社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DSM－48 (14)
2008－QAI－26 (14)
2008／3／7

東京大学におけるサーバ証明書発行体制の構築と課題

西村 健† 佐藤 周行‡

†‡東京大学情報基盤センター 〒113-8658 東京都文京区弥生 2-11-16
E-mail: †takeshi@itc.u-tokyo.ac.jp, ‡schuko@cc.u-tokyo.ac.jp

あらまし 東京大学のような総合大学においては、学部・研究科等の部局の独立性が高いこと、また部局内においても専攻等の下部組織の独立性が高い場合があることから、中央集権的な登録局を構築することは困難であるし、対応のための人員も不足する。そこで我々はサーバ証明書発行を例として、適切にドメイン管理体制を審査しつつ部局に権限を委譲する階層的な運用体制を構築した。この体制を紹介し課題を考察する。

キーワード PKI, EV SSL 証明書, 認証, 登録局

Construction of Registration Authority for Server Certificates in the University of Tokyo

Takeshi NISHIMURA† and Hiroyuki SATO‡

†‡Information Technology Center, the University of Tokyo 2-11-16 Yayoi, Bunkyo-ku, Tokyo, 113-8658 Japan
E-mail: †takeshi@itc.u-tokyo.ac.jp, ‡schuko@cc.u-tokyo.ac.jp

Abstract Large universities such as the University of Tokyo have several problems with graduate schools that are making decisions independently. Furthermore, some departments in a graduate school are even out of control of it in some cases. In such organization we have difficulties to manage one central registration authority in the point of view of information distributed and the cost.

We are currently managing distributed registration authority for server certificates, that delegates investigation role to the graduate school when possible. We will show the architecture of this registration authority and some consideration.

Keyword PKI, EV certificate, authenticate, registration authority

1. はじめに

今日我々は Web を通して数々の情報サービスを受けられるようになっている。Web は情報提供の場として重要度を増していくとともに、別の側面で特定のコミュニティにおける情報共有の場としても利用されてきている。多くの大学の Web ページが各学部からの広報の場として利用されている。その利便性から多くの情報が Web 上に掲載されるようになってきた。学部、学科など特定の単位のコミュニティの人々がこの Web によってつながりを持っている。

一方、Web においてやりとりする情報には機密性の高いものもあり、それらは通常 SSL (Secure Sockets Layer)/TLS (Transport Layer Security) プロトコルを通して暗号化される。これはクライアント（ブラウザ）とサーバとの間の暗号化であり、サーバの認証のためにサーバ証明書というデータが使用される。サーバ証明書は PKI (Public Key Infrastructure) という枠組みの上で認証局によって発行される証明書の一種であり、認証局はサーバの実在性や発行申請者の本人性など適切な審査ののちに、サーバのドメイン名とサーバ自身の持つ公開鍵をペアにしたものに認証局私有鍵によるデジタル署名を施されたサーバ証明書を発行する。ブラウザが認証局を信頼する、つまり認証

局公開鍵を持っているという前提の下で、サーバ証明書を用いることにより公開鍵暗号技術を用いた厳格な認証が行なうことができる。PKIにおいては発行される証明書は個人向けの個人証明書やサーバに対するサーバ証明書などの種類があるが、本論文では特にサーバ証明書を取り上げる。また、以下では認証局を、審査を行なう機関である登録局と発行を行なう機関である発行局に分けて論じる。

以上のように、サーバ証明書は認証局によってidentityを与えられたサーバに対する証明書であり、サービス利用者がアクセス先サーバを正しく認識していればフィッシング詐欺対策にもなりうる。つまり、認証局がサーバに与えた名称(DN, Distinguished Name)をサービス利用者が知っていればそれ以外の証明書を提示するサーバをフィッシングサイトであると判断することができる。しかし、上述の前提条件が不確かなことも多く、またブラウザ側のインターフェースも貧弱なためサーバ証明書単体でフィッシング詐欺対策として用いられることはほとんどない。

東京大学情報基盤センターPKIプロジェクトの取り組み[1,2]

東京大学は2004年に大学の教職員および学生の身分証としてICカードを採用し、認証基盤としてPKIを整備するという計画をプレスリリースとして出した。情報基盤センターはPKIを整備し、PKIアプリケーションの利用を促進し、PKI運用コストの最適化を検討し、東京大学および大学一般における最適な認証のフレームワークを開発するために「PKIプロジェクト」を発足させた。

PKIプロジェクトはすでに大学での運用に合わせたプライベートCAのプロトタイプを構築し、大学内の数部局と共同で実証実験を行なっている。一方でPKIアプリケーションの普及のため、既存のサーバ群と安全な認証を行なう上での問題に取り組んでいる。

