クライアント証明書管理手順

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
V1.8	2017/7/25	ホップアップメッセージの修正	NII
V2.0	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
V2.1	2018/7/9	メールテンプレートにおけるLの修正とSTの追記 誤植の修正	NII
V2.2	2020/6/4	システム画面の画像の変更	NII
V2.3	2020/7/15	機関の審査が完了していない場合などのエラーメッセージ、原因、対処方法を追記	NII
V.2.4	2021/3/30	システム画面の画像の変更	NII

目次

1. クライアント証明書管理手順
1-1. 証明書ダウンロード方法ごとの操作手順
1-2. クライアント証明書新規発行
1-2-1. 利用管理者によるクライアント証明書新規発行申請TSVファイル作成
1-2-2. TSVファイルの受け取り及び審査
1-2-3. クライアント証明書新規発行申請TSVファイルのアップロード
1-2-4. アクセスPIN取得URLの通知
1-2-5. アクセスPIN取得URLの引き渡し
1-2-6. ダウンロード完了通知メール受信
1-3. クライアント証明書更新発行
1-3-1. 利用管理者によるクライアント証明書更新申請TSVファイル作成
1-3-2. TSVファイルの受け取り及び審査
1-3-3. クライアント証明書更新申請TSVファイルのアップロード
1-3-4. アクセスPIN取得URLの通知
1-3-5. アクセスPIN取得URLの引き渡し
1-3-6. ダウンロード完了通知メール受信
1-3-7. 新クライアント証明書への置き換え完了通知
1-3-8. 旧クライアント証明書失効TSVファイルのアップロード
1-3-9. 旧クライアント証明書失効完了通知メール受信
1-4. クライアント証明書失効
1-4-1. 利用管理者によるクライアント証明書失効TSVファイルの作成
1-4-2. TSVファイルの受け取り及び審査
1-4-3. クライアント証明書失効申請TSVファイルのアップロード
1-4-4. クライアント証明書失効完了メール受信
1-5. クライアント証明書情報取得
1-5-1. クライアント証明書情報取得手順
1-6. 証明書のエクスポート手順（バックアップ作成）
1-6-1. Internet Explorerでの証明書のエクスポート手順（バックアップ作成）
1-6-2. Firefoxでの証明書のエクスポート手順（バックアップ作成）

1. クライアント証明書管理手順

本章では、サービス参加機関の利用管理者に配付するクライアント証明書の発行・更新・失効及び管理を行う登録担当者の操作方法について記述します。
サービス参加機関の利用管理者からクライアント証明書の発行要求があり、クライアント証明書の新規発行が必要な場合は「1-2. クライアント証明書新規発行」を行ってください。
既にクライアント証明書を本システムから発行していて、有効期間が切れるクライアント証明書の更新、失効された証明書の再発行を行う場合は「1-3. クライアント証明書更新発行」を行ってください。
クライアント証明書の失効を行う場合は「1-4. クライアント証明書失効」を行ってください。

手続きの種別	手続きを行う主な機会
新規証明書発行 (**1-2.クライアント証明書新規発行**)	新規にクライアント証明書の発行を必要とする場合。
	クライアント証明書の記載内容（主体者DN）を変更する場合。
証明書更新発行 (**1-3.クライアント証明書更新発行**)	クライアント証明書の記載内容(主体者DN以外)を変更する場合。
	クライアント証明書を、継続利用したい場合。
	失効されたクライアント証明書の再発行を行う場合。
証明書失効 (**1-4.クライアント証明書失効**)	クライアント証明書が不要になった場合や秘密鍵が危殆化した場合。

1-1. 証明書ダウンロード方法ごとの操作手順

新規証明書発行、証明書更新発行、証明書失効の手続きで使用する発行申請TSVファイルを作成するときに以下の証明書ダウンロード方法を選択してください。

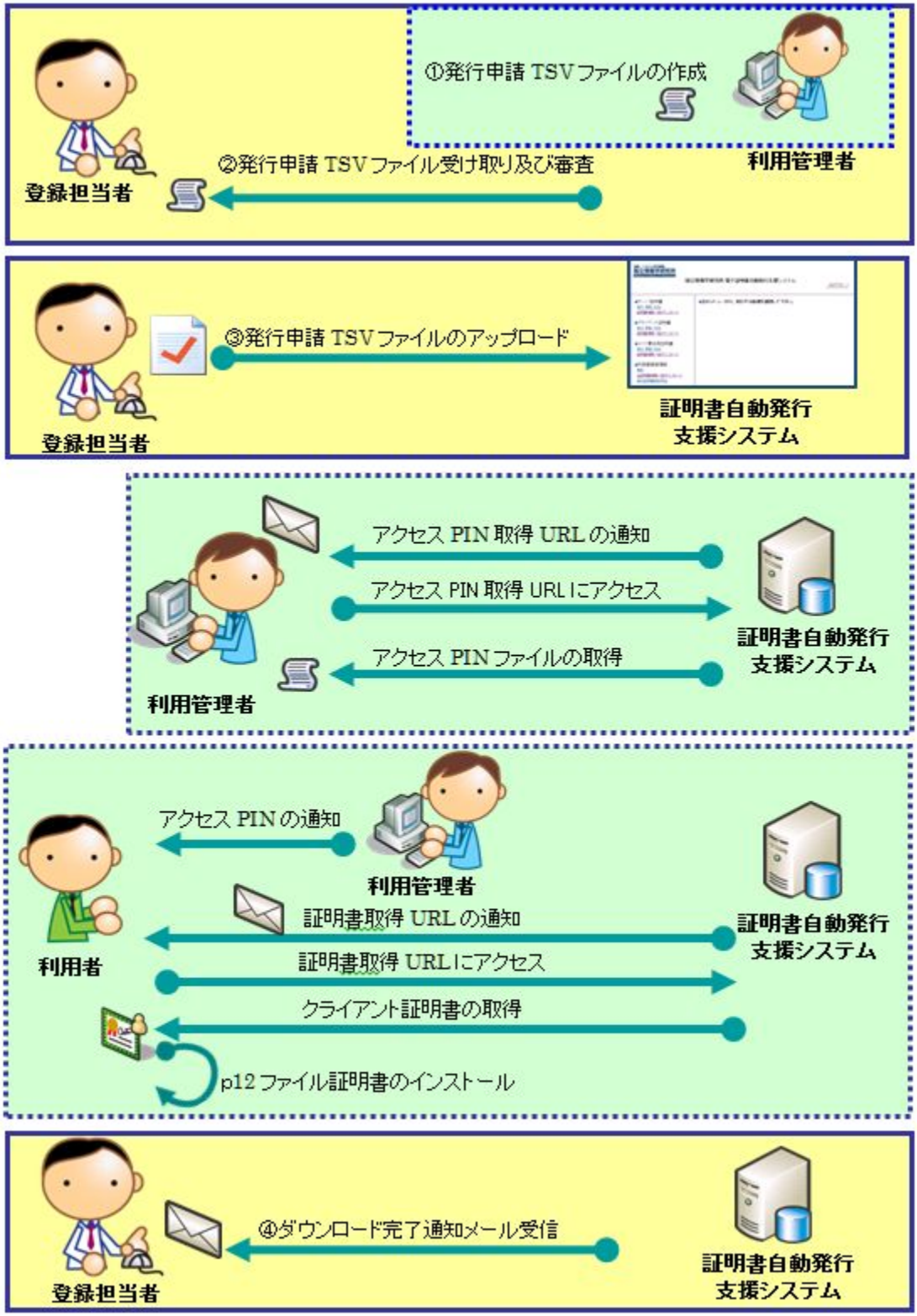
証明書ダウンロード種別	手続きを行う主な機会
P12_個別	P12証明書を発行、更新、失効を個別で行う場合
P12_一括	P12証明書を発行、更新、失効を一括で行う場合
ブラウザ発行	証明書を発行、更新、失効をブラウザで行う場合



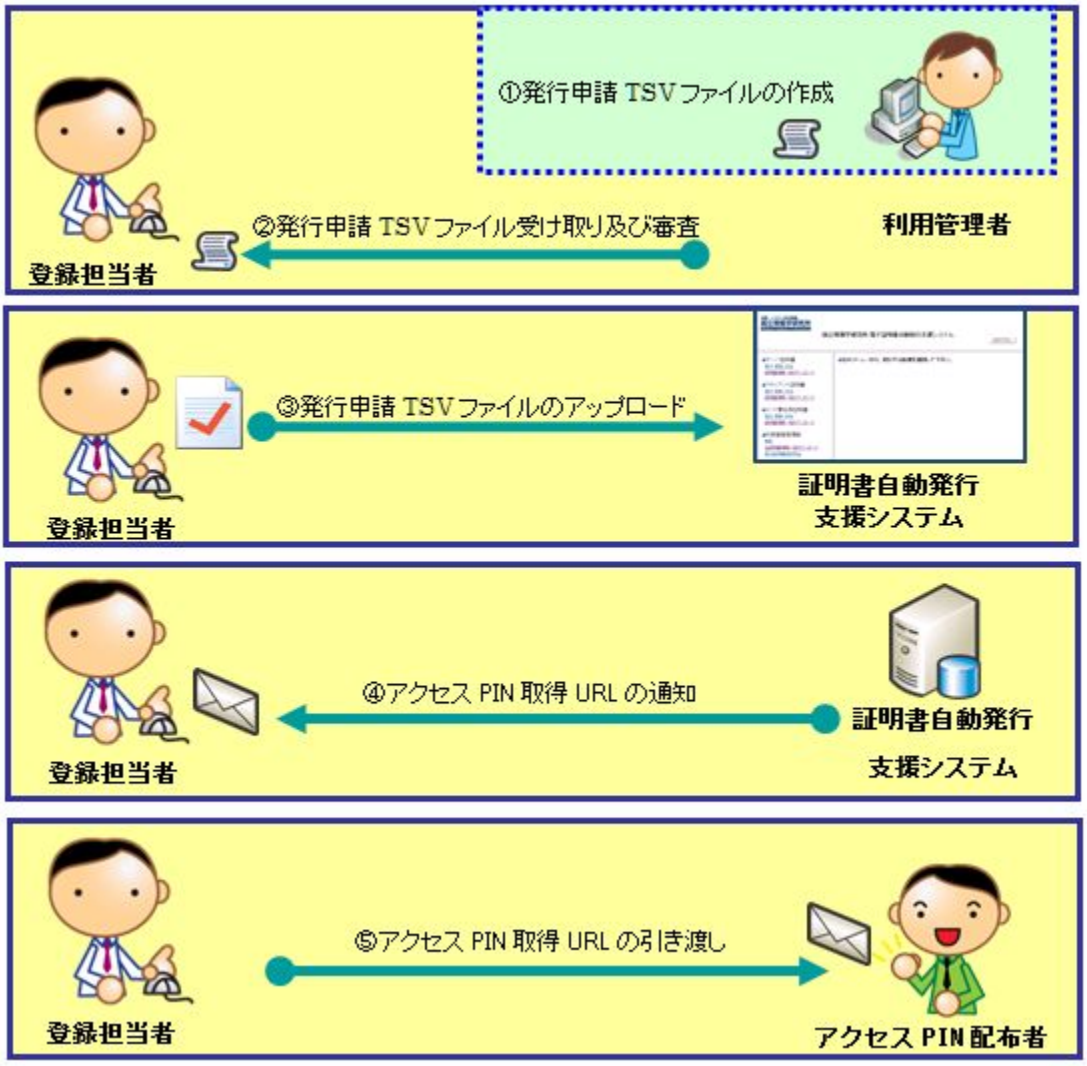
1つの発行申請TSVファイルに複数の証明書ダウンロード種別を選択することはできません。
証明書ダウンロード種別ごとに発行申請TSVファイルを分けて作成してください。

