

名古屋大学の UPKI サーバ証明書申請システム更新について

○宇田川暢、柘植朗

情報環境部 情報システム運用課

概要

名古屋大学では、国立情報学研究所の提供する「UPKI 電子証明書発行サービス¹」（以下、UPKI）を利用し、学内の各サーバ管理者の利用申請に対応して、サーバ証明書の発行を Web システムにより行ってきた。

しかしながら、UPKI のルール変更や申請内容に問題のある場合の手戻りへの対応、Web システムからの申請用ファイルのダウンロードと専用 Web サイトへのアップロードにかかる作業時間といった問題から、今回 Web システムを刷新することとした。本稿ではこの新 Web システムについて紹介する。

1 はじめに

名古屋大学では国立情報学研究所（以下、NII）が提供する「UPKI 電子証明書発行サービス（以下、UPKI）」を利用している。UPKI は 2015 年 1 月から正式にサービス提供が開始されたが、前身となる「UPKI オープンドメイン証明書自動発行検証プロジェクト」としてサービス提供されていた 2007 年から、名古屋大学では証明書発行サービスを利用してきた。

その際に、「名古屋大学 UPKI サーバ証明書発行プロジェクト」として、学内からの利用申請受付のための Web システム^{[1][2]}（以下、従来システム）を構築しており、これまで改修を繰り返しながら運用を続けてきた。

2 UPKI の概要

UPKI でサーバ証明書を発行する際には、次のような手順で申請を行う必要がある。

1. サーバ証明書の発行を希望する「利用管理者」が、CSR（Certificate Signing Request）を作成する。
2. 当該機関の「登録担当者」宛てに必要な事項と CSR を伝え、サーバ証明書の発行を依頼する。
3. 登録担当者は利用管理者が UPKI の定める基準を満たしているか確認し、また、その申請目的が妥当であるかを判断する。
4. サーバ証明書の発行が妥当であると判断した場合、登録担当者は UPKI の定めるフォーマットで申請用の TSV（Tab Separated Values）ファイルを作成し、UPKI の提供する「支援システム」に TSV ファイルをアップロードする。
5. TSV ファイルの内容に問題が無い場合は、発行申請が完了する。
6. 利用管理者宛てに UPKI から発行通知メールが送信される。
7. 利用管理者が発行通知メールに記載された URL から、発行されたサーバ証明書をダウンロードする。
8. 登録担当者宛てに UPKI からサーバ証明書のダウンロード完了通知が送信される。

UPKI では、登録担当者に対して、RA（Registration Authority）の役割である申請者の本人性や申請内容の妥当性の確認作業を委任しているため、登録担当者は申請受付時に厳格な確認を行う必要がある。

¹ <https://certs.nii.ac.jp/certs>

3 従来システムの概要

従来の申請システムでは基本的に次の手順で申請受付を行っていた。

1. サーバ証明書発行を希望する利用管理者は、CSRを作成する。
2. 利用者は多要素認証 CAS での認証後、申請ページにアクセスする。
3. 利用者は CSR に内容および、申請者情報などを記載して申請を完了する。
4. 申請システムは登録されている情報から、サーバ証明書の発行に際して IP アドレス発行責任者の承認が必要かの判定を行う。必要と判断された場合は次へ、不要と判断された場合は 7.へ移る。
5. 申請内容から、該当するネットワーク範囲の IP アドレス発行責任者に、承認メールが送付される。
6. IP アドレス発行責任者はメール本文記載の URL にアクセスし、申請システムで承認処理を行う。
7. 承認された場合、発行手続きを行うための TSV ファイルを生成し、登録担当者にメール送付する。
8. 登録担当者は TSV ファイルの内容を確認後、支援システムにアクセスし、アップロードする。
9. サーバ証明書の発行後、UPKI からダウンロード URL が利用管理者宛てにメール送付される。
10. 利用管理者によるサーバ証明書のダウンロード後、登録担当者に対して UPKI から取得完了通知メールが送付される。
11. 登録担当者は、取得完了通知メールに記載の証明書シリアル番号を申請システムに登録する。

