15－E008

ECの普及・高度化に関する調査研究

電子署名・認証利用パートナーシップ

(JESAP : Japan Electronic Signature and Authentication Partnership)

報告書2003

―活動と提言―

平成16年３月

財団法人日本情報処理開発協会
電子商取引推進センター

協力:電子商取引推進協議会

この報告書は、（財）日本情報処理開発協会電子商取引推進センターが競輪の補助金を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した事業の成果を取りまとめたものです。

国内の電子署名・認証にかかわる情報の共有や課題の解決と提言を行っていくため、関連する団体や有識者が参加する電子署名・認証利用パートナーシップ（JESAP）を平成 14 年 6 月に立ち上げました。

具体的な活動としては、情報共有や課題の解決のために開催する運営委員会活動と普及広報活動があります。運営委員会は、大山永昭東京工業大学教授を委員長とし、有識者と国内 PKI 推進に係わる団体からの委員、及び経済産業省、総務省、法務省、国土交通省、厚生労働省の PKI 推進関連部局からのオブザーバから構成され、今年度は 6 回開催しました。普及広報活動として、地方の団体と共催する講演会を 3 回開催しました。

今年度の活動は、2 冊の報告書にまとめました。1 冊は国内の PKI 推進活動の状況を紹介した報告書であり、もう 1 冊は、PKI 推進に係わる提言や JESAP の活動内容の紹介を著した報告書です。

本報告書は、運営委員会での議論を中心に、e-Japan 推進体制に対する提言、電子署名活用分野に対する提言、電子署名普及推進方法に対する提言、JESAP の活動紹介、及び、PKI 利用意識調査結果の紹介を行っています。

本報告書が、電子署名の利用を検討している企業、機関の方々にとって一助になることができれば幸いです。

平成 16 年 3 月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

運営委員会 委員名簿　［敬称略］

委員長	大山　永昭	東京工業大学
副委員長	黒岩　　惠	電子商取引推進協議会企画部会長
利用促進部会長	岩田　　彰	名古屋工業大学
連携・調整部会長	田尾　陽一	セコムトラストネット(株)

委 員	荒木　義晴	日本ベリサイン(株)
委 員	加藤　寛之	KPMG ビジネスアシュアランス(株)
委 員	桑原　　悟	新潟国際情報大学
委 員	西谷　研次	(株)UFJ 銀行
委 員	菅　　知之	関西大学
委 員	栗原　達雄	日本認証サービス(株)
委 員	鈴木　春洋	(株)中電シーティーアイ
委 員	鈴木　優一	エントラストジャパン(株)
委 員	岡田　雄樹	(株)東京三菱銀行
委 員	立川　雅章	(財)国際研修協力機構
委 員	坪田　幸司	東京電力(株)
委 員	牧野　二郎	牧野法律事務所
委 員	松本　　勉	横浜国立大学
委 員	松本　直人	(株)ネットアーク
委 員	牟田　　学	牟田学行政書士事務所
委 員	山崎　重一郎	近畿大学
委 員	米倉　昭利	(財)日本情報処理開発協会　電子署名・認証センター
委 員	喜多　紘一	(財)医療情報システム開発センター
委 員	光安　史枝	(財)金融情報システムセンター
委 員	大野　　実	全国社会保険労務士会連合会
委 員	石幡　吉則	電気事業連合会
委 員	池谷　千尋	電子申請推進コンソーシアム
委 員	寺川　　陽	(財)日本建設情報総合センター
委 員	田中　一志	日本税理士会連合会
委 員	佐藤　純通	日本司法書士会連合会
委 員	中西　　豊	日本行政書士会連合会
委 員	伊勢　禎和	(社)日本ネットワークインフォメーションセンター
委 員	安田　直義	NPO 日本ネットワークセキュリティ協会(JNSA)

オブザーバ	澤田　稔一	総務省 行政管理局
オブザーバ	名越　一郎	総務省 自治行政局

オブザーバ　赤阪　晋介　　総務省 情報通信政策局
オブザーバ　中垣　治夫　　法務省 民事局
オブザーバ　武末　文男　　厚生労働省 医政局
オブザーバ　武濤　雄一郎　経済産業省 大臣官房
オブザーバ　印南　朋浩　　経済産業省 商務情報政策局
オブザーバ　才木　　潤　　国土交通省 大臣官房
オブザーバ　星加　　司　　国土交通省 総合政策局

事務局
前田　陽二　電子商取引推進協議会
中川　宏之　日本 PKI フォーラム
小祝　香織　電子商取引推進協議会
川松　和成　電子商取引推進協議会

目次

まえがき

「電子署名・認証利用パートナーシップ（JESAP)」は、産、官、学、民が連携して、インターネット空間における安全・安心な情報インフラとしての PKI を普及するための体制として発足した。

これまで、政府、各地方公共団体、各業界団体、ユーザ企業等の組織ごとに進められてきた PKI の推進活動は、それぞれの分野において多大な成果を挙げ、一部は既に実用化に入っている。しかしながら、PKI が IT 社会における真のインフラとなるためには、相互の理解と連携が必須との認識から、関係団体間での情報共有と連携を図るための枠組み作りをスタートした。具体的には、2002 年 6 月 3 日に、PKI のユーザを中心に、30 名の民間、大学の有識者からなる委員と政府の PKI を推進している 5 省庁 9 つの部局の関係者で構成された第 1 回 JESAP 運営委員会を開催するに至った。

今年度は 6 回の運営委員会を開催し、多くの有識者から政府機関ならびに民間の活動状況が紹介されるとともに、相互理解を深めるための意見交換および議論が行われた。さらに、普及広報活動の一環として地方の団体と連携した講演会を 3 回と JESAP のフォーラムを 2 回開催した。JESAP のフォーラムでは、今後展開される公的個人認証サービスを中心テーマに置いた講演のほか、発表者を募る発表パートを実施し、好評を得ることができた。

本報告書は、活動内容の紹介と提言により構成されるが、事務局より、運営委員と部会員に個別に依頼して執筆していただいたものであり、提言については必ずしも運営委員会での合意を得たものではない。

第 1 章では、e-Japan 推進体制に対する提言として、政府や民間の推進体制と標準化に対する提言を紹介している。

第 2 章では、電子署名活用分野に対する提言として、士業分野をはじめとし、教育、医療、市民生活における利用についての提言を紹介する。

第 3 章では、電子署名推進方法に対する提言として、電子署名と実印を対応付けて説明することに対する課題、公的個人認証と属性認証との相互発展に関する提言、普及広報に対する提言を紹介する。

第 4 章では、部会における主な議論として、電子署名・認証の利用における疑問／不安、などを紹介する。

第 5 章では、今年の 1 月に行ったアンケート調査の結果を紹介する。

第 6 章では、15 年度の JESAP の活動概要を示す。

この報告書が、PKI の健全な発展と普及に貢献できることを期待する。

平成１６年３月

電子署名・認証利用パートナーシップ運営委員会

1．e-Japan 推進体制に対する提言

1.1　政府の実行体制の強化案

e-Japan の推進体制は、各府省情報化統括責任者（CIO）連絡会議、各府省情報化統括責任者（CIO）補佐官等連絡会議の設置など、府省間の連携も強化されつつあるように見える。

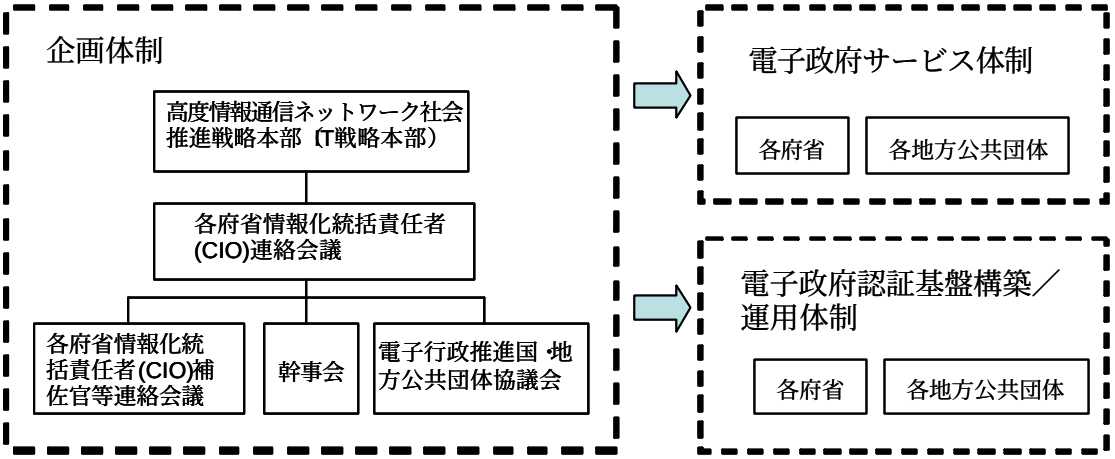

図 1-1 現在の電子政府推進体制（JESAP 事務局作成）

しかしながら、アクセンチュアの「電子政府進捗度調査」において 2001 年から 2003 年まで 1 位の座を守りつづけているカナダの電子政府プロジェクト「ガバメント・オンライン（GOL）」との比較で、推進体制で大きく違うところがある。それは、首相直轄のトレジャリ・ボード（予算庁）のトレジャリ・ボード・セクレタリアート「TBS（予算庁官房）」が予算を確保し、各省庁間に共通の機能やインフラの開発を行っている点である。かつ「TBS で電子政府にかかわる職員や、全省庁の CIO などの GOL プロジェクトの推進に深くかかわる人間は、全員、情報／IT の知識と経験を持つ IT プロフェッショナルである。日本のように CIO という肩書きだけを IT のバックグラウンドのない官房長や局長に押し付けることはない」（NIKKEI COMPUTER 2004.1.26　p81 より引用）といった点も注目に値する。このような体制のもとで、GOL の共通認証局（コモン CA）の運営や GOL の共通プラットホーム「セキュア・チャンネル」の推進などが省庁間共通で進められている。

そこで、今後下記の項目を省庁が連携して進めるためには、現在進めている体制の強化に加え、トレジャリ・ボード・セクレタリアート「TBS（予算庁官房）」に相当する実行組織を設立すべきではないかと考える。

（1）電子政府統合ポータルサイトのサービス機能の強化

国民が使いやすい官民連携の電子政府ポータルサイトの構築と運営

運営には、問い合わせの対応、広報活動を含む

（2）電子政府サービスの統合推進機能

電子政府サービスの各省庁・地方自治体が連携した推進と電子政府サービス全体に対する問い合わせの対応及び広報活動

（３）統合的な電子政府認証基盤の推進機能

統合的な電子政府認証基盤の設計及び運営

運営には、問い合わせの対応、広報活動を含む

1.2　官民の協力体制の強化案

平成 15 年 7 月、IT 戦略本部が「e-Japan 戦略Ⅱ」を策定した。その副題は、「IT の利活用による、「元気・安心・感動・便利」社会の実現を目指して」である。これは、IT 基盤整備の第一期が終わり、IT 利活用という第二期へと進むことを意味している。

それでは、具体的にどのような場面での IT 利活用を考えているのかと言えば、民を主役に官が支援する７つの先導的取り組みとして、

１ 医療、２ 食、３ 生活、４ 中小企業金融、５ 知、６ 就労･労働、７ 行政サービス

が挙げられている。ここで認識しておきたいのは、「行政サービス」は独立して存在するものではなく、１から６それぞれの分野の中に存在するということである。

そもそも、「行政サービス」を利用するのは、何らかの事情や理由がある。わざわざ面倒な役所の手続を行わせるのは、それ以上のメリットや必要性があるからである。多くの場合、それは生活をより豊かで安全なものにしたい、企業の活動を拡大し発展させたいといった利用者（市民、企業等）の願望から来ている。

それでは、果たして役所がそうした市民や企業の望むものを理解し、優れたサービスとして提供することができるであろうか。役所がービス提供者として素人であることを考えると、まずもって無理な話であろう。

政府が本気で利用者の視点に立ってサービスを提供したいのであれば､政府が持つ情報･知識を誰もが利用できるように公開して、民間サービスと行政サービスの垣根を低くすることが望ましい。

サービスはプロが行い、行政がそれをサポートし、必要な情報やノウハウを提供する。そうなれば、「行政サービス」だけが浮き上がることなく、利用者の視点に立ったサービスを提供するようになるはずである。

ところで、筆者は行政書士でもあるので、士業（法律関連のサービス業）の観点から、現在のオンライン行政サービスについて提言しておきたい。

現在のオンライン行政サービスは、「誰に使って欲しいのか」という点について、非常にあいまいである。全ての行政手続について、オンラインで誰でも（インターネット初心者の高齢者等でも）簡単に手続を済ませることができるなどという考えは、幻想に過ぎない。

一般市民にとって、生涯一度も利用しないであろう行政手続や、名前すら聞いたことがない役所はいくらでも存在する。だから、全ての手続ができる必要はなく、自分たちにとって関係がある手続が､見つけやすく使いやすくありさえすれば良いのである。もし､「誰に使って欲しいのか」を明確にしておかないと、誰にとっても使いにくいオンライン行政サービスとなってしまうだろう。

本人が簡単・迅速に、電子申請を初めとしたオンライン行政サービスを利用できるようになれば、手続を代理する士業などいらなくなるだろうし、そこを目指しても良い。自信を持って提供できるサービスであれば､「専門家に支払う費用を節約できます」といった宣伝も大いにけっこう

である。ところが、現状は、本人も代理人（士業等）も使いにくい中途半端なものになっているのである。

特許庁のパソコン電子出願は、インターネットも利用していないが、弁理士による利用率が非常に高い。それは、利用者のターゲットを明確にしたことと無関係ではないはずである。

「e-Japan 戦略Ⅱ」の IT 利活用を進めるにあたっては、
・行政は、サービスの利用者が誰であるかを考えること
・行政は、民間にサービスを手伝ってもらい、民間のサービスを活用すること
・民間は、行政が提供する情報等を自身のサービスに活用すること
の 3 点に注意することで、より利用者の視点に立ったものとなるだろう。

1.3 海外の PKI 関連団体との連携

(1) 国際標準化団体との連携

現在、国内で電子署名あるいは電子認証にかかわる標準化を取りまとめている機関はないように思われる。確かに、企業や団体が個々に米国や欧州で進められている標準化活動に参加している例は見受けられる。しかし、それらの企業や団体が、日本の代表として日本での多くの意見を吸い上げ、まとめているとは考えにくい。

EU では、強力に EU 内の標準化を進めている。電子署名あるいは電子認証にかかわる標準化については、下図に示すように EU 内の標準化団体の協力の下に EESSI を立ち上げて、成果をあげている。

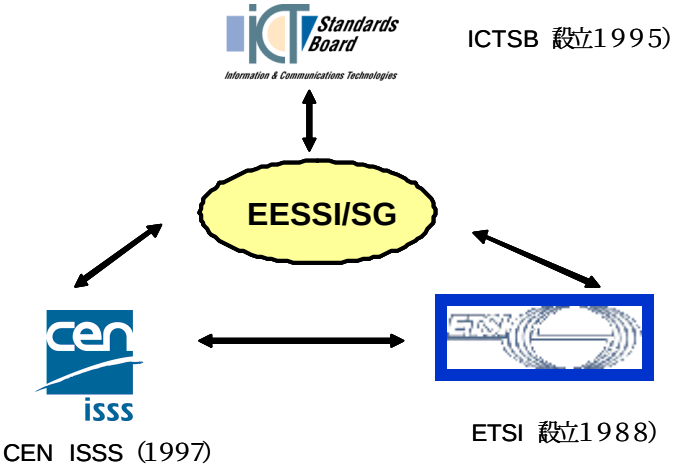

図 1-2 EESSI 関連の体制

① ICT standards board (http://www.ict.etsi.fr/home.htm)

ICTSB は、欧州の公的 3 標準化団体（CEN、CENELEC、ETSI）によって設立。

ICTSB の主な活動目的は、
・標準または仕様の要件を分析し、コーディネーションすること
・要件を標準化計画またはプロジェクトに移行させること
・最適な標準作成団体に作業を割り当てること

② CEN/ISSS（http://www.cenorm.be/isss/）

（CEN Information Society Standardization System）

ICT 活動を行う中枢機関として，CEN が 1997 年中頃に設立した団体。

CEN（Comite Europeen de Normalisation)は欧州における電子技術、通信技術分野を除く全分野の標準化を推進する目的で、1961 年に設立された組織。

③ ETSI（European Telecommunications Standards Institute）

1988 年に創設された非営利団体でヨーロッパの情報通信等の標準化団体。

テレコミュニケーションのすべての領域／無線通信、放送、および IT を含む。

（日本から、ARIB と TTC が参加）

今後、米国、欧州に続く第 3 極としてアジア域内の標準化活動を行うかどうかは議論があると思うが、少なくとも国内での議論は必要であろう。たとえば、JESAP が電子署名あるいは電子認証に関する標準化に係わる団体や機関とパートナーシップを組み、官学民が議論を進める場を提供するのも重要であると考える。

また、標準化に関する国際会議にも、技術面だけでなく政策面の話をする必要がある場合があり、こういった場合官民の協力が必要であると考える。

(2) 国際標準と国内標準

標準化を検討する場合、国際標準と同時に日本標準を確立する必要があると考える。日本の標準化を考え、かつ国際標準を考えるバランスの中で、日本のトータルの標準はできると考える。

PKI の利用は、日本国内で使われる割合は非常に高いと思われる。そこで、ただ国際標準にあわせるだけでなく、例えば商取引のときに日本の企業文化、商習慣があって、それを生かした日本国内での標準も検討すべきではないかと考える。

2．電子署名活用分野に対する提言

2.1　電子社会のビジョン

政府が 2003 年 7 月に発表した e-Japan 戦略Ⅱは、IT を駆使して無駄を排除し、日本全体の競争力を向上させる「構造改革」や、IT で新たな産業や市場を創出する「新価値創造」などを柱としている。そしてこれらを元に「元気・安心・感動・便利」な社会を目指すといったことがその基本理念になっている。同時に、2000 年から始まった e-Japan 戦略の成果としてブローバンドの普及などを挙げている。

ブローバンドの普及によりインターネットで大量の情報が交換されている。一方、そのブローバンドに流れる情報が、日本の競争力を本当に強化したのかというと、いくつかの疑問が浮かぶ。ブロードバンドの普及によって、多くの人々はインターネットなどのネットワークが便利なものであると認識したかもしれない。しかし、その便利さとは裏腹にネットワークセキュリティ上の様々な問題が表面化している。実際、ネットワーク上の脅威、リスクは、むしろ増加しているといえる。

インターネットのトラフィックが増加の一途をたどる一方、契約情報などといった、重要なトランザクションがインターネットを介してやり取りされることは、そのトラフィックの増加ほど増えていないのが現状ではないだろうか。現在のところ、従来において手書き署名や押印が必要であった契約書や受発注書類などが、電子データとして交換されることはまだそれほど多くない。ブローバンドなどの高速なネットワーク、ユビキタスネットワークなどの通信インフラは重要ではあるが、それだけで日本の競争力を高めるとは考えにくい。

情報セキュリティを確保し、安心してインターネット等を利活用できる環境を構築、そして電子認証・電子署名の整備がなされ、はじめて価値の高い情報がネットワークを介して交換されるようになると考えられる。整備された電子署名・認証が、ネットワークに流れるデータの価値を高め、結果として、日本全体の競争力に寄与することになる。

こうした将来の安心・便利なネットワークを考える上で、電子認証の重要性は比較的容易に理解できる。インターネットを介した電子認証は、特に企業においても広く受け入れつつある。企業経営においては、意思決定などのスピードが要求され、結果、いつでも、どこでも仕事が可能なことなどが重要な要素になっている。バーチャル・ワールドにおける情報交換が重要となるユビキタスネットワーク時代には、より安全で、使いやすい認証が要求される。ユビキタスネットワークと信頼のおける使いやすい電子認証は、「元気・安心・感動・便利」の基本的な要素となり、また、多くの「新価値創造」を産む可能性を秘めている。

電子署名の普及に関しては、まだ、多くの課題がある。例えば、電子署名を行った電子文書が民事裁判で押印や手書き署名を行った書類と同様な証拠になりうるということは、電子署名法などの法整備により確立しつつある。そして、これらの法律を前提とした多くの電子申請システムなどが既に開発されている。しかし昨今、これらが本当に利用されるのだろうかという疑問が多く発せられている。JESAP の中でも議論されてきたが、電子署名というものは、技術的課題への対応だけでなく、法律や制度の見直し、さらに電子データなどに対応した業務の最適化などが伴

って、初めて有効に機能することが分かってきた。これまでの紙と押印、手書き署名を前提とした社会と、電子データと電子署名を考慮した社会の間には、慣習や業務プロセスなどの面で大きな隔たりがある。これらを乗り越えることは非常に大きな課題であるが、来るべき社会が電子社会と仮定するならば、避けて通れない課題だと考えられる。

従来の紙ベースのモデルを、電子データや電子署名などを用いたものへ移行することで、既存のセキュリティ上の問題を解決することもできる。例えばこれまで、印影の複製は少なくとも世間では難しいと信じられていた。しかしIT技術は、押された印影から容易に印鑑を偽造することが可能にしてしまった。このようなIT技術の発達による紙ベースのセキュリティに潜む脆弱性を解決する事例として、世界的に重要な動きがいくつかある。その中のひとつに「電子パスポート」の導入がある。電子パスポートでは、ICカードに本人に関する情報が書き込まれるが、その情報の正当性を保証し改ざんを防止するために電子署名がなされることが検討されている。電子パスポートに限らず、これまで印刷技術に頼っていた偽造防止技術の多くは、今後電子署名技術に置き換えられていく、もしくは併用されていくと考えられる。

