

電子証明書更新手順書

(Windows)

令和7年6月1日

【更新処理の流れ（目次）】

以下の 1 から 6 を順に実施願います。

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」・・・・・・・・	5
2	証明書のインストール・・・・・・・・・・・・・・・・	6
	こんなときは！「新しい秘密交換キーをインポートします」・・・・	9
3	登録した証明書の確認	
	(1) Microsoft Edge（Chromium）の場合※Edge バージョン 136 以降・・・・	10
	(2) Microsoft Edge（Chromium）の場合※Edge バージョン 135 以前・・・・	12
	(3) Microsoft Edge（EdgeHTML）の場合・・・・・・・・	13
	(4) Internet Explorer の場合・・・・・・・・	14
4	証明書のバックアップ・・・・・・・・	15
5	証明書の削除	
	(1) Microsoft Edge（Chromium）の場合※Edge バージョン 136 以降・・・・	16
	(2) Microsoft Edge（Chromium）の場合※Edge バージョン 135 以前・・・・	19
	(3) Microsoft Edge（EdgeHTML）の場合・・・・・・・・	21
	(4) Internet Explorer の場合・・・・・・・・	23
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・・・・	25

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している端末（レセプトオンライン用端末または特定健診・保健指導システム用端末）で電子証明書を更新します。

【注意】必ずすべてのブラウザを閉じてから、手続きを実施してください。

1. 以下のいずれかの方法で電子証明書更新申請サイトへアクセスします。

● オンライン請求システムから更新申請サイトへアクセスする場合



1-1. 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。

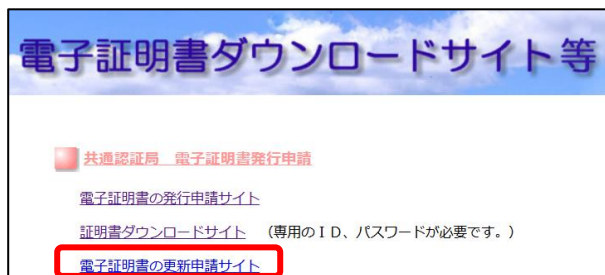
■ 証明書更新申請サイト URL

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

● オンライン請求システムをインストールしていないパソコン（特定健診・保健指導システム専用のパソコン）で更新作業を行う場合



1-1. デスクトップにある「証明書ダウンロードサイト」のアイコンをクリックします



1-2. 「電子証明書の更新申請サイト」をクリックし、更新申請画面へアクセスします

※「証明書ダウンロードサイト」のアイコンが無い場合、ご利用のブラウザから下記アドレスを直接入力し、電子証明書の更新申請サイトへアクセスしてください。

■ 証明書更新申請サイト URL

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

認証用の証明書の選択

サイト cert.obn.managedpki.ne.jp では資格情報が必要です:

011T123456 Online Billing NW Common Root CA - G1 2020/9/3

証明書情報

OK キャンセル

2. 左の画面が表示された場合、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

Cybertrust Managed PKI

証明書の更新

証明書更新申請

更新後証明書の取得

サイバートラスト マネージドPKI

サイバートラスト マネージドPKI の証明書の取得

証明書更新申請

現在お使いの証明書の更新申請を送信します。

3. 「証明書更新申請」をクリックします。

鍵更新申請情報の確認

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

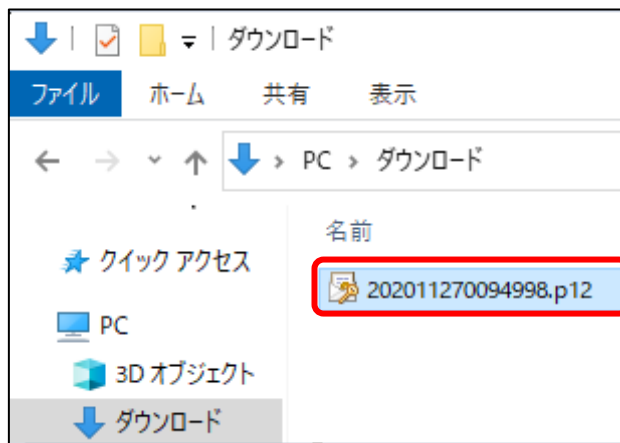
鍵をダウンロードします。鍵のダウンロードまたはインストールを行うには、「Download」ボタンをクリックしてください。

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. 保存場所に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】

