電子証明書の更新（Windows_ChromiumEdge版）

本資料では、電子証明書の更新手順を説明します。

■2026年10月　1.3版

作業の流れ

電子証明書の更新の作業の流れについて説明します。

①事前確認 ▶ ②電子証明書の更新

電子証明書の更新作業は、
<u>更新対象の電子証明書がインストールされている端末</u>で実施します。

電子証明書は**使用する端末1台につき、1枚必要**です。各システムを異なる端末で使用されている場合、それぞれ更新作業を行う必要があります。

※「端末名称等」は、電子証明書がどの端末にインストールされているか特定するために、電子証明書申請時に申請者様がご入力された情報です。この情報も参考に、電子証明書がインストールされている端末を特定し、更新手続きを行ってください。

①事前確認

電子証明書の更新前に以下を確認してください。

準備 1	更新対象の電子証明書がインストールされている端末を特定する → 2ページへ
準備 2	更新を行う端末のMPKIクライアント（※）の導入有無を確認する → 4ページへ

（※）電子証明書の更新のための専用アプリ

4ページをご確認いただいた上で導入有無が不明の際は設置業者様へご確認ください。

②電子証明書の更新

A. MPKIクライアントが<u>導入されている場合</u>
→MPKIクライアントを使用して更新（5ページへ）

B. MPKIクライアントが<u>導入されていない場合</u>
→電子証明書更新申請サイトで更新（19ページへ）

更新が必要な端末（電子証明書）の確認方法

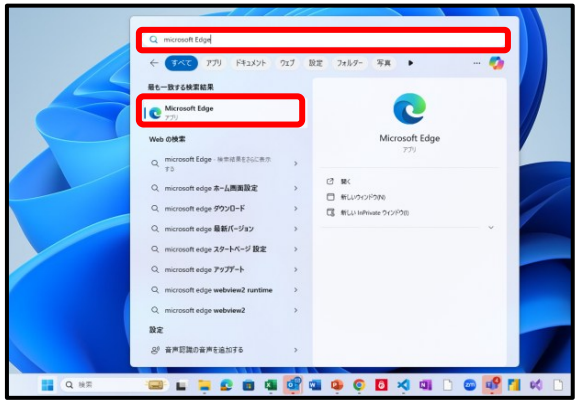
準備1 更新対象の電子証明書がインストールされている端末を特定する

オンライン資格確認、オンライン請求で利用しているパソコンにインストールされている電子証明書の有効期限を確認します。

注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

1 電子証明書の更新を実施する端末のタスクバーのスタートメニューをクリックします。※もしスタートメニューがない場合は検索バーをクリックします。

2 検索欄に「Microsoft Edge」を入力し、「Microsoft Edge」のアプリをクリックします。



3 Microsoft Edge画面右上の「…」をクリックし、「設定」をクリックします。

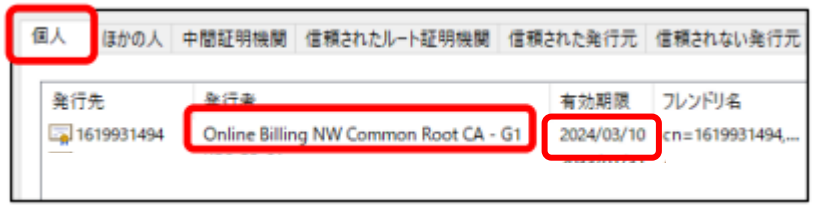
更新が必要な端末（電子証明書）の確認方法

準備1 更新対象の電子証明書がインストールされている端末を特定する

オンライン資格確認、オンライン請求で利用しているパソコンにインストールされている電子証明書の有効期限を確認します。

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

5 「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の有効期限を確認します。
<u>有効期限が90日未満になっているものが更新対象の電子証明書</u>です。



注意	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

更新対象の電子証明書がインストールされている端末が特定できました。
→準備2へ進みます。

MPKIクライアントの導入有無を確認

準備2

更新を行う端末のMPKIクライアントの導入有無を確認する

Windowsのスタートメニューから、MPKIクライアントが導入されているか確認します。

「MPKIクライアント」とは
電子証明書の更新に使うWindows用のアプリです（正式名称：Cybertrust Managed PKI Client）。
このアプリが導入されている端末では、アプリ上で電子証明書の更新が完了します。

1 Windowsのスタートボタンをクリックし、スタートメニューを開きます。

Windows10の場合

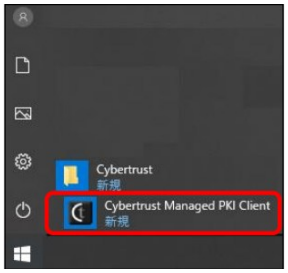
ディスプレイ左下にある以下のボタンがスタートボタンです。
クリックするとスタートメニューが開きます。

Windows11の場合

ディスプレイ中央下部にある画像のボタンがスタートボタンです。
クリックするとスタートメニューが開きます。

2 「**Cybertrust Managed PKI Client**」が表示されていれば、MPKIクライアント導入済です。

Windows10の場合



Windows11の場合

MPKIクライアントが導入されている場合
→次のページへ進んでください。

MPKIクライアントが導入されていない場合
→19ページへ進んでください。

A. 電子証明書の更新（MPKIクライアント導入済み）

本資料では、電子証明書の更新手順を説明します。

電子証明書の更新
（MPKIクライアント導入済み）

作業手順をご確認ください。
確認後、MPKIクライアントツール導入済みの方は次ページの手順へ進んでください。

手順 1　**MPKIクライアントの最新のバージョンを調べる**

▼

手順 2　**更新作業端末のMPKIクライアントのバージョンを確認する**

バージョンが最新の場合は手順4へ進みます。

▼

手順 3　**MPKIクライアントをバージョンアップする**

▼

手順 4　**タスクトレイにMPKIクライアントがあることを確認する**

▼

手順 5　**MPKIクライアントを用いて、証明書を更新する**

▼

手順 6　**外部記録媒体に電子証明書をバックアップする**

A. MPKIクライアントを用いた更新手順

手順1 MPKIクライアントの最新バージョンを調べる

MPKIクライアントのバージョンアップが必要な場合があります。まず、MPKIクライアントの最新バージョンを調べます。

注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

1 以下のURLから、医療機関等向け総合ポータルサイトへアクセスします。

医療機関等向け総合ポータルサイト
（こちらをCtrl押しながらクリックするとサイトへアクセスいただけます。）

https://iryohokenjyoho.hpdx.or.jp/csm?id=kb_article_view&sysparm_article=KB0011365

2 手順書・マニュアル一覧が表示されます。
「２．端末の設定や操作について知りたい方はこちら ⑨アプリケーションバージョン情報」をクリックします。

KB0011365

「手順書・マニュアル」の一覧

更新者：管理者95・ 8 日前・ 表示回数：492851・★★☆☆☆

1.アカウントの登録・変更について知りたい方はこちら

① アカウント関連の手順書

2.端末の設定や操作について知りたい方はこちら

① 端末の設定をするには（セットアップ手順書）
② 診療/薬剤情報・特定健診情報を閲覧するためには（セットアップ手順書）
③ 操作マニュアル
④ 電子証明書更新を簡単にするために
⑤ ネットワーク接続ガイド
⑥ オンライン資格確認等システムとの接続に係るネットワーク連携のパターン参考例
⑦ 医療機関等のテストに関する資料
⑧ セキュリティガイドライン等
⑨ アプリケーションバージョン情報

