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)

2020年11月10日

Ver. 1.30

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 | | | |

<目 次>

| 1. 本書の目的 | |
|---------------------------------------|----|
| 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 | 8 |
| 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 | 17 |
| 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 | 23 |
| 3.10. クライアント証明書の情報参照(クライアント側) | 24 |

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。

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。

| b | 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。ドキュメン のホストなどの組織のコンビューティング ニーズに応じて、インストールする役割、役割サービス、8 す。 | トの共有や Web サイト Eたは機能を決定しま |
| サーバーの選択 ワーハーの役割 | 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 | |
| 機能 | 統行する前に、次のタスクが完了していることを確認してください。 | |
| 雑誌 | 管理者アカウントに強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 から最新のセキュリティ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、ウィザードを閉じて、それらの作業 ドを再度実行してください。 | 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) > インストー | -ル(I) キャンセル |
| | | |
| | | |
| 2 | 役割と機能の追加ウィザード | _ 🗆 X |
| [▶] インストールの種類 | 役割と機能の追加 24 ビード の選択 | メーマン 対象サーバー WIN-NBSSD1916HG |
| La インストールの種類 開始する前に | 役割と機能の追加ウィザード 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、実行中の物理コンピューター、仮想コンピュ ンの仮想ハートティスク (VHD) にインストールできます。 | |
| と インストールの種類 間始する前に クスト せの空気 サーバーの選択 | 役割と機能の追加ウィザード の)登択 ペンストールの運動を選択します。役割および機能は、実行中の物理コンピューター、仮想コンピ ンの反思ノードティスク (VHD) にインストールできます。 ④ 役割ペースまた【機能ペースのインストー 役割、役割サーこと、および機能を追加して、1 名のサーバーを構成します。 | |
| こ インストールの種類 時はする前に サーバーの違来 サーバーの企園 商業 確認 | 役割と機能の追加ウメザード の選択 インストールの運動を選択します。位割および機能は、実行中の物理コンピューター、仮想コンピ ンの仮想し、ドライスク(VHD)にインストールを言す。 ④ 役割へースまたは繊維ペースのインストール 依認・疫謝・ビス、および嫌迷を急加して、1 台のサーバーを構成します。 〇 リエートテスクトップサービスのインストール 伝想デスクトップ インフラストックチャ (VOI) に必要す役割サービスをインストールして、仮想 ション (へ スのテスクトップ展開を作成します。 | |
| こ インストールの種類 開始する前に サーバーの選択 サーバーの選択 サーバーの認想 構築 結果 | 役割と機能の追加ウメザード 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、実行中の物理コンピューター、仮想コンピュ ンの優想ハード ディスク (VHD) にインストールで書す。 ④ 物調ペース主な目数ペースのインストール 役割、役割サービス、および機能を追加いて、1 台のサーバーを構成します。 ○ リモート デスクトップ サービスのインストール 仮想アスクトップ インフストランター (VD) に必要な役割サービスをインストールして、仮想て ション バースのデスクトップ展開を作成します。 | |
| L インストールの種類 開始する前に <u>インストールの種類</u> サーバーの理想 サーバーの理想 確認 結果 | 役割と職能の追加ウイゲード (の)遅択 インストールの優越を選択します。役割および機能は、東行中の物理コンピューター、仮想コンピュ の仮想ハード ディスク (VHD) にインストールできます。 (役割へ スまたは機能へ一スのインストール (役割 へえれたは機能へ一スのインストール (役割 へえれたはないて、1 台のサーバーを構成します。 ・ リモート デスクトップ サービスのインストール (役割 デスクトップ オードスのインストール (役割 デスクトップ オードスのインストール (役割 デスクトップ サービスのインストール (役割 デスクトップ オードスのインストール (公割 ケービスをインストールして、仮想 ション バースのデスクトップ展開を作成します。 | |
| L インストールの種類 開始する前に サーバーの違訳 サーバーの控制 確認 確認 結果 | 役割と機能の追加ウィザード の選択 ペンストールの種類を選択します。役割および物紙は、実行中の物理コンピューター、仮想コンピ ンの反則ハード ディオク (VHD) にインストールできます。 ④ 役割ペースまたは機能ペースのインストール 依割・役割・レビス、および様を追加して、1 缶のサーバーを構成します。 ・ リモート デスクトップ サービスのインストール 仮想デスクトップ インフストランチャ (VDI) に必要な役割サービスをインストールして、仮想す ション ベースのデスクトップ 無疑を作成します。 | |
| L インストールの種類 サーバーの選択 サーバーの運用 サーバーの運用 前認 範認 | 役割と機能の追加ウメザード の選択 ペンストールの種類を選択します。位割および機能は、実行中の物理コンピューター、仮想コンピ ンの仮想し、ドライスク(VHD)にインストールで書す。 ④ 役割ヘースまたは機能やこみのインストール 仮影・夜がして、たまび機能を追加して、1 台のサーバーを構成します。 〇 リモートテスクトップサービスのインストール 位勝アコウィングンフラストックホール 位勝アコウィングンフラストックホール 位勝アコウィングンフラストックホートの (UD) に必要な役割サービスをインストールして、仮想、 ション ベースのデスクトップ展開を作成します。 | |
| L インストールの種類 開始する前に サーバーの選択 サーバーの選択 サーバーの認 構造 確認 結果 | 役割と機能の追加ウメザード の遅択 インストールの理想を選択します。役割および機能は、実行中の物理コンピューター、仮想コンピュ >>の仮想ハードティスク(VHD)にインストールできます。 (243)ペースまたは総約ペースクリストール 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。 ○ Jモートテスクトップ サービスのインストール (役割アスクトダインフストーター)(役割テム)(クストール) (役割アスクトダインフストラール) (公割アスクトップ)(大)(公司)に必要な役割サービスをインストールして、仮想マ >>ョン パースのデスクトップ展開を作成します。 | |
| L インストールの種類 開始する前に ゲーパーの選択 サーパーの選択 サーパーの選択 特徴 構築 発展 | 役割と機能の追加ウメゲード の遅沢 ペンストールの種類を選択します。役割および機能は、実行中の物理コンピューター、仮想コンピュ ンの復知へ下すべろ (VHD)にインストールをます。 (9 (23)へーススは振動やニスクペンストール 位割、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。 ○ リモートアスクトップ サービスのインストール 仮想アスクトップ インフストランアレール (必要アスクトップ インフストランアレール)(23)の第一位、広想で、 ション バースのデスクトップ展開を作成します。 | |
| L インストールの種類 開始する前に サーバーの選択 サーバーの選択 サーバーの認 構築 構築 構築 | 役割と機能の追加ウメザード の選択 ペンストールの理聴を選択します。役割および特能は、実行中の物理コンピューター、仮想コンピュ かの反則ハード デスク (やわり) にインストールできます。 ・ 御神ーマスト みよび特定を追加して、1 台のサーバーを構成します。 ・ 「サート テスクトップ サービスのインストール 依絶テスワトップ インフストークトール 低絶テスワトップ インフストークトール 低地テスワトップ クレンストークトール 低地テスワトップ 原見を作成します。 < 新へ(P) 広へ(N).こ (2.21-1) | |

