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

<目)	次>
------	----

1. 本書の目的	3
2. 注意点	4
3. 設定手順	5
3.1. 手順の流れ	5
3.2. IIS クライアント証明書マッピング認証の役割追加	6
3.3. IIS へのアクセス許可ユーザーの作成(OS の設定)	8
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	9
3.5. サーバ証明書のインポート	15
3.6. サイトのバインド編集	16
3.7. 認証の設定	
3.8. IIS 多対 1 マッピング規則(ルール)の設定	
3.9. SSL 設定	24
3.10. クライアント証明書の情報参照(クライアント側)	27

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

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。

	役割と機能の追加ウィザード	_ _ ×
開始する前に		対象サーバー WIN-NBS5D19I6HG
開始する前に インストールの種類	このウィザードを使用すると、役割、役割サービス、または機能をインストールできます。ドキュメ のホストなどの組織のコンビューディングニーズに応じて、インストールする役割、役割サービス、 す。	ントの共有や Web サイト または機能を決定しま
サーバーの選択 サーバーの役割	役割、役割サービス、または機能を削除するには、次の手順を実行します: 役割と機能の削除ウィザードの起動	
個配 確認 結果	株(す96期)に、次辺ダスカッナ」ひていることを確認していことい。 管理者アカシントに違力なパスワードが設定されている 静的 IP アドレスなどのネットワークの設定が構成されている Windows Update から最新のケキュリティを更新プログラムがインストールされている	
	前提条件が完了していることを確認する必要がある場合は、ウイザードを閉じて、それらの作業 ドを再度実行してください。	きを完了してから、ウイザー
	統行するには、[次へ] をクリックしてください。	
	□ 既定でこのページを表示しない(<u>S</u>)	
	<前へ(P) 次へ(N) > インスト	-ル(I) キャンセル
B	役割と機能の追加ウィザード	_ 🗆 X
インストールの種類	の選択	対象サーバー WIN-NBSSD1916HG
インストールの種類 ^{開始する前に} インストールの種類	の選択 インストールの環境を選択します。役割および機能は、実行中の物理コンピューター、仮想コン ンの仮想ハードディスク (VHD) にインストールできます。	対象サーバー WIN-NBSSD1916HG ピューター、またはオフライ
インストールの種類 開始する前に インストールの種類 サーバーの選択	の選択 インストールの種類を選択します。役割および機能は、実行中の相理コンピューター、仮想コン ンの反則ハード ディスク (いわり) にインストールできます。 ・ (名割バース主体理論が一スククレスクストール 役割、役割サービス、および機能を追加して、1 台のサーバーを構成します。	対象サーバー WIN-NBSSD1916HG ピューター、またはオフライ
インストールの種類 開始する前に インストールの種類 サーバーの登録 サーバーの必想 福盛	 ①遅択 クストールの種類を選択します。役割および機能は、案行中の物理コンピューター、仮想コンの便見ハード ディスク (VFD) にインストールできす。 役割ハート ディスク (VFD) にインストール 使用、使割・ビス、みよび機能を追加して、1 台のサーバーを構成します。 リモート デスクトップ リーとごのインストール の差 プルリアイ ノンフラストラクティ (VFD) に必要な役割サービスをインストールして、(の ション バースのアスクトップ環境を採取します。 	対象サーバー WIN-NBSSD1916HG ゼューター、またはオフライ 見マシン ベースまたはセッ
インストールの種類 酸始する前に ウンストーの資料 サーバーの運射 サーバーの運射 構成 結束	 の遅択 ウストールの運転を選択します、役割たび(機能は、実行中の物理コンピューター、仮想コンの仮想)(ドディスク(VHD)にインストールできます。 (役割ペースまたは機能ペースのインストール 役割、役割サービス、おどび解除を追加して、1 台のサーバーを構成します。 (リモートデスクトワグサービスのインストール の逃デスクトリブインラストラクチャーム の逃デスクトリブインラストラクチャー(VD1)に必要な役割サービスをインストールして、仮 ション バースのデスクトップ環境を存成します。 	対象サーバー WTN-NESSD1990HG ピューター、またはオプライ ピューター、またはオプライ
	 (の)遅択 ヘントールの理想を選択します、役割たよび機能は、変行中の物理コンピューター、仮想コンクの限測しドライスグ (VHD) にインストールできます。 (税利ヘースまたは構築/ヘスのインストール 役割、役割サービス、および機能を追加して、1 かのサーバーを構成します。 (リモートテスクトップ サービスのインストール (必須テスクト)マブ サービスのインストール (必須テスクト)マブ インフストランド・VOI) に必要な役割サービスをインストールして、(税) ション ベースのデスクトップ獲得を作成します。 	1巻サーデー WIN-HBS3D19964G ゼューター、またはオプライ セスーター、またはオプライ
インストールの種類 開始する前に インストーの種類 サードーの選択 サイドの意思 確認 結果	 の遅択 ウストールの獲得を選択します、役割および機能は、実行中の物理コンピューター、仮想コンシの仮想レードディスク (VHD) にインストールできます。 役割ペースよたは機能ペースのインストール 役割、役割サービス、および機能を増加して、1 払のサーバーを構成します。 リモートテスクレッザ リービスのインストール 役割テスクトップ リービスのインストール 位置テスクトップ パージスクレストー 位置テスクトップ パージスクトックストーム 	対象サーバー WIN+NES5D19904G ピューター、またはオフライ
ロンストールの種類 開始する前に センストールの授助 ウーバーの運用 ウーバーの受動 構築 構築	 の遅択 ウストールの種類を選択します、役割たび機能は、案行中の物理コンピューター、仮想コンロの度想ルドライスク (VHO)にインストールできます。 (役割ヘスまたは編整ヘスのインストール 役割、役割サービス、および機能を追加して、1 缶のサーバーを構成します。 リモートネスクトップサービスのインストール 使用アスクトップ サービスのインストール 使用アスクトップ インコスストラケル (VOI)に必要な役割サービスをインストールして、役1 ション ベースのデスクトップ展開を作成します。 	が良サーバー。 WIN-HBSSD1916HG ゼユーター、またはオプライ 道マシン ベースまたはセッ
インストールの種類 酸始する前に サイトーの選択 ラーバーの選択 ラーバーの取用 発展 結果	 小ストールの環境を選択します、役割たび(機能は、案行中の物理コンピューター、仮想コンンの仮想しいドライスク (VHD)にインストールできます。 (初州へスまたは機能ペースのインストール 役割、役割サービス、および機能を追加して、1 台のサーバーを構成します。 (リモートラスクトック・レロ)に必要な役割サービスをインストールして、優勝ラスクトマインフラストラット(VD)に)に必要な役割サービスをインストールして、優かコント・スのテスクトップ環境を作成します。 	1巻9-7~- WIN-NBS3D19494G ゼユーター、またはオフライ 渡マシン ペースまたはセッ

