# 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

目次 2
はじめに
事前準備 6
1. 各種申請の流れ
1.1. 電子証明書の新規発行手続き7
1.2. 電子証明書の更新手続き8
1.2.1. MPKI クライアントを利用した電子証明書の更新
1.2.2. 電子証明書更新サイトからの電子証明書の更新
1.3. 電子証明書の失効手続き 11
2. 電子証明書の新規発行手続き 12
2.1. 電子証明書の新規発行申請12
2.2. MPKI クライアントのインストール12
2.3. 電子証明書のダウンロード15
2.4. 電子証明書のインストール18
2.4.1. こんなときは! 21
2.5. 登録した電子証明書の確認23
2.6. 電子証明書のバックアップ 24
3. 電子証明書の更新手続き 25
3.1. MPKI クライアントを利用した電子証明書の更新 25
3.1.1. MPKI クライアントのバージョンアップ 25
3.1.2. 電子証明書の更新
3.1.3. 電子証明書バックアップ 28
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 30
3.2.2. 登録した電子証明書の確認
3.2.3. 電子証明書のバックアップ 40
4. 電子証明書の失効手続き 42
4.1. 電子証明書の失効申請 42
4.2. 電子証明書の削除 43
5. 電子証明書の削除 44
6. サポート情報
6.1. MPKI クライアント利用環境 46
6.2. ご利用にあたっての注意事項 46
6.2.1. 認証用の証明書の選択画面が表示された場合

	6.2.2.	MPKI クライアントインストール時の注意事項	47
	6.2.3.	セッション無効時のトラブルシューティング	47
	6.2.4.	ルート証明書の取得とインストール	47
6.	3. MPK	I クライアントのバージョンアップ	55

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	<ul> <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UR</li> <li>L変更に伴う修正</li> </ul>
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	<ul> <li>・医療機関等向け総合ポータルサイトを追加</li> <li>・対応 0S に Windows11 を追加</li> </ul>
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. <b>各種申請の流れ</b> 」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 /	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
2023/02/ XX	1. 10. 0	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=4356711cc3537910615bd1877a0 131b6&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\_tebik i.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	有効期限の90日前、60日前、30日
示	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	有効期限の90日前~期限日
※支払基金のみ	
メール通知	有効期限の 75 日前、60 日前、45 日
※電子証明書の発行申請時に入力したメールアド	前、30日前、15日前、7日前~期限
レス宛に「no-reply@ssk.or.jp」からメール通知	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。

10

### 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-rep ly@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。 <u>https://www.ssk.or.jp/seikyushiharai/iryokikan/download/index.files/kyotu\_tebiki</u>.<u>pdf</u>

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、<u>Windows 8.1</u>と<u>Windows 10、</u>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。



□         □	2. 「…」をクリックし、「 <b>フォルダに表示</b> 」 をクリックします。
名前 日付時刻 種類 <b>2</b> 020/12/14 17:31 Windows インストー インストール(I) 修復(P) アンインストール(U) 互換性のトラブルシューティング(Y)	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。
Cybertrust Managed PKI Client セットアップ ウィザード         Cybertrust Managed PKI Client セットアップ ウィザード         Cybertrust Managed PKI Client セットアップ ウィザード         Cybertrust Managed PKI Client をインストールするために必要な手順を示します。         Co製品は、著作権に関する法律および国際条約っより保護されています。この製品の全部         Efficientの侵害となりますので         Efficientの侵害となりますので         Efficient          the system of the syste	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。
Cybertrust Managed PKI Client     インストール フォルダーの選択     「     インストール フォルダーの選択     「     マンストーラーは次のフォルダーへ Cybertrust Managed PKI Client をインストールはます。     このフォルダーにインストールするにはたい、1をクリックしてください。BIのフォルダーにインス     トールずるには、アドレスを入力するか「参照」をクリックしてください。     フォルダー(E):     「C*Users*terak.awa¥AppData*Local¥Programs*CybertrustMPKIDIi 参照(B)     ディスク領域(D)      キャンセル     く 戻る(B)     次へ(M) >	5. 「 <b>次へ</b> 」をクリックします。

d Cybertrust Managed PKI Client - X	6.「 <b>次へ</b> 」をクリックします。
インストールの確認	
Cybertrust Managed PKI Olient をインストールする準備ができました。 D次へ]をクリックしてインストールを開始してください。	
キャンセル 〈戻る(B) /次へ( <u>N</u> ) >	
Gybertrust Managed PKI Client      -      X	7. 「 <b>閉じる</b> 」をクリックします。
インストールが完了しました。	
Cybertrust Managed PKI Olient は正しくインストールされました。 終了するには、[閉じる]をクリックしてください。 Windows Update で、NET Framework の重要な更新があるかどうかを確認してください。	
キャンセル 〈 戻る(B) 開じる(Q)	
8	8.MPKI クライアントのインストールが完了
D	すると、スタートメニューに「Cybertrust Man
	aged PKI Client」か追加されよう。
<ul> <li>Cybertrust 新規</li> </ul>	
① Cybertrust Managed PKI Client 新規	
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	20210121xxxxxx
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 $\sim$ 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



