# 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

はし	こめに	<b>-</b>
0.	事前	<b>5準備</b> 4
1.	証明	月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
1	. 2.	証明書のインストール
	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	月書の更新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!
	2.1.	.2 MPKI クライアント利用時の証明書バックアップ
2	. 2.	更新申請画面からの更新23
	2.2.	.1 こんなときは!
3.	証明	月書の失効
4.	証明	月書の削除
5.	サオ	ペート情報
5	. 1.	MPKI クライアント利用環境
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
	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
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
	5.3.	.2 ルート証明書のインストール
	5.3.	.3 登録したルート証明書の確認
5	.4.	MPKI クライアントのバージョンアップ

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</li> </ul>
		ン資格確認等接続ガイド(IP-VPN 接続方式)の
		URL 変更に伴う修正
2021/04/27	1.4.0	・「5.3. ルート証明書の取得とインストール」を
		追加
2022/04/13	1.5.0	・「5.4. MPKI クライアントのバージョンアップ」
		を追加
		・医療機関等向け総合ポータルサイトを追加
2024/01/15	1.6.0	・対応 OS に Windows11 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=4356711cc3537910615bd1877a0 131b6&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、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	XXXXXXXXXXXXXXXX
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

オンライン請求システ	4
社会保険診療報酬支払基金 東京支部	
ユーザロとパスワードを入力して下さい。 ユーザロ パスワード <b>ログイン</b> 利用限約 プライパシーポリアー パスワードを忘れた方へ	
<ul> <li></li></ul>	读者

1-1. <u>レセプトオンライン請求端末</u>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.<u>オンライン資格確認端末</u>からダウンロ ードサイトにアクセス

「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。



## 1.2. 証明書のインストール

名前 更新日時	1. ダウンロードした証明書ファイルを右クリ
202011270094998.p12     PFX のインストール(I)     開く(O)     Skype で共有	$\begin{array}{c} \neg \neg$
★ 証明書のインボート ウィザード ★ 証明書のインボート ウィザードの開始 このウィザードでは、証明書、証明書信頼リスト、あよび証明書先かりストモ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システム上の領域です。 ● 限在のユーザー(C) ● ローカル コンビューター(L) ● 低行す るには、(次へ) をクリックしてください。 ※次化(1) ※次化(2) ※次化(2)	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「 <b>現在のユーザー</b> 」を選択 し、「 <b>次へ</b> 」をクリックします。
※ 証明書のインボートウィザード インボートする証明書フィル インボートするファイルを指定してください。 ファイルを(E): C¥Users¥xxxxx¥Downloads¥202002190000055.p12 参照(E) 注意:次の形式を使うと1つのファイルに複数の証明巻を保管できます: Personal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Synta XRG #12 (.PFX, P12) Cryptographic Message Synta XRG #12 (.PFX, P12) Microsoft ジリブル化された証明書ストア (.SST)	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、「 <b>次へ</b> 」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
← 😺 証明書のインボート ウィザード	ード]に「1.1.証明書のダウンロード」で設定し
秘密年-の保護	たパスワードを入力します。
セキュリティを維持するために、秘密キーはバスワードで保護されています。	「インポートオプション」について、以下の内容
秘密キーのパスワードを入力してください。	を設定します。
パスワード( <u>P</u> ):	「秘密キーの保護を強力にする」の
••••	
□ /(スワードの表示( <u>D</u> )	チェックを外す
	[このキーをエクスポート可能にする]を
」とは、「いはなどはか」とうのに) のオブションを有効にすると、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。	チェックする
□ のキーをエクスポート可能にする(M) ーのバックアップやトランスポートを可能にします。	[すべての抗張プロパティを含める]を
○ 仮想化バ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)	
☑ ·べての拡張プロパティを含める( <u>A</u> )	チェックする
	「 <b>次へ</b> 」をクリックします。
次へ(N) キャンセル	



.....

