1. 電子証明書のインストール手順（MicrosoftEdge 又は GoogleChrome）

1-1. 「証明書発行案内」のメールを受信していることを確認してください。

メール件名：証明書発行案内　　差出人：ca-support@ml.secom-sts.co.jp

認証情報パスワードを受領した時点で、メールの受信ができていない場合は、お手数ですが Medicertified 電子証明書認証局(pki-info@medis.or.jp)までご連絡下さい。

MEDIS-×××××　様

電子証明書の発行登録を受付けましたので、証明書発行サイトの URL をお知らせ致します。

以下の URL へアクセスし、電子証明書の発行を行ってください。

https://webra2.secomtrust.net/scira/Entrance.jsp?XXXXXXXXXXX

●URL は大切な情報です。他人に情報が漏れないよう十分ご注意ください。

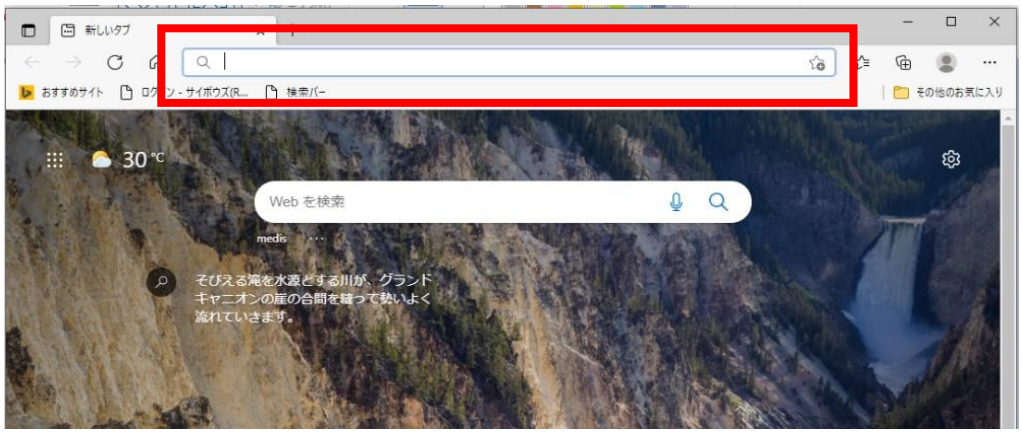
●証明書発行に関するご質問は、管理者様宛にお願いいたします。

※本メールは自動送信されています。返信なされませんよう、宜しくお願いいたします。

- URL は**ワンタイム URL** になっています。メールを受信してから **30 日以内**に電子証明書のダウンロードを行ってください。
- 証明書発行サイトから証明書をダウンロードできるのは **1 回のみ**となります。
- **ダウンロードを実施した日が**、電子証明書の**有効期間の開始日**となります。

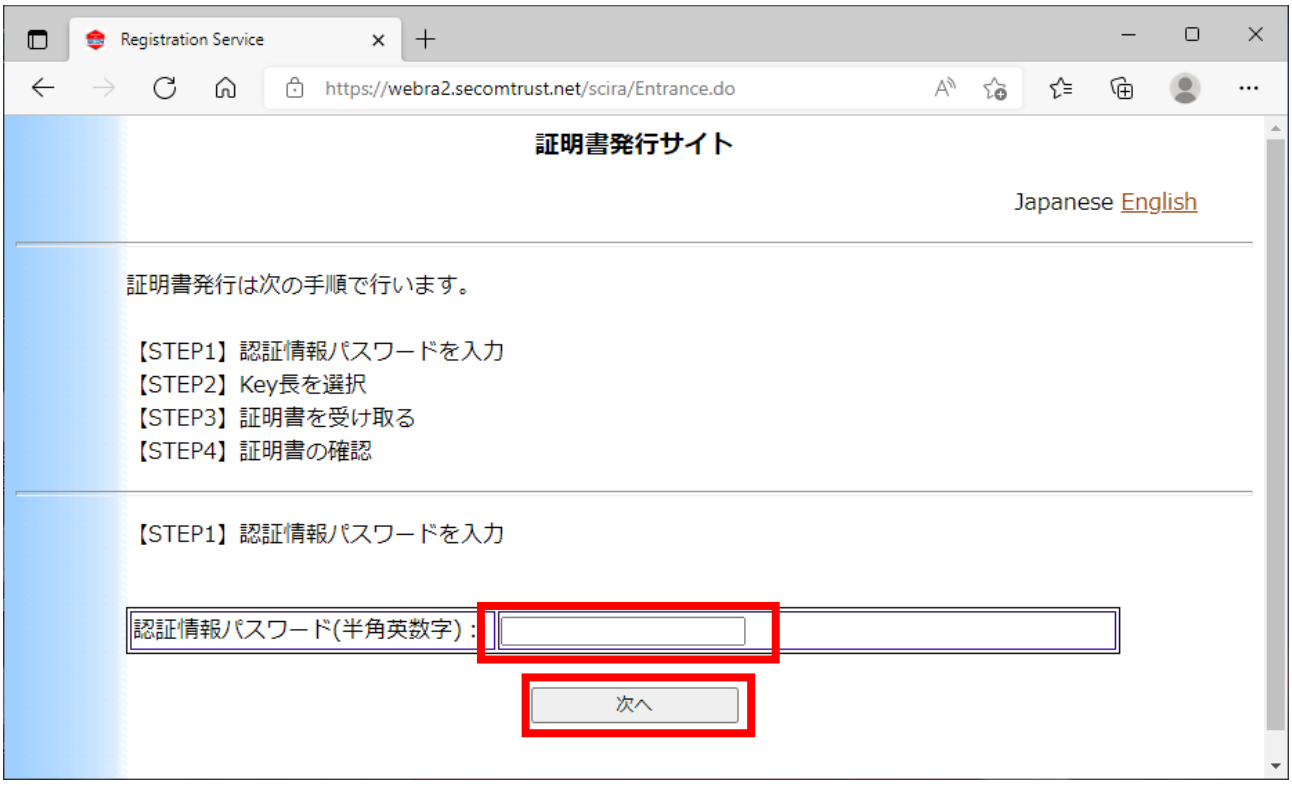
1-2. Microsoft Edge または Google Chrome のアドレスバーに「証明書取得用 URL」を入力して、発行サイトにアクセスしてください。「証明書取得用 URL」は、証明書発行案内メールに記載されています。

（画面例は Edge です）



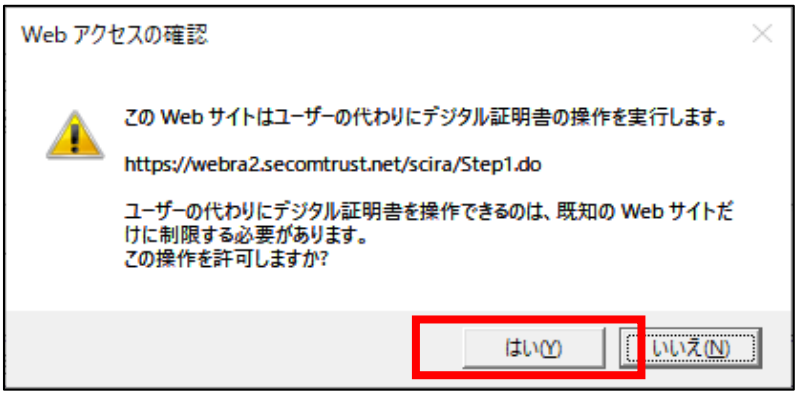
1-3. 証明書情報パスワードの欄に「認証情報パスワード」を入力して「次へ」をクリックしてください。