この手順について申請システムが介在する部分をシーケンス図で表したものを図1に示す。

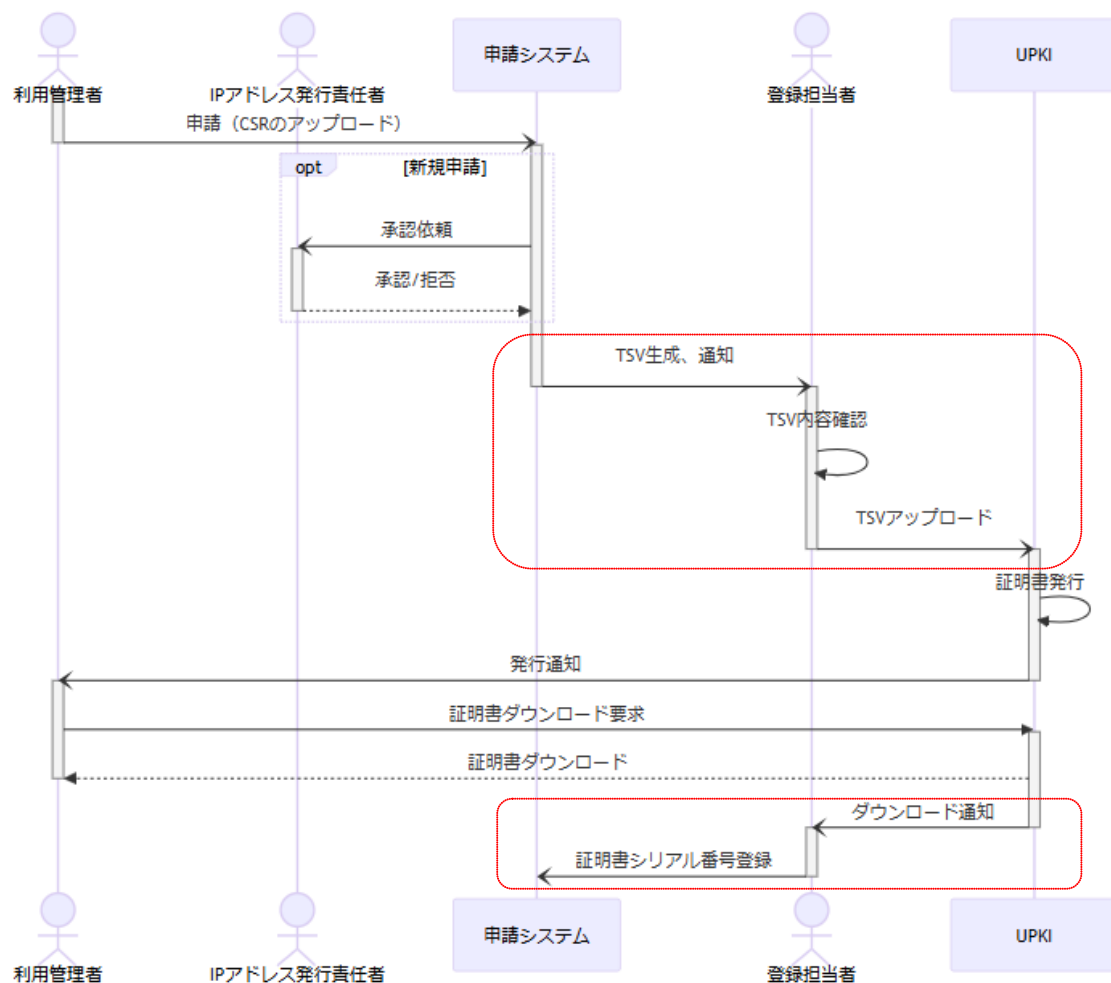


図1 従来システムでの発行申請手順

名古屋大学では、おもに部局などの単位でネットワークを分割し、それぞれ「IP アドレス発行責任者」として管理を委譲している。UPKI の求める申請内容の妥当性の確認の一部を、この IP アドレス発行責任者に依頼している形となる。

