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 1.9.0

令和８年11月６日

目次

目次 2
はじめに 6
事前準備 6
1. 各種申請の流れ 7
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
1.3. 電子証明書の失効手続き 9
2. 電子証明書の新規発行手続き 10
2.1. 電子証明書の新規発行申請 10
2.2. 電子証明書のダウンロード 10
2.3. 電子証明書のインポート 13
2.4. Java 実行環境に電子証明書をインポート 16
2.5. 登録した電子証明書の確認 20
2.6. Java 実行環境の電子証明書を確認する 22
2.7. 電子証明書のバックアップ 25
3. 電子証明書の更新手続き 27
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 27
3.1.1. こんなときは！ 34
3.2. Java 実行環境に電子証明書をインポート 36
3.3. 登録した電子証明書の確認 40
3.4. Java 実行環境の電子証明書を確認する 42
3.5. 電子証明書のバックアップ 45
3.6. 電子証明書の削除 46
4. 電子証明書の失効手続き 48
4.1. 電子証明書の失効申請 48
4.2. 電子証明書の削除 49
5. 電子証明書の削除 50
6. Java 実行環境の電子証明書を削除 52
7. サポート情報 55
7.1. ご利用にあたっての注意事項 55
7.1.1. 認証用の証明書の選択画面が表示された場合 55
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 55
7.1.3. 操作継続失敗画面表示時のトラブルシューティング 56
7.2. ルート証明書のダウンロードとインポート 57

7.2.1. ルート証明書のダウンロード..... 57
7.2.2. ルート証明書のインポート..... 58
7.2.3. ルート証明書の信頼性の設定..... 61

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
2025/02/19	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

Date	Version #	Summary of Changes
2026/03/02	1.7.0	・「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」内「鍵の取得」画面「パスワード」の入力桁数の記載を訂正
2026/10/01	1.8.0	・「支払基金」の名称を「DX 審査支払機構」に変更 ・「1.2.　電子証明書の更新手続き」及び「1.3.　電子証明書の失効手続き」に記載されている、メール通知の送信元アドレスを変更 ・「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」の URL を変更
2026/11/06	1.9.0	・「7.1.3. 操作継続失敗画面表示時のトラブルシューティング」の追加

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

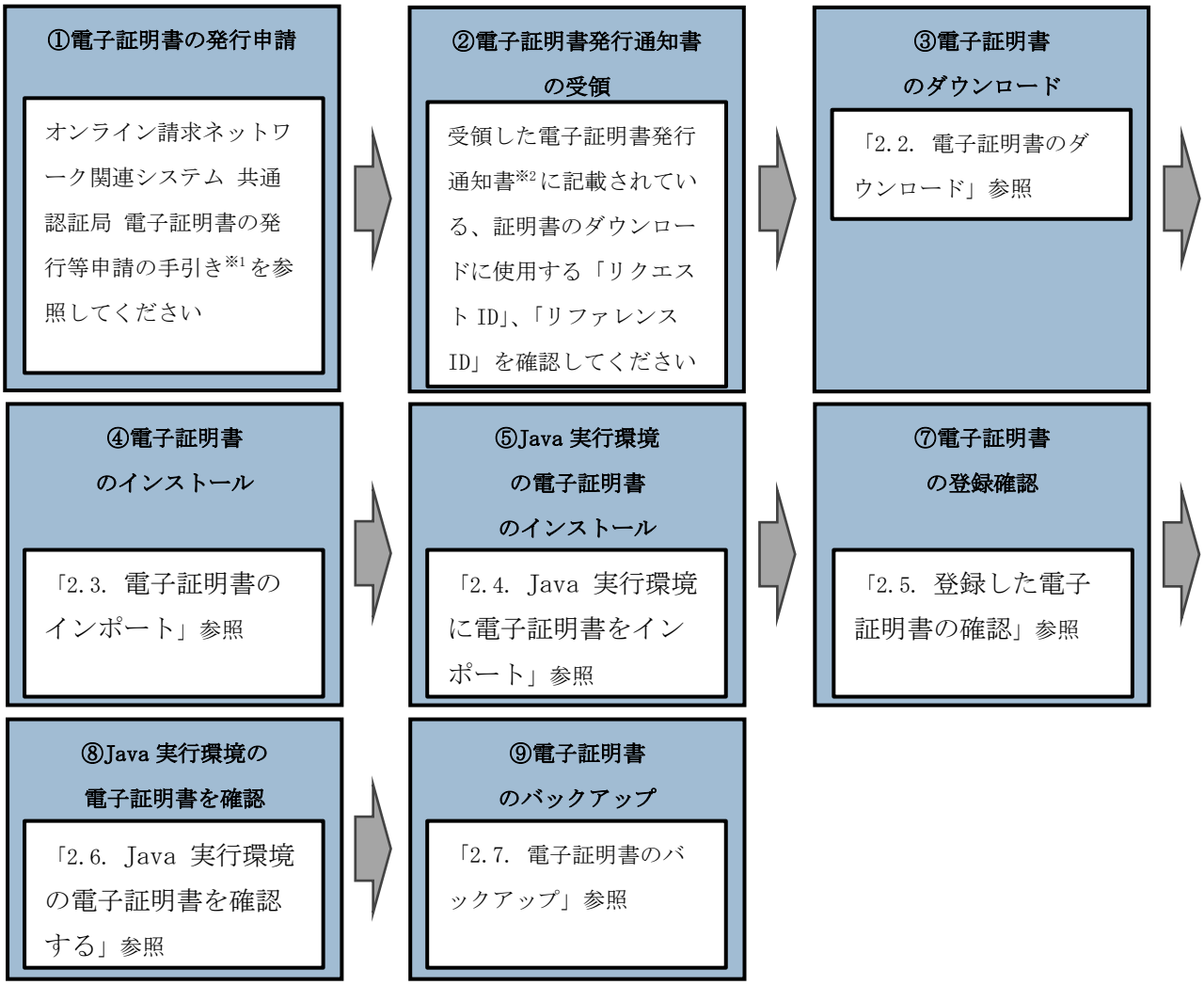
1.　各種申請の流れ

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。



※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.hpdx.or.jp/seikyushiharai/iryokikan/download/index.files/kyotu_tebiki.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

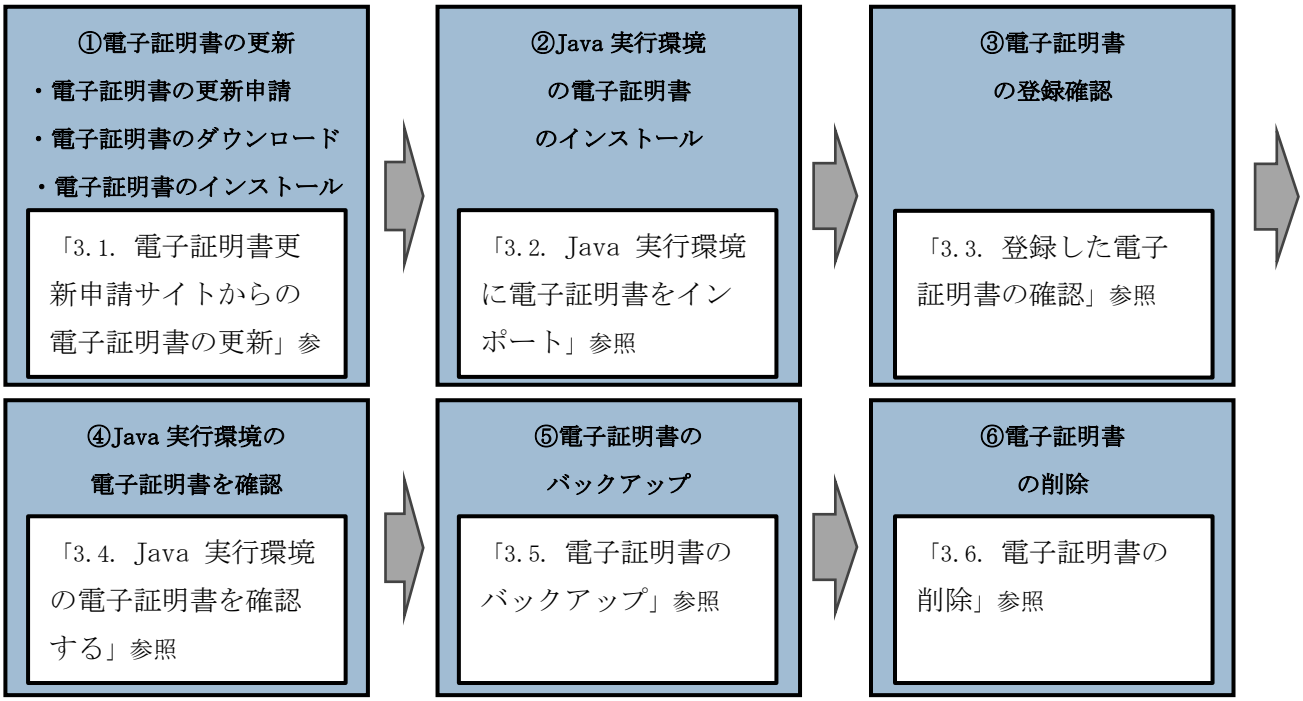
ブラウザから複数のタブやウインドウを開いた状態で、各種手続きを実施した場合、証明書が正しい申請内容で手続き出来ない場合があります。
必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

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 ※DX 審査支払機構のみ	有効期限の 90 日前～期限日
メール通知 ※電子証明書の発行申請時に入力したメールアドレス宛に「no-reply@hpdx.or.jp」からメール通知	有効期限の 75 日前、60 日前、45 日前、30 日前、15 日前、7 日前～期限日

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。



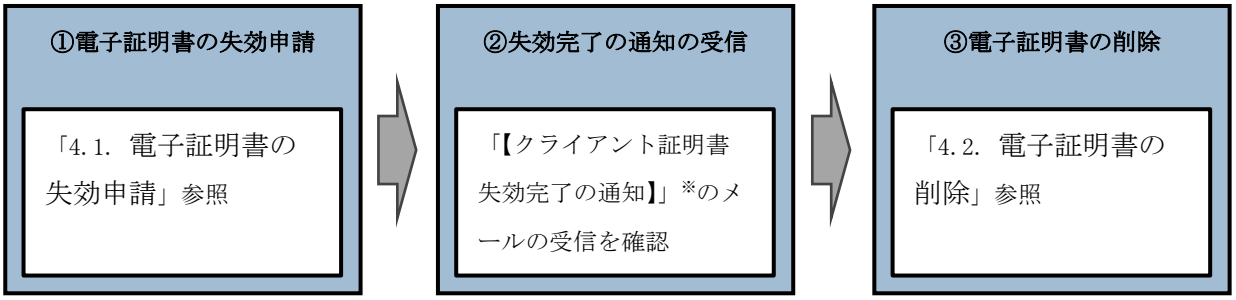
⑤電子証明書のバックアップまでの操作を更新前の電子証明書の有効期限（３年３か月）までに実施してください。
※更新前の電子証明書の有効期限（３年３か月）を過ぎると、更新済みの電子証明書がダウンロードできなくなります。

1.3.　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。



※　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-reply@hpdx.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.hpdx.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。

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）

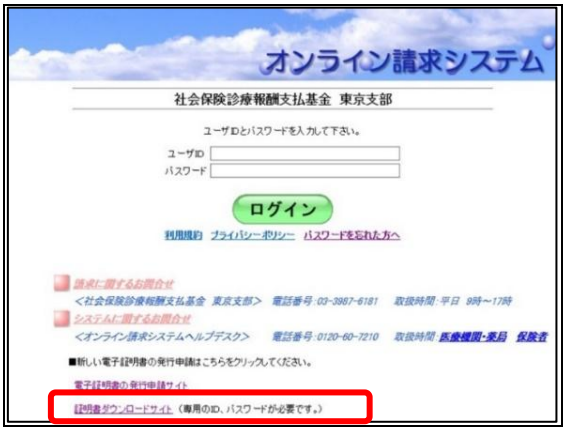
発行者	Online Billing NW Common Root CA - G1
発行先	※医療機関コード
端末名称等	※申請時に登録した端末名称等
リクエストID	20210121xxxxxxx
リファレンスID	XXXXXXXXXXX
電子証明書有効期間	YYYY/MM/DD ～ YYYY/MM/DD
ダウンロードサイト有効期限	YYYY/MM/DD

