

# 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 1.6.0

令和6年1月15日

## 目次

はじめに .....	4
<b>0. 事前準備 .....</b>	<b>4</b>
1. 証明書のダウンロードとインストール .....	5
1.1. 証明書のダウンロード .....	5
1.2. 証明書のインストール .....	8
1.2.1 こんなときは！ .....	11
1.3. 登録した証明書の確認 .....	12
1.4. 証明書のバックアップ .....	13
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） .....	14
1.6. 認証用の証明書の選択画面が表示された場合 .....	17
2. 証明書の更新 .....	18
2.1. MPKI クライアントを利用した更新 .....	18
2.1.1 こんなときは！ .....	19
2.1.2 MPKI クライアント利用時の証明書バックアップ .....	20
2.2. 更新申請画面からの更新 .....	23
2.2.1 こんなときは！ .....	26
3. 証明書の失効 .....	27
4. 証明書の削除 .....	29
5. サポート情報 .....	31
5.1. MPKI クライアント利用環境 .....	31
5.2. ご利用にあたっての注意事項 .....	31
5.2.1 MPKI クライアントインストール時の注意事項 .....	31
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 .....	31
5.3. ルート証明書の取得とインストール .....	32
5.3.1 ルート証明書のダウンロード .....	32
5.3.2 ルート証明書のインストール .....	33
5.3.3 登録したルート証明書の確認 .....	37
5.4. MPKI クライアントのバージョンアップ .....	39

Date	Version #	Summary of Changes
2020/09/28	1.0.0	初版
2020/12/11	1.1.0	<ul style="list-style-type: none"> <li>・「1.5 MPKI クライアントインストール」の保存手順の変更</li> <li>・「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</li> <li>・「3. 証明書バックアップ (MPKI クライアント編)」を追加</li> </ul>
2021/01/04	1.2.0	<ul style="list-style-type: none"> <li>・「1.1 証明書ダウンロード」のダウンロード方法の追記</li> <li>・手順案内様式の変更</li> </ul>
2021/03/22	1.3.0	<ul style="list-style-type: none"> <li>・「3. 証明書の失効」の変更</li> </ul>
2021/04/16	1.3.1	<ul style="list-style-type: none"> <li>・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</li> </ul>
2021/04/27	1.4.0	<ul style="list-style-type: none"> <li>・「5.3. ルート証明書の取得とインストール」を追加</li> </ul>
2022/04/13	1.5.0	<ul style="list-style-type: none"> <li>・「5.4. MPKI クライアントのバージョンアップ」を追加</li> </ul>
2024/01/15	1.6.0	<ul style="list-style-type: none"> <li>・医療機関等向け総合ポータルサイトを追加</li> <li>・対応 OS に Windows11 を追加</li> </ul>

## 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、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、設定してください。

- 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]

【医療機関・薬局向け】

インターネットから「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>

【訪問看護ステーション向け】

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](https://iryohokenjyoho.service-now.com/csm?sys_kb_id=4356711cc3537910615bd1877a0131b6&id=kb_article_view)

## 1. 証明書のダウンロードとインストール

### 1.1. 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」をご用意ください。

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、ご注意ください。

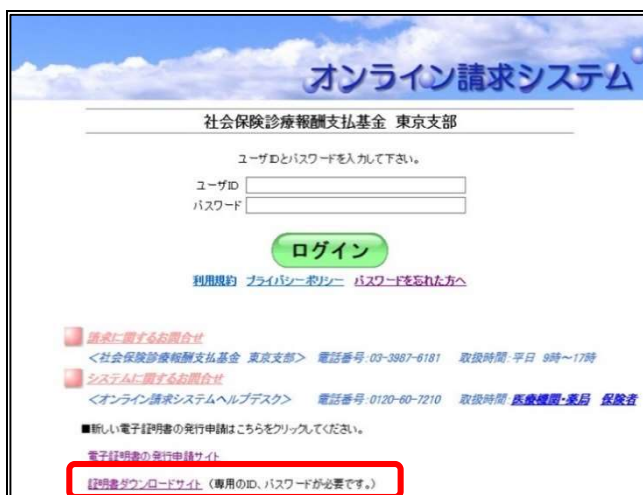
#### 電子証明書発行通知書の「電子証明書取得に関する情報」(サンプル)

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	20210121xxxxxxxx
電子証明書ダウンロードサイトリファレンスID	XXXXXXXXXXXXXXXX
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】

- ・オンライン請求のログイン画面



- 1-1. レセプトオンライン請求端末からダウンロードサイトにアクセス

【ダウンロードサイト】

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

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。

- ・電子証明書ダウンロードサイト



【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」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、「5.3. 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】



- 1-2. 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

「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。

## 証明書の取得画面

「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 を入力してください。

証明書パスワードは、任意の4桁の半角数字を入力してください。

リクエスト ID	202012100001000
リファレンス ID	FPwNiG5g4r
証明書パスワード	●●●●
証明書パスワード(確認用)	●●●●
<b>ダウンロード</b>	

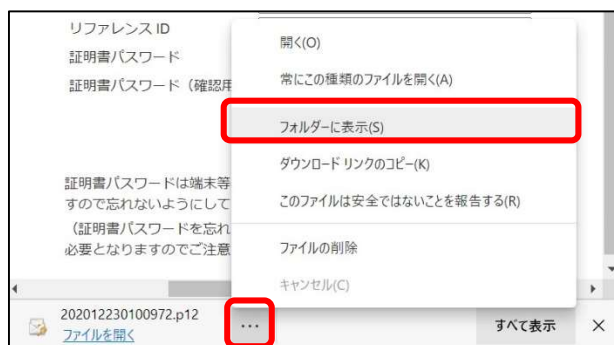
証明書パスワードは端末等へ証明書をインストールする際に必要となりますので忘れないようにしてください。