異常時を除き、図1において赤色の点線で囲まれた枠内が、登録担当者が対応する必要がある部分となる。証明書シリアル番号を従来システムに登録する理由は、UPKI が新規取得時と同一 DN（Distinguished Name）での更新時で異なるフォーマットの TSV ファイル作成を要求し、更新時には旧証明書のシリアル番号を記載する必要があるためとなっている。また、更新時には受付手順4.で IP アドレス発行責任者に対して、再度の承認作業を求めないようになっている。

4 従来システムでの問題点

従来システムでは、次のような問題が存在していた。

4.1 CSR の内容の厳密なチェック不足

CSR に含まれる DN のそれぞれの値チェックを申請受付時に行っているが、UPKI で利用を許されていない属性値に対する判定や CSR の再利用チェックを行っていなかった。そのため、支援システムに TSV をアップロードする際のエラー表示を確認し、初めて CSR に関する不具合が判明していた。

4.2 複数のホスト名（別名）への対応時の TSV ファイル修正

UPKI では複数の別名に対応したサーバ証明書を作成可能だが、従来システムには申請フォームに入力欄が存在していなかった。また、追加可能なホスト名の数や文字数に複雑な制約があるため、別途メールや Microsoft Forms で作成したフォームで申請を受け付け、登録担当者によるチェックの後に、従来システムから出力される TSV ファイルを手作業で加工して対応していた。

また、別名申請と発行申請が行われたタイミングによっては、別名申請が存在することを認識できず、別名を設定しないままサーバ証明書の発行を行ってしまう事があった。その場合は、再度 CSR の再作成と再申請を依頼していた。

4.3 特定の IP アドレス発行責任者への負担の集中

部局によっては複数の IP アドレス発行責任者が割り当てられている場合がある。しかしながら、従来システムでは IP アドレス発行責任者リストの最初にある担当者にのみ、承認依頼のメールが送られていた。そのため、特定の IP アドレス発行責任者に負担が集中しているという指摘がされることもあった。

4.4 学外 IP アドレス利用時の申請に非対応

近年では、大規模なシステムにおいても IaaS などを利用することが、大学でも一般的になってきている。しかしながら、従来システムでは申請できる IP アドレスの範囲が名古屋大学の管理するグローバル IP アドレスに限定されていたため、IaaS など学外の IP アドレスで UPKI サーバ証明書を利用する場合は、書面で申請書に CSR を添えて提出する必要がある。また、この申請内容をもとに登録担当者が TSV ファイルの作成を行っていた。

4.5 支援システムへの TSV ファイルの手動アップロード

UPKI 担当者は従来システムから送信されたメールに添付の TSV ファイルを受け取り、UPKI が別途提供しているクライアント証明書を利用して、支援システムに TSV ファイルをアップロードする必要がある。また、支援システムはアップロード時の TSV ファイルの内容確認機能を持っていないため、登録担当者は慎重にアップロードするファイルに問題が無いかを確認する必要がある。

4.6 サーバ証明書のシリアル番号の手動登録

前述の通り、UPKI ではサーバ証明書の更新時には、更新対象となる証明書のシリアル番号を TSV ファイル中に記載する必要があるため、必然的に申請システムには発行済みサーバ証明書の DN とそのシリアル番号とを紐づけたデータベースが必要になる。従来システムではこのデータベースへのシリアル番号登録を登録担当者が手動で行う必要があった。

5 従来システムでの問題解決方法の提案

名古屋大学では現在 800 を超える UPKI サーバ証明書を発行しており、これらの作業が登録担当者の負担となっていた。そのため、4章で挙げた問題点につき、以下の対応を行うことで解決できると判断した。

5.1 CSR の厳密なチェックの実施

利用管理者が申請フォームで CSR をアップロードした際に、CSR の内容を詳細にチェックし、UPKI の基準に従っているかの判定を行う。判定結果に問題がある場合は、申請者に不具合の詳細を表示して CSR の再作成を求めるエラーメッセージを表示する。

5.2 申請フォームの別名対応

申請フォームに別名の入力欄を追加し、CSR のアップロードと共に別名への対応依頼が完了するようにする。また、複雑な判定を行い、UPKI の仕様に合わない場合はエラーメッセージを表示する。