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）で証明書を取得します。

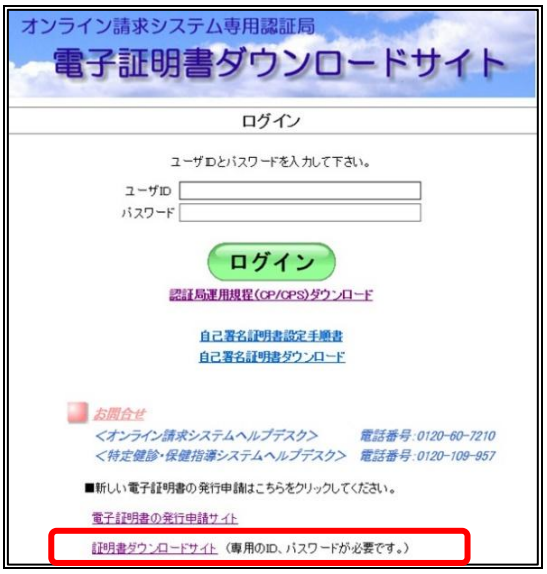
注意 **必ずすべてのブラウザを閉じてから、手続きを実施して下さい。**

【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



・電子証明書ダウンロードサイト





1．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。

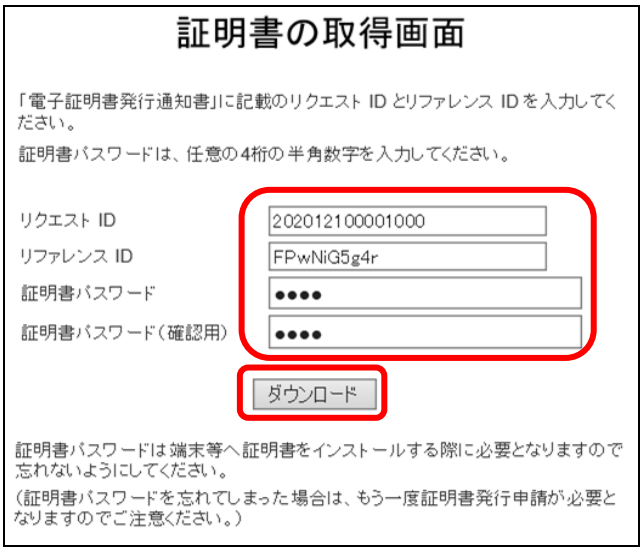
【ダウンロードサイト】

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！】

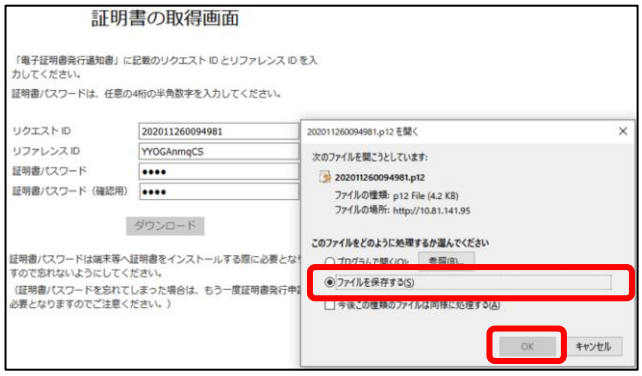
証明書のダウンロード画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**警告：潜在的なセキュリティリスクあり**」と表示される場合は、ルート証明書のインストールが必要であるため、「7.2. ルート証明書のダウンロードとインポート」を参照



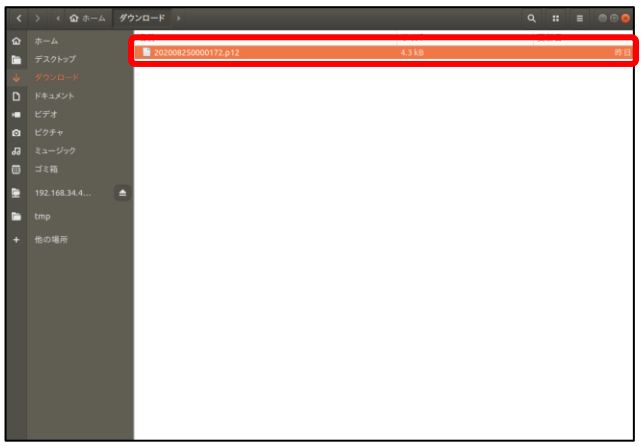
２．電子証明書発行通知書に記載の「**リクエスト ID**」と「リファレンス **ID**」及び「**証明書パスワード**」に任意のパスワード（鍵の暗号化・復号に利用）半角数字４桁を入力し、「**ダウンロード**」をクリックします。

【注意】

入力した証明書パスワードは、「2.3. 電子証明書のインポート」の「５．」及び「2.4. 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い。**



３．ポップアップ画面から「**ファイルを保存する**」を選択後「**OK**」をクリックし保存します。



４．証明書がダウンロードできていることを確認します。

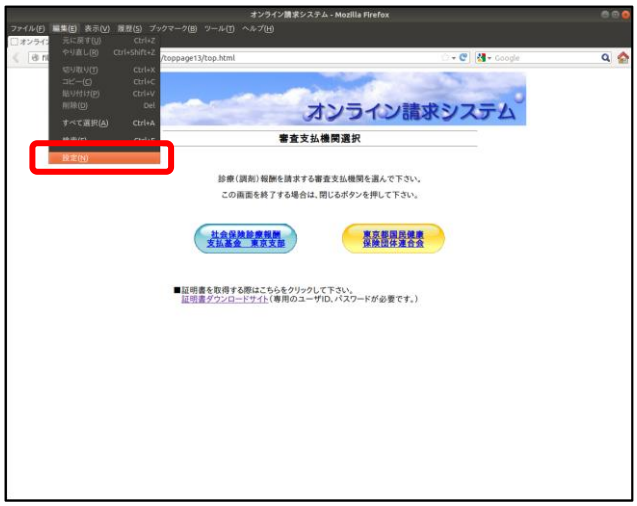
【注意】

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。

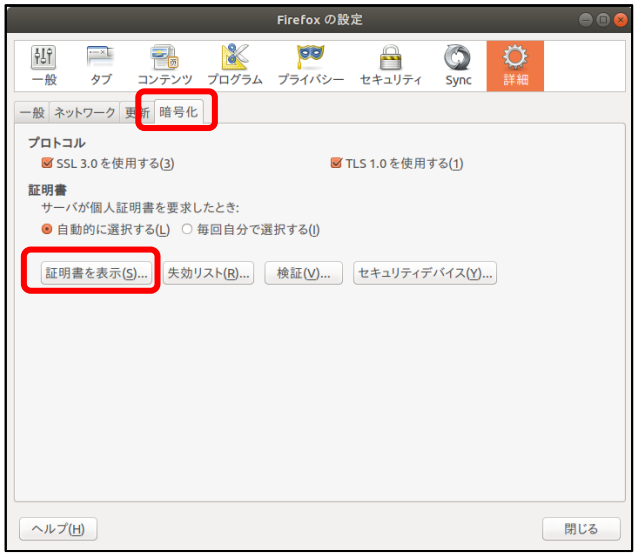
注意 **上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。**

2.3.　電子証明書のインポート

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。



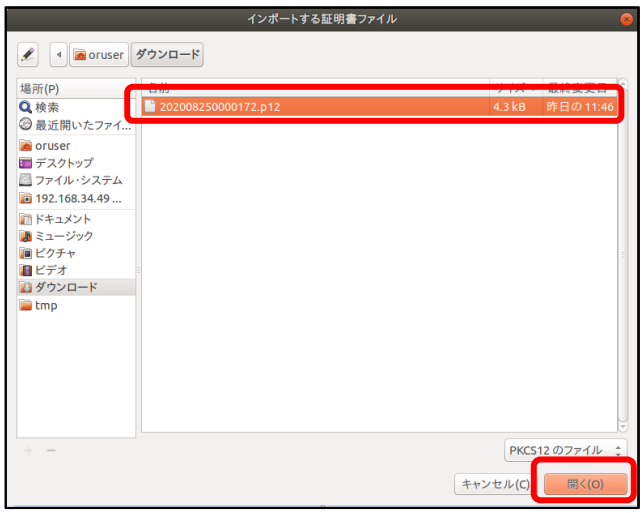
１．Firefox ブラウザを起動し、クライアント証明書をインポートする。ブラウザの「**編集**」をクリックし、メニュー一覧から「**設定**」をクリックします。



２．「**Firefox の設定**」が表示されます。「**詳細**」をクリックし、「**暗号化**」タブから「**証明書を表示（S)...**」をクリックします。



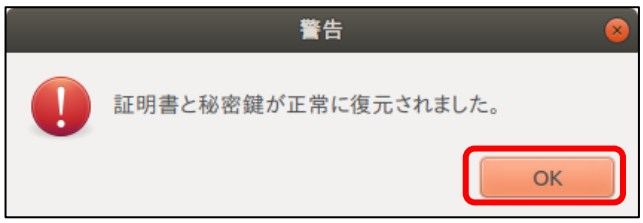
3．「**証明書マネージャ**」が表示されます。
「**あなたの証明書**」タブを選択し、「**インポート（M）…**」をクリックし、「2.2. 電子証明書のダウンロード」でダウンロードした、証明書の保管場所（デスクトップ）を指定します。



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、「**開く**」をクリックします。



5．「**パスワード入力**」画面が表示されます。
「2.2. 電子証明書のダウンロード」で「**証明書パスワード**」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。



6．「**警告**」画面が表示されます。
「**OK**」をクリックします。



７．証明書がインポートされます。
インポートした証明書を選択し、「**表示**」をクリックします。



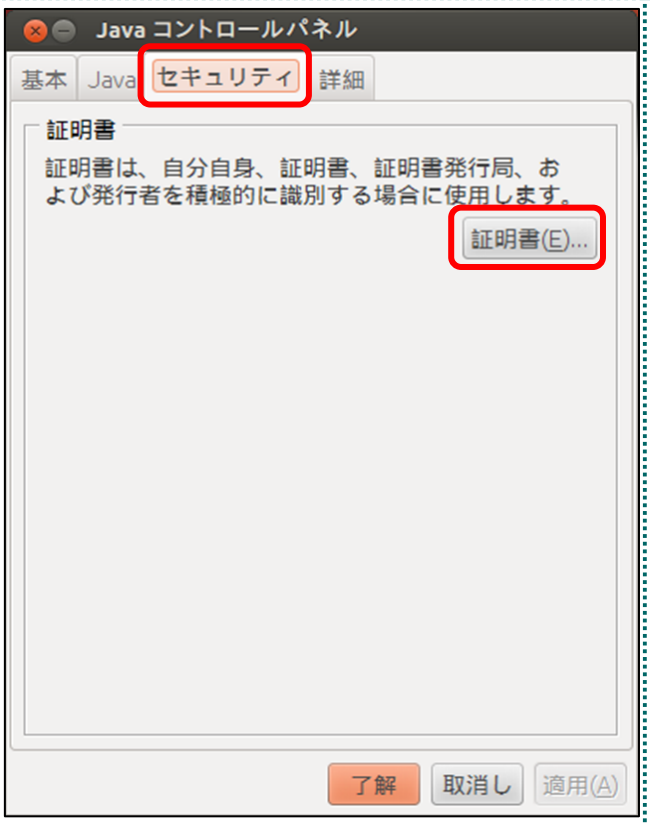
８．「**証明書**」画面が表示されます。
一般名称（CN）が「Online Billing NW Common Root CA」と表示されることを確認します。

