

サーバ証明書管理手順

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	ポ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	2018/07/09	メールテンプレートにおけるLの修正とSTの追記	NII
V2.2	2020/6/4	システム画面の画像の変更	NII
V2.3	2020/7/15	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
V2.4	2021/3/30	システム画面の画像の変更	NII

目次

1. サーバ証明書管理手順

1-1. サーバ証明書新規発行

1-1-1. 利用管理者による鍵ペア・CSRの作成

1-1-2. 利用管理者によるサーバ証明書新規発行申請TSVファイル作成

1-1-3. TSVファイルの受け取り及び審査

1-1-4. サーバ証明書新規発行申請TSVファイルのアップロード

1-1-5. ダウンロード完了通知メール受信

1-2. サーバ証明書更新発行

1-2-1. 利用管理者による鍵ペア・CSRの作成

1-2-2. 利用管理者によるサーバ証明書更新申請TSVファイル作成

1-2-3. TSVファイルの受け取り及び審査

1-2-4. サーバ証明書更新申請TSVファイルのアップロード

1-2-5. ダウンロード完了通知メール受信

1-2-6. 新サーバ証明書への置き換え完了通知

1-2-7. 旧サーバ証明書失効TSVファイルのアップロード

1-2-8. 旧サーバ証明書失効完了通知メール受信

1-2-9. 旧証明書失効依頼再通知について

1-3. サーバ証明書失効

1-3-1. 利用管理者によるサーバ証明書失効TSVファイルの作成

1-3-2. TSVファイルの受け取り及び審査

1-3-3. サーバ証明書失効申請TSVファイルのアップロード

1-3-4. サーバ証明書失効完了メール受信

1-4. サーバ証明書情報取得

1-4-1. サーバ証明書情報取得手順

1. サーバ証明書管理手順

本章では、サービス参加機関の利用管理者に配付するサーバ証明書の発行・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サーバ証明書の発行要求があり、サーバ証明書の新規発行が必要な場合は「1-1. サーバ証明書新規発行」を行ってください。