(証明書パスワードを忘れてしまった場合は、もう一度証明書発行申請が必要となりますのでご注意ください。)

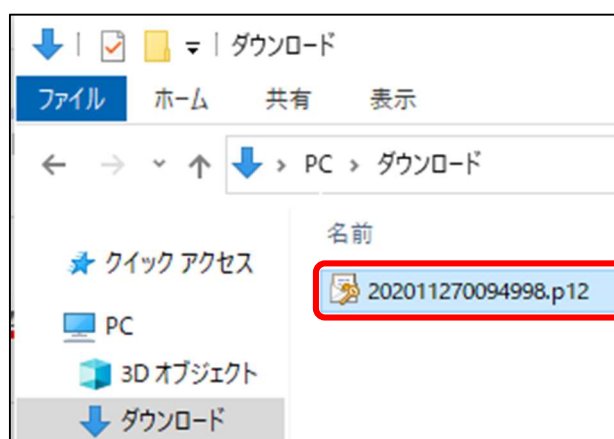
2. 証明書発行通知書に記載のリクエストIDとリファレンスID及び任意のパスワード（半角数字4桁）を入力し、「**ダウンロード**」をクリックします。

### 【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」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。**

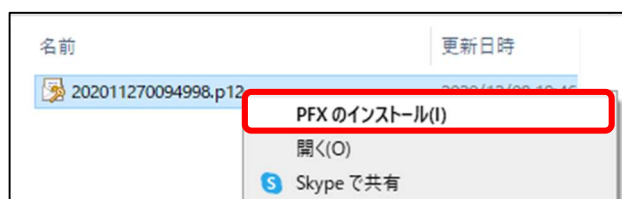


3. 画面下の【…】をクリックし、「**フォルダに表示**」をクリックします。

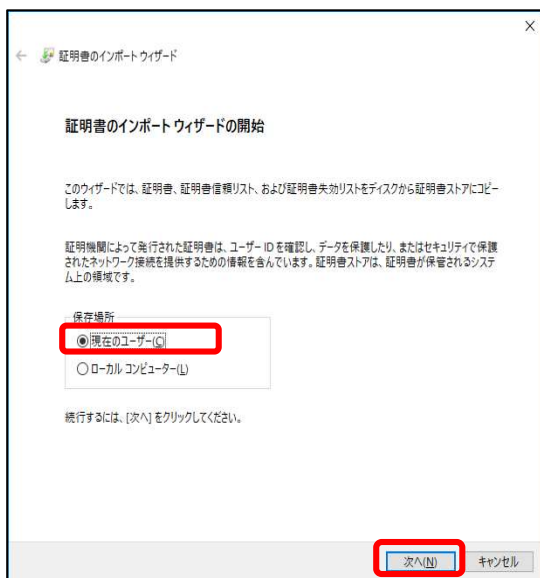


4. 証明書がダウンロードできていることを確認します。

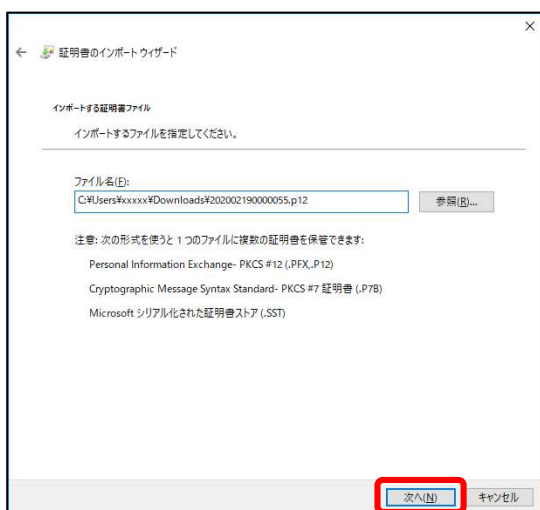
## 1.2. 証明書のインストール



1. ダウンロードした証明書ファイルを右クリックし、「PFX 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「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。

「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  
チェックする

[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。

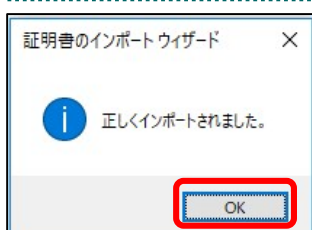
5. 「証明書ストア」が表示されます。「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択後、「次へ」をクリックします。



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！】

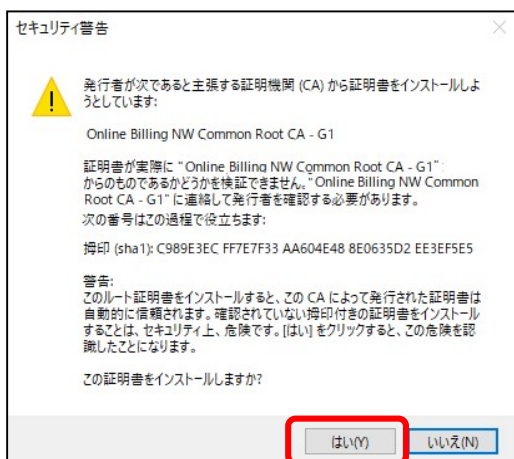
「新しい秘密交換キーをインポートします」が表示された場合、P11の「1.2.1 こんなときは！」を参照してください。



