# 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.	2024/9/6	初版作成	
1.00	2027/ 5/0		

<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 G 2 (Nippon RA Root Certification Authority G2) https://www.nrapki.jp/nrawp/cert/NipponRARootCertificationAuthorityG2.crt
- ■中間認証局 CA 3 G 2 (Nippon RA Certification Authority 3 G2) https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority3G2.crt
- ■中間認証局 CA4 G2(Nippon RA Certification Authority 4 G2) https://www.nrapki.jp/nrawp/cert/NipponRACertificationAuthority4G2.crt
- ■中間認証局 CA 5 G 2 (Nippon RA Certification Authority 5 G 2) 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。

セキュリティが強化された W. Mic セキュリティの構成と分析 Mic クスク スケジューラ Mic ディスクの管理 Mic	crosoft Corpo crosoft Corpo crosoft Corpo			8/III (Dr. 9/III)
セキュリティの構成と分析 Mic タスクスケジューラ Mic ディスクの管理 Mic	crosoft Corpo crosoft Corpo			20130-001
タスクスケジューラ Mic ディスクの管理 Mic	crosoft Corpo_			HIRK(R)
ディスクの管理 Mic				
	crosoft and V			1.4.17.01.0.0
デバイスマネージャー Mic	crosoft Corpo			上へ移動(U)
テレフォニー Mic	crosoft Corpo			下へ移動の
のパフォーマンス モニター Mic	crosoft Corpo		(A)1代码	(*************************************
フォルダー Mic	crosoft Corpo		ALL DUNCY >	
『ポリシーの結果セット Mic	crosoft Corpo			
レーティングとリモート アクセス Mic	crosoft Corpo			
ローカル バックアップ Mic	crosoft Corpo			
ーローカル ユーザーとグループ Mic	crosoft Corpo			
共有フォルダー Mic	crosoft Corpo			
承認マネージャー Mir	crosoft Corpo			
STREET MALE	crosoft Corpo	-		辞細設定(M)_

(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。

証明書スナップイン			×
このスナップインで管理する証明書:			
○ ユーザー アカウント( <u>M</u> )			
<ul> <li>サービス アカウント(5)</li> <li>● コンピューター アカウント(5)</li> </ul>			
	< 戻る(6)	次へ(N) >	キャンセル

- (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。

このスナップインで管理するコンと	コーターを選択してください。		
このスナップインで管理するコン	パコーター: のコンソールを実行しているコン	12-9-)	
<ul> <li>別のコンピューター(A):</li> </ul>			参照(R)
<ul> <li>コマンドラインから起動した これは、コンソールを保存し</li> </ul>	たときは選択されたコンピューター 」た場合にのみ適用されます。	を変更できるようにする(W)	

(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。

くナップイン シャナュリティが強化された W	ペンダー Microsoft Corpo	^	■ コンソール ルート □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	」 拡張の編集(凶)
セキュリティの構成と分析	Microsoft Corpo			削除(B)
タスク スケジューラ	Microsoft Corpo			
ディスクの管理	Microsoft and V			1. + 52 64 / 11
- デバイス マネージャー	Microsoft Corpo			上八登期(世)
テレフォニー	Microsoft Corpo		· · · · · · · · · · · · · · · · · · ·	下へ移動の
シバフォーマンス モニター	Microsoft Corpo	-	追加(A) >	1.1.15 00 (2)
<b>ゴ</b> フォルダー	Microsoft Corpo			
「ポリシーの結果セット	Microsoft Corpo			
シルーティングとリモート アクセス	Microsoft Corpo			
シローカル バックアップ	Microsoft Corpo			
ーローカル ユーザーとグループ	Microsoft Corpo			
共有フォルダー	Microsoft Corpo			
承認マネージャー	Microsoft Corpo			
証明書	Microsoft Corpo	~		詳細設定()