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。

| b | 役割と機能の追加ウィザード |
|---|---|
| 対象サーバーの選 | 3族サーバー WIIN-NB5501916HG |
| 開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能 確認 結果 | 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 フィルター: 名前 IP アドレス オペレーティング システム WIN-NB55D19I6HG 172.30.0.116 Microsoft Windows Server 2012 R2 Standard |
| | 1 台のコンピューターが見つかりました 20ペーンには、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 サーバーや、テーダ収集が完了していない、新たに追加された サーバーは表示されません。 |

 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。

| ーバーの役割の | の選択 |
|-----------|--|
| 開始する前に | 選択したサーバーにインストールする役割を 1 つ以上選択します。 |
| ハンストールの種類 | 役割 |
| ナーバーの選択 | |
| ナーバーの役割 | ■ Web Server (IIS) (16/43 個をインストール済み) |
| 時間に | ▲ ■ Web Server (15/34 個をインストール済み) |
| な三刃 | Common HTTP Features (4/6 個をインストール済み) |
| 課 | Performance (1/2 個をインストール済み) Performance (1/2 個をインストール済み) |
| | ▲ V 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 |
| | ID and Demain Restrictions (A.7h. (\$27) |

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。

→チェックする

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) "
- ・"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。

| - 🗆 X | |
|---------------------|-----------------------|
| Administrator 🎴 ర 🔎 | 検索 すべての場所 ~ mmd |
| | mmc |