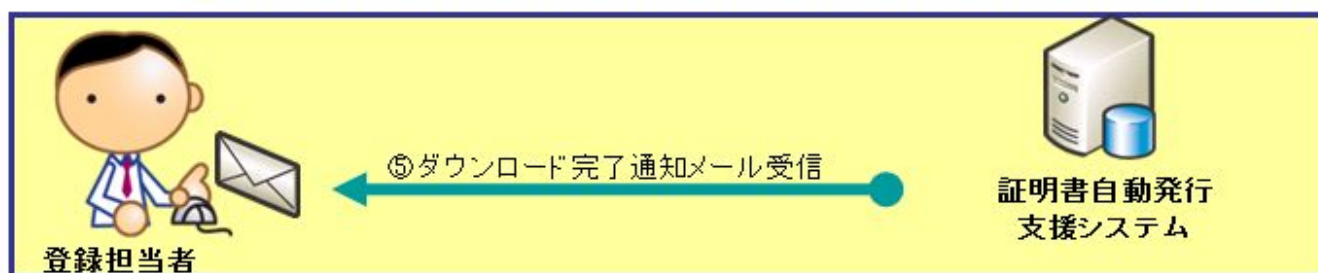
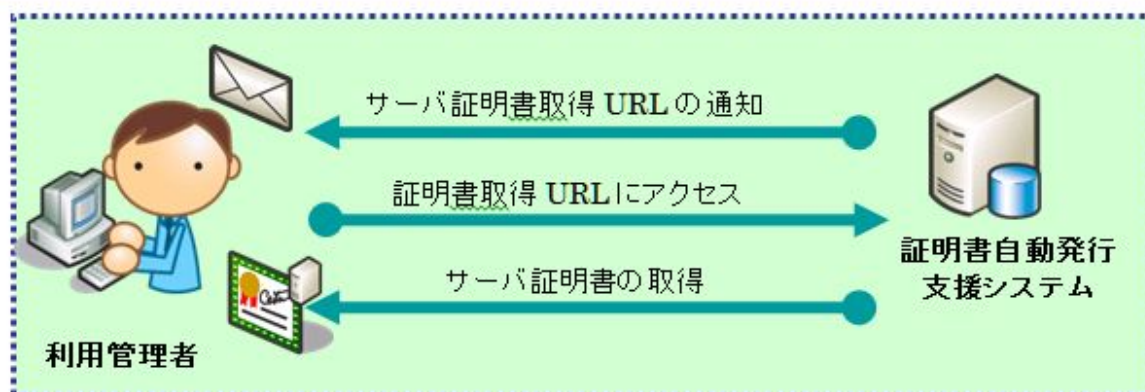
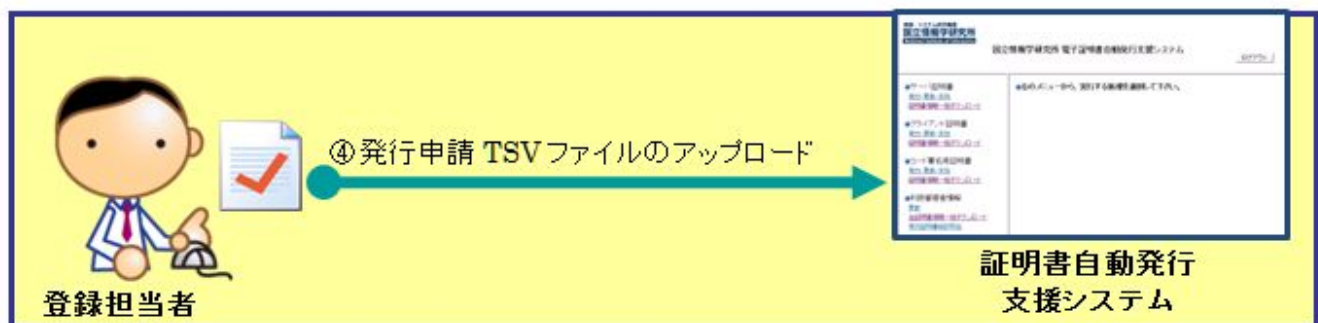
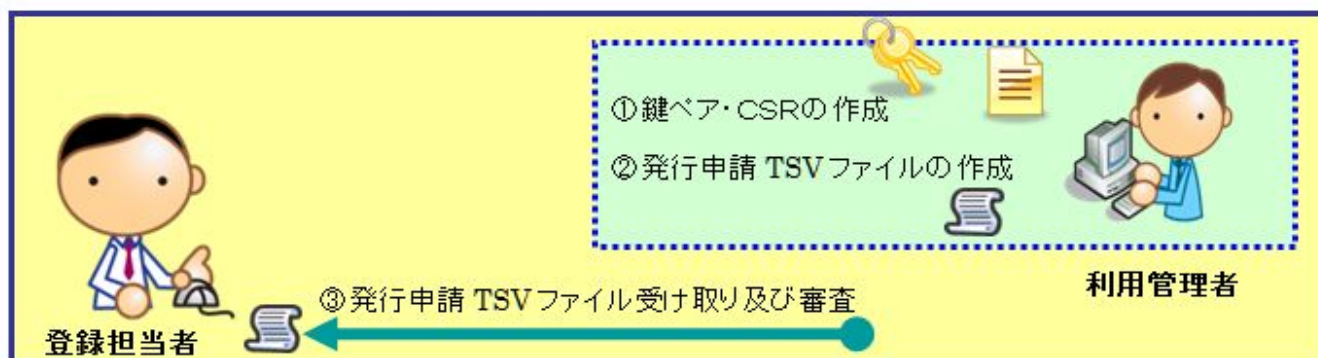
既にサーバ証明書を本システムから発行していて、有効期間が切れるサーバ証明書の更新、失効された証明書の再発行を行う場合は「1-2. サーバ証明書更新発行」を行ってください。

