# 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

## (Linux Firefox)

Version 1.6.0

令和7年2月19日

## 目次

目次	2
はじめに	5
事前準備	. 5
1. 各種申請の流れ	. 6
1.1. 電子証明書の新規発行手続き	6
1.2. 電子証明書の更新手続き	. 7
1.3. 電子証明書の失効手続き	. 8
2. 電子証明書の新規発行手続き	. 9
2.1. 電子証明書の新規発行申請	. 9
2.2. 電子証明書のダウンロード	. 9
2.3. 電子証明書のインポート	12
2.4. Java 実行環境に電子証明書をインポート	15
2.5. 登録した電子証明書の確認	19
2.6. Java 実行環境の電子証明書を確認する	21
2.7. 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	26
3.1. 電子証明書更新申請サイトからの電子証明書の更新	26
3.1.1. こんなときは!	33
3.2. Java 実行環境に電子証明書をインポート	35
3.3. 登録した電子証明書の確認	39
3.4. Java 実行環境の電子証明書を確認する	41
3.5. 電子証明書のバックアップ	44
3.6. 電子証明書の削除	45
4. 電子証明書の失効手続き	47
4.1. 電子証明書の失効申請	47
4.2. 電子証明書の削除	48
5. 電子証明書の削除	49
6. Java 実行環境の電子証明書を削除	51
7. サポート情報	54
7.1. ご利用にあたっての注意事項	54
7.1.1. 認証用の証明書の選択画面が表示された場合	54
7.1.2. セッション無効時の対応トラブルシューティング	54
7.2. ルート証明書のダウンロードとインポート	55
7.2.1. ルート証明書のダウンロード	55

7.2.2.	ルート証明書のインポート	56
7.2.3.	ルート証明書の信頼性の設定	59

Date	Version #	Summary of Changes
2020/12/14	1. 0. 0	初版
2021/01/04	1. 1. 0	・「1.1 証明書のダウンロード」のダウンロード方法の追
		記
		・手順案内様式の変更
2021/01/27	1. 2. 0	・「1.1 証明書のダウンロード」のダウンロード方法の追
		記及び画像を差し替え
		・「1.2 証明書のインポート」のインポート方法の追記及
		び画像を差し替え
		・「1.3 Java 実行環境に電子証明書をインポート」追加
		・「4 証明書の削除」削除方法の追記及び画像を差し替え
		・「5 Java 実行環境に電子証明書を削除」追加
2021/03/23	1. 3. 0	・「1.1 証明書のダウンロード」の 4. に「注意」追加
		・「1.6 Java 実行環境の電子証明書を確認する」追加
		・「3 証明書の失効」 修正
2021/04/28	1. 4. 0	・「6.2 ルート証明書のダウンロードとインストール」を
		追加
2024/10/01	1. 5. 0	・「1. 各種申請の流れ」を追加
		・章立ての見直し
2025/01/xx	1. 6. 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
		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、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

証明書の取得、更新および失効には、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。

[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

## 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。 電子証明書の発行申請 ②電子証明書発行通知書 ③電子証明書 のダウンロード の受領 オンライン請求ネットワ 受領した電子証明書発行 「2.2. 電子証明書のダ ーク関連システム 共通 通知書<sup>※2</sup>に記載されてい ウンロード」参照 認証局 電子証明書の発 る、証明書のダウンロー 行等申請の手引き\*1を参 ドに使用する「リクエス 照してください トID」、「リファレンス ID」を確認してください ④電子証明書 ⑤Java 実行環境 ⑦電子証明書 のインストール の電子証明書 の登録確認 のインストール 「2.5. 登録した電子 「2.3. 電子証明書の 「2.4. Java 実行環境 インポート」参照 に電子証明書をイン 証明書の確認」参照 ポート」参照 ⑧Java 実行環境の ⑨電子証明書 電子証明書を確認 のバックアップ 「2.7. 電子証明書のバ 「2.6. Java 実行環境 の電子証明書を確認 ックアップ」参照 する」参照

※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 参照

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

#### 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】

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、以下の手順で実施してください。



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。

#### 1.3. 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。

電子証明書の失効をする場合、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。

https://www.ssk.or.jp/seikyushiharai/iryokikan/download/index.files/kyotu\_tebiki
.pdf

お手元に電子証明書発行通知書が届きましたら「2.2. 電子証明書のダウンロード」以降 の手順を実施ください。

#### 2.2. 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。

発行者	Online Billing N₩ Common Root CA - G1
発行先	※医療機関コード
端末名称等	※申請時に登録した端末名称等
リクエストID	20210121xxxxxxx
リファレンスID	XXXXXXXXXXXX
電子証明書有効期間	YYYY/MM/DD $\sim$ YYYY/MM/DD
ダウンロードサイト有効期限	YYYY/MM/DD

#### 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)

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)で証明書を 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。

【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

41 A #38A #4 #8		8
社会保険診療報	訓文払基金 果尽文音	β
ユーザロとバス	フードを入力して下さい。	
ユ <i>−</i> ザЮ		
パスワード		
19月二間するお開介サ		
<社会保険診療報酬支払基金 東京支部>	電話番号:03-3987-6181	取扱時間:平日 9時~17時
2ステムに関するお開合せ、 くオンライン請求システムヘルプデスク>	電話番号:0120-60-7210	取扱時間:医療機関·菜局 1
■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。	
電子証明書の発行申請サイト		