<sup>・</sup>電子証明書ダウンロードサイト

オンライン請求システム専用認証局 電子証明書ダウンロードサイト		
ログイン		
ユーザロとバスワードを入力して下さい。 ユーザロ バスワード		
ログイン 認証局運用規程(CP/CPS)をウンロード		
自己署名証明書設定手順書 自己署名証明書ダクンロード		
<ul> <li>              え<u>ጠ合せ</u> 〈オンライン請求システムヘルプデスク&gt;             電話番号:0120-60-7210 〈特定健診・保健指導システムヘルプデスク&gt;             電話番号:0120-109-957      </li> <li>             新しい電子証明書の発行申請はこちらをクリックしてください。         </li> </ul>		
<u>電子記明書の発行申請サイト</u> <u>記明書ダウンロードサイト</u> (専用のID、バスワードが必要です。)		
接続がプライベートではありません 攻撃数が、 み取ろうとしている可能性があります。 NET-ERF_CERF_AUFH-ORITY_INVALIO		
IHER Z		

1. <u>レセプトオンライン請求端末またはオンラ</u> <u>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!】





<u>۲</u>

X

すべて表示

202012230100972.p12

ファイルを開く

5

17



# 2.4. 電子証明書のインストール

名前 更新日時 202011270094998.p12 PFX のインストール(I) 開く(O) S Skype で共有	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. 「 <b>証明書のインポートウィザード</b> 」が表示 されます。保存場所は「 <b>現在のユーザー</b> 」を選
証明書のインボート ウィザードの開始	択し、「 <b>次へ</b> 」をクリックします。
このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機關によって発行された証明書は、ユーザーIDを確認し、データを保護したり、またはセキュリティで保護 されたネットワープ接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の構成です。	
- 保存場所 ●限在のユーザー(C) ○ ローカル コンピューター(L)	
続行するには、「次へ」をクリックしてください。	
次へIN」 キャンセル	

×	3. 「インポートする証明書ファイル」が表示
↓証明書のインボートウイザード	されます。ファイル名に電子証明書のファイル
インボートする証明書ファイル	名が表示されていることを確認し、「 <b>次へ</b> 」を
インボートするファイルを指定してください。 ファイルる(E): C ¥Users¥cocxx¥Downloads¥202002190000055.p12 季篇(B)	クリックします。
注意: 次の形式を使うと 1 つのアイルに複数の証明巻を保留できます: Personal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P78) Microsoft シリアル化された証明書ストア (.SST)	
<u>次へ(N)</u> キャンセル	
	× 4. 「 <b>秘密キーの保護</b> 」が表示されます。「パ
☞ 証明書のインボート ウィザード	スワード」に「2.3. 電子証明書のダウンロー
秘密キーの保護 セキュリティを維持するために、秘密キーはパスワードで保護されています。	ド」で設定した「 <b>証明書パスワード</b> 」を入力し - ます。
秘密キーのパスワードを入力してください。	「 <b>インポートオプション</b> 」について、以下の内
ノ(スワード(P):	家を設定します
	日を収定します。
∼ インポート オブション(I):	エーックなめナ
インボートオブション(I): ・ 密キーの保護を強力にする(E) のオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。	チェックを外す
インボートオブション(I): ・ ・ 密キーの保護を決力にする(E) のオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 ・ のオークエフスポート可能にする(M) のパックマップーグレムニンフォームを可能にします。	<b>チェックを外す</b> [このキーをエクスポート可能にする]を
インボートオブション(I): ・ 認考キーの保護を強力にする(E) ・ のオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 ・ のキーをエクスポート可能にする(M) ・ のパックアップやトランスポートを可能にします。 	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
インボートオブション(I):  :密キーの保護を強力にする(E)  のオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。  のオーをエクスポート可能にする(M) のパックアップやトランスポートを可能にします。  伝想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)  マッドての拡張プロパティを含める(A)	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
インボートオブション(1): ・ 認率キーの保護を強力にする(E) のオブションを有効にすると、秘密キーがアブリケーションで使われるたびに確認を求められます。 ・ のキーをエクスポート可能にする(M) ・ のパックアップやトランスポートを可能にします。 ・ 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P) ・ のが、 ての拡張プロパティを含める(A)	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

.....