	内容	文書名等	更新日	版
A	医療機関等が導入するアプリケーション等バージョン情報	導入アプリケーション等のバージョン情報	2025/1/27	-

3 「**導入アプリケーション等のバージョン情報**」のファイルでMPKIクライアントのバージョンを確認します（画像の赤枠部分をご確認ください）。

「資格確認端末セットアップ手順書」において導入いただく支払基金が提供するアプリケーション等情報
※ 2025/O/O時点（左記の日付にバージョンアップしたアプリケーションのバージョン情報を赤字で記載）

#	アプリケーション名称	掲載ファイル	バージョン情報
1	連携アプリケーション	OQSComApp.zip	
2	ブラウザ拡張プラグイン（顔認証ライブラリ含む）	OQSFaceApp.zip	
3	配信アプリケーション	OQSDistroApp.zip	
4	MPKIクライアント	CybertrustManagedPKIClient.zip	X.X.X.X
5	環境切替ツール	ChangeEnvironment.zip	
6	顔認証付きカードリーダーアプリケーション		
	－富士通Japan株式会社	本人認証用カードリーダーソフト Caora ファームウェア	
	－パナソニック コネクト株式会社	XC-STFR1J-MN XC-STFR2J-MN	
	－株式会社USEN-ALMEX	管理コンソール アップデート管理ツール カードリーダー本体	
	－キヤノンマーケティングジャパン株式会社	管理アプリケーション アプリケーション OSソフトウェア	
	－アトラス情報サービス株式会社	アプリケーション カードリーダー本体	

4 表示されている数字がアプリの最新バージョンとなります。
表示されている数字をメモなどに控えておいてください。

注意	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

最新のMPKIクライアントのバージョンをメモしました。
→手順2へ進みます。

A. MPKIクライアントを用いた更新手順

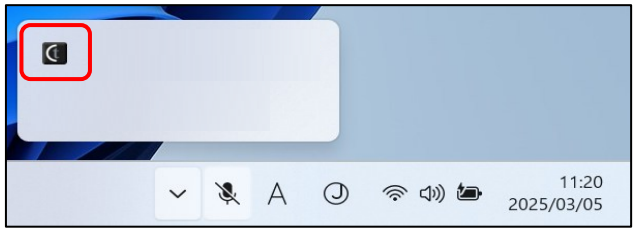
手順 2 更新作業端末のMPKIクライアントのバージョンを確認する

現在のMPKIクライアントのバージョンを確認し、バージョンアップが必要かどうか判断します。

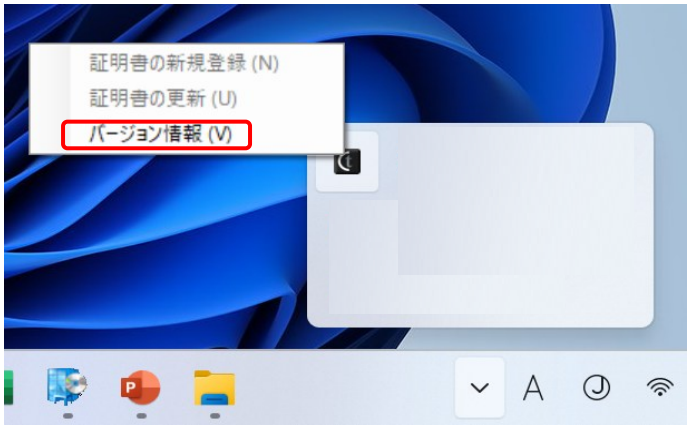
1 電子証明書の更新作業を行っている端末のデスクトップ右下より、「隠れているインジケーターを表示する」をクリックします。

2 タスクトレイが表示されます。タスクトレイの中に、以下のMPKIクライアントのアイコンが表示されていることを確認してください。

MPKIクライアントのアイコン



3 アイコンの上で右クリックし、バージョン情報をクリックします。



A. MPKIクライアントを用いた更新手順

手順 2

更新作業端末のMPKIクライアントのバージョンを確認する

現在のMPKIクライアントのバージョンを確認し、バージョンアップが必要かどうか判断します。

4 現在インストールされているMPKIクライアントのバージョンが確認できます。
バージョンを確認したら、OKを押します。

5 手順１の④（6ページ）で控えたバージョンの数字と資格確認端末内のアプリのバージョンの数字を比べます。

アプリのバージョンが6ページの最新バージョンより古い（数字が小さい）場合
→次のページの手順3に進んでください。

アプリのバージョンが6ページの最新バージョンになっている（数字が同じ）場合
→14ページの手順４に進んでください。

A. MPKIクライアントを用いた更新手順

手順 3

MPKIクライアントをバージョンアップする

電子証明書の更新で使用するMPKIクライアントをアンインストール（削除）して最新版をインストールします。

1 Windowsのスタートボタンの上で右クリックします。

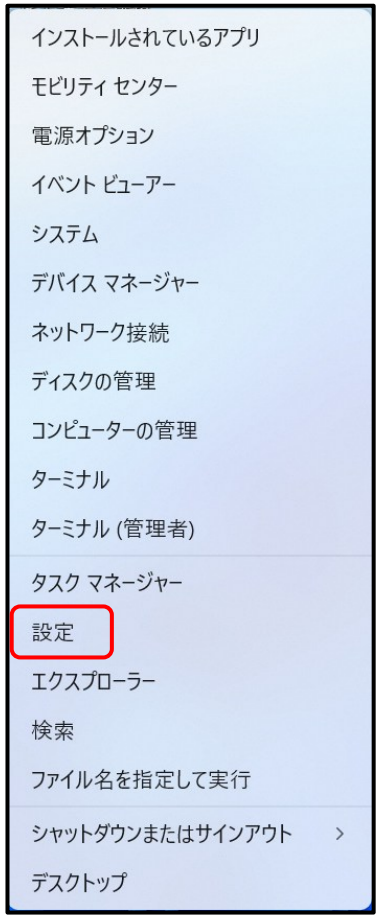
2 表示されたメニューから、「設定」をクリックします。

Windows10の場合

ディスプレイ左下にある以下のボタンがスタートボタンです。
クリックするとスタートメニューが開きます。

Windows11の場合

ディスプレイ中央下部にある画像のボタンがスタートボタンです。
クリックするとスタートメニューが開きます。



A. MPKIクライアントを用いた更新手順

手順 3

MPKIクライアントをバージョンアップする

電子証明書の更新で使用するMPKIクライアントをアンインストール（削除）して最新版をインストールします。

3 画面左側に表示されるメニューより、「アプリ」をクリックします。

4 「インストールされているアプリ」をクリックします。

A. MPKIクライアントを用いた更新手順

手順 3

MPKIクライアントをバージョンアップする

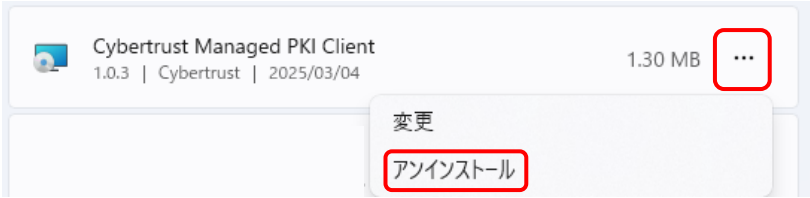
電子証明書の更新で使用するMPKIクライアントをアンインストール（削除）して最新版をインストールします。

