
電子証明書 導入マニュアル

2023 年 6 月 1 日

株式会社オーグス総研

目次

1	はじめに	2
2	電子証明書について	3
3	証明書の発行（ダウンロード）手順.....	4

1 はじめに

本マニュアルは、弊社WebECサービスでご利用いただく電子証明書の導入について説明したマニュアルです。

なお、本マニュアルは、以下の環境に対応した内容になっています。画面イメージは、ご利用のOS、ブラウザによっては本マニュアルの画面と多少異なる場合がありますのでご注意ください。

※ご利用のOSにより、サポートの対象となるWebブラウザが異なります。

【OS】		【Webブラウザ】
Microsoft Windows 10	/	Microsoft Edge
Microsoft Windows 10	/	Google Chrome
Microsoft Windows 11	/	Microsoft Edge
Microsoft Windows 11	/	Google Chrome

2 電子証明書について

電子証明書は、弊社サービスご利用の際に必ず必要となります。電子証明書が設定されているパソコンからのみ、弊社サービスのご利用が可能となります。また、証明書はご利用者個人に対して発行いたしますので、ご利用者の変更があった場合は、速やかに弊社コールセンターまでご連絡ください。

- 電子証明書の有効期限は3年間です。
- 万一、証明書が壊れたり、紛失したりした場合は、再発行いたします(無償)。

その他、電子証明書についてご不明な点がございましたら、弊社コールセンターまでお問い合わせください。

3 証明書の発行（ダウンロード）手順

1. 証明書のインストールには、次の2通のメールに記載の情報が必要になりますので、お手元にご用意ください。メールが手元に届かないなど、ご不明点がございましたら、弊社コールセンターまでお問い合わせください。

① 証明書発行メール(以下のいずれかの件名のメールが送信されます)

- 【オージス総研】証明書発行案内(URL 通知)
- 【オージス総研】証明書更新案内(URL 通知)

② パスワード通知メール

- 【オージス総研】証明書発行案内(パスワード通知)

2. 手順1の①[証明書発行メール]に記載の証明書発行サイトのURLにアクセスすると、下の画面が表示されます。[証明書発行メール]に記載のユーザIDと手順1の②[パスワード通知メール]に記載のパスワードを入力し、『ログイン』ボタンをクリックしてください。

オージス総研電子証明書発行サービス	
認証情報の入力	お問い合わせ
ユーザID パスワード ログイン	オージス総研イーキューブネットコールセンター メールアドレス: support@ecubenet.com