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！】

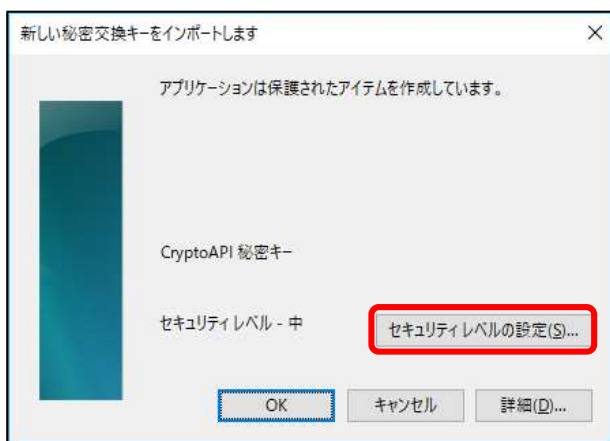
「セキュリティ警告」の画面が表示された場合、「はい」をクリックします。



「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、「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「1.3. 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。



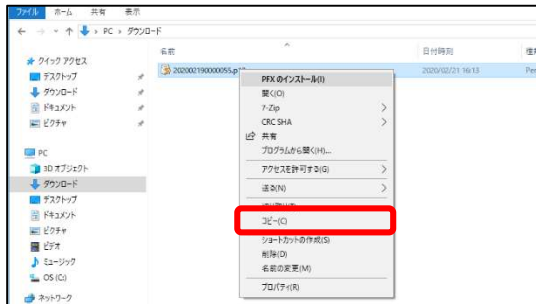
3. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。

個人	ほかの人	中間証明機関	信頼されたルート証明機関	信頼された発行元	信頼されない発行元
発行先	発行先	有効期限	フレンドリ名		
1619931494	Online Billing NW Common Root CA - G1	2024/03/10	cn=1619931494,...		
Client 001	KRS GP CA 2014	2033/01/31	<なし>		

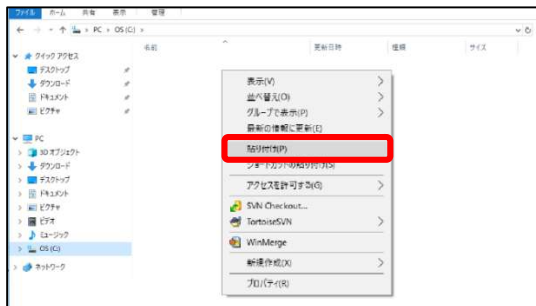
4. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

## 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、外部記録媒体等と共に忘れないように保管してください。



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、Windows 8.1、Windows 10 及び Windows 11 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。

### 【ダウンロードサイト】

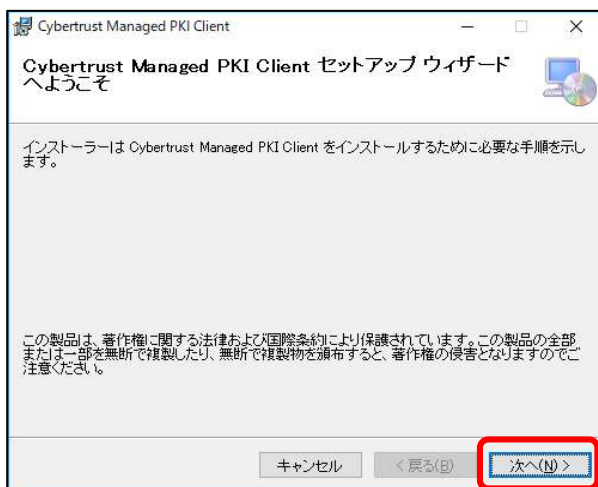
<https://cert.obn.managedpki.ne.jp/p/s>



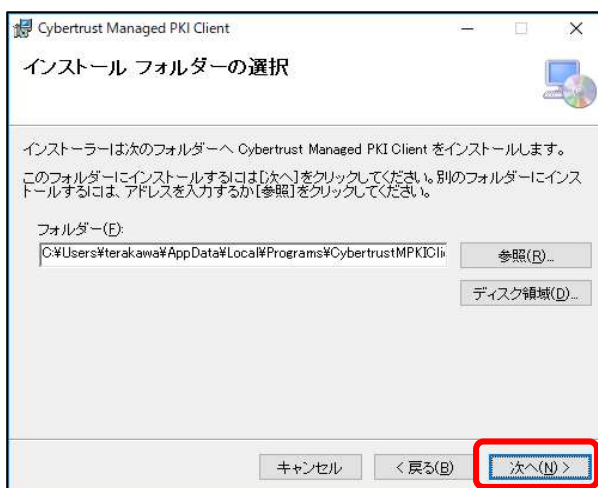
2. 【…】をクリックし、「フォルダに表示」をクリックします。



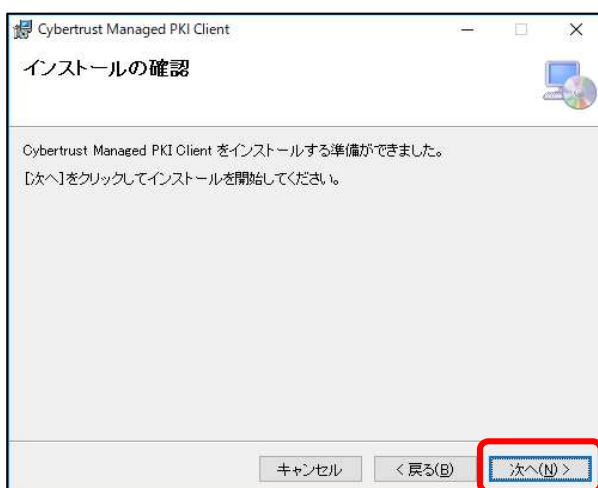
3. 「CybertrustManagedPKIClient.msi」ファイルを右クリックし、「インストール」をクリックします。



