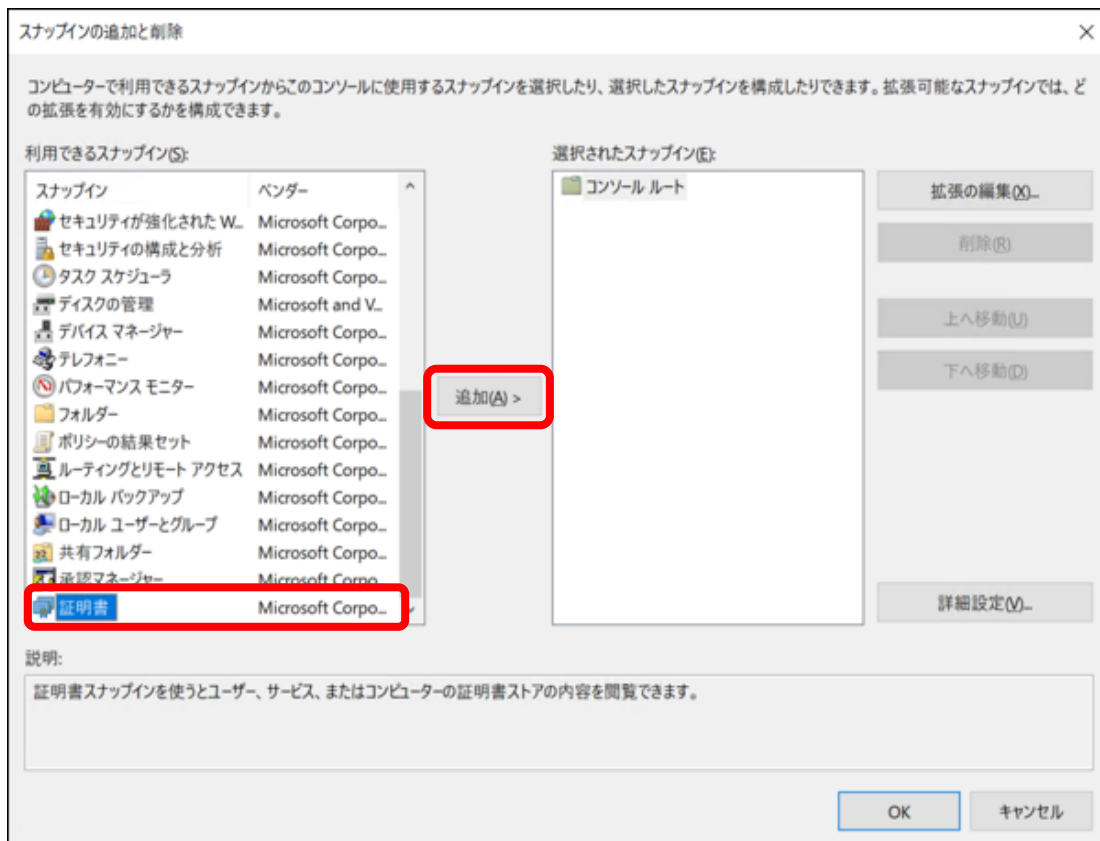
- (1) 画面左下の検索アイコン（または Windows キー）を押下し「mmc」と入力して、検索結果に表示された mmc（管理コンソール）を起動します。



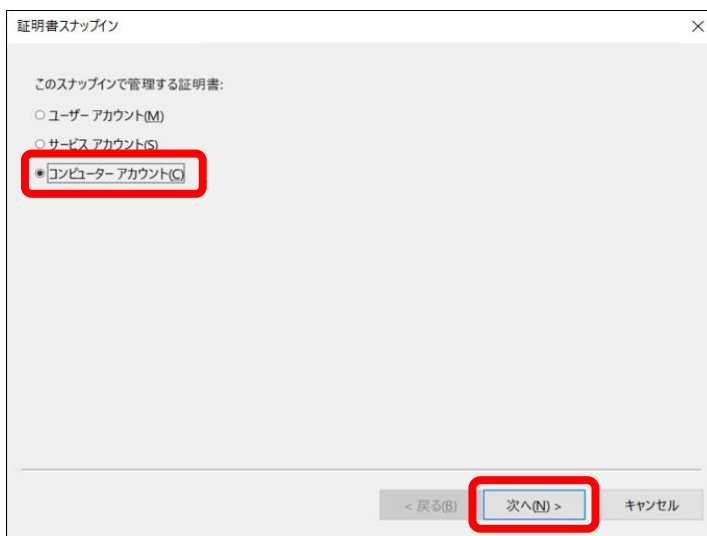
- (2) 「ファイル (F)」 - 「スナップインの追加と削除」を選択します。