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。

a	役割と機能の追加ウィザード
対象サーバーの選	択 ^{刘康世-//-} WIN-NBSSD1916HG
開始する前に インストールの理想 サーバーの理想 サーバーの役割 機能 確認 転集	 役割と機能をインストールするサーバーまたは仮想ハードディスクを選択します。 ●「サーバー ブールからサーバーを選択 ○ 仮想ハードディスクから選択 サーバー ブール フィルクー: 名前 IP アドレス オペレーディング システム WIN-NBSSD1916HG 172.30.0.116 Microsoft Windows Server 2012 R2 Standard はのコンピューターが見つかりました このページには、Windows Server 2012 を実行しており、サーバーマネージャーの【サーバーの追加】コマンドを使用して追加されたサーバーが表示されます。オフライン サーバート データの違か完了していない、新たに追加されたサーバーは表示されません。
	<前へ(E) 次へ(N) > インストール(I) キャンセル

 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。

	役割と機能の追加ウィザード
ナーバーの役割の	
開始する前に	進択したサーハーに1ノスドール9 G1支制化 1 フ以上1進択します。
インストールの種類	役割
サーバーの選択	
サーバーの役割	■ Web Server (IIS) (16/43 個をインストール済み)
機能	▲ ■ Web Server (15/34 個をインストール済み)
14:22	 Common HTTP Features (4/6 個をインストール済み)
7年80	 Health and Diagnostics (1/6 個をインストール済み)
結果	 Performance (1/2 個をインストール済み)
	▲ Security (インストール済み)
	✓ Request Filtering (インストール済み)
	✓ Basic Authentication (インストール済み)
	✓ Centralized SSL Certificate Support (インストール済み)
	✓ Client Certificate Mapping Authentication (インストール済み) =
	✓ Digest Authentication (インストール済み)
	✓ IIS Client Certificate Mapping Authentication (インストール済
	✓ IP and Domain Restrictions (インストール済み)

