# 公的個人認証サービス(JPKI)
# 利用者証明書連携ツール

## 操作マニュアル

Version1.02

2024 年2月

# 目次

**1. 概要 1**

**2. JPKI 利用者証明書連携ツールのインストール 2**

2.1. 画面からのインストール 2

2.2. サイレントインストール 5

**3. JPKI 利用者証明書連携ツールのアンインストール 6**

3.1. 画面からのアンインストール 6

3.2. サイレントアンインストール 8

**4. 証明書の確認 9**

**5. SSL クライアント認証 14**

# 1. 概要

公的個人認証サービス(以下 JPKI)利用者証明書連携ツールは、IC カードリーダライタに挿入されているマイナンバーカードから、利用者証明用証明書を Windows 証明書ストアに自動登録するものです。
HPKI セカンド電子証明書管理・認証プラットフォームにてマイナンバーカードを使用して認証する場合、このツールが必要になります。

JPKI 利用者証明書連携ツールの動作環境は、以下の通りです。

| | |
|---|---|
| 対応 OS | ・ Windows 10 32bit/64bit 版 ※1<br>・ Windows 11<br><br>※1 動作環境が Windows10 32bit の場合、setup_x86.exe を使用<br>動作環境が Windows10 64bit の場合、setup_x64.exe を使用<br>動作環境が Windows11 の場合、setup_x64.exe を使用 |
| 対応ブラウザ | Microsoft Edge (Version 100 以降)<br>Google Chrome (Version 99 以降) |
| その他 | JPKI 利用者ソフトがインストール済み<br>※最新のバージョンを使用してください(2023 年 12 月現在 3.5) |

※詳細については、地方公共団体情報システム機構、公的認証サービスポータルサイトの JPKI 利用者ソフトのダウンロードの要件に従ってください。

＜ご注意＞
- IC カードリーダライタは、マイナンバーカード対応のものを使用してください。
  対応のICカードリーダライタについては、下記サイトをご覧ください。
  https://www.jpki.go.jp/prepare/reader_writer.html
- JPKI 利用者ソフトは、下記サイトより入手ください。
  https://www.jpki.go.jp/download/

# 2. JPKI 利用者証明書連携ツールのインストール

## 2.1. 画面からのインストール

次の手順に従ってインストールしてください。

① 管理者アカウント(Administrator 権限のあるユーザ)でログオンしてください。

② 起動している他のアプリケーションを全て終了させます。

③ インストーラー(setup_x64.exe / setup_x86.exe)をダブルクリックしてください。
実行するインストーラーは、OSによって変わります。

- setup_x64.exe (Windows10 64bit、Windows11 OS)
- setup_x86.exe (Windows10 32 ビット OS)

④ インストーラーが起動すると、ようこそ画面が表示されます。

**図 2-1　JPKI 利用者証明書連携ツール　インストール(ようこそ)**

インストールを続行する場合は「次へ」ボタンを押してください。次画面を表示します。
インストールを中止する場合は「キャンセル」ボタンを押してください。

⑤　インストール先選択画面が表示されます。
インストール先フォルダ（デフォルト）が表示されています。インストール先を変更したい場合、「変更」ボタンを押して、インストール先を指定してください。

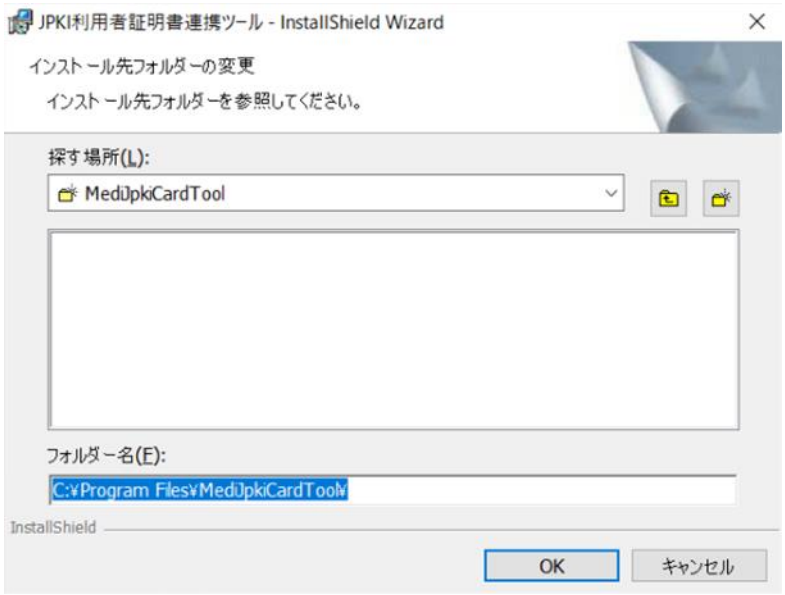



**図 2-2　JPKI 利用者証明書連携ツール　インストール（インストール先選択）**

インストール先フォルダを確定しインストールを続行する場合は「次へ」ボタンを押してください。インストールを中止する場合は「キャンセル」ボタンを押してください。

⑥　インストール準備画面が表示されます。「インストール」ボタンを押してください。インストールを中止する場合は「キャンセル」ボタンを押してください。「戻る」ボタンを押すと、前画面に戻ります。