ブラウザへのパスワードの保存は必要ありません



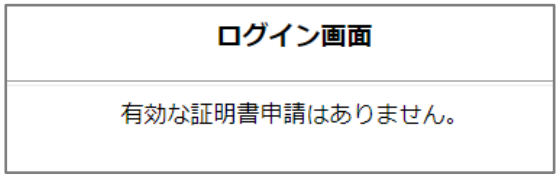
画面推移の途中で下記の画面が表示された場合は、「はい」をクリックしてください。

（この画面は表示されない場合もあります）



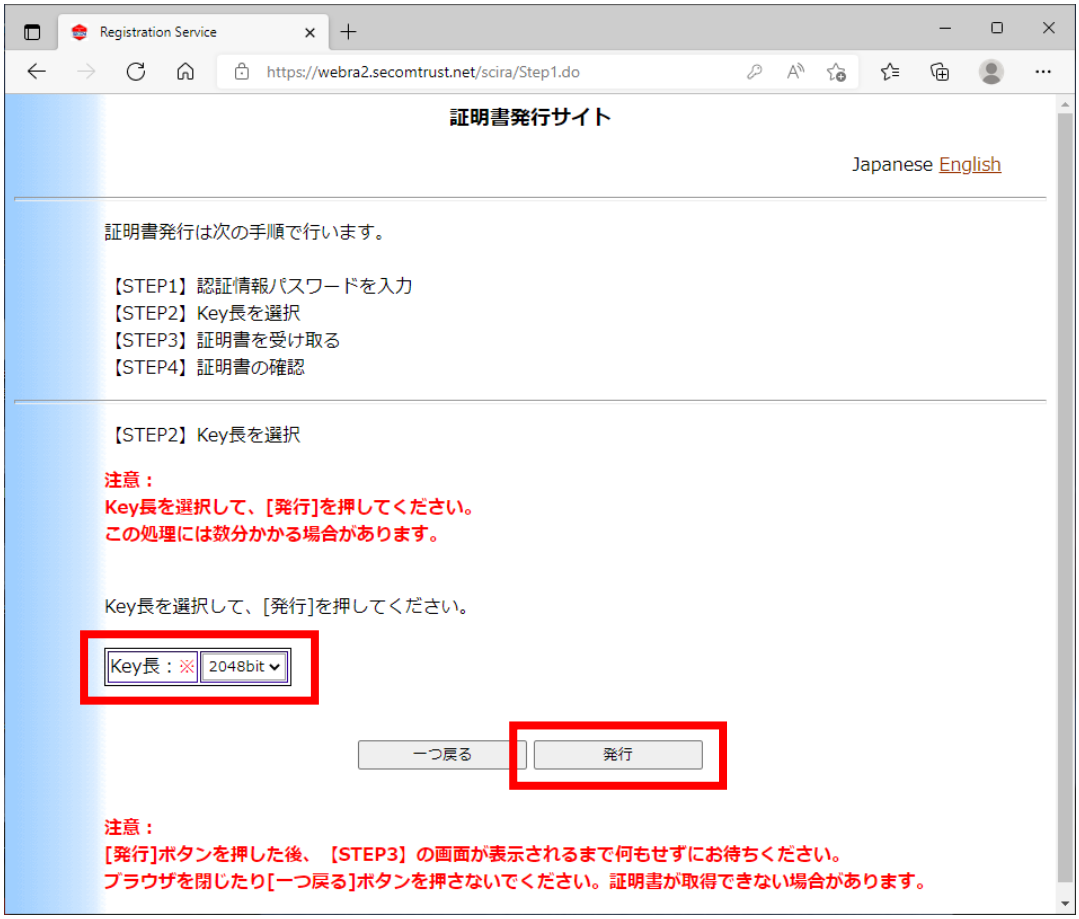
発行サイトへアクセスしたとき、すでに電子証明書ファイルがダウンロードずみの場合は下記の画面が表示されます。

（理由：電子証明書ファイルのダウンロードは 1 度しかできないため）



ダウンロードされたファイルがどこに保存されたのかわからなくなってしまった場合は、パソコン内を『EndUser.p12』のファイル名検索を行ってください。ダウンロードエラー等で、ファイルのダウンロードができなかった場合は、pki-info@medis.or.jp までお問い合わせください。

1-4. 「Key 長」の選択は『2048bit』として、「発行」をクリックしてください。



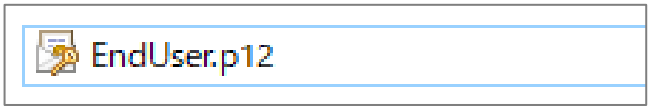
＜Microsoft Edge の場合＞　Google Chrome の場合は、次ページに記載

1-5. ダウンロードファイルを保存してください。

ファイル名は『EndUser.p12』です。

保存先に指定した場所にファイルがあるかを確認してください。

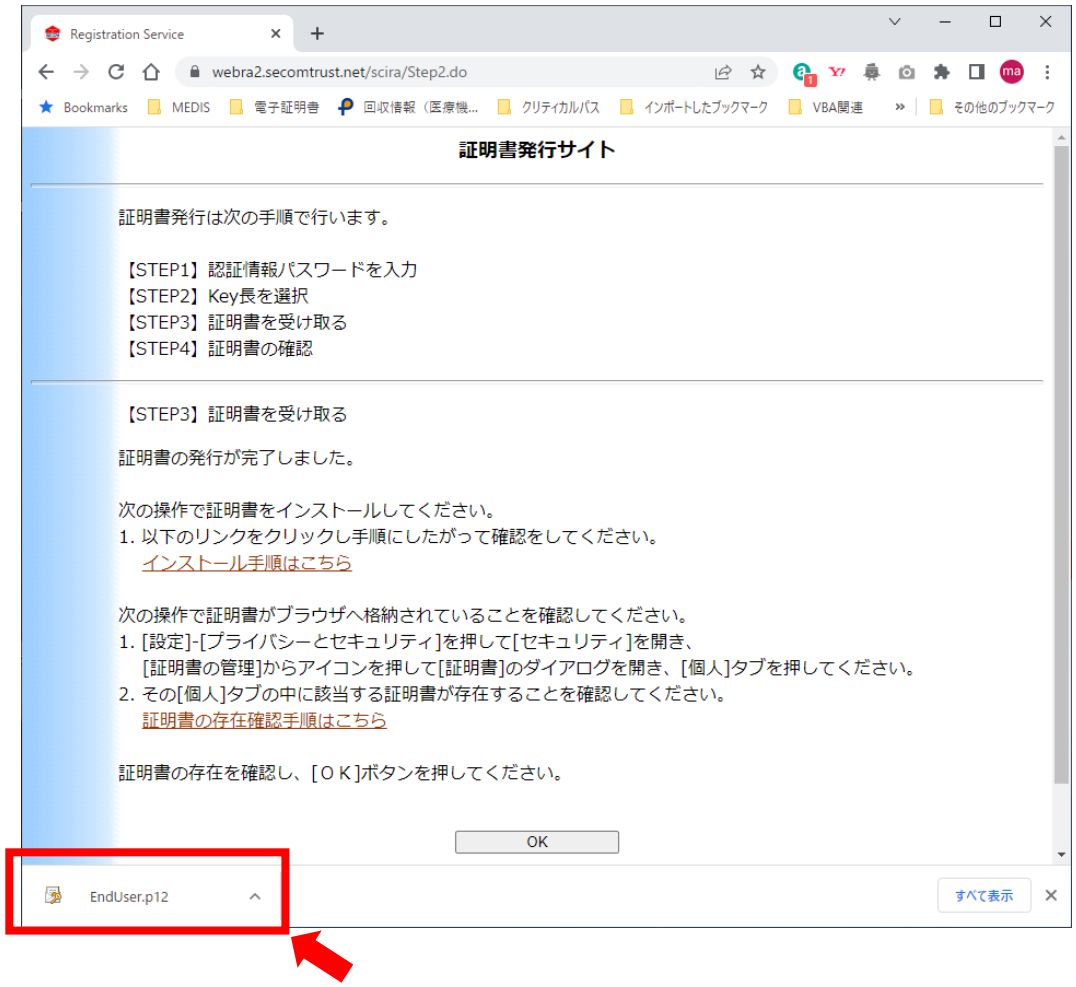
1-6. 保存されたファイルをクリックして開いてください。（次は（1-7）に進んでください）