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

→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。

・"パスワードを無期限にする(W)"

- ・"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。

NRA	統合認識	正基盤	システム		
令和証明書サービス 令和 三郎 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	利用者のメンテナン	x		
利用法人 詳細設定		/			
利用者 メンテナンス		±P			
利用者 削除	〒和証明書サービス 加入組織情	ŦŊ			
⊙ ヘルプ	以下のサービスを選択しています	r.			
NRA-PKIシステム サボートサイト	「テストサービス(CA4) 🗸]			
🕑 このサイトの実在証明					
	組織名	部門	住所	電話番号	
	本社	東京都 千代日 △ △ 日	3 I区 〇〇町1-2-3 パル 2階	123-4567-890	

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。

	スナップインの追加と削除					
コンビューターで利用できるスナップインからこのコンソールに使用するスナップインを違択したり、違択したスナップインを構成したりできます。拡張可能なスナップインで は、どの拡張を有効にするかを構成できます。						
利用できるスナップイン(S): 選択されたスナップイン(E):						
スナップイン	ベンダー	^	■ コンソール ルート	拡張の編集(≚)		
🚡 セキュリティの構成と分析	Microsoft Cor					
④タスク スケジューラ	Microsoft Cor			<u>削除(R)</u>		
ディスクの管理	Microsoft and					
二番 デバイス マネージャー	Microsoft Cor			上へ移動(U)		
	Microsoft Cor					
	Microsoft Cor		2242(4)	下へ移動(<u>D</u>)		
■ ノオルター	Microsoft Cor		1 <u>E</u> /JU(<u>A</u>) >			
画 ルーティンガとリモート マカ	Microsoft Cor					
▲□ーカル バックアップ	Microsoft Cor					
● ローカル ユーザーとグループ	Microsoft Cor	≡				
2 共有フォルダー	Microsoft Cor					
承認マネージャー	Microsoft Cor					
<mark>■</mark> 証明書	Microsoft Cor	$\overline{\mathbf{v}}$		詳細設定(⊻)		
		-				
説明:						
証明書スナップインを使うとユーザー、サービス、またはコンピューターの証明書ストアの内容を閲覧できます。						
OK +P221						

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。

i.	[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>) ○ サービス アカウント(<u>S</u>) ④ <u>コンピューター アカウント(C)</u>			
	< 戻る(B)	次へ(<u>N</u>) > キャン	ten l

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。

コンピューターの選択	x
このスナップインで管理するコンピュ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ピューター: ① ローカル コンピューター(L): (このコンソールを実行しているコンピューター))	
○別のコンピューター(A): 参照(R)	
□コイントラインから起動したときは連択されたコンピューターを変更 Cさるように9る(W) これは、コンソールを保存した場合にのみ適用されます。	
	_
< 戻る(<u>B</u>) 完了 キャンセノ	Ł

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

					<i></i>	
スナップイン	ベンター	^				拡張の編集(≚)
ha セキュリティの構成と分析	Microsoft Cor			☞ 証明書 (□−カ)	ルコンビューター)	¥(64/p)
シタスク スケジューラ	Microsoft Cor					則味(区)
■ ディスクの管理	Microsoft and					
当テバイス マネージャー	Microsoft Cor					上へ移動(U)
愛 テレフォニー	Microsoft Cor					
◎パフォーマンス モニター	Microsoft Cor		·····			下へ移動(<u>D</u>)
コフォルダー	Microsoft Cor		追加(<u>A</u>) >			
」ホリシーの結果セット	Microsoft Cor					
豊 ルーティングとリモート アク	Microsoft Cor					
💁 ローカル バックアップ	Microsoft Cor	_				
🐓 ローカル ユーザーとグループ	Microsoft Cor	=				
え 共有フォルダー	Microsoft Cor					
13 承認マネージャー	Microsoft Cor					
副 証明書	Microsoft Cor	\sim				詳細設定(⊻)
20 承認マネージャー ■ 証明書 む明: 証明書スナップインを使うとユーサ	Microsoft Cor Microsoft Cor fー、サービス、またはコ	~ ンピュ	ーターの証明書ストア	の内容を閲覧できます	•	詳細設定(⊻)

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
	ב] - 1/1–עלב
 □ ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィンドウ(W) ヘルプ(H) ◆ ● □ □ □ □ □ 	 □ ファイル(F) 操作(A) 表示(V) お気に入り(O) ウインドウ(W) ヘルプ(H) ◆ ● 2 (元) 自 Q (→ 12 (□))