透明性のある電子社会の誕生のためにも、電子署名の普及は欠かせない。現在、押印や手書き署名がなされた様々な文書が紙で保存されているが、これらはいずれ、電子データによる保存に置き換わっていくと考えられる。こうした書類は、その場で契約などの各種手続きに使われるだけでなく、多くの場合、その先も長期にわたって保存されることになる。こうした書類が安全に保存され、将来何らかの紛争や監査の必要性などが生じた場合に、これらの文書は再び重要な意味を持つことになる。電子署名がなされた文書についても、全く同じライフサイクルが形成されることになる。電子署名の場合、長期にわたって保管していた書類に対する改ざん検知や否認防止といった強力な枠組みが用意されているため、紙と比べより透明性のある文書保管技術として注目されている。

現在、電子署名を利用した電子入札システムが数多く稼動し始めている。電子署名技術は、透明性・公平性のある電子入札を実現し、場合によっては第三者が入札プロセスを監視できるような仕組みを提供することが可能である。一般に、行政機関・公的機関などにおいては、業務内容について高い透明性が要求される。バックオフィスにおける業務の透明性確保のために、電子署名は大きな役割を果たす。

電子文書や業務プロセスの電子化を議論する上で、効率性も重要な要素である。公共機関や銀行等において、印影や署名の照合は最も重要な作業の一つである。しかしその反面、それらは非常に煩雑で時間のかかる作業である。また、本来一致していない印影・署名を一致すると見做したり、逆に一致しているものを棄却してしまうリスクもある。それに対して、電子署名やデジタルタイムスタンプなどの技術は、強力かつ高速に改ざん・なりすましなどを検知することができる。このように、電子署名は非常に合理的な手法ではあるが、現在の業務プロセスに電子署名を組み込んだからといって、すぐさま効率化が図れるとは限らない。むしろ多くの場合、電子署名を有効に利用するためには、業務そのものを変革する必要があると考えられる。

電子認証・電子署名は、企業内・公的機関内における効率化だけでなく、日本全体の競争力を高めるためにも重要な要素になる。IT化により、多くの企業が業務の効率化、そして現在最も求められている業務のスピードアップを達成している。同様に日本の競争力を強化するためには、事業者消費者間（B2C）、事業者事業者間（B2B）、事業者政府間（B2G）等の対外的でオープンな

関係の連携した業務プロセスのスピードアップと効率化を目指す必要がある。そして、対外的でオープンな関係の連携した業務プロセスには、電子認証・電子署名が欠かせない。このような目標は、単独の企業や単独の政府機関だけによる努力では成し得ない面がある。また、組織間の取決めをいかにするかといった非技術的な課題が多い。

対外的でオープンな関係の連携した業務プロセススピードアップと効率化といった課題の対応は、やはり電子政府が牽引車になることが期待される。現在の電子政府関連のプロジェクトは、個々の政府機関が予算を確保し、自組織の電子化を行なうための道具されている面があるように見える。しかしそれでは、電子政府共通の課題を認識することは難しく、実際、互いに整合性の取れていない電子政府の仕組みが出来つつある。これによって個別の政府機関の最適化・効率化が達成できる可能性はあっても、各企業・各政府機関を超えた全体的な最適化・効率化、すなわち日本全体の競争力を高めることにはならない。電子政府プロジェクトは、来るべき電子社会のデザインを念頭において実施されるべきである。

我々は今、電子社会の入り口にいると考えられる。既存の社会システムは、そもそも、電子社会を想定したシステムというわけではない。また、未だの経験のない電子社会を正確にイメージすること自体容易なことではなく、まだ電子社会のあるべき姿が十分に見えているとは言いがたい。しかし、来るべき「電子社会」をどのようにデザインするかといったとは、「元気・安心・感動・便利」な社会の構築や日本の今後の競争力に大きな影響を与えることは間違いない。こうした中で電子署名・電子認証の果たす役割は非常に重要なものがあり今後も更なる努力が必要になると考えられる。

2.2 電子署名の士業分野での活用について

2.2.1 日本行政書士会連合会

現在、世界規模で情報通信技術（IT）を活用した社会経済構造の変革が進展しており、IT の活用と普及が、あらゆる分野の発展基盤として大きな期待をされている。社会経済活動のネットワークへの依存度が急速に拡大する中で、国・地方自治体を問わず、各種の申請・届出等の手続きを電子化することによって、利用者の利便を飛躍的に向上することが期待されている。

このような「電子政府・電子自治体」の実現に寄与するため、日本行政書士会連合会でも各種行政手続の担い手として、行政手続等のオンライン化に係る基盤整備にも積極的に取り組んできた。当連合会では、1997 年から 1998 年にかけて実施された財団法人ニューメディア開発協会による「電子公証システムによるオープンマーケット等の創出のための実証実験」に参加し、その成果を受けて 1998 年 10 月に行政書士の資格を電子的に認証する認証局を設置し電子証明書の発行を開始した。これは、士業分野でも最初の認証局ということで各方面から注目を集めた。

また、当連合会では、2002 年 3 月より 1 年間、電子署名法による特定認証業務の認定を受けた認証局の運用を行っていたが、その後、新たに電子代理申請の実用に資するための認証局の構築につき関係各方面と調整を行い、2004年2月から、特定認証業務を行う日本商工会議所において、政府認証基盤（GPKI）に相互認証する行政書士独自の電子証明書の発行をスタートさせる予定である。

この電子証明書（タイプ 1-G）は、平成 13 年 4 月 1 日付で施行された「電子署名及び認証業務に関する法律」で定められた特定認証業務の認定制度に基づき、国の認定を受けているもので、日本行政書士会連合会が公式に認定し、推奨する唯一の行政書士向けの電子証明書で、行政機関等への電子申請が可能となっている。

電子証明書と秘密鍵は、認証局ホームページよりダウンロードにて取得できるので、IC カード格納タイプと比べて、特別のカードリーダ等が必要でなく、価格的にも低価格となっている点に特徴がある。

電子政府構築計画に基づいて 2003 年 7 月には、e-Japan 戦略－2 が策定されるにいたって、いよいよ各官公署における電子申請及び電子調達が身近になってきた感が強いが、行政書士が関与する行政手続きについても、2004 年には、電子申請の形が具体的に明示されるようになってきそうだ。

電子申請時には、「電子署名及び認証業務の関する法律」により、申請者の本人確認と申請データの「改ざん」防止のため、政府認証基盤と相互認証を行った認証局が発行する電子証明書を添付して申請を行うことが基本となっている。したがって、代理申請を行う時にも、電子上での代理申請システムの構築が責務となっている。その時に、申請者の真の代理人であるという確認のために代理人の電子認証の必要性がある。

民法上の代理申請の場合は、「住民基本台帳法に基礎をおく個人情報の認証制度」を利用して行うことで解決できるかもしれないが、我々が業務として行うためには、誰がどういう資格で申請を行ったかが問題となってくる。そのために、日本行政書士会連合会では、日本商工会議所の協力を得て、今回「行政書士」の属性認証を行う認証サービスの提供を始めるに至った。

今後は、国を始め、都道府県等の地方公共団体の電子化も本格化してくるため、あらゆる申請時における行政書士の代理申請において、この認証サービスが利用される必要があり、そのためにも、色々なメディアを通じて国、地方公共団体に対しての周知が急務となっている。

日本行政書士会連合会では、上記のことを踏まえて、今後、行政書士の電子上での代理申請システムについてのあり方や構築について積極的に周知活動を行っていく予定である。

※ 参照：行政書士電子証明書のプロファイル概要

記載情報	Subject	SubjectAltName
利用者の氏名又は旧姓名若しくは通称名	cn（ローマ字）	cn（日本語）
行政書士の職名及び登録番号	t（ローマ字及び数字）	t（日本語）
団体名（日本行政書士会連合会）	o（ローマ字）	o（日本語）
事業所等の名称又は屋号		ou（日本語）
事業所等の所在地		st、l（日本語）

注：「事業所の名称又は屋号」は、平成 16 年 8 月 1 日以降から記載となります。

2.2.2　全国社会保険労務士会連合会

現在、全国でおよそ 27,000 人が活動する社会保険労務士は、以下のような事項を主な業務としている。

○労働社会保険諸法令に係る官公署への申請書等届出書類の作成、手続き、事務代理、審査請求等の代理

○人事・労務管理・教育訓練・労務計画・監査などコンサルティング業務及び個別労使紛争解決のあっせん代理

○就業規則の作成・労働条件の整備

○安全管理の対策・衛生管理の対策

また、この度の電子申請に直接関係する労働・社会保険の加入・脱退、労働保険の年度更新、社会保険の算定業務、そして、労災保険、雇用保険、社会保険（医療保険、公的年金）の給付申請などの書類の作成・提出・事務代理・審査請求などを行っている。

労働・社会保険諸法令における申請・届出などの手続きは、52 本の法律に基づいており、その手続き数は 980 種類にも及び、これは国が扱う法令手続き全体の 7.2%を占める。このことから想定すると、社会保険労務士が関わる取扱件数は年間相当な件数にのぼり、電子政府のシステムが完全なかたちで施行された折には、労働社会保険の分野において、電子申請の推進にかなりの役割を果たすこととなろう。

社会保険労務士の顧問事業所は、主として中小・零細企業であり、その割合は、わが国の企業全体の 99.3%、内 73%が従業員 20 人以下の企業が占めている。中小・零細企業の割合が多い、このような日本の企業の実態からみて、電子申請に十分対応するだけの人材確保など、中小・零細企業は国が実施する電子申請に対応するために相当な費用負担も含めて苦慮を強いられることが想定される。

このようなことに鑑み、労働・社会保険に精通した専門家の社会保険労務士が中小・零細企業の電子化を補完することによって、労働社会保険関係分野における電子申請が円滑に実施できるものと考える。

すでにご案内のとおり事業主に代わって労働・社会保険諸法令の労働社会保険官公署への手続きを行える専門家は、社会保険労務士とされている。

このような現状と実態を踏まえ、十分に対応し推進するため、全国社会保険労務士会連合会においては、平成 10 年 11 月政府の高度情報通信社会推進本部発表の「高度情報通信社会推進に向けた基本方針」の発表を受け、平成 11 年 4 月に「電子化検討委員会」を設置し、平成 13 年 9 月には社会保険労務士独自の認証局を連合会において構築することを、理事会において決定した。

そして、平成 13 年 10 月、構築へのさらなる詳細な検討、電子申請に対する準備、会員への周知・研修のあり方など、その実施に向けて、電子申請部会、電子化対策部会を擁した「電子化委員会」を設置した。

全国6ブロックに2名の世話役を置き､その元に都道府県会に対応するための責任者を決めて、会員への周知・パソコンの取り扱い方をはじめ、電子申請一連のシミュレータを作成するなど、

実地研修を行ってきた経緯がある。

全国社会保険労務士会連合会認証局は、去る平成 15 年 6 月 10 日に特定認証業務の認可を得て総務省ブリッジ認証局との相互接続を終え、全国の社会保険労務士全員に対して、この連合会の認証を受けるよう一人一人にダイレクトメールを送ることにより申請手続きを受けるよう案内し、また一人でも多くの会員が認証を受けるよう都道府県社会保険労務士会とも密接な連携をとっている。

昨年 10 月より、労働社会保険関係手続きにおいて、電子申請のサービスが開始されたが、現行のその手続き関係の法律や政省令が紙ベースの内容になっていることから大きく 2 点ほど、問題が浮上した。

一つは、労働社会保険の手続きにおいて、事業主、その従業員被保険者、市区町村長、場合によっては民生委員など多数の届出の印、証明印が必要となったことである。電子申請においてはこれら印鑑を必要とするものすべての電子署名が求められている。

従って、たとえ、社会保険労務士が認証を受けて電子申請を推進しようとしても、これら印鑑を押す者が全員それぞれ認証を受けていないと出来ないことになってしまうのである。

労働社会保険は国民の生活の基盤の手続きであることを考えると、国民全員が認証を持っていなければ、電子申請の推進はできないことになる。すなわち、電子申請が思うように進展するには相当な時間を要することになると考えられるのである。

もう一つは、申請に必要な添付資料の問題が挙げられる。仮に申請書が電子申請可能となったとしても、それを証する添付資料だけを、行政機関に現在と同じように、出向いて提出するか、郵送するかの方法を取らざるを得なくなっている。

そうすると、現在申請書に添付資料をクリップでとめて、持ち込むか郵送していることからすると、電子申請においては、現行に比べ全くの二重の手数がかかることになる。

これらのことは、申請側にとっても手数のかかることと同時に申請を受ける側の行政機関における事務の効率化という視点においても、現行と比べかなりの影響出ることが想定される。

労働社会保険諸法令分野においての電子申請の円滑な進展及び行政機関での事務の効率化への働きかけとして、私ども社会保険労務士は、士業としての国家資格者として、社会保険労務士独自の認証を受けた社会保険労務士が電子申請を行うということについては、複数署名あるいは添付資料などの省略が行えるよう現行の法律あるいは政省令の改正を臨んだ手当てを大いに望んでいるところである。

電子申請の進展にともなう社会保険労務士の業務の変化・影響という問題については、労働社会保険諸法令は、ご案内のとおりかなり法体系が複雑化してきている。そのなかにあって、社会保険労務士はこの法体系の専門家であって、行政機関への書類の作成や手続きのみならず、労使関係・労働条件・労働環境・教育訓練・労務監査・個別労働紛争解決など広い分野で活躍しており、今後のこれらの情勢には社会の進展とともに複雑化するなかにあって、益々要請されることになろうかと考えている。

今後、労働社会保険分野において社会保険労務士を活用していただくことによって、中小・零細企業への関与率も高まり、また、電子申請の進展にも、あるいは行政事務へも貢献できるものと信じている。

2.2.3 日本税理士会連合会

日本税理士会連合会は、政府の「e-Japan 重点計画に２００２」等により電子政府実現の一環として本年２月から開始された「国税電子申告・納税システム」に対応すべく、電子認証局を立ち上げ税理士証明書発行サービスを開始した。

本サービスは、主務大臣（総務大臣、法務大臣、経済産業大臣）より、電子署名及び認証業務に関する法律第４条第１項に規定する特定認証業務として認定されたものである。

また、本サービスは、「国税電子申告・納税システム」において利用可能とするため、政府認証基盤のブリッジ認証局と相互認証を行っている。

日税連税理士証明書発行サービスの概要

(1) 認定取得日　　平成１６年1月１６日

(2) 特定認証業務の名称　　税理士証明書発行サービス

(3) サービスの内容

税理士法（昭和２６年6月１５日法律第二百三十七号）の規定に従って日税連に備える税理士名簿に登録された者に対して､公開鍵暗号技術に基づく電子証明書を IC カードに格納し発行します。本サービスを利用できるのは、税理士に限られます。

(4) 電子証明書の利用範囲

①税理士法第２条に定める事務（税務代理、税務書類の作成等）

②自己の申告に係る行政機関への申告、申請届出等（ただし、電子証明書に記載する氏名が旧姓の場合を除く。）

③日税連または税理士会への申請、届出等

(5) 日税連税理士証明書発行サービスのシステム構築

本サービスは、株式会社 NTT データ、日本電気株式会社及び凸版印刷株式会社の協力を得て構築運用する。

2.2.4 日本司法書士会連合会

(1) 登記申請のオンライン化と PKI の必要性

司法書士業務のうち大きな比重を占める登記申請の代理業務について、インターネットを利用した申請手続のオンライン化は、電磁的記録の提供・交換によるため、従来の紙の書面を前提にした制度とは全く異なった観点からの検討が必要であった。

登記のオンライン電子申請化にあたりどのような問題をもたらすかを個別に検討するために、法務省では平成 13 年より「オンライン登記申請制度研究会」を設置し、「電子商取引を円滑にし、社会・経済活動のネットワーク化を推進し、もって経済を活性化するために、不動産登記申請及び商業登記申請のオンライン化を推進するための法制面及び技術面の調査研究を実施する」ため調査研究を進め、日司連も委員を派遣し、検討に参加し意見を提言してきた。

オンライン申請の導入を図るための法制度の検討は、技術面の調査研究の検討と表裏をなすものであるため、先端技術の導入のためには既存の法制度そのものを大幅に変容せざるを得なくなり、結果として１００年以上続いてきた我が国の不動産登記法の真正担保制度の原理を抜

本的に見直す必要が生じた。今年の通常国会に不動産登記法改正が上程され審議中であるが、法案成立後には平成１６年度末には施行の予定である。

「申請者等の認証」については、申請人の「実在性の確認」ならびに「申請意思の確認」をどのように行うのかという問題になる。

実在性については、法人の場合は、登記されている法人であることの確認が、個人の場合は、登録されている住民であることの確認が必要となる。

意思の確認については、電子データの作成名義人本の意思によるものであることを証明できることが必要となる。また、電子データの特質から改ざん防止の完全性が求められる。

申請人が法人の場合は、商業登記に基礎を置く電子認証（法人電子認証）がすでに平成 12 年秋から実施されており、個人の場合には、住民基本台帳制度に基礎を置く住基ネットワークにもとづく公的個人認証サービス（個人電子認証）が平成１６年１月 29 日より都道府県において開始されたところである。

登記の申請の代理を業とする司法書士が代理人としてオンライン申請する場合には、司法書士の資格を電子的に確認できる仕組みが必要となる。

特に今般の不動産登記法改正において、従前の登記済権利証に代替する「登記識別情報」の提供ができない場合の特例として、「登記の申請の代理を業とすることができる者」（司法書士と弁護士のみ）が代理人となって登記申請をするときは、登記義務者の本人確認につき内容が相当な情報を提供したときは、登記所による「事前通知制度」は適用されず、そのまま登記手続が進められることとなることから、電子データの中で司法書士の資格を確認できる仕組みが必要になる。

そこで、日司連は、電子認証局（資格属性の電子認証）を構築し、「登記義務者本人確認情報」ならびに「登記原因証明情報」その他の添付情報への電子署名を可能とする仕組みを設けるために設置の準備をしてきた。

(2) 日司連電子認証局の取組みの考え方

申請手続きが、オンライン電子申請によることとなっても、紙による書面申請の場合と同様に、登記される権利の真正性の確保が必要であることは言うまでもなく、登記制度の目的たる「取引の安全」に資するための公示制度の信頼性を確保するためには、申請手続きに関与する専門職の果たす役割は、今後さらに重要になる。

また、不動産取引において、複数の契約の同時履行を保証するためには、利害が相対立する複数の当事者から公正な第三者として双方代理の委任を受けて数個の登記申請を一括連件申請注する必要は今後も変らず、司法書士職能に要請される独自の職務領域である。

（注）中古住宅売買の場合の①売却物件に付いている既存担保の弁済による抹消登記、②負担の無い状態での所有権の移転登記、③移転された所有権に新規の住宅ローンの担保設定等の複数の登記と代金の支払いの同時履行を確保する要請を司法書士が担っている。

司法書士が代理人としてオンライン電子申請する場合において、登記の安全性と確実性を担保するため、ならびに専門資格者として一定の権限を担うためには、司法書士の本人確認と資格証明（属性認証）が必要となる。具体的には、登記申請の資格の有無の確認、登記受理通知・登記完了通知証の受領、登記識別情報の代理受領等において必要である。

司法書士資格の登録ならびにその証明事務は、司法書士法第８条によって司法書士の会員登録事務を行う日本司法書士会連合会が行うものであるから、司法書士資格の有無の属性を証明する電子証明書の発行は、資格登録権者である日司連のみができるものである。

上記の点は、他の専門士業においても同様に考えるべきであろう。仮に、民間の認証局で発行する電子証明書に司法書士資格を記載してもらうとしても、発行時において、その資格の有無の事実確認のため資格証明書を添付させるか登録機関への照会などの調査確認しかできない。発行の後もその資格が継続して有効であるか否かの証明には限界がある。すなわち士業団体からの退会や業務停止などの事由があった場合、これらの事由を本人が届けない限り民間の認証局ではそれらの事実を把握することはできないので、発行後の資格の喪失または停止については証明ができないという限界があると思われる。

日司連が自ら電子認証局を設置し、登録事務に連動した会員の本人確認と資格者証明を行うことにより､資格喪失者や業務停止者がある場合は直ちに電子証明書を失効させることができ、常に会員の資格の得喪変更を電子的に反映できる仕組みを保証できることとなり、法務局と利用者たる国民に資格者によるオンライン電子申請が安全かつ確実に行い得ることの信頼感を与えることが可能となる。

(3) 電子認証局のシステム再構築のねらい

今年６月から実施される商業法人登記のオンライン電子申請システムならびに来年の３月までには開始される予定の不動産登記オンライン電子申請においては、法務省から提供される申請アプリケーションソフトには代理人による申請の場合の仕組みもシステムに組み込まれることになっているが、法務省オンライン電子申請手続きに対応できるためには、電子署名法による特定認証業務の認定を取得する必要ならびに政府のブリッジ認証局（GPKI）との相互認証が可能となるシステムとすることが必要となる。

日司連の新しい電子認証局が政府のブリッジ認証局と接続することにより、オンライン登記申請においては、具体的には、現在の官公庁発行の添付書面等の電子データの授受、国庫金納付システムとの連携、登記受付通知の受領、補正確認・却下通知の受領、登記済証に代わる登記済データの授受等々において、代理人資格の電子認証が重要になる。他にも今後予定される裁判所への訴訟申立、督促手続申立、競売申立・入札等の各種の電子申立や、地方自治体への戸籍・国籍手続き等、登記以外の関連業務も電子申請化されてくることを踏まえて、自治体が平成 15 年から運用開始した公的個人認証サービス､ならびに商業登記所の法人電子認証等との相互連携において拡張性を持たせた柔軟なシステムの構築の可能性が出てくる。