5.3 複数の IP アドレス発行責任者への承認依頼

申請時に該当するネットワーク範囲の IP アドレス発行責任者全員に承認依頼メールを送信し、そのうちの誰か一人が承認または却下すれば承認作業完了とする仕様とする。また、承認作業後はその結果について再度全員にメール通知を行う。

5.4 学内 IP アドレスに限らない申請への対応

正引きによるホスト名の解決が DNS により可能な場合は、申請を受け付けることとした。その際に、学内 IP アドレスでない場合は、IP アドレス発行責任者の代わりに登録担当者が承認を行う。

5.5 TSV ファイルの自動送信

TSV ファイルを申請システムからダウンロードすることなく、登録担当者の操作により、操作した本人用のクライアント証明書を用いて、申請システムから直接 TSV ファイルを支援システムにアップロードできるようにする。

5.6 発行したサーバ証明書シリアル番号の自動取得

TSV ファイルの自動送信と同様の仕組みを利用し、支援システムから発行済みサーバ証明書情報の一覧を取得して、申請システムの内部 DB に証明書シリアル番号を格納する。その際、TSV ファイルを送信した履歴を利用し、支援システムへのリクエスト回数を最小限とする。

6 新システムの検討

5章で提案した内容を現行システムで改修するか、別途新規システムを構築するかといった検討を行った。その際に、筆者がすでに作成していた UPKI サーバ証明書管理用システム^[1]を改修し、上記に対応した申請機能を追加することとし、改修を行った。なお、このシステムは開発時に在籍していた新潟大学より、無償提供することを条件に、他大学等への配布を許可されている。