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。

💿 😼 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	ц П
このウィザードでは、証明書、証明書信頼リスト、お します。	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
証明機関によって発行された証明書は、ユーザー 護されたネットワーク接続を提供するための情報を2 テム上の領域です。	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 含んでいます。証明書ストアは、証明書が保管されるシス
保存場所 ○現在のユーザー(C) 回 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

 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。

● 😴 証明書のインポート ウィザード	×
インボートする証明書ファイル インボートするスライルを指定してください。	
ファイル名(E): C:WilippoRARootCertificationAuthority.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)	
広へ(N) キャンセ	216

- 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
★ 受 証明書のインボート ウィザード	★ 🚱 証明書のインポート ウィザード
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。	延明書ストアは、証明書が保管されるシステム上の様域です。 Windows に証明書ストアを目動的に進択させるか、証明書の場所を指定することができます。 ① 江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(L) ② 証明書をすべて広のストアに配置する(P) 証明書え下?: 【価額されたルート証明機能 参照(<u>R</u>)
次へ(N) キャンセル	次へ(N) キャンセル

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。

			×
🕙 🐓 証明	書のインボート ウィザード	•	
証明	目書のインボート ウィサ	「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	g定が指定されました:		
ユ 内望 ファ・	ザーが選択した証明書ストア 撃 イル名	信頼されたルート証明機関 証明書 C:¥NipponRARootCertificationAuthority.crt	
		完了(E)	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。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 C	A3)			
	/ール1 - [コンソール ルート¥証明書 (ローカ ウインドウ(火) ヘルプ(出) 発行先 ■ Microsoft Windows Hardware Commu- ■ Nippon RA Certification Authority 3 Carvippon RA Certification Authority 4 ■ Root Agency ■ www.verisign.com/CPS Incorp.by R	JULコンピューター)¥中間証明機間¥証明書] 発行者 Microsoft Root Authority Nippon RA Root Certification Authority Nippon RA Root Certification Authority Root Agency Class 3 Public Primary Certification Authority	有効期限 2002/12/31 2031/08/15 2031/08/15 2040/01/01 2016/10/25	
▶ 〇〇 スマートカードの信頼されたルート ▶ 〇〇 信頼されたデバイス ▶ 〇〇 Web ホスティング	K III		>	

コンソール1 - [コンソールルート¥証明書(ローカルコンピュータ-)¥信頼されたルート証明機関¥証明書] - □ × アイル(E) 操作(A) 表示(Y) お気に入り(Q) クィンドウ(W) ヘルプ(H) - □ × アイル(E) 操作(A) 表示(Y) お気に入り(Q) クィンドウ(W) ヘルプ(H) - □ × アイル(E) 操作(A) 表示(Y) お気に入り(Q) クィンドウ(W) ヘルプ(H) - □ × ● ① ① ○ ● ● ● ○ ● ○ 個人 ● ○ ● ○ 回人 ● ○ ● ○ 回人 ● ○ ● ○ 回人 ● ○ ● ○ ● ○ ● ○ 回人 ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ ● ○ <	ルート証明機関				
コンソールルート 発行者 有効期限 ● 正明書(D-カルコンピューター) ● 日本 第日前の C 欠berTrust Root 2025/05/13 ● 回人 □ 証明書 □ □カルコンピューター) ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	コンソール1 語 ファイル(E) 操作(A) 表示(V) お気に入り(Q) 中 中 名 市 自 保護	- [コンソール ルート¥証明書 (ローカル コン ウィンドウ(逊) ヘルプ(出)	ビューター)¥信頼されたルート証明機関¥証明	書]	_ _ ×
▲ Withing (D-7)ル コンビューター) ●	שראר בי אראר אין אראר בי 🗎	発行先	発行者	有効期限	操作
	 ▲ (1) 証明書(1-7)ハコンピューター) ▲ ④ (星橋されたルート証明機関 ● 証明書 ● 証明書 ● 正明書大羽以入 ● 証明書大羽以入 ● (1) 正明書 ● (1) 二 (1) 1	Glastimore CyberTrust Root Glass 3 Public Primary Certification GCopyright (c) 1997 Microsoft Corp. DigiCert Global Root CA Microsoft Root Certificate Authority Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certific	Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Copyright (c) 1997 Microsoft Corp. DiglCert Global Root CA Microsoft Root Authority Microsoft Root Authority Microsoft Root Certificate Authority 2010 Microsoft Root Certificate Authority 2011 Microsoft Root Certificate Authority 2011 Mippon RA Root Certificate Authority 2011 ND LIABILITY ACCEPTED, (c)97 VeriSign, 1 Thawte Timestamping CA VeriSign Class 3 Public Primary Certificatio	2025/05/13 2028/08/02 1999/12/31 2031/11/10 2020/12/31 2020/12/31 20221/05/10 2035/08/23 2036/03/23 2036/03/23 2036/03/23 2036/03/17 2036/07/17	証明書 ▲ 他の操作 ▶