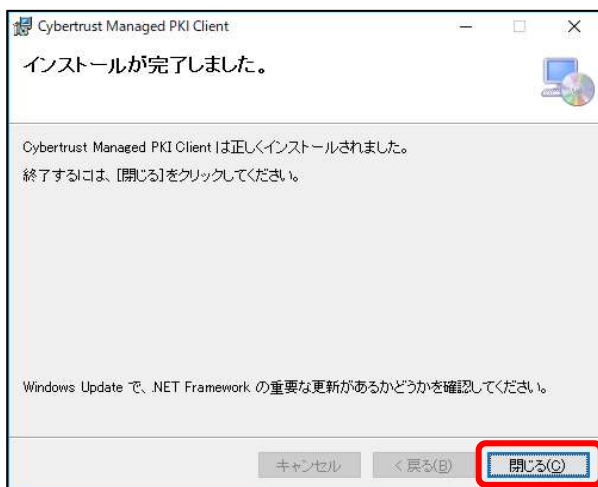
4. 「Cybertrust Managed PKI Client セットアップウィザード」が開始されます。「次へ」をクリックします。



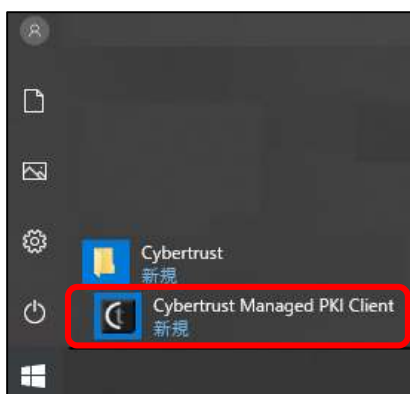
5. 「次へ」をクリックします。



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。



## 1.6. 認証用の証明書の選択画面が表示された場合



1. 「認証用の証明書の選択」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。

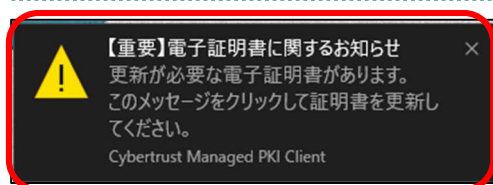
## 2. 証明書の更新

### 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、証明書の更新作業を行ってください。

#### 【お知らせが表示される条件】

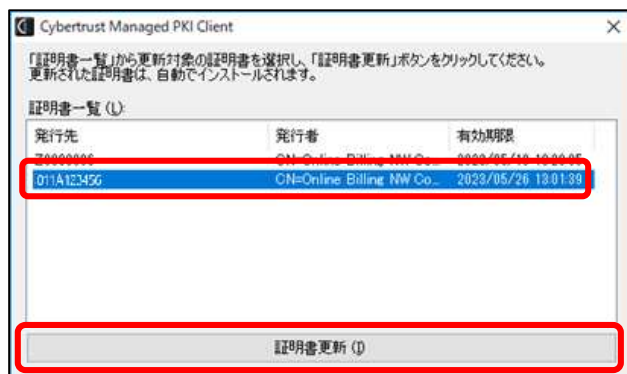
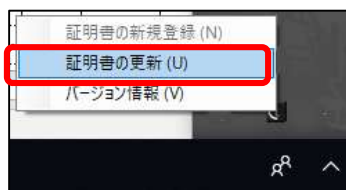
有効期限の 90 日前、60 日前、30 日前、15 日前、7 日前から毎日



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！】

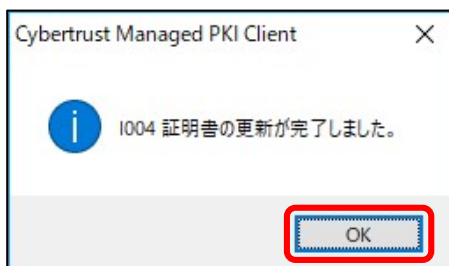
お知らせが表示されていない場合は、タスクトレイのアイコンを右クリックから操作できます。表示される以下のメニューから、[証明書の更新] をクリックします。



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。



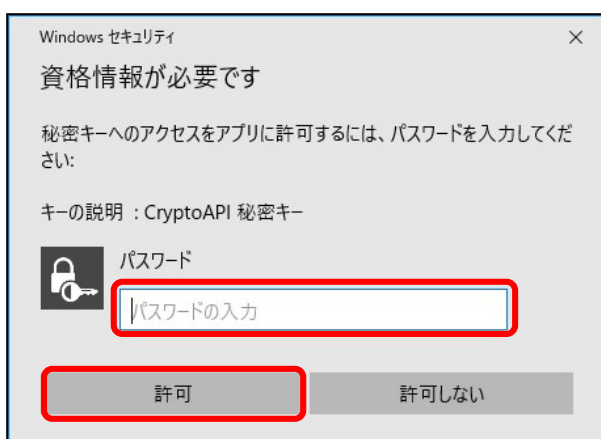
5. 「はい」をクリックします。



6. 「OK」をクリックします。

### 2.1.1 こんなときは！

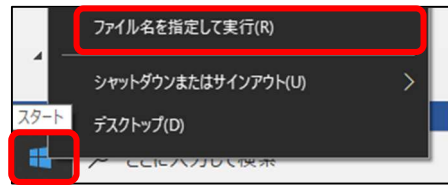
※パスワードの入力が求められた場合は、証明書のインストール時「1.2.1 こんなときは！」で設定したパスワードを入力します。



