

# 電子証明書更新手順書

(Windows)

令和5年3月1日

## 【目 次】

1	更新申請画面からの更新・・・・・・・・・・・・・・・・	1
	こんなときは！「証明書の更新作業に失敗した場合」・・・・・・・・	4
2	証明書のインストール・・・・・・・・・・・・・・・・	5
	こんなときは！「新しい秘密交換キーをインポートします」・・・・	8
3	登録した証明書の確認	
	(1) Microsoft Edge (Chromium) の場合・・・・・・・・	9
	(2) Microsoft Edge (EdgeHTML) の場合・・・・・・・・	10
	(3) Internet Explorer の場合・・・・・・・・	11
4	証明書のバックアップ・・・・・・・・・・・・・・・・	12
5	証明書の削除	
	(1) Microsoft Edge (Chromium) の場合・・・・・・・・	13
	(2) Microsoft Edge (EdgeHTML) の場合・・・・・・・・	15
	(3) Internet Explorer の場合・・・・・・・・	17
6	オンライン請求システムからログアウト及びログインをする・・・・	19

## 1. 更新申請画面からの更新

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用端末）で電子証明書を更新します。



1. オンライン請求システムで利用している電子証明書の有効期限が90日未満になると、電子証明書の更新を促すメッセージが表示されます。

「更新申請サイト」のリンクをクリックすると、更新申請画面へアクセスします。

### ■証明書更新申請サイト URL

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



2. 更新対象の証明書を選択し、「OK」をクリックします。

※「Online Billing NW Common Root CA」と表記されていることを確認



3. 「証明書更新申請」をクリックします。

## 鍵更新申請情報の確認

以下の内容で証明書更新申請を送信します。  
よろしければ「Submit」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

4. 「Submit」をクリックします。

## 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
リファレンス 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
Organization	ReceiptOnline
Country	JP

5. 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。

**鍵の取得**

ダウンロードしたい鍵の発行申請時のリクエスト ID と、鍵を暗号化するパスワードを入力してください。

リクエスト ID

パスワード

パスワードの確認

6. 「鍵の取得」画面に遷移後、**任意のパスワード半角数字 4 桁**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、「2. 証明書のインストール」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。**

**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。

7. 「**Download**」をクリックし、証明書を保存します。

**【保存】**を選択した場合

ブラウザで設定されている保存先に電子証明書が保存されます。なお、既定の保存場所は、「C:\Users¥[ユーザー名]¥Downloads」です。

**【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、必要に応じて、デスクトップ上に電子証明書を移動してください。

**【名前を付けて保存】**を選択した場合

電子証明書をダウンロードする際、選択した任意の場所に保存されます。

8. 証明書のインストールは、「2. 証明書のインストール」を参照ください。

9. 「5. 証明書の削除」を参照し、古い証明書を削除ください。

こんなときは！「証明書の更新作業に失敗した場合」

証明書または鍵の更新作業中に、ネットワーク等の障害で証明書または鍵の取得に失敗した場合や「証明書更新申請」をクリックした際に「この証明書は既に更新の上限回数に達しています。」とメッセージが表示された場合は、再度証明書または鍵を取得してください。