(3) 左画面の下方にある証明書を選択し、「追加」をクリックします。



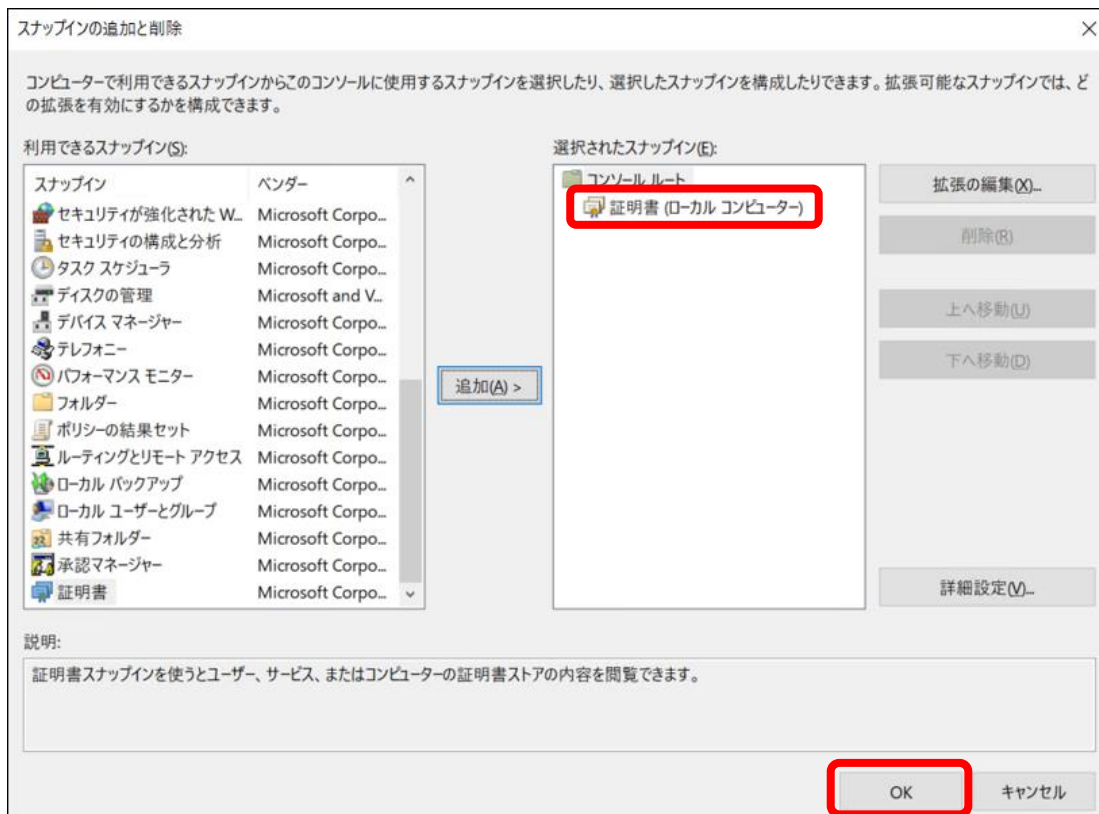
(4) 証明書スナップイン画面にて「コンピューターアカウント」を選択し、「次へ」をクリックします。



- (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ー」が選択されていることを確認し「完了」をクリックします。