5 アプリの一覧が表示されます。「**Cybertrust Managed PKI Client**」を探し、アンインストールをクリックしてください。

Windows10の場合

Windows11の場合

「・・・」をクリックするとポップアップが出ます。アンインストールをクリックします。



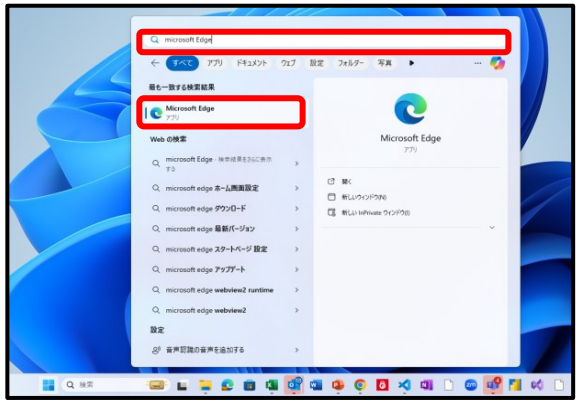
6 画面の指示に従い、**MPKIクライアント**をアンインストールしてください。

MPKIクライアントのアンインストールが完了しました。
この後、最新のMPKIクライアントを再インストールします。
⑦へ進んでください。

注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

7 電子証明書の更新を実施する端末のタスクバーのスタートメニューをクリックします。※もしスタートメニューがない場合は検索バーをクリックします。

8 検索欄に「Microsoft Edge」を入力し、「Microsoft Edge」のアプリをクリックします。



A. MPKIクライアントを用いた更新手順

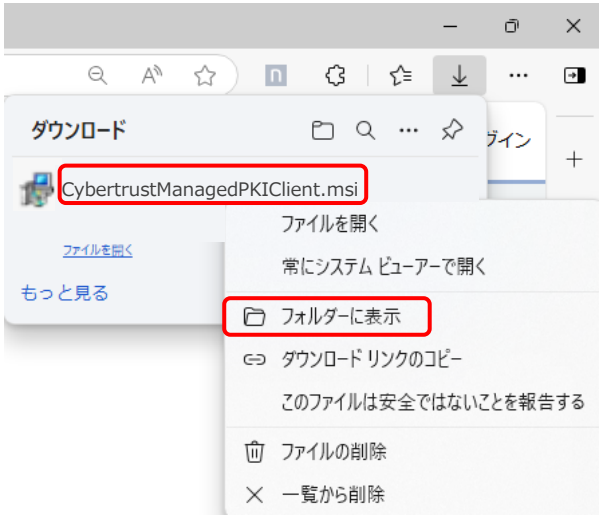
手順3 MPKIクライアントをバージョンアップする

電子証明書の更新で使用するMPKIクライアントをアンインストール（削除）して最新版をインストールします。

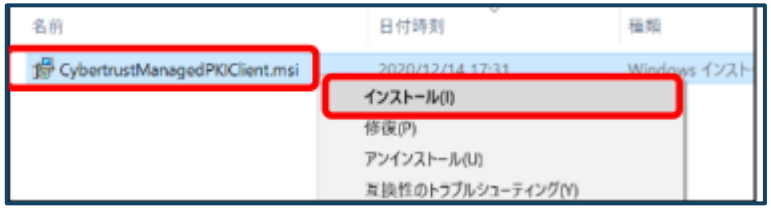
9 ブラウザが立ち上がったら、アドレスバーに下記URLを入力し、キーボードの「enter」を押してください。

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

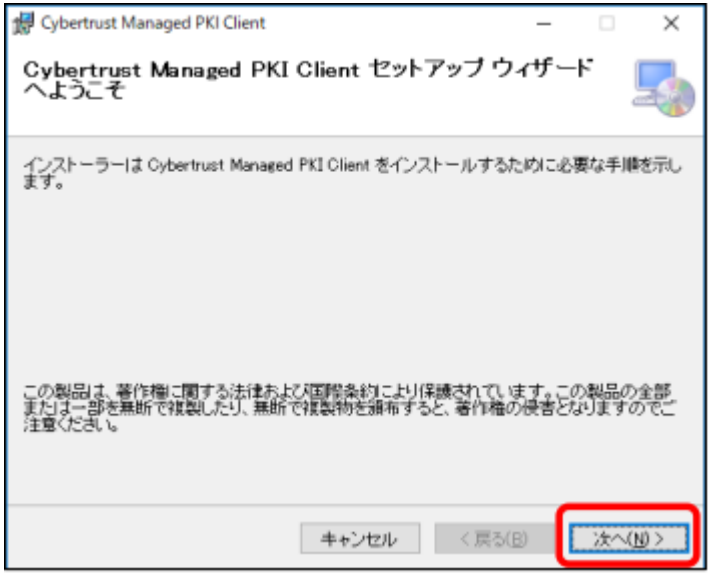
10 MPKIクライアントのインストーラーがダウンロードされます。ファイル名の上で右クリックし、「フォルダーに表示」をクリックします。