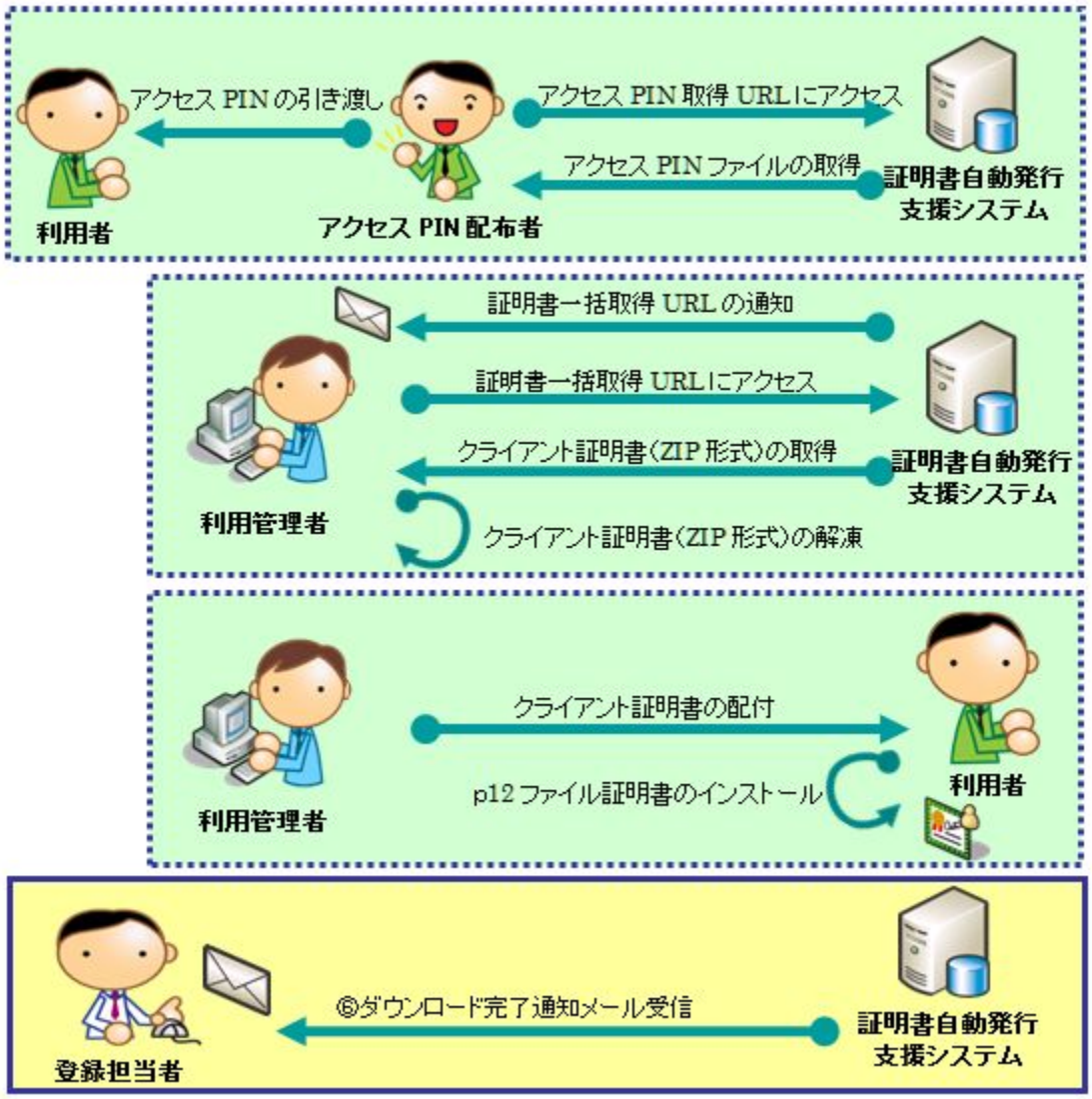
1-2. クライアント証明書新規発行

以下に記述する手続きにより、クライアント証明書の新規発行を行います。
【P12_個別】

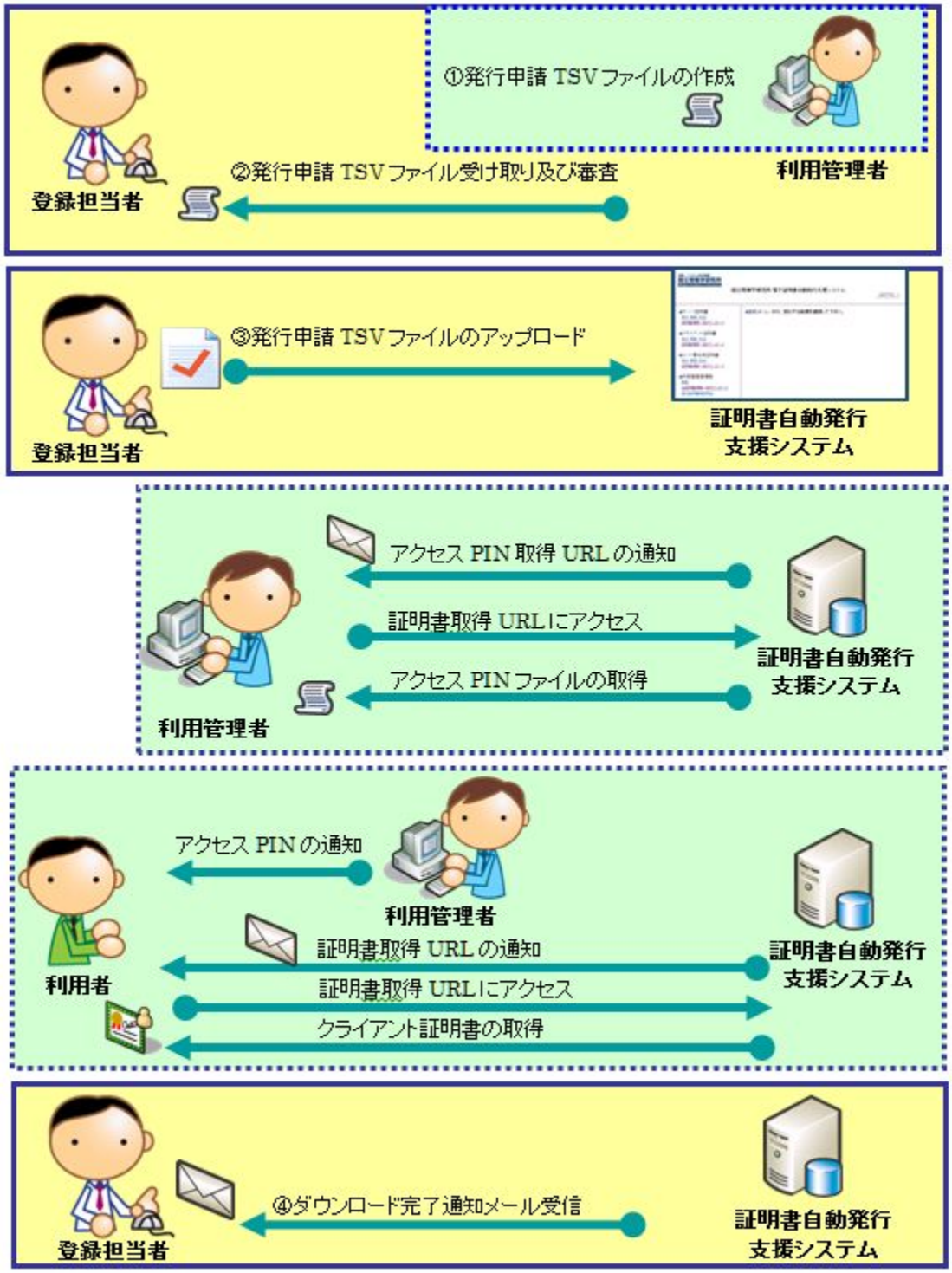

①発行申請 TSV ファイルの作成
利用管理者
②発行申請 TSV ファイル受け取り及び審査
登録担当者
③発行申請 TSV ファイルのアップロード
登録担当者
証明書自動発行
支援システム
アクセス PIN 取得 URL の通知
アクセス PIN 取得 URL にアクセス
アクセス PIN ファイルの取得
利用管理者
証明書自動発行
支援システム
アクセス PIN の通知
利用管理者
証明書取得 URL の通知
証明書取得 URL にアクセス
クライアント証明書の取得
p12 ファイル証明書のインストール
利用者
証明書自動発行
支援システム
④ダウンロード完了通知メール受信
登録担当者
証明書自動発行
支援システム

【P12_一括】


①発行申請 TSV ファイルの作成
②発行申請 TSV ファイル受け取り及び審査
利用管理者
登録担当者
③発行申請 TSV ファイルのアップロード
証明書自動発行
支援システム
登録担当者
④アクセス PIN 取得 URL の通知
証明書自動発行
支援システム
登録担当者
⑤アクセス PIN 取得 URL の引き渡し
登録担当者
アクセス PIN 配布者


アクセス PIN の引き渡し
アクセス PIN 取得 URL にアクセス
アクセス PIN ファイルの取得
利用者
アクセス PIN 配布者
証明書自動発行
支援システム
証明書一括取得 URL の通知
証明書一括取得 URL にアクセス
クライアント証明書（ZIP 形式）の取得
クライアント証明書（ZIP 形式）の解凍
利用管理者
証明書自動発行
支援システム
クライアント証明書の配付
p12 ファイル証明書のインストール
利用管理者
利用者
©ダウンロード完了通知メール受信
登録担当者
証明書自動発行
支援システム

【ブラウザ】



クライアント証明書新規発行
【利用管理者→登録担当者】 ①クライアント証明書新規発行申請TSVファイルを作成します。 **（1-2-1に記載）**

【登録担当者作業】

②クライアント証明書新規発行申請TSVファイルを利用管理者から受け取ります。利用管理者からTSVファイルを受け取るときには、利用管理者の本人確認を行ってください。**（1-2-2に記載）**

③クライアント証明書新規発行申請TSVファイルのアップロードを行ってください。**（1-2-3に記載）**

④アクセスPIN発行通知メールを受信します。**（1-2-4に記載）**※P12_一括のみ

⑤アクセスPIN発行通知メールをアクセスPIN配付者へ引き渡します。**（1-2-5に記載）**※P12_一括のみ

【アクセスPIN配付者→利用者】
・ アクセスPIN発行通知メールの情報を元に、アクセスPIN取得URLにアクセスします。※P12_一括のみ
・ アクセスPINを取得します。※P12_一括のみ
・ 利用者にアクセスPINを引き渡します。 ※P12_一括のみ

【利用管理者作業】
・ クライアント証明書発行受付通知メール受信を受信します。
・ クライアント証明書発行受付通知メールの情報を元に、利用管理者用証明書取得URLにアクセスします。
・ クライアント証明書のダウンロード。
・ クライアント証明書(ZIP形式)の解凍を行ってください。※P12_一括のみ

【利用管理者→利用者】

・ 利用管理者は利用者にクライアント証明書の配布を行ってください。※P12_一括のみ
・ 利用者はP12ファイル証明書のインストールを行ってください。※P12_個別、P12_一括のみ

【登録担当者作業】

⑥ダウンロード完了通知メール受信。**（1-2-6に記載）**

1-2-1. 利用管理者によるクライアント証明書新規発行申請TSVファイル作成

利用管理者は、クライアント証明書新規発行申請TSVファイルを作成します。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
作成したTSVファイルを登録担当者宛にメールで送付します。

1-2-2. TSVファイルの受け取り及び審査

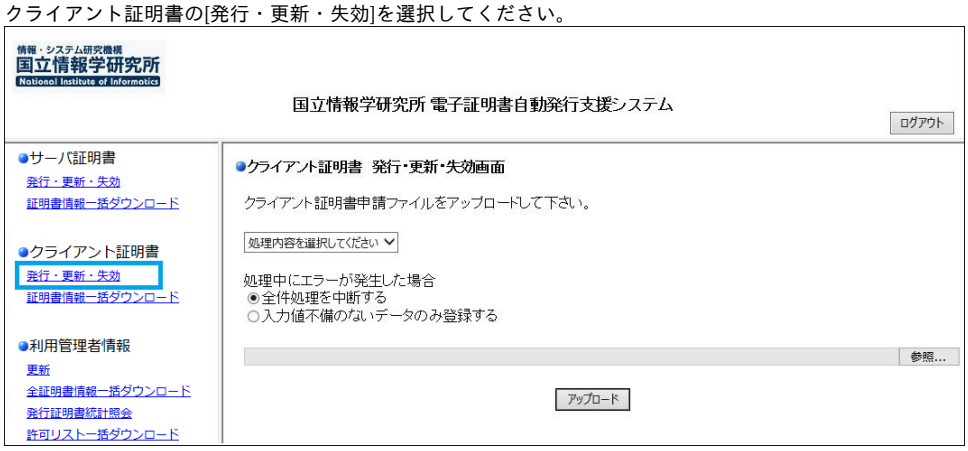
登録担当者は、利用管理者からクライアント証明書新規発行申請TSVファイルを受領します。その際、各機関の定められた手続きに従い利用管理者の本人性・実在性を審査してください。

1-2-3. クライアント証明書新規発行申請TSVファイルのアップロード

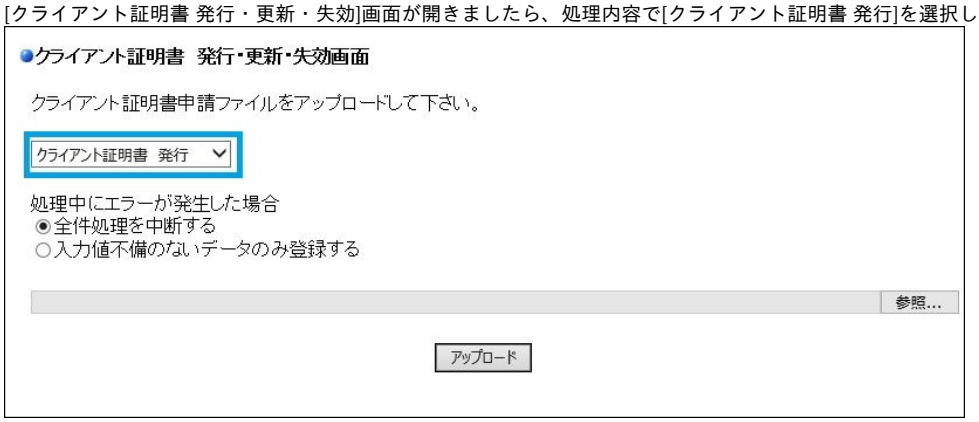
「1-2-2. TSVファイル受け取り及び審査」で受け取ったTSVファイルを本システムへアップロードしてください。アップロードする方法を以下に記述します。

クライアント証明書新規発行申請手続き

1. クライアント証明書の[発行・更新・失効]を選択してください。



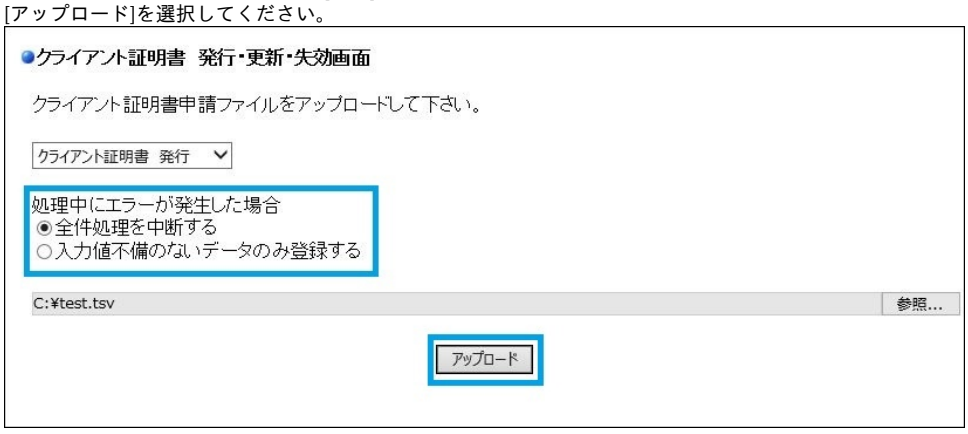
2. [クライアント証明書 発行・更新・失効]画面が開きましたら、処理内容で[クライアント証明書 発行]を選択してください。



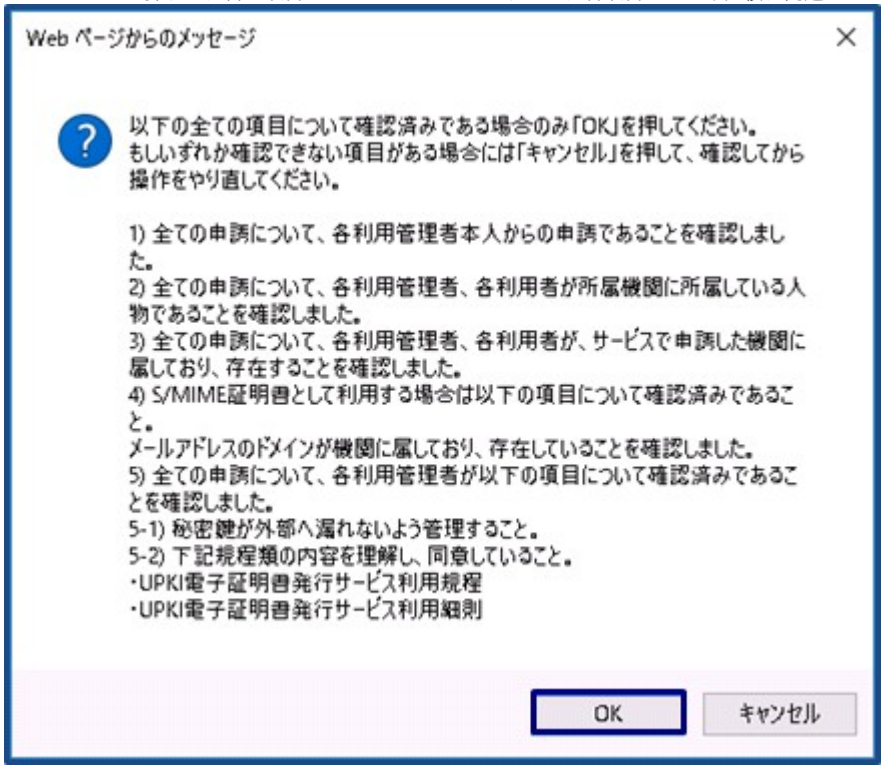
3. 証明書発行種別が決まりましたら、処理中にエラーが発生した場合の本システムの動作について選択し、チェックを入れてください。選択できる動作は以下の2つになります。