※「インストールボタン」を押すとユーザアカウント制御画面が表示されます。「はい」ボタンを押してください。

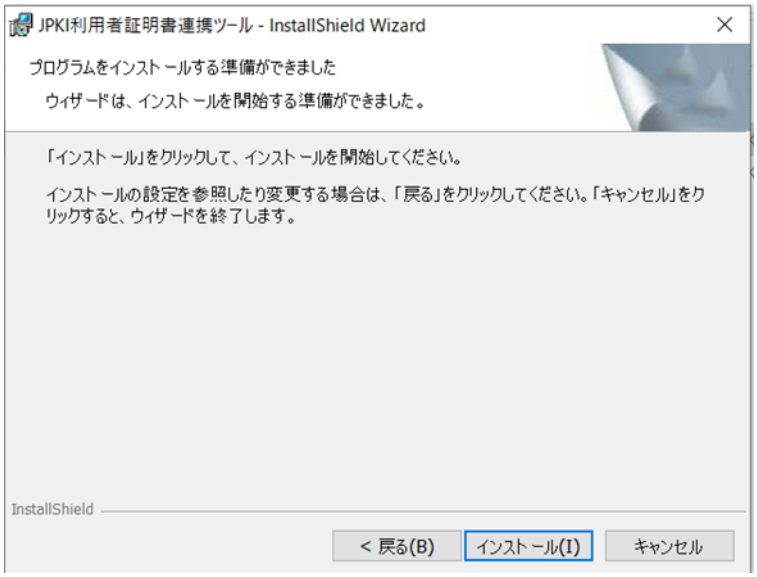



**図 2-3　JPKI 利用者証明書連携ツール　インストール（インストール準備）**

⑦　インストールの進み具合を示すインジケータ画面が表示されます。指定したフォルダへのインストールが始まります。

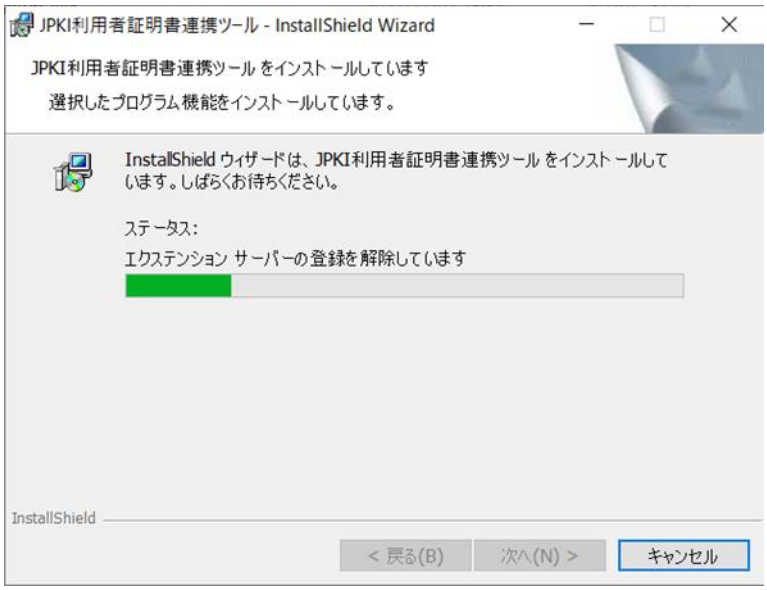



**図 2-4　JPKI 利用者証明書連携ツール　インストール（インジケータ）**

途中でインストールを中止する場合は「キャンセル」ボタンを押してください。

⑧　インストール完了画面が表示されます。「完了」ボタンを押してください

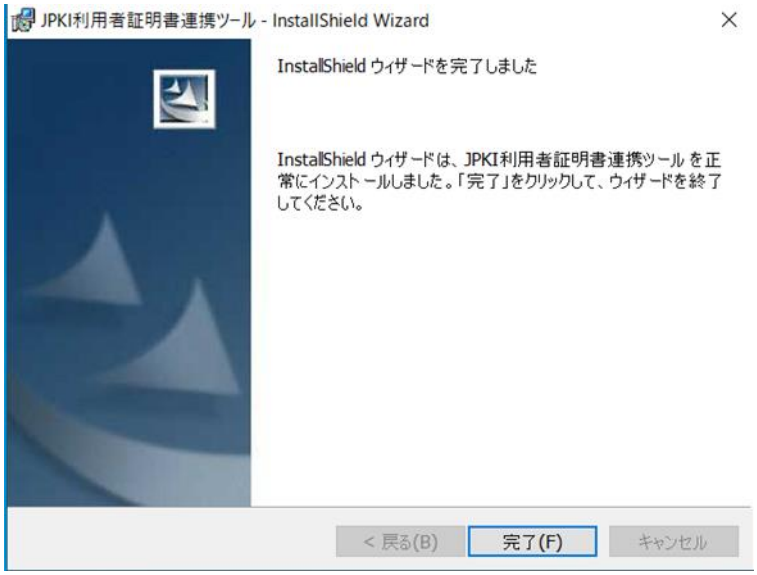



**図 2-5　JPKI 利用者証明書連携ツール　インストール（インストール完了）**

⑨　再起動確認画面が表示される場合があります。
インストール完了後、JPKI 利用者証明書連携ツールを利用するためにはコンピュータの再起動が必要な場合があります。
今すぐコンピュータを再起動する場合は「はい」を押してください。自動的にコンピュータが