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。

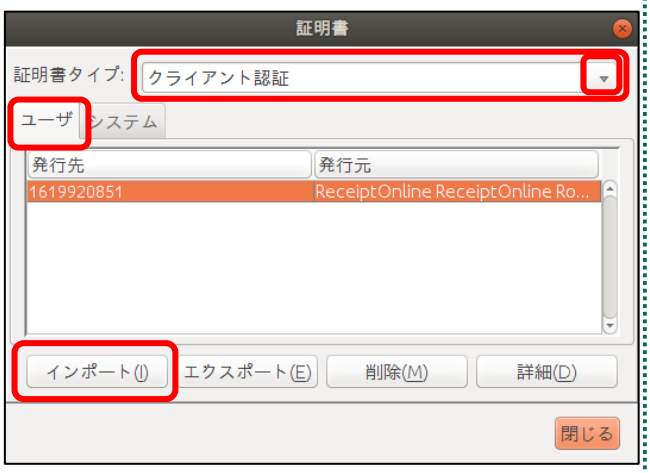
2.4.　Java 実行環境に電子証明書をインポート



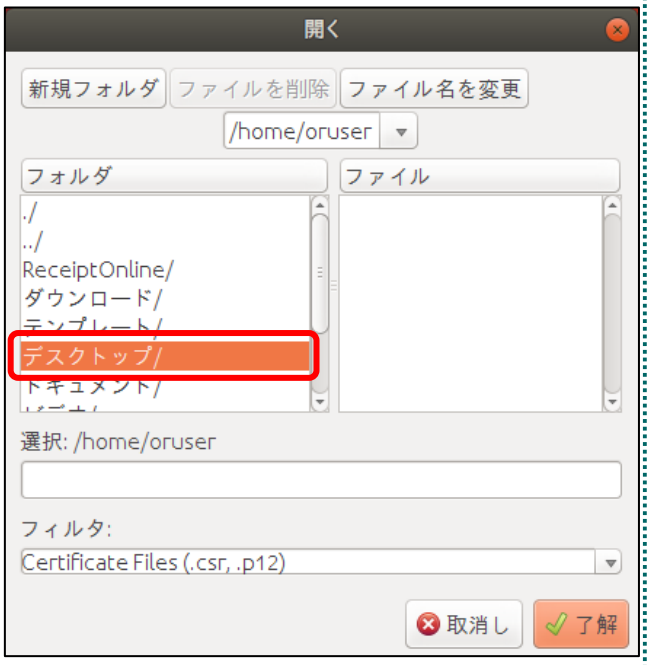
1．デスクトップ上の「**JRE 証明書**」アイコンをダブルクリックします。



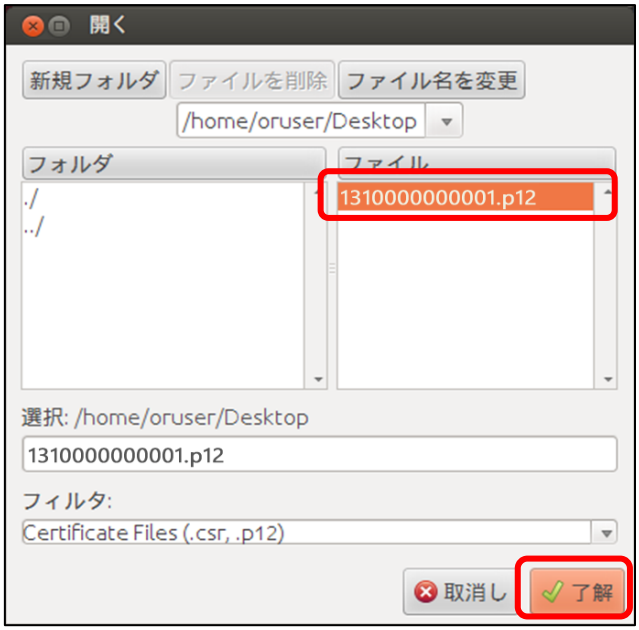
2．「**Java コントロールパネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書**」をクリックします。



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．「**開く**」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。



5．ダウンロードした電子証明書を選択し、
「**了解**」をクリックします。



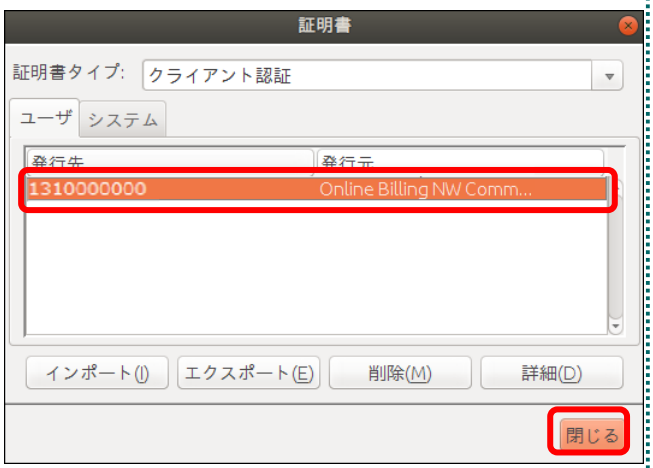
6．パスワード入力メッセージが表示されます。
「2.2. 電子証明書のダウンロード」で「**証明書パスワード**」に設定したパスワードを入力し、「**了解**」をクリックします。



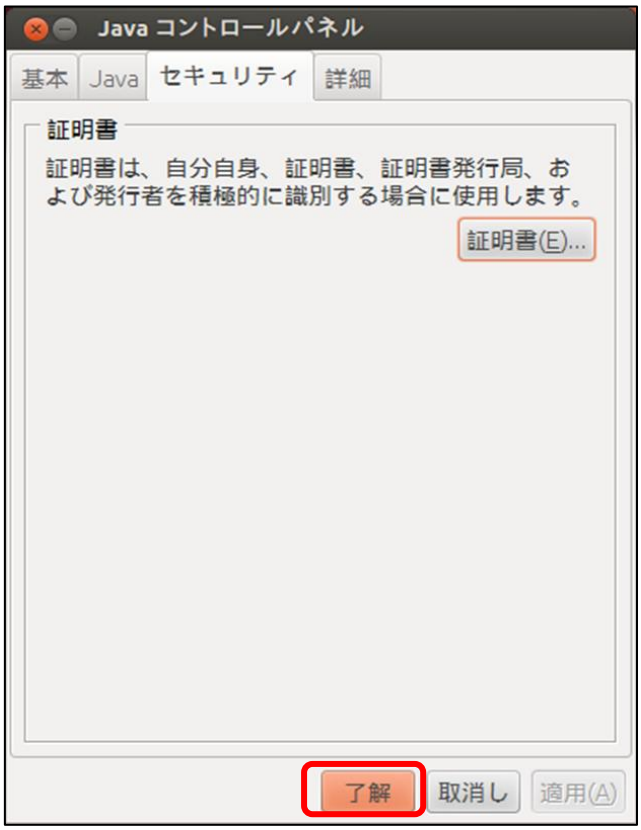
7．引続き、パスワード入力画面が表示されますが、**パスワードは入力せず**に、「**了解**」をクリックします。

【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．「**証明書**」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、「**閉じる**」をクリックします。



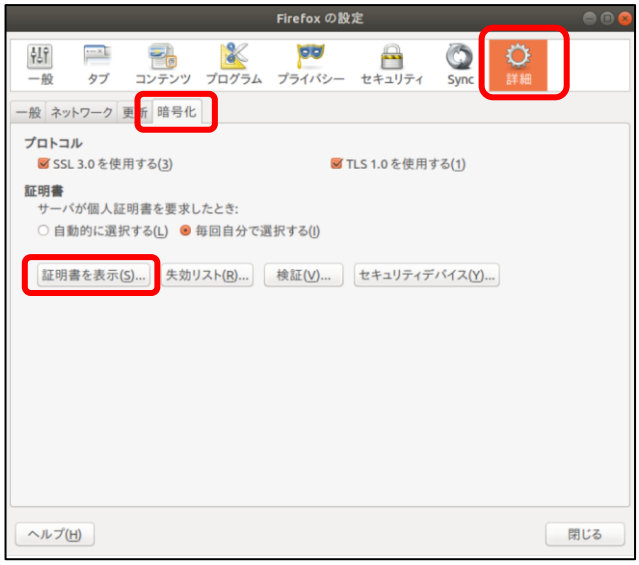
９．「**Java コントロールパネル**」画面に戻ります。「**了解**」をクリックします。

2.5.　登録した電子証明書の確認

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。



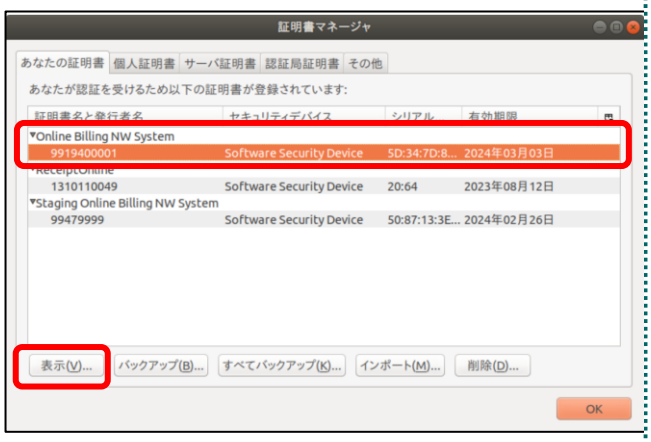
1．「**編集**」→「**設定(N)**」の順に選択します。



2．「**Firefox の設定**」画面が表示されます。「**詳細**」をクリックし、「**暗号化**」タブから「**証明書を表示(S)...**」をクリックします。



3．「**証明書マネージャ**」画面から「**あなたの証明書**」タブを選択します。



４．「2.3. 電子証明書のインポート」でインポートした証明書を選択し、「**表示**」をクリックします。

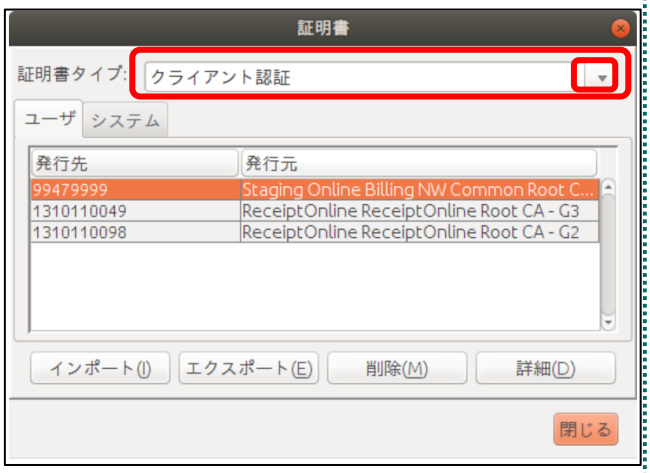


５．「**証明書**」画面が表示されます。「2.3. 電子証明書のインポート」でインポートした証明書を確認します。

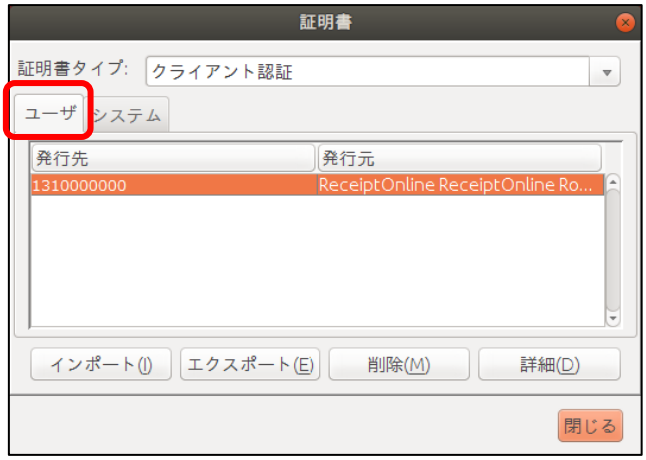
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

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。



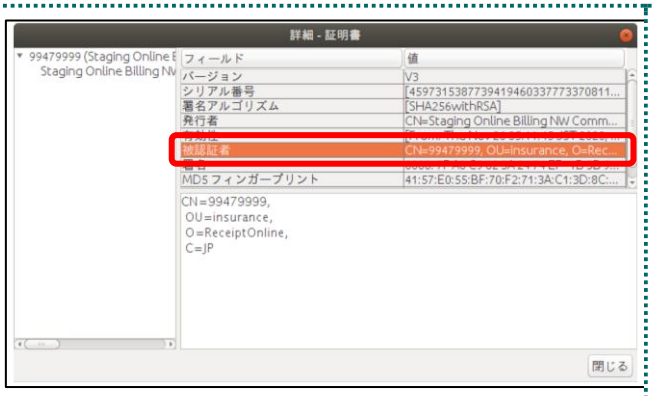
1．「**証明書タイプ**」の「**▼**」をクリックし、「**クライアント認証**」を選択します。



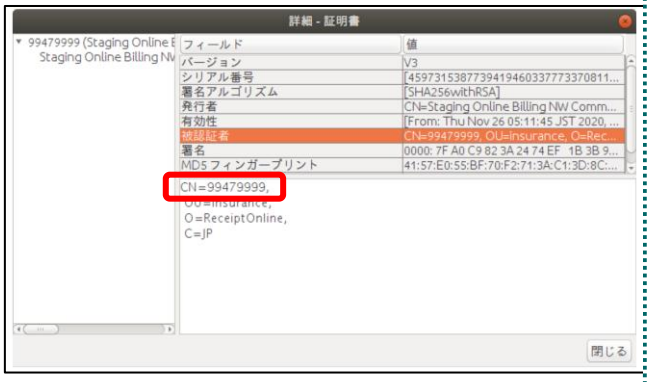
2．「**ユーザ**」タブを選択します。



3．「**発行先**」が「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**発行先**」と同じ証明書を選択し、「**詳細**」をクリックします。「**詳細-証明書**」画面が表示されます。