(4) 司法書士業務における PKI の活用

日司連が自ら電子認証局を設置する制度的な必要性については、不動産登記法改正との関連からの必要性と商業登記を含めた電子文書作成にあたっての必要性、ならびに民事訴訟法改正関連からの必要性が挙げられ、そこに司法書士業務における PKI の活用がある。

１）資格者代理人による「登記義務者申請権限確認報告」制度の創設。

改正不動産登記法案では、登記識別情報の提供がない場合、資格者代理人から本人確認報告情報の提供があり、それが登記官によって相当と認められれば、別途に登記所による事前

確認手続きを経ずに登記を行う旨の改正提案がなされている。この制度は資格者代理人（司法書士と弁護士）に限って認められることから、当該代理人が適格な資格者であることを担保する手段が必要となる。

2）登記識別記号の有効性検証

また、改正法は、登記済証の機能に代替するものとして「登記識別情報」制度を導入する。この登記識別情報とは英数字の組み合わせによるパスワードであるから、その登記識別情報が当該不動産の登記名義人に交付された正当なものであるか否かは見ただけでは確認する術がないので、取引の相手方や代理人は有効性の確認ができないかぎり安心した取引は事実上できないことになる。そこで、改正法は、法務省のオンライン申請システムを経由して登記申請の事前に登記識別情報の有効性の検証ができるシステムを用意することとしている。代理人司法書士が確認のため申請する場合には、登記申請委任状に登記識別情報の有効性検証の旨の委任事項を記載したものを利用することが想定されるので、登記申請代理権限がある資格者であることの電子証明書が必要となる。

3）登記原因証明情報制度の創設ならびにその他の電子文書の作成

改正不動産登記法により新たに導入される登記原因証明情報は高度な法的文書であり専門性を要求される文書であるので、司法書士が職務上作成する登記原因証明情報の書面には、司法書士法及び司法書士法施行規則の規定により、作成司法書士の記名押印が必要となる。電子的に作成された登記原因証明情報については、司法書士の電子署名を必要とする旨の改正がされる予定である。同様に、商業登記ならびに裁判事務等においても司法書士が作成した電子文書には司法書士であることの資格を確認できる電子認証の仕組みが必要となる。

4）公的個人認証の有効性確認

公的個人認証サービスについて、現行の公的個人認証法では資格者を含め民間からの有効性検証をする方法は現時点では認められていない。したがって、司法書士が受託する事件において電子署名・電子証明書の有効性を事前に確認する手段がなく、実務上に大きな不確定要素が生じる。

こうした指摘を受けて公的個人認証に関する法改正を総務省担当部局にも申入れ中であり、不動産登記法の施行までには改定されるべきものであるが、法改正後においても個人資格者が直接に都道府県の電子認証局に有効性検証を求めることは認めるべきではなく、法律上守秘義務を課せられた専門職団体が、電子署名法にもとづく特定認証業務の認定を受け、かつ政府電子認証基盤との相互接続可能な認定を受けた認証機関を経由してのみ検証できるものとする制度設計がされるべきであろう。

5）民事訴訟法改正によるオンライン申立制度の導入

民事訴訟法改正により、簡裁の督促手続のオンライン申立が可能になるように電子申立制度の導入が最高裁で準備されている。司法書士法改正により簡易裁判所における代理権の認定を受けた司法書士は代理人として申立を行うことになるが、その場合に電子上で司法書士であることならびに認定資格者であることの証明ができる仕組みが必要となる。

司法書士の資格認証はもちろんであるが、簡裁代理関係業務の認定を受けた司法書士であることもまた日司連のみが資格認証できる唯一の団体であることから、日司連の電子認証局の構築が必要となる。

2.3 教育分野

我が国の大学教育の見直しがさけばれるなか、魅力ある教育形態を模索して、大学間の競争と同時に相互の協力・協調関係に根差した住み分けや差別化の方向も検討されている。また一方で、いわゆる e-learning の範疇の技術的成果を利用したさまざまな施策が実現可能な段階をむかえている。

実際に、インターネットを利用した大学間の授業交換やこれに基づく単位互換、留学先から在席本校の遠隔講義を受講し、在籍本校を休学することなくできる海外留学、距離的、時間的制約を克服するための社会人向け専門大学院のオンライン授業などが検討や試行から実施の段階をむかえようとしている。これら遠隔地をネットワークで結んだ教育の実施に当っては、受講時のアクセス管理や、授業で与えられた課題提出時の本人確認、参加申込み時の資格確認、修了後の単位認定、成績、卒業なども安全、確実、快適に行われる必要がある。

これを実現するインフラストラクチャとしては、PKI の利用が最も妥当であり、形態としては PKI を利用したオンラインで利用できる学生証を導入することが、技術的な実現性と利用者すなわち学生と大学の自然な理解の点からも最も適していると言える。

もちろんここにも、PKI を利用したアプリケーションの課題があてはまることになるが、第一に、教育、研究、社会貢献を目的とする教育機関が中心であるため、過度な商業主義的競争や排他的な施策など、新しいパラダイム具現化の初期に起こりがちで発展の芽を摘んでしまうような類の障害を避けることができること、第二に、利用者、特に若い世代を中心とした学生は、好奇心、探究心が旺盛であるので、新しいものに対して柔軟であること、第三に、管理する資格や権限などが教育に関するものであり、直接的に広く一般の金銭的価値への転化がなされないので、未知の問題が発生しても影響範囲と対応が限定的ですむ可能性が高いことなど、この分野での PKI の利用は、停滞ぎみの PKI アプリケーションの突破口になる可能性もあると言える。

このオンライン国際学生証（仮称）の構想として、国際的な展開を目指し、国内、海外の大学間で連携でき、インターネットを用いたアプリケーションにも使用できる、アクセス管理とオンライン電子署名及び検証のインフラの実現を目指すことを提唱する。

この構想の実現のためには、必要な制度、運用及び技術インフラについて国内、海外の調査研究を行うことが必要となる。具体的な調査研究の項目としては、次があげられる。

○制度と運用関連の項目
- ①国際的合意／制度の実現可能な形態
- ②CA の位置付けと CP、CPS
- ③各大学で必要となる、規則、運用管理など
- ④参加各校のコンプライアンスと検証の現実的形態

○技術インフラとシステム関連の項目
- ①CA、認証サーバ、ディレクトリ、CRL など
  （自前の構築とアウトソーシングの考え方）
- ②オンライン学生証の発行、配布、利用環境

（IC カードなどの保管媒体と PC インタフェース）

③アプリケーションにおける署名／検証の実現

（S/MIME 利用、他）

この調査研究の成果を得て、当初は小規模実運用環境の構築を行い、パイロット運用・評価を行って本格的展開に発展させる。

この構想を、我が国主導で国際的に共通な枠組みとして実現することは、PKI の発展と我が国の大学教育への大きな寄与及び国際的な貢献であると言える。また特に我が、国のアジア圏の各国と協調し、アジア発の国際的規模の IT 技術関連の活動を行うことは、PKI のみならず、わが国を取り巻く環境での今後の IT 社会の発展にとって重要であり、意義深いものと言える。

2.4 医療分野

医療分野においては、2001 年 12 月に厚生労働省から出されたグランドデザインの中の５つのアクションプランの一つである「情報化のための基盤整備の促進」によれば、「個人認証ならびに資格認証」として、「診療に関連した情報がインターネット等によって安全に交換できるためには、公開鍵インフラストラクチャ（PKI）などの認証に関する社会的基盤が必要である。現在、政府機関の間にはこのような社会的インフラストラクチャが整備されつつあるが、医療は、公的機関と私的機関が混在する世界であり、医療の世界で用いる「医療公開鍵インフラストラクチャ」が必要である。そのため平成１５年度までに、認証に関する社会基盤をどのように整備していくか、その方向性と計画を明らかにすることとする。」とされている。

また、「電子認証システムの構築」として「電子カルテやオーダリングなどを用いネットワークを介して医療行為を行う際には、医師等の医療従事者の資格確認を厳密に行う必要がある。また個人情報保護の観点からも権限のある人のみが患者情報を見られるようなシステムを構築しなければならない。これらのシステムを構築することは喫緊の問題であり、平成１５年度までに医療分野における電子認証システムの仕様やガイドラインを作成することとしている。」とされている。

また、2004 年 2 月に出された、「e-JapanⅡ加速化パッケージ」においても「IT 規制改革の推進」の中で「これまでの制度の IT 化と比べ、IT 化が遅れている分野の早期規制改革」として、「診療情報の電子化など医療分野での IT 利用促進」をあげ「医療の質の向上と効率的な医療提供体制の構築に向けて、処方せん、診断書、出生証明書をはじめとする様々な診療情報の電子化など医療分野の IT 利用促進を図るための方策を包括的に検討し、2004 年９月までに結論を得る。(厚生労働省)」としている。

また、同、「現実世界の制度とサイバースペース上の制度で整合等を図る必要のある規制改革」としても「電子的手段による資格保有等証明の推進」の中で「重要情報のオンライン転送にあたり、医師、弁護士等の本人性、資格保有等の証明を電子的にできるようにするため、既存認証制度に対する属性情報追加等のニーズ把握を早期に行うとともに、制度の在り方について検討し、2004 年中に結論を得る。(内閣官房、総務省、法務省、経済産業省及び関係府省)」とし、医師資格保有の証明の検討をあげている。

これらと平行して厚生労働省では 2003 年 6 月より「医療情報ネットワーク基盤検討会」を開催し、「電子化された医療情報を個々の医療関係機関を超えて活用すること（地域における医療情報ネットワーク構築）についての基本的な考え方」、「医療情報の安全な伝送・参照のためのセキュリティ技術の活用策」、「患者・国民の視点に立った医療情報ネットワーク運用のあり方」あるいは「技術活用面、運用面での適正を期するための基盤整備のあり方」を検討事項とし、平成１５年末までに中間的なまとめを行い、平成１６年夏頃までに一定の結論を得ることを目標としている

現在までは「書類の電子化」、「公開鍵基盤」および「診療録等の外部保存」の観点で検討を行っている。公開鍵基盤としては電子政府・電子自治体への電子申請に対して添付書類としての診断書の電子化が要求されていることを踏まえ、当面、医師は「公的個人認証サービス」を用いるか、「民間の認定認証業務を行う認証局から発行される電子証明書」を使用して電子署名をおこなってはどうかとの検討を行っている。

この方式は、紙の診断書は診断書の記述項目として医療機関名、住所および医師名を記述し押印を行っていて、印鑑そのものには医師を識別する情報を持たせず、疑義がある場合は関係先へ問い合わせて連絡して確認できることを前提としている現状の運用と変わりないとするものである。しかし、電子化することにより、間接的な人的、物理的確認による規制がかかりにくくなるのと、資格確認が即時にできることが電子化の主旨である即決性からも要求されるので資格確認ができる電子証明書を発行・運用できる基盤を整備していくことが望ましい姿である。

また、公的個人認証サービスの電子証明書を用いる場合は、デジタル診断ファイルに民間で開発したシステムの中で署名をするために個々にプログラム開発をする必要があり「公的認証サービスの電子証明書」にアクセスするためのプロトコルを開発者に公開するか、現在、公的個人認証クライアントソフトに付属されているような医療専用の診断書署名プログラムを公的に提供する必要があり、現状では制約がある。また、公的個人サービスは電子証明書として「氏名、性別、住所、生年月日」の４情報が公開されるので、印鑑方式に比較して、個人情報保護上、問題があることを認識しておく必要がある。

民間医療施設間で交換されている書類の例として紹介状は印鑑を要求されているために現在、電子化が認められていなが、電子署名の導入により電子化の可能性がでてくる。この場合、国際規格である ISO/TS17090 に準拠したヘルスケア PKI の構築が検討されている。これは拡張領域の「subjectDirectoryAttribute」の［hcRole attribute］に医師等の資格を記述するものである。こうした証明書は電子政府・電子自治体への電子申請にも使用できることが望ましい。

（社）日本医師会で認証局は「医師会総合情報ネットワーク構想」を構成するツールの一つとして認められた研究事業プロジェクトである「ORCA プロジェクト」において計画されている。その最初の端緒として「ORCA プロジェクト」で認証局を立ち上げ、「日医標準レセプトソフト」のデータをセンターサーバーにバックアップする「バックアップサービス」から認証を開始している。詳細は http://www.orca.med.or.jp/certificate/index.html に公開されている。

また、（財）医療情報システム開発センターでは医薬品副作用情報収集システムに用いるための電子証明書を発行している。これはオンライン副作用報告を法人代表者名で行うことを義務づけているため製薬会社の法人代表者に対して発行された S/MIME 用の証明書でなければならないため、従来の認証局では発行された証明書を使用できなかった。詳細は

http://www.medis.or.jp/6_pki/index.html に公開されている。

また、医師等の公的資格の認証のための電子証明書に関しては、（財）医療情報システム開発センターにおいて ISO/TS17090 に準拠したヘルスケア PKI の構築を平成１４年、１５年と経済産業省の委託事業として実証試験を行っている。実証実験の「医療用公開鍵基盤ガイドライン」および「ヘルスケア PKI 認証局証明書」は暫定版として
http://www.medis.or.jp/6_pki/file/hpki_cp.pdf に公開されている。

医療の世界で信頼される「医療公開鍵インフラストラクチャ」を構築し、電子証明書の互換性を確保するにはヘルスケアドメインとして証明書のポリシーが一致し、その運用が信頼される必要がある。現在、厚生労働省を中心に進められている「医療情報ネットワーク基盤検討会」を通じてコンセンサスが形成され、方向付けされつつある。

2.5 市民生活

情報化社会の浸透に伴い、市民生活の中で情報セキュリティの必要性は高まっているが、しかしそれがフォーカスする問題そのものも変化している。これまでは、自宅やオフィスから居ながらしてインターネットを介して世界中のサービスにアクセスするというモデルの中で、本人認証の問題への対策として PKI の必要性が語られることが多かったと思う。しかし、市民生活の中の情報通信の環境は、パソコンから携帯電話へと大きくシフトしたと言ってよいと思う。この流れは、さらにユビキタス情報化社会という方向を示すものだと思うが、そこで深刻さを増しているセキュリティの問題は PKI が従来想定していた問題と違ってきている。

本節では、主に携帯電話を中心にしたユビキタス情報化という流れの中の市民生活の情報セキュリティに重心を置いて、その中で特に潜在的に高まっている個人情報保護と著作権問題に関連づけて、改めて PKI が必要であることを提言する。

(1) ユビキタス情報化

オフィスや家庭のような場所にパソコンがあるだけでなく、携帯物、市街、建物、交通機関、流通する商品の中など我々が生活するあらゆる環境の中に情報機器が遍在するユビキタス情報化は、着実に市民生活の中に浸透しつつある。例えば、携帯電話、非接触 IC カード、2 次元バーコードとカメラ付き携帯電話、RFID といったものは、すでにパソコンに近いかあるいはパソコン以上に我々の生活に身近なものになってきている。

携帯電話は、もはや音声通話のための機械というよりも、ショートメッセージによるコミュニケーションの機械になったと言ってよい。そして携帯電話はさらに多機能に進化し、デジタルカメラの画像の交換、GPS ナビゲーション、音楽配信、書籍の配信、電子決済などのサービスの端末などにもなろうとしている。

また、非接触 IC カードは、JR の suica に代表されるように交通カードを中心に、携帯電話に負けないくらい多くの利用者を獲得しています。さらにほかにも、無線 LAN によるホットスポットサービスが全国に広がり本格化し、私たち市民の日常生活をおくるいたるところに情報通信の機器が存在しているという環境ができつつある。

(2) ユビキタス情報化とビジネスチャンス

このユビキタス情報化は、一つの大きなビジネスチャンスである。インターネットのビジネスで

の利用は、すでに当然のことになってきているが、次の段階はこのユビキタス情報環境を自分のビジネスにどう活かすかということが勝者になるための鍵になっていると言ってよい。

例えば、インターネットの利用人口で言えば、パソコンからの利用者よりも携帯電話の利用者の方に軸足が移っている。そうであればビジネスマンとして、携帯電話の利用者を消費者として認知し、それをターゲットにした戦略をとることは当然のことである。

しかし、ユビキタス情報環境での利用者の行動は、自宅やオフィスのパソコンからインターネット利用している環境での行動と大きく違う。ですから、単にパソコン用のコンテンツの携帯電話版を作成したからといって、それで利用者が増えることは望めない。例えば携帯電話で興味にまかせてネットサーフィンする人はとても少ない。

ユビキタス化のポイントは、利用者が何時どこにいるのか、利用者は今何を欲しているのかといった利用者の属性と利用者の「いま」の時空位置などのコンテクストにフィットした的確なサービスの提供である。

小田急では、昨年から利用者が定期券を自動改札に通した「時刻と位置」と利用者のプロフィールに応じて携帯電話で広告を配信するグーパスというサービスを本格的に開始した。

お昼ご飯の時間にある若者がある駅で下車したときに、その駅前にあるファーストフードショップの新商品の情報が携帯メールに飛び込んでくれば、その店に入る可能性はかなり高い。そしてさらにもしその人のこれまでどのような昼食をとってきたかといった消費行動の履歴があれば、その広告メールの的確度はさらに向上する。そして実際にそういうことも全然不可能ではない。例えば会員カードを使った割引クーポン発行情報で個人の消費履歴を追跡することは簡単である。

(3) 利用者の属性と行動予測に基づくサービス

このような消費者の利便性の向上や経済的合理性のあるサービスは、好むと好まざるとによらず遠からず登場し、企業間の競争原理の中でより精度の高い効率の良いものに洗練されていくであろう。そして、その洗練の方向性として最も蓋然性が高いのが、サービスの個人適応と個人行動の予測である。例えば、アマゾン・コムである本を買った人はこの本も買うのではないかという予測サービスをするが、こういう統計的な傾向分析と個人行動の履歴を高度に結合したサービスが登場するであろう。

例えば、ある時間にある駐車場に車を止めある映画館のある映画を見た人は、次にはこういう場所のこういうレストランに行くだろうといったような予測ができるようになると、そういう情報を持たない商店街と持っている商店街とでは圧倒的な差がついてしまうであろう。

また、このような利用者の個人的な属性の把握や行動予測は、障害者や高齢者のための福祉サービスなどにも非常に有効である。その人がどのような障害を持っているのかという属性の認識と、これからその人がどのような行動をするのかという予測ができれば、障害に対応した介助サービスの提供や行く先々で事前の準備ができるので、ストレスなく行動することが可能になるであろう。

(4) 著作権管理と個人情報

現在の著作権管理技術は、個人情報保護のことをほとんど意識していない。むしろ誰がどの音楽ソースをいつ聞いたか何回聞いたかなどの情報を正確に記録しそれを確実にチェックする機構を一生懸命実現しようとしているのが現状である。

音楽産業における CD の売り上げは年々減少しているが､逆にインターネットを使ってダウンロ

ードで音楽を購入するというケースは増えている。携帯電話の着メロの購入もたいへんポピュラーになっている。こういう著作物のネット購入の裏側ではたいへん複雑な著作権管理機構が働き、確実に個人情報が収集されている。ひょっとするとすでに「こういう着メロを使っている人」というプロファイルによって私たちは分類されているかもしれない。少なくともこういう情報が次の段階としてマーケティングに利用されるようになるのは間違いないであろう。

また、ソニーのテレビの cocoon のように、どのようなテレビ番組を見てきたかという履歴から予約する番組のサジェスチョンをするという利用者適応機能を備えたものが出てきている。もちろんこういうサービスも携帯電話やインターネットとリンクしている。テレビ番組の視聴の傾向の分析ができると、それをもとにテレビコマーシャルも利用者に適応させることが可能になり、より効率的な宣伝が可能になるであろう。

(5) プライバシー・クライシス

しかし、一方で、これらは個人の行動を高精度で追跡や予測することを可能にする恐怖の技術でもあり、プライバシクライシスを起こしかねない。

自分がデートでどのような行動をするのか詳細な行動履歴をとられるのは嫌だな恥ずかしいなというレベルであるし、本当に嫌ならそういうサービスの利用を止めればよいのであるが、こういう情報が本人にコントロールできないところに流出すると非常に恐ろしいことになる。

例えば、警察による犯罪捜査にこのような情報を利用できることになると、行動予測は「犯罪の予防」という方向に進んでいくかもしれない。

どのようなビデオを見てどのようなものを購入してきたかという履歴から、知らないうちに犯罪者予備軍のリストに入れられてしまうかもしれない。

さらに、そのようにして集積された情報が悪意の第 3 者の手に渡った場合、ストーカー、脅迫、詐欺などの犯罪は容易になるでしょうし、さらに本人の行動予測に基づいた非常に巧妙な罠を使った犯罪まで考えられるかもしれない。危険な政治団体や宗教団体にそのような情報が渡ったらどうなるか想像するだけでも恐ろしい。

これまで日本では、個人情報が非常に安易に取引されていました。子供が生まれたとたんにベビー用品のダイレクトメールが来たり、子供が学校に進学すると受験産業からのダイレクトメールが来るといったことは珍しくもないことである。

