経済産業省受託調査研究

電子認証フレームワークとIPアドレス認証の展開に関する調査報告書

2007年3月

社団法人日本ネットワークインフォメーションセンター

電子認証フレームワークと
IP アドレス認証の展開に関する
調査報告書

2007 年 3 月

社団法人日本ネットワークインフォメーションセンター

はじめに

電子証明書の普及が進まないと言われて久しい。日本政府の電子入札システムや地方自治体の公的個人認証基盤、電子署名法の認定認証業務に基づく電子証明書など、電子証明書の発行数が多い分野は存在するものの、必要に迫られずに日常生活の中で電子証明書（クライアント証明書）が使われる場面は未だに少ないのではないだろうか。

2007 年 3 月 18 日にサービスが開始した IC カード乗車券は、電車やバスに乗れるだけでなくコンビニエンスストアでの支払いなどにも対応している。日常生活の中で利用可能な場面が多い。非接触 IC カードの場合、特に X.509 形式の電子証明書の取り扱いに関しては暗号モジュールの安全性に関して一定の評価を得ていないものの、高度な認証技術が多くの場面で簡単に利用されるようにした意義は大きい。

これはコンピューター技術やインターネット技術においてはしばしば注目される点であるが、ユーザの利便性を向上させかつ利用場面が増える状況を作るには、「相互運用性」と「インターフェースの整理」が重要である。例えば IC カード乗車券の場合には、読取装置に対する IC カードの相互運用性がある。またどの IC カード乗車券でも同一の読み取りインターフェースがあって整理が進んでいる。インターフェースが十分に整理されていれば、別のメーカーの読取装置であっても同じカードが利用できるはずである。

電子証明書の利用場面を増やし適切に普及させていくには、電子証明書や PKI（Public-Key Infrastructure）の「相互運用性」の確保と「インターフェースの整理」が必要なのではないかと考えられる。電子証明書自体のインターフェースを単純化して整理することは難しいが、相互運用性があるような「電子証明書の意味」を整理し、策定することは可能であろう。

電子証明書の利用用途に応じた整理は、電子認証におけるノウハウの蓄積がなければ難しい。本調査研究は電子認証に関するノウハウの蓄積を進め、より多くの利用場面で役立つような電子認証を作り出していくことが本調査研究の狙いである。

はじめに