デジタル世界の身分証明書 ― 情報基盤センターＰＫＩプロジェクト

みなさんは「カード」を何枚持っていますか？（ここでのカードは身分証明書として使えるたとえばパスポートや健康保険証を含むことにします。）たとえば運転免許証は、法律の定めるところによる自動車を運転する資格をもっていることを証明してくれます。たとえば健康保険証は、それによって健康保険制度の枠組みで医療を受ける権利を持っていることを証明してくれます。我々の世界では、いろいろな資格や権利を持っていることを「カード」を持っていることで証明しています。それに限らず、その「カード」を持つことで、本人が「ちゃんとした」人間であることを認めてくれることがあります。銀行口座を作るときに運転免許証を提示すれば本人確認になるというのは代表的な例です。

翻って考えて、コンピュータやウェブの世界ではどうでしょうか。たとえば学務システムを考えてみましょう。これを使う「権利」のためにそれぞれ ID とパスワードが発行されています。ID とパスワードの組み合わせによってシステムにアクセスしている人が本人であることを確認し、使う「権利」（資格）、たとえば自分に関するデータの閲覧の権利を得るわけです。これは実世界の「カード」をデジタル世界に置き換えたものといえるでしょう。コンピュータやウェブを使うときの ID は、昔と違って、今では持つ機会がずいぶん増えてきました。

「カード」や ID を利用した本人の確認と「権利」（資格）の獲得という枠組はとても便利で使いやすいものです。しかし、その使いやすさの裏にすくう問題がいろいろ出てきました。その最大のものは不正使用です。実世界では、不正使用を防ぐためにカードに顔写真をいれたり、さらに割印を押したり、パスワードを設定してきました。クレジットカードや銀行カードのように財産に直結する場合は、その対策も真剣です。コンピュータの ID の場合も、広い意味での政治的な権限や財産に関係することが増えたこともあり、対策の重要性が認識されてきました。このために今検討されている枠組のひとつとして PKI（ピーケイアイ）とよばれている技術があります。PKI は暗号技術を用いて本人確認のための厳格な枠組を提供しています。典型例として、GPKI とよばれる政府のための PKI があります。GPKI は、文書の作成者や申請者の本人確認を PKI 技術を用いて厳密に行うことによって、申請や契約を電子的に行うための枠組です。

では、PKI は私たちの大学生活を便利にしてくれるものなのでしょうか？答えは Yes です。宛先の人以外に見られたくない成績表をメールで送る、はんこを押した（＝押した当人がこの文書を確かに承認した）書類を出張先からメールで送る、インターネット（という誰がアクセスしてくるかわからないところ）から非公開内部ネットワークへのアクセスを本人確認を厳密にして行う、これらは PKI を使えば安全にできるようになります。さらに、応用として複数のウェブページの同時ログインにも使うこともできるようになります。

では、すぐにでも PKI か？というと、話はそう容易ではありません。「本人確認」のためのカードを発行することに相当する体制は、銀行やカード会社のそれと同じくデリケートかつ慎重な運用が要求されますし、また「資格」を誰がどう認定するのか、それを「本人確認」と同じ厳密性を持たせるにはどうしたらよいのか、今までのウェブの運用を楽にするための「資格」の与え方はどうしたらよいのか、といった問題は、本質的であり、現状では、既成品の解がありません。さらに、メールサーバの詐称防止体制や、秘密のデータを特定の相手

だけに提供する方法の提供など、本当に「便利になった」と実感できるためのアプリケーションの展開についてもまだ決定的な解はありません。しかし、この分野のもたらす利益の大きさを予感できるところまでに地平が開かれてきたというのが現状です。現在でも、その地平を押し広げるべく、技術開発とその展開が急ピッチで進められています。

情報基盤センターは、これらPKI基盤の構築における技術と運用面での研究と開発を行うために、「PKI プロジェクト」をたちあげました。解決すべき問題は山積していますし、技術の展開も速いのですが、東大の皆、ひいては関係するすべてのユーザと開発者が利益を最大限に享受できるように努力していきたいと思います。

（佐藤周行）