サーバ証明書の失効を行う場合は「1-3. サーバ証明書失効」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 (1-1.サーバ証明書新規発行)	新規にサーバ証明書の発行を必要とする場合。
	サーバ証明書の記載内容（主体者DN）を変更する場合。
証明書更新発行 (1-2.サーバ証明書更新発行)	サーバ証明書の記載内容(主体者DN以外)を変更する場合。
	サーバ証明書を継続利用したい場合。
	失効されたサーバ証明書の再発行を行う場合。
証明書失効 (1-3.サーバ証明書失効)	サーバ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. サーバ証明書新規発行

以下に記述する手続きにより、サーバ証明書の新規発行を行います。



サーバ証明書新規発行

【利用管理者→登録担当者】

- ①サーバ証明書を申請する際に必要となる鍵ペア及びCSRの作成を行います。(1-1-1に記載)
- ②サーバ証明書新規発行申請TSVファイルを作成します。TSVファイルに[①鍵ペア・CSRの生成]で生成したCSRを貼り付けます。(1-1-2に記載)

【登録担当者作業】

- ③サーバ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際には、利用管理者の本人確認を行ってください。(1-1-3に記載)
- ④サーバ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。(1-1-4に記載)

【利用管理者作業】

- ・サーバ証明書発行受付通知メール受信を受信します。
- ・サーバ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。
- ・サーバ証明書のダウンロード。

【登録担当者作業】

- ⑤ダウンロード完了通知メール受信。（1-1-5に記載）

1-1-1. 利用管理者による鍵ペア・CSRの作成

利用管理者はサーバ証明書の発行申請を行うため事前に鍵ペア及びCSRの作成を行います。

1-1-2. 利用管理者によるサーバ証明書新規発行申請TSVファイル作成

利用管理者は、サーバ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。

1-1-3. TSVファイルの受け取り及び審査

登録担当者は、利用管理者からサーバ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。

1-1-4. サーバ証明書新規発行申請TSVファイルのアップロード

「1-1-3. 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。

サーバ証明書新規発行申請手続き

1. 「ログイン方法」を参考に、本システムに接続してください。
2. サーバ証明書の[発行・更新・失効]を選択してください。

情報・システム研究機構 国立情報学研究所 National Institute of Informatics	
国立情報学研究所 電子証明書自動発行支援システム	
ログアウト	
●サーバ証明書 発行・更新・失効 証明書情報一括ダウンロード ●クライアント証明書 発行・更新・失効 証明書情報一括ダウンロード ●利用管理者情報 更新 全証明書情報一括ダウンロード 発行証明書統計照会 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	●左のメニューから、実行する処理を選択して下さい。

3. [サーバ証明書 発行・更新・失効]画面が開きましたら、処理内容で[サーバ証明書 発行]を選択してください。

●サーバ証明書 発行・更新・失効画面

サーバ証明書申請ファイルをアップロードして下さい。

サーバ証明書 発行 ▼

処理中にエラーが発生した場合

☒ 全件処理を中断する

☐ 入力値不備のないデータのみ登録する

参照...

アップロード

4. 処理中にエラーが発生した場合の支援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つとなります。
- ・ 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。

