オンライン請求ネットワーク関連システム
共通認証局

ユーザーマニュアル

(Windows ChromiumEdge)

Version 1.10.0

令和 7 年 2 月 19 日

目次

Publication History		
Date	Version #	Summary of Changes
2020/09/28	1.0.0	初版
2020/12/11	1.1.0	・「1.5 MPKI クライアントインストール」の保存手順の変更 ・「2.1 更新のお知らせ通知」の【お知らせが表示される条 件】を変更 ・「3.証明書バックアップ（MPKI クライアント編)」を追加
2021/01/04	1.2.0	・「1.1 証明書ダウンロード」のダウンロード方法の追記 ・手順案内様式の変更
2021/03/22	1.3.0	・「3. 証明書の失効」の変更
2021/04/16	1.3.1	・医療機関等向けセットアップ手順書とオンライン資格確認等接続ガイド（IP-VPN 接続方式）の URL 変更に伴う修正
2021/04/27	1.4.0	・「5.3. ルート証明書の取得とインストール」を追加
2022/04/13	1.5.0	・「5.4. MPKI クライアントのバージョンアップ」を追加
2024/1/15	1.6.0	・医療機関等向け総合ポータルサイトを追加 ・対応 OS に Windows11 を追加
2024/3/25	1.7.0	・医療機関等向けポータルサイトを削除、医療機関向け等総合ポータルサイトに統合
2024/5/13	1.8.0	・「1.2.証明書のインストール」4.「秘密キーの保護」「このキーをエクスポート可能にする」のチェックを外すに変更
2024/10/01	1.9.0	・「1. **各種申請の流れ**」を追加

Publication History		
Date	Version #	Summary of Changes
		・「3.1.2. **電子証明書の更新**」に電子証明書のバックアップファイル作成の手順を追加 ・章立ての見直し
2025/02/xx	1.10.0	認証局サービスの制約事項として、Web ブラウザについて複数ウィンドウ・タブを開いた状態で画面の操作を行うとデータ不整合が発生する データ不整合を発生させないため、Web ブラウザを用いた各操作の前後に必ず閉じるように注意文言を追加

はじめに

本書は、オンライン請求ネットワーク関連システム共通認証局（以下、「共通認証局」という。）において、利用者がオペレーションできる電子証明書の取得、更新、および更新ツール（MPKI クライアント）について記述したものです。

事前準備

電子証明書の取得、更新及び失効には、レセプトオンライン請求ネットワークの接続設定を行う必要があります。未設定の方は、システムベンダ等へご確認の上、設定ください。

- レセプトオンライン請求の場合

[ネットワーク接続設定と端末のセットアップ設定]
オンライン請求システムセットアップ CD-ROM に同梱の「オンライン請求システム操作手順書」参照

- オンライン資格確認の場合

[ネットワーク接続設定と端末のセットアップ設定]
インターネットで「医療機関等向け総合ポータルサイト」の下記の URL から「医療機関等向けセットアップ手順書」及び「オンライン資格確認等システム接続ガイド(IP-VPN 接続方式)」を参照
https://iryohokenjyoho.service-now.com/csm?sys_kb_id=4356711cc3537910615bd1877a0131b6&id=kb_article_view

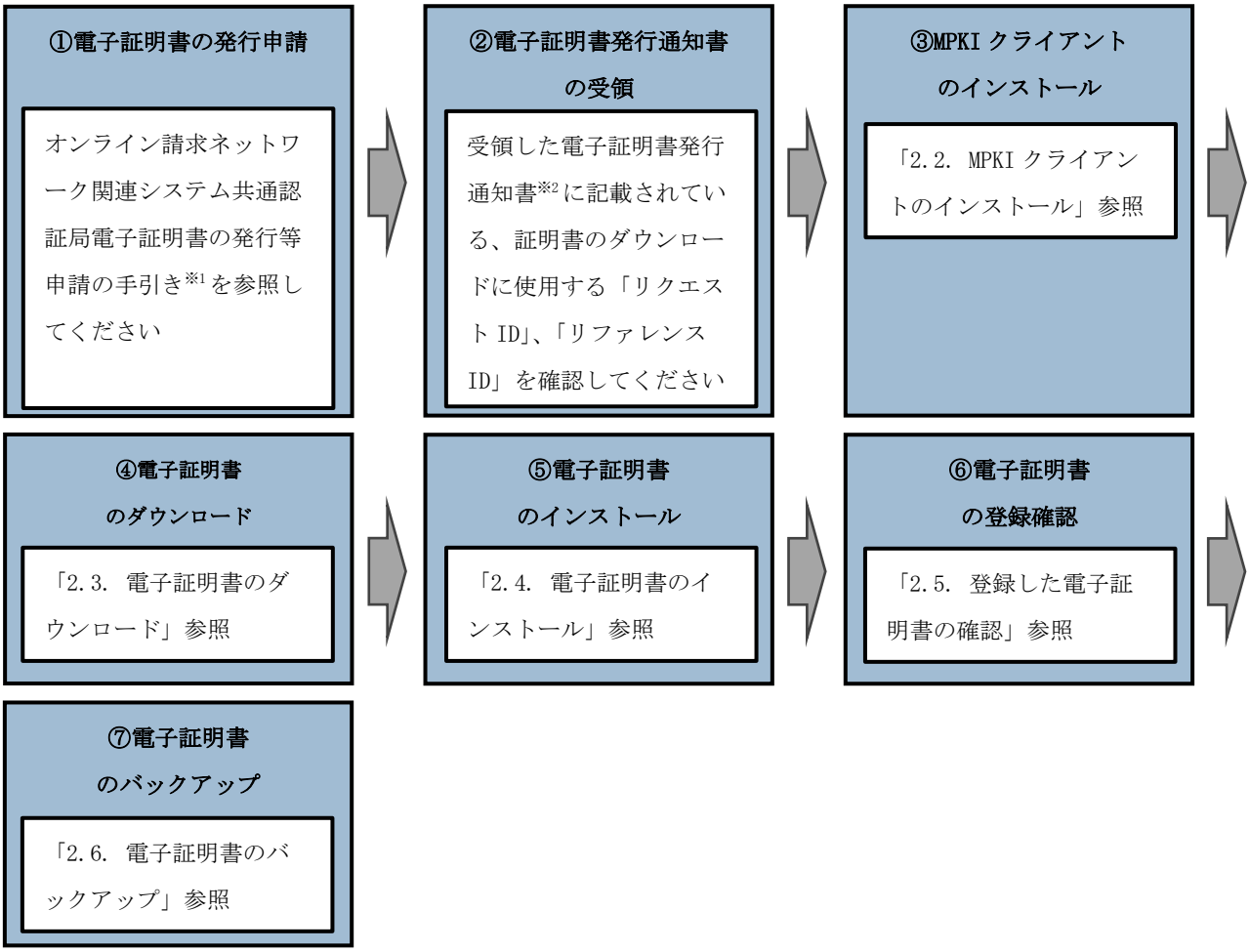
1. 各種申請の流れ

1.1. 電子証明書の新規発行手続き

注意

ブラウザから複数のタブやウインドウを開いた状態で、各種手続きを実施した場合、証明書が正しい申請内容で手続き出来ない場合があります。
必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

電子証明書の新規発行は、以下の流れでマニュアルの手順を実施してください。



※1 オンライン請求ネットワーク関連システム共通認証局電子証明書の発行等申請の手引き
https://www.ssk.or.jp/seikyushiharai/iryokikan/download/index.files/kyotu_tebiki.pdf

※2 電子証明書を新規発行した場合に簡易書留で郵送される通知書

1.2. 電子証明書の更新手続き

電子証明書の更新は、有効期限が 90 日未満となった場合に実施できます。

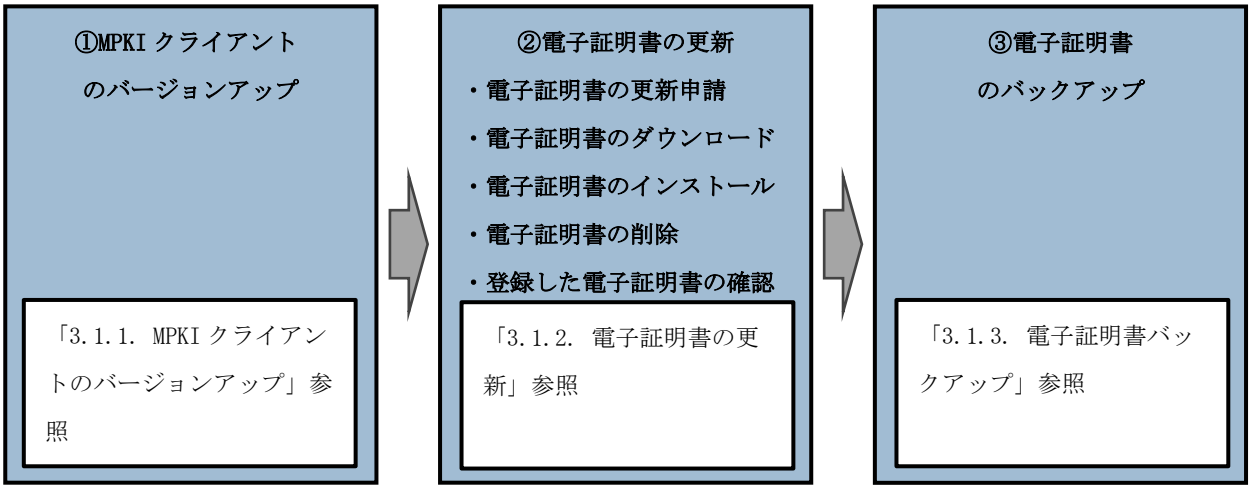
【更新手続き・有効期限に関する周知】

Windows の通知（MPKI クライアント）	有効期限の 90 日前、60 日前、30 日前、15 日前、7 日前～期限日
オンライン資格確認等システムにメッセージを表示	有効期限の 90 日前、60 日前、30 日前、15 日前、7 日前～期限日
オンライン請求システムにメッセージを表示 ※支払基金のみ	有効期限の 90 日前～期限日
メール通知 ※電子証明書の発行申請時に入力したメールアドレス宛に「no-reply@ssk.or.jp」からメール通知	有効期限の 75 日前、60 日前、45 日前、30 日前、15 日前、7 日前～期限日

電子証明書の更新をする場合、「1.2.1. MPKI クライアントを利用した電子証明書の更新」または「1.2.2. 電子証明書更新サイトからの電子証明書の更新」いずれかの手順で実施してください。