   全件処理を中断する・・・申請データに1件でもエラーがあった場合すべての申請を取りやめる。
   入力値不備のないデータのみ登録する・・・申請データにエラーがあった場合、エラーがあったデータのみ申請を無視して処理を続行する。
   ※　アップロードを行うTSVファイルの管理を容易にするために、通常は「全件処理を中断する」を 選択することを推奨致します。

   処理中のエラー動作内容を選択後、[参照]を選択して「1-1-3. TSVファイルの受け取り及び審査」で操作端末に保存したTSVファイルを選択し、[アップロード]を選択してください。



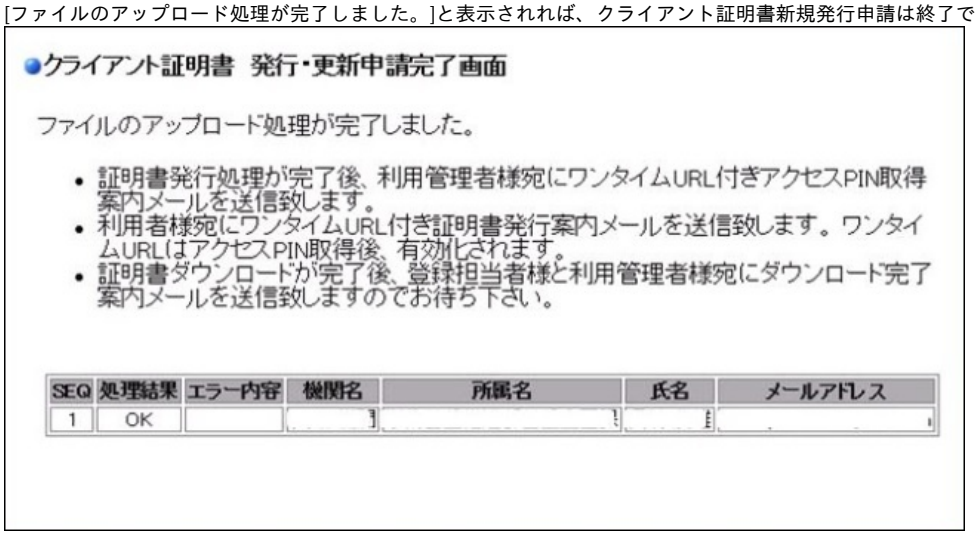
4. アップロードを押すと、審査項目がポップアップされますので、各項目をＩを確認後、問題がなければ[OK]を選択してください。



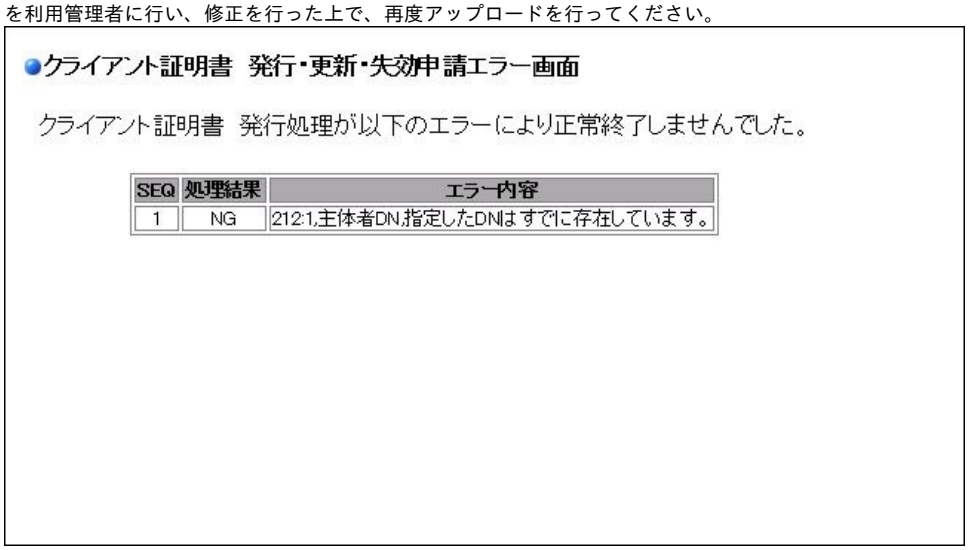
機関の審査が完了していない場合など、以下のエラーメッセージが表示されます。これらのエラーメッセージが表示された際にはそれぞれの対処方法の実施をお願いします。

エラーメッセージ	原因	対処方法
対象のドメインは許可されていないため発行できません。サービス窓口にお問い合わせください。	審査完了していないため発行できません。認証局による審査が完了しますと発行可能となります。	サービス窓口にお問い合わせください。
機関の証明書発行有効期限が切れています。サービス窓口にお問い合わせください。	証明書発行承認有効期限を超過しています。再度、認証局による審査が必要になります。	サービス窓口にお問い合わせください。
WHOISサーバへの接続に失敗しました。時間をおいて再度申請してください。再度申請しても接続に失敗するようでしたら、サービス窓口にお問い合わせください。	証明書発行時にWhoisサーバにドメイン所有者の変更がないか確認しますが、その際、何らかの原因でWhoisサーバ接続に失敗しています。	時間をおいて再度申請してください。再度申請しても接続に失敗するようでしたら、サービス窓口にお問い合わせください。
WHOISサーバに登録されている情報と一致しません。サービス窓口にお問い合わせください。	Whoisサーバに登録されている組織名、登録者名が変更された場合に表示されます。 例としまして「申請大学」を「学校法人申請学園　申請大学」に変更されますと表示されます。 この場合、認証局でWhoisサーバ情報の審査、更新が必要となります。	サービス窓口にお問い合わせください。
主体者DNのLが登録された値と一致しません。	利用機関ごとに指定されたLの値で申請がされていません。	「UPKI証明書 主体者DNにおける ST および L の値一覧」をご参照のうえ、正しいLの値で申請してください。
主体者DNのSTが登録された値と一致しません。	利用機関ごとに指定されたSTの値で申請がされていません。	「UPKI証明書 主体者DNにおける ST および L の値一覧」をご参照のうえ、正しいSTの値で申請してください。

5. [ファイルのアップロード処理が完了しました。]と表示されれば、クライアント証明書新規発行申請は終了です。



6. 申請ファイルにエラーがある場合は、以下のようにエラーの内容が表示されますので、エラーの内容を確認し、申請したTSVファイルの修正依頼を利用管理者に行い、修正を行った上で、再度アップロードを行ってください。



7. アップロード終了後、[ログアウト]を選択し、本システムを終了してください。

1-2-4. アクセスPIN取得URLの通知

本システムへTSVファイルのアップロードを行うと、本システムより登録担当者宛にアクセスPIN取得URLを通知するメールが自動送信されます。

1-2-5. アクセスPIN取得URLの引き渡し

登録担当者が取得されましたアクセスPIN取得URLはアクセスPIN配付者様へ引き渡してください。

1-2-6. ダウンロード完了通知メール受信

クライアント証明書新規発行依頼者である利用管理者がクライアント証明書のダウンロードを行った場合、本システムより、登録担当者宛にダウンロードが完了したことを通知するメールが自動送信されます。このメールは、電子署名されています。

