[全国共同利用情報基盤センター研究開発論文集 No.29]より

東北大学におけるサーバ証明書発行の試行運用についての報告

澤田勝己* 曽根秀昭**
*東北大学 情報部情報基盤課ネットワーク係
**東北大学 情報シナジーセンター ネットワーク研究部

概要

国立情報学研究所(以下、NIIという)と 7 大学の情報基盤センターを中心とした学術情報ネットワーク運営・連携本部 認証作業部会(以下、認証作業部会という)ではIT、ICTを活用した科学技術・教育研究活動の支援と活性化を目指してCSI (Cyber Science Infrastructue: 最先端学術情報基盤)構築のため研究開発に取り組んでいる。このCSI構築においても安全・安心な基盤構築は重要であり急務である。そこで安全・安心なCSI構築のためにUPKI (University Public Key Infrastructure: 大学間連携のための全国共同電子認証基盤)構想を提案、その一環として「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」を開始、東北大学も参加することとなった。

本稿は、本学における「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」参加に伴うサーバ証明書の試行運用及び今後の検討課題について報告する。

1.はじめに

東北大学を騙るフィッシングサイト(*)が設置され教職員や学生が誤って情報を入力する事故を防ぐため、サーバ証明書を利用して間違いなく東北大学が運用するサーバであることを証明する必要がある。

その一方で、サーバ管理者、利用者双方のサーバ証明書に対する知識や理解が薄く、サーバ管理者が導入しない、導入しても利用者が確認しないといった普及の面での問題がある。

NII と国立 7 大学の情報基盤センターを中心とした認証作業部会では IT、ICT を活用した科学技術・教育研究活動の支援・活性化を目指した安全・安心な CSI 構築のために UPKI 構想を提案、その一環として「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」が開始され、東北大学も参加することとなった。

本文は、本学における「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」参加に伴う実際のサーバ証明書の申請業務とサーバへの導入作業等の試行運用及び今後の検討課題について報告する。

---

*フィッシングサイト

フィッシング詐欺は金融機関やオンラインストアの Web サイトに似せた偽の Web サイト(フィッシングサイト)のこと。これを構築して個人情報を入力させ、不正かつ違法に情報を詐取する手法をフィッシング詐欺という。

2.サーバ証明書

2.1 概要

サーバ証明書は、正確には SSL サーバ電子証明書という(図 1)。

一般的に、利用者がIDやパスワード、個人情報を入力するようなサービスを提供するサーバは利用者のコンピュータとサーバの通信をパケットキャプチャ等で盗み見されても情報が閲覧できないようSSL (Secure Socket Layer)で暗号化している。ただ、フィッシングサイトでも見た目を似せて暗号化してしまえば誤って情報を入力してしまう危険性がある。

そこでTTP (Trusted Third Party: 信頼できる第三者機関)にサーバとその管理機関の実在性(架空ではないということ) 、本人性(なりすましではないということ)を証明してもらい、その証を発行してもらい利用者に公開する。その証がサーバ証明書である。

このように信頼できる第三者機関に証明してもらう方式をPKI(Public Key Infrasttructure: 公開鍵基盤)といい、この方式ではTTPのことをCA (Certificate Authority: 認証局)という。