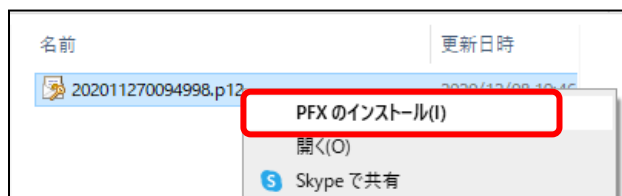
1. 更新申請画面の「更新後証明書の取得」をクリックします。

○一覧に情報が表示されている場合は、対象の更新済み証明書の「Download Key」ボタンをクリックして証明書を取得してください。

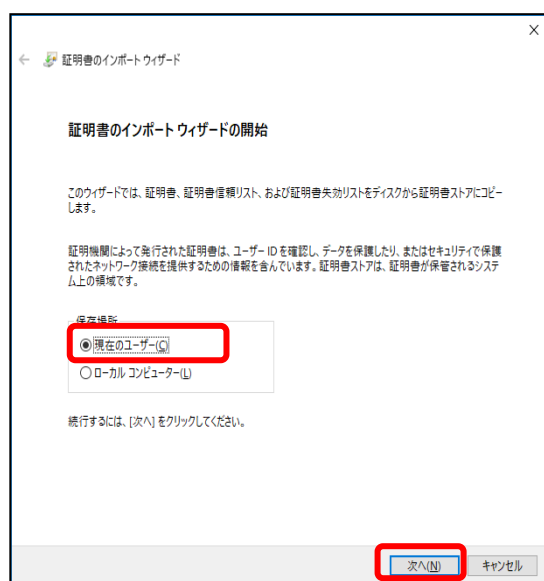
○一覧に情報が表示されていない場合は、更新申請が完了していませんので、「1.更新申請画面からの更新」からやり直してください。

2. 「Download Key」ボタンをクリック後に3ページの「鍵の取得」画面が表示されます。

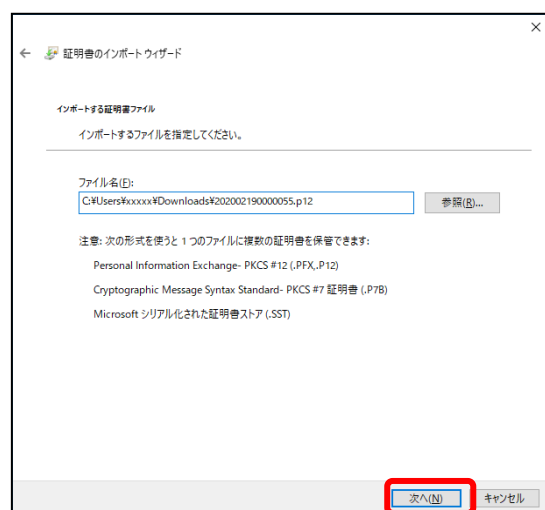
## 2. 証明書のインストール



1. ダウンロードした証明書ファイルを右クリックし、「PFX インストール」をクリックします。



2. 「現在のユーザー」を選択し、「次へ」をクリックします。



3. ファイル名に証明書のファイル名が表示されていることを確認し、「次へ」をクリックします。

4. [パスワード]に「1.更新申請画面からの更新」で設定したパスワードを入力します。

[秘密キーの保護を強力にする]の  
チェックを外す

[このキーをエクスポート可能にする]を  
チェックする

[すべての拡張プロパティを含める]を  
チェックする

【こんなときは！】

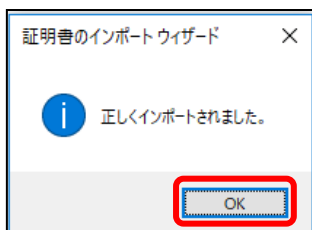
「秘密キーの保護を強力にする」のチェックが外せない場合は、セキュリティを強化する設定がされているため、P8『こんなときは！「新しい秘密交換キーをインポートします」』を参照

