電子政府を支えるPKI(Public Key Infrastructure)を「社会的信頼」という視点から考える

作新学院大学 人間文化学部　助教授
藤本一男
fujimoto@sakushin-u.ac.jp *

2002年5月20日
「電子署名電子認証シンポジウム実行委員会」

概 要

本稿は、2002年2月20日の津田塾大学数学計算機科学研究所の談話会で発表されたものです。今回、「電子署名・電子認証シンポジウム」の予稿集として、活用していただくべく、若干の誤記の修正し、著者の所属、日付だけを更新してここに公開します。(2002/5/20付記)

本稿では、PKIが、社会的な「インフラ」になるために必要な社会的要件について考察し、そこで技術的には解決しえない困難2点に注目する。

一つは、根源的なルート認証局の問題であり、もう一つは、ソフトウェアを媒介にした間接的経験という関係での利用者の経験蓄積の困難である。このどちらもが、社会化された情報システムに対する信頼の問題と不可分であり、情報技術が社会化した今日を象徴する問題状況である。

そして、これらの問題を解決するためには、利用者が信頼できる専門家を媒介にするしかないことを述べる。

1 はじめに

1.1 e-Japan計画の進行

2001年1月6日施行のIT基本法[1]以降、e-Japan[2]計画が5つの領域で進行している。なかでも、行政の情報化をうたった電子政府計画は、電子認証基盤を前提としており、サイバースペースで実社会と同様の信用を成立させようというものである。政府は、2003年（平成15年）の電子政府樹立をめざして、多くのプロジェクトを走らせている。

本稿では、この電子政府構想（すなわち電子申告制度）を支えるPKI（Public Key Infrastructure:公開鍵認証基盤）を社会的なシステムとして成立させるための条件である「信頼」のありようをめぐって考察していく。

なお、e-Japan計画の5つの重点計画は、以下の通り。このうち、4の行政の情報化がいわゆる電子政府計画である。電子署名法と政府の認証基盤が直接関係してくるのは、この4と3の電子商取引になる。

---

*発表時の所属は、津田塾大学 数学計算機科学研究所 客員研究員 / メモレックステレックス株式会社

[1]高度情報通信ネットワーク社会形成基本法」が正式名称。http://www.kantei.go.jp/jp/it/kihonhou/honbun.html

[2]http://www.e-japan.go.jp

e−Japan 計画の重点政策	
1	世界最高水準の高度情報通信ネットワークの形成
2	教育及び学習の振興並びに人材の育成
3	電子商取引等の促進
4	行政情報化及び、公共分野における情報通信技術の活用の推進
5	高度情報通信ネットワークの安全性及び信頼性の確保

また、「行政の電子化」は、次の 5 つをテーマとしている[3]。

- 行政情報の電子的提供…官報で公表が義務付けられている情報や統計資料、審議会答申、報道発表資料のインターネットによる提供。
- 申請・届出等の電子化…実質的にすべての申請・届出等を 2003 年度までのできる限り早期にインターネットで行えるようにする。
- 歳入・歳出の電子化…手数料納付、納税等をインターネットで行うことが可能となる。
- 調達の電子化…入札・開札がインターネットによることが可能となる。
- ペーパーレス化…行政内部や行政機関間の協議、通知、配布の電子化

1.2 前倒しアクションプラン

2001 年 6 月には、IT 基本法制定時の達成計画を大幅に前倒し修正した、6/26 改定アクションプラン[4]が発表され、さらに 9 月には、次年度（平成 14 年）達成可能内容の前倒し実施案と進捗状況が報告されている[5]

このように、政府は、非常に急ピッチで電子政府[6]の実現を急いでいる。電子政府案が登場する過程、IT 戦略会議/戦略本部での議論の内容の変化については、阿部 [2001] を参照。

2001 年の方針文書	
2001 年 1 月 6 日	IT 基本法施行
2001 年 1 月 22 日	e−Japan 戦略
2001 年 3 月 29 日	e−Japan 重点政策
2001 年 6 月 26 日	e−Japan2002 プログラム 〜平成 14 年度 IT 重点施策に関する基本方針〜
2001 年 9 月 14 日	第 5 回 IT 戦略本部「前倒し計画」