再起動します。後で再起動をする場合は「いいえ」を押してください。このまま画面を終了します。「いいえ」を押した場合、後で再起動を行ってください。

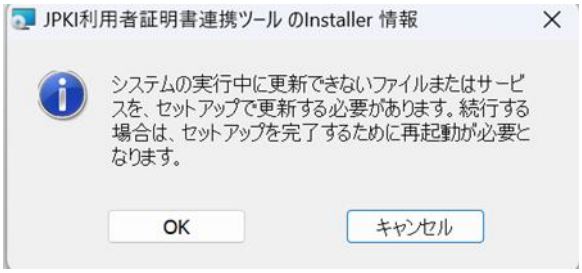



**図 2-2　JPKI 利用者証明書連携ツール　インストール（再起動確認）**

以上で JPKI 利用者証明書連携ツールのインストールは完了です。

## 2.2. サイレントインストール

setup_x64.exe（setup_x84.exe）　のコマンドラインオプション(/qn)を使用してサイレントインストールが可能です。
サイレントインストールの実施に関する注意事項は以下のとおりです。

- 管理者権限が必要なため、管理者権限を持つコマンドラインから実行する。
- カレントディレクトリを、インストーラーの存在するフォルダにしてください。

サイレントインストールのパラメータ（64bit）を以下に示します。

```
setup_x64.exe /s /v"/qn"
```

実行するインストーラーは、OSによって変わります。

- setup_x64.exe (Windows10 64bit、Windows11 OS)
- setup_x86.exe (Windows10 32 ビット OS)

パスを指定する場合のパラメータを以下に示します。

```
setup_x64.exe /s /v"/qn   INSTALLDIR=\"(インストール先のパス)\""
```

# 3. JPKI 利用者証明書連携ツールのアンインストール

## 3.1. 画面からのアンインストール

JPKI 利用者証明書連携ツールをアンインストールする場合は次の手順で行ってください。

① 管理者アカウント(Administrator 権限のあるユーザ)でログオンしてください。

② 起動している他のアプリケーションを全て終了させます。

③ 画面左下のスタートボタンを右クリック、[アプリと機能]をクリックします。アプリと機能一覧から[JPKI 利用者証明書連携ツール]を選択し、「アンインストール」をクリックします。

④ JPKI 利用者証明書連携ツールの削除を確認する画面が表示されます。
このままアンインストールを続行する場合は「はい」ボタンを、アンインストールを中止する場合は「いいえ」ボタンを押してください。

**図 3-1　JPKI 利用者証明書連携ツール　アンインストール(アンインストール確認)**

⑤ アンインストールが始まります。アンインストールの進み具合を示すインジケータが表示されます。「キャンセル」ボタンを押すと、アンインストールを中止します。

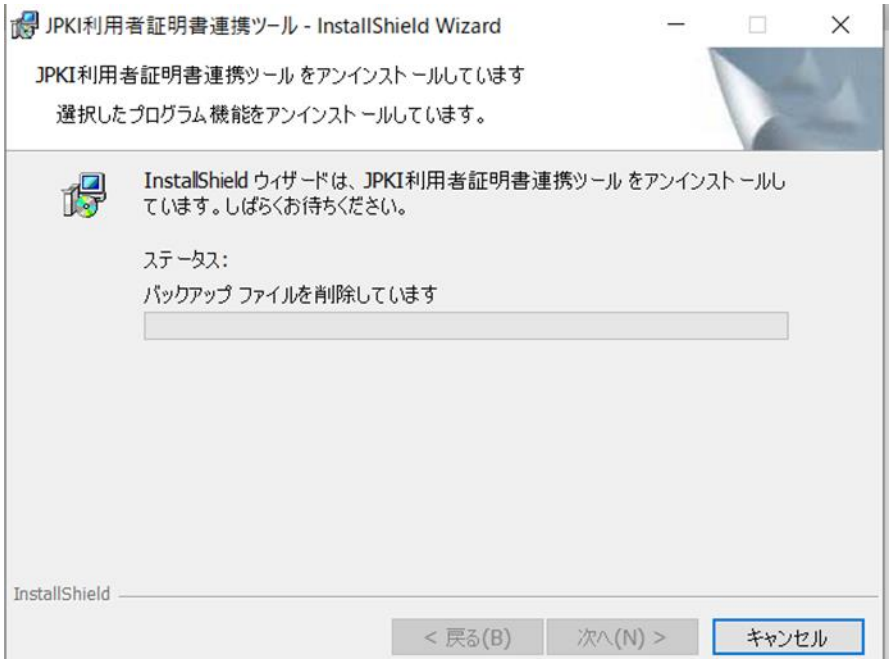



**図 3-2　JPKI 利用者証明書連携ツール　アンインストール(アンインストール中)**

⑥　再起動確認画面が表示される場合があります。

アンインストール完了後、JPKI 利用者証明書連携ツールのアンインストールを有効にするには再起動が必要となる場合があります。

今すぐコンピュータを再起動する場合は「はい」ボタンを押してください。自動的にコンピュータが再起動します。後で再起動をする場合は「いいえ」ボタンを押してください。このまま画面を終了します。「いいえ」ボタンを押した場合、後で再起動を行ってください。

