「サーバ証明書発行・導入の啓発・評価研究プロジェクト」

証明書更新手続きについて(加入者用)

1.01
2008 年 6 月 12 日

国立情報学研究所

改訂履歴		
版数	日付	内容
V1.00	2008/04/10	初版（配布開始）
V1.01	2008/06/12	証明書失効手続き文章修正

-- 目次 --

1. 証明書の更新のご連絡

「サーバ証明書発行導入における啓発・評価研究プロジェクト（以下「本プロジェクト」という。）では，平成 20 年 4 月 1 日以降発行する証明書の有効期限を平成 22 年 6 月 30 日まで延長しました。

平成 20 年 3 月 31 日以前に発行した証明書についても，更新手続きを行うことで，有効期限を平成 22 年 6 月 30 日に更新することが可能です。

証明書の更新をご希望される場合は，本書の手順によりお申し込みください。

なお，本プロジェクトは平成 21 年 3 月 31 日をもって終了します。平成 21 年度以降の証明書発行については現在検討中ですが，継続する場合においても本プロジェクトで発行した証明書は平成 21 年度前半を目処にすべて失効いたします。そのため，更新を行った場合でも，平成 21 年度に再度証明書の入れ替え作業が必要となりますのでご承知おきください。

なお，平成 21 年度以降の証明書発行については，詳細が決まり次第お知らせいたします。

2. 証明書の更新フロー

証明書更新の流れを図示します。本資料は証明書の更新手続き時の加入者の作業を説明するためのものです。

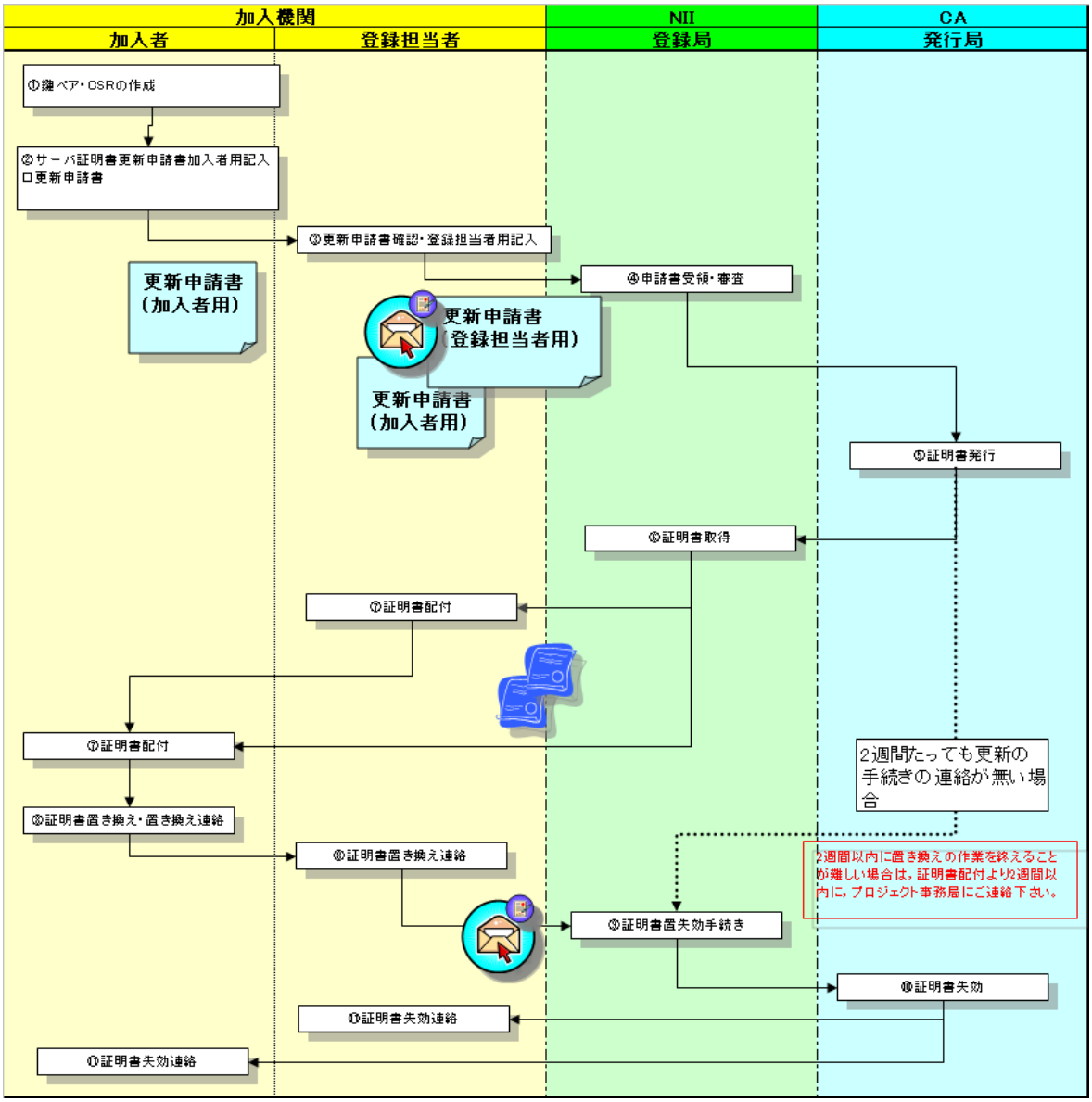

図 1 証明書の更新フロー

3. 鍵ペア・CSR の作成

サーバ証明書の更新には,**新たに更新用の鍵ペア,CSR を作成**していただく必要がございます。CSR を作成される場合，DN の項目は更新用の証明書と同じ値を入力してください。

鍵ペア・CSR の作成手順につきましては，UPKI イニシアティブの本プロジェクトホームページで公開させていただいております,「サーバ証明書インストールマニュアル v1.03」(以下，インストールマニュアルという)をご確認ください。

(https://upki-portal.nii.ac.jp/cerpj/niiodcamanual-v103.pdf)

項目	指定内容の説明と注意点	必須	文字数
Country Name	本認証局では必ず「JP」と入力してください。	○	JP 固定
State or Province Name	**本認証局では使用しないでください。「.」（ドット）を入力することで省略できます。**	×	省略
