はじめに -登録担当者用 支援システム操作手順書について-

改版履歴			
版数	日付	内容	担当
V.1.1	2014/12/22	初版	NII
V.1.2	2015/2/13	誤植の修正 利用管理者情報更新申請ファイル中の制限追記	NII
V.1.3	2015/4/1	サーバ証明書の発行・更新機能の修正 クライアント証明書の発行・更新・失効機能の追加 コード署名用証明書の発行・更新・失効機能の追加	NII
V.1.4	2015/12/11	全角文字使用可能文字の範囲を追記 Firefox操作時の条件を追記	NII
V.1.5	2016/4/21	誤植の修正	NII
V.1.6	2016/12/26	有効期限切れ間近の証明書更新の運用を修正 連絡先電話番号の修正	NII
V.1.7	2017/2/28	コード署名用証明書のダウンロード種別P12を削除	NII
V.1.8	2017/7/25	ホップアップメッセージの修正	NII
V.2.0	2018/2/26	SHA-1に関する記述削除 WindowsVistaの設定削除 発行証明書統計照会の説明追記	NII
V.2.1	2018/3/26	用語変更（事務局 ⇒ サービス窓口 ）	NII
V.2.2	2018/7/9	タイムスタンプURL画面の追加	NII
V.2.3	2019/9/10	Keygen廃止に伴う情報の追記	NII
V.2.4	2020/4/13	利用申請から利用開始までの図の更新 サービスの概要【参加申請】の文章を更新 Firefoxのバージョンについて修正	NII
V.2.5	2020/6/4	システム画面の画像の変更 画面の解説の修正 IIS7.5に関する記載の削除	NII
V.2.6	2020/9/16	Firefoxでの取得手順を修正	NII
V.2.7	2021/3/30	システム画面の画像の変更 許可リスト一括ダウンロードの追加 Firefoxでの登録担当者用証明書取得手順 を修正	NII
V.2.8	2021/10/12	Internet Explorer(OS:windows10)での登録担当者用証明書取得手順の変更	NII
V.2.9	2023/5/19	コード署名用証明書のCSR作成に関する手順を削除	NII
V.2.10	2023/12/14	クライアント証明書および登録担当者用証明書切り替え Internet Explorerでの手順をEdgeに修正	NII

目次

- 1. 本書の範囲
- 2. 登録担当者初期設定
  - 2-1. 登録担当者用証明書取得までの概要
  - 2-2. 登録担当者用証明書取得事前準備
    - 2-2-1. 証明書取得URLの通知
    - 2-2-2. アクセスPINの取得
  - 2-3. 登録担当者用証明書取得
    - 2-3-1. Microsoft Edge・Google Chromeでの登録担当者用証明書取得手順
      - 2-3-1-1. 新規／紛失による証明書取得手順
      - 2-3-1-2. 有効期限切れ間近の証明書更新手順
    - 2-3-2. Firefoxでの登録担当者用証明書取得手順
      - 2-3-2-1. 新規／紛失による証明書取得手順
      - 2-3-2-2. 有効期限切れ間近の証明書更新手順
- 3. 本システムへのログインと使い方
  - 3-1. 証明書申請手続き概要
  - 3-2. ログイン方法
  - 3-3. 本システムの画面の解説
  - 3-4. ログアウト方法

1. 本書の範囲

本書では以下（a、b、c、d、e）の作業について記述します。

マニュアル名	作業名
証明書自動発行支援システム操作手順書 (登録担当者用)	a.登録担当者が実施する本システムへのサーバ証明書の管理について b.登録担当者が実施する本システムへのクライアント証明書の管理について c.登録担当者が実施する本システムへのコード用証明書の管理について d.登録担当者が実施する本システムへの利用管理者情報の管理について e.登録担当者が本システムで扱うファイル形式について
証明書自動発行支援システム操作手順書(利用管理者用)	f.利用管理者が実施する本システムへのサーバ証明書発行申請・取得について（「支援システム操作手順書 / 利用管理者用」 2.サーバ証明書管理手順 に記載） g.利用管理者が実施する本システムへのサーバ証明書更新申請・取得について（「支援システム操作手順書 / 利用管理者用」 3.クライアント証明書管理手順 に記載） h.利用管理者が実施する本システムへのサーバ証明書失効申請について（「支援システム操作手順書 / 利用管理者用」 4.コード署名用証明書管理手順 に記載） i.本システムへの証明書アップロードフォーマットについて(「支援システム操作手順書 / 利用管理者用」 5.本システムで扱うファイル形式 に記載)
サーバ証明書インストールマニュアル※1	j.CSRと鍵ペアの作成方法について k.サーバ証明書のインストール方法について
クライアント証明書インストールマニュアル※2	l.Webブラウザへの証明書(P12)インストール手順について m.Webブラウザへインストールされた証明書(P12ファイル)の確認手順について n.S/MIME証明書インストール手順について o.デジタル署名付きメールの送信について
コード署名用証明書利用マニュアル※3	p.コード署名用証明書のインストール方法について q.コード署名用証明書を利用する手順について

※1 以下のマニュアルを総称して「サーバ証明書インストールマニュアル」と呼びます。
・証明書自動発行支援システム サーバ証明書インストールマニュアル はじめに -サーバ証明書インストールマニュアルについて-
・証明書自動発行支援システム サーバ証明書インストールマニュアル Apache(mod_ssl)編
・証明書自動発行支援システム サーバ証明書インストールマニュアル IBM HTTPServer編
・証明書自動発行支援システム サーバ証明書インストールマニュアル IIS7.5編
・証明書自動発行支援システム サーバ証明書インストールマニュアル IIS8.0・IIS8.5編
・証明書自動発行支援システム サーバ証明書インストールマニュアル IIS10.0編
・証明書自動発行支援システム サーバ証明書インストールマニュアル OpenLDAP編
・証明書自動発行支援システム サーバ証明書インストールマニュアル Tomcat編
・証明書自動発行支援システム サーバ証明書インストールマニュアル Nginx編

※2 以下のマニュアルを総称して「証明書インストールマニュアル」と呼びます。
・Webブラウザへのインストールマニュアル はじめに -Webブラウザへのインストールマニュアルについて-
・Webブラウザへのインストールマニュアル Internet Explorer・Edge・Chrome・Opera編 (Windows)
・Webブラウザへのインストールマニュアル Safari・Chrome・Opera編 (macOS)
・Webブラウザへのインストールマニュアル Firefox編 (Windows・macOS)
・Webブラウザへのインストールマニュアル Android編
・Webブラウザへのインストールマニュアル iOS編
・メーラーへのSMIME証明書インストールマニュアル はじめに -メーラーへのS/MIME証明書インストールマニュアルについて-
・メーラーへのSMIME証明書インストールマニュアル Microsoft Office Outlook編
・メーラーへのSMIME証明書インストールマニュアル Mozilla Thunderbird編
・メーラーへのSMIME証明書インストールマニュアル Apple Mail編

※3 以下のマニュアルを総称して「コード署名用証明書利用マニュアル」と呼びます。
・コード署名用証明書利用マニュアル はじめに -コード署名用証明書利用マニュアルについて-
・コード署名用証明書利用マニュアル Windows用(.exe,.cab,.dll)形式編

・コード署名用証明書利用マニュアル Windows PowerShell用スクリプト形式編
・コード署名用証明書利用マニュアル JAVA .jar形式編
・コード署名用証明書利用マニュアル Adobe AIR形式編
・コード署名用証明書利用マニュアル VBAマクロ形式編
・コード署名用証明書利用マニュアル Android用 .apk形式編

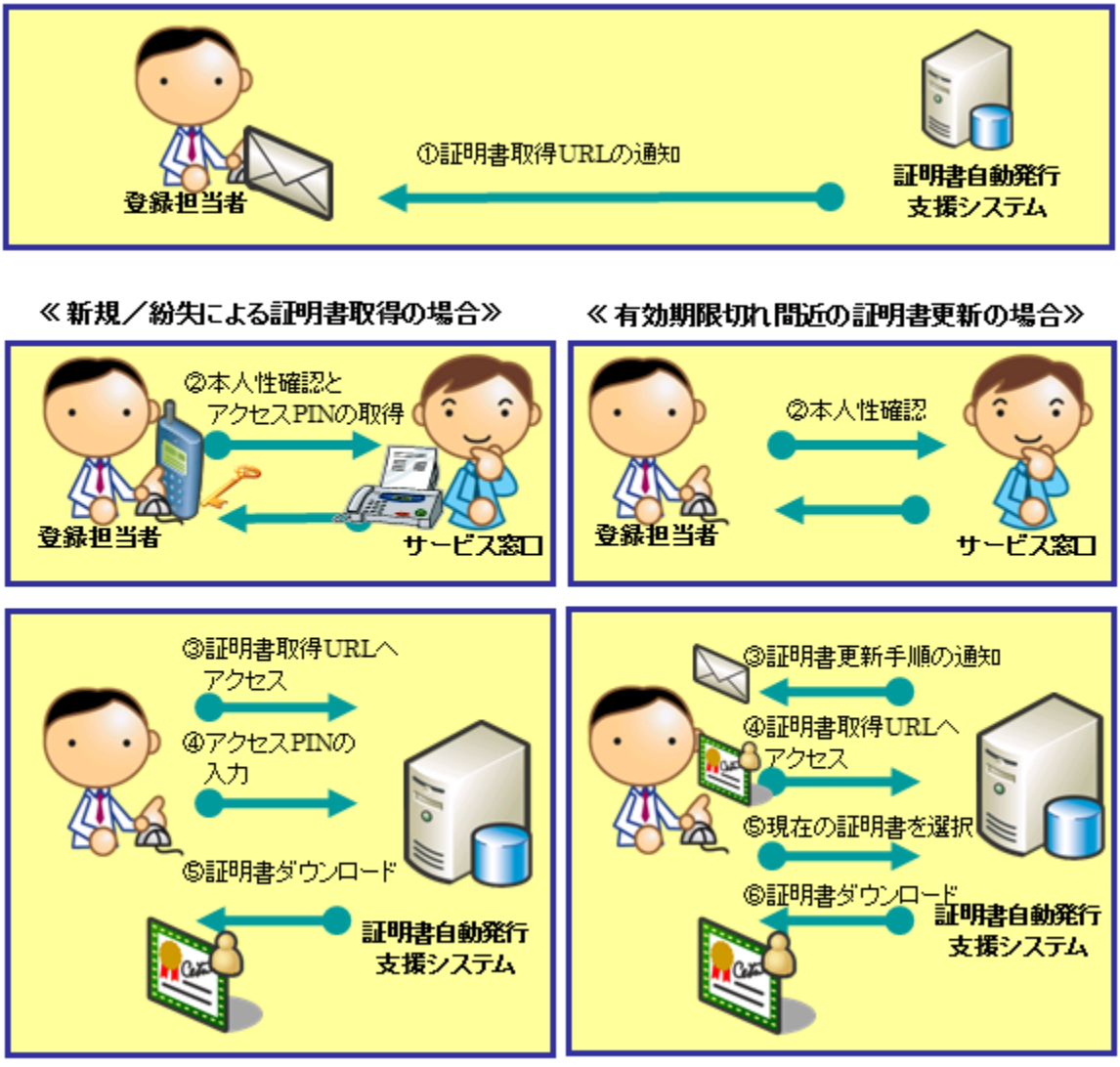
2. 登録担当者初期設定

本章では、登録担当者が本システムにログインするための証明書（以下、「登録担当者用証明書」）の取得方法、ログイン方法および登録担当者の操作画面について記述します。
本システムを利用するにあたって事前に以下のことを準備頂く必要があります。

