1. 個人認証の考え方と制度的な対応

大山 永昭[†]

キーワード 個人認証, RKI, 資格認証, 法人認証, 電子署名

1. ま え が き

情報機器やネットワーク技術等の発展により、現在、社会規模での情報化が進展している。社会の情報化は、生産性の向上、新たな産業の創出やサービスの質の向上等に繋がるため、欧米の諸外国では官・民の協力の下で積極的に推進されている。我が国においても、1994年に内閣総理大臣を長とする高度情報通信社会推進本部が設置され、基本方針の策定、制度の見直し、電子商取引に関わるさまざまな問題の検討等が行われてきた。さらに、2000年7月には、従来の高度情報通信社会推進本部および有識者会議を改組して、IT戦略本部およびIT戦略会議を設置し、IT基本法の国会への上程および戦略ペーパーの起草等が行われた。これらの動きはまさに、我が国社会の情報化がきわめて重要であり、国は明確な戦略をもって情報化を推進するという意志表明である。

本解説文では、はじめに高度に情報化された社会の将来像を明らかにし、次に、情報化された社会における基盤の一つとなる個人認証の必要性とその考え方を紹介する。さらに、個人認証を行うための具体的な手段となるPKI (Public Key Infrastructure) を用いた電子署名の法的効力について解説する。そして最後に、法人および個人の認証に関する制度的な対応と資格認証の考え方を紹介する。

2. 情報化社会の将来像

現在われわれは図1の概念図が示すように、物理的なリアル空間において、例えば、ショッピングセンターや役所あるいは銀行等に行って必要な社会活動をしている。これらの社会活動は、図2に示されるように、情報システムを活用して電子商取引、電子行政サービスやホームバンキング等のアプリケーションにより、例えば、家庭からネットワークを経由して同じことができるようになると考えられている。このことを一般化して考えると、高度に情報化された社会では、われわれの社会活動が従来のリアル空間から

電子的なサイバ空間にまで拡張することがわかる。もちろん、どちらの空間でどのような社会活動を行うかは、本人の意志に委ねられるべきであるが、われわれ皆がいつでも、

図1 リアル空間における社会活動の概念図

図2 サイバ空間における社会活動の概念図

われわれは物理的なサイバ空間に入ることにはできないため、われわれの代理を電子的にサイバ空間に送り、必要な社会活動を行う

[†] 東京工業大学 画像情報工学研究施設

'Personal Authentication and Institutional Support' by Nagaaki Ohyama (Tokyo Institute of Technology, Imaging Science and Engineering Laboratory, Yokohama)

どこでも、自由に、安全にどちらの空間においても社会活動ができるようになることが情報化された社会の将来像と考えられる。

サイバ空間での社会活動を可能にするためには、さまざまな問題を解決しなければならない。例えば、ショッピングに行くためには、現金あるいはクレジットカード等の支払手段が必要であるため、電子的なショッピングを実現するには、これらの機能を電子化してサイバ空間に持ち込む必要がある。ふたたびこのことに着目して一般論を考えると、われわれに帰属する現金等の有形物や権利や義務等の無形物を電子的にサイバ空間に持ち込むことが必要であることがわかる。特に後者の無形物は市民権に基づくものであり、その必要性は、サイバ空間には国境がない国際的な空間であること、および、他人に成りすますことがあり得る等の理由から明らかである。これらの情報は各人にとってきわめて重要な電子データであるため、その管理および利用は安全かつ容易であることが強く望まれる。ICカードはこの要求に応える、すなわち、われわれが社会活動を安心して行うために必要な各種の情報を、安全に管理・利用するための有力なツールとして期待されており、その目的および利用形態からサイバパスポートと呼ばれている。

3. 個人認証の考え方

個人認証の必要性は、①インターネット等のオープンネットワークにより作られるサイバ空間では成りすましが起こりえること、②行為に対する正当性の確認が必要なことがある、の2点に集約されるが、その具体的な手段は2段階に分解される。すなわち、本人確認と行為の正当性の確認である。以下ではこれらについて解説する。