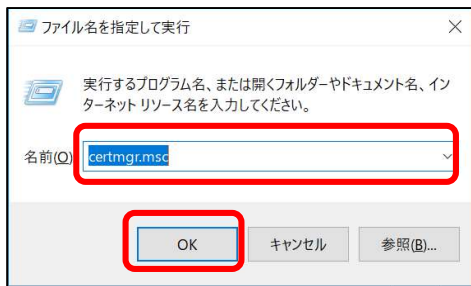
1. パスワードを入力し、「許可」をクリックします。

※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。

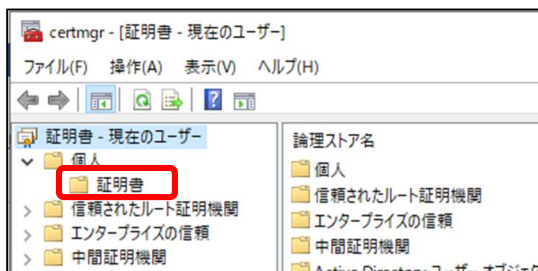
## 2.1.2 MPKI クライアント利用時の証明書バックアップ



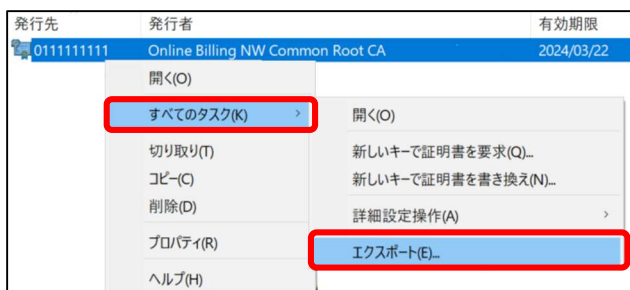
1. 画面の左下の Windows ボタンを右クリックし、「ファイル名を指定して実行」をクリックします。



2. 「certmgr.msc」を入力し、「OK」ボタンをクリックします。



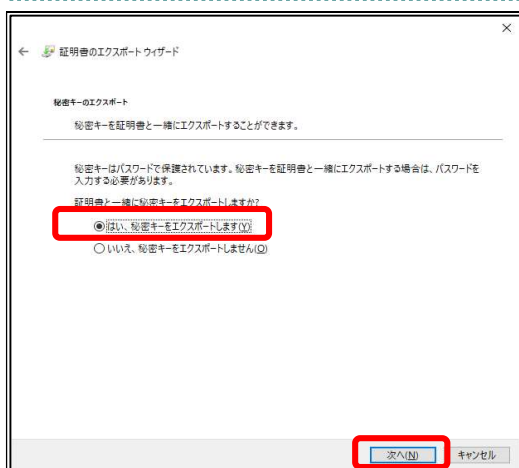
3. 「個人」から「証明書」をクリックします。



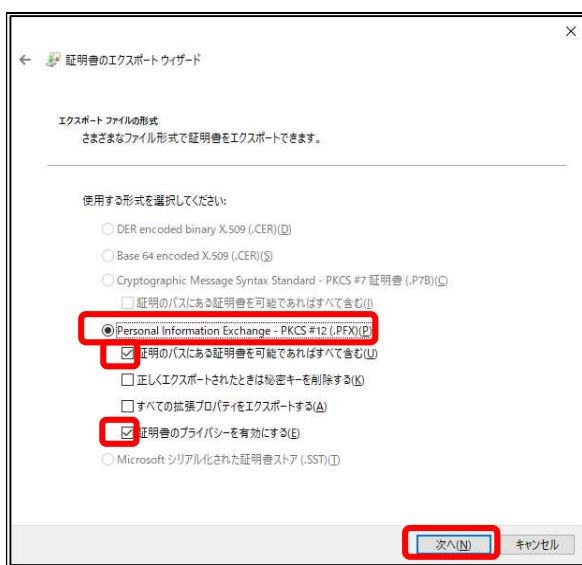
4. 発行者が「Online Billing NW Common Root CA」の有効期限が新しい証明書を選択し、右クリック後、「すべてのタスク」-「エクスポート」をクリック。



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)」を選択します。

[証明のパスにある証明書を可能であればすべて含む]を**チェック**する

[証明書のプライバシーを有効にする]を**チェック**する

【こんなときは！】

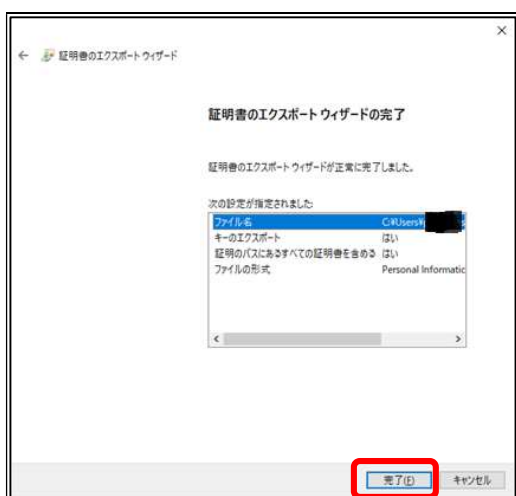
非活性（グレーアウト）で選択できない場合は、管理者権限を持っているユーザーで再度バックアップ手順を実施してください。



8. 「パスワード」と「パスワードの確認」に任意のパスワード（半角数字4桁）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。「正しくエクスポートされました」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。

【証明書更新申請サイト】

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

【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」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、「5.3. 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。

## 鍵更新申請情報の確認

以下の内容で証明書更新申請を送信します。  
よろしければ「Submit」ボタンをクリックしてください。

Common Name	0110119153
Organizational Unit	medical
Organizational Unit	hokkaido
Organization	ReceiptOnline
Country	JP
通知用メールアドレス	Test@cybertrust.co.jp
申請用データ	

Submit

4. 「Submit」をクリックします。

## 送信完了

申請情報を受け付けました。  
証明書の発行申請はこれで完了です。

### 申請の受付情報

リクエスト ID	202012140100076
リファレンス ID	zigLUVc29Q
証明書ステータス	発行済み

受け付けた申請情報の詳細は以下のとおりです。

Common Name	0110119153
Organizational Unit	medical
Organizational Unit	hokkaido
Organization	ReceiptOnline
Country	JP