事前確認事項
1. 所属機関がサービスに参加していること。 （サービスの参加状況につきましてはサービス窓口までお問い合わせください） 2. 登録担当者用証明書取得URLの案内メールを受信していること。

以下に、登録担当者用証明書の取得方法について記述します。

2-1. 登録担当者用証明書取得までの概要



登録担当者用証明書取得手続き概要
≪新規／紛失による証明書取得の場合≫ ①本システムから証明書取得URLを記述したメールが登録担当者宛に送信されます。受信したメールに記載された内容に従い、サービス窓口に連絡してください。 **（2-2-1に記載）** ②サービス窓口へ連絡し、本人性の確認後、アクセスPINを取得することができます。 **（2-2-2に記載）** ※アクセスPIN：証明書取得URLにアクセスするためのパスワード ③①で受信したメールに記載されている証明書取得URLへアクセスしてください。 **（2-3に記載）** ④アクセス後、②で受け取ったアクセスPINを入力してください。 ⑤アクセスPINが正しければ証明書の発行・ダウンロードが開始されます。 **≪有効期限切れ間近の証明書更新の場合≫** ①本システムから証明書取得URLを記述したメールが登録担当者宛に送信されます。受信したメールに記載された内容に従い、サービス窓口へ電話にて連絡を行ってください。 **（2-2-1に記載）** ②登録担当者用証明書による認証を行い、本人性確認を行います。 現在使用中の登録担当者用証明書をお手元に準備してください。 ③本システムから証明書更新手順を記述したメールが登録担当者宛に送信されます。 ④受信したメールに記載された内容に従い、メールに記載されている証明書取得URLへアクセスしてください。 **（2-3に記載）** ⑤アクセス後、現在使用中の登録担当者用証明書を選択してください。 ⑥証明書が正しければ証明書の発行・ダウンロードが開始されます。

2-2. 登録担当者用証明書取得事前準備

2-2-1. 証明書取得URLの通知

所属機関のサービス参加が受理されると、サービス窓口は本システムに機関情報の登録を行います。機関の登録が終了すると、登録された機関の登録担当者宛に、登録担当者用証明書の取得先URLを通知します。
以下のようなメールを本システムより受信したら、「2-2-2. アクセスPINの取得」に進んでください。
　※登録担当者用証明書取得が完了するまでこのメールは大切に保管してください。

証明書取得ＵＲＬ通知メール
【件名】 登録担当者用証明書発行受付通知 【本文】 　・・・・・ 【登録担当者用証明書取得方法】 **#以下のフォームから連絡し、アクセスPINを取得してください。** 1) 証明書取得URLに必要なアクセスPINの取得 　本メール受領後、下記問合せフォームにてご連絡ください。登録担当者本人の確認を以って、 　3)の証明書取得URLへアクセスする際に必要となるアクセスPINを、PDFにて登録担当者様宛に送信させていただきます。 　アクセスPINの取得に関するご連絡先： 　UPKIサービスデスク： https://certs.nii.ac.jp/contact/form 　アカウント作成（ご自身でサインアップ可能です）の上、お名前・ご所属と、アクセスPINを取得したい旨を記入してください。 **#以下のURLにアクセスし、証明書を取得してください。** 　2) 登録担当者用証明書の取得 次の証明書取得URLへアクセスして、登録担当者用証明書をダウンロードしてください。 証明書取得URL：https://～ ・・・・

2-2-2. アクセスPINの取得

証明書取得URLの案内メールを受信後、メール本文に記載された内容に従い、下記サービスデスクのフォームからご連絡ください。

- サービス窓口への連絡は、メールを受信した登録担当者本人が行ってください。 原則として、代理人を通したアクセスPINの通知は禁止としております。

アクセスPINの取得に関するご連絡先
UPKIサービスデスク： https://certs.nii.ac.jp/contact/form アカウント作成（ご自身でサインアップ可能です）の上、お名前・ご所属と、アクセスPINを取得したい旨を記入してください。

2-3. 登録担当者用証明書取得

アクセスPINの取得後、「2-2-1. 証明書取得URLの通知」に記載されたURLにアクセスし、登録担当者用証明書を取得してください。

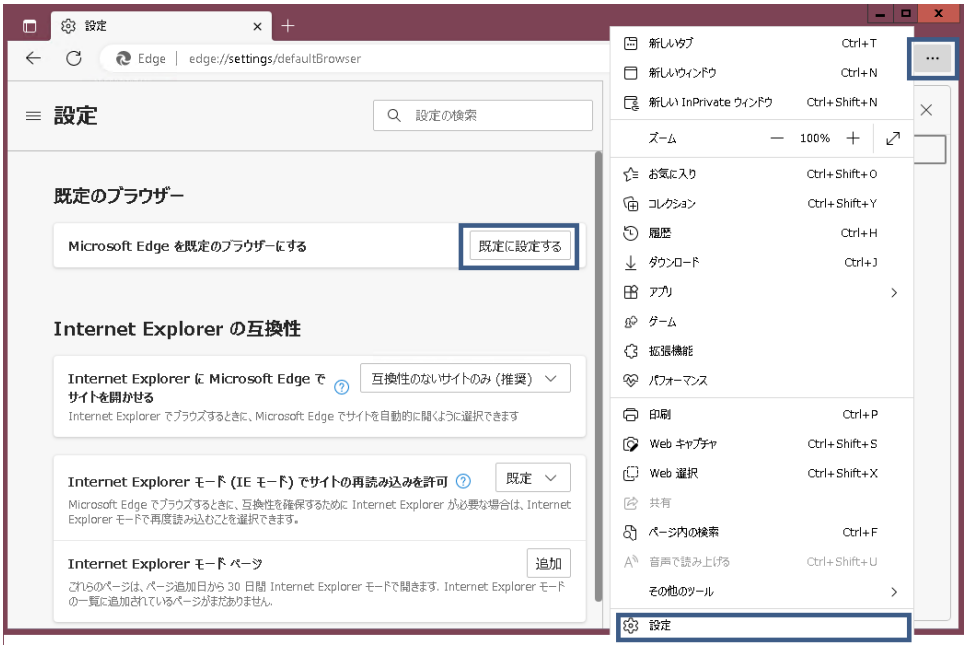
- ブラウザによって、取得方法が異なりますので注意してください。
  - **Microsoft Edge・Google Chrome： 2-3-1. Microsoft Edge・Google Chromeでの登録担当者用証明書取得手順**
  - **Firefox： 2-3-2. Firefoxでの登録担当者用証明書取得手順**

2-3-1. Microsoft Edge・Google Chromeでの登録担当者用証明書取得手順

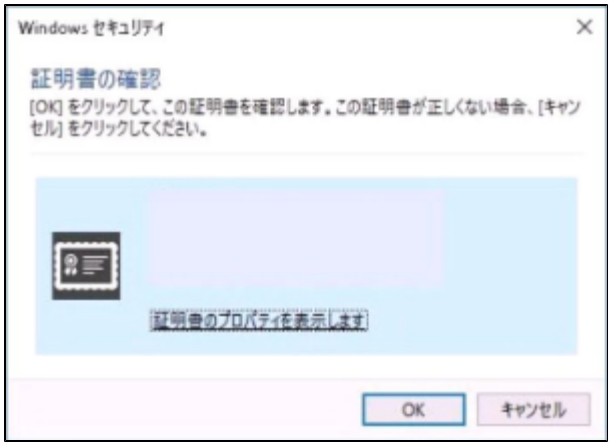
ここでは「Microsoft Edge・Google Chrome」での証明書取得について記述します。

2-3-1-1. 新規／紛失による証明書取得手順

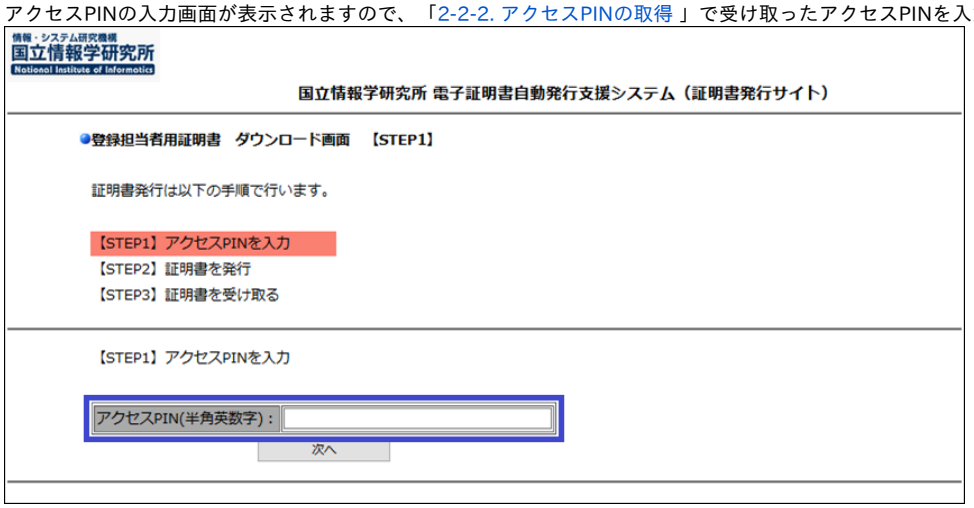
Microsoft Edge・Google Chromeでの登録担当者用証明書発行手続き
本システムを実際に利用するブラウザを「既定のブラウザ」と指定しておくことで クライアント認証（アクセス不可等）の失敗を防ぐことができます。 本書では、証明書取得前に以下の設定を行うことを推奨しています。 ブラウザより[メニュー]→[オプション]をクリック、 [一般]タブで[起動]-[Microsoft Edgeを既定のブラウザに設定する(D)]をクリックしてください。