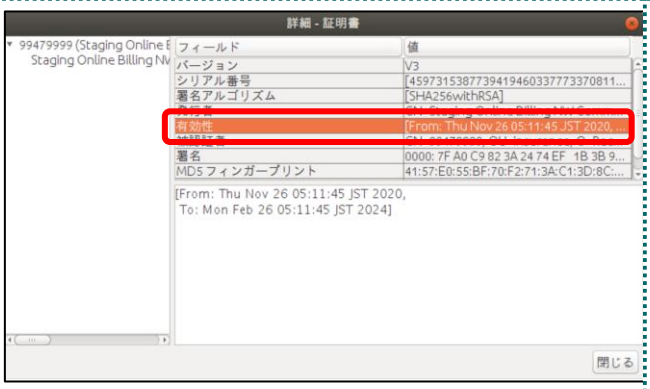
4．フィールド列の「**被認証者**」の行を選択します。



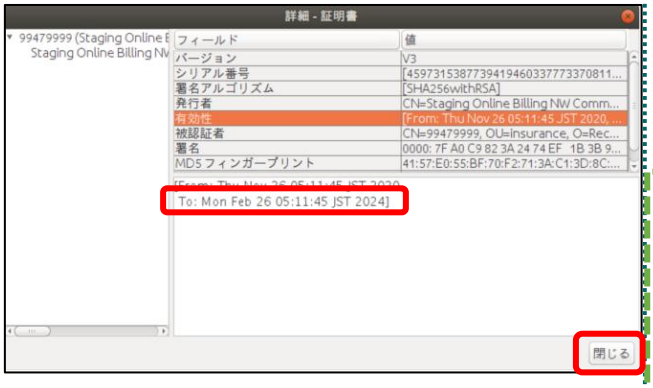
5．表示された以下の内容を確認します。

【注意】

「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**発行先**」情報と、「CN=」の右側に表示されている文字列が一致していることを確認してください。



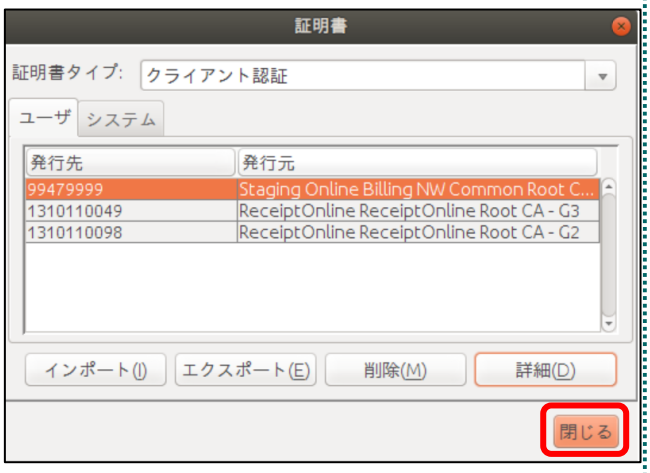
6．フィールド列の「**有効性**」の行を選択します。



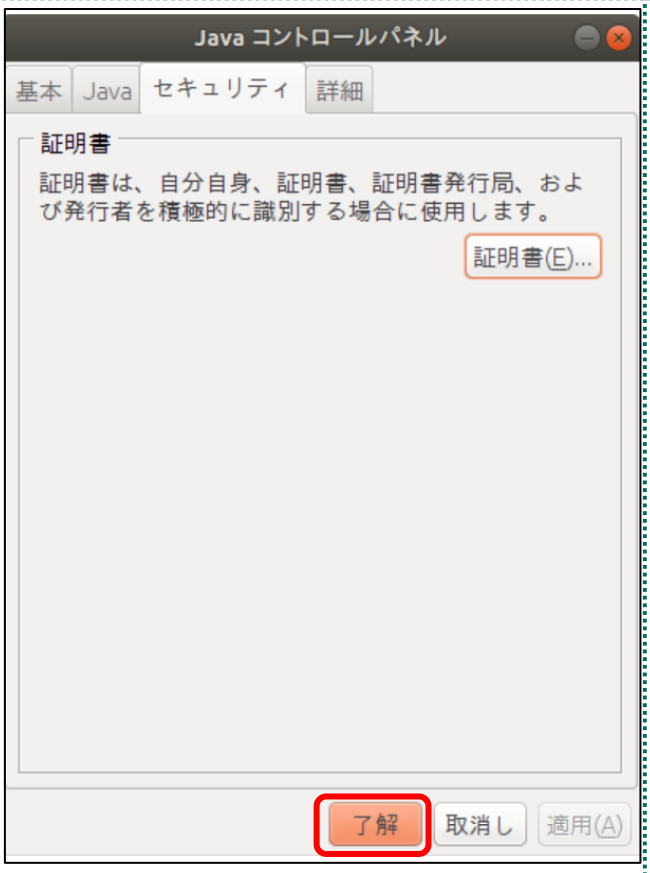
7．表示された以下の内容を確認し、「**閉じる**」をクリックします。

【注意】

「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**電子証明書有効期限**」情報と、「To:」の右側に表示されている年月日が一致していることを確認してください。



８．「**証明書**」画面に戻ります。「**閉じる**」をクリックします。



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。

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。



1．インポート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。

電子証明書の新規発行手続きの作業はこれで終了です。

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。



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

※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。

【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



2．更新対象の証明書を選択し、「OK」をクリックします。

※発行者が「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。

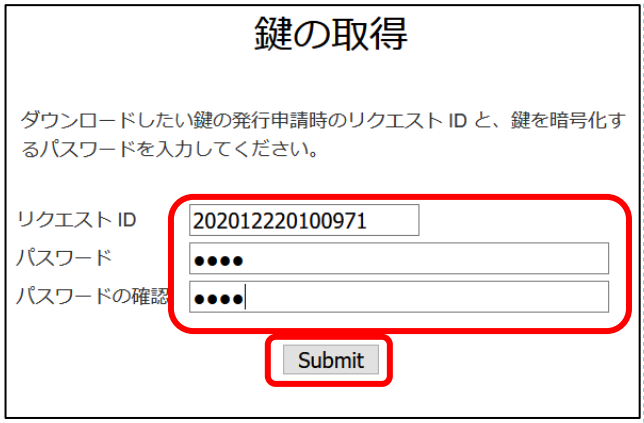


4．「**Submit**」をクリックします。



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。



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桁以上を入力し、「**Submit**」をクリックします。

【注意】

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い。**



７．「**Download**」をクリックします。



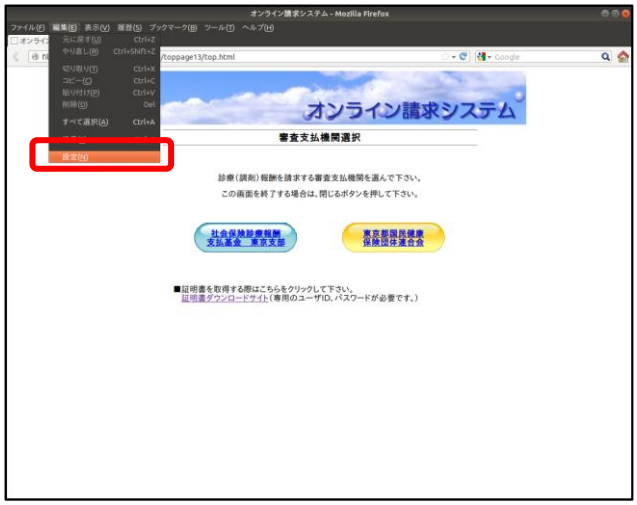
８．ポップアップ画面から「ファイルを保存する」を選択後、「**OK**」をクリックし、保存します。



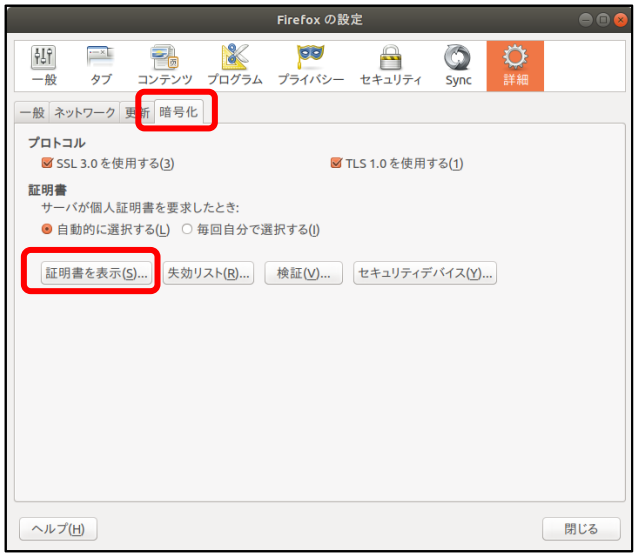
９．鍵がダウンロードできていることを確認します。

【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。



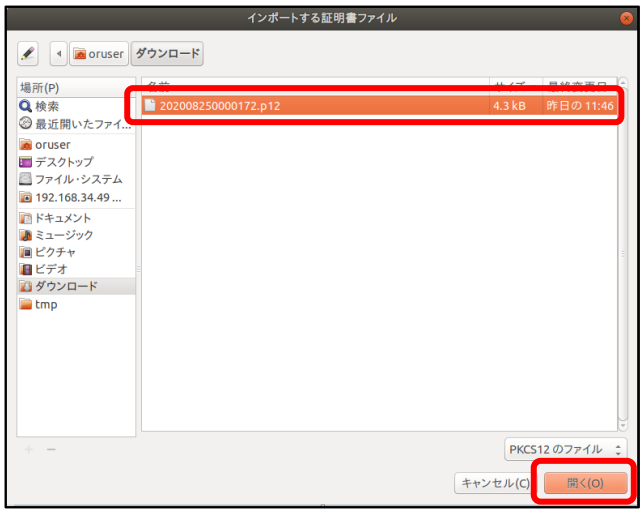
１０．Firefox ブラウザを起動し、クライアント証明書をインポートする。ブラウザの「**編集**」をクリックし、メニュー一覧から「**設定**」をクリックします。



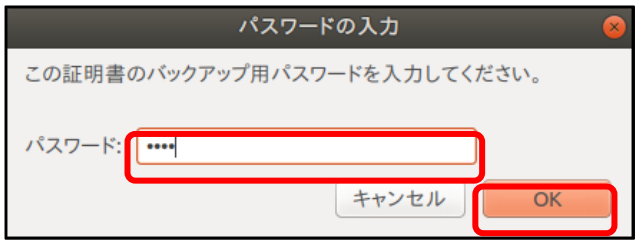
１１．「**Firefox の設定**」が表示されます。「**詳細**」をクリックし、「**暗号化**」タブから「**証明書を表示（S)...**」をクリックします。



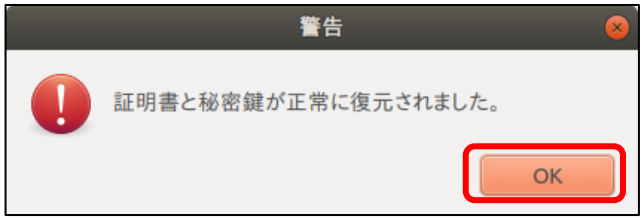
１２．「**証明書マネージャ**」が表示されます。「**あなたの証明書**」タブを選択し、「**インポート（M）…**」をクリックし、「3.1. 電子証明書更新申請サイトからの電子証明書の更新」でダウンロードした、証明書の保管場所（デスクトップ）を指定します。



１３．「**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、「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。



１４．「パスワード**入力**」画面が表示されます。
「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．「**警告**」画面が表示されます。
「**OK**」をクリックします。



１６．証明書がインポートされます。
インポートした証明書を選択し、「**表示**」をクリックします。



１７．「**証明書**」画面が表示されます。
一般名称（CN）が「**Online Billing NW Common 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。