ツタヤでドラえもんのビデオを借りたら、車のディーラー主催のドラえもんショウのダイレクトメールが届いたということで訴訟が起きたことがありますが、顧客情報を十分に持たない企業が個人情報業者のデータベースを利用する「ブラインド・レンタル」や顧客層が近い業者同士が違いに顧客情報をバーターする「リスト・スワップ」といったものも日常的に行われているそうである。

ユビキタス情報化によって得られる個人情報は、GPS による現在位置や交通機関の利用や決済の履歴といったもっとはるかに精度の高いものである。したがってこういう情報を守ることには重要な意味がある。

(6) 個人情報保護法

日本でもやっと個人情報保護法が成立し、2004 年の 4 月から施行される。

個人情報を取り扱う民間の事業者は、この法律によって様々な義務を課せられる。

特に個人情報の目的外使用は強く規制されますので、ブラインド・レンタルやリスト・スワッ

プなどを合法的に行うことは難しくなるはずである。

また、もし不正利用などがあった場合には、個人が地方自治体などに苦情を申し立てることができる。自治体の方もそれにきちんと対応しなければならない。

それでは、このような制度の整備でプライバシ・クライシスは解消するのか。

確かに個人情報の目的外使用などは法整備のおかげで違法にはなったが、実際に個人情報が漏洩したかどうか、実際に確かめて立件することは簡単ではないであろう。

個人情報を本当に保護するためには、制度と併せて技術的にも情報を守る仕組みが必要である。

また、ここで重要なのは、個人情報の保護と有効利用のバランスをとることである。

ユビキタス情報化社会では、個人情報をある程度開示した方が確かに便利なサービスを享受することができる。また、ビジネスを行う側から見ても、そういう情報を合法的に利用することはビジネス上の大きなメリットになる。したがって、法律ができたからと言って個人情報を扱うのは完全に止めようとか、個人情報は一切開示しないようにしようというのではなく、いかにして合法的に安全に利用するかという努力が必要になる。

(7) 個人情報保護と PKI

ユビキタス社会の利便性と個人情報の保護を両立させるための技術として、個人が本人の意志に基づいて自分に関する情報を暗号化して保護できる必要があると考えらる。そして PKI は、そのような基盤として現時点では最適なものであろう

個人情報の利用を認める相手のみに情報を開示する仕組みとして公開鍵暗号を利用することは適切である。さらに、現在の著作権保護技術を逆向きに使うと、個人情報がサービス主体によってどのように利用されたのかという記録を個人の側が正確に知ることができる。もちろんそのためには、PKI だけでなく信頼できる第 3 者や耐タンパ装置などを含む複雑な仕組みが必要になるが、実現不可能ではない。したがって、このような個人情報機構の研究の推進を提言したいと思う。

(8) メタ情報と電子署名

メタ情報とは、情報につけられた情報のことである。

「この情報はこういう条件に則って利用してください」という表示は、情報のメタ情報になる。個人情報に対して、本人がその利用条件になるルールを規定し、それに電子署名を施すことは、法的な保護を強化する技術になると考えられる。

特に、ユビキタス情報化社会では、データベースなどに蓄積されたものでない、ホットな個人情報を扱うことになるが、そのような情報に対しては特に電子署名による保護が有効だと考えられる。

例えば、刻々と変わる GPS による自分の現在位置を使ったサービスを受けるときに、自分のいまの現在位置の情報を暗号化した上で、それを誰がどこまで利用してよいかというルールを電子署名付きでくるんで送ることができれば技術的にも法的にもより安全な方法となるであろう。

交通標識の図柄が国際的に共通性を持っているように、情報の利用についてのルールを標準的なアイコンとして表示しようという試みが始まっている。これは、主に著作物の 2 次利用の条件についてのものであるが、複数の標識の組み合わせによってルールを表現しようというものである。この標識によるルールは、XML の RDF というメタ情報を記述する標準的な文法に則った機械可読な電子文書としても記述される。

個人情報についてもアイコンをスタンプするくらいの簡単な操作で、電子署名付きのメタ情報を生成するような機構が実現できるかもしれない。

ここでは、このような機構についての早期の研究を提言したいと思う。

(9) ユビキタス情報環境における属性認証

これまでの PKI が想定していた「仮想空間」における利用者認証とユビキタス情報環境における利用者認証では認証の意味がかなり違っている。どう違うのかというと、固有の名前が必要かどうかというところである。

これまでの PKI のデジタル証明書の主な目的は、本人固有の名前と暗号鍵をきっちりと対応づけることであった。

しかし、ユビキタス環境では、生身の肉体と情報機器を対応づけることも可能なので、名前は必ずしも必要ではない。

例えば、JR の自動改札で suica を利用するときに利用者の名前は不要である。カードを握っている人がその所有者だとわかるからである。

むしろ重要なことは、そのカードを持っている人が一定の属性認証機関から認定された属性を持っていることを証明することである。携帯電話や IC カードなどは、ユビキタス情報環境における属性認証装置として機能することになるであろう。

そのような属性認証機構は、必ずしも現在提案されている属性証明書のようなものとは限らないが、PKI がベースになることには変わらないであろう。

この予測から、ユビキタス情報環境における携帯情報機器を利用した属性認証機構についての研究も推進されるべきではないかと提言する。

(10) まとめ

市民生活の浸透しつつあるユビキタス情報化の流れの中における PKI の必要性について述べた。

新しいビジネスチャンスと個人情報保護を両立させるための技術として、これまでの発想とは違った観点から PKI をより発展させる研究が必要ではないかということを中心に提言を行った。

3．電子署名推進方法に対する提言

3.1　電子署名と実印／認印と対応付けて説明することの課題

PKI の署名鍵と公開鍵証明書はよく実印と印鑑証明書に例えられる。確かに公開鍵は印影に、本人のみが持つ署名鍵は実印に対応できる。公開鍵の登録は信頼できる認証局が厳格な本人確認のもとに行われる。同様に印鑑登録（印影の登録）も信頼できる公的機関（市役所など）で厳格な本人確認のもとに行われる。登録された公開鍵は本人名義とバインドするために権威のある認証局の電子署名が付された公開鍵証明書として発行される。印鑑証明書も印影のコピーの完全性を証明するために権威ある市町村長の押印が付されて発行される。

一方証明書の利用場面も同様な状況になる。電子署名文書には公開鍵証明書が添付されて利用者に送付され、受信した電子署名文書の検証者は添付された公開鍵証明書の有効性を検証して証明書にある公開鍵で電子署名を検証することで電子文書の完全性と本人名義の確からしさを確認できる。これはリアルの社会の実印に場合には、実印の押印文書に印鑑証明書が添付され利用者に渡され、利用者は印影と文書に押印された印影を比較検証することで、押印された文書の完全性と押印の本人性を検証することに対比される。両者は極めてよく似た対比となっている。

この類似性から公開鍵方式は厳格な実印との同等性が強調され、登録時の厳格な本人確認が必要になり、署名検証も認証パスの検証も含めて複雑な処理が求められる。このことから公開鍵証明書のコストも高くなり、電子署名の利用の普及を阻害しているのではないかと言う意見も出てくる。リアルの社会ではビジネス行為での本人性を検証するために必ずしも実印が求められていない。ほとんどのビジネス行為では三文判が通用し、実印が求められるのは不動産取引や自動車の購入契約などの限られた場面でしかない。従って、PKI の世界でも厳格で面倒な実印同等な仕組みだけではなく三文判と同様な気軽に使え、低コストな運用を可能にする電子署名を用いて普及を図るべきではないかとも言われることがある。リアル社会の政府に対する申請、届出の大部分は三文判でよく、実印を求められることは少ない。このことから電子政府の電子申請でも三文判電子署名を認めるべきではないかという意見がでてくる。

しかし、リアル社会の実印や三文判と PKI における公開鍵方式の署名鍵とは利用環境や利用方法において様々に異なった面を持っている。ここで問題を明確にするために以下にあげる幾つかの点について整理しておこう。

(1) 印鑑証明書と公開鍵証明書は同等な仕組みか（実印制度と PKI）？
(2) 実印と三文判
(3) 三文判 PKI について

(1) 印鑑証明書と公開鍵証明書は同等な仕組みか（実印制度と PKI）？

実印制度と PKI の仕組みについては冒頭に述べたように多くの類似点がある。しかし決定的な違いは実印制度が百余年の歴史と実績があるのに対して PKI はほんの十年以下の実績しかなく社会的な認知度は極端に少ない。また実印制度はリアルな社会の行為として押印の有効性の検証に

当たっては印鑑証明書と印影の比較だけにとどまらず対面での押印行為やその他の付随情報によって押印の意思やその有効性の確認が補強される。

それに対して PKI での電子署名はサイバー社会の特性として与えられたデータ（電子署名と証明書）の数学的一致を頼りにする以外にない。相手の表情や行為は一切捨象されている。従ってサイバー社会の特性として、署名鍵が漏洩して成りすまされたのか、登録時の本人確認のミスによる偽の署名なのかまたずさんな認証局の管理によって証明書が偽造されたものかの判断は極めて困難である。PKI で言えることは、署名鍵と公開鍵が対応しており、暗号鍵の強度が十分であり、署名鍵が本人にのみの所有で、本人の名義が公開鍵と一緒に正しくバインドされ、証明書の有効期限が切れていなく、失効もされていなく、認証局の鍵が正しく管理され、運用が厳格になされ・・・と言う仮定が正しければ、署名の検証結果は数学的にかなりの確度で信頼できるというものである。

従って署名検証の確度を高く保ちたければ、技術だけでなく登録や運用などの管理がより厳格に求められるようになる。もしこれらの管理運用が厳格になされたならば、実印による押印と印鑑証明書の印影の比較行為よりもはるかに確実な署名検証が可能であり、改ざんの有無も 100%に限りなく近く検知できる特性を持っている。

(2) 実印と三文判

実印は公的機関によって登録された印鑑証明書によって押印の印影比較を可能にする仕組みを持っているのに対して、三文判による押印は何の検証手段も持っていない。三文判は誰でも安価で購入でき成りすましができることは誰でも知っている。それでも通常のビジネス取引や申請に三文判が通用しているのは、今までの長い歴史の中で信頼度のレベルがある程度判断できるようになっていたからである。さらに三文判の利用領域はそれほどリスクの高くない分野で使うと言う慣行ができている。

しかし最近では銀行での押印偽造事件が多発して、銀行印を廃止しようと言う動きなどを見ると、同様に実印でも偽造事件が問題になることは見えている。最近の高精度なスキャナーで印影を取り込めば自動印鑑刻印機で実印でも銀行印でも三文判でも数分もかからずに簡単に偽造できてしまう。

この印影から印鑑が簡単に偽造できることに対して、PKI では公開鍵から署名鍵を偽造するのははるかに困難である。署名の安全性の観点からは認証局の運用や鍵管理がしっかりしていれば、公開鍵方式は実印など印鑑の押印に比べてはるかに優れた特性を持っている。

三文判 PKI や三文判電子署名というとき、これをリアルの世界に対比させて三文判が多く使われているのだから PKI にも三文判をと言うのは少し乱暴な議論に流れがちである。PKI は公開鍵方式を第 3 者の認証機関が公開鍵証明書を発行して証明書に載せた公開鍵を信頼してもらう仕組みである。三文判は第 3 者の何の証明もなく、単に署名者の自己主張としての印である。これをサイバーの世界に置き換えれば署名者が単にデジタル文書に自分の名前をタイプすることと同じである。誰でも偽造できるし、文書の完全性の保証もない。サイバーの世界の特徴は、特にインターネットの世界では、ネット上に流れるデジタルデータを誰かが盗聴し偽造することが可能で、しかもこれを発見することが困難であることである。現在のところデジタルデータの完全性と発信者の真正性を確保するための広く認められた技術は PKI 以外に実用的なものはない。日本の電

子署名法の定義によれば電子署名とは「改ざんの検出」と「本人性確認」ができる要件を満たさなければならない。この要件は PKI 技術が可能にしている。

(3) 三文判 PKI について

インターネットを飛び交う文書の真正性を確保するためには「改ざんの検出」と「本人性確認」の仕組みを欠かすことができない。リアルの世界で三文判がいかに多く使われていても、サイバーの世界ではこれと同等なものとして改ざん検出、本人性確認ができない電子署名は大きなリスクを伴う。三文判 PKI というとき考えなければならないのは基本的な PKI の仕組みを維持しながらリスクや脅威に何処まで対応できるかのセキュリティ基準（ポリシー）を明確にすることである。

金融の世界では小額取引の（リテール）セキュリティ基準と高額取引の（ホールセール）セキュリティ基準を分けてきた。ベリサインの証明書発行のポリシーでは本人確認の程度を分けてクラス 1、クラス 2、クラス 3 と分類して保証レベルを分けている。カナダ政府の PKI や米国政府の PKI でも証明書のポリシーとして目的に応じて 4 段階のセキュリティレベルを設定している。Rudimentary（初級）、Basic（基本）、Medium（中級）、High（高級）と分けそれぞれの証明書ポリシーを明確に規定している。例えば、初級レベルは PKI の試験的な導入時などに用いるもので失効確認の行わず、認証局の鍵管理も FIPS140 のレベル 1 でよい。基本レベルでは利害の伴わないメールなどに用いるものとして失効確認を行っても行わなくてもよく、認証局の鍵管理は FIPS140 のレベル 2 とする。中級レベルでは実用的な政府内も文書交換に用いるためのもので失効確認は行い、認証局の鍵管理は FIPS140 のレベル 3 とする。高級レベルではハイリスクな業務に使うもので失効確認を確実に行い、認証局の鍵管理は FIPS140 のレベル 3 または 4 とし、認証局の運用に厳重な管理を義務付けている。このように明確なポリシーのもとセキュリティレベルを分けて利用者には目的に応じて何種類の証明書でも発行できるようにする。

三文判 PKI というとき、このカナダ政府や米国政府が採用している初級または基本レベルの PKI を対応付けるべきと思われる。このレベルのポリシーでは認証局の厳格な運用は求めていなく、鍵管理も HSM（ハードウェアセキュリティモジュール）は必要としない。また本人確認も厳格な審査をしなくてよい。問題が起こってもそのリスクはそれほど大きなものにならない用途を想定している。従って運用コストもかなり安いものとなる。

日本ではポリシーのレベル分けについてあまり議論されてこなかった。政府の GPKI でもポリシーは 1 つで（米政府の中級に相当）下位のレベルや複数の証明書の使い分けについて検討されていない。三文判 PKI の提起を契機として PKI の証明書ポリシーの議論が深まることが期待される。

最後に直接実印と PKI の関係の話題に直結しないが、認証の問題について触れておきたい。現在の電子政府の電子申請アプリケーションでは電子署名を基本として作られている。しかし、提供すれば必ずしも電子署名を必須としなくても良い場合が多いと考えられる。電子申請や民間の e-ビジネスでは利用者がサービス提供者のシステムにログインし、各種のサービスを受ければよいからである。ただしこのとき相手認証は必須のものとなる。また電子申請などをワンストップサービスで行うためには SSO が必須の提供技術となる。このときプライバシー保護の観点から利用者のアイデンティティを一元管理するのではなく各省や各部門で分散管理し、アイデンティテ

ィの連携機能を設ければ安全で便利なサービスが可能となる。米国政府は最近 e-Authentication Initiative を作り国民サービスのために SAML や Liberty を想定したアイデンティティ連携の e-Authentication 基盤整備の準備を始めている。ここでも用途に応じてポリシーに応じて Authentication Context によって各種の認証技術を選択できるようにとしている。リスクの高いサービスには認証は PKI で行いリスクの低いサービスには ID、パスワードでもよいというように各種の認証レベルを分けて考えることをこの e-Authentication 基盤の基本に据えようとしている。

ここでも考え方は 1 つの手法にロックインするのではなく、ポリシーに応じて多様性を基本とする考え方をとっている。この方法によれば結果的に迅速な展開と総合的なコストを削減できるように思われる。日本でもシステムは用途によって選択するという多様性を身に着けるべきである。

3.2 公的個人認証と属性認証の相互発展

(1) 公的個人認証制度の開始

公的個人認証制度が、いよいよ開始された。

この制度は、いわゆる「行政手続オンライン化関係三法」の 1 つである公的個人認証法に基づく制度であり、これまでの制度・法律施行と併せて国民（住民）と国や地方公共団体との間の約 21,000 もの申請・届出の電子化（オンライン化）が可能になる。公的個人認証制度から発行される電子証明書について簡単にまとめると以下のようになる。

- 発行者：各都道府知事
- 発行対象者：地域住民
- 証明書記載情報：基本 4 情報（氏名、住所、性別、生年月日）
- 証明書格納場所：住基カード（IC カード）の中
- 価格：\500 程度（有効期間 3 年）
- 用途：国や地方公共団体への電子申請・届出（例、パスポートの交付請求、地方税の申告、年金関係手続き等）

(2) 公的個人認証証明書の利用

公的個人認証制度から発行される電子証明書は、行政に対する電子申請・届出に限定され、役所への申請時に、必要な添付書類の住民票や印鑑登録証明書の代替として利用される。ペーパレスの電子申請が可能になるわけである。

現実（リアル）の世界では、住民票や印鑑登録証明書は個人を認証する書類として民間でも利用できること、また民間の電子商取引の世界でも、これらの書類を代替する電子証明書を使用してのペーパレス化は非常に有意義であることを考えると、行政への電子申請・届出に閉じられた利用に限定されている現状は残念なことである。

将来的には、現実（リアル）の世界で運転免許証が本人確認手段として定着しているように、顔写真付住基カードとその中に格納されている電子証明書・電子署名用鍵が、対面取引と電子商取引の両面において本人確認手段や住民票・印鑑登録証明書の代替として市民権を得る時代が来

るかも知れない（現在、公的個人認証制度ではこれを容認していない）。

(3) 民間での個人証明書の利用

民間での電子商取引で利用可能な電子証明書には様々な種類があるが、前述の公的個人認証法に対比される証明書は、信頼性の面から考えても電子署名法による電子証明書が考えられる。

この証明書のプロファイルは、以下の通りである。

・発行者：民間認証サービス業者
・発行対象者：個人（住民、消費者、顧客、組織人等）
・証明書記載情報：氏名、住所、その他（若干の属性情報や電子メールアドレス）
・証明書格納場所：IC カード、PC のハードディスク
・価格：\10,000 弱～￥30,000 弱（有効期間と格納媒体に依存）
・用途：国や地方公共団体への電子申請・届出や民間での電子商取引（実質用途制限はない）。

電子署名法対応証明書は、利用用途の制限がない（公的個人認証証明書は、対行政への利用に制限）のが特長であり、公的個人認証証明書の持つオンライン取引におけるペーパレスの機能も具備している。

(4) 何故属性認証の採用か

電子署名法対応の証明書は、行政への電子申請分野では高価で有ることもあり後発の公的個人認証証明書に対して価格競争力を失うことは明白である。

そこで電子署名法対応の証明書に付加価値を付けて行政への電子申請で継続的に使用してもらうこと、さらに今後の民間での電子商取引での拡がり等を考慮に入れて、以下の課題を解決することが民間認証局としての使命と考えている。

① 行政への電子申請の全てが純粋個人としての住民の立場で行われないこと考えると、以下の例に示すような証明書が必要となると考える。
（ｉ）企業を代表して、電子申請を行う組織人（企業人）の証明書
（ii）任意団体の職員証明書
（iii）個人事業主の証明書
（iv）個人や組織の代理人として申請事務が行える資格を証明する資格証明書

② 申請者のプロファイルを相手に正確に認識（認証）してもらうための証明書記載項目の表記はローマ字だけでは不適切。ローマ字に加え日本語で証明書記載項目を記述することでの見読性を向上させる。

これら課題を解決する手段の１つの事例が、下記図３－1 に示すように既存の電子証明書に各種属性情報を日本語で付加することである。PKI の世界で標準化されている属性証明書（Attribute Certificate）と区別するために、ここでは「属性型証明書」と呼ぶ。

「属性型証明書」の特徴は

（ｉ）人の属性を様々な観点で表記できる。
ただし、現在表現できる属性は限られ、拡大には属性を保証する方法を確立・拡充する必要がある。

（ii）人の属性の保証は、現実（リアル）の世界で実際に使用している担保（住民票、印鑑証明書、登記簿謄本等）を利用しているためにその情報の信頼性に問題はない。
その属性の保証方法の信頼性が広く認められると完全なペーパレス化オンライン取引が実現できる。