× 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。

<ul> <li></li></ul>	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。
[死 ] をクリウすると、証明書かく2ボートされます。 次の設定が指定でれました	【こんなときは!】 「新しい秘密交換キーをインポートしま
<b>元</b> 7(① ] キャンセル	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。
証明書のインボート ウィザード ×	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。
レキュリティ響告         ×	「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" からのものであるかどうかを検証できません。"Online Billing NW Common Root CA - G1" からのものであるかどうかを検証できません。"Online Billing NW Common Root CA - G1" は単わ (chall): C989E3EC FF7E7F33 AA604E48 8E0635D2 EE3EF5E5</li> <li>警告: このルト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、セネリティ上、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> </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」
この証明書をインストールしますか? はい(Y) いいえ(N)	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。

新しい秘密交換キーをインボートします × 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。 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(S)	1.「 <b>セキュリティレベルの設定</b> 」をクリックし ます。
パスワードの作成 × このアイテムを保護するための、パスワードを作成します。	2.任意のパスワードを入力し、「 <b>完了</b> 」をクリ ックします。
このアイテム用に新しいパスワードを作成する。 CryptoAPI 秘密キーのパスワード: パスワード: 確認入力: < 戻る 完了(E) キャンセル	【※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。
新しい秘密交換キーをインボートします × 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。	3.「 <b>OK</b> 」をクリックします。
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(S)	
OK 詳細(D)	

#### 1.3. 登録した証明書の確認



個人	ほかの人	中間証明機関	信頼されたル−ト証明機関	信頼	された発行元	信頼されない発行元	4.「
発行	先	圣行妻			有効期限	フレンドリ名	Billi:
1 1 1	619931494 lient 001	Online Billin KRS GP CA 2	ng NW Common Root CA - 2014	G1	2024/03/10 2033/01/31	cn=1619931494, <なし>	証明書

**個人**」タブを開き、発行者が「Online ng NW Common Root CA」と表示されている 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。



#### 【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、<u>Windows 8.1</u>、<u>Windows 10 及び</u> 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。



Heff	
媛 Cybertrust Managed PKI Client - 🗌 🗙	4.「Cvbertrust Managed PKI Client セットア
Cybertrust Managed PKI Client セットアップ ウィサード	
	ップウィザード」 が開始されます。 「 <b>次へ</b> 」 をク
インストーラーは 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。	リックします。
この製品は、著作権に関する法律および国際条約により保護されています。この製品の全部 または一部を無断で複製したり、無断で複製物を通布すると、著作権の侵害となりますので、	
注意ください。	
キャンセル 〈 東ふ(B) ( 次へ(N) 〉	
嫒 Cybertrust Managed PKI Client - □ ×	5 「ガヘ」をクリック」ます
インストール フォルダーの選択	$5. \mathbf{[} \mathbf{K^{*}} \mathbf{]} \mathbf{z} \mathbf{y} \mathbf{y} \mathbf{y} \mathbf{y} \mathbf{z} \mathbf{z} \mathbf{y},$
インストーラーは次のフォルダーへ Oybertrust Managed PKI Client をインストールします。	
このフォルダーにインストールするには[次へ]をクリックしてください。別のフォルダーにインス トールするには、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¥terakawa¥AppData¥Local¥Programs¥CybertrustMPKICli 参照( <u>R</u> )	
ディスク領域( <u>D</u> )	
😸 Cybertrust Managed PKI Client - 🗆 🗙	
インストールの確認	6.「 <b>次へ</b> 」をクリックします。
[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 - □ ×     インストールが完了しました。     「     」	7.「 <b>閉じる</b> 」をクリックします。
Cybertrust Managed PKI Client は正しくインストールされました。 終了するには、【開じる】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 く 戻る(B) 開じる(C)	
8	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
	<b>PKI Client</b> 」が追加されます。
〇〇 Cybertrust 新規	
① Cybertrust Managed PKI Client 新規	

## 1.6. 認証用の証明書の選択画面が表示された場合

1 「認証田の証明書の選択」両面で発行者が

認証用の	証明書の選択	1.「認証用の証明者の選択」回面で発行有か
サイト cert.		「Online Billing NW Common Root CA」となっ
TEST Client 003 KRS GP CA 2014 TEST 2014/6/20		ていることを確認し、「 <b>OK</b> 」をクリックしてく ださい。
ā	<b>TEST Client 001</b> KRS GP CA 2014 TEST 2014/6/20	
ģ	011T123456 Online Billing NW Common Root CA 2020/7/3	
証明書情	報 OK キャンセル	

17

## 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】



Cybertrust Managed PKI Client × 1004 証明書の更新が完了しました。	4.「 <b>OK</b> 」をクリックします。
Cybertrust Managed PKI Client × 1006 更新前の証明書を削除しますか? はい(Y) いいえ(N)	5.「 <b>はい</b> 」をクリックします。
Cybertrust Managed PKI Client × i 1005 更新前の証明書の削除が完了しました。	6.「 <b>OK</b> 」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。