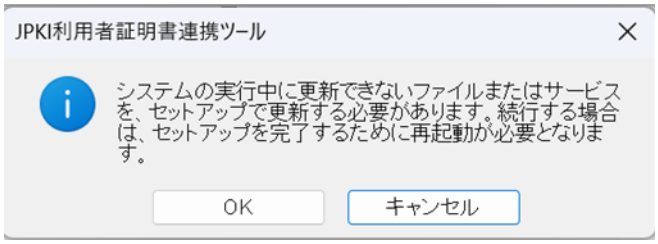
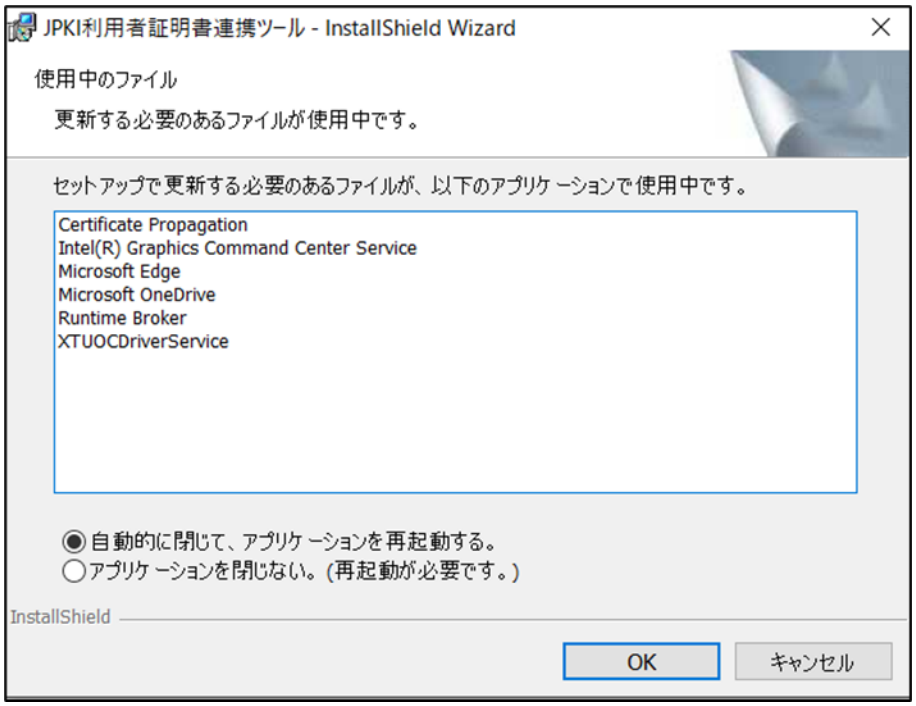



**図 3-3　JPKI 利用者証明書連携ツール　アンインストール（再起動確認）**

[注意]

ツールの実行中に、JPKI 利用者証明書連携ツールをアンインストールしようとした場合、以下のようなメッセージが表示されることがあります。アンインストールを継続する場合、「OK」ボタンを押してください。（このとき、「自動的に閉じて、アプリケーションを再起動する」を選択すると、アプリケーションが自動終了し、アンインストール処理が再開されます。「アプリケーションを閉じない（再起動が必要です）」を選択した場合、アンインストールが終了し、OS を再起動後、アプリケーションが削除されます。）



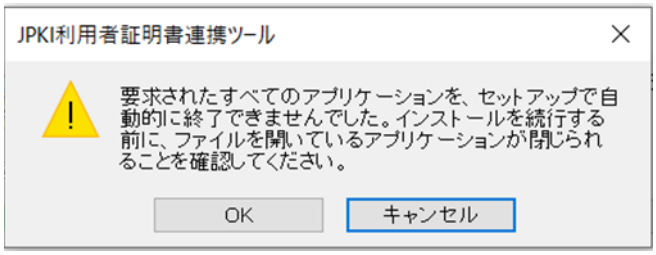



**図 3-4　JPKI 利用者証明書連携ツール　アンインストール（再起動警告）**

## 3.2. サイレントアンインストール

setup のコマンドラインオプション(/qn)を使用してサイレントアンストールが可能です。
実行するコマンドは、OS によって変わります。

- setup_x64.exe (64 ビット OS)
- setup_x86.exe (32 ビット OS)

サイレントアンインストールのパラメータ（64ビット OS）を以下に示します

```
setup_x64.exe /x /s /v"/qn"
```

# 4. 証明書の確認

本アプリケーションをインストールする事で、Windows 証明書ストアに JPKI 利用者証明書が登録され、SSL クライアント認証ができるようになります。証明書の確認方法を以下に示します。