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 | | | | | | |
|--|---------------|---|------------------|------------------|--|--|
| コンピ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、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(5): 選択されたスナップイン(5): | | | | | | |
| 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 | | | | | |
| 🕑 タスク スケジューラ | Microsoft Cor | | | 削除(<u>R</u>) | | |
| ディスクの管理 | Microsoft and | | | | | |
| ⇒デバイス マネージャー | Microsoft Cor | | | 上へ移動(U) | | |
| ポテレフォニー | Microsoft Cor | | | | | |
| ◎パフォーマンス モニター | Microsoft Cor | | | 下へ移動(<u>D</u>) | | |
| | Microsoft Cor | | 追加(<u>A</u>) > | | | |
| 」「ホリシーの結果セット | Microsoft Cor | | | | | |
| 豊ルーティンクとリモート アク | Microsoft Cor | | | | | |
| 1000000000000000000000000000000000000 | Microsoft Cor | = | | | | |
| 愛 ローカル ユーサービクルーノ | Microsoft Cor | | | | | |
| 20 共有ノオルター | Microsoft Cor | | | | | |
| 21月1日日 | Microsoft Cor | | | =***==ひまつい | | |
| 「「」」「」」「」」 | MICLOSOFT COL | V | | 評細設定(⊻) | | |
| =8RB · | | | | | | |
| 90/70・ 「江明事フキップノンを使うレューザー サービス まわけつンジューターの江明事フトマの内容を問題できます | | | | | | |
| 証明音人/ツノリノを使えたエージー、ジーにん、よにはコノヒューツーの証明音人/アリア)谷径開見にさます。 | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | OK キャンヤル | | |
| | | | | | | |
| | | | | | | |

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。

| Į. | E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 (コンビューター アカウント(<u>C</u>) | | | |
| | < 戻る(<u>B</u>) | 次へ(<u>N</u>) > | 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"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: ◎ □ーカル コンピューター(<u>L</u>): (このコンソールを実行しているコンピューター) | ן |
| ○別のコンピューター(<u>A</u>): 参照(<u>R</u>) | |
| □コマンド ラインから起動したときは選択されたコンピューターを変更できるようにする(<u>W</u>) 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(B) 完了 キャンセル | , |

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

| Microsoft Cor Microsoft Cor | | | 🗊 証明書 (ローカ) | レコンピューター | |
|--------------------------------|--|--|--|--|---|
| Microsoft Cor | | | | × | |
| | | | | | 削除(<u>R</u>) |
| vicrosoft and | | | | | |
| Microsoft Cor | | | | | L = 56754(11) |
| Microsoft Cor | | | | | |
| Microsoft Cor | | | | | 下へ移動(D) |
| Microsoft Cor | | 追加(A) > | | | · · · · · · · · · · · · · · · · · · · |
| Microsoft Cor | | | | | |
| Microsoft Cor | | | | | |
| Microsoft Cor | | | | | |
| Microsoft Cor | ≡ | | | | |
| Microsoft Cor | | | | | |
| Aicrosoft Cor | | | | | |
| Aicrosoft Cor | - | | | | 詳細設定(⊻) |
| | licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor | licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor | ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor ikrosoft Cor | icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor icrosoft Cor | licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor licrosoft Cor |

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 | |
|--|---|---|
| | a | コンソール1 - [コ] |
| □ 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) (中) □ □ □ □ □ | 3 ファイル(F) 操作(A) 表示(V) お気に入り(O) ◆ ● 2 ▲ □ 0 0 | ウィンドウ(W) ヘルプ(H) |
| | | 発行先 Baltimore CyberTrust Root Class 3 Public Primary Certif Copyright (c) 1997 Microsof インボート(1) rosoft Root Authority rosoft Root Certificate A I rosoft Root Certificate A I rosoft Root Certificate A I LIABILITY ACCEPTED, (I wte Timestamping CA ISign Class 3 Public Prim Y |

