14－ E007

電子署名・認証利用パートナーシップ
報告書 2002

平成15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。

国内の電子認証利用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、電子認証利用にかかわ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運営委員会を開催し、電子署名・認証を推進している団体や利用を進めている団体の活動報告を行い情報の共有を図るとともに、２つの部会（利用促進、連携・調整）を秋に立ち上げ具体的な検討に入りました。

本調査研究は、この部会での議論を中心に JESAP の活動を紹介するものです。部会での議論は短期間のため多くは結論が出ていませんが、電子署名・認証の推進の一助になれば幸いです。

平成１５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　トヨタ自動車(株)
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 岩田 和晃	日本ボルチモアテクノロジーズ(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 郷田 慎一	(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)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 高橋 則彦	(株)東京三菱銀行
委 員 立川 雅章	三井住友海上火災保険(株)
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	「マナブーズ・ルーム」サイト運営
委 員 山崎　重一郎	NPO 電子認証局市民ネットワーク福岡
委 員 米倉 昭利	(財)日本品質保証機構
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 赤地 祐一	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　小松　靖　　総務省 行政管理局
オブザーバ　猿渡 知之　　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　大野 秀敏　　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　長谷川　清次　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（委員会運営）
中川　宏之　日本 PKI フォーラム（委員会運営）
松山　博美　電子商取引推進協議会（WEB 制作・広報担当）
川松　和成　電子商取引推進協議会（委員会担当）
小祝　香織　電子商取引推進協議会（委員会・講演会担当）

目　次

序章

「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ました。

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ます。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ました。具体的には、平成 13 年 10 月から平成 14 年６月まで、JESAP を正式に発足させるための準備として、40 名を超える有識者が６回にわたり、「PKI 推進における課題」を中心にテーマ発表と討議を行い、解決すべき課題、運営のありかた等について検討してきました。

そして平成 14 年６月３日には、設立準備会での検討結果を踏まえ、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りました。以後、本年３月４日の第８回運営委員会まで、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ました。さらに、運営委員会で提言のあった課題の詳細検討を行うために、利用検討部会と連携・調整部会の２つの部会を８月に発足させ、９月より本格的な活動が開始しました。

本報告書は、電子政府に関連した活動と JESAP 運営委員会に参加している団体を中心に PKI 推進に係わる団体を紹介するとともに、利用検討部会と連携・調整部会の２つの部会において行われた検討内容を整理したものです。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します。

平成 15 年 3 月　電子署名・認証利用パートナーシップ運営委員会
委員長　大山　永昭

1．電子署名・認証利用パートナーシップ

(JESAP：Japan Electronic Signature and Authentication Partnership)

1.1　設立目的

インターネット上での取引（電子商取引）が経済活動の中で急激に広がりつつある。この電子商取引を安全かつ確実に行うためには、直接顔の見ることのできない取引相手を確認することや、情報の内容を第三者に改ざんされない仕組みを構築することが必要であり、このための中核技術として公開鍵基盤（PKI）がある。

政府および地方公共団体では電子政府実現のため GPKI（政府認証基盤）、LGPKI（地方自治体認証基盤）の構築が進められている。一方では電子署名の法律上の取扱いを明確にすべく、平成 13 年４月に電子署名及び認証業務に関する法律（電子署名法）が施行され、また法人認証については法務省が商業登記に基づく電子認証サービスを開始している。

また、民間企業において、インターネットを活用したビジネス活動が本格化しつつあるが、より安心かつ安全なネットワーク基盤としての PKI 利用も進展しつつあり、今後急速に立ち上がることが期待されている。

この PKI が急速に浸透していく過程においては、全く新しい制度や取決めを作り出していくことが重要になってくる。そしてこれらは、民間主導、かつ、世界的視野に立つものでなければならない。また、PKI 推進を巡る様々な課題について、個別の利害を超えて統一的なフレームを策定するために、ユーザの視点で PKI に関係する有識者が議論し、政府に具体的提言をしていくことが重要である。

このような状況において、国内における PKI 推進活動は、これまで政府、地方公共団体、業界団体、ユーザ企業等の組織ごとに進められており、必ずしも統一的な方針、さらにいえば、多くのユーザの意見を集めた接続性、運用性を重視したものになってはおらず、かつ、PKI 推進にかかわる情報の公開も十分ではないといった課題がある。

そこで、「電子署名・認証利用パートナーシップ」はかかる状況を鑑み、広く PKI 推進にかかわる団体や有識者が集まり、各団体の成果・課題等の情報を収集・蓄積・共有し、PKI 相互運用性の確保などの共通課題についてはユーザの視点で検討を行える場を提供するとともに、蓄積された各団体の成果、検討結果の普及、啓発活動に取り組む体制を設立するものである。

1.2　活動方針/運営理念

欧米、アジアにおいては、図 1-1 に示すとおり PKI に関する標準化や相互運用性等の検討組織が立ち上がり、活動を行っている。

JESAP を日本国内における PKI 推進のポータルな活動と位置付けその活動理念は以下のとおりである。

1.2.1 中立性、公開性の維持

特定の企業、省庁からの影響から独立した検討が進められる環境を維持する。また活動の中心は関連団体とのパートナーシップを主眼としており、参加団体、企業、個人の従来の活動を尊重し、議論の内容は Web 等での公開を前提とする。

1.2.2 広い層からの参加

全国各地の PKI 有識者が参加可能とすべく、電子会議、メーリングリスト等インターネットを利用して討議できる環境と運営を積極的に採用する。また、特定分野の専門家による、技術論、制度論を中心とした活動よりも広く利用者の視点での運用性、利便性などを重視した意見、要望を吸い上げる。

1.2.3 国内各業界に対する影響力の維持

民間を代表するオープンな PKI イニシアチブとしての地位を確立する必要がある。このためには、国内各業界を含むできるだけ多くの関係者の意見を集約して提言できる体制にしていく必要がある。さらに、日本の PKI に関わる最優秀技術者・有識者が結集できる体制にしていかなければならない。

図 1-1 世界の PKI 推進団体

1.3 活動の概要

「電子署名・認証利用パートナーシップ」の主要な活動として次の 2 つの活動がある。ひとつは PKI ユーザ団体と PKI ベンダーが連携して PKI 推進上の課題を抽出して整理・検討し、要望や提言をまとめる活動であり、もうひとつ多くの情報を共有・整理しユーザに対する PKI 利用促進のための情報提供等を行う活動である。各活動の概要（図 1-2）を以下に述べる。

1.3.1 課題抽出および検討活動

PKI を推進する団体やその利用が予定される業界団体等と連携し、政府認証基盤/地方公共団体認証基盤（GPKI/LGPKI）と民間との相互運用性や相互認証など、以下に示すような共通的な課題と対応策を検討し、情報･意見交換を踏まえて要望又は提言等を行う。

① ユーザの視点に立った課題の整理/検討
　使いやすさ、取引の安全保障、など
② 法律制度面の課題と整理/検討
　公的個人認証の扱い、など
③ PKI 構築に関する技術課題の整理/検討
　属性の扱い、長期保存、相互運用性、など

1.3.2 情報収集および普及活動

PKI 導入・利用のためのユーザーガイドの作成や研修会を実施することにより、PKI に関する情報の普及、共有化を図る。その活動例を以下に示す。

① 地方開催を含む研修会/シンポジウム、法律等専門家の講演
② 「電子署名・認証利用パートナーシップ」のホームページの開設・運営
③ PKI 導入事例の紹介
④ その他利用促進事業の検討

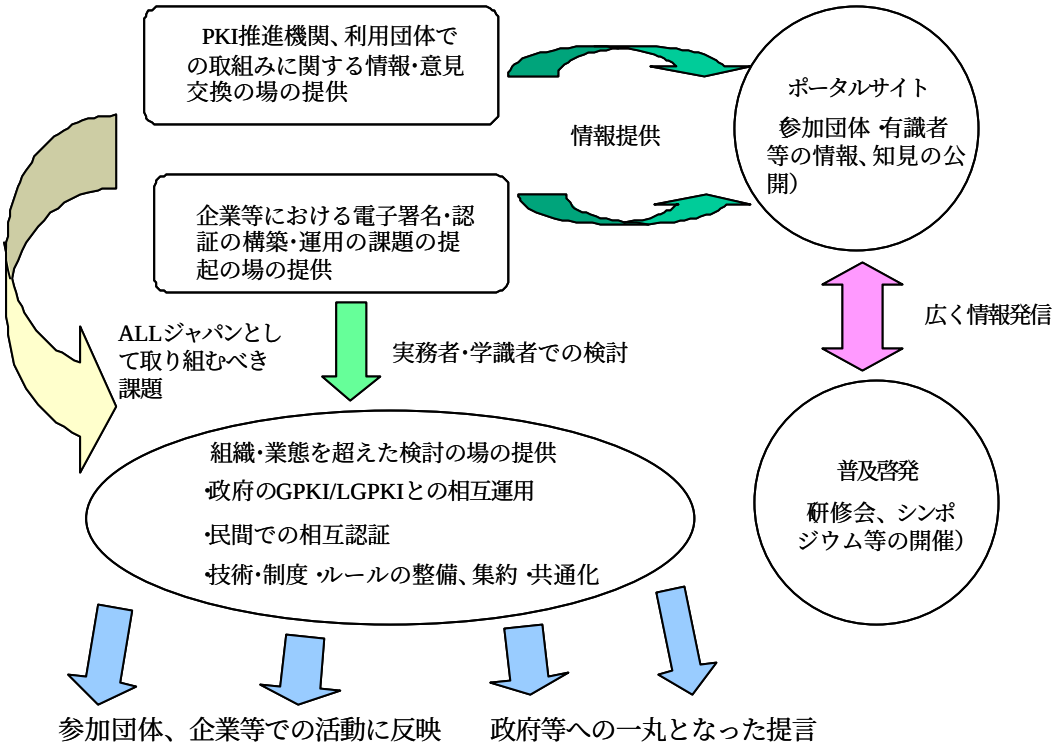

図 1-2 活動の概要

1.4 推進体制

PKI 推進にかかわる団体、及び有識者からなる運営委員会と、特定の条件なしに参加登録できる利用促進部会、連携・調整部会で構成される。各部会は必要に応じて WG を設定し議論を行う。リアルな会合以上に Web の掲示板などを多用して、遠隔地の部会メンバーがバーチャル上で参加できる検討体制とする。

1.4.1 運営委員会

情報交換および課題の整理・検討を行う。特に他の PKI 推進団体の活動内容およびその団体やユーザ団体（企業）が抱える課題について情報交換する。

課題の一部については利用促進部会、連携・調整部会において検討する。

1.4.2 利用促進部会

運営委員会等で出された課題のうち、利用者の観点、特にヒューマンインターフェースなど利用環境あるいは利用者のリテラシー向上のために今後何が必要になるか等の検討を行うとともに、PKI の普及広報活動の検討を行う。

1.4.3 連携・調整部会

運営委員会等で出された課題のうち、日本の PKI を推進するという視野に立って、相互

運用に関する検討、政府が運営する認証局についてユーザの観点からのチェック等を行う。

1.4.4 事務局

JESAP 事務局は当面、ECOM と PKI-J（日本 PKI フォーラム）の研究員が兼務で対応し、下記の事務を担当する。

- 運営委員会事務局
- 地方開催を含む講演会・シンポジウムの実施
- JESAP のホームページの運営

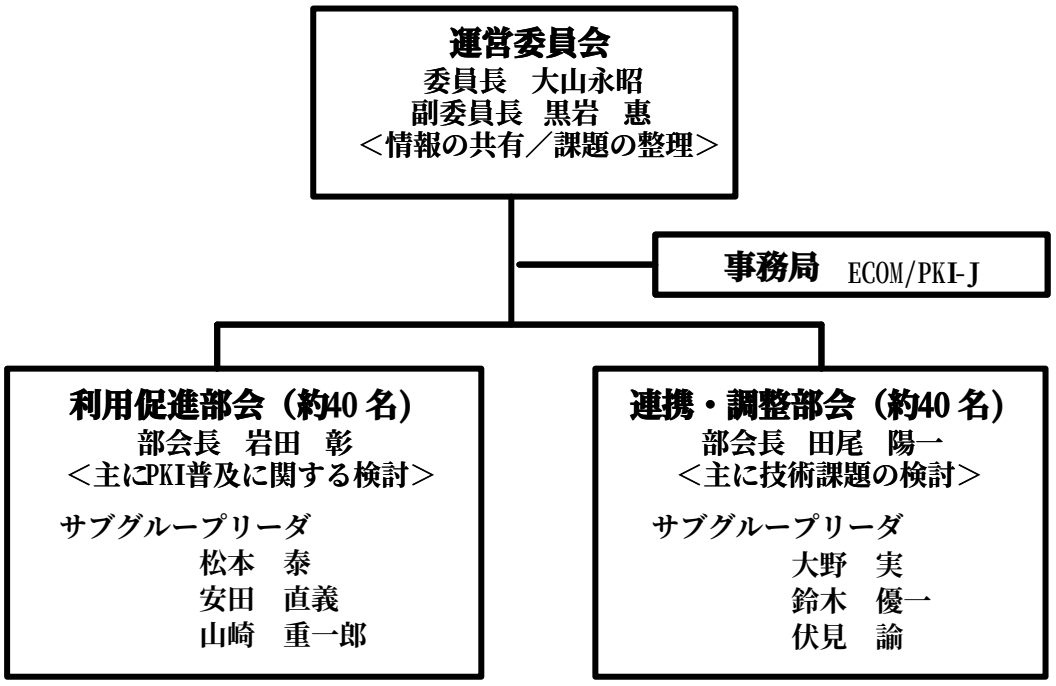

図 1-3 JESAP 推進体制

2．JESAP の活動報告

2.1　利用促進部会の活動報告

2.1.1　概括～PKI の三つの用途、二つの普及アプローチ

2.1.1.1　PKI プレーヤー拡大の必要性

PKI の必要性を説くことは、抽象論の範囲ならたやすい。インターネットに確実な本人確認の手段が必要なことや電子署名が必要なことは、インターネットを社会や経済の中でより高度に活用しようとしている人なら誰もが認めることである。しかし、現時点において、実際に PKI を日常的に利用している人、さらに言えば、PKI を日常的に使う必然性を本当に実感している人はどのくらいいるのだろうか。

PKI は、情報化社会の新しい社会制度の基盤となるものである。したがって PKI が電子政府などのフォーマルな用途の観点からシステムや制度が設計され普及が推進されること自体は自然なことである。

しかし、PKI が本当の意味で新しい社会インフラとしてそのコストとバランスするだけのメリットを社会に提供するようになるためには、行政機関や代理業（いわゆる士業）の関係者だけを対象にするだけでは明らかに不足であり、一般の民間人もプレーヤーにする必要がある。

デジタル証明書や電子署名などを適切に使用するには、一種のリテラシーが要求される。しかもそのハードルは決して低くはない。

PKI のプレーヤーになるということは、年に１回か２回電子署名をするというレベルではなく、PKI の概念や操作に習熟して日常的にデジタル証明書を使いこなすということである。

もちろん、一般の民間人がこういう面倒なことを学習してまで使うようになるには、明確なメリットが必要であることは言うまでもない。

PKI の利用を促進するための提言を行うには、現在と連続した形でどのように PKI の利用が展開されていくのかという具体的なビジョンを示す必要がある。

本節では、PKI の主要な用途の観点から、PKI の利用の大きな方向性について議論する。

そしてさらに、電子申請や届け出といった類のフォーマルなもの以外に、一般の市民生活の中でカジュアルに使われることを目的とした新しい PKI アプリケーションの試みについても言及する。

2.1.1.2　PKI の三つの用途～秘匿通信、認証、電子署名

PKI の主要な用途は、秘匿通信、認証、電子署名の三つであると言ってよい。

この三つの用途は、必要とする前提条件が質的にかなり異なっている。この中で最もハードルが低いものが秘匿通信であり最もハードルが高いものが電子署名である。そして、

実際の PKI の利用も、秘匿通信、認証、電子署名の順序で普及するであろう。

(1) 秘匿通信

秘匿通信のニーズは切実である。

秘匿通信で PKI を利用する理由も明確である。

暗号通信を行うには効率のよい共通鍵暗号が利用されているが、共通鍵暗号を使った暗号通信では、事前に通信を行う双方が暗号鍵を共有するための安全な手段が必要である。PKI は、この暗号鍵の安全な交換を実現する理想的な環境を提供する。事前に鍵交換を行うことが困難な場合や、暗号化通信を行う拠点が増えるに従って、秘匿通信に PKI を利用する有効性が高まる。

例えば、SSL のサーバ認証は、すでに金融関係や電子商取引のサイトなどでは当然のものになっている。現時点で最も中心的な PKI の用途と言ってよいであろう。

この SSL サーバ認証の目的は、実際にはサーバを認証したいということよりは、むしろそのサーバとクライアントとの間の通信を暗号化するための鍵交換のために利用されているというのが実状だと言って良い。これによって、パスワードやクレジットカード番号や利用者の個人情報などが盗聴から守られるということがより切実なニーズになっている。

また、最近では、無線 LAN の普及により、無線通信の秘匿化のニーズが高まっている。無線 LAN では、予想外の範囲の人に無線通信を傍受される危険性があることが広く認知されてきたためである。

セキュアな無線 LAN 通信の標準である IEEE 802.1X を実装した無線 LAN 装置や認証サーバが一般に手軽に利用可能になってきたために、これの利用を目的とした PKI の利用が今後進むことが予想される。これが一般化すれば、SSL のサーバ認証よりも遙かに大量のデジタル証明書が発行されることになるであろう。

他にも、拠点間の通信を暗号化する IPSec などの手段を用いた VPN も、拠点の数が増加するにつれて、事前に鍵を設定する方法よりも PKI を利用する方法が合理的になる。

多数の事業所や拠点を持つ企業や団体では、PKI を利用した VPN を活用するケースが増えることが予想される。また、PHS や携帯電話を使った無線通信にも無線 LAN と同様の傍受の危険性が存在するが、そういったモバイル環境でも VPN を使った秘匿通信が重要になってくるであろう。

ただし、現時点ではまだこれらの技術の実装は完成の域に達しているとは言いがたい。導入にあたっては、相互運用性や操作性などにまだまだ問題は残っている。しかし、こういった課題を一つ一つ解決していくことで、秘匿通信を目的とした PKI の利用は近い将来に大幅に進むものと予想される。

(2) 認証

PKI とは、インターネットの中の仮想世界の行為主体と現実世界の人物とをがっちりと結

びつけ、確実な本人認証を行うためのインフラであると言うことができる。

この認証を利用するアプリケーションとして現時点で代表的なものは SSL のクライアント認証であろう。しかし、SSL のクライアント認証は普及しているとは言い難い。

普及しない理由は明らかである。現在のほとんどのインターネットサービスでは、SSL サーバ認証による秘匿通信の下でのユーザ ID とパスワードによる利用者認証で十分であり、PKI に基づいた個体認証は必要ないからである。

しかし、将来的には、PKI を使った利用者認証は重要なものになる可能性がある。

インターネットでは、サーバの下に利用者がいるのではなく、利用者の側が主体となってサーバを選択してサービスを受ける広域分散型システムが基本である。

このような広域分散システムで利用者を認証し、適切な権限を割り当てる方法として、集中管理型でない PKI は適している。

ただし、個体認証だけで誰にどこまでの権限を割り当てるかということを判断することは極めて困難である。実際に機能する利用者認証を行えるようにするためには、PKI の個体認証と結びつけられた属性認証やアクセス制御ポリシー管理をきちんと統合的に設計する必要がある。