・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老人力して下さい。
120-F
ログイン
認証局運用規程(CP/CPS)ダウンロード
自己署名証明書設定手順書 自己署名証明書ダウンロード
お聞合せ   くオンライン請求システムヘルプデスク>   電話番号:0120-60-7210   く特定健診・保健指導システムヘルプデスク>   電話番号:0120-109-957   ■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。
電子証明書の発行申請サイト
(証明書 <u>おウンロードサイト</u> (専用のID、バスワードが必要です。)
▲ 警告: 潜在的なセキュリティリスクあり
Forefasはセキュリティとの頃在的な登場なを使むしたとの。 このサイトに別的すると、欠後者がパスワードやメールプドレス、ウレジットルードの詳細な情報を品み取るうとする地れが あります。
とすればいいであり この問題コンプヤイに思想が何、あなとてきるとてあるとてはかはなん。 転用のモットックのジアダンにした。またコンパルズがWDVのプロドリ国に、US体合な、めなたの所属後期のドットワーク変更 単に高格してくだかい、コプアゲイの整要など問題を取らるようでしょう。 17-00円の
<b>36</b> (88) <b>1</b> 8×26.
国際が2009年につめましましたしたはの可能は対応目ます。後部にないでくだか。 ウェアダイのは空間を見ついませない。 生活性の含ます。またはサーバーが定しい 年間に見なん。 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい 生活性の含ます。 またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい またはサーバーが定しい または または サーバーが定しい または サーバーが定しい または サーバーが定しい または サーバーが定しい または サーバーが定しい または サーバーが または サーバーが または サーバーが また サーバーが また サーバーが また サーバーが また サーバーが コー サーバーが また サーバーが また サーバーが また サーバーが コー サーバーが コー サーバーが コー サーバーが また サーバーが コー ・ サーバー サーバー オー サーバー また サーバーが また サーバー オー サーバー オー オー オー オー オー オー オー
A 27-37-15 Sec. January, JANAGAWA, USUARA 这种教会编辑
Ro GR AMELONICH?

オンライン請求端末より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

「オンライン請求システムのログイン画面」ま たは「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」の下部にある「電 子証明書ダウンロードサイト(専用の ID、パ スワードが必要です。)」をクリックします。

#### 【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
<b>キュリティ証明書を信頼しません</b> 」または
「警告:潜在的なセキュリティリスクあり」
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、「7.2. ルート証明
書のダウンロードとインポート」を参照

	1 0 電フ訂明書飛行協加書に訂書の「川方一つ
証明書の取得画面	
	ト ID」と「リファレンス ID」及び「証明書バ
「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。	<b>スワード</b> 」に任意のパスワード(鍵の暗号化・
証明書バスワードは、任意の4桁の半角数字を入力してください。	復号に利用)半角数字4桁を入力し、「 <b>ダウン</b>
	ロード」をクリックします。
リファレンス ID FPwNiG5g4r	
証明書バスワード	【注意】
証明書バスワード(確認用)	
للإث	人力した証明書パスワードは、「2.3. 電子証明
	書のインポート」の「5.」及び「2.4. Java
証明書バ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。	実行環境に電子証明書をインポート」の
(証明書バ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。)	
	」「り、」で使用します。設定したハスリートを
	忘れないようにしてください。
証明書の取得画面	
「電子証明書発行遺知書」に記載のリクエスト 印とりファレンス 印を入	$A_{\perp}$ を選択後「 $OK_{\perp}$ をクリック」 保存します
カしてください。 証明書パスワードは、任意の4所の半角数字を入力してください。	
リクエストロ 202011260094981 202011260094981.p12 老師( X リフェレンス D WyGGamme'S	
E研題/になつード     E研題/になつード     E研題/になつード     E研題/になつード     E研題/になつード     E研題/になつード     E研題/になつード     E研題/になつード     Emplo(なのののののののののののののののののののののののののののののののののののの	
グイルの通知時 piz rine (ed. ka) ファイルの場所: http://10.81.141.95	
証明書バスワードは編末帯へ証明書をインストールする際に必要とな すのであれないようにしてください	
(証明書)(スワードを忘れてしまった場合は、もう一度証明書発行中4 必要となりますのでご注意ください。)	
OK ++>±6	
	-
< ☆ ホーム ダンロード > Q # ■ ● @ Ø	4. 証明書がダウンロードできていることを確
© 8→4 ■ 7521+27 4318 10 10 10 10 10 10 10 10 10 10	認します。
<ul> <li>ドキュビト</li> <li>ビデオ</li> </ul>	
60 ビクチャー 42 ミュージック 川 ゴミ語	
■ 192.166.34.4 ▲	電子証明書はダウンロードフォルダに保存され
<ul> <li>◆ 他の場所</li> </ul>	ますので、デスクトップ上にファイルを移動し
	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。

#### 2.3. 電子証明書のインポート



	3. 「証明書マネージャ」が表示されます。 「あなたの証明書」タブを選択し、「インポー ト(M) …」をクリックし、「2.2. 電子証明書 のダウンロード」でダウンロードした、証明書 の保管場所(デスクトップ)を指定します。
インボートする証明書ファイル         ● ● のruse       ダウンロード         ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	4. 「インポートする証明書ファイル」が表示 されます。 保管場所からファイル名に選択されているファ イルが、「2.2. 電子証明書のダウンロード」で ダウンロードした証明書ファイルと同一である ことを確認し、「 <b>開く</b> 」をクリックします。
パスワードの入力  この証明書のバックアップ用パスワードを入力してください。 パスワード: ···· OK	5. 「 <b>パスワード入力</b> 」画面が表示されます。 「2.2. 電子証明書のダウンロード」で「 <b>証明</b> <b>書パスワード</b> 」に設定した証明書パスワードを 入力し、「OK」をクリックします。
警告 ※ 証明書と秘密鍵が正常に復元されました。 OK	6. 「 <b>警告</b> 」画面が表示されます。 「 <b>OK</b> 」をクリックします。



## 2.4. Java 実行環境に電子証明書をインポート



..... 1. デスクトップ上の「JRE 証明書」アイコン をダブルクリックします。

<ul> <li>Java コントロールパネル</li> <li>基本 Java セキュリティ 詳細</li> <li>証明書</li> <li>証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。</li> <li>証明書(E)</li> </ul>	2. 「Java コントロールパネル」画面が表示 されます。「セキュリティ」タブを選択し、「証 明書」をクリックします。
了解 取消し 適用(A)	
証明書       ●         証明書タイブ:       クライアント認証         ユーザ       システム         発行先       発行先         1619920851       ReceiptOnline ReceiptOnline Ro         インポート(1)       エクスポート(E)         削除(M)       詳細(D)         閉じる	3. 「証明書」画面が表示されます。「証明書 タイプ」の「▼」をクリックし、「クライアン ト認証」を選択します。「ユーザ」タブを選択 し、「インポート」をクリックします。

