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 1.3.1

令和 3 年 4 月 16 日

目次

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
2021/4/16	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

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。

0. 事前準備

証明書の取得には、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］
インターネットから「オンライン資格確認・医療情報化支援基金関係医療機関等向けポータルサイト」を検索し、「各種資料ダウンロード」の「端末の設定や操作について知りたい方はこちら」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://www.iryohokenjyoho-portalsite.jp/download/post-12.html

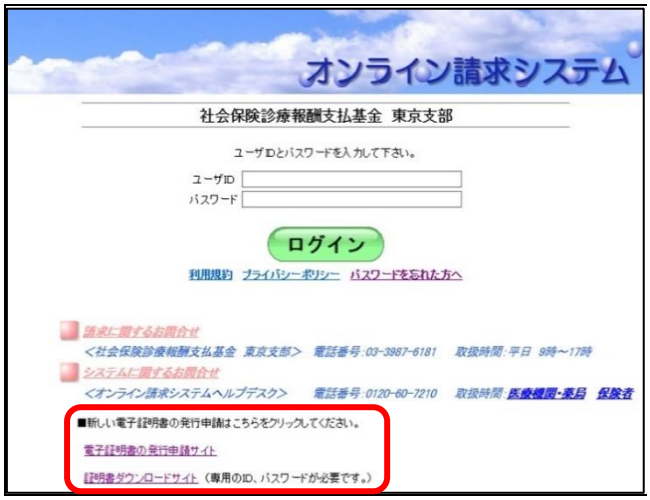
1. 証明書の取得とインストール

1.1. 証明書のダウンロード

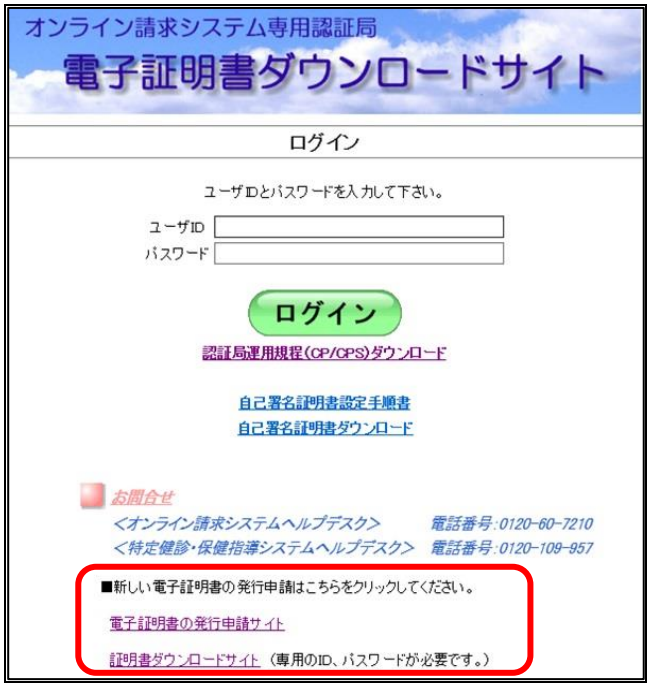
オンライン請求ネットワークへ接続の端末（レセプトオンライン請求用端末またはオンライン資格確認端末）で証明書を取得します。

【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．**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**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

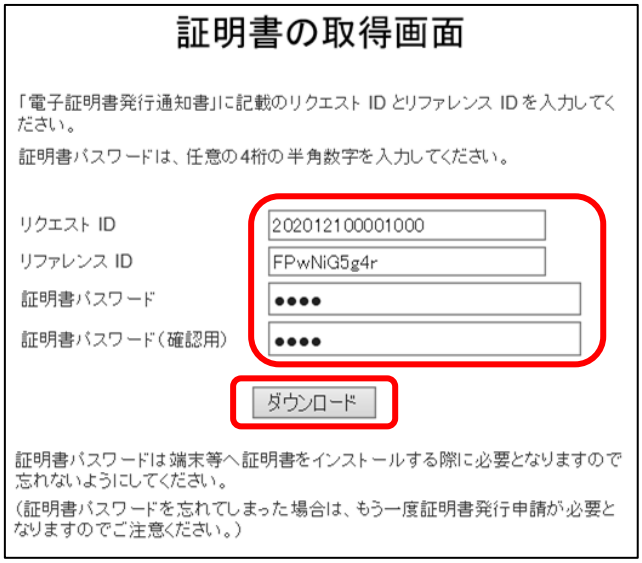
【レセプトオンライン請求用端末の場合】

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。

【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】

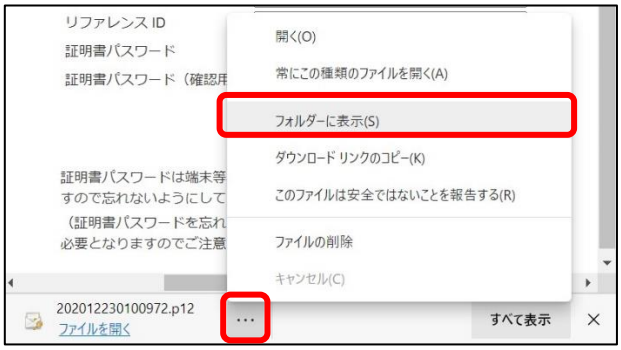
「医療機関等向けセットアップ手順書」に沿ってセットアップを行った方は、デスクトップにあるダウンロードサイトのアイコンからアクセスできます。