クライアント証明書ダウンロード完了通知メール

【件名】
クライアント証明書取得通知

【本文】

・・・・・
貴機関利用者の方がクライアント用証明書の取得を完了致しましたので、

下記の通り連絡をさせていただきます。

【対象証明書DN】

CN=test1.example.ac.jp
O=testkikan
L=Chiyoda-ku
ST=Tokyo
C=JP

【対象証明書シリアル番号】

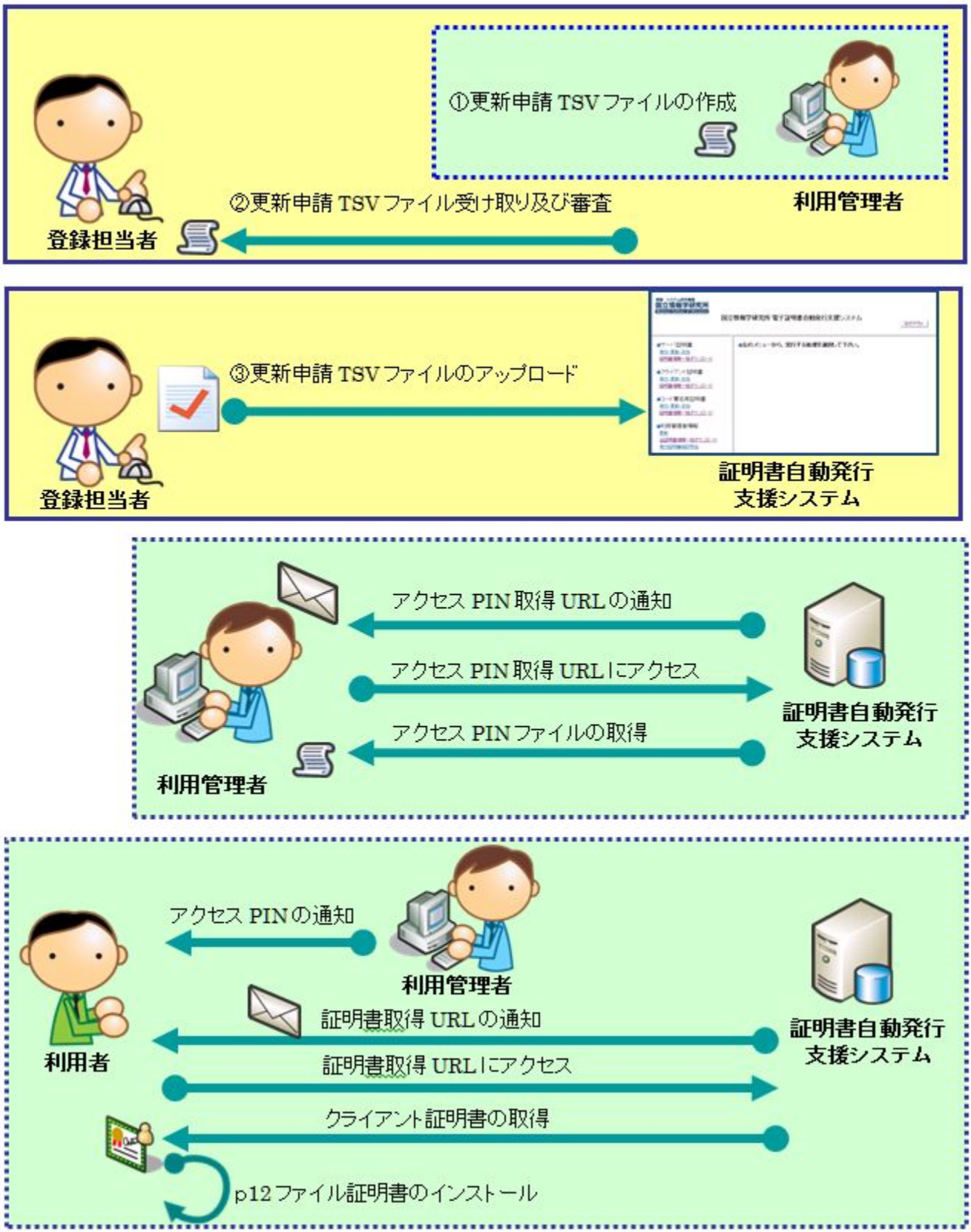
・・・・・

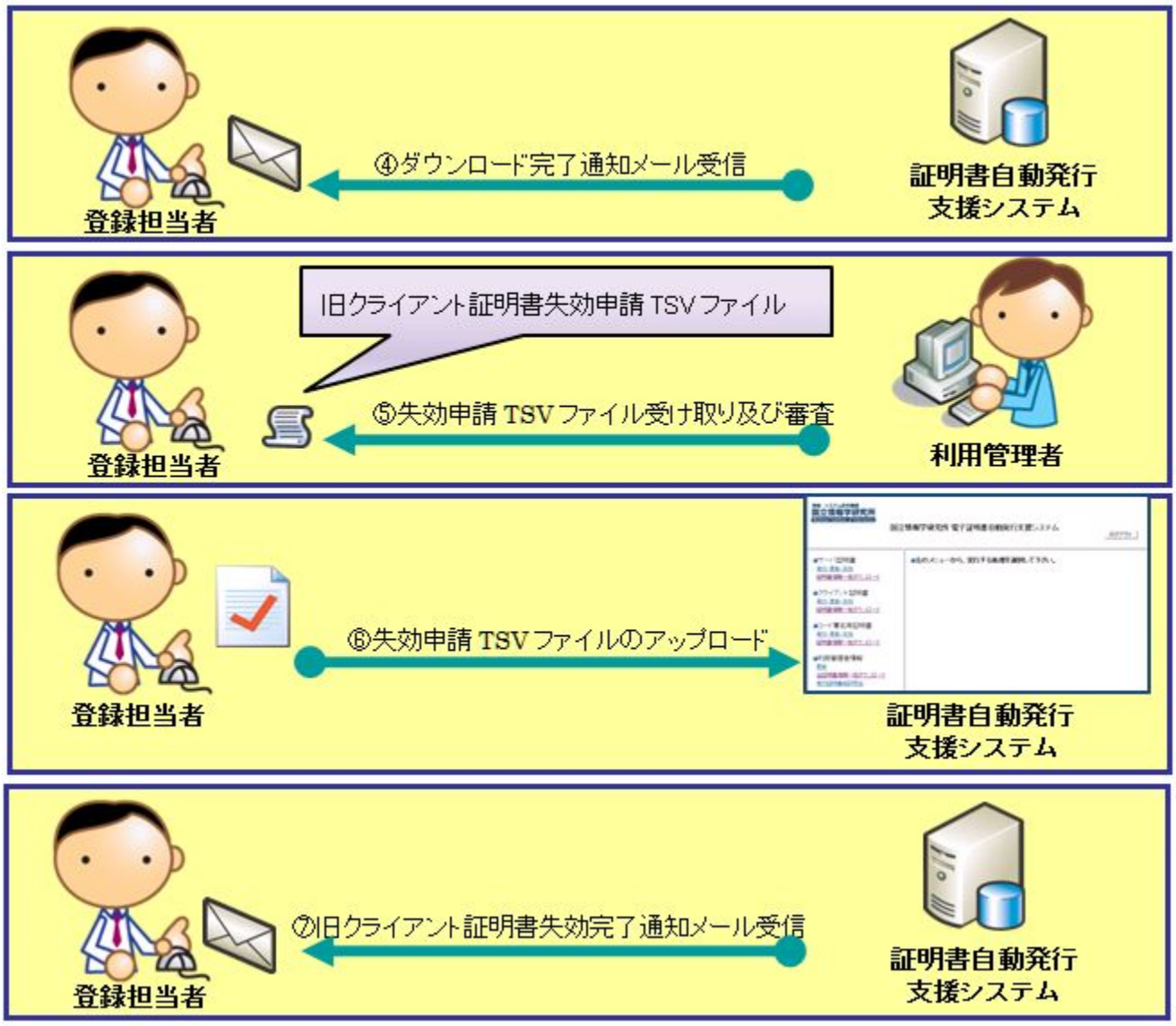


一定期間がたってもダウンロード完了通知メールが受信されない場合は、該当の利用管理者へ電話にて連絡を行い、状況を確認してください。

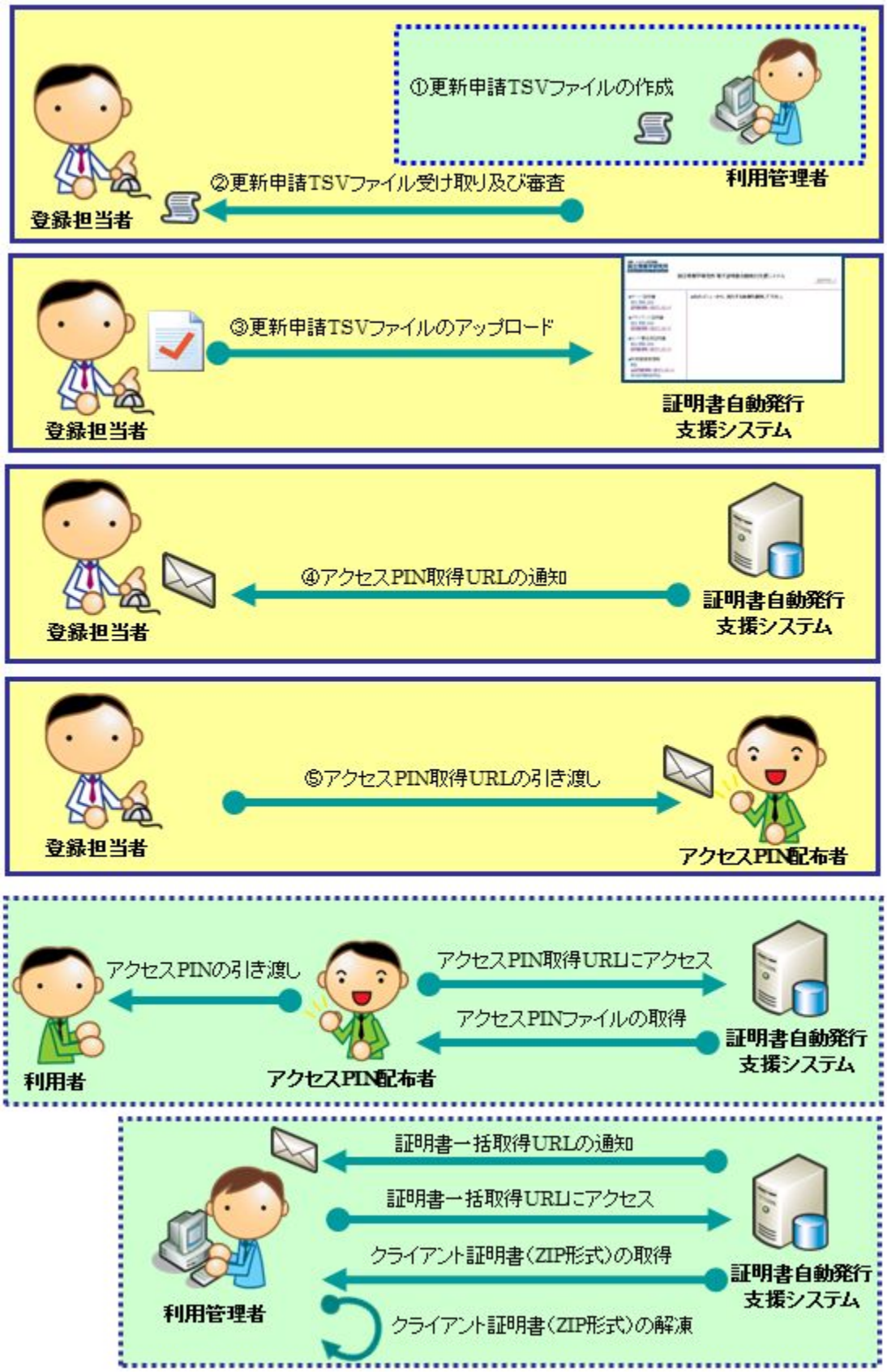
1-3. クライアント証明書更新発行

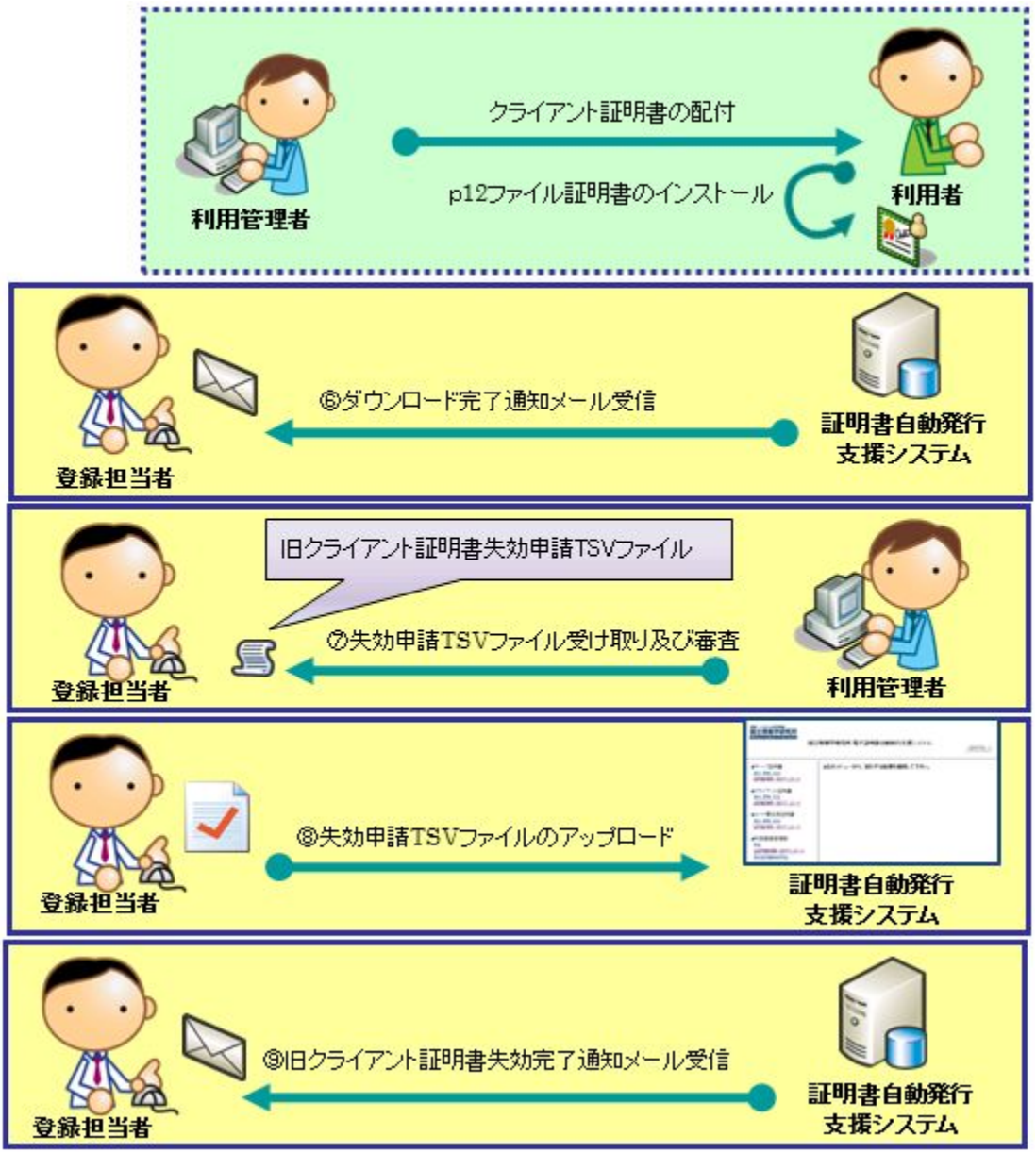
以下に記述する手続きにより、クライアント証明書の更新発行を行います。
【P12_個別】


①更新申請 TSV ファイルの作成
利用管理者
②更新申請 TSV ファイル受け取り及び審査
登録担当者
③更新申請 TSV ファイルのアップロード
登録担当者
証明書自動発行
支援システム
アクセス PIN 取得 URL の通知
アクセス PIN 取得 URL にアクセス
アクセス PIN ファイルの取得
証明書自動発行
支援システム
利用管理者
アクセス PIN の通知
利用管理者
証明書取得 URL の通知
証明書自動発行
支援システム
利用者
証明書取得 URL にアクセス
クライアント証明書の取得
p12 ファイル証明書のインストール

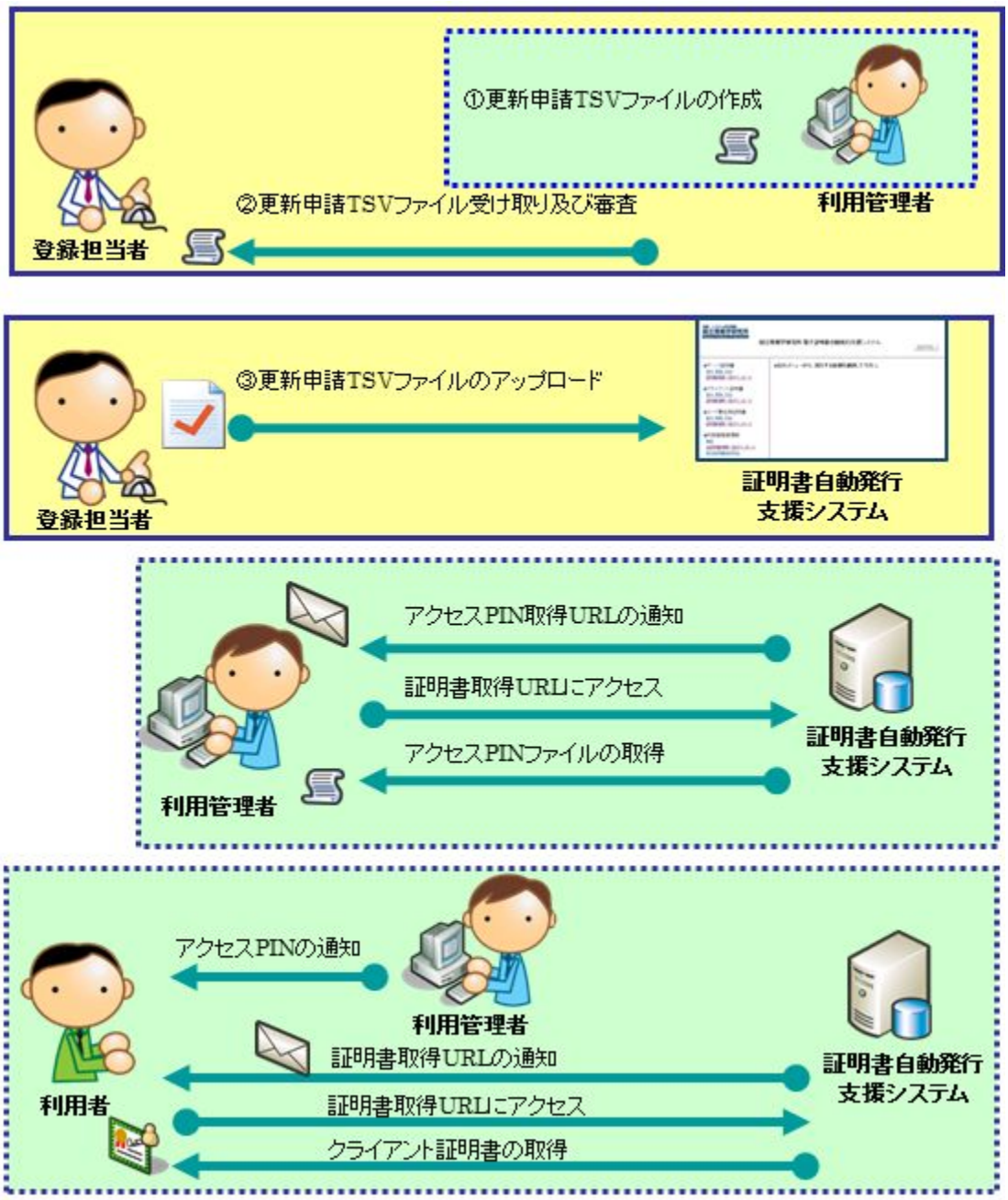

④ダウンロード完了通知メール受信
登録担当者
証明書自動発行
支援システム
旧クライアント証明書失効申請 TSV ファイル
⑤失効申請 TSV ファイル受け取り及び審査
登録担当者
利用管理者
⑥失効申請 TSV ファイルのアップロード
登録担当者
証明書自動発行
支援システム
⑦旧クライアント証明書失効完了通知メール受信
登録担当者
証明書自動発行
支援システム