1.3 電子署名法

2001 年 4 月 1 日、電子署名法（「電子署名及び認証業務に関する法律」平成 12 年法律第 102 号）が施行された[7]。この法律によって、デジタル署名が、従来の印鑑による押印と同等の社会的地位

[3] http://www.kantei.go.jp/jp/it/network/dai3/3siryou40.html
[4] e-Japan2002 プログラム http://www.kantei.go.jp/jp/it/network/dai5/5siryou2.html
[5] 第 6 回 IT 戦略本部　議事録)「e-Japan　重点計画、e-Japan2002　プログラムの加速・前倒し」 http://www.kantei.go.jp/jp/it/network/dai6/6gijiroku.html
[6] 電子政府の総合窓口 http://www.e-gov.go.jp/
[7] http://www.meti.go.jp/policy/netsecurity/digitalsign.htm

を得ることなった。こうして、サイバースペース内に、いわゆる現実社会の秩序が移入されたことになる[8]。

1.4 電子申告の現場での議論

このような政府の矢継ぎ早の計画に対して、電子申告が関係することになる専門家集団は、対応を迫られる。弁護士、税理士、行政書士などの士業と呼ばれる人たちは、様々な形で、電子申告に対応していこうとしている。

私も、この間、このような現場での勉強会に講師として呼ばれることがしばしばあるが、そこで議論されることは、電子政府を我々が受け入れてくにあたって、考えなくてはならない問題ばかりである。

1.5 勉強会での経験

勉強会は、まず、電子署名とはなにかから始まる。それを踏まえて、現在の実務がどのような変化をこうむるのか。それに対して、政府はどのような制度改革を考えているのか。その変化は、国民やその分野の専門家にどういう意味をもっているのか、などの議論に入ることになる。

しかし、公開鍵暗号方式を、一回の説明で理解するのは難しい。だが、その部分の理解が中途半端では、鍵の生成がどこで行われて、どのように配布するのか、また、どのように鍵を管理するのか、という部分にシステムの根幹にかかわる問題が潜んでいることは理解できない。

また、電子署名を「電子の印鑑」という比喩でとらえようとすることもある。電子署名法が、デジタル署名によって「本人が署名した」という「推定効」の成立を明記しているのだから、印鑑との類推で理解しようとするのは、当然のなりゆきである。

しかし、電子署名とは、暗号操作の一局面が、印鑑の機能と同じように使えるということであって、これまで長い歴史をかけて蓄積されてきた印鑑の機能を電子化したものではない、ということは、理解しておかないといけない。ここを誤解すると、電子署名が、印鑑の機能のすべてを電子化したものであるかのような期待をしてしまう。もしくは、そのようなことも可能なのではないか、と楽観することによって、電子申告が招来する従来制度との違いを過小評価してしまう可能性もある。

そのため、勉強会では、印鑑の比喩は限界をもった方便であることを説明し、まずは、共通鍵暗号方式を理解してもらう。そして、電子署名とは、いわゆる押印のイメージとは異なり、暗号化のことであることを理解してもらうようにしている。

この点を理解してもらった上で、公開鍵と本人の結びつきは、認証局によって支えられているという話をし、電子認証というシステムの信頼性は、認証局の確からしさに支えられているという理解に到達する[9]。

そして、ここが各専門分野での議論の出発点である。例えば、捨印、代理、三文判の機能、など、「電子の印鑑」ではどうなるのか[10]。また、このシステムを支えるのが、機能的には、認証局と利用者の自分の鍵の管理の問題（配布、更新、廃棄というライフサイクルを含む）であること

[8] なお、電子署名法に先立って 2000 年 10 月には、商業登記法の改正をうけて、法務省民事局が、「商業登記に基礎を置く電子認証制度」をスタートさせている。

[9] 本稿では、公開鍵方式についての解説は行わない。必要に応じて参考書など参照されたい。なお、「情報と社会」の講義 Web にも講義で用いた資料を参照できるようにしてある。http://edu.tsuda.ac.jp/ fujimoto/crypto/index.html

[10] このような領域は、政府でも検討されており『共通問題研究会』としてレポートがまとめられている。共通課題研究会『インターネットによる行政手続き実現のために』平成 12 年 3 月