11 表示された画面内の「**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。



12 「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。

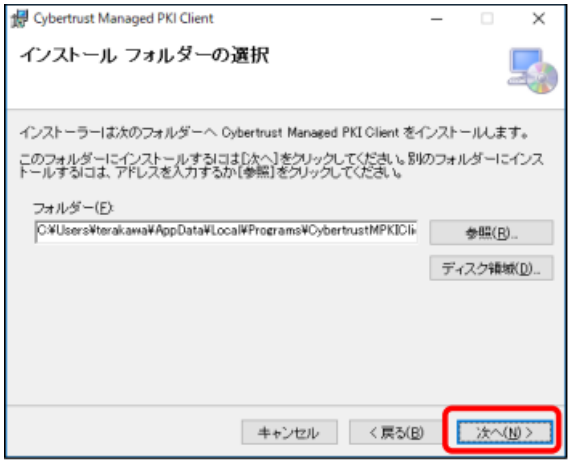


A. MPKIクライアントを用いた更新手順

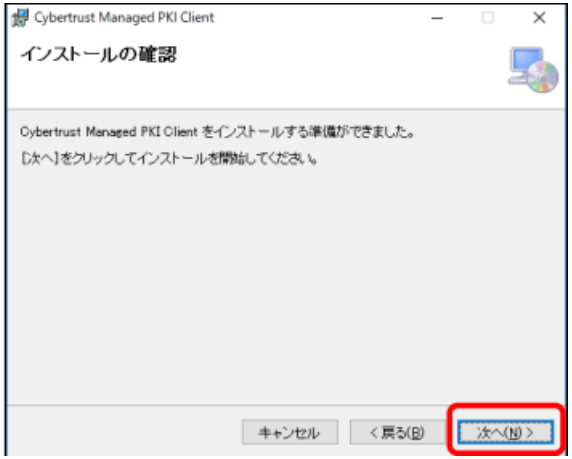
手順3 MPKIクライアントをバージョンアップする

電子証明書の更新で使用するMPKIクライアントをアンインストール（削除）して最新版をインストールします。

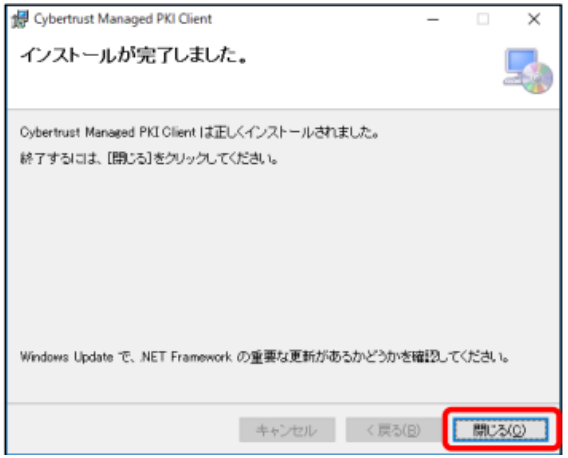
13 「次へ」をクリックします。



14 「次へ」をクリックします。



15 「閉じる」をクリックします。
ここまでで最新版のMPKIクライアントのインストール作業は終了です。



注意	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

MPKIクライアントの更新が完了しました。
→手順4へ進みます。

A. MPKIクライアントを用いた更新手順

手順4 タスクトレイにMPKIクライアントがあることを確認する

電子証明書を更新するにあたり、タスクトレイにMPKIクライアントが表示されていることを確認します。

1 電子証明書の更新作業を行っている端末のデスクトップ右下より、「隠れているインジケーターを表示する」をクリックします。

2 タスクトレイが表示されます。タスクトレイの中に、以下のMPKIクライアントのアイコンが表示されていることを確認してください。

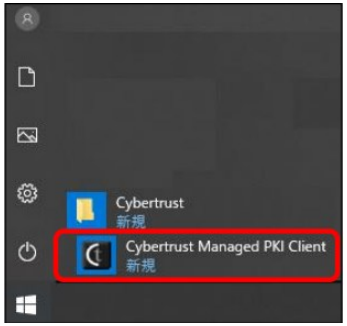
MPKIクライアントのアイコン

MPKIクライアントのアイコンが表示されていることを確認できました。
→手順5へ進みます。

こんなときは！

MPKIクライアントのアイコンが表示されていない場合、Windowsのスタートボタンをクリックし、表示されるメニューから「**Cybertrust Managed PKI Client**」をクリックします。

Windows10の場合



Windows11の場合

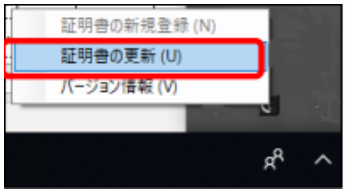
A. MPKIクライアントを用いた更新手順

手順 5

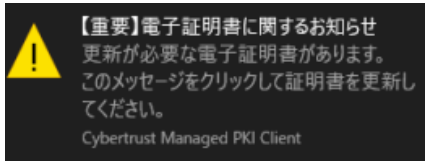
MPKIクライアントを用いて、証明書を更新する

MPKIクライアントのメニューから電子証明書を更新します。

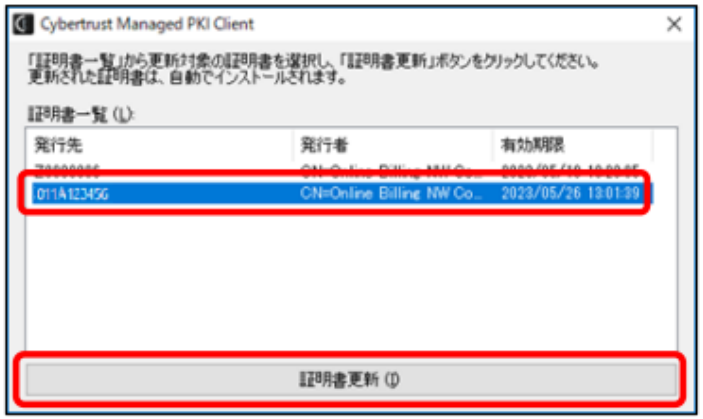
1. 手順４（14ページ）で確認した、MPKIクライアントのアイコンを右クリックします。
メニューが表示されるので、「**証明書の更新**」をクリックします。



以下のお知らせが表示されている場合、
クリックすることで②の画面が表示されます。

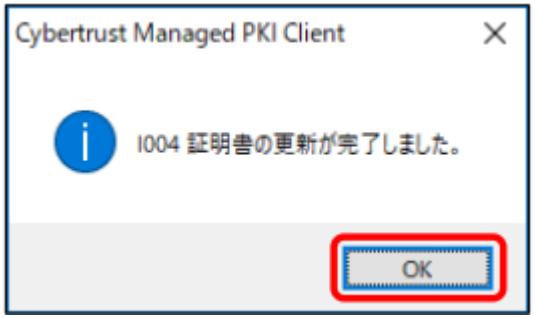


2. 証明書の一覧が表示されます。更新したい電子証明書をクリックし、「**証明書更新**」をクリックします。



3. 確認メッセージが表示されるので、「はい」をクリックします。

4. 以下のメッセージが表示されたら、「OK」をクリックします。



A. MPKIクライアントを用いた更新手順

手順 5

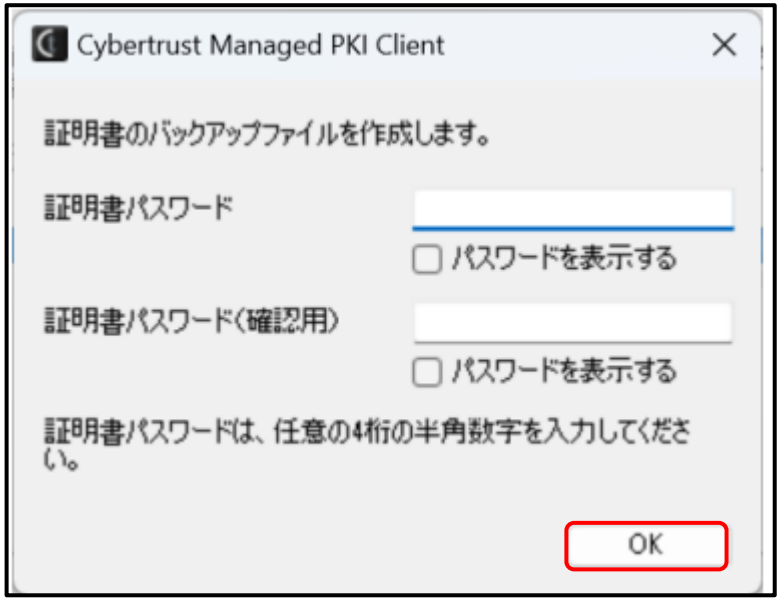
MPKIクライアントを用いて、証明書を更新する

MPKIクライアントのメニューから電子証明書を更新します。

5 バックアップファイルを作成するためのパスワード設定画面となります。
パスワードとして、**任意の半角数字4桁**を入力してください。
パスワードを入力した後、OKを押します。