●サーバ証明書 発行・更新・失効画面

サーバ証明書申請ファイルをアップロードして下さい。

サーバ証明書 発行 ▼

処理中にエラーが発生した場合

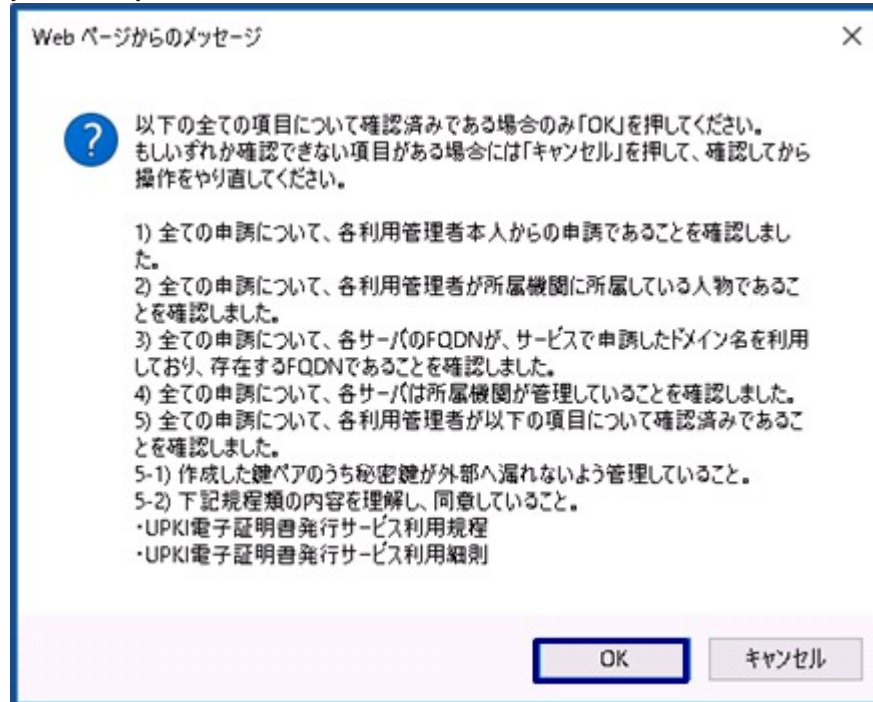
☒ 全件処理を中断する

☐ 入力値不備のないデータのみ登録する

C:\test.tsv 参照...

アップロード

5. [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。

6. 下記画面が表示されれば登録完了です。

●サーバ証明書 発行・更新・失効申請完了画面

ファイルのアップロード処理が完了しました。

- 証明書発行処理が完了後、利用管理者様宛にワンタイムURL付き証明書発行案内メールを送信致します。
- 証明書ダウンロードが完了後、登録担当者様宛にダウンロード完了案内メールを送信致しますのでお待ち下さい。