	4. 「 <b>開く</b> 」画面が表示されます。
	「デスクトップ」をダブルクリックします
新規フォルダ ファイルを削除 ファイル名を変更	
/home/oruser 💌	
フォルダ ファイル	
./ / ReceiptOnline/ ダウンロード/ テンプレート/ デスクトップ/ ドキュメント/	
選択: /home/oruser	
フィルタ:	
Certificate Files (.csr, .p12)	
② 取消し 🗸 了解	
⊗ ▣ 開く	5. ダウンロードした電子証明書を選択し、
※ ■ 開く     新規フォルダ   ファイルを削除   ファイル名を変更     /home/oruser/Desktop   ▼	5.ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く       新規フォルダ     ファイルを削除     ファイル名を変更       /home/oruser/Desktop ▼       フォルダ     ファイル       ./    /	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴァイル ゴォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ブァイル ブァイル ブォルダ ブァイル ブォック ブック	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く          新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼         フォルダ ファイル         フォルダ ファイル         131000000001.p12         選択: /home/oruser/Desktop         131000000001.p12	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
● 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴョン ジェイル ゴョ1000000001.p12 選択: /home/oruser/Desktop 131000000001.p12 フィルタ:	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く          新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼         フォルダ ファイル         フォルダ ファイル         フォルダ ファイル         131000000001.p12         ・/	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
● 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴョ1000000001.p12 道択: /home/oruser/Desktop 131000000001.p12 フィルタ: Certificate Files (.csr, .p12) ▼	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。

6. バスワード入力メッセージが表示されま す。 「2.2. 電子証明書のダウンロード」で「 <b>証明</b> 書パスワード」に設定したパスワードを入力 し、「 <b>了解</b> 」をクリックします。
7. 引続き、パスワード入力画面が表示されま すが、 <u>パスワードは入力せず</u> に、「 <b>了解</b> 」をク リックします。
【注意】 電子証明書はダウンロードフォルダに保存され ますので、デスクトップ上にファイルを移動し てください。
8. 「 <b>証明書</b> 」画面に戻ります。 「発行元」に「Online Billing NW Common Root CA」と表示されていることを確認し、「 <b>閉</b> じる」をクリックします。

Java コントロールパネル         基本       Java セキュリティ 詳細         証明書         証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。         証明書(E)	9. 「Java コントロールパネル」画面に戻り ます。「了解」をクリックします。
了解取消し適用(A)	

#### 2.5. 登録した電子証明書の確認



	証明書マネージャ	• •	<b>6</b> 4.	「2.3. 電-	子証明書の	<b>Dインポー</b>	-ト」で-	イン
なたの証明書 個人証明書 サーバ あなたが認証を受けるため以下の証 F町車名と登行また。 * Online Billing NW System 9919400001 1310110049 *Staging Online Billing NW System 99479999	な 証明書 認証局証明書 その他 明書が登録されています: セキュリティデバイス シリア Software Security Device 5D:34: Software Security Device 20:64 Software Security Device 50:87:1 サペてパックアップ(K)) インボート(M	y <u>有</u> 効期限 p Dr.8 2024年03月03日 2023年08月12日 3:3E 2024年02月26日 ) <u></u> 削除(D)	ポートクしま	、した証明	書を選択	し、「 <b>表</b> 示	<b>、</b> 」をク!	ノッ
証明書ビューア:"cn=991	19400001,ou=medical,ou=tokyo	OK	<u> </u>	「証明書」	画面が表	示されま	す。「2.3	3. 霍
-般(G) 詳細(D)			子証明	書のイン	ポート」	でインポ	ートした	証明

書を確認します。

この証明書は以下の用途に使用する証明書であると検証されました: SSL クライアント証明書 SSL サーバ証明書 メール署名者の証明書 メール受信者の証明書 発行対象 一般名称 (CN) 組織 (O) 部門 (OU) 9919400001 ReceiptOnline tokyo シリアル番号 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 発行者 Online Billing NW Common Root CA - G1 Online Billing NW System 一般名称 (CN) 組織 (O) 部門 (OU) <証明書に記載されていません> 証明書の有効期間 2020年12月03日 発行日 有効期限 2024年03月03日 
 証明書のフィンガープリント
 42:5B:AD:4E:75:E9:E2:B4:AC:EB:68:39:B4:25:95:3F:60:7F:A3:AF

 MD5 フィンガープリント
 28:DA:50:91:E6:0C:90:07:99:72:2E:3A:2C:DB:F4:3B
 閉じる(<u>C</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。