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。

6		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	-
€ WIN-NBS5D19I	6HG 🕨		
ファイル(<u>E</u>) 表示(⊻) ヘルプ(<u>H</u>)			
接続 . ↓ □ ② 分	WIN-NBS50	D19I6HG ホーム	
	フィルター:	▼ 蒙 検索(G) - 場 すべて表示(A) グループ化: 領域	
<u></u>		<u>ک</u> کے ا	J
	HTTP 応合へ IP アトレスおよ I ッダー びドメインの	MIME の種類 エラー ベージ サーバー証明 オイレクドリの参 バントラー 書 照 ピング	Y Y
	i 🕺 🗐	🗋 🖗 🐴 🔏 😂	

③ "インポート"をクリック。

サーバー証明書 SSL に対して構成された Web サイト は、この機能を使用します。	∙で Web サーバーが使用できる証明書	を要求および管理するに	操	作 インポート 証明書の要求の作成 証明書の要求の完了
フィルター:	🍞 検索(<u>G</u>) 🕞 🗔 すべて表示(<u>A</u>)	グループ化: -		ドメイン証明書の作成
名前 📩	発行先	発行元		自己署名入り証明書の作成
				更新された証明書の自動的な再バイ ンドを有効にする
			0	ヘルプ

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」

証明書のインポート	? ×
証明書ファイル (.pfx)(C):	
パスワード(P):	
証明書ストアの選択(S):	
個人	~
☑ この証明書のエクスポートを許可する(A)	
ОК	キャンセル

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。

	サイト バインド	? X
種類 水スト名 http	ポート IP アドレス バインド情報 80 *	追加(<u>A</u>) 編集(<u>E</u>) 削除(<u>R</u>) 参照(<u>B</u>)

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。

	サイト バインドのì	D追加 ? ×
種類(<u>T</u>): https v ホスト名(<u>H</u>):	IP アドレス(I): 未使用の IP アドレスすべて	א [*] −ト(<u>Q</u>): ע 443
□ サーバー名表示を要う	求する(<u>N</u>)	
SSL 証明書(F):		
DEMO	1	▶ 選択(上) 表示(⊻)
		OK キャンセル

④ https が追加されたことを確認し"閉じる"をクリック。

	サイト バインド	? X
種類 木スト名 http https	ポート IP アドレス パインド情報 80 * 443 *	这些加(<u>A</u>) 編集(<u>E</u>) 削除(<u>R</u>) 参照(<u>B</u>)
		閉じる(<u>C</u>)

【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。

サイト バインドの追加	?	×
種類(T): IP アドレス(I): ポート(O): https ~ 未使用の IP アドレスすべて ~ 443		
ホスト名(H):		
□ サーバー名表示を要求する(N)		
✓ TLS 1.3 over TCP を無効にする(B) QUIC を無効にします(A)		
 レガシ TLS を無効にする(G) HTTP/2 を無効にします(D) 		
□ OCSP ステープリングを無効にします(S)		
SSL 証明書(F):		
未選択 ~ 選択(L)		
ОК	キャンセル	¢

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。

🎒 =ग्र=ग			操作
S ar ar an			無効にする
グループ化: グループ化なし	-		編集
名前	状態	応答の種類	● ヘルプ
ASP.NET 偽装	無効		
匿名認証	有効		

 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。

・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	· _ 🗖 🗙
● ・ WIN-NBS5D19I6HG ・ サイト ・ Default Web Site ・	📴 🖾 🙆 🕡 🗸
ファイル(E) 表示(Y) ヘルプ(出)	
## 	操作 アクセス許可の編集 アクセス許可の編集 サイトの編集 パインド 基本設定 アプリケーションの表示 仮想ディレクトリの表示 Web サイトの管理 ● 開始 ● 得止 ● 得止 ● 修用は ● 第243 (https) 参照 ● **442 (https) 参照
< III 検能ビュー 🔐 コンテンツ ビュー	詳細設定 >
準備完了	€ <u>1</u> .:

② セクションのリストから" iisClientCertificateMappingAuthentication"を選択。

system.webServer/security/authentication/iisClientCertificateMappingAuthentication を選択

🥘 構	成エディター	
セクション(S):	system.webServer/security/authentication/iisClientCertificateMappingAp	•
▶ 最深のパ	system.net system.ransactions system.transactions system.web system.webServer system.webServer authentication authentication diagesAuthentication digestAuthentication digestAut	

③ "enabled" のプルダウンメニューから"True"を選択。

	構成エディター	
セク	ション(<u>ら</u>): system.webServer/security/ - 共	易所(<u>M</u>): ApplicationHost.config <loca th="" ▼<=""></loca>
⊿	最深のパス: MACHINE/WEBROOT/APPH	OST
	defaultLogonDomain	
	enabled	True 🗸
	logonMethod	True
	manyToOneCertificateMappingsEnabled	False
	manyToOneMappings	(Count=0)
	oneToOneCertificateMappingsEnabled	True
	oneToOneMappings	(Count=0)

④ 多対 1 マッピング規則 (ルール)を設定。

構成エディター セクション(S): system.webServer/security/auth - 場所(M): ApplicationHost.config <location -△ 最深のパス: MACHINE/WEBROOT/APPHOST defaultLogonDomain enabled True logonMethod ClearText manyToOneCertificateMappingsEnabled True ... (Count=0) oneToOneCertificateMappingsEnabled True oneToOneMappings (Count=0)

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。

עב	クション:	エディター - s	ystem.v	vebServer/secu	urity/authe	entication	/iisClientCertificateMap	pingAuthenticat	ion/manyTo 🍳
項	≣:								操作:
	name	description	enabled	permissionMode	userName	password	エントリ パス		コレクション
									追加
-									すべてクリア
_									🔞 ヘルプ
<				Ш				>	オンライン ヘルプ
プロ	パティ:								

20

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	\rightarrow "Allow"

→ 手順 3.3 で作成した OS ユーザーを設定

コレ!	クション エディ	୨– - systei	m.webSe	erver/security/a	uthenticat	ion/iisClient@	CertificateMa	ppingAuth	nentication/ma	y X
項目	∃:								操作:	
	name	description	enabled	permissionMode	userName	password	エントリ パス		コレクション	
	Demo		True	Allow	inetUsr	******			追加	
									すべてクリア	
<				Ш				>	項目 のプロパティ	=
プロ	パティ:								項目のロック	
	description								★ 削除	
	enabled			Tru	e					
	name			🕴 Dei	mo				オンライン ヘルプ	
	password			• •						
	permissionM	ode		Allo	w					
	rules			(Co	ount=0)					
	userName			ine	tUsr					

⑦ プロパティの"rules"を選択しリストボタンをクリック。

コレクショ	ョン エディター - syst	em.webSe	erver/security/a	uthenticat	tion/iisClient	CertificateMap	pingAuth	entication/ma ?	X
項目:								操作:	
na De < 7 □/(7-	me descriptio mo	n enabled True	permissionMode Allow III	userName inetUsr	password *******	エントリパス	>	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	-
desc enat nam pass perr rule user	rription bled sword nissionMode s Name		Tru P De Alla (Co ine	ne mo ow ount=0) etUsr	•••			 ※ 削除 ④ ヘルプ オンライン ヘルプ 	

- 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

→ クライアント証明書のサブ	ジェクトを指定
----------------	---------

コレクション エディター -	system.webServe	er/security/au	thentication/iisClier	ntCertificateMappingAut	hentic:	ation/man ?	X
項目:						操作:	
certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリパス		コレクション	
Subject	0	NRADemo	True			2000	
						セルロマ	
						9/(0/)/	
<		ш			>	項目 のプロパティ	Ξ
プロパティ:						項目のロック	
certificateEield		Subject				🗙 削除	
certificateSubField	certificateSubField						
compareCaseSensi	オンライン ヘルプ						
matchCriteria							

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

コレ!	クション エディター	- system.webSei	ver/security/auth	nentication/iisClientCe	ertificateMappingAuthenti	cation/man ?	X	
項目	∃:					操作:		
	certificateField	certificateSubField	matchCriteria	compareCaseSensitive	エントリ パス	コレカション	=	
	Subject	0	NRADemo	True		20 to		
	Issuer	0	Nippon RA Inc.	True		追加		
						9~(7))/		
<			Ш		>	項目 のプロパティ	Ξ	
プロ	ブロバティ:							
	certificateField		* Issuer			🗙 削除		
	certificateSubFiel	d	P 0			🔞 ヘルプ		
	compareCaseSensitive If True				オンライン ヘルプ			
	matchCriteria		Nippon RA In	Nippon RA Inc.				

