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
(Mac Safari)

Version 1.7.0

令和８年３月２日

目次

Date	Version #	Summary of Changes
2020/12/14	1.0.0	初版
2021/1/4	1.1.0	・「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
2021/1/27	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	・「1.3 Java 実行環境に電子証明書をインポート」の 9 に注意書きを追加 ・「3 証明書の失効」修正
2022/03/25	1.4.0	・6.2 ルート証明書のダウンロードと登録追加
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
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

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.ssk.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

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。

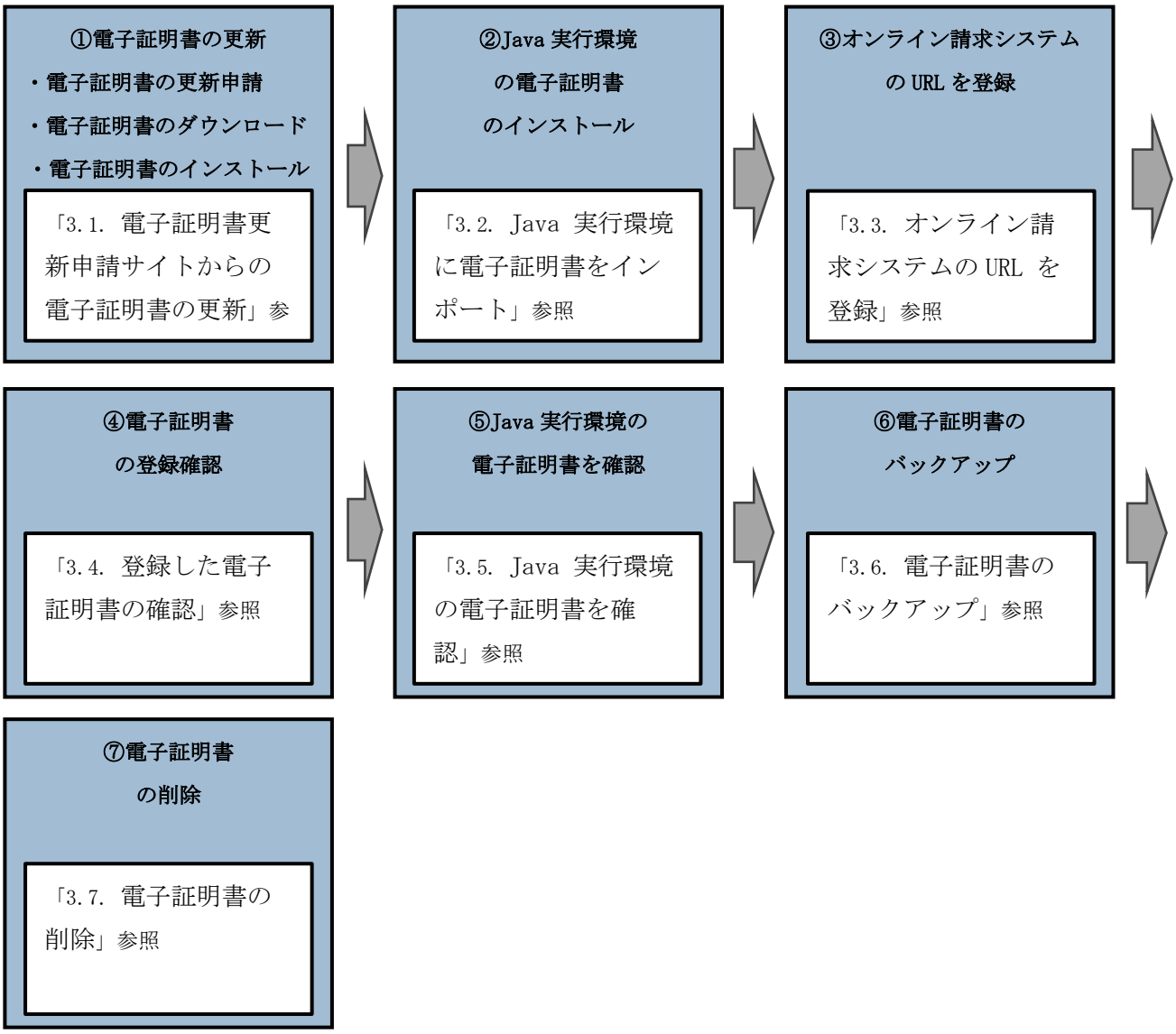
【更新手続き・有効期限に関する周知】

オンライン請求システムにメッセージを表示 ※支払基金のみ	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@ssk.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。

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。



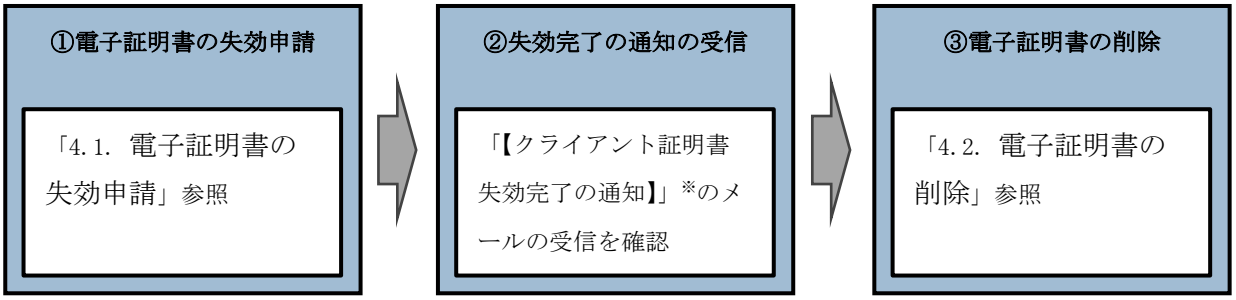
⑥電子証明書のバックアップまでの操作を更新前の電子証明書の有効期限（３年３か月）までに実施してください。
※更新前の電子証明書の有効期限（３年３か月）を過ぎると、更新済みの電子証明書がダウンロードできなくなります。

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@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

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）

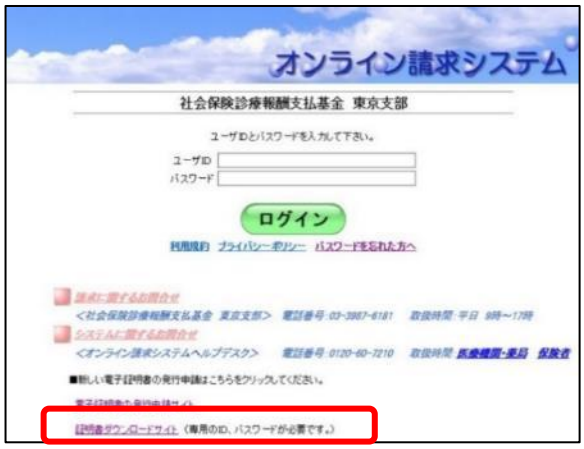
発行者	Online Billing NW Common Root CA - G1
発行先	※医療機関コード
端末名称等	※申請時に登録した端末名称等
リクエストID	20210121xxxxxxx
リファレンスID	XXXXXXXXXXX
電子証明書有効期間	YYYY/MM/DD ～ YYYY/MM/DD
ダウンロードサイト有効期限	YYYY/MM/DD

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）で電子証明書を取得します。

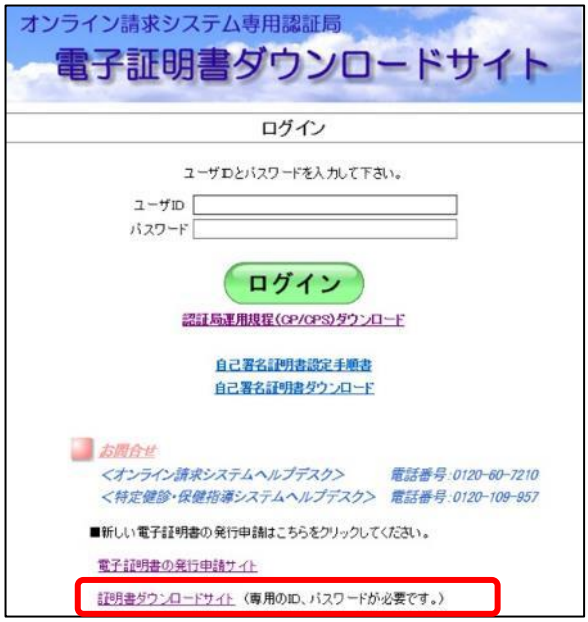
注意 **必ずすべてのブラウザを閉じてから、手続きを実施して下さい。**

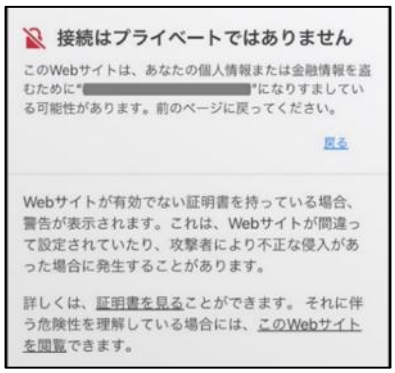
【レセプトオンライン請求用端末の場合】

・オンライン請求システムのログイン画面



・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。

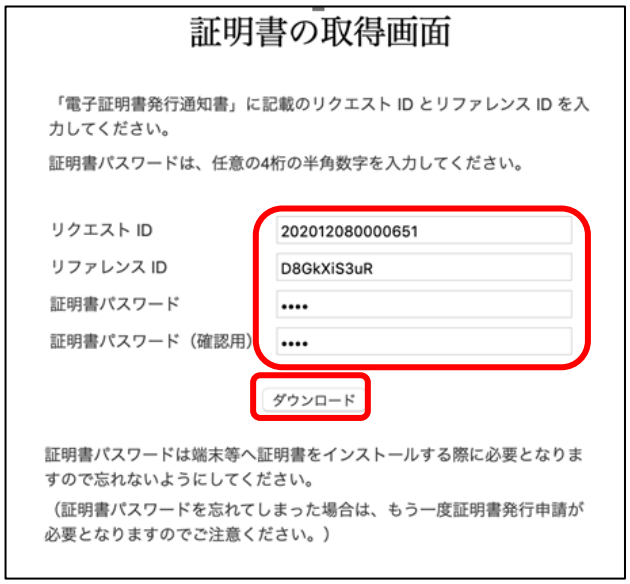
【ダウンロードサイト】

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「**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「**接続はプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「7.2. ルート証明書のダウンロードと登録」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**」に鍵の暗号化パスワード（任意のパスワード）半角数字 4 桁を入力し、「**ダウンロード**」をクリックします。

【注意】

入力した証明書パスワードは、「2.3. **電子証明書のインポート**」の「３．」及び「2.4. **Java 実行環境に電子証明書をインポート**」の「８．」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．ダウンロードした証明書は「**ダウンロード**」フォルダに自動保存されます。ブラウザの閉じるボタン（**×ボタン**）で終了してください。

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

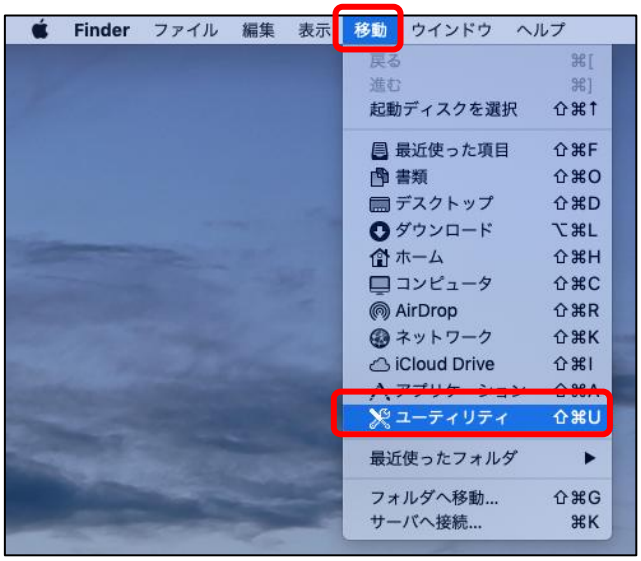
【セットアップ】

電子証明書をオンライン請求端末にセットアップします。

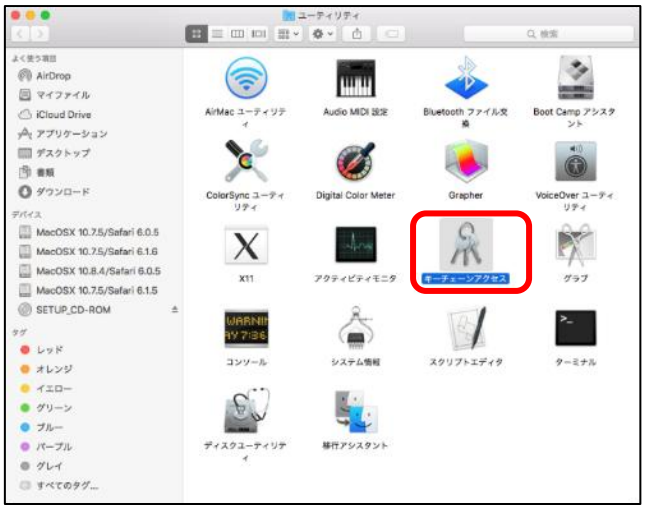
1．「**ダウンロード**」した証明書をダブルクリックします。

2．「**証明書の追加**」画面が表示されます。キーチェーンに「**ログイン**」を選択し、「**追加**」をクリックします。

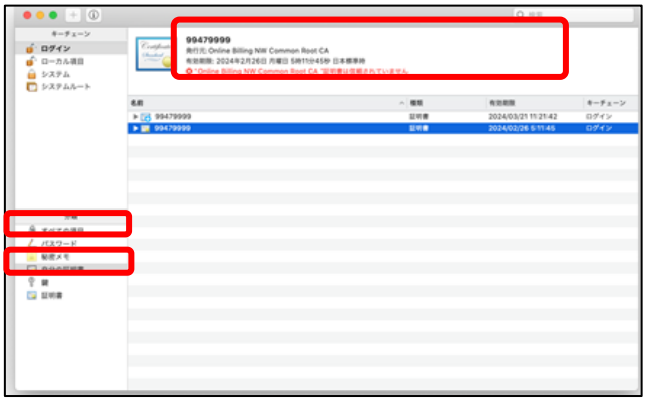
3．「鍵の取得」画面で入力した**鍵の暗号化パスワード（任意のパスワード）**を入力して、「**OK**」をクリックします。



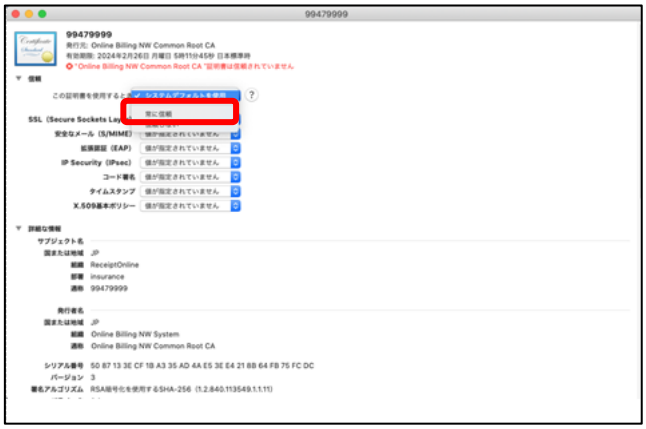
４．Finder のメニューバーから「**移動**」-「**ユーティリティ**」の順に選択します。



５．「**ユーティリティ**」画面が表示されます。「**キーチェーンアクセス**」アイコンをダブルクリックし、「キーチェーンアクセスを開く」を選択します。

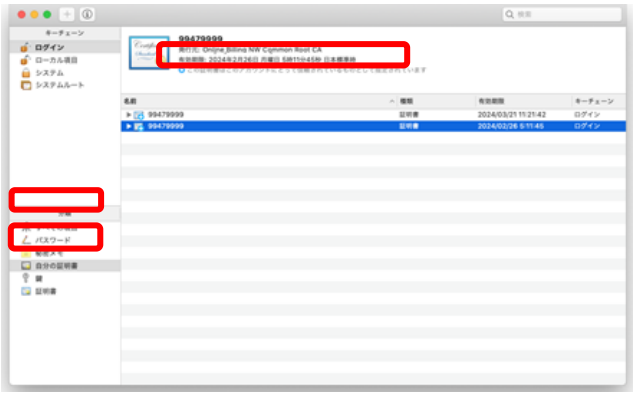


６．「**すべての項目**」→「**自分の証明書**」を開き、発行元が「Online Billing NW Common Root CA」と表記されている証明書をダブルクリックします。



７．「＞信頼」から信頼タブを開いて「**この証明書を使用するとき**」のプルダウンをクリックし、「**常に信頼**」を選択します。パソコンログイン時のパスワードを入力する画面がポップアップされます。

８．「**パスワード**」入力欄に OS アカウントのパスワードを入力して「**設定をアップデート**」をクリックします。



９．「**すべての項目**」→「**自分の証明書**」を開き、「**Online Billing NW Common Root CA**」が一覧に表示されていることを確認します。
（証明書をクリックし、上部の証明書詳細に確認すべき内容が「この証明書はこのアカウントにとって信頼されているものとして指定されています」になっていることを確認します。）