1.2.1. MPKI クライアントを利用した電子証明書の更新

（MPKI クライアントがインストールされている必要があります）



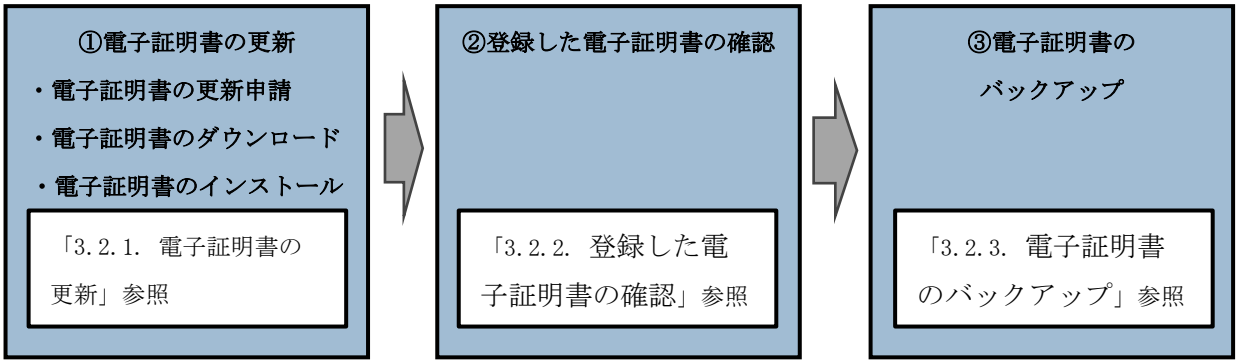
③電子証明書のバックアップまでの操作を更新前の電子証明書の有効期限（３年３か月）までに実施してください。
※更新前の電子証明書の有効期限（３年３か月）を過ぎると、更新済みの電子証明書がダウンロードできなくなります。

1.2.2.　電子証明書更新サイトからの電子証明書の更新

注意

ブラウザから複数のタブやウインドウを開いた状態で、各種手続きを実施した場合、証明書が正しい申請内容で手続き出来ない場合があります。

必ずすべてのブラウザを閉じてから、手続きを実施して下さい。



③電子証明書のバックアップまでの操作を更新前の電子証明書の有効期限（３年３か月）までに実施してください。

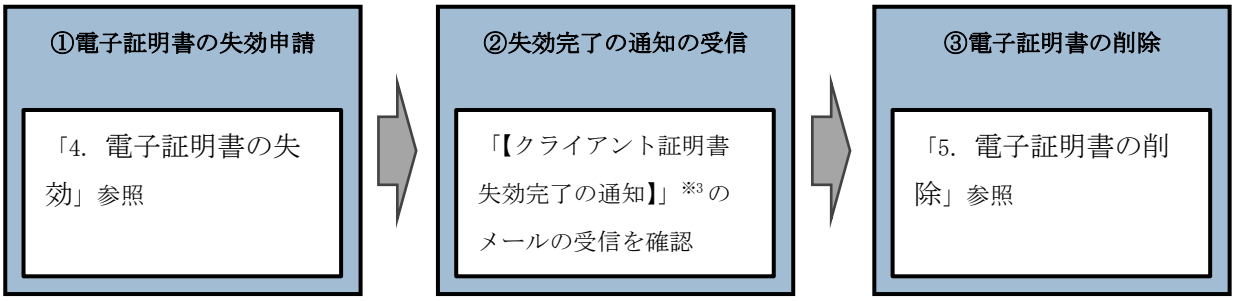
※更新前の電子証明書の有効期限（３年３か月）を過ぎると、更新済みの電子証明書がダウンロードできなくなります。

1.3.　電子証明書の失効手続き

注意

ブラウザから複数のタブやウインドウを開いた状態で、各種手続きを実施した場合、証明書が正しい申請内容で手続き出来ない場合があります。
必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

電子証明書を失効する場合、以下の流れでマニュアルの手順を実施してください。



※3 失効申請の後、共通認証局において失効処理が完了すると、メールアドレス「no-reply@ssk.or.jp」から電子証明書の発行申請時に設定したメールアドレス宛に「【クライアント証明書 失効完了の通知】」が送信されます。
なお、失効処理が完了するまで数日間要する場合があります。

2. 電子証明書の新規発行手続き

2.1. 電子証明書の新規発行申請

電子証明書の新規発行の手続きについては「オンライン請求ネットワーク関連システム共通認証局電子証明書の発行等申請の手引き」（下記 URL）を参照ください。
https://www.ssk.or.jp/seikyushiharai/iryokikan/download/index.files/kyotu_tebiki.pdf
お手元に電子証明書発行通知書が届きましたら「2.2. MPKI クライアントのインストール」以降の手順を実施ください。

2.2. MPKI クライアントのインストール

【MPKI クライアントとは】

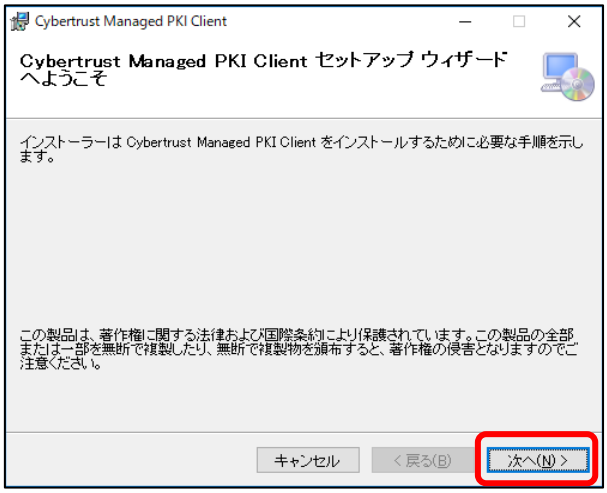
MPKI クライアントを使用すると、有効期限の前に更新をお知らせする機能や電子証明書の更新を簡易に行う機能が利用できます。
MPKI クライアントをインストールできる対象の OS は、Windows 8.1 と Windows 10、または Windows 11 です。
また、「Microsoft .NET Framework 4.8」以上がインストールされている必要があります。
利用環境の詳細は「6.1. MPKI クライアント利用環境」を参照ください。
インストール中にエラーが発生した場合は、「6.2.2. MPKI クライアントインストール時の注意事項」を参照ください。

注意 必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

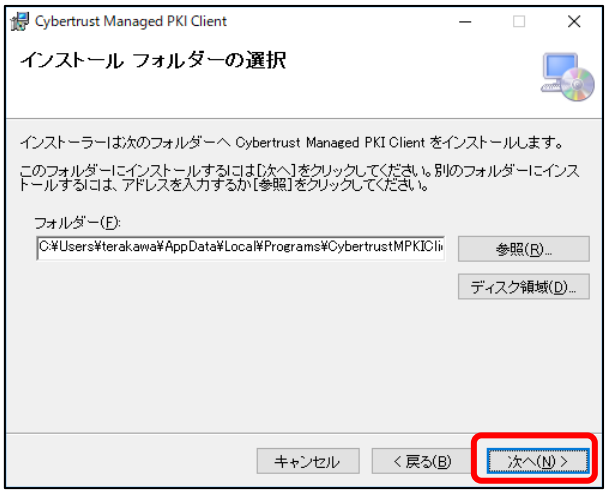
1．オンライン請求ネットワークへ接続の端末から MPKI クライアント取得用サイトにアクセスし、MPKI クライアントのインストーラーをダウンロードします。
【ダウンロードサイト】
https://cert.obn.managedpki.ne.jp/p/s

２．「…」をクリックし、「**フォルダに表示**」をクリックします。

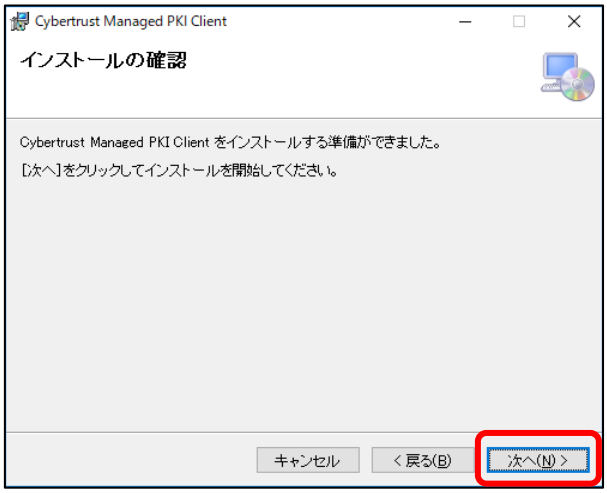
３．「**CybertrustManagedPKIClient.msi**」ファイルを右クリックし、「**インストール**」をクリックします。



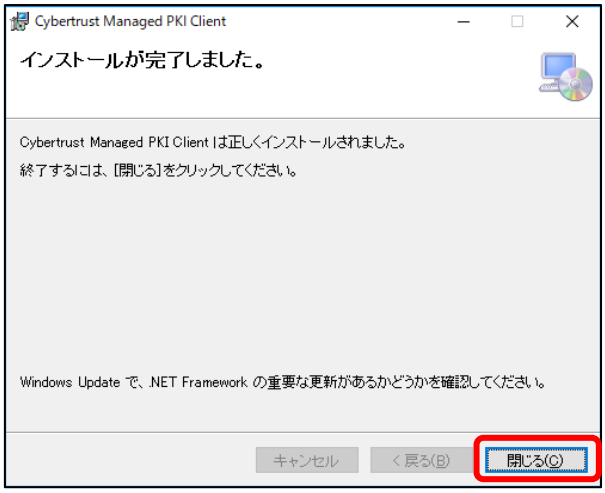
４．「**Cybertrust Managed PKI Client セットアップウィザード**」が開始されます。「**次へ**」をクリックします。



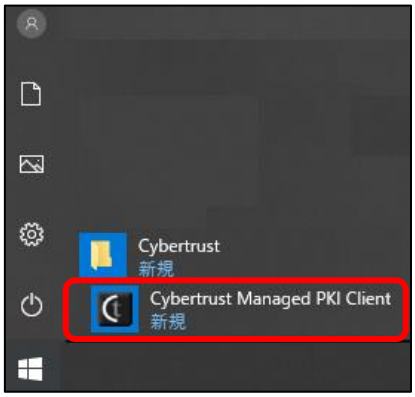
５．「**次へ**」をクリックします。



6．「**次へ**」をクリックします。



7．「**閉じる**」をクリックします。



8．MPKI クライアントのインストールが完了すると、スタートメニューに「**Cybertrust Managed PKI Client**」が追加されます。

注意　上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

2.3. 電子証明書のダウンロード

電子証明書をダウンロードサイトよりダウンロードします。
お手元に電子証明書発行通知書の「電子証明書取得に関する情報」をご用意願います。
電子証明書のダウンロード可能期間は、発行後 180 日以内ですので、期間内にダウンロードするようご留意願います。

電子証明書発行通知書の「電子証明書取得に関する情報」（サンプル）

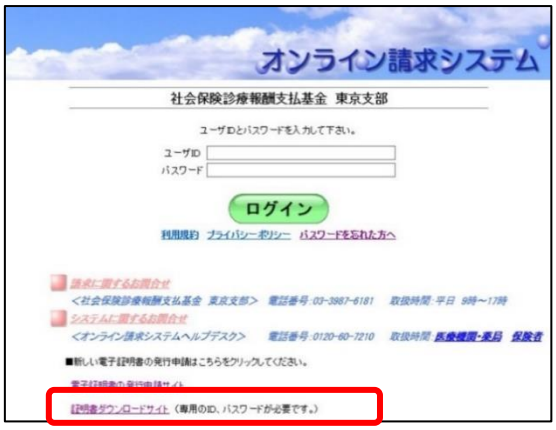
発行者	Online Billing NW Common Root CA - 01
発行元	※医療機関コード
端末名称等	※申請時に登録した端末名称
電子証明書ダウンロードサイトリクエストID	20210121xxxxxxx
電子証明書ダウンロードサイトリファレンスID	XXXXXXXXXXXXXXX
電子証明書有効期限	YYYY/MM/DD ～ YYYY/MM/DD
電子証明書ダウンロードサイト有効期限	YYYY/MM/DD