3.1 本人確認

本人確認は、よく知られているように、①所有物認証、②知識認証、③バイオメトリック認証の3種類の手段を、単独あるいはよりセキュリティを高めるために組合せて用いられる。①の方法は、登録された物品または特定の品の所有を確認するものであり、前者の具体的な例としては印鑑が、後者の例としては王冠や印籠がある。②の方法は、相手が特定の知識を有するかどうかで相手を確認する手法であり、合言葉を用いる手法もこの範疇に分類される。③は、生体に固有な特徴情報を用いる手法で、具体的には指紋や虹彩さらに最近ではDNA情報を用いるもの等がある。これらの手法には、それぞれに固有な特性があるため、現実のシステムでは費用対効果や慣例あるいは社会的な認知度等を考慮して選択されている。例えば、銀行のATMサービスでは、キャッシュカード等の磁気カードとパスワードが用いられていることから、このシステムでは所有物認証と知識認証を組合せている。また、商取引等で用いられる契約書では、印鑑を用いた記名捺印が慣例として用いられていることから、所有物認証になっている。一方、指紋等

を用いる手法は、本人確認の精度を高めること等を目的として研究・開発されており、すでに一部のシステムで利用されているが、その制度的な対応は措置されていない。

本人確認が行われる現実の場面には、前述のATMサービスのようなオンラインと記名・捺印をした書類等を用いるオフラインの運用形態がある。このことを歴史的な流れから見ると、言うまでもなく、過去はオフラインの手法が用いられてきたが、その後情報システム等の実用化にともなって、従来のオフラインの手法を用いることができないために、新たにオンラインの手法が開発・実用化された。そのため、これまで情報システムで用いる本人確認は、主としてオンラインの手法として考えられてきた。一方、自筆の署名や記名・捺印の電子版として電子署名技術が開発されてきたが、この手法は、その名称から一般的にはオフラインの手法と思われる。しかし、情報システムでの実運用をよく考えると、今後普及すると予想されている電子署名が用いる非対称鍵暗号方式（公開鍵暗号方式）は、オフラインの時間を極端に縮めることでオンラインになることから、オンラインとオフラインのどちらにも対応可能であることがわかる。特に、後述するように、電子署名の法的な効力を付与する新たな法律が実施されることを勘案すると、今後、サイバスペースにおける本人確認の手法は、オンライン、オフラインを問わずに非対称鍵暗号方式が主流になると予想される。そしてその理由としては、①2001年4月に実施される電子署名法を満たす限り、非対称鍵暗号方式を用いた電子署名技術を用いるほうが、行為に対する否認防止等に関する証明力が高くなること、②電子署名はオンライン、オフラインに対応できること、③GPKI（Government Public Key Infrastructure）やPKIが普及すると予測されること等があげられる。もちろん、大量な情報の秘匿通信等ではより効率的な共通鍵暗号方式が用いられるため、すべてが非対称鍵暗号方式になると言っているわけではなく、あくまで本人確認手段の動向についての予測である。

3.2 行為の正当性確認

現実の運用場面を考えると、個人認証を必要とするのは、サービス提供者あるいはサービス利用者が要求する何らかの行為の正当性確認である。すなわち、前述の本人確認は行為の主体を明確にするための中間的な手段といえることができる。このことを以下では、例をあげて説明する。

3.2.1 電子商取引の例

電子商取引の最も簡単な例として、B to Cを取り上げる。具体的には例えば、消費者が家庭からインターネットを介してサイバスペース上に開かれた商店に物品を注文する場面を想定する。この時、消費者から見れば、発注する商店の信用度と注文した通りの商品が送られてくるかが最も気になりとなる。一方、商店側から見ると、注文主が確かに代金を支払ってくれるかが心配になる。これら両者の心配事

は、互いに相手に対する不安であるため、両者間で解決することはきわめて困難である。この問題を解決するには、社会的に信頼される第3者機関による保証が有効であり、このことを目的とする組織は、一般的にTTP (Trusted Third Party) と呼ばれている。上記の例で、消費者の支払能力を保証するTTPは、既存の金融機関やクレジットカード会社等になるが、これらの組織にとってもサイバースペース内において与信を消費者に与えるためには、消費者の本人確認が必須となる。