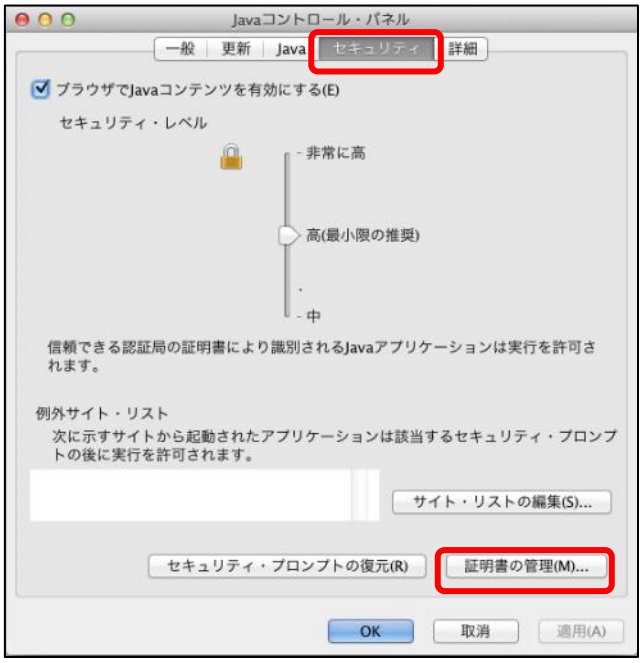
2.4. Java 実行環境に電子証明書をインポート

パソコン上にダウンロードした電子証明書を Java 実行環境にインポートします。
ここでは、Mac10.11、10.9、10.8 および 10.7 における操作手順を説明します。
Mac10.15、10.14、10.13、10.12 および 10.5 の場合、「2.5. オンライン請求システムの URL を登録」の手順へ進んでください。

1．Finder の画面に戻り、メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

2．「**アプリケーション**」画面が表示されます。
「**システム環境設定**」アイコンをダブルクリックします。

3．「**システム環境設定**」画面が表示されます。
「**Java**」アイコンをクリックします。

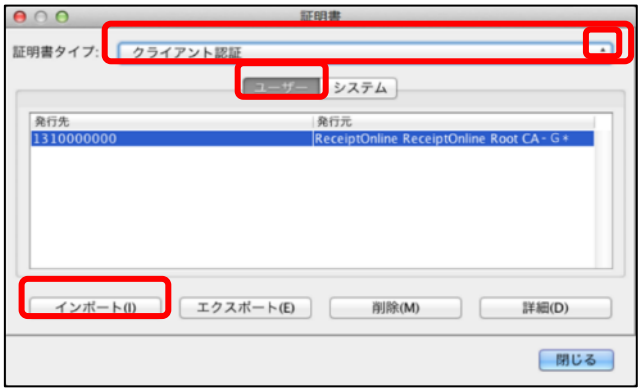


４．「**Java コントロール・パネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。
※Java のバージョンによっては、「**証明書**」ボタンと表示される場合があります。その場合は、「**証明書**」をクリックしてください。

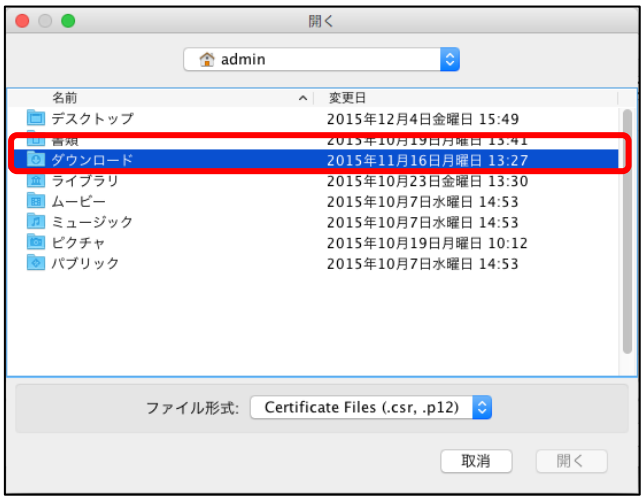
こんなときは！

Java コントロール・パネル画面が表示されない

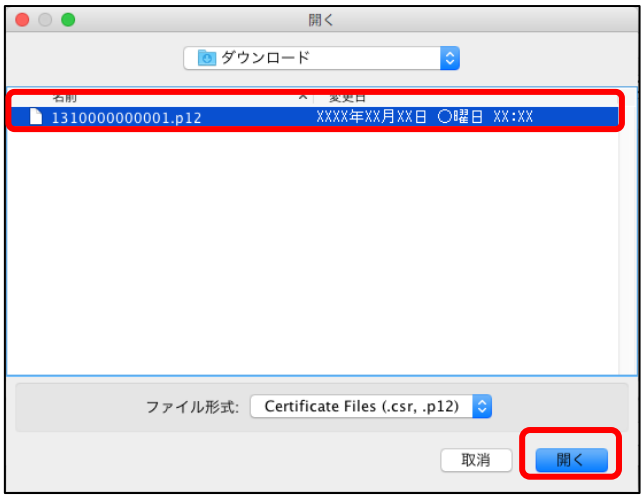
「**Java コントロール・パネルの再オープン**」をクリックしてください。



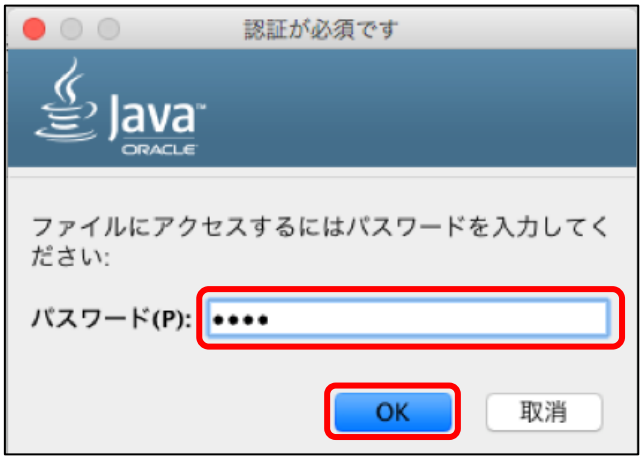
５．「**証明書**」画面が表示されます。「**証明書タイプ**」の「**▼**」をクリックし、「**クライアント認証**」を選択します。「**ユーザー**」タブを選択し、「**インポート**」をクリックします。



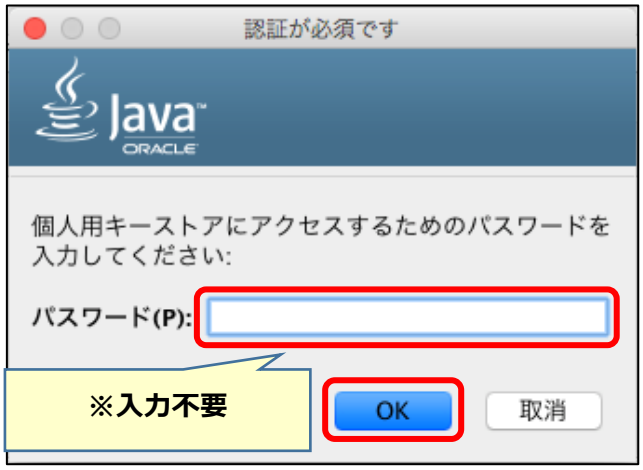
6．「**開く**」画面が表示されます。
「**ダウンロード**」をダブルクリックします。



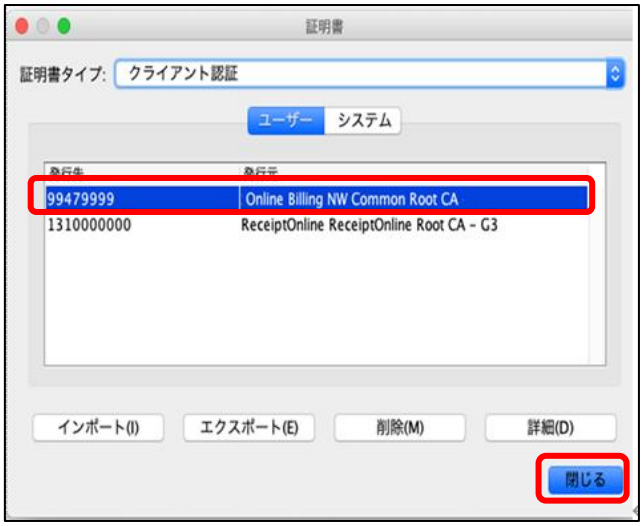
7．ダウンロードした電子証明書を選択し、
「**開く**」をクリックします。
※環境によって表示されるボタン名が異なる場合があります。「**開く**」の代わりに「**Open**」が表示された場合、「**Open**」をクリックします。



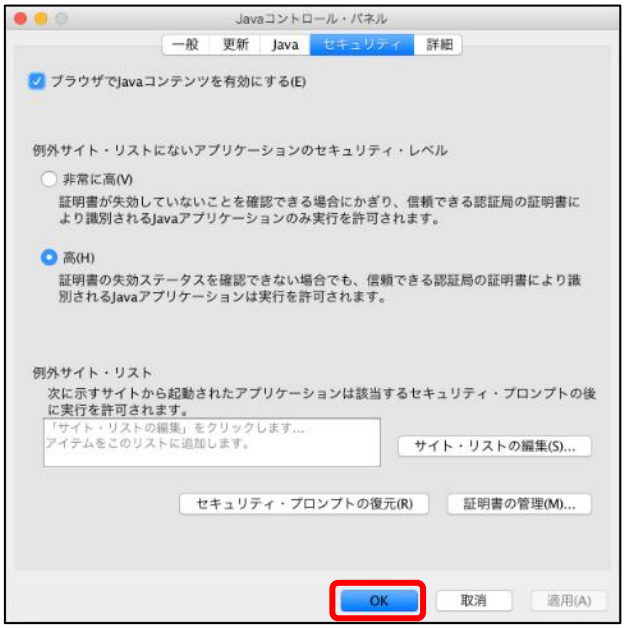
8．パスワード入力メッセージが表示されます。
「鍵の取得」画面で入力した**鍵の暗号化パスワード（任意のパスワード）**を入力して「**OK**」をクリックします。



９．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、「OK」をクリックします。

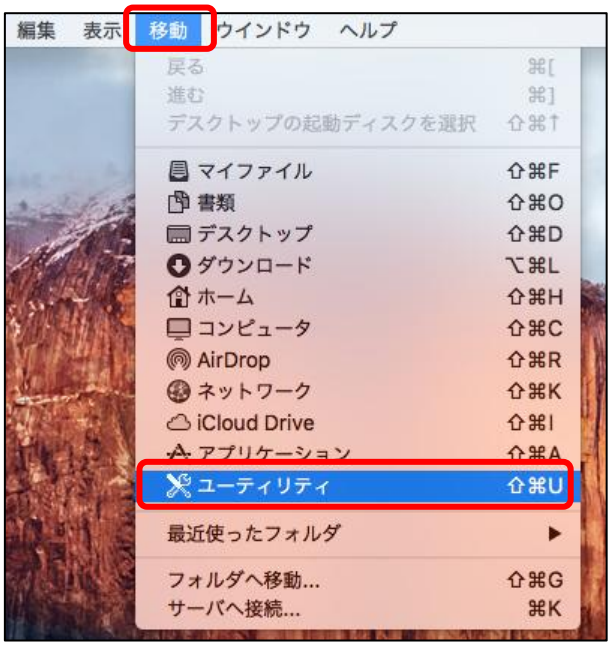


１０．「**証明書**」画面に戻ります。「**発行元**」に「Online Billing NW Common Root CA」が表示されていることを確認し、「**閉じる**」をクリックします。

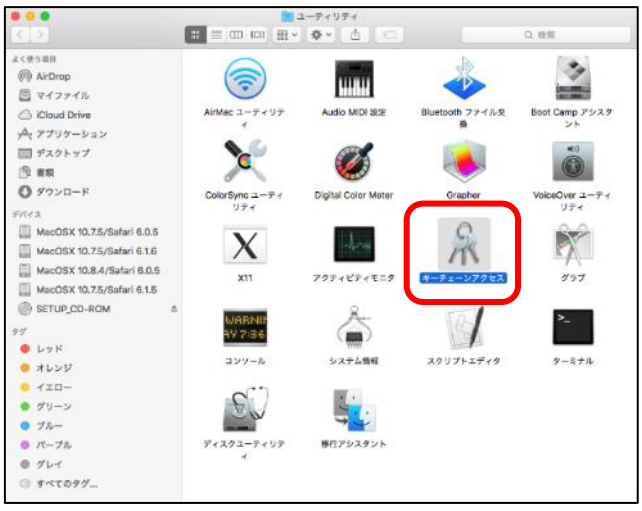


１１．「**Java コントロール・パネル**」画面に戻ります。「**OK**」をクリックします。

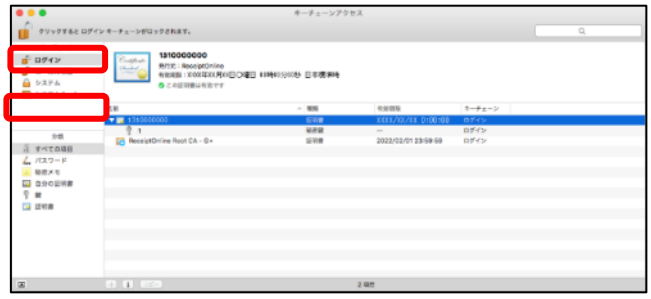
2.5. オンライン請求システムの URL を登録



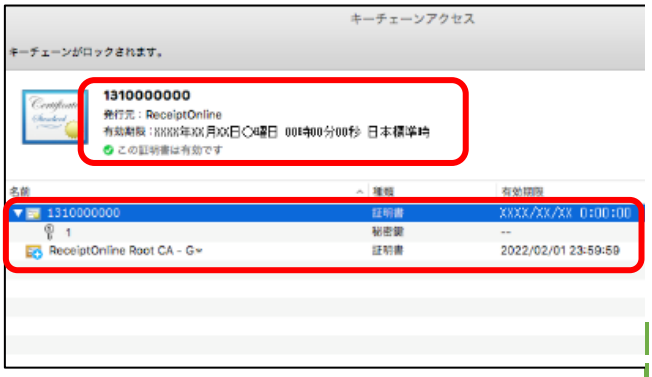
1．メニューバーから、「**移動**」-「**ユーティリティ**」の順に選択します。



2．「**ユーティリティ**」画面が表示されます。「**キーチェーンアクセス**」アイコンをダブルクリックします。



3．「**キーチェーンアクセス**」画面が表示されます。「**キーチェーン**」で「**ログイン**」を選択し、「**分類**」で「**すべての項目**」を選択します。



４．control キーを押しながら、「**名前**」と「**有効期限**」が「**電子証明書発行通知書（電子証明書取得に関する情報）**」に記載されている「**発行先**」及び「**電子証明書有効期間**」情報と同じ証明書を選択します。

【補足】

・「発行先」情報は、「都道府県番号+点数表番号+医療機関・薬局コード」の 10 桁です。
・点数表番号
　医療機関（医科）：1
　医療機関（歯科）：3
　薬局　　：4
・証明書の有効期限は、画面上部の有効期間欄に表示されている日時までとなります。
画面下部の有効期限の表示は OS に依存しているため、画面上部と異なる表示となる場合がありますが、証明書は、画面上部に表示されている有効期限までご使用いただくことができます。

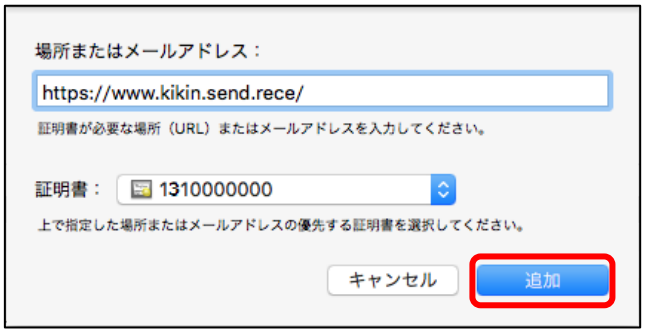
５．「**新規識別プリファレンス**」を選択します。

6．「場所またはメールアドレス：」に以下のオンライン請求システム（支払基金）の URL を入力します。

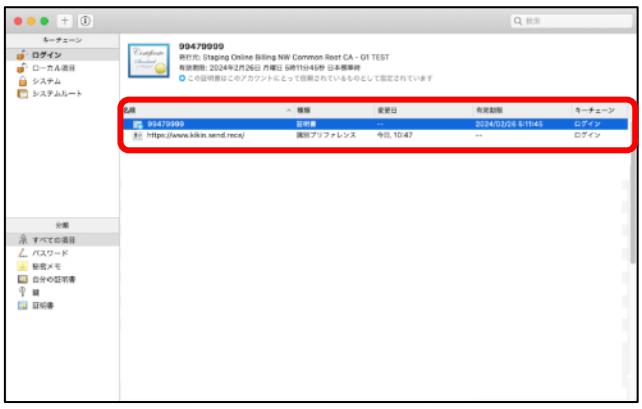
■医療機関・薬局の場合
https://www.kikin.send.rece/
（エイチ・テー・テー・ピー・エス・コロン・スラッシュ・スラッシュ・ダブリュー・ダブリュー・ダブリュー・ドット・ケイ・アイ・ケイ・アイ・エヌ・ドット・エス・イー・エヌ・デー・ドット・アール・イー・シー・イー・スラッシュ）

