COLUMN

電　子　認　証　い　ま　む　か　し

第 1 回　PKI がきた道

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

今月から，電子認証にまつわるコラムを開始することになりました．私たちはインターネットの研究を行っている WIDE プロジェクト（http://www.wide.ad.jp/）で PKI（Public Key Infrastructure）の実践に取り組んできました．そのような経験の中から垣間見てきた電子認証の特徴，そして，あるべき姿に触れてゆきたいと思います．

回 顔が見えない相手の認証

電子認証は，顔が見えない相手の認証に使われる技術である．顔が見えない相手の“なりすまし行為”といえば「振り込め詐欺」が挙げられるだろう．

「振り込め詐欺」は，電話をかけたときに名乗らずに「オレ」「わたし」と言って身近な人からの電話であるかのように装う．詐欺とまでいかなくても，いたずら電話の範疇でこのような電話を受けた経験がある．認証技術にかかわっているとこの手の話には非常に用心深くなる．意地になって「どなたですか？」という問いを繰り返したが，相手もしつこく，最終的には自分から電話を切ったような気がする．顔が見えない中で「オレ」や「わたし」で分かってもらおうとすること自体おかしいはずが，言われた方の心理としては声で認識すべきか？などと考えてしまうところが困る．

インターネット上で相手を認証したり，されたりする場面では，相手の顔が見えないことの方が多い．私たちは何種類もの ID/ パスワードを持っているが，それらを誰からもらったか思い出せるだろうか？　おそらく，最初から顔が見えないままにやりとりしていて知らない場合が多いだろう．実在のショッピングの場合と違って，オンラインショッピングでは，いつまでたっても店の人の顔を知ることがないかもしれない．このような「顔が見えない」環境では，相手と相互に認証し合うことをいかに確実に実行し，しかも現実社会と同等に，完璧でなくても妥協できるレベルにどのように到達させるかが課題である．

たとえば，電子認証の 1 つに PKI がある．PKI が相互認証の技術として社会に取り込まれるスピードは決して早くはない．今回は，そのあたりから「むかし」を振り返ってみたい．

回 多くの人にサービスを，と願って構えた PKI

「構え」とはつくり，備え，外観，姿勢を表す言葉である．PKI の取り組みは，姿勢は立派だが一般にはとっつきにくい点があるように思われる．私たちは，それを「構え」の多さであると考える．「構え」が多いと，逆に構えられてしまう．

その 1. 信頼できる第三者を出発点にしたモデル

何をよりどころにする認証でも，認証する側に何かしらを登録する必要がある．オンラインで短時間に認証をすませる電子認証でも最初の登録は必要である．顔が見えない，知らない相手を最初に登録するにあたって，自己申告で名乗られただけでは信用しかねるし，時間をかけて身分証明の書類を確認していては数多くをさばききれない．

PKI では最初の登録を通信当事者以外の「信頼できる第三者」が行い，みんなでそれを共通仕様と認めることで，より多くの人たちが認証し合える枠組みを作ろうとした．

人から信頼を得ることがどんなに難しいか，特に社会

に出てみればすぐ痛感する．しかし，すでにあるインターネットの世界では，IP アドレスと名前の対応づけを解決するときの考え方が，ルートドメインを信頼する，で成り立っていた．それならば PKI も似ているので，すぐに実用化が進むに違いない，と直感したがあまかった．どのような違いがあるのか，分析不十分のまま現在に至っている．

今思えば，インターネットの通信プロトコルが即効を旨としてきたのに比較すると，PKI は理想やあるべき姿の追求を旨としてきた．世間が必要性を唱える前から，大規模でも処理しきれるように，第三者の存在をありきとした．

特に，「信頼できる」をどのように構築するか，について人々は腕組みして用心深く待ち構える．

その 2. その名はオーソリティ！

PKI では，「信頼できる第三者」を CA（Certification Authority）と呼ぶ．Authority という言葉からは，おそらく日本では専門家中の専門家といった印象を持つ人が多いだろう．少なくとも「私はオーソリティです」と自分から言うところを聞いたことはない．日本語では，CA を認証局と呼んでおり，実情は単なる機関である．また，インターネットと同様に，CA も分散管理できる特徴を持っている．しかし，どうも中央集権的なにおいがするらしい．

インターネット上に今までなかった CA という新しいビジネスを始めるには，「信頼」を短期間のうちに確立することが重要である．たとえば，それはブランドイメージをいかに早く築くか，ということにつながる．PKI がセキュリティ分野であることから，安全性を印象づける方向になることは自然だろう．他の認証技術を実現するサーバと比べ，CA サーバが設備面や人的体制面でいかに安全に配慮しているかを示すことで，安全なオーソリティを築いた．

また，認証サービスでは，たとえばなりすましの問題で誰かが不利益を被った場合にどのような責任をとるか決める必要がある．そこで，CA に関する安全面での配慮に加え，責任範囲をポリシーとして提示する仕組みが整った．

オーソリティとしての責務を果たそうとする姿勢は立派だが，残念ながら，CA ポリシーは，多くの人が簡単に理解できる内容にはまだなっていない．

門構えが立派すぎると，入る方も緊張して身構える．

その 3. 便利さを実現するための万能性

より多くの人が認証し合える世界では，通信の当事者が逐一相手を登録する手間を減らすことを目指そうとする．PKI では，CA で一度登録した事実を，できるだけ長持ちさせようとする．長持ちすればするほど便利，という考えだ．また，一度登録した事実を使って，より多くのアプリケーションに利用できる方が便利という考えもある．最初の登録をしっかり行う分，万能の使い道を提供できる，と．

しかし，認証サービスに責任を持つ側としては，万能の使い道に責任をとることは難しい．特に，新しい分野のサービスではリスクを見切れていないため，ある限られた使い道を想定した責任しかとれない．

PKI は，万能性を高めるための枠組み作りについて，手を緩めない．一般に，サービスを受けるために認証を終えると，次には権限や属性を確認してサービスを受けるのにふさわしいか判断するフェーズに進む．PKI は権限や属性を確認するためのインフラも用意している．ただ，認証に PKI 利用を前提としているため，すぐに多くの人が便利と実感する場面を示しにくい．

どこでもドアが便利と説明されても，当面は電車も併用するだろう．人々は万能よりも移行しやすい構えを求める．

回 電子認証のさが

電子認証がインフラになろうとすると，大がかりになる分，広がるスピードが遅くてもしかたがない．

現実に溶け込みにくい点はあるが，PKI ほどインフラを目指して戦っている認証技術を私たちは今のところ知らない．PKI の利用は，相互認証ではないが，ユーザが店のサーバを認証する場面では広まった．また，相互認証的な使い方としては，日本では電子政府をはじめとする PKI の構築と応用が進んだ．PKI は，すっかり安全性の高い認証のシンボルになっている．しかし，同時に，サービスの安全性を高める役割を過剰に背負わされている面もある．

結局，「まずはつなげましょう，誰とでも」で納得していたインターネットの上に，「さて誰だっけ」をできるだけ共通の方法で提供しようとすると，「構え」が多くなる．すると，うかつには手を出しにくくなって，広がりが鈍くなる．それがインフラたらんとする電子認証のさがかもしれない．

ともあれ，PKI はある日突然独自に出てきたわけではなく，他の認証技術の特徴を受け継いでもいる．次回は，認証技術を牽引してきたツールを振り返りたい．

参考文献

1）青木隆一，稲田　龍：PKI と電子社会のセキュリティ，共立出版（2001）．

（平成 17 年 2 月 28 日受付）