2008－IOT－2 (1)
2008／7／24

脅威モデルの構築をもとにしたサーバ証明書発行体制の分類とその評価手法の提案

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@satolab.itc.u-tokyo.ac.jp

あらまし 現在のインターネットの安心・安全な通信の基礎となっている公開鍵認証基盤(PKI)において証明書の発行体制・審査体制の構築は重要な位置を占める。本研究では実際に起こりうる脅威の分析をもとに、商用・非商用を問わず世にある認証局の証明書発行体制の分類を試み、それらに対する評価軸の提案を行なう。

キーワード PKI, EV SSL 証明書, 認証, 登録局

Threat Model Construction to Classify and Evaluate Registration Authorities for Server Certificates

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@satolab.itc.u-tokyo.ac.jp

Abstract Today, demand of secure communication is increasing as we access increasing number of various confidential information on the Web. Public Key Infrastructure (PKI) is the most important component for secure communication on the Web, and constructing a system to investigate a person who applies for obtaining a certificate, which is called "Registration Authority" (RA), is the most important part of PKI.

In this paper we try to classify existing RAs by analyzing imaginary threats. We present an axis to classify those RAs.

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。インターネットが社会の基盤として普及するのに合わせて Web は情報提供の場として重要度を増しているが、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が拡大している。大学においても、多くの大学の Web ページが各大学・各学部からの広報の場として利用されている。多くの情報が Web 上に掲載され利用者の利便性が向上している。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) [1, 2] 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扱う。

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。

本論文では、フィッシング詐欺対策およびなりすまし対策の観点から、登録局の審査体制の問題によって引き起こされる脅威を考察し、その脅威を基にした評価方法を提案する。

本論文の構成

本論文は以下のように構成される。次節でサーバ証明書について実際に起こりうる脅威を整理し、第3節でその脅威を基にした評価軸の検討を行なう。第4節で実際の運用例での評価を行う。第5節で関連研究に触れ、第6節で本論文のまとめを行なう。

2. サーバ証明書の要件と想定される脅威

サーバ証明書の主な役割は、公開鍵とそのサーバの運営者の識別子（企業名や組織名）を結びつけることである。ここではサーバ証明書に期待される要件と、サーバ証明書を発行・運用する場において実際に起こりうる脅威についてまとめる。

まずサーバ証明書が識別子としての機能を果たすためには、サーバ証明書を参照し利用する者(relying party)のレベルを想定し、その利用者が相手を正しく識別できる方法を提供している必要がある。例えば、利用者がドメイン名のみによって相手を識別できることを想定するのであれば、サーバ証明書にはドメイン名のみを表示すればよいことになる。しかし実状を鑑みるにこの想定には問題がある。つまり、内情をよく知るものでなければu-tokyo.ac.jpとtokyo-u.jpのどちらが「東京大学」のドメインであるかを判別できないであろう。

上記の考察より、以下では運営者を一般名称(企業名や組織名）により識別できる利用者を想定する。

以下では、時系列を「申請時および証明書発行時」とそれ以外に分け、それぞれについて想定される脅威を考察する。

2.1. 申請時および証明書発行時の脅威

まずサーバ証明書発行の手順はおおまかに以下のようになり、これにあてはまらない手順は通常ありえない。

1. [申請者→審査者] 申請者による申請書類（CSRを含む）の作成、申請
2. [審査者] 申請の審査、証明書の発行
3. [審査者→申請者] 発行された証明書の送付

この場面での主な脅威はなりすましである。なりすましには2通りあり、(a)権限を持たない申請者が偽って申請する場合と(b)通信路上で申請書類（特にCSR）を改竄する場合が考えられる。証明書発行後の手順における盗聴・なりすましは大きな脅威とはなりえない。

上記(a)(b)の場合共に手順の通りに証明書が発行されその証明書をなりすました者が取得できたとすると、その者は正しく検証されるHTTPSの偽装サイト（フィッシングサイト）を構築できてしまう。もちろんドメイン名が正規のものと同一であるため通常のルーティングでは偽装サイトに到達することはない。偽装サイトをフィッシングに悪用するためにはルーティングテーブルの改竄やDNS poisoning、ARP spoofing等の攻撃の併用が必要である。

ともかくこの脅威による被害は、偽装サイトによるID/パスワード、クレジットカード番号、その他の個人情報の窃盗が挙げられる。さらに、このようなことが起こったという事実から発行した認証局の信用が失墜するという被害は、認証局にとっては甚大である。