【注意】

URL の文字列は正確に入力し、完全に一致していることを確認してください。/（スラッシュ）まで入力する必要があります。



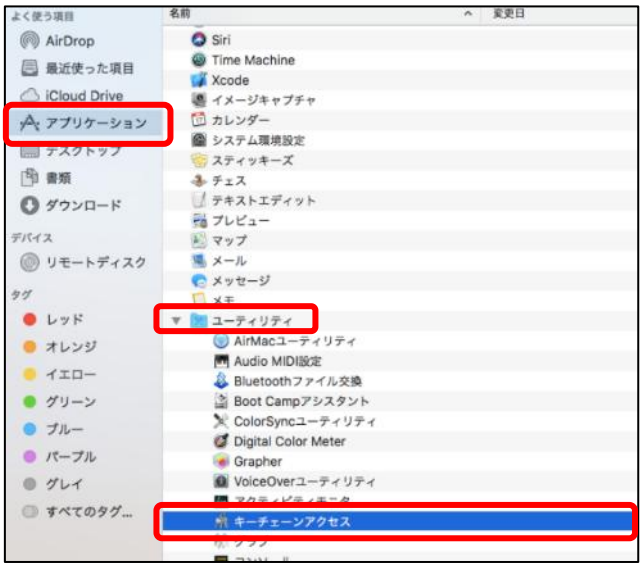
7．入力内容を確認し、「**追加**」をクリックします。



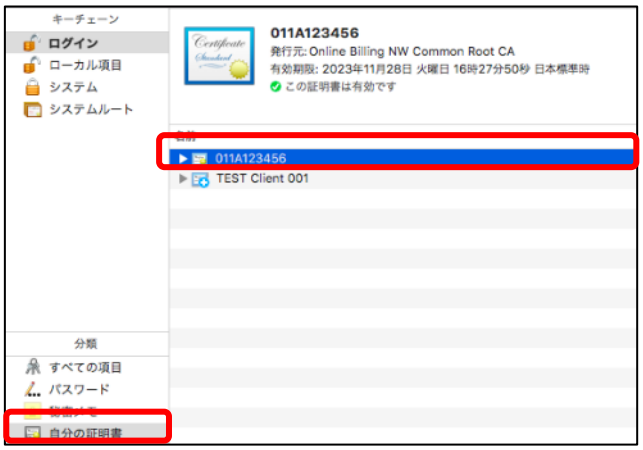
8．オンライン請求システム（支払基金）URL の識別プリファレンスの「変更日」が、「今日：変更時間」（例　今日：16:40）に更新されていることを確認します。

９．メニューバーから、「**キーチェーンアクセス**」-「**キーチェーンアクセスを終了**」の順に選択します。

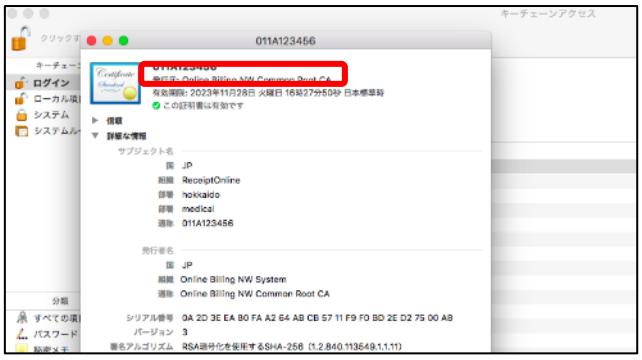
2.6.　登録した電子証明書の確認



１．Finder を起動して、「**アプリケーション**」→「**ユーティリティ**」→「**キーチェーンアクセス**」を開きます。



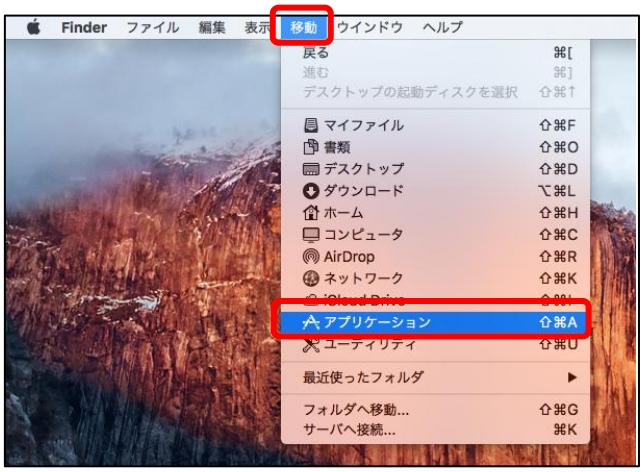
2．「**自分の証明書**」を開き、インポートされている証明書一覧を表示します。



3．証明書一覧から「**1.2.証明書のインポート**」でインポートした証明書をダブルクリックし、詳細を確認します。証明書情報ポップアップ画面が表示されます。発行元が「**Online Billing NW Common Root CA**」となっていることを確認し、「**×**」をクリックしてください。

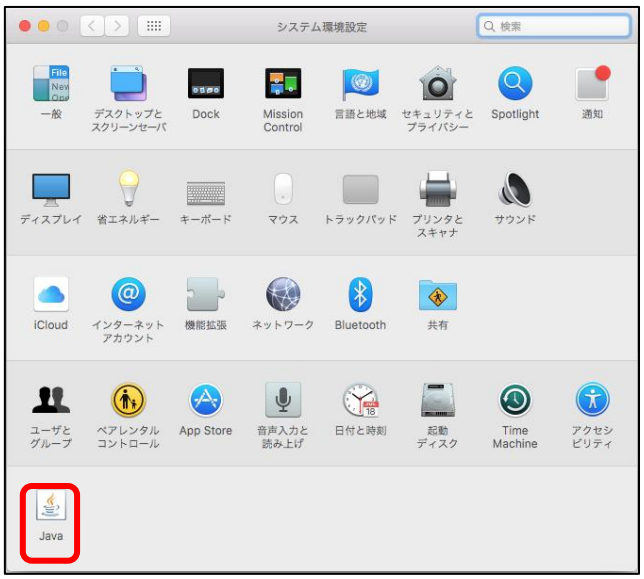
2.7.　Java 実行環境の電子証明書を確認

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．メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

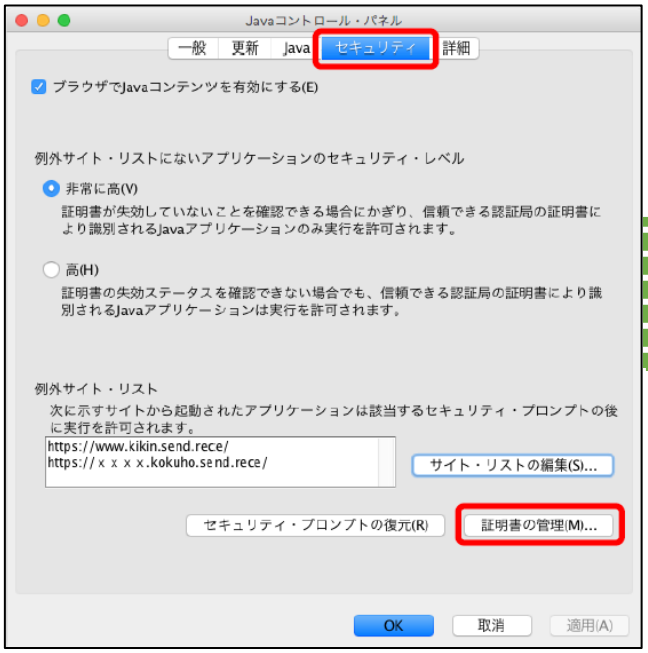
2．「アプリケーション」画面が表示されます。
「**システム環境設定**」アイコンをダブルクリックします。



3．「**システム環境設定**」画面が表示されます。「**Java**」アイコンをクリックします。

こんなときは！

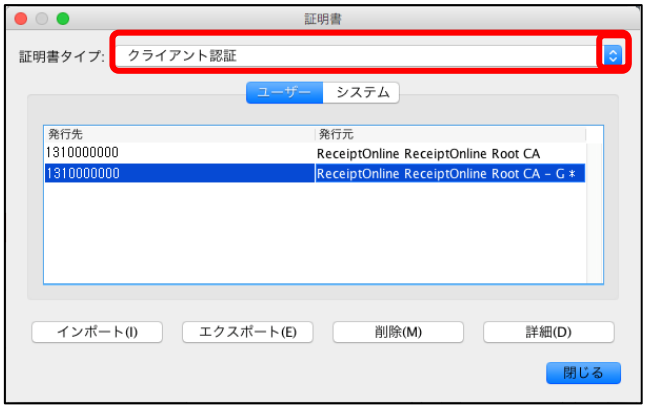
・「Java」アイコンをクリック後、「Java」画面が表示されます。
・「Java コントロール・パネル」画面が表示されない場合は、「Java コントロール・パネルの再オープン」をクリックしてください。



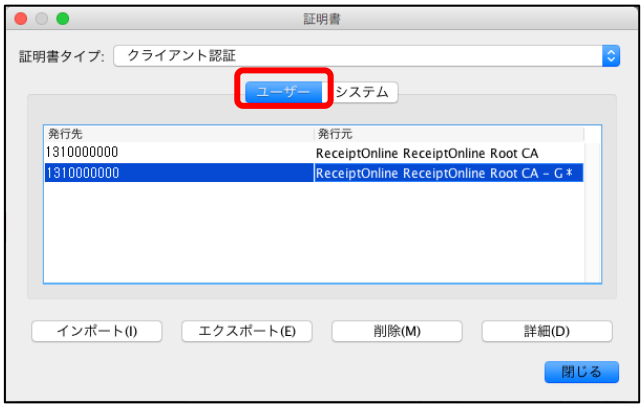
4．「Java コントロール・パネル」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。

【補足】

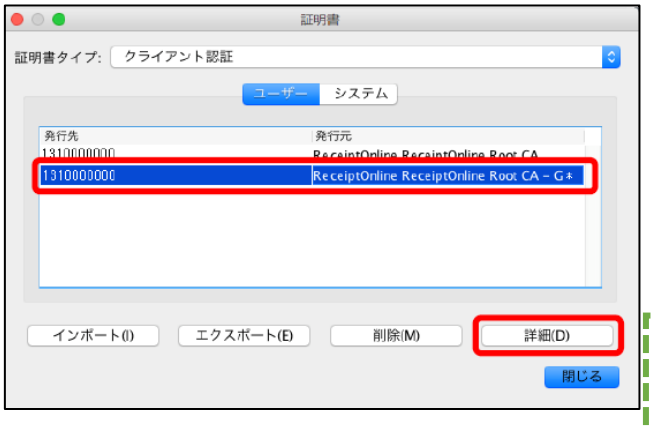
Java のバージョンによっては、「証明書」と表示される場合があります。その場合は、「証明書」をクリックしてください。



5．「**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。



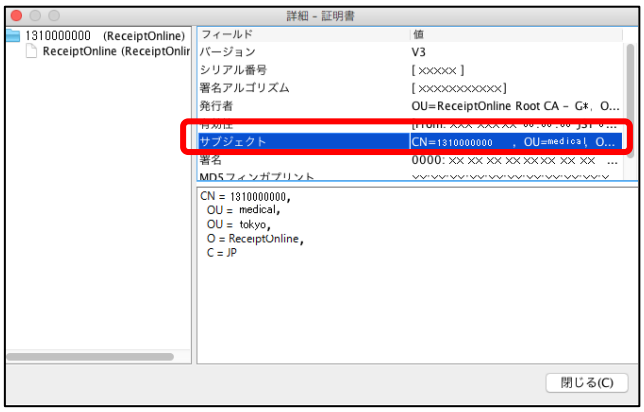
6．「**証明書**」画面が表示されます。「**ユーザー**」タブを選択します。



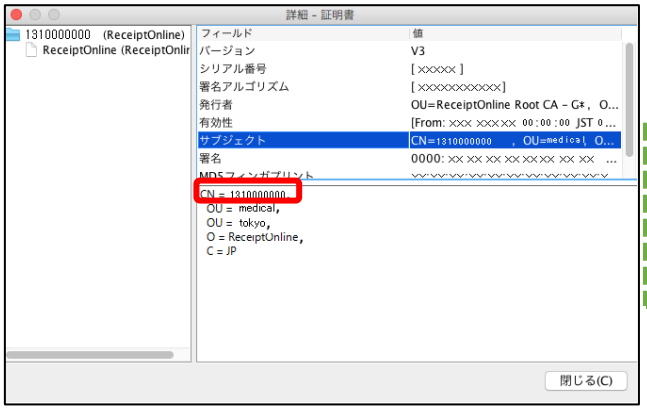
7．「**証明書**」画面が表示されます。「発行先」が「電子証明書更新のご案内（電子証明書取得に関する情報）」に記載されている「発行先」と同じ証明書を選択し、「**詳細(D)**」をクリックします。

【補足】

「発行先」情報は、「都道府県番号+点数表番号+医療機関コード」の10 桁、または10 桁の健診・保健指導機関コードです。
点数表番号
・医療機関（医科）：1
・医療機関（歯科）：3
・薬局　　：4



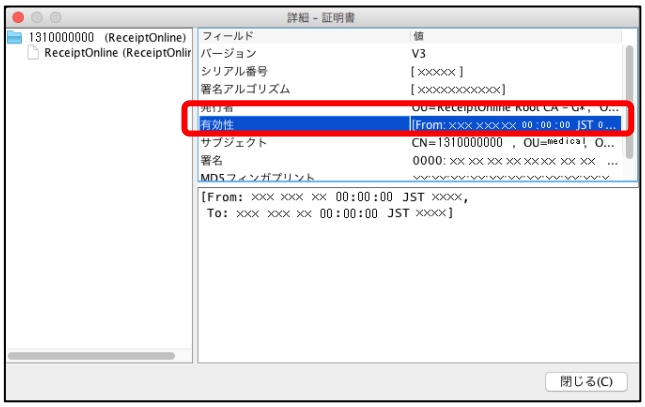
8．「**詳細-証明書**」画面が表示されます。フィールド列の「**サブジェクト**」の行を選択します。



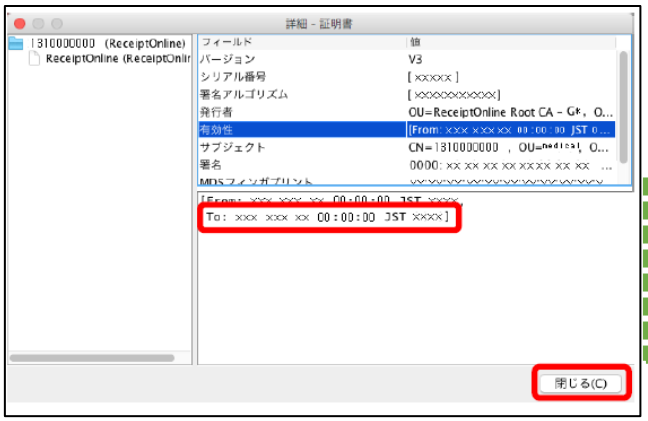
9．表示された以下の内容を確認します。

【補足】

「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。



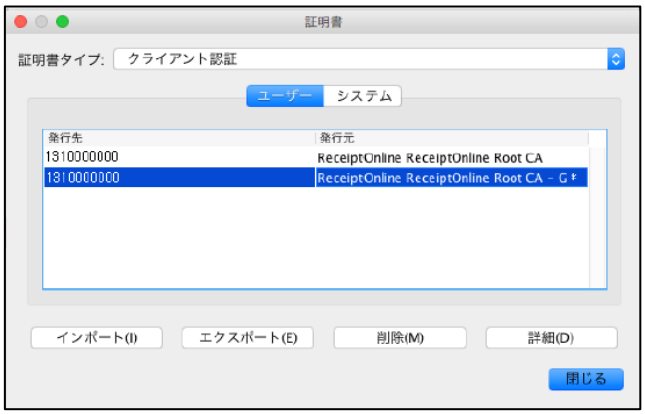
１０．フィールド列の「**有効性**」の行を選択します。



１１．表示された以下の内容を確認し、「**閉じる(C)**」をクリックします。

【補足】

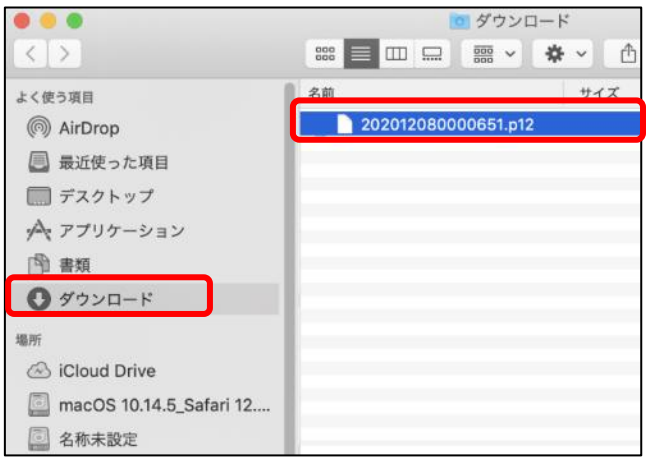
「電子証明書更新のご案内（電子証明書取得に関する情報）」に記載されている「電子証明書有効期限」情報と、「To:」の右側に表示されている年月日が一致していることを確認してください。