5. 「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択後、「次へ」をクリックします。

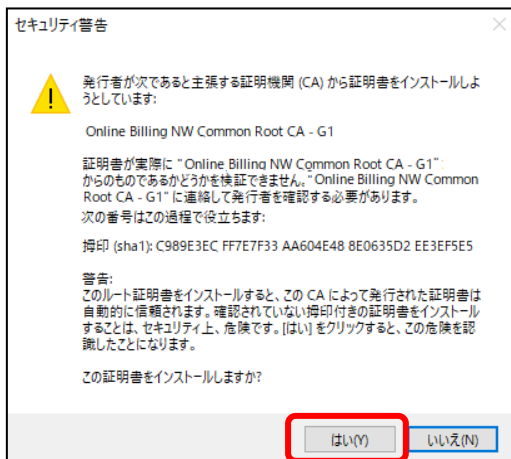




6. 「完了」をクリックします。



7. 「OK」をクリックします。



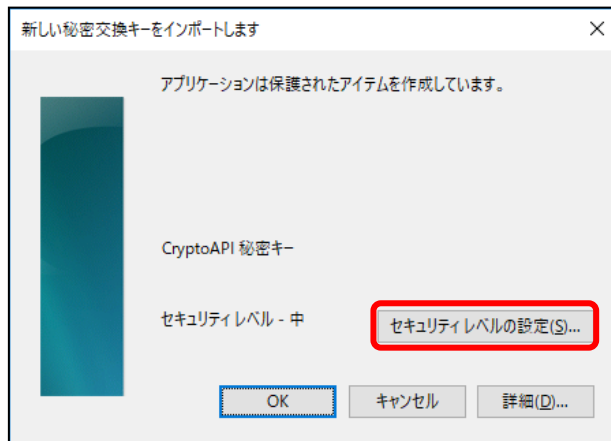
### 【こんなときは！】

「セキュリティ警告」の画面が表示された場合、「はい」をクリックします。

「証明書発行者（認証局）の証明書」は、インストールを行った証明書が「証明書発行者（認証局）」によって発行された証明書であることを確認（ご使用のブラウザが自動的に確認）する時に必要です。「いいえ」をクリックした場合は、「2.証明書のインストール」を再度行ってください。

## こんなときは！「新しい秘密交換キーをインポートします」

※証明書インストール時に「新しい秘密交換キーをインポートします」と表示された場合は、次の操作を行ってください。表示されない場合には「3. 登録した証明書の確認」に進みます。



1. 「セキュリティレベルの設定」をクリックします。



2. 任意のパスワードを入力し、「完了」をクリックします。

### 【※重要※】

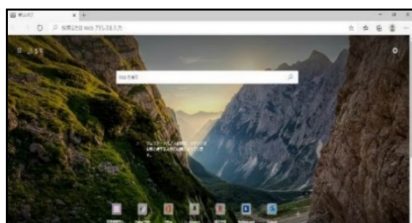
作成したパスワードは、今後の証明書の更新時に利用するため、忘れないよう大切に保管ください。