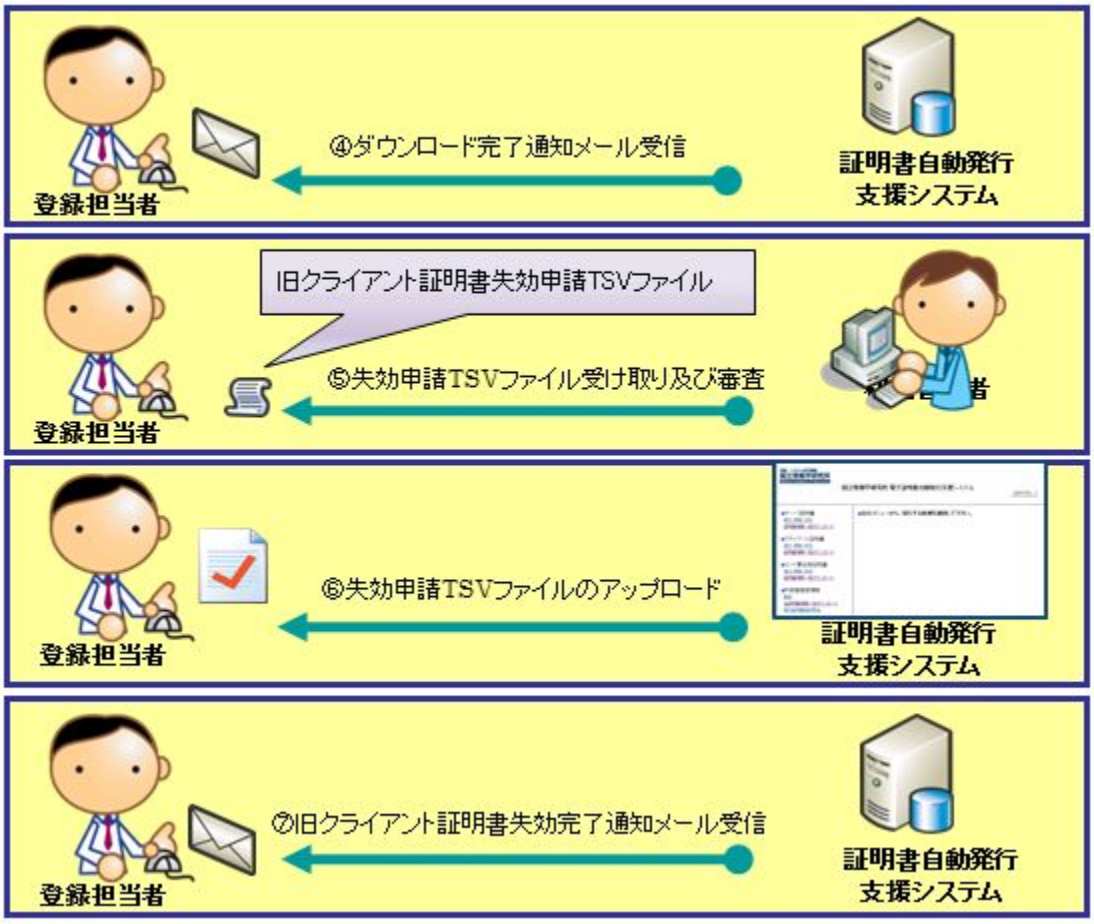
【P12_一括】


①更新申請TSVファイルの作成
利用管理者
②更新申請TSVファイル受け取り及び審査
登録担当者
③更新申請TSVファイルのアップロード
登録担当者
証明書自動発行
支援システム
④アクセスPIN取得URLの通知
登録担当者
証明書自動発行
支援システム
⑤アクセスPIN取得URLの引き渡し
登録担当者
アクセスPIN配布者
アクセスPINの引き渡し
アクセスPIN取得URLにアクセス
アクセスPINファイルの取得
利用者
アクセスPIN配布者
証明書自動発行
支援システム
証明書一括取得URLの通知
証明書一括取得URLにアクセス
クライアント証明書(ZIP形式)の取得
クライアント証明書(ZIP形式)の解凍
利用管理者
証明書自動発行
支援システム


クライアント証明書の配付
利用管理者
利用者
p12ファイル証明書のインストール
⑥ダウンロード完了通知メール受信
登録担当者
証明書自動発行
支援システム
旧クライアント証明書失効申請TSVファイル
⑦失効申請TSVファイル受け取り及び審査
登録担当者
利用管理者
⑧失効申請TSVファイルのアップロード
登録担当者
証明書自動発行
支援システム
⑨旧クライアント証明書失効完了通知メール受信
登録担当者
証明書自動発行
支援システム

【ブラウザ】


①更新申請TSVファイルの作成
利用管理者
②更新申請TSVファイル受け取り及び審査
登録担当者
③更新申請TSVファイルのアップロード
登録担当者
証明書自動発行
支援システム
アクセスPIN取得URLの通知
証明書取得URLにアクセス
アクセスPINファイルの取得
利用管理者
証明書自動発行
支援システム
アクセスPINの通知
利用管理者
証明書取得URLの通知
証明書取得URLにアクセス
クライアント証明書の取得
利用者
証明書自動発行
支援システム



クライアント証明書更新
【利用管理者作業→登録担当者】 ①クライアント証明書更新申請TSVファイルを作成します。 **（1-3-1に記載）**
【登録担当者作業】 ②クライアント証明書更新申請TSVファイルを利用管理者から受け取ります。利用管理者からTSVファイルを受け取るときには、利用管理者の本人性確認を行ってください。 **（1-3-2に記載）** ③クライアント証明書更新申請TSVファイルのアップロードを行います。 **（1-3-3に記載）** ④アクセスPIN発行通知メールを受信します。 **（1-3-4に記載）**※P12_一括のみ ⑤アクセスPIN発行通知メールをアクセスPIN配付者へ引き渡します。 **（1-3-5に記載）**※P12_一括のみ
【アクセスPIN配付者→利用者】 ・ アクセスPIN発行通知メールの情報を元に、アクセスPIN取得URLにアクセスします。※P12_一括のみ ・ アクセスPINを取得します。※P12_一括のみ ・ 利用者にアクセスPINを引き渡します。 ※P12_一括のみ
【利用管理者作業】 ・ アクセスPIN発行通知メールの情報を元に、アクセスPIN取得URLにアクセスします。※P12_個別のみ ・ アクセスPINを取得します。※P12_個別のみ ・ クライアント証明書発行受付通知メールを受信します。 ・ クライアント証明書発行受付通知メールを元に、利用管理者用証明書取得URLにアクセスします。 ・ クライアント証明書をダウンロードします。
【利用管理者→利用者】 ・ 利用管理者は利用者にクライアント証明書の配布を行ってください。※P12_一括のみ ・ 利用者はP12ファイル証明書のインストールを行ってください。※P12_個別、P12_一括のみ

【登録担当者作業】

⑥ダウンロード完了通知メールを受信します。**（1-3-6に記載）**

【利用管理者作業】
・ 旧クライアント証明書から新クライアント証明書への置き換え作業を行います。
・ 登録担当者に新クライアント証明書への置き換え完了通知を行います。

【登録担当者作業】

⑦利用管理者から新クライアント証明書への置き換え完了通知を受けます。**（1-3-7に記載）**

⑧[⑦新クライアント証明書への置き換え完了通知]がきたら、[⑥ダウンロード完了通知メール受信]でメールに添付されているファイルをそのまま失効申請TSVファイルとして本システムにアップロードします。**（1-3-8に記載）**

⑨旧クライアント証明書失効申請が成功すると、旧証明書失効完了通知メールが登録担当者と利用管理者宛に届きます。**（1-3-9に記載）**

1-3-1. 利用管理者によるクライアント証明書更新申請TSVファイル作成

利用管理者は、クライアント証明書更新申請TSVファイルを作成します。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
利用管理者は、作成したTSVファイルを登録担当者宛にメールで送付します。

1-3-2. TSVファイルの受け取り及び審査

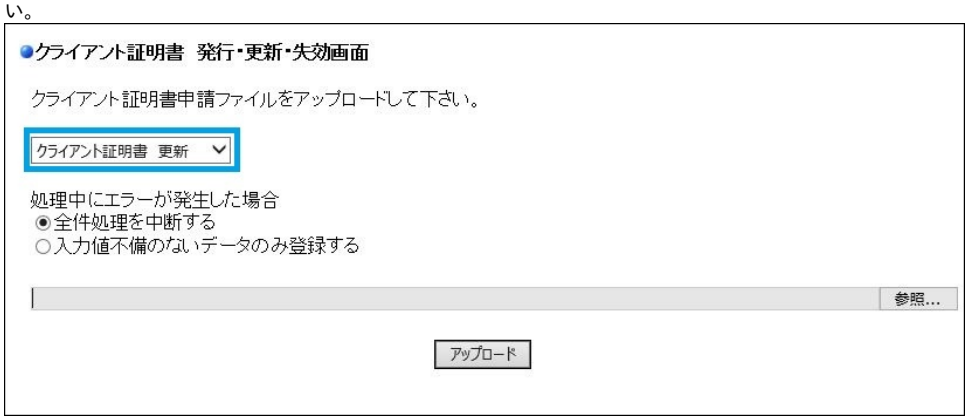
登録担当者は、利用管理者からクライアント証明書更新申請TSVファイルを受領します。その際、各機関の定められた手続きに従い利用管理者の本人性・実在性を審査してください。
クライアント証明書更新申請TSVファイルは登録担当者操作端末の適切な場所に保存します。
尚、クライアント証明書更新申請TSVファイルの「失効対象証明書シリアル番号」項目の調べ方については 「1-5. クライアント証明書情報取得」に記載しています。

1-3-3. クライアント証明書更新申請TSVファイルのアップロード

「1-3-2. TSVファイル受け取り及び審査」で受け取ったTSVファイルを本システムへアップロードしてください。アップロード方法に関しましては「1-2-3. クライアント証明書新規発行申請TSVファイルのアップロード」をご確認ください。「1-2-3. クライアント証明書新規発行申請TSVファイルのアップロード」の2.の手続きで、[クライアント証明書 更新]をクリックしてください。

クライアント証明書更新手続き

クライアント証明書更新申請TSVファイルのアップロード時、[クライアント証明書 更新]を選択してください。



1-3-4. アクセスPIN取得URLの通知

本システムへTSVファイルのアップロードを行うと、本システムより登録担当者宛にアクセスPIN取得URLを通知するメールが自動送信されます。

1-3-5. アクセスPIN取得URLの引き渡し

登録担当者が取得されましたアクセスPIN取得URLはアクセスPIN配布者様へ引き渡してください。

1-3-6. ダウンロード完了通知メール受信

利用管理者及び利用者が更新したクライアント証明書のダウンロードを行った場合、本システムより、登録担当者宛にダウンロードが完了したことを通知するメールが送信されます。また、旧クライアント証明書が有効の場合、TSVファイル（旧クライアント証明書失効申請TSVファイル）が添付されています。旧クライアント証明書の有効期限切れまたは、失効済の場合は、TSVファイルは添付されません。
登録担当者は「旧クライアント証明書から新クライアント証明書への置き換えが完了した」との連絡を利用管理者及び利用者から受けた後、メール添付のTSVファイルを本システムよりアップロードします。詳しくは、「1-3-7. 新クライアント証明書への置き換え完了通知」以降に手順を説明します。
旧クライアント証明書失効申請TSVファイルアップロードを行う日までこのメールは大切に保管してください。



一定期間がたってもダウンロード完了通知メールが受信されない場合は、該当する利用管理者へ電話にて連絡を行い、状況を確認してください。

TSVファイル付き更新クライアント証明書ダウンロード完了通知メール
件名: [UPKI]クライアント用証明書更新通知 添付ファイル: 1911649278160095962-test1.example.ac.jp.tsv 旧クライアント証明書失効申請TSVファイル CN=test1.example.ac.jp,O=testkikan,L=Chiyoda-kuST=Tokyo,C=JP 1911649278160095962 … 1911649278160095962 …
【本文】 ・・・・・ 【対象証明書DN】 ---------- CN=test1.example.ac.jp O=testkikan L=Chiyoda-ku ST=Tokyo C=JP ----------   【新証明書シリアル番号】 xxxxxxxxxx   【旧証明書のシリアル番号】 1911649278160095962 登録担当者は、利用管理者から更新証明書への置き換え完了の報告を受けた後に、 以下の手続きに従い旧証明書の失効を行って下さい。・・・・・

1-3-7. 新クライアント証明書への置き換え完了通知

利用管理者は該当のクライアント証明書の置き換えを行い、登録担当者へクライアント証明書の置き換え完了通知を行います。

1-3-8. 旧クライアント証明書失効TSVファイルのアップロード

登録担当者が[1-3-7. 新クライアント証明書への置き換え完了通知]の連絡を受けた後、[1-3-5. ダウンロード完了通知メール受信]に添付のTSVファイル（旧クライアント証明書失効申請TSVファイル）を本システムへアップロードします。アップロードする方法は[1-4-3. クライアント証明書失効申請TSVファイルのアップロード]を参考にしてください。

1-3-9. 旧クライアント証明書失効完了通知メール受信

クライアント証明書の失効を行った場合、本システムより、登録担当者と利用管理者宛に失効完了通知メールが送信されます。

クライアント証明書失効完了通知メール

【件名】
クライアント証明書失効完了通知

【本文】
・・・・・
下記クライアント証明書の失効が完了致しましたので、
連絡をさせていただきます。

【失効証明書DN】

CN=test1.example.ac.jp
O=testkikan
L=Chiyoda-ku
ST=Tokyo
C=JP

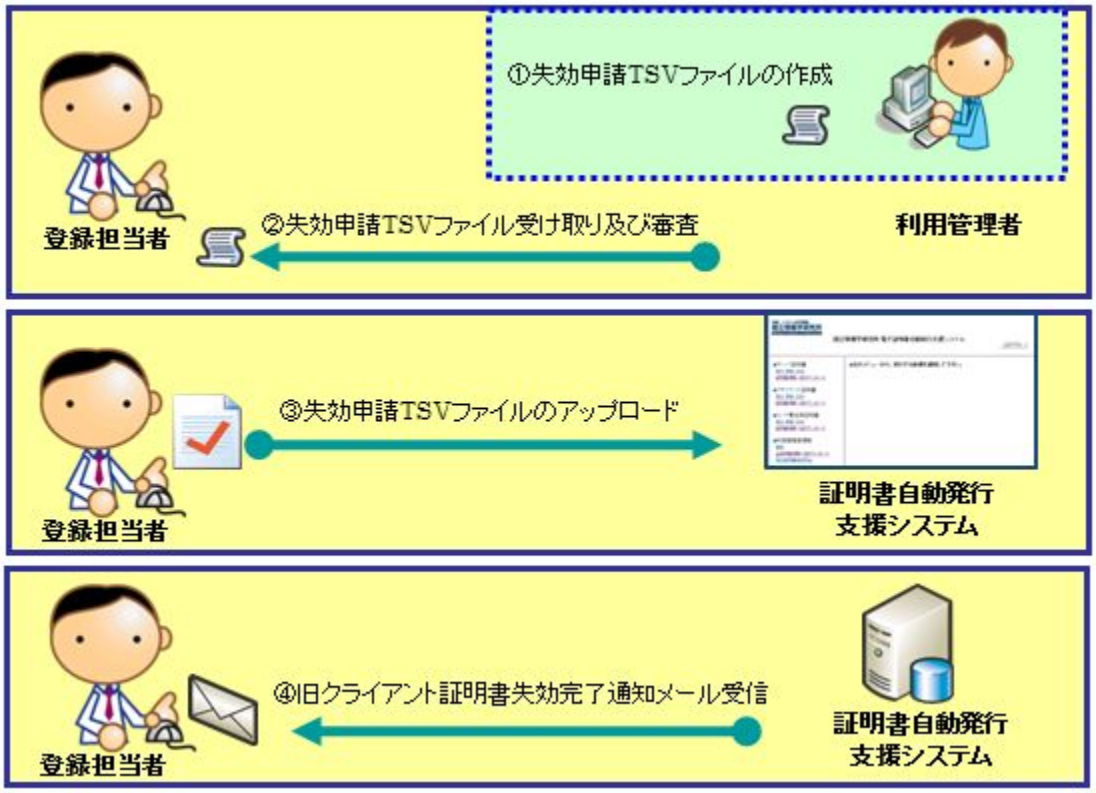
【失効証明書シリアル番号】
xxxxxxxxxx

【失効理由】
その他

・・・・・

1-4. クライアント証明書失効

以下に記述する手続きにより、クライアント証明書の失効を行います。



登録担当者用証明書取得手続き概要
【利用管理者作業】
①クライアント証明書失効申請TSVファイルを作成します。 **（1-4-1に記載）**

【登録担当者作業】

②クライアント証明書失効申請TSVファイルを利用管理者から受け取ります。利用管理者からTSVファイルを受け取るときには、利用管理者の本人確認を行ってください。**（1-4-2に記載）**