Windows セキュリティ × 資格情報が必要です 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 さい:	<ol> <li>パスワードを入力し、「許可」をクリックします。</li> <li>※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</li> </ol>
キーの説明 : CryptoAPI 秘密キー	ドです。
Rスワード Rスワードの入力 許可 許可しない	

19

## 2.1.2 MPKI クライアント利用時の証明書バックアップ

ファイル名を指定して実行(R)       シャットダウンまたはサインアウト(U)       スタート       デスクトップ(D)	1. 画面の左下の Windows ボタンを右クリック し、「 <b>ファイル名を指定して実行</b> 」をクリックし ます。
<ul> <li>□ ファイル名を指定して実行</li> <li>×</li> <li>● 実行するブログラム名、または開くフォルダーやドキュメント名、イン ターネットリソース名を入力してください。</li> <li>名前(Q)</li> <li>Certmgr.msc</li> <li>∨</li> <li>OK</li> <li>キャンセル</li> <li>参照(B)</li> </ul>	2.「certmgr.msc」を入力し、「OK」ボタンを クリックします。
	3.「 <b>個人</b> 」から「 <b>証明書</b> 」をクリックします。
発行先     発行者     有効期限       第行先     発行者     2024/03/22       第(O)     第(O)     第(O)       すべてのタスク(K)     開く(O)     第(O)       ブリ取り(T)     新しいキーで証明書を要求(Q)       コピー(C)     新しいキーで証明書を書き換え(N)       削除(D)     詳細設定操作(A)       ブロ/テャイ(R)     エクスポート(E)       ヘルプ(H)	4. 発行者が「Online Billing NW Common Root CA」の <u>有効期限が新しい証明書</u> を選択し、右クリ ック後、「 <b>すべてのタスク</b> 」-「エクスポート」を クリック。
★ ジ 取得者のエクスポート ウィザード 歴時者のエクスポート ウィザードの開始: このウィザードでは、取得者、取得者を意味りたトをとび取得者を取りた手程研考えトアからディスクにコど します。 正時時級によって向けされた記述時者に、ユーザールを確認に、データを確認したり、まただけもコリチャで修施 れたりありーク・可能を見解すまたのの事業をもなでいます。足明者が学校またものシステ 上述を構成です。 用けずまとには、(水へ)をクリックしてください。	5.「 <b>次へ</b> 」をクリックします。

<ul> <li>         ★ 愛 昭明金のエクスポート ウィザード         ★ 愛 昭明金のエクスポート ウィザード         ★ 総営キーのエクスポート             秋宮キーを証明金と一緒にエクスポートするととができます。         </li> <li>             秋宮本ーはバスワードで修復されています。秋宮本ーを証明金と一緒にエクスポートする場合は、バスワードを             入力するな、要求力するます。          ※ 回日会 レー場に松空ネーをエクスポートしますか?         ④ 広い、松宮キーをエクスポートしますか?         ④ 広い、松宮キーをエクスポートしますか?         ○ いいれ、松宮キーをエクスポートしますか?         ○ いいれ、松宮キーをエクスポートしますか?         </li> <li>             へいたい、松宮キーをエクスポートしますか?</li> </ul>	6.「 <b>はい、秘密キーをエクスポートします</b> 」を 選択し、「 <b>次へ</b> 」ボタンをクリックします。
★ 録 証明書のエクスポート ウィザード エクスポート フィルの形式 2まざまなファイル形式で証明書をエクスポートできます。 使用する形式を選択してください:	<ul> <li>7.「Personal Information Exchange - PKCS#12</li> <li>(.PFX)」を選択します。</li> <li>[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</li> <li>「証明書のプライバシーを有効にする]を</li> </ul>
<ul> <li>DER encoded binary X509 (CER)(<u>0</u>)</li> <li>Base 64 encoded X509 (CER)(<u>5</u>)</li> <li>Cryptographic Message Syntax Standard - PKCS #7 証明會 (.P7B)(<u>0</u>)</li> <li>証 証明の/(スにある証明會を可能であればすべてきむ(1)</li> <li>④ Personal Information Exchange - PKCS #12 (.PFX)(<u>P</u>)</li> <li>ビ 証明の/(スにある証明會を可能であればすべてきむ(<u>0</u>)</li> <li>□ 正し、エクスポートされたときは秘密キーを制除する(<u>6</u>)</li> <li>□ ゴ いたったったする(<u>1</u>)</li> <li>□ ゴ いたったったする(<u>1</u>)</li> <li>○ 証明のプライパシーを有効にする(<u>5</u>)</li> <li>○ Microsoft シリアル化された証明書ストア (.SST)(<u>1</u>)</li> </ul>	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
次へ(N)     キャンセル              ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	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。