3. 「OK」をクリックします。

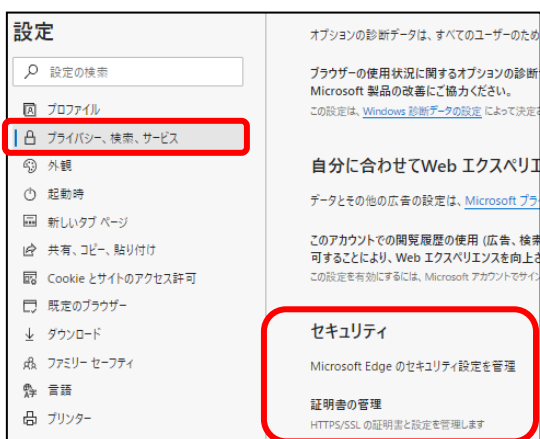
### 3. 登録した証明書の確認

#### (1) Microsoft Edge(Chromium)の場合



1. Edge を起動します。

2. 画面右上の【…】をクリックし、「設定」をクリックします。

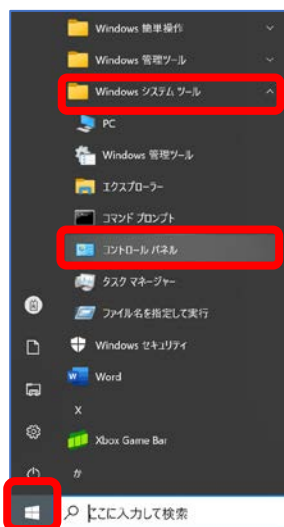



3. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。



4. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

## (2) Microsoft Edge (EdgeHTML) の場合



1. デスクトップ左下の  アイコンをクリックし、すべてのアプリ一覧の中から「Windows システム ツール」を選択し、「コントロール パネル」を選択します。

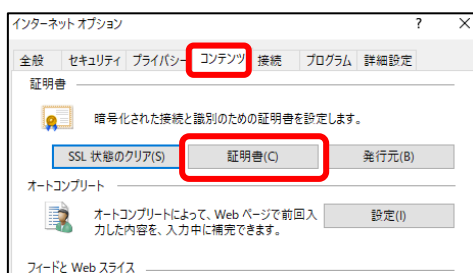
「コントロール パネル」画面が表示されます。



2. 「ネットワークとインターネット」を選択します。



3. 「インターネット オプション」を選択します。

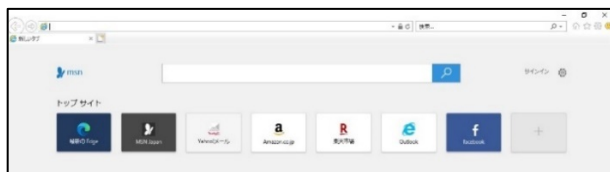


4. 「コンテンツ」タブを選択し、「証明書」をクリックします。

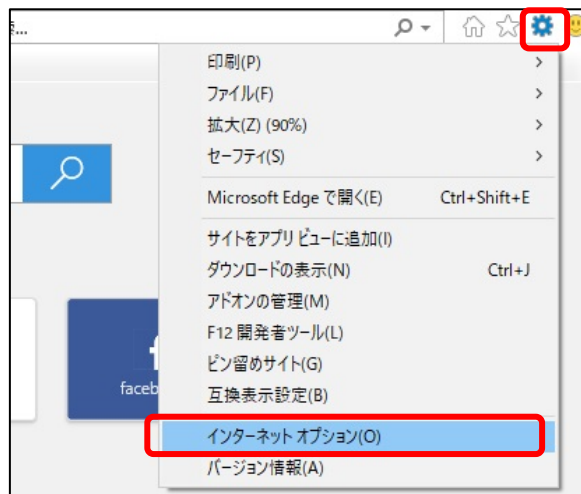


5. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

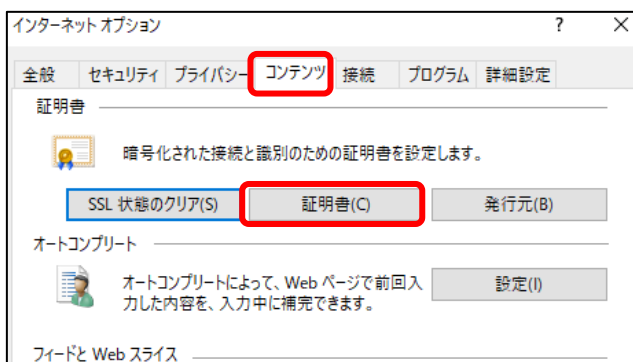
### (3) Internet Explorer の場合



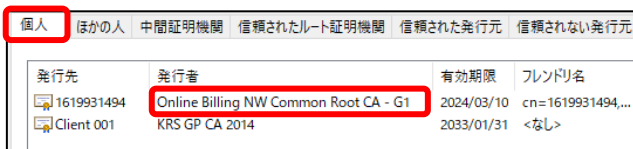
1. Internet Explorer を起動します。



2. 画面右上の「⚙」ボタンから「インターネット オプション」をクリックします。



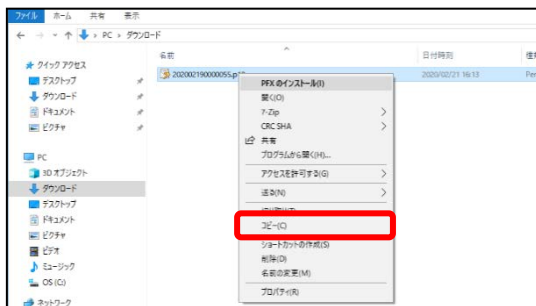
3. 「コンテンツ」タブを選択し、「証明書」をクリックします。



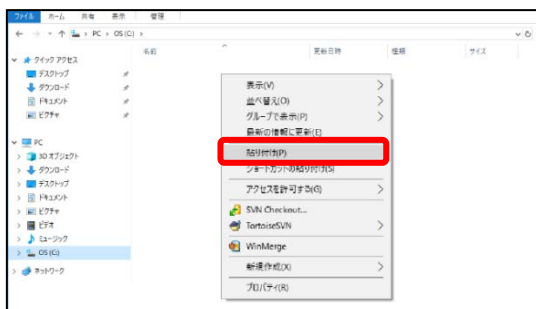
4. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