Locality Name	本認証局では必ず「Academe」と入力してください。	○	Academe 固定
Organization Name	更新対象の証明書 subject の O と同じ値を入力してください。	○	半角の英数字、別紙１記載文字以外で 64 文字以内
Organizational Unit Name	更新対象の証明書 subject の OU と同じ値を入力してください。	△	半角の英数字、別紙１記載文字以外で 64 文字以内
Common Name	更新対象の証明書 subject の CN と同じ値を入力してください。	○	FQDN の規格に則った文字で 64 文字以内

○:必須、△:任意、×:使用禁止

4. 更新用サーバ証明書申請書加入者用の記入

更新用サーバ証明書申請書(加入者用)に必要事項を記入し，貴学で決められた所定の方法により登録担当者へ提出してください。更新用サーバ証明書申請書(加入者用)とサーバ証明書失効申請書(加入者用)は以下の URL より取得することができます。記入内容の詳細は本紙後ろの「別紙１」をご確認ください。

更新用サーバ証明書申請書公開場所：https://upki-portal.nii.ac.jp/cerpj

登録担当者より申請書を受領後，申請内容に問題が無ければ証明書の更新手続きを行わせていただきます。
手続きが済み次第、新規申請時と同様の方法で更新した証明書の配付を行わせていただきます。

事務局（登録局），又は登録担当者より証明書を受領後，以下の手続きを行ってください。

5. 証明書の置き換え

サーバ証明書が到着しましたら，以前使用していた鍵ペア，証明書のバックアップを取り，新しく受領した証明書との置き換えを行ってください。証明書の置き換え方法については，インストールマニュアル「3. 証明書のインストール」，またはご使用のアプリケーションのマニュアルをご確認ください。

置き換え後，サーバを再起動し，SSL 通信が正常に行われることを確認してください。正常に動作することを確認後，以前使用していた鍵ペア，証明書の削除をお願いします。

6. 置き換え連絡

鍵ペア・証明書の削除後，必ず登録担当者へ証明書の置き換え終了の連絡を行ってください。置き換えの連絡様式は，本紙後ろの「別紙 2」をご確認ください。

登録担当者から登録局（事務局）への置き換え終了の連絡を持って，証明書の失効を行わせていただきます。

※なお，更新用の証明書発行から 2 週間たっても置き換え終了の連絡をいただけない場合は，登録局の判断により，更新用の証明書の失効を行わせていただくことがあります。置き換え作業に 2 週間以上の期間が必要となる場合は，発行後 2 週間以内にプロジェクト事務局までご連絡ください。