7. 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。

●サーバ証明書 発行・更新・失効申請エラー画面

サーバ証明書 発行処理が以下のエラーにより正常終了しませんでした。

SEQ	処理結果	エラー内容
1	NG	241:1.主体者DN,主体者DNの機関名が申請者の所属機関名ではありません。

8. 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。

1-1-5. ダウンロード完了通知メール受信

サーバ証明書新規発行依頼者である利用管理者がサーバ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。

サーバ証明書ダウンロード完了通知メール

【件名】
サーバ証明書取得通知

【本文】

．．．．．

貴機関利用管理者の方がサーバ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】

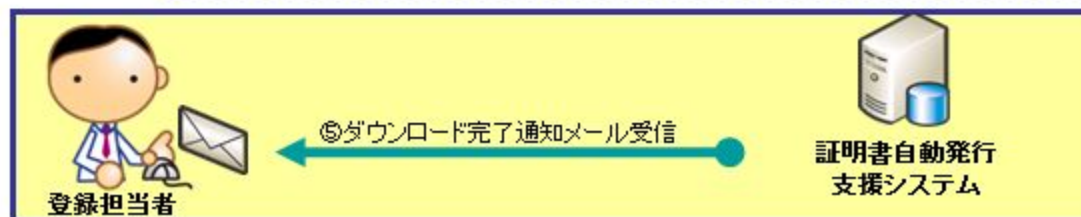
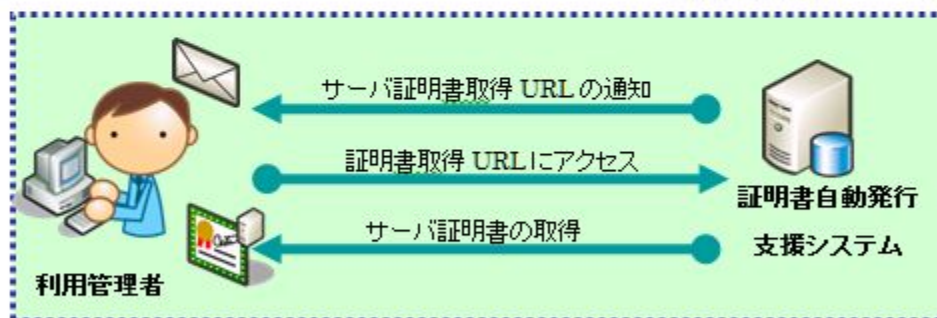
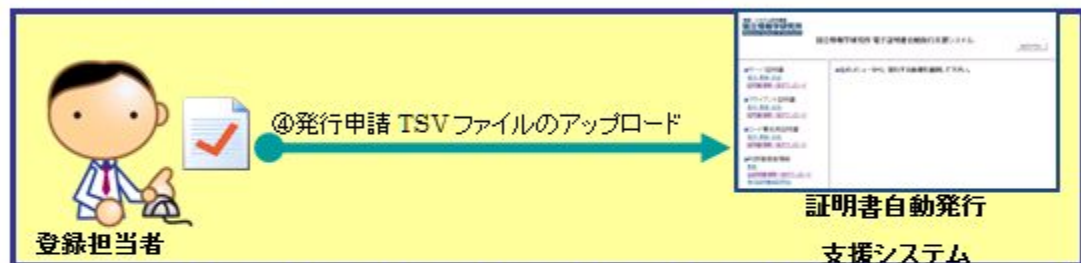
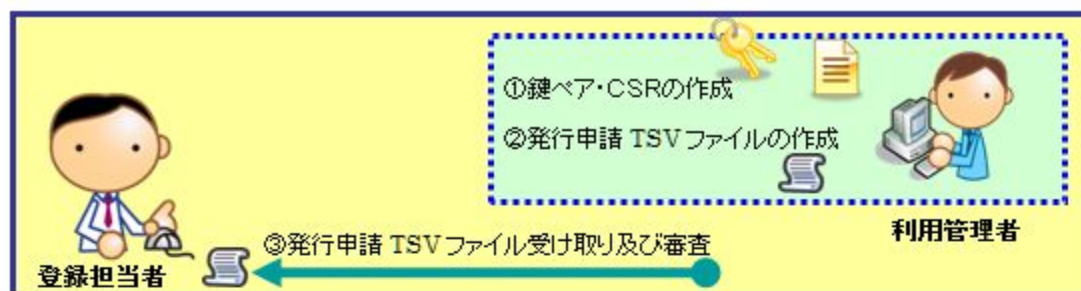
．．．．．