オンライン請求ネットワークへ接続の端末（レセプトオンライン請求用端末またはオンライン資格確認端末）で電子証明書を取得します。

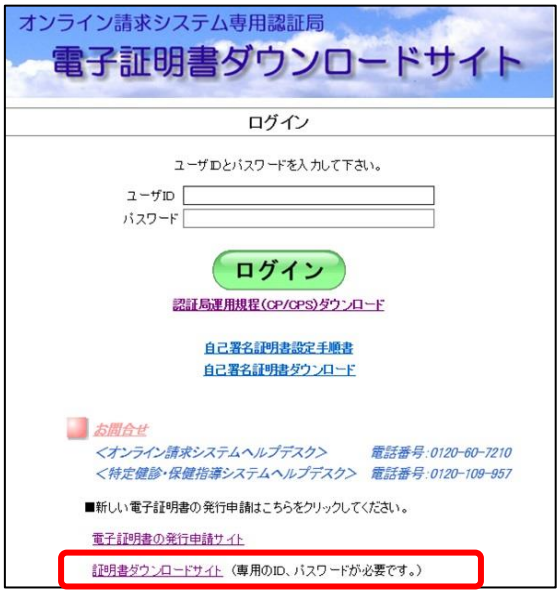
注意 必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

【レセプトオンライン請求用端末の場合】

・オンライン請求システムのログイン画面



・電子証明書ダウンロードサイト



1．<u>レセプトオンライン請求端末またはオンライン資格確認端末</u>からダウンロードサイトにアクセスします。

【ダウンロードサイト】

https://cert.obn.managedpki.ne.jp/p/rcd

【レセプトオンライン請求用端末の場合】

オンライン請求システムのログイン画面または電子証明書ダウンロードサイトよりアクセスできます。

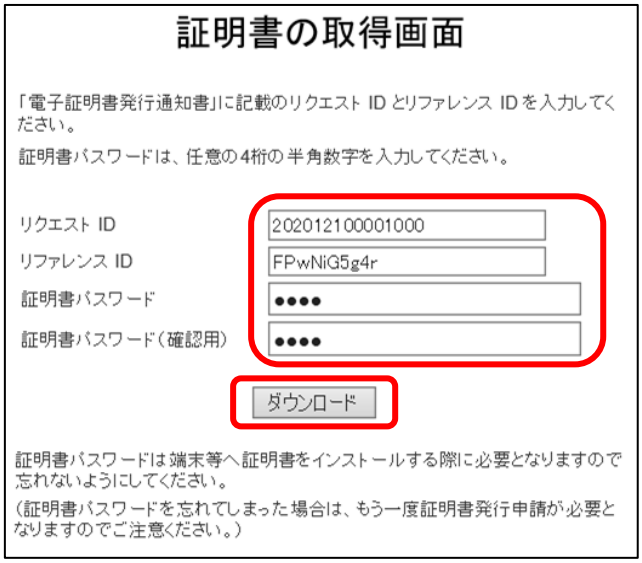
【こんなときは！】

証明書のダウンロード画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**接続がプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「6.2.4. ルート証明書の取得とインストール」を参照

【オンライン資格確認端末の場合】

【オンライン資格確認端末の場合】

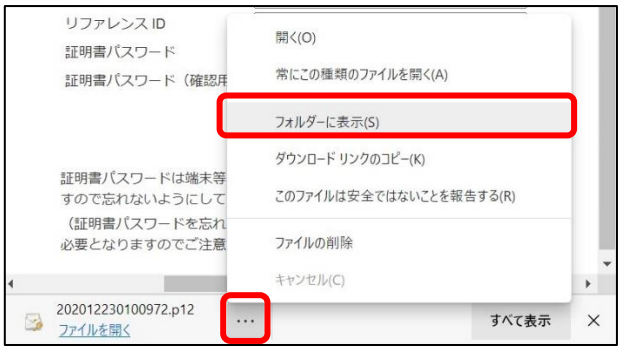
「**医療機関等向けセットアップ手順書**」に沿ってセットアップを行った方は、デスクトップにあるダウンロードサイトのアイコンからアクセスできます。



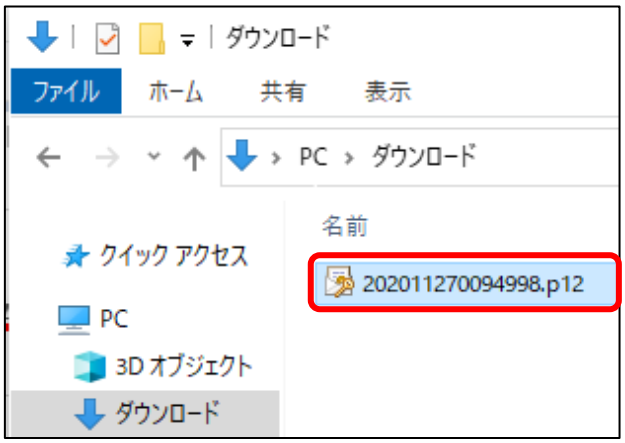
2．電子証明書発行通知書に記載の「**リクエスト ID**」と「**リファレンス ID**」及び「**証明書パスワード**」に**任意のパスワード（鍵の暗号化・復号に利用）半角数字 4 桁**を入力し、「**ダウンロード**」をクリックします。

【注意】

入力した証明書パスワードは、「2.3. 電子証明書のダウンロード」の 4 で使用します。設定したパスワードを忘れないようにしてください。



3．画面下の「…」をクリックし、「**フォルダに表示**」をクリックします。

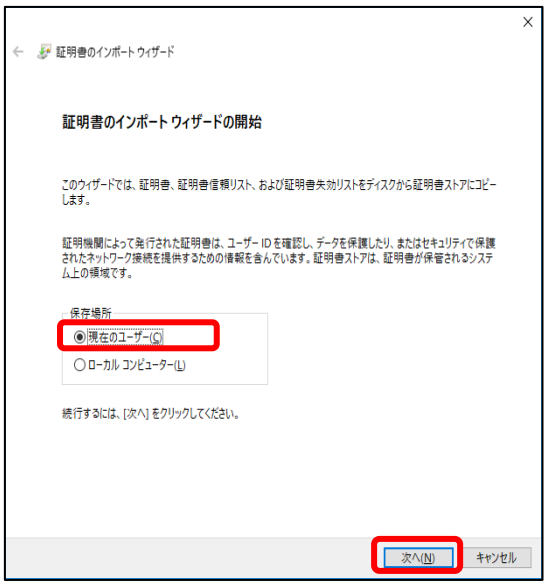


4．電子証明書がダウンロードできていることを確認します。

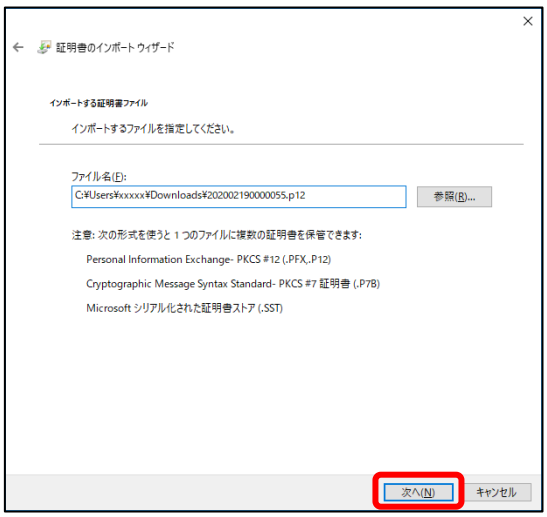
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

2.4. 電子証明書のインストール

1．ダウンロードした電子証明書ファイルを右クリックし、「**PFX のインストール**」をクリックします。



2．「**証明書のインポートウィザード**」が表示されます。保存場所は「**現在のユーザー**」を選択し、「**次へ**」をクリックします。



3．「**インポートする証明書ファイル**」が表示されます。ファイル名に電子証明書のファイル名が表示されていることを確認し、「**次へ**」をクリックします。

4．「**秘密キーの保護**」が表示されます。「**パスワード**」に「**2.3. 電子証明書のダウンロード**」で設定した「**証明書パスワード**」を入力します。

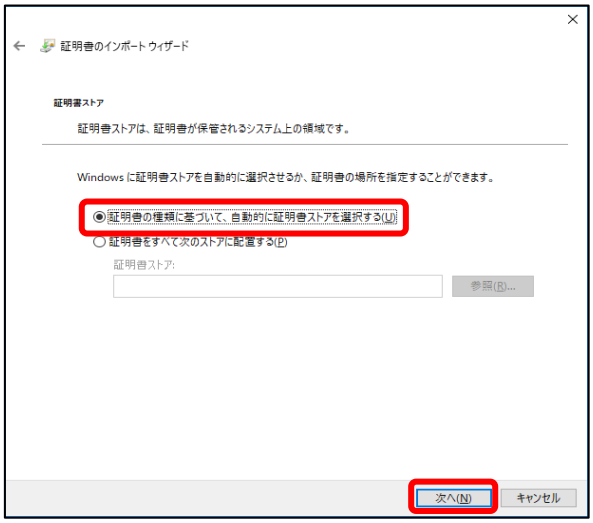
「**インポートオプション**」について、以下の内容を設定します。

[秘密キーの保護を強力にする]の
チェックを外す

[このキーをエクスポート可能にする]を
チェックを外す

[すべての拡張プロパティを含める]を
チェックする

「**次へ**」をクリックします。

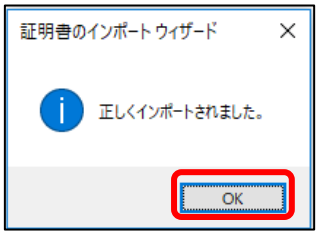


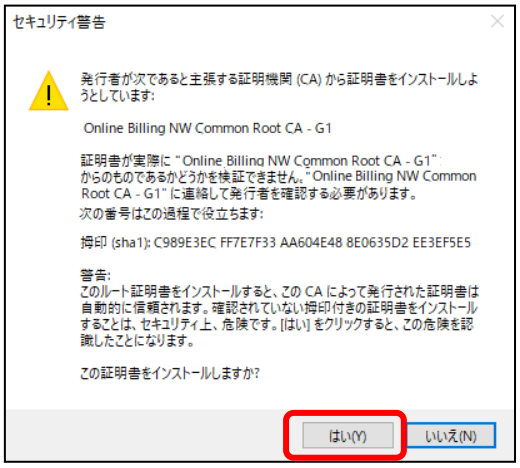
５．「**証明書ストア**」が表示されます。「**証明書の種類に基づいて、自動的に証明書ストアを選択する**」を選択後、「**次へ**」をクリックします。

