

総合システムについて

～ 学認対応への流れと証明書発行の状況 ～

後藤田 中
N.Gotoda

(香川大学総合情報センター)

1. 全国的な統合システムの推進

大学や関連機関の連携を推進する UPKI (全国共同電子認証基盤) が進められている。その大きな柱は、まず、NII(国立情報学研究所)によるオープンドメイン認証局の設置、それに基づく、サーバ証明書等の発行・配布である。また、一方で SSO(シングルサインオン)技術を利用した学認(学術認証連携)も全国的に進められている。これらの流れは、学内外に拘らない全国・世界的な情報発信・サービス共有を目的とした一つの統合(認証)システムを目指す形となっている。本学における、この統合システムの状況について報告するとともに、今後の課題などについても検討を行う。

2. SSO について

学認における SSO は、SAML(Security Assertion Markup Language)2.0 に基づく Shibboleth 認証によって実現されている。本学の学認への対応状況としては、調査の段階であるが、Shibboleth 認証による四国地区の連携大学とのフェデレーション(認証連携)自体は、既に本学へ導入されている。本学に設置されている大学連携 e-Learning 教育支援センター四国⁽¹⁾では、大学教育の共同実施の調整に基づき、連携大学向けに e-Learning による科目提供を行っている。同授業で利用する LMS(Learning Management System)の Moodle では、各連携大学が同様に設置している LMS とフェデレーションを行うことで、各大学が提供する科目のコンテンツ(収録映像ファイル等)へのアクセス性を高めている。具体的には、同一アカウントで、各大学の Moodle にログインでき、個別にアカウントを発行する必要がない。

受講者のアカウントである ID や Password は、受講者が所属する各大学に分散しているため、DS(Discovery Service)のリダイレクトを通じて、同情報の窓口である IdP(Identity Provider)から LDAP で参照される。IdP における認証を通じて、SP(Service Provider)である Moodle へアクセス可能になる。

本学では、平成 28 年度に進められる教育システムのリプレースと合わせて学認対応を予定している。今後の対応準備として、テストフェデレーションの申請、仮アカウントによる検証を経て、運用フェデレーションの申請対応を行う予定である。

3. UPKI 証明書発行サービスについて

SSO 可能な SP 用のサーバを含め、学内から発信・配布されるあらゆる情報の信頼性を高めるため、証明書の存在は欠かせない。近年では、フィッシングサイトのように正規のサイトを模倣して情報を抜き出そうとする手口もあり、正規サイトのドメインや管理者の実在性を証明書で確認できることは重要である。従来、ベリサインやグローバルサインといった商用由来の認証局から証明書を取得する場合、高額な費用を申請者が個別に負担する必要があった。このため、学内でサーバ証明書が設置される Web サイトは、ごく少数の主要な部分に限られ、多く存在する研究室等のサイトでは、費用の面からも設置が難しくなっていた。そこで本学では、NII による UPKI 発行サービスを利用することで、従来と比較し、証明書の取得数に関係なく、コスト的に安価(一定)な形で証明書の取得が可能となった。

3.1. 証明書自動発行プロジェクトでの発行状況

本学は、UPKI 発行サービスに先行し、オープンドメイン証明書自動発行プロジェクト⁽²⁾に参加した。対象ドメインは、「kagawa-u.ac.jp」である。2009 年 7 月から 2014 年 12 月までの約 5 年半、52 件の証明書の申請・発行が行われた(表 1)。うち証明書の更新等、FQDN(Fully Qualified Domain Name)の重複を除くと 31 件であり、学内では同件数のサーバで証明書を設置したことになる。なお、同プロジェクトは、2015 年 6 月末に終了し、同時に証明書も失効するが、既に本学では、後述する次期サービスに移行している。このため、2015 年 1 月以降の本学での発行証明書は、この影響を受けず、SHA-2 プロファイルの場合、25 ヶ月有効であ

る。

表 1 2009 年～2014 年の UPKI 証明書発行状況

	発行件数
2009 年	7 件
2010 年	2 件
2011 年	7 件
2012 年	12 件
2013 年	11 件
2014 年	13 件
発行総計	52 件