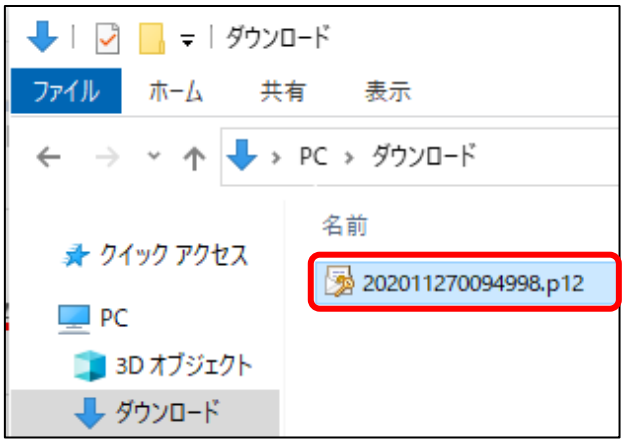
２．証明書発行通知書に記載のリクエストIDとリファレンスID及び任意のパスワード（半角数字4桁）を入力し、「**ダウンロード**」をクリックします。

【注意】

入力した証明書パスワードは、「1. 2. 証明書のインストール」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。**



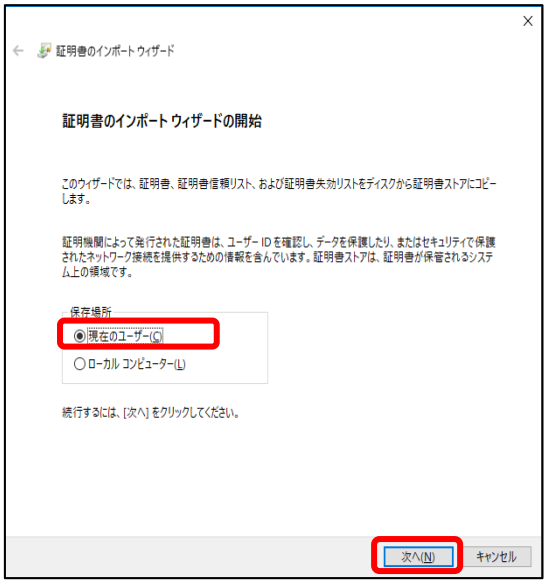
３．画面下の【…】をクリックし、「**フォルダに表示**」をクリックします。



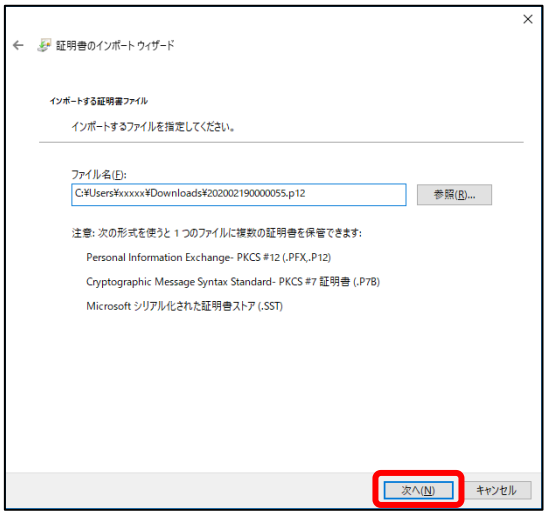
４．証明書がダウンロードできていることを確認します。

1.2. 証明書のインストール

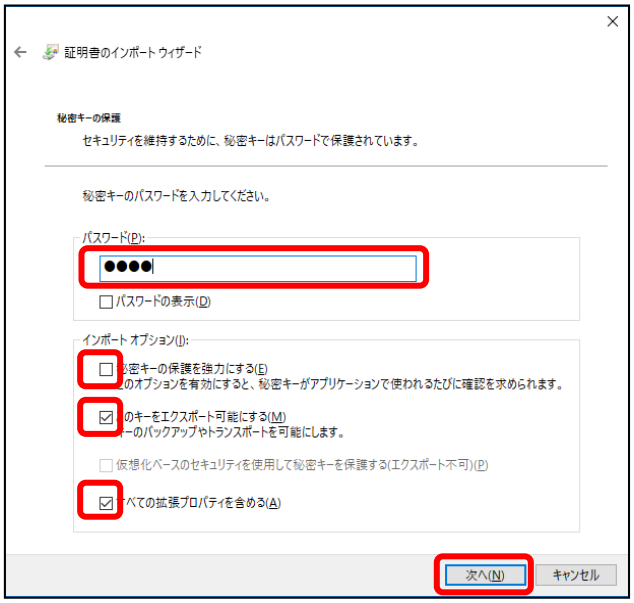
1．ダウンロードした証明書ファイルを右クリックし、「**PFX インストール**」をクリックします。



2．「**現在のユーザー**」を選択し、「**次へ**」をクリックします。



3．フィル名に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。

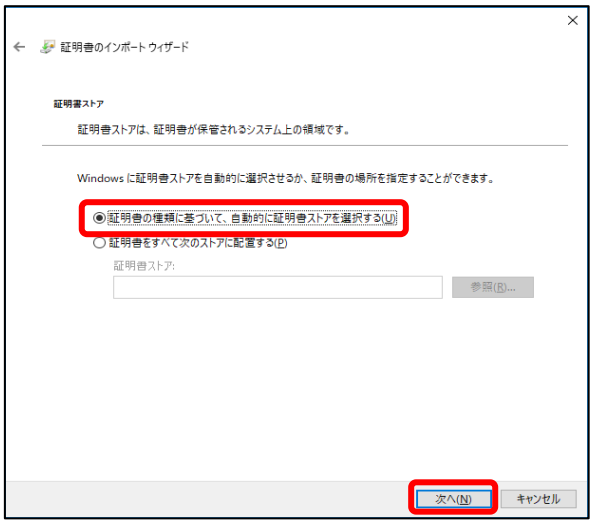


4．［パスワード］に**「1.1.証明書のダウンロード」で設定したパスワードを入力**します。

［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
チェックする
［すべての拡張プロパティを含める］を
チェックする