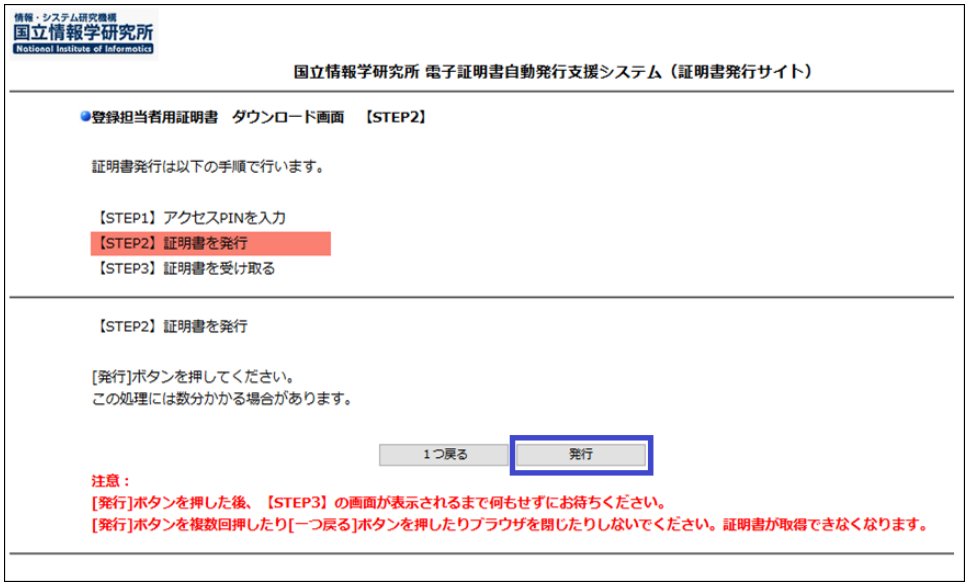
1. 「2-2-1. 証明書取得URLの案内メール受信」の指示に従って、メールに記述された証明書取得URLにアクセスしてください。
   ≪新規／紛失による証明書取得の場合≫
   デジタル証明書の選択画面が表示される場合は、キャンセルしてください。



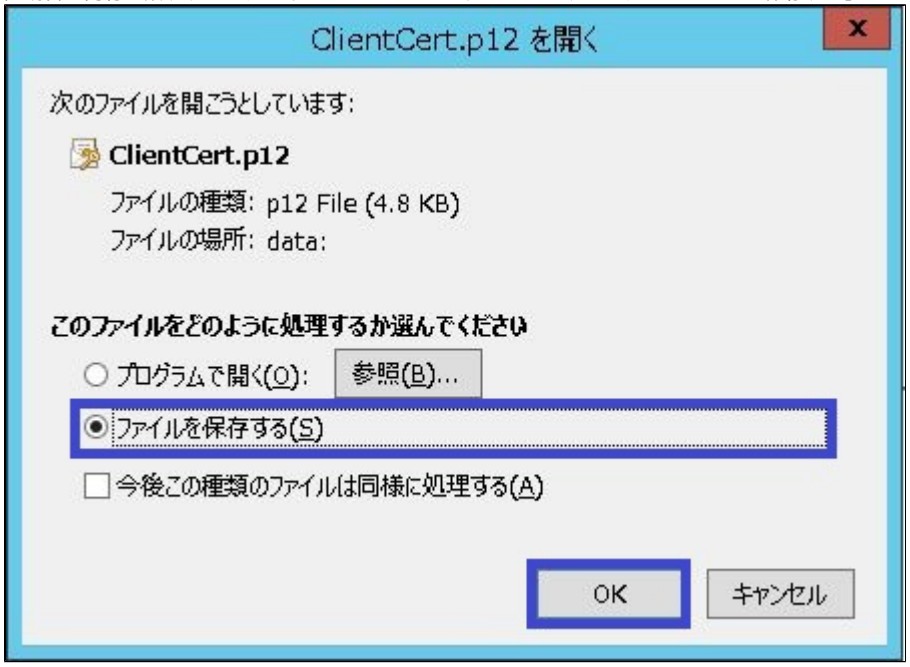
2. アクセスPINの入力画面が表示されますので、「2-2-2. アクセスPINの取得 」で受け取ったアクセスPINを入力してください。



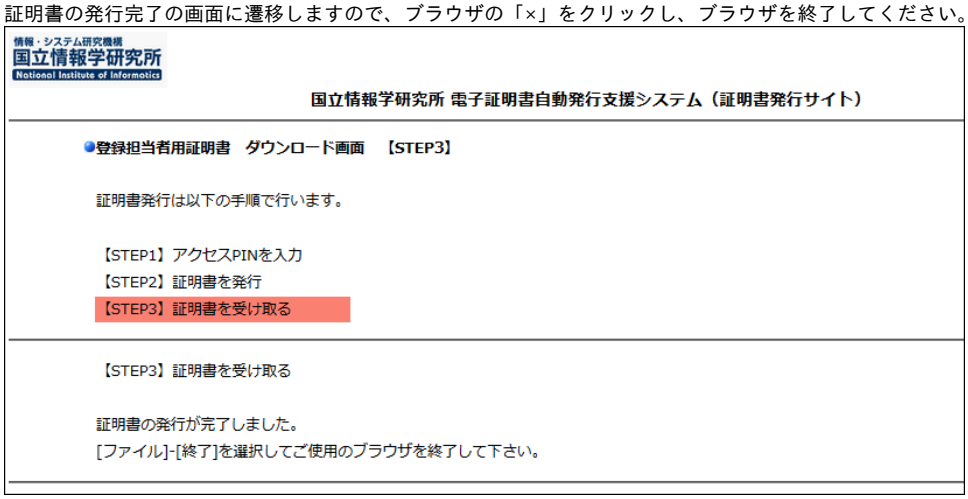
3. アクセスPINの認証が成功しましたら、[発行]を押してください。
[発行]は、1回のみ押すようにしていただき、押したあとは、[発行]を複数回押したり、[1つ戻る]を押すことのないようにお願いします。
処理に時間を要する場合がありますが、【STEP3】画面が表示されるまでお待ちください。



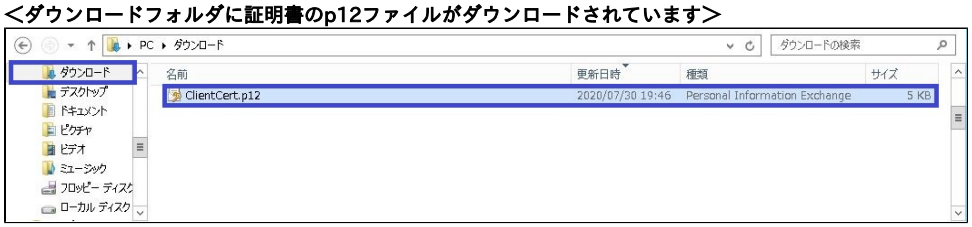
4. 証明書の発行が成功すると、以下のポップアップが表示されますので、「ファイルを保存する」にチェックを入れ、[OK]を選択してください。



5. 証明書の発行完了の画面に遷移しますので、ブラウザの「×」をクリックし、ブラウザを終了してください。



＜ダウンロードフォルダに証明書のp12ファイルがダウンロードされています＞



6. P12ファイルのインポート

   ダウンロードしたP12ファイルをインポートする必要があります。
   下記マニュアルを参照して、インポートしてください。
   証明書のインポート手順 Microsoft Internet Explorer, Edge編・Google Chrome編

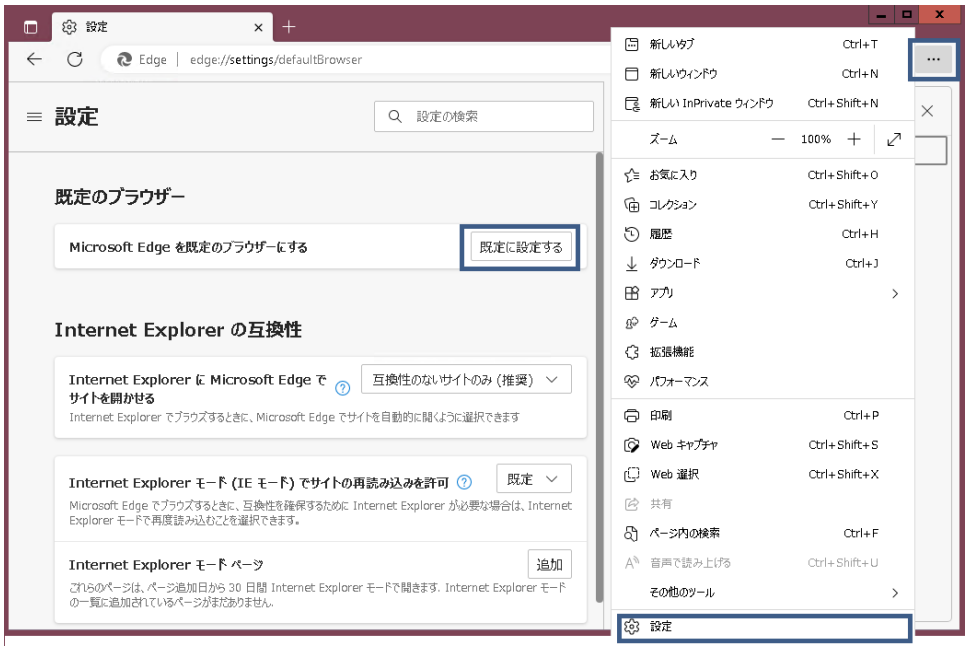
   また、このファイルをバックアップしておくことをお勧めします。ただし取り扱いには十分ご注意ください。
7. 証明書の存在確認
   証明書のインポートが完了しているかの確認は、下記マニュアルを参照してください。
   証明書の存在確認手順 Internet Explorer編

2-3-1-2. 有効期限切れ間近の証明書更新手順

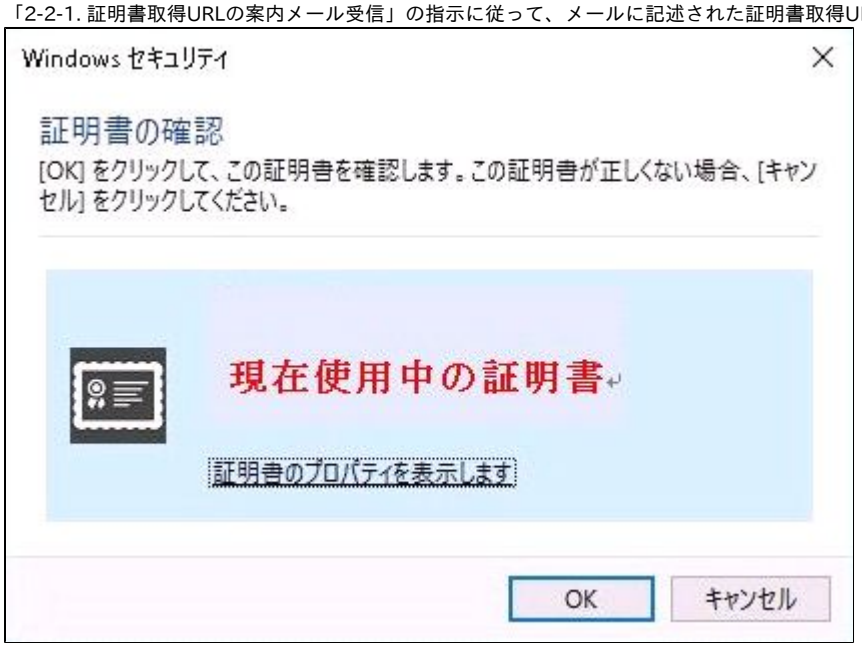
Microsoft Edge・Google Chromeでの登録担当者用証明書発行手続き