3. クライアント証明書のダウンロードを行います。

「Step1 クライアント証明書のダウンロード」下部の「ダウンロード」ボタンをクリックしてください。

オージス総研電子証明書発行サービス

Step 1 クライアント証明書のダウンロード

まず始めに電子証明書導入マニュアルを[こちら](#)からダウンロードしてください。

「ダウンロード」ボタンを押して、クライアント証明書をダウンロードしてください。この処理には数分掛かることがあります。

ダウンロードしたクライアント証明書は電子証明書導入マニュアルを参照のうえ、インストールしてください。



**インストールが完了するまで、
ブラウザを閉じずにご対応ください。**

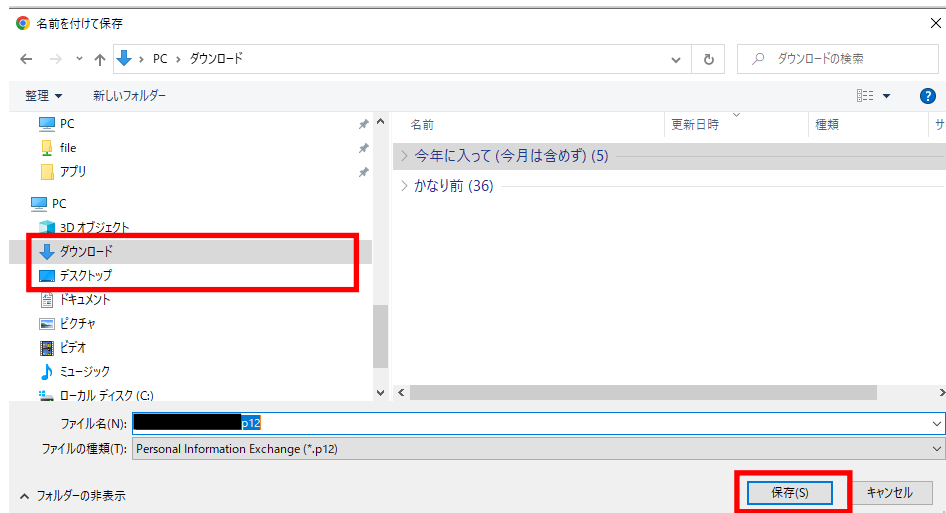
Google Chromeの場合：

証明書を保存する場所を選択するダイアログが表示されます。

ご利用者様にて保存場所を決定ください。

※ファイル名は変更しないでください。

※保存場所についてはダウンロードもしくはデスクトップを推奨いたします。



※上記ダイアログはブラウザの設定により表示されないこともございます。

ダウンロード後は、画面左下に以下のダイアログが表示されますので、赤枠を選択し、証明書のインポート作業(p.9)へ進んでください。



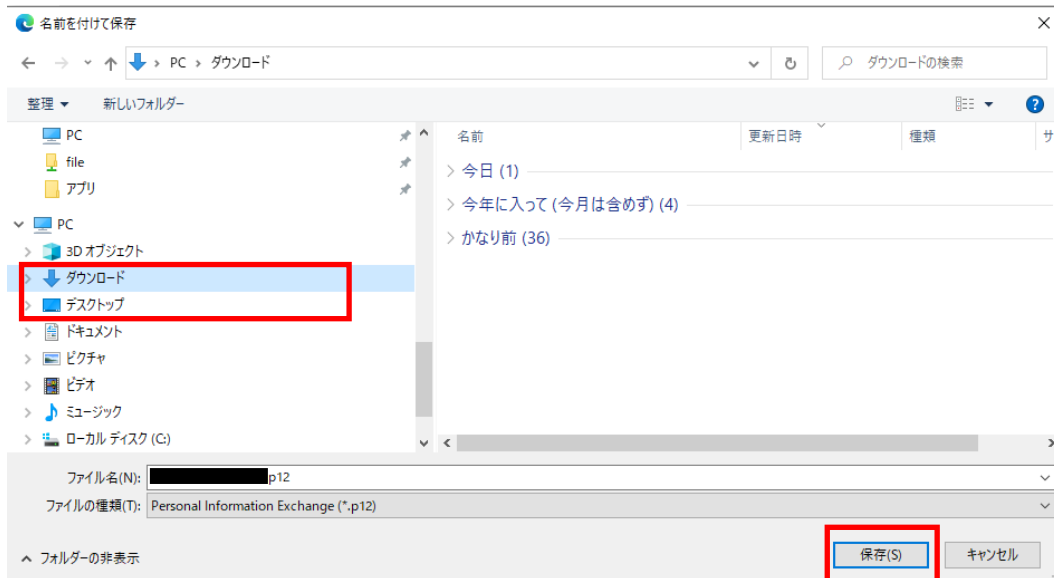
Microsoft Edgeの場合：

証明書を保存する場所を選択するダイアログが表示されます。

ご利用者様にて保存場所を決定ください。

※ファイル名は変更しないでください。

※保存場所についてはダウンロードもしくはデスクトップを推奨いたします。



保存完了後、画面右上にダウンロードされたファイルが表示されます。

「ファイルを開く」を選択し、証明書のインポート画面(p.9)へ進んでください。