PKIプロジェクトは同時に既存の商用のものも含めたサーバ証明書に対する利用者の理解を進める啓蒙・啓発の役割も担っており、またPKI運用コストの最適化の一環として、運用コストのうち大きな部分となる登録局の運用に関する知見を深めているところである。

国立情報学研究所のプロジェクトへの参画

一方で国立情報学研究所(NII)は、2007年に大学等の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することを目的として「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」[3](以下、NIIプロジェクトという)を開始した。ブラウザに信頼されていない認証局によるサーバ証明書は一般に検証が難しく、サービス利用者に検証を省略するように説明しているところも多い。もちろん検証の省略はフィッシング詐欺にもつながるもので決して容認されるものではない。上記プロジェクトは大学で運用されているこのようなサーバ証明書を一掃しサービス利用者側のリテラシー向上させることを目的の一つとしている。このため、セコムトラストシステムズというWebTrust for CA[4]認定の主要なブラウザから信頼される商用認証局をルート認証局とするサーバ証明書を、2009年3月までという期間限定ながら無償で配付している。

また、登録局はNIIにおいて運用されるが、参加大学に対して審査権限をほぼ全て委譲し、大学内での審査に任せているのが特徴である。

東京大学内でのサーバ証明書発行のための登録局の構築

我々PKIプロジェクトは、上記NIIプロジェクトが学内での登録局構築のテストケースになると考え、NIIプロジェクトに参加し東京大学内でのサーバ証明書発行の窓口となることにした。

第一に考慮すべきことはコスト削減である。前述のように学内で発行されるサーバ証明書に関するサーバおよび申請者の審査は大学に任されることになるが、他大学でも同様と思われるが新プロジェクトに専任で割ける人員もなく、PKIプロジェクト内の数人でまかなう必要があった。東京大学という規模のサーバ群を対象に我々が全ての審査を行なうのは非現実的であったため、大学内の各部局に部局内のサーバおよび申請者を審査する階層的な登録局を構築した。実際には部局内の審査の役を担うのは、既存の学内コンピュータネットワークの運用管理を行なう組織の部局担当者であり、部局側での追加の人員は必要とせず、また部局単位で審査等の負荷の分散を行なったため、合理的なコストで登録局を運用できるようになった

と考えている。

本論文の構成

本論文は以下のように構成される。次節で大学での登録局構築の問題点を整理し、第 3 節で我々が構築した登録局の解説を行なう。第 4 節で登録局運用によって明らかになってきた課題を考察する。第 5 節で本論文のまとめを行なう。

2. 大学において登録局を展開する場合の問題点

近年、Web における SSL/TLS の信頼性の崩壊が叫ばれている。これまで SSL のサイトであれば安全に利用できると考えられていたものが、そうではないと認識されるようになってきた、というものである。崩壊の過程には以下の 3 つの状態が考えられる。(ここで単に SSL サイトと書く場合、ブラウザから信頼された認証局が発行したサーバ証明書を持つサイトを指す)

1. SSL サイトは全て信頼できる
2. 一部のドメインの SSL サイトは信頼できない
3. 全てのドメインの SSL サイトは信頼できない

ここで、本来の SSL およびサーバ証明書の役割は実在性の証明であり、サイトが安全に利用できるか、信頼できるかとは無関係であることに注意が必要である。ともかく、2006 年に SSL を利用したフィッシングサイトが確認されて以降そのようなサイトは数百件に上るとも言われており、現在は 2.の状態にあると考えられる。つまり、ブラウザの脆弱性によるものを除けば、ネームサービスの改変を伴うファーミングや中間者攻撃(Man In The Middle attack)のような攻撃をもってしても、ドメインによる識別は可能であり信頼できないサイトは一部のドメインに限られる。

この原因はブラウザが認証局を信頼するかの判断基準になっている WebTrust for CA がドメイン認証のみを要求しているからであり、当然の帰結である。ドメイン認証とは、ドメインの所有権の確認のみを WHOIS 等によって行なう認証方式である。逆に SSL 利用のフィッシングサイトで被害が出ているということは、ドメイン名を確認しないサービス利用者が少なからずいるということを示していると考えられる。

本来認証局毎に審査項目や要求要件などをがあり、それらを元にした「保証レベル」がある。保証レベルによって認証局が分類され、利用者が保証レベルによって自由に選択できるのが PKI が想定する本来あるべき姿である。だが現状は WebTrust for CA のみが判断基準になってしまい、分類も大雑把には「パソコン」「それ以外 (携帯電話など)」程度の区分しか利用者には見えない。

