PKI Lovers

東京電機大学
佐々木　良一

公開鍵暗号とデジタル署名の概念が、DiffieとHellmanによって、米国のIEEEという学会の論文誌に招待論文として発表されたのは、1976年のことである。公開鍵暗号とそれを利用したデジタル署名の技術があったからこそ、インターネットでできることが飛躍的に広がったという意味で、これらの技術は20世紀の応用数学分野における最大の発明の1つといって良いだろう。

私が、日立製作所で、デジタル署名の応用システムの研究および研究管理に最初に携わってからでも15年以上になるが、今でも公開鍵暗号やデジタル署名、そしてそれらをベースとするPKI（Public Key Infrastructure）の仕組みは美しいと思う。そして、何とか、これらが、社会の中でさらに大きな位置を占めるようになってほしいと考えている。米国にもこういうように考える人はいて、弁護士のR.Merrill氏によるとそれらの人々をPKI Loversと呼ぶのだそうだ。そう言う意味では、私も立派なPKI Loversの一人だろう。

電子署名法が成立したにもかかわらず、PKIの普及はあまり進んでいないという声も強い。この分野についてビジネスとして否定的な見方をする人も増えてきている。

ビジネスがどう動いていくかの予測は本当に難しい。セキュリティという当たらない研究をずっと続けてきた人間としてはなおさらである。セキュリティの研究を始めたときにはISDNの立ち上がりとともにセキュリティシステムが普及すると考えていたのだが実際は、インターネット時代になってからであった。しかし、時代は動くべき方向に動き、そして動くときには、技術者の予想をはるかにこえて激しく動くのだと思っている。

わたしは、15年前の段階で認証機関の必要性を認識し、そのサービスの実現を損害保険会社などに勧めつつ、自分でそのビジネスを立ち上げようなどとは全く考えていなかった。1990年代中盤になって、ベリサインなど新興の企業がサービスをはじめるのを見て、米国のベンチャー精神のすごさを痛感するとともに、時代はやはり動くべき方向に動くのだと思った。そして、その後、暗号やデジタル署名などの技術を核としたシステムの受注が日立としても急速に増大し、私たちの研究成果が、特許の活用とともにビジネスに直接的に結びつく時代となっていった。

今後、認証機関はいろいろに機能を拡大していくだろうと考えている。従来は狭義の認証機関が中心だったが、今後は、時刻や取引内容そのものを公証する機関や、取引主体の信頼を証明するブランド認証機関も出現してくると考えられる。そして、それらがアプリケーションと結合して大きなビジネスになっていくだろう。この予想があたってほしいというのが、PKI Loversとしての私の願いである。