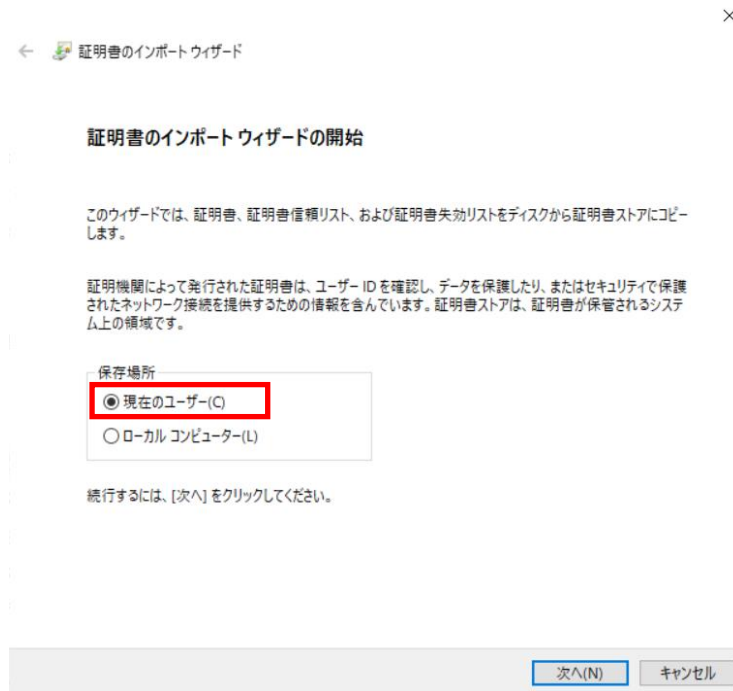


上記画面が表示されない、もしくは消えてしまった場合は、下記操作にてご確認ください。

手順: 画面右上の「…」→「ダウンロード」を選択。



「証明書のインポートウィザード」が表示されることを確認します。

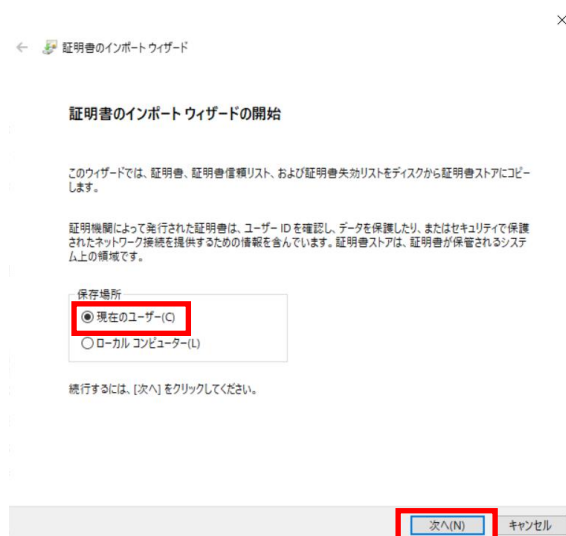


以上で証明書のダウンロードは完了となります。

続いて、クライアント証明書のインストールを実施してください。

4. ダウンロード済みのクライアント証明書をインストールします。

「証明書のインポートウィザード」が表示されるので、「現在のユーザ」を選択し「次へ」をクリックします。



「インポートする証明書ファイル」画面が表示されるので、「次へ」をクリックします。

×

← 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): 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

「パスワード」画面が表示されるので、パスワード情報を入力します。

1. 「パスワード」に手順1の②[パスワード通知メール]に記載のパスワードを入力します。
2. 「秘密キーの保護を強力にする」にチェックが入っていないことを確認します。
3. 「このキーをエクスポート可能にする」にチェックが入っていないことを確認します。
4. 「すべての拡張プロパティを含める」にチェックが入っていることを確認します。
5. 「次へ」をクリックします。

×

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

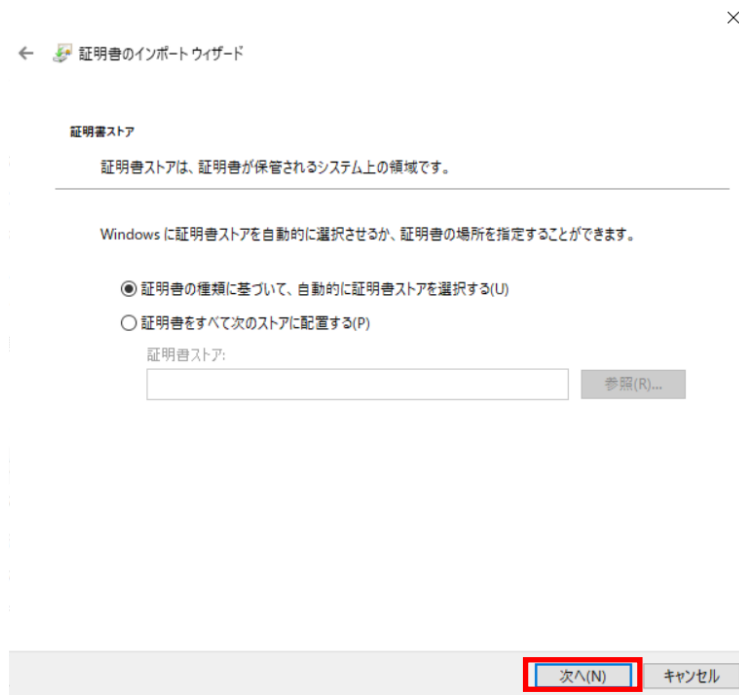
パスワード(P): ☐ パスワードの表示(D)