#### (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。

+	証明書のインポート ウィザード		
	証明書のインポート ウィザードの開始		
	このウィザードでは、証明書、証明書信頼リスト、およ ます。	はび証明書失効リストをディスクから証明書ストアにコピーし	
	証明機関によって発行された証明書は、ユーザーID れたネットワーク接続を提供するための情報を含んで の領域です。	)を確認し、デ−タを保護したり、またはセキュリティで保護さ でいます。証明書ストアは、証明書が保管されるシステム上	
	保存場所 ○現在のユーザー(C)		
	<ul> <li>ローカル コンピューター(L)</li> <li>総行するには「次へ」をクリックしてください。</li> </ul>		
		次へ(N) キャンセル	

(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。



(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。

← ಶ 証明書のインポート ウィザード	
証明書のインポート ウィ	ザードの完了
[完了]をクリックすると、証明書	がインポートされます。
次の設定が指定されました:	
ユーザーが選択した証明書スト	7 信頼されたルート証明機関
内容	証明書
ファイル名	$C: {\tt W} users {\tt A} dministrator {\tt Y} Downloads {\tt Y} Nippon {\tt R} A Root {\tt C} ertification {\tt A} users {\tt A} and {\tt A} a$
۲.	, ,
	完了(F) キャンセル

(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。

€.	嵾 証明書のインポート ウィザード
	証明書のインボート ウィザードの開始
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピーします。
	証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護さ れたネットワーク接続を提供するための情報を含んでいます。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。
	保存場所 ○現在のユーザ−(C)
	◎ ローカル コンピューター(L)
	続行するには、[次へ] をクリックしてください。
	次へ(N) キャンセル

(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。



(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。

~	ᡒ 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。

← 🛛 疑明書のインポート ウィザード		
証明書のインポート ウィザ	ードの完了	
[完了]をクリックすると、証明書が	インポートされます。	
次の設定が指定されました。		
ユーザーが選択した証明書ストア	中間証明機関 証明書	
ファイル名	$C: \verb"¥Users" \verb"Administrator" \verb"¥Downloads" \verb"Nippon" \verb RACertification \verb Author" and the set of $	
<	>	
	完了(F) キャンセル	ŀ

(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。

最深のパス: MACHINE/WEBROOT/APPHOST/	Default Web Site
defaultLogonDomain	
enabled	True
logonMethod	Clearlext
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:										
(	descriptio	on									
	enabled					True					
	name					P DEM	0				
F	password					••	•••••				
	permissio	nMode				Allow	Allow				
	ules					(Cou	(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	0	REIWA CERTIFICATES SERVICES	True	MACHINE/WEBROOT/APPHOST			
	Issuer CN Nippon RA Certification Authority 3 True MACHINE/WEBROOT/APPHOST		MACHINE/WEBROOT/APPHOST					
<					2			
プロ	(ティ:							
	ertificateField			₹ Issuer				
	ertificateSubField	đ		* CN				
	ompareCaseSens	itive		* True				
	natchCriteria			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。

יעב	コレクション エディター - system.webServer/security/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/								?	$\times$	
項目	∃:								操作:		
	name	descri	enabled	permissionMode	userName	password	エントリ パス		コレクション		-
	DEMO		True	Allow	inetUsr	*******	MACHINE/WEBROOT/APPHOST		追加		
									すべてクリア		
									項目のプロパティ		-
<								>	項目のロック		
プロ	パティ:								★ 削除		
	description								117		
	enabled					True			オンライン ヘルプ		
	name					PEMO					
	password										
	permissionMode	•				Allow					
	rules (Count=2)										
	userName					inetUsr					

- (8) プロパティを既存の認証設定と同様に設定します。
  - enabled  $\rightarrow$  "True"
  - ・name → 任意で指定
  - ・password → OS ユーザーのパスワードを設定
  - $\cdot \text{ permissionMode } \rightarrow \text{``Allow''}$
  - ・userName → OS ユーザーを設定