以上のことから、この例における個人認証の目的は、消費者が物品を注文すること（行為）にともなう支払能力（正当性）に対する与信付与の可否（確認）であり、そのために消費者毎の与信情報と本人確認が組合えられることがわかる。

3.2.2 在宅医療の例

遠隔医療や在宅医療の分野においても、情報化の進展にともなってインターネットを介したサービスの提供が望まれている。これらのアプリケーションでは機微な個人情報を扱うため、プライバシー保護等を目的とした各種のセキュリティ技術の導入が必要である。具体的な例としては、患者の本人確認や電文の秘匿通信、さらには医師の資格確認等があげられるが、これらの中から最後の資格確認に焦点を当てて、個人認証を説明する。

資格確認を必要とする具体的な例として、患者が家庭からインターネット等のオープンなネットワークを介して医療相談を行う場合を取り上げる。この場合、例えば朝起きて腹痛を感じ、家庭のコンピュータを用いて医師のアドバイスを受けることを想定する。首尾よく医師がコンピュータ画面に出てきてくれて、症状を伝えた後に処方箋をもらい、薬を近所の薬局で購入できたとする。このような状況が近未来において実現されれば、医療機関への往復と待ち時間の節約となり、きわめて便利になると期待されるが、現実にはここで資格認証が必要になる。なぜならば、現行の医師法および医療法では、処方箋を出すことや医学的な処置を施す等の医療行為を行うには医師免許が必須と規定されているためである。したがって、このケースにおける資格認証は、医療サービスを提供する人の医師免許の確認と本人確認が組合わされて行われることがわかる。この場合も個人認証の必要性は、医療サービスを、インターネットを介して行うという行為の正当性確認になっていることがわかる。

以上のことからわかるように、個人認証はサイバースペース内で行う各種の社会活動において、その行為の正当性を確認することであり、そのための手段として本人確認と正当性の保証あるいは確認の2ステップが組合えられる。これらは、密接に連携して初めて本来の目的を達成できること、および情報化された社会におけるその重要性のために、近

年では、認証の問題としてしばしば議論されている。次章では、この認証に関する課題とその解決を図るための制度的な対応について解説する。

4. 制度的な対応²⁾

個人認証を含め、さまざまなアプリケーションにおいて認証の重要性がしばしば指摘されているが、認証の本質的な議論は、誰（あるいはどの組織）が何を何のために認証するか、すなわち、何に対して責任を負うかという責任論である。そのため、社会的な混乱を避け、便利な情報化社会を構築するためには、制度的な裏打ちが必須となる。本章では、2003年ごろを目途として整備されつつある制度的な対応について解説する。

4.1 電子署名に関する法律

これまで法務省から提示された公式の見解により、記名・捺印と自筆の署名は法的に同等であるとされていたが、2000年6月に「電子署名および認証業務に関する法律」が国会で審議・成立し、2001年4月1日の施行が予定されている。この法律は、非対称鍵暗号方式を用いる電子署名の法的な効力（自筆の署名と法的に同等である）を認めるとともに、認証サービスの安全性確保を目的として認証業務を行なう組織に対する鍵管理等の運用要件等を規定するものである。

この法律の実施により、電子署名を用いたオフラインの本人確認が制度的に可能になるため、個人認証を行うために必要な一方の手段（本人確認）に対する環境が整うことになる。これに対し、行為の正当性を確認する方は、後述の公的な資格認証を除けば民間が自主的に行うものと考えられており、現時点では制度的な手当ては行われていない。したがって、企業における各人の決裁権限や与信等に関する属性情報については、属性証明書を発行する組織の責任の下で運用されると思われる。

4.2 法人認証に関する制度

法人認証に関する制度としては、法務省が既存の法人登記に関する制度を基として認証サービスの提供を予定している。この認証の目的は、電子商取引の進展にともなう必要となる、取引法人の特定と代表者等が電子署名に用いる公開鍵の証明書の発行等である。この認証サービスの開始により、人格を持つ法人の存在確認が可能になり、電子商取引の進展に大きく資すると期待される。