＜Google Chrome の場合＞　Microsoft Edge の場合は前ページに記載

1-5. ダウンロードファイルを保存してください。

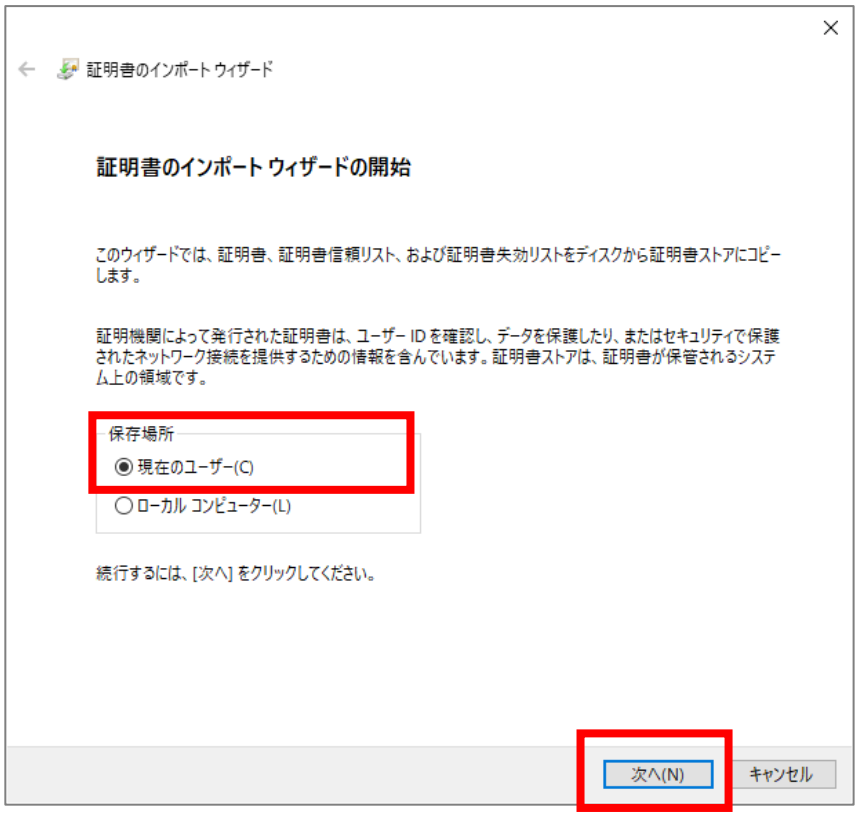
保存先を指定する画面が出たら、任意の場所を指定してください。



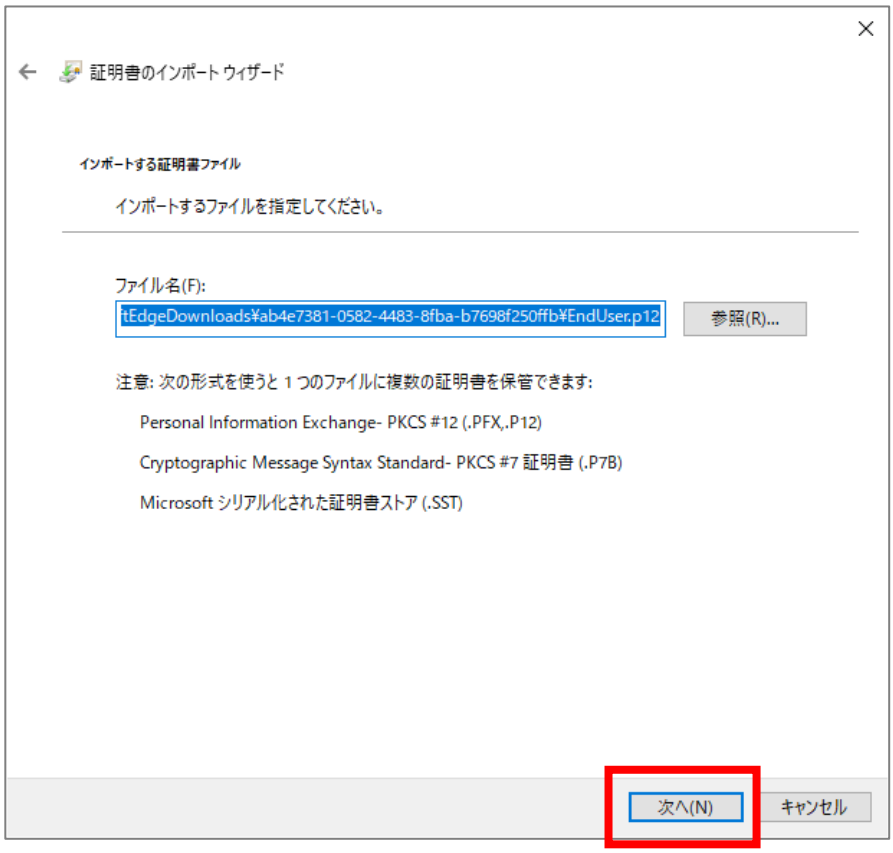
1-6. 『EndUser.p12』 をクリックして開いてください。

1-7. 『EndUser.p12』のファイルを開くと、インポートウィザード画面が表示されます。

保存場所は「現在のユーザ」を選択して、「次へ」をクリックしてください。

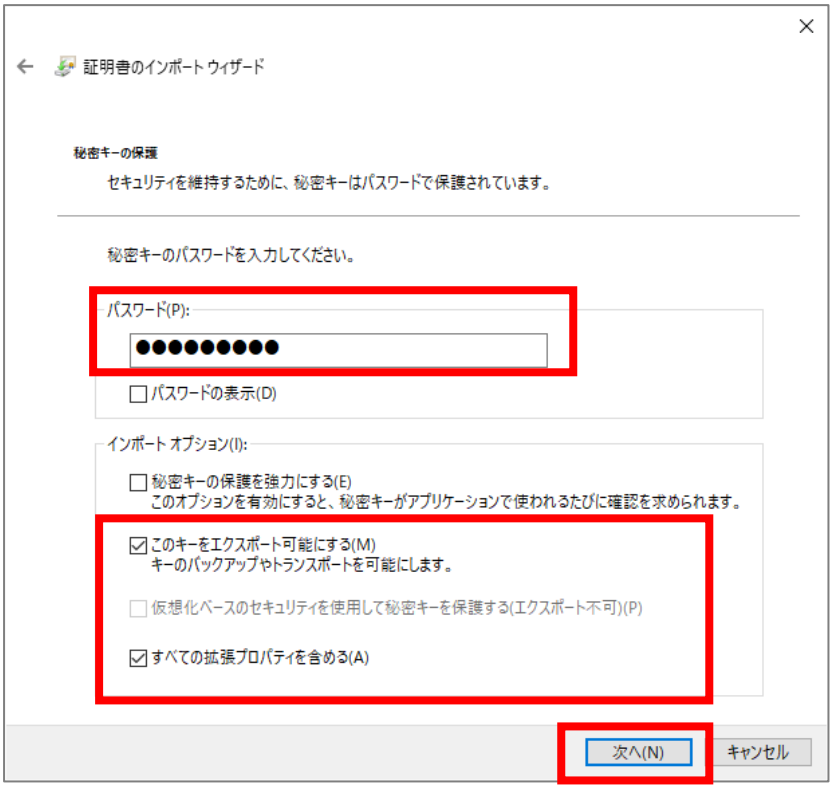


1-8. ファイル名に『EndUser.p12』 までのパスが表示されていることを確認して「次へ」をクリックしてください。



1-9. パスワードに 「認証情報パスワード」 を入力してください。大文字、小文字を区別します。

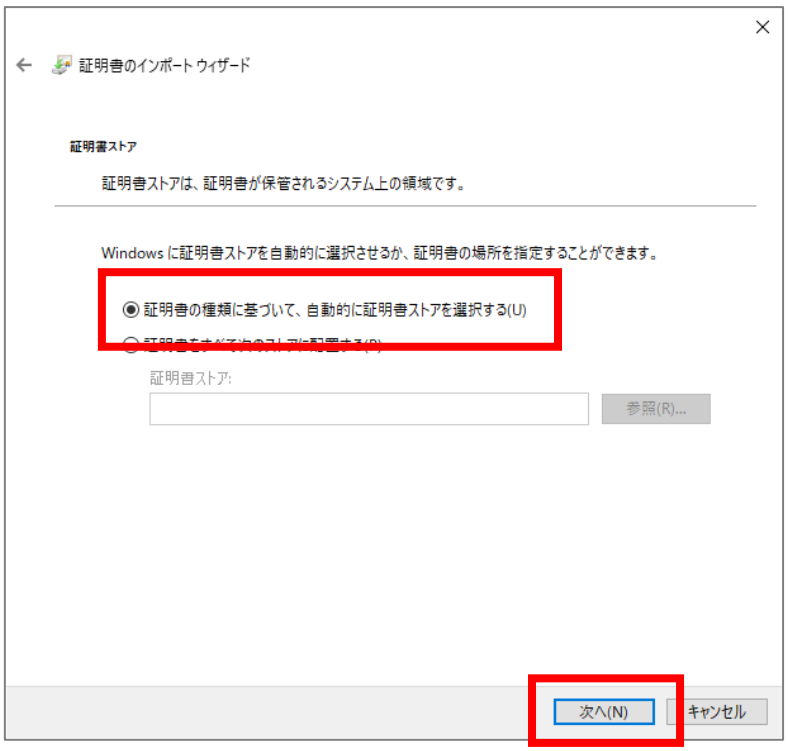
インポートオプションは、
「このキーをエクスポート可能にする」 と 「すべての拡張プロパティを含める」 にチェックを入れてください。
入力が終わったら 「次へ」 をクリックします。



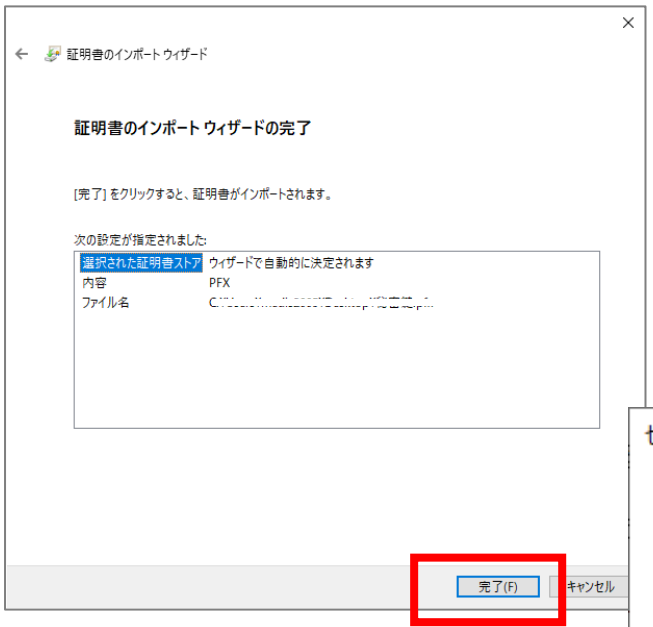
「このキーをエクスポート可能にする」 のオプションについて
初期値ではチェックが入っていません。チェック無の状態にすると、パソコンから秘密鍵（pfx ファイル）のエクスポートができなくなります。（エクスポートウィザードの画面で、「はい、秘密キーをエクスポートします」がグレーアウトして選択することができなくなります）

秘密キーをエクスポートするときに、「はい、秘密キーをエクスポートします」がグレーアウトして選択できない場合は、1-7 から 1-11 の手順をマニュアル通りに再度行ってください。

1-10.「証明書の情報に基づいて、自動的に証明書ストアを選択する」 を選択して「次へ」をクリックしてください。

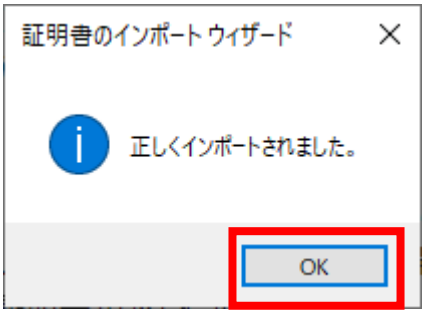


1-11.「完了」をクリックしてください。



画面推移の途中で下記の画面が表示された場合は、
「はい」をクリックしてください。
（この画面は表示されない場合もあります）

1-11. 「OK」をクリックしてください。



以上で電子証明書のインストールが完了しました。

※続けて、証明書情報の確認を行います。

バックアップについて

手順 1-5 で保存した 『EndUser.p12』ファイルは、電子証明書のバックアップファイルにすることができます。
その場合は、『EndUser.p12』ファイルを USB などの別の媒体に保存し、『認証情報パスワード』 とともに保管してください。
バックアップからの復元や、別のパソコンに、電子証明書をインストールしたい場合は、『EndUser.p12』ファイルをインストールしたいパソコン上で開いて、手順 1-7 からの操作を行ってください。