2.2. 通常運用時の脅威

サーバ証明書発行後からそのサーバ証明書を更新するまでの期間は、基本的に認証局が介入することはなく、運用はサーバ管理者（通常は証明書申請者と同一）に任される。この場合の主な脅威は、サーバ上の秘密鍵の漏洩・危殆化によって第三者が秘密鍵の情報を得ることである。2.1 の場合と同様、偽装サイトの構築が可能になり、偽装サイトを通して ID/パスワード等を窃盗される恐れがある。ただしこの場合認証局の信用が失墜するということは通常なく、サーバ管理者の責任問題に止まると思われる。

また別の脅威として、認証局がサーバ証明書発行後のサーバ運用体制の変更を把握しきれていないことに起因する問題もある。大きくはドメイン移管等によるドメイン管理主体の変更から、サーバ管理者の異動、サーバの移行等多くの場合において元サーバ管理者および元サーバによる不正の余地を残す。もちろんこれらはサーバ管理者側が適切に処理していれば問題とならないが、認証局がサーバの運用体制の適正さに依存している部分である。

3. 審査体制の評価軸

以上述べた脅威の考察を踏まえて、審査体制の脅威への対応度という意味で評価軸となりうる指標を列挙すると以下のようになる。

(a) **申請者の認証**
申請者を人として認証する場合、教職員証などで本人確認をすることを言う。また申請者が審査者の顔見知りであることを確認する場合や申請が Web による申請で ID/パスワード等でのアクセス制限がかけられている場合もこれに当たる。電子メールの到達性のみで申請者を確認する場合など、この項目を実施しない場合もある。

(b) **申請者の所属の確認**
(a)に加えて、申請 FQDN が表す組織に申請者が所属していることを確認することを言う。場合によっては教職員名簿等によりさらに細かい内部組織単位での所属の確認が行われることもある。また、申請 FQDN の管理主体がはっきりしている場合は、申請可能な者をその管理主体に限定することによって申請の正当性を個人レベルで確認することが可能である。

(c) **申請者ー審査者間の通信路の強度**
紙ベースで申請書の受け渡しを行う場合も含めて、申請者と審査者の間のやりとりに他者が介入できないことを保証する。紙ベースの場合の受け渡し手段として手渡し、郵便（学内便）等が考えられる。また電子的な通信手段としては SSL 暗号化通信（例えば HTTPS）や電子メールが考えられる。手渡し以外の場合にはすりかえ／改竄を 100%防止することは不可能であるが、封緘シール等ですりかえをより困難にすることは考えられる。
電子メールについては便利である反面 S/MIME 等の技術を併用しない場合は、差出人の偽装が容易、紛失の可能性がある、経路上での盗聴・改竄が容易、などの理由からその信頼性は他の手段より劣ると言わざるを得ない。

(d) **提供する保証レベル**
世の中で広く用いられている X.509 証明書 [4] では、証明書の内容として組織名を表す Organization Name (O)やその下の部署名を表す Organizational Unit Name (OU)が存在する。O や OU がそれぞれの名称として妥当なものであることを保証するのが保証レベルである。(b)とも関連して一般に OU レベルの保証を与えることは困難であるが、特に大学のような内部組織（部局）の独立性が高い組織では、それぞれの部局を識別することに意味があり、OU レベルの保証を与えることが望まれる。

(e) **定期検査**
発行申請時の審査のみでは、その後の異動等の状況変化に対応できない。場合によってはサーバ、サーバ管理者、ドメイン管理者に変化がないか定期的にチェックすることが有効である。

4. 実例を用いた審査体制の評価

4.1. 東京大学パブリックサーバ証明書発行プロジェクト [11]

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」[9]（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。NII 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、WebTrust for CA [10]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参加大学に対して配付している。

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。

東京大学はこの NII プロジェクトに参加している。東京大学における登録局構成は以下の通りである。[7]

まず、NII 側との窓口として東大登録局(TRA)と呼ばれる登録局がある。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。

審査は対面での確認を原則としており、外部監査等での証拠能力を重視して紙ベースの申請・承認を行なっている。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。

4.2. ドメイン認証のみの登録局

主なブラウザにルート認証局として登録されたいわゆるパブリックな証明書を発行できる認証局の中で最もシンプルそして最低限の審査体制としてドメイン認証のみを行うものがある。つまり WebTrust for CA の基準を満たす最低ラインである。ここでは例として StartCom Free [6]を取り上げるが、他のドメイン認証の登録局も審査体制としては違いはない。