これに対して、CA/Browser Forum[5]が推進する EV (Extended Validation) SSL 証明書が 2006 年後半より現われ始めた。従来のサーバ実在性の確認等に加えて法的実在性も確認するなど審査基準を厳格化したものが基準として定義されており、その基準を満たしたサーバにのみ EV SSL 証明書が発行される。従来のサーバ証明書の真部分集合であり、本来あるべき姿に沿ったものといえる。EV SSL 証明書を持つサイトは全て信頼できると謳っており、ブラウザではアドレスバー背景が緑色になるなどそれと分かる表示がなされる。

翻って大学におけるサーバ証明書の問題であるが、Web の歴史的経緯も含め、大学のサーバ管理は、特に研究室レベルのサーバの場合であれば、ルーズになされている場合が未だに存在する。例えば、教職員以上に知識を持つ学生が管理しているとか、研究目的のものを流用しているとか、助教・助手が仕事で手一杯なので学生が管理を手伝う、などである。特に管理者が学生の場合、何かあった場合の責任をとることができないので問題である。管理していた学生が卒業し管理者不在になったという話も聞く。

このような責任の所在が不明確で管理体制があやふやなサーバにまで証明書を発行していては、SSL の信頼性崩壊と同様、サーバ証明書の信頼性が崩壊してしまう可能性がある。そのようなサーバがサーバ証明書を必要とし申請を行うかという問題もあるが、今回の場合証明書を無償で発行するということもあり可能性は高いと考えられた。

加えて、東京大学のような総合大学においては、部局の独立性が高く、また部局内においても専攻等の下部組織の独立性が高い場合があることから、サーバの所属は部局単位もしくはより細かい単位であることが必要である。部局毎に意思が異なる、つまり独立の法人のような立場であるので、仮にあるサーバから情報が発信されるとして、その情報源のサーバの所属は○○大学とするよりも○○

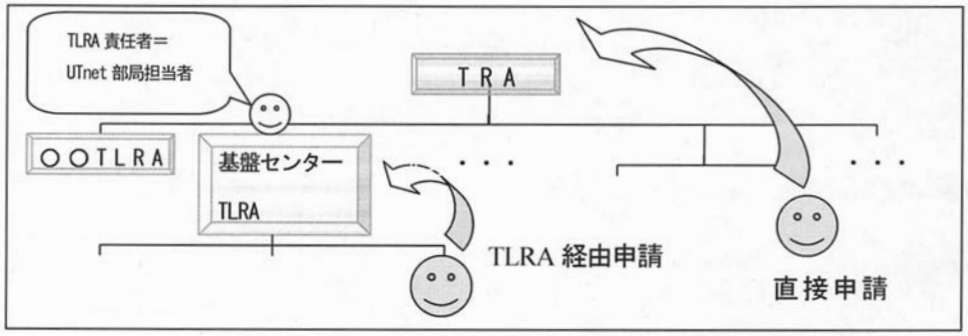

図 1 TRA と TLRA、および 2 種類の申請の方法

学部、さらには○○研究室とするほうが誤解が少ない。部局まで明示するということは、保証レベルを上げる、つまりより確かな保証を与えるサービスとなる。

またこれは大学に限らないが、先般のフィッシングサイトの事例にもあるようにブラウザでサーバ証明書を確認する手段が貧弱であると考える。利用者にとっては確認のために何度もクリックしなければならないのは手間で、しかも表示される情報は馴染みの薄い英語であったりする。より手軽で見やすい確認手段が求められている。

まとめると、大学における登録局は審査を厳しくしなければならず、また結果は分かりやすく提示しなければならない。

3. 東京大学における登録局構成

東京大学における登録局構成は以下の通りである。

まず、我々PKI プロジェクトが NII 側との窓口であり東大登録局(TRA)と呼ばれる。TRA は下記条件に合致しない証明書発行申請（直接申請）の審査も行なうが、条件が合えば一部の審査権限を部局単位の下位組織に委譲する。

部局単位の発行審査組織が東大部局登録局(TLRA)である。TLRA 責任者が TRA に設置申請を行ない、その承認をもって正式に設置される。実際の担当者は、UTnet という既存の学内コンピュータネットワークの管理組織における部局担当者が兼務するという形をとっており、新たに一から組織を作るよりも組織構築のコストは格段に低い。

TRA と TLRA の関係を図示したものが図1である。

審査は対面での確認を原則としており、証明書発行直接申請時および TLRA 設置申請時には、教職員による本人確認、および部局内でのドメイン管理体制を示した文書、TLRA 設置申請時には加えて申請者の本人確認方法を示した文書を提出してもらうことにより審査を行なう。

サーバ証明書発行については、NII 側で示されているとおり CSR (Certificate Signing Request)を提出してもらうが、ここで Organizational Unit Name (OU)に部局の英語名称を記載してもらい、審査の上で発行証明書に記載する形にしている。これによって発行された証明書をインストールしたサーバの利用者は、部局名を確認しより確かな保証を受けることができる。