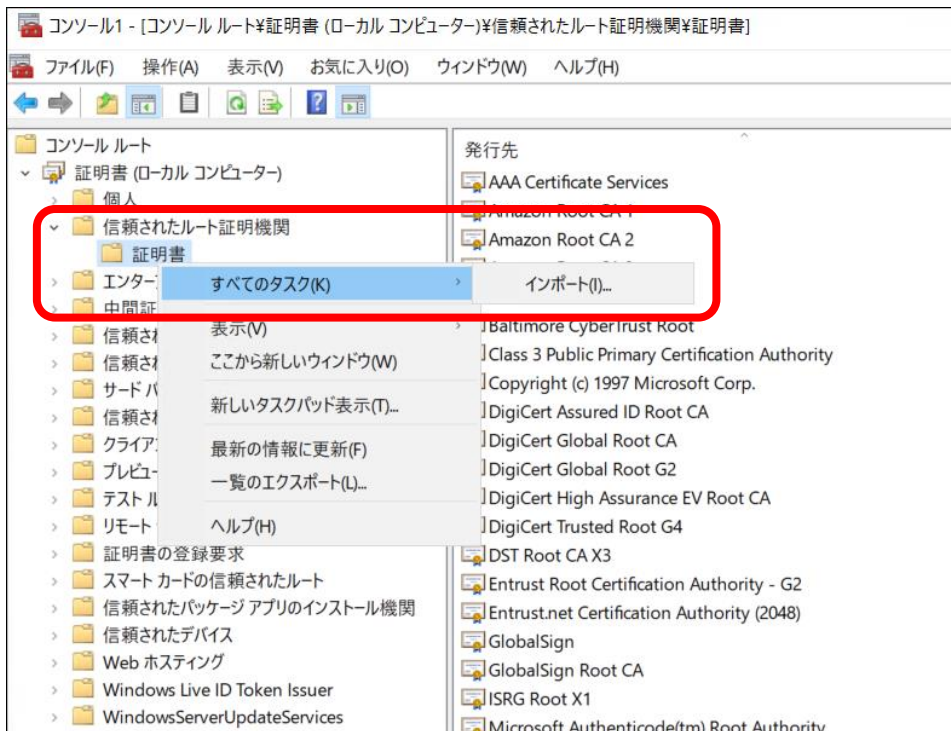


- (6) 手順(3)の「スナップインの追加と削除」画面の右側に「証明書」が追加されたことを確認し「OK」をクリックします。



(7) ルート証明書をインポートします。

「信頼されたルート証明機関」 - 「証明書」を右クリック、「すべてのタスク」 - 「インポート」を選択します。



(8) 証明書のインポートウィザードの開始を確認し、「次へ」をクリックします。



(9) 「参照」をクリックし、手順 2.1.1. でダウンロードした新しいルート認証局の証明書を選択します。

← 証明書のインポート ウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):  
.\Administrator\Downloads\NipponRA RootCertificationAuthorityG2.crt 参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (PFX,P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (P7B)
- Microsoft シリアル化された証明書ストア (SST)

次へ(N) キャンセル

(10) 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」をクリックします。

← 証明書のインポート ウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

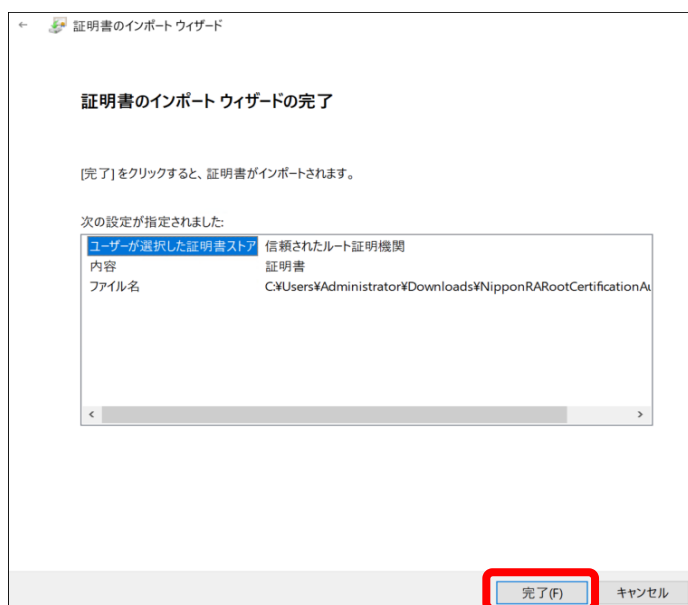
○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

● 証明書をすべて次のストアに配置する(P)

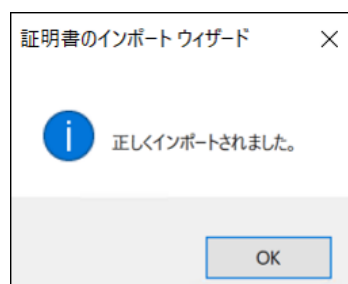
証明書ストア:  
信頼されたルート証明機関 参照(R)...