（iii）取引場面に応じた相手認証を、属性を活用することで確かなものにできる。
行政への電子申請・届出、民間での電子商取引での利用が可能である。

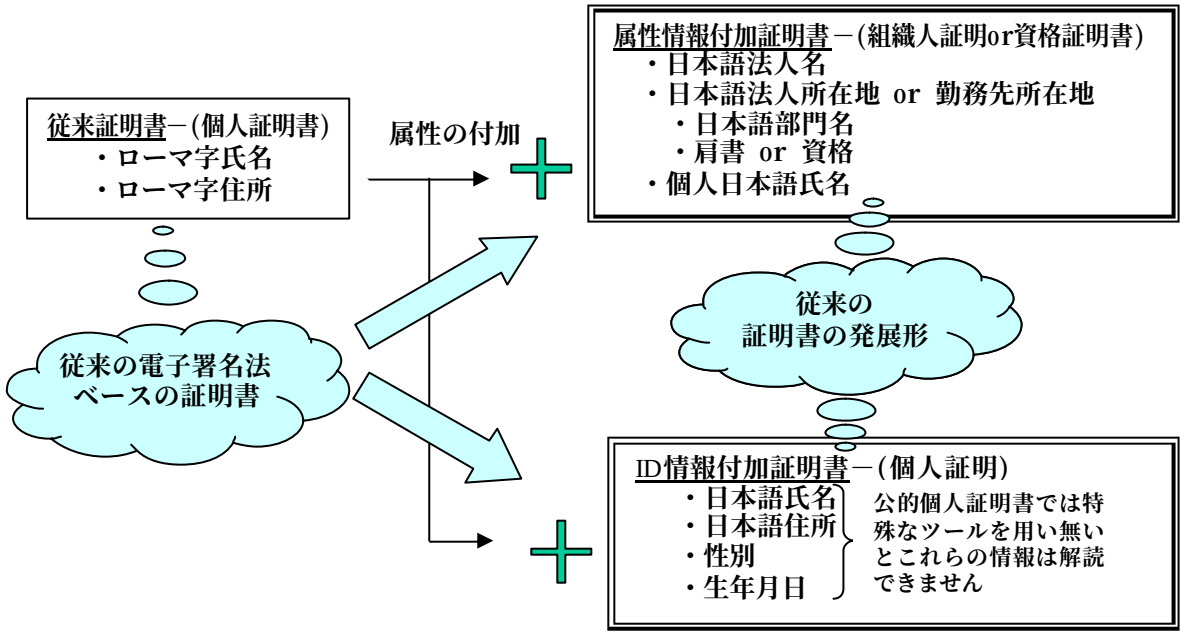

図 3-1 電子証明書への属性情報の付加（事例）

(5) まとめ

平成 13 年 4 月の電子署名法の施行以来、行政への電子申請・届出へ利用可能な電子証明書の発行は、民間認証サービス業者の運営する認定認証業務に依存してきた。その間、中央官公庁の電子申請・届出システムの整備は順調に進み、地方公共団体への波及を今年早々の公的認証サービスの開始が拍車をかけている。この間、特定の用途としての国土交通省の電子入札用の証明書に属性型証明書は使用されてきたが、属性型証明書の本格的な利用はこれからである。国民や住民としての属性で中央官公庁や地方公共団体に対しての電子申請・届出は、公的認証サービスから発行される電子証明書で十分用が足りる。しかし国民や住民以外の特性を必要とされる行政への電子申請・届出や民間の電子商取引では属性型証明書は十分利用価値がある。ここに、民間の電子署名法対応証明書と公的個人認証証明書は、棲み分けと協調関係を確立し、相互発展する可能性を持っている。公的個人認証サービス構想が浮上した時に、公的個人認証証明書の民間での活用法は、民間認証サービス業者に配慮し概略以下のように述べられ現在まで踏襲されている。

① 民間認証局には、公的個人認証制度の電子署名用秘密鍵を使用した電子署名を電子署名法対

応の証明書利用申込書に付加することを許可しこの電子署名の有効性検証も公的個人認証制度の仕組を活用できる。また、この電子署名は、住民票、印鑑登録証明書を代替できる（電子署名法対応の証明書発行申請のペーパレス化）。

注）民間認証局は公的個人認証証明書の利用を認められた数少ない機関の１つである

② 民間認証局は、住民の公的個人認証証明書をベースに属性証明書を発行し民間で活用することを推奨する（行政からの提案ベース）

これら構想に私ども民間認証サービス業者は異存はあるはずも無く、今回記述した属性型証明書もまさに本構想を具現化したものである。

なお、属性型証明書に関する今後の課題は、

① 属性の種類を拡大する場合、その属性を証明する方法の模索

② その属性を証明する担保が、紙の文書で有ればそれを電子化する（ペーパレス化のため）方策の検討

③ さらに属性型証明書を取得する際に添付する担保書類（電子的な書類を含む）と実際の取引（行政への電子申請・届出、民間での電子商取引）での同一担保書類の二重提出の抑制

等である。これらは現在先行している中央官公庁への電子申請・届出システムの中での改善を期待するところである。e-Japan 重点計画-2003 では、行政・公共分野の情報化と共に電子商取引の促進が挙げられている。この中で、電子署名法対応証明書、公的個人証明書の果たす役割は、益々重要度が増す。両者の共存共栄を願って本節のまとめとする。

3.3 電子署名の普及広報に対する提言

電子署名・認証について、その運用等に関するガイドラインを民間が作成したり、電子署名法（電子署名及び認証業務に関する法律）が施行されたりして、業務への適用が始まっているが、普及状況はどのようになっているか、今後の普及広報は如何に行うべきかについて記述する。

(1) 電子署名・認証の普及状況

平成１５年９月に経済産業省が電子署名に関して、国民１０００人に対してインターネットを通して、年齢層別にアンケートを行った。その結果において現状の電子署名の認知度と利用率は以下のとおりである。

約８０％が電子署名を知っているとの回答が得られ､用語としての認知度は高いといえる。しかし、電子署名法については、知っている及び聞いたことがあるとの回答は約４０％であり、電子署名との間でかなりの乖離が見られる。

また、電子署名を実際に利用したことがあると答えた人の割合は、１０％未満であり普及にはほど遠い状況にある。

利用しない理由について、電子署名の全体像が不明なため利用に不安がある、盗聴、改変等セキュリティ上の不安がある等の回答が多く見られ、電子署名に対する認識不足や誤った理解があり、普及啓発が行き届いていないことを示している。

(2) 現状の普及広報活動

電子署名の普及広報について、現状以下の取り組みがなされている。

① 政府による広報

電子署名法の主務官庁である総務省、法務省、経済産業省においては、それぞれ以下の関連サイトで電子署名法、関連規則等の法令関連及び認定を受けた認証業務一覧が紹介されている。

総務省：http://www.soumu.go.jp/joho_tsusin/top/ninshou-law/law-index.html

法務省：http://www.moj.go.jp/

経済産業省：http://www.meti.go.jp/policy/netsecurity/digitalsign.htm

② 各種団体による広報

電子署名・認証に関する調査、研究もしくは業務を行っている団体は、非常に多岐にわたっておりその全てをここで紹介することは難しいが、その中で JESAP を除く広報をあわせ行っている主な団体について述べる。

電子署名法における特定認証業務の認定に係る調査を行っている指定調査機関である（財）日本品質保証機構（JQA）及び（財）日本情報処理開発協会（JIPDEC）においては、電子署名・認証に係る活動内容、指定調査機関業務の紹介、電子署名・認証ハンドブック等を公開している。また、両団体は、総務省、法務省、経済産業省と共同で平成 12 年度から全国７～８都市において「電子署名・認証　普及啓発セミナー」を実施している。

（財）日本品質保証機構：http://www.jqa.jp/11it/denshininsho.html

（財）日本情報処理開発協会：http://www.jipdec.jp/esac/

独立行政法人情報処理推進機構（IPA）のセキュリティセンターにおいては、暗号技術の一環として電子署名・認証に関する調査・開発等を手がけており、以下のサイトで成果を公開している。

独立行政法人情報処理推進機構：http://www.ipa.go.jp/security/ipg/crypt.html

電子商取引に関する技術、制度、運用等の標準化について研究している電子商取引推進協議会（ECOM）において電子認証、電子公証に取り組んでいる認証・公証ワーキンググループでは、平成８年からの研究成果を以下のサイトで公開するとともに毎年の研究成果をセミナーで発表している。

電子商取引推進協議会：http://www.ecom.jp/index.html

電子取引の発展に必要な基盤としての PKI について、アジアの PKI の共通化をはかっていくことを目標とし、アジアの国／地域と協力して相互運用性の確保や普及活動を行っている日本 PKI フォーラム（JPKI）では、その成果を以下のサイトで公開するとともに、日本国内での PKI 普及に向けたシンポジウムを開催している。

日本 PKI フォーラム：http://www.japanpkiforum.jp/

③ 認証事業者による広報

電子証明書の発行をビジネスマン、消費者等広く一般を対象にしている認証事業者においては、適用業務向けの電子証明書取得手続きの説明、認証業務実施規程（CPS）、電子証明書失効リスト（CRL）等の公開以外に、PKI 等認証技術の説明を行っているところもある。個々の事業者が行っている事項については省略するが、上記政府の URL に記載されている認定を受けた認証業務一覧等から検索いただきたい。

(3) 普及広報活動への提言

前述のように電子署名という用語の認知度は高いとは言え、電子署名法及び電子署名の仕組みに関する理解はまだまだ低い。実際に利用した人が１０％未満であることがそれを裏付けている。今まで、電子署名法や電子署名、電子認証の仕組みを理解してもらうためにセミナー主体の広報活動が行われ、この分野に興味を持つ人達には有効であったと思われるが、今後、より広範囲に電子署名を理解してもらうためには、新たな普及広報活動を展開する必要があると考える。

電子署名を利用する場が増えれば、電子署名、電子認証の仕組みを理解したいと思う人が増えるであろうし、電子署名の法的効果についても関心を持つ人が増えるであろう。電子署名利用の場の拡大こそが、効果的な普及広報活動の源ではないだろうか。

平成１３年から電子政府システムがスタートし、政府と民間企業の電子商取引、電子申請・申告等に電子署名が使われ始めている。本年（平成１６年）においては、年初から公的個人認証サービスや国税電子納税・申告システムが稼動し、ビジネス界だけではなく一般国民も電子証明書の交付を受け､それを用いた電子署名を行えるようになってきている。また、６月からオンライン登記申請が稼動することになっており、電子署名の利用範囲がさらに拡大する。

これらのサービスはいずれも電子政府システム関連であるが、電子署名の利用の場が拡大していることには相違ない。これらサービス及び利用方法の説明を通して、電子署名の仕組みや電子署名の法的効果等について理解をもってもらうことが最も効果的な普及広報活動ではないだろうか。

特に、国税電子納税・申告システムは、確定申告を行う人にとっては利便性が向上するものであり、諸外国の例から判断すると今後の利用が増えることが予想される。従来より行われているセミナー等は企業人、認証事業者等をねらいにしていたが、例えば国税電子納税・申告システム向けのセミナーを行えば、一般納税者や税理士が聴衆者になり、電子署名に対する理解者が拡大することになる。広く国民が利用できるアプリケーションごとに同様な活動を行うことが、電子署名の普及を促進する１つの手段になると考える。

このことは、JIPDEC が実施した平成１５年度「電子署名・認証　普及啓発セミナー」において、セミナー参加者に行ったアンケート結果によっても裏付けられている。736 名の回答者のうち 441 名が電子署名の活用事例に関心があり、今後のテーマとしてもより具体的な活用事例の紹介を望んでいる。電子政府システムや企業間電子商取引等において、電子署名・認証システムをどのように導入、利用すれば良いか、具体的なメリット、デメリットとして何があるか、コストとして何を考慮しなければならないか等を知りたがっていると思われる。

また、同アンケートで電子署名・認証普及促進のための手段として何が有効かとの問い合わせも行った。その結果、オープンな電子証明書体験システムの開設を望む声がもっとも多く、次いでテレビ、新聞等公共メディアによる広報、セミナーによる広報となっている。オープンな電子証明書体験システムの開設の要望は、前述した経済産業省のアンケート結果とあわせ見ると、理屈としてインターネット商取引におけるセキュリティ対策として電子署名・認証が有効であると理解するだけでは物足りなく、使い勝手を含めて理解し

たいとの現れであると考えられる。

ただし、実際に体験システムを広く一般に提供するためには、運用者の決定、コスト負担等の大きな問題があり、実施意義を含めて十分な検討が必要であると思われる。同様にテレビ、新聞等公共メディアによる広報で効果をあげるためには、人気タレントを用いたコマーシャルが有効であると思うが、高額な出演料負担の問題があり、実現はかなり難しい。

やはり、費用面を考慮すると電子署名・認証の普及にはセミナーを地道に行うことが重要であると思うが、今後は従来のやり方だけではなくセミナー活動を講演内容、地域等で層別し、本報告書と対を成す「電子署名・認証利用パートナーシップ報告書　－国内の PKI 進捗状況－」の４章に記述されている電子署名認証推進・活用団体の協力をいただき実施することを検討する必要があると考える。

4．部会における主な議論

4.1　電子署名・認証の利用における疑問／不安

部会活動では、昨年度に引き続き、継続的なウォッチ活動として「電子署名・認証の利用における疑問・不安」を抽出・整理する活動を行った。
また、それらの整理の仕方として、本年度は電子掲示板を利用する方法を提案した。

「疑問・不安を整理する」枠組みとして、以下の 6 つの分野を設定している。
（１）PKI のシステム構成における技術的な問題（インタオペレタビリティの問題も含む）
（２）PKI 実装上の技術的な問題
（３）PKI の普及過程の技術的問題
（４）PKI の普及過程の制度的・社会的な問題（アクセシビリティの問題も含む）
（５）PKI が普及しきれないときの制度的/社会的な問題
（６）PKI の社会システムとしての脅威・脆弱性の問題

以下に、昨年度からの継続の項目も含め、6 つの分野の疑問・不安点の例を示す。今年度は、昨年度の問題例示に対していくつかの項目が増え、また昨年指摘した問題の具体例指摘がマーケットで行われた事例などを追加している。昨年からの変化として、問題が解決された事項はない。

（１）PKI のシステム構成における技術的な問題（インタオペレタビリティの問題も含む）
(1A) 複数の PKI システムを統合するようなシステム構成、あるいは複数の PKI システムを同時に利用するクライントからみて、CRL や OCSP のインタオペラビリティに欠陥がある場合の問題点。

(1B) 企業体の合併、分割、大規模組織改変、消滅などに関する問題点の徹底解明不足。一般的に急激な利用環境変動の影響が CRL のような形でしか対応しきれていないことの問題性がどこまで掘り下げられているか。

(1C) 電子署名のメタファーとして、印影の映像を付加するといった方式をとっている場合に、理解が深くない利用者は印影イメージ自体に意味があると誤認識し、電子署名としての保障メカニズムを確認しないで、（虚偽の）電子署名を信任してしまう可能性があるのではないか。
特に、ホームページの安全性を主張するマーク等の場合に、マークのイメージ自体（単純アニメージはコピー可能）を信任すべき証拠と誤認してしまう利用者の行動を誘起する可能性がある。

(1D) 現在のように、通常の利用者が用いているブラウザ等のメカニズムが一般的なセキュリティ問題にさらされており、その結果としてメーカ等から「ブラウザダウンロード」を頻繁に行

うよう求められている状況においては、ブラウザ自体が悪意ある攻撃者によって悪意あるコードにすり替えられ、あるいはのっとられる可能性がある。そのことを前提とすると、一般利用者が「見ている」画面は操作される可能性の幅が非常に大きくなり、PKI の利用者サイドでの実装上の厳密性に大きな問題を投げかける。

(1E) 長野県での住民基本台帳ネットワークへの侵入実験結果のように、PKI の応用システムが、一般の業務システム、事務システムと何らかの意味で結合している場合に、PKI 応用システムへの侵入等のセキュリティ問題が発生する可能性がある。

このような「何らかの意味での結合」は、無線結合を始めとする多様なネットワーク化手段の発達や、ユービキタスコンピューテイングの進展によるコンピュータ類似機器の多様な利用環境では、予測困難な形で形成される可能性があり、非常に注意深い点検や監査が進むことが望まれる。

（２）PKI 実装上の技術的な問題

(2A) 秘密キーの管理について、その重要性の程度が一般利用者に十分に認識されない可能性がある。これは、秘密キーそれ自体を「見ても」その重要性の程度はわからず、運用されているシステムにおいて果たす役割との関係で初めてはっきりしてくる問題だからだという側面もある。また逆に十分な理解を経ずに過度に深刻さを強調すると便利には使われにくくなるという問題がある。(2003 年度岩崎さんの指摘事例など)

(2B) 認証と署名の違いに基づく課題

PKI を用いた認証と電子署名は同じメカニズムを用いている。すなわち、情報発信者が持つ秘密キーを用いて署名を行い、情報受信者は公開キーを用いてそれが信頼できるものであることを確認する。あるサイトにアクセスするに際して認証が必要である場合に、アクセス主体は相手に秘密キーを見せるわけではないが、そのメカニズムを用いていることを承知している。しかし、相手が悪意あるサイトである場合に、このメカニズムを用いて任意の文書にアク?セス主体の署名を獲得する危険性がないわけではない。この場合、認証においては、アクセス主体は相手方のリードに従って秘密キーを用いるということに落とし穴が発生する可能性があることを示している。

(2C) 認証と原本性保証の違いに基づく課題

原本性保証では、ドキュメントに対する保証は永続性が要求される事柄である。これに反して、認証は一過性のものであり、また頻繁に発動されるものである。このような運用上の違いを無視して、もし同じキーペアを認証と原本性保証に対して使い続けるとするなら、セキュリティの弱みを持つ可能性がある。

また、原本性保証等の応用におけるキーの有効必要期間が非常に長期にわたるということに基づく PKI の脆弱性も指摘される。この点については、たとえば第 5 回情報セキュリティシンポジウム（日本銀行金融研究所、2003-03-07）において包括的に議論されている。

なお、認証と原本性保証の違いのほかに、暗号化と署名の違いと複数キー利用の必要性を指

摘することもある。一部の PKI 製品（エントラストなど）は、この暗号化と署名の違いに対応する複数キー提供を製品機能レベルで行っている。

（３）PKI の普及過程の技術的問題

a(3A) 電子認証・電子署名が広く社会で利用されるようになった時に、PKI 製品の技術的欠陥（たとえば、CA 鍵危殆化を招くようなセキュリティホール）が発見された場合、特定の暗号解読技術が飛躍的に発展した場合の対応。

(3B) クローズドグループ内でプライベート CA 局の運用がかなりな程度行われている状況において、そのような運用になれてしまった利用者がオープンな場でも既知のルート認証のない証明書を受け取り信用してしまう状況がありうる。

この問題は 2003 年度秋に、「総務省の CA 局の認証の問題点」として、すなわち既知のルート認証局以外のルート CA 局の認証方法の問題として多少異なる形で具体的な問題に即して問題提起された。総務省の方式の場合、フィンガープリントの照合が実際には行われないのではないかという疑問と関連した問題指摘である。しかし、原理的には、総務省のみでなくすべてのプライベート CA 局に関しての潜在的に共通する問題であると同時に、利用者側の「慣れ」の問題も重視しておかなければならない事柄である。

（４）PKI の普及過程の制度的・社会的な問題（アクセシビリティの問題も含む）

(4A)ユーザに PKI あるいは暗号化の下でのシステム動作を積極的かつある程度標準化された形式で見せた方が良いのかどうか（たとえば Web の利用環境において）――見せない場合は、セキュリティ保護を利用者が確認?できず悪意ある攻撃を防げないという不具合があり、見せた場合はシステムの癖のある動作が利用者に不安を与え、かえって余計なリアクションを誘発する可能性がある。

(4B) PKI 固有の問題ではないが、PKI と結合して利用する個体認証の機構における、プライバシー問題、バイオメトリクスに対する身体障害者のアクセシビリティ問題など。

(4C) 証明書失効の時期とリアルワールドでの事象の時間的なずれに起因する問題。たとえば、所有者が失効を知ったのが失効事由発生よりあとであった場合に、その間に行われた取引に対してどのように取り扱うべきかといった問題（具体例としては、2003 年度岩崎さんの指摘例を参照）。

(4D) 多くの PKI に基く「証明書」が混在し、それらの「証明している事柄」の違い、認証局の CP/CPS の違いなどから、互換性がなくなる事態が利用者から見て非常に複雑であり、広範な利用に対する妨げとなる可能性がある。

（５）PKI が普及しきれないときの制度的/社会的な問題

(5A) デジタルデバイドの一形態として、PKI 対応が出来る市民、出来ない市民という生活行動

上の差別が生じる可能性。特に役所が一律に行う場合に、予算の限界の中で「取り残される市民」が発生する可能性がある。

（6）PKI の社会システムとしての脅威・脆弱性の問題

(6A) 電子認証・電子署名が広く社会で利用されるようになった時に、公開鍵一般に関する暗号解?読技術が飛躍的に発展した場合の対応。（量子コンピュータの早期実現などを想定）

(6B) 現在でも「PKI とは何か」の納得いく説明が一般市民に対しては難しい状況から見ると、利用が広がったとしても、「PKI とは何かを理解しない、理解できない」で利用することが大半であるということになると想像される。これは、「電気とは何かを知らないで電気を使う」、「テレビとは何か知らないでテレビを見る」のと違うのか、違わないのか。違わないとしても、「電気は安全に使いましょう」式の広報活動は必要なのかどうか。

(6C) (6B)の具体例として「安全な通信を行うための証明書」といった、一般向けにわかりやすいと称される説明のし方がかえって誤解と理解の混乱をもたらす可能性も指摘されている。すなわち、このような表現では、実際にどのような点で「安全」であり、どのようなことは「安全」として保証されていないのかが極めて不明確であると思われる。一般利用者が過度の信頼をしたり、理解が混乱し、システム運用者の予定しない行動を起こす可能性がある。

また、具体的問題点の指摘はまだだが、問題領域として以下の補足的な視点を提示する。

・キー情報がカードに格納されるとした場合のカードの取り扱いに関するいろいろな問題
・非常に多くのキー情報を個人が管理しなければならなくなった場合の問題
・大規模災害
・一部のシステムが利用者から利用できない状況――それによる直接の不具合
・一部のシステムが利用者から利用できない状況――それにつけこむ犯罪
・PKI の延長としての個人識別の問題点、リスク
・警察・司法・軍事上の理由などによる暗号化の制限、開示要求、事業者への管理要求の高度化などがあった場合の問題
・技術の陳腐化、競合技術の拡大
・インターネットが第２世代からさらに第３世代へとそれ自体が安全性を高めた場合
・その他