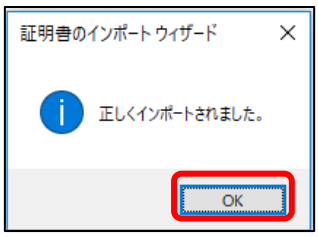
【こんなときは！】

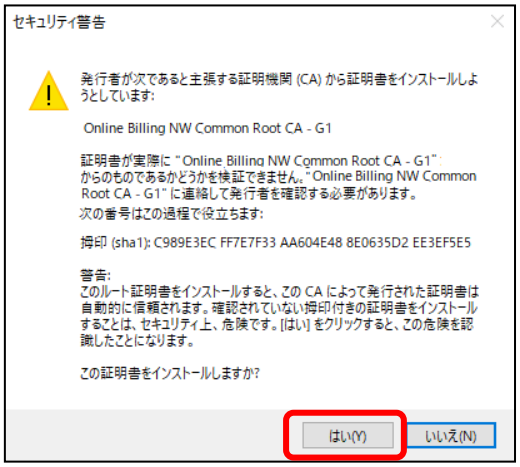
「秘密キーの保護を強力にする」のチェックが外せない場合は、セキュリティを強化する設定がされているため、P10「1.2.1 こんなときは！」を参照



5．**「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．「**完了**」をクリックします。





7．「**OK**」をクリックします。

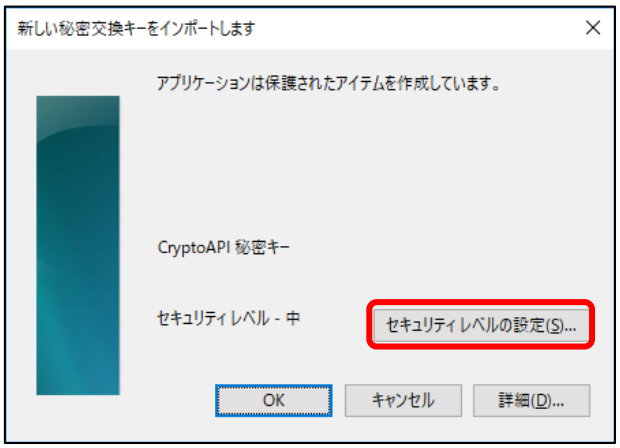
【こんなときは！】

「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。

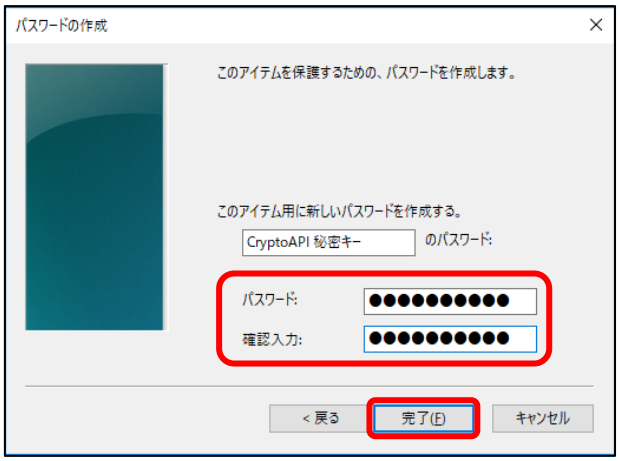
「証明書発行者（認証局）の証明書」は、インストールを行った証明書が「証明書発行者（認証局）」によって発行された証明書であることを確認（ご使用のブラウザが自動的に確認）する時に必要です。「いいえ」をクリックした場合は、「1.2.証明書のインストール」を再度行ってください。

1.2.1 こんなときは！

※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「1.4. 登録した証明書の確認」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。

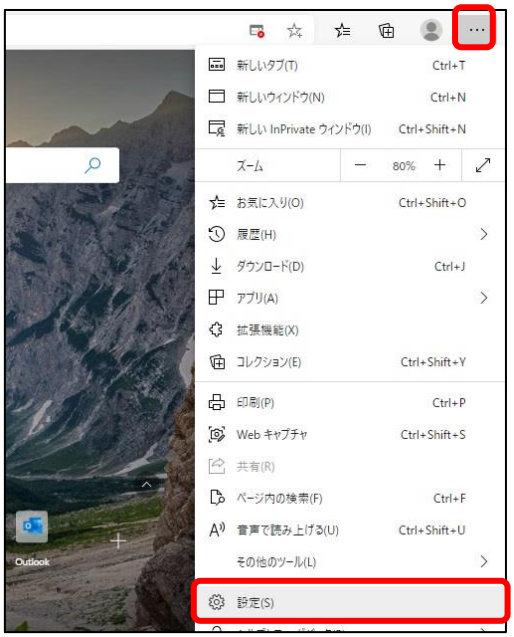
【※重要※】

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。

1.3. 登録した証明書の確認

1．Edge を起動します。



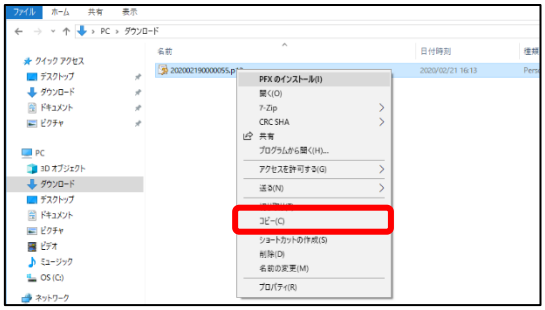
2．画面右上の【…】をクリックし、「**設定**」をクリックします。

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。

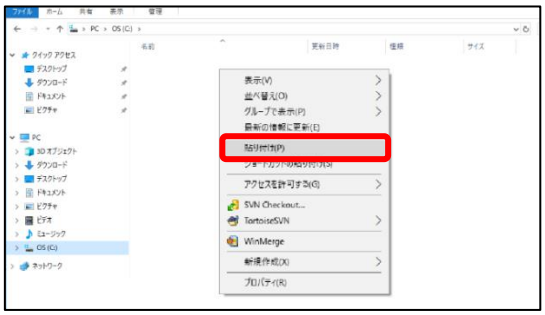
４．「**個人**」タブを開き、発行者が「**Online Billing NW Common Root CA**」と表示されている証明書が登録されていることを確認します。