7. その他

用語	説明
オープンドメイン認証局	本プロジェクトで使用する，サーバ証明書を発行するための認証局。Web Trust for CA に準拠しており，世界的に信頼できる証明書の発行が可能です。また，この証明書は，主要なウェブブラウザ等の PKI アプリケーションに標準でルート認証局が搭載されているため、商用のサーバ証明書と同様に利用することができます。
登録局	プロジェクト参加申請、証明書発行申請にあたり、審査業務を行なう NII の事務窓口です。
登録担当者	本プロジェクトの参加機関側の事務的な窓口をお願いする方。大学の規模に応じて複数名選出していただくことが可能です。
加入者	Web サーバを管理し，本プロジェクトのサーバ証明書を利用される方。プロジェクト参加機関内の教職員の方であれば，どなたでも加入者となれます。
加入者サーバ	加入者の方が管理する Web サーバ。
利用者	PKI 加入者サーバにアクセスする，不特定多数の方々のことを，この説明では利用者と呼びます。利用者は、ウェブブラウザ等の標準の機能を利用して加入者サーバの証明書を検証いたします。

プロジェクト事務局（連絡先）

各種申請やお問い合わせこちらにご連絡ください。

〒101-8430　東京都千代田区一ツ橋 2 丁目 1 番 2 号
国立情報学研究所 学術基盤推進部 基盤企画課 連携システムチーム
サーバ証明書発行・導入における啓発・評価研究プロジェクト　事務局
TEL 03-4212-2218／FAX 03-4212-2230
E-mail cerpj@nii.ac.jp

別紙１ 更新用サーバ証明書申請書（加入者用）

○ 更新用サーバ証明書申請書(加入者記入用)					
申請情報	加入者情報	所属			
		氏名			
		E-Mail			
	サーバ情報	FQDN			
		サーバソフト名 及び バージョン			
	ＣＳＲ	-----BEGIN CERTIFICATE REQUEST-----			
		1 ページ			
		-----END CERTIFICATE REQUEST-----			
		※ コピー(カット)アンドペーストを利用してCSRの貼り付ける場合は、セルをダブルクリックしてから行なってください。			
確認欄	失効理由	▼ 失効理由を選択してください。			チェック欄
		鍵危殆化			☐
		内容変更			☐
		取り替え			☐
		運用停止			☐
		その他			☐
確認欄	確認実施日				
	確認項目	▼ 申請するにあたり、次の内容を確認してください。			チェック欄
		作成した鍵ペアのうち秘密鍵が外部へ漏れないよう管理しています。			☐
		新規鍵ペアで本CSRを作成しました。(以前の鍵ペアは使用していません)			☐
		更新用サーバ証明書を受領してから，2週間以内にプロジェクト事務局に証明書置き換えが終了した旨の連絡を行わなかった場合には，登録局によって本申請書で申請した証明書の失効を行うことに同意します。			☐

図 2 更新用サーバ証明書申請書（加入者用）

所属：加入者の所属部署を部名から記入してください

氏名：加入者の氏名を記入してください

E-Mail：加入者の(ac.jp ドメインでの)連絡先 E-Mail を記入してください。

FQDN：サーバの FQDN を記入してください。

サーバソフト名:証明書を更新するサーバのサーバソフト名及び Version を記入してください。

CSR：「３.鍵ペア・CSR の作成」で作成した CSR を貼り付けてください。

失効理由：取替えにチェックをつけてください。

確認項目：記述されている内容に確認・同意し，チェック欄にチェックをつけてください。

別紙 2 証明書置き換え終了連絡フォーム（加入者用）

下のフォームをメール本文に記入の上、更新用証明書の発行日から **2 週間以内に登録担当者へ**送付してください。

※ 発効日から置き換え終了まで 2 週間以上かかる場合，**削除予定日を記入して必ず 2 週間以内に登録担当者へ**送付してください。

=== ここから ===

1）作業進捗：（置き換え終了　　置き換え未実施）

↑どちらかを記述してください。

2）以前の証明書のシリアル番号：

3）以前の証明書の DN:

4）鍵ペア・証明書を削除した日付:

↑置き換えが終了した場合は削除日を記入してください。終了していない場合は記入しないでください。

5）証明書置き換え予定日:

↑置き換えが終了していない場合予定日を記入してください。

=== ここまで ===