×	5. 「 <b>証明書ストア</b> 」が表示されます。「 <b>証明</b>
← 🦻 証明書のインポート ウイザード	書の種類に基づいて、自動的に証明書ストアを
証明書ストア 証明書ストアは、証明書が保管されるシステム上の領域です。 Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ● 庭明書の準頼に基づいて、自動的に証明書ストアを選択する(U)	<b>選択する」</b> を選択後、「 <b>次へ</b> 」をクリックしま す。
○証明書をすべて次の入トアに記載する(2) 証明書ストア: 参照(2)	
次へ(2) キャンセル	
×	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。「 <b>完了</b> 」をクリックします。
(売了)をクリックすると、証明書がインポートされます。 次の設定が指定されました: [選択された証明書入ト]: ウィザードで自動的に決定されます 内容 PFX	【こんなときは!】
ファイル-各 C:WJsers¥xxxxxx WDownloads¥202002190000055,p12	「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。
<b>東7(D)</b> キャンセル	

.....

証明書のインボート ウィザード ×	7. 「 <b>正しくインポートされました</b> 」が表示さ れます。「 <b>OK</b> 」をクリックします。
ビキュリティ警告         ×	【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、「 <b>はい</b> 」をクリックします。
<ul> <li>発行者が次であると主張する証明機関(CA)から証明書をインストールしようとしています:</li> <li>Online Billing NW Common Root CA - G1</li> <li>証明書が実際に"Online Billing NW Common Root CA - G1": からものであるかどうかを検証できません。"Online Billing NW Common Root CA - G1": たらものであるかどうかを検証できません。"Online Billing NW Common Root CA - G1"に這幅して発行者を確認する必要があります。 次の者号は203程を役立ちます:</li> <li>環印(sha1): C989E3EC FFTE7F33 AA604E48 8E0635D2 EE3EF5E5</li> <li>警告: このいート証明書をインストールすると、この CA によって発行された証明書は 自動的に信頼されます。確認されていない時印付きの証明書をインストール することは、セキュリティ上、危険です。(はい)をクリックすると、この危険を認 識したことになります。</li> <li>この証明書をインストールしますか?</li> </ul>	「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。

新しい秘密交換す	⊧-をインポートします ×	1. 「 <b>セキュリティレベルの設定</b> 」をクリック
	アブリケーションは保護されたアイテムを作成しています。	します。
	CryptoAPI 秘密キー	
	セキュリティレベル - 中 セキュリティレベルの設定( <u>S</u> )	
	OK キャンセル 詳細( <u>D</u> )	





## 2.5. 登録した電子証明書の確認

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)	4. 「 <b>個人</b> 」タブを開き、発行者が「 <b>Online B</b>
発行 [] [] []	先 619931494 llient 001	整行書 Online Billing NW Common Root CA - G1 KRS GP CA 2014	有効期限 フレンドリ名 2024/03/10 cn=1619931494, 2033/01/31 <なし>	illing 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。



#### 【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 の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



Cybertrust Managed PKI Client ×	2. 更新したい電子証明書を選択し、「証明書
「証明書一覧」から更新対象の証明書を違択し、「証明書更新」ボタンをクリックしてください。 更新された証明書は、自動でインストールされます。	<b>更新</b> 」をクリックします。
III明書一覧 (L):	
発行先 発行者 有効期限 2000000 0000000 0000000 0000000 0000000	
011A123456 CN=Online Billine NW Co_ 2023/05/26 13:01:39	
I正8月書更新(D	
	- 5
Cybertrust Managed PKI Client $ imes$	3. 「はい」をクリックします。
1003 選択した証明書を更新します。よろしいですか?	
はいM いいえM	
Cybertrust Managed PKI Client × 1004 証明書の更新が完了しました。	4. (OK) 2//// Carro
Cybertrust Managed PKI Client 🛛 🗙	5. 「パスリード」に鍵の暗号化パスリード
	(任意のパスワード) 半角数字4桁を入力して
証明書のバックアップファイルを作成します。	「 <b>OK</b> 」をクリック <b>します</b> 。
証明書パスワード □ パスワードを表示する	
証明書パスワード(確認用)	
□ パスワードを表示する	
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。	
OK	

🖉 名前を付けて保存		× 6. 証明書の保存先を指定して「保存」をク
← → × ▲ ▲ × × × × × × × × × × × × × × × ×	く 〇 ドキュメントの絵索	· ックします.
· · · · · ·		
整理 * 新しいフォルダー	^	
■ ドキュメント ★ 名前	史新日時	
⊻ 9720-⊦ * ■		
ファイル名(N): 202008140081347.p12		~
ファイルの種類(T):		~
作成者: 在安保庾診療職開文	タワ: タワの追加	
		+ L2/201
Cybertrust Managed PKI Client	^	
<ul> <li>1006 更新前の証明書を</li> <li>はい()</li> </ul>	削除しますか? いいえ( <u>N)</u>	
i 1006 更新前の証明書を (上いの) Cybertrust Managed PKI Client	削除しますか? いいえ(N) ×	8.「 <b>OK</b> 」を <b>クリック</b> 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。

Windows セキュリティ ×	<ol> <li>パスワードを入力し、「許可」をクリック</li></ol>
資格情報が必要です	します。 <li>※パスワードは、電子証明書のインストール時</li>
秘密キーへのアクセスをアプリに許可するには、パスワードを入力してくだ	「2.4.1.こんなときは!」で設定したパスワ
さい:	ードです。
1 050-95 - CUPPOAF120日1 パスワード パスワードの入力 許可 許可しない	