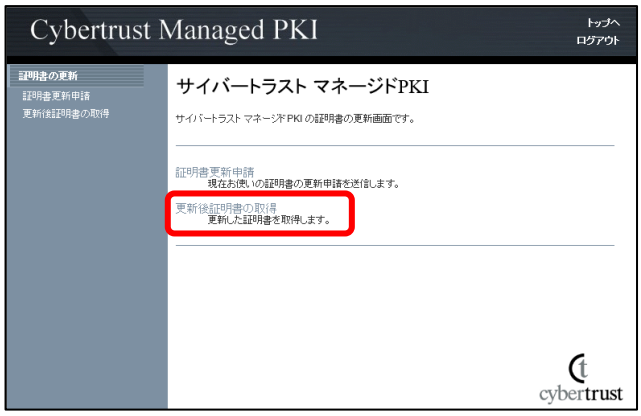
注意　**必ずすべてのブラウザを閉じてから、手続きを実施して下さい。**



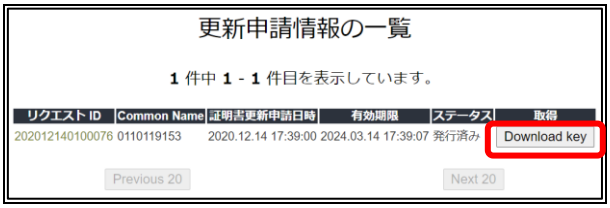
１．**更新対象の証明書がインストールされた端末**からオンライン請求ネットワークに接続して更新申請画面へアクセスします。

【証明書更新申請サイト】

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

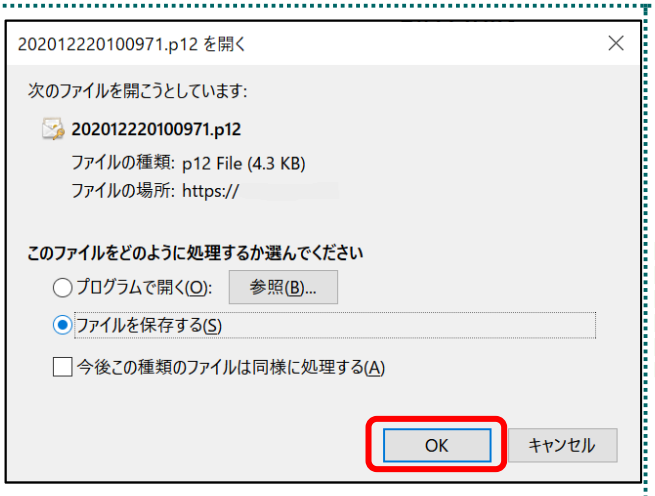


２．「**証明書の更新申請**」画面の「**更新後証明書の取得**」をクリックします。



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「**Download 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、「3.1. 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。



４．ポップアップ画面から「ファイルを保存する」を選択後、「OK」をクリックして、証明書ファイルを保存します。

【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。

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。

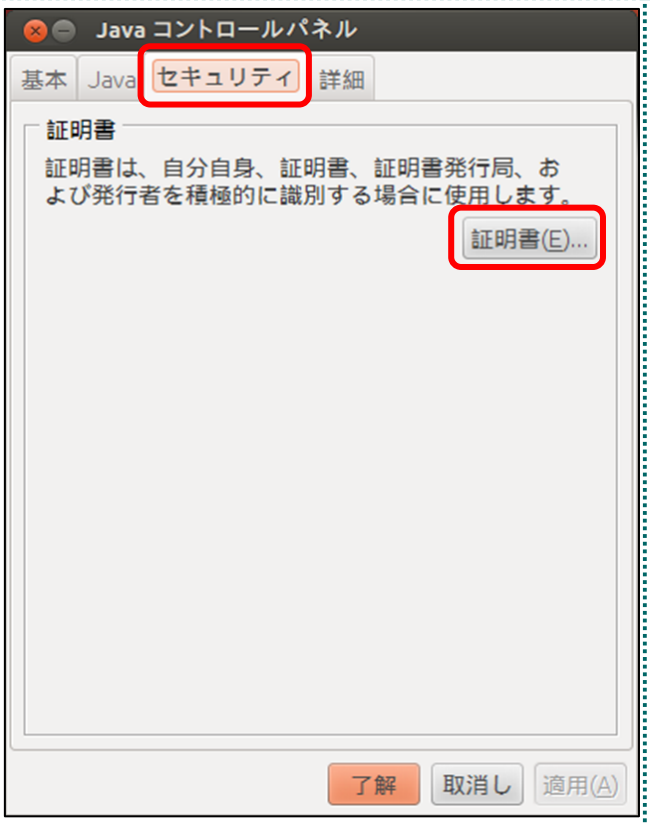
６．「5. 電子証明書の削除」及び「6. Java 実行環境の電子証明書を削除」を参照し古い証明書を削除します。

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。

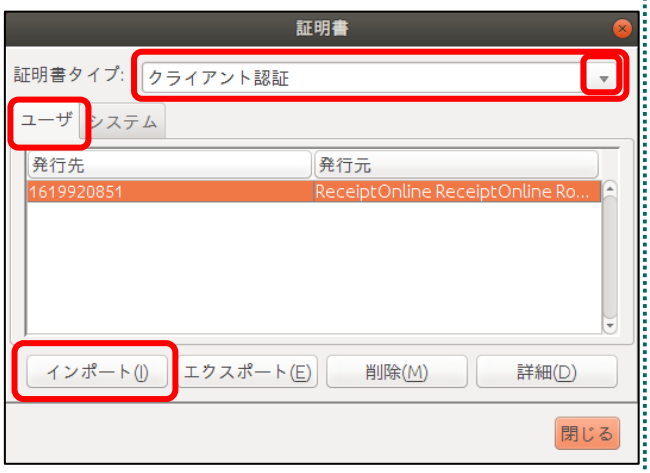
3.2.　Java 実行環境に電子証明書をインポート



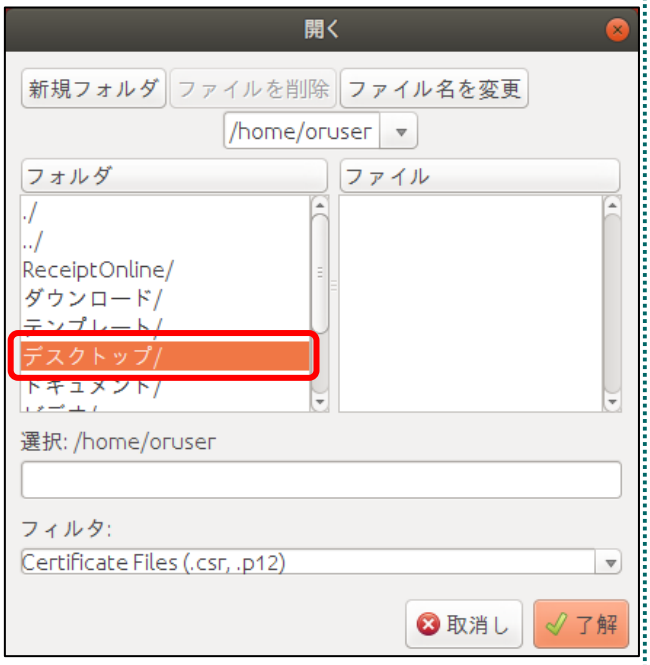
1．デスクトップ上の「**JRE 証明書**」アイコンをダブルクリックします。



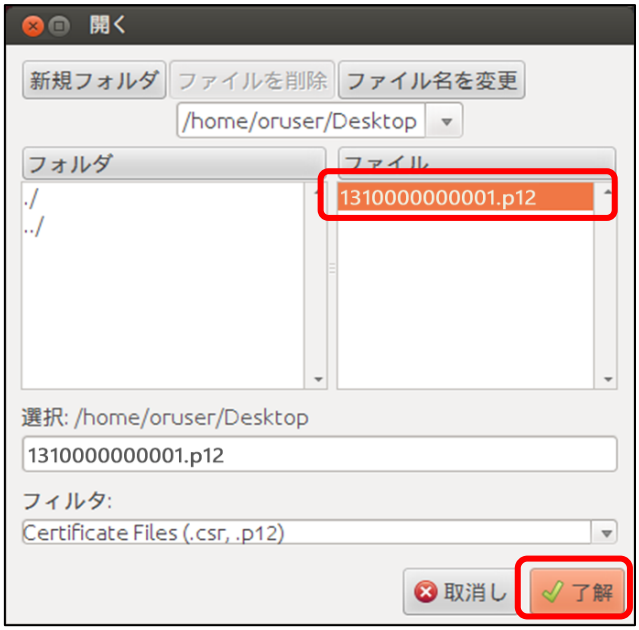
2．「**Java コントロールパネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書**」をクリックします。



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．「**開く**」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。



5．ダウンロードした電子証明書を選択し、
「**了解**」をクリックします。



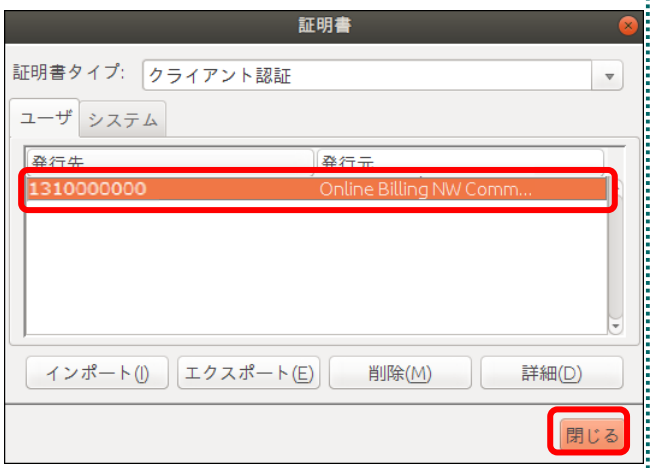
６．パスワード入力メッセージが表示されます。
「1.1. 証明書のダウンロード」で「**証明書パスワード**」に設定したパスワードを入力し、「**了解**」をクリックします。



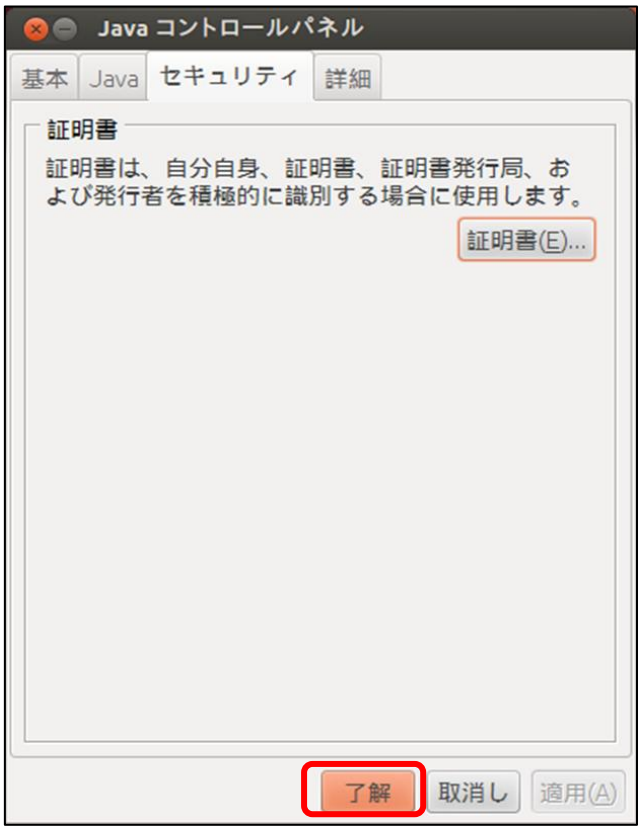
７．引続き、パスワード入力画面が表示されますが、**パスワードは入力せず**に、「**了解**」をクリックします。

【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．「**証明書**」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、「**閉じる**」をクリックします。



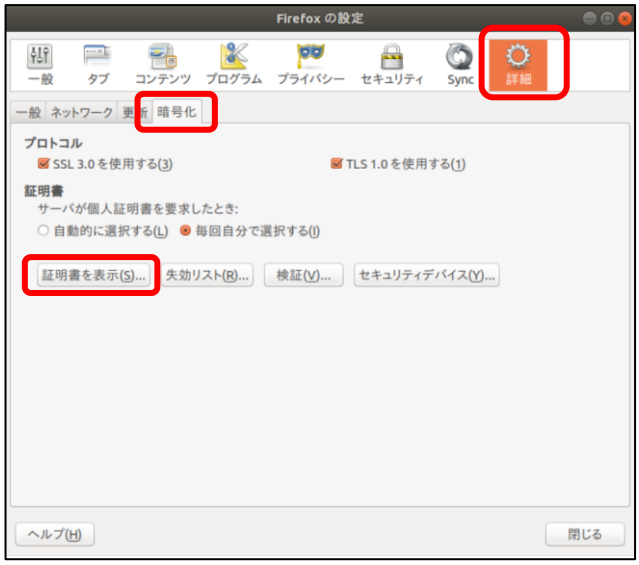
９．「**Java コントロールパネル**」画面に戻ります。「**了解**」をクリックします。