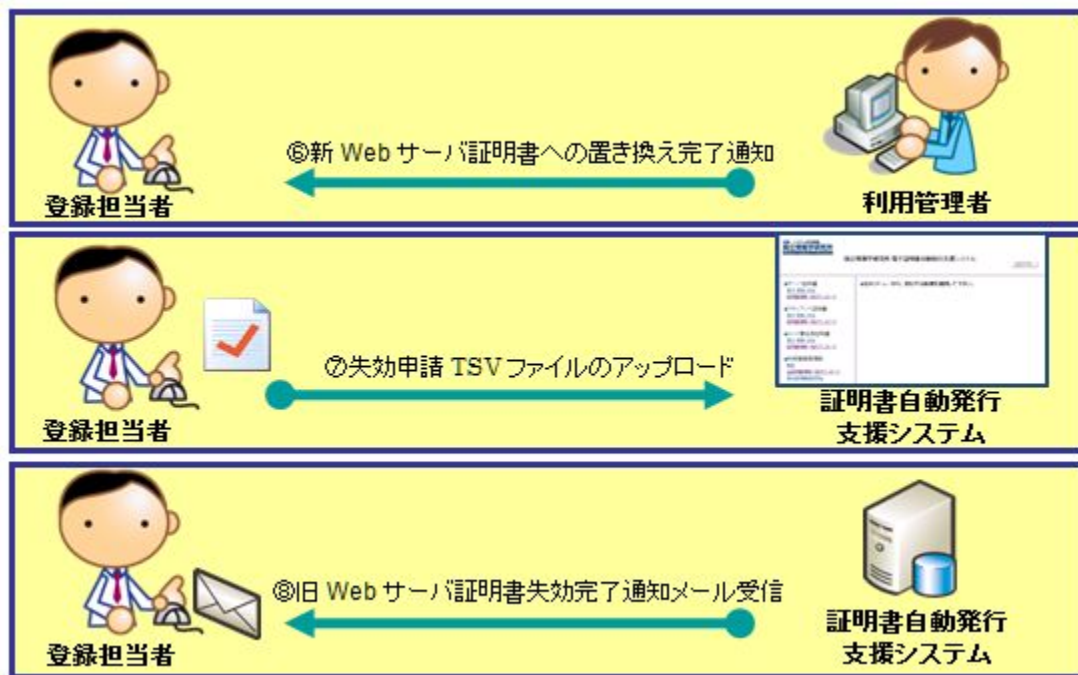


一定期間がたってもダウンロード完了通知メールが受信されない場合は、該当の利用管理者へ電話にて連絡を行い、状況を確認してください。

1-2. サーバ証明書更新発行

以下に記述する手続きにより、サーバ証明書の更新発行を行います。





サーバ証明書更新
【利用管理者作業→登録担当者】 ①サーバ証明書を更新申請する際に必要となる鍵ペアCSRを作成します。（1-2-1に記載） ②サーバ証明書更新申請TSVファイルを作成します。TSVファイルに[①鍵ペア・CSRの生成]で生成したCSRを貼り付けます。（1-2-2に記載）
【登録担当者作業】 ③サーバ証明書更新申請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際には、利用管理者の本人性確認を行ってください。（1-2-3に記載） ④サーバ証明書更新申請TSVファイルのアップロードを行います。（1-2-4に記載）
【利用管理者作業】 ・サーバ証明書発行受付通知メールを受信します。 ・サーバ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。 ・サーバ証明書をダウンロードします。
【登録担当者作業】 ⑤ダウンロード完了通知メールを受信します。（1-2-5に記載）
【利用管理者作業】 ・旧サーバ証明書から新サーバ証明書への置き換え作業を行います。 ・登録担当者に新サーバ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】 ⑥利用管理者から新サーバ証明書への置き換え完了通知を受けます。（1-2-6に記載） ⑦[⑥新サーバ証明書への置き換え完了通知]がきたら、[⑤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。（1-2-7に記載） ※[⑤ダウンロード完了通知メール受信]から2週間のうちに、[⑦旧サーバ証明書の失効申請]が行われないと本システムより旧サーバ証明書失効依頼のメールが再通知されます。 ⑧旧サーバ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。（1-2-8に記載）

1-2-1. 利用管理者による鍵ペア・CSRの作成

利用管理者はサーバ証明書の更新申請を行うため事前に鍵ペア及びCSRの作成を行います。

1-2-2. 利用管理者によるサーバ証明書更新申請TSVファイル作成

利用管理者は、サーバ証明書更新申請TSVファイルを作成します。TSVファイルには「1-2-1. 利用管理者による鍵ペア・CSRの作成」で生成されたCSRの情報が必須です。

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。

1-2-3. TSVファイルの受け取り及び審査

登録担当者は、利用管理者からサーバ証明書更新申請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。

サーバ証明書更新申請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、サーバ証明書更新申請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「1-4. サーバ証明書情報取得」に記載しています。

1-2-4. サーバ証明書更新申請TSVファイルのアップロード

アップロード方法に関しましては「1-1-4. サーバ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。「1-1-4. サーバ証明書新規発行申請TSVファイルのアップロード」の3.の手続きで、[サーバ証明書 更新]をクリックしてください。

サーバ証明書更新手続き

サーバ証明書更新申請TSVファイルのアップロード時、[サーバ証明書 更新]を選択してください。

●サーバ証明書 発行・更新・失効画面

サーバ証明書申請ファイルをアップロードして下さい。

サーバ証明書 更新

処理中にエラーが発生した場合
☒ 全件処理を中断する
☐ 入力値不備のないデータのみ登録する

参照...