#### 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。



【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

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。
Steps://ext.obs.maragedpit.rej.p/pt	<ol> <li>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。</li> <li>【電子証明書更新申請サイト】 https://cert.obn.managedpki.ne.jp/p/ru</li> </ol>
	<ul> <li>※オンライン請求システムにログインすると、</li> <li>電子証明書更新申請サイトのリンクがあります。</li> <li>【こんなときは!】</li> </ul>
<b>jstatu/シーノハイトドにはのりません</b> から個人情報 (パスワード、メッセージ、クレジットカードなど) を盗 みあらうとしている可能性があります。 NET:ERR_CERT_AUTHORITY_INVALID             J#細設定	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 再新対象の電子証明書を選択し、「 <b>OK</b> 」
× 認証用の証明書の選択 サイト cert.obn.managedpki.ne.jp では資格情報が必要です: のlilT123456 Online Billing NW Common Root CA - G1 2020/9/5	2. 更利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
<b>証明書情報</b> OK キャンセル	

3.2.1. 電子証明書の更新

.....

.....

Cybertrust M 延明書の更新 証明書更新申請 更新後証明書の取得	1anaged PKI サイバートラスト マネージドP サイバートラスト マネージドPKI の証明書の 証明書更新申請 現在お使いの証明書の更新申請を送信します。	3. す。	「証明書更新申請」をクリックしま
<b>建</b> 更 以下の内容で証明書更	夏新申請情報の確認 <sup> 新申請を送信します。</sup>	4.	「Submit」をクリックします。
よろしければ ISubm	it」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		

申課 証明書の	送信完了 請報を受け付けました。 )発行申請はこれで完了です。 申請の受付情報	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。
リクエスト ID リファレンス ID 証明書ステータス	202012140100076 zigLUVC29Q 発行済み	
受け付けた申請情報の Common Name Organizational Unit Organizational Unit Organization Country	戸詳細は以下のとおりです。 0110119153 medical hokkaido ReceiptOnline JP	
避の取得 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 パスワードので 認 Submit		<ul> <li>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。</li> <li>【注意】</li> <li>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</li> </ul>
鍵をダウンロードします。 (こは、「Download」ボタ)	鍵の取得 <sup>鍵のダウンロードまたはインストールを行う</sup> ジをクリックしてください。 Download	い。 7. 「Download」をクリックします。





2. RETTOREN (V.P. L. H. M. L.	<  13. 「 <b>秘密キーの保護</b> 」が表示されます。
← よ 証明者のインボート ワイサード	「 <b>パスワード</b> 」に「3.2.1. 電子証明書の更
秘密キーの保護	新」で設定した <b>鍵の暗号化パスワード</b> を入力し
セキュリティを維持するために、秘密キーはパスワードで保護されています。	ます。
秘密キーのパスワードを入力してください。	「インポートオプション」について、以下の内
ノプスワード(P):	
••••	谷を設定します。
□ パスワードの表示(D)	[秘密キーの保護を強力にする]の
	チェックを外す
したサイロホス度を取力にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。	[このキーをエクスポート可能にする]を
□ 1のキーをエクスポート可能にする(M) −のバックアップやトランスポートを可能にします。	チェックを外す
□ 仮想化ペースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)	「ナベアの世界プロパティな合めて」な
☑ すべての拡張プロパティを含める(A)	
	チェックする
次へ(N) キャンセル	「次へ」をクリックします。
×	14 「 <b>証明書ストア</b> 」が表示されます。「 <b>証</b>
← 🦻 証明書のインボートゥィザード	田書の毎短に甘べいて、白動的に訂田書っしマ
証明書ストア	明音の種類に基づいて、日朝时に証明音へ下/
証明書ストアは、証明書が保管されるシステム上の領域です。	を選択する」を選択後、「次へ」をクリックし
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	ます。
⑥ 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(U)	
○ 血 分目ですべてのの入りに配置す の(1) 証明書ストア:	
参照(的	
次へ(N) キャンセル	
★ 夢 証明書のインポートウィザード	15. 「訨明書のインボートウイザードの完
弦明書のインボートウィザービの中で	<b>了</b> 」が表示されます。「 <b>完了</b> 」をクリックしま
証明者のインボート ワイサートの完了	す。
(元 /) モクリックすると、証明書がインボートされます。 次の設定が得定されました:	
選択された証明毎ストア  ウィザードで自動的に決定されます 内容 PK ファイル名 C+VJsersiFixxxxx VDownloadsV202002190000055.p12	【こんなときは!】
	「午」い初家な協た」たくいだ。 [ 午 ] い初家な協た」たくいだ。 [ 1 + + - *
	表示された場合、P21の「2.4.1. こんなとき
	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。
売了(D) キャンセル	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。