インポート オプション(I):

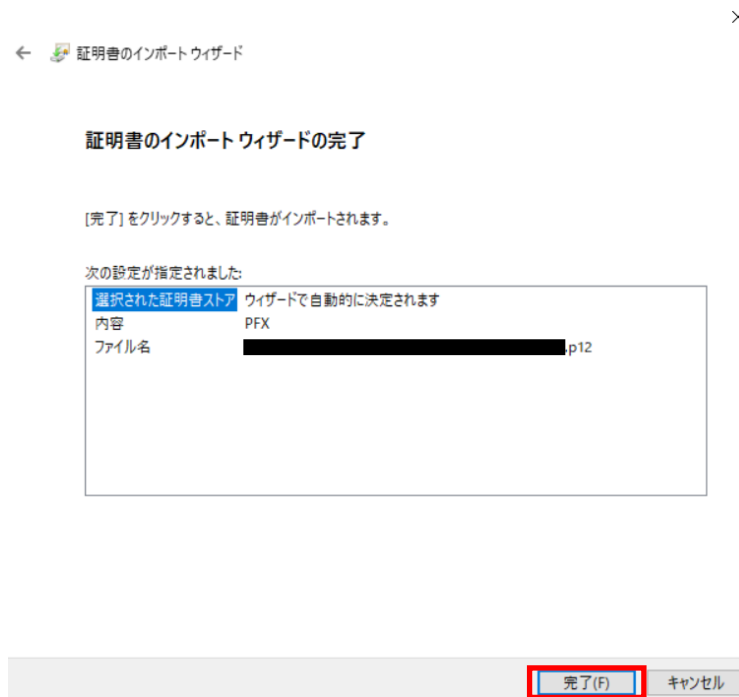
- ☐ 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- ☐ このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- ☐ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- ☒ すべての拡張プロパティを含める(A)