このような、PKI に基づいたアクセス制御の研究はすでにいくつか登場しているが、まだ未解決な問題がいくつも残っており、しばらくは腰を据えた研究が必要である。

PKI を使った個体認証は、こういった研究が成果をあげ、属性認証などを含めた実装が共通の枠組みの中で容易に利用可能になった時点で大きく発展することになるだろう。

ただし、利用者認証の手段は、PKI 以外にも技術的な選択肢がある。またサービスの観点から見ると、利用者認証の目的は PKI が提供する個体認証ではなく、その個体が持つ属性の認証である。PKI が将来も利用者認証の手段として最も合理的なものであり続けるかどうかは不明である。

(3) 電子署名

電子署名は、現在の技術では、PKI 以外の方法では実現不可能なものである。

PKI の用途の本命は電子署名であると言っても過言ではないであろう。

電子署名を行うための実装もすでに存在している。S/MIME 対応の電子メールソフト、及びいくつかのアプリケーションでは、すでに実用的に利用できるレベルにある。

しかし、電子署名の利用はブレークしていない。

その理由は、技術的課題よりもむしろ社会制度や慣習的側面およびリテラシー的側面による障壁が大きい。

PKI の用途の中で、電子署名の利用が最も時期が遠いと予想されるのはこのためである。

デジタル証明書を取得すれば、電子署名付きの文書を作ることができる。しかし、その電子署名は何を意味しているのか、どういう目的のために利用できるのか、そして電子署名を付けることに何の現実的メリットがあるのか、といった利用者の疑問に答えることは

難しい。

確かに、電子署名法によって電子署名が法的に位置づけられたことは大きなインパクトがあった。しかし、現在の電子署名法は、大ざっぱに言って、実印レベルの電子署名を定義したという地点に留まっていると言ってよいだろう[1]。

一般的な民間人は、日常生活において、実印を使うことはめったに無い。生涯に数回あるかどうかというところだろう。民間人が実印を使用するそのような生涯の大イベントを電子的に行うということは、現実的に考えてみて当分の間はありそうもない。

電子署名の普及を阻害している要因の中のリテラシー的側面に対しては、草の根的なアプローチが可能かもしれない。一般の民間人が日常的に電子署名を使い、その概念や操作などに慣れ親しむ機会を作ることを一つの目的とした PKI アプリケーションを考えることができる。

2.1.1.3 普及に向けた二つのアプローチ

JESAP の参加メンバーは、色々な異なるモチベーションにより JESAP に参加しており、PKI（電子認証、電子署名）に対する取り組みも様々なものがある。そのため、PKI に対する認識も取り組みも大きく異なり、利用促進に対する考えも全く異なった見方からの意見が出ている。ただし、「PKI の普及とは、証明書の普及ではなく、そのアプリケーションの普及にある」という点については、利用促進に関する共通の認識となっている。

---

[1] なお、本部会でなされた「実印」レベルの電子署名という把握に対しては、以下のような二つの意見が寄せられている。いずれも、本質的な指摘と思われる。

[意見①] そもそも、リアルワールドでの取引において用いられている「実印」は、法律レベルで定義されているものではなく、印鑑登録制度という社会制度と結び付けられて、一定の取引類型において用いられているものである。一方、電子署名法第3条は、電磁的記録に記録することができる情報について行われる措置であって、当該情報が当該措置を行った者の作成に係るものであることを示すためのものであり、当該情報について改変が行われていないかどうかを確認することができるものであるもの（すなわち、電子署名法第二条の「電子署名」）のうち、一定の要件を満たすものについて、民事訴訟法上の推定効が受けられる「押印」と同等の効力を認めた規定であり、民事訴訟法上の推定効の要件である「押印」は「認印」であっても構わない。したがって、電子署名を「実印」相当と理解又は表現することは誤りであり、誤解を招くおそれがある（法務省からの見解を元に文章を事務局作成）。

[意見②] 印鑑登録制度という社会制度（これ自体は地方自治体レベルのもの）と結び付けられている「実印」は、唯一のものである。一方、PKIによる電子署名は、例えそれが厳格なポリシ[例、証明書の拡張鍵使用目的(extendedKeyUsage)に、nonRepudiation bit がOnになっている私有鍵でかつ、本人の署名時に画面上等で適切な確認措置をとったと認められた署名のみを有効とみなすmachine readableなポリシ]で運営されているものであろうとなかろうと、私有鍵を複数持つことは可能である。こうした、《一対多》の関係からすると、「実印レベル」という表現は厳格なポリシで運営されているPKIでなされた電子署名を指し示すメタファーとして適切ではない（日本司法書士会連合会から参加された委員の見解を元に文章を事務局作成）。

この共通認識を出発点として、利用促進のアプローチについて大別を試みると、以下のように方向性の違う二つがある。

(1) 法制度などの整備と共にセキュリティの基準を満足させるために使用せざる得ない状況になるという普及のパターン（フォーマルで公共財的な方向性）。

(2) 使えるアプリケーションが PKI を意識することなく使用されることが普及を促進する（カジュアルで草の根的な方向性）。

前者は、インターネットにおいて、健全なセキュリティを持った社会の建設という側面があり、そのために、トップダウンに普及を進めて行くといった考えがある。しかし、本当にインフラを実現するためには、多くの壁を乗り越えていく必要があることを多くの人が痛切に感じているのではないだろうか。

後者は、利用者の利便性を前面に、インターネットの爆発的な普及と同じように、便利だから普及する、簡単に使えるから普及するといったものを目指している。

本部会で出た意見は、必ずしもこの二つに分けられる訳ではないが、どちらかの性格を持った利用促進に関する多くの意見があった。

2.1.2 カジュアルな PKI〜で気軽に利用するためのアプローチ

PKI をカジュアルに利用できるアプリケーションシステムの例として、電子地域通貨システム Travecoup と P2P 型のネットワークシステム VPC を紹介する。また、今後、PKI をバックエンドとする情報システムを草の根的に普及させるための、構築要件を考察する。

2.1.2.1 電子地域通貨システム Travecoup

Travecoup は、電子署名で作られた決済専用の電子通貨である。

Travecoup は、特定非営利活動法人電子認証局市民ネットワーク福岡（CACANet 福岡）によって開発された。

日本円などの法定通貨は、貴重であるが故に価値がある。

法定通貨の価値は、通貨の供給量と景気のバランスによって決定される。したがって、中央銀行による通貨供給量の管理が非常に重要になる。この管理に失敗すると通貨システムが崩壊する。

これに対して、「私はこの券と引き替えで 1 時間の介護サービスを行います」という券を考えることが可能である。このような券を「自己償還型債券」と呼ぶことにする。

自己償還型債券の価値を信頼し認めるコミュニティでは、この券を決済手段として受け入れることが可能である。そしてこの券を流通させることによって実質的に通貨として利用できるようになる。

自己償還型債券の価値は、通貨供給量に影響されない。

もし、日本円が 100 分の１に暴落したとしても、介護１時間券の価値はやはり介護サービス１時間受けられるという価値を持ち続ける。つまり、自己償還型債権を通貨と考えるとこの通貨システムは、中央銀行によってコントロールされなくても自律的に機能する。

地域通貨とは、一定のコミュニティで自主的に通貨を発行して流通させてしまおうという活動である。地域通貨は、地域の中に潜在している財やサービスを担保として通貨を発行し、それを地域の中で環流させることによって地域経済の活性化とグローバル経済からの保護がはかれると言われている。

従来の電子マネーは、「貴重なお金」のデジタル版を作ろうと努力してきた。

デジタルデータは、完全な複製をほとんどコスト無しにいくらでも生成できるため、「貴重なデータ」を作るのは技術的に非常に困難である。

これに対して、自己償還型債券による地域通貨は、ぜんぜん貴重なものではない。決済が必要になったとき、必要なだけのお金をその場で発行して使うことができるため、金融機関からお金を借りる必要もない。

自己償還型債券は、通貨発行者が「私は、この証書と交換で～という財やサービスを提供します」という意志を表明した文書によって実現される。

電子署名を用いれば、このような文書を電子化することはたやすい。

そして、電子署名法によって、このような文書の法的な効力も保証されている。

紙は優れたデバイスである。

電源なしで高精細度の表示が可能、小さく折り畳んでポケットに入れて持ち運ぶことができ、偽造はかなり困難で、暗証番号なしで手渡した瞬間に決済を完了することができる。

貨幣の電子化は、紙幣に対する優位点を良く考えてから実施しなければ必ず失敗する。

電子署名による電子貨幣は、紙幣よりも優れた性質も持っている。現在のスキャナやプリンタを用いると、紙幣の偽造は比較的簡単であり、偽造を防ぐ印刷物を作るのはコストがかかる。これに対して電子署名の偽造は極めて困難でありチェックも簡単である。

自己償還型債券による貨幣は貴重なものではないので、これを電子署名によって実現すると、紙や印刷機なしにいつでもどこでも端末一つで通貨発行ができるようになる。これも貨幣の電子化の大きなメリットの一つである。

従来の研究では、希少な電子貨幣を作ろうとして努力が行われてきたが、貨幣の電子化のメリットをわざわざ捨てていたともいえる。

電子地域通貨システム Travecoup は、自己償還債券を PKI を用いる電子署名付き文書として実現したシステムである。WEB メールをベースにした、だれでも簡単に使えるものである。

Travecoup には、この他にもコミュニティの中にある財やサービスや求められている財やサービスの情報を共有するシステムや通貨の価値を時間と共に減価するシステムなども盛り込まれている。

地域コミュニティの中にある財やサービスを交換する決済に Travecoup を使うことは、地域の活性化という効果と同時に、一般の民間人が電子署名を日常的に使うことによって、PKI の概念や操作に自然に接近できるという効果が期待できる。

2.1.2.2　P2P 型のネットワークシステム VPC

従来は、インターネットでビジネスを行うためにはサーバが必要であった。

しかし、P2P（Peer to Peer）型というネットワークシステムを用いれば、近い将来に、携帯電話だけでインターネットビジネスを開始できるかもしれない。P2P 型ネットワークシステムとは、全ての端末システムがサーバにもクライアントにもなるシステムである。

携帯電話で稼働する P2P 型ネットワークシステムを利用すると、携帯電話がブラウザになるだけでなく、サーバにもなれるようになる。

P2P 型ネットワークシステムを使ったコンテンツ流通は、一つのサーバに多数のクライアントがアクセスするというモデルではなく、端末から端末へコンテンツをコピーする行為の連鎖によって行われることになる。

これまで P2P 型ネットワークシステムというと、違法コピーの天国のようなアンダーグラウンドな場として認知されてきた。

これに対して、VPC（Virtual Private Community）は、PKI をベースに信頼できる権限管理を可能にする P2P 型ネットワークシステムである。

自分が何かコンテンツを作成したとしよう。

このコンテンツを誰かの端末にコピーしてしまうと、あとは自分の携帯の電源を切ってしまっても、そのコピーのコピーが増殖していくのを待つだけで、コンテンツが配信され、しかも、そのコピーが利用されるたびに、自分のところに使用料が次々に入ってくるという仕組みを構築するのが VPC である。

VPC は、富士通研究所で研究開発が進められているシステムである。昨年、名古屋市で PDA を使った実験が行われたが、今年は携帯電話を使った実験が行われる。

VPC は、利用者の権限に応じた適応能力を備えたシステムである。

サイバー法の研究者として著名なレッシグは、サイバースペースにおいて、プログラムの仕様（code）が利用者を制約する力は、法律（code）と同じくらい強力であると述べている。

VPC は、利用者の権限に対応した仕様のプログラムのみを実行可能にするよう制御することによって、P2P 型のコンテンツ配信においてアクセス制御を実現する。

例えば、コンテンツの使用料金が未払いの利用者には、最初の 10 秒間だけの再生のみを行う仕様のプログラムのみが実行でき、使用料金を支払った利用者には、コンテンツの全体を再生する仕様のプログラムを実行できるようにする。

VPC では、このような利用者適応を信頼できるものにするために、耐タンパ装置の内部で利用者の権限の判断や実行可能なプログラムのローディングの制御を行うことを想定して

いる。この内で、利用者の権限を判断する機構のことを「トラストエンジン」と呼んでいる。

トラストエンジンは、PKI による個体認証と属性証明書に基づく属性認証、およびコンテンツと共に配信されるポリシー証明書の三つの電子署名付きデータによって制御される。各端末は、それぞれの所有者のデジタル証明書とその秘密鍵が格納されている。また、利用者の属性は、属性認証機関が発行した属性証明書として表現され、やはり端末システムに格納されている。また、必要に応じて対価の支払いなどを契機にして属性認証機関から属性証明書を発行してもらうこともできる。

VPC においてはコンテンツとそのコンテンツを処理するプログラム群は一体化されて配信される。

利用者のコンテンツに対する権限を VPC ではロールと呼んでいる。ロールの実体は、その権限で実行可能なプログラムの集合体である。

ポリシーは、どのような属性を持った人にどのようなロールを割り当てるかという規則の集合である。コンテンツの発行者がこのポリシーを定める。ポリシーにコンテンツ発行者が電子署名を施したものをポリシー証明書と呼んでいる。

VPC では、コンテンツ、コンテンツの処理プログラム、ポリシー証明書の３組をポリシーサービスパッケージ（PSP）と呼んでいる。VPC を使って配信されるコンテンツとは、実際はこの PSP である。

VPC は、PKI による利用者認証を本格的に利用するアプリケーションである。

広域分散環境における属性認証やポリシー管理のための統合されたスマートなアーキテクチャを備えている。

PKI は、P2P 型ネットワークシステムのような本格的な広域分散システムに出会って初めてそのメリットが実感できる認証インフラであると言うことができるかもしれない。

2.1.2.3　カジュアルなアプリケーションと草の根的なアプローチ

カジュアルなアプリケーションの普及のためには、草の根的な啓蒙、啓発といった普及活動によるアプローチが必要となろう。法制度などの整備によるアプローチでは、その性格から、PKI は敷居が高く、認証局の運用は難しいという印象を与えている。実際、多くの人にとって認証局は、神秘的にも思えるのではないか。しかし、実際には、認証局の運用といっても、色々なレベルがあり、軽い運用の認証局が多数あっても全く問題がないはずである。こうしたことは、実際に自分で認証局を立ち上げて見ないとなかなか分からない。そして、実は、認証局の運用はさほど難しくない、使えるアプリケーションもあるといったことを、啓蒙、啓発していくことも重要ではないかという意見がある。

三文判 PKI の要求は、難しいこと抜きで使ってもいいのではないかという発想と、そもそも、三文判 PKI という保障レベルの PKI の基準もあってもよいではないかという発想の二つがある。いずれにせよ、高い保障レベルの PKI だけが重要であるということはないと

いう点で一致している。

使いやすいアプリケーションの普及が PKI の普及を促すという認識は一致している。しかし、電子政府等で要求されるような「実印」レベルの押印に相当する電子署名といってしまうと、そのセキュリティレベルの問題に重きを置かれ、なかなか使いやすいというレベルまで到達しないように思われる（実社会でも、「実印」の押印がなされる場面では、利便性の要請よりも他の要請の方がしばしば重視される）。

電子政府等が要求する「実印」相当の電子署名とは逆に発想に、カジュアルな PKI アプリケーションがある。今日、社会インフラとしてのインターネットの重要性について、多くの人々が実感していることは間違いない。しかし、社会インフラとなったが故に、そのセキュリティの問題の解決が大きな課題になっている。そうした中で、「便利だけど安全」を目指すカジュアルな PKI アプリケーションへの要求は確実にあるものと思われる。

2.1.3 フォーマルな PKI～法制度的な整備を通じ公共財的に利用していただくアプローチ

2.1.3.1 法制度などの要因からの普及

米国で PKI が広く使用されつつある例として医療関係がある。これは、医療保険の積算と責任に関する法律（略称 HIPPA）が原動力になっている。米国では、こうした医療情報の IT 化に関する法的な未整備状態が改善されつつあり、結果、医療情報の IT 化を促進している。こうした動きは、何らかの形での政府関与がないとなかなか動かない。医療情報の IT 化は、誰もが望んでいることのように思われるが、実際には既存の仕組みがあり、IT 化は既存の制度や仕組みを多少なりとも変更しなければ機能しない。法制度があるから普及するというのではなく、本来あるべき姿にするための目標があり、そのための制度、及び、PKI 等で実現される機能があるといった構図が必要だと思われる。こうした動きが、結果として、色々な業界における IT 化を進め、ひいては、日本の IT 技術の国際競争力強化にもつながるのではないだろうか。

こうした法制度などの整備から普及を促す為には、PKI などの運用基準などの整備はかかせない。実際、電子署名法の特定認証業務認定などはこうした動きのひとつだと考えられる。これらの多くの場合、コンプライアンス（法令順守）が求められる業務に PKI の署名が要求されることが多い。そのため、PKI 自体のセキュリティの基準（クライテリア）も求められることになる。こうしたことは、国際的な IT 技術（IT セキュリティ技術）をキャッチアップしていく上でも非常に重要な要因ではあろう。しかし、一方、基準を作成しようとすると、コストを無視して敷居の高い方へシフトしていく傾向が見られるように思われる。つまり、問題は起こりにくい方向へ行く一方、それは、使われにくい状況をも生み出しているように思われる。高いクライテリアや法律的な議論が、PKI は、難しいもの、コストがかかるものと思われる要因になっていることも注意すべきことだと思われる（これは、前節の三文判の議論とリンクしている問題である）。

2.1.3.2　企業内や企業グループでの制度的なアプローチ

本部会において、企業内で、PKI を効果的に導入した例が紹介されている。これは、企業グループ内で、セキュリティポリシにより PKI の署名、暗号を強制するもので、制度的なアプローチといえよう。

どこの企業でもセキュリティポリシが整備されつつある。PKI は、情報セキュリティを考える上での３大基本要素である機密性（Confidentiality)、完全性（Integrity)、可用性（Availability）の中の機密性、完全性などを提供することができる。また、よく考えられた PKI は、更に、管理統制や利便性も提供することができる。

セキュリティポリシの整備は、情報の分類と管理を促し、結果、その情報に相応しい機密性、完全性などの必要性の程度がわかってくるのが通例である。逆にセキュリティポリシの整備が行われない中、闇雲に機密性、完全性といっても、導入への必要性は理解されにくい。セキュリティポリシが整備されて始めて PKI 導入目的が明確になり、そして、ROI（Return on Investment）が評価できると思われる。

もうひとつ企業に普及するための要因としては、グループ企業のエクストラネットや、インターネットからの企業内部へのセキュアなアクセスの要求がある。このように、セキュリティポリシが普及し成熟することは、PKI の普及をも促すものと思われる。

セキュリティポリシなどが整備されたとしても、なお、企業内における PKI の設備や運用基準をどうすればよいかといったことを決定するにあたっては、難しい側面がある。これらの基準をどこに持っていくかということは、多くの場合、コストとのトレードオフとなる。このことが、ユーザからすれば、コスト構造を分かりにくくしている（結果、SIer やサービスプロバイダは、そのコストの根拠を示すことに多くの時間を費やすこととなる)。適当な基準があればよいが、電子署名法の特定認証業務などは、あまりにも敷居が高い。企業内で使用する PKI の運用基準案を作成することや、よりカジュアルな CP/CPS をサンプルとして作成して公開するといったことなども、企業における PKI の普及につながるかもしれない。

インターネット上のサービスにおける応用として三井住友海上火災の事例があげられる。同社では、代理店 Web システム用認証局を構築し、代理店の認証を PKI ベースでやることにより、大きな成果を上げている。多くの場合、使用している代理店の利用者は PKI を意識しているわけではない。それでも、サービス提供者である同社は、強い認証である PKI の Web のクライアント認証を有効に使っている。