「Download」をクリック後、直接「ファイルを開く」を選択すると証明書が保存されず、「4 証明書のバックアップ」に影響がありますので、ご留意願います。

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。



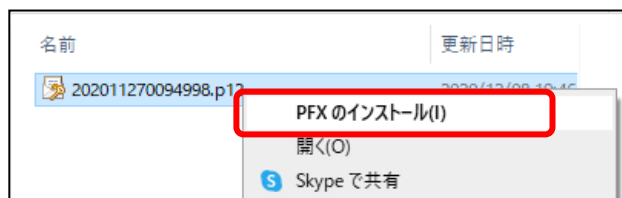
1. 更新申請画面の「更新後証明書の取得」をクリックします。

○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。

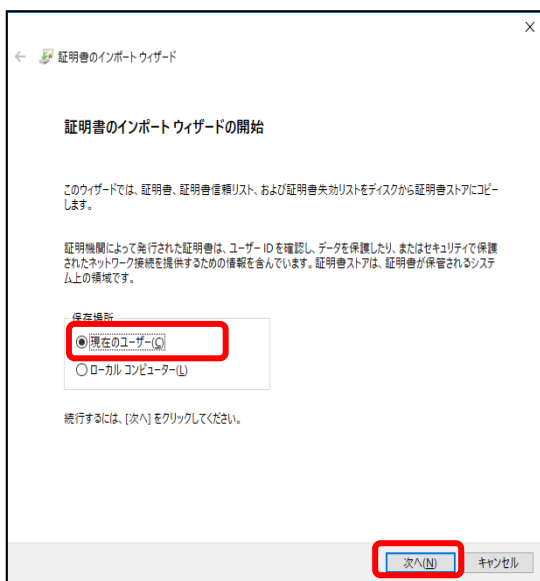
○一覧に情報が表示されていない場合は、更新申請が完了していませんので、「1.更新申請画面からの更新」からやり直してください。

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。

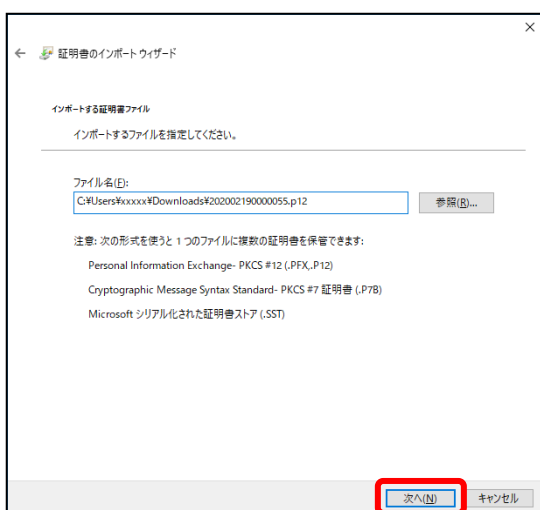
2 証明書のインストール



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
チェックを外す

[すべての拡張プロパティを含める]を
チェックする

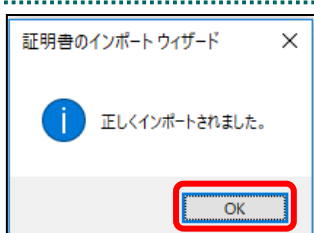
【こんなときは！】

「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、P9『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

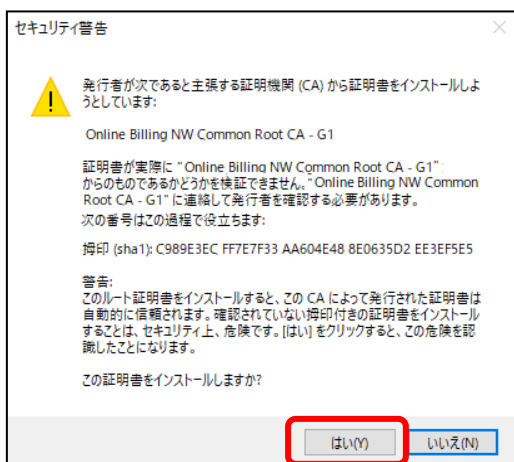
5. 「証明書の種類に基づいて、自動的に証明書ストアを選択する」を選択後、「次へ」をクリックします。



6. 「完了」をクリックします。



7. 「OK」をクリックします。



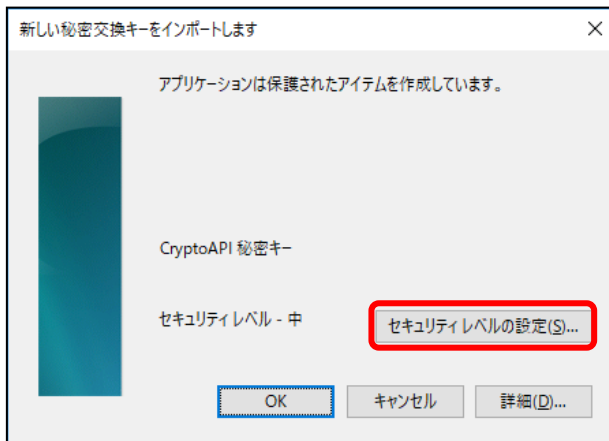
【こんなときは！】

「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※】

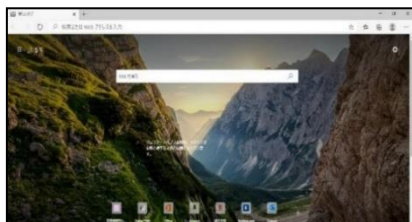
作成したパスワードは、今後の証明書の更新時に利用するため、忘れないよう大切に保管ください。