６．「**証明書のインポートウィザードの完了**」が表示されます。「**完了**」をクリックします。

【こんなときは！】

「新しい秘密交換キーをインポートします」が表示された場合、P21 の「2.4.1. こんなときは！」を参照してください。





7．「**正しくインポートされました**」が表示されます。「**OK**」をクリックします。

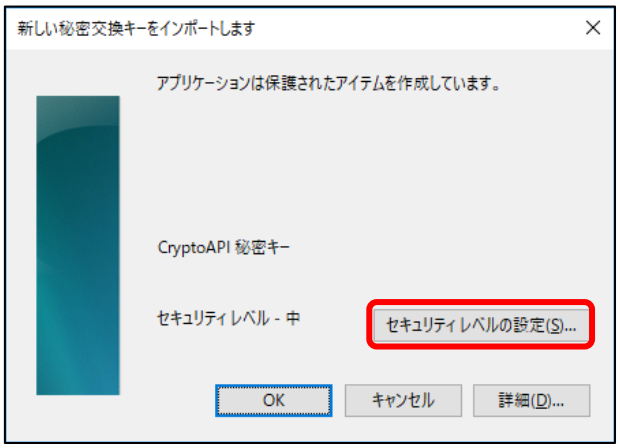
【こんなときは！】

「セキュリティ警告」の画面が表示された場合、「**はい**」をクリックします。

「証明書発行者（認証局）の証明書」は、インストールを行った証明書が「証明書発行者（認証局）」によって発行された証明書であることを確認（ご使用のブラウザが自動的に確認）する時に必要です。「いいえ」をクリックした場合は、「**2.4. 電子証明書のインストール**」を再度行ってください。

2.4.1. こんなときは！

※電子証明書インストール時に「**新しい秘密交換キーをインポートします**」と表示された場合は、次の操作を行ってください。表示されない場合には「2.5. 登録した電子証明書の確認」に進みます。



1．「**セキュリティレベルの設定**」をクリックします。

2．任意の「**CyptoAPI 秘密キー**」のパスワードを入力し、「**完了**」をクリックします。

【※重要※】

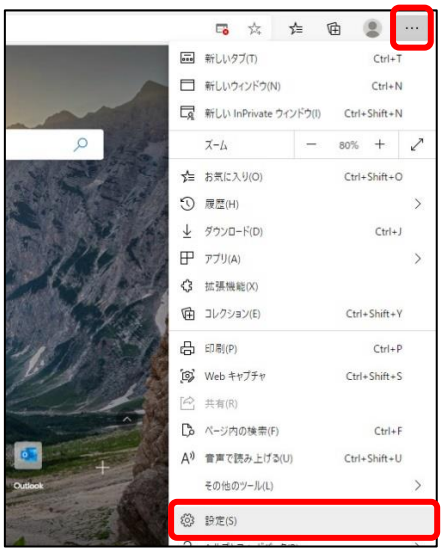
作成したパスワードは、今後の証明書の更新時に利用するため、忘れないよう大切に保管ください。

3．「**ＯＫ**」をクリックします。

2.5.　登録した電子証明書の確認

注意　必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

1．Edge を起動します。



2．画面右上の「…」をクリックし、「**設定(S)**」をクリックします。

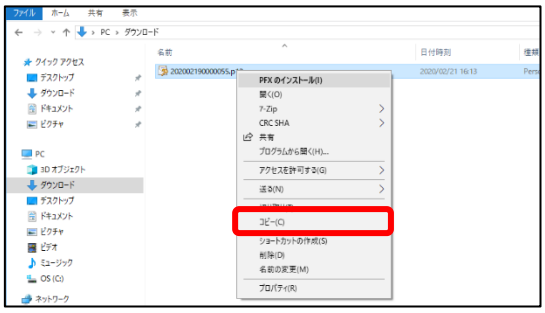
3．「**プライバシー、検索、サービス**」を選択し、「**セキュリティ**」の「**証明書の管理**」をクリックします。

4．「**個人**」タブを開き、発行者が「**Online Billing NW Common Root CA**」と表示されている電子証明書が登録されていることを確認します。

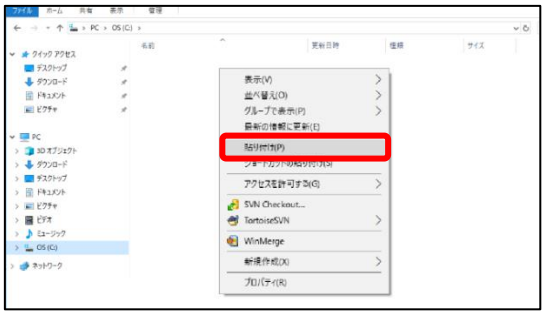
注意 **上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。**

2.6. 電子証明書のバックアップ

外部記録媒体等へ電子証明書をバックアップします。バックアップした電子証明書はパソコンが故障した際などに他のパソコンにインストールすることができます。その際には、「2.3. 電子証明書のダウンロード」で設定したパスワードも必要となるため、忘れないように保管ください。



1．インストールを行った電子証明書ファイルを選択し右クリックで「**コピー**」を選択します。



2．外部記録媒体等のフォルダを開き、「**貼り付け**」を選択します。

【注意】

「電子証明書」「電子証明書発行通知書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理してください。これら 3 つの情報が第三者に渡ると、電子証明書が不正に使用される恐れがあります。

<u>電子証明書の新規利用開始の作業はこれで終了です。</u>

3. 電子証明書の更新手続き

有効期限が切れる前に必ず、「3.1. MPKI クライアントを利用した電子証明書の更新」または「3.2. 電子証明書更新申請サイトからの電子証明書の更新」のいずれかの手順を実施してください。

※「3.1. MPKI クライアントを利用した電子証明書の更新」の手順を実施するには MPKI クライアントがインストールされている必要があります。

MPKI クライアントがインストールされている場合、タスクバーのタスクトレイに  が表示されております。（タスクトレイをすべて表示してご確認ください。）

3.1. MPKI クライアントを利用した電子証明書の更新

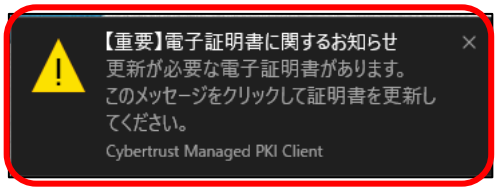
3.1.1. MPKI クライアントのバージョンアップ

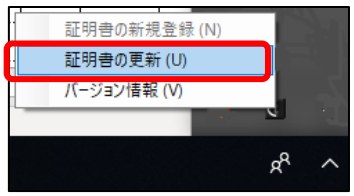
以下の手順を実施してください。

(1) 「6.1. MPKI クライアント利用環境」を読み、利用環境の確認を行って下さい。

(2) 利用環境の条件を満たしている場合、「6.3. MPKI クライアントのバージョンアップ」の作業を行ってください。

3.1.2. 電子証明書の更新

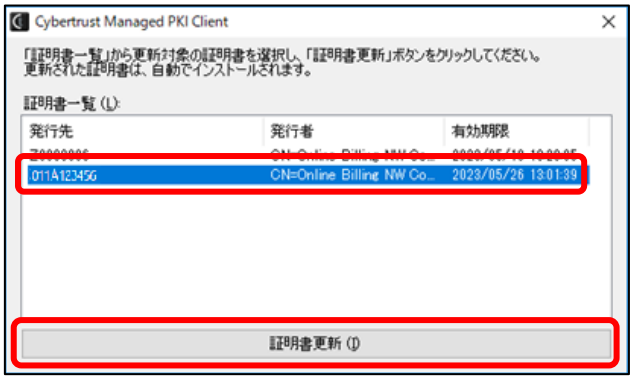




1．「**電子証明書に関するお知らせ**」通知をクリックします。

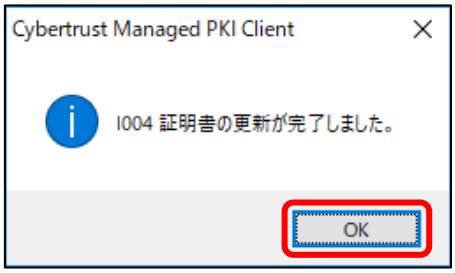
【こんなときは！】

お知らせが表示されていない場合は、タスクトレイのアイコンを右クリックから操作できます。表示される以下のメニューから、┼「**証明書の更新**」┼ をクリックします。