本システムを実際に利用するブラウザを「既定のブラウザ」と指定しておくことで クライアント認証（アクセス不可等）の失敗を防ぐことができます。

本書では、証明書取得前に以下の設定を行うことを推奨しています。
ブラウザより[メニュー]→[オプション]をクリック、 [一般]タブで[起動]-[Microsoft Edgeを既定のブラウザに設定する(D)]をクリックしてください。

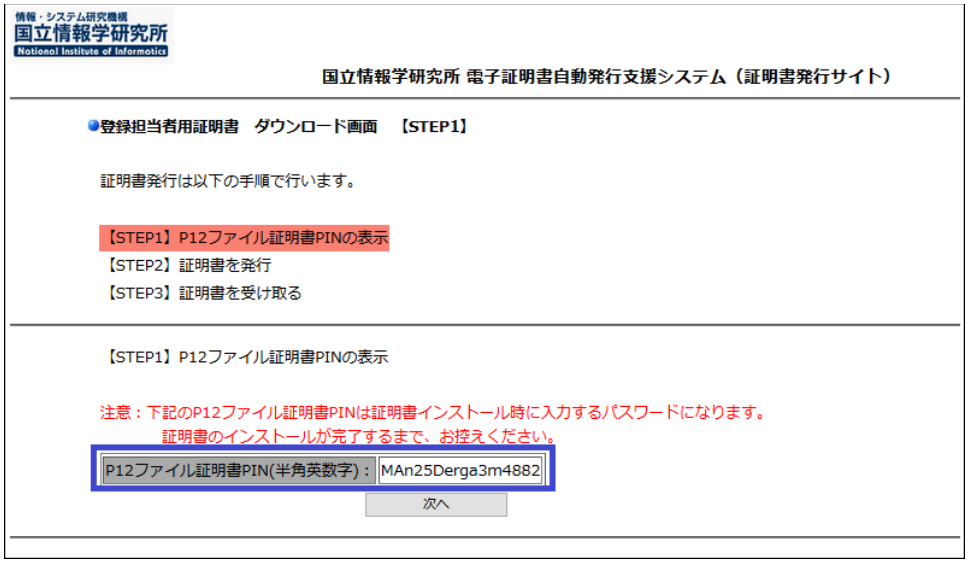


1. 「2-2-1. 証明書取得URLの案内メール受信」の指示に従って、メールに記述された証明書取得URLにアクセスしてください。

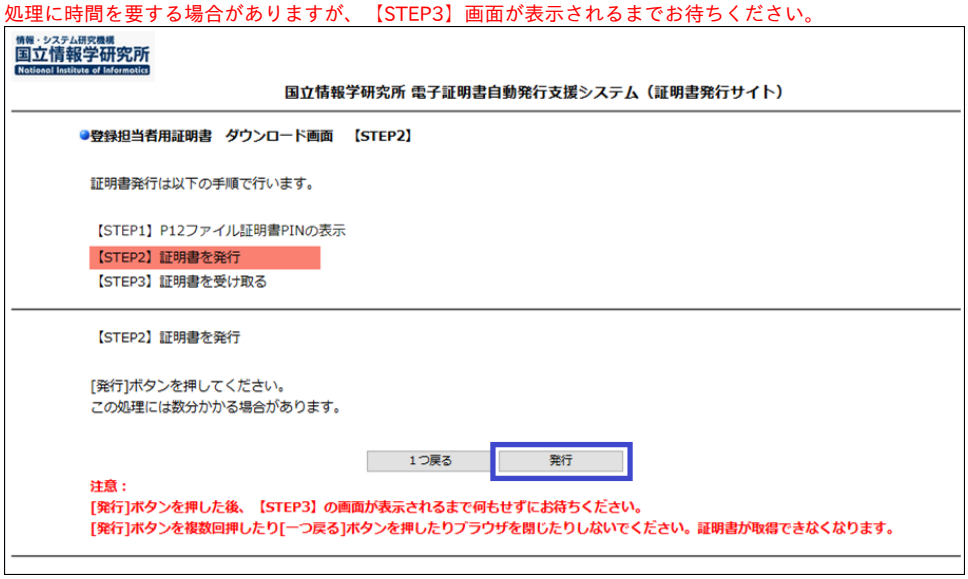


≪有効期限切れ間近の証明書更新の場合≫ 登録担当者用証明書を既に取得しており、証明書を更新する場合は、現在使用中の証明書の選択画面に表示されますので選択してください。

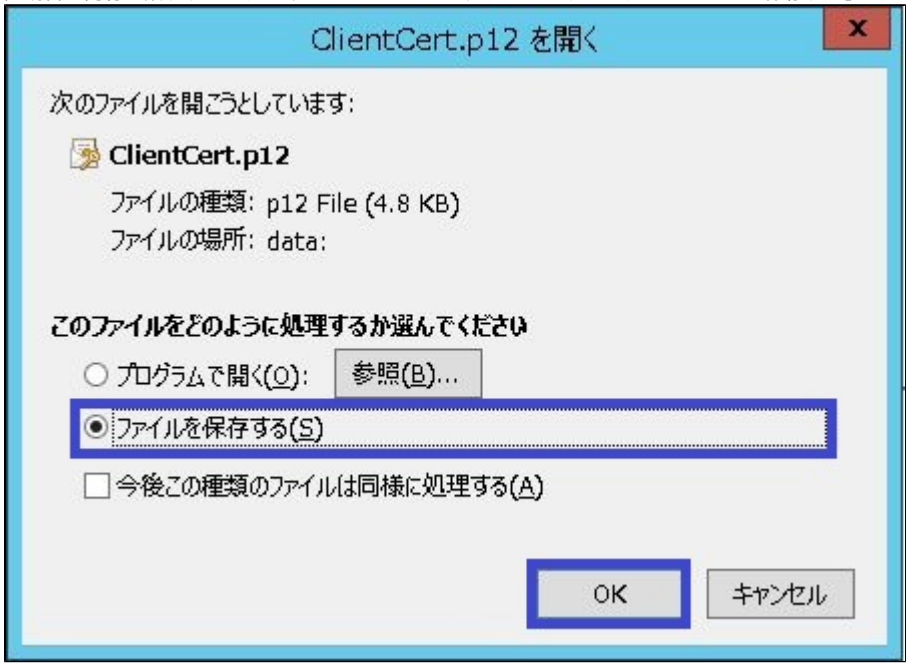
2. クライアント認証に成功しますと、以下の画面に遷移します。
「P12ファイル証明書PIN」が表示されますので、必ずお控えください。
お控えいただかなかった場合、P12ファイルのインポートが出来なくなりますので十分ご注意ください。



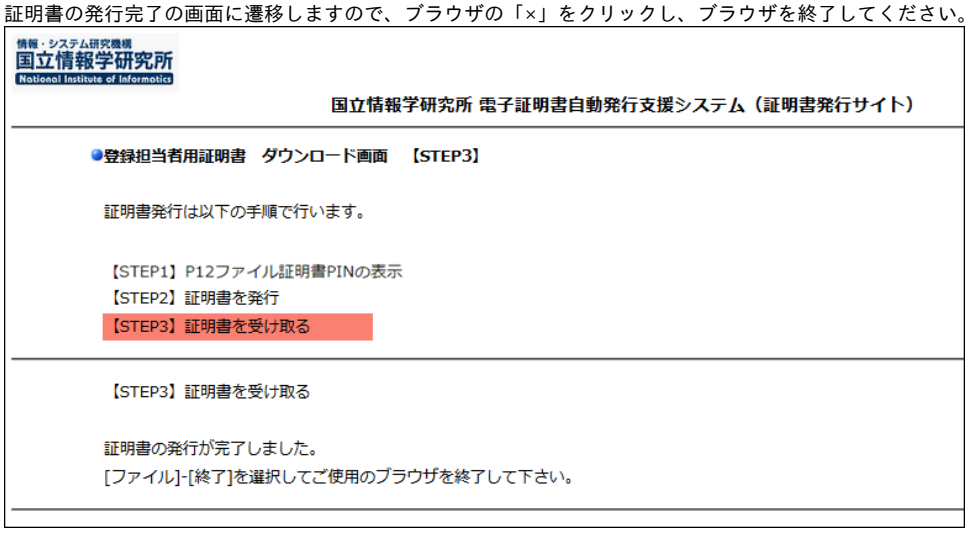
3. クライアント認証が成功しましたら、[発行]を押してください。
[発行]は、1回のみ押すようにしていただき、押したあとは、[発行]を複数回押したり、[1つ戻る]を押すことのないようにお願いします。
処理に時間を要する場合がありますが、【STEP3】画面が表示されるまでお待ちください。



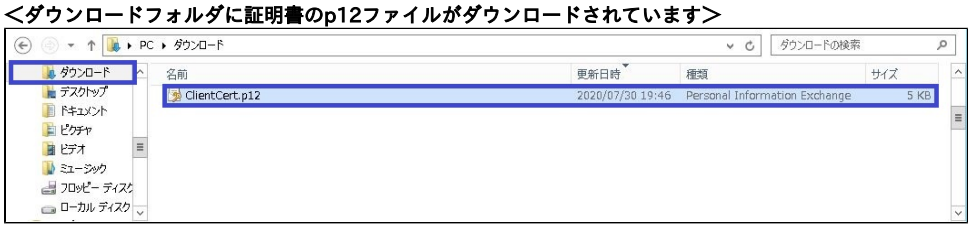
4. 証明書の発行が成功すると、以下のポップアップが表示されますので、「ファイルを保存する」にチェックを入れ、[OK]を選択してください。



5. 証明書の発行完了の画面に遷移しますので、ブラウザの「×」をクリックし、ブラウザを終了してください。



＜ダウンロードフォルダに証明書のp12ファイルがダウンロードされています＞



6. P12ファイルのインポート

   ダウンロードしたP12ファイルをインポートする必要があります。
   下記マニュアルを参照して、インポートしてください。
   証明書のインポート手順 Microsoft Internet Explorer, Edge編・Google Chrome編