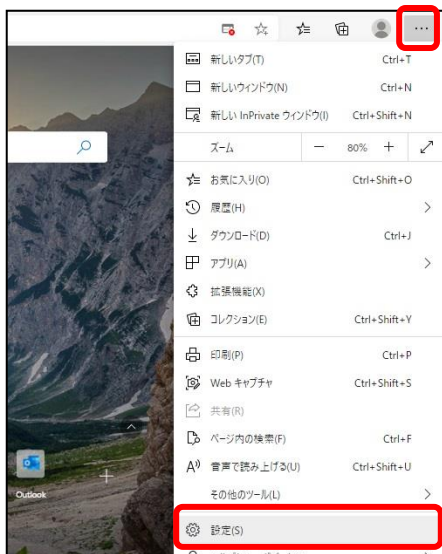
3. 「OK」をクリックします。

3 登録した証明書の確認

(1) Microsoft Edge(Chromium)の場合 ※Edge バージョン 136 以降



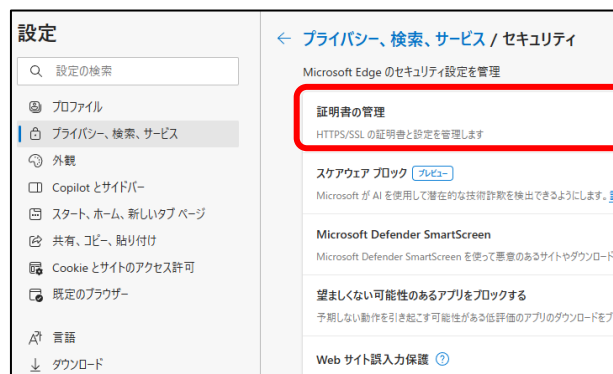
1. Edge を起動します。



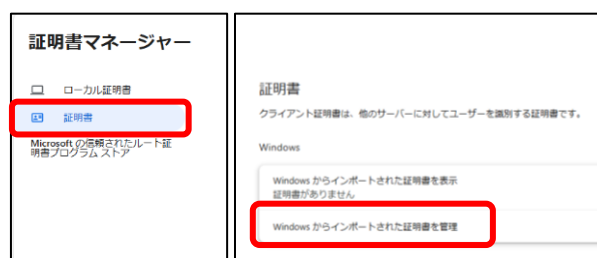
2. 画面右上の【…】をクリックし、「設定」をクリックします。



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



4. 「証明書の管理」をクリックします。

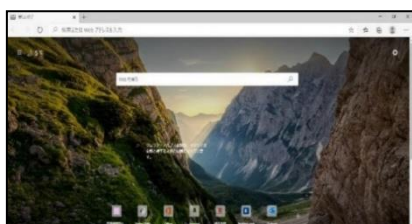


5. 証明書マネージャーの「証明書」を選択し、「Windows からインポートされた証明書を管理」をクリックします。

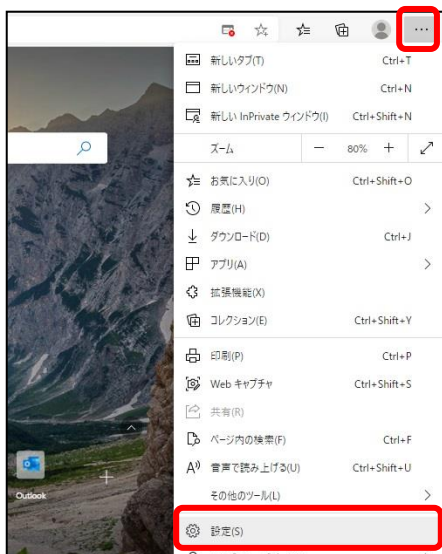


6. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

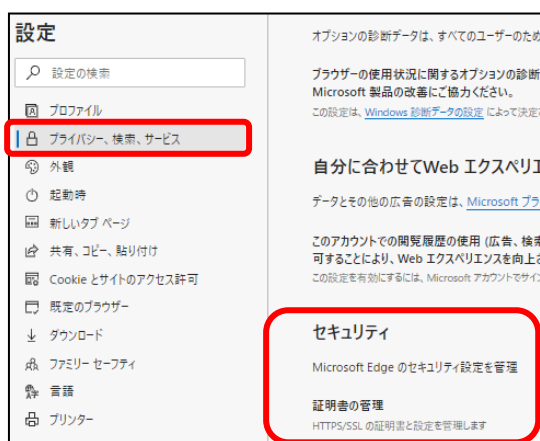
(2) Microsoft Edge(Chromium)の場合 ※Edge バージョン 135 以前