**操作手順**

〈Microsoft Edge をご使用の場合〉

① マイナンバーカードを IC カードリーダライタに挿入します。

② Microsoft Edge を起動してください。

③ 画面右上の[…]から[設定]メニューを押してください。

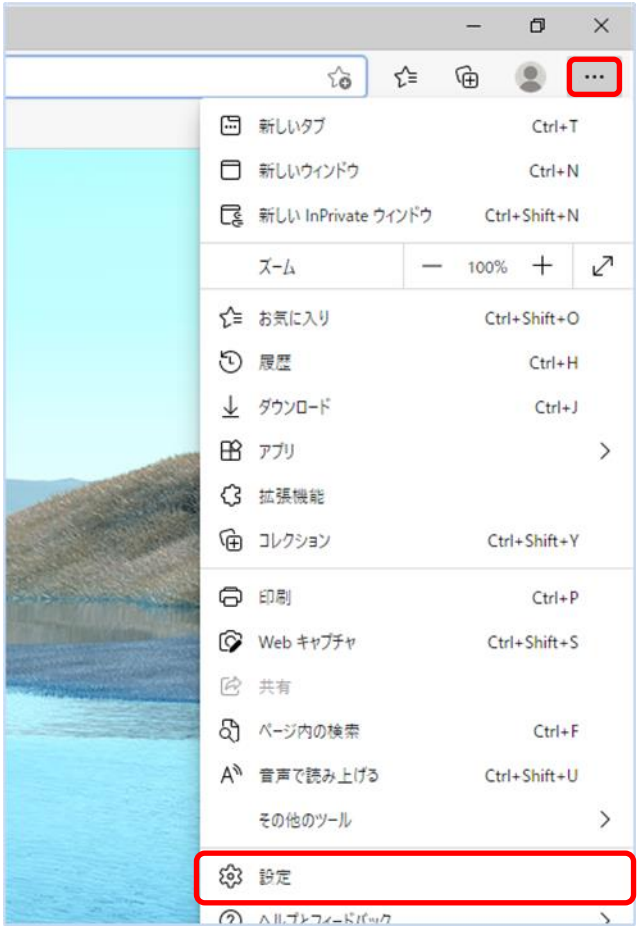



図 4-1 Microsoft Edge 画面(メニュー)

④ 左画面のメニューから、「プライバシー、検索、サービス」をクリックし、セキュリティの項目から「証明書の管理」をクリックしてください。

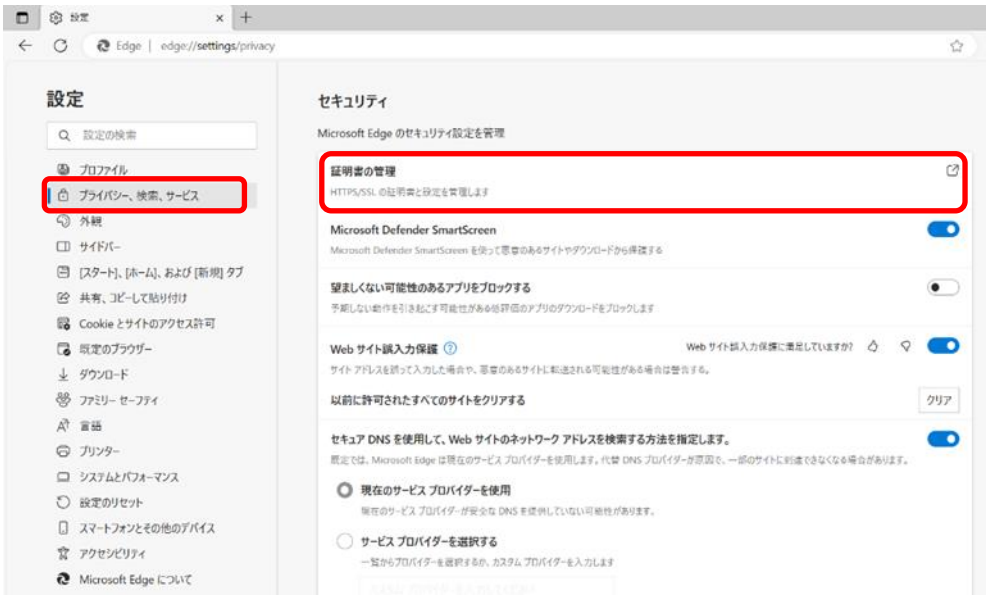



図 4-2 Microsoft Edge 設定画面（セキュリティ）

「個人」タブを選択すると証明書の一覧が表示されます。発行者「Japan Agenncy for local Authority Information Systems」の証明書があることを確認してください。