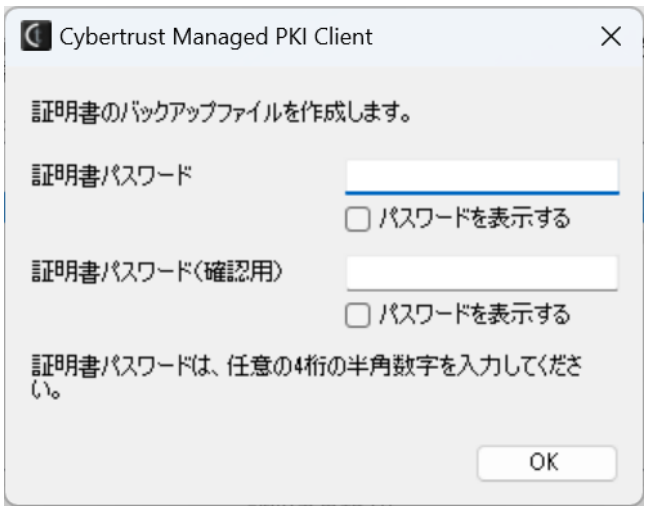


2．**更新したい電子証明書**を選択し、「**証明書更新**」をクリックします。

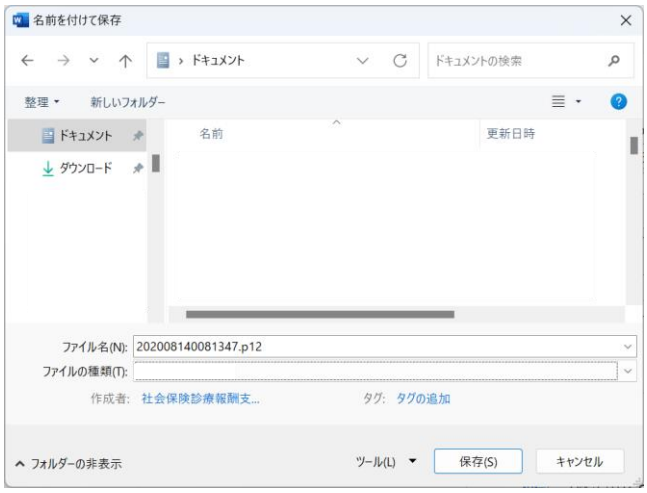
3．「**はい**」をクリックします。



4．「**ＯＫ**」を**クリック**します。

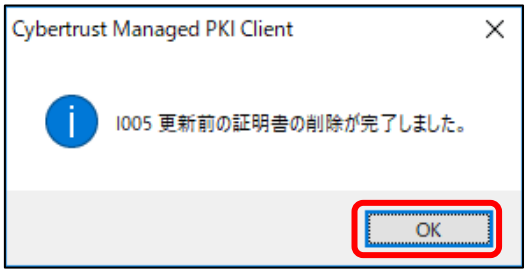


5．「**パスワード**」に**鍵の暗号化パスワード（任意のパスワード）半角数字４桁**を入力して「**ＯＫ**」をクリック**します**。



6．証明書の保存先を指定して「保存」をクリックします。

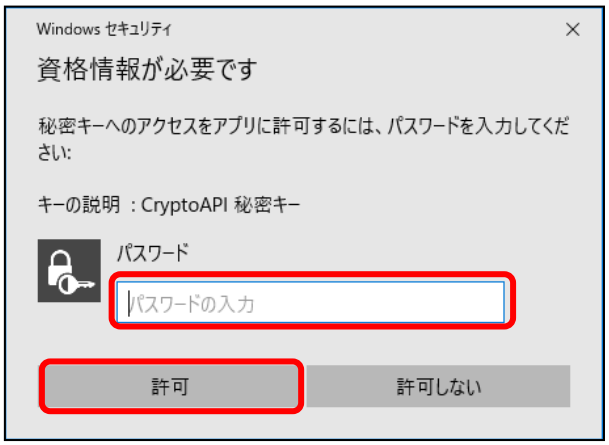
7．「**はい**」を**クリック**します。



8．「**OK**」を**クリック**します。

3.1.2.1.　こんなときは！

※パスワードの入力が求められた場合は、電子証明書のインストール時「2.4.1.　こんなときは！」で設定したパスワードを入力します。

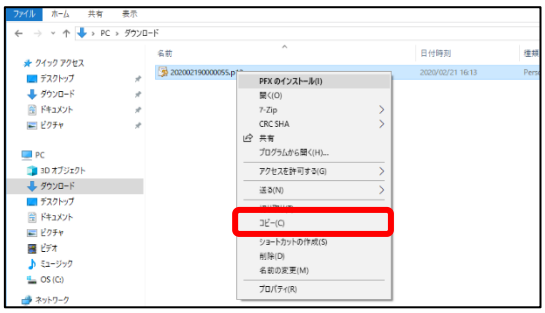


1．パスワードを入力し、「**許可**」をクリックします。

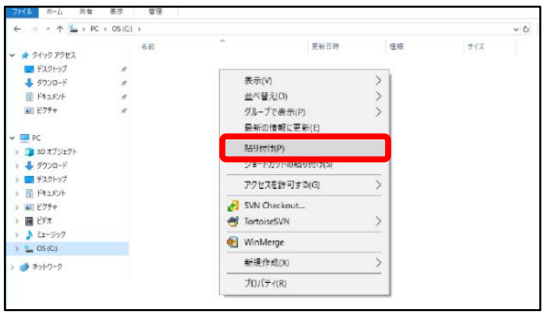
※パスワードは、電子証明書のインストール時「2.4.1.　こんなときは！」で設定したパスワードです。

3.1.3.　電子証明書バックアップ

外部記録媒体等へ電子証明書をバックアップします。バックアップした電子証明書はパソコンが故障した際などに他のパソコンにインストールする事が可能です。その際には、「3.1.2.　電子証明書の更新」の「５．」で設定したパスワードも必要となるため、忘れないように保管ください。



1．「3.1.2.　電子証明書の更新」を行った電子証明書ファイルを選択し右クリックで「**コピー**」を選択します。



2．外部記録媒体等のフォルダを開き、「**貼り付け**」を選択します。

【注意】

「電子証明書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理してください。これら 2 つの情報が第三者に渡ると、電子証明書が不正に使用される恐れがあります。

MPKI クライアントを利用した電子証明書の更新の作業はこれで終了です。

3.2.　電子証明書更新申請サイトからの電子証明書の更新

3.2.1.　電子証明書の更新

注意　必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

１．更新対象の電子証明書がインストールされた端末からオンライン請求ネットワークに接続して　「**更新申請画面**」へアクセスします。

【電子証明書更新申請サイト】

https://cert.obn.managedpki.ne.jp/p/ru

※オンライン請求システムにログインすると、電子証明書更新申請サイトのリンクがあります。

【こんなときは！】

証明書の更新画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**接続がプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「6.2.4.　ルート証明書の取得とインストール」を参照

２．更新対象の電子証明書を選択し、「ＯＫ」をクリックします。

※「Online Billing NW Common Root CA 」と表記されていることを確認

3．「**証明書更新申請**」をクリックします。

4．「Submit」をクリックします。

５．「**送信完了**」画面の「**証明書ステータス**」が「**発行済み**」となれば電子証明書が発行されます。

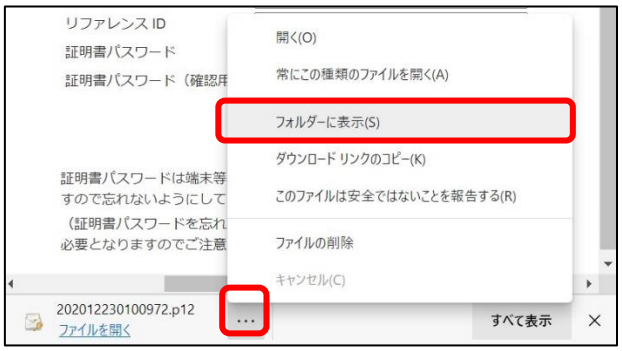
「**証明書ステータス**」は、「**鍵生成中**」→「**発行要求中**」→「**発行済み**」と遷移します。

６．「鍵の取得」画面に遷移後、「**パスワード**」に**任意のパスワード（鍵の暗号化・復号に利用）半角数字４桁**を入力し、「Submit」をクリックします。

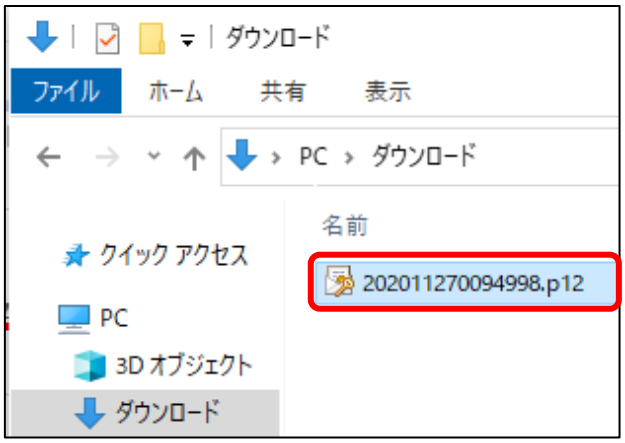
【注意】

入力したパスワードは、「3.2.1. 電子証明書の更新」の「１３．」で使用します。**設定したパスワードを忘れないようにしてください。**

７．「Download」をクリックします。

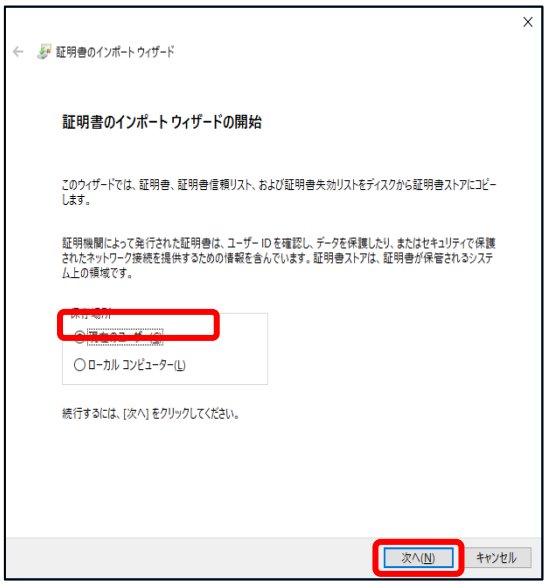


８．画面下の「…」をクリックし、「**フォルダに表示**」をクリックします。

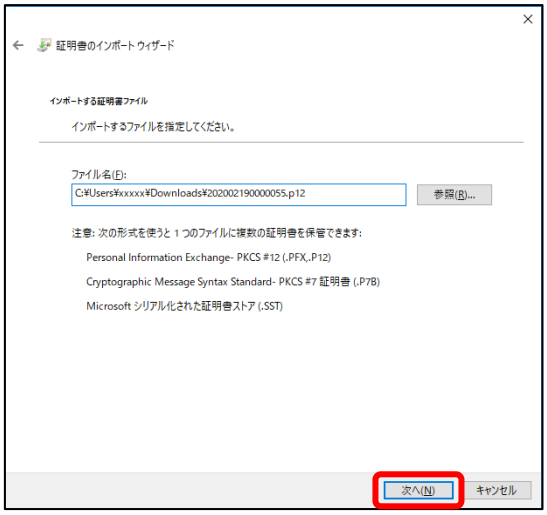


９．鍵がダウンロードできていることを確認します。

１０．ダウンロードした電子証明書ファイルを右クリックし、「**PFX のインストール**」をクリックします。

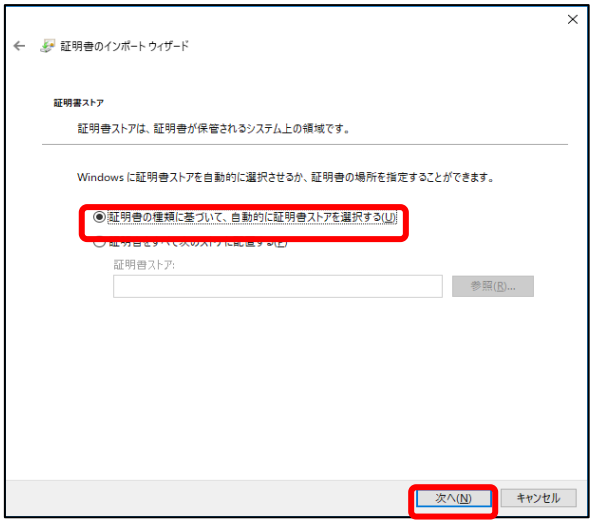


１１．「**証明書のインポートウィザード**」が表示されます。保存場所は「**現在のユーザー**」を選択し、「**次へ**」をクリックします。



１２．「**インポートする証明書ファイル**」が表示されます。ファイル名に電子証明書のファイル名が表示されていることを確認し、「**次へ**」をクリックします。

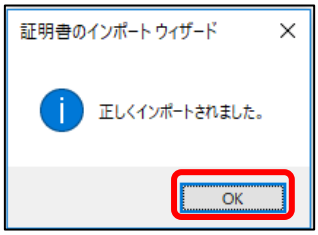
１３．「**秘密キーの保護**」が表示されます。
「**パスワード**」に「3.2.1. 電子証明書の更新」で設定した**鍵の暗号化パスワード**を入力します。
「**インポートオプション**」について、以下の内容を設定します。
[秘密キーの保護を強力にする]の
チェックを外す
[このキーをエクスポート可能にする]を
チェックを外す
[すべての拡張プロパティを含める]を
チェックする
「次へ」をクリックします。

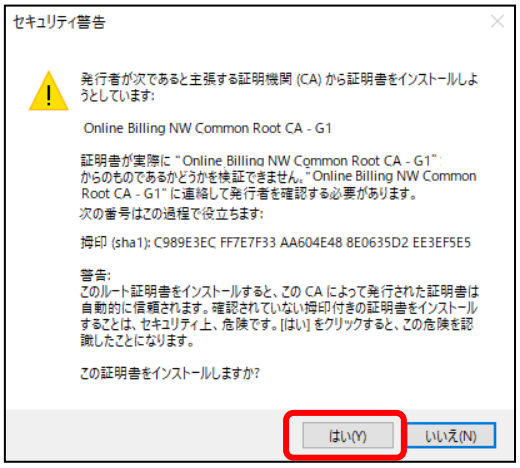


１４．「**証明書ストア**」が表示されます。「**証明書の種類に基づいて、自動的に証明書ストアを選択する**」を選択後、「**次へ**」をクリックします。

１５．「**証明書のインポートウィザードの完了**」が表示されます。「**完了**」をクリックします。

【こんなときは！】
「**新しい秘密交換キーをインポートします**」が表示された場合、P21 の「2.4.1. こんなときは！」を参照してください。





１６．「**正しくインポートされました**」が表示されます。「**ＯＫ**」をクリックします。

【こんなときは！】

「**セキュリティ警告**」の画面が表示された場合、「**はい**」をクリックします。

「**証明書発行者（認証局）の証明書**」は、インストールを行った証明書が「**証明書発行者（認証局）**」によって発行された証明書であることを確認（ご使用のブラウザが自動的に確認）する時に必要です。「**いいえ**」をクリックした場合は、「3.2.1. 電子証明書の更新」の手順「１０．」から再度行ってください。

