

PKIをめぐる社会的動向

PKIについて、公開鍵暗号技術を利用した単一のシステムとして理解するのは簡単だ。しかし、幅広い用途を前提とすると、PKIの技術は複雑であり、多様性を持つことがわかる。本稿では、JNSAのPKI相互運用技術WGリーダを務めるセコム株式会社IS研究所の松本泰氏が、社会システムとしてのPKIという観点から、PKIについて再検討し、PKIの持つ多様性と社会との関わりについて解説する。

松本 泰
(Yasushi Matsumoto)

セコム株式会社
IS研究所



ハードウェアの設計、UNIX上でのビデオテックシステム、大規模パソコン通信システム、各種インターネットサービスなどの設計、開発、運用に従事した後、1998年よりセコムのサイバーセキュリティ事業の立ち上げなど情報セキュリティ分野に携わる。2001年よりNPO JNSAのPKI相互運用技術WGリーダ。

はじめに

PKIは、社会とのつながりが強い技術と言えます。IT技術が、社会に深く浸透すると共に、社会の基盤としてのIT技術が求められるようになってきました。そして、社会の基盤となりえるIT技術のひとつにPKIがあると言えます。

なぜ社会の基盤としてPKIがあるかということに関して、ひとつには公開鍵暗号技術の技術としての性格があります。一般論として公開鍵暗号技術は広く仕様をオープンにしてもセキュリティを保てる仕組みが可能だと言え、そのため幅広い標準化がなされている基盤技術としてのPKIがあります。

様々な社会的な要求からPKIの利用が進行していますが、PKIの技術は理解できても、こうした動向は分かりにくいところがあるかもしれません。PKI技術は、法制度まで含めた社会システムとして取り込まれる傾向がありますが、それが既存の法制度等との整合も求められることになり、これが大きな課題となっている面もあります。

PKIを理解する重要なキーワードに、信頼関係モデル

(Trust model)、信頼点 (Trust point) などがありますが、この「信頼」自体は、IT技術で実現できるものではありません。PKIの場合、信頼関係をマシンリーダブルな標準化された証明書で表しコンピュータによる自動処理を可能にします。この場合、社会において何が信頼できるかといったことは、既存の法制度等に大きく依存する訳です。

PKIの課題としてよくこの証明書のコスト等の話が語られます。PKIが使う公開鍵証明書は、いわば単なる電子データであり、この証明書の価値とそのコストは、純粋に技術面からだけの理解は難しいところがあります。証明書の本質的な価値は何らかのことを証明していることであり、そのコストも何らかのことを証明することにより発生するコストということになります。

この章では、「Webサーバ証明書」、「デバイスのPKI」、「電子署名と電子文書保存」、「公的分野のPKI」、「身分証明書などのICカード」の5つのトピックを取り上げます。これらのトピックから、PKIと社会システムとの関係、そしてPKIをめぐる社会的動向を説明します。

身近なPKIと電子署名に関する動向

「Webサーバ証明書」の動向

Webサーバ証明書は、その存在が広く認知されていて一番身近なPKIと言えます。しかし、その存在ほどには、本質的な存在理由はそれほど知られていないようにも見えます。とはいえ、この章の最初にWebサーバ証明書を取り上げるのは、身近なPKIであり理解しやすいということがあります。

Webサーバ証明書は、インターネットの成長と共に普及してきましたが、この証明書にも変化が見られます。一つはWebサーバ証明書の低価格化です。そして逆の方向へ向かうものとしてEV証明書があります。ここでは、このEV証明書と、高い信頼性と低コストのWebサーバ証明書の発行を両立させるための試みとして新たな証明書発行モデルであるUPKIの例を説明します。

Webサーバ証明書の国際標準WebTrust for CA

一般にWebサーバ証明書を認証事業者から購入する場合、発行される証明書の信頼点となるルート認証局 (の自己署名証明書) が、利用するWebブラウザの証明書ストアに予め信頼する認証局として登録されていることが、暗黙の前提になっていることと思います。主要なWebブラウザの証明書

ストアに予め信頼する認証局として登録されている認証局 (あるいはその下位認証局) のことを、ここではオープンドメイン認証局 (*1) と呼ぶことにします。

オープンドメイン認証局として登録されるための基準はWebブラウザによって様々ですが、多くの場合はWebTrust for CAという実質上の国際標準の認定を受けていることが求められます。つまりほとんどの商用のWebサーバ証明書は、WebTrust for CAという国際標準に則って発行された証明書であると言えます。