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。



### 鍵の取得

ダウンロードしたい鍵の発行申請時のリクエスト ID と、鍵を暗号化するパスワードを入力してください。

リクエスト ID

パスワード

パスワードの確認

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。

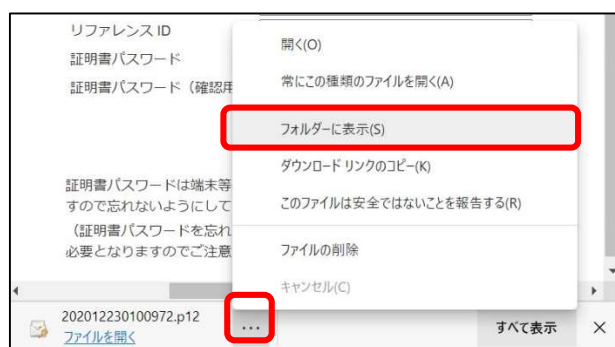
**【注意】**

入力した証明書パスワードは、「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。**

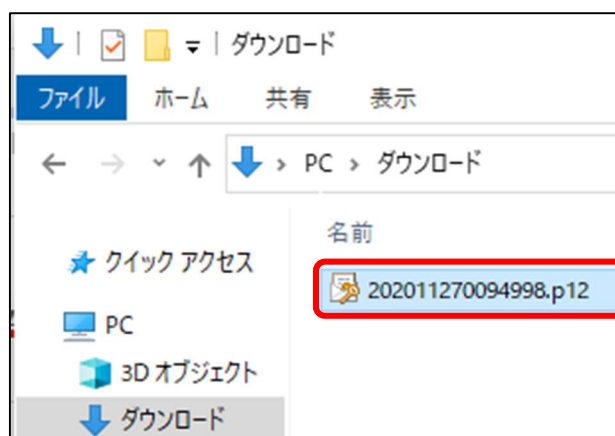
### 鍵の取得

鍵をダウンロードします。鍵のダウンロードまたはインストールを行うには、「Download」ボタンをクリックしてください。

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。

## 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。

更新申請情報の一覧					
1 件中 1 - 1 件目を表示しています。					
リクエスト ID	Common Name	証明書更新申請日時	有効期限	ステータス	取得
202012140100076	0110119153	2020.12.14 17:39:00	2024.03.14 17:39:07	発行済み	Download key
Previous 20		Next 20			

### 3. 証明書の失効



1. 失効対象の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。

【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」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、「5.3. ルート証明書の取得とインストール」を参照

証明書失効申請情報の入力画面

電子証明書発行時に送付しました「電子証明書発行通知書」をお手元にご用意ください。  
証明書失効申請情報を入力してください。

リクエスト ID

リファレンス ID

・リクエスト ID : 電子証明書発行通知書に記載のリクエスト ID を入力してください。  
・リファレンス ID : 電子証明書発行通知書に記載のリファレンス ID を入力してください。

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。

証明書失効申請情報の入力画面

失効処理完了のご連絡のため、メールアドレスを入力してください。

リクエスト ID

リファレンス ID

メールアドレス

メールアドレス(確認用)

・メールアドレス: 申請者が所属する部署または申請者のメールアドレスを入力してください。  
・メールアドレス(確認用): 確認のため、もう一度メールアドレスを入力してください。  
※失効処理を完了後、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」をご連絡します。

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入力内容確認画面」へ遷移します。

**証明書失効申請情報入力内容の確認画面**

以下の内容で証明書失効申請を送信します。  
よろしければ「申請」ボタンをクリックしてください。  
内容に誤りがあれば、「戻る」ボタンをクリックしてください。

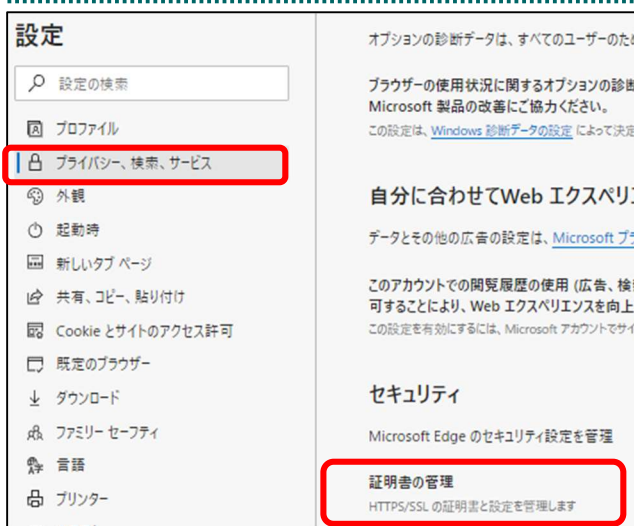
リクエスト ID	202103190101509
リファレンス ID	gdFNXXeFRP
メールアドレス	11@22.33

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てに失効完了をご連絡します。

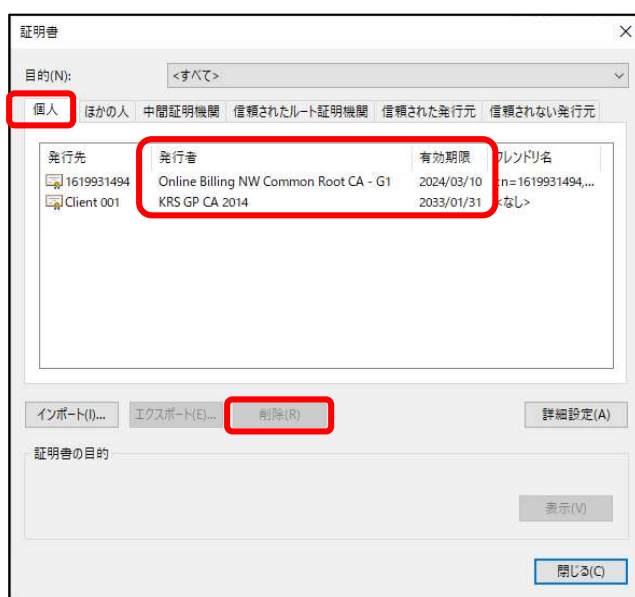
## 4. 証明書の削除



1. Edge を起動し、画面右上の「設定」をクリックします。

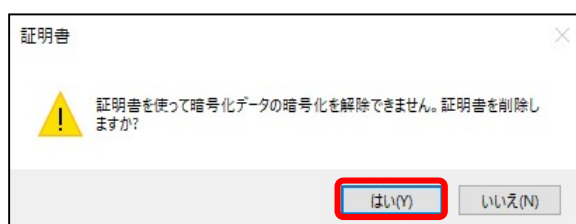


2. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。



3. 「証明書」が表示されます。「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. 「証明書」が表示されます。削除を行った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。