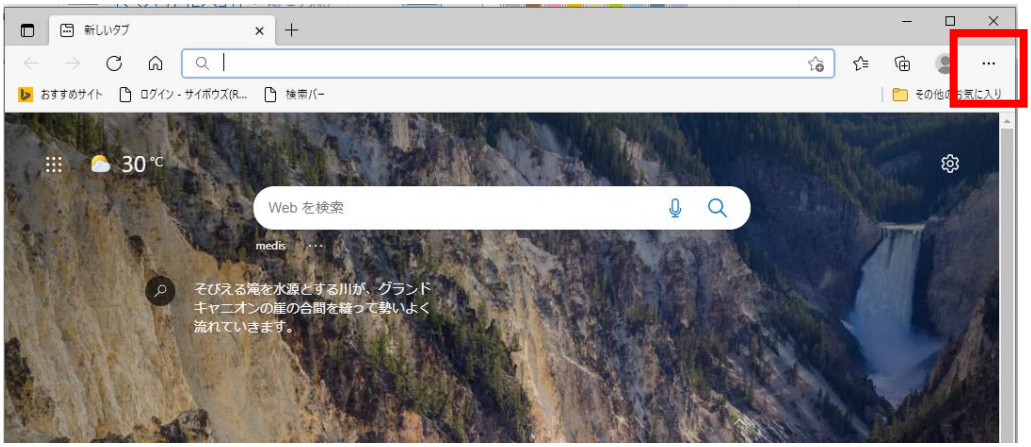
『EndUser.p12』ファイルが保存できていなかった場合　または　バックアップファイルを複製したい場合

手順は、P.17 の 「4. 秘密鍵のエクスポート手順」 を参照して、バックアップファイルを作成してください。
エクスポートした秘密鍵のファイルから電子証明書の復元を行う場合は、手順 1-7 からの手順において
『EndUser.p12』 は、秘密鍵のファイル名（任意で付けたファイル名）
「認証情報パスワード」 は、秘密鍵のエクスポート時に任意で決定したパスワード
にそれぞれ読み替えてください。

2. 電子証明書の確認手順（MicrosoftEdge 又は GoogleChrome）

＜Microsoft Edge の場合＞　Google Chrome の場合は、次ページに記載

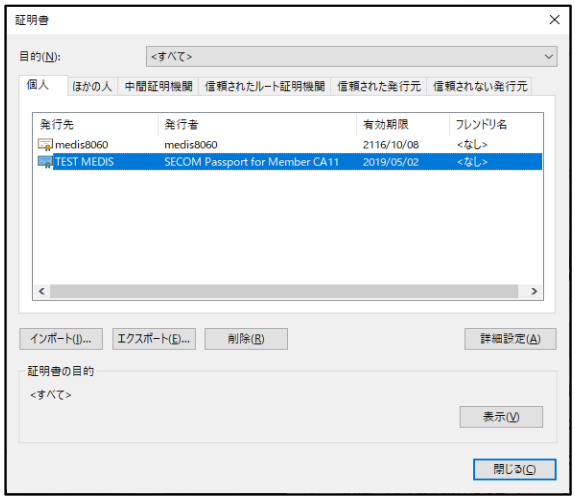
2-1. Edge を起動して右上の「…」をクリックします



2-2. 「設定」をクリックします

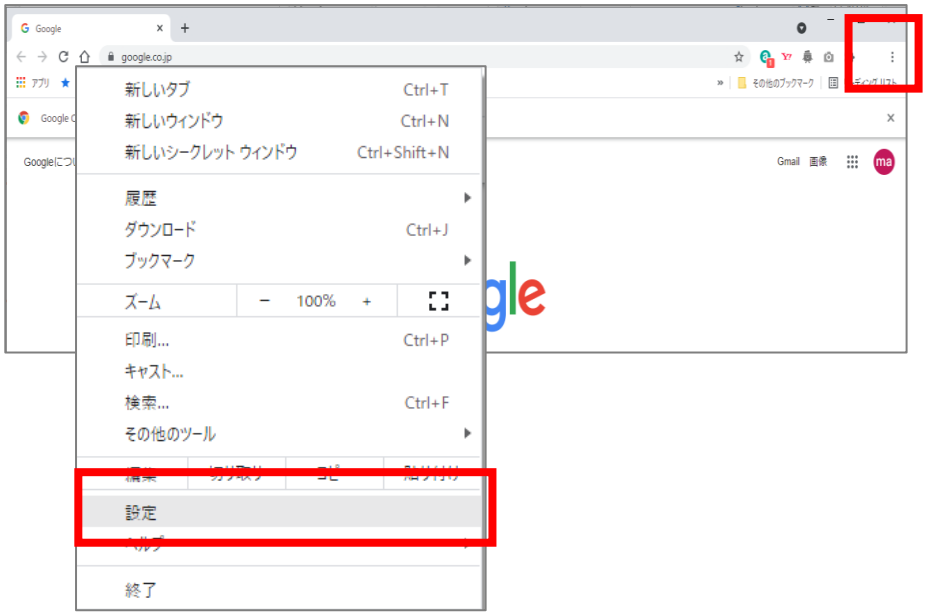
2-3. 「プライバシー、検索、サービス」をクリックします。
画面をスクロールして、「セキュリティ」にある「証明書の管理」をクリックします