3.3.　登録した電子証明書の確認

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。



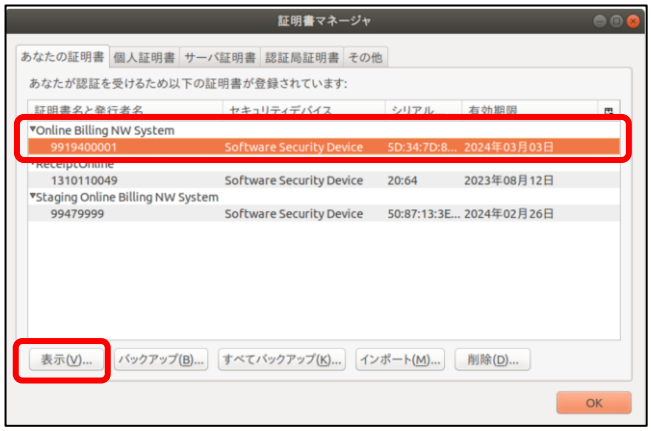
1．「**編集**」→「**設定(N)**」の順に選択します。



2．「**Firefox の設定**」画面が表示されます。「**詳細**」をクリックし、「**暗号化**」タブから「**証明書を表示(S)...**」をクリックします。



3．「**証明書マネージャ**」画面から「**あなたの証明書**」タブを選択します。



４．「1.2. 証明書のインポート」でインポートした証明書を選択し、「**表示**」をクリックします。

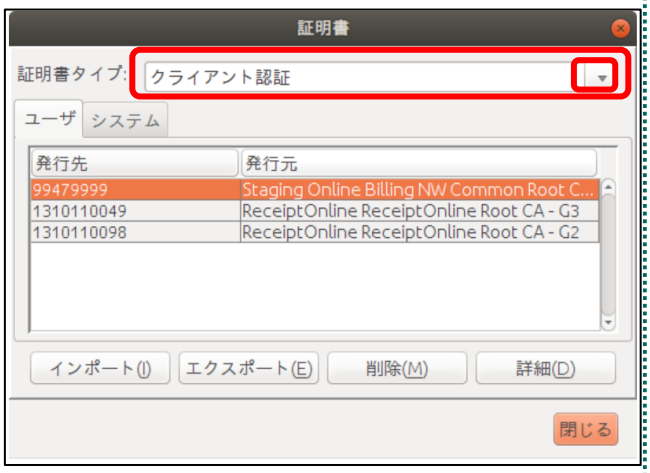


５．「**証明書**」画面が表示されます。「1.2. 証明書のインポート」でインポートした証明書を確認します。

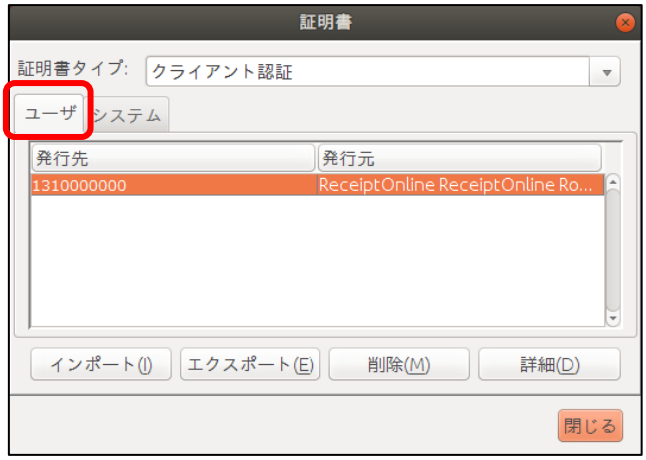
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

3.4.　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。



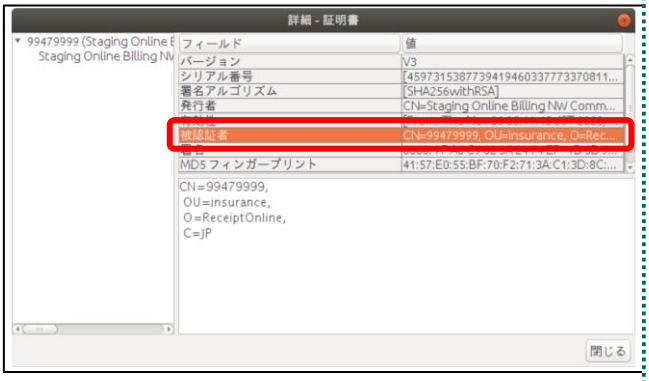
1．「**証明書タイプ**」の「**▼**」をクリックし、「**クライアント認証**」を選択します。



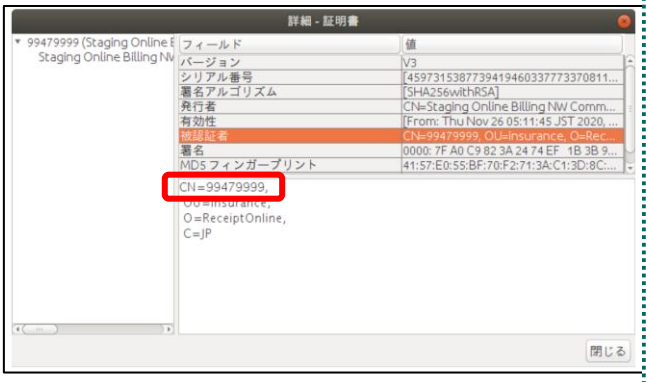
2．「**ユーザ**」タブを選択します。



3．「**発行先**」が「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**発行先**」と同じ証明書を選択し、「**詳細**」をクリックします。「**詳細-証明書**」画面が表示されます。



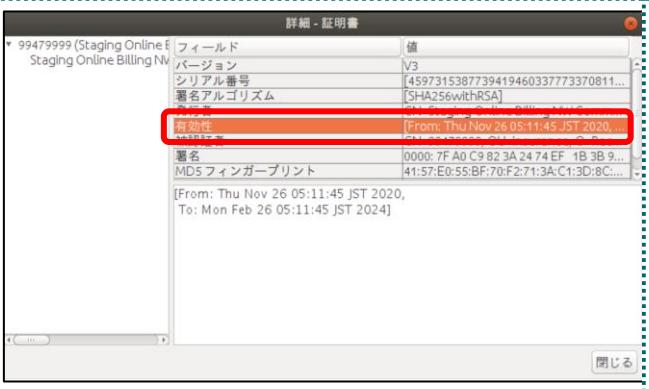
4．フィールド列の「**被認証者**」の行を選択します。



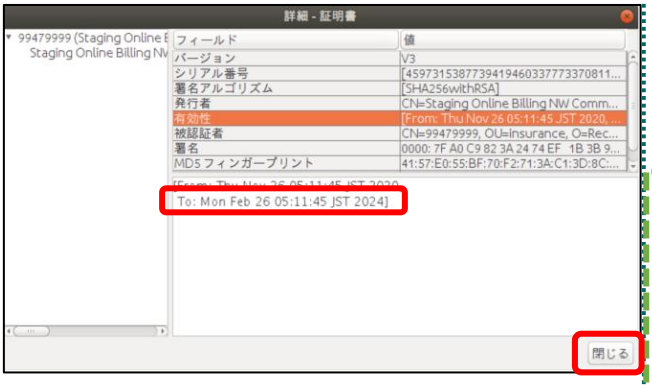
5．表示された以下の内容を確認します。

【注意】

「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**発行先**」情報と、「CN=」の右側に表示されている文字列が一致していることを確認してください。



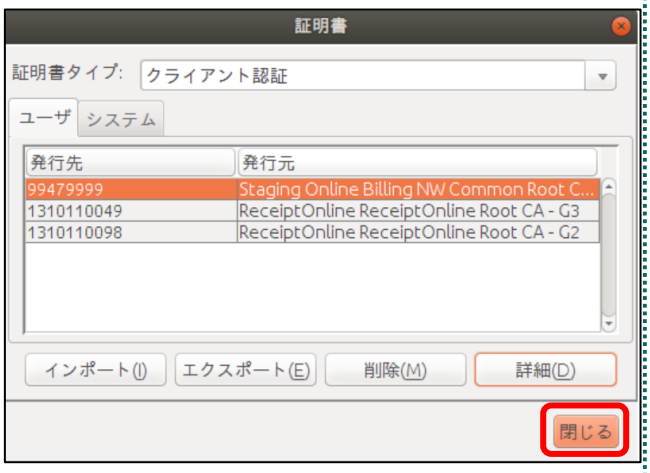
6．フィールド列の「**有効性**」の行を選択します。



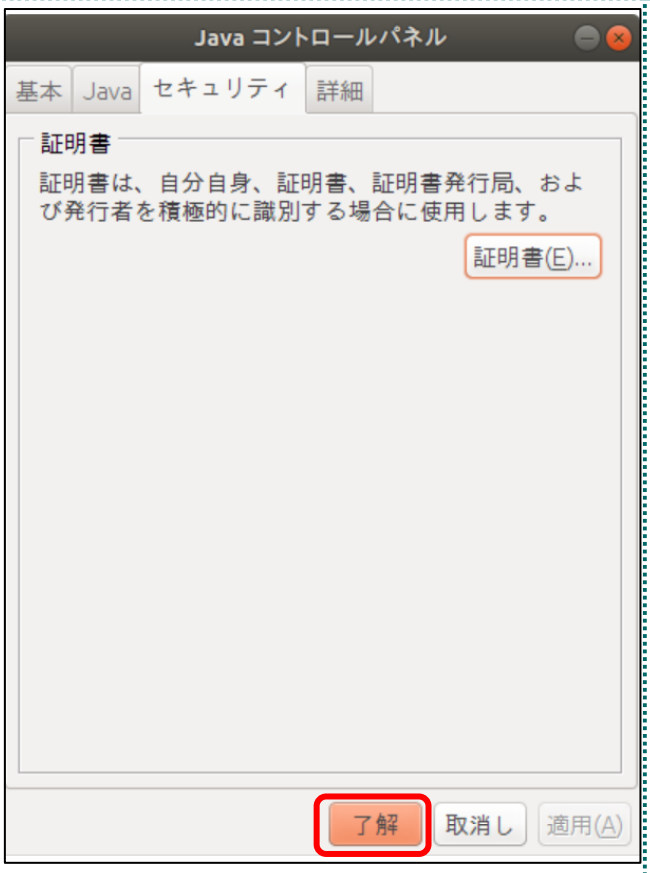
7．表示された以下の内容を確認し、「**閉じる**」をクリックします。

【注意】

「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**電子証明書有効期限**」情報と、「To:」の右側に表示されている年月日が一致していることを確認してください。



８．「**証明書**」画面に戻ります。「**閉じる**」をクリックします。



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。

以上でJava実行環境の電子証明書の確認は完了しました。オンライン請求システムまたは特定健診・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。



1．インポート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．「1.1.　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、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。