同社がこのような代理店 IT 化に熱心に取り組んだ背景には、保険料の自由化、リスク細分化といった時代の流れなどにより、保険料計算が紙タリフやポケット電卓では事実上不可能になっていることがある。加えて、代理店数の減少している一方で競争が激化しているため、代理店の差別化戦略として、オンライン計上入力、精算業務、戦略的 IT の活用が要請されている（その際には、代理店手数料制度の改訂もなされたとのことである)。

以上から、PKI を使用して IT 化を進めるモチベーションとしては以下のようなものが考えられる。

(1) オンラインシステムが不可欠

保険契約内容が複雑（リスク細分型）になり、ホストコンピュータの顧客 DB、車両価格 DB、ロジカルチェック等を利用しないと計算が出来ない。セキュリティ管理上 PKI 使わざるを得ない保険会社としては守秘義務を確保するために、代理店の担当顧客 DB 以外には、アクセスできないセキュアなシステムを構築しなければならない。

(2) 必要経費として妥当な価格

代理店業務のなかで、各種保険の案内、保険料シミュレーション、契約計上、保険会社との精算業務などオンラインで行う業務はミッションクリティカルなコア業務であり、そのシステム使用料（含む公開鍵証明書）は常識の範囲の金額であれば違和感無く受け入れられる

(3) 保険料計算間違いの辛さを知っている

保険料率表の読み間違いや電卓の打ち間違いにより保険料を間違った場合、10 円多くても少なくても、必ず申込人に追徴保険料もらいに行くか返すかしないと、「規則」違反となり、例えば３ヶ月間手数料３%カットなど処分を受けることになる。オンラインによるロジカルチェックで有ればそんな心配は一切無い。抜群に便利であることを誰もが容易に理解できる。

三井住友海上火災の例では、サービス提供者である同社としての IT 化を推進するというモチベーションがあり、そのため、代理店にとってセキュアで使いやすいサービスを提供することが非常に重要であったと思われる。また、使いやすいサービス（アプリケーション）が代理店の IT 化を促進したのだと考えられる。

電子政府においては、サービスを提供する主体は官側にある。官側にオンラインでの入札や申請の率を高め、そして行政の効率化を図るといった強いモチベーションがあれば、結果としてよい使いやすいサービスを提供することにつながるのではないだろうか。

2.1.3.3　教育分野など新分野での PKI の活用に向けて

大学などの教育分野において、PKI の活用が求められている。現在、日本の大学は、「18歳人口の減少」、「入学者の基礎学力の低下」、「国際レベルへの引き上げ」などの課題に直面している。このような状況の下、一方では、文部科学省が各大学の独立／独自経営での存続を促すために、規制と保護の両方を緩める方針を表明している。

これを受け、各大学は、教育対象を就学年齢以外にも拡大する「生涯教育」、在学生のための教育の質と量の改善及び、教育の独自性を目指すための「e-ラーニングの導入」、「地域の高等学校との関連強化」、「他の国内大学との連携」、さらには、「国際的な大学間の連

携」など、様々な施策を模索することになる。

これらの施策は大学ごとに違い多岐にわたるが、共通要素として「どこにいても受けられる教育」は、ひとつの重要なキーワードである。これを経済的に実現するためには、インターネットの活用が有効／必須であり、今後、教育の分野では、PKI は重要な位置を占める可能性が高い。

大学をはじめとした教育機関が、教育コンテンツの内容の個性を競うことは重要であるが、アクセス管理や意思表示のためのデジタル署名などをそれぞれ独自のものにすることは、これを開発する側にとっても、利用する側すなわち、教育を受ける側にとっても望ましいことではない。

そこで、日本国内に限定せずに、大学／教育機関を国際的に共通な枠組みとして捉え、学生や教員などの身分や本人確認のための「国際オンライン学生証／身分証（仮称）」、教育コンテンツやオンライン・コースのための「国際的アクレディテーションの電磁的証明」、各大学が発行する「オンライン認定」、「電磁データによる卒業証明、成績証明などの各種証明書」を PKI に基づく国際的な規格の下に統一することは大きな意味をもつ。これを日本発世界の取組みとして推進することは、世界規模のネットワーク社会実現に大きく貢献するものであると考える。

このように現在 PKI の活用が進んでいない分野では、新しいビジネスモデルやキラーアプリケーションの創出が求められている。法制度整備・IT 化推進は既存の業務を IT 化するというだけでは、既存のビジネスモデルの範囲を超えるものではない。今後は、既存のフォーマルな社会制度等の分析に基づき、インターネット・PKI を利用した既存のビジネスにはない、新しいビジネスモデルの創出に向けた、連携・利用促進の試みをなしていくことが必要であろう。

2.1.4 利用促進の前提となる相互運用性の問題

2.1.4.1 認証用途での利用拡大と相互運用性の問題

無線 LAN や Internet VPN などの新しい認証には PKI の認証が利用できるケースが多い。これまでになかった新しいプロトコルの認証などでは、従来からの平文のパスワードはなく、何らかの強い認証が実装されている。実際に PKI で実装されることも多く、スマートカードや USB トークンを使ったシングルサインオン的な用途の PKI による認証が現実的になってきた。

このように、新しいネットワークインフラの認証への要求は、新しい認証方法の普及を促す。しかし、こうした新しいネットワークインフラでは、新たな相互運用性の問題も避けて通れない。相互運用実験などを行うことによりメーカや SIer の技術を高めていくことは、結果的に利用促進につながっていくと思われる。

PKI の普及が使いやすいアプリケーションにあることは、共通の認識である。その使いや

すいアプリケーションの開発を促進するには、やはり、PKI の相互運用性の問題は避けて通れない。こうしたことを地道に解決していくことも重要な課題である。

2.1.4.2　相互運用性の問題の除去

エンドユーザに対する直接の利用促進ではなく、PKI を応用した開発や、システム構築を促進することも重要だと考えられる。そのためには、PKI を応用した開発者や、PKI システムを構築する SIer にとって避けて通れない PKI の相互運用性の問題を解決する必要がある。

利用者にとっては、関係のない話題かもしれないが、アプリケーションシステムの開発者や、SIer にとっての技術の壁や敷居の高さを取り除くことは、やはり重要になる。

日本ネットワークセキュリティ協会 JNSA では、PKI の相互運用性に関連する WG の活動がいくつかなされている。昨年度の、IPsec の相互接続実験では、IPsec の VPN の PKI で認証を行った相互接続実験を行っている。また、今年度は、無線 LAN の同じく PKI で認証を行った相互接続実験を行っている。こうした相互接続実験は、PKI 認証を使った問題点や解決方法を明らかにし、また、SIer などの技術力向上に貢献していると思われる。

同じく JNSA の昨年度の PKI の相互運用実験である Challenge PKI 2001 では、CA の相互認証、GPKI と同じようなブリッジモデルでの相互認証などの相互運用実験を行っている。今年度の Challenge PKI 2002 では、PKI のアプリケーションのコア部分の相互運用性の問題を解決するための PKI 相互運用テストスィートの開発などを行っている。こうした、活動は、PKI の認証局や、アプリケーションレベルでの相互運用性の問題点の解決方法を明らかにすることにより、PKI を応用したアプリケーションの開発を促進すると思われる。

PKI を応用したアプリケーションの開発を促進することは、使いやすい PKI アプリケーションが多く開発される可能性を高めることをめざすものである。

2.2　連携調整部会の活動報告

2.2.1　概括

本部会では、本年度の活動テーマとして以下の課題を設定してきた。

① 政府－民間連携の課題
② 民間 PKI 連携の可能性
③ 使える PKI（三文判 PKI）

メーリングリスト上の議論をベースに本年度の活動をまとめるはずであったが、現在のところ十分な共通認識にまでには達していない。

利用促進部会と同様に、③の使える PKI（三文判 PKI）については、広く誰でもが使える PKI の必要性という観点からの議論がなされた。その結果、従来の実印相当の厳格な運用を中心とした PKI の議論とは異なる、以下のような認識が得られた。

しかし、実社会で実印を使用する機会は極めて少ない。むしろ本人の厳格な推定なしで

も、おおむね本人らしさが認められる三文判や単なる署名で、たいていのビジネスが成立っている。PKI の世界でも実印レベルの PKI ばかりではなく三文判 PKI の世界を広めなければならないのでないか。そうしなければ結局高価で使えない PKI となってしまう。こうした認識を提言レベルのものへと深化させるためには、以下の問題を明確にすることが今後の課題と思われる。

ⅰ）三文判 PKI の用途は何か

- ビジネス分野でのメッセージ交換
- 小額電子商取引
- 申請、届出（電子政府）

ⅱ）使うアプリケーションは何なのか

- 署名メール（S/MIME）
- リモート VPN
- Web アプリケーション
- E-Form

ⅲ）三文判 PKI のポリシー

- PKI（署名）をどのような目的に使うのか
- 認証局を誰が運用するのか、１つの認証局か複数の認証局の連携か
- 信頼点を何処に置くのか
- 保証のレベルはどうするのか
- 商用サービス（VeriSign や JCS など）との関係はどうなのか
  （加えて、PGP との違いは何か、PKI が普及しないのは本当に三文判 PKI がないからか等・・・）

こうした三文判的な PKI を含めた PKI の用途は、認証、電子署名、原本性保障、暗号化など多岐にわたる。すなわち、従来の暗号のイメージを超えた普遍的なセキュリティインフラストラクチャへの手段として大きな可能性がある。PKI を手段として用い、セキュリティが保障する基盤を構築することは、高度なオープン・ネットワークやオープン・システムを展開するための必要条件かもしれない。

しかし、PKI も決して万能ではない。またその仕組みはやや複雑であり、一般社会での受容という面から見ると広い意味でのリスクをはらむことも予想される。

こうした問題認識に基づき、以下では、PKI をめぐる海外の状況、PKI の安全性の課題並びに電子認証における連携調整の課題について論じることとする。

2.2.2 海外における PKI の状況

日本政府の GPKI は行政手続の安全なオンライン化を図ること、すなわち電子申請の安全

基盤として進められてきた。ここでは、かなり高度なセキュリティを設定した単一の証明書ポリシーを前提にしている。それに対し、米国・カナダ政府の PKI 政策は、政府内の業務の安全基盤としての各省の PKI を連携させることをめざす視点から進められてきている。その結果、多様な PKI の用途を想定して４段階の安全レベルの証明書ポリシーを設定し、それぞれのレベルでの柔軟な連携を可能にさせる方向性がとられている。ここでは米国、カナダ政府の証明書ポリシーを概観し、さらに国民サービスの状況を概観することにする。また公開鍵を利用するための証明書や署名鍵などクレデンシャルの扱いについても、カナダ・フィンランドでは異なったアプローチをとっている。以下では、フィンランドの IC カードの仕様についても見ておくことにする。

2.2.2.1　米国、カナダ政府の PKI の証明書ポリシー

４段階のセキュリティレベルを想定した政府 PKI の証明書ポリシーは、はじめにカナダ政府が５年ほど前から検討してきたものであり、米国政府もこのポリシーに従った運用を行っている。以下の表に各ポリシーのレベルの基本的な考え方を示す。この証明書ポリシーは電子署名に用いるための証明書ポリシーで、暗号用途の証明書ポリシーには別途４段階の証明書ポリシーを設定している。この表には各レベルでの内容についてはほんの１例しか示していないが、実際の証明書ポリシーには RFC2459 の証明書発行手順、鍵の安全性、運用管理、物理的安全性などについてそれぞれのレベルについての違いを明記している。

表 2-1　４段階の証明書ポリシー

ポリシレベル	失効チェック	本人登録方法	想定される脅威
Rudimentary 初歩	失効情報チェック無し FIPS140 Level1	e-Mail で登録	悪意の利用が想定されず、高価値でないデータの完全性をサポート
Basic 基本	失効チェックあり FIPS140 Level2	電子的登録が可能だが,複数の本人確認を行う	データ改ざんなどのリスクを想定するが、主要な脅威でない
Medium 中位	失効チェックあり FIPS140 Level2	対面登録、公的な ID を提示	データ改ざんのリスクがある環境で高価値のトランザクションを行う
High 高位	失効チェックあり FIPS140 Level3	対面登録、写真付き公的 ID を提示	データ改ざんの脅威があり、非常に高い価値のトランザクションを行う

日本の GPKI の証明書ポリシーのレベルはこの米国、カナダ政府の PKI と比較すると中位または高位のレベルに相当するものである。電子政府の実際の応用を考えると複数レベル

のポリシーを設定し柔軟でコスト効果の高い PKI を導入しても良いのではないだろうか。

この複数レベルの証明書ポリシーについて考え方は、別途議論のあった三文判 PKI の定義や利用範囲の明確化のためにも参考にすべきものと思われる。

2.2.2.2 カナダ政府の公的個人認証サービス GOL

カナダ政府は市民が政府に対する電子申請をインターネットで行うためのサービスを GOL（Government OnLine）として開始している。このサービスは日本の公的個人認証サービスと同等のもので、政府が電子申請のための証明書を発行するサービスである。基本的にこのサービスで発行される証明書は政府に対する電子申請のためのもので、民間同士のトランザクションに用いられるものではない。以下の表に日本の公的個人認証サービスとカナダ政府の GOL の比較を行う。

表 2-2 日本とカナダの比較

	日本の公的個人認証サービス	カナダの GOL
サービス時期	2003 年度まで	2005 年までに順次
達成効果		市民満足度を 10%向上
費用	無料または低廉	無料
目的	G to C	G to C
証明書所有者名	住民基本４情報 氏名、住所、年齢、性別	MBUN (Meaningless But Unique Number; 無意味な数字)
証明書発行枚数	1 枚	複数枚
クレデンシャル	IC カード	ローミング

ここで特徴的なものは証明書への本人情報の記載内容である。日本では証明書に住民基本台帳の４情報、すなわち氏名、住所、生年月日、性別を記載するとしているのに対して、カナダでは MBUN という無意味な数字列で証明書からは個人を特定する情報を載せないとしている。この MBUN と実際の本人情報とのマッピングは政府内部で行うこととしている。これは証明書に記載内容から個人のプライバシ情報の漏洩を防ぐためとしている。

また証明書発行については日本では本人当り１枚であるが、カナダでは本人が希望すれば MBUN を変えて証明書の用途別に複数枚の証明書の発行が出来るとしている。

証明書や鍵情報（クレデンシャル）を格納させる媒体として日本では住基カードの IC カードを想定しているが、カナダでは証明書を ePass と言い、クレデンシャルは本人が携行するものではなく、本人のパスワードと管理サーバの暗号鍵で２重に暗号化した状態でネットワークのリポジトリに格納する。そして、本人が使用するときは、本人のパスワードをベースとしてリポジトリから検索しブラウザにダウンロードして署名に用い、使用後はメモリから消去され鍵情報はブラウザに残さない。このため、利用者はブラウザだけで電

子申請の署名が可能で IC カードリーダ等の装置を必要としないという利点がある。

このように例え証明書が市民と政府間のみの使用であってもプライバシの考慮や、特定の IC カードに依存するかどうかについては議論のあるところである。特に IC カードについてはカードリーダの費用と、API の標準化など相互運用性に多くの課題を残しているものである。

2.2.2.3 フィンランドの市民サービス

フィンランドでは政府が市民サービスに大きく踏み込んだサービスを提供している。ここでは FINEID（http://www.fineid.fi）という、フィンランドの市民カードを希望者に有料で発行される。カードに印刷された顔写真によって身分証明書代わりになるほか、電子申請など官用用途ばかりでなく、民用のオンライン取引におけるトークン、ヨーロッパ 15 ヶ国域内での地域パスポートとしても機能する。FINEID は 1999 年 12 月から運用が開始されている。

FINEID は今まで IC カードの API が明確に定義されていないため相互運用性に大きく問題になっていたことから IC カードの API を厳格に定義することになった。

FINEID は、証明書に対応する私有鍵の扱いや、カード内部のフォーマットが PKCS#15 に準拠することによる IC カードの相互運用性やポータビリティを向上させたことなどの特徴がある。こうしたことから、欧州における身分証明書 IC カード関係の標準化の、ひとつの参照モデルになっていると思われる。

FINEID の主な仕様書と、標準などとの関係は以下のとおりである。

表 2-3 FINEID

FINEID 仕様書	FINEID についてのコメント	参照している仕様書（標準）
FINEID S1	Framework for the Electronic ID application in the smart card.	PKCS#15 v1.0、ISO/IEC 7816-4 and ISO/IEC FDIS 7816-8
FINEID S4-1	Implementation profile 1 of the FINEID S1 specification.	FINEID S1 and RFC 2459
FINEID S4-2	Implementation profile 2 (for organizational usage) of the FINEID S1 specification.	FINEID S1 and RFC 2459

上記の様に、ISO/IEC7816-4、7816-8 などの IC カードの標準に、カード内のクレデンシャルのフォーマットとして PKCS#15、そしてクレデンシャルの証明書のフォーマット、及び、証明書プロファイルとして RFC2459（RFC2459 の最新版は、RFC3280）に準拠している。

IC カード自体が標準化されたとしても、その中のフォーマットが標準化されなければ、多くのアプリケーションで使用されることは難しい。そのため、公的な用途の IC カードの

場合、PKCS#15 などの標準化された暗号クレデンシャルのフォーマットを使うことは非常に意味がある。IC カードに関しては、色々なアプリケーションに依存したデータも記録されるかもしれないが、暗号クレデンシャルに関しては標準化されたフォーマットが採用されるべきである。

実際のアプリケーションは、直接、IC カードをアクセスするのはない。代わりに、PKCS#11 などの暗号クレデンシャルをアクセスするための API を介したアクセスをなす。そのため、IC カード内のクレデンシャルのフォーマットを知っているべきプログラムは、PKCS#11 ドライバなどであったりする。そして多くの場合、IC カード内の暗号クレデンシャルのフォーマットは、独自のフォーマットがなされ、特定の PKCS#11 ドライバのような独自のソフトを介さなければ使用できないという構成になっている。これは、企業内などの使用においては、大きく問題になることは少ないが、電子政府のような用途の場合には問題が多い。そのため、PKCS#15 は、FINEID のような公的な目的の IC カードや、PC 環境以外で使用される IC カード内のフォーマットとして使用される傾向にある。

FINEID のもうひとつの特徴は、暗号クレデンシャルとして、IC カード保有者の、二つの証明書とこの証明書に対応した二つの秘密鍵（私有鍵）、そして、IC カード保有者の信頼点の証明書が格納される。

この二つの証明書は、それぞれ、認証用・暗号用の証明書であり、もうひとつは、否認防止の署名のための証明書である。そして、それぞれの証明書は X.509 証明書 v3 フォーマットの証明書であり、クリチカルな鍵使用目的（keyUsage）証明書拡張を持つが、その内容が異なる。そして、この証明書に対応した二つの RSA の鍵が IC カードに格納されるが、この鍵の使用に異なるプロテクションが施されている。

日本で予定されている公的個人認証サービスでは、クレデンシャルの格納媒体として住民基本台帳のカード以外にも利用者の要求する IC カードも OK としているが、API 仕様の明確化と仕様の公開および十分な実証実験がなされる必要があるだろう。

2.2.3 認証と PKI の安全性の課題

2.2.3.1 「認証と PKI の安全性の課題」における調査分析

本節では、PKI の普及に伴って存在しうる課題について幅広な観点から脅威の可能性や脆弱性の可能性を議論する。ここでの議論は決して PKI は危険性をはらむということを警告する趣旨ではない。社会のいかなるシステムも、セキュリティの厳密な観点から言えば完全に安全ではない。完全に安全ではないという視点から見たときに、どこにそのようなセキュリティが破れる可能性の目があるのかを事前に理解しておくことは重要である。そのような視点でこの章の議論は行われる。このような事前理解の視点は、セキュリティにおけるリスク分析の基本的な方法論、考え方と一致しているとも言える。