2-4. 「証明書」画面が表示されます。（次は（2-5）に進んでください）

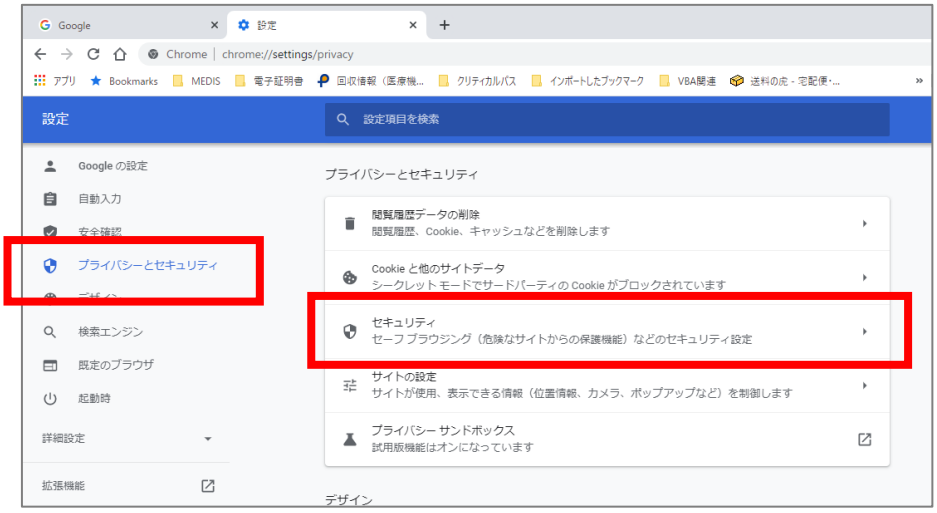


＜Google Chrome の場合＞　Microsoft Edge の場合は、前ページに記載

2-1．Chrome を起動して右上の「⋮」をクリックして、「設定」をクリックします。

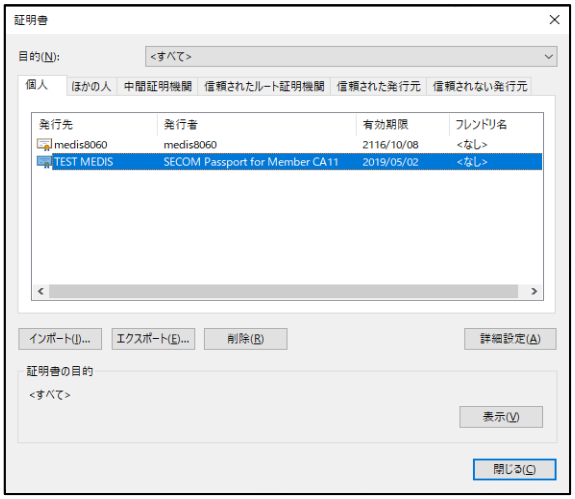


2-2．「プライバシーとセキュリティ」をクリックして、「セキュリティ」をクリックします。

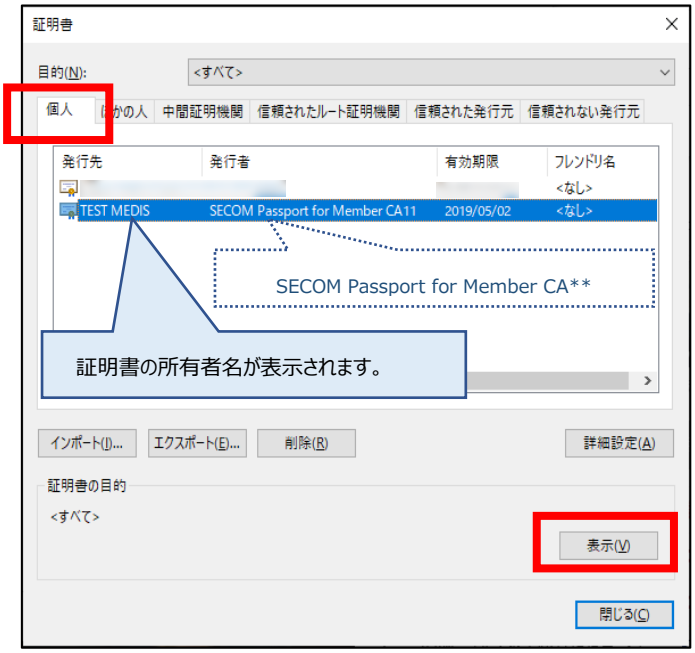


2-3．画面をスクロールして「証明書の管理」をクリックします。

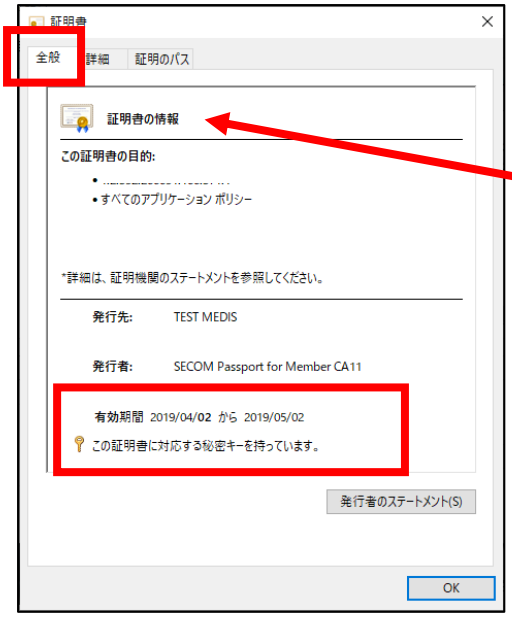
2-4．「証明書」画面が表示されます。



2-5. 「個人」タブに表示されている一覧の中から、インストールした証明書を選択して、「表示」をクリックします。

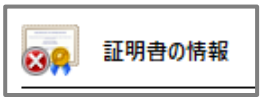


複数表示されて行場合は、発行者が SECOM Passport for Member CA** となっているものを探してください。
発行先には、証明書の所有者名が表示されます。
同一氏名の証明書が複数表示される場合は、有効期限を見て適宜判断してください。
※サーバー証明書の場合は、FQDN または IP アドレスが表示されます。



＜全般＞

有効期間を確認します

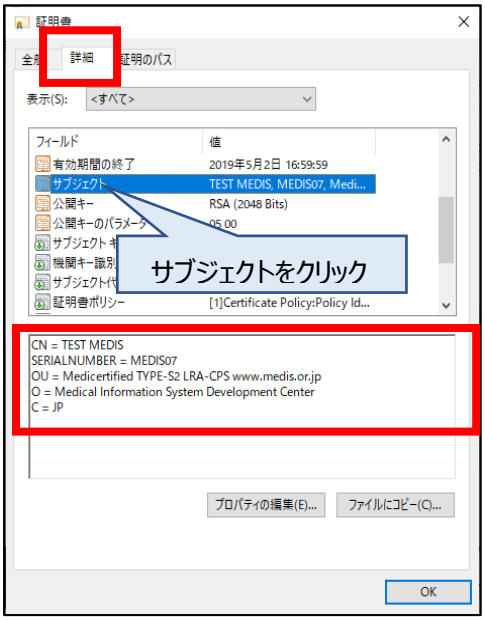


上図のように証明書のアイコンに赤い×印がつき、

「信頼された証明機関がこの証明書を確認できません。」

と表示されていた場合は、ルート証明書が正しくインストールされていません。

「EndUser.p12」のインポート(P.5～の手順)を再度実施してください。

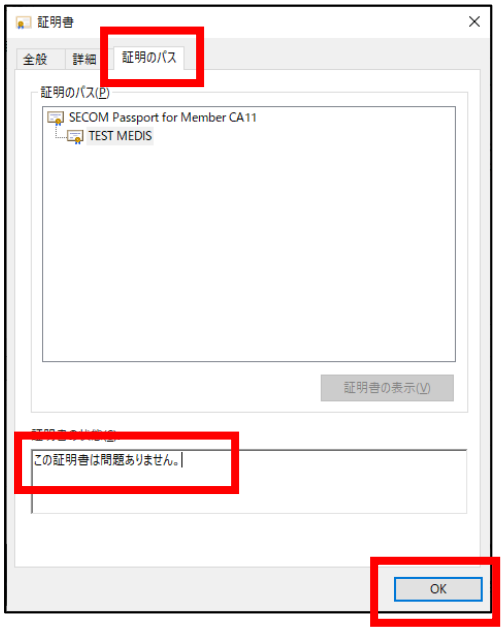


＜詳細＞

証明書の記載事項を確認します。

※サブジェクト代替名では、証明書の記載メールアドレスを確認できます。

記載事項の誤りがあった場合は Medicertified 電子証明書認証局(pki-info@medis.or.jp)までご連絡下さい。



＜証明書のパス＞

上段がルート証明書、下段がクライアント証明書(発行対象者の証明書)になります。

それぞれ、「この証明書は問題ありません」と表示されていることを確認します。

各画面の確認ができたら「OK」をクリックしてください。

記載事項の誤り等があった場合は、電子証明書認証局(pki-info@medis.or.jp)までご連絡下さい。

3. 公開鍵のエクスポート手順　公開鍵のエクスポートは何回でも行うことができます。

公開鍵のファイルは

◆法人代表者証明書の場合・・・PMDA に提出、または ICSR 受付サイトへの登録に必要なファイル

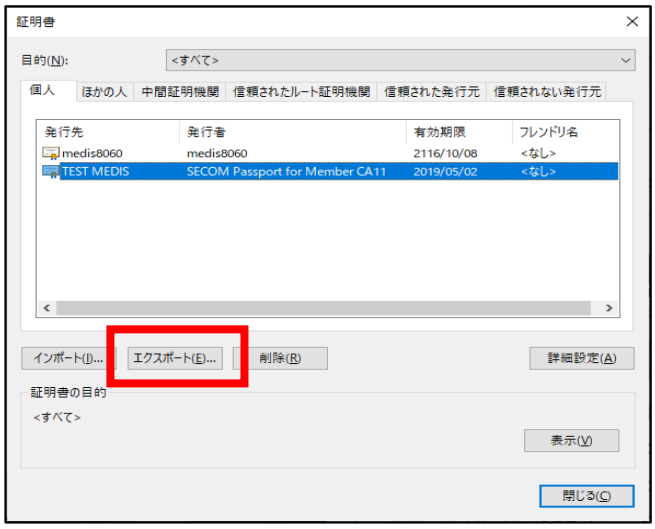
◆個人証明書の場合・・・申請電子データシステム（ゲートウェイシステム）のユーザ登録に必要なファイル

3-1.「個人」タブに表示されている一覧の中から、エクスポートする証明書を選択して「エクスポート」をクリックします。

下記画面の表示手順は、P.9 の

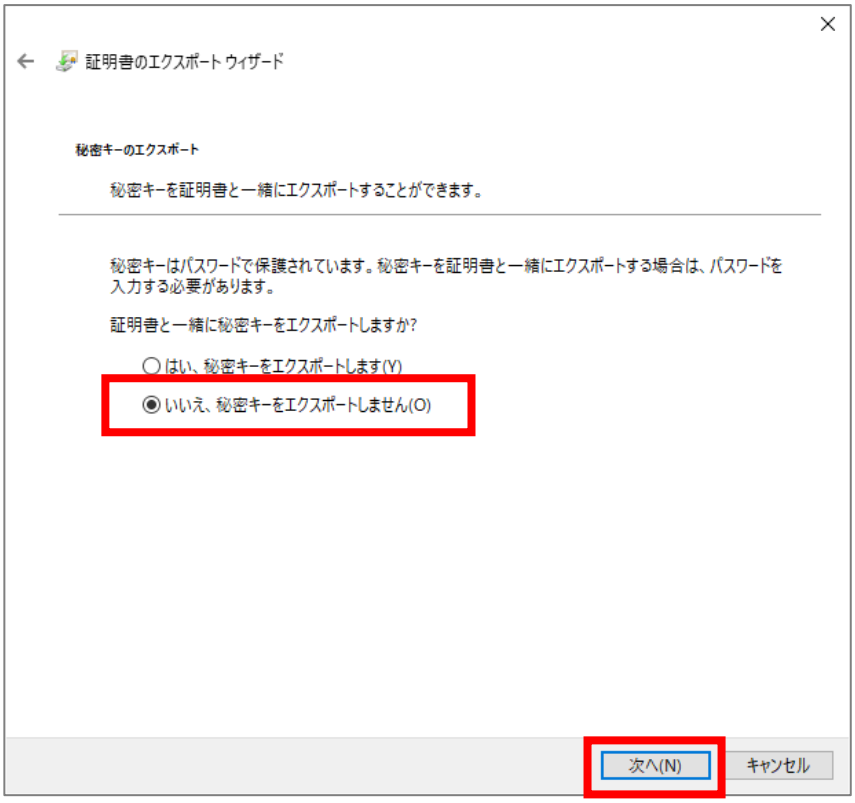
「2. 電子証明書の確認手順（MicrosoftEdge 又は GoogleChrome）」