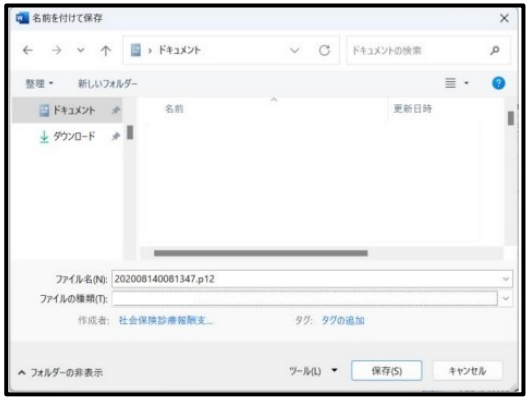
※**更新前の電子証明書のパスワードと異なるパスワードでも構いません。**

※ここで設定するパスワードは、バックアップファイルを用いて電子証明書をインストールするときに必要となりますので、忘れないようにしてください。

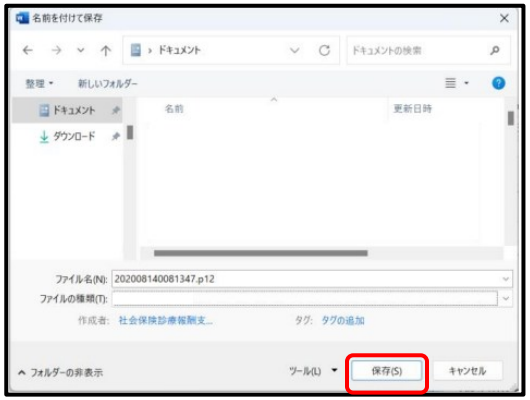


6 バックアップファイルの保存先を選択します。

※サンプル画像では「ドキュメント」フォルダとしていますが、「デスクトップ」や「ダウンロード」フォルダなどご希望の保存先で問題ありません。



7 保存をクリックします。



A. MPKIクライアントを用いた更新手順

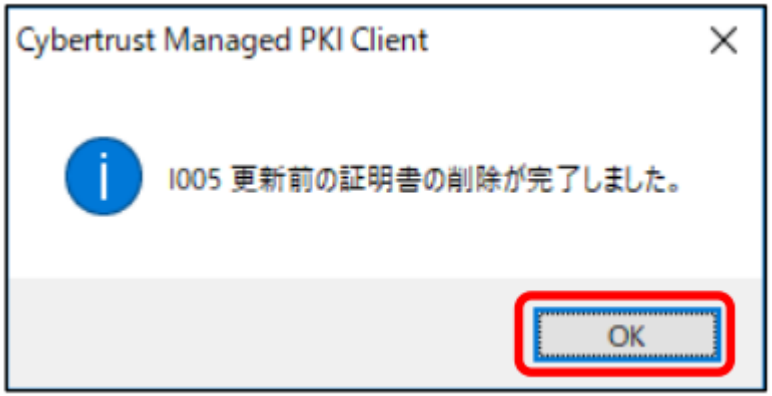
手順5

MPKIクライアントを用いて、証明書を更新する

MPKIクライアントのメニューから電子証明書を更新します。

8 更新前の証明書を削除するメッセージが表示されますので、「はい」をクリックします。

9 「OK」をクリックします。



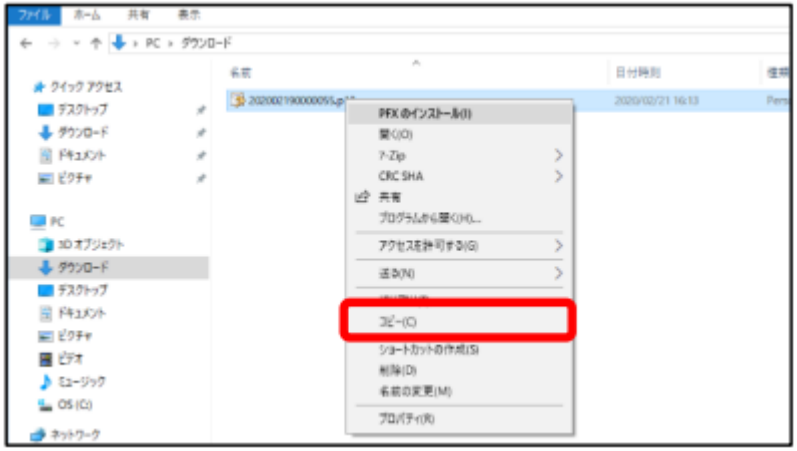
電子証明書が更新できました。
次に電子証明書のバックアップを取得します。
→手順6へ進みます。