## 4 証明書のバックアップ

外部記録媒体等へ証明書をバックアップします。バックアップした証明書はパソコンが故障した際に他のパソコンにインストールします。その際には、「1. 更新申請画面からの更新」で設定したパスワードも必要となるため、忘れないように保管ください。



1. インストール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. 外部記録媒体等のフォルダを開き、「貼り付け」を選択します。

### 【注意】

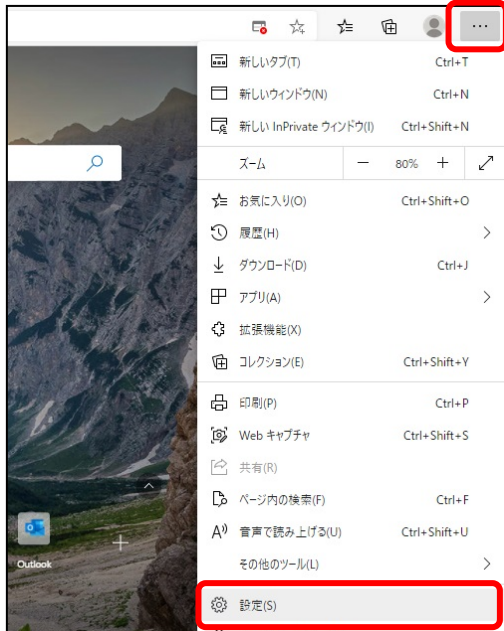
「証明書」「証明書の取得画面で入力した証明書パスワード」は厳重に管理してください。証明書の情報が第三者に知られると、証明書が不正に使用される恐れがあります。

証明書を紛失した場合、または、第三者に知られた可能性がある場合は、速やかに証明書失効申請を行ってください。また、パソコンを紛失した場合も証明書が不正に使用される恐れがあります。速やかに証明書失効申請を行ってください。

**証明書のインストール作業はこれで終了です。**

## 5. 証明書の削除

### (1) Microsoft Edge(Chromium)の場合



1. Edge を起動し、画面右上の「設定」をクリックします。



2. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。

証明書

目的(N): <すべて>

個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元

発行先	発行元	有効期限	フレンドリ名
1619931494	Online Billing NW Common Root CA - G1	2024/03/10	cn=1619931494,...
Client 001	KRS GP CA 2014	2033/01/31	<なし>

インポート(I)... エクスポート(E)... 削除(R) 詳細設定(A)

証明書の目的

表示(V)

閉じる(C)

3. 「個人」タブを開き、有効期限が古い証明書を選択し、「削除」をクリックします。

※発行者が「Online Billing NW Common Root CA」が含まれる表記となっていることを確認します。

※新しくインポートした電子証明書を削除しないよう、有効期限の日付を十分確認して「削除」をクリックしてください。

証明書

!

証明書を使って暗号化データの暗号化を解除できません。証明書を削除しますか?