を参照してください。

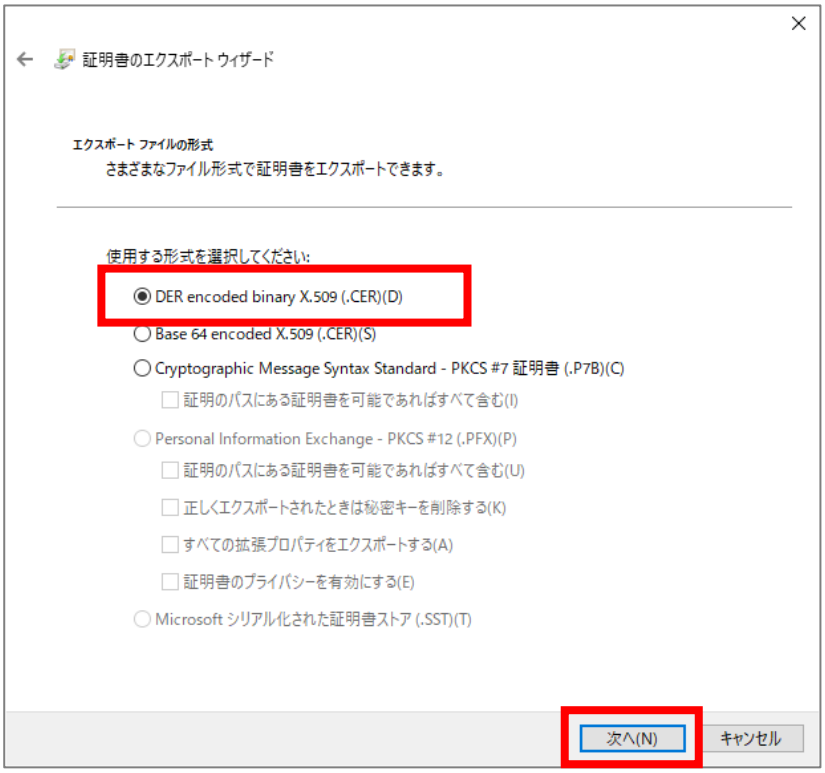


3-2. 証明書のエクスポートウィザードが表示されたら、「次へ」をクリックします。

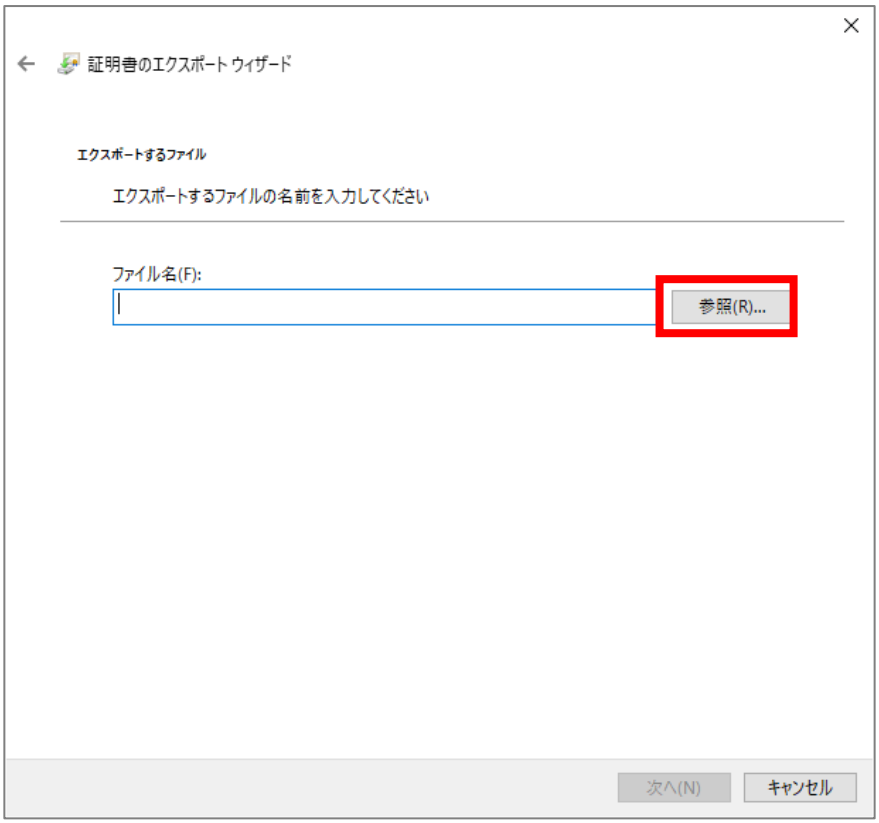
3-3. 証明書のエクスポートウィザードが表示されたら、「いいえ、秘密キーをエクスポートしません」を選択して「次へ」をクリックします。