(1) 本調査分析のミッション

JESAP 全体のミッションは未着手の課題や組織横断的な検討課題の抽出を行い、整理して標準化団体や業界団体に提言するものであると考えられる。その中で、本節でのテーマを検討するためにサブワーキンググループ【電子署名・認証の安全性】としての活動を行った。このサブワーキンググループのテーマは電子署名・認証の安全性について課題・脅威を抽出することであるが、それには２つの視点がある。

(A) 署名の安全性に対する技術的な課題の抽出

(B) まだ広く認知されていない PKI 実施上の脅威の抽出

今回はこれら２つを特に区別することなく課題抽出を行った。

本来、課題抽出に基づいて、それに対する解決策や不具合発生防止策を提言すべきであるが、今回の作業では問題を見る目を育てるとの立場から、一部をのぞきあえて解決策の提示を急がないこととした。

ここでの作業はいわばエンドレスな作業であり、今後課題の解決策が提示され、実装に移されていくという面とともに、PKI 利用が深まればより実践的な課題が数多く新たに提示されてくる可能性があると考えられる。

(2) 課題抽出のアプローチ

課題を幅広に抽出するという立場からすると、多くの視点からの問題提起がありうるので、課題の領域をいくつかに分類し、それぞれに考えうる課題をリストアップして行くというアプローチを取った具体的には、次の６つの分野を提案している。これらは、ミッション（A）（B）を含むものである。また、PKI という言葉で、その応用である認証等を代表させている。

(a) PKI のシステム構成における技術的な課題（インタオペラビリティの課題も含む）

(b) PKI 実装上の技術的な課題

(c) PKI の普及過程の技術的課題

(d) PKI の普及過程の制度的・社会的な課題（アクセシビリティの課題も含む）

(e) PKI が普及しきれないときの制度的/社会的な課題

(f) PKI を社会システムとしての見たときの脅威・脆弱性の課題

2.2.3.2　課題の列挙

下記に、設定した分類に従い課題点として挙げられたものを列挙した。これらは、具体的な課題の緒として示したものもあるし、また課題を解析すべき領域や視角のみを示したものもある。

(1) PKI のシステム構成における技術的な課題（インタオペレラビリティの課題も含む）

① 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アントからみて、CRL や OCSP のインタオペラビリティに欠陥がある場

合の課題点。

② 企業体の合併、分割、大規模組織改変、消滅などに関する課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課題性がどこまで掘り下げられているか。

③ 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。

④ 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。

(2) PKI 実装上の技術的な課題

① 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課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。

② 認証と署名の違いに基づく課題もある。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鍵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認している。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したが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。

③ 認証と原本性保証の違いに基づく課題もある。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。

(3) PKI の普及過程の技術的課題
① 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 製品お技術的欠陥（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。

② 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。

(4) PKI の普及過程の制度的・社会的な課題（アクセシビリティの課題も含む）
① 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。

② PKI 固有の課題ではないが、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。

③ 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課題。たとえば、所有者が失効を知ったのが失効事由発生より後であった場合に、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課題。

(5) PKI が普及しきれないときの制度的/社会的な課題
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・脆弱性の課題

① 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）

② 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。

2.2.3.3　課題の具体例記述

前節に示した課題について、以下に具体的な問題状況と解説を２点示すことにする。

（具体例１）　秘密鍵管理の重要性

～秘密鍵の管理方法によっては、かえって認証の強度が下がってしまう危険性について

シナリオ例：利便性のために、パスワードによる保護をかけずに秘密鍵を格納・利用している場合。当該 PC さえ入手できれば、パスワードの入力なしに証明書が不正利用できてしまう（たとえば、ブラウザにクライアント証明書格納）。

解決法：証明書を外部装置（IC カードや USB トークンのようなもの）に格納することを強制し、使用する証明書も当該装置に格納されているものに限定する。また、利用の際の PIN コード入力も必須とする。

課題：

・外部装置の利用を強制できるかどうかは、アプリの実装による。
・IC カードや R/W の価格は低価格化が進みつつあるが、大企業などでは導入数が膨大で、コストがかかる。
・IC カードなどを利用しても、それ自体が盗難にあった場合の危険性がある。

考察：

証明書はハードディスクその他、PC には格納せず、耐タンパ性を持った IC カードなどに格納することが重要。要求される強度を考慮し、

・本人の知識（パスワード・PIN コードなど）
・本人の所有物（IC カード自体）
・生体的特長（指紋認証など）

を組み合わせて、IC カードなどの内部に格納された証明書の使用自体も保護するべき。

（具体例２）署名の有効性（証明書失効のタイミング）

～証明書が失効する前に施された署名は、本当に有効か？

シナリオ例：ある人が、自分の証明書が盗まれた（ノート PC やカードの紛失など）ことに気が付き、その証明書を失効させた時点をＡとする。

この場合、失効の開始日をＡとすると

実際に盗難されてから失効処理がなされるまでの期間が長いほど、「証明書が有効な時点で」不正に署名が利用される可能性が高くなる。

Ａよりも前に遡って失効を開始することを認めると

故意に遡って失効させて、本人が正当に署名したものでも無効にできてしまう（否認可能）恐れあり。

（注、実際に CRLv2 には Invalid Date という拡張があり、失効したと思われる時点を指し示すことができる）

本当に「失効状態」になったのはいつかを断定するのは難しいのではないか。

解決法：

技術的には、有効な解決法が即答できない。

考察：

最終的には裁判等、司法の判断となるはずで、すべてをシステムで解決するのは現実的ではないが、もう少し一般にも認識されるべき問題ではないか。

2.2.3.4 補足的な視点

次に示すような抽象的な視点については、特に具体的な議論は当サブワーキンググループの活動の中では未実施だが、これらのファクターが引き起こすかもしれない不具合を今後考察してみることは有益であるかもしれない。

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課題

- **非常に多くの鍵情報を個人が管理しなければならなくなった場合の課題**
- **大規模な災害**
- **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課題点、リスク**
- **警察・司法・防衛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課題**
- **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**

2.2.4 代理業と電子認証をめぐる課題

2.2.4.1 代理申請要請の本質

代理申請要請の本質は、「申請制御機能」への期待と要請によるものであり、本人に代わり（依頼を受けて）申請のために必要な専門知識や申請書作成ノウハウを背景に、状況に応じて資料や添付書類等の収集を制御し、本人の代理人として申請書等を作成・届出することにある。

この代理申請の本質は、これまでの紙ベースでの代理申請と、今後期待される電子申請における代理申請と異なるものではない。この代理申請の本質、役割、使命をふまえ、代理業と電子認証について考察したい。

2.2.4.2 電子申請における代理申請の意義とあり方

電子政府構築当初、一般への普及に先だって専門代理業者が、その職業的見地から電子申請の知識及び一般ユーザには手の届かない機材等の導入等効率的な業務の運用方法をより早く蓄積していくことが予測される。

そのような背景から、専門代理業者に対し以下の役割の担い手として期待を寄せるところである。

- 申請に不慣れな者への権利擁護、支援
- 情報弱者の権利擁護（いわゆるデジタルデバイドへの対応）
- 電子申請推進の起爆剤としての機能
- 政府の情報化推進計画の円滑な実施に寄与
- 企業や政府によるアウトソーシング（業務の外部委託による効率化・コスト削減等）の補助
- 電子申請の目的に沿った代理申請の実現
- 資格者等に限定されない広義に捉えた代理申請の実現

2.2.4.3 代理申請を実現するための要件

代理申請を実現するためには、その代理人がどのような資格をもって申請者本人を代理しようとしているのかを明らかにしなければならない。

インフラとしては、以下を構築する必要がある。

- 代理申請機能を実装した汎用申請システムの開発
- 代理人資格の認証の仕組み
- 委任事項を明示する委任状フォーマットの規程と委任状取り消しの仕組みの開発

2.2.4.4　代理申請における問題点

代理申請における問題点として次の事項があげられる。

(1) 多重（複数）署名方式の問題点

・　署名の順番に関すること
・　申請書等に対する善意の加筆訂正が改ざんとみなされること
・　電子署名と紙に押印した印鑑との併用申請に関すること

(2) 添付資料に関する問題点

・　画像データへの署名方法が確立されていないこと
・　原本提出が求められる資料（スキャナー等で読み込んだものでは受付けないとされているもの）の電子データ化
・　別途郵送による受付け側の事務の煩雑さ
・　登記済証等の役所が発行する証明書の電子化に関すること

注、　多重（複数）署名と添付資料に関する問題点は必ずしも代理申請に限られた論点ではなく、電子申請における共通の課題とも言える。

(3) 代理人の属性認証の問題点

弁護士、司法書士、税理士、行政書士、社会保険労務士等、専門資格者が代理人として電子申請を行う場合、それを受理する行政機関等は、代理人の本人性の確認もさることながら、その代理人の属性である資格を明確に把握できるようにしなければならない。

現段階では、属性を証明する認証局は構築されておらず、また、電子署名法においても特定認証業務としての運用は本人確認のための認証のみしか規定していない。

このような状況下で代理人の資格属性をインターネット上で証明するには、各士業法で定められた法定団体（連合会等）が特定認証業務を行う認証局を構築し、本人性証明に付加した属性情報としてその資格証明を担保していく必要があるであろう。

(4) 代理申請要請の本質に係る申請制御機能と電子申請フローの整合性確保

専門資格者である代理人が下書き作成した電子申請文書への電子署名、配布書類等が、申請書等への回覧が必要となる。そのため、例えば、下書きした申請書ファイルをフロッピーディスクに保存して申請者本人に手渡し、本人の電子署名を付してもらうといった業務フローが生じる。

このような、紙による申請時に行っていたフローをそのまま電子申請の現場に持ち込むことは、電子申請そもそもの、迅速性、簡便さといったメリットを損なう要因となり、各ユーザにとって電子化の恩寵を十分に享受できない結果を惹き起こす。

行政機関に対する電子申請においては、現状では、完成した申請書等をしかるべき担当

部局に届け、結果通知を発するところだけが議論されており、申請書自体の作成過程については特に言及されていない。ユーザ側の利便という観点に立ち戻った場合、電子申請に見合った業務フロー及び諸制度自体の見直しをしていかなければならないだろう。

2.2.4.5　問題の解決案（技術）

(1) 多重（複数）署名、署名文書への加筆

・　現在標準となっている署名フォーマットで多重署名や署名に対するコメントの記入が改ざんなしに可能であるものの、対応する製品がほとんどない。

(2) 画像データへの署名

・　「電子透かし（watermark)」による方法

(3) 原本提出が求められる資料

・　「アナログ透かし」による方法

（注、　(2)及び(3)については技術的には可能であるが、インフラ整備、費用対効果の観点から現時点では実現に困難をきたすことが予想される。）

(4) 別途郵送による受付側の事務の煩雑さについて

・　電子署名データを三次元バーコード化し、郵送する資料に刷り込む。受付行政機関は先に電子的に受理した申請書等と郵送資料に付加されたバーコードを照合し審査する。

(5) 登記済証等の役所が発行する証明書の電子化

・　IC カード等への格納

・　代替物としての ID／パスワード

2.2.4.6　問題の解決案（制度・運用編）

(1) 多重（複数）署名方式の問題点

・　署名紙文書の添付、電子署名文書の委託、事後確認等代替手段の活用により署名者の限定を行う。

・　制度の主旨として連署を求める場合を除き、署名行為を分離し、各当事者が署名したものを申請行為者（代理人等）が一体化して署名する。

　一見すると、多重署名のように見えるが、実態的にはそれぞれの証明事項、申請事項に対して署名者が異なっているため、それぞれのパートに分離しても処理上の問題は発生しない。

　例えば、健康保険の傷病手当金の請求においては、被保険者、事業主、医師、代理人等のパートを分離し、それぞれが作成し、最後に代理人が取りまとめて一体化する「構

成制御ファィル」という方法で対応する。

(2) 申請書等に対する通常の加筆訂正が情報システム上では改ざんとみなされること

・　申請書の作成行為と署名行為を分ける（関係者の内容確認後、申請行為者が署名)。

実際の代理人による申請の場合は、申請書等を代理人が作成し、その申請書に申請行為者が署名する。さらに添付する証明書等についても、指定された証明用紙等を代理人が直接証明者に配布し、証明・署名を受け、回収することが想定される。

この際、各署名権者が自己の署名を施す前に、随時、補正や再提出を代理人が署名権者に依頼する等の調整をおこない、最終的な申請書類を完成させる。それ以降の加筆訂正は、補正や再申請として処理する。

その際のファイルのやりとり・制御のセキュリティ対策としては、次の方法が考えられる。

ａ．申請人が電子署名したファイルをフロッピーディスクに書き込む。そのフロッピーディスクを受け取る。

ｂ．申請人が電子署名したファイルを、メール添付で、受け取る。

ｃ．代理人が開設した WEB サイトにて、申請人が電子署名を施し、それを WEB 送信させることによって受け取る。

注、ｂ．及びｃ．は、データの安全性という点において、さらなる検討を要するであろう。

(3) 添付資料に関する問題点

・　電子化に馴染まない添付資料は、極力減らし事後調査体制へ行政組織の見直しを進める。

・　民が発行する証明書、添付資料の原本保管義務を申請者側に課すための法的整備を行う。また、行政が発行する証明書等は、行政がみずから確認していくシステム・仕組み（行政の内部処理として対応する仕組み）を構築する。

・　代理人が書類電子化の支援を積極的に行う。デジタル化する機能を有しない民の証明者等にかわって、代理人が電子領収書等の作成・支援をする。

例えば、電子領収書が必要な場合、電子領収書エディタと IC カード R/W を持った代理人が立ち会って、その場で電子領収書を作り署名だけ当人にして貰うという方法が考えられる。

・　一部添付書類は郵送とする。電子申請書に、別送する書類を記載し、送信番号、進達番号等を付与し、行政が後日、簡便に突号できるシステムを構築する。

・　原則として電子データの提出を求め、ユーザがそれに応じることができない場合には代替方策を採用する。

・　専門家が本人確認や調査確認をして電子署名付きの報告書データを作成する。

2.2.4.7　代理申請の類型から見ての考察

代理申請には大きく分けて、二つの類型がある。一つは、申請者本人が自己の時間短縮の便宜を図るため身内や知人に個人的レベルで頼んで行うもの。もう一つが、申請者自身に申請の知識及び大量処理能力が乏しく専門家に依頼するものである。電子申請の普及率が高まるにつれ前者の領域が若干ずつとも拡大することは予測可能であるが、専門知識を要する申請、個人レベルでは到底扱えない大量処理を伴う申請等においては、現行の紙における申請等と同様、専門家の出番を待つより一般的な解決策は見当たらないであろう。

一般ユーザが専門家に対して求める究極的要素は、安心である。不備を含んだ申請やその遅滞により自己の財産を脅かすことにもなりかねない重要な案件については、少々のコストを代償にしても安心できる専門家に依頼したくなるのが人の情である。この社会通念とも言える感覚は、電子申請の土壌においても変わることはない。

また、一方で電子申請それ自体が目新しいものとして一般ユーザから敬遠されがちになることも否めない。電子申請という技術が文化として消化され、国民生活に浸透されるにはそれなりの時間を要するであろう。その時間の穴を埋める役目としても専門家の存在を無視することはできない。専門家が積極的に電子申請活用を推進することで、社会へその成功（時には失敗）例を示すことは、電子申請に対するニーズを増していくきっかけとなり得るからである。

電子政府の発達過程において、専門代理業者のポジションが、電子政府発足当初は電子申請できるもの全般に、普及時には専門性に特化された申請に絞られていくことが、この国の電子政府育成のプロセスとして適当ではなかろうか。そうすることで、大きく広がった申請制御機能の振幅を時勢に合わせ適宜調整していく機能として、専門代理業者は、政府から国民への電子申請リテラシーの橋渡し役を担うこととなろう。

2.3　PKIに関する政策・連携調整策・利用促進策への提言に向けて

以下は、現時点でのJESAPの議論を、要約的に日本のPKI政策全般へ向けた仮の提言形式としてまとめたものである。JESAPでの議論は現在進行形であり、ここでなされた提言は、JESAPのホームページ等で適宜、より適切なものへとアップされることとなろう。

注、本節における「今後の検討に向けた補充」は、JESAP部会参加者から本報告書草稿に関して事務局に寄せられた意見等を元に事務局が今後の検討のために参考として挿入した。

2.3.1　PKI政策全般に対する提言

2.3.1.1　PKIの安全性の課題に対する提言

[提言]

PKIの安全性の課題等について大局的な視点から系統的・継続的に実態調査を行うこと、課題抽出を行っていく体制組織化が必要である

[背景]

2.2.3 での検討より導かれた、今後の政府施策や業界努力、研究の方向性についての提言である。制度や技術の基本に関わる課題抽出は、民間ビジネス推進の中ではなかなか系統的に研究・調査しにくいミッションである。また課題点として個別には指摘されていても、それが制度化に活かされていく経路が保障しにくい課題であるとも思われる。そのため、提言で述べたような体制作りが必要と考えられる。

2.3.1.2 海外との連携・調整への提言

[提言]

PKI 及び関連技術の進歩等をにらみつつ、電子的な認証基盤全般について、各国政府・組織との連携のための仕組み作りをなしていくべきである

[背景]

日本政府の GPKI は行政手続の安全なオンライン化を図り電子申請の安全基盤を確保することを目ざして、進められてきた。ここではかなり高度なセキュリティを設定した単一の証明書ポリシーを前提にしている。それに対して海外では、多様な PKI の用途を想定して複数段階の安全レベル（米国・カナダ政府では４段階）の証明書ポリシーを設定し、それぞれのレベルでの柔軟な連携を可能にさせる方向性をとっている。このような諸外国の動きと整合性を取ることが必要であろう

さらに、Liberty Alliance Project [2]に基づいた仕様採用の検討を開始[3]した米国連邦調達局（GSA）等など、より先進的な取組みとの国際的な連携についても、今後、検討が必要となるものと思われる。

2.3.1.3 PKI の相互運用性の課題に対する提言

[提言]

PKI の「相互運用性」の課題を抽出し、解決策に向けた議論を行うオープンな体制作りが必要である

---

[2] Liberty Alliance Projectは、OASISのSAML(Security Assertion Markup Language)仕様を基盤とし、複数ドメイン間でのシングルサインオン、さらには他の仕様等を用いて、一貫した属性情報の伝達・情報資産へのアクセスコントロールを実現することをめざすものである。同 Projectは米国Sun社・ソニー・NTTドコモなどを中心とするベンダー団体により進められている[OASISについては後述脚注９を参照されたい]。
参考 http://www.projectliberty.org/
Liberty Alliance Projectは、インターネット上でのシングルサインオンサービスの提供を目指し、技術開発などを行なう企業連合（NTTCOMのIT用語辞典を一部改。http://nttcom.e-words.ne.jp/w/Liberty20Alliance.html）

[3] 2003年3月、米連邦調達局（GSA）と米国防総省は、Web認証の標準化を目的とした「Liberty Alliance Project」に参加すると発表した。 参考 http://www.zdnet.co.jp/news/0303/06/nebt_18.html

[背景]

GPKI/LGPKI/公的個人認証基盤などの PKI においては、さまざまな組織をまたいで連携可能な、オープンなシステムを指向しなければならない。その際、いかにしてシステム間の「相互運用性」を確保するかは、大きな技術的課題であり避けて通ることができない問題であろう。検討は、さまざまな利害関係者が存在すること等から、JESAP のような中立的でオープンな場でなされるべきである。その際、相互運用性に関する技術的問題を、一般の人々にも分かりやすい言葉で説明していくことが必要であろう（例えば、具体的な利用シナリオ毎に整理した説明を行うなど）。