## 2.6. Java 実行環境の電子証明書を確認する

電子証明書が Java 実行環境に正しくインポートされたことを確認します。

証明書       1. 「証明書ダイブ」の「▼」をグリッグし、「クライアント認証」         ユーザッステム       発行売         発行売       発行売         1310110098       ReceiptOnline Bulling NW Common Root CA-G2         1310110098       ReceiptOnline ReceiptOnline Root CA-G2         (インボート()       エクスボート(E)         期間       ●         ア       システム         (インボート(E)       第時(M)         (エーザ)       ステム         (エーザ)       ステム         (エーザ)       ステム         (エーザ)       ステム         (エーザ)       ステム         (エーザ)       エーザ         (エーザ)       ステム         (エーザ)       エーザ         (エーザ)       ステム         (エーザ)       (ステム         (エーザ)       (ステム         (エーザ)       (エーザ)         (エーザ)       (エーザ)         (エート)       (エクスボート(E)         (国際(M))       詳細(D)
証明書タイプ:       クライアント認証         ユーザ システム       保行売         発行売       発行売         1310110098       ReceiptOnline ReceiptOnline Root CA-G2         1310110098       ReceiptOnline ReceiptOnline Root CA-G2         (インボート()       エクスボート(E)         期間書タイプ:       クライアント認証         ユーザ       システム         第日書タイブ:       クライアント認証         マーザ       システム         第日書       (1)         第13000000       ReceiptOnline ReceiptOnline Root         2.       「ユーザ」タブを選択します。
ユーザ システム         発行先       免行元         1310110099       ReceiptOnline Root CA - G3         1310110098       ReceiptOnline Root CA - G2         インボート()       エクスポート(E)         第時書       2.         エ明書       マ         ユーザ システム       発行元         泉行元       東行元         1310000000       ReceiptOnline ReceiptOnline Root         エーザ システム       東行元         泉行元       東行元         1310100000000000       ReceiptOnline ReceiptOnline Root         アンボート(E)       削除(M)         詳細(E)       デ
単行先       単行元         99979999       Staging Online Billing WCommon Root Carling         1310110099       ReceiptOnline ReceiptOnline Root CA-G2         1310110098       ReceiptOnline ReceiptOnline Root CA-G2         インボート()       エクスボート(E)         期降(M)       詳細(D)         第15       第15         2.       「ユーザ」 タブを選択します。
1310110098       ReceiptOnline ReceiptOnline Root CA-G2         インポート()       エクスポート(E)         期除(M)       詳細(D)         開じる       2.         「ユーザ」ステム       マ         泉行先       発行元         1310000000       ReceiptOnline ReceiptOnline Roming         アンボート(D)       エクスポート(E)         削除(M)       詳細(D)
インボート() エクスボート(E) 削除(M) 詳細D         間じる         2. 「ユーザ」タブを選択します。         証明書タイブ: クライアント認証         ユーザ システム         発行先         発行先         第行先         第行先         第行先         第七一下(0) エクスボート(E) 削除(M) 詳細D
<b>聞じる</b> <b>ご明書</b> タイブ: クライアント認証 ユーザ システム 発行先 発行た 第131000000 ReceiptOnline ReceiptOnline Ro ビリアントじ 単時(M) 詳細(D)
証明書タイプ: クライアント認証       2. 「ユーザ」タブを選択します。         ユーザ システム       文子ム         発行先       発行元         1310000000       ReceiptOnline ReceiptOnline Ro         インポート()       エクスポート(E)         単細D       詳細D
証明書       2. 「ユーザ」タブを選択します。         証明書タイブ: クライアント認証       マ         ユーザ システム       マ         発行先       発行元         131000000       ReceiptOnline ReceiptOnline Ro         インポート()       エクスポート(E)         削除(M)       詳細(D)
<ul> <li>証明書</li> <li>② 2. 「ユーザ」タブを選択します。</li> <li>② 2. 「ユーザ」タブを選択します。</li> </ul>
証明書タイプ: クライアント認証 マーザ システム 発行先 1310000000 ReceiptOnline Ro インポート(J) エクスポート(E) 削除(M) 詳細(D)
ユーザ       システム         発行先       発行元         1310000000       ReceiptOnline ReceiptOnline Ro         インポート(1)       エクスポート(E)         削除(M)       詳細(D)
発行先       発行元         131000000       ReceiptOnline ReceiptOnline Ro         インポート(J)       エクスポート(E)         削除(M)       詳細(D)
1310000000       ReceiptOnline ReceiptOnline Ro         インポート()       エクスポート(E)         詳細(D)
インポート( <u>)</u> エクスポート( <u>E</u> ) 削除( <u>M</u> ) 詳細( <u>D</u> )
閉じる
<sup>ユーザ</sup>   システム   ている「 <b>発行先</b> 」と同じ証明書を選択し、「 <b>詳</b>
AG在 Alianononon ReceiptOpline PerceiptOpline Pe
Martin
インポート(J) エクスポート(E) 削除(M) 詳細(D)
閉じる

.....



証明書       ●         証明書タイプ:       クライアント認証       ▼         ユーザ       システム       ●         発行先       発行元       ●         1310110049       ReceiptOnline Billing NW Common Root CA.       ●         1310110098       ReceiptOnline ReceiptOnline Root CA.       ●         インポート(()       エクスポート(E)       削除(M)       詳細(D)         閉じる        ●	8. 「 <b>証明書</b> 」画面に戻ります。「 <b>閉じる</b> 」を クリックします。
Java コントロールパネル          基本 Java セキュリティ 詳細         証明書         証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。         証明書(E)         証明書(E)	<ol> <li>「Java コントロールパネル」画面に戻ります。</li> <li>「了解」をクリックします。</li> </ol>

#### 2.7. 電子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ポートすることができます。その際には、「2.2. 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、忘れないように記録し 保管してください。

なお、セキュリティやコンプライアンス上の理由からバックアップファイル作成の目的以 外の目的で電子証明書の複製を行うことは禁止されております。





 2.外部記録媒体等をパソコンに接続し、認識 されたドライブを開いて右クリックし、表示さ れたメニューより「貼り付け」を選択します。
 3.バックアップが確実に実施されたことを確 認します。

4. 「2.2. 電子証明書のダウンロード」で設 定したパスワードを保管してください。

【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。これら3つの情報が第三者に渡ると、証明書が不正に使用される恐れがあります。

<u>電子証明書の新規発行手続きの作業はこれで終了です。</u>

## 3. 電子証明書の更新手続き

## 3.1. 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。
2/21/22/22/22/22/22/22/22/22/22/22/22/22	<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】</li> <li>https://cert.obn.managedpki.ne.jp/p/ru</li> <li>※オンライン請求システムにログインすると、 電子証明書更新申請サイトのリンクがありま す。</li> </ol>
	【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」または 「警告:潜在的なセキュリティリスクあり」 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、「7.2. ルート証明 書のダウンロードとインポート」を参照
《人証明書の要求     COサイトはわなたの個人証明書を求めています:     Ca85.managedpki.ne.jp.(p.443)     IIIIE: "Cybertrust Japan Co.,Ltd."     Ref 3: "Cybertrust Japan Co.,Ltd."     HETE: "Cybertrust Japan Co.,Ltd."     HETE: Cybertrust Japan Co.,Ltd."     Strigt: Cybertrust Cybertrust Japan Co.,Ltd."     Strigt: Cybertrust Cybertrust Cybertrust Cybertrust Japan Co.,Ltd."     Strigt: Cybertrust Cyb	<ol> <li>2. 更新対象の証明書を選択し、「OK」をクリ ックします。</li> <li>※発行者が「Online Billing NW Common Root CA」と表記されていることを確認</li> </ol>

Cybertrust Managed PKI サイバートラストマ サイバートラストマンドPI 国産業には、の定時参支数の 変形した期間を取用。 新した期間を取用。ます。	ネージドPKI Ki の延明書の更新画面です。 <sup>通転式</sup> 低LIT.	3.	「 <b>証明書更新申請</b> 」をクリックします。
	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更 よろしければ「Submi	新申請を送信します。 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		

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	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。
シリアレンス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       Organizational Unit     ReceiptOnline       Country     JP	
健の取得     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     パスワードの確認     ・・・・     Submit     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、「3.1. 電子証明書更新申請サイトからの電子証明書の更新」の「14.」及び「3.2. Java 実行環境に電子証明書をインポート」の「6.」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。 Download	<b>い。</b> 7. 「「Download」をクリックします。