次へ(N) キャンセル

(11) 「完了」をクリックします。



(12) 正しくインポートされたことを確認し「OK」をクリックします。

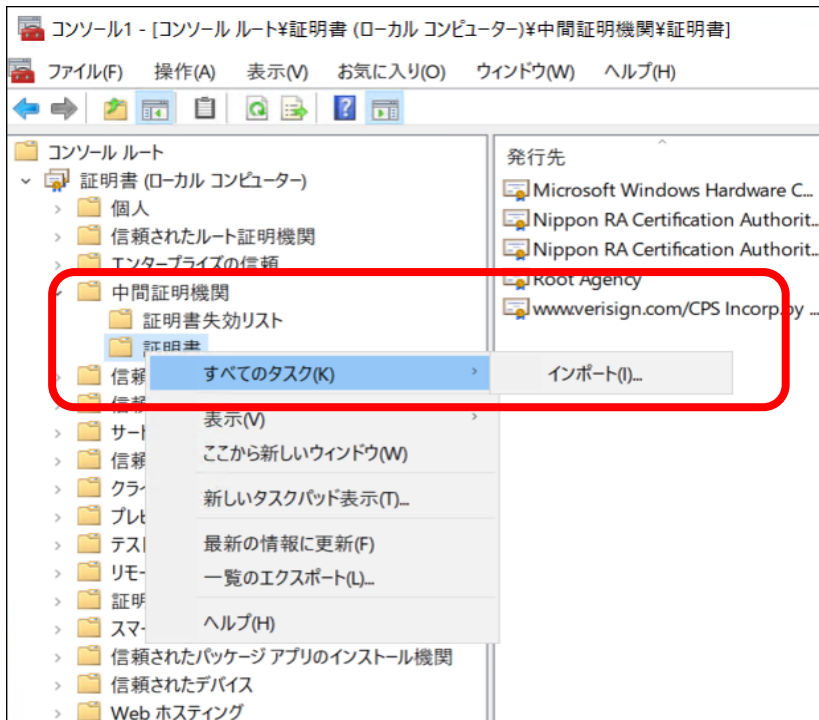


(13) インポートされた新しいルート認証局の証明書を確認します。



(14) 中間証明書をインポートします。

「中間証明機関」－「証明書」を右クリック、「すべてのタスク」－「インポート」を選択します。



(15) 証明書のインポートウィザードの開始を確認し、「次へ」をクリックします。



(16) 「参照」をクリックし、手順 2.1.1. でダウンロードした新しい中間認証局の証明書を選択します。

← 証明書のインポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):  
Jsers¥Administrator¥Downloads¥NipponRACertificationAuthority3G2.crt

参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

Personal Information Exchange- PKCS #12 (PFX,P12)

Cryptographic Message Syntax Standard- PKCS #7 証明書 (P7B)

Microsoft シリアル化された証明書ストア (SST)

次へ(N) キャンセル

(17) 証明書ストアが「中間証明機関」であることを確認し「次へ」をクリックします。

← 証明書のインポートウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

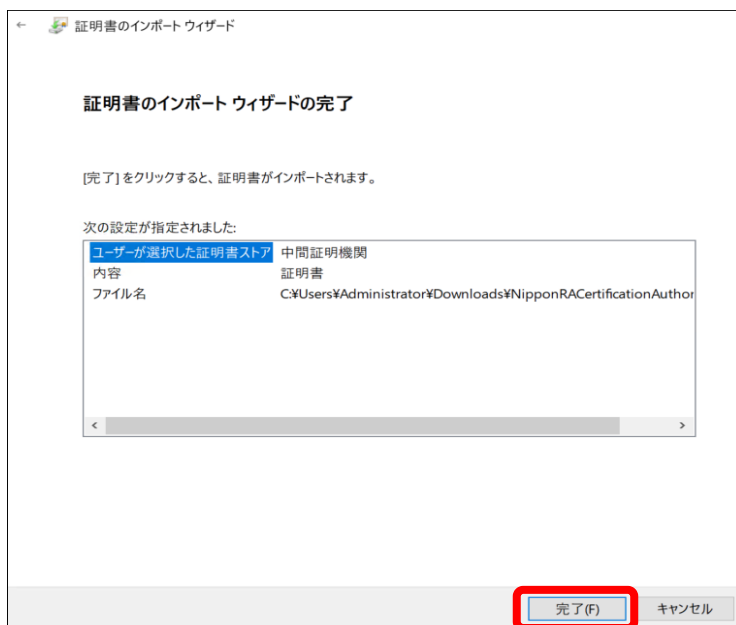
● 証明書をすべて次のストアに配置する(P)

証明書ストア:  
中間証明機関

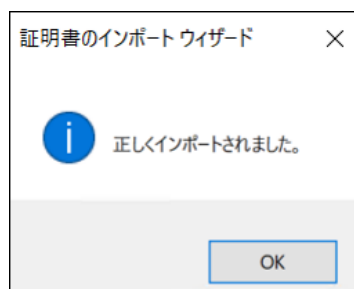
参照(R)...

次へ(N) キャンセル

(18) 「完了」をクリックします。



(19) 正しくインポートされたことを確認し「OK」をクリックします。



(20) インポートされた中間認証局の証明書を確認します。

(図は Nippon RA Certification Authority 3 G2)