4.3 個人認証に関する制度

本人確認については、前述の電子署名と民間の認証サービスにより可能になるが、電子政府サービスの実施に必要な個人の市民権の確認を含めた個人認証を行うためには、戸籍あるいは住民基本台帳等を基とした属性証明の付加が必要になる。このことを主目的の一つとして、自治省は平成10年に住民基本台帳の改正法案を国会に提出した。その後この改正法案は、国会での慎重な審議を経て平成11

年8月に成立し、現在は平成14年8月に実施すべく法律に明記されている住民基本台帳ネットワークシステムの構築と住民基本台帳カードの発行の準備が行われている。さらに電子署名法の実施に呼応して、現在、地方自治体の条例により行われている印鑑登録制度を基とした新たな制度（地方自治体による個人認証基盤）の実施について、平成15年を目途として検討している。

これらのことから、個人を対象とする本人確認は、民間の認証局と地方自治体による認証サービスの2つが実用化されると予想される。もちろん、これらの使い分けは、現実の必要性により最適に選択されるべきである。

4.4 資格認証に関する制度

遠隔医療の例の項で説明したように、法的に免許を必要とする職種のサービスをサイバースペース内で提供するためには、資格認証が必要になる。そして、この資格認証の対象となる具体的な例としては、医師や看護婦等の医療従事者、任意代理を業とする税理士、行政書士等があげられる。これらの職種に対する制度的な対応は未だ検討段階であり、具体的に新たな法整備を含めた環境整備は着手されていない。しかし、これらの職種に対する資格認証の必要性は明確なため、今後、何らかの手段を用いた環境整備がなされると予想される。ただし、これらの資格は当該本人の属性情報であるため、資格認証を実施するための責任主体は、職種によって異なっている。すなわち、医師や看護婦等の免許は、厚生省により発行されるとともに、これらの免許を有する人の原簿も現状では厚生省により管理されているため、資格認証を行う責任主体は厚生省にある。一方、税理士や行政書士はそれぞれ大蔵省および自治省の所管であるが、これらの職種を業として行うには、それぞれ税理士会および行政書士会に登録することが義務付けられているため、それぞれの資格認証を行う責任主体は各会にある。

以上のことからわかるように、資格認証については実施の責任主体が多岐にわたるため、一律に実施することは困難であると予想される。したがって、本件については必要

性が顕在化するにしたがって、順次実施されると考えられる。

5. む す び

本解説文は、「個人認証の考え方と制度的な対応」と題して、はじめに高度に情報化された社会の将来像を紹介した。次に、個人認証の必要性を具体的な例を用いて説明し、その実施は、本人確認と行為の正当性確認の2ステップで行われることを解説した。さらに、個人認証を実施する際の支えとなる制度的な対応として、電子署名に関する新たな法律と法人および個人の認証に関する政府の環境整備の状況を紹介した。そして最後に、法的に免許を必要とする職種のサービスを提供するために必要となる資格認証の考え方を解説した。

個人認証は、情報化された社会にとって必須のサービスであるため、そのサービスの安全かつ確実な提供はきわめて重要な課題である。本文で説明したように、政府による制度的な対応は着実になされているが、課題に対する対策の一般論と同じように、現実にはサービス提供システムの確実な運用と新たな技術の開発・実用化が不可欠である。そのためには産・官・学の密接な協力の下に、今後とも個人認証を含めた社会の情報化を積極的に推進することが重要である。

〔文 献〕

- 1) 大山永昭：“ICカードを用いた電子身分証明の構想”，ITUジャーナル，27，9，pp.18-22（1997）
- 2) 総理官邸のホームページ：www.kantei.go.jp参照

大山 永昭 1982年，東京工業大学大学院総合理工学研究科物理情報工学専攻博士課程修了。1983年，東京工業大学工学部附属画像情報工学研究施設助手。1986～1987年，アリゾナ大学放射線科学研究員（画像再構成についての研究）。1988年，東京工業大学工学部附属画像情報工学研究施設助教授を経て，1993年，同教授となり，現在に至る。専門分野は医用画像工学，光情報処理。工学博士。