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。
the downwardship de united of the angle of the united of the angle of the united of the angle of the united	<ul> <li>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。</li> <li>【電子証明書更新申請サイト】</li> <li>https://cert.obn.managedpki.ne.jp/p/ru</li> </ul>
Cybertrust Managed PKJ PR# 2 Minit Pr# 2 Minit Pr# 2 Minit Pr/ ートラスト マネージドPKJ Cycle - レイントラスト マネージドPKJ - レイントラスト - レージ - レイントラスト - レージ - レイントラスト - レージ - レー	2. 更新申請画面の「 <b>更新後証明書の取得</b> 」を クリックします。
更新申請情報の一覧 1 件中1-1件目を表示しています。 <u> 9/212入FID Common Name 歴史時度度新申時日時 有効</u> 期度 2万-921 取得 202012140100076 0110119153 2020.12.14 17:39:00 2024.03.14 17:39:07 発行済み Previous 20 Next 20	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「Down load 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 <b>の設定</b> 」をクリック
新しい秘密交換キーをインボートします	1++
アプリケーションは保護されたアイテムを作成しています。	しより。
CryptoAPI 秘密キー	
セキュリティレベル - 中 セキュリティレベルの設定( <u>S</u> )	
OK キャンセル 詳細( <u>D</u> )	
パスワードの作成 ×	2.任意の「CyptoAPI 秘密キー」のパスワー
このアイテムを保護するための、バスワードを作成します。	ドを入力し、「 <b>完了</b> 」をクリックします。
	【※重要※】
このアイテム用に新しいパスワードを作成する。	作成したパスワードは、今後の証明書の更新
CryptoAPI 秘密キーのパスワード:	時に利用するため、忘れないよう大切に保管
パスワード: ●●●●●●●●●●	ください。
< 戻る 完了(E) キャンセル	
新しい秘密交換キーをインポートします X	3. 「 <b>OK</b> 」をクリックします。
アプリケーションは保護されたアイテムを作成しています。	
CryptoAPI 秘密キー	
セキュリティレベル - 高 セキュリティレベルの設定( <u>S</u> )	
OK キャンセル 詳細( <u>D</u> )	



#### 3.2.2. 登録した電子証明書の確認

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	良された発行元	信頼されない発行元	4. 「 <b>個人</b> 」タブを開き、発行者が「 <b>Online B</b>
発行	ī先	圣行去	有効期限	フレンドリ名	illing NW Common Root CA」と表示されている
i⊒ 1 i⊒(	1619931494 Client 001	Online Billing NW Common Root CA - G1 KRS GP CA 2014	2024/03/10 2033/01/31	cn=1619931494, <なし>	電子証明書が登録されていることを確認しま
					च <u>े</u> .

#### 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。



#### 【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。



# 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	てから、手続きを実施して下さい。
http://www.awagedpole.ow.gog/ml	<ol> <li>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。</li> <li>【電子証明書失効申請サイト】</li> <li>https://cert.obn.managedpki.ne.jp/p/rx</li> </ol>
	【こんなときは!】
接続がプライベートではありません 攻撃音が、 から@人病報 (パスワード、メッセージ、クレジットカードなど)を盗 み取ろうとしている可能性があります。 NETGER, CERT, AUTHORITY_INVALID	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
<b>联相限定</b>	
	<ul> <li>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。</li> </ul>

.....