※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

6	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	_ D X					
WIN-NBS5D19I6H	IG ・サイト ・ Default Web Site ・		🖸 🖄 🔞 •					
ファイル(E) 表示(⊻) ヘルプ(<u>H</u>)								
接続			操作					
🔍 - 🖬 🖄 😥	● 構成上ナイター		■ 適用					
セクション(S): ateMappingAuthentication - 場所(M): ApplicationHost.config < k ・								
▲ WIN-NBS5D1916HG (WIN-	A · WIN-NBS5D1916HG (WIN- の アカルケーション ブール A 最深のパス: MACHINE/WEBROOT/APPHOST/Default Web Site							
⊿ <u>1</u> サイト	▲ ¹ ● サイト defaultLogonDomain 構成							
🔺 🌏 Default Web Site	a 🕘 Default Web Site enabled True 構成の検索							
NraPkiDemo	logonMethod	ClearText	ヤカション 🔗					
⊿ 😝 test	manyToOneCertificateMappingsEna	True						
⊳ 🔐 app	manyToOneMappings	(Count=1)	'oneToOneMappings'要					
	oneToOneCertificateMappingsEnab True							
	oneToOneMappings (Count=0)							
			❷ ∧レプ					

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。

 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。

● SSL 設定
このページでは、Web サイトまたはアプリケーションの SSL 設定を変更することができます。
✓ SSL が必要(Q)
クライアント証明書:
○ 無視(I)
○ 受理(<u>A</u>)
● 必要(<u>R</u>)

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	e : Disabled				
Reject Connections	: Disabled				
Disable HITP2	: Not Set				
Disable QUIC	: Not Set				
Disable TLS1.2	: Not Set				
Disable ILS1.3	: Set				
Disable OCSP Stapling	: Not Set				
Enable loken Binding	: Not Set				
Log Extended Events	: Not Set				
Disable Legacy ILS Versions	: Not Set				
Enable Session licket	: Not Set				
Extended Properties:					
Property1a					
Receive window	: 1048576				
Extended Properties:	. 1				
May Sattings Dan Ename	: 1				
Max Settings Per Frame	. 2/90202				
Fixtondod Deponentions	: 4294907295				
PropertyId	• 2				
Extended Properties:	. 2				
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。

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。

	コンソール1	- [コンソール	ルート]					_	
-	ファイル(F)	操作(A)	表示(V)	お気に入り(O)	ウィンドウ(W) ヘルプ(ト	H)		- 8 ×
	ファイル(F) 新規(開く(C 上書を 名前花 スナッ: オブシ オブシ 1 C:¥I 2 dev 3 serv 終了(操作(A) 作成(N) D) を付けて保存 プインの追加 ヨン(P) J.Sers¥Kom mgmt rices X)	表示(V) F(A) と削除(M). ine¥Deskto	お気に入り(O) 	ウインドウ(Ctrl+N Ctrl+O Ctrl+S Ctrl+M	W) ヘルプ(F 頁目はありませ	ł) Ż∕u∘	<mark>操作 コンソール ルート</mark> 他の操作	_ 6 ×
スナ	スナップインを追加したり、スナップインコンソールからスナップインを削除し								

③ 左画面の下方にある証明書を選択、"追加"をクリック。

+	N'NE	•		甘酒の毎年(2)
	N			143200/0萬天(〇)…
セキュリティ テノノレート	Microsoft Corp			削除(R)
セキュリティが短化された…	Microsoft Corp			
セキュンノコの構成と方が	Microsoft Corp			
ラブスノスノジューノ	Microsoft and V			上八階劃(山)
リーバイス マネージャー	Microsoft Corp			下八移動(D)
1パフォーマンス モニター	Microsoft Corp		A) >	1 1 1 1 1 1 1 1 1 1
フォルダー	Microsoft Corp			
「ポリシーの結果セット	Microsoft Corp			
- ローカル ユーザーとグループ	Microsoft Corp			
印刷の管理	Microsoft Corp			
共有フォルダー	Microsoft Corp			
承認マネージャー	Microsoft Corp			
1 証明書	Microsoft Corp	~		詳細設定(⊻)
明:				