次へ(N) キャンセル

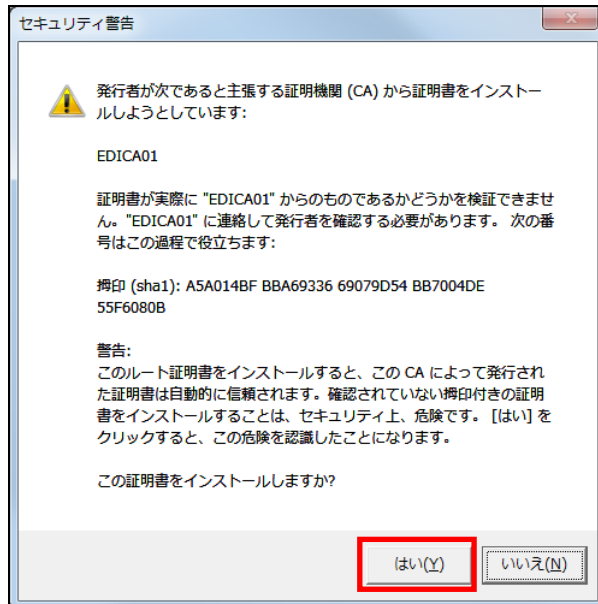
「証明書ストア」画面が表示されるので、「次へ」をクリックします。



「証明書のインポートウィザードの完了」が表示されるので、「完了」をクリックします。

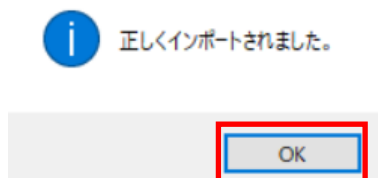


「セキュリティ警告」が表示されるので、「はい」をクリックします。



「正しくインポートされました。」と表示されるので、「OK」をクリックします。

証明書のインポートウィザード ×



以上でクライアント証明書のインストールは完了です。

続いて、クライアント証明書のインストール完了確認を実施してください。

5. クライアント証明書のインストール完了確認を行います。

Google Chromeの場合：

[1] 画面右上部の[⋮]→[設定]を選択します。



[2] [セキュリティとプライバシー] の [セキュリティ] をクリックします。



[3] [証明書の管理]をクリックします。



[4] 証明書管理画面が表示されます。

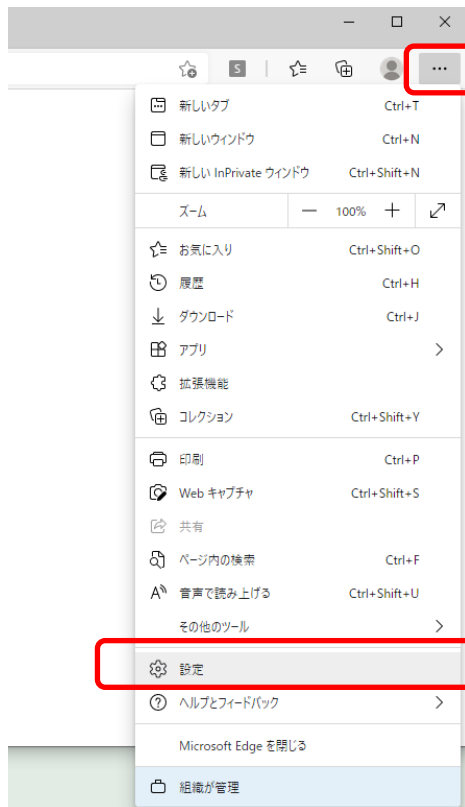
※複数証明書が入っている場合は下記の証明書の確認を行ってください。

- ・ 発行元:ご自身の名前(ローマ字表記)
- ・ 発行者:EDICA01
- ・ 有効期限:インストール日から3年後の日付



Microsoft Edgeの場合：

