名大における UPKI 証明書の利用

○川田良文、山田一成、瀬川午直

部局系技術支援室　研究所・センター技術系

はじめに

サーバ証明書はサーバが本物であることを証明したり、通信内容を暗号化したりするために必要な電子的な証明書で、セキュアな Web サーバや mail サーバを構築するために欠くことのできないものである。しかし、一般の証明書発行会社から購入する場合、サーバごとに年間３万～８万円程度の費用負担が発生し、そのためか大学内での普及が進んでいないように思われる。名古屋大学は、国立情報学研究所が昨年から開始している「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」の参加機関であるため、このプロジェクトの実施期間中(2007/04/01ー2009/03/31)は無料でサーバ証明書を取得することができるようになっている。本稿は、そのプロジェクトにより発行される証明書の取得方法や利用例について解説することにより、名古屋大学内でのサーバ証明書普及の一助となることをめざす。

1　UPKI「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」

国立情報学研究所と全国の大学・研究機関で推進する CSI(Cyber Science Infrastructure : 最先端学術情報基盤)事業の一つである UPKI(University Public Key Infrastructure : 全国大学共同電子認証基盤)は、大学が有する教育研究用計算機、電子コンテンツ、ネットワークを安全・安心に有効活用するための電子認証基盤の構築を目的としている。「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」は、UPKI のプロジェクトの一つで、次のような目的をもっている。

- 大学等のサーバ証明書の普及を推進
- 認証局を用いた研究開発
- 学術機関の Web サーバ信頼性向上
- サーバ証明書の導入・運用ノウハウの共有
- 参加者のサーバに対してのサーバ証明書無償配布

また、このプロジェクトで配布するサーバ証明書（以後、UPKI サーバ証明書）の発行対象となるサーバは、下記のすべての条件を満たす必要がある。

- プロジェクト参加機関が所有または管理するサーバであること
- 暗号化通信、あるいはサーバの実在証明を必要とするサーバであること
- 参加機関に割り当てられた DNS ドメイン以下の FQDN を持つサーバであること
- 参加機関に割り当てられた IP アドレスを持つサーバであること
- サーバの利用者が特定少数ではないこと

2　名古屋大学 UPKI サーバ証明書プロジェクト

名古屋大学では、情報連携統括本部が中心となって「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」に参加し、2007 年 7 月に「名古屋大学 UPKI サーバ証明書発行プロジェクト」を開始した。名古屋大学のプロジェクトでは、「加入者（サーバ証明書の発行を受けようとする人）が正規の教職員（名古屋大学の場合は助教・助手あるいは掛長以上）であること」、「サーバが適切に管理されていること」、「サーバが実在すること」を国立情報学研究所のプロジェクトに代わって審査することをもとめられている。また、サーバが発行対象となる条件を満たしているかどうかも確認しなければならない。これら多数の項目を審査するにあたって手続きを円滑に進めるため、名古屋大学では「サーバ証明書発行申請及び管理アプリケーション」を情報連携統括本部が管理する Web サーバ上に設置している。名古屋大学内で UPKI サーバ証明書を取得したい管理者は、このアプリケーションを用いて発行申請を行わなければならない。また、証明書が不要となった場合などの失効申請や、取得した証明書一覧の確認を行うこともできるようになっている。アプリケーションのトップページを図１．に示す。URL は https://app.icts.nagoya-u.ac.jp/csi_server_cert/ である。

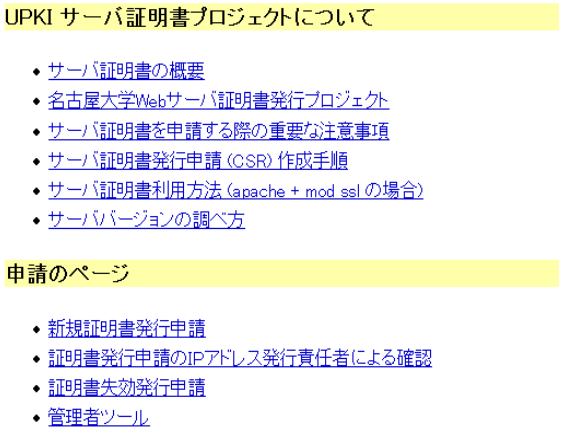

図１．アプリケーションのトップページ

2.1　証明書発行申請

発行申請の流れは次のようになっている。

- 図１で「新規証明書発行申請」をクリックする。このあとログイン画面があらわれるので、名古屋大学 ID または全学 ID を使用してログインを行う。
- 図２の「サーバ証明書発行申請」画面で、あらかじめ作成しておいた CSR（Certificate Signing Request: 証明書発行要求）などの情報を入力し、「利用規約に同意して申請する」ボタンを押す。この時、ログインした ID の資格審査や CSR などの内容確認が行われ、不備がある場合は「エラー」となる。審査を通過すれば申請を受け付けた旨のメッセージが表示されて、申請者の作業は終了となる。
- 申請が受け付けられるとアプリケーションから以下の 3 通のメールが発信される。
  1) 申請者宛に「発行申請を受理」した旨のメール
  2) 該当する IP アドレス管理責任者宛に「サーバが適切に管理されているかどうか」を問い合わせるメール
  3) 登録担当者（情報連携統括本部職員）宛に「申請があった」ことを通知するメール