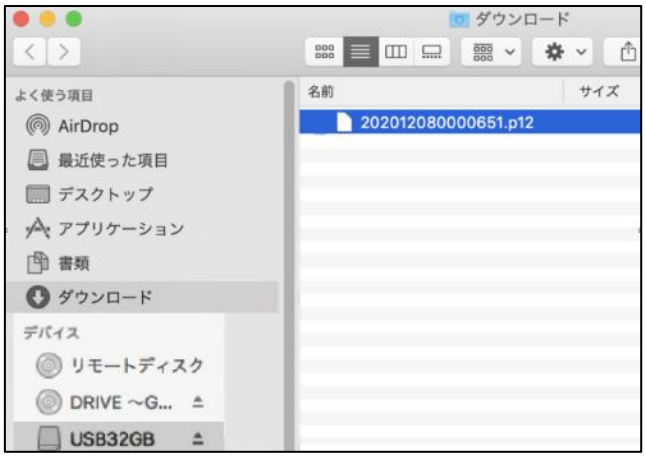
１２．「**証明書**」画面が表示されます。以上で電子証明書の確認は終了です。

2.8.　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、忘れないように保管ください。



1．インポートした証明書が**「ダウンロードフォルダ」**に入っていることを確認し、インストールを行った証明書ファイルを選択し**Command キー**を押しながら外部記録媒体等へドラッグ＆ドロップします。



2．外部記録媒体等を開いてバックアップが確実に実施されたことを確認します。

【注意】

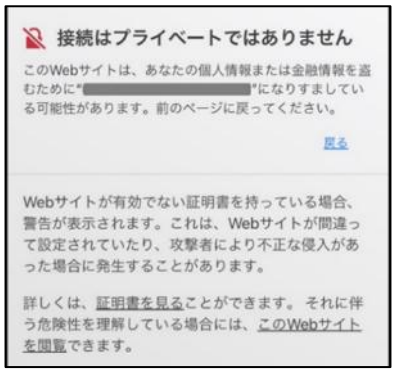
「電子証明書」「電子証明書発行通知書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理してください。これら 3 つの情報が第三者に渡ると、電子証明書が不正に使用される恐れがあります。

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。



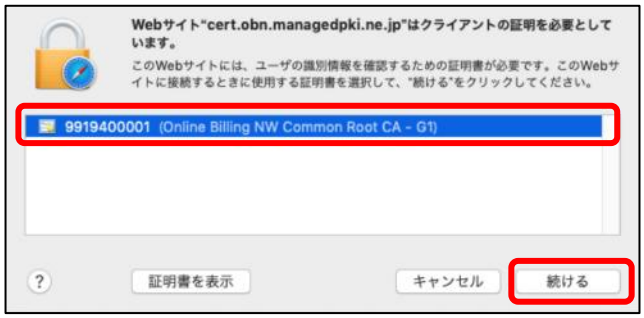
1．**更新対象の証明書がインポートされた端末**からオンライン請求ネットワークに接続して更新申請画面へアクセスします。

【証明書更新申請サイト】

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

【こんなときは！】

証明書の更新申請サイトを開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**接続はプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「7.2.　ルート証明書のダウンロードと登録」を参照



2．電子証明書の選択画面が出てきたら、更新対象となる証明書を選択し、「**続ける**」をクリックします。

3．パスワードに OS アカウントのログインパスワードを入力して「**許可**」をクリックしてください。

4．「**証明書更新申請**」をクリックします。

5．「**Submit**」をクリックします。

６．「**送信完了**」画面の「**証明書ステータス**」が「**発行済み**」となれば電子証明書が発行されます。

「**証明書ステータス**」は、「**鍵生成中**」→「**発行要求中**」→「**発行済み**」と遷移します。

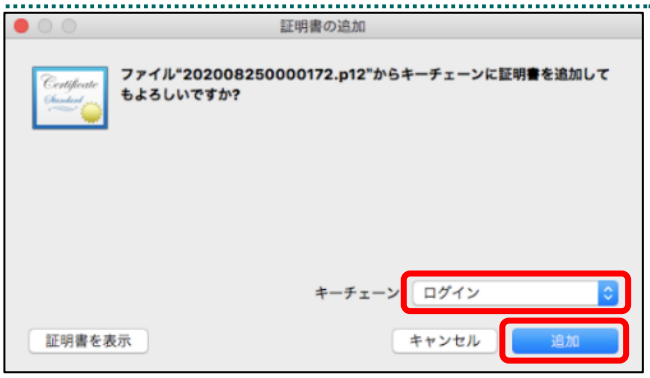
７．「鍵の取得」画面に遷移後、「**パスワード**」に**鍵の暗号化パスワード（任意のパスワード）半角数字４桁以上**を入力し、「**Submit**」をクリックします。

【注意】

入力した証明書パスワードは、「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「１１．」及び「3.2. Java 実行環境に電子証明書をインポート」の「８．」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。**

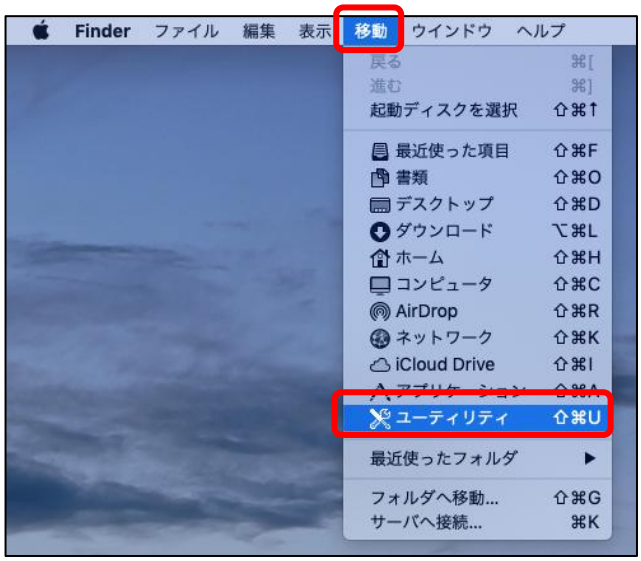
８．「**Download**」をクリックし、証明書を保存します。

９．「**ダウンロード**」フォルダを開き、ダウンロードした証明書をダブルクリックします。

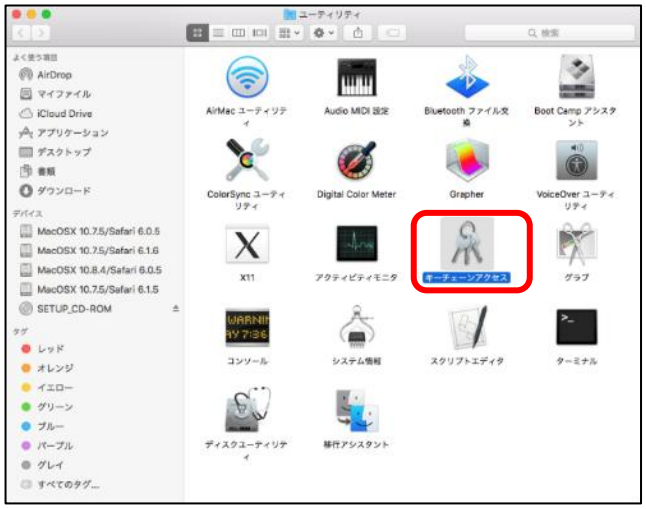


１０．「**証明書の追加**」画面が表示された場合は、キーチェーンに「**ログイン**」を選択し、「**追加**」をクリックします。

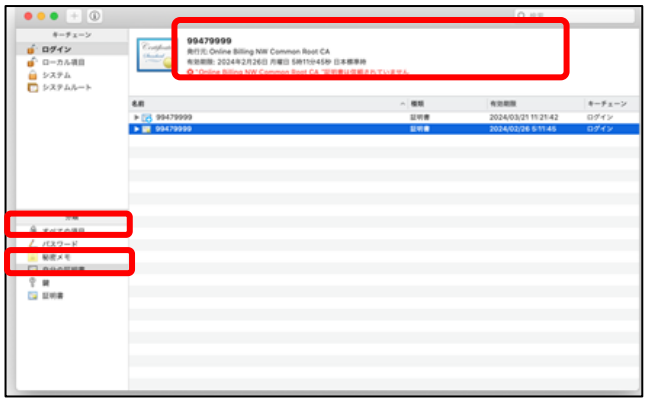
１１．「**鍵の取得**」画面で入力した**鍵の暗号化パスワード**（任意のパスワード）を入力して「OK」をクリックします。



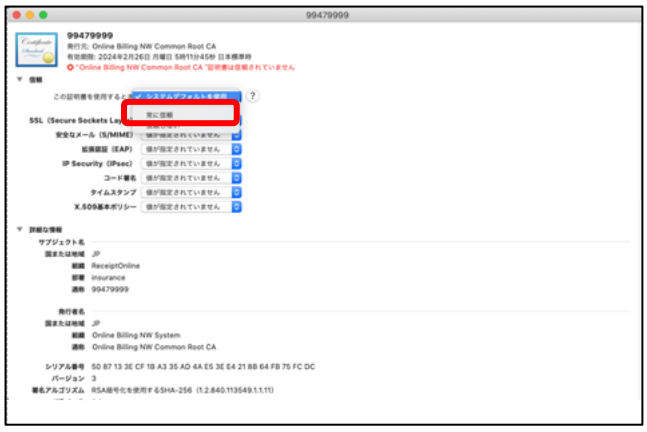
１２．Finder のメニューバーから「**移動**」-「**ユーティリティ**」の順に選択します。



１３．「**ユーティリティ**」画面が表示されます。
「**キーチェーンアクセス**」アイコンをダブルクリックします。

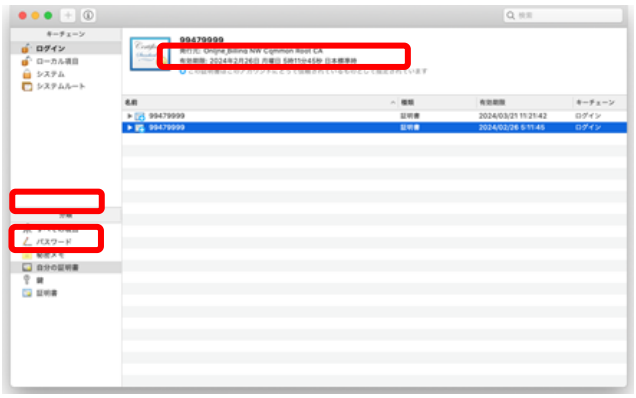


１４．「**すべての項目**」→「**自分の証明書**」を開き、発行元が「Online Billing NW Common Root CA」と表記されている証明書をダブルクリックします。



１５．「＞信頼」から信頼タブを開いて「**この証明書を使用するとき**」のプルダウンをクリックし、「**常に信頼**」を選択します。パソコンログイン時のパスワードを入力する画面がポップアップされます。

１６．**「パスワード」**入力欄に OS アカウントのパスワードを入力して**「設定をアップデート」**をクリックします。



１７．**「すべての項目」**→**「自分の証明書」**を開き、**「Online Billing NW Common Root CA」**が一覧に表示されていることを確認します。（証明書をクリックし、上部の証明書詳細に確認すべき内容が「この証明書はこのアカウントにとって信頼されているものとして指定されています」になっ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。

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。

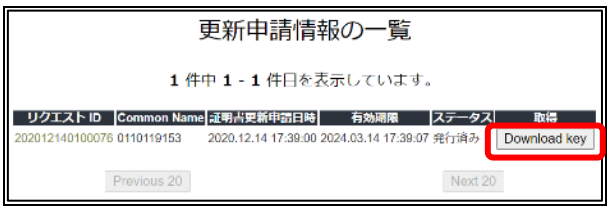
注意	必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

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

【電子証明書更新申請サイト】

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

2．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。

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。

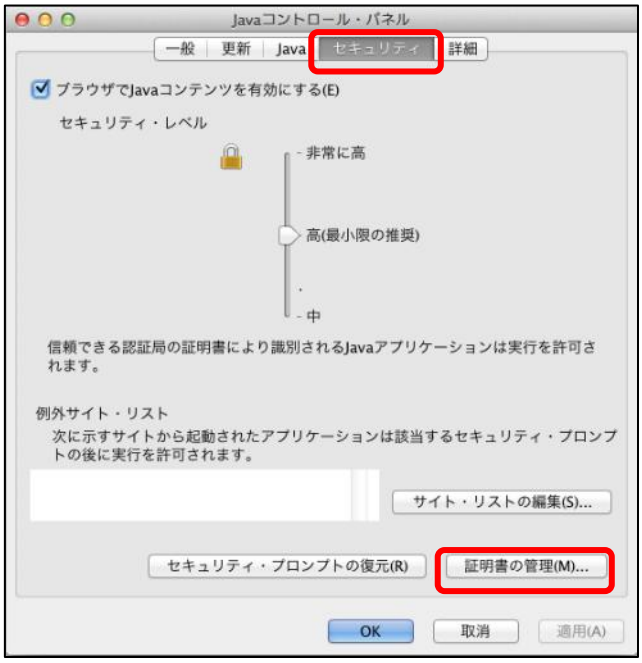
3.2. Java 実行環境に電子証明書をインポート

パソコン上にダウンロードした電子証明書を Java 実行環境にインポートします。
ここでは、Mac10.11、10.9、10.8 および 10.7 における操作手順を説明します。
Mac10.15、10.14、10.13、10.12 および 10.5 の場合、「3.3. オンライン請求システムの URL を登録」の手順へ進んでください。

1．Finder の画面に戻り、メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

2．「**アプリケーション**」画面が表示されます。
「**システム環境設定**」アイコンをダブルクリックします。

3．「**システム環境設定**」画面が表示されます。
「**Java**」アイコンをクリックします。



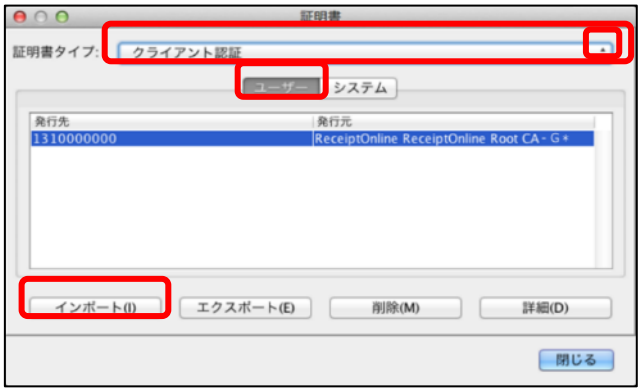
４．「**Java コントロール・パネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。

※Java のバージョンによっては、「**証明書**」ボタンと表示される場合があります。その場合は、「**証明書**」をクリックしてください。

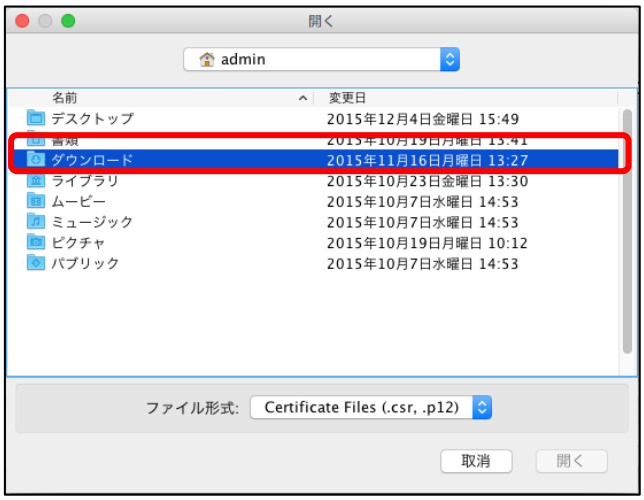
こんなときは！

Java コントロール・パネル画面が表示されない

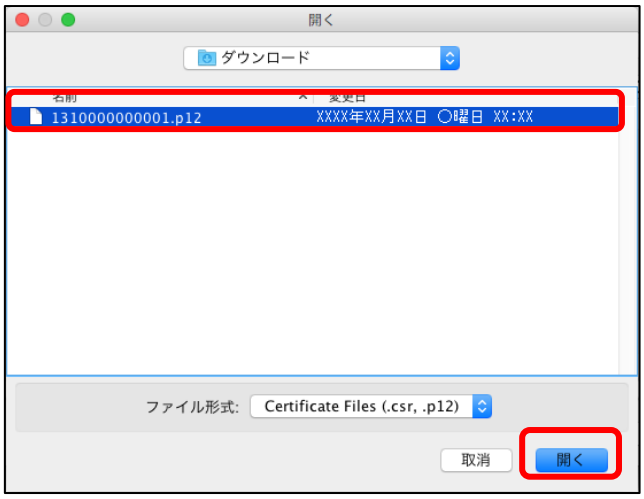
「**Java コントロール・パネルの再オープン**」をクリックしてください。



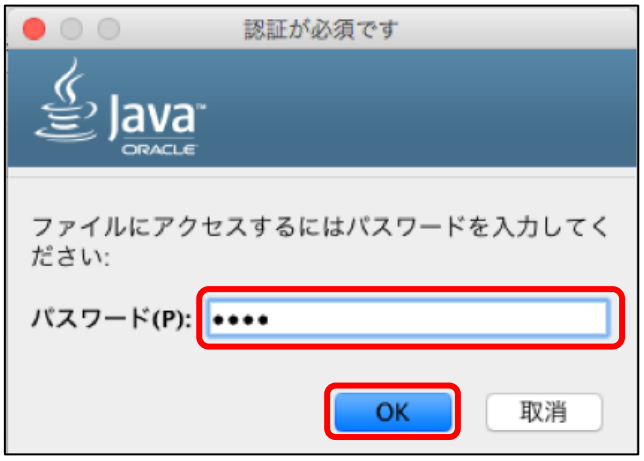
５．「**証明書**」画面が表示されます。「**証明書タイプ**」の「**▼**」をクリックし、「**クライアント認証**」を選択します。「**ユーザー**」タブを選択し、「**インポート**」をクリックします。