1.4. 証明書のバックアップ

外部記録媒体等へ証明書をバックアップします。バックアップした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します。その際には、「1.1.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】

「証明書」「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。証明書の情報が第三者に知られると、証明書が不正に使用される恐れがあります。
証明書を紛失した場合、または、第三者に知られた可能性がある場合は、速やかに証明書失効申請を行ってください。また、パソコンを紛失した場合も証明書が不正に使用される恐れがあります。速やかに証明書失効申請を行ってください。

証明書のインストール作業はこれで終了です。

1.5. MPKI クライアントインストール
（更新時に簡単に更新ができるツール）

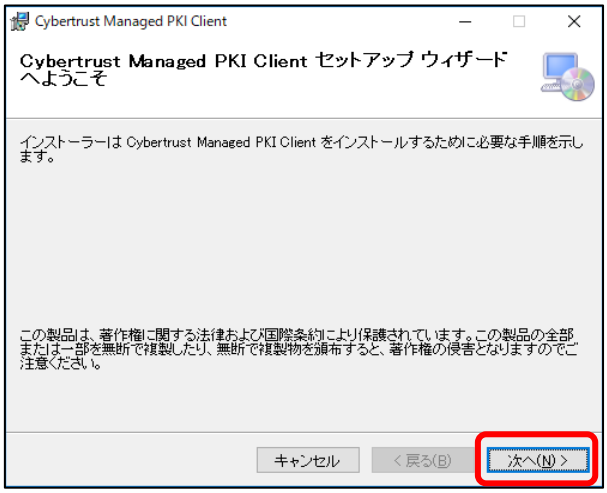
【MPKI クライアントとは】

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、Windows8 と Windows10 です。
利用環境の詳細は「5.1 MPKI クライアント利用環境」を参照ください。

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

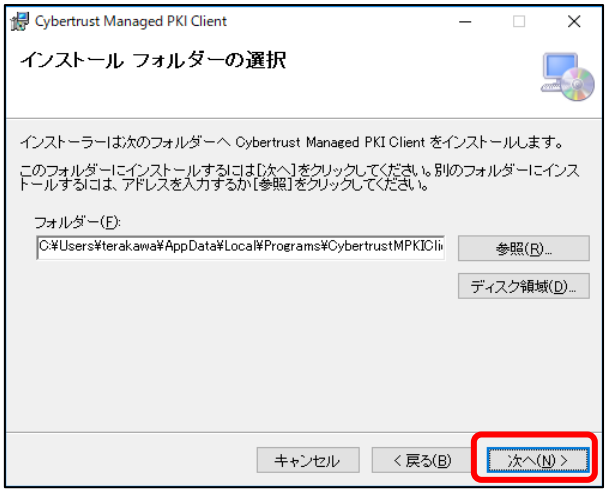
2．【…】をクリックし、「**フォルダに表示**」をクリックします。

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。

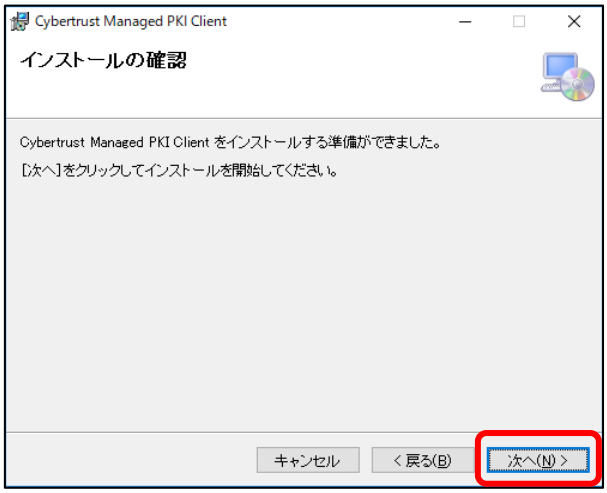


4．「Cybertrust Managed PKI Client セットアップウィザード」が開始されます。

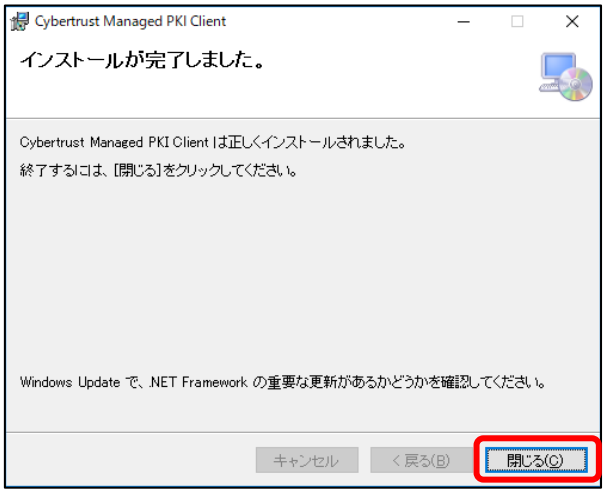
「**次へ**」をクリックします。



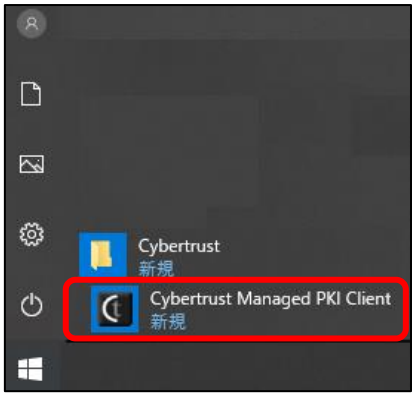
5．「**次へ**」をクリックします。



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以下が追加されます。

1.6. 認証用の証明書の選択画面が表示された場合

1．「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。

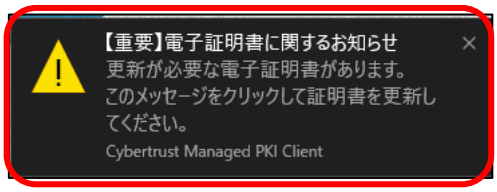
2. 証明書の更新

2.1. MPKI クライアントを利用した更新

証明書の有効期限が迫ると、お知らせが表示されます。有効期限が切れる前に、「2.2.証明書の更新手順」の作業を行ってください。

【お知らせが表示される条件】

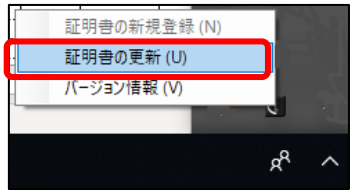
有効期限が切れる 90 日前、60 日前、30 日前、15 日前、7 日前から毎日
有効期限が切れた場合