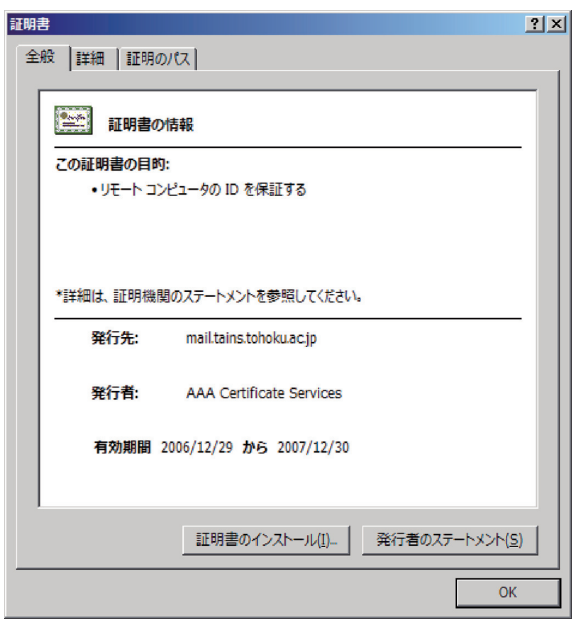

図 1: サーバ証明書

2.2 発行

サーバ証明書を発行してもらうためにはサーバでCSR (Certificate Signing Request: 証明書発行要求書)を生成する必要がある。CSRは秘密鍵とペアになる公開鍵情報を持っており、別の秘密鍵からの生成、同じ秘密鍵からの再生成でも同じCSRを生成することができないことで安全性・信頼性を高めている。そのため、秘密鍵の厳重な保管が重要である。

CSR を作成した後、機関の証明する書類(個人であれば戸籍謄本、運転免許証などの身分証明書、法人であれば法人格を証明する登記簿、印鑑証明など)を添付して CA に申請する。CA での審査が通るとようやくサーバ証明書が発行される。

しかしながら、CA によって求められる書類が異なっていたり、手続きや審査の厳しい緩い、手続きに要する時間や費用もばらつきがある。一見、手続きや審査が緩く短時間で安価に発行してもらえる方が良いように思えるが、サーバ証明書や CA 自体の信頼性も関係するため、一概に判断できるものではない。どの CA から発行してもらうかはサーバ証明書ひいてはそのサーバ証明書を利用してサーバ(サービス)を提供する機関の信頼性にも大きく影響する。

3.UPKI とサーバ証明書発行・導入における啓発・評価研究プロジェクト

3.1 UPKI

UPKI とは NII の認証作業部会にて安心・安全な CSI 構築のために提案された構想である。

技術としてのベースは前述の PKI 方式だが、その運用においては大学をはじめとする学術研究機関の組織体系や実情に即した、教育研究を念頭に置いた基盤構築を目的とする。

3.2 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

「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 の一環として NII の認証作業部会を中心に開始されたプロジェクトである。以下は文献[2] [3]から筆者が抜粋・要約したものである。

[目的]
(評価研究)
・大学等のサーバ証明書普及
・認証局を用いた研究開発→登録発行業務の改善
(啓発)
・学術機関の Web サーバの信頼性向上
・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の無償配布

[期間]
2007 年 4 月 1 日～2009 年 3 月 31 日

[背景]
大学におけるサーバ証明書導入が進んでおらずサーバの台数に対してサーバ証明書が不足していること、商用のサーバ証明書発行サービスと比較した場合に機関確認(審査)の方法が必ずしも適正ではないことを挙げている。

普及していないという点に関していえば、企業は情報漏洩がそのまま企業の利益や社会的信頼に大きく影響する危機感を持っているのに対して、大学は教育研究が主であり組織の本質が違うことも関係していると思われる。

また、機関確認については組織体系やシステムの運用ポリシーがトップダウン式に統制され組織責任が明確である企業と対して、それぞれの部局(研究科や学部、学科など)が水平展開している組織体系の大学では運用ポリシーに差異があり、責任区分が明確でない場合が多々ある。

[特徴・趣旨]
こうしたことを踏まえ、プロジェクトでは NII が WebTrust for CA 認定のルート認証局(セコムトラストシステムズ)の下位認証局として NII オープンドメイン認証局を構築、事務局を設置して参加機関へのサーバ証明書発行を通じてサーバ証明書の普及しない原因、普及させる上での課題を整理し、普及促進のための方策を検討する。さらに UPKI におけるキャンパス PKI 層の証明書発行業務の自動化を目指す。