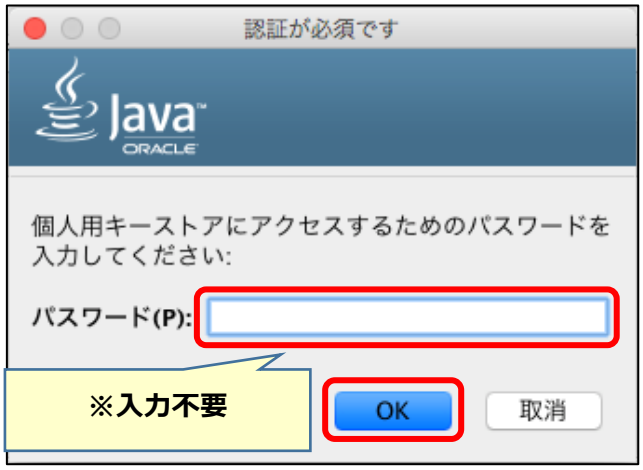
6．「**開く**」画面が表示されます。
「**ダウンロード**」をダブルクリックします。



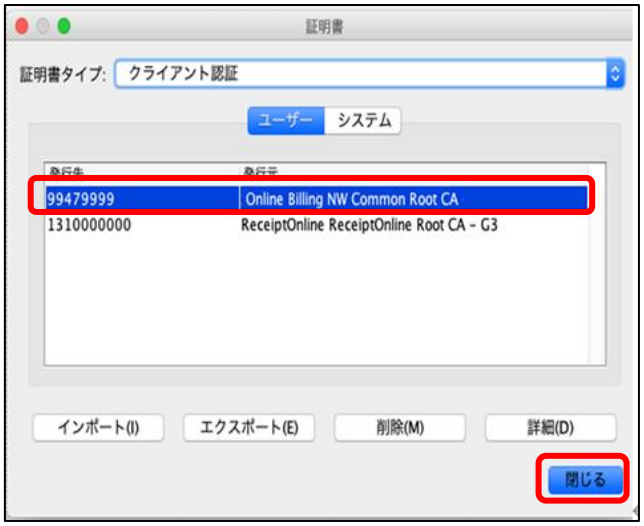
7．ダウンロードした電子証明書を選択し、
「**開く**」をクリックします。
※環境によって表示されるボタン名が異なる場合があります。「**開く**」の代わりに「**Open**」が表示された場合、「**Open**」をクリックします。



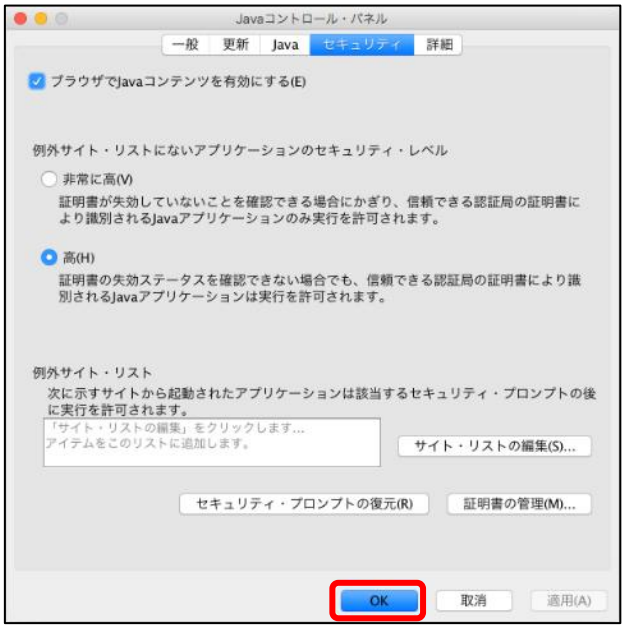
8．パスワード入力メッセージが表示されます。
「**鍵の取得**」画面で入力した「**鍵の暗号化パスワード（任意のパスワード)**」を入力して
「**OK**」をクリックします。



９．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、「OK」をクリックします。

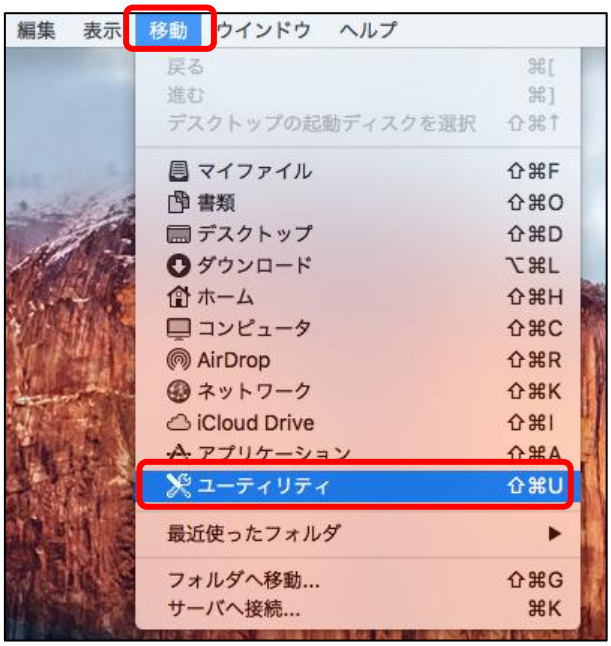


１０．「証明書」画面に戻ります。「発行元」に「Online Billing NW Common Root CA」が表示されていることを確認し、「閉じる」をクリックします。

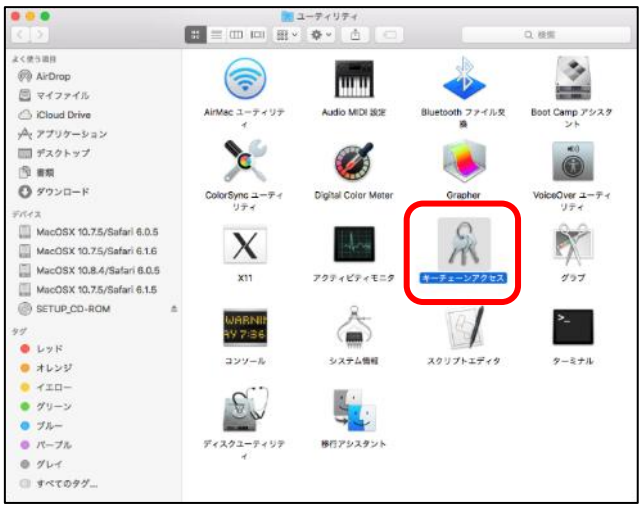


１１．「Java コントロール・パネル」画面に戻ります。「OK」をクリックします。

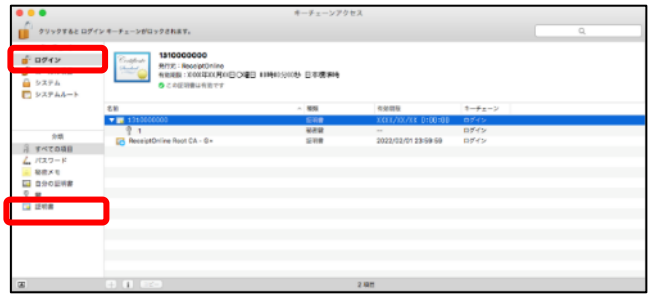
3.3. オンライン請求システムの URL を登録



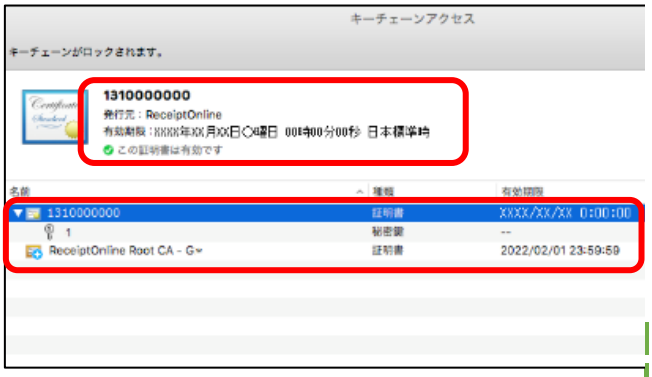
1．**メニューバー**から、「**移動**」-「**ユーティリティ**」の順に選択します。



2．「**ユーティリティ**」画面が表示されます。「**キーチェーンアクセス**」アイコンをダブルクリックします。



3．「**キーチェーンアクセス**」画面が表示されます。「**キーチェーン**」で「**ログイン**」を選択し、「**分類**」で「**すべての項目**」を選択します。



4．control キーを押しながら、「**名前**」と「**有効期限**」が「**電子証明書発行通知書（電子証明書取得に関する情報）**」に記載されている「**発行先**」及び「**電子証明書有効期間**」情報と同じ証明書を選択します。

【補足】

・「発行先」情報は、「都道府県番号+点数表番号+医療機関・薬局コード」の 10 桁です。
・点数表番号
　医療機関（医科）：1
　医療機関（歯科）：3
　薬局　　：4
・証明書の有効期限は、画面上部の有効期間欄に表示されている日時までとなります。
画面下部の有効期限の表示は OS に依存しているため、画面上部と異なる表示となる場合がありますが、証明書は、画面上部に表示されている有効期限までご使用いただくことができます。

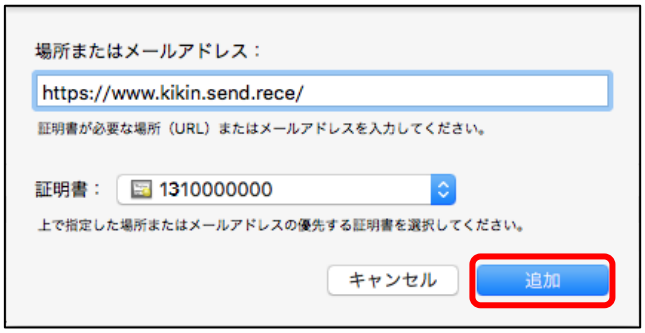
5．「**新規識別プリファレンス**」を選択します。

6．「場所またはメールアドレス：」に以下のオンライン請求システム（支払基金）の URL を入力します。

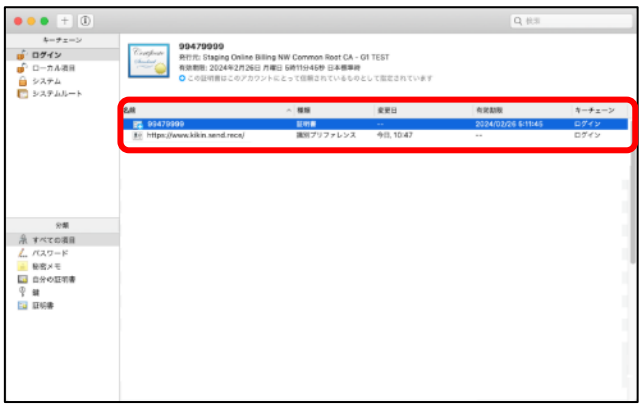
■医療機関・薬局の場合
https://www.kikin.send.rece/
（エイチ・テー・テー・ピー・エス・コロン・スラッシュ・スラッシュ・ダブリュー・ダブリュー・ダブリュー・ドット・ケイ・アイ・ケイ・アイ・エヌ・ドット・エス・イー・エヌ・デー・ドット・アール・イー・シー・イー・スラッシュ）

【注意】

URL の文字列は正確に入力し、完全に一致していることを確認してください。/（スラッシュ）まで入力する必要があります。



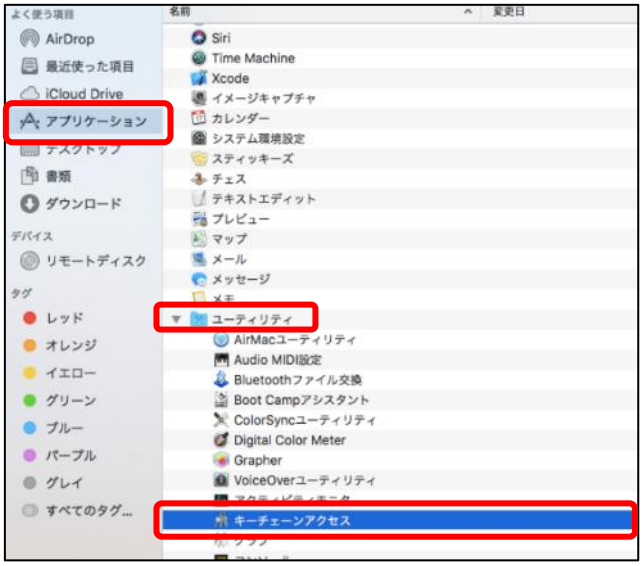
7．入力内容を確認し、「**追加**」をクリックします。



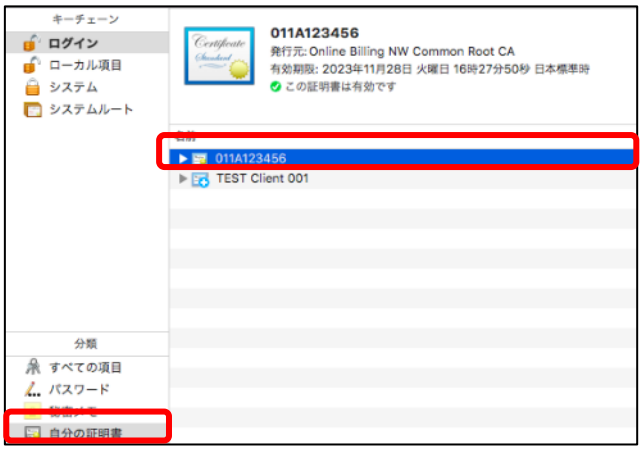
8．オンライン請求システム（支払基金）URL の識別プリファレンスの「変更日」が、「今日：変更時間」（例　今日：16:40）に更新されていることを確認します。

９．メニューバーから、「**キーチェーンアクセス**」－「**キーチェーンアクセスを終了**」の順に選択します。

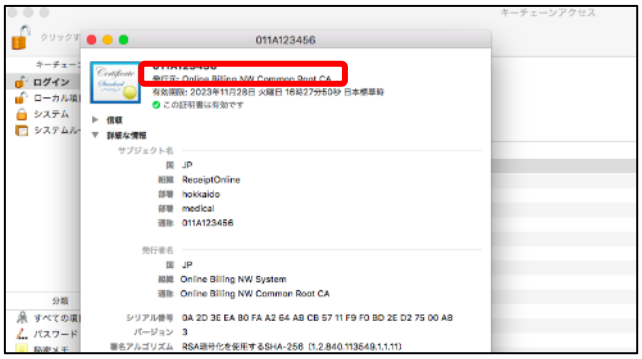
3.4.　登録した電子証明書の確認



1．Finder を起動して、「**アプリケーション**」→「**ユーティリティ**」→「**キーチェーンアクセス**」を開きます。



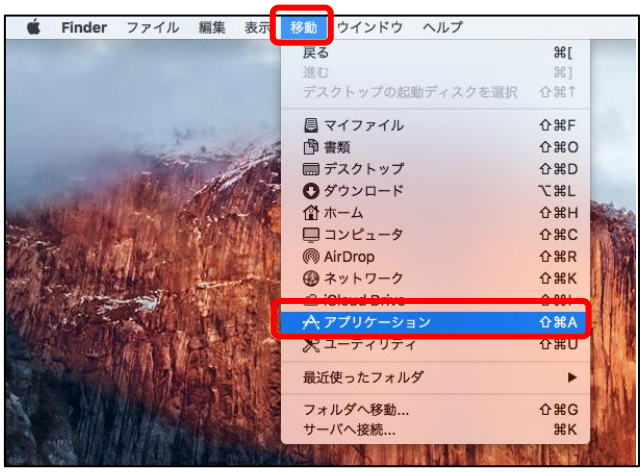
2．「**自分の証明書**」を開き、インポートされている証明書一覧を表示します。