## 2.2. クライアント証明書認証の設定

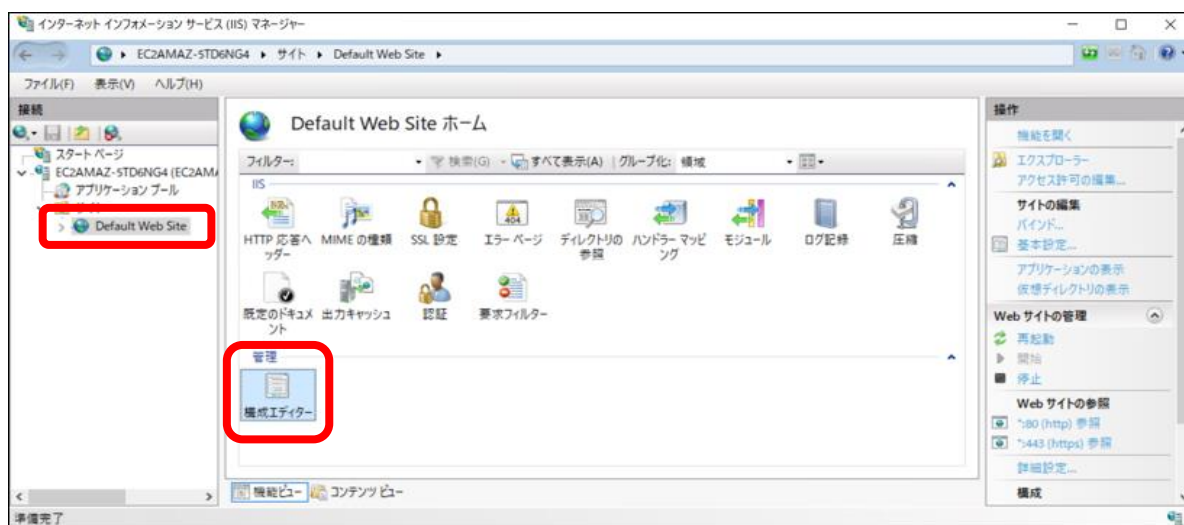
クライアント認証において、新しい認証局の証明書を許可する設定手順を以下に記載します。

なお、クライアント認証の条件に発行局（認証局）を指定していない場合は、本設定は必要ありません。

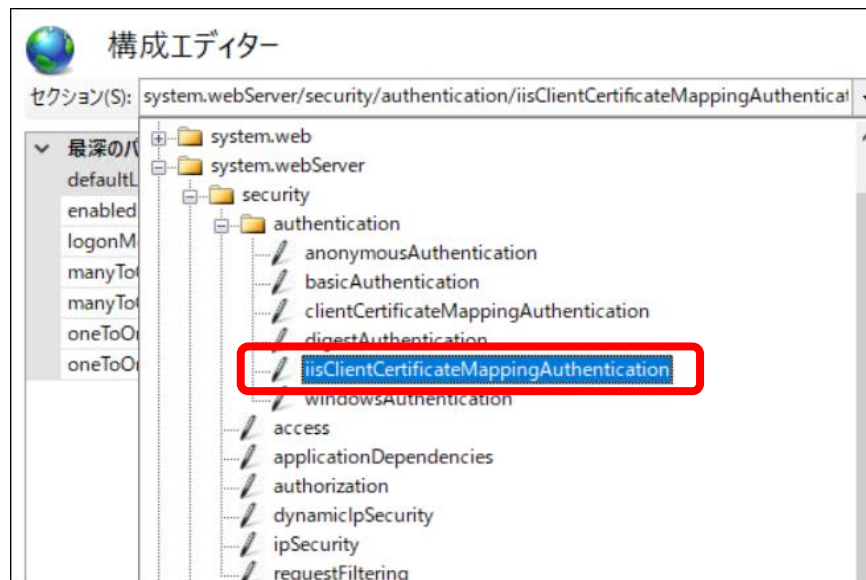
(1) インターネットインフォメーションサービス（IIS）マネージャを実行します。

「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」を選択してください。

(2) 「Default Web Site ホーム」－「構成エディター」をダブルクリックします。



(3) セクションより「iisClientCertificateMappingAuthetication」に移動します。



- (4) 「enabled」を「true」に設定していることを確認し、「manyToOneMappings」の右横のボタンをクリックしコレクションエディターを開きます。

構成エディター

セクション(S): system.webServer/security/authentication/iisC 場所(M): ApplicationHost.config <location path='Defau

▼ 最深のパス: MACHINE/WEBROOT/APPHOST/Default Web Site

|                                     |                                                                                               |
|-------------------------------------|-----------------------------------------------------------------------------------------------|
| defaultLogonDomain                  |                                                                                               |
| enabled                             | True                                                                                          |
| logonMethod                         | ClearText                                                                                     |
| manyToOneCertificateMappingsEnabled | True                                                                                          |
| manyToOneMappings                   | (Count=1)  |
| oneToOneCertificateMappingsEnabled  | True                                                                                          |
| oneToOneMappings                    | (Count=0)                                                                                     |

