経済産業省受託調査研究

電子認証フレームワークのあり方に関する調査報告書

2006 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の
あり方に関する
調査報告書

2006 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

インターネットの普及に伴い、電子認証の重要性は大きくなってきた。ネットバブルと呼ばれる 2000 年以降の ICT の発展に伴い、インターネットを使った様々なサービスで電子認証が実施されている。金融機関が実施しているインターネット・バンキング・サービスでは、様々な趣向を凝らしたユーザ認証システムが採用され、ユーザの預金口座を保護する取り組みが行われている。日本政府が実施している電子政府の電子申請システムでは、PKI（Public-Key Infrastructure）を使った電子認証が採用されている。掲示板システムの発展型であるブログの多くでも、パスワードを使ったユーザ認証が行われている。

電子認証とは、ユーザ認証システムのようにアクセスしようとする者（以下、アクセス者と呼ぶ)、もしくはアクセスする先の本人性を確認する技術やその行為を総称したものである。電子認証の対象はユーザである場合があれば、サーバである場合もある。本人でない者による不正なアクセスを防ぐセキュリティを実現する為の仕組みである。コンピューターシステムが持つセキュリティ機能には、大きく分けると対策的アプローチを取るものと構築的アプローチを取るものの二種類がある。前者は不正アクセス等があった後に取られる事後策であるのに対し、後者は不正アクセスが起こらないようにする仕組みを作る事前策である。電子認証は後者の構築的アプローチを取るものだと言える。

2002 年以降、インターネットの IP アドレスを管理している「インターネットレジストリ」でも電子認証の強化策が実施され始めた。2003 年にはアジア太平洋地域の RIR（Regional Internet Registry：地域インターネットレジストリ）である APNIC が、2004 年には主に北米地域の RIR である ARIN や主にヨーロッパ地域の RIPE NCC が、それぞれ認証局を構築し、電子証明書を使った電子認証を実施している。JPNIC でも 2002 年度より調査研究を開始し、2004 年度に認証局の運用を開始した。

しかし、電子認証の技術を適切な利用には様々な要素の検討が必要となる。近年問題になっている「オレオレ証明書」や「オレオレ認証局」がそのいい例であろう。オレオレ証明書とは、ユーザが証明書の信頼性を確認する手段が提供されていないにも関わらずオンライン・サービスで使われ、ユーザがその場で信頼する設定をすることが促されるような自己署名証明書を意味する。事前にその証明書の正しさを確認できないため、本当の通信相手なのか、なりすまし行為が行われているのかが区別できない。オレオレ認証局はオレオレ証明書を認証局証明書として発行されたもので、ユーザが一度その証明書をユーザ環境に組み込んでしまうと、それ以降その認証局が発行したあらゆる証明書を有効だと見なしてしまう可能性がある。

他に、認証結果についてユーザに適切な警告や通知を行なうようなユーザ環境の検討が必要である。PKI を使った電子認証を使うと、暗号アルゴリズムや一方向性ハッシュアルゴリズムを破らなければ、成りすましやメッセージの改ざん行為は理論的に

難しい。しかしユーザの初期設定や注意を促すダイアログボックスの部分が悪用されると、いとも簡単になりすましやメッセージの改ざんができるようになってしまう。

電子認証の適切な利用のためのノウハウが欠乏していることは、IETF（Internet Engineering Task Force）の SAAG（セキュリティエリアのミーティング）や JNSA（日本ネットワークセキュリティ協会)の PKI 相互運用 WG においても度々議題に挙がってきた。電子認証技術の標準化は進んでいるものの、その最良の適用方法をまとめた BCP（Best Current Practice：最良と考えられる実践的知識）のドキュメント化は進んでいないという指摘に対してどのようにアプローチすべきかという課題である。

本調査研究では、「電子認証フレームワーク」という仕組みの検討を通じてこの問題に取り組むこととした。電子認証フレームワークは、電子認証に関わる各種ノウハウをドキュメント化し、参加者のコンセンサスと専門家のレビュを通じて、標準技術的なノウハウの集約を図る枠組みである。日本国内で主体的に技術的な知識の集約を図ることで、これまで主に予め標準化されている技術を利用するだけの状況にある電子認証の分野において、セキュリティ文化の向上やより高度なセキュリティ技術の研究開発を促すという狙いもある。

本調査研究は 2005 年度から 2008 年度の 3 年度の計画で取り組むものである。1 年目である 2005 年度は､「電子認証フレームワークのあり方に関する調査研究」と題し、電子認証の専門家の意見集約を図り、既存の電子認証に関わるガイドライン・ドキュメントの基本的な調査を行った。来年度は実際にノウハウとなるドキュメントを試験的に策定し、レビュのプロセスに関する調査研究を進める予定である。一方、電子認証の実践的な取り組みを並行して実施している。「IP アドレス認証の展開」と題し、2004 年度までに構築した JPNIC の認証局を使って、IP アドレス管理指定事業者（JPNIC から IP アドレスの割り振りを受けている通信事業者）の電子認証や、BGP（Border Gateway Protocol）における電子認証の適用に取り組む。これらの電子認証は、ユーザの所属性の認証やサーバ間の認証である。

電子認証というと自然人の厳密な認証に目が向けられがちであるが、インターネットにおける電子認証の需要は、この仮名的な認証の方が需要が高いと考えられる。なぜなら、社会システムの一部として実装されているネットワーク・アプリケーションの多くは、ユーザを戸籍上実在する人間として捉えるよりも、会社組織への所属や、支払能力を持つこと、他システムに予め登録されていること、といった属性の検証に重点が置かれている為である。電子認証フレームワークは、電子認証の種類に応じてノウハウのドキュメント化を行うことで、分野ごとに適用しやすいノウハウの蓄積を行うことができる仕組みであることが望ましい。従って、JPNIC の実施しつつある電子認証もひとつの事例となることが望ましい。

電子認証の技術の多くは、米国またはヨーロッパにおいて発展してきたものである。日本国内では暗号技術の研究では先進的な取り組みが行われているものの、PKI のような電子認証の概念を規定する技術の発展の例を見ない。日本において開発が進むアプリケーション・サービスは、日本独自の側面で、電子認証に対する要求事項があるはずである。日本国内における科学技術の発展を考える場合、既に確立された概念に則った、既存の技術を利用するだけでなく、主体的な概念形成と技術開発に取り組むことが望ましいと考えられる。

電子認証は、他のセキュリティの技術と同様に「利便性と安全性のシーソー」になりがちとなる技術だと言われている。これは安全性を向上させるには利便性を犠牲にしなければならず、利便性を向上させるには安全性を犠牲にしなければならないという社会的・学術的な通念である。しかし電子認証適用の社会的な影響を踏まえた、実践的なノウハウに基づいて構築されたシステムには、必ずしもこの通念が当てはまらないと思われる。非接触 IC カードを使った自動改札機や社員証システムは、そのよい例である。電子認証の利用によって、むしろ利便性が向上し、その一連の認証の上で新たなサービスが適用できる応用的な基盤となっている。

日本における電子認証はどのような形で普及するべきなのか。電子署名法などの電子署名に関する法整備や SSL/TLS のサーバ証明書の普及が進みつつある現在、この疑問に答える為の取り組みを開始し、利便性と安全性を共に確保した、安心できるネットワーク社会の発展が本調査研究の目指すところである。