3．証明書一覧から「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」でインポートした証明書をダブルクリックし、詳細を確認します。証明書情報ポップアップ画面が表示されます。発行元が「**Online Billing NW Common Root CA**」となっていることを確認し、「**×**」をクリックしてください。

3.5.　Java 実行環境の電子証明書を確認

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．メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

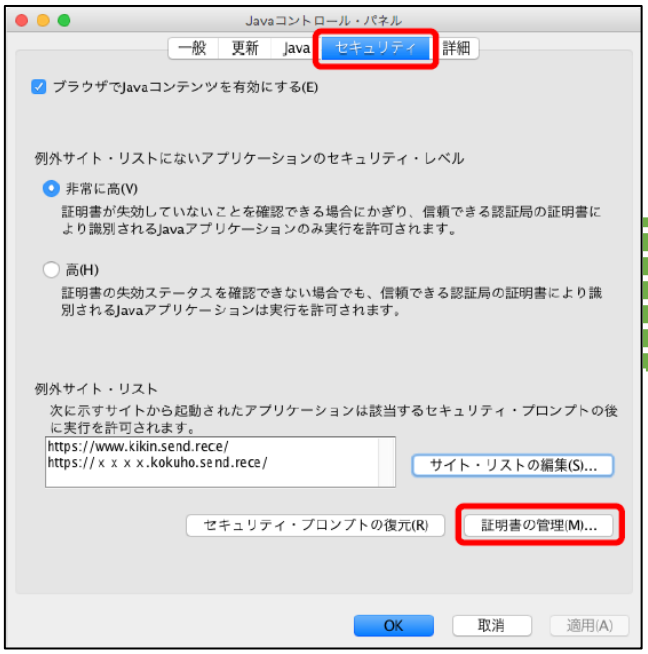
2．「**アプリケーション**」画面が表示されます。
「**システム環境設定**」アイコンをダブルクリックします。

3．「**システム環境設定**」画面が表示されます。「**Java**」アイコンをクリックします。

こんなときは！

・「Java」アイコンをクリック後、「Java」画面が表示されます。

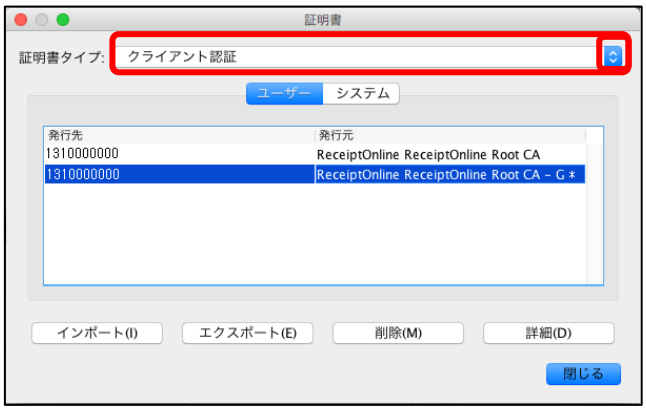
・「Java コントロール・パネル」画面が表示されない場合は、「Java コントロール・パネルの再オープン」をクリックしてください。



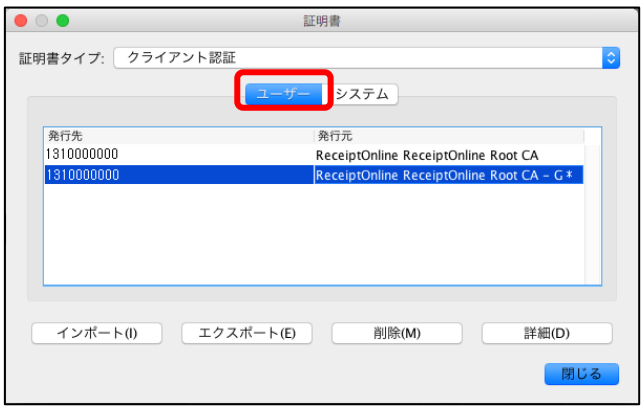
4．「Java コントロール・パネル」画面が表示されます。「セキュリティ」タブを選択し、「証明書の管理(M)」をクリックします。

【補足】

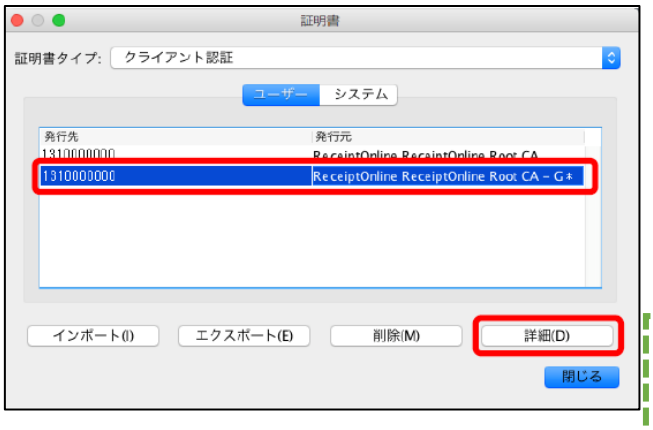
Java のバージョンによっては、「証明書」と表示される場合があります。その場合は、「証明書」をクリックしてください。



5．「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。



6．「**証明書**」画面が表示されます。「**ユーザー**」タブを選択します。



7．「**証明書**」画面が表示されます。「**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(D)**」をクリックします。

【補足】

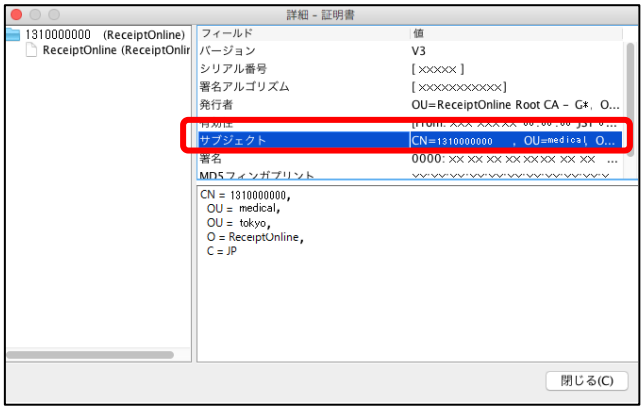
「**発行先**」情報は、「都道府県番号+点数表番号+医療機関コード」の10 桁、または10 桁の健診・保健指導機関コードです。

点数表番号

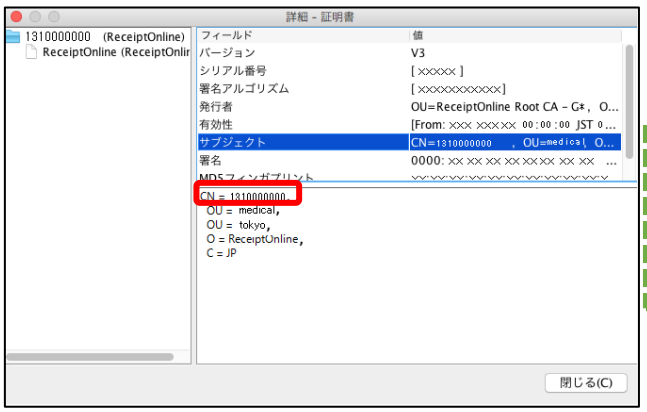
・医療機関（医科）：1

・医療機関（歯科）：3

・薬局　　：4



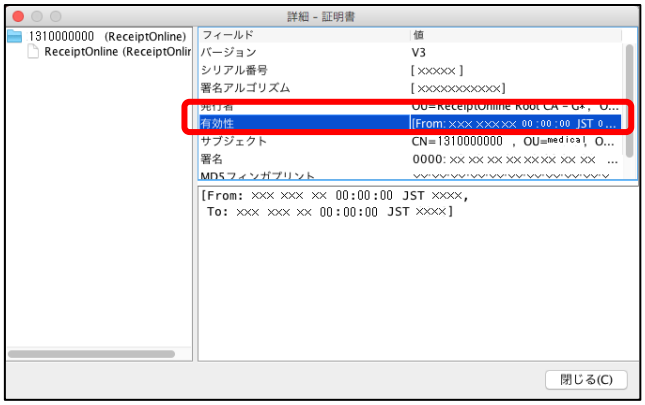
8．「**詳細-証明書**」画面が表示されます。フィールド列の「**サブジェクト**」の行を選択します。



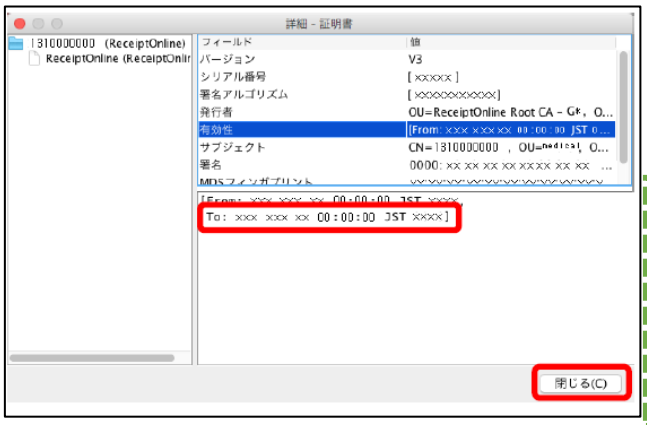
９．表示された以下の内容を確認します。

【補足】

「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。



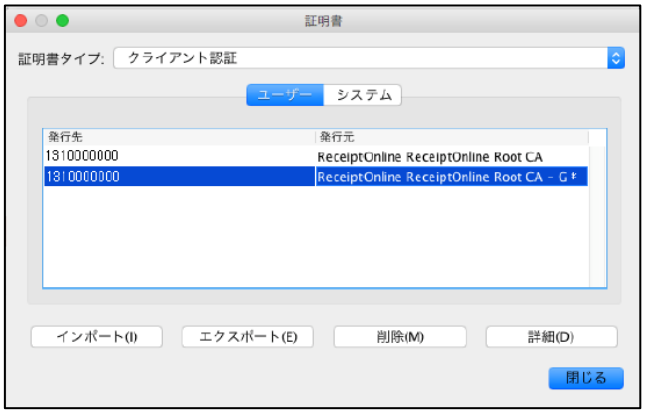
１０．フィールド列の「**有効性**」の行を選択します。



１１．表示された以下の内容を確認し、「**閉じる(C)**」をクリックします。

【補足】

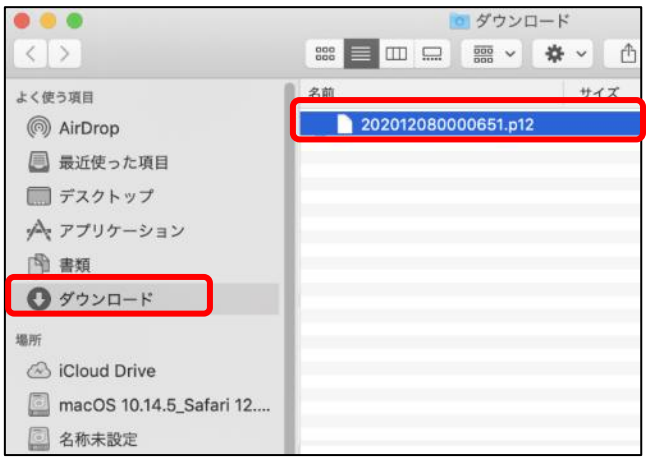
「**電子証明書更新のご案内（電子証明書取得に関する情報）**」に記載されている「**電子証明書有効期限**」情報と、「To:」の右側に表示されている年月日が一致していることを確認してください。



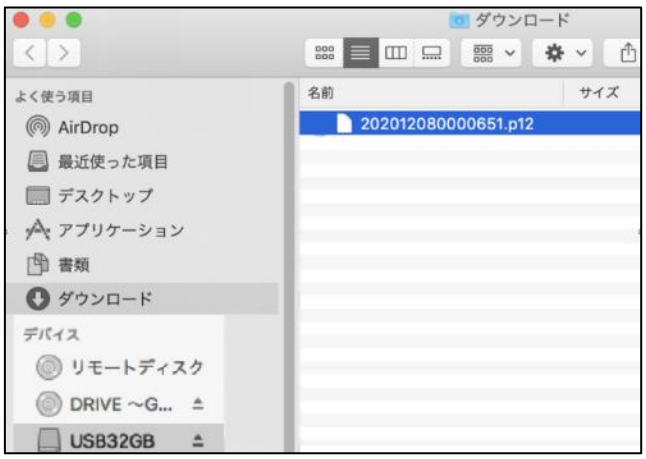
１２．「**証明書**」画面が表示されます。以上で電子証明書の確認は終了です。

3.6.　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、「**鍵の取得**」画面で入力した**鍵の暗号化パスワード（任意のパスワード）**も必要となるため、忘れないように保管ください。



１．インポートした証明書が「**ダウンロードフォルダ**」に入っていることを確認し、インストールを行った証明書ファイルを選択し**Command キー**を押しながら外部記録媒体等へドラッグ＆ドロップします。



２．外部記録媒体等を開いてバックアップが確実に実施されたことを確認します。

【注意】

「電子証明書」「鍵の取得画面で入力した証明書パスワード」は厳重に管理してください。これら 2 つの情報が第三者に渡ると、電子証明書が不正に使用される恐れがあります。

3.7. 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。

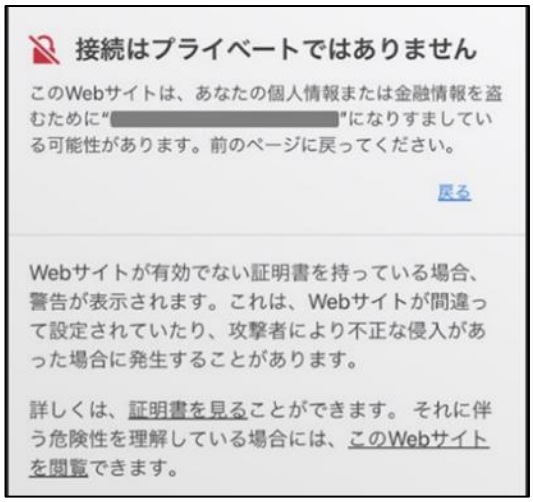
失効手続き後は、失効申請の取消しはできませんので、

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。**



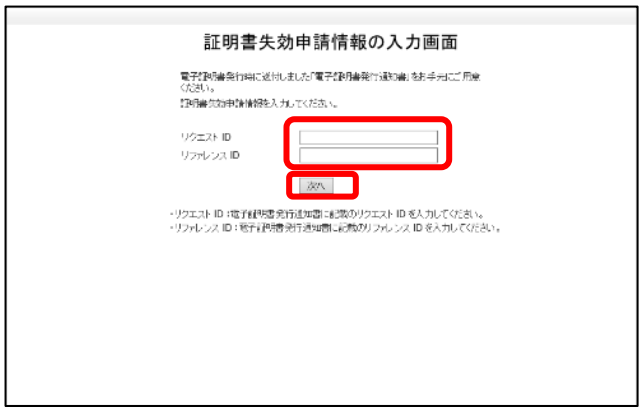
1．**失効対象の証明書がインストールされた端末**からオンライン請求ネットワークに接続して失効申請画面へアクセスします。

【証明書失効申請サイト】

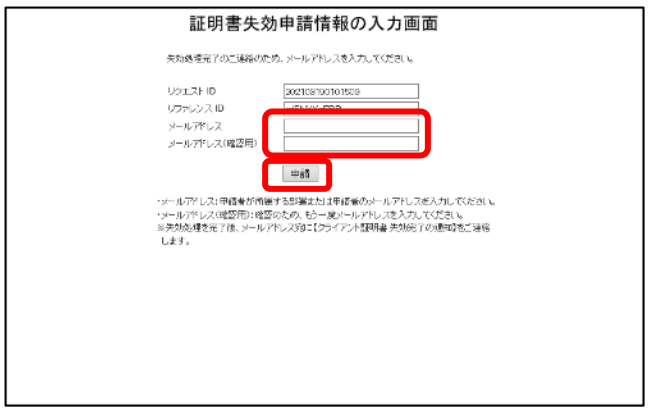
https://cert.obn.managedpki.ne.jp/p/rx

【こんなときは！】

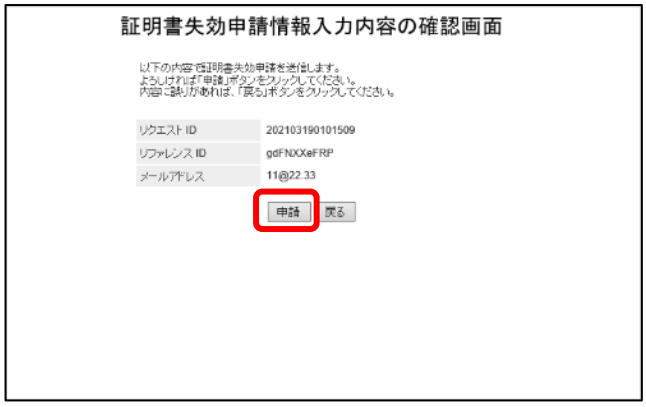
証明書の失効画面を開く時、ブラウザの画面に「**お使いの PC は Web サイトのセキュリティ証明書を信頼しません**」または「**接続はプライベートではありません**」と表示される場合は、ルート証明書のインストールが必要であるため、「7.2.　ルート証明書のダウンロードと登録」を参照