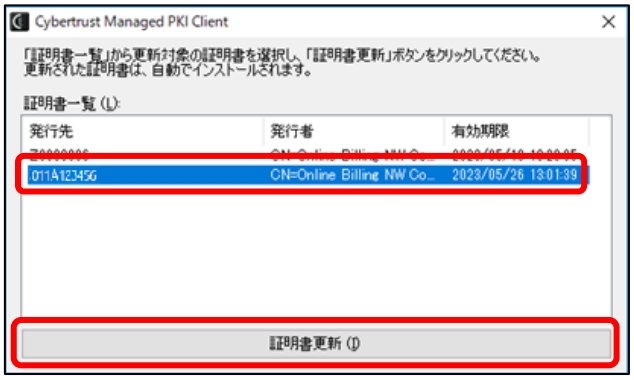


1．「**証明書に関するお知らせ**」通知をクリックします。

【こんなときは！】

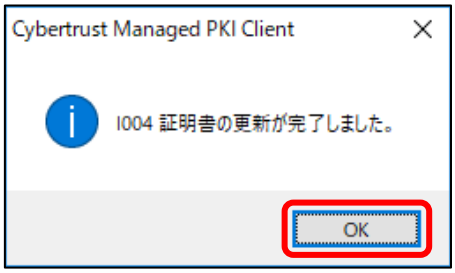
お知らせが表示されていない場合は、タスクトレイのアイコンを右クリックから操作できます。表示される以下のメニューから、[証明書の更新] をクリックします。





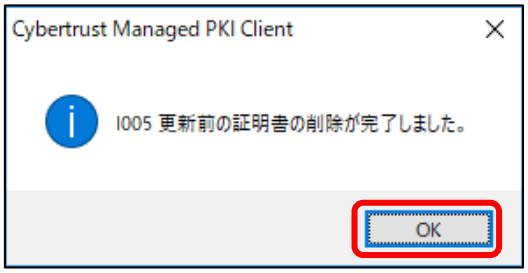
2．**更新したい証明書**を選択し、「**証明書更新**」をクリックします。

3．「**はい**」をクリックします。



4．「**OK**」をクリックします。

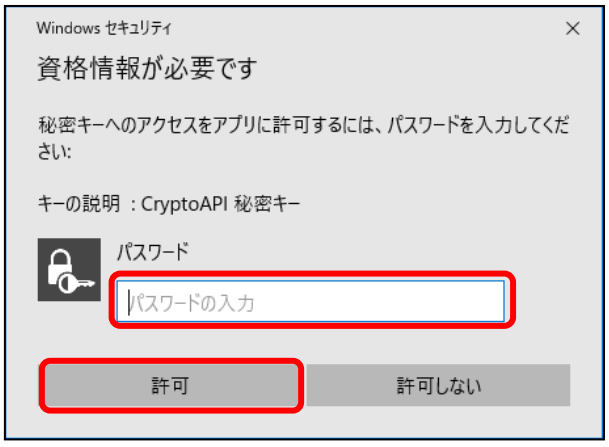
5．「**はい**」をクリックします。



6．「**OK**」をクリックします。

2.1.1 こんなときは！

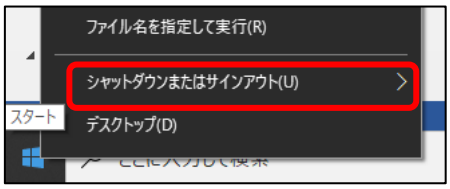
※パスワードの入力が求められた場合は、証明書のインストール時「1.2.1　こんなときは！」で設定したパスワードを入力します。



1．パスワードを入力し、「**許可**」をクリックします。

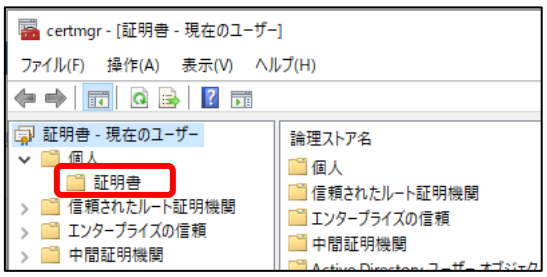
※パスワードは、証明書のインストール時「1.2.1　こんなときは！」で設定したパスワードです。

2.1.2 MPKI クライアント利用時の証明書バックアップ



1．画面の左下の Windows ボタンを右クリックし、「**ファイル名を指定して実行（R)**」をクリックします。

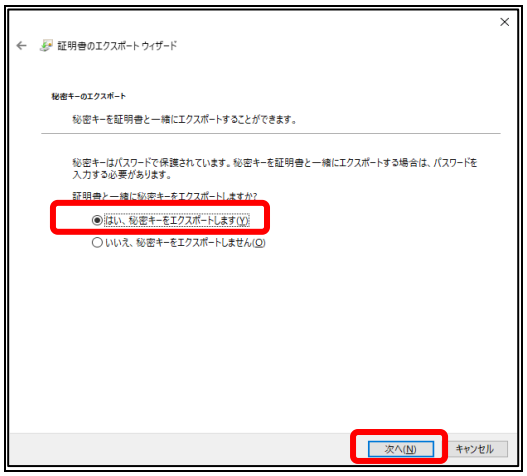
2．「**certmgr.msc**」を入力し、「**ＯＫ**」ボタンをクリックします。