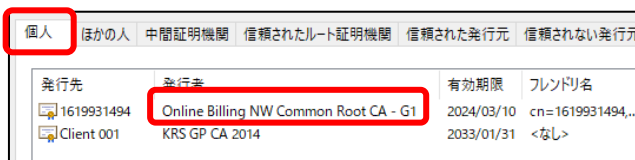
1. Edge を起動します。



2. 画面右上の【…】をクリックし、「設定」をクリックします。

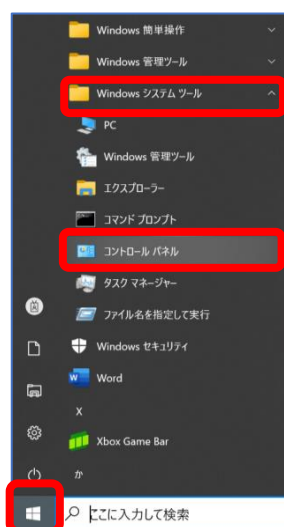


3. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。



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。

(3) 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。

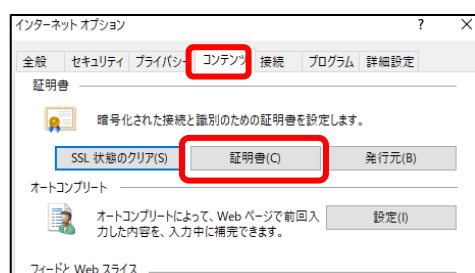
「コントロールパネル」画面が表示されます。



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。

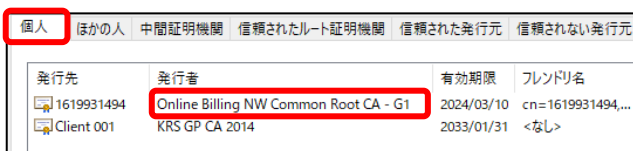
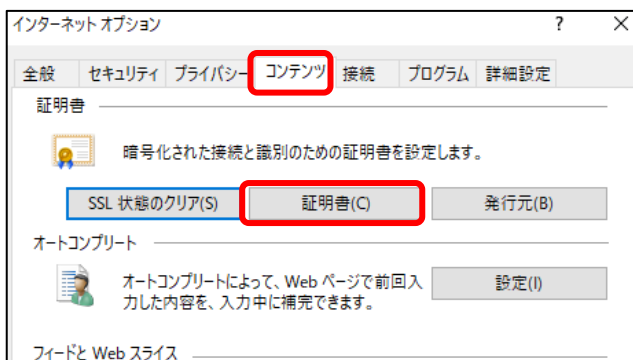
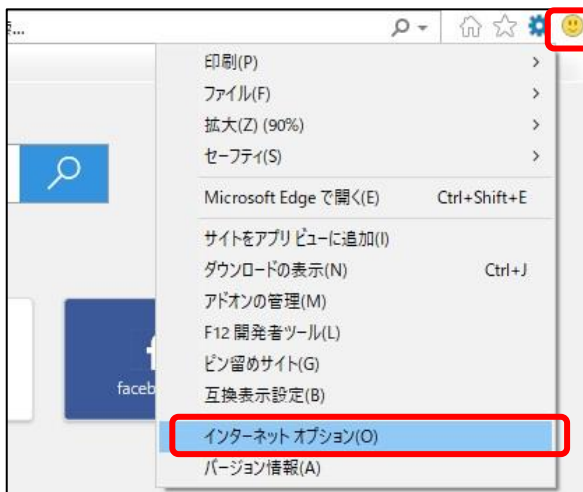
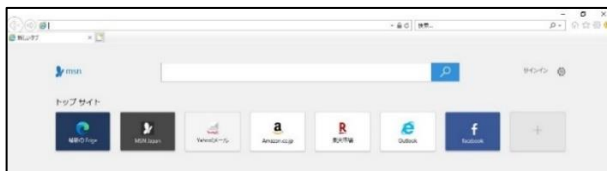


4. 「コンテンツ」タブを選択し、「証明書」をクリックします。



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。

(4) Internet Explorer の場合



1. Internet Explorer を起動します。

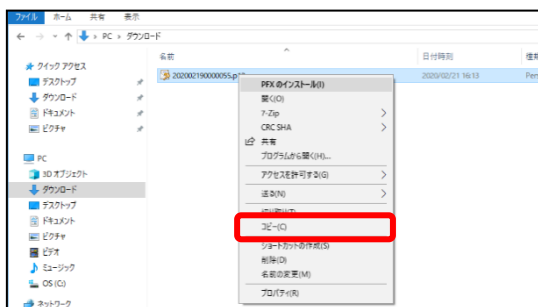
2. 画面右上の「」ボタンから「インターネット オプション」をクリックします。

3. 「コンテンツ」タブを選択し、「証明書」をクリックします。

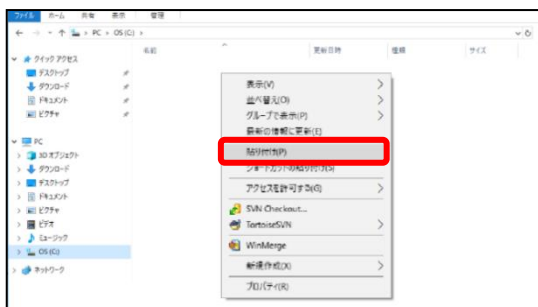
4. 「個人」タブを開き、発行者が「Online Billing NW Common Root CA」と表示されている証明書が登録されていることを確認します。

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などに他のパソコンにインストールします。その際には、「1. 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。