アップロード

1-2-5. ダウンロード完了通知メール受信

利用管理者が更新したサーバ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、旧サーバ証明書が有効の場合、TSVファイル（旧サーバ証明書失効申請TSVファイル）が添付されています。旧サーバ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「旧サーバ証明書から新サーバ証明書への置き換えが完了した」との連絡を利用管理者から受けた後、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、「1-2-6. 新サーバ証明書への置き換え完了通知」以降に手順を説明します。

旧サーバ証明書失効申請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ファイル付き更新サーバ証明書ダウンロード完了通知メール

件名: [UPKI] Webサーバ用証明書更新通知

添付ファイル: 1911649278160095962-test1.example.ac.jp.tsv

旧サーバ証明書失効申請TSVファイル CN=test1.example.ac.jp,O=testkikan,L=Chiyoda-ku,ST=Tokyo,C=JP 1911649278160095962 ... 1911649278160095962 ...

• • • • •

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

XXXXXXXXXXXX

191164927816009596

1-2-6. 新サーバ証明書への置き換え完了通知

1-2-7. 旧サーバ証明書失効TSVファイルのアップロード

1-2-8. 旧サーバ証明書失効完了通知メール受信

サーバ証明書失効完了通知

■ ■ ■ ■ ■

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

XXXXXXXXXXXX

その他

■ ■ ■ ■ ■

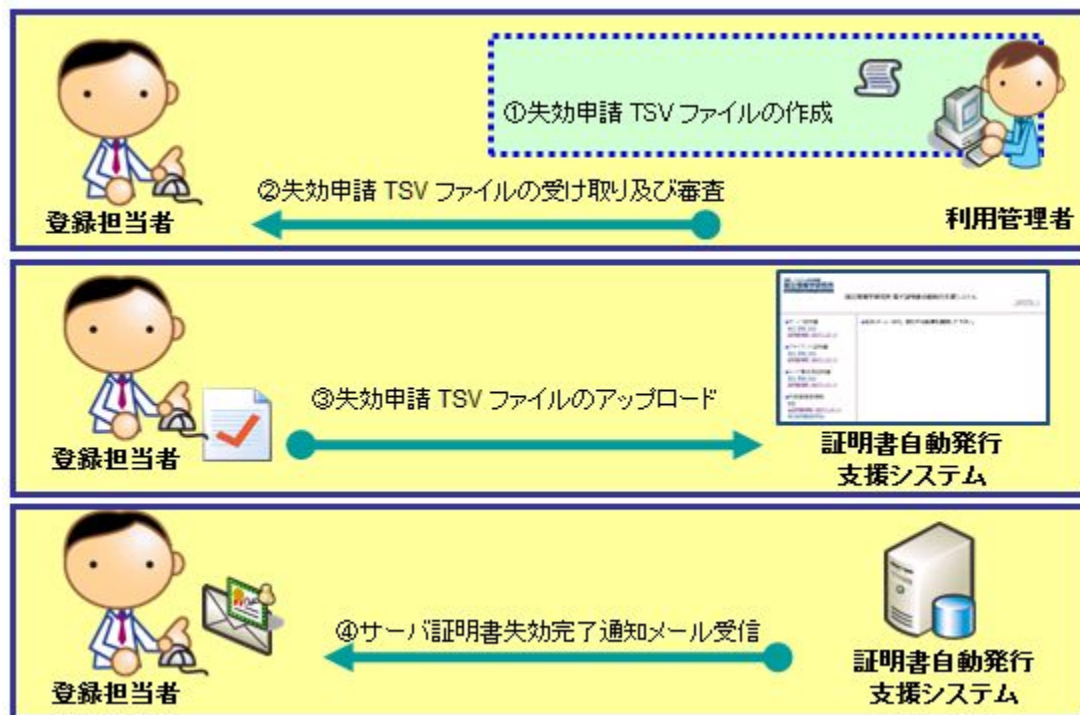
1-2-9. 旧証明書失効依頼再通知について

利用管理者による新サーバ証明書のダウンロード完了から2週間経過後、旧サーバ証明書が有効のままであった場合、旧サーバ証明書の失効依頼再通知メールが本システムから送信されます。
 本メールを受信した場合は、利用管理者へ置き換え状況の確認を行い、[1-2-7. 旧サーバ証明書失効TSVファイルのアップロード]に従い速やかに失効申請を行ってください。
 尚、本メールには旧サーバ証明書失効TSVファイルは添付されておられませんのでご注意ください。
 <再通知が行われる主な原因>