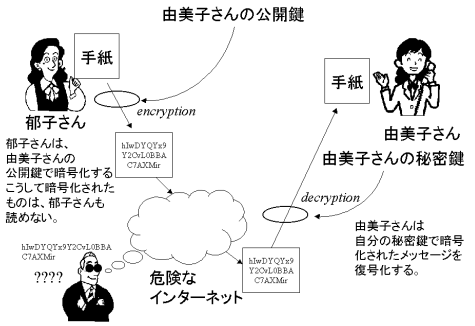

図 1: 公開鍵暗号方式による「暗号」

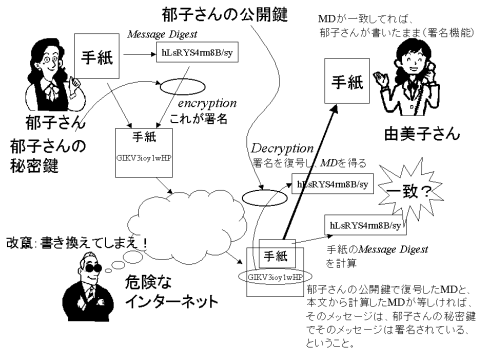

図 2: 公開鍵暗号方式による「署名」

に理解が到達すると、専門家団体としてやらねばならないことの作業量に、皆が驚くことになる。これまでの印鑑の管理とは、まったく異なった管理を、すべての構成員が要求されるし、従来は、疑問に思われることもなかったようなことが、電子化したらどうなるのだ、という疑問として表面化してくる。現行法の解釈の問題がでてくる領域もある。それは、IT がもたらす可視化という機能なのであるが、このような IT 化を契機にして、従来のありかたを見直すことが、あらゆる分野で進行している。

2　認証局の「信頼性」

次に、公開鍵暗号方式における認証局の問題を中心に、システムに対する信頼の問題を整理していく。

2.1　PKI の技術的安全性

PKI が社会のインフラの一つとして実装され利用される場合には、提供される信用の内容を含めて、その安全性が問題になる。

技術的な問題の中心は、採用されている暗号アルゴリズムの強度の問題である。RSA 方式の場合、暗号の強度は、大きな桁数の数を二つの素数に分解することの計算量の膨大さ、すわなち時間的困難さに依拠しているので、計算機のパワーやアーキテクチャが進化する過程で、今日では使用に耐えるアルゴリズム、鍵長も、危険になることもある。

また、数学的原理を実装しているのは、ソフトウェアであるから、そのソフトの完全性の度合いも問題になるし、これらを前提にして、ハードウェア（サーバーやネットワーク）の信頼性が問題とされる。

2.2　鍵管理をめぐる問題

しかし、このような技術的・機械的な問題が当面生じないとした場合でも、運用上のミスがあれば、認証局の正しさは、簡単に崩壊する。電子署名が、成りすましを防ぐのは、公開鍵と本人の関係が正しい場合であって、ここで成りすまされれば、もともこもない。このような危険は、認証局に対する、直接的なクラッキングによって生じるよりも、利用者本人が管理する責任を有する秘密

鍵の管理のルーズさによって生じる可能性も大いに存在する。これは、インターネット利用において、利用者に課せられる ID、Password の管理問題と同様である。

また、本人が鍵をきちんと管理していたとしても、鍵の発行から本人に渡る過程も問題になる。鍵生成の際に、本人確認をどのように行うのか[11]。鍵のコピーは、どこにも存在していない、という保証はどのようにして可能なのか。利用者は、どのようにしてこの点を確かめられるのか。電子情報のコピー自由という性格は、物理的実体を持つ印鑑ではまったく必要のなかった管理上の問題を引き起こしている。まだ、我々は、このような電子的な貴重品の管理の方法をよくわかっていない。

2.3 認証局の安全性

電子署名法が、デジタル署名を社会的に有効なものと認定した。これを支えるのが、電子認証のシステムであり、日本国の認証の原点（ルート CA:Certificate Authority）は、GPKI（政府認証基盤）である[12]。このシステムは、コンピュータとネットワークを基礎に構築されるので、この領域の信頼性は、相当高いレベルのものが要求される。だが、ここは、システムの冗長化などの手法によって、技術的にあルートる水準（たとえば、メインフレームレベル）を期待することが可能である。