証明書矢効甲請情報の人力画面	3. 失効申請者の申請者のメールアドレスとメ
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 202103190101509	ールアドレス(確認用)を入力し、「申請」をク
リンテレンス ID [gh N0Xe+(P]] メールアドレス メールアドレス(編2用)	リックします。「 <b>証明書失効申請情報の確認画</b>
申請	面しへ遷移します。
・メールアドレス:申請者が所留する部署または申請者のメールアドレスを入力して ・メールアドレス確認的:確認のため、もう一度メールアドレスを入力してくされ、 ※失効処理を完て後、メールアドレス第回にひライアンド証明書,失効定ての通知』者 します。	
証明書失効申請情報入力内容の確認	 <sup>画面</sup> 4. 内容を確認し、「 <b>申請</b> 」をクリックしま
証明書失効申請情報入力内容の確認 以下の空間機動地構成近にます。 といければ甲基ボジンをパックしてだされ、 内部に動があれば、使らボタンをパックしてだされ、	 <sup>画面</sup> 4. 内容を確認し、「申請」をクリックしま す。
証明書失効申請情報入力内容の確認 以下の作意理明書大効申該活動します。 よういければ申題におつをジックしてびまし。 内部に使いがあれば、「家らボタンをクリックしてびきまし。 リクエストID 202103190101509	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>生効申請が承認されると入力されたメールアド</li> </ul>
証明書失効申請情報入力内容の確認 以下の作電は明素が明まぎ意にます。 よういければ甲酸ボタンをジンクしてださい。 内部に時があれば、「戻ちボタンをジンクしてださい。 ワンエスト ID 202103190101509 リファレンス.ID gdFNDXeFRP	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>失効申請が承認されると入力されたメールアド</li> </ul>
証明書失効申請情報入力内容の確認 以下の作意信即場大効申目を送信します。 ようしければ「申請ポタッをスリックしてびきん」 内前に思いがあれば、「戻ちポタッをスリックしてびきん」 クロンストロ リファレンス ID リファレンス ID メールアドレス 11(822.33)	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>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。</li> </ul>
証明書失効申請情報入力内容の確認 以下の内容で確明壊決助申請ぎ途(はよす。 よべいければ「申請」ポタッをフルップ、てびさみ、 内容に違いがあれば、「戻る」ポタンをクリップ、てびさみ、 リクエスト ID リファレンス. ID ログアレンス. ID ログアログアレンス. ID ログアログアレンス. ID ログアログアレンス. ID ログアログアログアログアログアログアログアログアログアログアログアログアログアロ	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>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。</li> </ul>
証明書失効申請情報入力内容の確認 以下の許確で現時違決が申請者送信します。 より、ければ申請があったがで送信し、 内容に追いがあれば、探らが考ジをクリックしての送信し、 リクエスト ID 202013190101509 リファレンス ID gdFNXX&FRP メールアドレス 11@22.33 甲請 戻る	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>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。</li> </ul>
証明書失効申請情報入力内容の確認 しての時では明確決め申請を送信します。 とうしければ申請があったのでのない。 Print # があれば、「夜らがすうとうりうしてのされ、 リクエスト ID 202103190101509 リファレンス ID g6FNDX6FRP メール77 Lス 11(922.33 単語 戻る	<ul> <li>画面</li> <li>4. 内容を確認し、「申請」をクリックします。</li> <li>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。</li> </ul>

# 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。

	🖪 🌣 🗲 🕼	a 😩 \cdots	1. Edge を起動し、	画面右上の「 <b>設定(S)</b> 」を
	新しいタブ(T)	Ctrl+T	クリックします。	
E	新しいウィンドウ(N)	Ctrl+N		
The second secon	こ 新しい InPrivate ウインドウ(I)	Ctrl+Shift+N		
		009/ L Z		
		00% 1 2		
	■ お気に入り(O)	Ctrl+Shift+O		
S S S S S S S S S S S S S S S S S S S	) 履歴(H)	>		
	_ ダウンロード(D)	Ctrl+J		
	□ アプリ(A)	>		
	3 拡張機能(X)			
6	∃ コレクション(E)	Ctrl+Shift+Y		
2/1/1050/ E	<b>ユ</b> 印刷(P)	Ctrl+P		
<b>P</b>	Web キャプチャ	Ctrl+Shift+S		
	3 共有(R)			
C,	る ページ内の検索(F)	Ctrl+F		
A	<ul> <li>) 音声で読み上げる(U)</li> </ul>	Ctrl+Shift+U		
Outlook	その他のツール(L)	>		
- in the first	(2) 完定			
設定	オプションの診断データ	は、すべてのユーザーのため	2. 「プライバシー	• <b>、検索、サービス</b> 」を選択
▶ 設定の検索	ブラウザーの使用状況	に関するオプションの診断	し、「セキュリティ」	」の「 <b>証明書の管理</b> 」をク
🔊 プロファイル	Microsoft 製品の改 この設定は、 <u>Windows</u> 影	善にご協力ください。 <sup> </sup> 断デ−タの設定によって決定る	リックします。	
┃ □ プライバシー、検索、サービス				
· ③ 外観	自分に合わせて	Web エクスペリエ		
<ul> <li></li></ul>	データとその他の広告の	D設定は、 <u>Microsoft プラ</u> ・		
■ 新しいタブページ	このアカウントでの開発	「履歴の使用 (広告、検索		
図 Cookieとサイトのアクセス許可	可することにより、Wel この設定を有効にするには	o エクスペリエンスを向上さ 、Microsoft アカウントでサイン		
□ 既定のブラウザー				
业 ダウンロード	セキュリティ			
戌、ファミリー セーフティ	Microsoft Edge のセ	キュリティ設定を管理		
槷 言語	証明書の管理			
品 ブリンター	HTTPS/SSL の証明書と読	没定を管理します		

# 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。

証明書   ×	3. 「 <b>電子証明書</b> 」が表示されます。「 <b>個人</b> 」
目的(N): <すべて> 、	タブを開き、 <b>有効期限が古い電子証明書</b> を選択
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	し、「削除」をクリックします。
発行先 日19931494 口 1619931494 口 1619931494 Client 001 保RS GP CA 2014 Client 001 Client 001 Clie	※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。
インボート(I) ゴクスボート(E) 削除(R) 詳細設定(A)	
証明書の目的	
· ≠=∩∩	
2010(1)	
閉じる(C)	
証明書	4. 「 <b>はい</b> 」をクリックします。
証明書         ×	5.「 <b>電子証明書</b> 」が表示されます。削除を行
目的(N): <すべて> <	った電子証明書が一覧から削除されていること
個人 ほんのし 内側部的換照 使調されたリーム部の換照 使調されたみたテー 使調されたいなたテ	を確認し「閉じろ」をクリックします
発行先         発行者         有効期限         フレンドリ名           G Client 001         KRS GP CA 2014         2033/01/31         <なし>	
インボート(D エクスボート(E) 削除(R) 詳細設定(A) 証明書の目的 更(*A(C))	