3-4. 「DER encoded binary X.509」が選択されていることを確認して「次へ」をクリックします。

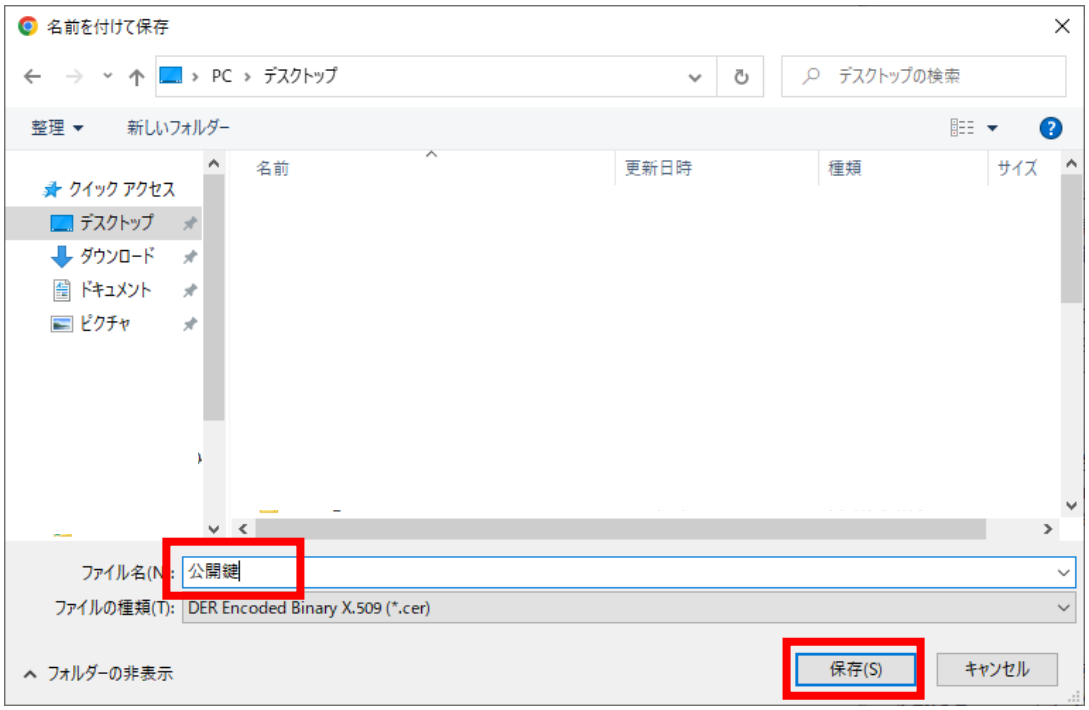


3-5. 参照ボタンをクリックして、任意の保存先とファイル名を指定してください。

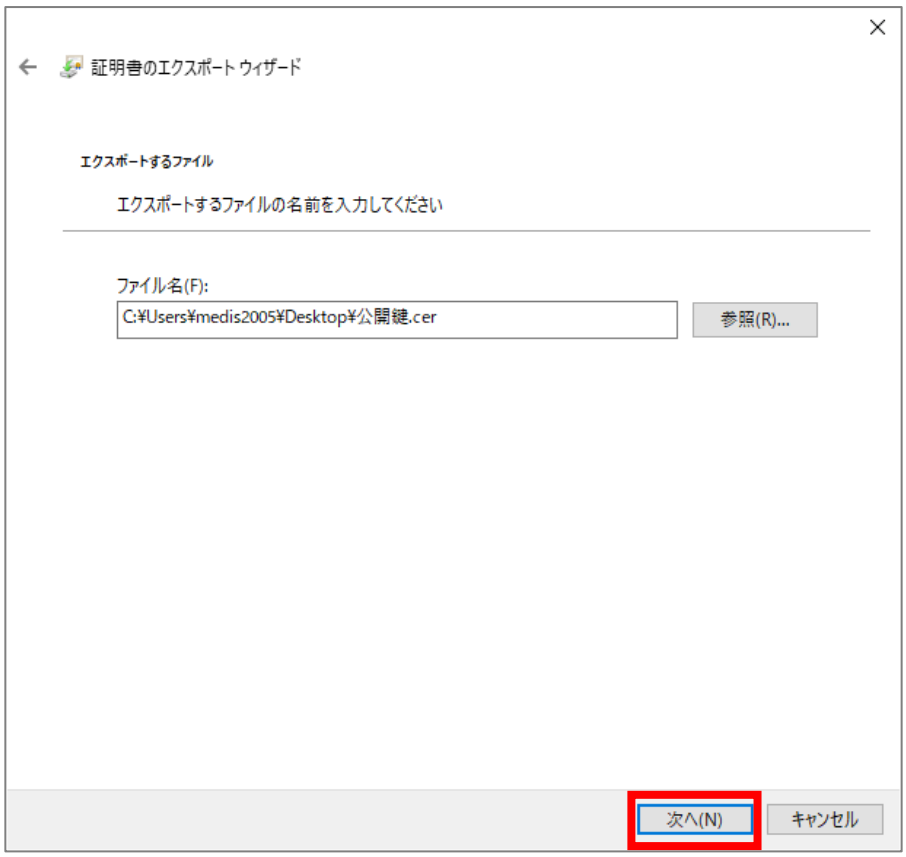


3-6. 保存先とファイル名を入れて「保存」をクリックします。

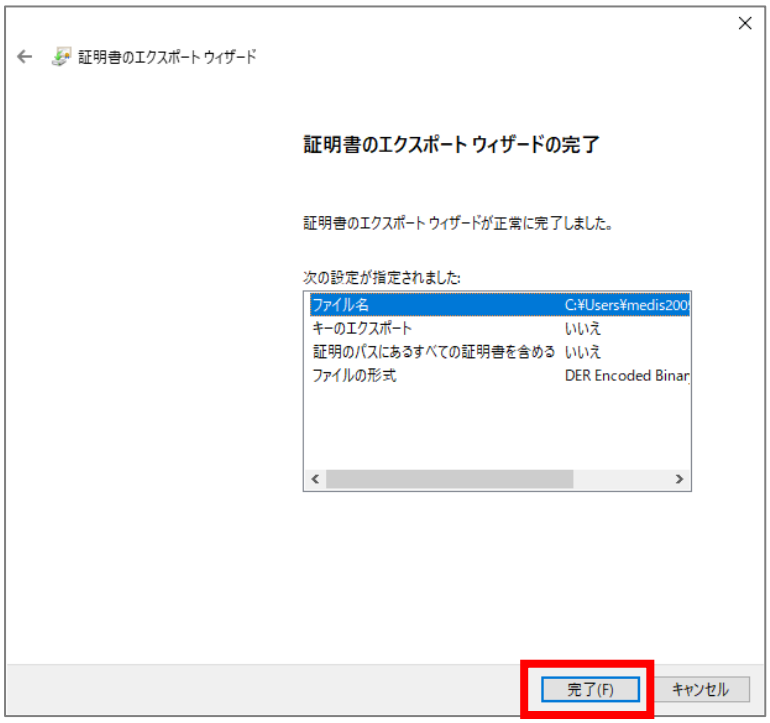
下図は、保存先：デスクトップ　ファイル名：公開鍵　とした例です

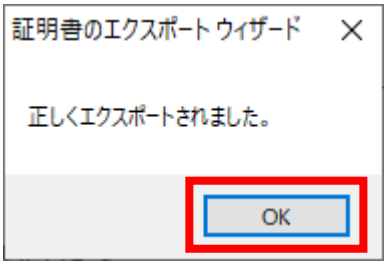


3-7．ファイル名に指定した保存先とファイル名が表示されていることを確認して「次へ」をクリックします。



3-8．「完了」をクリックして、「正しくエクスポートされました」の表示画面で「OK」をクリックします。





指定した場所にファイルが保存されていることを確認してください。ファイル名の後につく拡張子は 『 .cer 』になります。公開鍵のファイルは右記のアイコンで表示されます。

ファイル容量は 1KB 程度です。ダブルクリックすると証明書の所有者情報や有効期間の確認ができます

4. 秘密鍵のエクスポート手順

秘密鍵のエクスポートは何回でも行うことができます。エクスポートするたびにパスワードを変更することができます。

秘密鍵のファイルは

◆法人代表者証明書の場合・・・EDI ツールへの設定、または R3 署名・暗号化ツールへの設定に必要なファイル

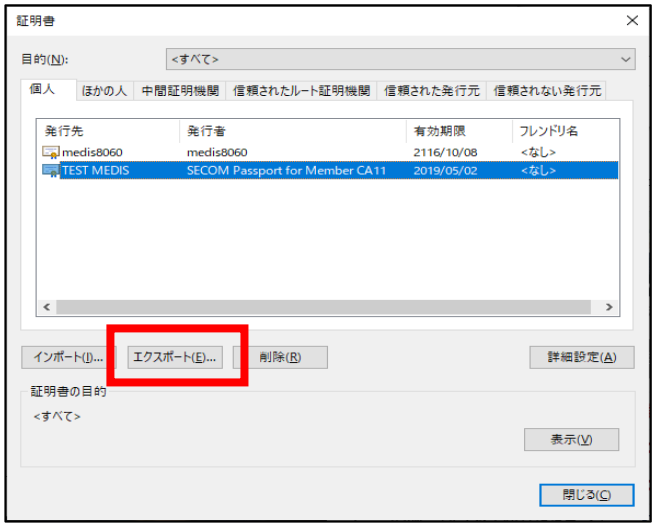
◆個人証明書の場合・・・申請電子データシステム（ゲートウェイシステム）を利用するパソコンにインポートするために必要なファイル

4-1. 「個人」タブに表示されている一覧の中から、エクスポートする証明書を選択して「エクスポート」をクリックします。

下記画面の表示の手順は、P.9 の

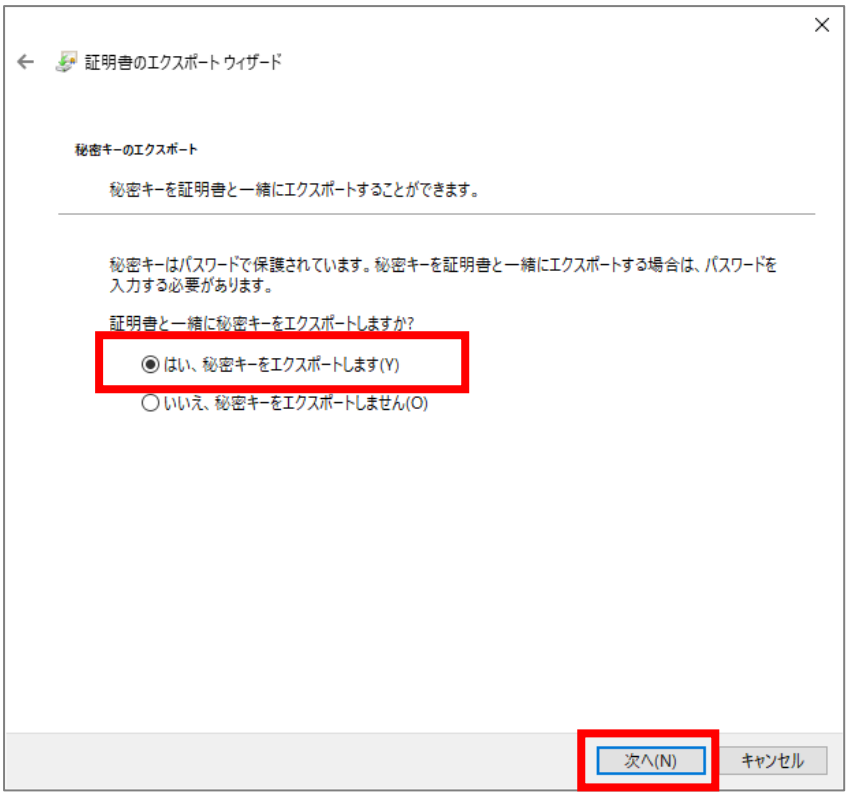
「2. 電子証明書の確認手順（MicrosoftEdge 又は GoogleChrome）」

を参照してください。



4-2. 証明書のエクスポートウィザードが表示されたら、「次へ」をクリックします。

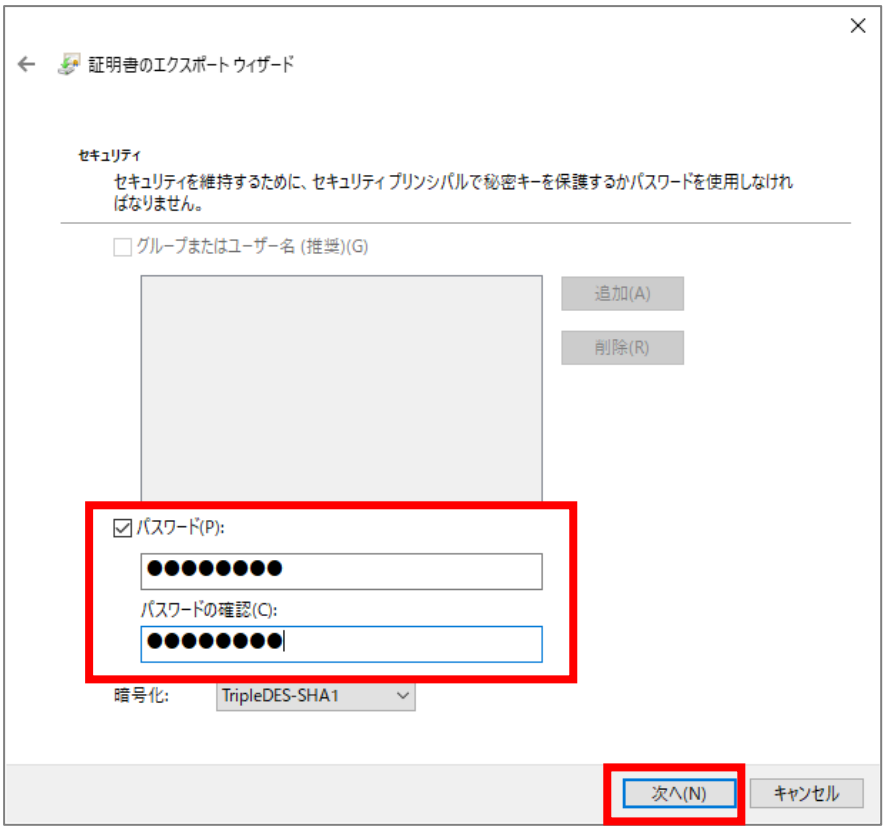
4-3. 証明書のエクスポートウィザードが表示されたら、「はい、秘密キーをエクスポートします」 を選択して、
「次へ」をクリックします。
「はい、秘密キーをエクスポートします」がグレーアウトして選択できなくなっている場合は、P.6 を参照してください。