3.2. UPKI 証明書発行サービスでの発行状況

先行する UPKI オープンドメイン証明書自動発行プロジェクトでは、無償利用であったが、新しいサービス⁽³⁾では、有償である。従来同様、契約はドメインごとに必要であり、追加のドメインを申し込む場合は、別料金が発生する。ただし、ドメインが同一であれば、任意の FQDN で追加料金なしに発行が可能となっている。同サービスの利用料は、CiNii(NII 学術情報ナビゲータ)⁽⁴⁾と同じく学内構成員(常勤の教員・研究者)の規模に基づいており、香川大学は、2015 年 6 月現在で、約 600 人であり、6 万円/年の契約に該当する(2015 年 6 月にサービス利用料の請求が行われている)。2014 年 12 月に同サービスの第 1 回の申込みを行い、表 2 に示す通り、1 月下旬より、順次新しい証明書が発行なされ、年度末時点で総計 13 件の発行となっている。全てサーバ証明書の発行であるが、コード署名証明書、クライアント証明書の発行にも対応している。

表 2 2015 年 1～3 月期の UPKI 証明書発行状況

	発行件数
2015 年 1 月	4 件
2015 年 2 月	2 件
2015 年 3 月	7 件
発行総計	13 件

4. 証明書発行に関する課題と検討

4.1. 申請者の準備に関する負担

現在、例えばサーバ証明書を申請する場合、対象サーバのドメイン名から、鍵の暗号方式等の指定まで申請者が行う。これらをプロファイルとした TSV ファイルを、文字エンコーディングや文字種も含め厳格なフォーマットで直接記述し、申請

前に用意する必要がある。この過程で、申請者は、事前に NII から提供される記述方法を熟読する必要がある一方で、作成した TSV ファイルが申請方式に沿っているかを確認する方法も熟知する必要がある。このため、申請者にとって、深い前提知識を必要とし、自ら全ての準備を行う必要があるため、申請手続きの入口までの敷居が非常に高くなっているのが現状である。さらに、コード署名証明書では、申請までの方法がより複雑である。NII から提供される網羅的な資料を、今後、申請者に分かり易い形で提供するかが、学内への普及課題である。

4.2. 証明書発行増に伴う受付担当者の負担

現在、学内での申請は、申請者と該当部局の受付担当者間でのメールのやりとりに基づいている。申請があった際、NII が提供するサイトにおいて、受付担当者が代行の発行手続きを行う。この手続きの中で、申請書の書式等を含めたエラーチェックがシステム的に行われる。仮に、エラーが発生した場合、TSV の修正依頼を再度申請者に行う必要がある。こうした対応を含め、今後証明書の発行申請(新規・更新)の増加に伴う、受付担当者の事務的負担が増える可能性がある。近い将来、この負担軽減が課題となる事が予想される。

4.3. 課題改善に関する検討

申請者への負担については、いくつかの事例に基づき、テンプレートのプロファイルを用意した上で、別途マニュアルを提供することで、負担減が可能と考えている。また、受付担当の負担減については、NII の証明書発行・配布の仕様に対応する CA アプライアンスの製品登場が待たれる。

5. まとめ

現在の本学の学認への対応状況とサーバ証明書の発行状況について報告した。今後、統合システム構築に向けて、引き続き、環境整備を推進する予定である。

参考文献

- (1) 知プラ e, 大学連携 e-Learning 教育支援センター四国, <http://chipla-e.itc.kagawa-u.ac.jp/> (アクセス日:2015 年 6 月 15 日)
- (2) UPKI イニシアチブ, NII, <https://upki-portal.nii.ac.jp/> (アクセス日:2015 年 6 月 15 日)
- (3) 電子証明書発行サービス, NII, <https://certs.nii>

ac.jp/ (アクセス日:2015年6月15日)

(4) CiNii, NII, <http://ci.nii.ac.jp/> (アクセス日:2015年6月15日)