   また、このファイルをバックアップしておくことをお勧めします。ただし取り扱いには十分ご注意ください。
7. 証明書の存在確認
   証明書のインポートが完了しているかの確認は、下記マニュアルを参照してください。
   証明書の存在確認手順 Internet Explorer編

2-3-2. Firefoxでの登録担当者用証明書取得手順

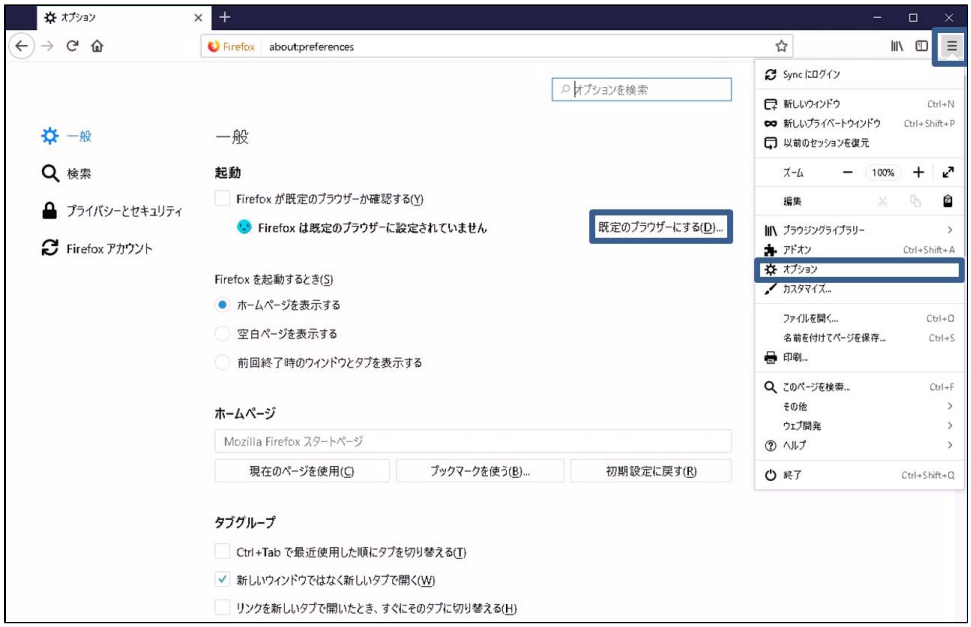
ここでは「Firefox(OS:windows10)」での証明書取得について記述します。

> **<Firefoxでのブラウザ発行につきまして>**
> Firefox Version 68以降をご利用ください。

2-3-2-1. 新規／紛失による証明書取得手順

Firefox(OS:Windows10での登録担当者用証明書発行手続き

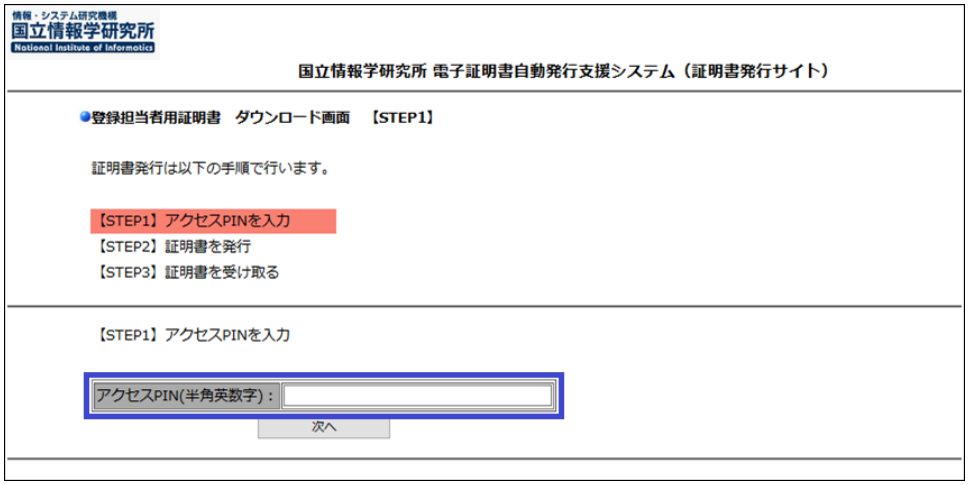
本システムを実際に利用するブラウザを「既定のブラウザ」と指定しておくことで クライアント認証（アクセス不可等）の失敗を防ぐことができます。
本書では、証明書取得前に以下の設定を行うことを推奨しています。
ブラウザより[メニュー]→[オプション]をクリック、 [一般]タブで[起動]-[Firefoxを既定のブラウザに設定する(D)]をクリックしてください。



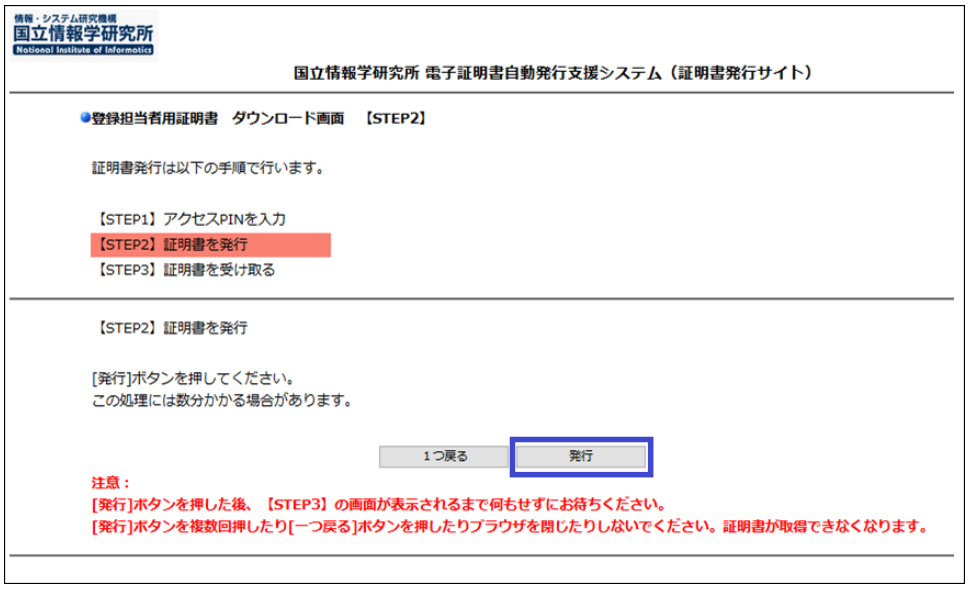
1. 「2-2-1. 証明書取得URLの案内メール受信」の指示に従って、メールに記述された証明書取得URLにアクセスしてください。
   アクセスPINの入力画面が表示されますので、「2-2-2. アクセスPINの取得 」で受け取ったアクセスPINを入力してください。
   デジタル証明書の選択画面が表示される場合は、キャンセルしてください。



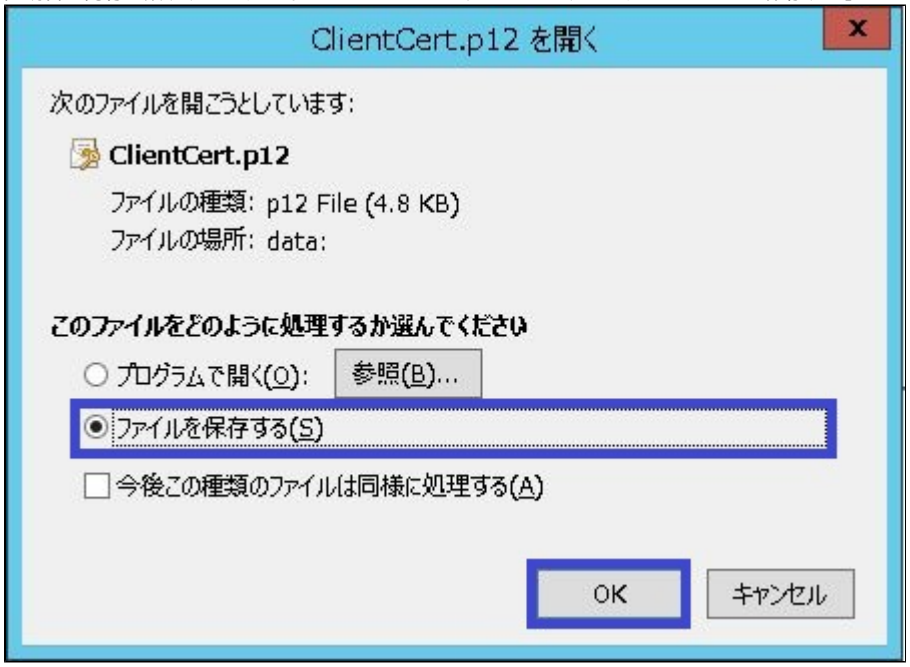
下記の画面に遷移した後、「アクセスPIN（半角英数字）」欄にアクセスPINを入力してください。



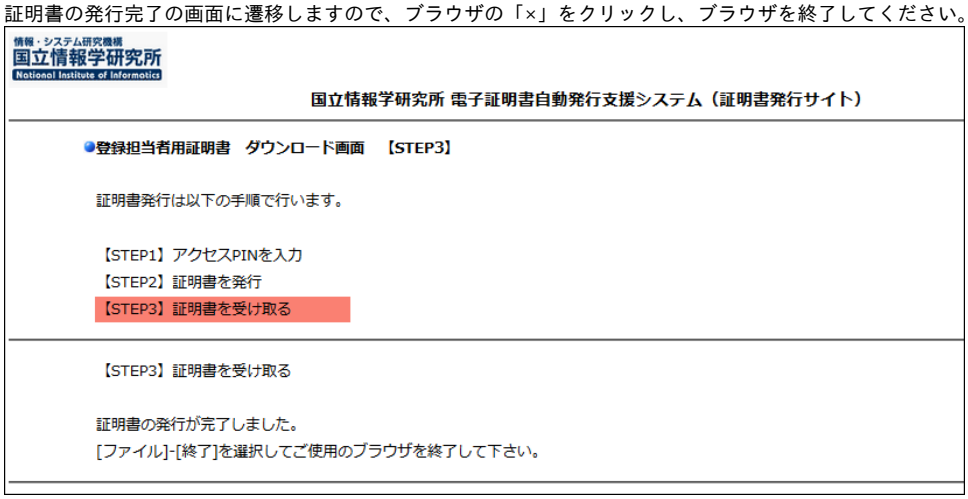
2. アクセスPINの認証が成功しましたら、[発行]を押してください。
[発行]は、1回のみ押すようにしていただき、押したあとは、[発行]を複数回押したり、[1つ戻る]を押すことのないようにお願いします。
処理に時間を要する場合がありますが、【STEP3】画面が表示されるまでお待ちください。