次ページからの手続きは、電子証明書の失効手続きです。

失効手続き後は、失効申請の取消しはできませんので、

ご留意ください。

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から、手続きを実施して下さい。



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失効申請画面へアクセスします。

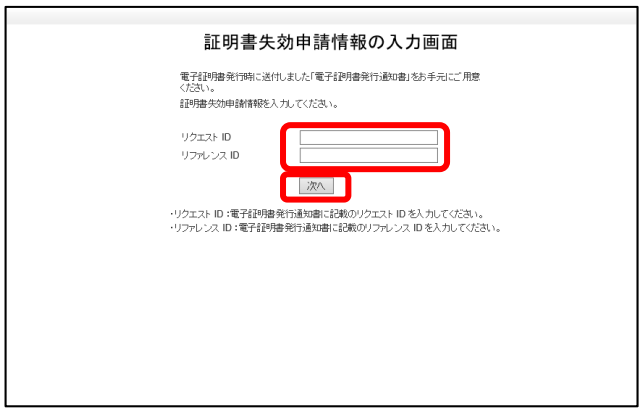
【証明書失効申請サイト】

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

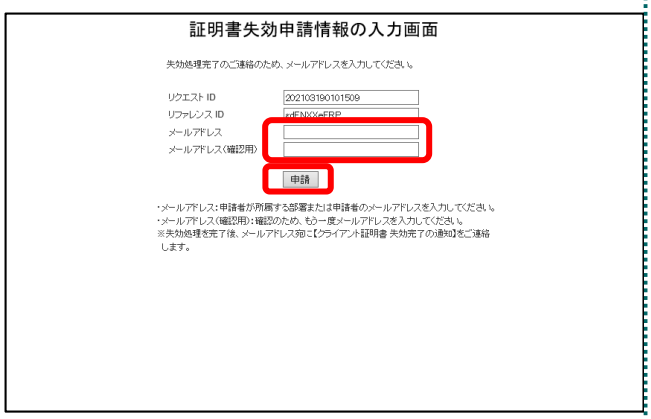


【こんなときは！】

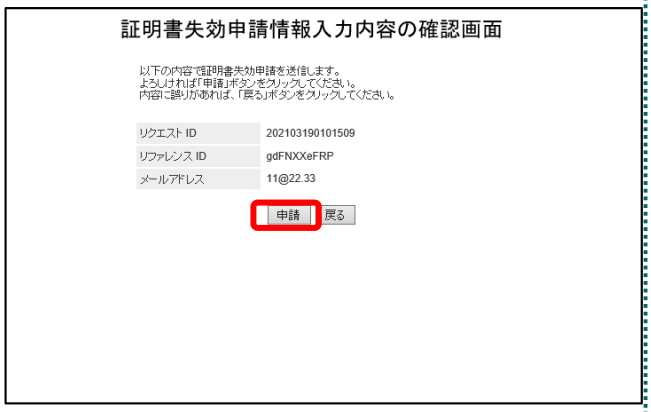
証明書のダウンロード画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**警告：潜在的なセキュリティリスクあり**」と表示される場合は、ルート証明書のインストールが必要であるため、「7.2.　ルート証明書のダウンロードとインポート」を参照



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。



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。



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に失効完了をご連絡します。

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。

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。

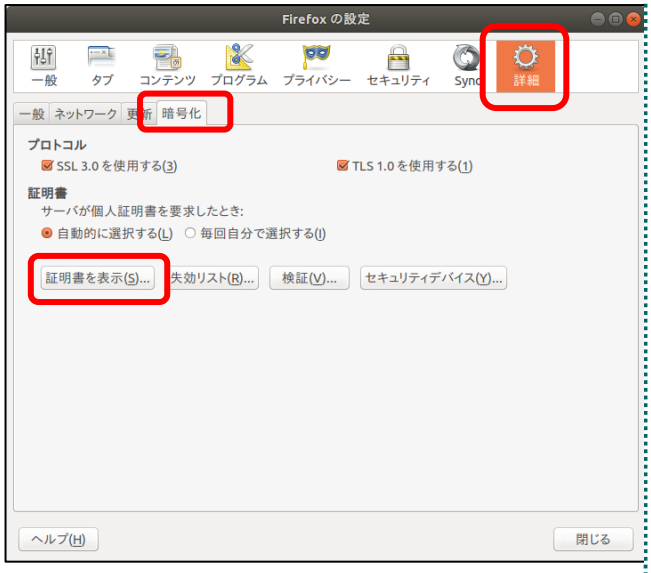
電子証明書の失効手続きの作業はこれで終了です。

5.　電子証明書の削除

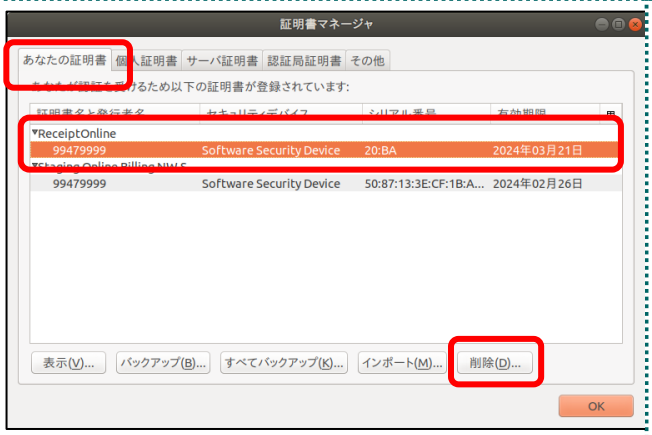
注意　**必ずすべてのブラウザを閉じてから、手続きを実施して下さい。**



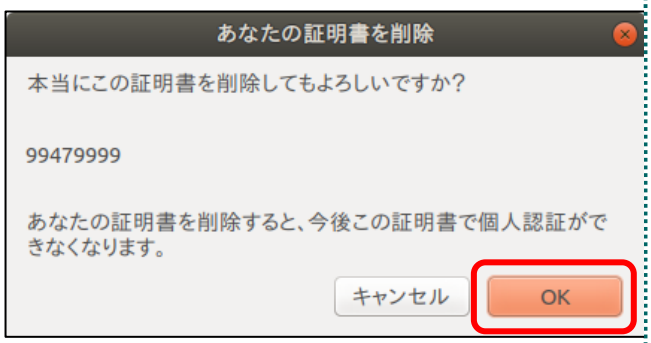
１．メニューバーから「**編集**」→「**設定**」の順に選択します。



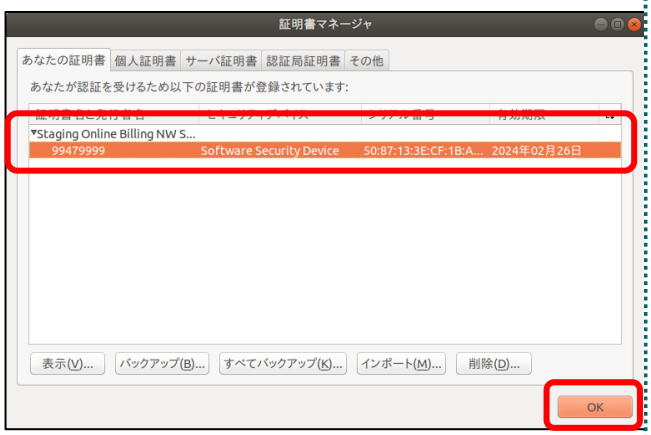
２．「**Firefox の設定**」が表示されます。
「**詳細**」をクリックし、「**暗号化**」タブから「**証明書を表示（S)...**」をクリックします。



３．「**証明書マネージャ**」が表示されます。
「**あなたの証明書**」タブを開き、削除対象の古い証明書（「**有効期限**」の日付が古い証明書）を選択し、「**削除**」をクリックします。



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。



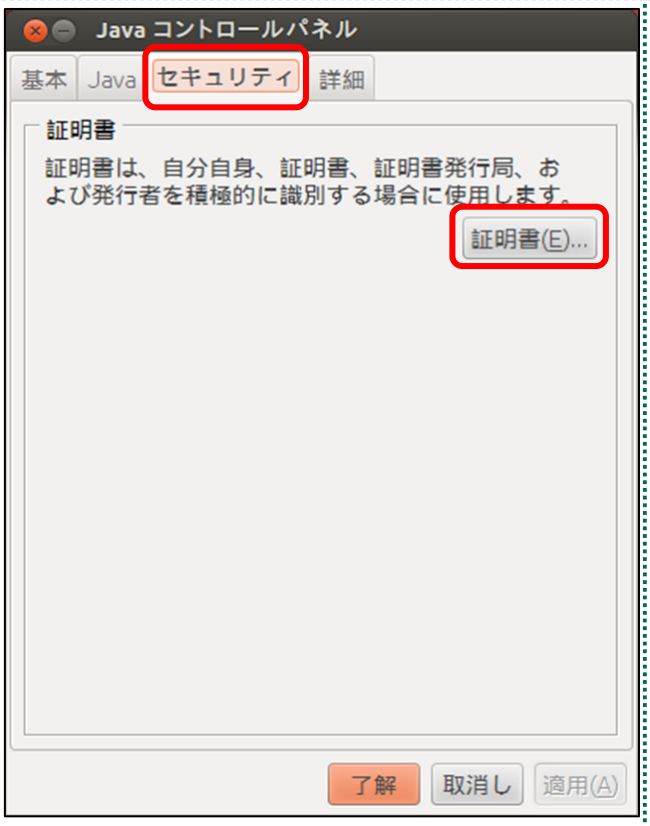
５．「**証明書マネージャ**」が表示されます。
削除を行った証明書が一覧から消えていることを確認します。
確認後、「OK」をクリックします。

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。

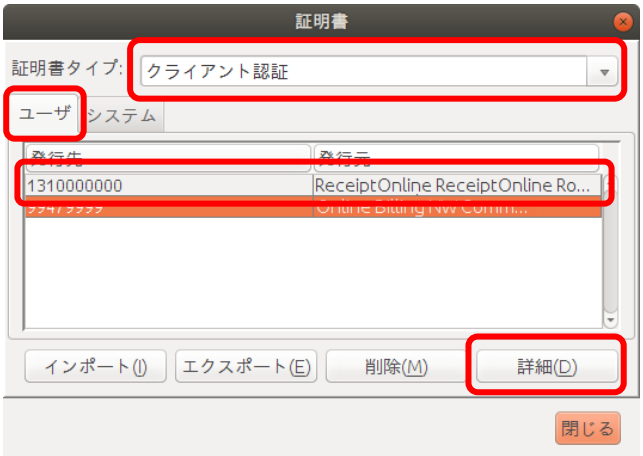
6.　Java 実行環境の電子証明書を削除



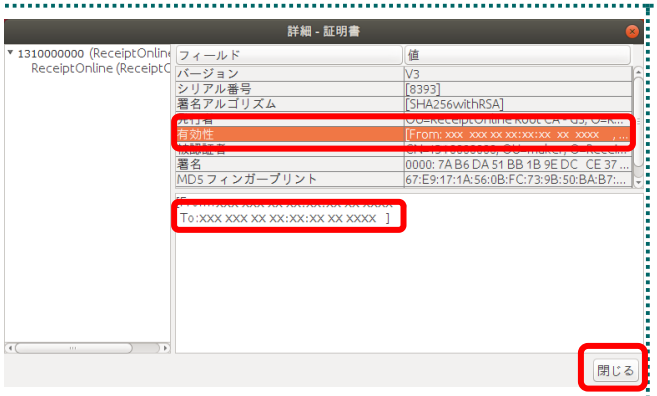
１．デスクトップ上の「**JRE 証明書**」アイコンをダブルクリックします。



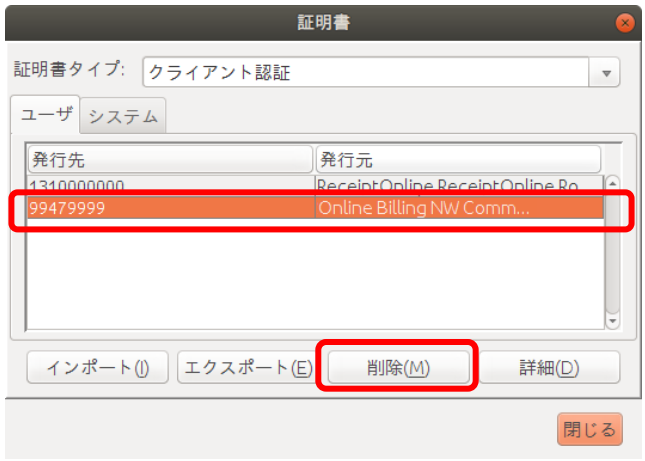
２．「**Java コントロールパネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書**」をクリックします。



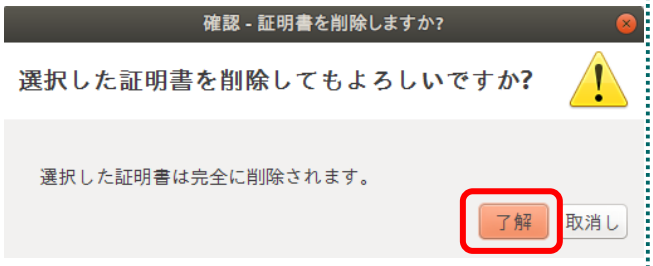
３．「**証明書**」画面が表示されます。
「**証明書タイプ**」の「**▼**」をクリックし、「**クライアント認証**」を選択します。
「**ユーザ**」タブを選択し、複数行表示される証明書を選択し、「**詳細**」をクリックします。
（古い有効期限の日付を確認するため、手順「３」、及び「４」を繰り返します。）