★ 愛 証明書のエクスポート ウィザード エクスポートするファイル エクスポートするファイルの名前を入力してください ファイル名(D): C@Uterr#paku#Desktop#夏新後の証明書.pfx ●第個(D) ★#ソゼル	9.「 <b>参照</b> 」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、「 <b>次へ</b> 」をク リックします。
★ ■ 証明書のエクスポート ウィザード 証明書のエクスポート ウィザードの完了 証明書のエクスポート ウィザードの完了 延明書のエクスポート ウィザードの完了 延明書のエクスポート ウィザードの完了 正明書のエクスポート ウィザードの完了 この目前の「日本」の一日」 正明書のエクスポート ウィザードの完了 この目前の「日本」の一日」 正明書のエクスポート ウィザードの完了 正明書のエクスポート ウィザードの完了 この目前の「日本」の一日」 この日本」の一日」 この目前の「日本」の一日」 この目前の目前の「日本」の一日」 この目前の目前の一日」 この目前の一日」 この目前の「日本」の一日」 この目前の目目	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。
証明書のエクスボート ウィザード × 正しくエクスボートされました。	

## 2.2. 更新申請画面からの更新

ttp://ert.don.managedpl.ong.jp/m     Communication     Comm	<ol> <li>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。</li> <li>【証明書更新申請サイト】 https://cert.obn.managedpki.ne.jp/p/ru</li> <li>【こんなときは!】</li> </ol>
	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
× 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IITI23456 Online Billing NW Common Root CA - G1 2020/9/3	<ol> <li>更新対象の証明書を選択し、「OK」をクリ ックします。</li> <li>※「Online Billing NW Common Root CA」と表 記されていることを確認</li> </ol>
Cybertrust Managed PKI           証明書の更新         サイバートラスト マネージドP           証明書更新申請         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.「証明書更新申請」をクリックします。

鍵更	三新申請情報の確認	┓ 4.「Submit」をクリックします。
以下の内容で証明書 よろしければ「Subn	更新申請を送信します。 nit」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	
	送信完了	5.証明書ステータスが「発行済み」となれば記 明書が発行されます。
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。		証明書ステータスは、「 <b>鍵生成中」→「発行要案</b> 中」→「発行済み」と遷移します。
	光1」中间はこれした」(9。	
	申請の受付情報	
リクエストロ	申請の受付情報 202012140100076	
リクエスト ID リファレンス ID	申請の受付情報 202012140100076 zigLUVC29Q	
リクエスト ID リファレンス ID 証明書ステータス	<ul> <li>申請の受付情報</li> <li>202012140100076</li> <li>zigLUVC29Q</li> <li>発行済み</li> </ul>	
リクエスト ID リファレンス ID 証明書ステータス 受け付けた申請情報の	申請の受付情報 202012140100076 zigLUVC29Q 発行済み 洋細は以下のとおりです。	
リクエスト ID リファレンス ID 証明書ステータス 受け付けた申請情報の話 Common Name	申請の受付情報 202012140100076 zigLUVC29Q 発行済み   詳細は以下のとおりです。 0110119153	
リクエスト ID リファレンス ID 証明書ステータス 受け付けた申請情報の Common Name Organizational Unit	<ul> <li>申請の受付情報</li> <li>202012140100076</li> <li>zigLUVC29Q</li> <li>発行済み</li> <li>詳細は以下のとおりです。</li> <li>0110119153</li> <li>medical</li> </ul>	
リクエスト ID リファレンス ID 証明書ステータス 受け付けた申請情報の Common Name Organizational Unit Organizational Unit	申請の受付情報 202012140100076 zigLUVC29Q 発行済み 詳細は以下のとおりです。 0110119153 medical hokkaido	
リクエスト ID リファレンス ID 証明書ステータス 受け付けた申請情報の Common Name Organizational Unit Organizational Unit Organizational Unit	申請の受付情報 202012140100076 zigLUVC29Q 発行済み 詳細は以下のとおりです。 0110119153 medical hokkaido ReceiptOnline	