図２．サーバ証明書発行申請画面

- 前項 2)のメールを受け取った IP アドレス管理責任者が、メールの内容にしたがってアプリケーションにログインし、該当サーバが「適切に管理されているかどうか」を報告する。
- 適切に管理されていると報告された場合は、アプリケーションから以下のメールが発信される。
  1) 申請者宛に「管理状況が確認できた」旨のメール
  2) 該当する IP アドレス管理責任者宛に「サーバの管理状況が確認された」旨のメール
  3) 登録担当者宛に「管理状況が確認できたので、国立情報学研究所に発行申請を行う」よう要請するメール
- 登録担当者が国立情報学研究所に発行申請を行う。発行されたサーバ証明書は国立情報学研究所から申請者に直接メールで送付される。

2.2 証明書失効申請

秘密鍵の漏洩や破損などの理由で証明書を取り替える必要が生じた場合や、サーバの廃止などで証明書が不要になった場合などに、証明書失効申請を行う。図３が証明書失効申請画面である。ここでは自分が取得したサーバ証明書の一覧を確認することもできる。

図３．サーバ証明書失効申請画面

3 UPKI サーバ証明書の利用環境

3.1 推奨環境

UPKI サーバ証明書は下記のサーバ、およびブラウザで適切に認識されることが確認されている。動作が確認され、プロジェクトのサポート対象となっているサーバソフトは Web サーバだけであるが、名古屋大学での動作実績として postfix、cyrus、courier-IMAP でも問題なく利用できている。

- 推奨サーバ

  Apache (mod_ssl)

  Apache-SSL

  Microsoft IIS5.0 IIS6.0

  IBM HTTPServer6.0.2 以上

  JakartaTomcat

・ 推奨ブラウザ

Netscape Communicator 4.78 以上

Netscape Communicator 7 以上

Microsoft IE 5.5 以上

Microsoft IE (MacOS) 5.2 以上

Opera 7.6 以上

Firefox 1.0 以上

Safari 1.2.2 以上

通常、サーバ証明書が正しいものであるとブラウザが判断するためには、ルート認証局証明書がそのブラウザのルート認証局証明書リストに格納されている必要がある。UPKI サーバ証明書の階層は図 4 のようになっており、最上位の認証局証明書（ルート認証局証明書）は Builin Object Token ValiCert Class 1 VA である。上記推奨ブラウザは、このルート証明書をリストに格納していることが確認されている。逆に、このルート認証局証明書をもっていないブラウザ（携帯電話ブラウザの多く）では、UPKI サーバ証明書は正しいものと認識できない。そのため、UPKI サーバ証明書は携帯電話を対象とするサービスには適していないことになる。

図 4． 証明書の階層

3.2 名古屋大学での導入例

2008 年 3 月末現在で 39 件の UPKI サーバ証明書が利用されている。下記に主なものを列挙する。

・ 名古屋大学 Web ページ
・ 情報連携基盤センターWeb ページ
・ IP アドレス管理システム https://ipdb.nagoya-u.ac.jp/ipdb/
・ 統合サーバ（情報連携統括本部が運用するサーバで、各部局が個別に管理している Web サーバや Mail サーバなどを集約しようとするもの）
・ 全学メールサーバ

これらで利用しているサーバソフトは apache+mod_ssl、postfix、courier-IMAP、Cyrus である。

おわりに

国立情報学研究所が平成 18 年度に実施した「大学等における電子証明書の利用状況に関する実態調査」によると、SINET 加入機関全体で 2,300～3,500 台分のサーバ証明書が不足していると推定されるそうである。その理由としては最初に述べたように毎年発生する高額な費用負担の問題や、課長職以上といった管理職の対応が必要な手続きのわずらわしさ（厳格な運用のためにはいたしかたない面もある）などが考えられる。これに対し、UPKI サーバ証明書は現在のところ無料であり、手続きも Web とメール確認だけで事足りるので、導入のハードルはかなり低くなっていると思われる。また、2009 年 3 月末のプロジェクト終了後も正式運用として継続される方向で検討中とのことである。色々なサーバで利用してみていただきたい。

参考文献

[1] 平野靖、内藤久資　名古屋大学情報連携基盤センターニュース Vol.6No.4 p379-391 2007 年

[2] https://upki-portal.nii.ac.jp/

[3] https://upki-portal.nii.ac.jp/cerpj

[4] https://app.icts.nagoya-u.ac.jp/csi_server_cert/