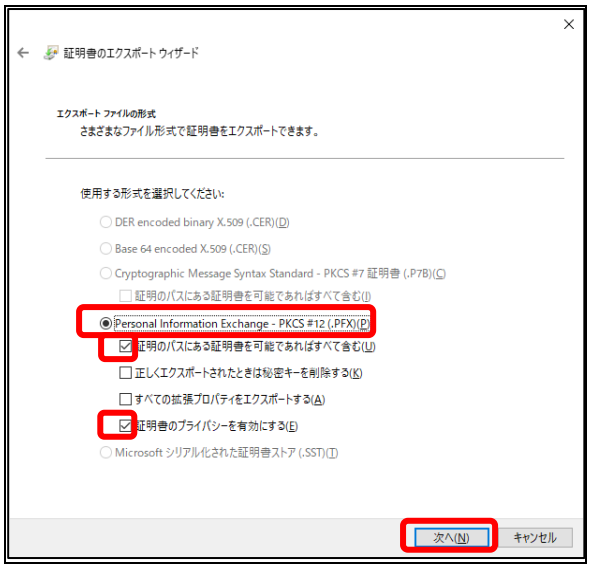
3．「**個人**」から「**証明書**」をクリックします。

4．発行者が「**Online Billing NW Common Root CA**」の有効期限が新しい証明書を選択し、右クリック後、「**すべてのタスク**」-「**エクスポート**」をクリック。

5．「**次へ**」をクリックします。



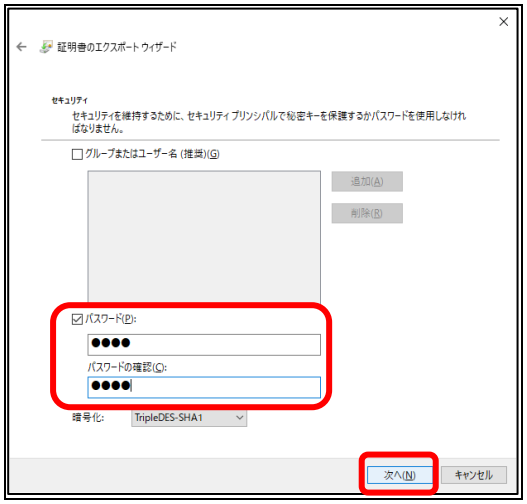
６．「**はい、秘密キーをエクスポートします**」を選択し、「**次へ**」ボタンをクリックします。



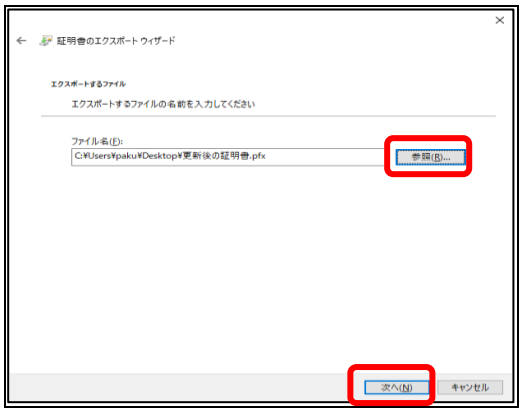
７．「Personal Information Exchange - PKCS#12(.PFX)」を選択し、「**証明のパスにある証明書を可能であればすべて含む**」と「**証明書のプライバシーを有効にする**」にチェックを入れて「**次へ**」ボタンをクリックします。

【こんなときは！】

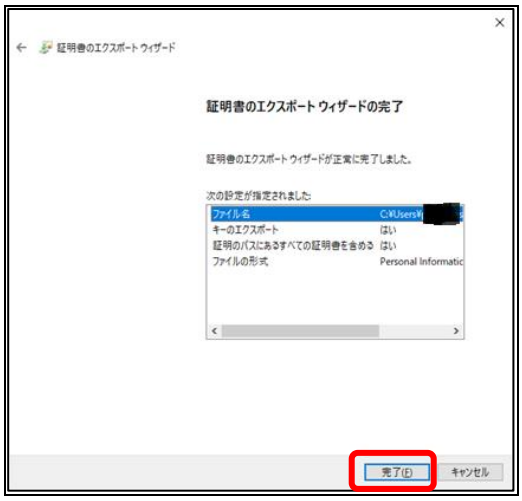
非活性（グレーアウト）で選択できない場合は、管理者権限を持っているユーザで再度バックアップ手順を実施してください。



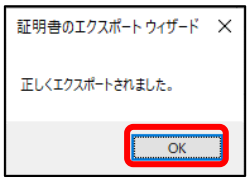
８．「**パスワード**」と「**パスワードの確認**」を入力し、「**次へ**」ボタンをクリックします。



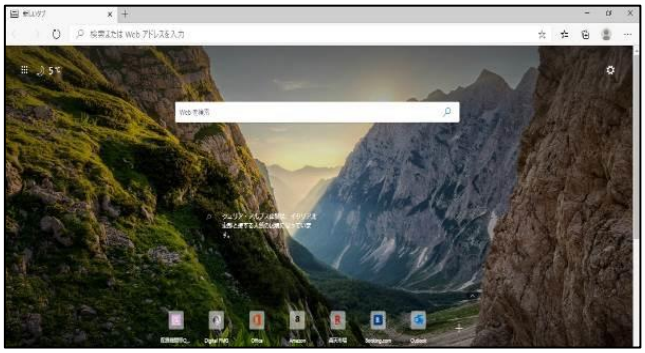
９.「**参照**」ボタンをクリックして、証明書をバックアップするフォルダを選択し、「**次へ**」をクリックします。



１０.「**完了**」ボタンをクリックします。「**証明書のエクスポートウィザードが正常に完了しました**」が表示され、「**ＯＫ**」をクリックします。



2.2. 更新申請画面からの更新



１．**更新対象の証明書がインストールされた端末**から更新申請画面へアクセスします。

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

２．更新対象の証明書を選択し、「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．証明書ステータスが「**発行済み**」となれば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、**任意のパスワード半角数字４桁**を入力し、「Submit」をクリックします。