参加機関である大学は機関内における機関責任者と登録担当者を置いて発行・変更・失効の各種申請業務、サブドメイン、部局、担当者等の実在性・本人性等の確認業務を試行的に行い、運用の問題点や課題を整理してプロジェクトにフィードバックする。

サーバ証明書発行の本人性確認、実在性確認を事務局、機関責任者、登録担当者に分担し、確認する人と項目を最適化することで、責任区分を明確にするとともに効率的に短時間で

の発行が可能となる。

[参加条件]
(参加対象)
SINET 加入の大学、短期大学、高等専門学校、大学共同利用機関、その他独立行政法人

(参加単位)
機関単位(部局単位は不可、機関内でとりまとめる)

(参加条件)
・プロジェクトの趣旨に賛同しフィードバックを行う
・機関内における確認作業、情報保管に責任を負う
・事務局への申請に際してデジタル署名を行う

[発行条件]
(対象サーバ)
参加機関または参加機関に属する部局が所有または管理しておりサーバ認証を必要とするサーバ

(対象ドメイン)
参加機関の主となる 1 ドメイン(東北大学は tohoku.ac.jp)

[責任を負う確認項目]

審査項目	審査者	プロジェクト			
		認証局	機関責任者	登録担当者	加入者
機関	本人性				
	実在性	○			
ドメイン	本人性		○		
	実在性	○			
機関責任者	本人性	○			
	実在性	○			
登録担当者	本人性	○			
	実在性		○		
加入者	本人性			○	
	実在性			○	
加入者サーバ	本人性				○
	実在性			○	

4. 東北大学における試行運用

プロジェクトの参加にあたって、本学における機関内確認をどのように行うかを検討した。これはプロジェクト参加申請書中の確認実施手順実査票として事務局に回答しなければならない。図 2 は本学における試行運用フローである。

