NII サーバ証明書プロジェクトの総括

水元 明法[1)], 末永 光弘[1)], 中村 素典[1)]

1) 国立情報学研究所 学術基盤推進部

mizumoto@nii.ac.jp

概要：国立情報学研究所では、平成 19 年 4 月より「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」を開始し，平成 21 年より「UPKI オープンドメイン証明書自動発行検証プロジェクト」を経て平成 27 年 6 月まで実施した。本稿では二つのプロジェクトの総括を行う。

1 はじめに

国立情報学研究所(以下 NII)では学術情報ネットワーク運営連携本部認証作業部会において、平成 17 年度より全国大学共同電子認証基盤(UPKI: University Public Key Infrastructure)の構築を進めてきた。その活動は以下の 6 つである。

1) UPKI 共通仕様の制定
2) 外部向けサーバの証明書発行サービス
3) 大学間無線 LAN ローミング
4) 情報基盤センター及び NII コンテンツサービスの SSO 検討
5) CSI 向け認証局仕様版の作成と配付
6) S/MIME 証明書の試験運用

本稿では、このうち「外部向けサーバの証明書発行サービス」として実施されたサーバ証明書プロジェクトについて、総括と成果報告を行う。

2 サーバ証明書プロジェクトの経緯

2.1 第一期プロジェクト

UPKI における活動の一つとして、大学におけるサーバ証明書の普及推進と証明書発行プロセスの研究を行うことを目的に、平成 19 年度から平成 20 年度にかけて「サーバ証明書の発行・導入における啓発・評価研究プロジェクト」(第一期プロジェクト) を実施した。後述する第二期プロジェクトへの移行に伴い、第一期プロジェクトは平成 21 年 9 月末まで認証局の運用を延長した。第一期プロジェクトでは、合計 97 機関に対して、述べ 2,413 枚のサーバ証明書を発行し、サーバ証明書の発行・導入における啓発に関しては、一定の成果を得ることができたと考える。

また、サーバ証明書発行に必要な機関審査や発行審査を全て商用認証局が行うのではなく、NII や加入機関が分担する証明書発行フロー「学術スキーム」[1]の実装と検証を行い、これが実用的であることが確認された。それと同時に、持続的なサービスとするためには、NII や加入機関における業務の効率化などの改善すべき点が明らかになった。

2.2 第二期プロジェクト

プロジェクト参加機関からの継続を求める意見が多かったことから、平成 21 年度から平成 23 年度には「UPKI オープンドメイン証明書自動発行検証プロジェクト」(第二期プロジェクト) を実施してサーバ証明書発行プロジェクトを継続した。

第二期プロジェクトでは、合計 276 機関に対して、延べ 9,561 枚のサーバ証明書を発行した。プロジェクト参加機関の増加を実現すると共に、第一期プロジェクト事務局としてサーバ証明書の登録発行業務を運用してきた結果をもとに、証明書発行の効率化を進めることを目的としてプロジェクトで開発した「電子証明書自動発行支援システム」[2]での自動化による業務の効率化をはかることができた。

2.3 第二期プロジェクトの延長

平成 24 年度からは第二期プロジェクトを平成 27 年 6 月まで延長し(第二期プロジェクト延長)、プロジェクト終了時点で 337 機関 360 ドメインに対し、延べ 23734 枚の証明書を発行した。

2.4 証明書発行枚数の推移

プロジェクトで発行した証明書の発行枚数は Figure.1 のとおり右上がりに推移しており、有効な証明書の枚数としては 11200 枚程度に達した。

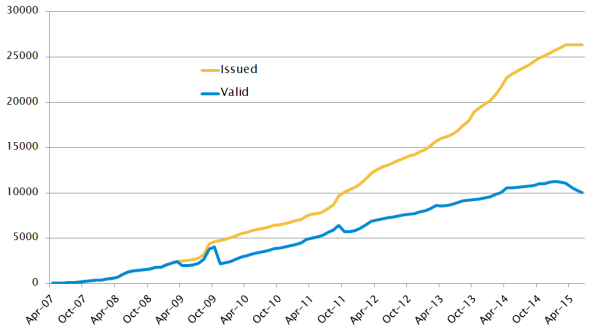

Figure.1 サーバ証明書のべ発行数と有効数の推移

3 発行した証明書

サーバ証明書プロジェクトでは、実施期間を通じて、大学等の高等教育・研究機関が持つ主たるドメインを対象とし、OV 証明書(Organization Validation: 対象の組織の法的実在性を確認した上で発行される証明書)を無償での発行を実施した。