③クライアント証明書失効申請ファイルのアップロード。**（1-4-3に記載）**

④クライアント証明書失効完了通知メール受信。**（1-4-4に記載）**

1-4-1. 利用管理者によるクライアント証明書失効TSVファイルの作成

利用管理者は、クライアント証明書失効TSVファイルを作成します。
TSVファイル作成用Webアプリケーション（TSVツール）を提供しておりますので、ご利用ください。
利用管理者は、作成したTSVファイルを登録担当者宛にメールで送付します。

1-4-2. TSVファイルの受け取り及び審査

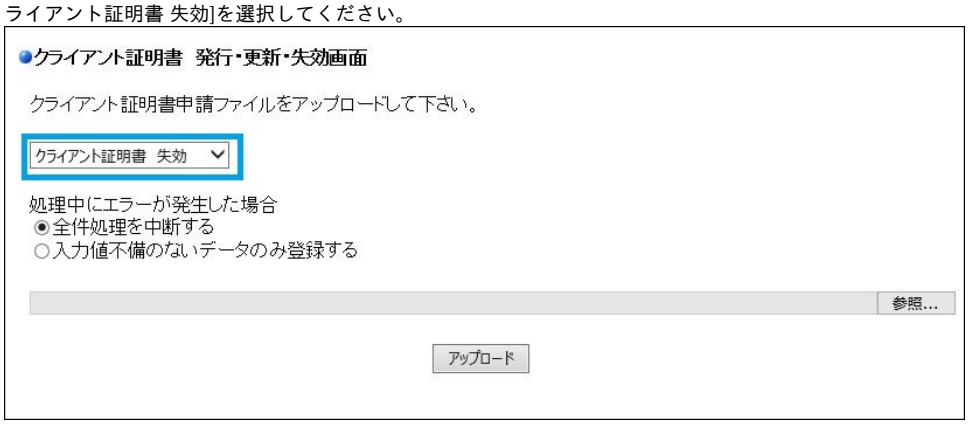
登録担当者は、利用管理者からクライアント証明書失効申請TSVファイルを受領します。その際、各機関の定められた手続きに従い利用管理者の本人性・実在性を審査してください。
クライアント証明書失効申請TSVファイルは登録担当者操作端末の適切な場所に保存します。
尚、クライアント証明書失効申請TSVファイルの「失効対象証明書シリアル番号」項目の調べ方については「1-5-1.クライアント証明書情報取得手順」に記載しています。

1-4-3. クライアント証明書失効申請TSVファイルのアップロード

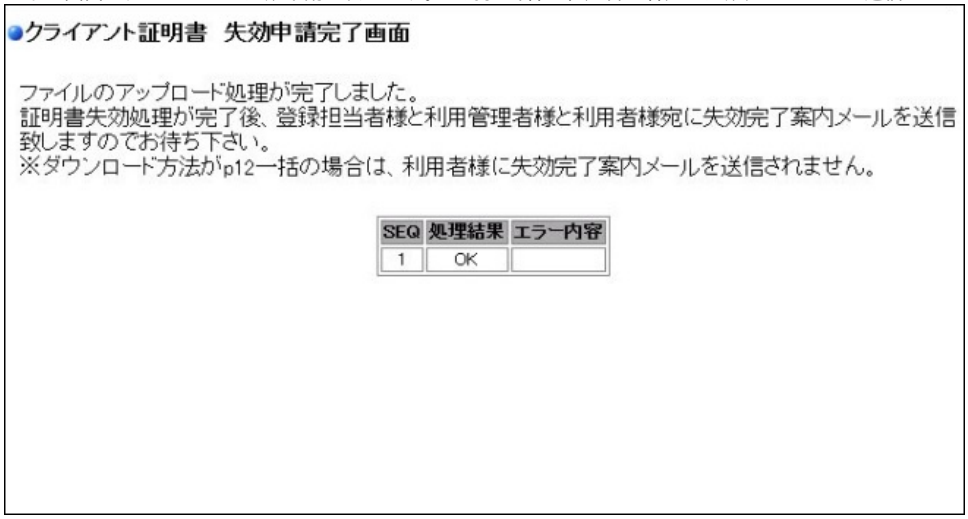
証明書の失効処理を実施する必要がある場合は、以下の手続きを実施してください。

クライアント証明書失効申請手続き

「1-4-2. TSVファイル受け取り及び審査」で受け取ったTSVファイルを本システムへアップロードしてください。本システムへのアップロード時、[クライアント証明書 失効]を選択してください。



以下の画面が表示されたら失効申請が終了です。登録担当者と利用管理者宛に失効完了メールが送信されます。



1-4-4. クライアント証明書失効完了メール受信

クライアント証明書の失効を行った場合、本システムより、登録担当者と利用管理者宛に失効完了通知メールが送信されます。このメールは、電子署名されています。

クライアント証明書失効完了通知メール
【件名】 クライアント証明書失効完了通知 【本文】 ・・・・・ 下記クライアント証明書の失効が完了致しましたので、 連絡をさせていただきます。   【失効証明書DN】 ---------- CN=test1.example.ac.jp O=testkikan L=Chiyoda-ku ST=Tokyo C=JP ----------   【失効証明書シリアル番号】 xxxxxxxxxx   【失効理由】 その他 ・・・・・

1-5. クライアント証明書情報取得

クライアント証明書の情報取得について説明します。

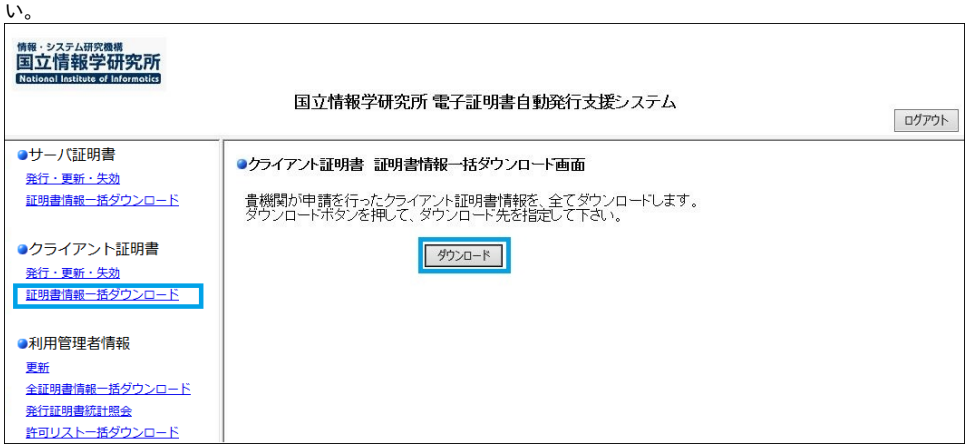
主な利用用途
1. 過去に申請したクライアント証明書発行・失効・更新履歴や処理状況を知りたい場合。 2. クライアント証明書の更新・失効に当たり、旧クライアント証明書のシリアル番号を確認したい場合。 3. 過去に申請したCSR一式、あるいは過去に発行されたクライアント証明書一式を取得したい場合。 4. 各クライアント証明書の利用管理者情報を知りたい場合。

1-5-1. クライアント証明書情報取得手順

クライアント証明書取得手順について説明します。
※取得したファイルの中身については「支援システム操作手順書 / 登録担当用 / その他 -利用管理者情報、TSVファイル形式-」 2.本システムで扱うファイル形式 を参照してください。

クライアント証明書情報取得方法

[証明書一括ダウンロード]を選択し、クライアント証明書 証明書一括ダウンロード画面で[ダウンロード]を選択してください。



1-6.証明書のエクスポート手順（バックアップ作成）

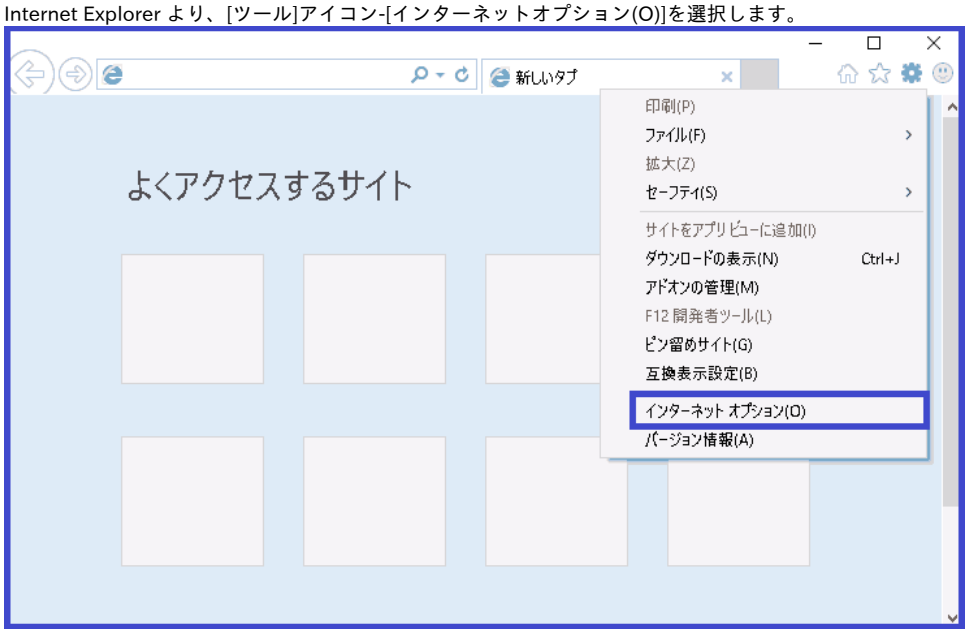
証明書のエクスポート手順（バックアップ作成）について説明します。

1-6-1. Internet Explorerでの証明書のエクスポート手順（バックアップ作成）

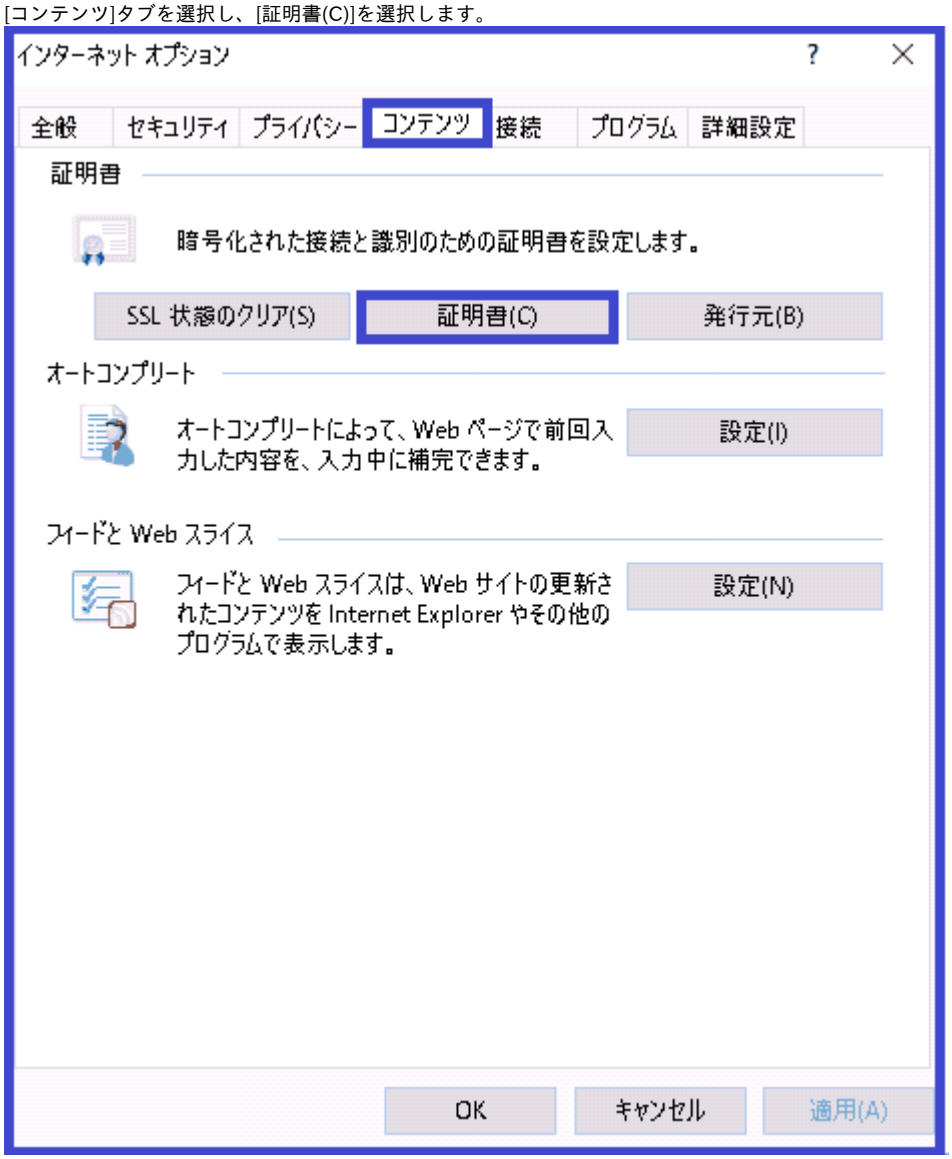
ここでは[Internet Explorer]での証明書のエクスポート手順(バックアップ作成)について記述します。

Internet Explorerでの証明書発行手続き

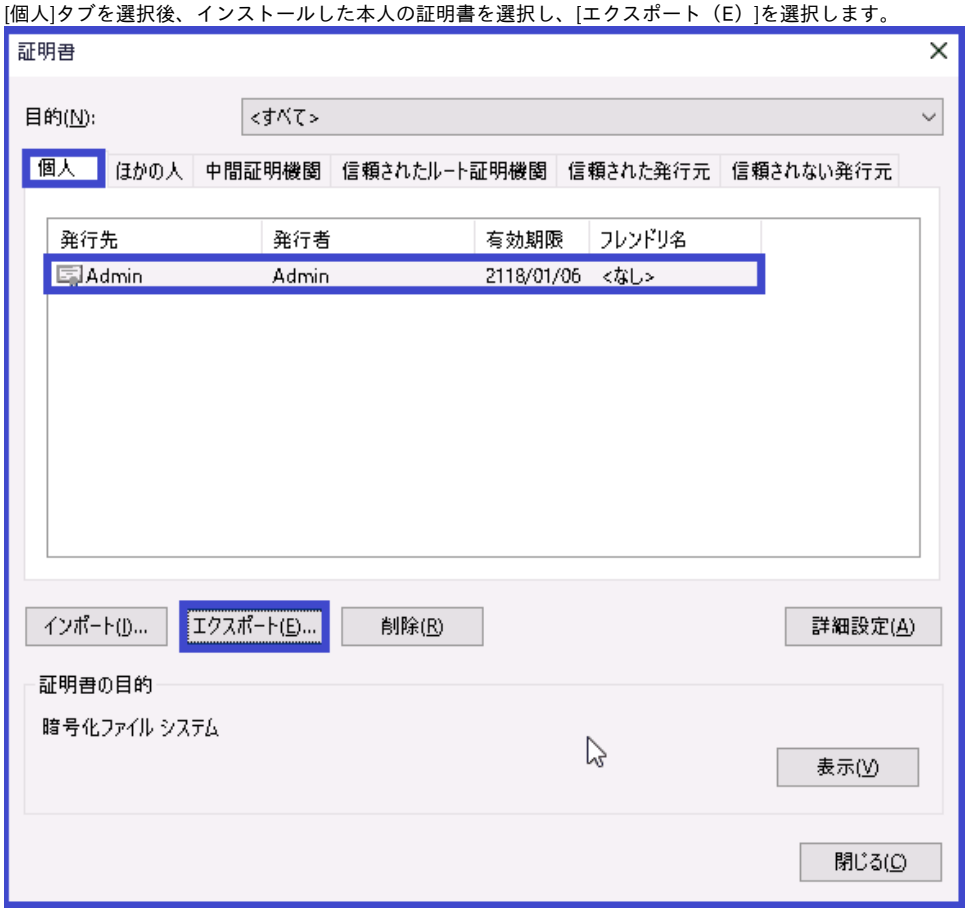
1. Internet Explorer より、[ツール]アイコン-[インターネットオプション(O)]を選択します。