注意】

入力した証明書パスワードは、「3.2.証明書のインストール」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。**

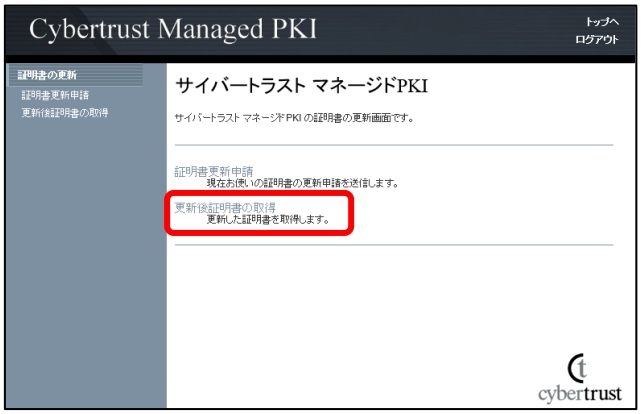
７．「Download」をクリックし、証明書を保存します。

８．証明書のインストールは、「1.2　証明書のインストール」を参照ください。

９．「4. 証明書の削除」を参照し、古い証明書を削除ください。

2.2.1 こんなときは！

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証明書または鍵の取得に失敗した場合は、再度証明書または鍵を取得してください。

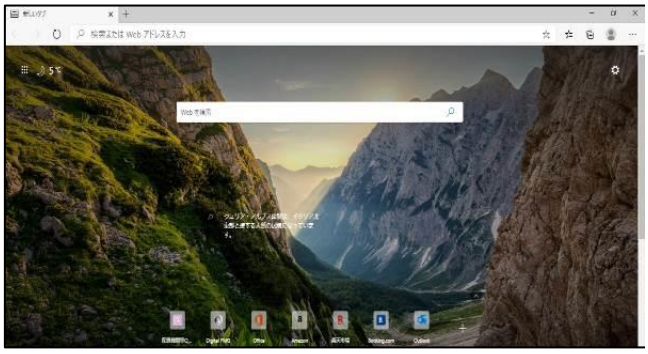


1．更新申請画面の「**更新後証明書の取得**」をクリックします。

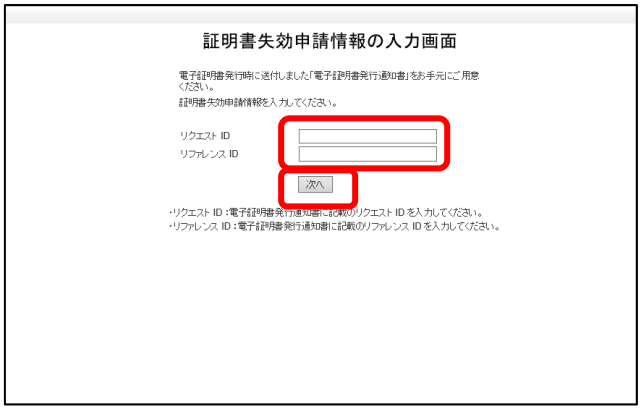
○一覧に情報が表示されている場合は、対象の更新済み証明書の「**Download Key**」ボタンをクリックして証明書を取得してください。

・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、「2.2.更新申請画面からの更新」からやり直してください。

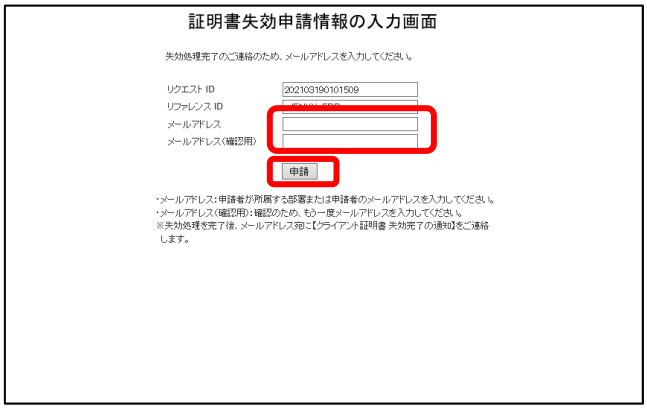
3. 証明書の失効



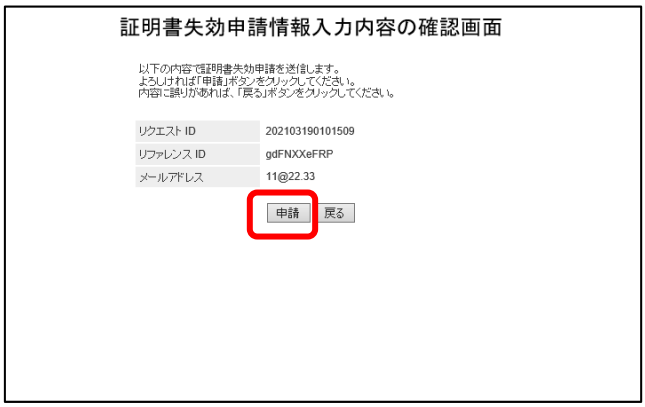
１．**更新対象の証明書がインストールされた端末**から失効申請画面へアクセスします。
https://cert.obn.managedpki.ne.jp/p/rx