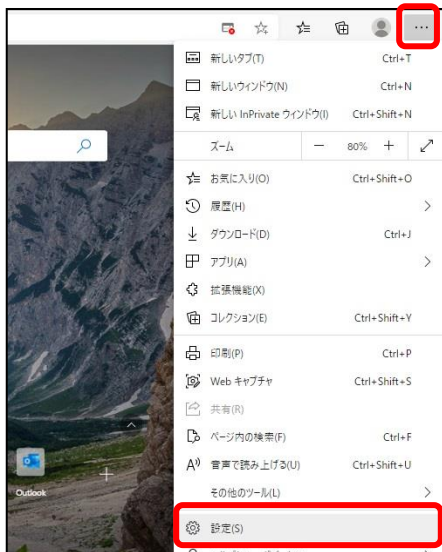
証明書のインストール作業はこれで終了です。

5 証明書の削除

(1) Microsoft Edge(Chromium)の場合 ※Edge バージョン 136 以降



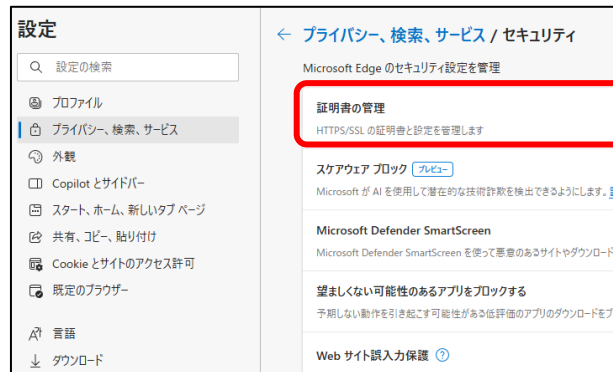
1. Edge を起動します。



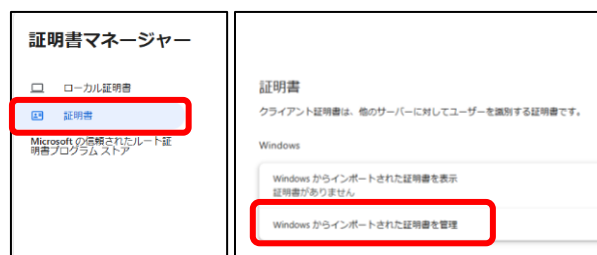
2. 画面右上の【…】をクリックし、「設定」をクリックします。



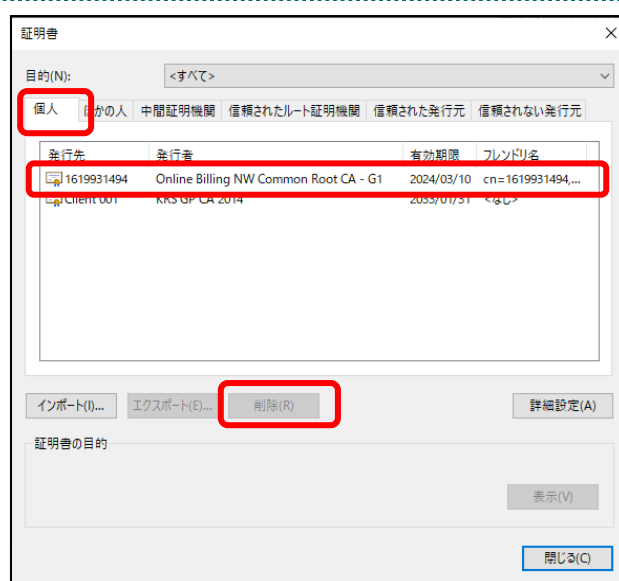
3. 「プライバシー、検索、サービス」を選択し、「セキュリティ」をクリックします。



4. 「証明書の管理」をクリックします。



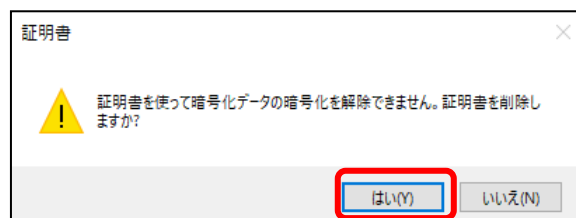
5. 証明書マネージャーの「証明書」を選択し、「Windows からインポートされた証明書を管理」をクリックします。



6. 「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。



7. 「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	発行者	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)

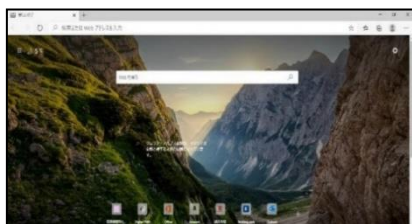
証明書の目的

表示(V)

閉じる(C)

8. 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。

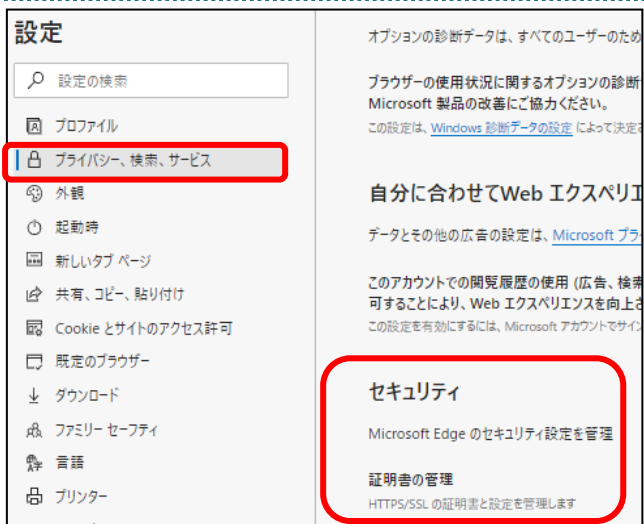
(2) Microsoft Edge(Chromium)の場合 ※Edge バージョン 135 以前