また、検討にあたっては、相互運用性を確保すべき PKI アプリケーションを明確化することが望ましい。その上で、幅広いアプリケーションでの相互運用を可能とする相互運用性仕様書の作成などに取り組む体制作りを行っていくべきである。

2.3.2 電子政府行政への提言

2.3.2.1 電子的な申請に対する行政の対応への提言

[提言]

代理申請を実現するために、以下のような対応を行なうべきである

1．代理申請機能を実装した汎用申請システムの開発
2．代理人資格の認証の仕組み
3．委任事項を明示する委任状フォーマットの規程と委任状取り消しの仕組みの開発

[背景]

政府に対する代理申請は、非常に数多く行われているものである。紙ベースで行われている代理申請がペーパーレスで行われるようになった場合、行政の効率化や省資源に資するところが大きいものと思われる。しかし、現時点では、電子申請を受け取る行政側に過渡期の混乱が見受けられる。今後、現状の手続きと PKI の特性とを把握した上でのしっかりとした仕組み作りが行われるべきである。

また、この代理申請の電子化は、将来的な、代理行為全般の電子化へのモデル事例としての意味もあろう。2.1.1.1 で述べたように、行政機関や代理業（いわゆる士業）の関係者だけでなく、一般の人々にも PKI プレーヤーとなってもらう必要がある。その際、適切に使いこなすための敷居が高い PKI について、繰返し電子署名を利用する立場にある電子申請行為者が、代理人やサポーターとしての役割を果たすことも期待されよう。

[今後の検討に向けた補充]

電子申請の三要素は，以下のようなものであろう。

ｉ　電子行政サービス：行政サービスの電子化・オンライン化

ii　電子行政マネジメント：IT を活用した透明性の高い効率的な行政経営・管理

iii　電子デモクラシー：オンラインやオフラインによる市民の行政参加

また、電子申請の５つのゴールは、以下のようなものと考えられる。

i　行政サービスの向上

ポータル、ノンストップ（週７日 24 時間）、ワンストップ、バリューパッケージ（官民連携）、カスタマイズ、紙申請との連携

ii　行政事務の効率化

ナレッジマネジメント、BPR（業務フローの改善）、手続の簡素化・合理化

iii　民主主義の促進

パブコメ、議事公開、電子投票、市民会議室、E-デモクラシー

iv　新しい文化の構築

組織改革、人材の育成、部局横断的、縦割りから水平構造へ、情報共有、権限委譲（意志決定の分散）、経済的な合理性、ビジョンの共有、自発的な参加

情熱と希望、挑戦と変革、多様性の尊重、失敗を認め生かす、協働と連携、改善の欲求、アイデアの創造、サービスの工夫

v　住民と行政の新たな関係の実現

透明性、説明責任、コミュニケーション機会の増大、政治への信頼強化、相互の尊敬・信頼・期待、意志決定への市民参加

電子申請の利用決定プロセスには、知る、信頼する、準備する、利用する再利用する（リピーター）、他人に教える（くちコミ）という 5 段階があるものと考えられる。

PKI（電子認証・署名）の効果は、信頼性の向上に貢献するところにある。一方で、準備や操作が面倒、複雑になる欠点がある。そこで、使いやすさを殺さずに生かす術が探られねばならない。例えば、IC カードには単に技術的な利点のみならず、「形として目に見える」という点でも利点がある[4]。リアルとバーチャルの接点は、リアル社会で存在し利用される、わかりやすいものの延長に構築されることが望ましいと思われる（リアルで信頼がなければ、バーチャルにも信頼なし）

行政が電子証明書の使用を、市民に押し付けることは好ましくない[5]。PKI 電子署名が技術的にはセキュアであっても、使い勝手や使う人の意識によって実際のセキュリティレベ

---

[4] ただし、「形として目に見える」という点だけならば、ID・パスワードを格納した単なる磁気カードでも同様の効果がある。なお、都道府県には、「一人一保険証化」に向け磁気カードの採用を開始する動きが見られる。この際は、サーバーサイドでクレデンシャル（ユーザーの機密情報）を保護するしっかりとした仕組みの採用の検討が必要であろう[例えば、カナダ政府が採用するePass方式（2.2.2.2参照）]

参考　日本経済新聞2003年1月7日付38面
http://www.power-edit.co.jp/kinugawajuku/1headline/nikkei01.html）

[5] 例え任意であっても、電子証明書・電子署名がなければ電子申請が利用できないと言うのならば、もはや任意と言えない。

ルは変わってくるはずである。可能な限り、十分な情報提供（各認証方法のリスクとメリット、被害例、被害状況など）をした上で、市民が自らが好む認証手段を選ぶことができるようなインフラ整備が求められる。

今の電子申請に足りないものは、マーケティングの視点と監視と評価の視点と思われる。

行政が取り入れるべきマーケティングの視点とは、利用者の背景・生活をイメージした住民の新しい生活スタイルや、様々な市民セグメンテーション[6]のニーズへの対応を図ることといえよう。まず「電子申請、電子行政サービス」ありきのスタイルでは、市民と行政との情報が双方向でないため市民の側から、ニーズ、サービス満足度、クレームつけ、改善提案を行うことが難しく、結果、電子申請を利用してもらうための仕組み作りが不十分となりがちであろう。

また、行政が取り入れるべき監視と評価の視点とは、システム構築・運営の費用や利用状況等の情報公開、第三者機関（NPO）等による監視、公正な基準に基づいた適切な評価などを行政の側が受け入れ、その上で、電子申請を改善していく姿勢といえる。

今後、こうした取組みを続けていくことが、市民に NO と言われない電子申請インフラ作りのための鍵となるのではなかろうか。

2.3.2.2　教育分野での PKI 利用に向けた提言

[提言]

大学／教育機関を国際的に共通な枠組みとして捉え、教育分野における認証基盤について国際的な規格作りに取組むべきである。

［背景］

教育分野では、大学間での単位交換など、組織間での連携が求められている場合が多い。今後、日本国内に限定せずに、PKI を用いた認証基盤により教育分野での組織間連携に向けた取組みをはかるべきである。すなわち、教育機関での認証の必要性を国際的に共通なものとして捉え、国際的に統一的な規格の下に「国際オンライン学生証／身分証（仮称）」、「国際的アクレディテーションの電磁的証明」、各大学の「オンライン認定」、「電磁データによる各種証明書」などの構築に向けた取組みを行うべきである。

[今後の検討に向けた補充]

上記のような試みは、今後、紙に頼り過ぎない省資源で効率的な社会を築いていくための情報リテラシー教育という側面もある。したがって、情報化社会の将来にむけた人的資本への投資であるという認識をもってもよいのではないか。

さらに国境を容易に超えることができるバーチャル空間の特性を活かし、国際的な大学間連携が構想されてもよいだろう。国境の壁・言語の壁などから、現状の国際的な大学間

[6]性別、年齢、職業、家族構成、年収、資産保有状況、住所 地域の特性など

連携では相当のコストが発生している。そのため、経済的に恵まれていない人々は、相当のエリートでない限り、留学のチャンスに恵まれないのが通例である。PKI を用いた認証基盤がシステム化されることで国を超えた大学間連携が安価に可能にしていくことは、IC カードなどにおいて最高水準の技術力を有する日本が世界に向けて果たしうる平和的国際貢献といえるのではなかろうか。

また、大学には各地域からかなりの信頼が寄せられているのが通例である。したがって、市民大学的な試みなどと連携し、大学が地域コミュニティを電子化する際の身近な信頼点としての機能を果たすことが検討されてもよかろう。また、鍵ペアと当人とを結びつける本人性確認の場としての機能を果たすことも、望ましいと思われる。この点は、大学に限らずとも、財政難と少子化により少なからず社会的役割の再編が求められているのであろう学校が、地域において果たしうる機能かもしれない。

2.3.2.3　地域活性化・差別化への PKI 活用に向けた提言

[提言]

PKI の利用促進を通じ、地域の活性化や差別化へとつなげていくための活動・施策を試みるべきである。

[背景]

PKI に基づく電子的な認証基盤構築に対しては、地方における期待の方がむしろ大きいように見受けられる。横並びで進んだインフラ整備の次の段階として、地域の活性化・差別化のための基盤として注目されていることがその一因と考えられる。

今後、電子署名が普及し、バーチャルなコミュニケーションがより実質的なものとなった場合、大都市と地方都市・農村の間における情報格差を縮小することが可能となるかもしれない。そのためにも、PKI を全国的に普及促進させる活動（加えて、国際的に普及促進させる活動）が大切と思われる。

[今後の検討に向けた補充]

地域における行政・民間共用の認証基盤を整備し、地域の活性化や自立化が図る施策は、負荷分散・危険分散・既存資産活用などの観点から、より社会コストを抑えた利用しやすい認証基盤となる可能性がある。

各地において、電子商取引の活発化や電子自治体の推進などにより、企業活動のみならず住民生活の場にもインターネットは浸透してきている。PKI を活用することによるセキュリティの確保が、ネットワーク基盤上で一般的になれば、企業はユーザへのより高い付加価値サービスが提供可能となり、住民は自治体からのワンストップサービスやノンストップサービスなど、より質の高い行政サービスを受けることができるようになろう。

インターネットには、地域格差が生じにくいという特性がある。企業が中央に負けない

企業競争力を得て地元産業が活性化し、住民が質の高い行政サービスを受けることができるためには、インターネット上での認証基盤（PKI 等）も、地域重視で構築するという視点があってもよいのではなかろうか。

セキュリティが確保された安全で信頼のできる情報認証基盤を地域が持つために、自らの手で認証基盤を活用する姿勢・自立的に取り組む姿勢が必要であろう。

現状では、行政の手による認証基盤の整備は、上からの中央集中の論理で進んでいるように見受けられる。しかし、GPKI や LGPKI 等で採用されているブリッジ・モデルは複数の信頼点を許容しつつ相互に認証し合うためのメカニズムであり、そもそも各地の認証局がそれぞれに信頼できる認証メカニズムを作り上げていくためのものといえよう。

さらに、2.3.1.2 で述べた Liberty Alliance Project に基づく仕様などにおいては、情報資産の分散管理は常識となりつつある。各地域の情報資産の活用のためのそれぞれの取り組みを尊重し、ボトムアップに認証基盤を作り上げていくという考えには、技術的な裏付けが存在する。したがって、中央はそうした新技術を踏まえた上でポリシー統一等の役割を担い、認証基盤の構築およびその発展は、地域ブロック単位で責任を持って担っていくという方向性は、十分検討に値しよう。各地域において基盤整備に自発的に取り組むことは、ビジネスチャンスの獲得・住民の情報リテラシーの向上等のメリットがあると考えられる。今後、各地域におけるこうした取組みを推進しつつ、日本全体としてもこうした考え方の採用をセキュリティ面・経済性の面の観点等から検討していくことが必要ではなかろうか。

2.3.3 行政分野以外での電子署名活用に対する提言

2.3.3.1 電子署名の利用促進に向けた地域通貨活用の提言

[提言]

現状では一般の人々が実用的に使う機会の少ない電子署名を気軽に使っていただくために、電子マネー・地域通貨など、PKI の特性を活かすことのできる便利なツールの開発・普及を促進していくべきである。

[背景]

PKI による電子署名は、バーチャルな空間に「顔の見える関係」を作り上げられる画期的な技術である。しかし、文書等に対してなした電子署名がいかなる意味を有するか（又は有しないか）は、技術ではなく慣習や制度によって定まるものである。電子署名が社会に広く受け入れられていくためには、慣習・制度面に踏み込んだ検討が必要と思われる。その際、はじめから過度にフォーマルなものを志向したのでは、逆に電子署名の普及を阻害しかねない。安心して電子署名をなすためのスタンダード作りを検討することは必要であ

るが、一方で、電子署名を一般化させるための試行錯誤[7]に皆で取り組んでいけるカジュアルな組織作りも大切と思われる。

[今後の検討に向けた補充]

電子署名を社会に普及させるためのスタンダード作りは、実際には、監査・紛争処理・トラブル相談など既存の社会制度をバーチャル化するなどといった比較的フォーマルな作業となるのかもしれない。しかし、その際も、使いやすい仕組みを作り上げるために、市民や各種コミュニティの声を反映していくことが大切と思われる。以下、参考までに、NPO 法人 CACAnet 福岡のコミュニティ認証局を用いた活動を検討中の NPO 法人 CCCNET（東京都町田市）の取組みを紹介したい。

女性の就労支援などをめざす地域事業系 NPO である同法人は、現在、電子認証を総会決議等に用いようとしている。NPO の総会に参加する人々は、広域に分散していることがしばしばのため、事務処理コストの節減等、オンラインで議決をなすメリットが大きいという。株式総会の議決権行使のみならず、地域住民が気軽に参画・参加できる NPO 法人でこうした試みが広がっていけば、PKI を用いた電子署名が一般の人々にもなじみ深いものとなっていくのではなかろうか。

また、同法人では、就労支援事業に Travecoup などの地域通貨を用いることも検討しているという。就労支援事業にいかなる形態の地域通貨を用いることが望ましいかは、なお検討の余地があろうが、改ざん・否認・なりすましを効果的に防止できる PKI ベースの電子地域通貨はその有力な候補となるものと思われる。ただし、数年前から各地域で多数試みられている地域通貨構想は、かけ声の割には、期待されたほどの成果をあげられていない模様である。内部の事務処理の効率化という側面の強い総会決議の電子化と異なり、組織間・地域間などの連携が必要となる地域通貨では、仕組み作り PKI ベースの電子地域通貨が広く利用され地域の活性化・差別化に役立たせるためには、まずは地域通貨を用いるローカルなコミュニティ等が相互に連携する仕組みを作り上げていく必要があるのかもしれない。また、電子地域通貨システムの情報セキュリティ確保のあり方や決済モデルの法的位置づけ等、技術的な検討も必要となろう。これらを検討する場として、地方自治体や地域の大学（市民大学的なもの等）の働きが期待されようか。

[7] 例えば、電子的地域通貨には、CACAcet福岡のTravecoup（これまでのバージョン）のように対人的な（債権的な）関係に基づくものと、LETS(Local Exchange Trade System)のようにコミュニティへの対世的な関係に基づくものとがある[前者はIOU(I owe you)型、後者はIOC(I owe community)型とも言われる]。こうした仕組みの違いを理論的に把握することもむろん大切であろうが、同時にいかなる仕組みが受け入れられるかは、試行錯誤の結果決まることを忘れてはならない（なお、CACAcet福岡のTravecoupはシステム的には、LETSのようなIOC(I owe community)型の用いられ方をすることも可能とのことである）。

2.3.3.2　司法分野・医療分野等での電子署名活用に向けた提言

[提言]

司法分野や医療分野など電子的な契約関係が必要とされている分野において、電子署名を広く活用していただくための仕組み作りの検討が必要である。

[背景]

e-Japan 重点計画-2002 においては、2003 年度までに、電子情報を紙情報と同等に扱う行政を実現することを目標としてかかげている。また、かかる行政の情報化と並び、公共分野全般の情報化をもめざし、広く国民生活の利便性の向上とともに、経済社会全体の情報化の起爆剤になることをめざすとする[8]。行政分野以外の公共分野のうち、特に国民のアクセシビリティ向上が求められるものとしては、医療や司法と関わる分野があげられよう。

両分野では、完全性・機密性の確保等、情報セキュリティに関する要請が、場合によっては行政分野以上に強いといえよう。センシティブな医療情報は確実に受取人のみに伝えられねばならず、重要な契約への意思表示を示した文書は、可能な限り当人の意思を正確に反映したものでなければならず、また、改ざんや否認がなされないようにしなければならない。こうした要請を満たしうるものとして、PKI を活用した電子署名・暗号化システムがもっとも有力なものであろう。

[今後の検討に向けた補充]

現時点の日本では診療契約・司法分野での PKI の活用はさほど進んでいない[9]。その理由は、技術的な要因以外のものが大きいのかもしれない。診療契約・司法分野で PKI、とりわけ電子署名の活用が必要とされるのは、組織内の事務処理の補助[10]の場面よりは、むしろ組織間・個人間での契約関係の締結・履行[11]に関わる場面であろう。確かに、電子署名法の施行により、電子署名を付した文書の成立について真正性が推定されるようになり[12]、また、電子消費者契約及び電子承諾通知に関する民法の特例に関する法律により、消費者が行う電子消費者契約の要素に特定の錯誤があった場合についての法的整備も行われた。しかし、現実に電子署名が社会的に広く用いられておらず司法判断も蓄積されていない現状では、

---

[8] http://www.kantei.go.jp/jp/singi/it2/kettei/020618-2-4.html

[9] 日本PKIフォーラムの調査によると、マレーシア・台湾においては、ICカードに本人の医療情報（かルテ情報）をIDカードに入れて、医療機関間で参照しあうことが行われているとのことである。
http://www.japanpkiforum.jp/journal/contents/b_kankyou.html

[10] 組織内の事務処理において、新たな契約が締結されることは少ない（事務処理に先立って、予めの契約（例えば雇用契約）が結ばれるのが通例）。

[11] 医療行為は、意識のない患者に対し緊急避難的になされる場合等を除き、一般に診療契約に基づいてなされる。日本においては、診療契約は準委任契約（民法 656条）であるとの解釈が通説的である。

[12] [電子署名及び認証業務に関する法律第三条]
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

個別の電子商取引等の具体的場面における、実体法上の効力などについて、その細かな点に不明点が未だ残るだろう。したがって、今後の電子署名普及のためには、単なる法的整備というよりはむしろ、具体的なビジネスシナリオに即した形で電子署名制度の普及啓発活動をなしていくといった取り組みが求められているのかもしれない。

リアルワールドでは、両当事者は、既存の取引慣行や標準約款等を利用しつつ契約を交わすのが通例である。契約締結にあたり、取引慣行や標準約款は、いわゆる公共財としての役割を果たしているのである（こうした慣行・標準約款の存在は裁判においても尊重される）。インターネットなどのバーチャルワールドでは、RosettaNet による情報機器・電子部品分野における電子商取引の標準など、いくつかの分野では標準的な電子商取引の慣行や標準的な約款が確立しつつあるものの、多くの電子商取引分野では未だ慣行が確立していない[13]。

情報機器・電子部品分野では、パーツの標準化が B2B 電子商取引の進展に大きな役割を果たし、その後の ebXML 仕様策定にも大きな影響を与えた。司法・診療契約分野でも、よく用いられる構成要素の標準化が必要であろう。

ここで、診療契約分野は広く市民と関わりあう領域であり、司法分野は市民の権利義務関係についての規範的役割を果たす領域であることからすれば、両分野の電子化は、それぞれの領域内に留まらない幅広いインパクトを及ぼすものとなりうることに留意すべきである。例えば、ひとたび、診療契約分野における申込・受諾・締結・履行等が電子署名を用いてなされるようになれば、広く市民が電子署名になじむこととなろう。司法の場での争訟手続きの争点整理・証拠調べ等において電子署名が活用されるようになれば、ビジネスの場での電子署名の利用に安心感を増すこととなろう。その他、租税申告の場で電子署名が用いられることにも同様の効果が期待できるかもしれない（ただ、公共性が強いにせよ、私人間の関わりが前面に出る診療契約や司法分野はやはり、一般市民への電子署名の普及において特別の役割を果たすものと思われる）。