パスワードの入力 😣	14. 「パスワード <b>入力</b> 」画面が表示されま
この証明書のバックアップ用パスワードを入力してください。	す。
パスワード:	「3.1. 電子証明書更新申請サイトからの電子 証明書の更新」で「パスワード」に設定したパ スワードを入力し、「OK」をクリックします。
	15 「 <b>礬告</b> 」画面が表示されます
當告	$\begin{bmatrix} \mathbf{OK} & \mathbf{F} & \mathbf{F} \end{bmatrix}$ $\begin{bmatrix} \mathbf{OK} & \mathbf{F} & \mathbf{F} \end{bmatrix}$
証明書と秘密鍵が正常に復元されました。	
ок	
証明書マネージャ 🚔 🕾 😒	16.証明書がインポートされます。
あなたの証明書 個人証明書 サーバ証明書 認証局証明書 その他	インポートした証明書を選択し、「 <b>表示</b> 」をク
証明書名と発行者名 セキュリティデバイス シリアル番号 有効期限  G VReceiptOnline	リックします。
99479999 Software Security Device 20:BA 2024年03月21日 200/06.01/07/20000 Software Security Device 50:97:12:25:75:18:14 2024年03月21日	
39413333 301 wale security bence 30.01, 13-5LCL, 15A, 2024+02/3201	
表示() パックアップ(B)) すべてパックアップ(K)) インボート(M)) 削除(D)	
ОК	

─ 一般名称(CN)が「Online Billing NW Common
Root CAL と表示されることを確認します
Root CA」と表示され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。

### 3.1.1. 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。

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。
2020日第三日 第三日 1950 1970年7日 2040 10 00 00 00 00 00 00 00 00 00 00 00 00	<ol> <li>1. 更新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>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】</li> <li><a href="https://cert.obn.managedpki.ne.jp/p/ru">https://cert.obn.managedpki.ne.jp/p/ru</a></li> </ol>
Суbertrust Managed PKI         Руба поток           Zинаолем	<ol> <li>2.「証明書の更新申請」画面の「更新後証明 書の取得」をクリックします。</li> </ol>
	<ul> <li>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。</li> <li>※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、「3.1.電子証明書更新申請サイトからの電子証明書の更新」からやり直してください。</li> </ul>

.....

202012220100971.p12を開く ×	4. ポップアップ画面から「ファイルを保存す
次のファイルを開こうとしています:	る」を選択後、「OK」をクリックして、証明書
ジョン 202012220100971.p12 ファイルの種類: p12 File (4.3 KB) ファイルの種類: p12 File (4.3 KB)	ファイルを保存します。
ファイルの場所: https:// <b>このファイルをどのように処理するか選んでください</b> ① プログラムで開く( <u>O</u> ): 参照( <u>B</u> ) ④ ファイルを保存する( <u>S</u> ) ① 今後この種類のファイルは同様に処理する( <u>A</u> ) OK キャンセル	【注意】 電子証明書はダウンロードフォルダに保存され ますので、デスクトップ上にファイルを移動し てください。

5. 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、「2.3. 電子証明書の インポート」及び「2.4. Java 実行環境に電子証明書をインポート」を参照し、保存した証明書ファ イルをブラウザにインストールします。

6. 「5. 電子証明書の削除」及び「6. Java 実行環境の電子証明書を削除」を参照し古い証明書を 削除します。

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。

## 3.2. Java 実行環境に電子証明書をインポート



..... 1. デスクトップ上の「JRE 証明書」アイコン をダブルクリックします。

<ul> <li>Java コントロールパネル</li> <li>基本 Java セキュリティ 詳細</li> <li>証明書</li> <li>証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。</li> <li>証明書(E)…</li> <li>証明書(E)…</li> </ul>	2. 「Java コントロールパネル」画面が表示 されます。「セキュリティ」タブを選択し、「証 明書」をクリックします。
証明書       マ         証明書       クライアント認証         ユーザ       システム         発行先       発行元         1619920851       ReceiptOnline ReceiptOnline Ro         インポート(1)       エウスポート(E)         削除(M)       詳細(D)         閉じる	3. 「証明書」画面が表示されます。「証明書 タイプ」の「▼」をクリックし、「クライアン ト認証」を選択します。「ユーザ」タブを選択 し、「インポート」をクリックします。

	4. 「 <b>開く</b> 」画面が表示されます。
	「デスクトップ」をダブルクリックします
新規フォルダ ファイルを削除 ファイル名を変更	
/home/oruser 💌	
フォルダ ファイル	
./ / ReceiptOnline/ ダウンロード/ テンプレート/ デスクトップ/ ドキュメント/	
選択: /home/oruser	
フィルタ:	
Certificate Files (.csr, .p12)	
② 取消し 🗸 了解	
⊗ ▣ 開く	5. ダウンロードした電子証明書を選択し、
※ ■ 開く     新規フォルダ   ファイルを削除   ファイル名を変更     /home/oruser/Desktop   ▼	5.ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く       新規フォルダ     ファイルを削除     ファイル名を変更       /home/oruser/Desktop ▼       フォルダ     ファイル       ./     ./       ./     ./	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴァイル ゴォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ファイル ブォルダ ブァイル ブァイル ブォルダ ブァイル ブォック ブック	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く          新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼         フォルダ ファイル         フォルダ ファイル         131000000001.p12         選択: /home/oruser/Desktop         131000000001.p12	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
● 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴョン ジェイル ゴョ1000000001.p12 選択: /home/oruser/Desktop 131000000001.p12 フィルタ:	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
※ ■ 開く          新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼         フォルダ ファイル         フォルダ ファイル         フォルダ ファイル         131000000001.p12         ・/	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。
● 開く 新規フォルダ ファイルを削除 ファイル名を変更 /home/oruser/Desktop ▼ フォルダ ファイル フォルダ ファイル ゴョ1000000001.p12 道択: /home/oruser/Desktop 131000000001.p12 フィルタ: Certificate Files (.csr, .p12) ▼	5. ダウンロードした電子証明書を選択し、 「 <b>了解</b> 」をクリックします。