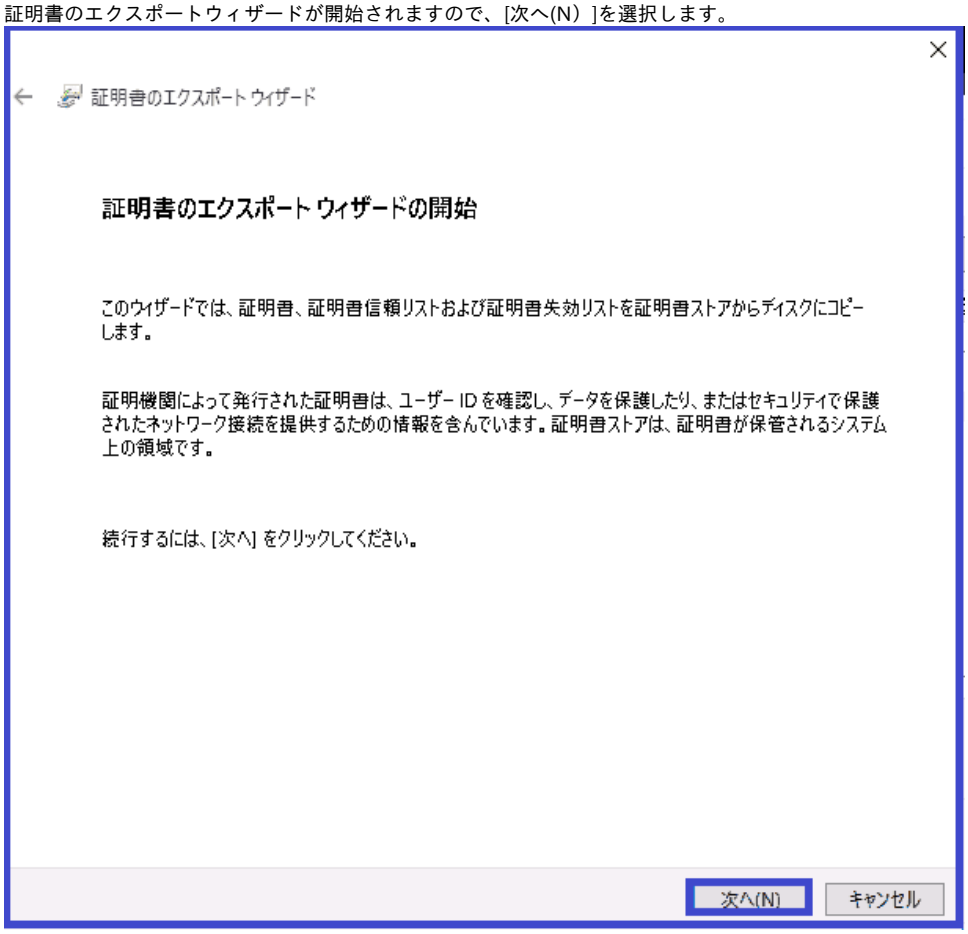
2. [コンテンツ]タブを選択し、[証明書(C)]を選択します。



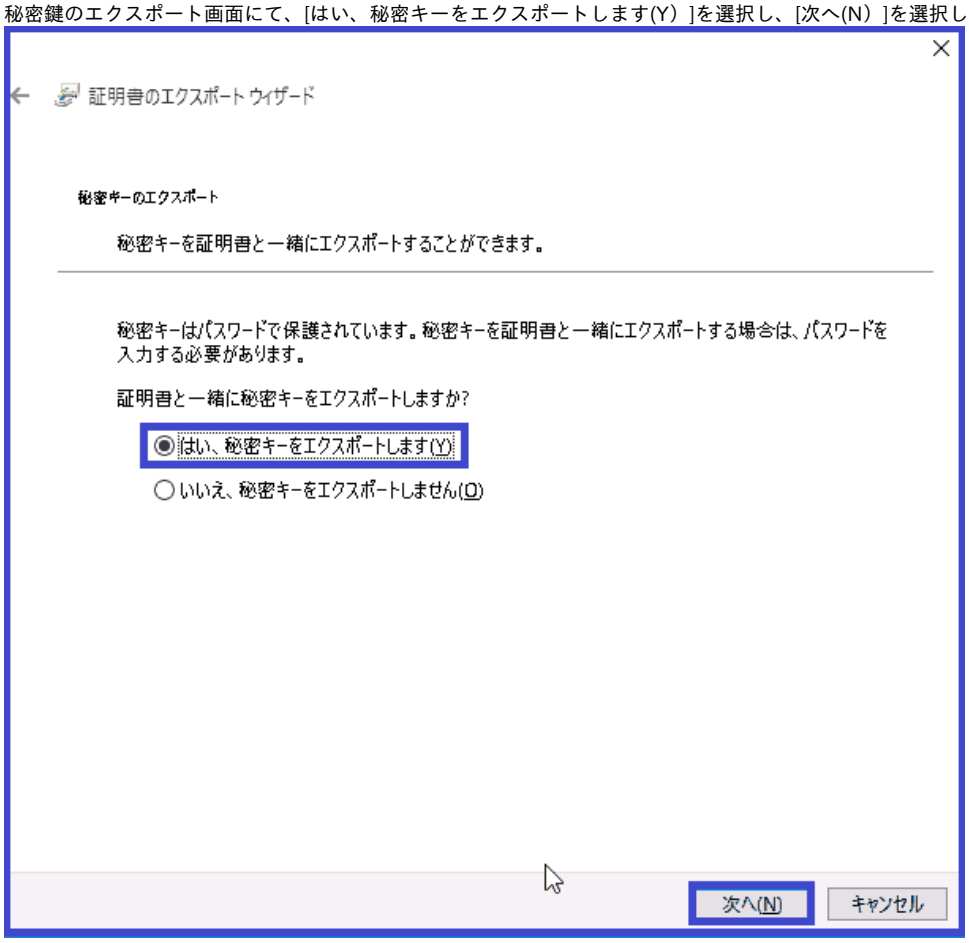
3. [個人]タブを選択後、インストールした本人の証明書を選択し、[エクスポート（E）]を選択します。



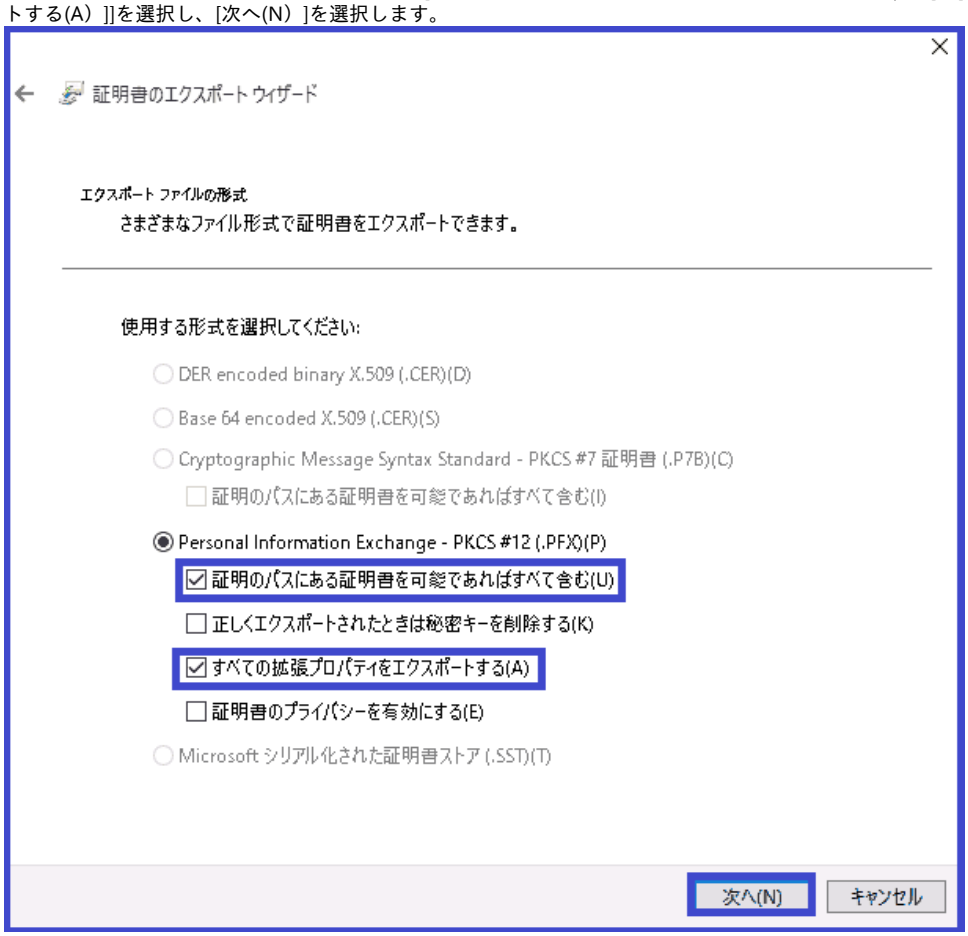
4. 証明書のエクスポートウィザードが開始されますので、[次へ(N）]を選択します。



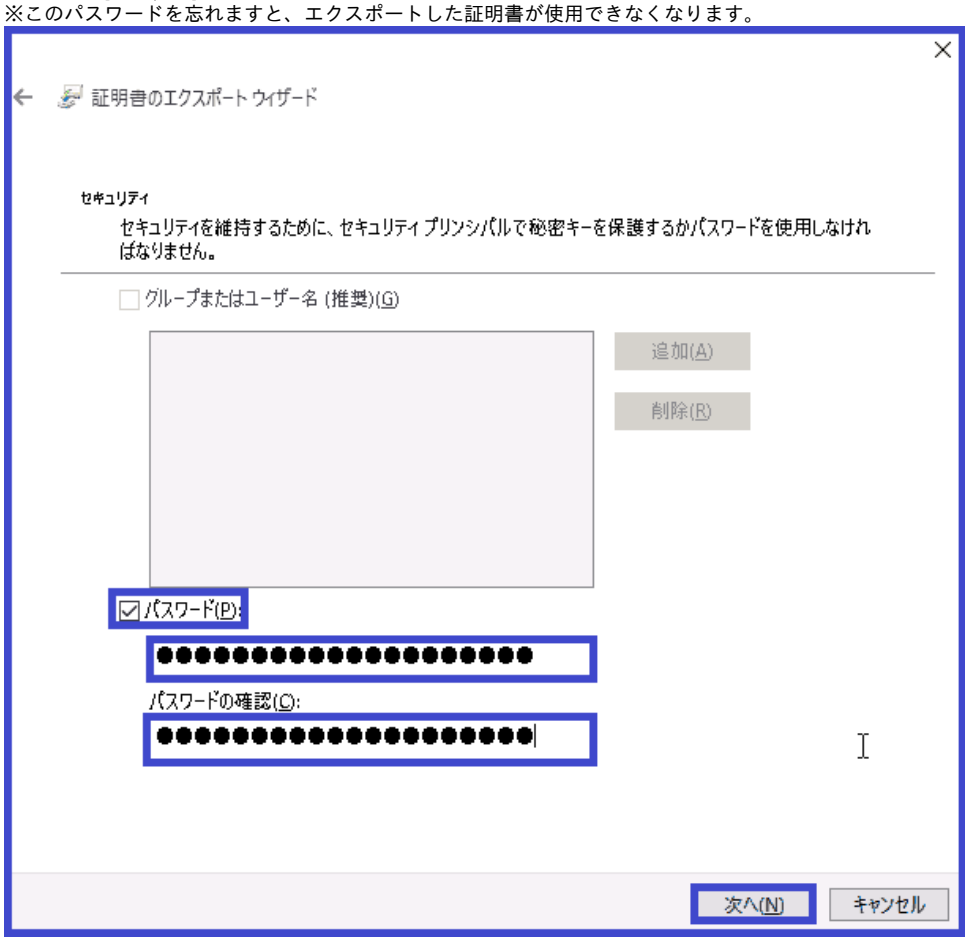
5. 秘密鍵のエクスポート画面にて、[はい、秘密キーをエクスポートします(Y）]を選択し、[次へ(N）]を選択します。



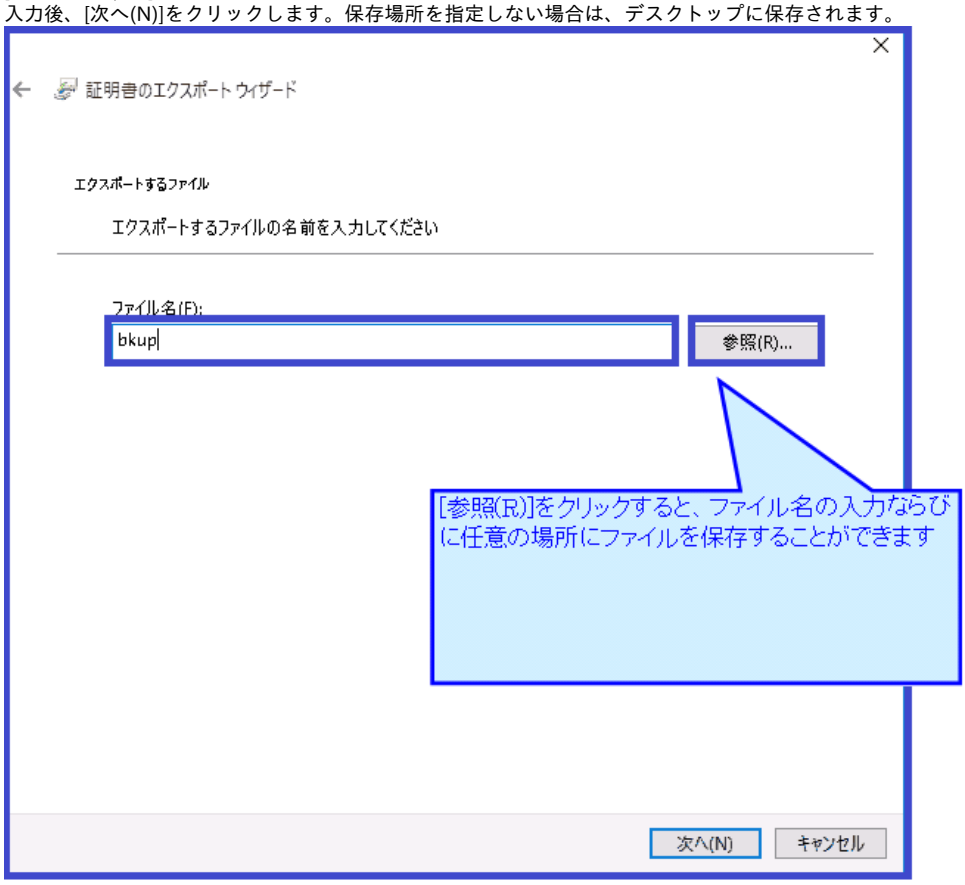
6. エクスポートファイルの形式の選択画面にて、[証明のパスにある証明書を可能であればすべて含む(U）]と[すべての拡張プロパティをエクスポートする(A）]]を選択し、[次へ(N）]を選択します。