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．「**証明書失効申請情報入力内容の確認画面**」が表示されます。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。

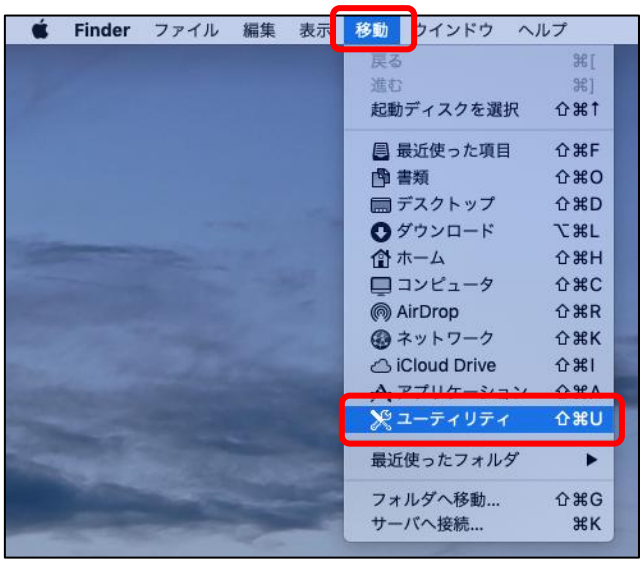
注意	上記の操作が終了したら、必ずすべてのブラウザを閉じて下さい。

4.2.　電子証明書の削除

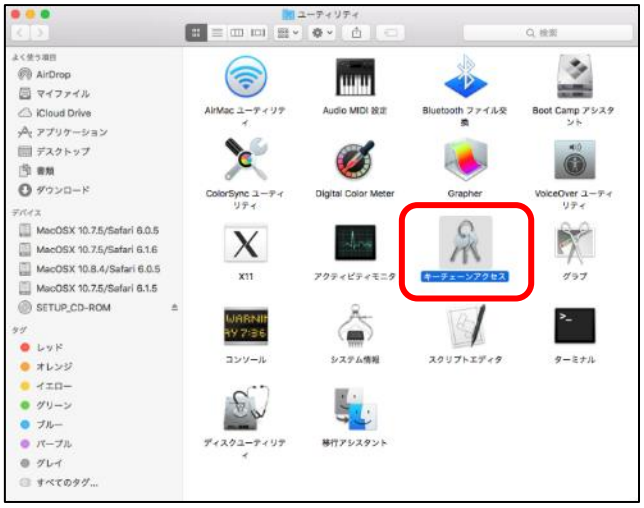
失効申請の後、共通認証局において失効処理が完了すると「【クライアント証明書 失効完了の通知】」の通知メールを受信後、「5. 電子証明書の削除」及び「6. Java 実行環境の電子証明書を削除」の手順に従い該当の電子証明書の削除を行ってください。
なお、失効処理が完了するまで数日間要する場合があります。

電子証明書の失効手続きの作業はこれで終了です。

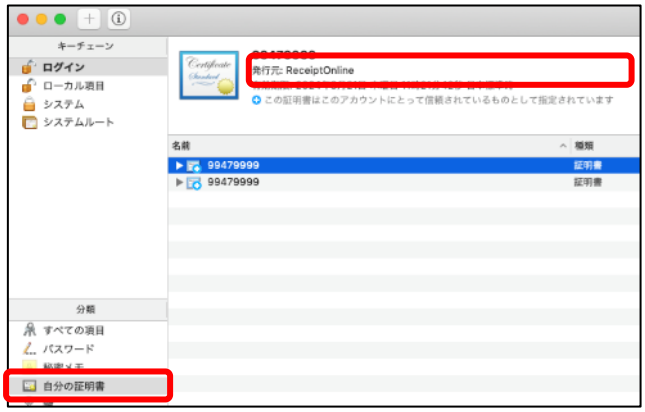
5. 電子証明書の削除



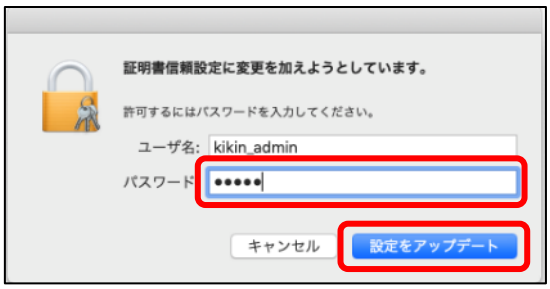
1．メニューバーから、「**移動**」→「**ユーティリティ**」を開きます。



2．「**ユーティリティ**」画面が表示されます。「**キーチェーンアクセス**」アイコンをダブルクリックします。



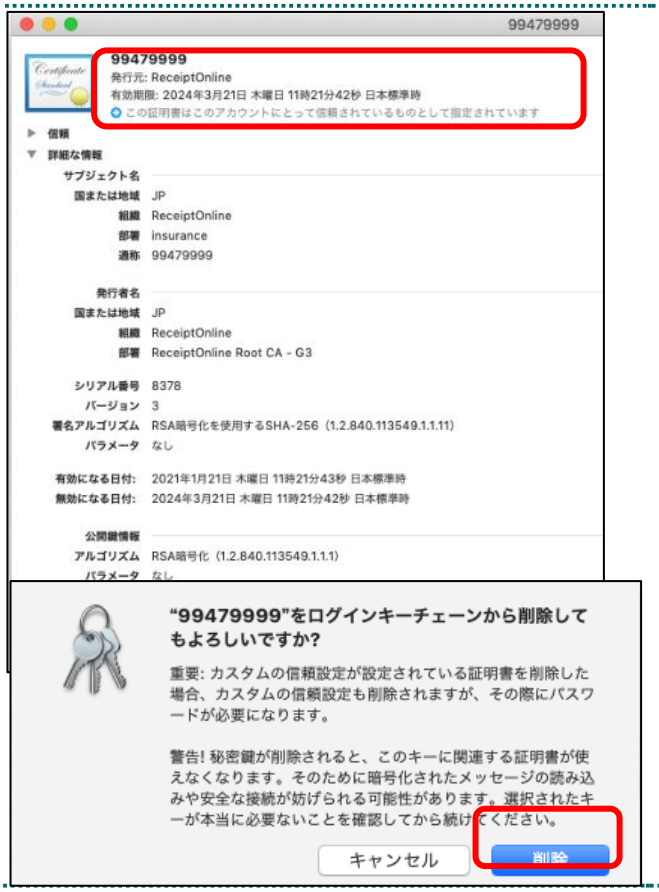
3．「**自分の証明書**」を開き、「**有効期限**」の日付が古い証明書をダブルクリックします。



こんなときは！

パスワードを求められたときは

パスワード入力欄にパソコンログイン時のパスワードを入力し、「**設定をアップデート**」をクリックします。



4．「**有効期限**」の日付が古いことを確認し、キーボード上の「**Del**」を押下します。「**削除**」をクリックします。

6. Java 実行環境の電子証明書を削除

1．メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

2．「**アプリケーション**」画面が表示されます。

「**システム環境設定**」アイコンをダブルクリックします。

3．「**システム環境設定**」画面が表示されます。

「**Java**」アイコンをクリックします。

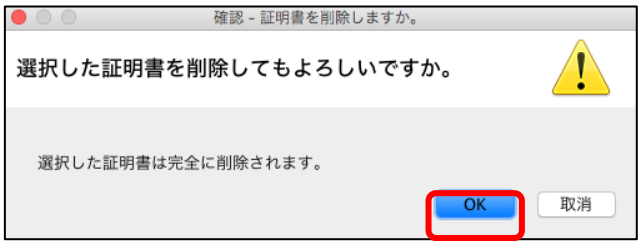
４．「**Java コントロール・パネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。
※Java のバージョンによっては、「**証明書**」と表示される場合があります。その場合は、「**証明書**」をクリックしてください。

こんなときは！

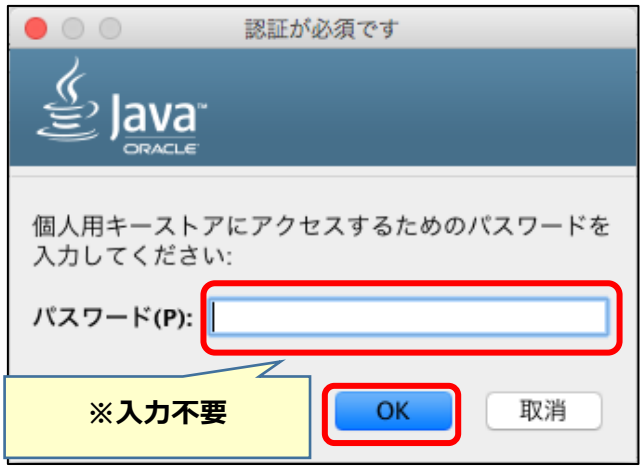
Java コントロール・パネル画面が表示されない

「**Java コントロール・パネルの再オープン**」をクリックしてください。

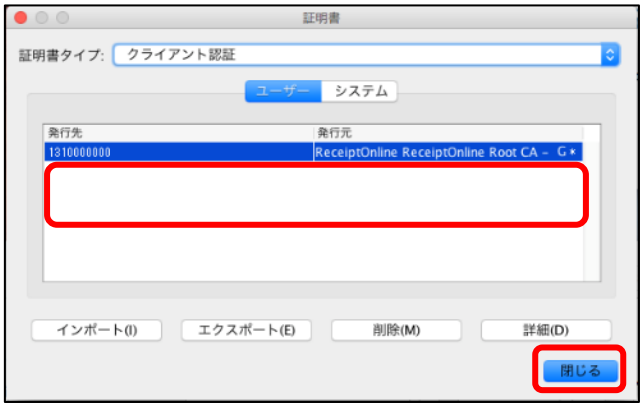
５．「**証明書**」画面が表示されます。「**証明書タイプ**」の「▼」をクリックし、「**クライアント認証**」を選択し、「**ユーザー**」タブをクリックします。
有効期限の古い証明書が選択されていることを確認し、「**削除(M)**」をクリックします。



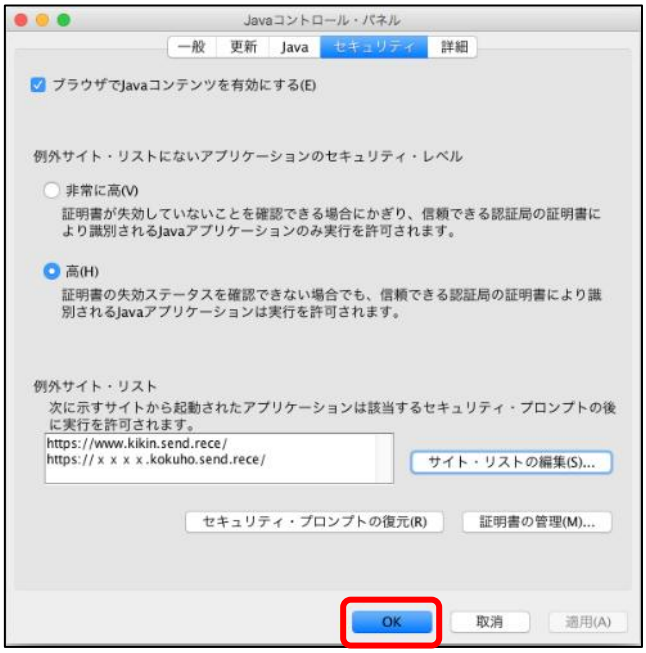
6．証明書削除確認メッセージが表示されます。
「OK」をクリックします。



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「OK」をクリックします。



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

7.　サポート情報

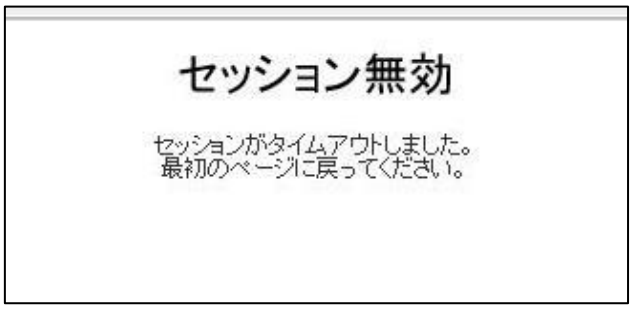
7.1.　ご利用にあたっての注意事項

7.1.1.　認証用の電子証明書の選択画面が表示された場合

１．「証明書の選択」画面で発行者が「Online Billing NW Common Root CA」となっていることを確認し、「**続ける**」をクリックしてください。

２．「証明書の選択」画面で「発行者：Online Billing NW Common Root CA 」となっていない場合には、「認証用の証明書の選択」画面から、「Online Billing NW Common Root CA 」をクリック（青反転することを確認）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ー用 URL へアクセスし直してください。

7.2.　ルート証明書のダウンロードと登録

7.2.1.　ルート証明書のダウンロード

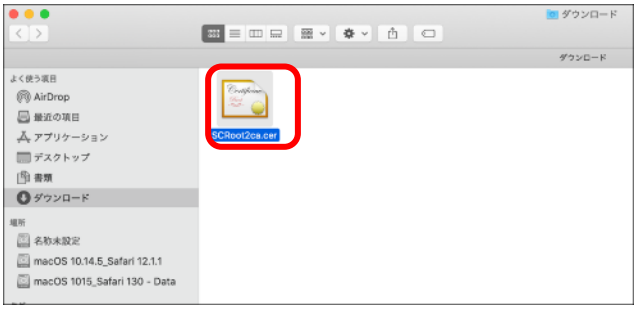
注意　必ずすべてのブラウザを閉じてから、手続きを実施して下さい。

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

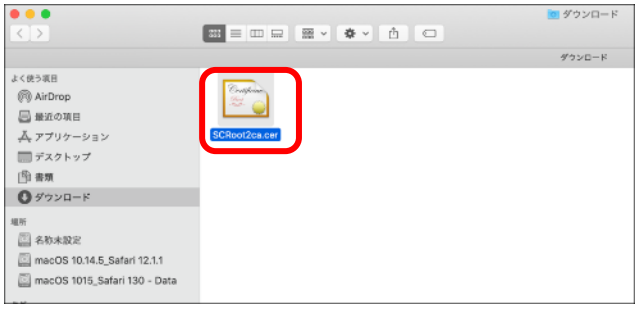
2．ポップアップ画面から「**許可**」をクリックします。



3．ルート証明書がダウンロードできていることを確認します。

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.　ルート証明書の登録

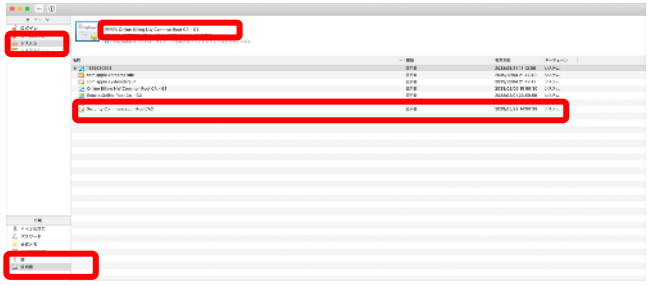


4．ルート証明書が「**ダウンロード**」フォルダに入っていることを確認し、「SCRoot2ca.cer」ファイルを選択し**ダブルクリック**します。

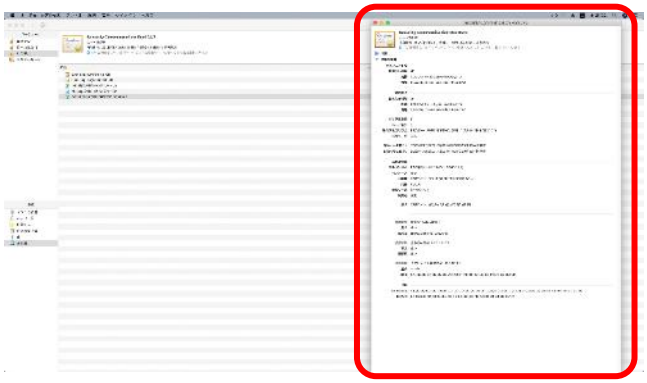
こんなときは！

パスワードを求められたときは

５．パスワード入力欄にパソコンログイン時のパスワードを入力し、「**キーチェーンを変更**」をクリックします。



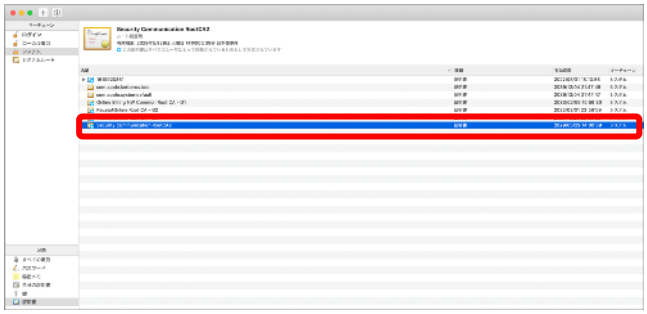
６．「**システム**」→「**証明書**」を開き、発行元が「Security Communication RootCA2」と表記されている証明書をダブルクリックします。