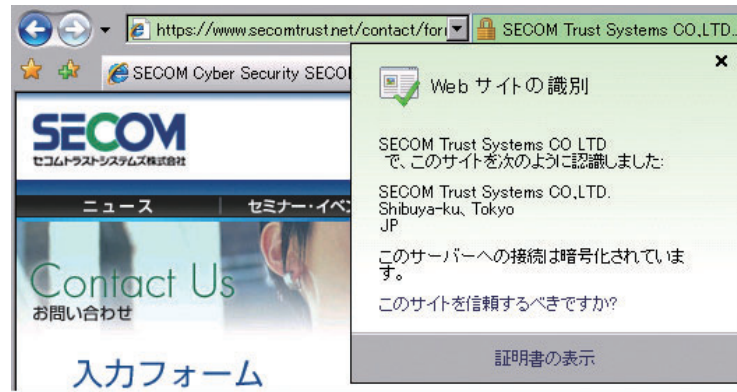
WebTrust for CAの抱える問題

WebTrust for CAは、アメリカとカナダの公認会計士協会が策定した、認証局の信頼性を保証するサービスとされており、従って商用のWebサーバ証明書は一定の信頼性を満たしたものであると考えられがちです。

しかし実際にWebTrust for CAが認定の基準とするのは、各認証事業者が規定するCP/CPS (Certificate Policy / Certification Practices Statement : 証明書ポリシー / 認証実施規程) であり、このCP/CPSにどれだけ忠実な運用を行うか、がポイントとなっています。CP/CPSの中で定める発行審査の内容については認証局に裁量が認められており、必

*1 オープンドメイン認証局は、パブリック認証局と表現されることが多いですが、これは公的な認証局という意味ではありません。本稿では、Webブラウザの証明書ストアに組み込まれるようなモデルをオープンドメインモデルと称しています。

図1 EV証明書の表示 (Internet Explorer 7.0)



ずしもこれらの認証局の発行する証明書が一定の信頼性を満たしているとは言えない状況でした。

一般的にWebサーバ証明書の発行審査としては、1) ドメインの本人性確認、2) 組織の実在性確認、3) 申請者の本人性確認および実在性確認などがありますが、認証局によってはこれらの発行審査の一部しか実施せずにWebサーバ証明書を発行しているものもあります。

■ フィッシング詐欺とEV証明書

昨今のフィッシング詐欺などにおける偽サイトを見破る方法として、

- 1) Webサーバ証明書がオープンドメイン認証局から発行されたものであること
- 2) そのWebサーバ証明書に記載された組織名等を確認すること

が有効であると言われてきました。商用のWebサーバ証明書であれば証明書記載事項について認証局が発行審査において確認しているの、なりすましは難しいだろう、と考えられていたからです。しかし、オープンドメイン認証局であっても前述のように発行審査はまちまちなので、発行審査の甘い認証局からWebサーバ証明書を入手する偽サイト運営者も出現してきました。

このような状況が続くと「証明書は一体何を証明していることになるのか」という認証事業者にとっては存在意義を否定さ

れかねない状況につながります。そこで、認証事業者やWebブラウザベンダーなどが協力してCA/Browser Forum (*2) を立ち上げ、新たなWebサーバ証明書の規準「WebTrust for EV」を策定しました。この規準に則って発行されるのが、いわゆるEV証明書です。

■ EV証明書の概要

EV証明書の目玉はなんといってもWebブラウザにおけるアドレスバーの表示が緑色に変わることですが、実際には大きく分けてWebブラウザ側の対応と、証明書を発行する認証局側の対応に分けられます。

認証局側の対応：認証局は組織の実在性確認をより厳格に行うために、対象を法人のみに限定し、確認のために登記事項証明書等の提出を求めるとともに、証明書には登記情報にもとづいた記載を行います。また、EV証明書であることを示すオブジェクト識別子も記載します。

Webブラウザの対応：従来のWebブラウザはいわゆる南京錠マークによって通信が暗号化されていることしか判別できませんでしたが、EV証明書に対応したWebブラウザでは、

- 1) EV証明書であること(アドレスバーが緑色に変化)
- 2) 発行対象の組織名 (南京錠マーク右)
- 3) 証明書を発行した認証事業者などの情報 (南京錠マークをクリック)