<ul> <li>認証が必須です</li> <li>ジョva・</li> <li>ファイルにアクセスするにはパスワードを 入力してください:</li> <li>バスワード(P): *****</li> <li>丁解 取消し</li> </ul>	6. パスワード入力メッセージが表示されま す。 「1.1. 証明書のダウンロード」で「 <b>証明書パ</b> スワード」に設定したパスワードを入力し、 「 <b>了解</b> 」をクリックします。
<ul> <li>※入力不要</li> <li>認証が必須です</li> <li>認証が必須です</li> <li>認証が必須です</li> <li>パスワードを入力してくたさい:</li> </ul>	7. 引続き、パスワード入力画面が表示されま すが、 <u>パスワードは入力せず</u> に、「 <b>了解</b> 」をク リックします。 【注意】 電子証明書はダウンロードフォルダに保存され ますので、デスクトップ上にファイルを移動し てください。
証明書          証明書タイブ:       クライアント認証         ユーザ       システム         算行生       発行士         1310000000       Online Billing NW Comm         インポート(1)       エクスポート(E)         削除(M)       詳細(D)         開じる	8. 「 <b>証明書</b> 」画面に戻ります。 「発行元」に「Online Billing NW Common Root CA」と表示されていることを確認し、「 <b>閉</b> じる」をクリックします。

Java コントロールパネル         基本       Java セキュリティ 詳細         証明書         証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。         証明書(E)	9. 「Java コントロールパネル」画面に戻り ます。「了解」をクリックします。
了解取消し適用(A)	

#### 3.3. 登録した電子証明書の確認



	証明書マネージャ 🛛 🔘 🕲 🔘	4. 「1.2. 証明書のインホート」でインホー
*** 01798 # 00 1 1709 # 44		
なたの証明書 個人証明書 サ	ーハ証明書 認証局証明書 ての他の の証明書が登録されています。	トした証明書を選択し、「 <b>表示</b> 」をクリックし
江田津々と称に多々		ナナ
Online Billing NW System		より。
9919400001	Software Security Device 5D:34:7D:8 2024年03月03日	
1310110049 Staging Online Billing NW Sysl 99479999	Software Security Device 20:64 2023年08月12日 tem Software Security Device 50:87:13:3E 2024年02月26日	
表示(V) ノバックアップ(B).	「すべてパックアップ(X)」「ンボート(M)」 前除(D) OK	
証明書ビューア:"cn= &(C) 詳細(D) この証明書は以下の用途(	9919400001,ou=medical,ou=tokyo,o=receiptonline,c=jp" の こ使用する証明書であると検証されました:	5. 「 <b>証明書</b> 」画面が表示されます。「1.2. 証明書のインポート」でインポートした証明
SSL クライアント証明書		青を確認します。
SSL サーバ証明書		
SSL サーバ証明書 メール署名者の証明書		
SSL サーバ証明書 メール署名者の証明書 メール受信者の証明書		
SSLサーバ証明書 メール署名者の証明書 メール受信者の証明書 <b>発行対象</b> 一般名称 (CN) 組織(O) 部門(OU) ソリアル番号 <b>発行者</b> 一般名称 (CN)	9919400001 ReceiptOnline tokyo 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 Online Billing NW Common Root CA - G1	
SSLサーバ証明書 メール署名者の証明書 メール受信者の証明書 <b> 発行対象</b> 一般名称 (CN) 組織 (O) 影門(OU) ソリアル番号 <b> 絶行者</b> 一般名称 (CN) 組職(O) 影門(OU) ジリアル番号	9919400001 ReceiptOnline tokyo 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 Online Billing NW Common Root CA - G1 Online Billing NW System cistem #: CIB 행숙 37 (1):#14 (A)	
SSLサーバ証明書 メール要名者の証明書 メール受信者の証明書 発行対象 一般名称(CN) 組織(0) 部門(OU) ンリアル番号 発行者 一般名称(CN) 組織(0) 部門(OU) <b>E明書の有効期間</b> を行日 自効期間	9919400001 ReceiptOnline tokyo 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 Online Billing NW Common Root CA - G1 Online Billing NW System <証明書に記載されていません> 2020年12月03日 2024年12月03日	
SSLサーバ証明書 メール署名者の証明書 メール受信者の証明書 発行対象 一般名称(CN) 組織(0) 部門(OU) シリアル番号 発行者 一般名称(CN) 組織(0) 部門(OU) 距明書の有効期間 を行つ 「初期限 証明書の有効期間 を行う を行うま に入り、 にの の にの にの の の にの の にの の にの の にの の にの の たの で の にの の にの の にの の にの の たの で の の にの の にの の にの の にの の にの の たの で の たの で の 有 の たの の にの で の たの の で の たの の で の にの の たの で の たの の で の にの の で の たの たの で の で の たの にの の で の たの で の で の たの たの で の で の にの の で の にの の たの にの の で の で の たの たの で の で の で の で の で の で の で の の で の で の つ で つ つ い つ い つ い つ い つ い つ で つ い つ い つ い つ い つ い つ い つ い つ い っ い つ い つ い し い へ い つ い つ い し い っ い い っ い つ い つ い い っ い つ い つ い い っ い っ い こ っ い っ い っ つ っ い っ い っ い つ い つ っ つ っ っ こ っ っ つ っ つ い つ っ つ に つ い つ い つ っ つ い っ っ っ い つ っ つ い つ つ つ い つ っ つ い つ っ つ い つ い つ い つ っ つ い つ い つ っ つ つ つ つ つ つ つ つ つ い つ つ つ つ つ つ つ つ つ つ つ つ し つ つ つ つ つ つ つ つ つ つ つ つ つ	9919400001 ReceiptOnline tokyo 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 Online Billing NW Common Root CA - G1 Online Billing NW Common Root CA - G1 Online Billing NW System <証明書に記載されていません> 2020年12月03日 2024年03月03日 42:5B:AD:4E:75:E9:E2:B4:AC:EB:68:39:B4:25:95:3F:60:7F:A3:AF 28:DA:50:91:E6:0C:90:07:99:72:2E:3A:2C:DB:F4:3B	
SSLサーバ証明書 メール受信者の証明書 メール受信者の証明書 キロサ象 の範囲でのにの 部門(OU) シリアル番号 発行者 一般名称(CN) 組織(O) 部門(OU) <b>証明書の有効期間</b> 発行日 降行却限 <b>証明書のフィンガープリント</b> MD5 フィンガープリント	9919400001 ReceiptOnline tokyo 5D:34:7D:88:42:0D:0C:40:5C:1B:E1:04:0E:A5:AE:DF:0C:00:78:07 Online Billing NW Common Root CA-G1 Online Billing NW Common Root CA-G1 Online Billing NW System < 証明書に記載されていません> 2020年12月03日 2024年03月03日 2024年03月03日 42:5B:AD:4E:75:E9:E2:B4:AC:EB:68:39:B4:25:95:3F:60:7F:A3:AF 28:DA:50:91:E6:0C:90:07:99:72:2E:3A:2C:DB:F4:3B	