はい(Y) いいえ(N)

4. 「はい」をクリックします。

証明書

目的(N): <すべて>

個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元

発行先	発行元	有効期限	フレンドリ名
Client 001	KRS GP CA 2014	2033/01/31	<なし>

インポート(I)... エクスポート(E)... 削除(R) 詳細設定(A)

証明書の目的

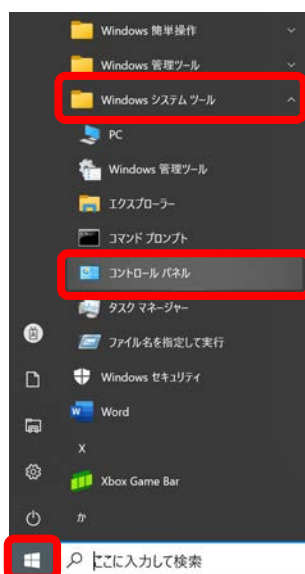
表示(V)


閉じる(C)

5. 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、「閉じる」をクリックします。



## (2) Microsoft Edge (EdgeHTML) の場合



1. デスクトップ左下の  アイコンをクリックし、すべてのアプリ一覧の中から「Windows システムツール」を選択し、「コントロールパネル」を選択します。

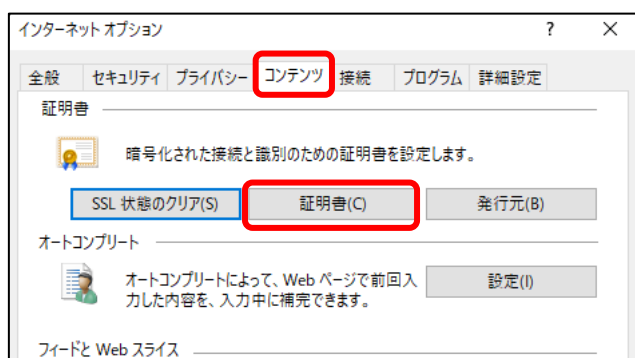
「コントロールパネル」画面が表示されます。



2. 「ネットワークとインターネット」を選択します。



3. 「インターネットオプション」を選択します。



4. 「コンテンツ」タブを選択し、「証明書」をクリックします。

証明書

目的(N): <すべて>

個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元

発行先	発行元	有効期限	フレンドリ名
1619931494	Online Billing NW Common Root CA - G1	2024/03/10	cn=1619931494,...
Client 001	KRS GP CA 2014	2033/01/31	<なし>

インポート(I)... エクスポート(E)... 削除(R) 詳細設定(A)

証明書の目的

表示(V)

閉じる(C)

5. 「個人」タブを開き、有効期限が古い証明書を選択し、「削除」をクリックします。

※発行者が「Online Billing NW Common Root CA」が含まれる表記となっていることを確認します。

※新しくインポートした電子証明書を削除しないよう、有効期限の日付を十分確認して「削除」をクリックしてください。

証明書

!

証明書を使って暗号化データの暗号化を解除できません。証明書を削除しますか?

はい(Y) いいえ(N)

6. 「はい」をクリックします。

証明書

目的(N): <すべて>

個人 ほかの人 中間証明機関 信頼されたルート証明機関 信頼された発行元 信頼されない発行元

発行先	発行元	有効期限	フレンドリ名
Client 001	KRS GP CA 2014	2033/01/31	<なし>

インポート(I)... エクスポート(E)... 削除(R) 詳細設定(A)

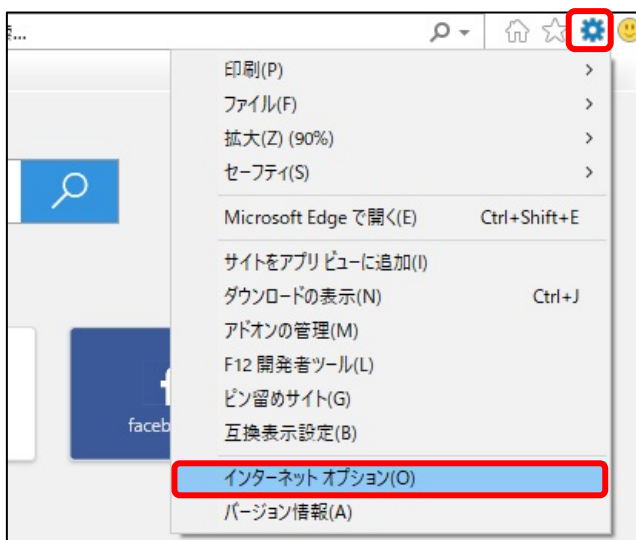
証明書の目的


表示(V)