- (5) 「rules」の右横のボタンをクリックしコレクションエディターを開きます。

項目:

| name | description | enabled | permissionMode | userName | password | エントリパス                  |
|------|-------------|---------|----------------|----------|----------|-------------------------|
| DEMO |             | True    | Allow          | inetUsrr | *****    | MACHINE/WEBROOT/APPHOST |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |
|      |             |         |                |          |          |                         |

< >

プロパティ:

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| description    |                                                                                                 |
| enabled        | True                                                                                            |
| name           | DEMO                                                                                            |
| password       | ●●●●●●●●●●                                                                                      |
| permissionMode | Allow                                                                                           |
| rules          | (Count=1)  |
| userName       | inetUsrr                                                                                        |

(6) 既存のクライアント認証の条件を確認します。

下図のように、発行元（認証局）の CN の値を指定している場合は設定変更が必要となります。

- (例) ・ クライアント証明書のサブジェクト O の値が「matchCriteria」と同じ  
・ 発行元の CN の値が「matchCriteria」と同じ

| 項目:              |                     |                                     |                      |                         |
|------------------|---------------------|-------------------------------------|----------------------|-------------------------|
| certificateField | certificateSubField | matchCriteria                       | compareCaseSensitive | エントリパス                  |
| Subject          | O                   | REIWA CERTIFICATES SERVICES         | True                 | MACHINE/WEBROOT/APPHOST |
| Issuer           | CN                  | Nippon RA Certification Authority 3 | True                 | MACHINE/WEBROOT/APPHOST |

| プロパティ:               |                                     |
|----------------------|-------------------------------------|
| certificateField     | Issuer                              |
| certificateSubField  | CN                                  |
| compareCaseSensitive | True                                |
| matchCriteria        | Nippon RA Certification Authority 3 |

※「クライアント証明書のサブジェクト O の値」のみや「発行元の O の値」を指定している場合は、設定変更は不要です。

(7) クライアント認証の設定変更をします。

既存の認証設定に加え、新しい認証局の証明書を許可する設定を追加します。

「rules」のコレクションエディターを閉じ、「manyToOneMappings」画面に戻り「追加」をクリックします。

コレクション エディター - system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/

| 項目:  |           |         |                |          |          |                         |
|------|-----------|---------|----------------|----------|----------|-------------------------|
| name | descri... | enabled | permissionMode | userName | password | エントリパス                  |
| DEMO |           | True    | Allow          | inetUsr  | *****    | MACHINE/WEBROOT/APPHOST |

| プロパティ:         |            |
|----------------|------------|
| description    |            |
| enabled        | True       |
| name           | DEMO       |
| password       | ●●●●●●●●●● |
| permissionMode | Allow      |
| rules          | (Count=2)  |
| userName       | inetUsr    |

**操作:**  
コレクション  
**追加**  
オブジェクト  
項目のプロパティ  
項目のロック  
削除  
ヘルプ  
オンライン ヘルプ

(8) プロパティを既存の認証設定と同様に設定します。

- enabled → “True”
- name → 任意で指定
- password → OS ユーザーのパスワードを設定
- permissionMode → “Allow”
- userName → OS ユーザーを設定

コレクション エディター - system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/

| 項目:            | 操作:                     |
|----------------|-------------------------|
| permissionMode | Allow                   |
| userName       | inetUsr                 |
| password       | *****                   |
| エン트리パス         | MACHINE/WEBROOT/APPHOST |

プロパティ:

|                |           |
|----------------|-----------|
| description    |           |
| enabled        | True      |
| name           | DEMO G2   |
| password       | *****     |
| permissionMode | Allow     |
| rules          | (Count=0) |
| userName       | inetUsr   |

操作:

- コレクション
- 追加
- すべてクリア
- 項目のプロパティ
- 項目のロック
- 削除
- ヘルプ
- オンライン ヘルプ

(9) プロパティの「rules」を選択しリストボタンをクリックします。

コレクション エディター - system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/

| 項目:            | 操作:                     |
|----------------|-------------------------|
| permissionMode | Allow                   |
| userName       | inetUsr                 |
| password       | *****                   |
| エン트리パス         | MACHINE/WEBROOT/APPHOST |

プロパティ:

|                |           |
|----------------|-----------|
| description    |           |
| enabled        | True      |
| name           | DEMO G2   |
| password       | *****     |
| permissionMode | Allow     |
| rules          | (Count=0) |
| userName       | inetUsr   |

操作:

- コレクション
- 追加
- すべてクリア
- 項目のプロパティ
- 項目のロック
- 削除
- ヘルプ
- オンライン ヘルプ

(10) 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、認証条件を設定します。

サブジェクトのプロパティを設定します。

- certificateField → “Subject”
- certificateSubField → “O”
- compareCaseSensitive → “True”
- matchCriteria → クライアント証明書のサブジェクトを指定

| 項目:              |                     |                             |                      |        | 操作:      |
|------------------|---------------------|-----------------------------|----------------------|--------|----------|
| certificateField | certificateSubField | matchCriteria               | compareCaseSensitive | エントリパス | コレクション   |
| Subject          | O                   | REIWA CERTIFICATES SERVICES | True                 |        |          |
|                  |                     |                             |                      |        | 追加       |
|                  |                     |                             |                      |        | 項目のプロパティ |
|                  |                     |                             |                      |        | 項目のロック   |
|                  |                     |                             |                      |        | 削除       |
|                  |                     |                             |                      |        | ヘルプ      |
|                  |                     |                             |                      |        | オンラインヘルプ |

| プロパティ:               |                               |
|----------------------|-------------------------------|
| certificateField     | ⇨ Subject                     |
| certificateSubField  | ⇨ O                           |
| compareCaseSensitive | ⇨ True                        |
| matchCriteria        | ⇨ REIWA CERTIFICATES SERVICES |

(11) 再度「追加」をクリックして、発行元（新しい認証局）のプロパティを設定します。

- certificateField → “Issuer”
- certificateSubField → “CN”
- compareCaseSensitive → “True”
- matchCriteria → 発行元証明書のサブジェクトを指定

| 項目:              |                     |                                        |                      |        | 操作:      |
|------------------|---------------------|----------------------------------------|----------------------|--------|----------|
| certificateField | certificateSubField | matchCriteria                          | compareCaseSensitive | エントリパス | コレクション   |
| Subject          | O                   | Nippon RA                              | True                 |        |          |
| Issuer           | CN                  | Nippon RA Certification Authority 3 G2 | True                 |        | 追加       |
|                  |                     |                                        |                      |        | 項目のプロパティ |
|                  |                     |                                        |                      |        | 項目のロック   |
|                  |                     |                                        |                      |        | 削除       |
|                  |                     |                                        |                      |        | ヘルプ      |
|                  |                     |                                        |                      |        | オンラインヘルプ |

| プロパティ:               |                                          |
|----------------------|------------------------------------------|
| certificateField     | ⇨ Issuer                                 |
| certificateSubField  | ⇨ CN                                     |
| compareCaseSensitive | ⇨ True                                   |
| matchCriteria        | ⇨ Nippon RA Certification Authority 3 G2 |

(12) 「rules」のコレクションエディターを閉じ、追加した設定が反映されていることを確認します。

| name    | description | enabled | permissionMode | userName | password | エントリパス                  |
|---------|-------------|---------|----------------|----------|----------|-------------------------|
| DEMO    |             | True    | Allow          | inetUsr  | *****    | MACHINE/WEBROOT/APPHOST |
| DEMO G2 |             | True    | Allow          | inetUsr  | *****    | MACHINE/WEBROOT/APPHOST |

#### 【補足】

既存の認証条件と追加した認証条件の両方を許可するルールとなり、現認証局および新認証局の証明書を認証することが可能となります。

#### ■ 既存の認証条件

- ・クライアント証明書のサブジェクト O の値が「REIWA CERTIFICATES SERVICES」と同じ
- ・発行元の CN の値が「Nippon RA Certification Authority 3」と同じ

| certificateField | certificateSubField | matchCriteria                       | compareCaseSensitive | エントリパス                  |
|------------------|---------------------|-------------------------------------|----------------------|-------------------------|
| Subject          | O                   | REIWA CERTIFICATES SERVICES         | True                 | MACHINE/WEBROOT/APPHOST |
| Issuer           | CN                  | Nippon RA Certification Authority 3 | True                 | MACHINE/WEBROOT/APPHOST |

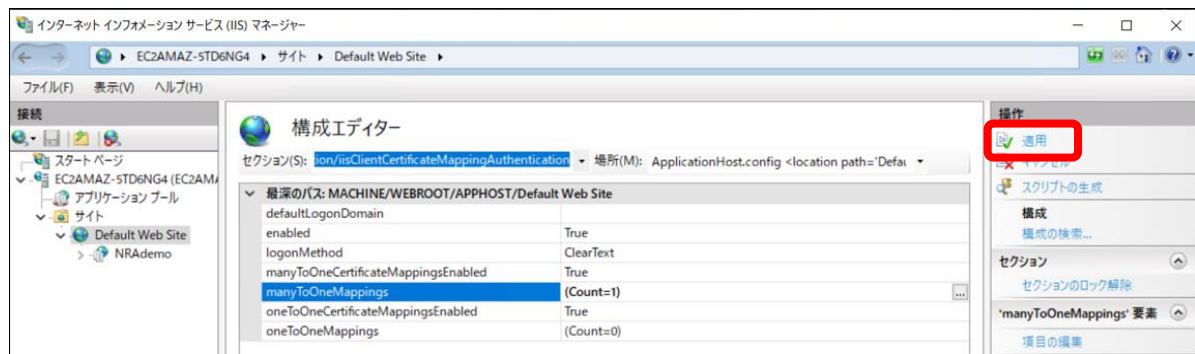
#### ■ 追加した認証条件

- ・クライアント証明書のサブジェクト O の値が「REIWA CERTIFICATES SERVICES」と同じ
- ・発行元の CN の値が「Nippon RA Certification Authority 3 G2」と同じ