4-4. 「Personal Information Exchange-PKCS #12(.pfx) 」 を選択し、
「証明のパスにある証明書を可能であればすべて含む」 と 「すべての拡張プロパティをエクスポートする」
にチェックを入れて「次へ」をクリックします。

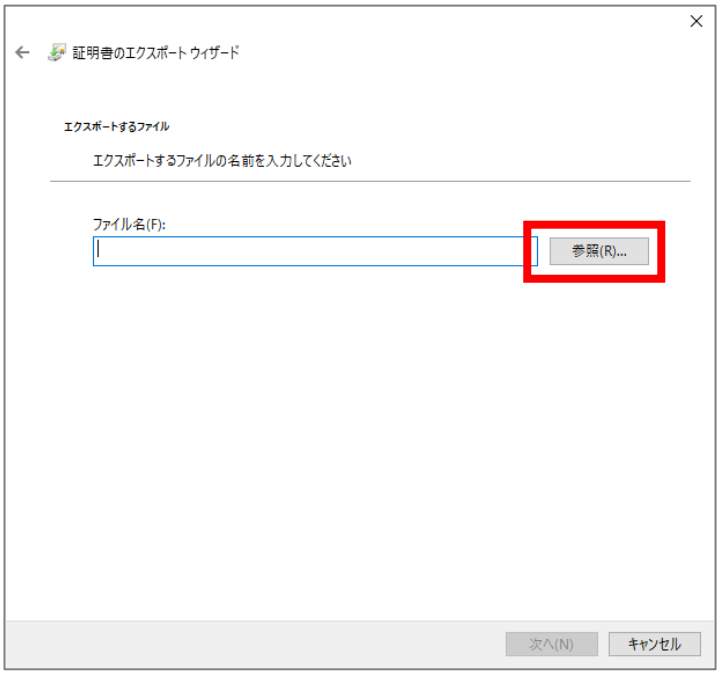
※「正しくエクスポートされたときは秘密キーを削除する」にはチェックを入れないでください。

4-5．パスワードにチェックを入れて、任意のパスワードを入力してください。パスワードの確認の欄にも同じパスワードを入力します。**ここで入力したパスワードは忘れないようにしてください。** 忘れてしまうと、エクスポートした証明書が使用できなくなります。
（その下にある「暗号化」は、そのままで結構です）



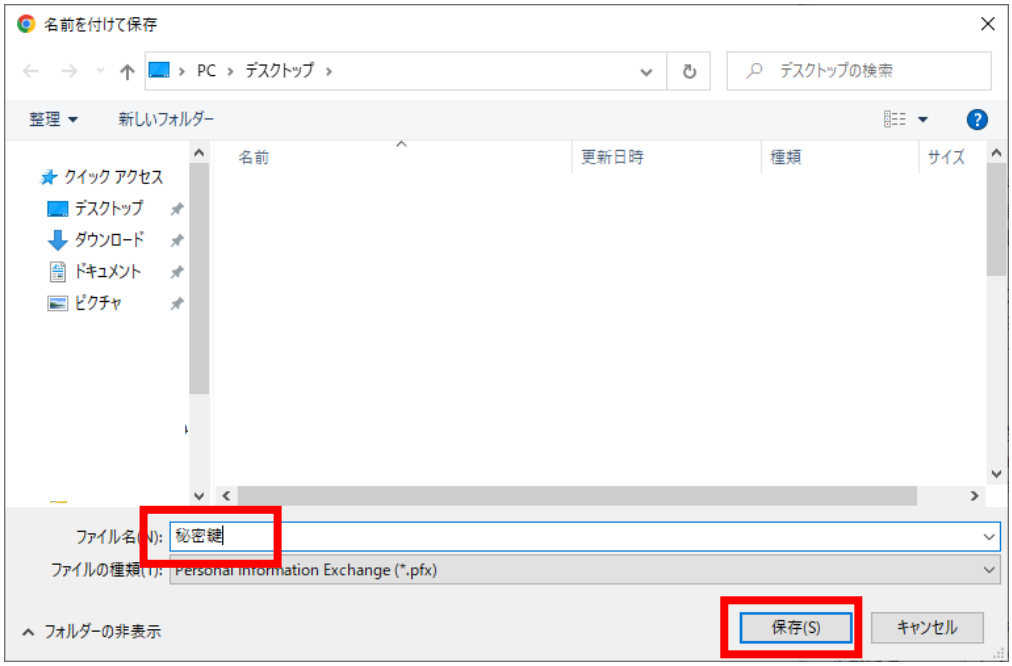
パスワードの文字制限はありませんが、法人代表者の証明書で署名暗号化ツールを使用する場合は８文字以上にすることを推奨しています。

4-6．参照ボタンをクリックして、任意の保存先とファイル名を指定してください。



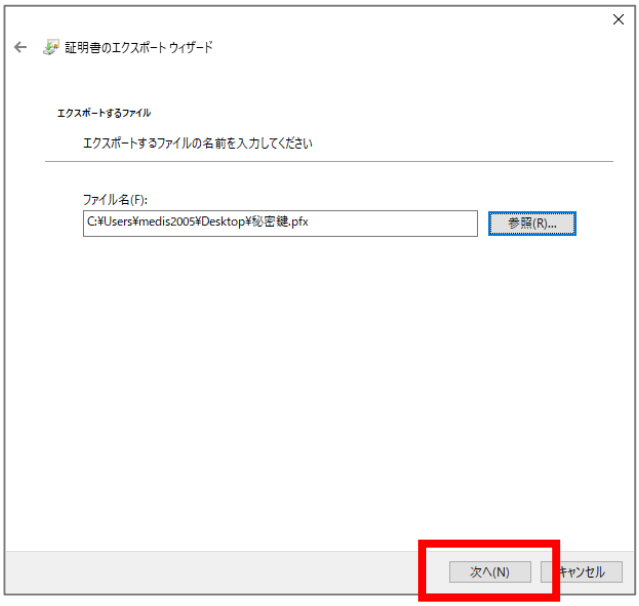
4-7．保存先とファイル名を入れて「保存」をクリックします。

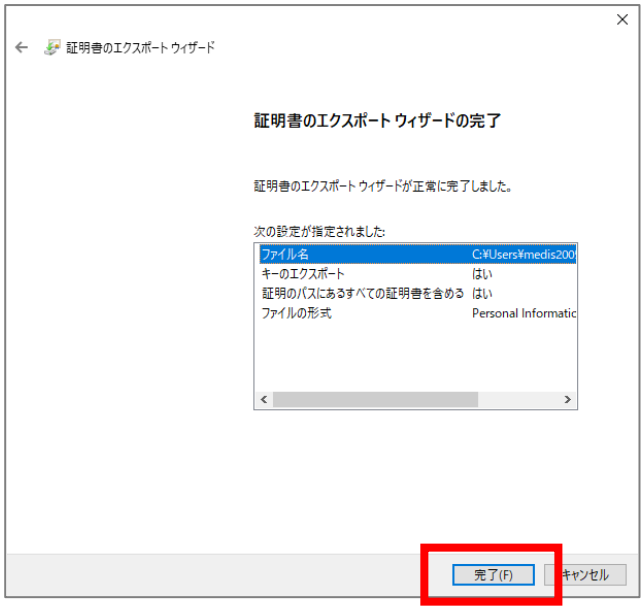
下図は、保存先：デスクトップ　ファイル名：秘密鍵　とした例です



4-8．ファイル名に指定した保存先とファイル名が表示されていることを確認して「次へ」をクリックします。

4-9．「完了」をクリックして、「正しくエクスポートされました」の表示画面で「OK」をクリックします。





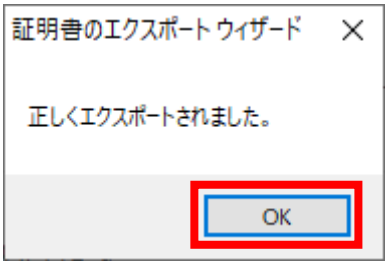
指定した場所にファイルが保存されていることを確認してください。

ファイル名の後につく拡張子は 『 .pfx 』になります。

秘密鍵のファイルは右記のアイコンで表示されます。ファイル容量は 3KB 程度です。

このファイルをバックアップファイルとして保存する場合は、

エクスポート時のパスワードとともに保管してください。



法人代表者証明書について

秘密鍵の拡張子が 『.pfx』でも署名暗号化ツールの設定には支障ありません