が簡単に判別できるようになりました (図1)。

表1 商用証明書との審査項目の比較 (*5)

審査項目	審査者	商用サービス				本プロジェクト			
		オンライン認証		機関認証					
		登録局	加入者	登録局	加入者	登録局	機関責任者	登録担当者	加入者
機関	本人性確認	×		○					
	実在性確認	×		○					
ドメイン	本人性確認	○		○	×	→	○		
	実在性確認	○		○	○				
機関責任者	本人性確認				○				
	実在性確認				○				
登録担当者	本人性確認				○				
	実在性確認				×	→	○		
加入者	本人性確認	×		○	×	→	○		
	実在性確認	×		○	×	→	○		
加入者サーバ	本人性確認		○		○				○
	実在性確認		○		○				○ ←

EV証明書は、必ずしも証明書の低価格化を防ぐためではなく、証明書本来の目的である安全・安心が成立しなくなるという「信頼の失墜」を防ぐための業界全体の意向を示したものであるのではないのでしょうか。

■ UPKIとサーバ証明書プロジェクト

国立情報学研究所 (以下NII) では、7大学等 (*3) の全国共同利用の情報基盤センターと協同で「大学間連携のための全国共同電子認証基盤構築事業」(以下UPKI (*4)) を推進しており、大学の認証基盤普及へ向けて様々な取り組みが行われています。ここでは、NIIが主体となって取り組んでいるUPKIのプロジェクトの一つである「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」(以下サーバ証明書プロジェクト) について着目してみます。

商用のWebサーバ証明書における発行審査の多くは、企業というトップダウンによる統治が可能な組織を想定したものです。これに対して教育研究機関である大学の組織は、産学連携など他の財源にもとづく共同研究や、複数の大学で教職を兼任している教授といったように、トップダウンでの一元的な統治が難しい組織という特色を持っています。このため、Webサーバ証明書を発行するにあたっては、発行審査の内容によっては大学組織に確認することが適切ではない(財源である企業に確認した方がよい) 場合なども考えられます。

このサーバ証明書プロジェクトでは、このような大学組織の特殊性を考慮して発行審査プロセスの大学最適化を行う「発行プロセスの研究」に取り組んでいます。また実際の

オープンドメイン認証局を用いて検証することによって、WebTrust for CAの基準にも通用する実用性のある証明書であることを証明しています。

■ サーバ証明書プロジェクトにおける発行プロセス

このプロジェクトの特徴は、既定の認証事業者における発行審査を分析した上で、各発行審査をできるだけ確認コストの低い組織に委任することで、最適化を行っている点にあります。プロジェクトでは、Webサーバ証明書発行において認証局が行う発行審査を審査対象(組織(機関)・ドメイン・加入者・加入者サーバ)と審査内容(本人性確認・実在性確認)について分類しています。

これに、プロジェクト特有のステークホルダーである機関責任者、登録担当者を加えた上で、それぞれの審査項目について「誰に確認してもらおうと手早いのか?」「誰が責任を負うべきか?」という観点から審査者を決めていきます。責任範囲を細分化することによって、大学のように複雑な組織構造であっても、対応しやすくなると考えられます (表1)。

■ 全国規模での発行審査の分担

プロジェクトは約700のSINET (*6) 加入機関を対象としていますが、これだけ多様な組織にまたがった発行審査の運用事例はほとんどないといつてよいでしょう。全ての組織に適用可能な画一的な審査手続きを規定することは設計面からも実用面からも難しいため、サーバ証明書プロジェクトでは、それぞれの審査項目について具体的にどのような審査手続き

*2 CA/Browser Forum (<http://www.cabforum.org/>) の国内での対応を目指した「有限責任中間法人 日本電子認証協議会 (<http://www.jcaf.or.jp/>) も設立されています。

*3 北海道大学、東北大学、東京大学、名古屋大学、京都大学、大阪大学、九州大学の7大学および東京工業大学、高エネルギー加速器研究機構

*4 ▶ <https://upki-portal.nii.ac.jp/>

*5 「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」説明会資料プロジェクト概要説明から引用
 ▶ <https://upki-portal.nii.ac.jp/item/ldata/odatao/serpj>

*6 SINET (Science Information Network) は、国立情報学研究所が運営する学術研究用ネットワークです。▶ <http://www.sinet.ad.jp/>