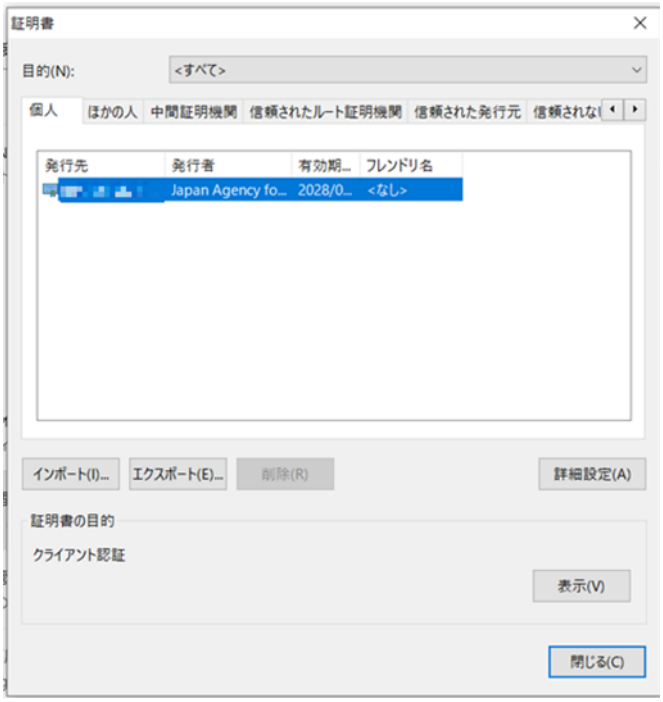



図 4-3 Windows 証明書ストア証明書確認（証明書一覧）

**<Google Chrome をご使用の場合>**

① マイナンバーカードを IC カードリーダライタに挿入します。

② Google Chrome を起動してください。

③ 画面右上の[⋮]から[設定]メニューを押してください。

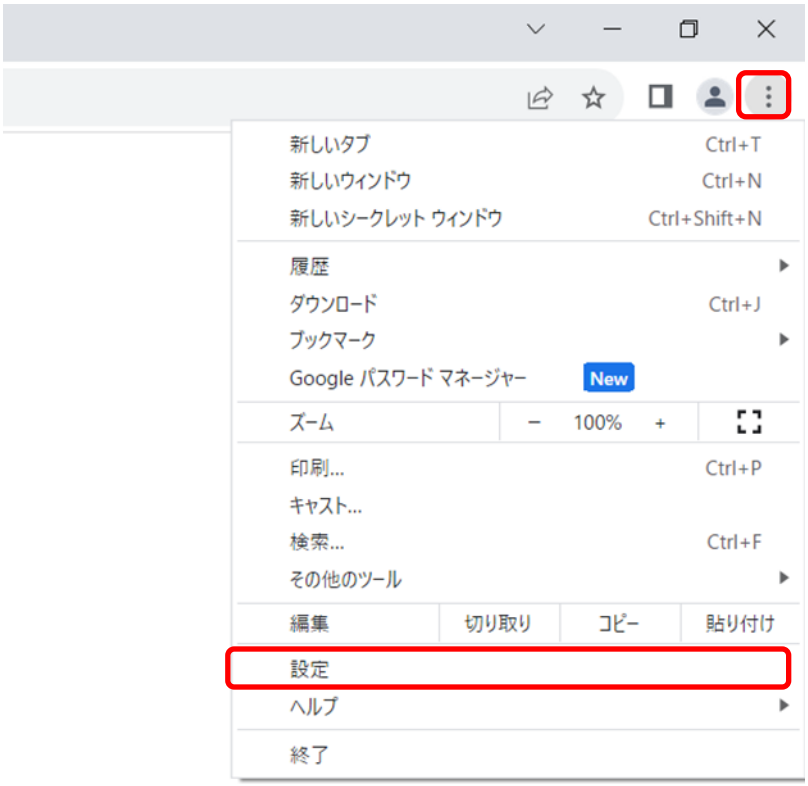



図 4-4 Google Chrome 画面(メニュー)