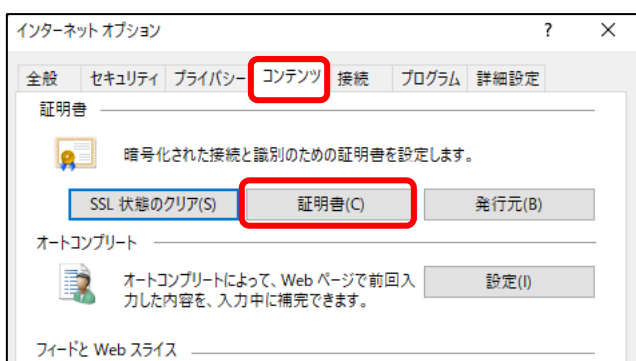
閉じる(C)

7. 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、「閉じる」をクリックします。

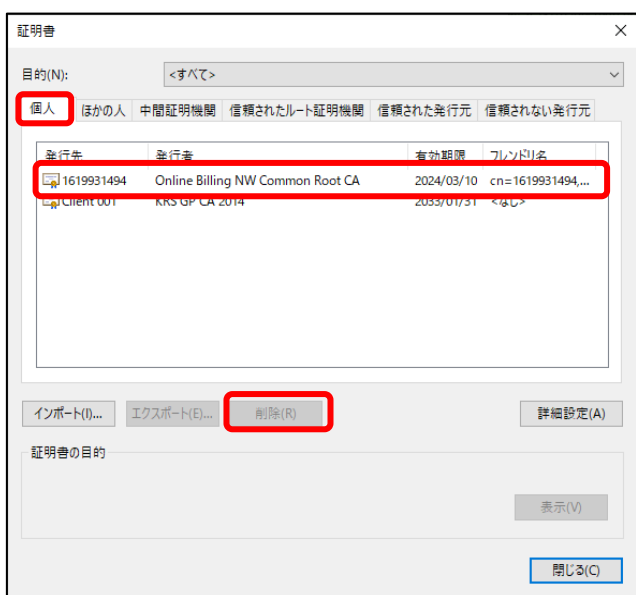
### (3) Internet Explorer の場合



1. Internet Explorer を起動し、画面右上の「」ボタンから「インターネットオプション」をクリックします。



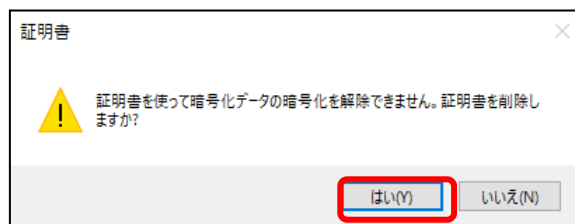
2. 「コンテンツ」タブを選択し、「証明書」をクリックします。



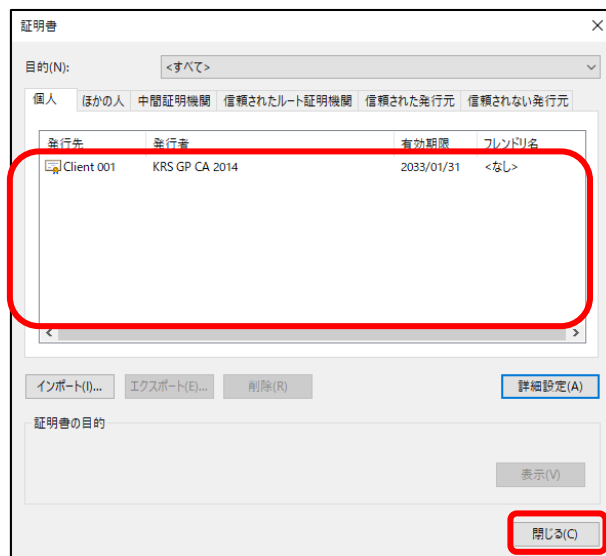
3. 「個人」タブを開き、有効期限が古い証明書を  
選択し、「削除」をクリックします。