注意 上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

3.2.1.1.　こんなときは！

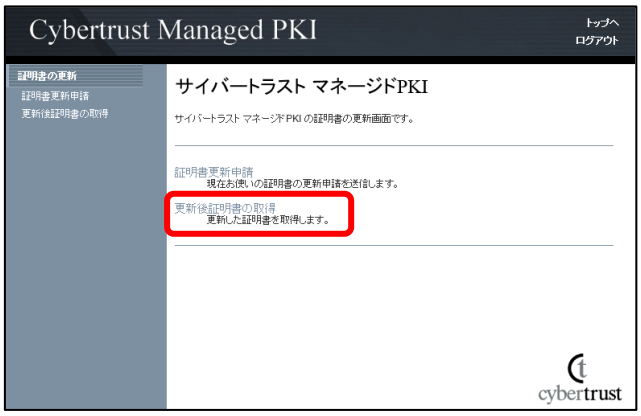
電子証明書または鍵の更新作業中に、ネットワークやシステム等の障害で電子証明書または鍵の取得に失敗した場合は、再度電子証明書または鍵を取得してください。

注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

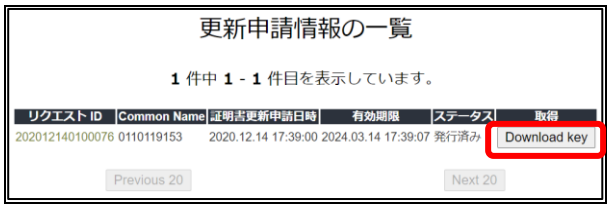
1．更新対象の電子証明書がインストールされた端末からオンライン請求ネットワークに接続して 更新申請画面へアクセスします。

【電子証明書更新申請サイト】

https://cert.obn.managedpki.ne.jp/p/ru



2．更新申請画面の「**更新後証明書の取得**」をクリックします。



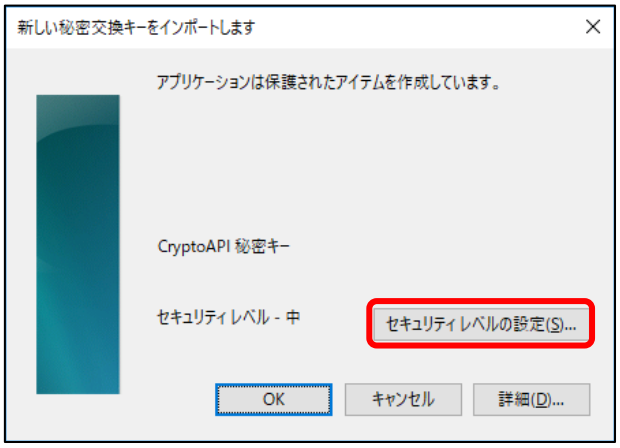
3．更新申請情報の一覧に情報が表示されている場合は、対象の更新済み電子証明書の「**Download Key**」ボタンをクリックして電子証明書を取得してください。

※更新申請情報の一覧に情報が表示されていない場合は、更新申請が完了していませんので、「3.2.1. 電子証明書の更新」の最初からやり直してください。

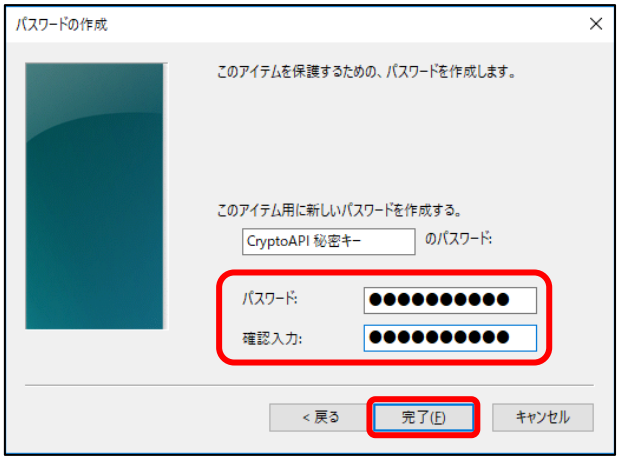
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

3.2.1.2.　こんなときは！

※電子証明書インストール時に「**新しい秘密交換キーをインポートします**」と表示された場合は、次の操作を行ってください。表示されない場合には「3.2.2. 登録した電子証明書の確認」に進みます。



1．「セキュリティレベル**の設定**」をクリックします。



2．任意の「**CyptoAPI 秘密キー**」のパスワードを入力し、「**完了**」をクリックします。

【※重要※】

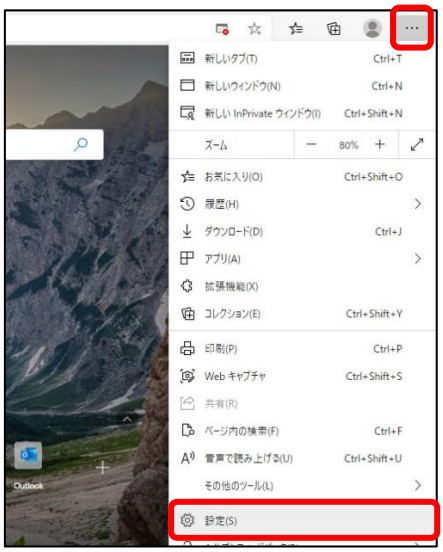
作成したパスワードは、今後の証明書の更新時に利用するため、忘れないよう大切に保管ください。

3．「**ＯＫ**」をクリックします。

3.2.2.　登録した電子証明書の確認

注意　必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

1．Edge を起動します。



2．画面右上の「…」をクリックし、「**設定(S)**」をクリックします。

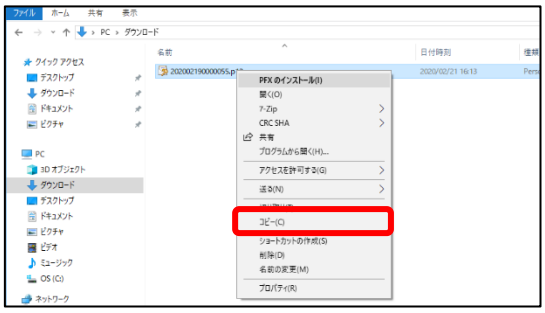
3．「**プライバシー、検索、サービス**」を選択し、「**セキュリティ**」の「**証明書の管理**」をクリックします。

４．「**個人**」タブを開き、発行者が「**Online Billing NW Common Root CA**」と表示されている電子証明書が登録されていることを確認します。

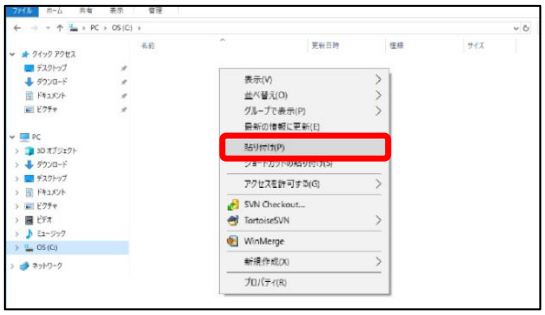
注意　**上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。**

3.2.3.　電子証明書のバックアップ

外部記録媒体等へ電子証明書をバックアップします。バックアップした電子証明書はパソコンが故障した際などに他のパソコンにインストールすることできます。その際には、「3.2.1. 電子証明書の更新」で設定した鍵の暗号化パスワードも必要となるため、忘れないように保管ください。



１．インストールを行った電子証明書ファイルを選択し右クリックで「**コピー**」を選択します。



２．外部記録媒体等のフォルダを開き、「**貼り付け**」を選択します。

【注意】

「電子証明書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理してください。これら２つの情報が第三者に渡ると、電子証明書が不正に使用される恐れがあります。

電子証明書更新申請サイトからの電子証明書の更新の作業はこれで終了です。

次ページからの手続きは、電子証明書の失効手続きです。

失効手続き後は、失効申請の取消しはできませんので、

ご留意ください。

4.　電子証明書の失効手続き

4.1.　電子証明書の失効申請

注意　必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

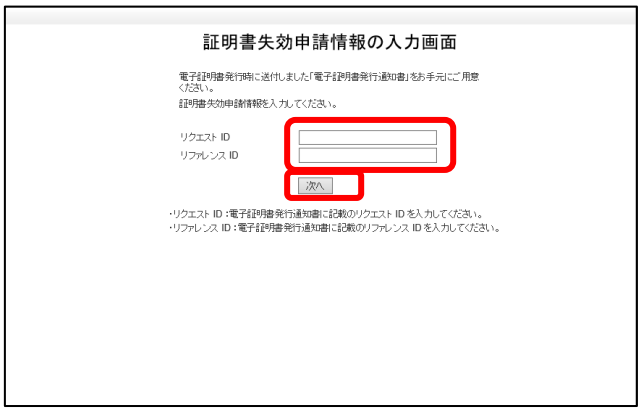
1．**失効対象の電子証明書がインストールされた端末**からオンライン請求ネットワークに接続して「**証明書失効申請情報の入力画面**」へアクセスします。

【電子証明書失効申請サイト】

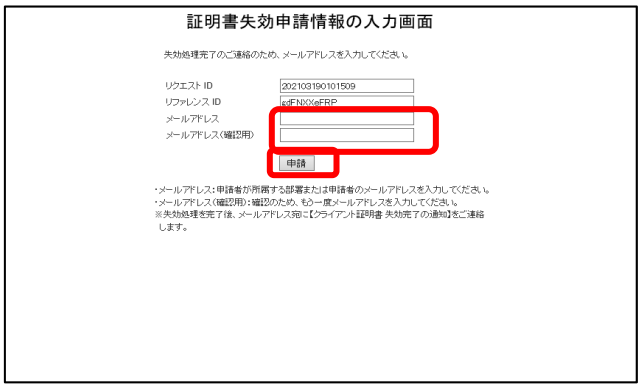
https://cert.obn.managedpki.ne.jp/p/rx

【こんなときは！】

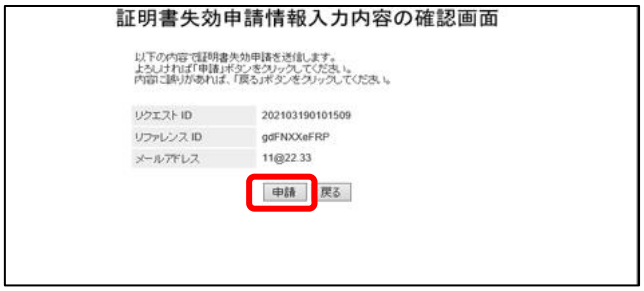
証明書の失効画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**接続がプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「**6.2.4.　ルート証明書の取得とインストール**」を参照



2．電子証明書発行通知書に記載の「**リクエスト ID**」と「**リファレンス ID**」を入力し「**次へ**」をクリックします。「**証明書失効申請情報の入力画面**」が切り替わります。



３．失効申請者の申請者のメールアドレスとメールアドレス(確認用)を入力し、「**申請**」をクリックします。「**証明書失効申請情報の確認画面**」へ遷移します。