④ 左画面のメニューから、「プライバシーとセキュリティ」を押してください。右画面をスクロールし、プライバシーとセキュリティの「セキュリティ」を押してください。

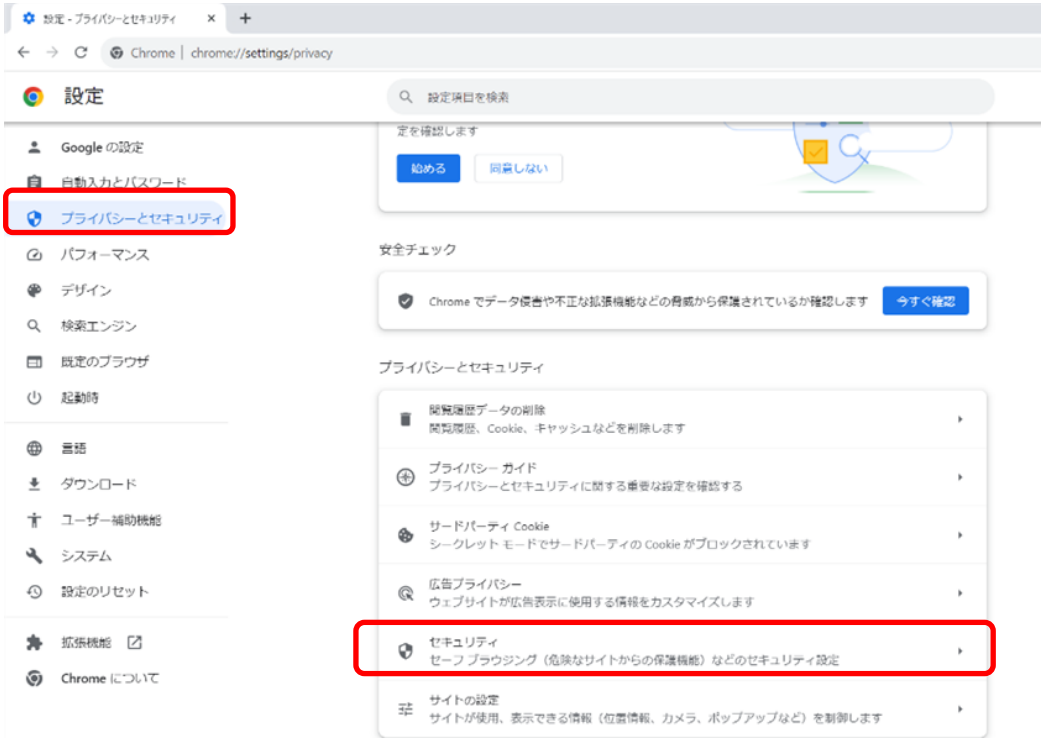



図 4-5 Google Chrome 設定画面（セキュリティ）

⑤ 右画面をスクロールし、詳細設定の「証明書の管理」を押してください。

図 4-6 Google Chrome 設定画面（証明書の管理）

「個人」タブを選択すると証明書の一覧が表示されます。発行者「Japan Agenncy for local Authority Information Systems」の証明書があることを確認してください。

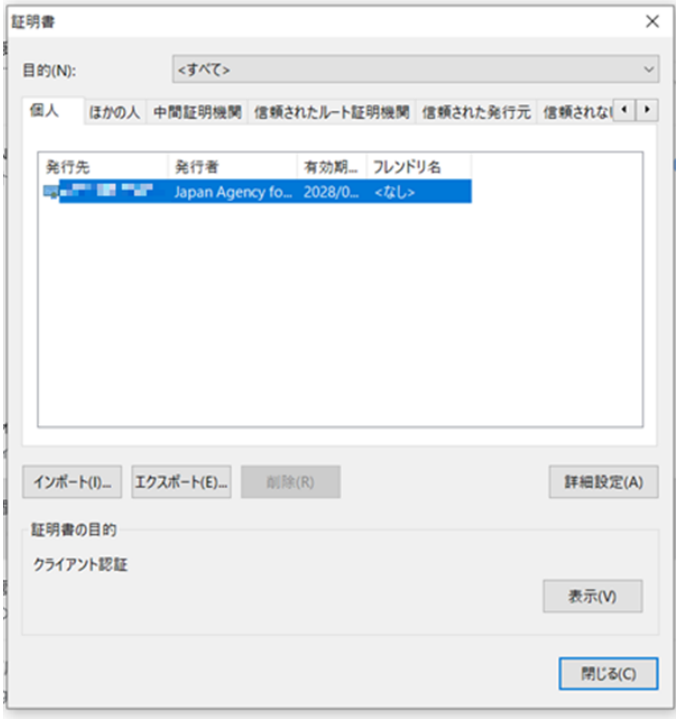



図 4-7 Windows 証明書ストア証明書確認（証明書一覧）

# 5. SSL クライアント認証

ブラウザを使用して SSL 認証を行う URL へ接続する場合の、SSL クライアント認証の手順について説明します。

ブラウザを使用する場合の SSL クライアント認証の手順は以下のようになります。

① URL 接続要求
② Windows 証明書ストアに格納されている、SSL クライアント認証に用いる証明書の選択
③ PIN(パスワード)認証
④ URL 接続成功

＜注意＞ ： SSL 認証を行う場合は、マイナンバーカードをリーダライタに挿入してから Web サーバへの接続操作を行ってください。挿入されていないと証明書選択画面で IC カード内の証明書が選択できない場合があります。また引き続き異なる IC カードで SSL 認証を行う場合、いったんブラウザを終了し再起動してから Web 接続を行ってください。

**操作手順**

**<Microsoft Edge をご使用の場合>**

① マイナンバーカードを IC カードリーダライタに挿入します。
② Microsoft Edge を起動して、指定 URL へ接続します。
③ Windows 証明書ストアの証明書のうち、SSL クライアント認証に使用可能な証明書の一覧が表示されます。発行元が JPKI となる証明書を選択して、「OK」ボタンを押してください。PIN 入力画面が表示されます。