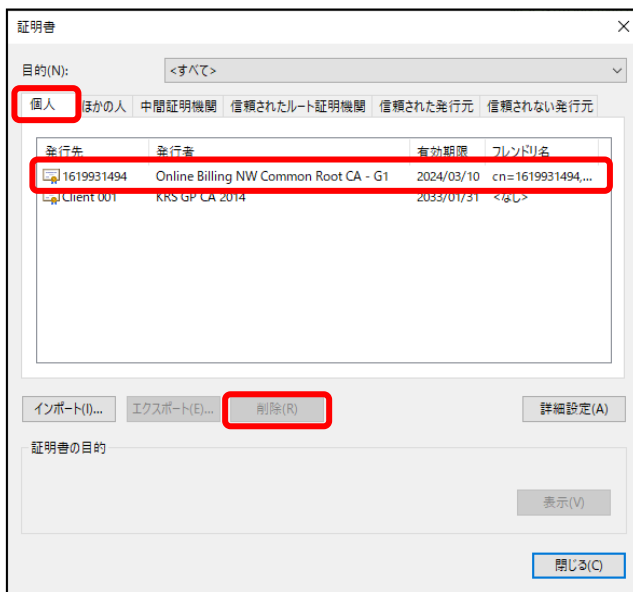
1. Edge を起動します。



2. Edge を起動し、画面右上の「設定」をクリックします。



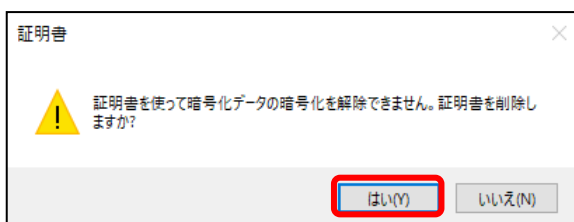
3. 「プライバシー、検索、サービス」を選択し、「セキュリティ」の「証明書の管理」をクリックします。



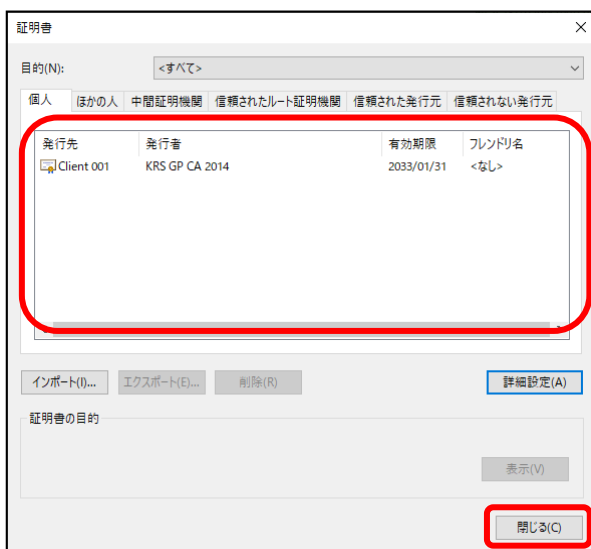
4. 「個人」タブを開き、有効期限が古い証明書を選択し、「削除」をクリックします。

※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。

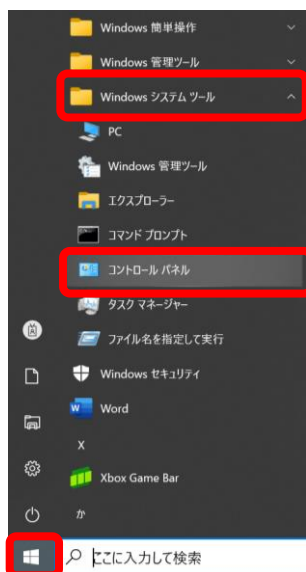


5. 「はい」をクリックします。



6. 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) 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。