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。

証明書スナップイン		×
このスナップインで管理する証明 言 :		
	< 戻る(3) 売了 キャンセ	211

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

ンピューターで利用できるスナッフ の拡張を有効にするかを構成	プインからこのコンソールは できます。	使用	するスナップインを選択したり、選択したスナップインを構成したりで	きます。拡張可能なスナップイン
用できるスナップイン(<u>S</u>):			選択されたスナップイン(E):	
スナップイン	ベンダー	^	א-ע ערב 📖	拡張の編集(<u>X</u>)
🔓 セキュリティ テンプレート	Microsoft Corp		🗊 証明書 - 現在のユーザー	Vici 7.4
🔐 セキュリティが強化された	Microsoft Corp			<u>削除(R</u>)
ねセキュリティの構成と分析	Microsoft Corp			
🥑 タスク スケジューラ	Microsoft Corp			上へ移動(U)
〒 ディスクの管理	Microsoft and V			
豊 デバイス マネージャー	Microsoft Corp		2	下へ移動(<u>D</u>)
🖻 パフォーマンス モニター	Microsoft Corp		追加(<u>A)</u> >	
🗎 フォルダー	Microsoft Corp			
∬ ポリシーの結果セット	Microsoft Corp			
晃 ローカル ユーザーとグループ	Microsoft Corp			
副印刷の管理	Microsoft Corp			
刻 共有フォルダー	Microsoft Corp			
🏹 承認マネージャー	Microsoft Corp			
副 証明書	Microsoft Corp	~		詳細設定(⊻)
88.				
99:				
明書スナップインを使うとユー	ザー、サービス、またはコン	パニ-	-ターの証明書ストアの内容を閲覧できます。	

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。

🚟 コンソール1 - [コンソール ルート¥証明書 - 現在の]	ユーザー¥個人¥証明書]			—	
🚟 ファイル(E) 操作(A) 表示(V) お気に入り(<u>0) ウィンドウ(W) ヘルプ(H)</u>				_ 8 ×
🗢 🤿 🙍 📰 📋 🗟 📑					
🧰 コンソール ルート		発行者	有効期限	操作	
√ □ 証明書 - 現在のユーザー ○ □ □ □ ↓	🕼 test test	Nippon RA Certification Authority 4	2017/02/15	証明書	
▼ ■ 四八 ■ 証明書				他の操作	ľ₽ ►
> 🧮 信頼されたルート証明機関					
> 📔 エンタープライズの信頼					
> 🚞 中間証明機関					
> 📔 Active Directory ユーザー オブジェクト					
> 🧮 信頼された発行元					
> 🧮 信頼されていない証明書					
> 📔 サードパーティルート証明機関					
> 🧾 信頼されたユーザー					
> 📔 クライアント認証発行者					
> 🧰 ほかの人					
> MSIEHistoryJournal					
> 📔 スマートカードの信頼されたルート					
	<		>		
個人 ストアには 1 個の証明書があります。	•				

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	
■ 証明書 ×	
全般 詳細 証明のパス	
表示(5): <すべて> ~	
フィールド 値 ^	
 (三) パージョン V3 (三) シリアル番号 Of 97 09 	
 	
Image: State Stat	
□ 有効期間の終了 2016年2月24日 23:59:00 □ サブジェクト test@test.co.jp, test test, 7F34600A9CF ↓	*発行者"はクライアント証明書の証明機関を示します。
CN = Nippon RA Certification Authority 4	CN=証明機関(発行・認証局)
O = Nippon RA Inc. C = JP	WAIDA Tot Ninnen DA Contification Authority 2 th/t
	※NRA Cは、Nippon RA Certification Authority 3 または
	Nippon RA Certification Authority 4 が表示されます。
プロパティの編集(丘) ファイルにコピー(丘)	O=発行局を管理する日本 RA の英字表記
	C=国
OK	

(2) サブジェクト



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 ×	
全般 詳細 証明のパス 証明のパス	
R 1907 AL CN=Nippon RA Boot Certification Authority, Q=Nippon RA Inc.C=JP CN=Nippon RA Certification Authority 4 Q=Nippon RA Inc.C=JP CN=Nippon RA Certification Authority 4 Q=Nippon RA Inc.C=JP La 1.2.840.113549.1.9.1=#16077465737440746573742e636f2e6a70.CN	"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)
<	
ОК	

※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。