[1] 画面右上部の[⋮]→[設定]を選択します。



[2] [プライバシー、検索、サービス]の[証明書の管理]をクリックします。



[3] 証明書管理画面が表示されます。

※複数証明書が入っている場合は下記の証明書の確認を行ってください。

- ・ 発行元:ご自身の名前(ローマ字表記)
- ・ 発行者:EDICA01
- ・ 有効期限:インストール日から3年後の日付

発行先	発行者	有効期限	フレンドリ名
	EDICA01	2022/12/02	

【補足】「ファイルを開く」で「証明書のインポートウィザード」が表示されない場合

Google Chromeの場合：

[1] 画面右上部の[⋮]→[設定]を選択します。



[2] [セキュリティとプライバシー] の [セキュリティ] をクリックします。



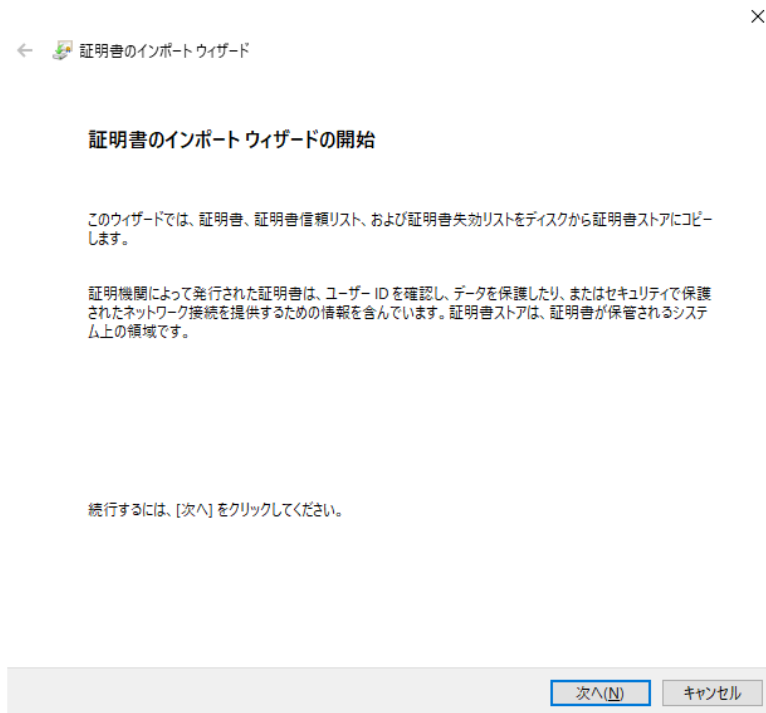
[3] [証明書の管理]をクリックします。



[4] [インポート]をクリックします。

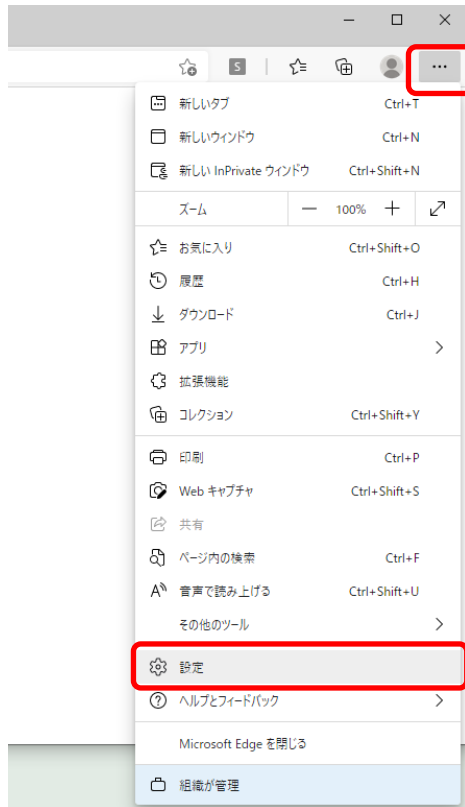


- [5]「証明書のインポートウィザード」が表示されるので、「次へ」をクリックして、次の画面の[参照...]でダウンロードしたファイルを指定します。
- (以降は、前述の操作と同様となります。)
- ダウンロードしたファイルが見当たらない場合は、「【補足】ダウンロードした証明書がどのフォルダにあるかわからない場合」(p.22)をご確認ください。