| certificateField | certificateSubField | matchCriteria                          | compareCaseSensitive | エントリパス                  |
|------------------|---------------------|----------------------------------------|----------------------|-------------------------|
| Subject          | O                   | REIWA CERTIFICATES SERVICES            | True                 | MACHINE/WEBROOT/APPHOST |
| Issuer           | CN                  | Nippon RA Certification Authority 3 G2 | True                 | MACHINE/WEBROOT/APPHOST |

クライアント証明書情報の確認方法については、後記の [Appendix2](#) をご参照ください。

- (13) 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します。



- (14) IIS を再起動し設定を有効にします。

Web サーバ ホームを選択し、再起動をクリックしてください。



### 3. Appendix1（中間認証局の確認方法）

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。サービス名の後の（CA4）等の表記がご利用いただいている中間認証局です。表記がなければ CA3 をご利用いただいております。

統合認証基盤システム

利用法人テスト  
担当者1 様 ログイン中

サービス情報メンテナンス  
利用法人 詳細設定  
利用者 メンテナンス  
利用者 削除

データ  
ファイル送信

ヘルプ  
チャットで  
お問い合わせ

このサイトの実在証明  
www1.nrapki.co.jp  
cybertrust

利用者メンテナンス

利用法人組織の選択

利用者のメンテナンス

利用法人テスト 加入組織情報

以下のサービスを選択しています。

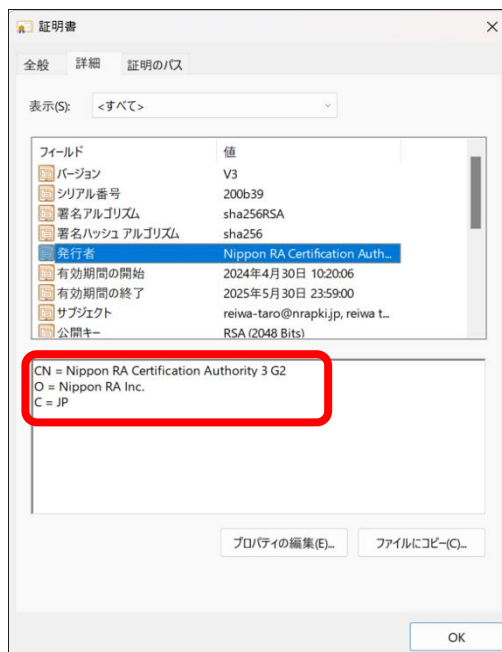
テストサービス (CA4)

| 組織名 | 部門  | 住所        |
|-----|-----|-----------|
| 本社  | 北海道 | test test |

## 4. Appendix2（クライアント証明書情報の確認方法）

「2.2.クライアント証明書認証の設定」について、認証条件に指定しているクライアント証明書の情報は以下のとおりです。

### (1) NRA-PKI の発行局



“発行局”はクライアント証明書の証明機関を示します。

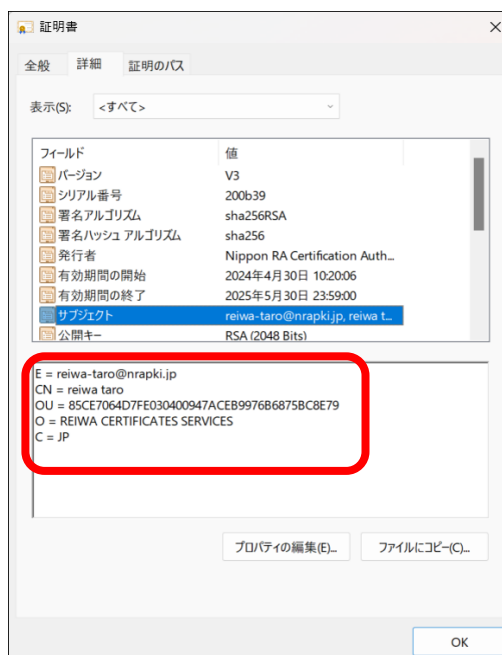
CN=証明機関（発行・認証局）

（ 現認証局：Nippon RA Certification Authority 3  
新認証局：Nippon RA Certification Authority 3 G2 ）

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

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

以上