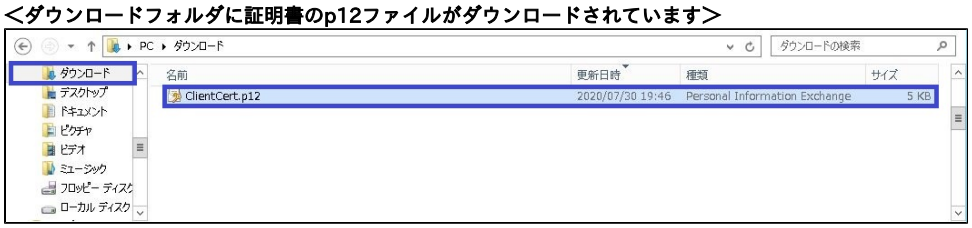
3. 証明書の発行が成功すると、以下のポップアップが表示されますので、「ファイルを保存する」にチェックを入れ、[OK]を選択してください。



4. 証明書の発行完了の画面に遷移しますので、ブラウザの「×」をクリックし、ブラウザを終了してください。



＜ダウンロードフォルダに証明書のp12ファイルがダウンロードされています＞



5. P12ファイルのインポート

   ダウンロードしたP12ファイルをFirefoxにインポートする必要があります。
   下記マニュアルを参照して、インポートしてください。
   証明書のインポート手順 Firefox編

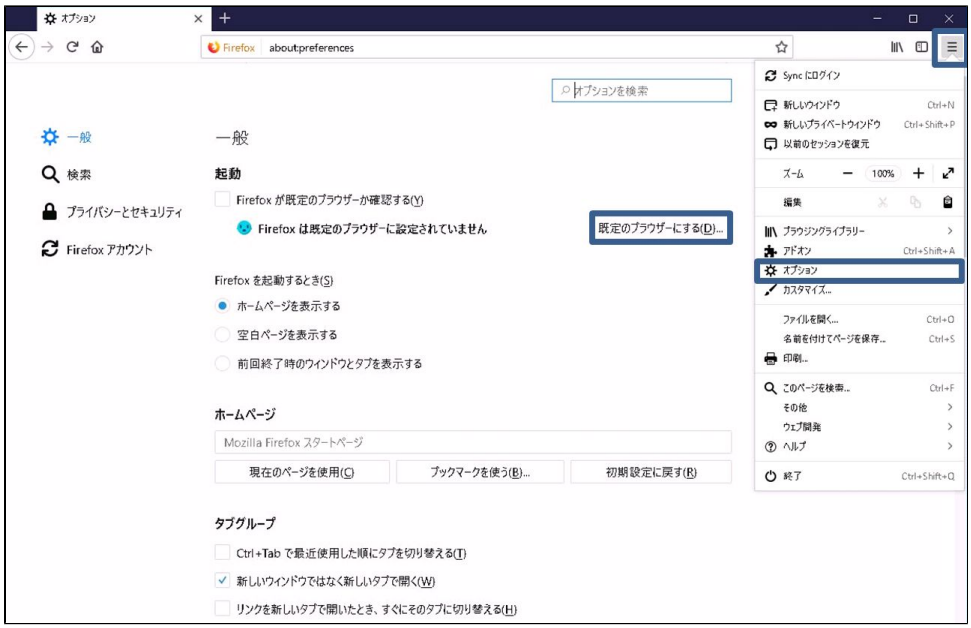
   また、このファイルをバックアップしておくことをお勧めします。ただし取り扱いには十分ご注意ください。
6. 証明書の存在確認
   証明書のインポートが完了しているかの確認は、下記マニュアルを参照してください。
   証明書の存在確認手順 Firefox編

Firefoxをリフレッシュしますと取得した証明書も削除されます。削除により証明書が失われた場合は、一連の作業(申請～発行～インストール)全てがやり直しとなってしまうため、十分ご注意ください。

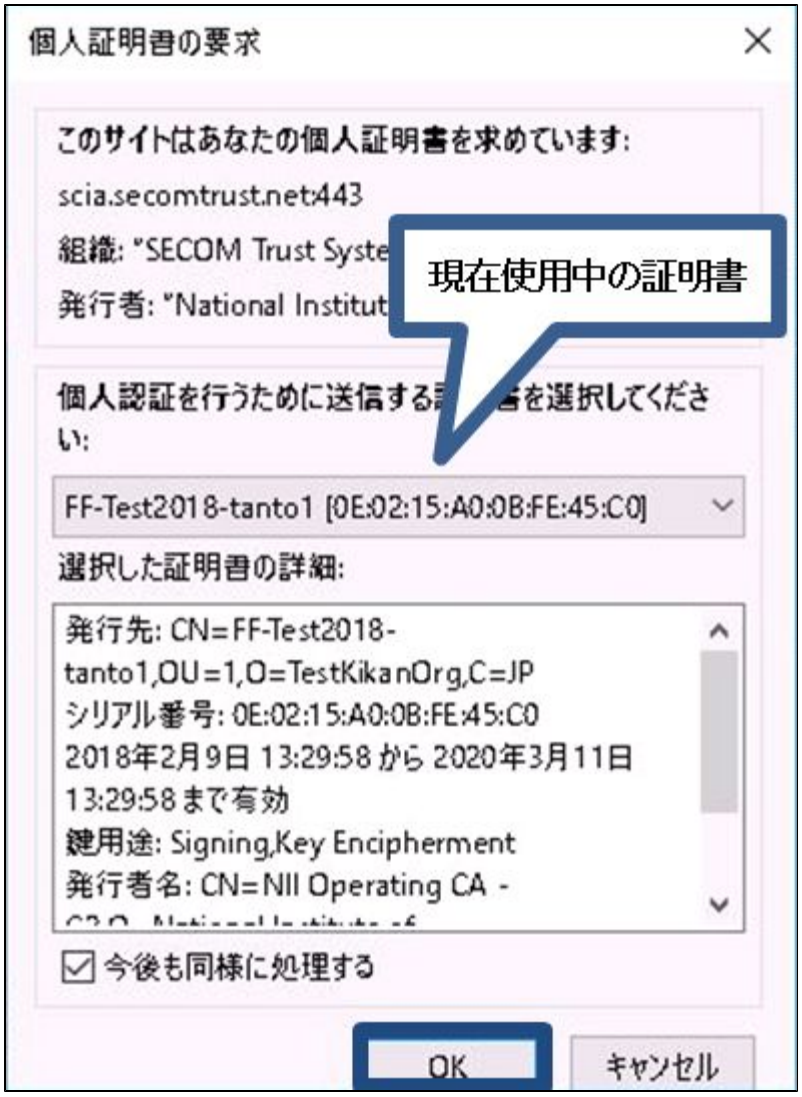
2-3-2-2. 有効期限切れ間近の証明書更新手順

Firefox(OS:Windows10での登録担当者用証明書発行手続き

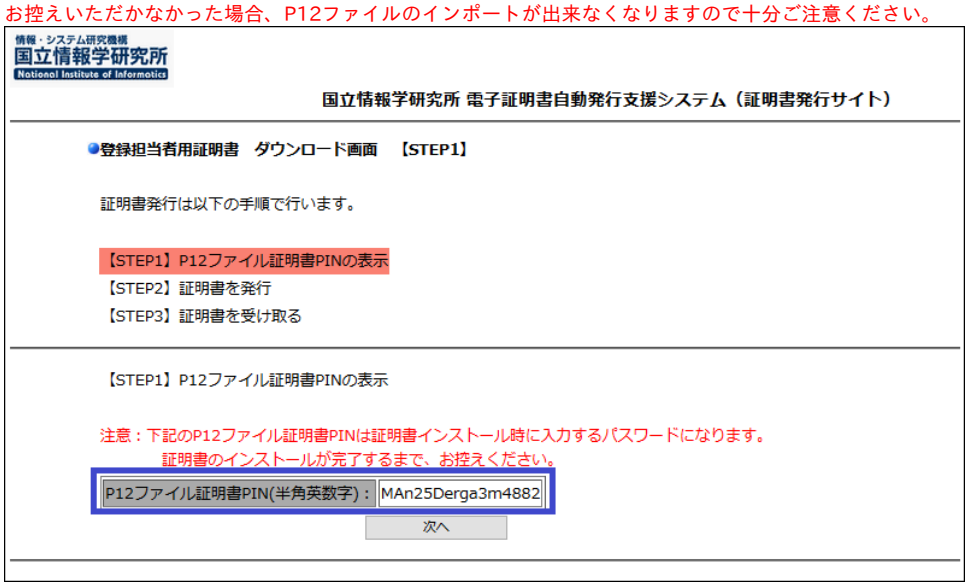
本システムを実際に利用するブラウザを「既定のブラウザ」と指定しておくことで クライアント認証（アクセス不可等）の失敗を防ぐことができます。
本書では、証明書取得前に以下の設定を行うことを推奨しています。
ブラウザより[メニュー]→[オプション]をクリック、 [一般]タブで[起動]-[Firefoxを既定のブラウザに設定する(D)]をクリックしてください。



1. 「2-2-1. 証明書取得URLの案内メール受信」の指示に従って、メールに記述された証明書取得URLにアクセスしてください。
   登録担当者用証明書を既に取得しており、証明書を更新する場合は、現在使用中の証明書の選択画面に表示されますので選択してください。

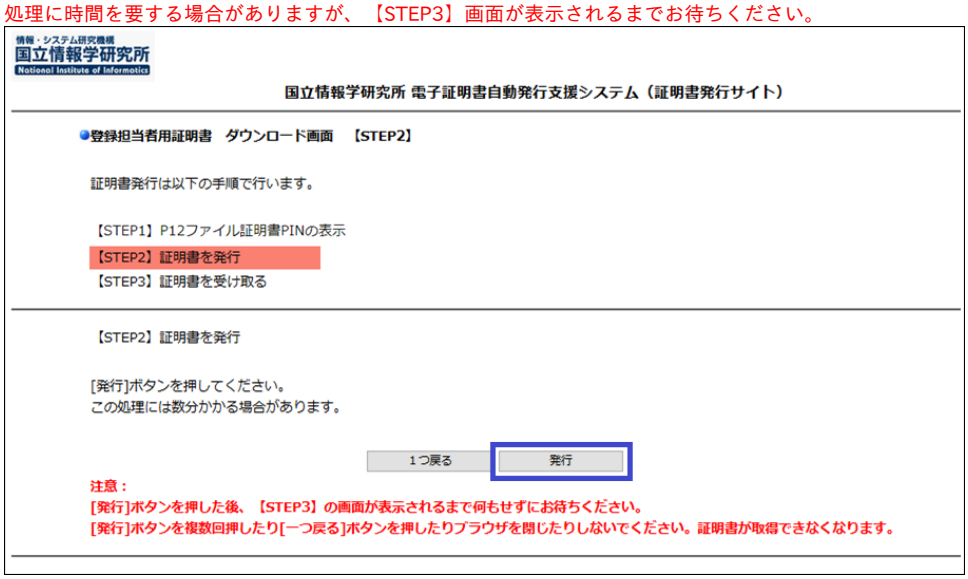


クライアント認証に成功しますと、以下の画面に遷移します。
「P12ファイル証明書PIN」が表示されますので、必ずお控えください。
お控えいただかなかった場合、P12ファイルのインポートが出来なくなりますので十分ご注意ください。