4.2 民間認証局発行の電子証明書は、電子申請現場で使えるのか

電子証明書、認証システムを利用する立場から、様々に述べてみたい。筆者の場合、行政書士という仕事柄、電子申請に的を絞りそれら利用について言及する。電子政府・電子自治体における申請現場では、どのような利用となるのか。また、代理人として申請する場合の代理申請システムでの認証技術利用、すなわち電子証明書利用について提言したい。

今日現在、電子政府にあってはほとんどの省庁で電子申請システムが稼働している。国土交通省所管の公共工事等、物品役務提供等における電子入札も稼働している。
電子申請・電子入札現場で民間認証局発行の電子証明書は使えるや否や。

(1) IC カード格納の電子証明書利用では、各民間認証局との互換性があるのか。

電子入札（国土交通省所管）では、１月３１日現在のところ８認証局発行の電子証明書が利用できることになっている。これらは IC カードへ格納される証明書である。それぞれの認証局では IC カードとカードリーダーのセットにて販売している。ここで、やっかいな問題を抱えることになっている。例えば A 認証局発行の IC カードを B 認証局指定のカードリーダーに挿入して、適正に証明書内容を読み込みできるのかどうか。つまりそれぞれに互換性があるのかどうか、全く解らない点である。

たしかに当事者たる入札参加者としては、単独で利用すれば他のカードリーダーとの互換性を気にするまでもない。ところが、代理にて手続する者にとっては、この問題は避けては通れない。代理人の環境では A 認証局指定のカードリーダーを利用、委任者が B 認証局発行の IC カードであった場合では、適正に委任者が電子署名できない畏れが多分にある。

つまり、代理人の環境には、委任者が利用する数ほどカードリーダーを設置しておかないと委任者から電子的委任を受けることができない。こうした事態が想定される。

筆者としては、１月２９日開始された公的個人認証サービスでの互換性カードリーダーを用意すれば、民間認証局発行の IC カードを受け入れる仕組み作りを提言したい。こうした汎用性あるカードリーダーでなければ、電子証明書の普及もままならないのではないかと危惧する。既に電子入札に利用できる電子証明書が、通常の行政手続たる電子申請に利用可能とする民間認証局発行のものも出てきてもいる。

代理申請する者にとっては危急に対応せざるを得なくなってもいる。

(2) 証明書中での CN 項の扱いはどうなのか。

よく知られているように電子証明書には基本領域と拡張領域がある。そこで特に証明書中拡張領域 CN 欄の記載方式について言及したい。

例として総務省申請・届出システムを取り上げる。このシステムには委任状登録が可能とし代理申請ができるとしている。委任状を作成するとき委任者が「電子署名」を為すが、委任者電子証明中の拡張領域の CN 欄に日本語氏名が記載されていないとエラーとなる。つまり電子署名できない。電子証明書中拡張領域 CN 欄に日本語氏名のみが記載されていることが条件となっている。

ところが、総務省申請・届出システムに利用できるとする民間認証局発行の電子証明書には、拡張領域の CN 欄について所定の要件を満たしていないのもある。こうした電子証明書では、代理システムでの委任状登録は不可能としている。そもそも電子署名できないのですから。委任状に電子署名できなければ、受任者たる代理人とってもきわめて困ることになる。代理人たる行政書士としては、要件を満たす電子証明書を重ねて取得するように委任者に指導するという本末転倒の事態もあり得る。同時に申請者は、申請先省庁ごとに電子証明書を準備することになるかもしれない。

重ねて分かり難くしているのが民間認証局発行の電子証明書である。電子申請現場では

法人として申請するのか個人として申請するのかによって、民間電子証明書の利用度が全く違ってくる。現行の民間電子証明書は、あくまで個人を特定しその個人を証明するものである。ところが、認証局によっては事業所単位で利用者（事業所に所属する者）に証明書を発行している。ここで誤解が生じることとなる。この証明書は事業所法人が電子申請する場合の電子証明書だとの誤った認識が産まれてもいる。まさか、事業所が取得した電子証明書を、証明書中に社員の氏名が記載されているので、記載されている当社員が個人的申請時に使えるとの説明もできはしないであろう。

混乱を防ぐには、法人として申請する場合は、電子認証登記所発行の法人代表者電子証明書を取得することにつきるであろう。

事ほど左様に、民間認証局発行の電子証明書については、よくよく検討して取得しなければならない。既に電子入札現場では混乱も起きている。

(3) 公的個人認証サービスでの公的個人電子証明書の扱いがどうなのか。

１月２９日開始された公的個人認証サービスが、行政書士等の事務所パソコン環境に影響を与えている。電子申請での代理手続をする者、行政書士等にとっては環境整備を避けては通れないことになった。

公的個人電子証明書の利用現場として、電子申告、社会保険手続、不動産登記、法人登記、自動車登録等が上げられている。自宅や会社に居ながらにしての電子申請ができるるがうたい文句である。残念ながら自宅にカードリーダーを設定してまで、手続をしなければないならないほどの緊急性が申請者側にない。そこで多くの者は次のようにするであろう。公的個人電子証明書を格納住基 IC カード媒体を手続してくれる「代理人」のところへ持参する。

例えば、自動車販売店へ住基カードを持参して、車庫証明申請・自動車登録申請での手続きをする。あるいは勤務先へ持参して社会保険の手続をする。不動産の売買で所有権移転手続をするに、従来と同じように司法書士事務所へ持参し司法書士に代理申請を依頼する。また、一般行政手続では、行政書士事務所にカード持参し、行政書士を代理人として委任状に電子署名する。

公的個人電子証明書を所持するも、その利用現場での電子申請システムに精通していないとなかなか利用できる現況ではない。一生の内に一回しか申請しない手続物に、わざわざ時間をかけてパソコン環境を整備するとは思えない。自動車登録等についても紙時代ではほとんど自動車販売店ディーラーまかせの行政手続（車庫証明、登録等）であり、これがオンラインになったからとて自宅にて個人で電子申請しようなどと思いもしないだろう。そのようなしちめんどい環境整備に戸惑うより、希望の車が手元に届くのが先だとするのが一般的感情である。

公的個人電子証明書の使用先は、ほとんど自宅外であろう。IC カードという証明書格納媒体も持ち出し携帯性に優れてもいる。

いきおい行政書士等の代理にて電子申請する者は、依頼者が IC カードを持参してくることを想定しなければならない。あるいは、事務所へそれを持参するように説明しなければならない。

１月２９日にオープンした公的個人認証サービスポータルサイトは、こうした事務所にとってもきわめて利便性がよいものとなっている。

事務所側環境整備をしておけば、「公的個人認証サービスクライアントソフト」にて依頼者の電子証明書を表示できる。表示させることで、依頼者が間違いなく証明書中の本人なのかどうか確認できうる。つづいて、先のポータルサイトオンライン窓口にて証明書の有効性のチェックをする。

こうした作業をまず行った上で、実際の電子申請手続に向かうことになるでありましょう。この作業を事務所側としては絶対的にしておくべきです。後々の紛争予防のためでもある。

(4) 行政書士等が代理人として申請する場合の電子署名とはどうなのか。

全国市長会は、１月２７日に「電子自治体推進に関する意見書」を出している。その意見書には、次の事に触れている。

「５　資格認証について　電子申請における医師、弁護士、行政書士等の本人性、資格保有等の証明については、地域住民の生活や行政手続の代理申請等の種々の場面で必要となるものであり、早期に制度検討が望まれる。」

現在稼働中の省庁電子申請システムで代理申請システムを導入しているのが、総務省、財務省、環境省、金融庁と一部のシステムのみである。４月には国土交通省がこれを実装する予定としている。こうした代理申請システムに、資格者たる行政書士等がどのような証明書で電子署名するかについては、未だに明確な法的結論は出ていない。

多くの行政書士は「申請現場で使えればよし」との感覚が多数を占めている現状である。

(5) 電子署名で手続きする社会とは、いったいどのような社会なのか

認証システムなり電子署名を説明するに、日本の印鑑文化と印鑑登録制度との類似点を強調する人が多い。印鑑、登録制度を持ち出すすことで、かえって認証システムなり電子署名を複雑にしている趣もある。中には、電子署名・認証業務法での認定を受けている電子証明書が実印であり、認定を受けていないのが認印だと主張するむきもある。

電子署名・認証業務法での解釈に誤りがあるのではないかとさえ思える。電子署名について印鑑文化を持ち出すと誤解を招くと言わざるを得ない。公開鍵暗号化方式での電子証明書技術は、そもそもがサイン（自署）文化での国が発祥である。

日本の行政手続では、押印の廃止へと向かっている。自署にて申請する方式が多くなっている。今後は、行政手続では電子署名（電子的自署）が必須との認識を醸成したいところだ。電子的印鑑ではない「電子的自署」なのだという認識である。

たとえば、現行の実印と印鑑証明書の取扱を考えてみよう。

役所に印鑑証明書交付申請するに、代わりのものもできる。また書類に押印するのも本人が了承すれば、代わりのものが押印できる。ようするに、押印やら証明書発行手続を代わりの者にさせることができる利便性が印鑑なのである。この利便性の認識が、電子署名のときに間違って取り込まれるのではないかと危惧する。

つまり、自身の秘密鍵電子証明書を他人に預ける者が出てくるということである。印鑑を預けて押印させているのだから、電子印鑑たる電子証明書も代わりの者に預けて電子署名させてもかまわないだろうとの認識である。これが、代わりの者が電子署名したのかどうかさえ解ら

なくなってくるのだ。

こうなると電子認証システムの根本的制度への無理解となってくる。電子署名・認証業務法の法的意味合いも瓦解してしまう。

印鑑制度をもちだすと、必ず誤解される所以である。

電子的自署とは、「あなた自身による手書き署名です」と言えるではないか。電子政府・電子自治体としても、電子署名の意味合いについて徹底して啓蒙していく必要がある。

4.3 政府・自治体の認証局の証明書の表現と将来の電子申請

(1) 「安全な通信を行うための証明書」という表現について

政府関係各省庁で、省庁や自治体の自己署名証明書を指して用いられる「安全な通信を行うための証明書」という表現はわかりづらく感じる。「SSL のサーバ証明書などを検証するために使用される」という意味合いから、安全に通信を行うために必要な証明書であるので間違いではない。しかし、自らの証明書（秘密鍵を含み、確実な手段でデリバリーされた PKI 証明書を特定の PC やデバイスにパスワード設定して格納したようなもの）や、公開鍵証明書（認証局のではないもの）との違いがわかりづらく、これらの違いを理解するにあたりマイナス要因として働くことが懸念される。

とはいえ、ほかに誤解を与えにくく、かつ平易で適切な表現も無いのも事実である。関係各省庁や自治体においては、表現方法による誤解を最低限に防ぐためにも、PKI についての知識が豊富でない人々にもわかりやすい解説・説明を付け加えていただきたいと望む。

(2) 「安全な通信を行うための証明書」をインストールする際の確認方法

「安全な通信を行うための証明書」が、無条件（パスワードの入力等を必要とせず）に PC にインストールできるのは良いのか？という疑問がメーリングリストで話題に上った。前節で述べたように、これは「自己署名証明書＝ルート認証局の証明書」を指しており、信頼ポイントとなる証明書であるので、この証明書の真正性を確認してからインストールすることは非常に重要である。この証明書が間違いなく総務省のものなのかをチェックするには、フィンガープリントの照合をする以外の方法はない。フィンガープリントについては官報等の信頼できる媒体にて掲載され、これらと照合することで確認が可能である。ただし、とある省庁においては通常の Web サイトに掲載されているものもあり（SSL ではなく、通常の HTTP)、この場合サーバが詐称される可能性を考えると、この情報のみを元に確認することはあまり推奨できない。これらを一般の人々が理解することを求めるのは難しく、フィンガープリントの公開方法にも工夫が必要と考える。

(3) 将来、ネットカフェ等の PC から電子申請できるようになるか

カードリーダも安価に販売されるようになってきており、多数の国民・市民が IC カードに格納された証明書を持つようになれば、ネットカフェ等の共用の PC からも電子申請などが可能になるのではないか？という趣旨の議論。

これについては、技術的には可能であると思われるが、解決していかねばならないセキュリティ上の課題が多く、時間はかかるのではないかと思われる。

また、「安全な通信を行うための証明書」等のルート証明書をネットカフェ等の PC にインストールできては危険ではないかとの指摘もある。これについては PKI の仕組みで解決できる問題ではなく、当該 PC の設定等に委ねられることになってしまう。ただし、ネットカフェ等の PC が信頼できないのは周知の事実であり、現状では、自分や、組織で信頼できる PC を使い申請するしかないだろう。

これについて、「自分が信頼する証明書は、自分のカード内に存在しており、それを信頼点として利用する仕組みが必要（信頼できない PC 内の証明書は利用しない）」との意見があがった。なお、欧州の ID カードプロジェクトでは、否認防止の証明書、認証・署名・暗号用の２種類のユーザ証明書に信頼点の証明書（CA の自己署名証明書）が入っているのが普通であるとのことで、我が国においてもこのような方式の採用も検討する必要があるのではないだろうか。

5．電子署名・認証の利用形態と利用動向

本章では、電子署名・認証の利用形態について、2002 年 2 月に実施した調査「電子署名及び電子認証の現状及び将来像に関する調査」と同じ電子署名・認証の先進ユーザを対象に再度同じ項目でアンケート調査を実施し、前回からの利用状況や導入検討状況の変遷を定量的に把握する。また、電子署名・認証を利用する上での阻害要因を整理する。

5.1 アンケート調査実施概要

アンケート調査の実施要領を表 5-1 アンケート調査は、2004 年 1 月 19 日に電子メールで ECOM 会員企業（正会員約 250 社弱）に質問表（本章の末に添付）を送信し、2004 年 2 月 13 日に回収することで実施した。回収調査票（有効分）は 45 票であり、それを集計対象票とした。

表 5-1 アンケート調査の実施要領

項目	実施要領
調査対象	・ECOM 会員企業
調査方法	・調査票は、Microsoft Word ファイルで作成 ・調査票発送は、上記ファイルを電子メール送信により実施 ・調査票回収は、電子メール受信および FAX 回収で対応
回収数	・有効回答数 45　（回収数は 48）
調査時期	・2004 年 1 月 19 日～2004 年 2 月 13 日

5.1.1 アンケート調査票回収企業の概要

回答企業の属性を図 5-1 から図 5-5 に示す。業種別では、前回に比べると多種の業種から回答が得られている。中でも情報サービス業からいずれも多くの回答が得られている。常雇用従業員規模については、前回は 5000 人以上の大企業からの回答比率が高かったが、今回の調査では規模に偏りなく回答が得られた。また、売上高や情報化投資額についても規模に偏りなく、広範囲の企業から回答が得られた。

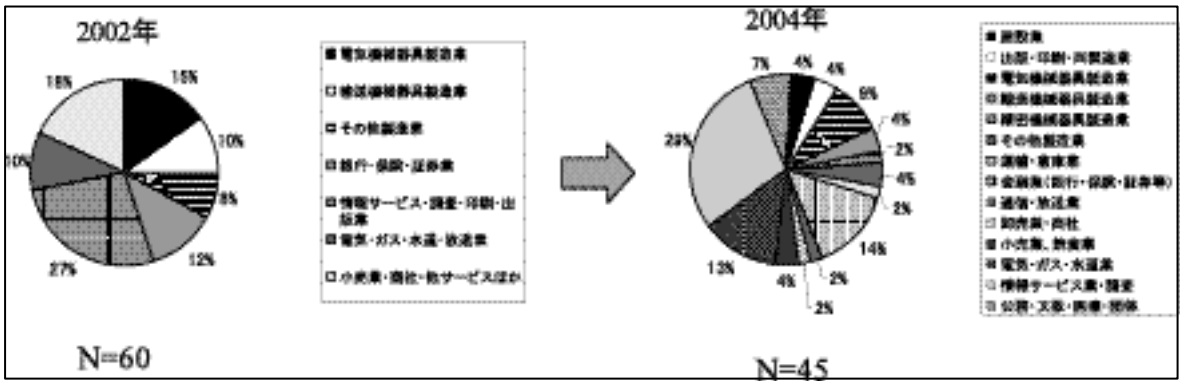

図 5-1 回答企業の業種

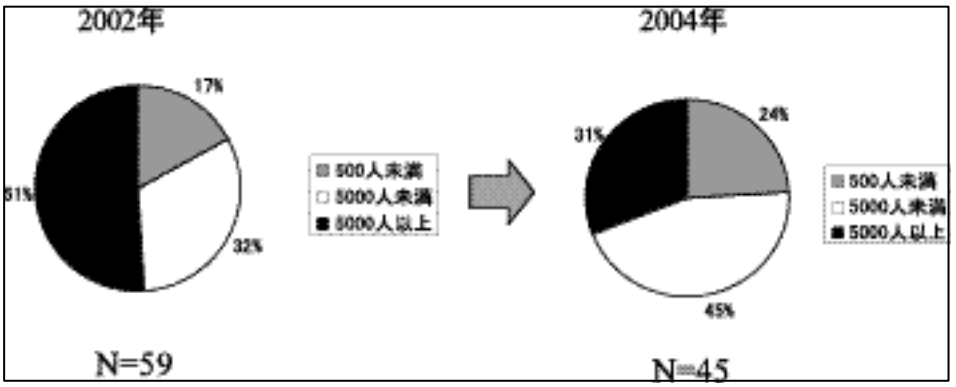

図 5-2 回答企業の従業員数

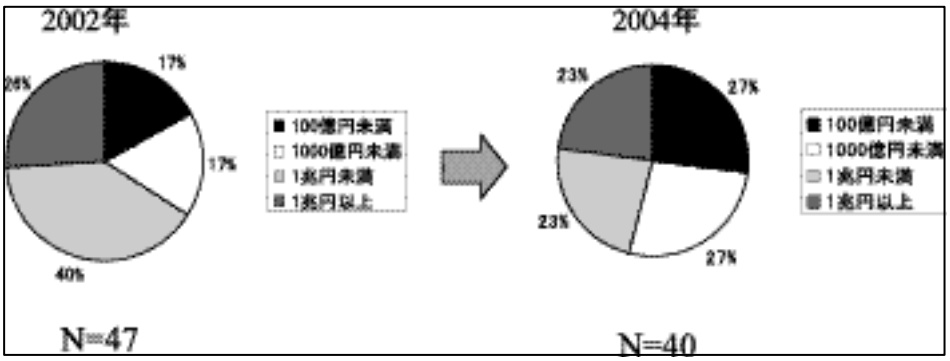

図 5-3 回答企業の売上高

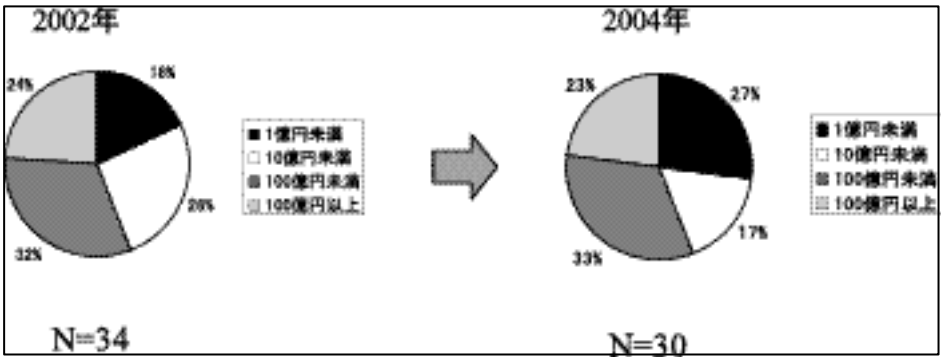

図 5-4 回答企業の情報化投資額

情報化投資額に占めるセキュリティ対策費については 2002 年の調査時点と比べると情報投資額の 10%以上の比率が大幅に伸びており、社会的な要請や企業の関心の高さを伺うことができる（図 5-5）。また、今後の通し額の見通しについても依然として同水準以上という、という傾向が強く見られる。

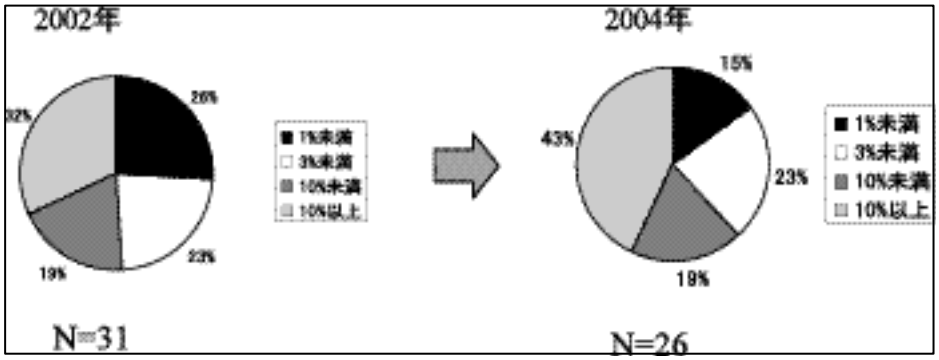

図 5-5 回答企業のセキュリティ対策費比率

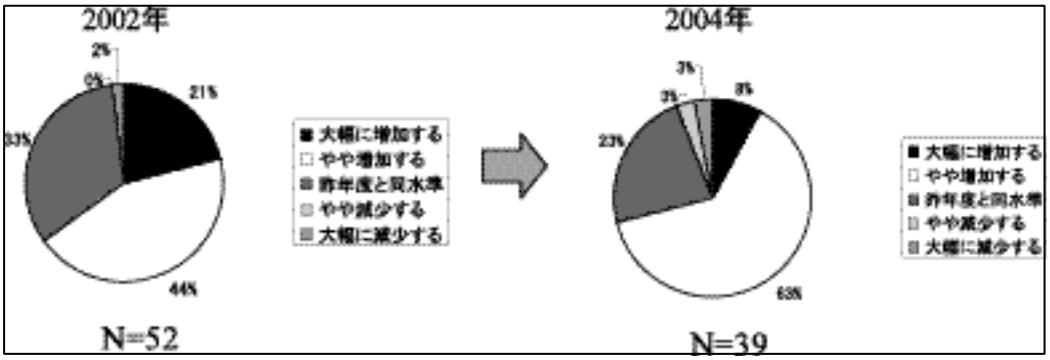

図 5-6 回答企業のセキュリティ対策額見通し

5.1.2 アンケート調査結果

ここでは､ECOM 会員企業向けに実施したアンケート調査より､PKI の利用の実態について整理、分析する。

(1) PKI の利用状況

PKI を現在利用している企業は、全体の半数以上の 55%となっている。PKI の導入可能性を最大限考慮すると、PKI を将来的に導入する可能性のある企業の比率は約 80%となる。