また、採用されている暗号技術の強度は、その時点、および当面の技術的な進歩を想定した上で、十分な強度を確保することは難しくはない。

2.4 PKI を信頼する際の二つの問題

2.4.1 ルート CA は、どこをルートとするのか

PKI の仕組みを理解し、認証局の重要性がわかった場合に、すぐに疑問に思うことがある。それは、ある認証局は、かならず上位の認証局を必要とするということである。これをどのように実現するのか。政府の認証基盤 GPKI は、総務省の CA が自己証明。他の府省が、相互認証、という構造で構成されている。

確かに、無限に上位をもとめる階層構造を構築することは、不可能である。しかし、原理的なルート CA は存在しなくてはならい。これは、社会が統合シンボルを有しているのと同じ理由で、シンボリックなものとして求められるしかない。ここでは、信用を提供するシステムへの信頼の関係を整理しながら考えていく。結論的にいえば、提供側（政府）が、これをルートとしてくれといっているもの（GPKI）を、利用者が信頼する、という関係である[13]。

2.4.2 ソフトウェアを媒介にした経験の蓄積の困難

今ひとつの困難は、電子認証は、それ自体では意味をなさず、なにかの行為（電子社会での電子的な行為）のための条件になるので、行為の連鎖の中にある。にもかかわらず、その経験は、利用者の直接的な経験としては、蓄積しえない、という点である。

---

[11] Verisign の証明書を Microsoft に成りすまして取得した事例があったが、これなどは、登録のずさんさの例である。「米マイクロソフトの“ 偽デジタル証明書事件 ”が残した教訓」http://itpro.nikkeibp.co.jp/free/ITPro/ANALYST/20010403/1/

[12] http://www.gpki.go.jp

[13] こう考えると、原理上は、まったくことなった認証構造をもつといわれる PKI と PGP が、究極的には、同じ信頼構造によって維持されていることがわかる。

電子認証では、押印の場合のような身体的な経験は成立しない。電子的な bit である「印影」（という暗号の状態）を直接視認することも不可能である。すべての行為は、ソフトウェアを媒介とした間接的な経験でしかない。このような極度な間接経験をもって、信用という抽象的な対象を認識しなくてはならない。

3　信頼と信用、安全

こうした問題を考えていくために、「信用」「信頼」を整理しておく。

信用とは、「name に対応する value の確からしさ」から構成される内実を要素として、その「確からしさを実現する仕組み」への信頼によって成立している。我々が、信用という言葉を使う場合に、この全体を総称して呼んでいることも多い。

3.1　信頼とはなにか

近年、日本型システムの崩壊が話題になる中で、「信頼」に対する、様々な社会科学的なアプローチが試みられている。ここでは、山岸 [1999] に依拠して論を進める。

信頼とは、他者の行為に対する期待である。それは、山岸によれば、以下の内容を区分して用いなければ、議論が混乱する。

まず、相手の「意図」が関係する。それゆえ、ある（期待された/されていない）行為意図と能力を区分しなくてはならない。ここで、能力がない場合は、「信頼」の候補にはならない。浮気する能力がないことを、浮気しないと信頼している、とは言わないからである。

このように、意図に焦点を当てた場合でも、「不確実性」の存在が問題になる。つまり、相手の行為が意図に沿ったものであろうとなかろうと問題にならない場合、別の表現を用いれば、自分にとって危機的な状況に関係ない場合。そこでも「信頼」は問題にならない、と山岸は言う。そのような不確実性が存在しない状況は「安心」と呼ぶ。

つまり、相手の出方によっては、自分が危機的な状況におかれる可能性があり、相手が、こちらの期待にそった行為をしない可能性がある局面で、相手を信頼する、しない、ということの議論が可能になるというのである。

3.2　機械的システムを信頼することはない

では、信頼の対象はなんだろうか。それは、人である。確かに、機械装置の信頼性という言い方で、機械装置のある特性－ダウンせずに機能しつづける性能の指標とする。

しかし、山岸の整理によれば、我々が信頼の対象としてのは、人間（行為）である。つまり、自然に対しては、信頼という行為が成立しようがない。自然には意思がないからである。つまり、機械のような人工物は、直接にその機械装置を信頼しているのではない。これは、それを設計し、製造し、メンテナンスしている人間に対してする信頼が媒介になっていて、それが、機械装置に対する信頼、であるかのように観念されているに過ぎない。