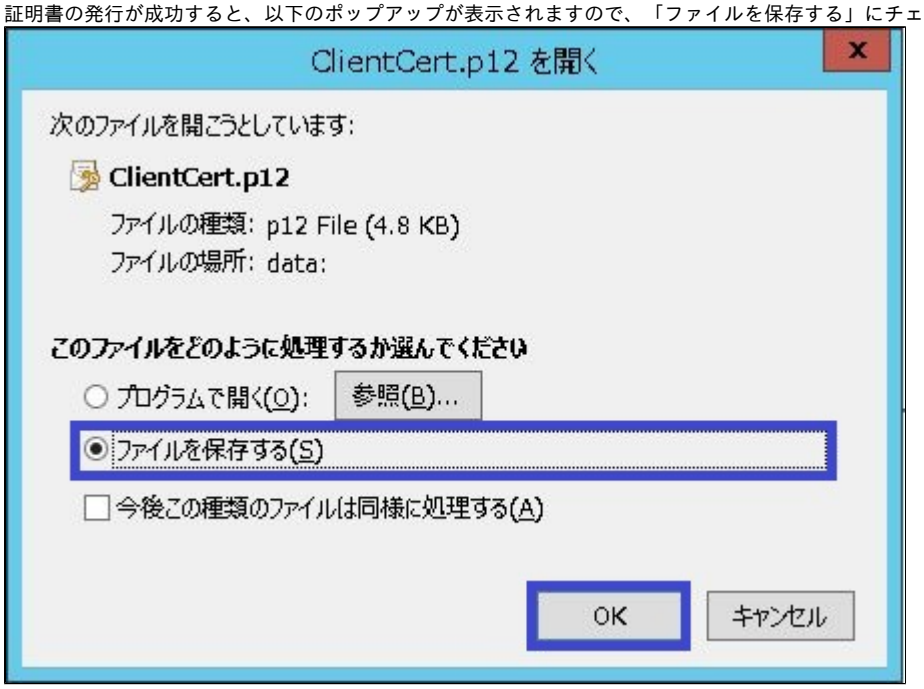


2. クライアント認証が成功しましたら、[発行]を押してください。
[発行]は、1回のみ押すようにしていただき、押したあとは、[発行]を複数回押したり、[1つ戻る]を押すことのないようにお願いします。

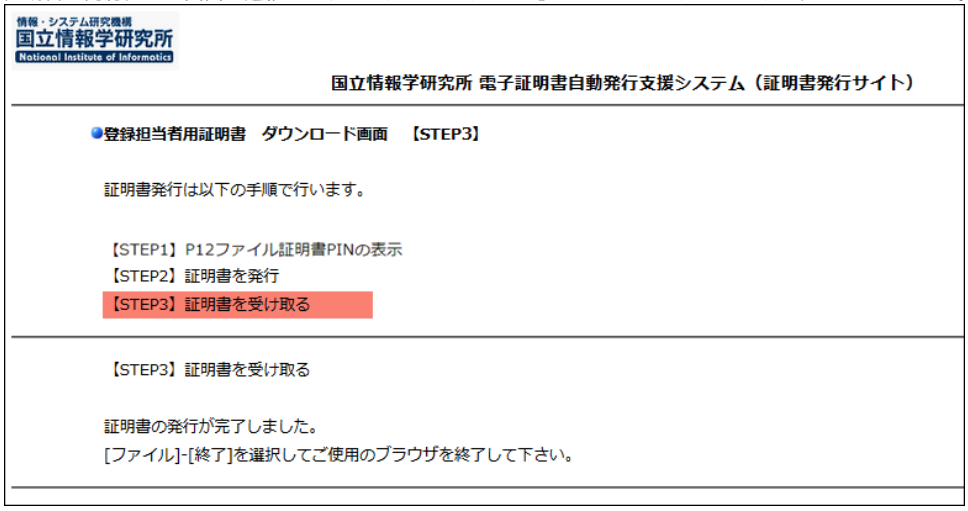
処理に時間を要する場合がありますが、【STEP3】画面が表示されるまでお待ちください。



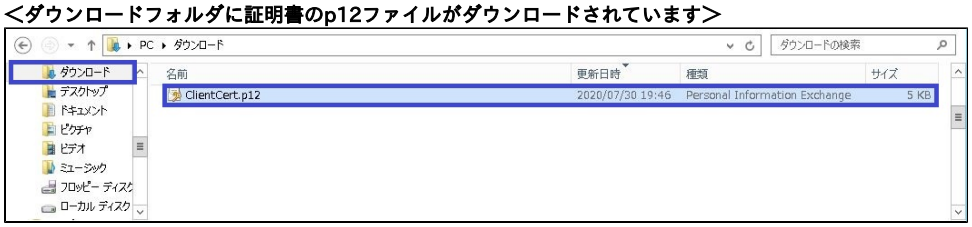
3. 証明書の発行が成功すると、以下のポップアップが表示されますので、「ファイルを保存する」にチェックを入れ、[OK]を選択してください。



4. 証明書の発行完了の画面に遷移しますので、ブラウザの「×」をクリックし、ブラウザを終了してください。



＜ダウンロードフォルダに証明書のp12ファイルがダウンロードされています＞



5. P12ファイルのインポート

   ダウンロードしたP12ファイルをFirefoxにインポートする必要があります。
   下記マニュアルを参照して、インポートしてください。
   証明書のインポート手順 Firefox編

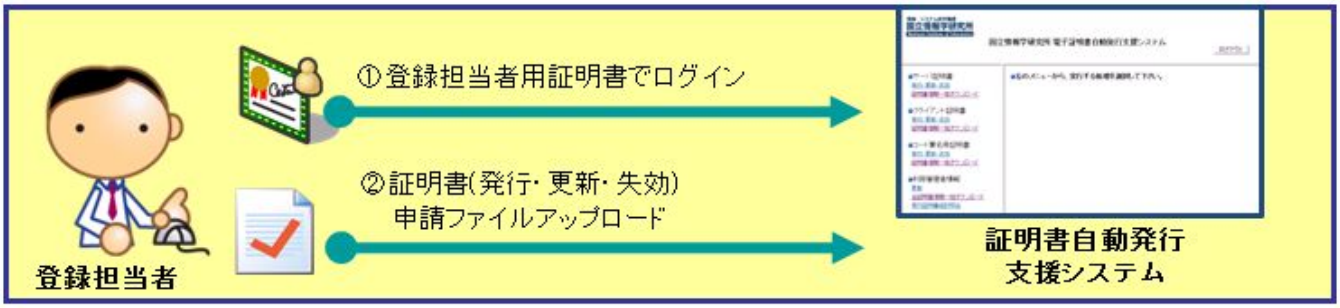
   また、このファイルをバックアップしておくことをお勧めします。ただし取り扱いには十分ご注意ください。
6. 証明書の存在確認
   証明書のインポートが完了しているかの確認は、下記マニュアルを参照してください。
   証明書の存在確認手順 Firefox編

Firefoxをリフレッシュしますと取得した証明書も削除されます。削除により証明書が失われた場合は、一連の作業(申請～発行～インストール)全てがやり直しとなってしまうため、十分ご注意ください。

3. 本システムへのログインと使い方

本章では本システムにアクセスするまでの流れ、本システムの機能について記述します。

3-1. 証明書申請手続き概要



証明書申請手続き概要
[2-3. 登録担当者用証明書取得]で取得した登録担当者用証明書を用いて本システムにログインしてください。 **(3-2に記載)** URL: https://scia.secomtrust.net/upki-odcert/lra/SSLLogin.do

サーバ証明書の発行・更新・失効申請を行います。（「サーバ証明書管理手順」 に記載）
クライアント証明書の発行・更新・失効申請を行います。（「クライアント証明書管理手順」 に記載）
コード署名用証明書の失効申請を行います。（「コード署名用証明書管理手順」 に記載）

ログインするブラウザに、「2-3. 登録担当者用証明書取得」で記述した証明書が導入済みであることをご確認下さい。

3-2. ログイン方法

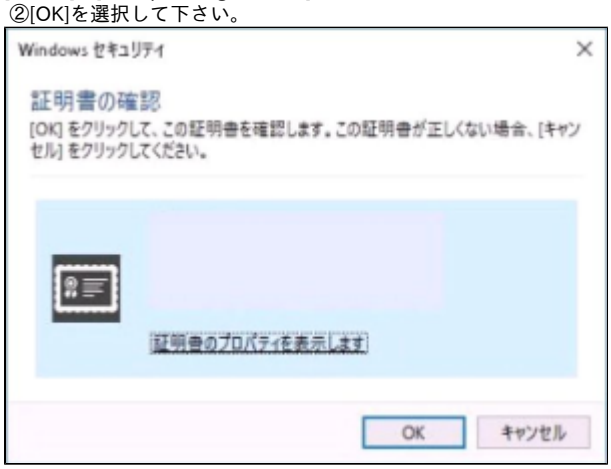
「2-3. 登録担当者用証明書取得」で記述したとおり、ブラウザに登録担当者用証明書を事前にインストールしてください。事前に取得した登録担当者用証明書を用いて、本システムへログインする方法を記述します。

本システムURL	https://scia.secomtrust.net/upki-odcert/lra/SSLLogin.do

本システムへのアクセス方法

1. [2-3. 登録担当者用証明書取得]にて証明書をインストールしたブラウザで以下のURLにアクセスしてください。
   URL: https://scia.secomtrust.net/upki-odcert/lra/SSLLogin.do
   ※ブラウザの「お気に入り」などに上記URLを保存しておくことをお勧めします。

2. アクセスするとクライアント認証のための証明書の確認画面が表示されます。
   ①デジタル証明書欄で[2-3.登録担当者用証明書取得]にて証明書をダウンロードした証明書が選択されていることを確認します。
   [名前]：機関情報申請tsvファイルにて指定した[登録担当者氏名の英字]項目のローマ字が表示されます。
   [発行者]：[NII Operating CA - G2]が表示されます。
   ②[OK]を選択して下さい。