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」が切り替えます。



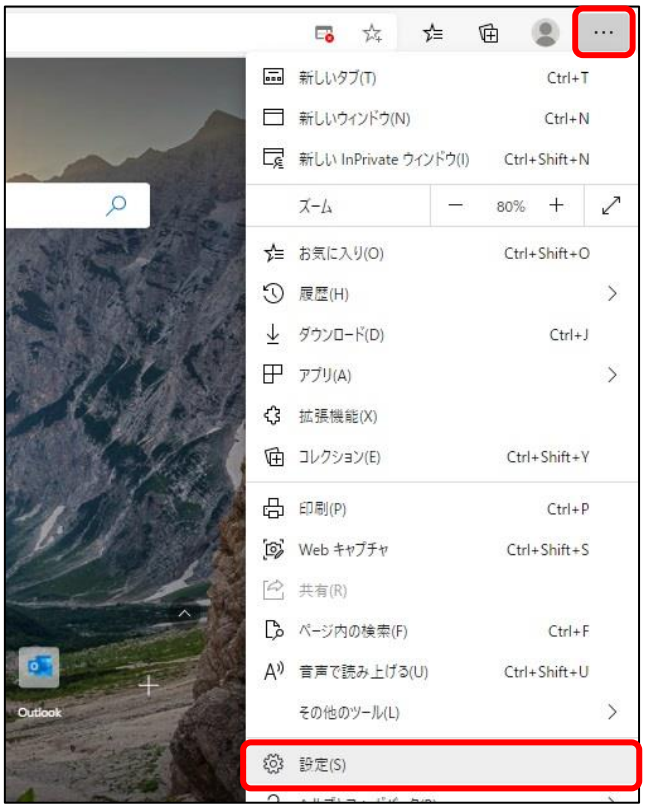
３．失効申請者の申請者のメールアドレスとメールアドレス(確認用)を入力し、「**申請**」をクリックします。「証明書失効申請情報の確認画面」へ遷移します。



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。

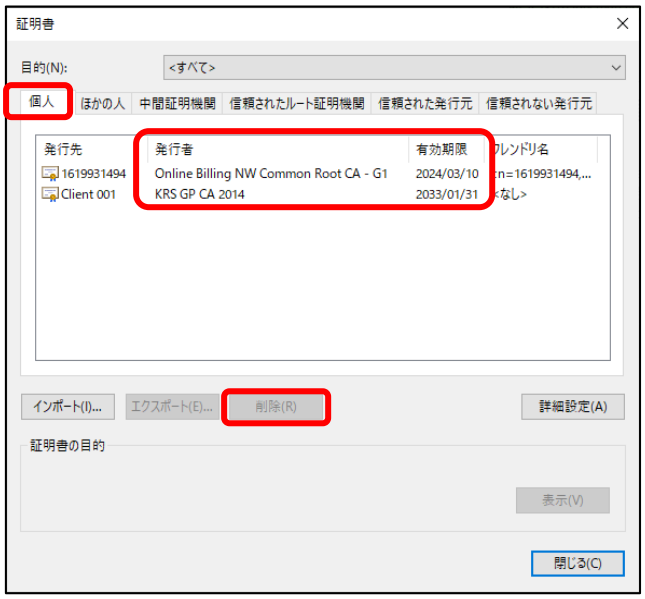
５．「4. 証明書の削除」を参照し、失効申請をした証明書を削除ください。

4. 証明書の削除

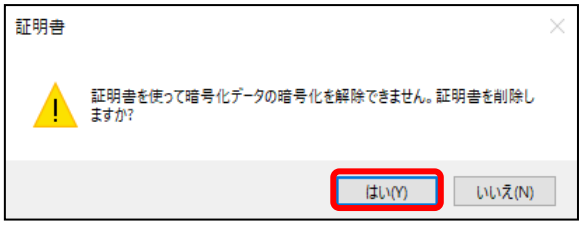


1．Edge を起動し、画面右上の「**設定**」をクリックします。

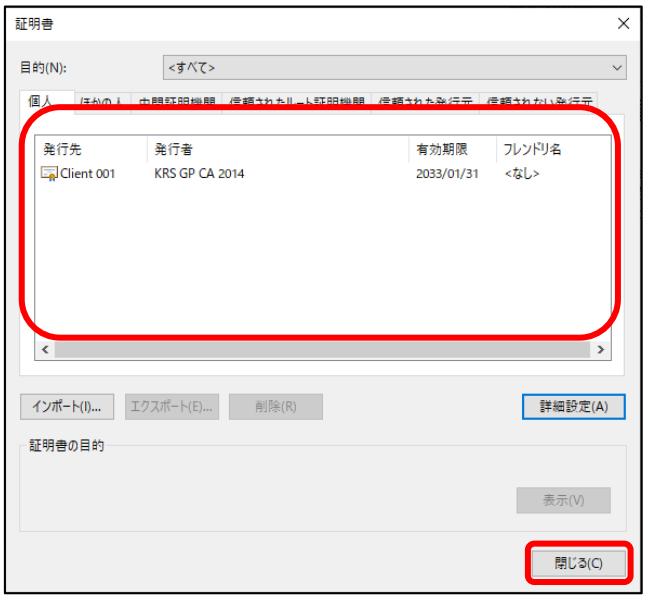
2．「**プライバシー、検索、サービス**」を選択し、「**セキュリティ**」の「**証明書の管理**」をクリックします。



3．「**個人**」タブを開き、**有効期限が古い証明書**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．削除を行った証明書が一覧から消えていることを確認し、「**閉じる**」をクリックします。

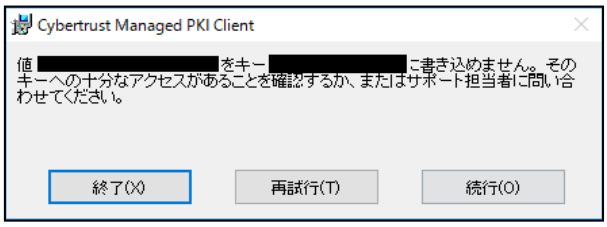
5. サポート情報

5.1. 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>
</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 3.5」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>

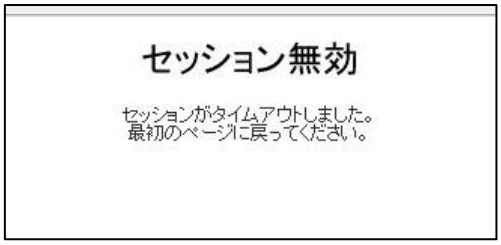
5.2. ご利用にあたっての注意事項

5.2.1 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。

5.2.2 セッション無効時の対応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。