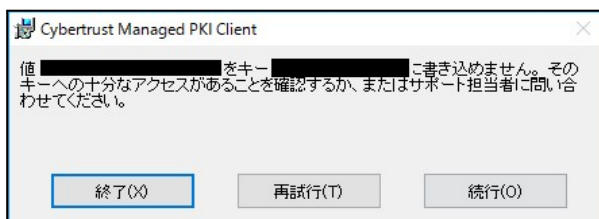
## 5. サポート情報

### 5.1. MPKI クライアント利用環境

対応 OS		32bit	64bit
	Windows 8.1	○	○
	Windows 10	○	○
	Windows 11	-	○
依存するソフトウェア	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。		
表示言語	日本語のみ		
サポートする Proxy 認証の種類	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		

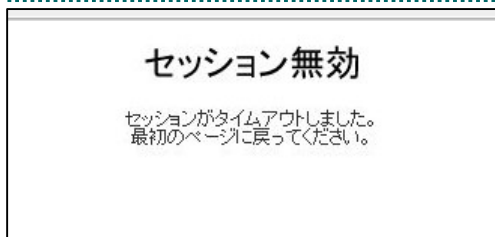
### 5.2. ご利用にあたっての注意事項

#### 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してください。

#### 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。

## 5.3. ルート証明書の取得とインストール

### 5.3.1 ルート証明書のダウンロード



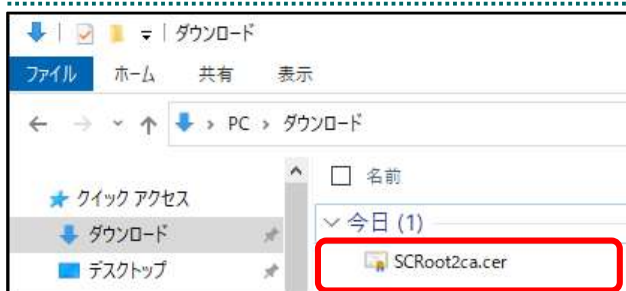
1. オンライン請求ネットワークへ接続の端末からルート証明書のダウンロードサイトにアクセスします。