4．フィールド列の「**有効性**」の行を選択します。
表示された有効期限を確認し、「**閉じる**」をクリックします
「To:」で始まる日付が有効期限です。



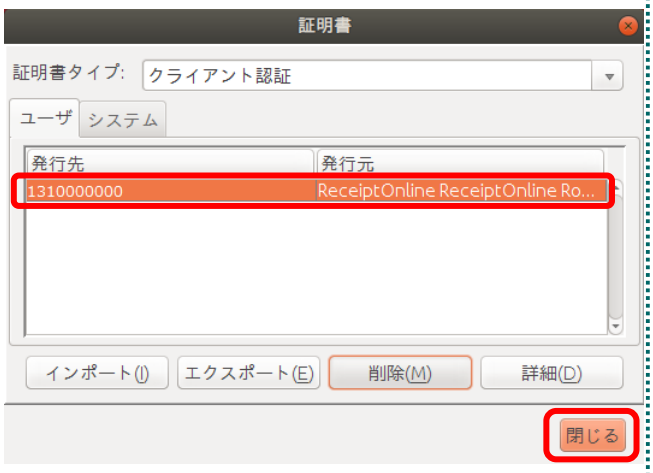
5．有効期限の古い証明書が選択されていることを確認し、「**削除**」をクリックします。



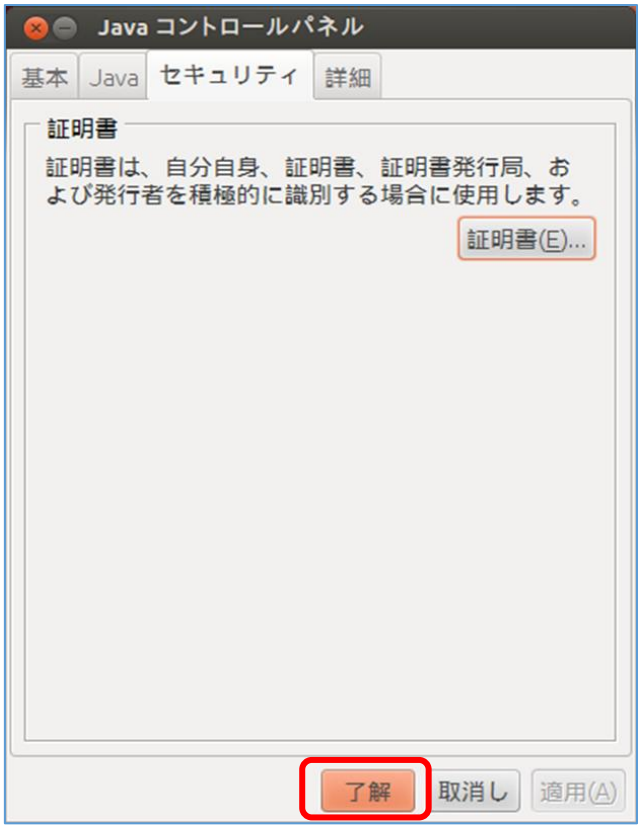
6．証明書削除確認メッセージが表示されます。
「**了解**」をクリックします。



7．パスワード入力メッセージが表示されます。
パスワードを入力せず、「**了解**」をクリックします。



８．「**証明書**」画面に戻ります。
証明書が削除されたことを確認し、「**閉じる**」をクリックします。



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。

7.　サポート情報

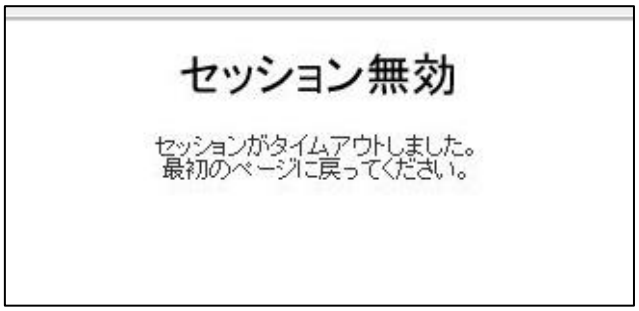
7.1.　ご利用にあたっての注意事項

7.1.1.　認証用の証明書の選択画面が表示された場合



１．発行者が「Online Billing NW Common Root CA」となっていることを確認し、「OK」をクリックしてください。

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



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用 URL へアクセスし直してください。

7.1.3. 操作継続失敗画面表示時のトラブルシューティング



複数のタブやウインドウで共通認証局の画面を開いた場合や、ブラウザの「戻る」ボタンなどで前の画面へ戻った場合に、この画面が表示されることがあります。
この画面が表示された場合は、共通認証局の画面を開いているタブとウインドウをすべて閉じ、ブラウザを終了してください。
その後、ブラウザを起動し、利用する手続きの最初の画面から操作をやり直してください。
再度操作を行う際は、共通認証局の画面を複数のタブやウインドウで開かないでください。

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

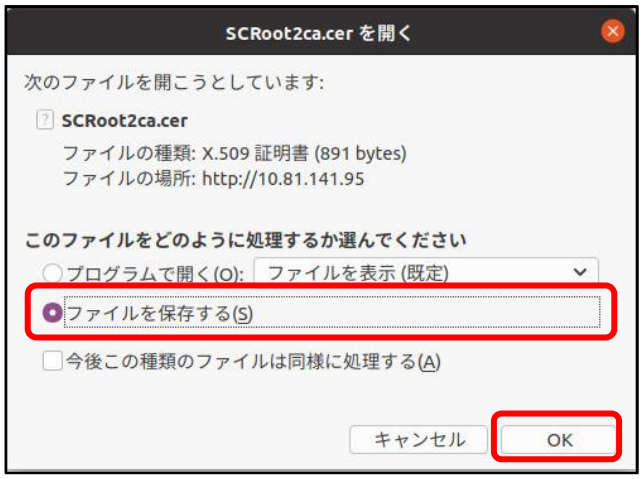
注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。



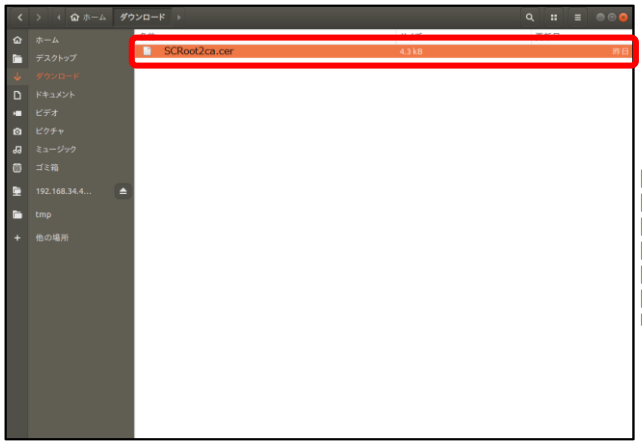
１．オンライン請求ネットワークへ接続の端末からルート証明書のダウンロードサイトにアクセスします。

【ルート証明書ダウンロードサイト】

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



ポップアップ画面から「**ファイルを保存する(S)**」を選択後「**OK**」をクリックし保存します。



２．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。

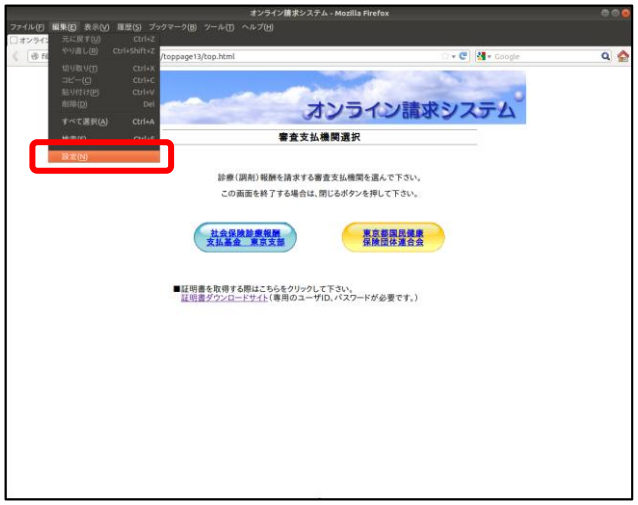
【注意】

ルート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。

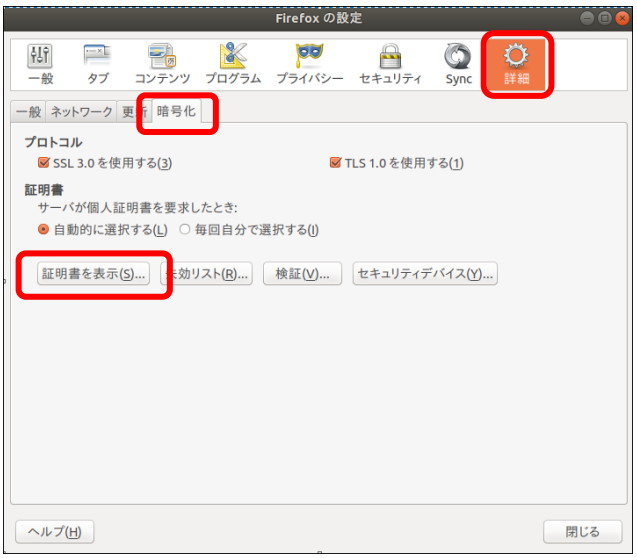
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

7.2.2. ルート証明書のインポート

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。



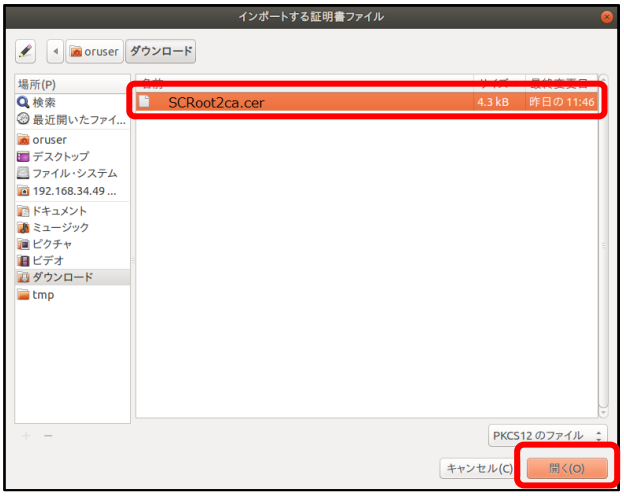
1．メニューバーから「**編集**」→「**設定**」の順に選択します。



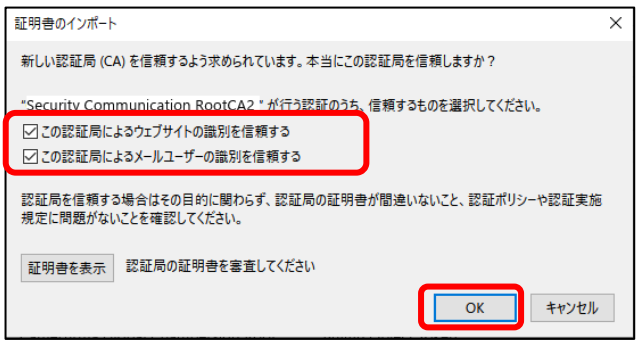
2．「**Firefox の設定**」が表示されます。
「**詳細**」をクリックし、「**暗号化**」タブから
「**証明書を表示（S)...**」をクリックします。



3．「**証明書マネージャ**」が表示されます。
「**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。



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、「**開く**」をクリックします。



5．「**証明書のインポート**」画面が表示されます。
すべてのチェックボックスにチェックを入れ、「**OK**」ボタンをクリックします。



6．ルート証明書がインポート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。

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。



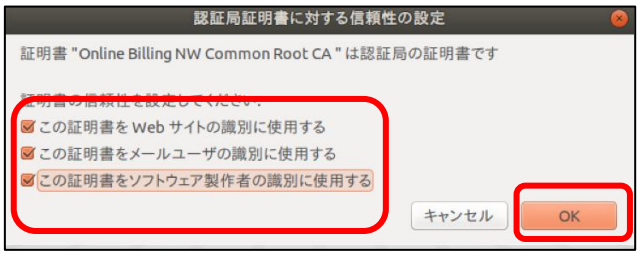
1．「認証局証明書」タブを選択します。



2．「Online Billing NW System」に含まれる証明書を選択し、「**信頼性を設定**」ボタンをクリックします。

【補足】

証明書が複数表示されている場合は、全ての証明書に対して実施してください。



3．「**認証局証明書に対する信頼性の設定**」画面が表示されます。
すべてのチェックボックスにチェックを入れ、「OK」ボタンをクリックします。
「**証明書マネージャ**」画面に戻ります。

【補足】

既にチェックが入っている場合はそのまま「OK」ボタンをクリックします。