A. MPKIクライアントを用いた更新手順

手順 6　外部記録媒体に電子証明書をバックアップする

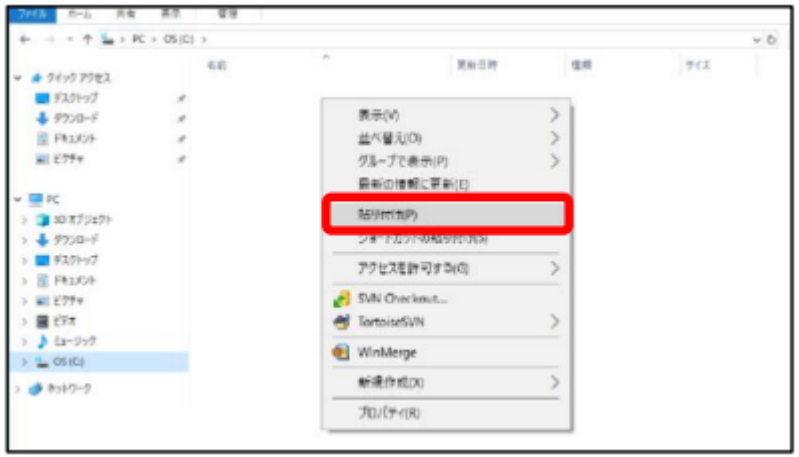
端末の故障、交換に備え、更新後の証明書をバックアップします。

1 手順５の⑦（16ページ）で電子証明書を保存したフォルダを開きます。
電子証明書を右クリックし、コピーを選択します。



2 外部記録媒体（USBメモリなど）のフォルダを開き、フォルダの上で右クリックから「貼り付け」を選択します。

※バックアップファイルを外部記録媒体に保存する際、手順5の⑤（16ページ）で作成したパスワードも忘れないように保管ください。



以上で電子証明書更新作業は終了です。
次ページ以降の対応は不要です。

B. 電子証明書の更新（MPKIクライアント未導入）

本資料では、電子証明書の更新手順を説明します。

電子証明書の更新
（MPKIクライアント未導入）

手順 1 電子証明書更新申請サイトへアクセスする

▼

手順 2 電子証明書を更新する

▼

手順 3 更新した電子証明書をダウンロードする

▼

手順 4 ダウンロードした電子証明書をインストールする

▼

手順 5 電子証明書が正しくインストールされていることを確認する

▼

手順 6 古い電子証明書を削除する

▼

手順 7 外部記録媒体に電子証明書をバックアップする

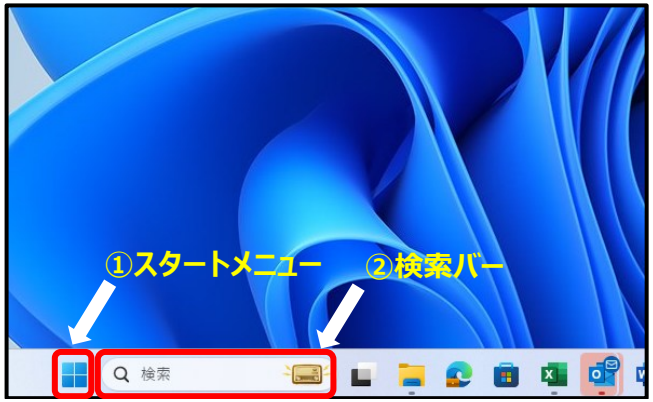
B. 電子証明書更新申請サイトからの更新手順

手順1 電子証明書更新申請サイトへアクセスする

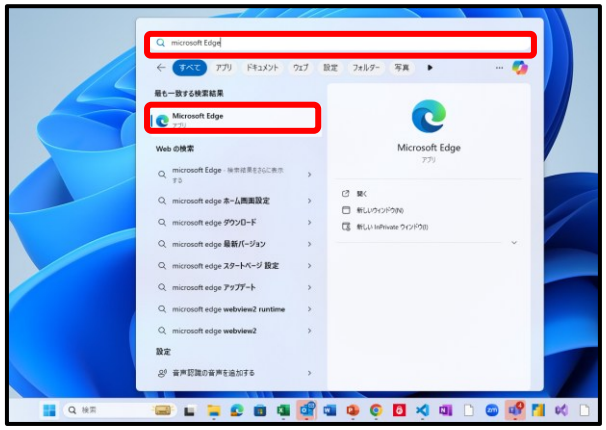
MPKIクライアント未導入の場合に、電子証明書更新申請サイトへアクセスします。

注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

1. 電子証明書の更新を実施する端末のタスクバーのスタートメニューをクリックします。※もしスタートメニューがない場合は検索バーをクリックします。

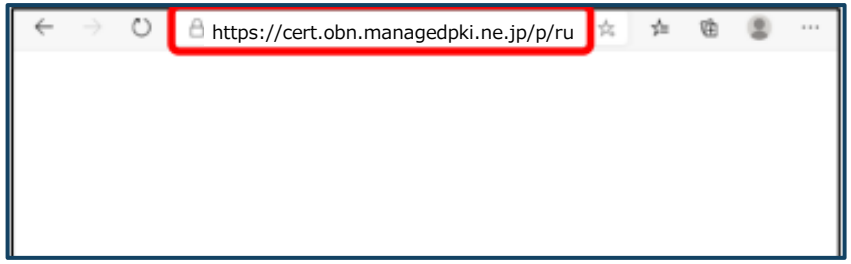


2. 検索欄に「Microsoft Edge」を入力し、「Microsoft Edge」のアプリをクリックします。



3. ブラウザが立ち上がったら、アドレスバーに下記URLを入力し、キーボードの「enter」を押します。

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



手順2へ進みます。

B. 電子証明書更新申請サイトからの更新手順

手順2 電子証明書を更新する

電子証明書更新申請サイトにアクセスした後、電子証明書の更新をします。

1 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**」と表示されていることを確認します。

2 「証明書更新申請」をクリックした後、「鍵更新申請情報の確認」が表示されるので「Submit」をクリックします。

3 「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、自動的に「鍵生成中」→「発行要求中」→「発行済み」と遷移します。

次に、更新後の電子証明書をダウンロードします。
→手順3へ進みます。

B. 電子証明書更新申請サイトからの更新手順

手順 3

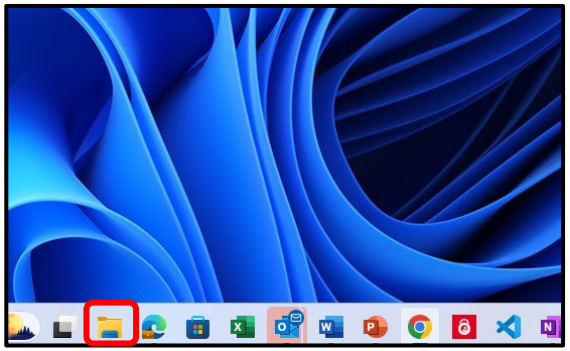
電子証明書をダウンロードする

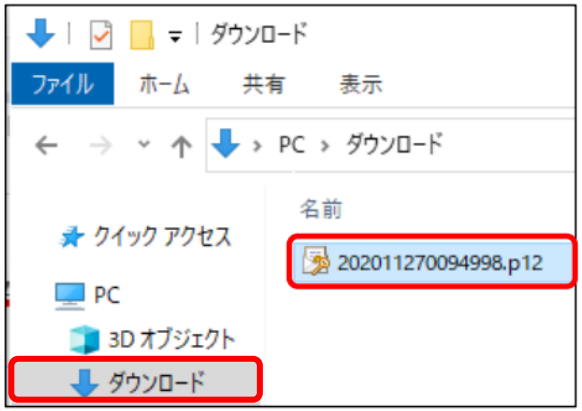
電子証明書の更新後、電子証明書をダウンロードをします。

1 「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桁以上**を入力し、「Submit」をクリックします。
※パスワードは後ほど利用するため、メモ等に控えてください。

