COLUMN

電　子　認　証　い　ま　む　か　し

# 第 4 回　電子認証の苦悩（2）

櫻井 三子　mine@ax.jp.nec.com
日本電気（株）

木村 泰司　taiji-k@is.naist.jp
奈良先端科学技術大学院大学

## 回 認証とサービスの間にある隔たり

これから先，電子認証がもっと成熟したら，インターネット上で展開される世界はどこまで現実社会に近づくだろう？　また，越えてゆけるだろう？

筆者らは，WIDE プロジェクト内での PKI（Public Key Infrastructure）実験を通じて，認証の応用をいくつか試みてきた．まずは，会員証的な使い方．会員かどうかを証明書で確認して，会員専用の情報を提供する場面を用意した．次に，名刺的な使い方．イベントの参加申し込み時に証明書を提示することで，証明書に記載されている名前などの情報を取り出し，申し込みフォームの一部自動入力を実現した．さらに，学割的な使い方．パーティの参加申し込み時に会員証を提示すると，パーティの参加費用が割り引かれる．

これらの応用の意図は，まずサービスの醍醐味を実感してから，このようなサービスの享受には認証がどんなレベルであるべきかに立ち戻って考える，ということであった．しかし，認証（ユーザが本人であるかどうかの判断）と認可（ユーザがどんなサービスを受けられるかの判断）がごちゃまぜで，誤解を与えるとか，PKI が本来目指している厳密認証の姿をまず忠実に示すべきだといった指摘は常にあり，葛藤してきた．

## 回 Ten risks of PKI

今から約 5 年前の 2000 年 11 月，Computer Security Journal に“Ten Risks of PKI”[1] という記事が掲載された．この記事は“PKI を導入すれば認証は万全だ”といった誇大な宣伝文句をたしなめるため，PKI の 10 個のリスクを指摘したものである．筆者らが実験を通じて指摘されてきたことの多くを含んでいると感じる．そこで文献 1）で挙げられたリスクが，むかしもいまも変わっていないか，軽減策があるかなどについて改めて話し合ってみた．今回は文献 1）に記載されている各リスクを概説し，それに対する著者らの“Response”をお送りする．

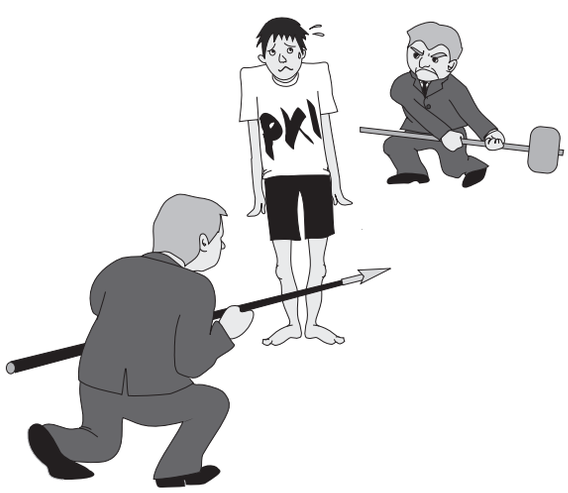
この記事では，1 つの証明書を使っていろいろな店舗で買い物ができるような使い方を想定している．これこそが誇大な宣伝文句の示すことなのかもしれないが，現実にはこのような証明書が浸透しているわけではない．読者によってはピンとこないかもしれないが，このようなモデルが現実になったとしたら，と想像して読んでいただきたい．

## 回 Risk #1: Who do we trust, and for what?

**[ 概要 ]**「CA を信頼する」という言葉によって，CA が認可まで保証しているかのように聞こえるが，認証が終わったあとの認可のリスクは証明書の検証者が負う．

**[ 回答 ]** 第三者が登場する電子認証に共通したリスクで，今でもこのリスクを回避できているといえない状況だと思われる．認証のための証明書を発行した CA は，品物を売ってもよいか悪いかの判断に関して，責任をとれない．

たとえば，文献 2）で例として出てくるが，運転免許証で酒類を売ってよいかを判断している店のことを考えるとよく分かる．本来それで買い物をすることはできないし，損害を補償してくれるわけでもない．しかし運転免許証が 18 歳以上に発行され，18 歳以上に酒を売ってよい場合は，運転免許証を持っている人には酒を売ってもよいと店は考える．年齢を証明する書類をあれこれ