審査は特定のメールアドレス（例えば webmaster@ドメイン名）へのメール到達性および返答によって行われる。すなわち申請者を人として認証することはなく、また組織名称(O)を保証することもない。第 2 節での議論によりこのような審査体制の下で発行された証明書は利用者がサイトを識別するのに十分な情報を持つとは言い難い。

4.3. EV SSL 証明書

一方 WebTrust for CA の審査基準をより厳密にしたものとして CA/Browser Forum [8]が推進する Extended Validation (EV) SSL 証明書がある。これは各認証局が最低限守るべき基準であり、EV SSL 証明書を発行する認証局はこの基準にのっとって運用している。

EV SSL 証明書は法人のみを対象としており、証明書中の Organization Name (O)にその法人の名称を記載されていることを保証しているところが特徴である。EV SSL 証明書では、申請法人が実在し確かに事業を行っていることの確認を主眼としており、その確認をもってフィッシング対策としている。すなわちその法人内の部署等については言及しない。

4.4. 名古屋大学 UPKI サーバ証明書発行プロジェクト [3]

東京大学と同様に NII プロジェクトに参加している大学は多くあり、その中で名古屋大学はオンラインでの申請および審査を行っている[3]。認証は全学で使われている ID でのシングルサインオン環境として実現されている。審査過程の多くが自動化されているため大変効率的である。

東京大学と同様、組織内での審査であるため

	東京大学	StartCom Free	EV SSL 証明書	名古屋大学
申請者認証	○	×	○ (法人のみ)	○
所属確認	○ (部局レベル)	×	○	○
通信路強度	学内便	メール	○	Web, メール
保証レベル	○(O,OU)	×	○(O)	○(O)
定期検査	対象 TLRA のみ	×	×	×

図 1: 各登録局の審査体制の比較

Organization Name (O)の記載の保証は行うが、下部組織（部局等）についての言及はない。審査過程においてネットワーク管理者への確認が電子メールによって行われるためメールの信頼性に依拠することになる。

4.5. 審査体制評価のまとめ

各登録局での審査体制の比較を図 1 に示す。

現状の EV でないサーバ証明書の審査には多くのものが抜けており、また EV SSL 証明書がそれをカバーするものであることが分かる。

また、NII プロジェクトで行われている審査体制のレベルはおおむね高いといえる。東京大学の登録局のみ、OU レベルの保証レベルを提供する。

5. 関連研究

フィッシングなど Web 上での詐欺行為に対して現状の SSL サーバ証明書および審査基準である WebTrust for CA では不十分であることが明らかになってきた。EV SSL 証明書の審査基準はそれを補完するものであり、法的存在性や事業継続性など厳密な審査が必要とされている。

PKI の審査体制に関する詳細な分析に関する研究は多くはないが、Naqvi ら[5]の論文では、Grid における認証その他の部分について脅威モデルを構築している。

6. まとめ

本論文では、フィッシング詐欺対策およびなりすまし対策の観点から、登録局の審査体制の問題に起因する脅威を考察し、その考察を基にして審査体制を評価するための評価軸を提案した。またその評価軸を基にいくつかの登録局の評価を行った。

現行の登録局ではサーバの運用体制は審査の対象外となっているが、サーバの運用体制に起因する脅威も少なくない。今後はサーバ運用体制に対する審査も含めた審査体制、およびその評価基準を考えていきたい。

文　献

[1] T. Dierks, C. Allen, "The TLS Protocol", RFC 2246, January 1999.

[2] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., November 1996.

[3] 平野靖, 内藤久資, "UPKI イニシアティブ「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」と名古屋大学における事例", 名古屋大学情報連携基盤センターニュース Vol. 6 No. 4, pp379-391, 2007 年 11 月.

[4] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile", RFC 2459, January 1999.

[5] S. Naqvi, M. Riguidel, "Threat Model for Grid Security Services," Lecture Notes in Computer Science 3470, pp. 1048-1055, 2005.

[6] E. Nigg, "StartCom Free SSL Certification Authority Policy & Practices," StartCom Ltd., December 2007.

[7] 西村健, 佐藤周行, "東京大学におけるサーバ証明書発行体制の構築と課題," 第 48 回分散システム／インターネット運用技術・第 26 回高品質インターネット合同研究発表会 (2008-DSM-48), pp79-84, 2008 年 3 月.

[8] CA/Browser Forum, "EV SSL Certificate Guidelines," http://cabforum.org/

[9] 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

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

[11] 東京大学情報基盤センターPKI プロジェクト, パブリックサーバ証明書発行東大登録局, http://www.pki.itc.u-tokyo.ac.jp/cerpj