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

		-	-	
対応 0S		32bit	64bit	
	Windows 8.1	0	0	
	Windows 10	0	0	
	Windows 11	_	0	
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「Mic	erosoft .N	ET Framew	or
	k 4.8」以上がイン	ストールさ	れている事	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 Prox	(y
	認証の種類は、以下	のとおり-	です。	
	・Basic 認証			
	・NTLM 認証			

# 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

認証用の サイト cert.c	証 <b>明書の選択</b> obn.managedpki.ne.jp:では資格情報が必要です:	×	「証明書の選択」画面で発行者が 「Online Billing NW Common Root CA」となっ
	TEST Client 003 KRS GP CA 2014 TEST 2014/6/20 TEST Client 001 KRS GP CA 2014 TEST		ていることを確認し、「 <b>OK</b> 」をクリックして ください。
ģ	2014/6/20 011T123456 Online Billing NW Common Root CA 2020/7/3		
証明書情報	級 OK キャンセル		

6.2.2. MPKI クライアントインストール時の注意事項

闄 Cybertrust Managed PKI Client ×	左記のエラー画面が表示された場合は、「終
値 キーへの十分なアクセスがあることを確認するか、またはサポート担当者に問い合わせてください。	了」をクリックし、再度インストールを実施く ださい。
終了(X) 再試行(T) 続行(O)	

#### 6.2.3. セッション無効時のトラブルシューティング



#### 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。

接続がプライベートではありません
攻撃者が、 のら個人情報 (パスワード、メッセージ、クレジットカードなど) を盗 み取ろうとしている可能性があります。
NET::ERR_CERT_AUTHORITY_INVALID
詳細設定

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。
	<ol> <li>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</li> </ol>
② この増援のファイルはデバイスに指導を与える可能 があるため、SCRoot2ca.cer はブロックされました。 保存 」除 すべて表示 ×	2. 画面下の「 <b>保存</b> 」をクリックします。
	<ol> <li>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。</li> </ol>
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。

6.2.4.1. ルート証明書のダウンロード

□ 名前 更新日時 <sup>×</sup> 種類	1. ダウンロードしたルート証明書をダブルク
~ 今日 (1)	リックします。
Image: SCRoot2ca.cer         2021/03/29 13:37         セキュリティ証明書	
開いているファイル - セキュリティの警告 ×	2. 「 <b>セキュリティの警告</b> 」画面が表示されま
このファイルを開きますか?	す。「 <b>開く</b> 」をクリックします。
名前: d8bbwa¥TampStata¥Downloads¥SCRoot2ca (1) cor	
種類・ セキュリティ証明書	
発信元: C·¥Users¥meishu¥AppData¥Local¥Packages¥Micros	
開く(O) キャンセル	
✓ このファイルを開く前に常に確認する(W)	
インターネットのファイルは役に立ちますが、このファイルの種類はコンピューター	
に問題を起こす可能性があります。発信元が信頼できない場合は、このソフ トウェアを開かないでください。 <u>危険性の説明</u>	
■ 証明書 ×	3. 「 <b>証明音</b> 」画面が衣示されより。「 <b>証明音</b>
全般 詳細 証明のバス	<b>のインストール</b> 」をクリックします。
正明書の情報	
<ul> <li>リモートコンピューターに ID を証明する </li> </ul>	
<ul> <li>ソフトウェアがソフトウェア発行者の送信であるか確認する</li> </ul>	
<ul> <li>●公開後のソフトウェアの変更を禁止する</li> <li>■ ■ スソールを保護する</li> </ul>	
<ul> <li>● 電子メールを休護9 ○</li> </ul>	
発行先: Security Communication RootCA2	
発行者: Security Communication RootCA2	
有効期間 2009/05/29 から 2029/05/29	
証明書のインストール(I) 発行者のステートメント(S)	
ОК	