前回の調査結果と比較してみると前回 PKI を利用予定していた企業が実際に利用段階に入っているように見える。ただし、利用予定のないところは依然として同じ程度の割合いとなっており、必要のある企業、ない企業が二極化してきたようにも見れる。

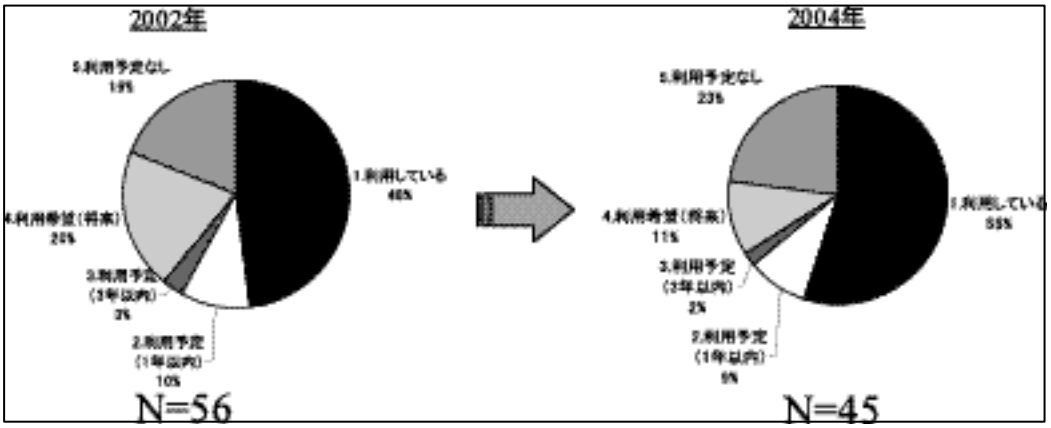

図 5-7 PKI の利用状況

(2) PKI の利用理由

PKI を利用している理由については､「セキュリティ技術面」によるところが最も多く、これは前回、今回ともに変わらない。

前回から特に違いの見られる項目は「６．取引相手の要望」で、前回の倍以上の選択率となっている。これは、電子政府のサービス開始を始めとした公共機関の仕様上の影響によるところが大きいと思われる。

その他の項目の回答傾向は前回と今回では、大きな違いは見られなかった。

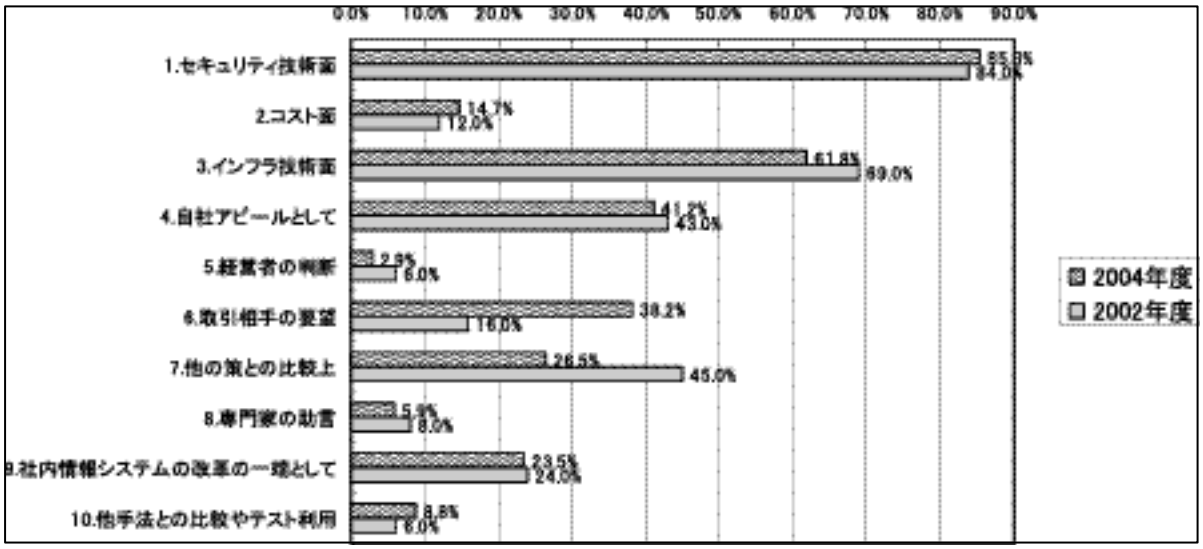

図 5-8 PKI の利用理由

(3) PKI の利用立場

PKI を利用する立場については、前回多かった「ユーザとして」の利用比率が更に増える結果（図 5-9）となった。

今回の調査分について、利用の内訳を分析した結果を図 5-10 に示す。利用で最も多かったのは、企業間取引（B to B）の業務利用である。この場合、認証局を自社で構築・運用するというケースも 3 割弱みられた。

B to C については、外部の機関に対外サーバを認証してもらい、一般向けに使用しているケースが多いものと思われる。

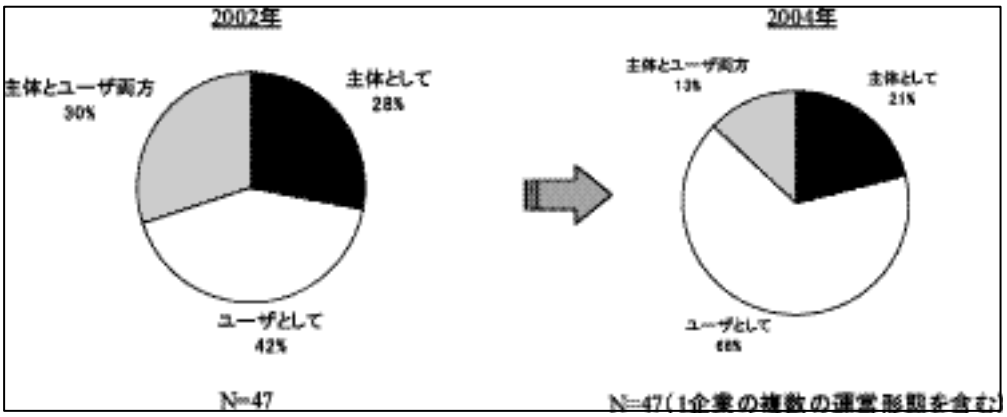

図 5-9 PKI の利用立場

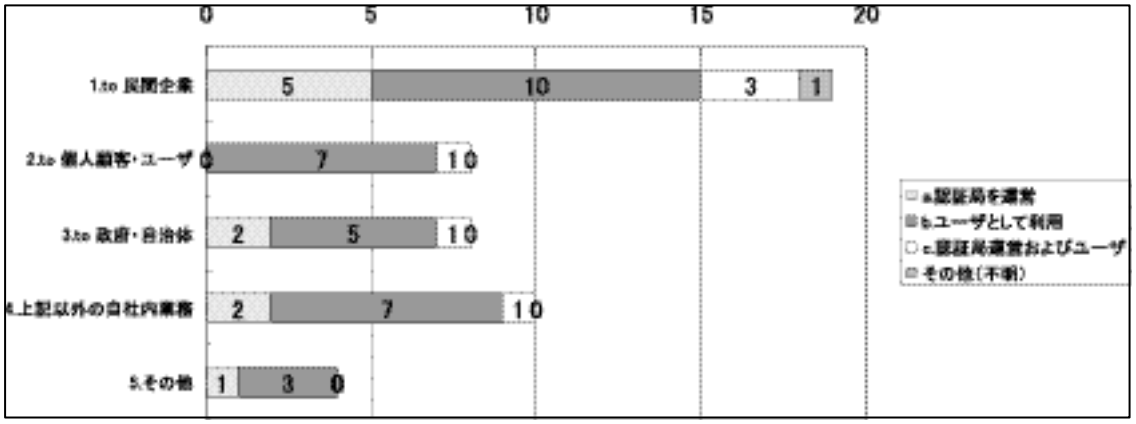

図 5-10 PKI の利用立場（内訳）

(4) PKI 認証局の運営方式

PKI 認証局の運営方式については、2002 年の調査では「認証局の全機能を内部化している」が最も比率が高かった。今回の調査でも同項の比率は大きく変わってはいないが、前回では少なかった「全機能を外部化（アウトソース）」の比率が飛躍的に上がり 2 極化の傾向がみられている。

これは一部の企業を除くと、認証局の運用業務を企業内で継続して行うのが（コストや人材的に）難しくなってきているためと推測される。

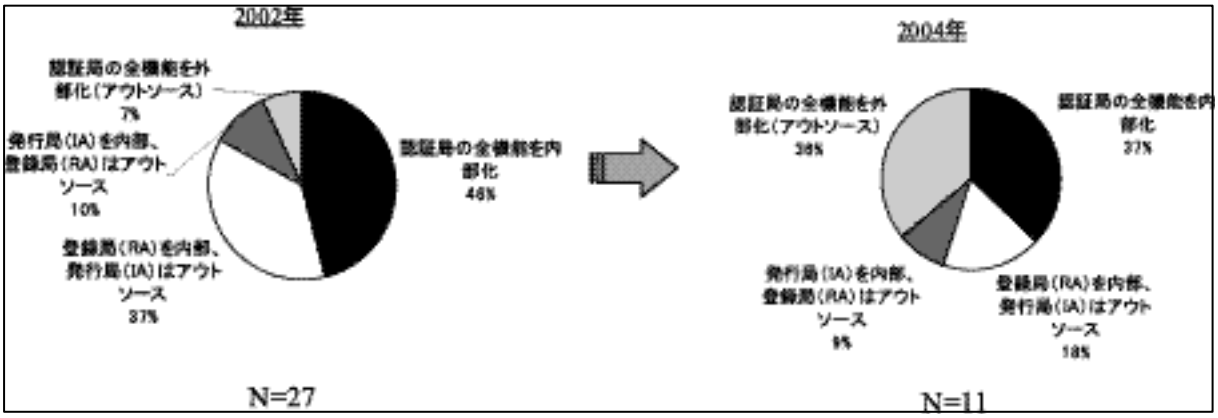

図 5-11 PKI 認証局の運営方式

(5) 認証機関の PKI サービスの利用状況

認証機関を運用している企業（８社）から得られた PKI システムの利用者数の結果は図 5-12 のようになった。比較的大人数の運用を行なっているケースが多いことがわかる。

また、当初計画からの比較では、「-50%～+50」「+50%以上」を合わせると 86%となり、計画以上の利用となっていることがわかる。

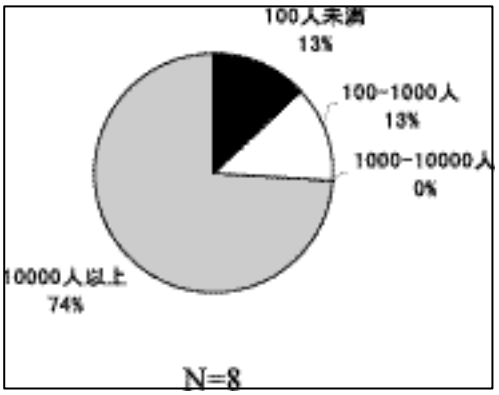

図 5-12 PKI システムの利用者数

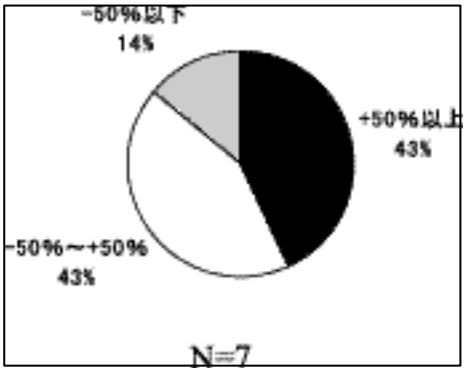

図 5-13 PKI システムの利用者数の計画値との乖離

(6) PKI システムの費用

PKI システムの費用（構築コスト、ランニングコスト）については十分な回答数が得られなかったため、統計的な整理は省略する。

参考までに得られた回答値を以下に示す。

◆認証局の機能を全て内部で行なう方式

	構築コスト（百万円）	ランニングコスト（百万円）
A 社	0.5	0.6
B 社	250	170

◆認証局の機能を全て外部で行なう（アウトソース）方式

	構築コスト（百万円）	ランニングコスト（百万円）
C 社	198	18
D 社	5.5	4

(7) PKI の課題

ここでは PKI の普及課題として、「PKI ユーザが感じている PKI の課題」および「PKI 非ユーザが PKI を導入していない理由」について調査分析を実施し、PKI の課題の位置付けを整理した。

コスト的な問題は導入前の時点で把握されているが、「２.技術、法制度面での信頼性」、「３.PKI システムの操作性/使い勝手」、「６.関連手続き、教育の煩雑さ」などは実際に導入してから課題が顕著となっている。

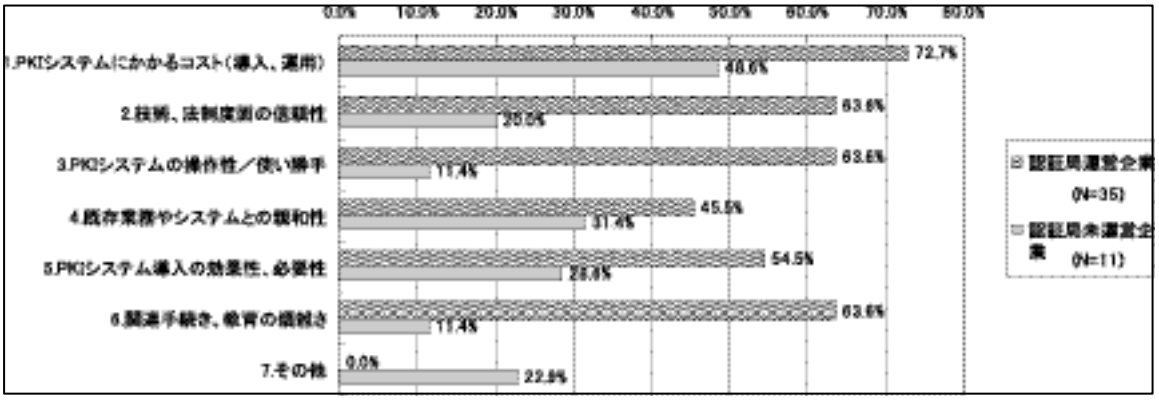

図 5-14 PKI システムの課題

アンケート内容

Q1. 貴社では PKI（公開鍵暗号基盤：Public-Key Infrastructure）を利用していますか。以下から１つだけお選びください。

1. 利用している
2. 利用していないが、１年以内に利用する予定である
3. 利用していないが、３年以内に利用する予定である
4. 具体的な計画はないが、利用したいと考えている
5. 利用していないし、予定もない

ご回答番号（　　）

→5.と回答した方は Q8.へお進みください

Q2. Q1 で「1～4」に回答した企業にお尋ねします。貴社で PKI を利用する理由をお聞かせ下さい。いくつでもお選びください。

1. セキュリティ対策上の用件を満足しているから
2. コスト面での要求を満足しているから
3. 今後の世の中のインフラ技術になると判断しているから
4. 信頼性／安全性等の自社アピールになるから（ユーザの囲い込み等）
5. 経営者が導入に積極的だから
6. 取引相手の要望があるから
7. 現状彩り得る方策として最良のものだから
8. セキュリティ関連の専門家の助言に従って
9. 社内情報システムの改革の一端として
10. 他の手法との比較や実験的なテスト利用のため
11. その他　→具体的に：（　　）

ご回答番号（　　）

Q3. 貴社では PKI をどのような業務に利用してますか（業務用途）。また、その業務は PKI をどのような立場で利用するものですか（利用形態）。以下から該当するものをいくつでもお選びください。

（業務用途）

1. 民間企業（顧客や取引先など）との電子商取引業務
2. 個人（顧客やユーザなど）との電子商取引業務
3. 政府、自治体との電子商取引業務
4. 上記以外の自社内業務（　　）
5. その他（　　）

（利用形態）

a. PKI を主体としてのみ利用している（自らの意思で認証局を持ち、証明書を発行している）
b. PKI をユーザとしてのみ利用している（他社が発行した証明書を取引に利用している等）
c. PKI を主体とユーザの両方を立場で利用している

ご回答（下記表枠で足りない場合は、枠を追加ください）

業務用途(1～5)	利用形態（a～c）	備考（具体的な業務内容等）

（Q4-Q7 は自社で PKI の認証局を運営されている企業の方への質問です。該当しない場合は、Q.8 へお進みください。）

Q4. 貴社の PKI システムの認証局はどのような運営方式ですか。複数の方式がある場合は、いくつでもお選びください。

1. 認証局の機能を全て内部で行う方式
2. 認証局の機能のうち登録局（RA）を内部に置き、発行局（IA）はアウトソースして運営する方式
3. 認証局の機能のうち発行局（IA）を内部に置き、登録局（RA）はアウトソースして運営する方式
4. 認証局の機能を全てアウトソースして運営する方式

ご回答番号（　　）

Q5. 貴社で運営されている PKI システムの利用者数（RA への登録者数）はどの程度ですか。またサーバ認証用の電子証明書の累積発行枚数はどの程度ですか。当初計画と現状の概算値（2004 年 1 月時点）についてご回答ください。

	当初計画	現状
利用者数（RA 登録者数）	人	人
サーバ認証用の電子証明書発行枚数	枚	枚

Q6. 貴社の PKI システムの費用（構築コスト、ランニングコスト）はおよそどの程度ですか。Q4 でお答えいただいた方式毎にご回答下さい。（下記表枠で足りない場合は、枠を追加ください）

認証局方式番号（Q4 の 1-4）	構築コスト	ランニングコスト（注）
	百万円	百万円／年
	百万円	百万円／年

注：ランニングコストは、人件費、回線利用料、サービス利用コスト等を全て含むものとします。

Q7. 貴社では、PKI についてどのような点に課題を感じていますか。<u>いくつでも</u>お選びください。

1. PKI システムにかかるコスト（導入、運用）
2. 技術、法制度面の信頼性
3. PKI システムの操作性／使い勝手
4. 既存業務やシステムとの親和性
5. PKI システム導入の効果性、必要性
6. 関連手続き、教育の煩雑さ
7. その他　→具体的に（　　）

<u>ご回答番号（　　）</u>

PKI を利用していないあるいは自社で認証局を構築・運用していない企業の方にお尋ねします。

Q8. PKI を利用していない、あるいは自社で認証局を構築・運用していない理由をお聞かせ下さい。いくつでもお選びください。

1. PKI システムにかかるコスト（導入、運用）が高い
2. 技術、法制度面でまだ信頼できる段階でない
3. PKI 関連製品の操作性／使い勝手が悪い
4. 既存業務やシステムをどの程度変更しなければならないか不明である
5. PKI システム導入の効果性、必要性を感じない
6. 関連手続き、教育が煩雑である
7. その他　→具体的に（　　）

ご回答番号（　　）

Q9. 貴社の業種は何ですか。取扱額の多いものを以下から１つだけお選びください。

1. 農林水産業、鉱業、窯業	9. 鉄鋼・非鉄金属・金属製品製造業	17. 卸売業・商社
2. 建設業	10. パルプ・紙・紙加工品製造業	18. 小売業、飲食業
3. 食料品・飲料・たばこ製造業	11. 繊維・衣服・その他繊維製品製造業	19. 電気・ガス・水道業
		20. 情報サービス業・調査
4. 出版・印刷・同関連業	12. 化学工業、石油・石炭製品製造業	21. マスコミ・広告業
5. 一般機械器具製造業	13. その他製造業	22. その他のサービス業
6. 電気機械器具製造業	14. 運輸・倉庫業	23. 公務・文教・医療・団体
7. 輸送機械器具製造業	15. 金融業（銀行・保険・証券等）	24. その他（　）
8. 精密機械器具製造業	16. 通信・放送業	

ご回答番号（　　）

Q10. 貴社の常雇用従業員数はどのくらいですか。以下から１つだけお選びください。

1. 100 人未満	4. 500～1000 人未満	7. 3000～5000 人
2. 100～300 人未満	5. 1000～2000 人未満	8. 5000 人以上
3. 300～500 人未満	6. 2000～3000 人未満	

ご回答番号（　　）

Q11. 貴社の昨年（2002 年）１年間の売上高はどのくらいですか。

昨年１年間（2002 年）　→　　百万円

Q12. 貴社の昨年１年間（2002 年）の情報化投資額はどのくらいですか。また、その中に占めるセキュリティ対策関連投資額の割合はどのくらいですか。おおよその比率（%）をお答え下さい。なお、ここでいう投資額とは、情報システムや通信システムの導入に関わるハードワエア関連諸経費、ソフトウェア関連諸経費、サービス／回線使用量他関連諸経費、人件費、保守・運用関連諸経費の合計と定義します。