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 | а Н |
| 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3 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(<u>C</u>) | |
| ◎ □−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。

| | x |
|---|---|
| ● 🔗 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 | |
| インポートするファイルを指定してください。 | |
| | - |
| ファイル名(E): | |
| C:#NipponKARootCertificationAutnonty.crt 参照(<u>B</u>) | |
| 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 シリアリノと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"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 |
|------------------------------|---|
| ★ 証明書のインボート ウィザード | ● 🐓 証明書のインボート 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。 | 証明書ストア 証明書ストアは朝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。 G 証明書の機関に基クいて、目動的に証明書ストアを選択する(U) E 証明書でて次のストアに定選する(E) IIII IIIII書でて次のストアに定選する(E) IIIII書でて次のストアに定選する(E) IIIII書でたた。 使類(た) 使類(た) |
| 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。

| 📀 😅 証明書のインポート ウィザード | x |
|--|-------|
| 証明書のインボート 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: | |
| ユーザーが確択した証明書ストア 信頼されたルート証明機関 | ٦ - ١ |
| 内容 証明書 フェイルター CVXNIppopPARostCartificationAuthority.crt | |
| C.+NpponteReducer incation Automotiver | |
| | |
| | |
| | |
| | _ |
| | |
| | |
| | |
| | |
| 売了(E) キャ | ンセル |

① 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⑦~②までを繰り返します。



③ 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/ | 43) | | | |
|---|---|---|--|---|
| | -ル1 - [コンソール ルート¥証明書 (ローカ ウインドウ(W) ヘルブ(出) 発行先 Microsoft Windows Hardware Compu- Gal Nippon RA Certification Authority 1 Root Agency Wwww.verisign.com/CPS Incorp.by R | ルコンピューター)¥中間証明機関¥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 2031/08/15 2040/01/01 2016/10/25 | - □ × - a × 操作 延明書 ▲ 他の操作 → |
| ▶ ○ 信頼されたユーザー ▶ ○ クライアント怒延発行者 ▶ ○ リモートテスクトップ ▶ ○ スマートカードの信頼されたルート ▶ ○ 保軽されたデバイス ▶ ○ Web ホスティング | си | | > | |

| ルート証明機関 | | | | |
|---|--|---|---|---|
| | - [コンソールルート¥証明書 (ローカルコン ウインドウ(W) ヘルブ(H) 発行先 GBabtimore CyberTrust Root Copyright (c) 1997 Microsoft Corp. DigiCert Global Root CA Microsoft Root Authority Microsoft Root Certificate Authority Microsoft Root Certifi | ビューター)¥信頼されたルート証明機関¥証明 発行者 Baltimore CyberTrust Root Class 3 Public Primary Certification Authority Copyright (c) 1997 Microsoft Corp. DigiCert Global Root CA Microsoft Authenticode(tm) Root Authority Microsoft Root Authority Microsoft Root Certificate Authority 2010 Microsoft Root Certificate Authority 2011 Nippon RA Root Certificate Authority 2011 Nippon RA Root Certificate Authority 2011 Nippon RA Root Certification Authority No LIABULITY ACCEPTED, (c)97 VenSign, I Thawte Timestamping CA | 有効期限 2025/05/13 2028/08/02 1999/12/31 2031/11/10 2020/12/31 2020/12/31 2020/12/31 2036/07/23 2036/07/23 2031/08/15 2004/01/08 20321/01/01 2036/07/17 | × |
| ▶ ○ スマートカードの信頼されたルート ▶ ○ 信頼されたデバイス ▶ ○ Web ホスティング | < III | | > | |
| | | | | |

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」

| ? | × |
|------|--------|
| | |
| _ | |
| | |
| | |
| | |
| | |
| | \sim |
| | |
| キャンセ | IL |
| | +++>2 |

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 | | | | |
|--|---|--|--|--|
| 種類 ホスト名 ポート IP アドレス パインド情報 http 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 | 自加 ? × |
|--|---|
| 種類(T): https v ホスト名(出): □ サーバー名表示を要求する(N) | π ^t −ト(<u>0</u>): ✓ 443 |
| SSL 証明書(E): DEMO | Y 選択(L) 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 | ? × |
|--------------------------|--|---|
| 種類 木スト名 http https | ポート IP アドレス /バインド情報 80 * 443 * | 这加(<u>A</u>) 編集(<u>E</u>) 削除(<u>R</u>) 参照(<u>B</u>) |
| | | 閉じる(<u>C</u>) |

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



② "匿名認証"を選択し、"無効にする"をクリック。

| (`) =30 =,T | | | | 操作 |
|------------------|----|-------|--|-----|
| S BUC BLE | | | | 1 |
| グループ化: グループ化なし 🔹 | | | | 編 |
| 名前 | 状態 | 応答の種類 | | 0 ^ |
| ASP.NET 偽装 | 無効 | | | |
| 匿名認証 | 有効 | | | |
| | | | | |