PKI は、信用を提供する。その信用とは、貨幣が、その額面の金額と対応する価値の結びつきの確からしさを保証しているのと同じ意味での信用である。それは、信頼ではない。信頼とは、人間の他者に対する態度である。この信頼の対象が、システムのような物質にも拡大して語られることもあるが、信頼の対象は人でしかありえない。つまり、信頼は、対象の反応に対する期待が存在し

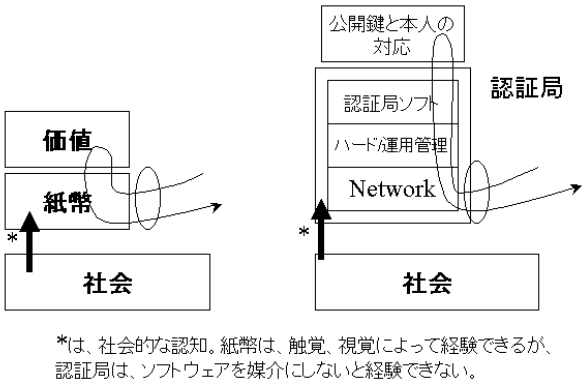

図 3: 信用のスタック

て成立するものであり、その意味では、期待を裏切る意思が存在しなければ、私たちは、信頼という行為自体をおこなわない。

我々が機械装置に対して信頼性と呼ぶファクタは、安心性である。機械装置は、ある意図をもって壊れるわけではない。

3.3 システムは、信用を提供する

それでは、機械装置は、直接には信頼の対象ではないとしたら、なにの対象なのだろうか。これは、先にもふれたように、信用を提供している。認証局であれば、ある人の公開鍵とその人の関係の保証しているのだ。貨幣の額面と価値の関係から考えると、精巧に作られた紙幣というハードウェアである。そのハードウェアが体現している対応関係（額面と価値）を保証しているのが、財務省である。

このように考えていくと、機械装置が自動化装置として提供する信用としての「認証」に我々は頼ろうとしていることがわかってくる。

そうであれば、問題は、この機械装置が安定して動くことを保証するところまでは、従来の情報技術の延長に、安定したシステムを期待することができる。

そこで問題になるのが、認証局が提供する信用が、現実世界になにか対応するものがあって、その電子的な表現なのか、ということである。もちろん、個人であれ、法人であれ、実在する実体との関係づけを行うことが認証局の課題なのであるから、それがないわけがない。だが、現実世界では、多様なレベルの対応関係が存在しており、それらがうまく住み分けを行って安定した制度となっている。電子的な世界は、それとは独立な新たな信用を創造するのか、それとも、新たな個人、法人をつくりあげるのか。これは、電子マネーの価値の所在が現実世界なのか、電子の世界のインターラクションなのか、という問題にもつながっていく。

4 PKI をめぐる信頼と信用

PKI は、信用を提供する。利用者は、そのようなシステムを（構築、メンテ、法的裏付けをする人々を媒介にして）信頼する。ユーザは、システム単体ではなく、構築、メンテナンス総体を信頼する。

4.1 PKI（情報技術）と信用

青木、稲田は、PKI を内包する電子社会のセキュリティを論じる中で、認証局が提供するものは、信用である、という（青木、稲田 [2001]）。そして、社会的には、認証の起点である信頼点（Trust Point、trust anchor）が必要だ、という言い方で、ルート CA（Certificate Autority:認証局）について語る（前掲書:62）。ここで、なぜ、信用の起点が、信用点ではなく、信頼点になるのか。それは、CA は、原理上、つねに上位の認証を必要とするからであるが、無限に続く認証の連鎖は、実装することができず、ある段階で、利用者に認めてもらうことで（つまり認証局は、利用者に認証されて）シンボリックに根源的ルートとなる。

我々の社会は、それをシンボルとして共有することで成立している。絶対神、天皇、などが、シンボルであるのは、そのような社会統合の機能をになっているからである。このような社会的なシンボルは、実体としては存在しない。多くの人が認めているが故にシンボルとして成立している。実体がないとはいえ、それは十分にリアルであって、簡単に破壊することはできない。