Microsoft Edgeの場合：

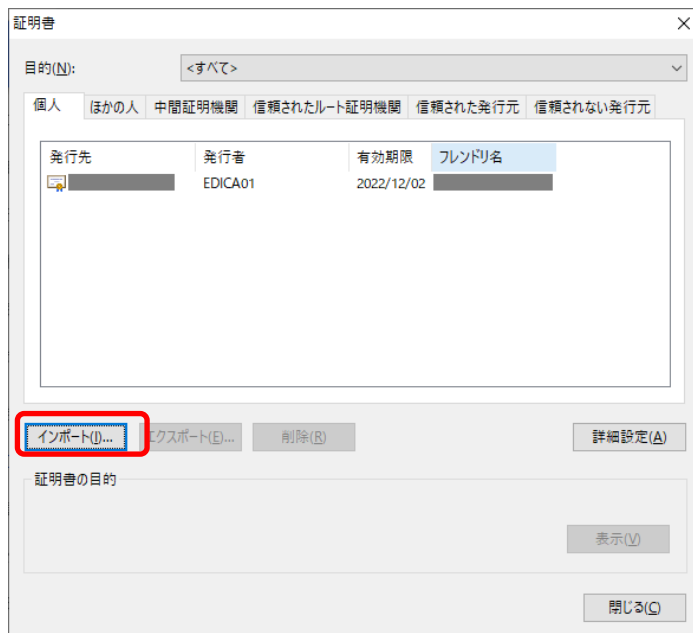
[1] 画面右上部の[⋮]→[設定]を選択します。



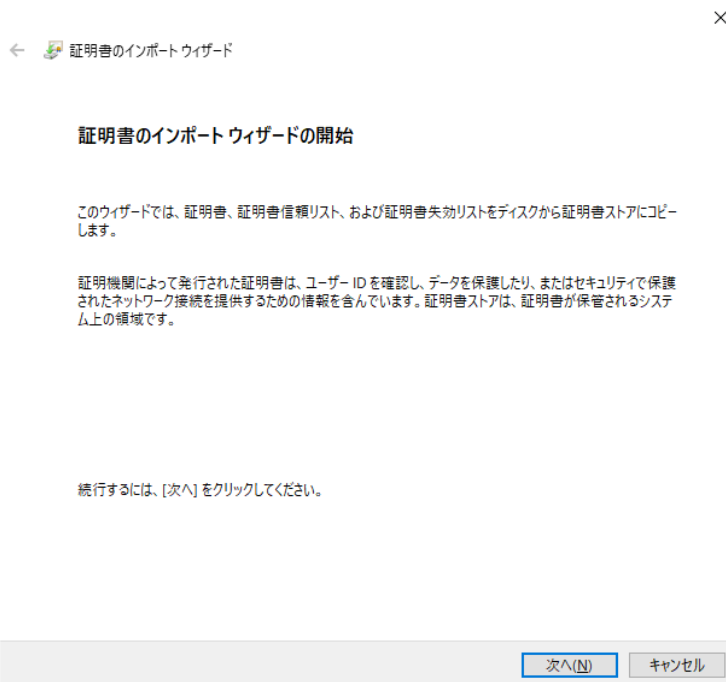
[2] [プライバシー、検索、サービス]の[証明書の管理]をクリックします。



[3] [インポート]をクリックします。



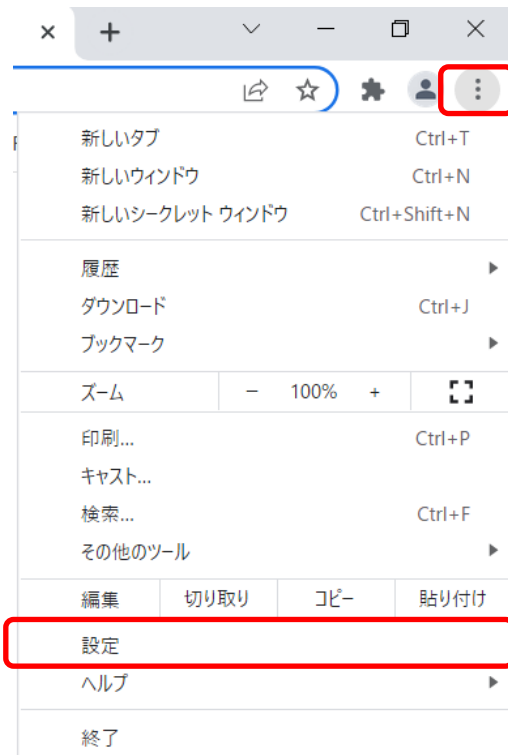
[4] 「証明書のインポートウィザード」が表示されるので、「次へ」をクリックして、次の画面の[参照...]でダウンロードしたファイルを指定します。
(以降は、前述の操作と同様となります。)
ダウンロードしたファイルが見当たらない場合は、「【補足】ダウンロードした証明書がどのフォルダにあるかわからない場合」(p.22)をご確認ください。



【補足】ダウンロードした証明書がどのフォルダにあるかわからない場合

Google Chromeの場合：

[1]画面右上部の[⋮]→[設定]を選択します。



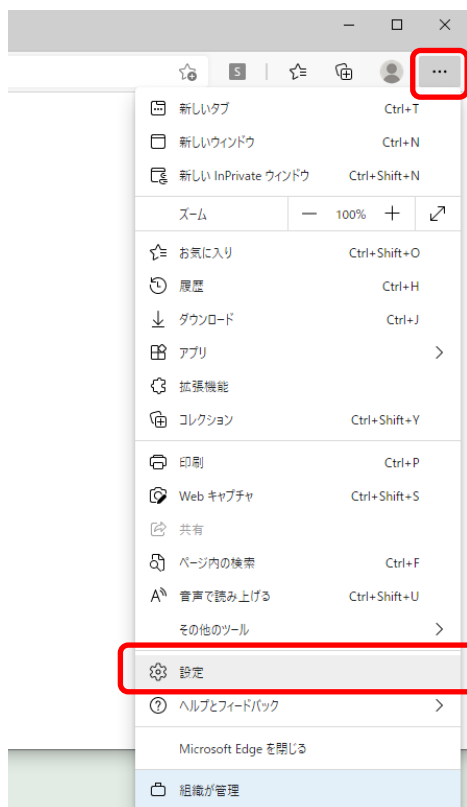
[2]ダウンロードを選択し、保存先に表示されているフォルダパスをご確認ください。

※ファイル名は「OGIS-xxxxxx-xxxxx.p12」となります。(xには数字が入ります)



Microsoft Edge の場合：

[1] 画面右上部の[⋯]→[設定]を選択します。



[2] [ダウンロード]を選択し、保存先に表示されているフォルダパスをご確認ください。

※ファイル名は「OGIS-xxxxxx-xxxxx.p12」となります。(xには数字が入ります)