3.1. 東大シール

我々は、ブラウザによる証明書確認手順の煩わしさを排し手軽で分かりやすいサーバの確認方法を提示するため、1 つの logo program として、「東大シール」なるサービスを提供している。
これはベリサインおよびセコムトラストシステムズ等でも行なわれているサービスであるが、本プロジェクトで発行した証明書をインストールしたサーバ上のページにシールと呼ばれる特定の画像（図 2）を掲載してもらう。これをクリックすると、そのサーバに対する検証結果ウィンドウが表

図 2 東大シール画像

図 3 サイト検証結果画面

示され、ドメイン名、所属部局、有効期限等が簡潔に表示される（図3）。シール画像および検証結果画面はシールサーバと呼ばれるサーバにて提供される。シールサーバは発行および失効したサーバ証明書一覧をデータベースにて保持しており、証明書の状態を適切に表示することができる。また、クリックされたシールのリンク元はHTTPのREFERERヘッダにより取得するため、偽装サイトによるなりすましを困難にしている。当然利用者は表示された検証画面のURLが正しくシールサーバのものであることを確認しなければならない。

ここでも部局名の日本語名称および英語名称を用意し、シールをクリックした利用者に部局名まで提示し間違いなく当該部局のものであるという確認手段を提供している。

4. 運用実績および課題

本プロジェクトは2007年3月にスタートし、現在5部局にTLRAが設置され、40数枚の発行実績がある。発行対象は実に様々で、実際に研究室レベルのサーバに対する証明書申請も来ている。システムとしてはTLRAの下に更に専攻登録局を設置することも可能であるが、現在のところ実際に設置された例はない。

TLRAの分散配置のためにUTnetという既存の組織を利用したが、必ずしもドメイン管理体制と一致しているわけではなく、この枠に収まらない組織からの申請が相談を含めて数件あった。また、同じくUTnetの枠に収まらない事例で、組織の活動停止や別組織への移行など流動的な部局が多くあることが明らかになってきた。前者は直接申請という形で、後者は証明書の失効・サーバ管理者の変更という形でダイレクトにTRAのコストとして現われてくる。今後も同様の事例は増えてくると思われるため、UTnetの枠にとらわれない、それらを統括する組織（例えば総長室）に対してTLRAを設置する用意が必要である。

将来的には、ドメイン管理も含めたシステムを我々が提供し、その一部としてサーバ証明書の発行を行うという形態も考えられる。ただ、歴史的に独立して運用していたという経緯もあり、各部局で管理方法はさまざまなので、各部局が納得する形で統一したインターフェースを提供しそれに移行するのは相当の時間を要すると思われる。

TLRA設置に際して種々の文書を要求しているが、このハードルが高いためTLRAが設置されずその分が直接申請されるというのは本意ではない。そのような事例が増えるようであれば、初めのうちはTRAが肩代わりする形で本来TLRAが行なう処理を代行し、次第に部局担当者へ権限を移すという方法が効果的だと考える。ただ、TLRAの代行は部局内の管理体制の事前調査が必要であり、それがTRAが支払うコストとして妥当なものである場合に限られる。

5. まとめ

我々PKIプロジェクトは、NIIが行なっているサーバ証明書を発行するプロジェクトに参加し、東京大学内でサーバ証明書を発行するための審査体制を構築した。部局の独立性を保ちつつ厳格な審査を低コストで行なうため、東大登録局(TRA)を上位登録局、東大部局登録局(TLRA)を下位登録局とする階層的な登録局を構築した。また証明書に部局名を記載しこれも保証することとした。我々が発行した保証レベルの高いサーバ証明書は東大シールによって手軽な方法で視覚化される。

今回はNIIのプロジェクトと連携しての活動だったが、ベリサインのマネージドPKIのように学内で登録局を持つ運用は今後増えていくと思われる。この場合、各部局との連携をうまく図ることがポイントになることは間違いない。今回得られた様々な知見を役立てることができるだろう。

文　献

[1] 西村　健, 佐藤　周行, “自律的組織の集合体としての大学における PKI の運用,” 情報処理学会全国大会 講演論文集(分冊 4), pp. 327-328, 2007 年 3 月

[2] 東京大学情報基盤センターPKI プロジェクト, http://www.pki.itc.u-tokyo.ac.jp/

[3] 国立情報学研究所, 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, https://upki-portal.nii.ac.jp/cerpj

[4] The American Institute of Certified Public Accountants, “WebTrust Program for Certification Authorities,” http://www.webtrust.org/

[5] CA/Browser Forum, “EV SSL Certificate Guidelines,” http://cabforum.org/