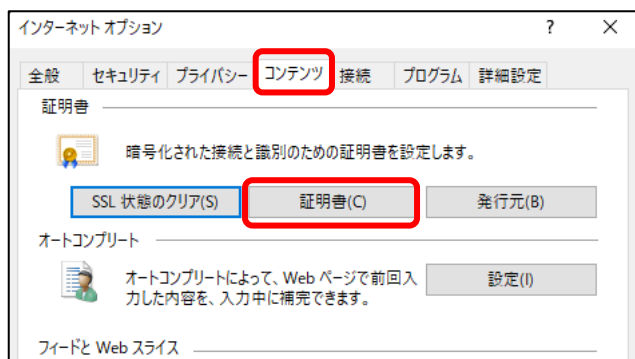
「コントロールパネル」画面が表示されます。



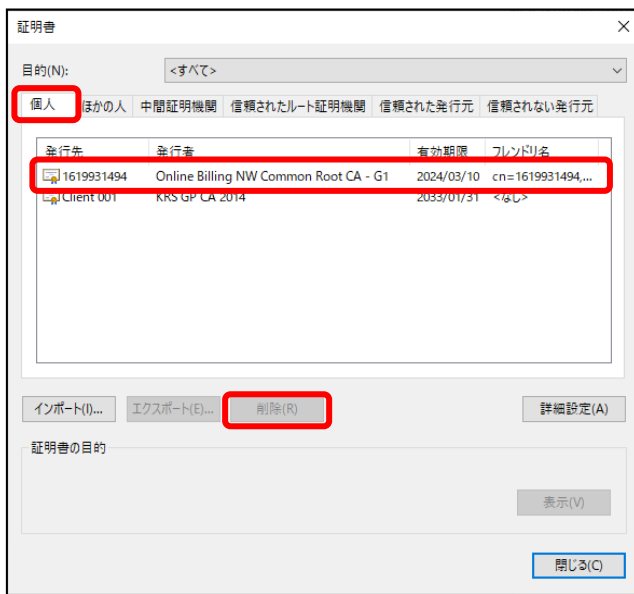
2. 「ネットワークとインターネット」を選択します。



3. 「インターネットオプション」を選択します。



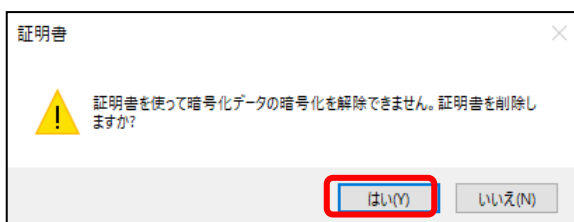
4. 「コンテンツ」タブを選択し、「証明書」をクリックします。



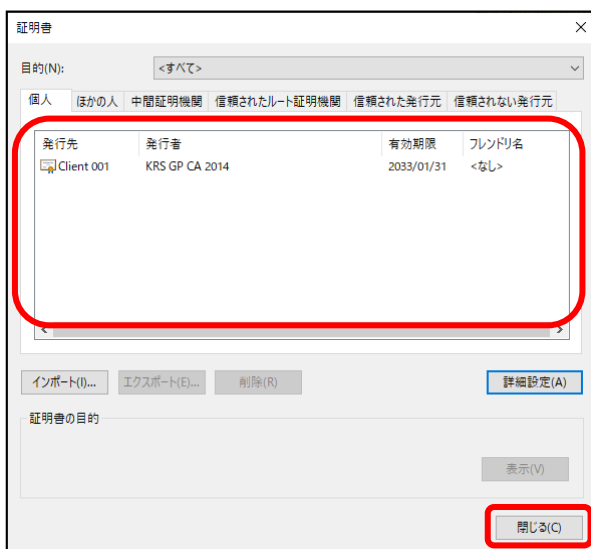
5. 「個人」タブを開き、有効期限が古い証明書を選択し、「削除」をクリックします。