コレクション エディター	- system.we	ebServer/secu	urity/authentication/iisClientCertificateMappingAuthentication/manyToOneMappings/			?	×
項目:				操	作:		
permissionMode Allow Allow	userName inetUsr inetUsr	password	エントリ パス MACHINE/WEBROOT/APPHOST	コレ 項	クション 追加 すべてクリア 目 のプロパティ		8
✓ TDIT∓+ description enabled name password permissionMo rules userName	de		True PDEMO G2 Allow (Count=0) inetUsr	<b>×</b> @	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 Allow	userName inetUsr inetUsr	password	エントリ パス MACHINE/WEBROOT/APPHOST	기 項[	クション 追加 すべてクリア 目のプロパティ 項目のロック		
プロパティ:					削除		
description enabled name password permissionMo rules	de		True P DEMO 62 Allow (Count=0)		オンライン ヘルプ		
userName			illetosi				

- (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  $\rightarrow$  "Subject"
  - certificateSubField  $\rightarrow$  "O"
  - compareCaseSensitive  $\rightarrow$  "True"
  - matchCriteria

→ クライアント証明書のサブジェクトを指定

目:					操作:	
certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリパス	コレクション	
Subject	0	REIWA CERTIFICATES SERVICES	True		追加	
					 すべくクリア	
					項目 のプロパティ	=
					 項目のロック X 削除	
certificateField			Subject		ヘルプ オンライン ヘルプ	
certificateSubField	d		° 0			
compareCaseSens	sitive		₹ True			
			REIWA CERTIEI	CATES 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  $\rightarrow$  "Issure"
- certificateSubField  $\rightarrow$  "CN"
- compareCaseSensitive  $\rightarrow$  "True"
- $\cdot$  matchCriteria
- → 発行元証明書のサブジェクトを指定

項目	∃:					掃	作:	
	certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリパス	L	レクション	
	Subject	0	Nipoon RA	True			追加	
	lssuer	CN	Nippon RA Certification Authority 3 G2	True			91(2)	
						項	目 のプロパティ	-
<						×	項目のロック 削除	
プロ	<u>パティ:</u>					0	ヘルプ オンライン ヘルプ	
1	certificateField		9	Issuer			12212 002	
	certificateSubField	d	9	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。

יעכ	クション エディタ	9– - system.w	ebServer/	security/authentica	tion/iisClient	CertificateMa	appingAuthentication/manyToOneMappings/			?	×
項目	:		損	作:							
	name DEMO DEMO G2	description	enabled True True	permissionMode Allow Allow	userName inetUsr inetUsr	password	エントリ パス MACHINE/WEBROOT/APPHOST		レ <b>クション</b> 追加 すべてクリア		
								•	ヘルプ オンライン ヘルプ		

#### 【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

項目	項目:									
	certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリ パス					
	Subject	ect O REIWA CERTIFICATES SERVICES True MACHINE/WEBROO		MACHINE/WEBROOT/APPHOST						
	Issuer CN Nippon RA Certification Authority 3 True		True	MACHINE/WEBROOT/APPHOST						
<						>				
プロ	パティ:									
	certificateField			₹ Issuer						
	certificateSubField	d		* CN						
	compareCaseSen:	sitive		₹ True						
	matchCriteria			Nippon RA Certification Authority 3						

- ■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

項目	1:				
	certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリパス
	Subject	0	REIWA CERTIFICATES SERVICES	True	
	lssuer	CN	Nippon RA Certification Authority 3 G2	True	
<					>
プロ	パティ:				
	certificateField		₹ İssu	er	
	certificateSubFiel	d	* CN		
	compareCaseSen	sitive	* True	2	
	matchCriteria			pon RA Certification Auth	nority 3 G2