#### 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。

取得

Next 20

Cybertrust	Managed PKI	トップへ ログアウト
証明書の更新 王明書更新申請 更新(波証明書の取) 得	サイバートラスト マネージドPKI サイバートラスト マネージドPKIの証明者の更新画面です。 証明書 更新中語 現在方法、の証明者の更新申録を送信します。 更新代記明者の取得 更新人た証明者を取得します。	<b>(</b> t cyber <b>trust</b>
	更新申請情報の一覧	

1件中1-1件目を表示しています。

02012140100076 0110119153 2020.12.14 17:39:00 2024.03.14 17:39:07 発行済み Download key

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

Previous 20

.....

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

	<ol> <li>4. 失効対象の証明書がインストールされた端</li> <li>末からオンライン請求ネットワークに接続して</li> <li>「証明書失効申請情報の入力画面」へアクセス</li> <li>します。</li> <li>【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!】 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
田明書失効申請情報の入力画面     電子評理意作時に送けました「電子評判書を行き回慮するか手元にご用き     この     ロウェンクはの     ロウェンクはの     ロウェンクはの     ロウェンクはの     マイ証明書を行き起した     マクエンクはの     マイ証明書を行き起した     マクエンクはの     マクエンク	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           実施建売Tのご386のため、メールアドレスを入力してくだき、い、           ソフニスト ID           ソフニンス ID           ソフトレンス ID           メールアドレスをNINGGERP           メールアドレス(WERP)           ・レアレフに2010年10日           ・ケールアドレス:           ・	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	↓ 4. 内容を確認し、「申請」をクリックします。
以下の中容では副導き外外用語を送信します。 よなしければ作用語が多と変わったてでなる。 や容可に思いがわれば、「見な」が多くさりっかしてがきょ。	失効申請が承認されると入力されたメールアド
U2エスト ID 202103190101509 Uファレンス ID gdFNXXeFRP メールアドレス 11@22.33	レス宛てに失効完了をご連絡します。

## 4. 証明書の削除



証明書	×	3.「訨明書」か表示されます。「 <b>個人</b> 」タブを開
目的(N):	<\$7\7\$ ~	き、 <b>有効期限が古い証明書</b> を選択し、「 <b>削除</b> 」を
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	クリックします。
発行先 同 1619931494 同 Client 001	発行者 有効期限 7レンドリ名 Online Billing NW Common Root CA - G1 2024/03/10 n = 1619931494, KRS GP CA 2014 2033/01/31 なし>	※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) 二 証明書の目的	エクスボート(E) 削除(R) 詳細設定(A)	
	表示(V) 閉じる(C)	
証明書	×	4.「 <b>はい</b> 」をクリックします。
<u>!</u> 証明書 ますか?	eを使って暗号化データの暗号化を解除できません。証明書を削除し (はい(Y) いいえ(N)	
証明書	×	5.「証明書」が表示されます。削除を行った証
目的(N):	<\$\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	   明書が一覧から削除されていることを確認し、
個人 (平400) 発行先 GLient 001	中間証明機器 信頼されたⅡ→5証明機器 信頼されたみ行开 信頼された1.94行开 発行者 有効期限 フレンドリ名 KRS GP CA 2014 2033/01/31 <なし>	「 <b>閉じる</b> 」をクリックします。
インポート(I) : 証明書の目的	エクスポード(E) 削除(R) 詳細設定(A)	
	表示(V) 閉じる(C)	

## 5. サポート情報

#### 5.1. 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			ľ
	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			эху
	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

₿ Cybertrust Managed PKI Client ×	左記のエラー画面が表示された場合は、「終了」
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聞い合 わせてください。	をクリックし、再度インストールを実施してく ださい。
終了(X) 再試行(T) 続行(O)	

## 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
セッション無効	合は、セッションが無効であることを示す画面
セッションがタイムアウトしました。 最初のページに戻ってください。	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 ヘ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