2 「Download」をクリックします。

3 「タスクバー」の「フォルダ」をクリックし「ダウンロード」フォルダをクリックして「鍵がダウンロードできていることを確認します。





電子証明書をダウンロードした後は、インストール作業が必要です。
→手順4へ進みます。

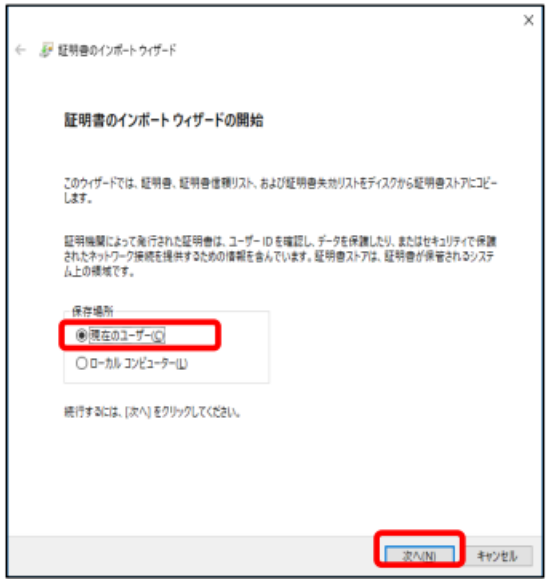
B. 電子証明書更新申請サイトからの更新手順

手順4 ダウンロードした電子証明書をインストールする

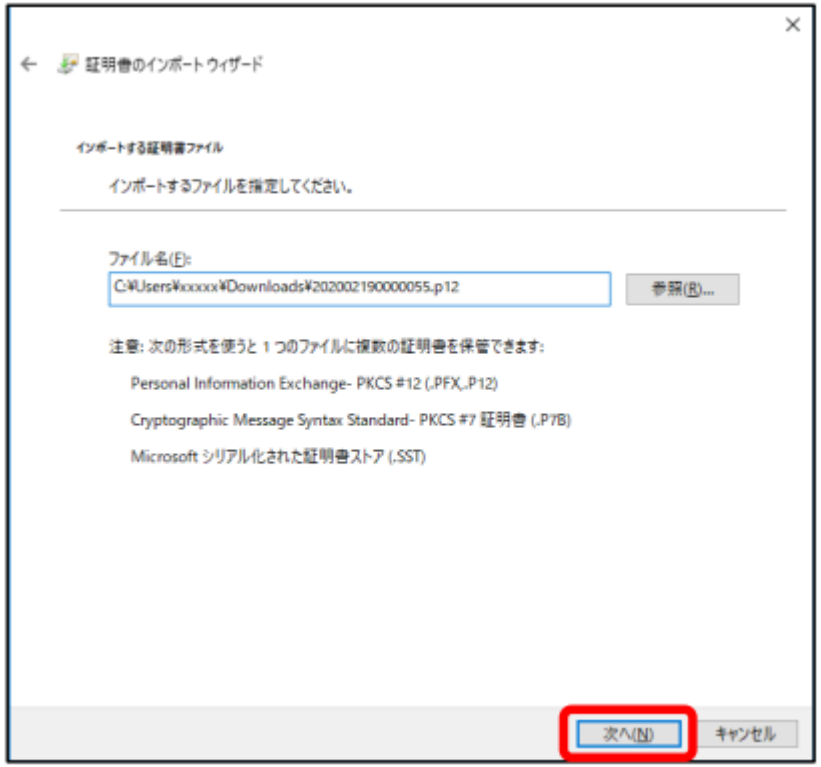
デスクトップにダウンロードした電子証明書をインストールします。

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。
※表示されない場合は、ダウンロードしたファイルをダブルクリックしてください。

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。



B. 電子証明書更新申請サイトからの更新手順

手順4 ダウンロードした電子証明書をインストールする

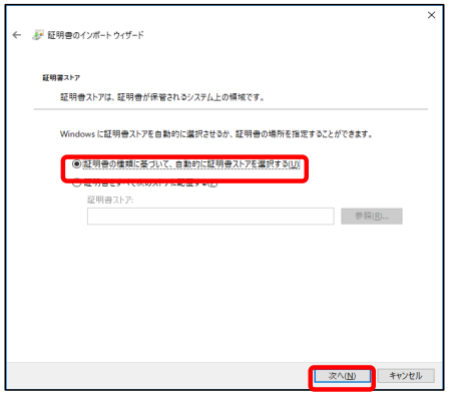
デスクトップにダウンロードした電子証明書をインストールします。

4 「秘密キーの保護」が表示されます。
「パスワード」に手順3の①（22ページ）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]のチェックを外します**
- **[このキーをエクスポート可能にする]をチェックを外します**
- **[すべての拡張プロパティを含める]をチェックします**

・「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。

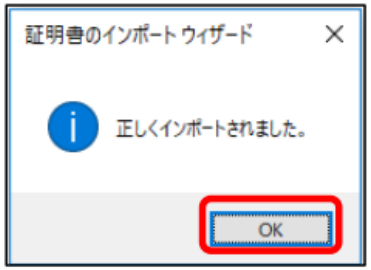
B. 電子証明書更新申請サイトからの更新手順

手順4

ダウンロードした電子証明書をインストールする

デスクトップにダウンロードした電子証明書をインストールします。

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。
※「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。



注意	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

電子証明書のインストールが完了しました。
次に、電子証明書が正しくインストールされているか確認します。
→手順5へ進みます。

B. 電子証明書更新申請サイトからの更新手順

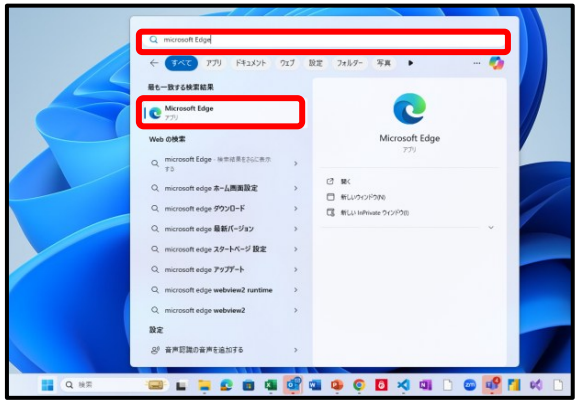
手順5 電子証明書が正しくインストールされていることを確認する

電子証明書が正しくインストールされたか確認するために、電子証明書の有効期限が更新日から3年3か月後の日付になっていることを確認します。

注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

1. 電子証明書の更新を実施する端末のタスクバーのスタートメニューをクリックします。※もしスタートメニューがない場合は検索バーをクリックします。

2. 検索欄に「Microsoft Edge」を入力し、「Microsoft Edge」のアプリをクリックします。



3. 画面右上の「…」をクリックし、「設定」をクリックします。

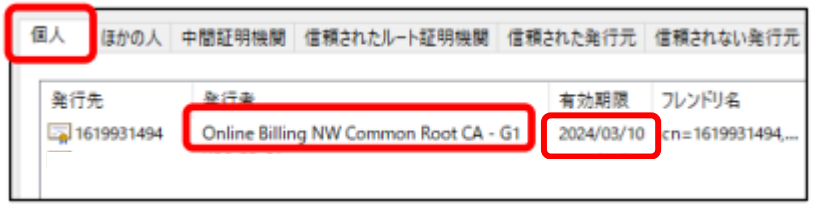
B. 電子証明書更新申請サイトからの更新手順

手順5 電子証明書が正しくインストールされていることを確認する

電子証明書が正しくインストールされたか確認するために、電子証明書の有効期限が更新日から3年3か月後の日付になっていることを確認します。

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

5 「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の有効期限を確認します。
有効期限が更新した日付から3年3か月先の日付になっていることが確認できれば電子証明書の更新が完了しております。