４．内容を確認し、「**申請**」をクリックします。
失効申請が承認されると入力されたメールアドレス宛に失効完了をご連絡します。

注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

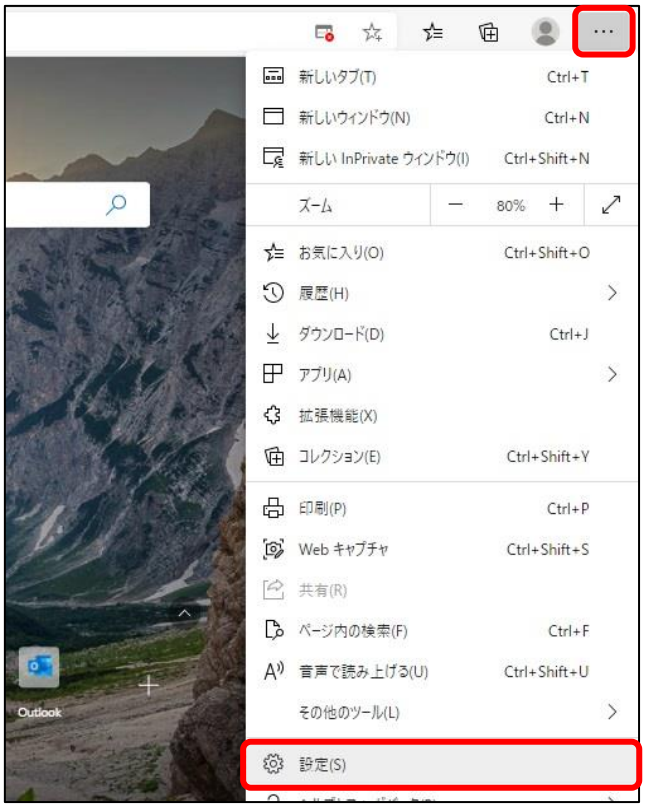
4.2.　電子証明書の削除

失効申請の後、共通認証局において失効処理が完了すると「【クライアント証明書 失効完了の通知】」の通知メールを受信後、「5. 電子証明書の削除」の手順に従い該当の電子証明書の削除を行ってください。
なお、失効処理が完了するまで数日間要する場合があります。

電子証明書の失効手続きの作業はこれで終了です。

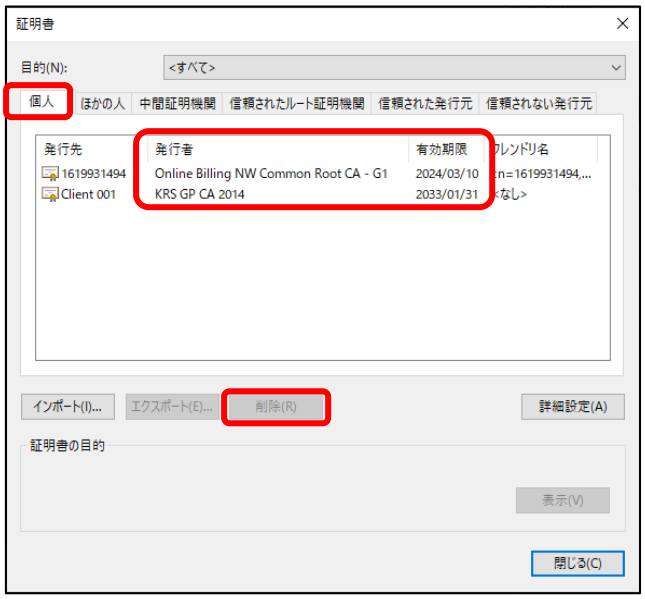
5. 電子証明書の削除

注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

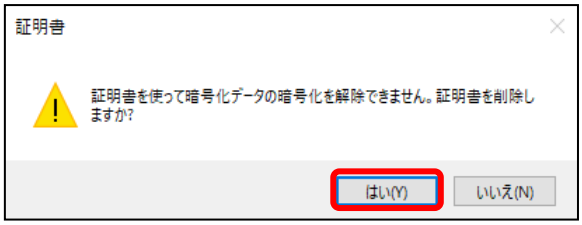


1．Edge を起動し、画面右上の「**設定(S)**」をクリックします。

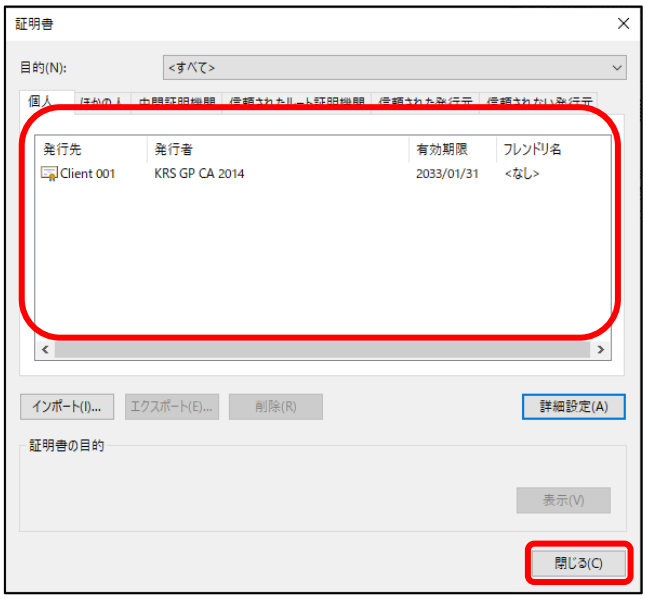
2．「プライバシー、**検索、サービス**」を選択し、「**セキュリティ**」の「**証明書の管理**」をクリックします。



3．「**電子証明書**」が表示されます。「**個人**」タブを開き、**有効期限が古い電子証明書**を選択し、「**削除**」をクリックします。
※発行者が「Online Billing NW Common Root CA」が含まれる表記となっていることを確認します。



4．「**はい**」をクリックします。



5．「**電子証明書**」が表示されます。削除を行った電子証明書が一覧から削除されていることを確認し、「**閉じる**」をクリックします。

注意 上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

6. サポート情報

6.1. MPKI クライアント利用環境

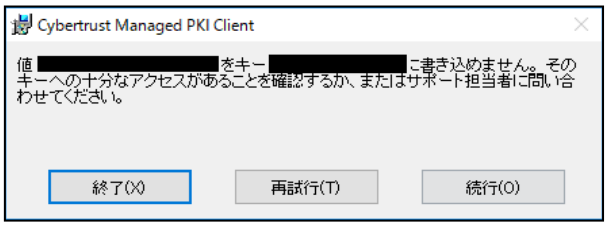
<table>
<tr><td>対応 OS</td><td>
<table>
<tr><td></td><td>32bit</td><td>64bit</td></tr>
<tr><td>Windows 8.1</td><td>○</td><td>○</td></tr>
<tr><td>Windows 10</td><td>○</td><td>○</td></tr>
<tr><td>Windows 11</td><td>-</td><td>○</td></tr>
</table>
</td></tr>
<tr><td>依存するソフトウェア</td><td>MPKI クライアントを利用するためには、ご使用の PC に「Microsoft .NET Framework 4.8」以上がインストールされている必要があります。</td></tr>
<tr><td>表示言語</td><td>日本語のみ</td></tr>
<tr><td>サポートする Proxy 認証の種類</td><td>MPKI クライアントがサポートする Proxy 認証の種類は、以下のとおりです。
・Basic 認証
・NTLM 認証</td></tr>
</table>

6.2. ご利用にあたっての注意事項

6.2.1. 認証用の証明書の選択画面が表示された場合

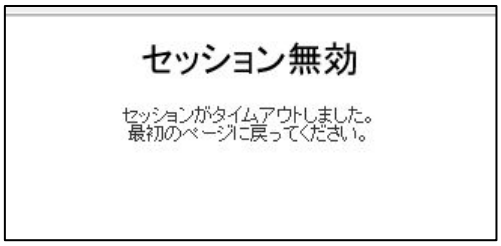
「証明書の選択」画面で発行者が「Online Billing NW Common Root CA」となっていることを確認し、「OK」をクリックしてください。

6.2.2. MPKI クライアントインストール時の注意事項



左記のエラー画面が表示された場合は、「終了」をクリックし、再度インストールを実施ください。

6.2.3. セッション無効時のトラブルシューティング



画面上の操作状態で一定時間作業を行わない場合は、セッションが無効であることを示す画面が表示されます。このような状態では引き続き作業ができないため、右上の「×」をクリックし、ブラウザを閉じた後再度ブラウザからユーザー用 URL へアクセスし直してください。

6.2.4. ルート証明書の取得とインストール

「https://cert.obn.managedpki.ne.jp/p/～」のサイトを開く際に、以下の画面に遷移する場合、下記の手順の通りルート証明書のインストールを実施してください。

6.2.4.1. ルート証明書のダウンロード

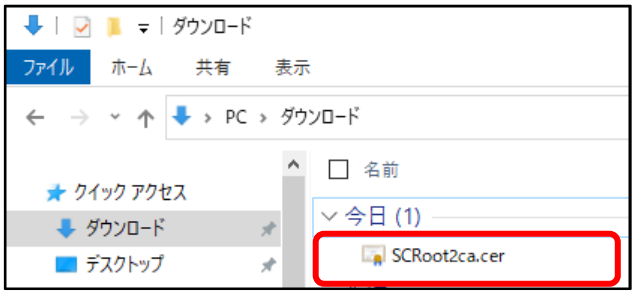
注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