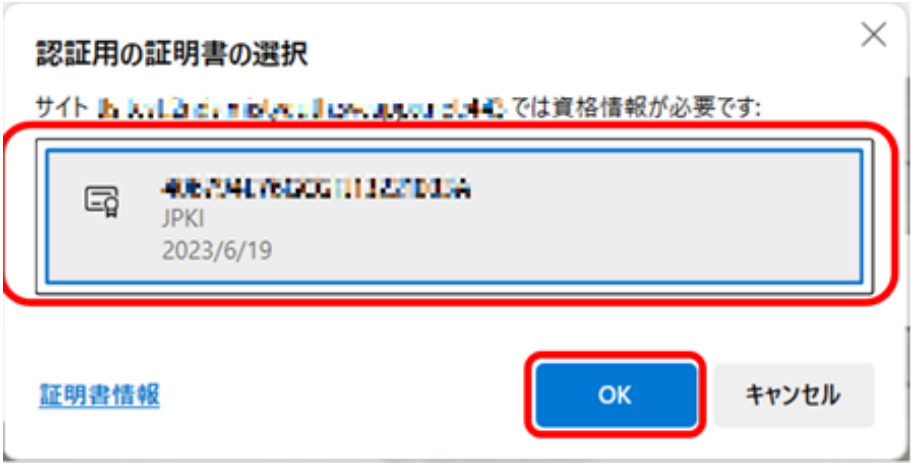



図 5-1 Microsoft Edge における SSL クライアント認証（証明書選択）

④ IC カードの PIN(パスワード)を入力して、「OK」ボタンを押してください。PIN(パスワード)認証が実施されます。

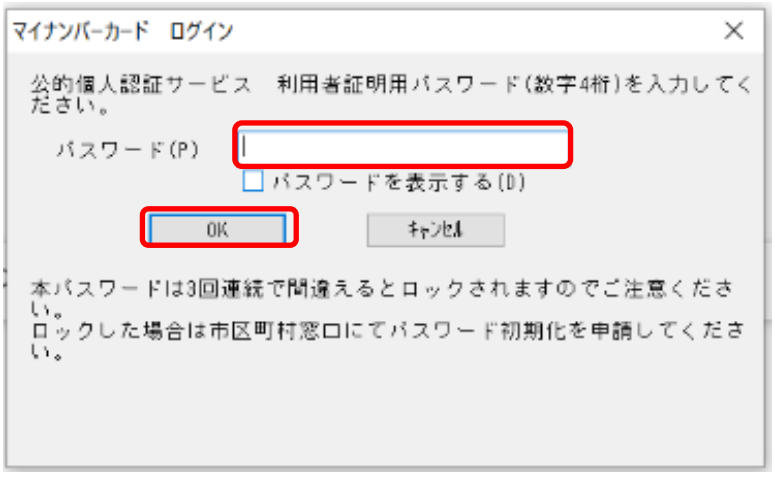



図 5-2 Microsoft Edge における SSL クライアント認証(PIN(パスワード)入力)

⑤ PIN(パスワード)認証に成功すると、目的のページが表示されます。ブラウザのアドレス入力領域に鍵アイコンが表示されます。

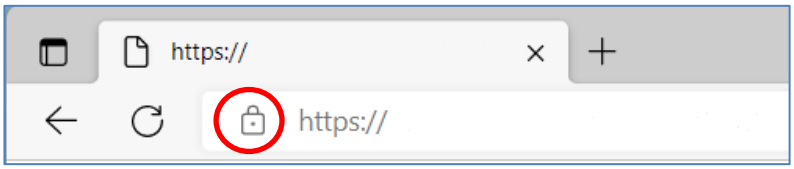



図 5-3 Microsoft Edge における SSL クライアント認証(認証成功)

**<Google Chrome をご使用の場合>**

① マイナンバーカードを IC カードリーダライタに挿入します。

② Google Chrome を起動して、指定 URL へ接続します。

③ Windows 証明書ストアの証明書のうち、SSL クライアント認証に使用可能な証明書の一覧が表示されます。発行元が JPKI となる証明書を選択して、「OK」ボタンを押してください。PIN 入力画面が表示されます。

図 5-4 Google Chrome における SSL クライアント認証（証明書選択）

④ IC カードの PIN(パスワード)を入力して、「OK」ボタンを押してください。PIN（パスワード）認証が実施されます。

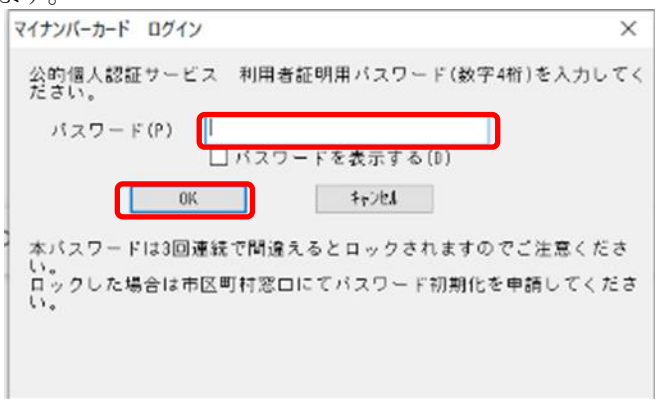



図 5-5 Google Chrome における SSL クライアント認証（PIN(パスワード)入力）

⑤ PIN(パスワード)認証に成功すると、目的のページが表示されます。ブラウザのアドレス入力領域に鍵アイコンが表示されます。

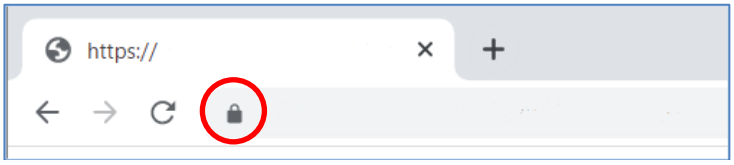



図 5-6 Google Chrome における SSL クライアント認証（認証成功）