これに対して、認証局は、物理的実体である。破壊することも可能だ。しかし、この内部にやどるものが、社会的信用である場合には、その信用の起点が必要になる。それは、信頼点、人々による認知対象となるほかない。それは、みなが正しいと考えるから正しいのであって、皆が認めなくなれば、それが提供しうる確からしさは、意味をもたない。

4.2 社会化したシステムの信頼性は、機械的システムの信頼性の総和ではない

公開鍵暗号方式が実現するデジタル署名による「成りすまし」の防止という機能が成立するには、認証局が正しく機能していないくてはならず、数学的原理、ソフトウェア的実装の正しさなどの機械的要素は、システムとしての信頼性の必要条件でしかない。

ところで、通常システムの信頼性というときには「稼動の安定」を指し、処理の機能、内容の正しさそれ自体をあらわす用語ではない。情報システム監査の視点では、データのインテグリティが話題になるが、この電子認証のシステムでは、データ、および処理の内実が、そのまま問題になる。そこでは、名前（題目）と電子的実体（エンティティ）の対応関係が問題になり、それは、信用と呼ばれるべきである。

メインフレームが、定義されたフォーマットによって正規化されたデータを入力とし、処理し、出力する、というような、管理されたプロセスが前提になる場合には、処理装置たるコンピュータが「稼動すること」、その上で動く「ソフトウェアにバグがないこと」、そして、「運用管理が正しく行われ」ていれば問題はなかった。その意味では、閉じた世界であるがゆえに、システムの信頼性という言葉が意味を持ったのである。

しかし、PKI は、電子媒体上に計算機処理可能な形で提示されている信用情報である。上に述べたような「処理」は、この信用情報をもとに、別のシステムが担当する「販売システム」であったりする。ネットワーク上の店舗開設者からみれば、アクセスしてくるお客さんが、安心していい客なのかどうかを知りたいし、お客の側からすれば、その店舗が、本当に商品を提供してくれるような店なのかを知りたい。PKI は、ネットワーク上での行為者を現実世界に存在する具体的な人間に関連づけるという確かさ（信用）を提供し、取引における不確実性を縮減する機能を果たしている。これは、貨幣が額面と価値の関連づけを提供し、それを発行主体（財務省）が保証する、というのと同じ関係である。貨幣は、その所持者から独立して「価値」であるので、所持者がなにものであろうとも、発行主体が社会的に信頼されている限り、額面は信用される。

すなわち、ここでは、かつてのクローズなシステムをめぐって成立していた人間とコンピュータ

の関係とは異なった関係が登場しており、そのことが我々に戸惑いを与えている。

4.3 専門家の役割

ここで、専門家が果たす重要な社会的役割について見ておきたい。

電子的コミュニケーションの社会的な浸透は、中間過程を排除するように進行する。その意味では、電子申告制度が進行すれば、その申告を当該領域の専門家として代行していた専門家も当然、不要になる。例えば、税金の処理などでは、本人が、直接 Web で申告するようなことになれば、税理士の代理申請は不要になる。

しかし、これまでの社会は、様々な専門家を擁することで、個々人が、すべての専門家になる必要がない環境を形成し維持してきた。すべての人が、自分の社会生活に必要な領域の専門家になるのは、個人への負担が大きなものになるし、現実的に不可能である。それを強行することは、社会的な密度の低下をうみだすことにしかならない。専門家は、社会総体のコストを低減してきた。このコストと、電子化によって中間過程が排除されることがもたらすコストの低減は、社会的なコストが電子化によってどのように変化するのかの問題として検討されなくてはならない。

4.4 ソフトウェアを媒介にしないと経験できない世界

以上のような領域に加えて、電子化の場合に、ソフトウェアを媒介にしてしか体験できない世界であるという特徴からも必要になる専門家の役割がある。

自分が信頼できるかどうか検討しているシステムがある場合に、十分なソフトウェアに関する知識を有しているようなことは、まれである。

そこでは、製造者、販売者を信じるということを媒介にして、そのソフトウェアが描き出す世界を信用し、システムを信頼するのである。この、電子化された世界においては、直接的な信頼は成立せず、生体に埋め込まれた電極で bit を直接体験するような SF 的な世界が実現しないかぎり、必ず間接的な経験になる。ここに、電子的世界を経験する時に際立って問題になる領域がある。