このように司法・診療契約分野での電子署名の利用は、PKI 全般の利用促進につながりうるものであろう。では、司法の場や診療契約での電子署名利用促進のためにいかなる手立てがなされるべきなのだろうか。ここでは仮に三つの要請をかかげておくこととする

第一に、ビジネス全般の要求と同様に、タイムスタンプや属性認証など PKI の応用分野を使いやすいものとしていく必要があろう。文書の成立時刻や代理権限の存在をバーチャルワールドで確定できる手段を提供することは、多くの分野で共通する要求である。

第二に、各主体がなす行為を標準化し、機械可読な（machine readable）形式で定義し

---

[13] この点、電子商取引に広く用いられることを目指したebXML仕様を策定、法律文書の標準をめざすLegalXML仕様の策定開始など、OASISが意欲的な動きを見せている。
RosettaNetは、情報機器メーカや電子部品メーカが中心となって、BtoBの基盤となる標準規約を定めるために作られた団体。 OASISは、ビジネスにおける情報交換用技術標準を作成する国際的な団体。2002年秋に米国PKIフォーラムを吸収している。　共に@ITのXML用語事典を一部改
http://www.atmarkit.co.jp/fxml/dictionary/indexpage/xmlindex.html）

ていく必要があろう。この要求も多くの分野で存在しようが、とりわけ契約などの法律行為や準備書面提出などの訴訟行為については、その有効性を定めた法規が存在し、情報システム構築の際には、特別の配慮が求められる。例えば、一定のかんちがい（要素の錯誤による意思表示）が無効にされるとの規定[14]に対して、電子的な契約の意思表示をなるべく有効とするために、かんちがいの発生をなるべく少なくする仕組みを用意する必要があろう（無効・取消事由の発生は、当事者に連絡や再交渉の手間を負担されることとなる）[15]。そのためには、何が「契約の要素」なのか等を把握し、契約締結フローの適切な場面でそれを提示できるような情報システムの構築などが必要となろう[16]。一定の目的に向けて行為することが同意されている組織内の事務処理とは異なり、参加当事者の目的設定自体の同意をめざす契約行為では、契約の内容について両当事者の理解が隔たっていることもしばしばであり、システム構築の際には特別の配慮が必要であろう。

第三に、ビジネス側の要求のうち、情報システム側が担いきれない部分について、各種制度（法規や保険など）が担っていくための仕組み作りの検討が必要であろう。その際、情報システム構築技術の進歩等に柔軟に対応できる技術中立な制度制定が心がけられるべきであろう。

---

[14] 参考 [民法95条] 意思表示ハ法律行為ノ要素ニ錯誤アリタルトキハ無効トス 但表意者ニ重大ナル過失アリタルトキハ表意者自ラ其無効ヲ主張スルコトヲ得ス

[15] 現行の電子署名法により真正性が担保されるのは表示が署名者によりなされたことのみである。

[16] そのためには、契約の類型化が必要となる。この類型化は動的かつ妥当な形式でなされなければならない。例えば、日本の民法では13種の有名契約が存在するが、各種の特別法や両当事者の合意によりそこから派生する個別の契約がなされる。その細部について、全て情報システム側が把握することは経済的ではなかろうが、繰返し用いられる要素については、フロントエンドでのインターフェイスやバックエンドで用いられるAPI等の標準化の必要があろう。

この点、EUでは、EESSIを中心が議論をリードする形で、API、ヒューマンインターフェイスについての規範の整備が進んでいる。

また、OASISのLegalXML eContracts TC [http://www.oasis-open.org/committees/legalxml-econtracts/]による、契約文書のXML化の試みも行われている。

3．国内における PKI 推進の状況

日本における PKI 推進の動きが広がりを見せている。

GPKI/LGPKI の動きに対応するように政府系の研究団体や民間団体においては、電子政府のサービスに対応するための検討が進められている。また、GPKI とは独立した民間におけるサービス、PKI 関連の調査研究も進められている。また、PKI に関する一般の人々に対する普及啓発活動も起こってきた。

図 3-1 に、JESAP 運営委員会に参加する団体を中心に、PKI 推進にかかわる団体の活動の位置付けを示す。この他にも多くの団体において PKI の推進または利用に関する検討が進められている。また、個人でも「Manaboo's Room＜http://www.manaboo.com/＞」のような PKI を理解する上で優れた Web サイトも登場している。

以下、電子政府推進の状況について簡単に紹介するとともに、JESAP 運営委員会に参加する団体を中心に、PKI 推進に関わる団体について紹介する。

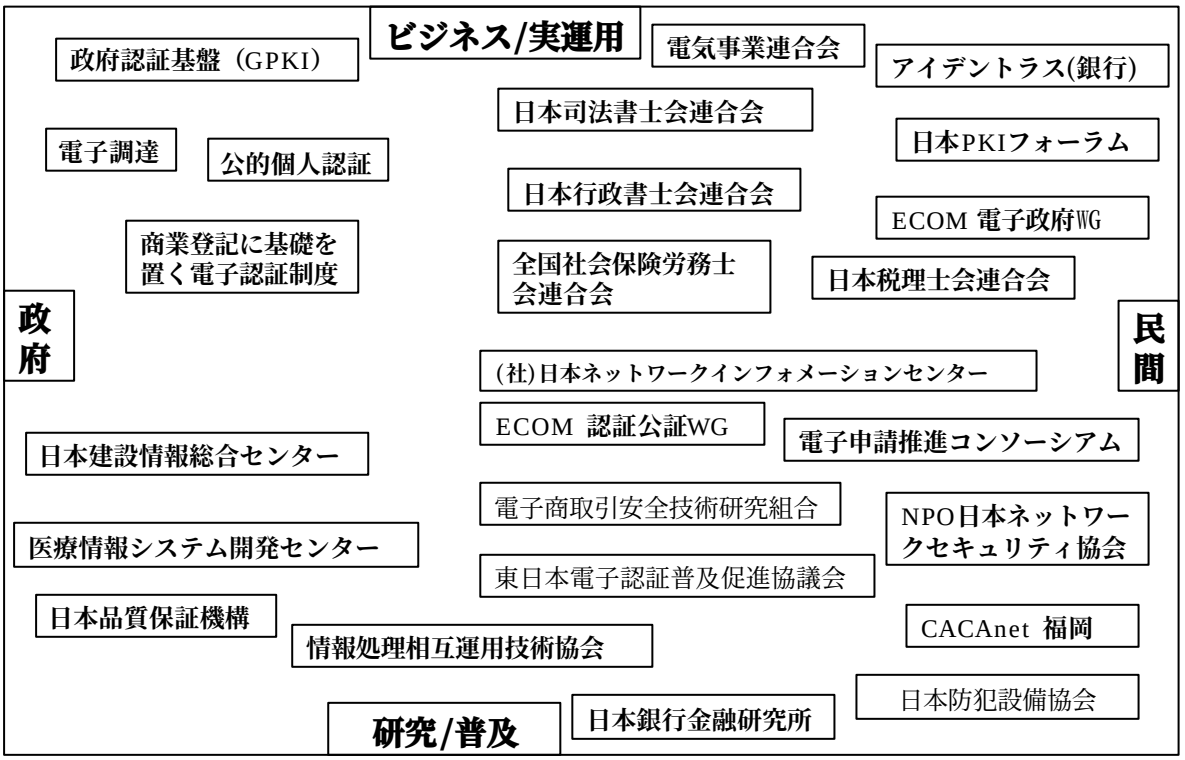

図 3-1 PKI 推進関連団体の位置付け

3.1 電子政府

3.1.1 政府認証基盤（GPKI）

(1) 電子政府と GPKI

いつでも、どこでも、誰でも、インターネットを経由して、国の行政機関等に対して、申請・届出等の手続や行政情報の検索・閲覧等が行えるのが電子政府である。GPKI は、この電子政府を実現するための一つの基盤であり、申請・届出等の手続の電子化にあたっては必要不可欠な仕組みとなるものである。

(2) GPKI に至る経緯

国の行政機関においては、従来各府省が個々に行っていた情報化の施策を、政府全体としての計画に基づき進めるものとし、GPKI の整備についても、次のとおり取り組んできている。

- 平成６年の第一次行政情報化推進基本計画では、電子政府構築に向けて各種行政の手続を推進することが示された。
- 平成９年の第二次行政情報化推進基本計画においては、初めて政府と国民とのインターフェース部分の情報化を積極的に進め、21 世紀初頭に電子政府を実現することが宣言された。
- 平成 11 年にミレニアム・プロジェクトが立ち上げられ、この中で平成 15 年度（2003 年度）までに GPKI を整備することが明確に取り決められた。
- ミレニアム・プロジェクトを受け、平成 12 年３月には、申請・届出等手続の電子化推進のための基本的な枠組みが決定され、総務省、経済産業省及び国土交通省の３省は先行的に府省認証局を構築し、さらに総務省においては、それらを相互に接続するブリッジ認証局を構築することとされた。
- 平成 14 年６月に策定された e-Japan 重点計画-2002 においては、基盤整備の前倒しを図るため、先行府省以外の各府省は、平成 14 年度までに府省認証局を整備し運用を開始することが決定された。

(3) GPKI の範囲と他の認証基盤

ブリッジ認証局と各府省の府省認証局が相互認証を行うことによって、GPKI という一つの仕組みとなる。一方で、法務省による商業登記認証局、電子署名法に基づく民間認証局、地方公共団体による公的個人認証サービスに基づく認証局、地方公共団体の職員を認証する LGPKI が構築され、又は構築される予定となっているが、これらの認証局とブリッジ認証局は順次相互認証を行っていく。なお、これはあくまでも申請・届出等手続の電子化のためであって、民間の電子商取引において、民間の認証局間を

仲立ちする役割は果たさない

商業登記認証局については、平成 12 年度に商業登記法の一部改正を行って認証局の運用を開始し、平成 13 年度にブリッジ認証局との相互認証を完了している。また、電子署名法に基づく民間認証局も続々と立ち上がってきている。

地方公共団体による認証局については、地方公共団体の職員を認証する LGPKI と、住民を認証する公的個人認証サービスに基づく認証局が、それぞれ平成 15 年度に運用を開始するべく準備を行っている段階である。

(4) GPKI の整備方針

GPKI の整備方針の大きな柱は、次のとおりである。

① 申請者の利便性の向上と、GPKI 全体の効率的な構築を図る。また、適切なセキュリティ対策によって安全性・信頼性を確保する。

② 国際的に認められ、または国際的に用いられている標準（デファクトスタンダード）となっている仕様・技術を採用することにより、汎用性・拡張性を確保する。

③ ブリッジ認証局の相互認証のための基準として、府省認証局との間、民間認証局との間のそれぞれについて、技術基準と運用基準が定められている。府省認証局については、官職認証業務に関する基準として、技術基準、運用基準ともに CP/CPS（Certificate Policies /Certificate Policies Statements）が CP/CPS ガイドラインに準拠していること、相互認証業務に関する基準として、相互運用性仕様書に適合しかつ相互認証のテストに合格することとされている。

(5) 今後の予定

行政への電子申請や電子入札を目的として電子署名法の認定を受ける事業者が出てきており、今年度中に複数の民間認証局がブリッジ認証局と相互認証を行うものと見込まれている。

一方、府省認証局は、平成 14 年度（2002 年度）中にすべての府省において構築され、あわせてブリッジ認証局との相互認証が行われる予定となっている。

府省認証局の運用を行っている総務省、経済産業省及び国土交通省においては、既に認証基盤を活用した電子申請が行われており、他の府省においても、府省認証局の構築に合わせ、行政手続のオンライン化が進められることになっている。

3.1.2 公的個人認証

(1) 検討の経緯

平成 13 年５月に、総務省内に検討委員会を設置し、オンライン申請のための利用者の電子証明書を地方公共団体が発行する制度について検討し、平成 14 年２月にその成

果を公表している。総務省は、その成果を踏まえた法律案を作成し、平成 14 年６月に国会に提出している。

(2) 制度の概要

① 認証局

認証局における本人確認機関は全国の市町村長であり、利用者は市町村窓口で証明書を入手する。証明書の発行については、証明書の公証力、運営経費等の経済性等を考慮し都道府県知事がこれを行う。つまり、概念的には 47 の都道府県単位の認証局がそれぞれの住民に対して証明書を発行することとなる。

② 手続き

オンライン申請用に電子証明書の発行を受けたい人は、その者が記録されている住民基本台帳の市町村の窓口に出向き申請手続きを行う。本人確認は、基本４情報（住所、氏名、年齢、性別）をもとに住民基本台帳と照らし合わせ、その人の実在性を確認する。その上で写真付きの身分証明書等により、本人性の確認を行う。

鍵の生成は、信頼性担保の観点から鍵生成装置を認証局側が提供することを考えている。各窓口に鍵生成装置を配備し、本人が秘密鍵、公開鍵をつくる形態を想定している。格納媒体については、セキュアな媒体ということで基本的に IC カードが考えられている。

窓口では、申請者の公開鍵をもとに都道府県知事が発行した電子証明書と自己署名証明書を IC カードに入れ交付する。

なお、都道府県知事の意向により指定認証機関の中から法人を選択し、電子証明書の発行業務等を委任できる制度が考えられている。

③ 認証の方法

自宅もしくは企業等からオンライン申請を行った場合、行政機関は受け取った証明書の有効性確認のため、都道府県知事から失効情報（CRL 等）を入手する。この時、有効性確認のできる者は各府省、地方公共団体、特定認証事業者、もしくはそれと同程度の信頼性を有する民間認証事業者に限定される予定である。なお、電子証明書の有効期間は３年間とされている。

④ 失効情報

失効情報については、利用者の氏名、住所等に変更が生じた場合には職権で電子証明書を失効させ自動的に失効リストに載せることにより、電子証明書の信頼性が確保される。

失効情報の提供については、失効リストをつくって配る方法と、OCSP（Online Certificate Status Protocol）レスポンダを利用し個別に回答する方法の２つの方法が想定されている。

(3) 今後の予定

本制度は電子政府・電子自治体の一つの共通基盤になるものであり、平成 14 年度には全国実用試験が計画されている。本番規模のシステムを構築し、各府省の汎用受付システム、自治体の受付システム、GPKI、LGPKI、民間事業者との接続試験及び、実際の窓口での IC カードを使用したモニターへの電子認証書の発行試験等が行われる予定である。

3.1.3 電子調達

(1) 電子入札の背景

平成 13 年 1 月に策定された e-Japan 戦略の中に「政府調達の電子化」という項目がある。また、透明性の確保や公正な競争の促進等を目的に、公共工事の入札及び契約の適正化の促進に関する法律が平成 13 年 4 月 1 日に施行され、この指針の中に「入札契約の IT 化の促進」が盛り込まれている。

国土交通省では、公共事業分野における CALS/EC の取り組みを行っている。CALS/EC は、IT 活用により公共事業の一連のプロセスにおける、部門をまたいだ情報の共有、有効活用を通じて業務プロセスの改善に資することを目的とした取り組みである。電子入札も入札契約段階における CALS/EC 導入の一環と位置づけられる。

国土交通省が策定した CALS/EC のアクション・プログラムでは、平成 8 年度から平成 16 年度までの期間を 3 つのフェーズの分け、順次実現を図ってきている。平成 14 年度を初年度とする第 3 フェーズでは、電子入札、電子納品の全面導入、電子契約の開始、光ファイバーデータ流通環境の整備及び、電子決済システムの構築等が目標として掲げられている。

(2) 電子入札の概要

国土交通省の場合、電子入札施設管理センター（e-BISC センター）において、電子入札システムを運用している。

認証局は、現在 1 社で行っているが、平成 15 年度より導入予定の電子入札コアシステム（後述）においては、複数認証局対応となるため、認証局内の価格、サービス競争の環境が整う。

電子入札導入効果としては、応札者の移動にかかるコストや移動時間の低減が大きいと考えられる。ちなみに、国土交通省の直轄工事だけでみても、年間 260 億円のコスト縮減効果が試算されている。

また、一連の手続きをネット公開することにより、透明性、競争性が確保されるというメリットも期待できる。

(3)　電子入札の取り組みの現状

国土交通省の電子入札においては、平成13年11月に第1号案件の開札が行われ、工事97件、コンサル業務や設計2件の計99件に適用された。平成14年度は2,000件に適用される予定であり、さらに、平成15年度は全案件（約54,000件）に適用されることとなっている。（当初計画の1年前倒し）

なお、電子入札システムについては、国土交通省が開発したシステムをベースにして、広範な公共発注機関が共通の道具として使うための「電子入札コアシステム」が、（財）日本建設情報総合センター（JACIC）と（財）港湾空港技術サービスセンター（SCOPE）の共同で開発・提供されている。

3.1.4　商業登記に基礎を置く電子認証制度

(1) 商業登記とは

商業登記とは、会社その他の法人に関する一定の事項を登記簿に記載することで、その登記簿を公開し、取引の安全に資している。

法務局、地方法務局、同支局、出張所等、商業登記事務を取り扱う登記所は全国に700ヶ所あり、全国約350万件の会社、法人の登記を管轄、所管している。

(2) 商業登記の役割

① 会社は、登記をすることにより法人格を取得する。登記が効力要件、成立要件となる。

② 登記事項に変更があれば、遅滞なく変更登記をする義務が法律上規定されている。

③ 登記すべき事項は、登記しなければ善意の第三者に対抗できない。登記しなければ、その内容を知らない人に対して主張できないということで、登記が対抗要件と言われる所以である。

④ 故意・過失により不実の登記をした者は、善意の第三者に対抗できない。故意・過失によって実際と違う登記をしてしまった場合であっても、そのことを知らない善意の第三者には不実であることを主張できず、登記どおりの責任を負わされる。

(3) 登記の内容の正確性担保のための手段

登記内容の正確性を確保し、信頼性を高めるため、次の手続、手段が用意されている。

① 登記の申請には添付書面が必要である。

② 代表者の印鑑提出の義務がある。

③ 無効、取消しの原因がある場合には、申請が却下される。

④　登記を怠ると過料の制裁がある。
⑤　虚偽の登記申請には刑事罰が科せられる。

(4) 電子認証制度のあらまし

①　商業登記に基づく電子認証

紙の世界では、登記簿謄本、資格証明書、印鑑証明書など、登記所が発行した書面により、法人の法人格の存在、代表権限の証明、本人性の証明を行う。この機能をそのまま電子の世界でも提供しようというのが、商業登記に基づく電子認証制度である。

②　商業登記に基づく電子認証制度の特徴

登記簿の記載内容に基づいて、登記上の会社代表者の電子証明書が発行される。証明書の内容としては、本人の氏名以外にも、商号、本店、代表者の資格等を登記簿の記載内容に基づいて証明される。

これは、法律に基づき登記官が行う公的な証明であり、会社等の認証を行う上で最も重要な登記簿に基づいた電子証明書ということになる。

特徴的なのは、商業登記に基づいているので、商号変更、本店移転、あるいは代表者の交代等の登記事項の変更があると、それをリアルタイムに電子証明書に反映させることが可能となっている。

③　電子証明書の失効・保留

電子証明書の失効や保留については、法人代表者による使用廃止届、使用休止届があり、また、登記の申請、変更登記の申請等があり、それらによって失効や保留（効力停止）がリアルタイムでできる仕組みが用意されている。

④　電子証明書の取得まで

法人代表者が、管轄登記所（登記簿を所管している法務局）に電子証明書の発行を申請すると、電子認証登記所からインターネット経由で交付される仕組みになっている。

なお、申請時には、必要な申請情報を用意するほか、秘密鍵と公開鍵の鍵ペアを作成し、公開鍵を法務局に届け出て申請を行い、法務局で一定の審査が行われた後、シリアル番号等が告知され、その番号を以って電子認証登記所から証明書の取得を行う。