7 新システムでの申請手順

新しい申請システムでの受付手順は、図2のようになった。

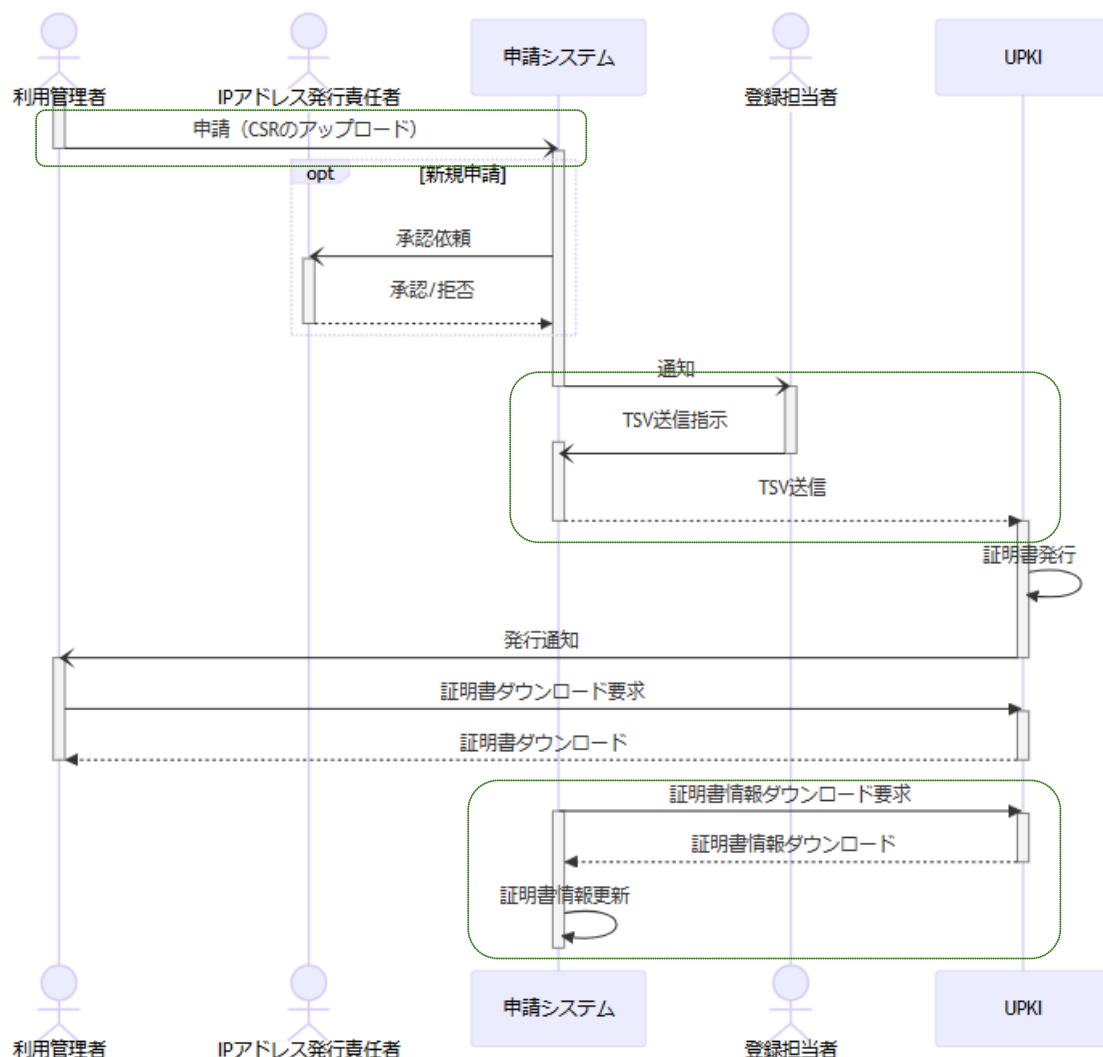


図2 新システムでの受付手順

緑色の点線で囲まれた枠の部分が主な改善点となっている。この変更により、登録担当者は申請システムからの通知メールに記載されたリンクから申請内容の確認用ページに遷移し、内容を確認して TSV 送信ボタンをクリックするだけで、申請にかかる手続きを完了することができるようになった。また、いままでは例外対応していた内容についても前述のとおり自動化したため、申請に関する登録担当者の負担が大幅に軽減された。

8 今後について

本稿執筆時点ではまだ提案の段階だが、サーバ証明書などの運用基準を定める CA/Browser Forum において、サーバ証明書の有効期限を最大 47 日とすることについて議論がされている²。現在パブリック CA が発行可能とされているサーバ証明書の最長有効期限が 398 日であることからすると、大幅な短縮となる。

一般的にサーバ証明書の有効期限短縮はセキュリティの面において利点があるが、サーバ証明書の更新作

² <https://github.com/cabforum/servercert/pull/553>

業が自動化されていない場合は、サーバ管理者の労力の増加につながり、UPKI の仕組みにおいては登録担当者の負担増加にもなる。

サーバ証明書の有効期限が短縮され続けてきた過去の経緯から、UPKI の事務局でも数年前からサーバ証明書の自動発行対応への検討を行っている³と事務局の担当者から伝え聞いている³が、現時点で具体的な実現方法などは提示されていない。これについて、システム改修の問題だけでなく、RA の機能を登録担当者に委任している部分をどのようにするかという調整が難しいためではないかと推測している。いずれにしろ、CA/Browser Forum と UPKI の状況を見守るしかない状態である。

UPKI のように長期間提供されるサービスにおいては、サービス側の仕様変更および学内での運用の習熟による改善の要望により、システムの改修が必要になる。そのため、運用担当者の業務を分析し、また、利用者からの意見を取りまとめることで、業務プロセスとシステムの改修を継続的に行っていく仕組みが肝要であると考えており、今後も実践していきたい。

参考文献

- [1] 平野靖, et al, “UPKI イニシアティブ「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」と名古屋大学における事例”, 名古屋大学情報連携基盤センターニュース, 2007 年 11 月, P379–P391
- [2] 川田良文, et al, “名大における UPKI 証明書の利用”, 平成 19 年 第 3 回 名古屋大学技術研修会報告, 2008 年 3 月
- [3] 宇田川暢, “UPKI サーバ証明書管理用ツールの開発”, 大学 ICT 推進協議会 2019 年度年次大会論文集, 2019 年 12 月, P335 – P336