なにかを確認する場合に、複数の人間が、直接経験できることを共有して判定することに依存して私達の社会は構成されている。しかし、筆跡鑑定や声紋鑑定という作業が専門家に依頼される場合があるように、直接経験では決着がつけられない場合に、専門家による判定に依存することがある。ソフトウェアを媒介にすることによってしか成立しない経験には、これと同じような状況がある。

5 私たちは誰を信頼するのか

さて、以上のようにみてくると、PKI が導入され、順調に機能するためには、電子署名に対する法的な位置付けだけでなく、利用者によるシステムに対する信頼が不可欠であることがわかる。原理的なルート CA,TrustPoint を物理的に設定することが不可能である以上、原信頼点として（実際には、それが、システム、すなわち電子政府）の信頼を実現しなくてはならない。これは、機能的な信用をベースにすることは、ことの半分でしかない。もう半分、そして、より本質的には、この電子政府が国民にどのような利便性を提供するのか、という点にもとづいて、国民が、システムを支持することをようにならなければならない。そのためには、個々人がシステムの仕組み、機能に対する必要最低限の理解を有することと、国民の側にたって、システムの機能上、制度上、信用

上の問題に応える専門家の存在が必須なのである。

国民は、このような専門家を選出、罷免する能力を求められる。電子ネットワークは、中間過程を排除して、社会の仕組みをシンプルにする、と言われるが、そうして成立する社会が、それ以前の社会と同等の確かさを維持するために必要とされる人々の能力、労力の総和が、低減する確証は、どこにもない。また、社会としての統合性が堅牢になる保証もどこにもないのである。

参考文献

[1] 青木隆一、稲田　龍、監修：村井　純『PKI と電子社会のセキュリティ』共立出版、2001/10

[2] 阿部隆幸『日本版電子政府　電子政府構想の経緯と新アクションプラン』東京税理士会講演会資料、2001（非売品）

[3] 石井和平「信頼と情報　-情報社会における社会資本の意義-」『社会情報研究』No4、pp33-46、日本社会情報学会、2000

[4] ウォーウィック・フォード＋マイケル・バウム (訳：山田慎一郎)『デジタル署名と暗号技術』ピアソン・エデュケーション、1997/12

[5] 大貫直人・藤本一男「ディレクトリ・サービスの生かし方」『日経コミュニケーション』2000/3/6,pp172-177、3/20,pp170-175

[6] 岡野一郎『電子署名と電子ネットワーク上の個体性』第６回日本社会情報学会大会報告、2001/10

[7] 岡村久道『電子署名法の解説』http://www.law.co.jp/OKAMURA/jyohou/e-sign.htm

[8] カーライル・アダムズ＋スティーブ・ロイド (訳：鈴木優一)『PKI 公開鍵インフラストラクチャーの概、標準、展開』ピアソン・エデュケーション、2000/7

[9] Simon Garfinkel（監訳:山本和彦、訳:株式会社ユニテック）『PGP 暗号メールと電子署名』オライリー・ジャパン、1996

[10] 千葉隆之「信頼の社会学的解明に向けて」『年報社会学論集』第 9 号、pp211-222、関東社会学会、1996

[11] 辻井重男『暗号と情報社会』文春新書、1999/12

[12] 夏井高人『電子署名法　電子文書の認証と運用のしくみ』リックテレコム、2001/12

[13] ルドルフ・キッペンハーン (訳：赤根洋子)『暗号の攻防史』文春文庫、2001/1

[14] Wiener, Lauren Ruth, ”Digital Woes – Why We should Not Depend on Software”,1993, Addison-Wesley Publishing Company

[15] 山岸俊男『安心社会から信頼社会へ　日本型システムの行方』中公新書、1999/6

[16] 『電子署名・電子認証シンポジウム』資料集、同シンポジウム実行委員会、2000/2

[17] 藤本一男『電子申請を支える電子のハンコ=電子認証の仕組みと社会関係』東京税理士会講演会資料、2001（非売品）

■ 2002 年 2 月 12 日入稿