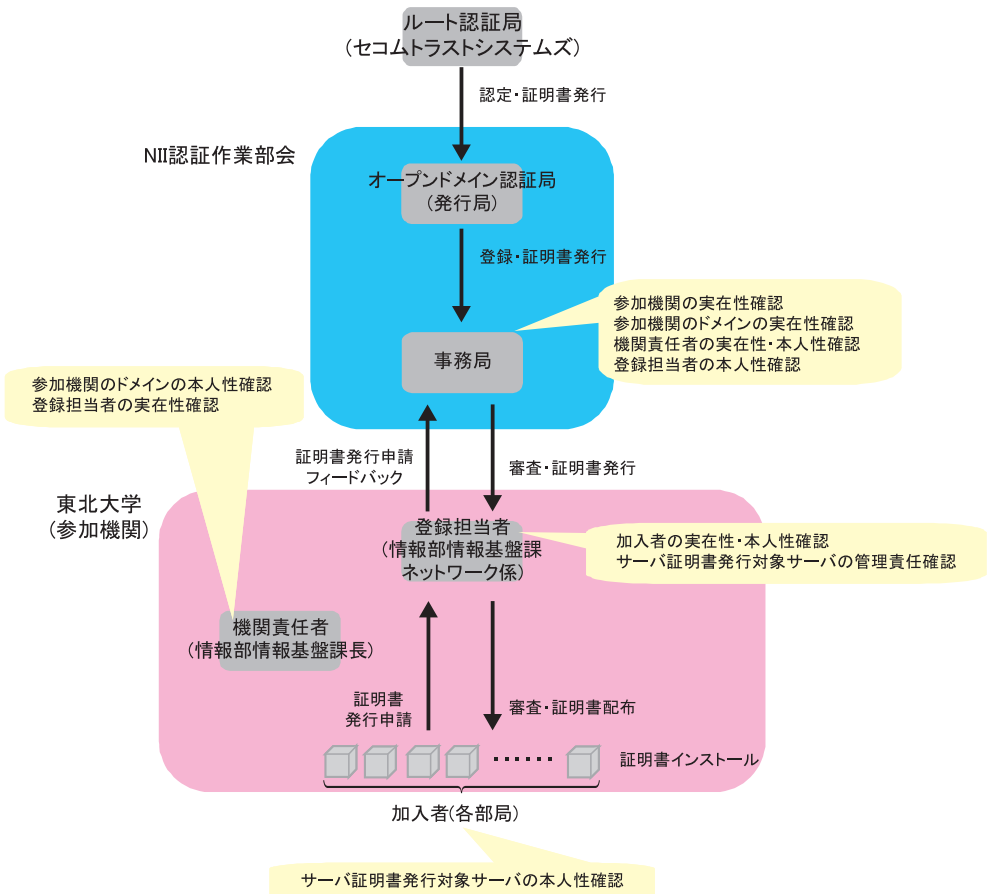

図 2: サーバ証明書発行フローと確認(責任)区分

(1)ドメイン

″tohoku.ac.jp″のドメインが本学の所有であることの確認は、JP ドメインを管理する日本レジストリサービス(JPRS)の Whois データベースを客観性のある情報として、登録されている登録担当者、技術連絡担当者に直接口頭で確認、承認を行うこととした。

″tohoku.ac.jp″の場合、登録担当者は機関責任者である情報基盤課長であり、技術連絡担当者は情報シナジーセンターの教授及び直属の上司であるネットワーク係長であったため対面・口頭で直接確認を行い、承認を得た。

(2)登録担当者の実在性・本人性の確認

本学における登録担当者は筆者(澤田)になっている。本人性確認は機関責任者は登録担当者である筆者の所属長であり面識があるため、対面・口頭で直接の確認を行い、指示を受けた。実在性の確認は人事部職員課が管理している職員録、座席表、内線番号表を客観性のある根拠とした。

(3)加入者の実在性・本人性の確認

実在性の確認は登録担当者と同じく人事部職員課管理の職員録、座席表、内線番号表を客観的根拠とした。本人性の確認は、申請が間違いなく本人の意志により本人が行ったものかの

確認である。申請書をメールでやりとりすることが前提のため S/MIME 証明書または添付する Microsoft Office ファイル等のデジタル署名が(事務局も推奨していることもあり)望ましいと考えた。しかしながら、部局数が多く担当者が異動等で変わることからその都度、すべての部局においてデジタル署名を施せるソフトウェアを利用しているとはいえないことを考慮して、まずは電話もしくは対面での確認のみとした。

また、サーバの設定や証明書導入等の実作業を本学教職員でなく、学生やベンダ担当者が行っている場合は、学生やベンダ担当者の実在性・本人性確認が発生し煩雑になるとともに責任の所在があいまいになるため申請は必ずその部局の本学教職員から行うこととした。

(4)サーバの管理責任の確認

主にCSRに記載されたFQDN (Fully Qualified Domain Name: 完全なドメイン名)の確認となる。サーバ証明におけるFQDNは、"https://"に続くドメイン名またはサブドメイン名 (ホスト名に相当する)の確認となる。

本学では"tohoku.ac.jp"のサブドメイン(例: "subdomain.tohoku.ac.jp")でサーバを設置する際は必ず筆者が所属するネットワーク係に利用・登録申請を義務付けている。申請を行わないと"tohoku.ac.jp"の DNS サーバに権限委譲の設定をしないため勝手に運用できない仕組みになっている。申請されたサブドメイン、DNS サーバ、管理者の情報は同係でデータベース化されている。

まず、サーバ証明書の発行が申請されている FQDN がデータベースに存在するかを確認する。存在していなければサブドメインの利用・登録申請を指示することとした。

次にサーバ証明書発行申請の部局、担当者がデータベースの部局、担当者と一致しているかを確認する。一致していなければ、まずはデータベースの担当者に確認及び承認を得ることとした。