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。

| 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 | · 💶 🗖 🗙 |
|---|-----------|
| ● ・ WIN-NBS5D19I6HG ・ サイト ・ Default Web Site ・ | 🖸 🐼 🟠 🔞 🗸 |
| ファイル(E) 表示(Y) ヘルプ(出) | |
| Bkk Comparison of the image o | 提作 |
| < III 検能ビュー 🔐 コンテンツ ビュー | 詳細設定 > |
| 準備完了 | ¶.: |

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/iisClientCertificateMappingA | • |
| ▶ 最深のバ ■ □ system.net ■ □ system.transactions ■ □ system.webServer ■ □ system.webServer ■ □ authentication ■ □ authentication ■ □ authentication ■ □ authentication ■ □ significateMappingAuthentication ■ □ access ■ □ applicationDependencies ■ □ authorization ■ □ authorization ■ □ access ■ □ authorization ■ □ authorization ■ □ authorization | |

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(S): system.webServer/security/ ・ 3 | 易所(<u>M</u>): ApplicationHost.config <loca th="" ・<=""></loca> |
|--|--|
| ▲ 最深のパス: MACHINE/WEBROOT/APPH | IOST |
| defaultLogonDomain | |
| enabled | True 🗸 |
| logonMethod | True |
| manyToOneCertificateMappingsEnabled | Faise |
| 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。

ManyToOneMappings のリストボタンをクリック。

| 2ク | ション(<u>S</u>): system.webServer/security/aut | h • 場所(M): ApplicationHost.config <location th="" •<=""></location> |
|----|--|---|
| ⊿ | 最深のパス: MACHINE/WEBROOT/APPI | HOST |
| | defaultLogonDomain | |
| | enabled | True |
| | logonMethod | ClearText |
| | manyToOneCertificateMappingsEnabled | True |
| | manyToOneMappings | (Count=0) |
| | oneToOneCertificateMappingsEnabled | True |
| | oneToOneMappings | (Count=0) |

⑤ コレクションエディターの "追加"をクリック。

| יעב | クション 3 | エディター - s | ystem.v | vebServer/secu | urity/authe | entication | /iisClientCertificate | eMappingAuthentica | ation/manyTo |
|-----|--------|-------------|---------|----------------|-------------|------------|-----------------------|--------------------|--------------|
| 項目 | ≣: | | | | | | | | 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 |
| < | | | | III | | | | | オンライン ヘルプ |
| プロ | パティ: | | | | | | | | |
| | | | | | | | | | |

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 \rightarrow "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

 $(4) permission Mode \rightarrow ``Allow''$

(5)userName

→ 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 | १– - syste | m.webSe | rver/security/a | uthenticat | ion/iisClient(| CertificateMap | pingAuth | entication/ma | X |
|----|-------------|-------------|---------|-----------------|------------|----------------|----------------|----------|---------------|---|
| 項 | ∃: | | | | | | | | 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 | コパティ: | | | | | | | | 項目のロック | |
| | description | | | | | | | | ▲ 削哧 | |
| | enabled | | | Tru | e | | | | ⑧ ∧ルプ | |
| | 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。

| 1: | | | | | | | | 操作: | |
|--|-------------|-----------------|-------------------------|---------------------|---------------------|--------|---|------------------------|--|
| name Demo | description | enabled True | permissionMode Allow | userName inetUsr | password ******* | エントリパス | | コレクション 追加 すべてクリア | |
| | | | Ш | | | | > | 項目のプロパティ | |
| リパティ: description | | | | | | | | ¥ 削除 | |
| enabled | | | Tru | e | | | | 0 NJ | |
| | | | * De | mo | | | | オンライン ヘルプ | |
| name | | | • • | | | | | | |
| name password | | | | | | | | | |
| name password permissionM | lode | | Allo | W | | | | | |
| name password permissionM rules | lode | | Allo (Co | ount=0) | | | | | |

- 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

| コレ | クション エディター - s | system.webServe | r/security/au | thentication/iisClier | ntCertificateMappingAuthent | icat | tion/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 | | | lê ta |
| | | | | | | | すべてカリア |
| _ | | | | | | | |
| < | | | | | 1 | > | 項目のプロパティ 🛛 🗆 |
| プロ | パティ: | | | | | 1 | 項目のロック |
| | certificateField | | 8 Subject | | • | | 🗙 削除 |
| | certificateSubField | | ° 0 | | L | | 🕡 ヘルプ |
| | compareCaseSensiti | ive | * True | | | | オンライン ヘルプ |
| | matchCriteria | | RADemo | | | | |
| | | | | | | | |