確認するより効率がよいからである．しかしトラブルが起きたときは店がリスクを負うか，約款の内容によってはユーザがリスクを負う．

リスクを軽減するには，たとえば支払い能力を確認できたり保険をかけたりできるクレジットカード機能つきの証明書の登場が望まれるだろう．

## 回 Risk #2: Who is using my key?

**[ 概要 ]** non-repudiation（否認防止, しらばっくれ防止）は，秘密鍵が本人にしか使えない状況だった，という証拠があって初めて成立する．もしも non-repudiation 保証つきの秘密鍵を所有するユーザが知らないうちに使われると，ユーザが責任を全部負わされるリスクがある．

**[ 回答 ]** このリスクは今も変わらない．PKI の仕組みだけでは避けられないリスクのように思われる．お店に届いた注文書に自分のサインがついていたら，その注文の責任を取らされるということである．電子データである秘密鍵が他人に使われたことを証明することは難しいので non-repudiation はいまだにユーザ側のリスクが高い機能だろう．

もちろん秘密鍵を勝手に使われないための策は必要で，簡単には人に渡せないものに仕立てることが肝要だと思う．秘密鍵を物に閉じ込めることができる IC カードに秘密鍵を格納して（すると秘密鍵は IC カードから取り出すことが難しくなる）ユーザの証明書として使うケースが増えている．

IC カードを使わない場合でも，他人が秘密鍵を本人の承諾なしで使う可能性は以前よりは減っているようだ．日本では 2005 年から個人情報保護法が全面施行となった関係で，PC 上のデータ保護の製品が多数売られている．ユーザの PC 上のデータ保護の必要性の認識が高まっていると言えるだろう．non-repudiation の実現には及ばないかもしれないが，これをリスク軽減に向けた追い風として受け止めたい．

## 回 Risk #3: How secure is the verifying computer?

**[ 概要 ]** 証明書の検証者のコンピュータ上で偽のルート CA 証明書の混入を許してしまうと，偽の認証を正しいと判定してしまうリスクがある．

**[ 回答 ]** 公開鍵暗号を利用する電子認証に共通のリスクであろう．このリスクは本質的には改善されていないように思われる．たとえば，フィッシングのような偽の Web サーバを使った詐欺行為に対して電子認証の効果が出ないとなると，消費者への嫌がらせや架空請求などの被害が横行する可能性がある．リスクの軽減策として，消費者があらかじめフィンガープリントを確認した CA 証明書だけを使うことが挙げられるが，本コラム第 3 回でも取り上げたように，まだ敷居が高いかもしれない．

## 回 Risk #4: Which John Robinson is he?

**[ 概要 ]** 証明書に記載されている情報だけでは，同姓同名の証明書を区別することができないかもしれず，証明書の検証者のリスクになる．

**[ 回答 ]** インターネット上でグローバルに利用することを想定する電子認証に共通のリスク．この指摘は本コラム第 3 回で書いた「有効な同名サーバ証明書」の問題と本質的に同じだ．すべての CA 同士が証明書に記載する名前を協議し，同姓同名を避けるような解決は，規模拡張性の観点とビジネスの観点から不可能であろう．リスク軽減の策として，証明書の発行元（CA）の違いをもとに見分ける方法がある．また消費者の証明書に関しては，インターネット上のユーザの識別手段としてよく使われているメールアドレスが同名の区別に使えると考えられる．

## 回 Risk #5: Is the CA an authority?

**[ 概要 ]** CA は証明書に記載する名前の割り当てに関してのオーソリティではない．また CA は SSL という技術の利用を許可するような組織でないにもかかわらず，SSL に使える証明書の発行をコントロールしている．間違いが起きたときは証明書の検証者にリスクがある．

**[ 回答 ]** ホスト名や企業名などすでに使われている名前を利用する電子認証に共通のリスク．リスク軽減のためには，認証局が，証明書の中の軸となる識別子の登録機関と同一機関であるか，または非常に近い立場である必要がありそうだ．これについては別の機会にもう少し詳しく触れたい．

□　　□　　□

今回は 10 個のリスクのうち #5 までをお送りした．記事の端々では，PKI が多くのことを実現するかのような宣伝文句が取り上げられており，本コラム 1 回目で書いた「構え」の多さが思い出される．記事はそれに対する反応とも感じられる．次回は #6 以降をお送りする．

**参考文献／ URL**

1）Ellison, C. and Schneier, B.: Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure, Computer Security Journal, Vol. XVI (Nov. 1, 2000).

2）Perez, A.: Response to Ten Risks of PKI, http://homepage.mac.com/aramperez/responsetenrisks.html

（平成 17 年 5 月 26 日受付）