1．<u>オンライン請求ネットワークへ接続の端末</u>からルート証明書のダウンロードサイトにアクセスします。

【ルート証明書ダウンロードサイト】

https://cert.obn.managedpki.ne.jp/p/cert

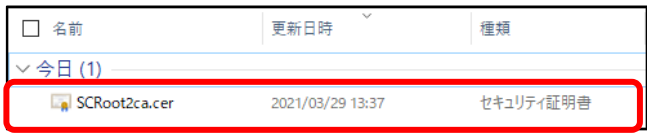
2．画面下の「**保存**」をクリックします。



3．ルート証明書がダウンロードできていることを確認します。

注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

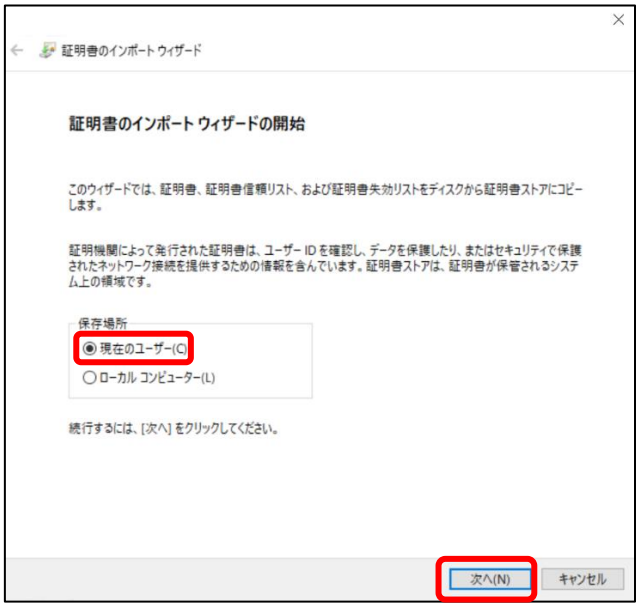
6.2.4.2. ルート証明書のインストール



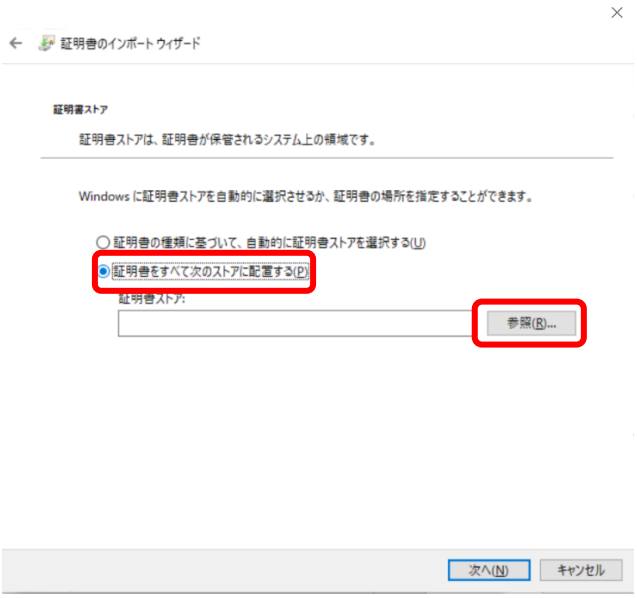
1．ダウンロードしたルート証明書をダブルクリックします。

2．「**セキュリティの警告**」画面が表示されます。「**開く**」をクリックします。

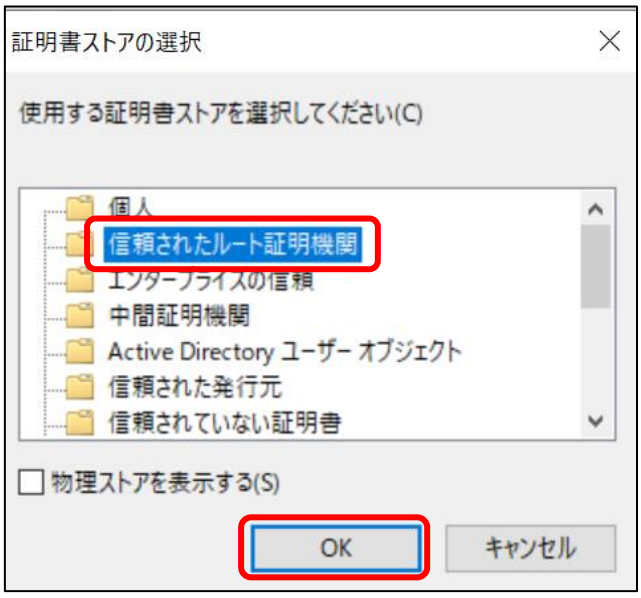
3．「**証明書**」画面が表示されます。「**証明書のインストール**」をクリックします。



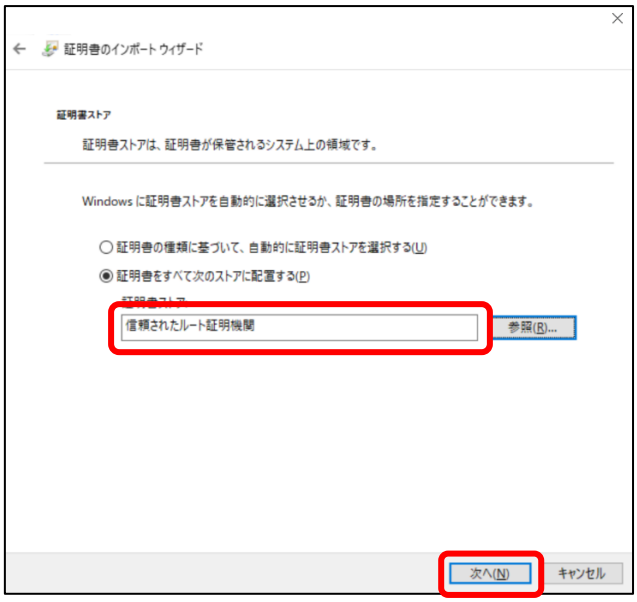
４．「**証明書のインポートウィザード**」画面が表示されます。「**現在のユーザー**」が選択されていることを確認し、「**次へ(N)**」をクリックします。



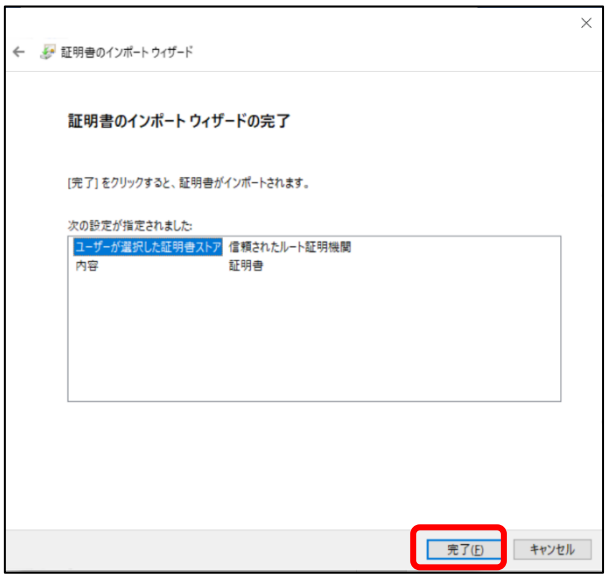
５．「**証明書をすべて次のストアに配置する(P)**」を選択し、「**証明書ストア**」の右側にある「**参照(R)…**」をクリックします。



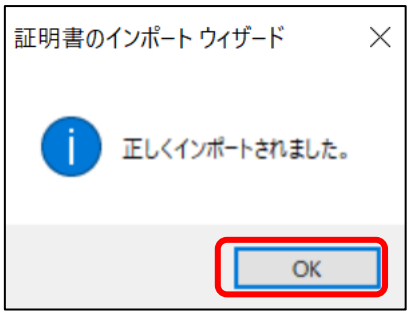
6．「**証明書ストアの選択**」画面が表示されます。「**信頼されたルート証明機関**」を選択して「**OK**」をクリックします。



7．「**証明書のインポートウィザード**」画面が表示されます。「**証明書ストア**」に「**信頼されたルート証明機関**」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。



8．「**完了**」をクリックします。

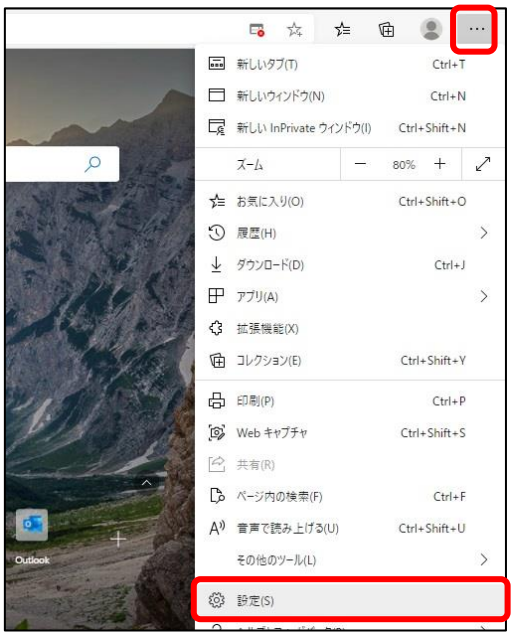


9．「**正しくインポートされました。**」のメッセージを確認し、「**OK**」をクリックします。

6.2.4.3.　登録したルート証明書の確認

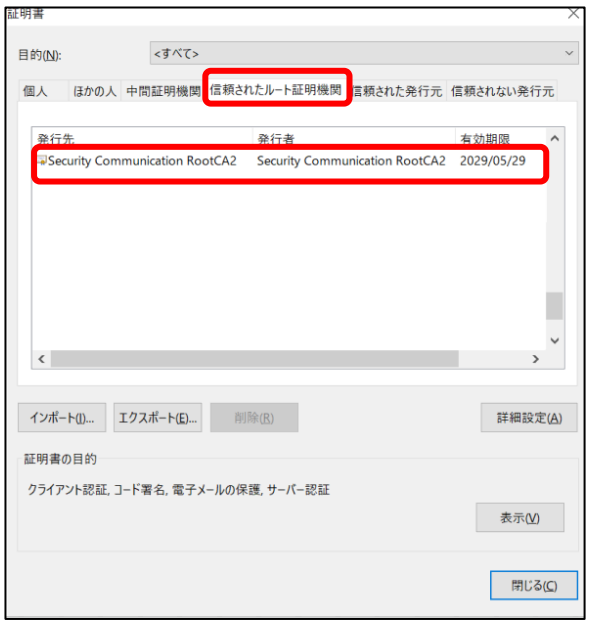
注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

1．Edge を起動します。



2．画面右上の「…」をクリックし、「**設定**」をクリックします。

3．「**プライバシー、検索、サービス**」を選択し、「**セキュリティ**」の「**証明書の管理**」をクリックします。



４．「**証明書**」画面が表示されます。

「信頼されたルート証明機関」タブを開き、発行者が「Security Communication RootCA2」と表示されているルート証明書が登録されていることを確認します。

注意　上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

ルート証明書のインストールの作業はこれで終了です。

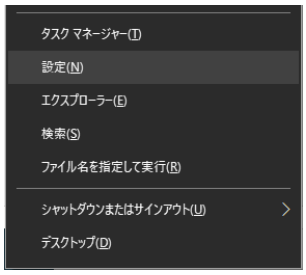
6.3. MPKI クライアントのバージョンアップ

【MPKI クライアントとは】

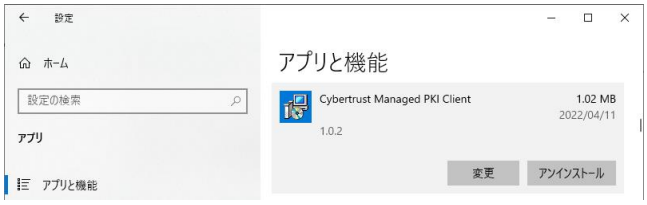
MPKI クライアントを使用すると、有効期限の前に更新をお知らせする機能や電子証明書の更新を簡易に行う機能が利用できます。
MPKI クライアントをインストールできる対象の OS は、Windows 8.1 と Windows 10、または Windows 11 です。
利用環境の詳細は「6.1. MPKI クライアント利用環境」を参照ください。
インストール中にエラーが発生した場合は、「6.2.2. MPKI クライアントインストール時の注意事項」を参照ください。

【バージョンアップとは】

MPKI クライアントは、必要に応じてセキュリティアップデートなどが行われます。アップデートが行われた場合、共通認証局運営主体より、アップデートの周知が行われます。アップデートの周知があった場合に、本章の手順に従って、旧バージョンのアンインストール、最新バージョンのダウンロード・インストールの実施をお願いいたします。



1．オンライン請求ネットワークへ接続の端末で、キーボードの「⊞」キーを押しながら「X」キーを押し、表示された一覧から「**設定**」>［**アプリ**］または「**コントロールパネル**」>「**プログラムと機能**」をクリックします。



2．アンインストールしたいアプリを選択し、「**アンインストール**」または「**アンインストールと変更**」を選択し、画面の指示に沿って、アンインストール作業を行います。

3．「2.1. MPKI クライアントのインストール」の手順に従って、MPKI クライアントのインストール作業の実施をお願いいたします。