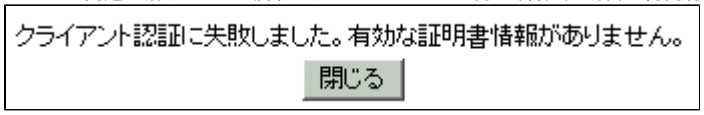
3. SSLクライアント認証が完了し、以下の画面が表示されればログイン成功です。



以下の画面がでる場合、登録担当者用証明書が失効されているか証明書が無効です。

クライアント認証の失敗画面がでると本システムを利用することができませんので、

選択した登録担当者用証明書が適切な証明書か再度確認してください。
それでも問題が解決しない場合、サービス窓口へ登録担当者用証明書の再発行を依頼してください。



登録担当者用証明書の中間CA切り替え後（2023/12/14以降）、特定の条件下でご利用いただいた場合に証明書が複数表示されることがあります。
「CA切り替え後」に登録担当者用証明書（SECOM Passport for Member RSA CA16から発行された証明書）を発行し、インポートした状態の端末（パソコン等）で、個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされますと、UPKI電子証明書発行サービスにアクセスした際、下記画面のように複数の証明書が表示されるようになりますので、その場合は、登録担当者用証明書を選択していただく必要があります。
登録担当者用証明書は、証明書選択後に「証明書情報」から証明書情報を表示し、サブジェクトに「L=Academe-ops」が固定値で設定されていることから判別可能です。
もし、端末に個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされなければ、選択画面は表示されません。

a. **登録担当者用証明書の中間CA切り替え後（2023/12/14以降）、特定の条件下でご利用いただいた場合に証明書が複数表示されることがあります。**
「CA切り替え後」に登録担当者用証明書（SECOM Passport for Member RSA CA16から発行された証明書）を発行し、インポートした状態の端末（パソコン等）で、個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされますと、UPKI電子証明書発行サービスにアクセスした際、下記画面のように複数の証明書が表示されるようになりますので、その場合は、登録担当者用証明書を選択していただく必要があります。
登録担当者用証明書は、証明書選択後に「証明書情報」から証明書情報を表示し、サブジェクトに「L=Academe-ops」が固定値で設定されていることから判別可能です。
もし、端末に個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされなければ、選択画面は表示されません。



「CA切り替え前」は、「NII Operating CA - G2」からしか、登録担当者証明書が発行されないため、システムで登録担当者証明書を特定できるので、選択画面が表示されなかったものになります。

もし、証明書選択画面で個人認証用証明書を選択した場合は、UPKI電子証明書発行サービスにアクセス権限がないためログインできませんので、ご注意ください。
その場合は、一旦、ブラウザを閉じて開き直し、登録担当者用証明書を選択すればログイン可能になります。

b. **登録担当者用証明書の中間CA切り替え後（2023/12/14以降）、特定の条件下でご利用いただいた場合に証明書が複数表示されることがあります。**

「CA切り替え後」に登録担当者用証明書（SECOM Passport for Member RSA CA16から発行された証明書）を発行し、インポートした状態の端末（パソコン等）で、個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされますと、UPKI電子証明書発行サービスにアクセスした際、下記画面のように複数の証明書が表示されるようになりますので、その場合は、登録担当者用証明書を選択していただく必要があります。
登録担当者用証明書は、証明書選択後に「証明書情報」から証明書情報を表示し、サブジェクトに「L=Academe-ops」が固定値で設定されていることから判別可能です。
もし、端末に個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされなければ、選択画面は表示されません。



「CA切り替え前」は、「NII Operating CA - G2」からしか、登録担当者証明書が発行されないため、システムで登録担当者証明書を特定できるので、選択画面が表示されなかったものになります。

もし、証明書選択画面で個人認証用証明書を選択した場合は、UPKI電子証明書発行サービスにアクセス権限がないためログインできませんので、ご注意ください。
その場合は、一旦、ブラウザを閉じて開き直し、登録担当者用証明書を選択すればログイン可能になります。

c. **登録担当者用証明書の中間CA切り替え後（2023/12/14以降）、特定の条件下でご利用いただいた場合に証明書が複数表示されることがあります。**

「CA切り替え後」に登録担当者用証明書（SECOM Passport for Member RSA CA16から発行された証明書）を発行し、インポートした状態の端末（パソコン等）で、個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされますと、UPKI電子証明書発行サービスにアクセスした際、下記画面のように複数の証明書が表示されるようになりますので、その場合は、登録担当者用証明書を選択していただく必要があります。
登録担当者用証明書は、証明書選択後に「証明書情報」から証明書情報を表示し、サブジェクトに「L=Academe-ops」が固定値で設定されていることから判別可能です。
もし、端末に個人認証用証明書（SECOM Passport for Member RSA CA16から発行された証明書）がインポートされなければ、選択画面は表示されません。



「CA切り替え前」は、「NII Operating CA - G2」からしか、登録担当者証明書が発行されないため、システムで登録担当者証明書を特定できるので、選択画面が表示されなかったものになります。

もし、証明書選択画面で個人認証用証明書を選択した場合は、UPKI電子証明書発行サービスにアクセス権限がないためログインできませんので、ご注意ください。
その場合は、一旦、ブラウザを閉じて開き直し、登録担当者用証明書を選択すればログイン可能になります。



「CA切り替え前」は、「NII Operating CA - G2」からしか、登録担当者証明書が発行されないため、システムで登録担当者証明書を特定できるので、選択画面が表示されなかったものになります。

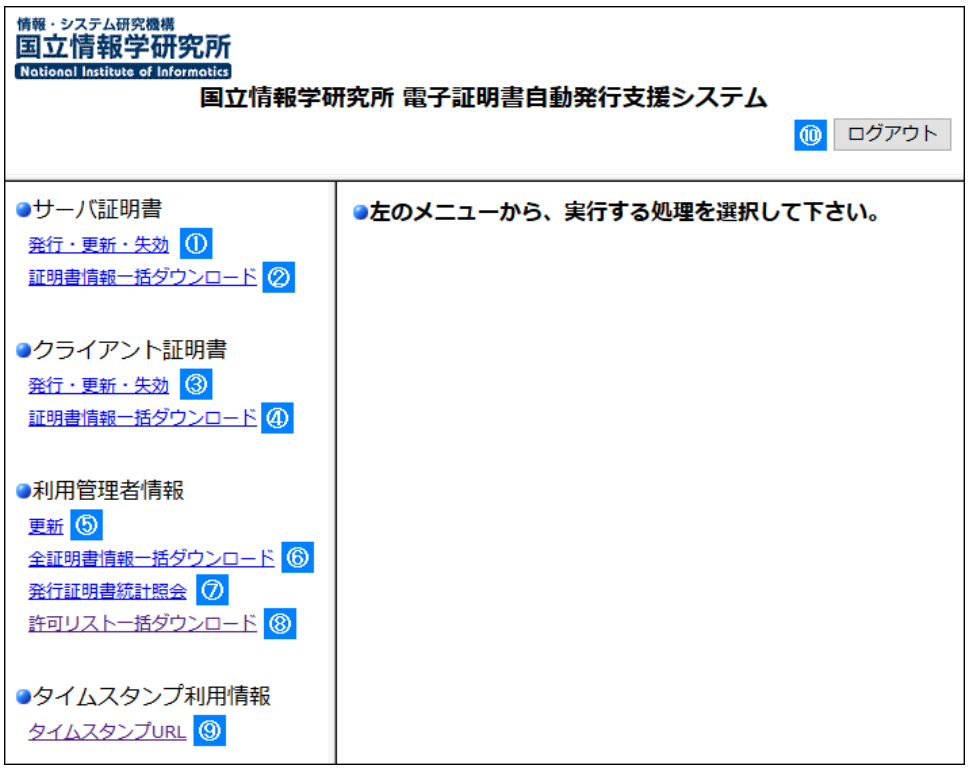
もし、証明書選択画面で個人認証用証明書を選択した場合は、UPKI電子証明書発行サービスにアクセス権限がないためログインできませんので、ご注意ください。
その場合は、一旦、ブラウザを閉じて開き直し、登録担当者用証明書を選択すればログイン可能になります。

3-3. 本システムの画面の解説

本システムのインターフェースの説明を行います。

本システムインターフェースの説明

1. 本システムは「**サーバ証明書-発行・更新・失効**」、「**サーバ証明書-証明書一括ダウンロード**」、「**クライアント証明書-発行・更新・失効**」、「**クライアント証明書-証明書一括ダウンロード**」、「**利用管理者情報-更新**」、「**利用管理者情報-全証明書情報一括ダウンロード**」、「**利用管理者情報-発行証明書統計照会**」、「**利用管理者情報-許可リスト一括ダウンロード**」、「**タイムスタンプ利用情報-タイムスタンプURL**」、「**ログアウト**」の10個のインターフェースを持ちます。各インターフェースの機能は以下の「インターフェースの詳細説明」のとおりです。



【インターフェースの詳細説明】

サーバ証明書	①発行・更新・失効	サービス参加機関のサーバ証明書の発行・更新・失効に使用
	②証明書情報一括ダウンロード	本システムより発行したサーバ証明書の情報を取得するときに使用
クライアント証明書	③発行・更新・失効	サービス参加機関のクライアント証明書の発行・更新・失効に使用
	④証明書情報一括ダウンロード	本システムより発行したクライアント証明書の情報を取得するときに使用
利用管理者情報	⑤更新	本システムより申請を行った利用管理者情報を更新するときに使用
	⑥全証明書情報一括ダウンロード	本システムより申請を行った利用管理者情報を取得するときに使用
	⑦発行証明書統計照会	本システムにて、各ドメインごとに発行状況の統計を表示するときに使用
	⑧許可リスト一括ダウンロード	本システムにて、各ドメインごとに許可されたサーバ証明書で指定可能な「OU」を表示するときに使用
タイムスタンプ利用情報	⑨タイムスタンプURL	タイムスタンプクライアント(例 SigntoolやAcrobat)で利用可能なタイムスタンプURLを参照する際に使用
ログアウト	⑩ログアウト	本システムからログアウトするときに使用

※権限の付与状況により表示されるインターフェースが異なります。

3-4. ログアウト方法

「3-3. 本システムの画面の解説」で説明した【⑩ログアウト】のボタンを選択することで、本システムからログアウトし、セッションをクリアすることができます。



ログアウトボタンを押さずに本システムとのセッションを遮断した場合、本システム作業者のログアウト情報をログに記録することができません。作業終了後は可能な限りログアウトボタンをクリック作業を終了してください。