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。

## 3.4. Java 実行環境の電子証明書を確認する

電子証明書が Java 実行環境に正しくインポートされたことを確認します。

証明書 😣	1. 「 <b>証明書タイプ</b> 」の「▼」をクリックし、
証明書タイプ: クライアント認証	「 <b>クライアント認証</b> 」を選択します。
ユーザ システム	
<b>発行先</b> 発行元	
99479999 Staging Online Billing NW Common Root C 1310110049 ReceiptOnline ReceiptOnline Root CA - G3	
1310110098 ReceiptOnline ReceiptOnline Root CA - G2	
インポート() エクスポート(E) 削除( <u>M</u> ) 詳細(D)	
閉じる	
証明書 😣	2. 「ユーザ」タブを選択します。
証明書タイプ: クライアント認証 ▼	
ユーザシステム	
発行先	
1310000000 ReceiptOnline ReceiptOnline Ro	
インポート(I) エクスポート( <u>E</u> ) 削除( <u>M</u> ) 詳細(D)	
88.14.7	
「おしる」	
<b>証明書</b>	3. 「発行先」が「電子証明書更新のご案内
	(雷子証明書取得に関する情報) に記載され
111111111111111111111111111111111111	
ユーザ システム	
叠行车 叠行元 1310000000 ReceiptOnline ReceiptOnline Ro	<b>細</b> 」をクリックします。「 <b>詳細−証明書</b> 」画面
	が表示されます。
【インボート(I)】 【エクスポート(E)】 削除(M) 詳細(D)	
閉じる	

.....

.....



証明書 証明書タイプ: クライアント認証 ユーザ システム 発行先 発行元 99479999 Staging Online Billing NW Common Root C 1310110049 Receipt Online Receipt Online Root CA - G3 1310110098 Receipt Online Receipt Online Root CA - G3 () インポート() エクスポート(E) 削除(M) 詳細(D) 閉じる	8. 「証明音」回面に戻りまり。「闭しる」を クリックします。
	-
Java コントロールパネル       ● ●         基本 Java セキュリティ 詳細         証明書         証明書は、自分自身、証明書、証明書発行局、および発行者を積極的に識別する場合に使用します。         証明書(E)         証明書(E)	9. 「Java ユンドロールハイル」。画面に戻りま す。「了解」をクリックします。

保健指導システムに接続してください。

.....

#### 3.5. 電子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ポートします。その際には、「3.1. 電子証明書更新申 請サイトからの電子証明書の更新」で設定したパスワードも必要となるため、忘れないよ うに記録し保管してください。



つの情報が第三者に渡ると、証明書が不正に使用される恐れがあります。

## 3.6. 電子証明書の削除

「5. 電子証明書の削除」及び「6. Java 実行環境の電子証明書を削除」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。



## 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お	から、手続きを実施して下さい。
Ktps://cet.downaragedpix.rego/pin/ Cooper	<ol> <li>1. 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>失効申請画面へアクセスします。</li> <li>【証明書失効申請サイト】</li> <li>https://cert.obn.managedpki.ne.jp/p/rx</li> <li>【こんなときは!】</li> </ol>
登告: 潜在的なセキュリティリスクあり	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」または 「警告:潜在的なセキュリティリスクあり」 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、 を参照
	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  メ効応調定のご時級のため、メールアドレスを入力してびため、	<ol> <li>3. 失効申請者の申請者の「メールアドレス」 と「メールアドレス(確認用)」を入力し、「申 請」をクリックします。「証明書失効申請情報 の確認画面」へ遷移します。</li> </ol>
証明書失効申請情報入力内容の確認画面                し「下の内容で理明最大効申請を送信します。 よろしすけば「甲菌」ボタンをジックしてだされ。 P内容ご創りが吸れば、「戻らばチタンをジックしてだされ。                 リクエスト ID             ロクロンス ID             のdFNXXEFRP             メールフドレス             11@22.33                 中語             戻る	<ul> <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」及び「6. Java 実行環境の 電子証明書を削除」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。

## 5. 電子証明書の削除



あなたの証明書を削除 本当にこの証明書を削除してもよろしいですか? 99479999 あなたの証明書を削除すると、今後この証明書で個人認証がで きなくなります。	4. 確認画面が表示されます。 「OK」をクリックし、証明書を削除します。
Euglasta-ジャ     OK       超明書マネージャ     ● ● ●       あなたの証明書 個人証明書 サーバ証明書 認証局証明書 その他     あなたが認証を受けるため以下の証明書が登録されています:       あなたが認証を受けるため以下の証明書が登録されています:     シガルを書う       たちたちまま     ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	<ol> <li>「<b>証明書マネージャ</b>」が表示されます。</li> <li>削除を行った証明書が一覧から消えていること</li> <li>を確認します。</li> <li>確認後、「OK」をクリックします。</li> </ol>
表示( <u>)</u> パックアップ( <u>B</u> )) すべてパックアップ( <u>S</u> )) インボート( <u>M</u> )) 削除( <u>D</u> ) OK	

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. Java 実行環境の電子証明書を削除



1. デスクトップ上の「**JRE 証明書**」アイコン をダブルクリックします。

⊗ Java コントロールパネル	2. 「Java コントロールパネル」画面が表示
基本 Java セキュリティ 詳細	されます。「 <b>セキュリティ</b> 」タブを選択し、「 <b>証</b>
□ 証明書	明書」をクリックします。
証明書は、自分自身、証明書、証明書発行局、お よび発行者を積極的に識別する場合に使用します。 証明書(E)	
証明書 😣	3. 「 <b>証明書</b> 」画面が表示されます。
証明書タイプ: クライアント認証 ▼	「 <b>証明書タイプ</b> 」の「▼」をクリックし、「 <b>ク</b>
ユーザシステム	<b>ライアント認証</b> 」を選択します。
	「 <b>ユーザ</b> 」タブを選択し、複数行表示される証
TS1000000         Receiptontine Receiptontine Rolling           19241 3223         Online Billing IVW Comm.	明書を選択し、「 <b>詳細</b> 」をクリックします。
	(古い有効期限の日付を確認するため、手順
, T	「3」、及び「4」を繰り返します。)
インポート(j) エクスポート(E) 削除(M) 詳細(D) 閉じる	