- 「1-2-6. 新サーバ証明書への置き換え完了通知」を利用管理者が行わず、登録担当者が旧サーバ証明書の失効を延期させている場合
- 「1-2-6. 新サーバ証明書への置き換え完了通知」を利用管理者が行ったものの、登録担当者が何らかの理由で、旧サーバ証明書の失効を実施しなかった場合

失効申請依頼再通知
【件名】 サーバ証明書更新(旧証明書の失効申請)再通知 【本文】 利用管理者の方がサーバ用更新証明書を取得してから2週間が経過いたしました。 旧証明書から更新証明書へ置き換えた上で、速やかに失効申請をお願い申し上げます。 #該当のサーバの更新状況を確認してください。 【旧証明書のシリアル番号】 XXXXXXXXXX

1-3. サーバ証明書失効



以下に記述する手続きにより、サーバ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サーバ証明書失効申請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サーバ証明書失効申請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際には、利用管理者の本人確認を行ってください。（1-3-2に記載）

③サーバ証明書失効申請ファイルのアップロード。（1-3-3に記載）

④サーバ証明書失効完了通知メール受信。（1-3-4に記載）

1-3-1. 利用管理者によるサーバ証明書失効TSVファイルの作成

利用管理者は、サーバ証明書失効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。

1-3-2. TSVファイルの受け取り及び審査

登録担当者は、利用管理者からサーバ証明書失効申請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。

サーバ証明書失効申請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、サーバ証明書失効申請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「1-4. サーバ証明書情報取得手順」に記載しています。

1-3-3. サーバ証明書失効申請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。

サーバ証明書失効申請手続き

「1-3-2.TSVファイル受け取り及び審査」で受け取ったTSVファイルを保存し、本システムにアップロードしてください。本システムアップロード時、[サーバ証明書 失効]を選択してください。

●サーバ証明書 発行・更新・失効画面

サーバ証明書申請ファイルをアップロードして下さい。

サーバ証明書 失効

処理中にエラーが発生した場合

☒ 全件処理を中断する

☐ 入力値不備のないデータのみ登録する

参照...

アップロード

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処理後メールが送信されます。

1-3-4. サーバ証明書失効完了メール受信

サーバ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。

サーバ証明書失効完了通知メール

【件名】
サーバ証明書失効完了通知

【本文】
．．．．．

下記サーバ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. サーバ証明書情報取得

サーバ証明書の情報取得について説明します。

主な利用用途

1. 過去に申請したサーバ証明書発行・失効・更新履歴や処理状況を知りたい場合。
2. サーバ証明書の更新・失効に当たり、旧サーバ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サーバ証明書一式を取得したい場合。
4. 各サーバ証明書の利用管理者情報を知りたい場合。

1-4-1. サーバ証明書情報取得手順

サーバ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「[本システムで扱うファイル形式](#)」を参照してください。

サーバ証明書情報取得方法

「サーバ証明書-証明書情報一括ダウンロード」を選択し、サーバ情報 証明書情報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。

情報・システム研究機構
国立情報学研究所
National Institute of Informatics

国立情報学研究所 電子証明書自動発行支援システム

ログアウト

●サーバ証明書 発行・更新・失効 証明書情報一括ダウンロード	●サーバ証明書 証明書情報一括ダウンロード画面 貴機関が申請を行ったサーバ証明書情報を、全てダウンロードします。 ダウンロードボタンを押して、ダウンロード先を指定して下さい。 ダウンロード
●クライアント証明書 発行・更新・失効 証明書情報一括ダウンロード	
●利用管理者情報 更新 全証明書情報一括ダウンロード 発行証明書統計照会 許可リスト一括ダウンロード	