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 | \rightarrow "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 | フション エディター | - system.webSei | ver/security/aut | hentication/iisClientCe | ertificateMappingA | uthentic | ation/man | ? X |
|-----|--------------------|---------------------|------------------|-------------------------|--------------------|----------|-----------|-----|
| 項目 | 1: | | | | | | 操作: | |
| | certificateField | certificateSubField | matchCriteria | compareCaseSensitive | エントリ パス | | コレクション | - |
| | Subject | 0 | NRADemo | True | | | 20.60 | |
| | Issuer | 0 | Nippon RA Inc. | True | | | シュート | |
| | | | | | | | 9~(0))/ | |
| < | 1 | | III | | | > | 項目 のプロパティ | - |
| プロ | パティ: | | | | | | 項目のロック | |
| - (| certificateField | | Issuer | | | | 🗙 削除 | |
| | certificateSubFiel | d | ° O | | | | ⑦ ∧ルプ | |
| | compareCaseSen | sitive | rue | | | | オンライン ヘルプ | |
| | matchCriteria | | Nippon RA II | nc. | | | | |
| | | | | | | | | |
| | | | | | | | | |

※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。

 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。



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) ^ | 、ルプ(H) | | _ 8 | × |
| - | ファイル(F) 新規(開く(C 上書さ 名前花 スナッ: オプシ: 1 C:¥L 2 dev 3 serv 終了(| 操作(A) 年成(N) り) 皆保存(S) E行けて保存 プインの追加 コン(P) Jsers¥Komi mgmt ices X) | 表示(V) {(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) ^ 頁目は: | Jレプ(H) ありません。 | <mark>操作</mark> コンソール ルート 他の操作 | _ 6 | • |
| スナ | ップインを追力 | ロしたり、スナ | ップイン コン | ソールからスナップ | インを削除し | L | | | | |

③ 左画面の下方にある証明書を選択、"追加"をクリック。

| | 122.00 | | | |
|----------------|------------------|--------------|------------------|----------------------|
| テッノイン | ~ <u>></u> y- | | | 払張の福果(込)… |
| セキュリティ テンプレート | Microsoft Corp | | | 削除(R) |
| セキュリティが強化された… | Microsoft Corp | | | 1221624(<u>15</u>) |
| 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>U</u>) |
| ディスクの管理 | Microsoft and V | | | |
| デバイス マネージャー | Microsoft Corp | 14 | | 下へ移動(<u>D</u>) |
|)パフォーマンス モニター | Microsoft Corp | | (<u>A</u>) > | |
| 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 | | | |
| 証明書 | Microsoft Corp | \checkmark | | 詳細設定(⊻) |
| | | | | |
| 8: | | | | |
| | ニーサービス キたけつい | 14'n- | 明書ストアの内容を閲覧できます。 | |

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書: ● ユーザーアカウント(M) ○ サービス アカウント(S) ○ コンピューター アカウント(C) | | | |
| | | | |
| | < 戻る(<u>B</u>) | 完了 | キャンセル |

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。

| トップイン | ベンダー | ^ | א-ע ערב 🛄 | 拡張の編集(X) |
|------------------------------|----------------------------------|---|-----------------|---------------------------------|
| セキュリティテンプレート セキュリティが強化された | Microsoft Corp Microsoft Corp | | 😱 証明書 - 現 | 在のユーザー 削除(<u>R</u>) |
| 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 | | | |
| デバイス マネージャー | Microsoft Corp | | | 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 | | | |
| 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 | | | |
| 17 88 m | Microsoft Corp | ~ | | 詳細設定(⊻) |

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。

| ြ ユンソール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 | | |
| ✓ □ 個人 □ 証明書 | | | | 他の操 | 作 | • |
| > 🧮 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







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 | |
| Et #907.4(E) CN=Nippon RA. Root Certification Authority,O=Nippon RA.Inc.,C=JP CN=Nippon RA Certification Authority 4,O=Nippon RA Inc.,C=JP 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) |
| < > > 証明書の表示(V) | |
| 証明書の状態(S): この証明書は問題ありません。 | |
| 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。