	<ol> <li>フィールド列の「<b>有効性</b>」の行を選択します。</li> <li>表示された有効期限を確認し、「<b>閉じる</b>」をクリックします</li> <li>「To:」で始まる日付が有効期限です。</li> </ol>
証明書       ◆         証明書タイブ:       クライアント認証       ▼         ユーザ       システム       ◆         発行先       発行元       ●         131000000       Paceipt Online Receipt Online Ro       ●         99479999       Online Billing NW Comm       ●         インポート(1)       エクスポート(E)       削除(M)       詳細(D)         閉じる	5. 有効期限の古い証明書が選択されているこ とを確認し、「 <b>削除</b> 」をクリックします。
確認 - 証明書を削除しますか? 選択した証明書を削除してもよろしいですか? 選択した証明書は完全に削除されます。 了解 取消し	6. 証明書削除確認メッセージが表示されま す。 「 <b>了解</b> 」をクリックします。
<ul> <li>認証が必須です</li> <li>ジョンコ</li> <li>個人用キーストアにアクセスするためのパ スワードを入力してください:</li> <li>パスワード(P):</li> <li>※入力不要</li> <li>了解 取消し</li> </ul>	7. パスワード入力メッセージが表示されま す。 <u>パスワードを入力せず</u> 、「 <b>了解</b> 」をクリックし ます。

証明書 😣	8. 「 <b>証明書</b> 」画面に戻ります。
証明書タイプ: クライアント認証 ▼	証明書が削除されたことを確認し、「 <b>閉じる</b> 」
ユーザシステム	をクリックします。
発行先 発行元	
131000000 ReceiptOnline Ro	
インポート( <u>)</u> エクスポート( <u>E</u> ) 削除( <u>M</u> ) 詳細( <u>D</u> )	
閉じる	
	9. 「Java コントロールパネル」画面に戻り
● Java コントロールパネル	ます。「 <b>了解</b> 」をクリックします。
基本 Java セキュリティ 詳細	
証明書は、自分自身、証明書、証明書発行局、お よび発行者を積極的に識別する場合に使用します。 証明書(E)	
「解 取消し 適用(A)	

## 7. サポート情報

## 7.1. ご利用にあたっての注意事項

7.1.1. 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:		<	1. 発行者が「Online Billing NW Common Root CA」となっていることを確認し、「OK」を
ģ	<b>TEST Client 003</b> KRS GP CA 2014 TEST 2014/6/20		クリックしてください。
ģ	<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			

7.1.2. セッション無効時の対応トラブルシューティング



#### 7.2. ルート証明書のダウンロードとインポート

7.2.1. ルート証明書のダウンロード



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。

注意	必ずすべてのブラウザを閉じて	こから、手続きを実施して	下さい。
コンストロ         第二級 第二級 第二級 727-20 7- 2727-20 7- 2728-20 2012/01 2012/01 1000 1000/01 2012/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 1000/01 2012/01 10000/01 10000/0100000000	2-27/2#2224.4400011 httos:           United Control (1990)           Internet (1990) <th><ul> <li>1. メニューバーから に選択します。</li> <li>2. 「Firefox の設定」 「詳細」をクリックし 「証明書を表示 (S)</li> </ul></th> <th>「<b>編集</b>」→「設定」の順 が表示されます。 、「<b>暗号化</b>」タブから 、」をクリックします。</th>	<ul> <li>1. メニューバーから に選択します。</li> <li>2. 「Firefox の設定」 「詳細」をクリックし 「証明書を表示 (S)</li> </ul>	「 <b>編集</b> 」→「設定」の順 が表示されます。 、「 <b>暗号化</b> 」タブから 、」をクリックします。
ヘルプ(円)	閉じる		

## 7.2.2. ルート証明書のインポート

証明書マネージャー ×	3. 「証明書マネージャ」が表示されます。
あなたの証明書       認証の決定       個人証明書       サーバー証明書       認証局証明書         認証局を識別するため以下の証明書が登録されていまま             証明書名と発行者名       セキュリティデバイス       に           素示(い)       信頼性を設定(t)       インボート(い)       エクスボート(い)       削除または信頼しない(t)         OK	「認証局の証明書」タブを選択し、「インポー ト(M)…」をクリックし、「7.2.1. ルート証 明書のダウンロード」でダウンロードした、証 明書の保管場所(デスクトップ)を指定しま す。
インボートする証明書ファイル         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	4. 「インポートする証明書ファイル」が表示 されます。 保管場所からファイル名に選択されているファ イルが、「7.2.1. ルート証明書のダウンロー ド」でダウンロードした証明書ファイルと同一 であることを確認し、「 <b>開く</b> 」をクリックしま す。
明書のインポート X	┃ 5. 「 <b>証明書のインポート</b> 」画面が表示されま
行しい認証局 (CA) を信頼するよう求められています。本当にこの認証局を信頼しますか?	t.
Security Communication RootCA2 * が行う認証のうち、信頼するものを選択してください。	すべてのチェックボックスにチェックを入れ、
○この認証局によるメールユーザーの識別を信頼する	「OK」ボタンをクリックします。
窓証局を信頼する場合はその目的に関わらず、認証局の証明書が間違いないこと、認証ポリシーや認証実施 見定に問題がないことを確認してください。	
証明書を表示 認証局の証明書を審査してください OK キャンセル	

証明書マネージャー	× (	6. ルート証明書がインポートされていること
あなたの証明書         認証の決定         個人証明書         サーバー証明書         認証局証明書           認証局を識別するため以下の証明書が登録されています <th></th> <th>を確認します。</th>		を確認します。
SECON Hust Systems CO., ED.     Contract Issue Surg SV CA C2     Second Structure Security Device		
Security Communication RootCA2 Builtin Object Token		
✓ SECOM Trust.net		
Security Communication Root CA Builtin Object Token	~	
表示( <u>V</u> ) 信頼性を設定( <u>E</u> ) インボート( <u>M</u> ) エクスボート( <u>X</u> ) 削除または信頼しない( <u>D</u>		
ок	<u>.</u>	
注意 上記の操作が終了したら、	どずす~	べてのブラウザを閉じて下さい。

#### 7.2.3. ルート証明書の信頼性の設定

「認証局証明書に対する信頼性」の設定を行う場合の操作について説明します。