※発行者が「**Online Billing NW Common Root CA**」が含まれる表記となっていることを確認します。

※新しくインポートした電子証明書を削除しないよう、有効期限の日付を十分確認して「削除」をクリックしてください。



4. 「はい」をクリックします。



5. 削除を行った証明書が一覧から削除されていることを確認し、「閉じる」をクリックします。

## 6. オンライン請求システムからログアウト及びログインをする

オンライン請求システムからログアウトし、再度ログインすることによって、赤字等で表示されている電子証明書の更新を促すメッセージが消えます。

### (1) ログアウトをする

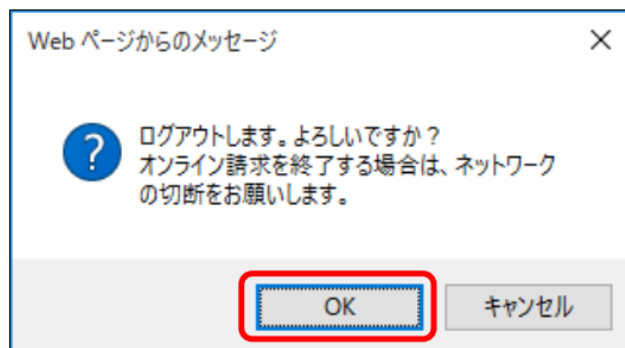


1. 電子証明書の更新作業※を完了したら、【ログアウト】ボタンをクリックします。

確認メッセージが表示されます。

※ 電子証明書の更新作業

電子証明書のダウンロード、インポート及び有効期限の古い電子証明書を削除



2. 【OK】ボタンをクリックします。

ログアウトされます。



3. 「環境選択」画面を閉じる場合は、画面右上の【X】ボタンをクリックします。

## (2) ログインをする

### ■Windows の場合



1. デSKTOP上の「オンライン請求」アイコンをダブルクリックします。

### ●医療機関・薬局の場合



2.

### ●医療機関・薬局の場合

「審査支払機関選択」画面が表示されるので、【社会保険診療報酬支払基金】ボタンをクリックすると、「環境選択」画面が表示されるので、【請求】ボタンをクリックします。

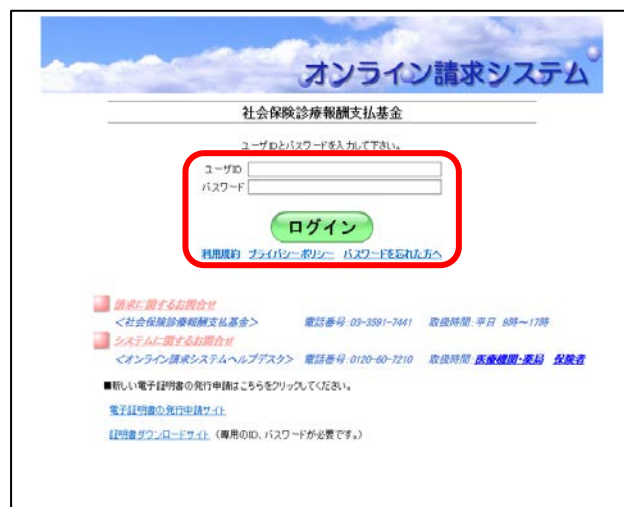


### ●保険者・実施機関の場合



### ●保険者・実施機関の場合

「環境選択」画面が表示されるので、【レセプトデータ配信 再審査請求】ボタンをクリックします。



3. オンライン請求システムの「ユーザ ID」と「パスワード」を入力し、【ログイン】ボタンをクリックします。

オンライン請求システムの「トップページ」画面が表示されます。



4. 電子証明書の有効期限表示が黒色で記載されていることで、電子証明書の更新が完了したことが確認できます。