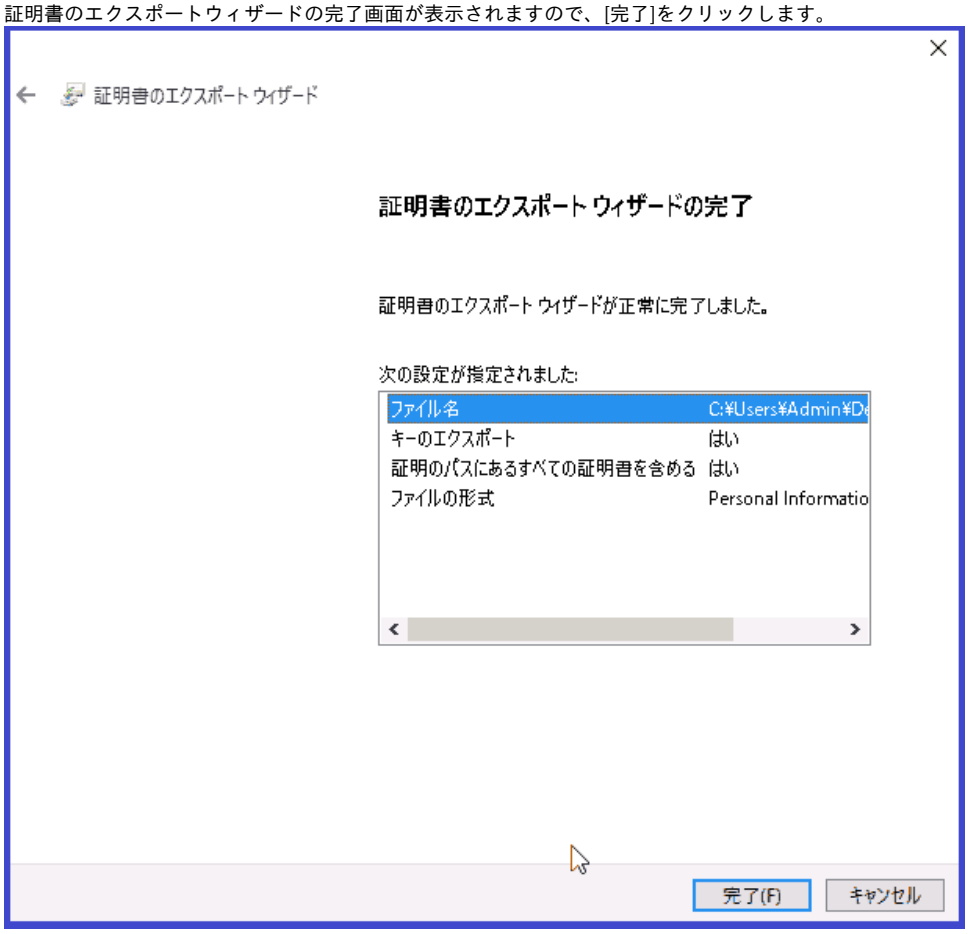
7. [パスワード(P）]にチェック後、入力欄に任意でパスワードを決めて入力してください。[パスワードの確認(C）]の欄に同じパスワードを入力してください。[次へ(N）]をクリックします。
※このパスワードを忘れますと、エクスポートした証明書が使用できなくなります。



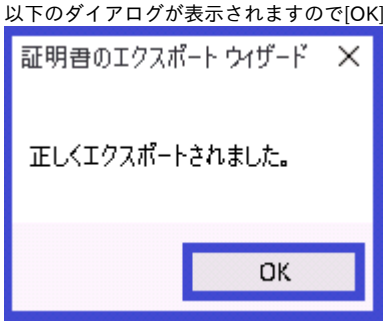
8. [ファイル名(F）]にエクスポートファイルの名前を任意の半角英数字で入力してください。
入力後、[次へ(N)]をクリックします。保存場所を指定しない場合は、デスクトップに保存されます。



9. 証明書のエクスポートウィザードの完了画面が表示されますので、[完了]をクリックします。



10. 以下のダイアログが表示されますので[OK]をクリックします。



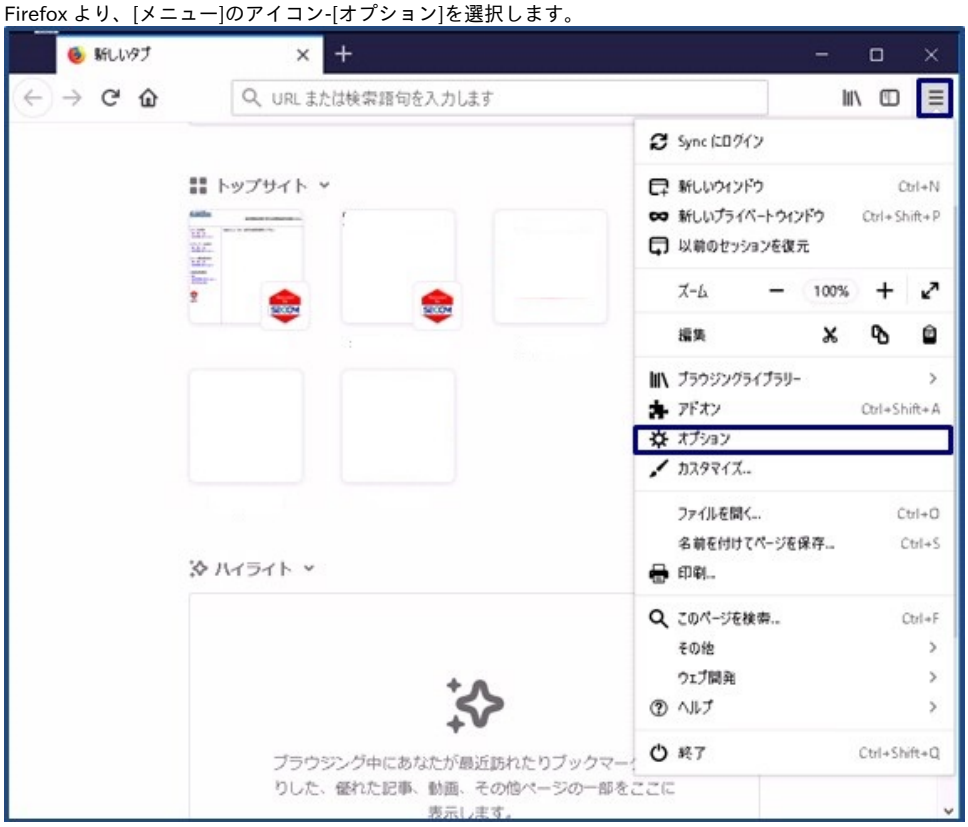
以上で、Internet Explorerでの証明書のエクスポート（バックアップ作成）は完了しました。
エクスポートした証明書は、安全な場所に保管してください。

1-6-2. Firefoxでの証明書のエクスポート手順（バックアップ作成）

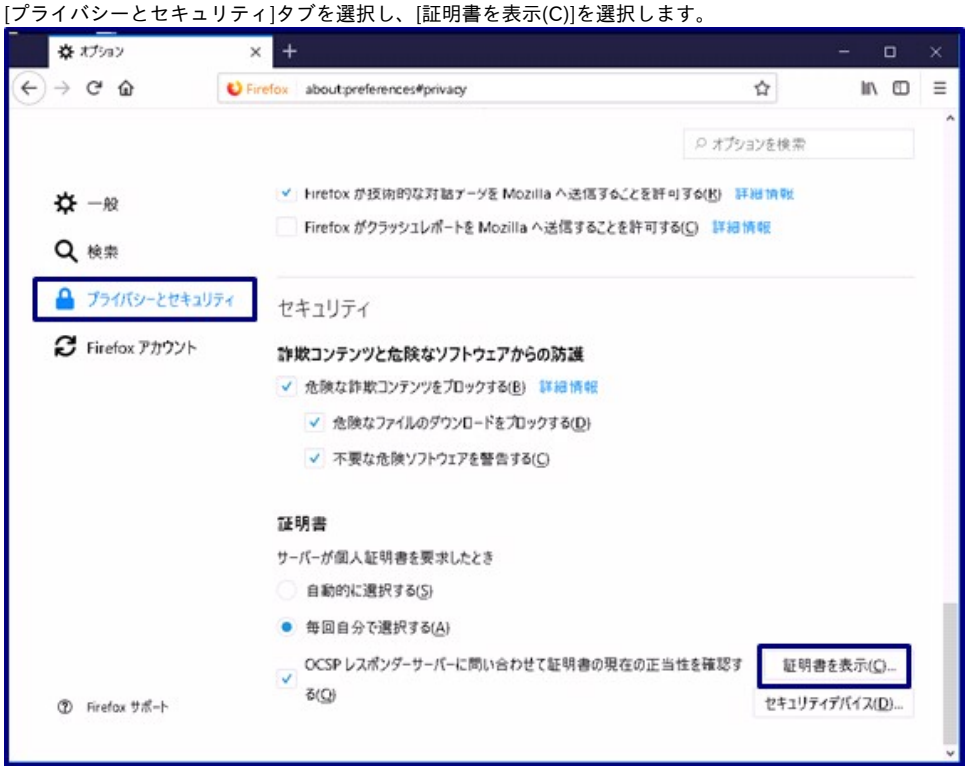
ここでは[Firefox]での証明書のエクスポート手順(バックアップ作成)について記述します。

Firefoxでの証明書発行手続き

1. Firefox より、[メニュー]のアイコン-[オプション]を選択します。



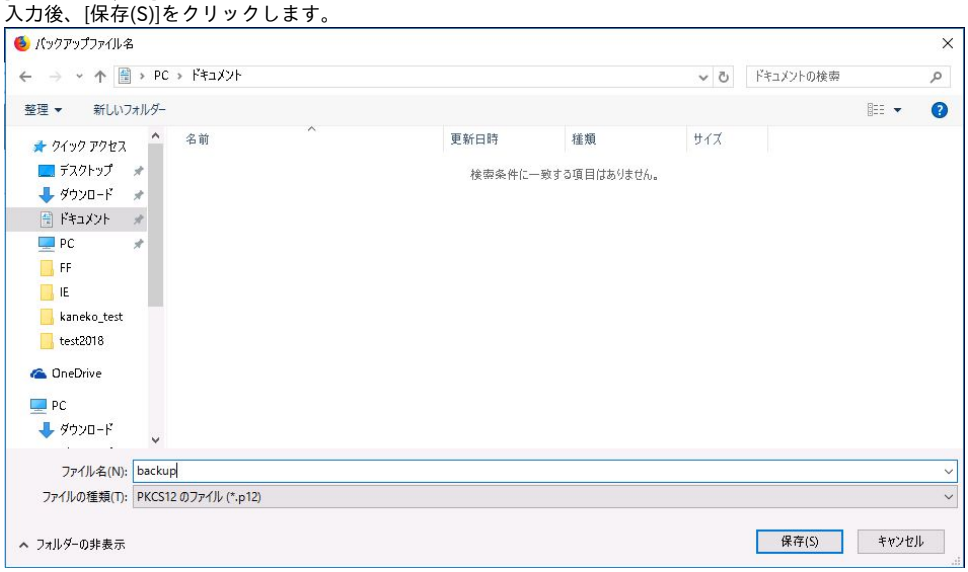
2. [プライバシーとセキュリティ]タブを選択し、[証明書を表示(C)]を選択します。



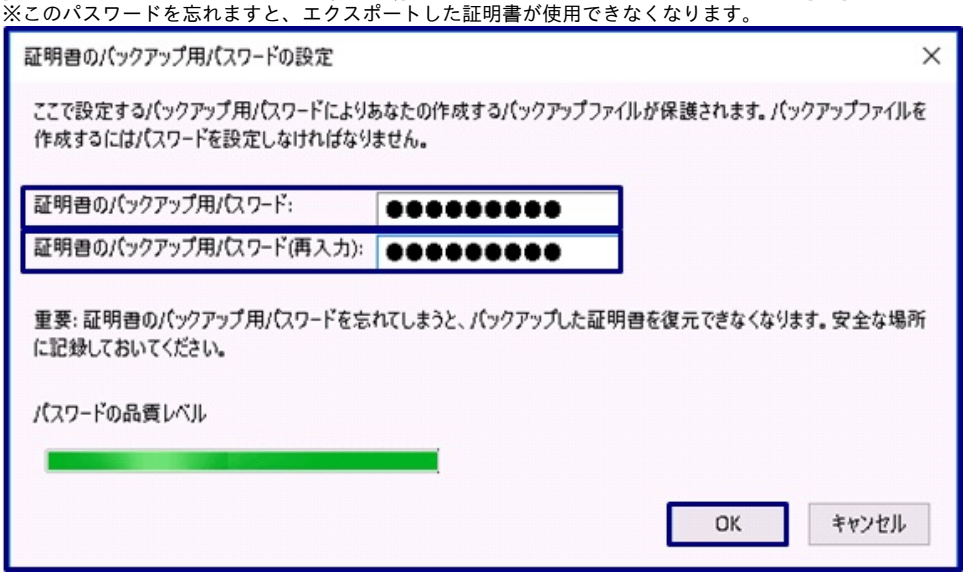
3. [あなたの証明書]タブを選択後、インストールした本人の証明書を選択し、[バックアップ（B）]をクリックします。



4. [ファイル名(N）]にエクスポートファイルの名前を任意で入力してください。
入力後、[保存(S)]をクリックします。



5. 証明書のバックアップ用パスワードの設定画面にて、[証明書のバックアップ用パスワード]の欄に任意でパスワードを決めて入力してください。
[証明書のバックアップ用パスワード(再入力)]の欄に同じパスワードを入力してください。[OK]をクリックします。
※このパスワードを忘れますと、エクスポートした証明書が使用できなくなります。



6. 保存先にバックアップが作成されているかご確認ください。



以上で、Firefoxでの証明書のエクスポート（バックアップ作成）は完了しました。
エクスポートした証明書は、安全な場所に保管してください。