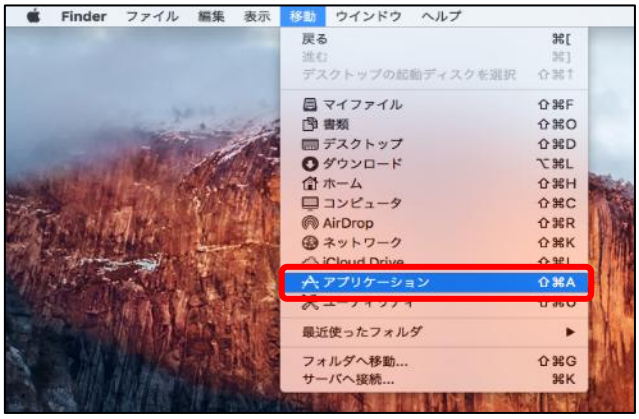
７．証明書情報ポップアップ画面が表示されます。発行元が「Security Communication RootCA2」となっていることを確認します。信頼の「▼」をクリックします。

「**この証明書を使用するとき：**」を「**常に信頼**」にし、「×」をクリックします。

８．パスワード入力欄にパソコンログイン時のパスワードを入力して「**設定をアップデート**」をクリックします。



９．「**システム**」→「**証明書**」を開き、「**Security Communication RootCA2**」が一覧に表示されていることを確認します。
（証明書をクリックし、上部の証明書詳細に確認すべき内容が「**この証明書はこのアカウントにとって信頼されているものとして指定されています**」になっていることを確認します。）



１０．　メニューバーから、「**移動**」-「**アプリケーション**」の順に選択します。

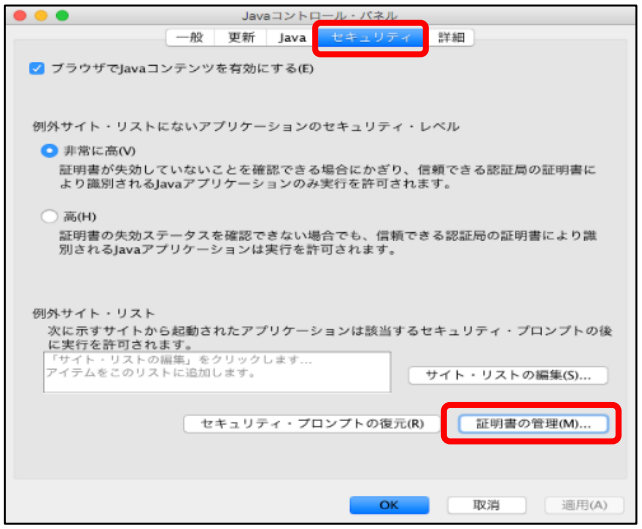
１１．「**アプリケーション**」画面が表示されます。
「**システム環境設定**」アイコンをダブルクリックします。

１２．「**システム環境設定**」画面が表示されます。「**Java**」アイコンをクリックします。

こんなときは！

１３．「**Java**」アイコンをクリック後、「**Java**」 画面が表示されます。

・「**Java コントロール・パネル**」画面が表示されない場合は、「**Java コントロール・パネルの再オープン**」をクリックしてください。

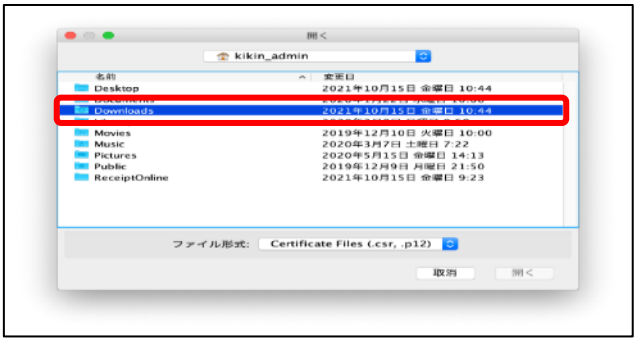


１４．「**Java コントロール・パネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。

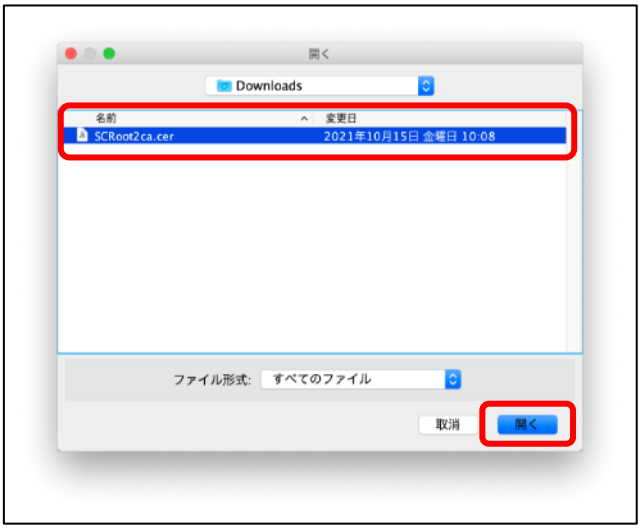
【補足】

Java のバージョンによっては、「**証明書**」と表示される場合があります。その場合は、「**証明書**」をクリックしてください。

１５．「**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、「**署名者のCA**」を選択します。「**ユーザー**」→証明書一覧から、「ReceiptOnline ReceiptOnline Root CA -G2 」をクリック（青反転することを確認）し、「**インポート(I)**」をクリックしてください。



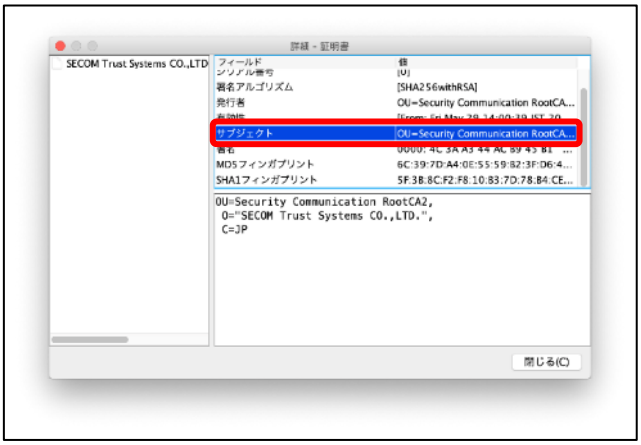
１６．「**開く**」画面が表示されます。
「**ダウンロード**」をダブルクリックします。



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

※環境によって表示されるボタン名が異なる場合があります。「**開く**」の代わりに「Open」が表示された場合、「Open」をクリックします。

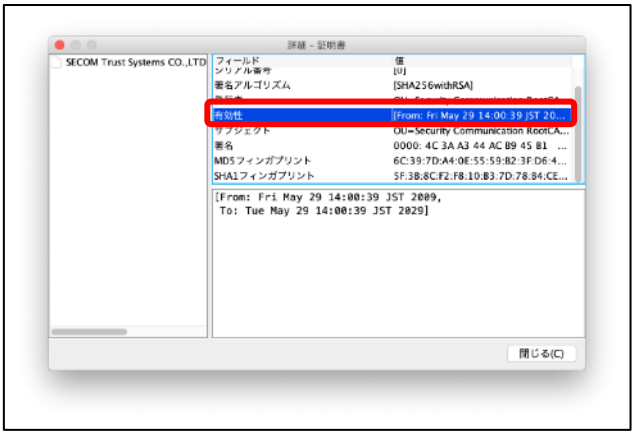
１８．「**証明書**」画面が表示されます。「**発行先**」が「Security Communication RootCA2」に記載されている「**発行先**」と同じ証明書を選択し、「**詳細(D)**」をクリックします。



１９．「**詳細-証明書**」画面が表示されます。フィールド列の「**サブジェクト**」の行を選択します。表示された以下の内容を確認します。

【補足】

「Security Communication RootCA2」に記載されている「**発行先**」情報が一致していることを確認してください。

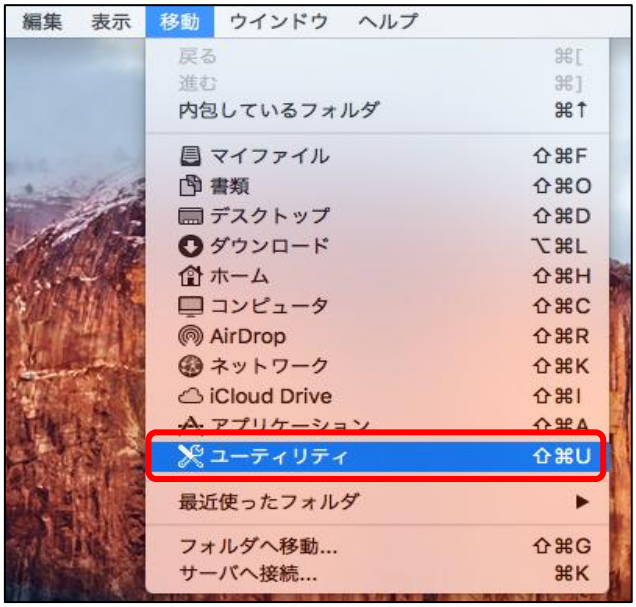


２０．フィールド列の「**有効性**」の行を選択します。表示された以下の内容を確認し、「**閉じる**」をクリックします。

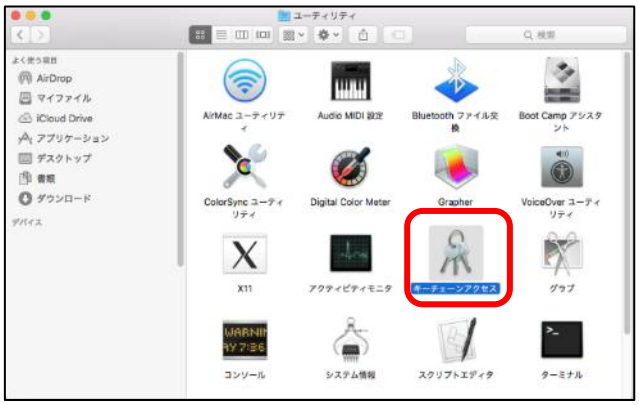
【補足】

「Security Communication RootCA2」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。

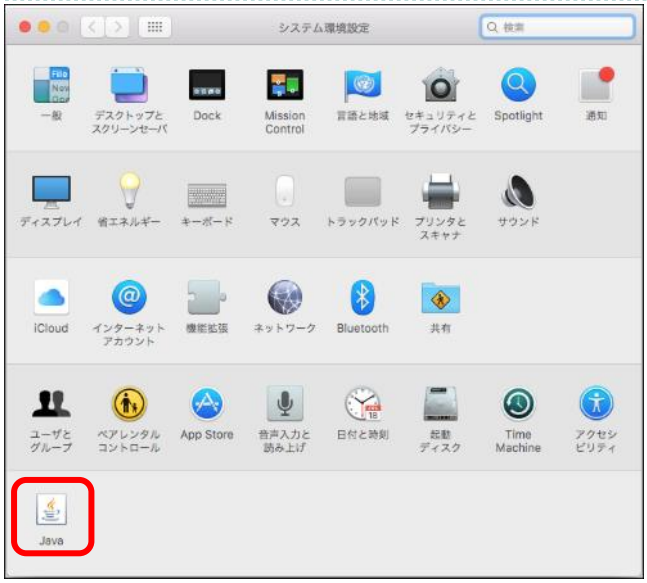
7.2.3. 登録したルート証明書の確認



１．メニューバーから、「**移動**」-「**ユーティリティ**」の順に選択します。



2．「**ユーティリティ**」画面が表示されます。「**キーチェーンアクセス**」アイコンをダブルクリックします。

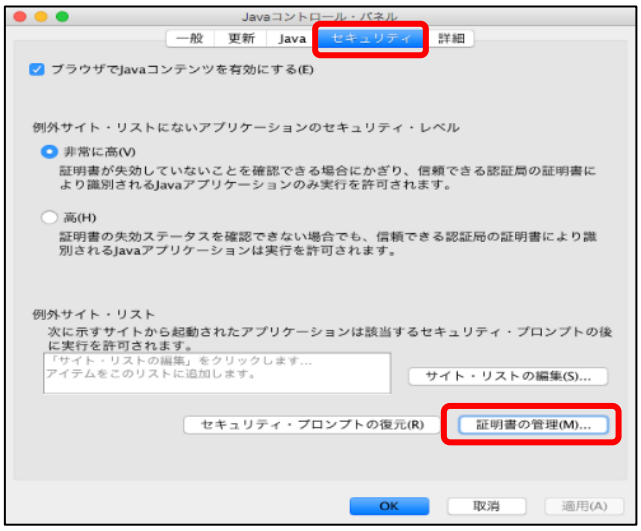


3．「**システム環境設定**」画面が表示されます。「**Java**」アイコンをクリックします。

こんなときは！

4．「**Java**」アイコンをクリック後、「**Java**」画面が表示されます。

・「**Java コントロール・パネル**」画面が表示されない場合は、「**Java コントロール・パネルの再オープン**」をクリックしてください。

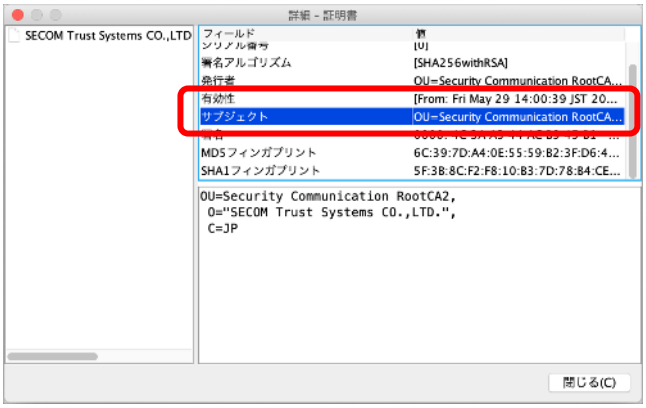


５．「**Java コントロール・パネル**」画面が表示されます。「**セキュリティ**」タブを選択し、「**証明書の管理(M)**」をクリックします。

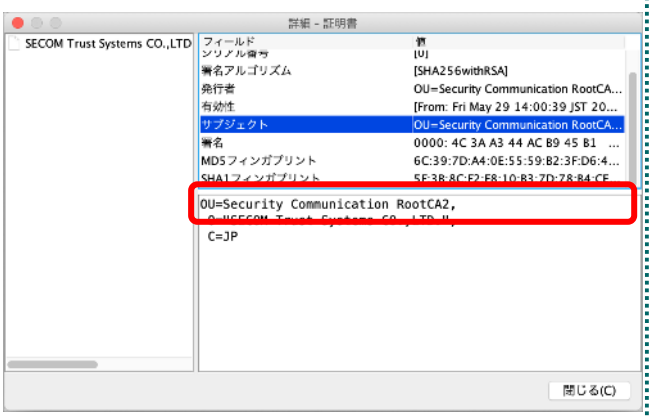
【補足】

Java のバージョンによっては、「**証明書**」と表示される場合があります。その場合は、「**証明書**」をクリックしてください。

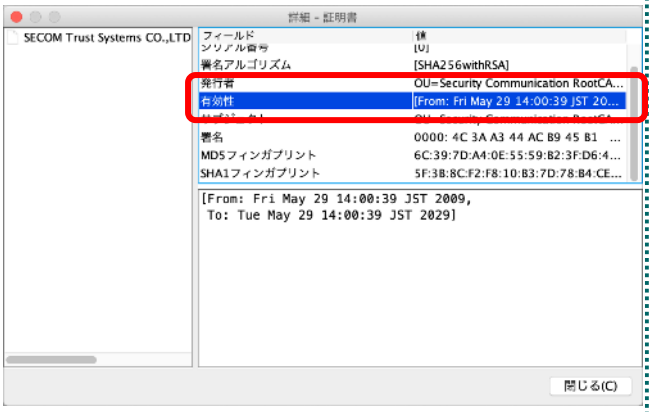
６．「**証明書**」画面が表示されます。「**発行先**」と「**発行元**」が同じであることを確認し、「**詳細(D)**」をクリックします。



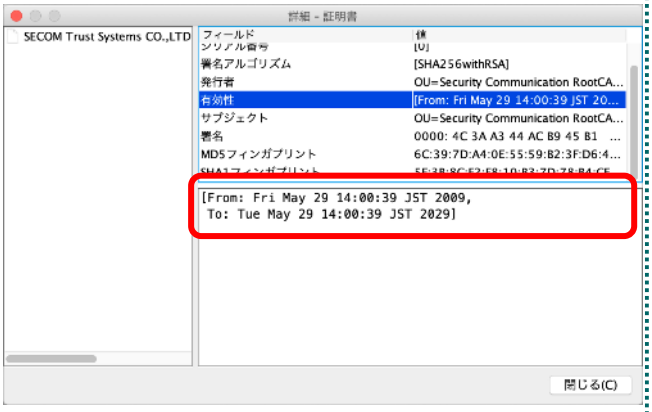
７．「**詳細-証明書**」画面が表示されます。フィールド列の「**サブジェクト**」の行を選択します。



８．表示された OU が「Security Communication RootCA2」であることを確認します。



９．フィールド列の「有効性」の行を選択します。



１０．表示された有効期間が切れてないことを確認します。