注意	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

電子証明書が正しくインストールされていることを確認できました。
→手順6へ進みます。

B. 電子証明書更新申請サイトからの更新手順

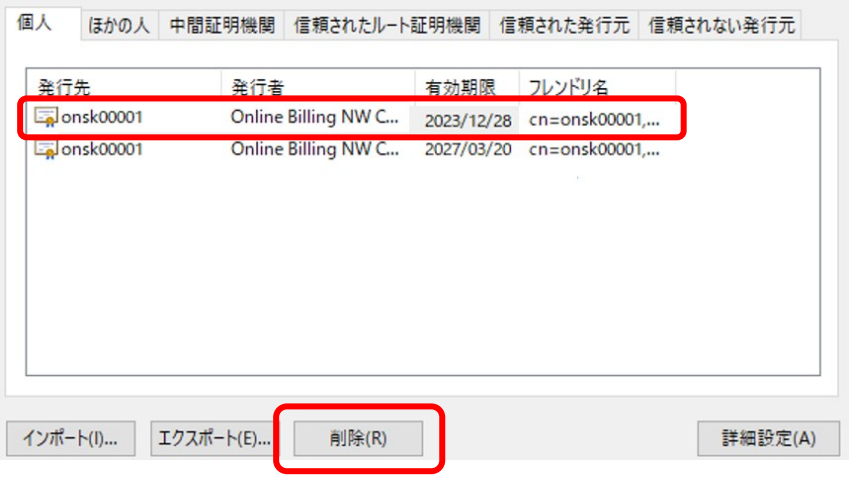
手順6　古い電子証明書を削除する

古い電子証明書は有効期限を過ぎると使用できなくなり、オンライン資格確認等システム・オンライン請求システムにログインできなくなるため、削除します。

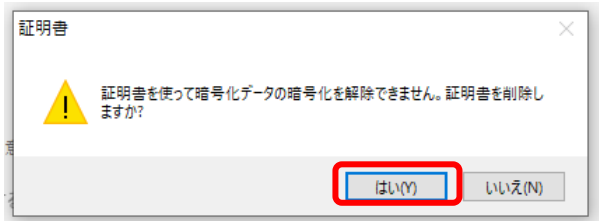
注意	以下の作業に進む前に、必ず全てのブラウザを閉じて下さい。

1 手順5の①～④（26～27ページ）と同じ手順で、Edgeの「設定」から「証明書の管理」を開きます。

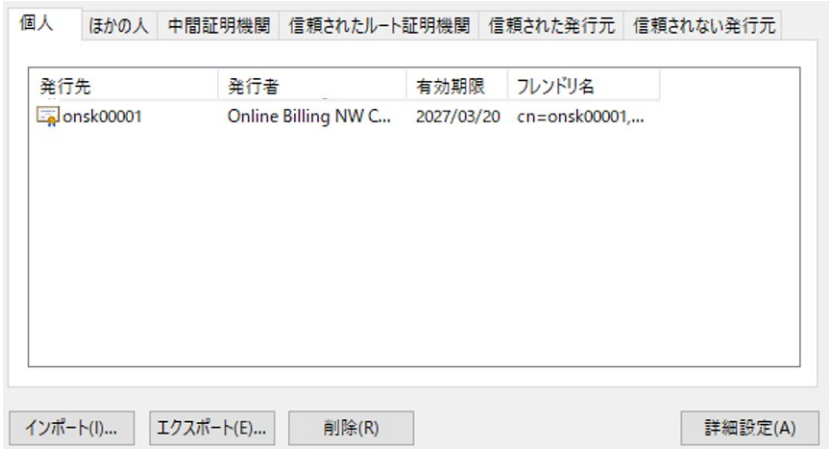
2 「電子証明書」が表示されます。「個人」タブを開き、有効期限が古い電子証明書を選択し、「削除」をクリックします。
※発行者が「Online Billing NW Common Root CA」と表示されていることを確認します。
※有効期限が新しい電子証明書は削除しないでください。



3 「はい」をクリックします。



4 「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	上記の操作が完了したら、必ず全てのブラウザを閉じて下さい。

古い電子証明書の削除が完了しました。
→手順7へ進みます。

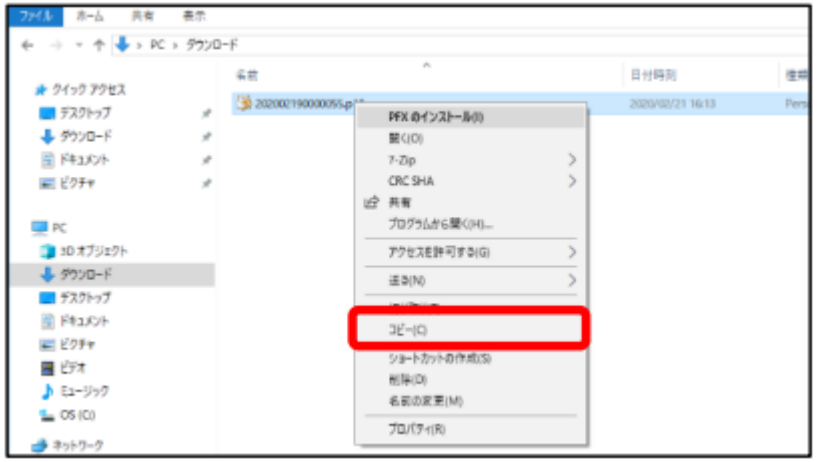
B. 電子証明書更新申請サイトからの更新手順

手順7

外部記録媒体に電子証明書をバックアップする

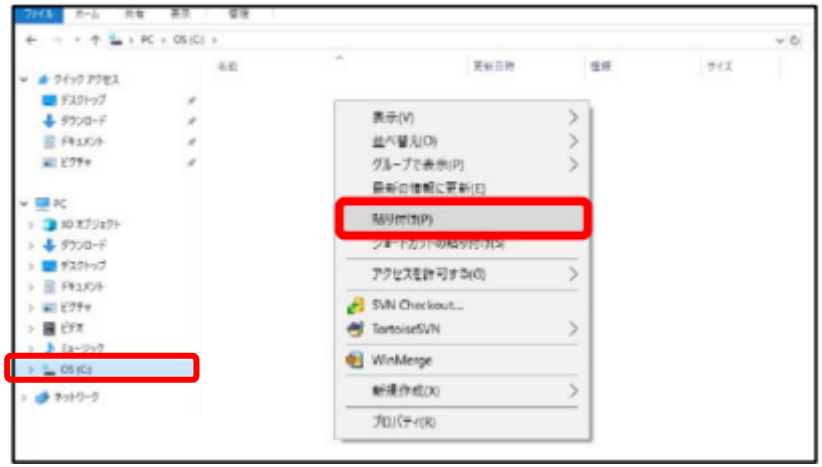
端末が変わった際にバックアップを取った電子証明書が必要になるため、外部記録媒体に電子証明書をバックアップします。

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。
※手順4の③（23ページ）でインストールした電子証明書を格納した格納先になります



2 外部記録媒体（USBメモリーなど）のフォルダを開き、フォルダの上で右クリックから「貼り付け」を選択します。

※バックアップファイルを外部記録媒体に保存する際、手順3の①（22ページ）で作成したパスワードも忘れないように保管ください。



以上で電子証明書の更新作業は終了です。

改定履歴

年月	版数	頁	変更区分	変更内容
2025年3月	1.0	-	-	初版
2025年12月	1.1	6,7,8 2,3,11,13,20,25,26,27 22,28	変更 変更 変更	MPKIクライアントのバージョン確認手順を更新 ブラウザを使用する際の注意を追記 パスワードの桁数についての記載を訂正
2026年5月	1.2	1	変更	更新対象となる電子証明書についての説明を追記
2026年10月	1.3	1,4,20 19,29 28	変更 変更 追加	用語の説明及び案内文言を追加 古い電子証明書の削除手順の追加に伴う手順番号の変更 古い電子証明書の削除手順を追加