Ktp://ent.doe.maragedplit.vs.js/jr/d         スレライン語家システム           方ンライン語家システム           客文払備気温化           必定(用) 局断を請求する考え払構成を満んですい、 この面面を持ずする場合は、閉じるボタンを押してするい、           上公会業度変更           実施業度期である。           単二の業を見前する場合に、防したパタンプレービングに(専用のユービID, パスワードが必要です。)	<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>
Cの種類のファイルはデバイスに損害を与える可能 があっため、SCRootZca.cerはプロックされました。 保存 別除 すべて表示 ×	2. 画面下の「 <b>保存</b> 」をクリックします。
<ul> <li>↓ ○ ● =   ダウンロード</li> <li>ファイル ホーム 共有 表示</li> <li>← → ~ ↑ ◆ &gt; PC &gt; ダウンロード</li> <li>★ クイック アクセス</li> <li>▲ ダウンロード</li> <li>▲ ダウンロード</li> <li>▲ デスクトップ</li> <li>★ SCRoot2ca.cer</li> </ul>	<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>

### 5.3.2 ルート証明書のインストール

☐ 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。
□ SCRoot2ca.cer 2021/03/29 13:37	
	L
開いているファイル - セキュリティの警告 ×	2.「セキュリティの警告」画面が表示されます。
このファイルを開きますか?	「開く」をクリックします。
名前:d8bbwe¥TempState¥Downloads¥SCRoot2ca (1).cer	
発行元: <b>不明な発行元</b>	
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	
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. 「証明書」 画面が表示されます。 「 <b>証明書のイ</b>
	ンストールレをクリックします
1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	
この証明書の目的:	
<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> <li>(19) (19) (19) (19) (19) (19) (19) (19)</li></ul>	
<ul> <li>公開後のワフトウェアの変更を禁止する</li> <li>電子メールを保護する</li> </ul>	
祭行先: 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(小 発行者のステートメント/S)	
ОК	

←      疑明者のインポートウィザード	4. 「
	示されます。「現在のユーザー」が選択されてい
証明書のインポート ウィザードの開始	ることを確認し、「 <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。	
係存場所 ● 現在のユーザー(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(N) キャンセル	
	5 「江田書なオベブルのフトアに配置する」な
←	
	選択し、「証明書ストア」の石側にある「 <b>参照</b> 」
証明書ストア	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が、証明書の場所を指定することができます。	
○ 証明書の種類に変づいて、自動的に証明書ストアを選択する(」) ● 近明書をすべて次のストアに配置する(D)	
○ ( <u>enser</u> ) ( <u>enser</u> ) 2.9(R)	
次へ( <u>N</u> ) キャンセル	



×	8.「完了」をクリックします。
← 参 証明書のインボートウィザード	
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、証明書がインボートされます。	
次の設定が指定されました:	
ユーザーが登切した証明会入下         値構会れたルート証明機関           内容         証明書	
第7(E) キャンセル	
	9. 「正しくインポートされました。」のメッセ
証明書の12ホート ワイサート ×	ージを確認し、「 <b>OK</b> 」をクリックします。
正しくインボートされました。	
ОК	

#### 5.3.3 登録したルート証明書の確認



明書		×	4.「証明書」画面が表示されます。
目的(M):     <すべて>     >       個人     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       つこた     つこた     + + + + + + =		~	「信頼されたルート証明機関」タブを開き、発行
		れた発行元 信頼されない発行元	者が「Security Communication RootCA2」と表
Security Communica	ation RootCA2 Security Communication	n RootCA2 2029/05/29	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。
۲		>	
インボート(!) エクスボ	ート(E) 削除(B)	詳細設定( <u>A</u> )	
証明書の目的			
クライアント認証, コード署名	8, 電子メールの保護, サーバー認証		
		表示( <u>V</u> )	
		閉じる(C)	

#### 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、<u>Windows 8.1</u>、<u>Windows 10、</u>及び <u>Windows 11</u>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。

タスクマネージャー(1)       設定(N)       エクスプローラー(1)       検索(5)       ファイル名を指定して実行(R)	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「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」
	> [ <b>アプリ</b> ] をクリックします。
<ul> <li>◆ 設定 - □ ×</li> <li></li></ul>	<ol> <li>アンインストールしたいアプリを選択し、</li> <li>[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。</li> </ol>
← → ○ A https://cert.obn.managedpki.nejp/p/s/ ☆ ☆ @ @ …	<ol> <li>「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。</li> </ol>