第一期プロジェクトで発行した証明書は、有効期限を当初は 2009 年 3 月 31 日まで、後に 2010 年 6 月 30 日までと変更し[3]、鍵長 1024bit 以上、署名アルゴリズムは SHA1 with RSA Encryption であった。第二期プロジェクトで発行した証明書は、有効期限を発行から 25 ヶ月間とし、鍵長 1024bit 以上、署名アルゴリズムは SHA1 with RSA Encryption であった。ただし第二期プロジェクト延長期間において、鍵長を 2048bit とすることが決まり、CP が改訂[4]されている。

4 成果

プロジェクトの目的として、「1. 大学におけるサーバ証明書の普及啓蒙」「2. 学術スキームを実現するための証明書発行プロセスの実装・検証・システム化」があげられる。

プロジェクト参加機関を対象とし、プロジェクト終了後に実施したアンケート（以下 2015 年アンケート）において、プロジェクト参加の理由について質問したところ、9 割以上の機関で「サーバ証明書が無償で発行されるため」との回答を得ている。さらに「機関のサーバ証明書不足を解決したかったため」(約 35%)、「(学内認証局や独自認証局など)プライベート証明書をパブリックな証明書に切り換えたかったため」（約 30%）と続いている。コスト面で折り合いがつかずに証明書が不足していた状況、自己署名証明書を使わざるを得なかった状況を、プロジェクトに参加することで解消できるといった期待があったととらえることができる。

「UPKI プロジェクト参加後の機関内におけるサーバ証明書の使用数の増減をお答えください。」という設問の回答では 7 割以上の機関で証明書利用数が増えたとの回答があり、最初にコスト面での障壁を取り除くことで利用の後押しがなされ、機関での証明書利用数も増加していったと考えられる。

また、学術スキームを実現するための証明書発行プロセスの実装・検証・システム化については、十分な成果が得られたものと考えている。先述の通り、第二期プロジェクト（延長まで含む）での証明書発行数は 23734 枚に達したが、この申請を商用認証局のスキームを用いた場合、プロジェクト事務局のみで処理するのは困難である。学術スキームを導入したことによる実在性・本人性確認の手順を一部各機関に委任する確認実施フローと、電子証明書自動発行支援システムによる効率化で、プロジェクト参加機関は迅速に証明書を発行することが可能になった。これは、2015 年アンケートの自由記述においても読み取ることができており、プロジェクト参加機関も実感しているところである。学術スキームについては、NII が 2015 年より実施している UPKI 電子証明書発行サービス（サーバ証明書プロジェクトの後継事業としての性質を持つ）でも引き継がれ、電子証明書自動発行支援システムとあわせてサービス運営の効率化に貢献していることを付け加えておく。

調査の回答と、のべ 23734 枚に上る証明書の

発行数をあわせて考えると、プロジェクトの目的は達成され、成果をあげたと言える。

すでに各機関での予算面での削減効果については述べたが、プロジェクトによって全体でも大きな費用削減効果があったことを、加えて成果としてあげたい。第二期プロジェクトを例として費用の削減効果を試算する。第二期プロジェクトにおける合計委託経費は、およそ 4000 万円程度であった。この間に、のべ 9,561 枚のサーバ証明書を発行している。プロジェクトで発行する証明書と等価である、セコムパスポート for Web SR2.0 を購入するための経費は、年額 57,750 円である。単純にこの価格で有効期間 2 年の証明書を 9,561 枚購入した場合の経費（直接購入経費）は、1,104,295,500 円となる。ただしセコムトラストシステムズにおいても、複数枚一括購入による価格が設定されている。30 枚以上を購入する場合は、一枚当たりの価格が 30,000 円となる。この価格で有効期間 2 年の証明書を 9,561 枚購入した場合の経費は、573,660,000 円である。これと年額 57,750 円の場合の差額、すなわち、530,635,500 円がバルク契約により削減できる経費となる。したがって、直接購入経費から、本プロジェクトの委託経費とバルク契約による削減経費を差し引いた、537,435,000 円がサーバ証明書プロジェクトに参加し、学術スキームを導入したことによる経費削減を意味する。