昨年（2002 年）１年間の情報化投資額　　→　　百万円
上記費用に占めるセキュリティ対策費の比率　　→　　%程度

Q13. 貴社のセキュリティ対策関連投資額は、今後どのようになるとお考えですか。昨年（2002 年）１年間の投資額を基準にご回答下さい。以下から１つだけお選びください。

1.大幅に増加する　　2.やや増加する　　3.昨年度と同水準　　4.やや減少する 5.大幅に減少する

ご回答番号（　　）

Q14. 最後にあなた様のお名前、会社名、所属部署名、役職、連絡先をご記入下さい。

お名前				
貴社名				
所属部署名			役職	
ご連絡先	TEL		e-mail	

ご協力ありがとうございました

6．平成 15 年度活動概要

6.1 JESAP 運営委員会活動概要

今年度開催された運営委員会の紹介を行う。（所属・役職は発表当時のまま）

(1) 第１回 JESAP 運営委員会

テーマ「公的個人認証（個人証明証）」

①「公的個人認証の今後の展開」猿渡　知之　企画官（総務省　自治行政局）

②「個人向け証明書の検討」前田　陽二主席研究員（ECOM）

(2) 第２回 JESAP 運営委員会

テーマ「教育分野における利用」

①「教育分野における証明書の利用」前田　陽二主席研究員（ECOM）

(3) 第３回 JESAP 運営委員会

テーマ「属性認証」

①「医療分野における証明書の活用」喜多　紘一（財）医療情報システム開発センター）

②「認証における属性情報の活用（JCSI が発行する属性型証明書)」栗原　達雄（日本認証サービス（株))

③「属性証明に関する代理士業のあり方について」河端　祐一（全国社会保険労務士会連合会）

④「教育分野における証明書の活用」桑原　悟（新潟国際情報大学）

(4) 第４回 JESAP 運営委員会

テーマ「電子決済、電子納税及び金融機関における電子決済について」

①「電子政府の総合窓口（e-Gov）と各府省電子申請システムの連携イメージ」
（財務省　会計センター　横江宏文上席専門官）

②「国税電子申告・納税システム」（国税庁　官官房企画課　遠山金一主査）

③「金融機関がネット上で提供する個人向け電子支払手段の概要」
（(財）金融情報システムセンター　調査部　杉崎博氏）

(5) 第５回 JESAP 運営委員会

①「アジア PKI フォーラムの活動概要と加盟各国の PKI への取組」宮崎　敦夫（日本 PKI フォーラム）

②「バイオメトリクス、スマートカード、PKI 連携の欧米における動向」松本　泰（JNSA）

③「モバイルコマースにおける PKI の現状と課題－mITF モバイルコマース部会認証 WG の活動状況－」田中俊昭（KDD 研究所：モバイル IT フォーラム　モバイルコマース部会技術専門委員会　認証 WG リーダ）

(6) 第６回 JESAP 運営委員会

テーマ：JESAP 報告書２００３　提言内容について

6.2 普及広報活動概要

JESAP 主催のフォーラム（電子署名・認証フォーラム）を年２回開催するとともに、各地で活躍する団体と共催の講演会を３回行った。

(1) 電子署名・認証フォーラム

① 第１回電子署名・認証フォーラム

期日：平成１５年9月２４日（水）～２５日（木）

会場：工学院大学新宿キャンパス（東京都新宿区）

出席者：２２１名

プログラム委員：(アイウエオ順)

佐藤　慶浩（情報ネットワーク法学会）
鈴木　優一（エントラストジャパン株式会社）
塚本　克治（工学院大学）
前田　陽二（電子商取引推進協議会）
松本　　泰（セコム株式会社）
松山　博美（電子商取引推進協議会）
牟田　　学（行政書士）
安田　直義（株式会社ディアイティ/JNSA）

プログラム：

第１日目：9月２４日

挨拶

濱中栄治（電子商取引推進協議会事務局長）

講演１　公的個人認証サービス利用における展望

大山永昭（JESAP 運営委員長／東京工業大学工学部フロンティア創造共同研究センター教授）

パネルディスカッション１　公的個人認証サービス利用促進のための提言

コーディネーター：大山永昭（JESAP 運営委員長／東京工業大学工学部フロンティア創造共同研究センター教授）

パネラー：　佐藤純通（日本司法書士会連合会副会長）
牟田学（電子申請情報サイト運営／行政書士）
前田陽二（電子商取引推進協議会主席研究員）
松本泰（セコム(株) TS 事業部ソリューション技術部）
山碕良志（総務省自治行政局自治政策課課長補佐）

講演２　ネットワーク社会における“安全と信頼”の構築に向けた政府の取り組み

印南朋浩（経済産業省商務情報政策局情報セキュリティ政策室室長）

講演３　新しい社会システム創出へ向けて

田尾陽一（JESAP 運営委員会部会長／セコムトラストネット(株)代表取締役社長）

パネルディスカッション２　電子署名・認証からみた eJAPANII 推進への提言

コーディネーター：牧野二郎（牧野法律事務所弁護士）

パネラー：　瓜生和久（経済産業省商務情報政策局情報政策課長補佐）
小村元（富士通(株) ソフト・サービス事業推進本部電子行政事業推進統括部統括部長）
鈴木優一（エントラストジャパン(株)最高技術責任者）
安田直義（(株)ディアイティ技術本部開発部／特定非営利活動法人日本ネットワークセキュリティ協会主席研究員）
米倉昭利（(財)日本情報処理開発協会電子署名・認証センター長）

講演４　電子署名・認証利用に向けた課題と展望
松山博美（電子商取引推進協議会主席研究員）

第２日目：９月２５日

＜A会場＞

〔セッション A1 電子申請とビジネス支援〕
座長　牟田　学（電子申請情報サイト運営／行政書士）

講演　コンパクト・ポータル
木村吉博（東京大学大学院新領域創成科学研究科環境学専攻博士課程）

講演　専門職代理人の電子申請ビジネスモデル
大野実（全国社会保険労務士会連合会）

講演　国税電子申告・納税システム（e-Tax）と税理士事務所認証局その技術的・法的考察
齋藤聰明（東京税理士会理事）
阿部隆幸（関東信越税理士会川口支部）

講演　神戸港における港湾物流情報プラットホーム（PF）輸入実証実験について
向井芳樹（神戸市みなと総局経営部企画情報化主査（IT 担当））

〔セッション A3 利用モデル紹介〕
座長　鈴木優一（エントラストジャパン(株)最高技術責任者）

講演　東日本電子認証普及促進協議会の取組みについて
大友洋一（東日本電子認証普及促進協議会／東北電力(株)）

講演　東日本認証センターの展開について
遠藤恵美子（東日本認証センター運営事務局／東北インフォメーション・システムズ(株)）

講演　「Patease」における個人情報保護機能
植田均（(株)ステラクラフト）

講演　IT 書面一括法・電子署名法の対応した電子契約サービスのご紹介と導入事例
千田一樹（(株)エヌ・ティ・ティ・データ産業システム事業本部）

〔セッション A3 実現方式〕

座長　松本泰（セコム(株) TS 事業部ソリューション技術部）

講演　JAVA JCE を使った GPKI 対応パス認証／パス構築ライブラリィの試作

稲田龍（富士ゼロックス(株) ISC ソリューション開発センター）

増田健作（富士ゼロックス情報システム（株)）

講演　DocuWorks 5.0 に組み込まれた電子署名機能

稲田龍（富士ゼロックス(株) ISC ソリューション開発センター）

講演　CryptoAPI を使った S/MIME アプレット

澤野弘幸（(株)オレンジソフト）

講演　電子署名に必要なタイムスタンプ

上畑正和（セイコーインスツルメンツ（株）ソリューション事業統括本部ソリューションビジネス部担当部長）

＜B会場＞

〔セッション B2 電子署名の利用ビジョン〕

座長　松山博美（電子商取引推進協議会主席研究員）

講演　電子認証の利用検討－リアル社会との連携

千葉昌幸（三菱総合研究所(株)）

前田陽二（電子商取引推進協議会主席研究員）

講演　電子証明書を活用した品質劣化保証モデル

立川雅章（(財）国際研修協力機構）

講演　セキュリティ社会におけるロボットへの期待

小林一清（(有）東京機械工業）

講演　電子署名に基づく電子地域通貨について

山崎重一郎（特定非営利活動法人電子認証局市民ネットワーク福岡）

〔セッション B3 将来ビジョン〕

座長　安田直義（(株)ディアイティ／特定非営利活動法人日本ネットワークセキュリティ協会主席研究員）

講演　インターネットレジストリにおけるレジストリデータの保護と応用

木村泰司（(社）日本ネットワークインフォメーションセンター）

講演　複合社会における電子認証ビジョン（衛星運用管制の視点から）

野村和哉（富士通(株) 宇宙システム部）

＜C会場＞

〔セッション C1 応用および関連技術〕

座長　塚本克治（工学院大学大学院情報通信システム研究室教授）

講演　決済機能を持つ簡易な DRM システムについて

天野光司（工学院大学情報学専攻修士２年）

塚本克治（工学院大学大学院情報通信システム研究室教授）

講演　耳介による個人認証
篠原克幸（工学院大学大学院画像応用工業研究室助教授）
講演　電子文書の原本性確保を支える一翼としての電子認証
山本隆彦（(株)松村組情報システム部／（社）日本土木工業協会 CALS/EC 部会電子文書原本性 SWG）
講演　長期署名フォーマットに基づくデジタル署名文書の長期保存について
宮崎一哉（三菱電機(株) 情報技術総合研究所情報技術総合研究所）

〔セッション C2 個人認証と運営〕
座長　佐藤慶浩（情報ネットワーク法学会理事／日本ヒューレットパッカードアジアパシフィック・セキュリティ・コンサルティングマネージャ）
講演　電子政府認証基盤を活用するコンパクト・ポータル～C2G2B モデル
木村吉博（東京大学大学院新領域創成科学研究科環境学専攻博士課程）
講演　電子署名・認証の普及に資する認証局監査のあるべき姿について
丸山満彦（監査法人トーマツエンタープライズリスクサービス部シニアマネージャー）
野見山雅史（監査法人トーマツエンタープライズリスクサービス部システム監査技術者・公認情報システム監査人）
講演　電子身分証明書トークンの日欧比較
林慶司（セコム(株)IS 研究所）
講演　水平的な手続整備に向けて～個人情報保護と PKI～
木村吉博（東京大学大学院新領域創成科学研究科環境学専攻博士課程）

〔セッション C3 属性認証及び利用モデル〕
座長　前田　陽二（電子商取引推進協議会主席研究員）
講演　電子署名利用形態に関する考察－属性情報の分析
田中稔（三菱電機インフォメーションシステムズ(株)インターネットセキュリティセンター担当部長）
前田陽二（電子商取引推進協議会主席研究員）
講演　属性型証明書の実例と利用形態
町田陽（日本認証サービス(株)企画担当部長）
講演　電子手形サービスにおける電子認証について
八ツ井博樹（信金中央金庫）
講演　使って楽しい PKI（PKI の普及のために）
谷口誠（東京税理士会情報システム委員会／行政書士谷口事務所）

② 第２回電子署名・認証フォーラム
期日：平成１６年２月２３日（月）～２４日（火）
会場：工学院大学新宿キャンパス（東京都新宿区）

出席者：２５８名

プログラム委員：(アイウエオ順)

川松　和成（電子商取引推進協議会）
佐藤　慶浩（情報ネットワーク法学会）
鈴木　優一（エントラストジャパン株式会社）
塚本　克治（工学院大学）
前田　陽二（電子商取引推進協議会）
松本　　泰（セコム株式会社）
牟田　　学（行政書士）
安田　直義（株式会社ディアイティ/JNSA）

プログラム：

第１日目：２月２３日

挨拶

宮川秀眞（電子商取引推進協議会所長）

講演１　日本のセキュリティ対策における認証（仮題）

印南朋浩（経済産業省商務情報政策局情報セキュリティ政策室長）

講演２　公的個人認証サービス利用・電子申告（仮題）

岩崎吉彦（国税庁長官官房企画課情報技術室長）

講演３　公的個人認証サービス利用・パスポートの電子申請（仮題）

北村進（外務省領事移住部旅券課）

講演４　公的個人認証サービス利用の展望（仮題）

大山永昭（JESAP 運営委員長／東京工業大学教授）

パネルディスカッション　公的個人認証サービス展開と課題（仮題）

コーディネーター：大山永昭（JESAP 運営委員長／東京工業大学教授）

パネラー：　印南朋浩（経済産業省商務情報政策局情報セキュリティ政策室長）
岩崎吉彦（国税庁長官官房企画課情報技術室長）
北村進（外務省領事移住部旅券課）
松本泰（JESAP 企画委員／セコム（株）TS 事業部ソリューション技術部）
鈴木春洋（JESAP 企画委員／（株）中電シーティーアイ）

第２日目：２月２４日

＜A会場＞

〔セッション A1 標準・実装〕

座長：安田直義（(株）ディアイティ技術開発本部／特定非営利活動法人日本ネットワークセキュリティ協会主席研究員）

講演　W3C XKMS を適用した認証サーバーの試作

武田哲（三菱電機（株））

講演　電子署名・認証の活用と情報セキュリティ関連規格

日笠光一郎（(財）日本品質保証機構 IT 事業部部長）
講演　UTF8 問題と移行のシナリオ
島岡政基（セコムトラストネット（株））

〔セッション A2 証拠性〕
座長：塚本克治（工学院大学大学院情報通信システム研究室教授）
講演　PKI 活用したアカウンタビリティ保証モデルの提案
立川雅章（(財）国際研修協力機構国際部）
講演　電子商取引トランザクションの証拠性を確保するスキームの提案
半田富己男（大日本印刷（株））
講演　電子文書の原本性確保を支える一翼としての電子認証　その２
山本隆彦　（(株）松村組）

〔セッション A3 認証〕
座長：鈴木優一（エントラストジャパン（株）最高技術責任者）
講演　属性認証利用ガイドライン
前田陽二（電子商取引推進協議会主席研究員）
東山栄一（NEC ソフト（株））
講演　属性認証による匿名認証システム
加藤岳久（東芝ソリューション（株））
講演　宇宙ステーションにおける認証サービスの実現方法
野村和哉（富士通（株））

＜B会場＞
〔セッション B1 事例と動向〕
座長：佐藤慶浩（情報ネットワーク法学会）
講演　たいせい G-net.における電子署名契約の導入
鼠入俊之（大成建設（株））
講演　UFJ 銀行が提供する融資契約の電子化サービスについて
川島慶一（(株）UFJ 銀行）
講演　バイオメトリクス認証におけるプライバシー問題への各国対応状況
池野修一（セコム（株））

〔セッション B2 電子政府〕
座長：牟田学（電子申請情報サイト運営／行政書士）
講演　電子政府における民間認証業務について
佐藤孝一（(株）中電シーティーアイ）
講演　扶養控除等申告書の電子化についての試案（法令編）
阿部隆幸（阿部隆幸税理士事務所）

講演　扶養控除等申告書の電子化についての試案（技術・総括編）
齋藤聰明（東京税理士会理事）
講演　電子自治体における個人情報への権限認証とアクセス制御について
山崎重一郎（近畿大学）

〔セッション B3 事例紹介〕
座長：松本泰（JESAP 企画委員／セコム（株）TS 事業部ソリューション技術部）
講演　ネットワークセキュリティにおける PKI 利用技術の紹介
芦川宏（(株）中電シーティーアイ）
講演　認定認証局の運用と電子署名・認証の普及促進について
村瀬晋二（(株）中電シーティーアイ）
講演　電子署名がビジネスを変える
村井克規（サートラスト（株））
講演　Web サービスによる暗号化／電子署名サーバーの実現
澤野弘幸（(株）オレンジソフト）

＜C会場＞
「公的個人認証サービス普及解説講習会」
「チャレンジ PKI 成果報告会」

(2) 共催講演会
① 電子認証普及・啓発セミナーin 秋田
期日：平成１５年１０月２４日（金）
会場：ホテルメトロポリタン秋田（秋田市中通）
出席者：１４０名
プログラム：
挨拶
龍田勝利(東日本電子認証普及促進協議会会長／テクノ・マインド(株) 代表取締役会長）
基調講演　電子政府・電子自治体構築における公的電子認証の取組み
山崎良志（総務省自治行政局自治政策課課長補佐）
講演　電子商取引における電子認証の展開
松山博美（電子商取引推進協議会主席研究員）
講演　保険業界における活用事例と活用モデルの提案
立川雅章（電子署名・認証利用パートナーシップ（JESAP）運営委員／（財）国際研修協力機構国際部）
パネルディスカッション　今後の e ビジネスの発展と PKI の展開について
モデレーター：新堀聡（日本ユニシス（株）アドバンステクノロジ本部事業開発統括部ビジネスアグリゲーション部長）
パネリスト：　山碕良志（総務省自治行政局自治政策課課長補佐）

松山博美（電子商取引推進協議会主席研究員）
立川雅章（電子署名・認証利用パートナーシップ（JESAP）運営委員／（財）国際研修協力機構国際部）
吉野恭司（秋田県産業経済労働部長）
國井匡裕（東日本認証センター運営事務局／東北インフォメーション・システムズ(株)取締役社長）

② 情報セキュリティ普及啓発セミナー

期日：平成１５年１２月１２日（金）
会場：長良川国際会議場及び岐阜ルネッサンスホテル（岐阜市長良福光）
出席者：２００名
プログラム：
主催者挨拶
辻正（経営情報化協会理事長）
前田陽二（電子商取引推進協議会主席研究員）
基調講演１　情報セキュリティ総合戦略
印南朋浩（経済産業省商務情報政策局情報セキュリティ政策室室長）
基調講演２　情報セキュリティをめぐる動向
佐々木良一（東京電機大学工学部情報メディア学科教授）
パネルディスカッション　公的個人認証制度と地方自治体における電子行政取り組みの現状
コーディネーター：岩田彰（名古屋工業大学副学長）
パネラー：　佐々木良一（東京電機大学工学部情報メディア学科教授）
印南朋浩(経済産業省商務情報政策局情報セキュリティ政策室室長）
坂口　裕信（岐阜県知事公室情報政策課　課長）
本田　祐吉((株) サイバーウェイブジャパン　取締役 EC 事業部長）
鈴木　春洋（(株) 中電シーティーアイ理事　先端 IT 開発部長）
前田陽二（電子商取引推進協議会主席研究員）

③ 電子認証普及・啓発セミナーin 札幌

期日：平成１６年２月３日（火）
会場：札幌全日空ホテル（札幌市中央区）
出席者：２１３名
プログラム：
挨拶：
早坂英二（東日本電子認証普及促進協議会副会長）
基調講演　PKI への取り組みをはじめとする我が国の情報セキュリティ政策の最新動向
山崎琢矢（経済産業省商務情報政策局情報セキュリティ政策室課長補佐）
講演１　電子商取引における電子認証活用の展望

前田陽二（電子商取引推進協議会主席研究員）

講演 2　事例に見る電子認証の重要性

川島昭彦（日本ベリサイン株式会社代表取締役社長兼 CEO）

パネルディスカッション　今後の e ビジネスの発展と PKI の展開について

コーディネーター：山本強（北海道大学大学院工学研究科教授）

パネリスト：　山崎琢矢（経済産業省商務情報政策局情報セキュリティ政策室課長補佐）

籔紀洋(北海道総合企画部 IT 推進室情報政策課地域情報化グループ主幹）

前田陽二（電子商取引推進協議会主席研究員）

川島昭彦（日本ベリサイン株式会社代表取締役社長兼 CEO）

畠山樹代実（ほくでん情報テクノロジー株式会社データセンター事業部長）

執筆者一覧

委員	桑原　　悟	新潟国際情報大学	2.3
委員	鈴木　優一	エントラストジャパン(株)	3.1
委員	栗原　達雄	日本認証サービス(株)	3.2
委員	牟田　　学	牟田学行政書士事務所	1.2
委員	山崎重一郎	近畿大学	2.5
委員	米倉　昭利	財）日本情報処理開発協会　電子署名・認証センター	3.3
委員	喜多　紘一	財)医療情報システム開発センター	2.4
委員	大野　　実	全国社会保険労務士会連合会	2.2.2
委員	田中　一志	日本税理士会連合会	2.2.3
委員	佐藤　純通	日本司法書士会連合会	2.2.4
委員	中西　　豊	日本行政書士会連合会	2.2.1
企画委員	松本　　泰	セコム（株）	2.1
部会	伏見　　諭	（株）情報数理研究所	4.1
部会	家森　　健	行政書士	4.2
部会	岩崎　貴行	（株）シーエーシー	4.3
事務局	前田　陽二	電子商取引推進協議会	1.1／1.3／5／6

（敬称略）

電子署名・認証利用パートナーシップ報告書 2003
―活動と提言―
平成 16 年３月発行

発行所　財団法人　日本情報処理開発協会
　　電子商取引推進センター
　　東京都港区芝公園３丁目５番８号
　　機械振興会館３階
　　TEL：０３（３４３６）７５００
印刷所　新高速印刷株式会社
　　東京都港区新橋５丁目８番４号
　　TEL：０３－３４３７－６３６５

（本報告書は再生紙を使用しています。）　15-E008

ISBN4-89078-614-7 C2055

定価 5,000円（本体4,762円＋5％税）