【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。



### 5.3.2 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。



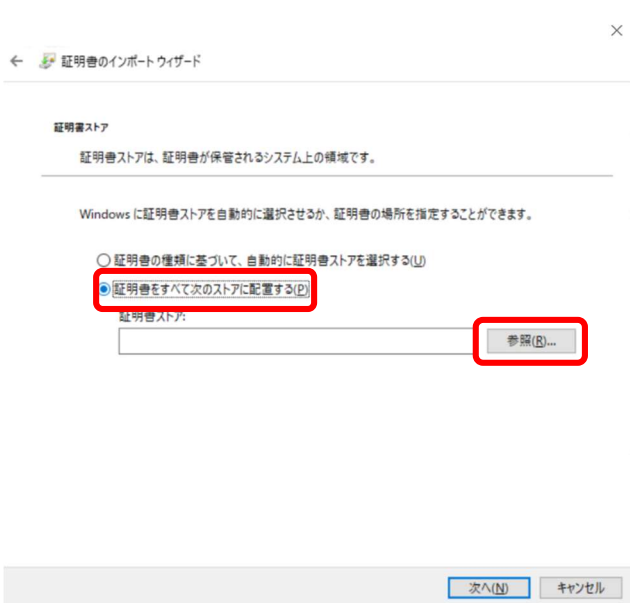
2. 「セキュリティの警告」画面が表示されます。「開く」をクリックします。



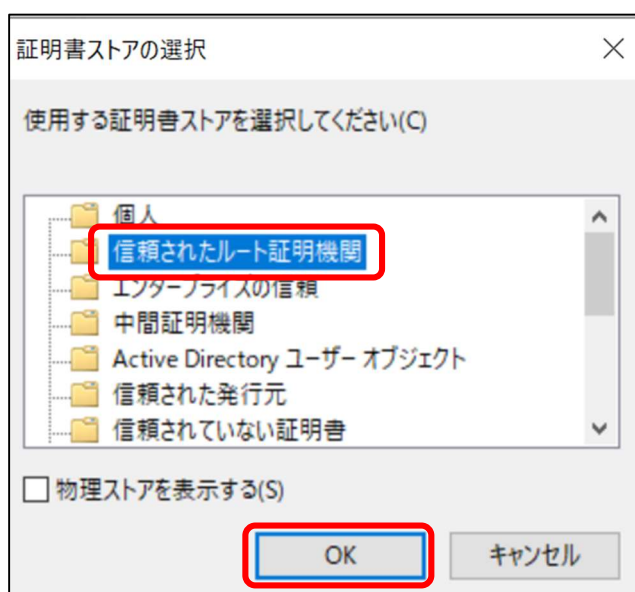
3. 「証明書」画面が表示されます。「証明書のインストール」をクリックします。



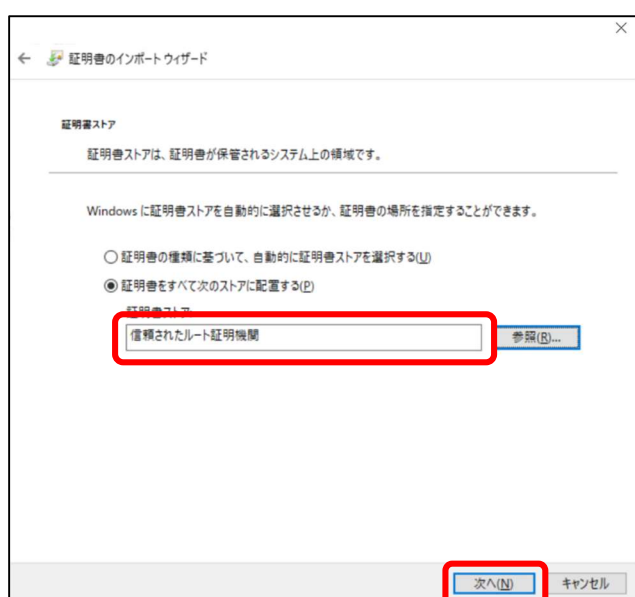
4. 「証明書のインポートウィザード」画面が表示されます。「現在のユーザー」が選択されていることを確認し、「次へ」をクリックします。



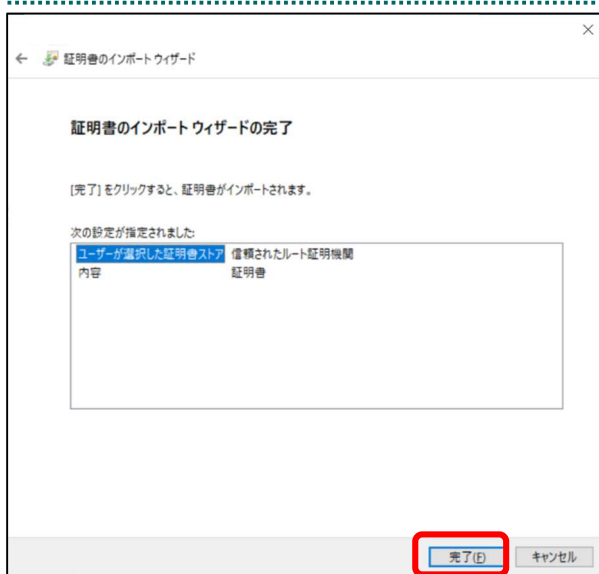
5. 「証明書をすべて次のストアに配置する」を選択し、「証明書ストア」の右側にある「参照」をクリックします。



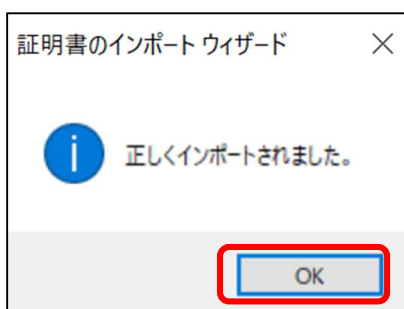
6. 「証明書ストアの選択」画面が表示されます。  
「信頼されたルート証明機関」を選択して「OK」をクリックします。



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。

### 5.3.3 登録したルート証明書の確認



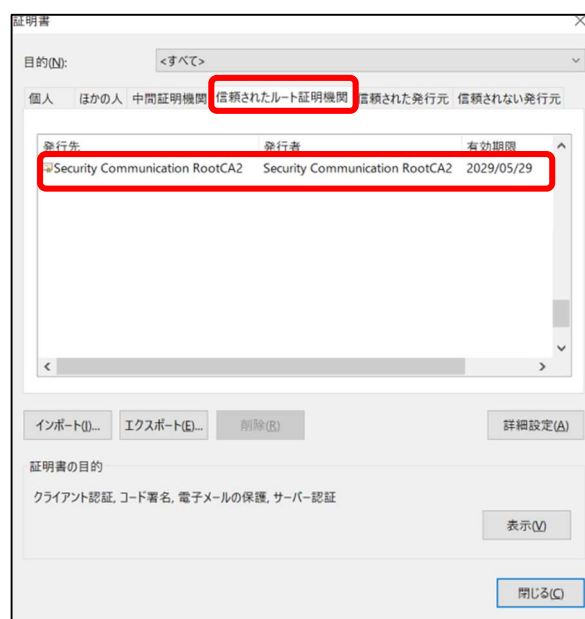
1. Edge を起動します。



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. 「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」と表示されている証明書が登録されていることを確認します。

## 5.4. 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】

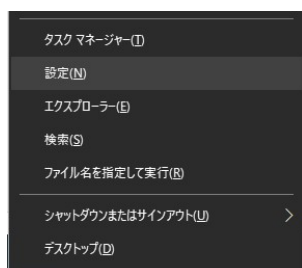
MPKI クライアントを使用すると、有効期限の前に更新をお知らせする機能や証明書の更新を簡易に行う機能が利用できます。

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、Windows 10、及び Windows 11 です。

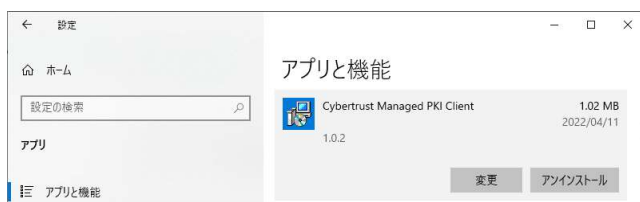
利用環境の詳細は「5.1 MPKI クライアント利用環境」を参照ください。

### 【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「**Windows**」キーを押しながら「**X**」キーを押し、表示された一覧から「**コントロールパネル**」>「**プログラムと機能**」または「**設定**」>「**アプリ**」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. 「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)」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。