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。

💐 インターネット インフォメーション サービス (	(IIS) マネージャー		- 🗆 ×
← → ec2amaz-std6	NG4 ・ サイト ・ Default Web Site ・		😰 🗠 🟠 🔞 •
ファイル(F) 表示(V) ヘルプ(H)			
接続 、 こ 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2	<ul> <li>構成エディター</li> <li>セクション(S): Ion/fisGlientCertificateMappingAuther</li> <li>場際のパス: MACHINE/WEBROOT/APPHOST/D</li> </ul>	titestion • 場所(M): ApplicationHost.config <location manytoonemappings'="" path="Defau •&lt;br&gt;efault Web Site&lt;/th&gt;&lt;th&gt;操作&lt;br&gt;図 適用&lt;br&gt;ズ 1000000&lt;br&gt;ズ 2000万の生成&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;ul&gt;     &lt;li&gt;✓ ・ ● サイト&lt;/li&gt;     &lt;li&gt;✓ ● Default Web Site&lt;/li&gt;     &lt;li&gt;&gt; ● NRAdamo&lt;/li&gt; &lt;/ul&gt;&lt;/td&gt;&lt;td&gt;defaultLogonDomain&lt;br&gt;enabled&lt;/td&gt;&lt;td&gt;True&lt;/td&gt;&lt;td&gt;構成&lt;br&gt;構成の検索&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;And And And&lt;/td&gt;&lt;td&gt;manyToOneCertificateMappingsEnabled&lt;br&gt;manyToOneMappings&lt;/td&gt;&lt;td&gt;True&lt;br&gt;(Count=1)&lt;/td&gt;&lt;td&gt;&lt;br&gt;セクション  セクションのロック解除&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;oneToOneCertificateMappingsEnabled&lt;br&gt;oneToOneMappings&lt;/td&gt;&lt;td&gt;True&lt;br&gt;(Count=0)&lt;/td&gt;&lt;td&gt;" 要素="" 💿<br="">項目の編集</location>	

#### (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。

💐 インターネット インフォメーション サービス (IIS) マネーシ	<b></b> <del>1</del> -					- 0	×
← → • EC2AMAZ-5TD6NG4 +						🔛 🔤 🙆	• •
ファイル(F) 表示(V) ヘルプ(H)							
₩       •    <	EC2AMAZ-5TD6NG	4 ホーム (G) - G) すべて表示(A) ! ! サーバー証明 ディレクトリの 参照 変証 要求フィルター	ルーブ化: 領域 です。 バンドラーマッピ モジュール ング	・ 皿・ ログ記録 ワーカープロセ ス	<ul> <li>操作</li> <li>サーボーの</li> <li>季目</li> <li>デブリケー</li> <li>デブリケー</li> <li>サイトの表</li> <li>新いいい</li> <li>ドの取得</li> <li>ペルブ</li> </ul>	き理 /aン ブールの表示 示 tb Platform コン	示 ポーネン

## 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	E基盤	シフ	、テム
利用法人テスト 担当者1 様 ログイン中	利用者メンテナンス			
♥ サービス情報メンテナンス	利用法人組織の選択	利用者のメン	テナシス	
利用法人 詳細設定				
利用者 メンテナンス	利用法 (二寸), 443 (0)時間(0)			
利用者 剤除	利用法人テスト 加入組織領報			
◎ データ	以下のサービスを選択しています。			
ファイル送信	テストサービス (CA4) 🗸			
◎ ヘルプ				
チャットで	組織名	部門		住所
のこのサイトの実在証明	本社	:	北海道 test test	
wwwl.nrapki.co.jp				

## 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

🗋 証明書		× ** *********************************
全般詳細証明のバス		元前省はノノーノノー証明督の証明候則で示しより
表示(S): <すべて>	×	CN=証明機関(発行・認証局)
フィールド	值	/ 現認証局: Nippon RA Certification Authority 3
<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	200b39 sha256RSA	く 新認証局: Nippon RA Certification Authority 3 G2
習名ハッシュ アルゴリズム 発行者	sha256 Nippon RA Certification Auth	O=発行局を管理する日本 RA の英字表記
■ 有効期間の開始 ■ 有効期間の終了 ■ サブジェクト	2024年4月30日 10:20:06 2025年5月30日 23:59:00 reiwa-taro@nrapki.jp. reiwa t	C=国
□□ 公開+-	RSA (2048 Bits)	
CN = Nippon RA Certificatio O = Nippon RA Inc. C = JP	n Authority 3 G2 プロ/(ティの編集(E) ファイルにコピー(C	

(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