上記は第二期プロジェクト 3 年間における経費から試算したものであるため、1 年間の経費削減効果は、約 1.8 億円となる。学術スキームでは、通常は商用認証局が実施していた作業を NII やプロジェクト参加機関が分担することになる。実際に削減された費用を算出するためには、プロジェクト全体での業務委託契約費だけでなく、NII における人件費等を部分的に加味する必要がある。また、本プロジェクトでは、無償でサーバ証明書を発行するものであるため、有償の場合と単純には比較できないという側面もある。しかしながら、そうした要素を考慮したとしても、学術スキームの導入による費用削減の効果は十分にあったものと考えられる。

5 後継事業の検討

大学では、サーバ証明書プロジェクトで発行したサーバ証明書を利用したサービスが多く運用されてきた。大学サービスのセキュリティや信頼性を担保するインフラの一部として、サーバ証明書の利用が定着化している現状にある。普及啓蒙、証明書発行の検証や効率化のフェーズを経た現在、大学からはサービスの継続的な運用が強く望まれていた。こうした現状は、大学サービスのトラストアンカーとして NII が実質的に機能していることを意味する。また、学術スキームを信頼性高く、かつ、効率よく運用していく上では NII の存在は不可欠である。ドメインと機関の関係を保証し，大学サービスの信頼性の礎となる証明書発行サービスを NII が提供していくことには大きな意義がある。

NII では 2013 年に、後継事業の検討のため、プロジェクト参加機関にアンケート調査を行った。その結果によると、まずサーバ証明書プロジェクトを有料化した場合の料金に関する問いに対し、サーバ証明書一枚ごとに対しては数千円から数万円程度、機関定額制の料金に対しては数万円から数十万円程度支払ってでも、継続的な利用を希望するとの回答が得られている。

また、サービス拡充のために、他の種類の証明書利用状況についても質問した。既にクライアント証明書を利用している大学は 41 機関あり、主にネットワーク認証などに利用している。そのうち、10 機関は商用認証局から購入し、31 機関はクライアント証明書発行のためのサーバ（CA）を独自に運用して、証明書を管理している。クライアント証明書を NII が提供するのであれば乗り換えたいとの回答を 40 機関から得ており、さらにコード署名用証明書についても 59 機関から NII のサービスから購入したいとの調査結果を得ている。

後継事業である UPKI 電子証明書発行サービスにおいては、プロジェクトの成果とアンケー

ト調査の結果を踏まえ、サーバ証明書・クライアント証明書（S/MIME 含む）・コード署名用証明書の 3 種を有償で発行している。とくにサーバ証明書においては、発行対象のドメイン数でサーバ証明書プロジェクトを上回るなど、さらなる成果をあげつつある。

6 おわりに

本稿では NII が実施したサーバ証明書プロジェクトの経緯と発行枚数から全体を俯瞰し、成果としてサーバ証明書の普及・啓蒙、および学術スキームの実現とシステム化による発行業務の効率化と費用削減効果について述べた。その成果は後継事業にも引き継がれ、電子証明書のさらなる普及と効率的な発行業務を行っている。

後継事業に移行した機関の数は、有償化したにもかかわらず 9 割に達し、これだけでも、大学等における、NII が提供するサーバ証明書利用の定着を物語っている。プロジェクトに参加いただいた 337 機関の協力に感謝を述べ、プロジェクト成果報告のまとめとする。

参考文献

[1] 島岡政基，西村健，古村隆明，中村素典，佐藤周行，岡部寿男，曽根原登、学術機関のためのサーバ証明書発行フレームワーク、電子情報通信学会論文誌、B95、7、817-882、2012.

[2] 島岡政基、西村健、中村素典、曽根原登、岡部寿男、UPKI サーバ証明書プロジェクトにおける証明書自動発行支援システムの開発、電子情報通信学会技術研究報告、109、438、229-234、2010.

[3] 国立情報学研究所オープンドメイン認証局証明書ポリシ 第 3.10 版 2008 年 3 月 28 日改版、https://upki-portal.nii.ac.jp/docs/webfm_send/50、2008.

[4] 国立情報学研究所オープンドメイン認証局 2 証明書ポリシ 第 1.20 版 2013 年 10 月 1 日改版、https://repo1.secomtrust.net/sppca/nii/odca2/NIIODCA2-CP-V1.pdf、2013.