※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。

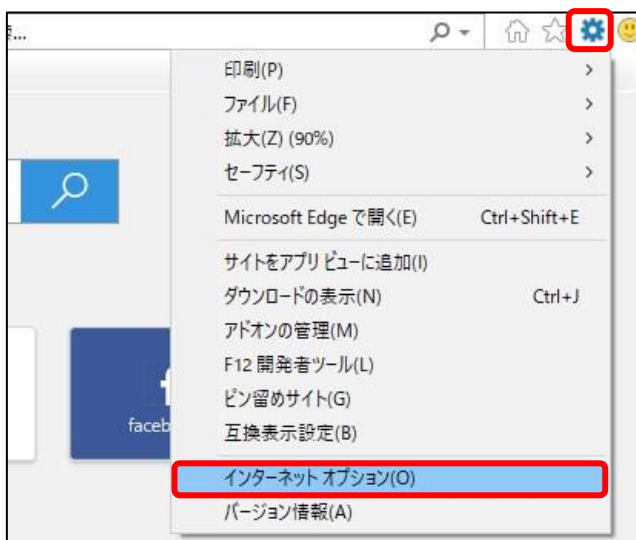


6. 「はい」をクリックします。

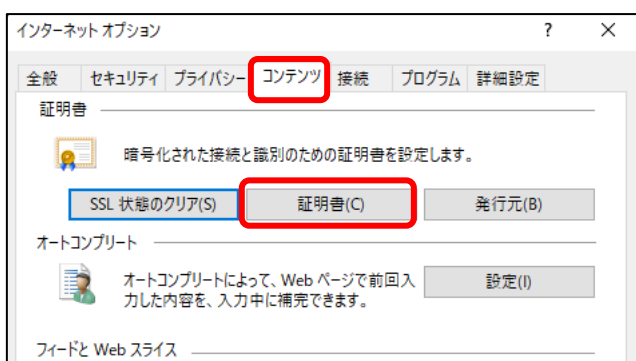


7. 削除を行った証明書が一覧から消えていることを確認し、「閉じる」をクリックします。

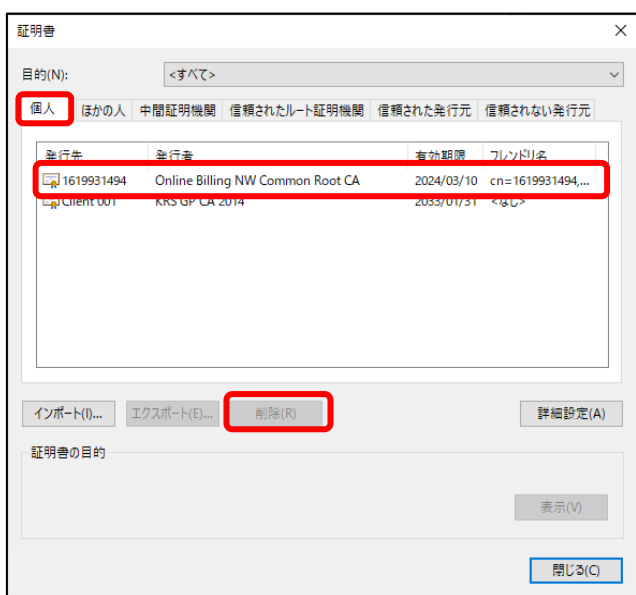
(4) Internet Explorer の場合



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。



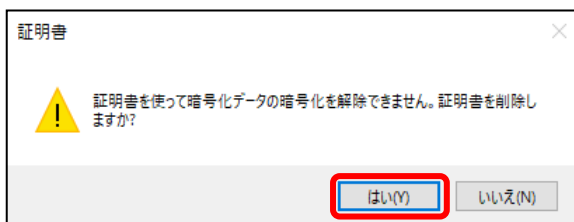
2. 「コンテンツ」タブを選択し、「証明書」をクリックします。



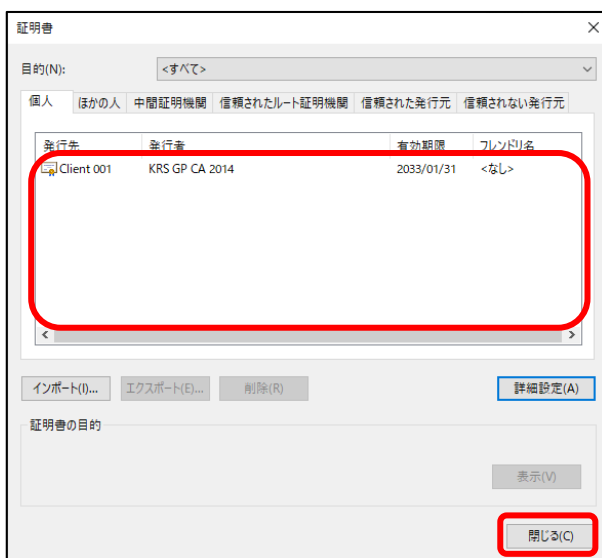
3. 「個人」タブを開き、有効期限が古い証明書を選択し、「削除」をクリックします。

※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。



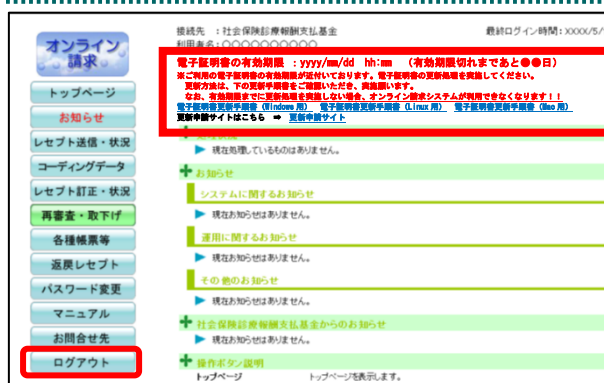
5. 削除を行った証明書が一覧から削除されていることを確認し、「閉じる」をクリックします。

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。

※オンライン請求システムをインストールしていないパソコン（特定健診・保健指導システム専用のパソコン）の場合、本対応は不要です。

(1) ログアウトをする

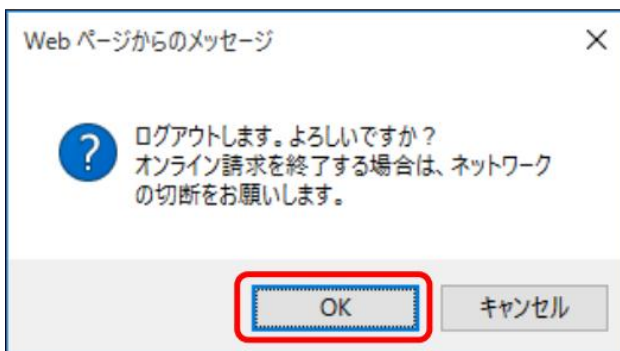


1. 電子証明書の更新作業※を完了したら、【ログアウト】ボタンをクリックします。

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【×】ボタンをクリックします。

(2) ログインをする

■Windows の場合



1. デスクトップ上の「オンライン請求」アイコンをダブルクリックします。

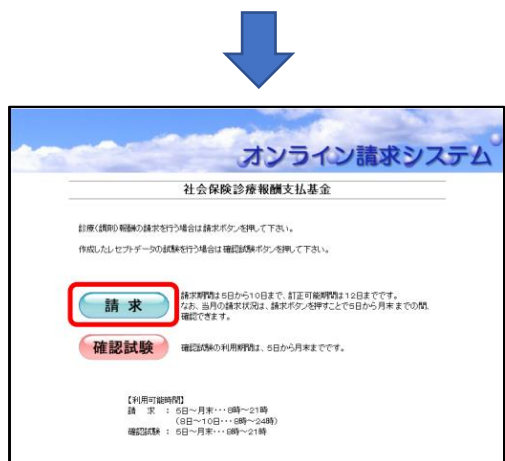
●医療機関・薬局の場合



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。

オンライン請求システム

社会保険診療報酬支払基金

ユーザIDとパスワードを入力して下さい。

ユーザID
パスワード

ログイン

利用規約 プライバシーポリシー パスワードを忘れた方へ

■ 請求に関するお問合せ
<社会保険診療報酬支払基金> 電話番号: 03-3591-7441 取扱時間: 平日 9時~17時

■ システムに関するお問合せ
<オンライン請求システムヘルプデスク> 電話番号: 0120-60-7210 取扱時間: 医療機関・薬局 保険者

■ 新しい電子証明書の発行申請はこちらをクリックしてください。
[電子証明書の発行申請サイト](#)

[証明書ダウンロードサイト](#) (専用のID、パスワードが必要です。)

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。

オンライン請求

接続先: 社会保険診療報酬支払基金
利用者名: 〇〇〇〇〇〇〇〇〇〇〇〇

最終ログイン時間: XXXX/5/10 10:00

電子証明書の有効期限: yyyy/mm/dd hh:mm

処理状況
▶ 現在処理しているものはありません。

お知らせ
▶ システムに関するお知らせ
▶ 現在お知らせはありません。

運用に関するお知らせ
▶ 現在お知らせはありません。

その他のお知らせ
▶ 現在お知らせはありません。

社会保険診療報酬支払基金からのお知らせ
▶ 現在お知らせはありません。

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。