⑤　電子署名とその検証

実際に法人代表者が電子証明書を利用する場合には、相手方である契約の申込先は、署名確認等をした後、電子認証登記所に電子証明書の有効性を確認できる仕組みが設けられている。

(5) 現状と今後の予定

① これまでの主な動き

平成 12 年 10 月から東京法務局と前橋法務局でシステム運用が始まり、平成 13 年 3 月から、商業登記に基づく電子認証を利用する形で、債権譲渡登記のオンライン申請が導入されている。

また、平成 13 年 6 月から、GPKI との相互認証が実施されている。

さらに法務省では、平成 14 年 1 月からの「公証制度に基礎を置く電子公証制度」の運用開始との連携、平成 14 年 4 月からの商法等改正に伴う会社関係書類の電子化等への対応を実施している。

② 商法改正による会社関係書類の電子化

平成14年4月1日に施行された商法等の改正により、オンラインではないものの、会社関係書類の電子化が行われ、議事録、就任承諾書、定款など、登記申請書の添付書面が電子的に作成されている場合には、その電子的記録に電子署名を行い、フロッピーやCD-Rを申請書に付けて法務局に提出することで、登記の申請ができるようになった。

③ 利用手数料の改定（引下げ）

電子政府実現に伴う利用見込み件数の増加，実施経費の削減等により，平成15年４月１日から利用手数料が大幅に引き下げられることとなった。

証明期間	3月	6月	9月	12月	15月～27月
手数料（円） 改定前	24,000	48,000	72,000	96,000	超過期間3月ごとに 24,000円を加算した額
	↓	↓	↓	↓	↓
改定後	**2,500**	**4,300**	**6,100**	**7.900**	**1,800円**を加算した額

④ 今後の主な取組みと課題

- 電子認証制度の運用の早期全国展開
- 電子署名の普及と利用環境の拡大等

3.2 業界団体における推進状況

3.2.1 日本司法書士会連合会

(http://www.shiho-shoshi.or.jp/)

(1) 設立年月日/会員規模

1927 年 設立

全国 46 各都府県と北海道 4 会、計 50 司法書士会。17,200 余名。

(2) 主な活動と成果

① 司法書士会の主な活動

司法書士会では、司法書士の業務（a.不動産登記手続 b.商業登記手続 c.供託手続 d.裁判所に提出する書類の作成など）に関連して、司法制度改革、消費者問題、成年後見制度等の問題に組織的に取り組んでいるが、登記業務に関連する登記情報システムの研究、オンラインによる登記申請に向けての研究は、司法書士総合研究所を中心にかなり早くから取り組んできた。また、近年はIT化対策のため執行部内に高度情報化対策部を設置し、重点事業として取り組んでいる。

A．司法書士総合研究所

・「登記情報システム部会」（総研第１部）における研究

「オンラインによる登記申請システム」に関する中間報告書

http://www.shiho-shoshi.or.jp/shuppan/think/sk01-971.htm

「オンラインによる登記情報公開システム」に関する分析と提言

http://www.shiho-shoshi.or.jp/shuppan/think/sk01-961.htm

「登記オンライン申請と電子認証」に関する分析

http://www.shiho-shoshi.or.jp/shuppan/think/sk110331/sk110331.htm

・「不動産登記法改正部会」（総研第６部）での研究

「不動産登記法改正答申書」

http://www.shiho-shoshi.or.jp/shuppan/think/think98-180.htm

・総研第10部（比較法・アジア班）

「韓国・中華民国の土地登記情報システムの概要」

B．高度情報化対策部

a) 1999～2001

「日司連電子認証局」の立ち上げ（債権譲渡登記オンライン申請への対応）

司法書士が代理人として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には、司法書士の本人確認と資格証明が必要との考えから、司法書士電子証明書の発行は、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とした。（司法書士登録事務は、司法書士法第６条により日司連が行うものとされている）

・日司連認証局規則

http://www.shiho-shoshi.or.jp/ca/rule.htm

・日本司法書士会連合会認証局運用規定（CPS）

http://www.shiho-shoshi.or.jp/ca/cps.htm

＊ 今後のオンライン電子登記申請システムにおいて、申請アプリケーションに代理人システムが組み込まれることを想定し、GPKIのブリッジ認証局との相互認証が可能となるシステムとするよう準備中である。

b) 2001～2002

・「IT 化社会対策部会」（３ワーキングチーム）

高度情報化社会における司法書士職能のあり方についての対策

各種行政電子申請制度の方向性と、司法分野での電子申請制度等を見極めながら、高度情報化社会における司法書士職能のあり方、会員の便宜に供するような情報機構、高度情報化社会の中での連合会および司法書士会のあるべき方向性と必要な制度確立のための事業化へ向けての対策を講じるため、連合会内でのコンピュータネットワーク（Web）利用による通信体制構築、オンライン登記申請への対応可能な日司連電子認証局の再構築、オンライン登記申請のためのトレーニングシステム、行政官庁・裁判所および他士業の電子化への対応および進捗状況に関する調査研究を行っている。

・「電子登記対策部会」（２ワーキングチーム）

オンライン申請の実施に向けた登記申請制度の変革についての対策

登記制度が、電子政府の実現という要因により不動産登記と商業登記のオンライン申請の実施へ向け準備され、国民の負担軽減と利便性の向上が重要な要素とされ申請手続が簡明となり国民の利用しやすい制度となることは専門家としても歓迎するものである。しかしながら、登記とは単に申請行為に止まるものではなく、不動産の権利義務の変動に直接影響し、また商業登記においても単に会社の内容を申告するのではなく取引相手の利害、権利義務に影響を及ぼすものであり、国民の経済取引の安全確保に不可欠な制度である。そこで、司法書士は登記専門職として登記制度の信頼性確保、真正担保制度の構築について積極的に提言する責務があるとの認識のもとに、法務省の委託により財団法人民事法務協会に設置された「オンライン登記申請制度研究会」に委員を派遣し、登記の電子申請制度の法整備ならびにシステム構築に参加している。

(3) 連絡先

日本司法書士会連合会 高度情報化対策部
対策部長 佐藤純通 jun2@ss.iij4u.or.jp
〒160-0003 東京都新宿区本塩町９番地３ 司法書士会館３Ｆ 連合会事務局
TEL：03-3359-4171(代表)　FAX：03-3359-4175
MAIL：postmaster@nisshiren.jp

3.2.2 日本税理士会連合会

(http://www.nichizeiren.or.jp)

(1) 設立年月日/会員規模

1957 年 設立（1942 年創立）

全国 15 税理士会

税理士会員 66,444 人

税理士法人会員 260 （2002 年 8 月末日現在）

(2) 主な活動

日本税理士会連合会は、税理士及び税理士法人の使命及び職責にかんがみ、税理士及び税理士法人の義務の遵守及び税理士業務の改善進歩に資するため、税理士会及びその会員に対する指導、連絡及び監督に関する事務を行い、並びに税理士の登録に関する事務を行うことを目的として、税理士法（昭和 26 年６月 15 日法律第 237 号）により設立された特別法人である。

税理士は、税務に関する専門家として、独立した公正な立場において、申告納税制度の理念にそって、納税義務者の信頼にこたえ、租税に関する法令に規定された納税義務の適正な実現を図ることを使命（税理士法第１条）としており、その業務として、税務代理、税務書類の作成、税務相談、会計業務、税務訴訟における補佐人業務などを行っている。

日本税理士会連合会では、e-Japan 電子政府の行政手続きにおいて国税及び地方税の申告等が果たす役割は大きく、これらへの積極的な取り組みが必要と認識しており、2003 年度から実施される電子申告・申請に備え、GPKI 接続を前提とした税理士の認証局の構築を準備中である。

(3) 連絡先

日本税理士会連合会

所在地：〒141-0032 東京都品川区大崎 1-11-8 日本税理士会館８階

TEL：03-5435-0931(代表)　FAX：03-5435-0941

MAIL：金田　kaneda@nichizeiren.jp

3.2.3 全国社会保険労務士会連合会

(http://www.shakaihokenroumushi.jp/)

(1) 設立年月日/会員規模

1978 年 12 月１日 設立

26,119 名（2002 年６月現在）

(2) 主な活動

社会保険労務士法（昭和 43 年６月３日法律第 89 号）により設立された法定団体。厚生労働省を主務省庁とする。社会保険労務士の品位を保持し、その資質の向上と業務の改善進歩を図るため、都道府県に設置されている社会保険労務士会およびその会員の指導および連絡に関する事務並びに社会保険労務士の登録に関する事務のほか、試験事務を行うことを目的とする。

社会保険労務士は、顧問となっている企業等との継続的な関係の中で、実務家とし

て、労働社会保険関係諸法令（健康保険、厚生年金、労災保険、雇用保険等）に基づく申請等の手続きを行うのみではなく、法律家として労働社会保険関係諸法令についての専門的な知識を生かし、法律問題や労務管理等の相談、指導を行っている。

2003 年 10 月から主に開始される厚生労働省での電子申請受付業務に対応して、当会では、特定認証業務および総務省ブリッジ認証局接続を前提とした認証局を構築中である。

社会保険労務士は、申請者本人証明、事業主証明、医師証明等を含んだ申請書類の処理を行っており、それらの電子化への検討は今後の大きな課題となる。

・厚生労働省電子申請システム実証実験モニター及び研究会参加（2001 年７月～2002 年３月）

・代理申請に関する制度的・技術的課題研究会参加（2001 年 10 月～2002 年３月）

・組織体制（電子化委員会、電子申請部会、電子化対策部会）」

(3) 連絡先

全国社会保険労務士会連合会

〒112-8520 東京都文京区小石川 2－22－2 和順ビル９階

TEL：03-3813-4864　FAX：03-3813-4589

MAIL：河端 祐一 kawabatayu@shakaihokenroumushi.jp

3.2.4　日本行政書士会連合会

（http://www.gyosei.or.jp）

(1) 設立年月日・会員規模

1953 年２月 22 日設立

35,850 名（2002 年７月 31 日現在）

(2) 主な活動と成果

［当連合会の概要］

行政書士は行政書士法に規定された法律関連の資格であり、官公署提出書類及び権利義務事実証明に関する書類の作成を主たる業務としている。

当連合会は行政書士法に基づいて設立された法人であり、全国 47 の都道府県行政書士会の全国組織である。行政書士の登録事務を独占的に行うほか、各行政書士会及び個々の行政書士への指導、連絡、行政書士業務に関する調査研究などを主な業務としている。

［高度情報通信社会への対応と検討］

・1996 年 8 月、企画開発部に電子商取引ワーキンググループ設置

（～1998 年 3 月）

「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」への準備と参加

・1997 年１月、高度情報通信社会対策委員会設置（～1997 年３月）
・1998 年４月、高度情報通信社会対策本部設置（～現在）
・1999 年６月、認証局運営委員会設置（～現在）

［認証局の設置］

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。

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、現在は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っている。

［報告書］

・高度情報通信社会に対応した行政書士システムの確立に向けて（1997.3）
・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（1998.5）
・高度情報通信社会と行政書士（1999.6）

(3) 連絡先

日本行政書士連合会
MAIL：安西由加利　ngr-y-anzai@staff.gyosei.or.jp
〒153-0042　東京都目黒区青葉台３丁目１番６号　行政書士会館２階
TEL：03-3476-0031　　FAX：03-3463-0507
担当役員　赤地祐一（高度情報通信社会対策本部委員、認証局運営委員会委員）
MAIL：akachi-y@gyosei.or.jp

3.2.5 電気事業連合会

（http://www.fepc.or.jp）

(1) 設立年月日／会員規模

1952 年 11 月 20 日　設立
一般電気事業者（電力会社 10 社＝北海道電力・東北電力・東京電力・中部電力・北陸電力・関西電力・中国電力・四国電力・九州電力・沖縄電力）

(2) 主な活動と成果

電力業界大の情報化の取り組みとして、従来、EDI におけるビジネスプロトコルの標準化などの課題解決に取り組んできたが、2001 年に政府 IT 戦略本部が「e-Japan2002 プログラム」を決定したのに伴い、電力業界における申請・届出等手続きのオンライン化についても推進している。

電力業界の電子申請化の状況は、経済産業省や国土交通省等への届出の一部が、2001

年度に可能となっており、今後、電力業界固有の手続きを始め、税法・保険法等一般的なものを含め、電子化される予定である。現在、電力会社８社が試行的な要素も含め電子申請を実施している。

しかしながら、業務面、システム面に於いて解決すべき課題が多いことや、手続きの中には対面での説明が必要な報告等、必ずしも電子化に馴染まないものもあることから、一律に電子化が進まないのが現状である。このため、実効性のある行政手続きの電子化を実現すべく、政府に対し、直接または日本経団連を通して、各府省の申請システムの仕様統一、代表者「社長」以外による申請を可能とする電子署名制度の整備などについて、要望しているところである。なお、日本経団連に於いては、電気事業連合会の要望を含めて「e-Japan 重点計画の見直しにあたって」と題した提言を 2002 年４月９日の IT 戦略本部に提出している。

(3) 連絡先

電気事業連合会
情報通信部　副部長　藤原　康明　fujiwary@fepc.or.jp
〒100-8118　東京都千代田区大手町１丁目９番４号　経団連会館２階
TEL：03-4535-3282(直通)　FAX：03-3230-8085

3.2.6 アイデントラス（銀行）

Identrus プロジェクト参加銀行（50 音順）
東京三菱銀行
みずほコーポレート銀行
三井住友銀行
UFJ 銀行

(1) 設立年月日／会員規模

1999 年 4 月　Identrus LLC 設立（本社米国ニューヨーク）
2002 年 6 月現在　世界の有力金融機関 61 機関が参加、内 15 金融機関が認証局開局済。日本では 1999 年４月の UFJ 銀行参加以降、みずほコーポレート銀行、東京三菱銀行、三井住友銀行が順次参加。2002 年 2 月までに、上記 4 行が全て認証局を開局。

(2) 主な活動と成果

アイデントラス電子認証スキーム（アイデントラス・スキーム）とは、『世界共通の電子認証規格』を実現するために日米欧の金融機関が設立したアイデントラス社が推進する電子認証スキームを指す。

またアイデントラスプロジェクト参加銀行の一部は、同スキーム上での決済アプリケーションを開発中（エレノア決済）。

① アイデントラス社の役割

参加金融機関共通の『運用ルール策定』

世界標準の技術に基づく『システム要件の策定』
スキーム、製品間の『整合性の監視』
参加金融機関を認証する『最上位（ルート）認証局の運営』

② 参加金融機関の役割
アイデントラス社の策定した仕様に準拠した認証局の運営
顧客企業の社員やサーバー用のデジタル証明書発行
有効性確認サービスの提供

③ 成果

A．海外
認証局共同構築：韓国（主要２行）、イタリア（同７行）、スペイン（同２行）
電子政府（BtoG）での採用：豪州、英国
BtoB への適用：リース契約書の電子化（RBOS）
金融サービスへの実装：Standard Chartered、ABN Amro
決済との連携（パイロット）：Wellsfargo、ABN Amro、Hypovereins、UFJ 銀行（以上、エレノア決済）、Nordea（その他）

B．国内
認証局構築：2002 年２月までに４大金融グループが全て認証局を開局。
普及促進：GPKI 相互接続の共同検討（アイデントラス自身がブリッジ認証局と相互認証する必要あり）

C．実用化
中小企業向けマーケット・プレース（東京三菱、UFJ）、各種業務書類の電子化（みずほコーポレート）、ファクタリング・サービスの電子化（東京三菱、みずほコーポレート）等で利用実験を実施。
三井住友銀行では、法人向けインターネット・バンキングで、みずほコーポレート銀行では、シンジケート・ローンの電子入札手続で、各々実用利用を予定。

(3) 連絡先（50 音順）

東京三菱銀行　IT 事業部　高橋
TEL：03-3240-7550
みずほコーポレート銀行　e-ビジネス業務部　佐藤
TEL：03-3215-6153
三井住友銀行　EC 業務部　鈴木淳
TEL：03-3282-8609
UFJ 銀行　決済業務部　郷田
TEL：03-5252-1311

3.3 調査研究団体における検討状況

3.3.1 電子商取引推進協議会（ECOM）：認証・公証 WG

(http://www.ecom.jp/)

(1) 設立年月日・会員規模

2000 年 4 月 協議会設立

2000 年 4 月 認証・公証 WG 設立

約 50 名参加

(2) 主な活動と成果

電子商取引推進協議会（ECOM）のミッションは、わが国における BtoB、BtoC、GtoB 等の EC 普及促進のための調査、ルール作成、標準作成、政策提言、国際協力、啓蒙活動である。その中でワーキンググループは、テーマ別に WG を設定し、会員企業から有識者を集め、報告書をまとめる活動を行っている。

認証公証 WG では、電子認証システムの普及発展のため、旧 ECOM（電子商取引実証推進協議会）時代に WG を立ち上げて以来、これまで表 3-1 に示すように「認証局運用ガイドライン」「相互認証ガイドライン」など多くの成果を発表してきた。

表 3-1 認証公証 WG 成果報告書/ガイドライン

1996～1999	2000	2001
(1)認証局運用ガイドライン (2)認証局の責任に関する提言 (3)相互認証ガイドライン (4)認証のレベルと本人確認方式に関する提言 (5)企業間電子商取引への認証技術の適用 (6)電子公証システムガイドライン	(1)電子署名利用システムの構築・利用ガイドライン (2)電子認証サービス約款作成ガイドライン (3)電子署名文書長期保存に関する中間報告	(1)電子署名プログラム Protection Profile (2)証明書利用形態に関する考察 (3)電子署名文書長期保存に関するガイドライン

① 今年度の活動

今年度は、「電子署名文書長期保存」に関する検討を継続するとともに、「証明書利用形態に関する考察」の延長上の課題として「属性認証」を取り上げ、下記の SWG 構成で検討を行っている。

② SWG1 電子認証システム仕様検討

PP 評価・認証・登録

属性認証システム仕様検討
SWG2 属性証明書利用検討
SWG3 電子署名文書長期保存
タイムスタンプ局要件検討
タイムスタンプの利用検討

(3) 連絡先

電子商取引推進協議会
〒105-0011 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
MAIL：info@ecom.jp

3.3.2 電子商取引推進協議会（ECOM）：電子政府 WG

(http://www.ecomjp/)

(1) 設立年月日/会員規模

2000 年４月 協議会設立
2000 年４月 電子政府 WG 設立
約 50 名参加

(2) 主な活動と成果

電子商取引推進協議会（ECOM）のミッションは、わが国における BtoB、BtoC、GtoB 等の EC 普及促進のための調査、ルール作成、標準作成、政策提言、国際協力、啓蒙活動である。その中でワーキンググループは、テーマ別に WG を設定し、会員企業から有識者を集め、報告書をまとめる活動を行っている。

電子政府 WG では、民間ビジネスの視点で捉えた電子政府のあり方と活用に関する調査、提言を行っている。活動テーマは、以下の３点である。

・電子政府が、民間活動にいかに寄与しえるか。
・ビジネス効果を高める上で、電子政府はどうあるべきか。
・電子政府を最大活用する上で、民間システムは如何にあるべきか。

① 今年度の活動

今年度は、電子行政アウトソーシング、電子行政ポータル、ベンチマークの３つのテーマについて、サブ WG やタスクフォースによる活動を実施している。電子行政サービスの利用者（個人、企業）は質的・量的に拡大し進展している。電子政府も利用者と同期を取り成長することが必要であり、民間の EC 適用の場を拡大する電子政府実現について提言を行っていく。