確認はすべて人事部職員課管理の職員録、座席表、内線番号表を客観的根拠として連絡を行うこととした。

5.サーバ証明書の導入

5.1 CSR の生成

今回のプロジェクトにおけるサーバでの主な作業はサーバ証明書発行申請前の CSR の生成、サーバ証明書発行後のインストールの 2 つである。

まず、CSRの生成においては生成時に入力する識別(DN: Distinguished Name)情報はプロジェクトで指定されており誤りがあるとサーバ証明書を発行できない。

項目	設定内容
Country Name(C)	JP
State or Province Name(ST)	入力しない
Locality Name(L)	Academe
Organization Name(O)	参加機関名
Organizational Unit Name(OU)	部局名(省略可)
Common Name(CN)	サーバ名(FQDN)

表: プロジェクト指定の DN 情報

上記のうち、注意が必要な項目を説明する。OpenSSL で CSR を生成する際に"State or

Province Name(ST)"を省略する場合はピリオド"."を入力する。"Organization Name(O)"は、参加機関名であるが、申請したドメイン(xxx.ac.jp)の JPRS Whois に登録されている"g.[Organization}"の項目と一致しなければならない。本学"tohoku.ac.jp"は Whois では"g.[Organization}"は"Tohoku Universiry"と登録されているため、これを入力した。また、"Common Name(CN)"は実際に運用・公開する URL の中に用いる FQDN でなければならない。例えば、URL は"https://alias.tohoku.ac.jp/"なのに、CN を"realname.tohoku.ac.jp"としてサーバ証明書を取得、DNS サーバで"alias.tohokuac.jp"の CNAME を"realname.tohoku.ac.jp"に向けて設定したとしても"https://alias.tohoku.ac.jp/"では公開できずあくまで"https://realname.tohoku.ac.jp/"での公開しかできない。

5.2 サーバ証明書のインストール

インストールは対象となるサーバソフトウェアによってコマンドラインであったり、GUI であったりが異なるので、ここでは具体的な手順の説明は割愛する。

注意する点は、ルート CA から直接にサーバ証明書を取得している場合と異なり、ルート CA 下位の中間 CA から証明書を取得した場合である。

今回のプロジェクトで発行されるサーバ証明書もセコムトラストシステムズのルート CA 下位の NII オープンドメイン CA から発行されるため、NII のオープンドメイン CA は中間 CA にあたる。

この場合は、発行されたサーバ証明書と同時に発行した中間 CA(今回のプロジェクトでは NII のオープンドメイン CA)の証明書もインストールしなければならない。

証明書の認証はドメインの権限委譲と同じようにルートからの階層構造となっているため、途中で認証が途切れるとそこから下位の認証ができないためである。

6.今後の課題

6.1 機関内確認の手法

今回は諸般の事情を考慮して電話または対面による確認にとどめた。本来、認証作業部会では S/MIME 証明書やデジタル署名を用いた本人性確認を推奨しているが、先に述べた教職員の移り変わりやソフトウェアの問題もあり、全学的な実施は困難であると思われる。

他大学において申請プロセスを Web や IC カードを用いて自動化する試みも行われている。本学も将来的な全学認証基盤の構築を見据え、連携した申請システムの構築を検討したい。

6.2 サーバ証明書普及に向けた啓発

もっとも検討しなければならないのは、サーバ証明書とは何か、何故導入する必要があるのかといった知識や理解をどのように浸透させていくかということである。

手続きの最適化もさることながら、まずはサーバ証明書の重要性を広くアナウンスを行い、積極的に導入してもらうための説明やサポートを充実させていくことが先決である。

【参考文献】

[1]UPKI イニシアティブ: https://upki-portal.nii.ac.jp/
[2]サーバ証明書・導入における啓発・評価研究プロジェクト概要説明, 国立情報学研究所 学術情報ネットワーク運営・連携本部 認証作業部会
[3] サーバ証明書・導入における啓発・評価研究プロジェクト参加方法の説明, 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