6.2.4.2. ルート証明書のインストール

×	4. 「 <b>証明書のインポートウィザード</b> 」画面が
差 証明書のインポート ウィザード	表示されます。「 <b>現在のユーザー</b> 」が選択され
証明書のインボートウィザードの開始	ていることを確認し、「 <b>次へ(N)</b> 」をクリックし
	ます。
このウイザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
証明機関によって発行された証明書は、ユーザーID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステ ム上の領域です。	
保存場所	
<ul> <li>● 焼生のユーダー(L)</li> <li>○ ローカル コンビューター(L)</li> </ul>	
続行す るには、[次へ] をクリックしてください。	
次へ(N) キャンセル	
×	5. 「証明書をすべて次のストアに配置する
₽ 証明書のインボートゥィザード	(P)」を選択し、「証明書ストア」の右側にある
証明書ストア	「参照(R)…」をクリックします。
証明書ストアは、証明書が保管されるシステム上の領域です。	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 ○ 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(J)	
Windows に証明告ストアを自動的に選択させるか、証明告の場所を指定することができます。 <ul> <li>○ 証明告の憧憬に基づいて、自動的に証明告ストアを選択する(U)</li> <li>● 証明告をすべて次のストアに配置する(P)</li> </ul>	
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。 <ul> <li>○ 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(<u>U</u>)</li> <li>◎ 証明書をすべて次のストアに配置する(<u>P</u>)</li> <li>証明書ストア:</li> </ul>	
Windows に証明会ストアを自動的に選択させるか、証明会の場所を指定することができます。 <ul> <li>ご証明会の種類に基づいて、自動的に証明会ストアを選択する(U)</li> <li>ご証明会をすべて次のストアに配置する(D)</li> <li>証明会ストア:</li> </ul>	
Windowsに証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。         ●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(L)         ●証明書をすべて次のストアに配置する(D)         証明書をすべて次のストアに配置する(D)         証明書をすべて次のストアに配置する(D)         証明書をすべて次のストアに配置する(D)	
Windows に証明巻ストアを自動的に選択させるか、証明巻の場所を指定することができます。 <ul> <li>・ 証明巻の増増に基づいて、自動的に証明巻ストアを選択する(L)</li> <li>● 証明巻をすべて次のストアに配置する(P)</li> <li>証明巻ストア:</li> </ul>	
Windows に証明告入トアを自動的に選択させるか、証明告の場所を指定することができます。	
Windows に証明告入ドアを自動的に選択させるか、証明告の場所を指定することができます。         ● 証明告の環境に基づいて、自動的に証明告入ドアを選択する(L)         ● 証明告をすべて次のストアに配置する(D)         2時音ストア         ● 歴明者入下         ● 歴史の書の	



←	書のインボートウィザード	×	8.	「完了」を	をクリックします。
証	明書のインポート ウィザードの完了				
[完	了」をクリックすると、証明書がインポートされます。				
次0	D設定が指定されました:				
<b>A</b>	-ザーが裏沢した証明會ストア 電源されたルート証明機関 電				
	<b>先了</b> (	E キャンセル			
証明書のインポート ウィザード ×			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。
(	正しくインポートされました。				
	ОК				



6.2.4.3. 登録したルート証明書の確認

EBI# X			4. 「 <b>証明書</b> 」画面が表示されます。		
的(N):         <すべて>         >           組人         ほかの人         中間証明機関         信頼されたルート証明機関         言頼された発行元         信頼されない発行元		~ 、	「信頼されたルート証明機関」タブを開き、 発行者が「Security Communication RootCA2」		
N/C# N/C# #A1900	+				
Security Communica	mmunication RootCA2 Security Communication RootCA2 2	1 RootCA2 2029/05/29	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。		
<		>			
	- <b>ト/E</b> ) 約150/1D)	詳細設定(A)			
インポート() エクスポ		In the second gap			
インポート(I) エクスポ 証明書の目的	- L (P) Halley (P)	a the sector (ca)			
インボート() エクスボ 証明書の目的 クライアント認証, コード署名	5, 電子メールの保護, サーバー認証	表示(1)			
インボート() エクスボ 証明書の目的 クライアント認証, コード署4	4. 電子メールの保護,サーバー認証	表示(Y)			

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。

<u>ルート証明書のインストールの作業はこれで終了です。</u>

#### 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、<u>Windows 8.1</u>と <u>Windows 10、</u>また は <u>Windows 11</u>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. <u>オンライン請求ネットワークへ接続の端末</u>
	で、キーボードの「■」キーを押しながら
エクスプローラー( <u>E</u> )	
検索( <u>5</u> )	「A」キーを押し、衣示された一見から「設
ファイル名を指定して実行( <u>R</u> )	定」> [アプリ] または「コントロールパネ
	<b>ル</b> 」>「 <b>プログラムと機能</b> 」をクリックしま
デスクトップ(D)	す。
<ul> <li>вя</li> </ul>	2. アンインストールしたいアプリを選択し、
ω ホ-ム アプリと機能	「 <b>アンインストール</b> 」または「 <b>アンインストー</b>
設定の検索 の Cybertrust Managed PKI Client 1.02 MB 2022/04/11 2022/04/11	<b>ルと変更</b> 」を選択し、画面の指示に沿って、ア
עליד 1.0.2	ンインストール作業を行います。
室 アブリと機能 変更 アンインストール	
() A http://cot.cha.managadaki.pa.in/p/c/	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。
CybertrustManagedmsi すべて表示 ×	
2.1.03803	