② 過去の活動成果

「電子政府の戦略的実現への提言」（2001 年度成果）
ECOM 調査レポート(1)「電子政府に関する意識調査」

ECOM 調査レポート(2)「海外における電子政府政策の状況」-在日大使館を通じて-
ECOM 調査レポート(3)「ベンチマーク報告Ⅰ」欧米編
ECOM 調査レポート(4)「ベンチマーク報告Ⅱ」アジア・オセアニア編
ECOM 調査レポート(5)「日本における電子自治体」
ECOM 調査レポート(6)「行政ポータル事例」-国内・海外-

(3) 連絡先

電子商取引推進協議会
〒105-0011 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
MAIL：info@ecom.jp

3.3.3 日本 PKI フォーラム（PKI-J）

(http://www.japanpkiforum.jp/)

(1) 設立年月日/会員規模

2000 年 12 月 設立

（注）アジア地区における国際間相互認証など、円滑な電子商取引普及のためにアジア PKI フォーラムの設立を日本が提唱。2001 年６月にアジア７カ国、地域の合意を得てアジア PKI フォーラム（会長：金井日立会長）が正式発足し、2002 年１月に日本の代表組織として、日本 PKI フォーラムと名称変更。

約 90 社・団体

(2) 主な活動と成果

アジア PKI フォーラムの日本国内での推進組織として、PKI に関する技術的・制度的課題の検討や、アジア・オセアニア各国/地域との連携・交流・情報交換を行い、PKI を利用したグローバルな電子商取引市場やシームレスなインターネットセキュリティ環境の実現を目指す。

① アジア・オセアニア各国/地域での PKI 利用状況、法制度等の調査

アジア・オセアニア各国/地域での PKI ビジネスの現状を把握するため、アジア・オセアニア各国/地域における主要ビジネス分野での PKI の利用動向および電子署名・電子認証に関わる法制度に関する調査を行った。

a) 主要ビジネス分野での PKI の活用事例の調査・研究に関して、次の項目について各国/地域の状況をヒアリング調査した。
・主要ビジネス分野での電子署名・電子認証の適用状況
・電子署名・電子認証の普及度、普及阻害要因

b) 電子署名・電子認証に関わる法制度および予想される紛争事例に関し、次の項について各国/地域の状況を調査した。
・電子署名・電子認証の法制度の整備状況、各国・地域間での違いの比較

・紛争事例調査

c) 認証局の運用方法の調査・分析

d) 韓国・シンガポールの PKI 普及度合い・利用動向の比較調査

② 国際間相互認証実証実験の実施

アジア圏の中で PKI の整備が比較的進んでいる日本、韓国、シンガポールの３カ国において、以下の各プロセスに従って実証実験を行った。

- 相互接続モデルの作成
- テスト用アプリケーションソフトウェアの開発
- 実証実験環境の構築とテスト実施
- 検証と評価

今後も実験参加国・地域の拡大、実験内容の拡充を図りながら継続してゆく。

③ アジア PKI フォーラムへの参加

2001 年６月に設立されたアジア PKI フォーラムの事務局を務めるとともに、Business case/Application WG, Legal Infrastructure WG, Interoperability WG, World wide Collaboration WG の４つのワーキンググループでの活動に参加している。

④ 国際シンポジウムの開催

以下を目的として、１回/年の頻度で国際シンポジウムを開催する。

- PKI に関する情報交換、討論を通しての有効性の啓蒙
- 技術的課題、制度的課題の討論を通しての相互運用の推進
- アジア各国の協力、連携の推進

⑤ 成果物

（全て日本 PKI フォーラムウェブサイトからダウンロード可能）

- 平成 13 年度情報化推進基盤整備（アジア電子商取引共通基盤整備事業）
- アジア各国/地域の PKI に関わる法整備およびビジネス環境の動向に関する調査報告書
- "Achieving PKI Interoperability: Results of the JKS-IWG Interoperability Project"
- Recommendations on Technical Certificate Profile
- 2001 年国際間相互認証の実証実験・開発成果報告書および実証実験報告書

(3) 連絡先

推進本部長 笹森 道夫

〒143-0016 東京都大田区大森北１丁目 23 番５号 第一小田ビル５階

TEL：03-5767-0671(代表)　FAX：03-3761-3313

MAIL：info@japanpkiforum.jp

3.3.4 電子申請推進コンソーシアム

(http://www.e-ap.gr.jp/)

(1) 設立年月日/会員規模

2000 年４月 設立

37 社

(2) 主な活動と成果

「電子申請推進コンソーシアム」は、「行政への申請・届出手続きの電子化推進」を目指す企業・団体で構成された任意団体である。

インターネットと XML を活用した、利用者（住民・企業）にとって使いやすいワンストップ、ノンストップの「窓口サービス」の実現に向け、電子フォームポータルサービスなどのサービスモデルの提案や様々な標準化活動を推進し、次の５つの委員会を設置して電子申請の普及に向け積極的な活動を行っている。

① UI（ユーザインターフェース）検討委員会

電子申請において利用者のニーズに応じて必要な申請を容易にナビゲーションし、各申請における書類作成においても必要なガイダンスが受けられる標準的な UI を検討する。2002 年には岐阜県との実証実験の成果をベースにモデル的な電子申請の UI を発表した。

② セキュリティ検討委員会

ネットワークを介した申請には“なりすまし”、電子文書には“改竄、すり替え”といった行為が、痕跡を残さず容易に行えるという問題がある。

・利用者が安心して電子申請を行えるよう、電子申請と行政側での処理をインディペンド化する施策の検討している。

・電子申請関連セキュリティ技術は細分化されその数も多いので、会員技術を中心とした電子申請に関するセキュリティ・マップの作成と、推奨システムの構築を行い発表している。

③ タグ普及委員会

１年余検討した電子申請のタグ標準化の成果を普及するための応用モデルシステム、電子申請アプリケーションのあり方を検討し、事業化可能なものはジョイント・ベンチャーの提起・調整を行うなど会員企業間事業を支援する。

④ 代理申請検討委員会

司法書士と連携して、債権譲渡、商業登記、不動産登記のオンライン申請のより利用しやすい技術的な課題などを検討し、関係する機関とともに意見を交流し、法務省などへの要望・提言や、行政書士と連携しての活動を行っている。

⑤ 実証実験委員会

電子申請は申請者、受付窓口担当者、申請技術提供者の交流によって初めて利用度の高いシステムの構築が可能である。このため、行政との連携、申請代行者との

連携、そして申請者と連携した実験をコンソーシアムは呼びかけ、実験を推進しモデルシステムを提唱していく。

岐阜県との電子申請実証実験の推進にあたっては、UI 検討委員会、セキュリティ検討委員会、タグ普及委員会、代理申請検討委員会と連携し、これら委員会の活動成果を積極的に活用していくものである。

⑥　電子申請普及に向けた取り組み

政府の申請・届出等手続のオンライン化に関する取り組みを本コンソーシアムでは設立以後、３期に分けて特徴づけて活動をしている。

第１期 会員連携による環境整備：要素技術連携のための基礎作業
（設立 2000 年４月～2001 年９月）

第２期 普及期に向けての体制整備：実証実験推進体制のための組織整備
（2001 年 10 月～2002 年３月）

第３期 各種実証実験の推進と普及の為の行政機関を交えた課題の整理
（2002 年４月～2003 年３月迄）

これ以降は第４期、第５期として、他の団体と同様の活動目的・内容・形態となる。

⑦　各種実証実験の推進と普及のための行政機関を交えた課題の整理

まず、電子申請関連技術を核としたプラットフォームの確立が最も重要であるが、岐阜県との電子申請実証実験はコンソーシアムとしてのプラットフォームに育つ可能性が十分にある。

さらに、コンソーシアムの公益性を高める事業展開として、公益的な視点での専門家としての提言の発表と、公益的な立場での関係機関・団体等とのコラボレーションに取り組んでいく。前者に関しては代理申請検討委員会において債権譲渡登記オンライン申請普及のための提言を報告書としてまとめた。

A．複数認証システム相互確認システム共同開発

電子申請に関連し、各種団体や行政機関および外国の機関などが、それぞれ異なる認証技術を利用していることが十分考えられる。そこで、コンソーシアムでは、セキュリティ検討委員会を中心に会員である認証技術主要３社の協力を得ながら、相互認証できるシステムを開発した。これは共同の常設デモコーナーを設置しており、一般の方も確認できる。

B．岐阜県行政書士会との共同実証実験

従来の申請の専門事業者である行政書士と連携して、ニーズの強い分野および電子申請によって惹起される代理申請を業務とする士業間融合問題の解決策等を検討する。

電子申請システム構築の際に大きな問題となる添付書類の問題を、専門家介在添付書類確認による専門家確認証の添付で代替するという、カナダ等で採用され

ている方式の実験等の実施。

C．業界団体と提携したワンストップ・マルチ申請システムの研究開発

例えば、ある業界団体の会員企業がチェーン展開する際、店舗の進出時に必要な各種申請（保健所、労働基準監督署、消防署、市役所等）を一括して申請できるシステムを開発し、当該業界団体とコンソーシアムによるモデル自治体での実験を検討している。これは、まず、当該業界団体の業務に対応してワンストップ・マルチ申請の会員向け電子フォームポータルサービスのシステムを構築し、これに対応できる自治体との実験を行うというもの。自治体の企業誘致の一助とするため、申請 Web 画面には対応自治体の進出優遇策の紹介なども検討している。

D．電子自治体推進地元企業提携方式の研究

電子申請、電子自治体の各種システムは、地元の地場産業・商店街振興などの地域情報化システムや、地域ポータル、NPO による福祉・教育など地域問題解決支援システムとの連携が迫られるようになる。したがって、電子申請などのシステムの開発および運用はできるだけ、地元の事情に精通した地元の情報サービス関連企業が開発することが理想的だと考え、コンソーシアムによる先進技術の地元企業への移転に関する研究を行っている。

(3) 連絡先

電子申請推進コンソーシアム
事務局長 鹿野谷武文
東京都新宿区北町６番地 神楽坂六番館 103 号 (株)デジタル経済研究所内
TEL：03-3513-5036　FAX：03-3513-5037

3.3.5 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（JNSA）

NPO Japan Network Security Association (JNSA)
(http://www.jnsa.org/)

(1) 設立年月日/会員規模

2000 年４月 任意団体 JNSA として発足（会員 54 社）
2001 年７月 特定非営利活動法人（NPO）として移行
149 社（2002 年９月現在）

(2) 主な活動と成果

JNSA の活動は、４つの部会と西日本支部の活動で構成されている。部会は、(1)技術部会、(2)政策部会、(3)マーケティング部会、(4)教育部会、であり、部会の下に 19 の WG が活動している。また、学校法人工学院大学の LINCS 研究所と共同研究を行っており、定常的な実験・評価・議論なども行っている。

① 技術部会

【セキュリティポリシーWG】

国際的な基準を意識しながら、日本の各組織や産業などに適応させた個別のテンプレート、もしくはガイドラインや考え方、基本的な作業の進め方などを議論している。2001 年度の活動成果：「情報セキュリティポリシーサンプル」

【不正アクセス調査 WG】

不正アクセス攻撃技術に関して実地検証を元に調査研究し、そのメカニズムを説明できるような資料を作成公開することを目標としている。

【コンテントセキュリティ WG】

コンテント自身が製作者、著作者の意図に反した用いられ方、取得のされ方が行われる場合がある。コンテントセキュリティのあるべき姿を模索する。

【セキュリティ評価 WG】

中立的な立場で業界標準となるセキュリティ評価基準の策定を目的とする。

【相互接続 WG】

2001 年度までは IPsec の相互接続性の実証実験を行い、IPA からも結果を情報公開している。2002 年度は企業においても普及の始まっているワイヤレス LAN 環境について、セキュリティ機構についての接続性などに関する勉強会、実験 評価を行う。

【技術用語 WG】

・セキュリティに関する用語の定義の認識の違いにより、情報に誤解を生む可能性があり、用語の定義と解説を作成し、かつ、英訳語集も作成する。

【IRT（Incident Response Team）調査研究 WG】

既存情報セキュリティ対応組織・活動についての調査、脆弱性データベースなど IRT 等に必要な技術要素の調査を行い、JNSA としてどのような緊急対応活動が行えるかを検討し、可能性をまとめる。

【次世代 IDS（Intrusion Detection System）-WG】（仮称）

IDS 似た目的を持つ Honeypot に関する位置付け、役割、技術、運用方法などについて調査する。

【インターネット VPN-WG】

VPN が使用可能な、いわゆる Hotspot/ISP を調査し、VPN を利用するための必要条件をまとめるとともに、現状での問題等を整理する。

【不正プログラム調査 WG】

トロイの木馬、スパイウェア、リモートアクセスツールなど、様々な不正プログラムを分類し、その利用目的を明らかにし、合わせて具体的な対策方法も示して、この種の技術に関する正しい知識を広めていく。

【情報セキュリティ標準調査 WG】

認定制度そのものに焦点を置いた調査を目的とした WG である。調査対象は、ISO15408，17799，ISMS，SSE-CMM 他である。

【PKI 相互運用技術 WG】（Challenge PKI 2001）

今年度も昨年に引き続き IPA からの委託（「電子政府情報セキュリティ相互運用支援技術の開発」）を受けた。PKI を現実に動かす際の相互運用性の問題点などを検証し、下記のような内容を開発作成するプロジェクトと、これらの経過を解説し議論する WG とからなる。

(1) PKI 相互運用テストスイートの開発（サンプル実装の開発を含む）

(2) GPKI のテストケースの設計

(3) GPKI 実装ガイドライン

(4) GPKI 総合運用実証実験

また、2002 年７月の横浜 IETF の PKIX-WG のセッションで、昨年の Challenge PKI 2001 での成果を発表した。

② 政策部会

【セキュリティ被害調査 WG（情報セキュリティインシデント調査プロジェクト）】

昨年度は、企業に対し、アンケート及びヒアリングによって情報セキュリティ対策の取り組み状況と発生した被害の費用を調査した。（調査報告書は、IPA よりに公開されている。）今年度は、昨年作成した被害や対策費用の算出モデルの精緻化を行うと共に、対策と被害発生の相関についても調査していく。

【セキュリティベンダーとしての管理基準策定 WG】

IT セキュリティ業界の健全な発展、並びに JNSA 所属企業の一般顧客や関連省庁への信頼性向上のため、ベンダーとしての管理基準案及び運用案を取りまとめ「JNSA 行動指針（案）」を 2001 年度に策定した。現実的な運用案を取りまとめることが今年度の課題となっている。

【個人情報保護ガイドライン作成 WG】

個人情報保護が法制化されるにあたり、個人情報保護自体に対する考え方を整理したガイドラインを作成し、企業の個人情報の取扱いに関する意識向上、各種セキュリティ対策の実施を促していくことを目的としている。

【成果物取扱規程 WG】

JNSA 成果物の公開ポリシーについての JNSA としてのガイドラインを作成し、権利関係や２次利用などについての、包括的なルールを定めることを目的としている。

【セキュリティ監査 WG】

総務省、経済産業省（「情報セキュリティ監査研究会」）などが検討している、地方自治体関係のセキュリティ監査の検討に呼応し、地方自治体向けセキュリティ監査基準の策定を行うための基礎的な議論を行い、考え方や内容についての啓発セミナーを全国主要都市で開催することなどを目標としている。

③ マーケティング部会

主な活動内容は、「Network Security Forum 2002」の開催、JNSA セキュリティセミナーの開催、会報「JNSA Press」の発行（年３回）、などであるが、2002 年度は

啓発ビデオを作製する。

【CD-ROM 作成 WG】

セキュリティ啓発活動の一環として、ドラマ仕立てのセキュリティ啓発 CD-ROM を作成する。CD-ROM は、2002 年中には完成、配布予定である。

④　教育部会

ネットワークセキュリティ技術者の育成のために、産学協同プロジェクトを進め、大学や企業で行うべき教育のカリキュラムの検討やユーザ教育の在り方についての調査・検討などを行う。

【スキルマップ作成 WG】

IPA から委託された「情報セキュリティプロフェッショナル育成に関する調査研究」を行う。実施は NRA（ネットワークリスクマネージメント協会）と共同で行う。

⑤　西日本支部

主な活動予定は下記の通り。

- ユーザと一体となったビジネスに繋がるサロン風の啓発活動による西日本の活性化
- 電子自治体の情報セキュリティ対策支援 WG によるコンサル活動等

(3) 連絡先

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

事務局長　下村 正洋　（株式会社ディアイティ）

事務局

〒136-8741

東京都江東区新砂 1-6-35 N ビル東陽町（株）ディアイティ内

TEL：03-5633-6061　　FAX：03-5633-6062

MAIL：sec@jnsa.org　　http://www.jnsa.org/

西日本支部

〒530-0047

大阪市北区西天満 2-3-14　西宝天満ビル４階（株）ヒューコム内

TEL：06-6362-2666

3.3.6 社団法人日本ネットワークインフォメーションセンター (http://www.nic.ad.jp/)

(1) 設立年月日/会員規模

1997 年３月 設立

366 会員（2002 年７月末現在）

(2) 主な活動と成果

2002 年度下半期より、IP アドレスあるいはドメイン名を対象とする認証サービスの

調査・研究を開始する予定だが、詳細は未定。

電子認証・電子署名等の分野における主たる活動実績はない。

(3) 連絡先

社団法人日本ネットワークインフォメーションセンター
インターネット推進部企画課 伊勢禎和 yise@nic.ad.jp
〒101-0047 東京都千代田区内神田２丁目３番４号 国際興業神田ビル６階
TEL：03-5297-2311　FAX：03-5297-2312

3.3.7 財団法人医療情報システム開発センター（MEDIS-DC）

The Medical Information System Development Center
(http://www.medis.or.jp)

(1) 設立年月日

1974 年７月

(2) 主な活動と成果

① 事業内容

本財団は、医療情報システムに関する基本的かつ総合的な調査、研究、開発および実験を行うとともに、これらの成果の普及および要員の教育研修等を行うことにより、医学、医術の進展に即応した国民医療の確保に資し、もって国民福祉の向上と情報化社会の形成に寄与することを目的としており、次の事業を行っている。

- 医療情報システムに関する基本的かつ総合的な調査、研究、開発および実験
- 医療情報システムに関する安全性および信頼性の研究
- 医療情報システムの開発成果の普及促進
- 医療情報システムに関する教育、研修および啓蒙
- 医療情報システムに関する資料その他の情報の収集および提供
- 医療情報の収集および提供
- 医療情報システムの研究開発に関する国際協力

前各号の事業の実施に伴う内外関係機関との提携および交流

これらの事業の実施に当たっては、厚生労働省、経済産業省と密接な連携を保ちつつ、コンピュータ関連企業、医療関係者、医学系および工学系研究者等の幅広い参加の下に、各種調査研究事業等を推進していくこととしている。

② 最近の事業内容

A．標準化推進事業（情報に関連した標準の開発と普及）

- 標準病名マスターの開発と提供
- 手術コードの開発と提供
- 薬剤コードの開発
- 電子カルテ用標準的データ項目セットの開発と提供

- 医療材料コードの開発
- 国際規格化への対応
- 部門間情報の標準的情報交換の実装実験
- 小規模診療施設用電子保存医療材料物流システム設備整備事業

B．基盤技術の研究・開発（情報技術を利用するための基盤技術）

- 情報交換のためのセキュリティ技術（暗号化と認証）
- 情報保存のためのセキュリティ技術（電子署名と原本性保証）
- 医療・保健・介護分野の IC カード利用技術

C．情報システムの開発・運用

- 地域医療保健計画
- 結核・感染症発生動向調査
- 医療機関行政情報
- 要介護認定情報管理
- 急性期入院医療における包括的支払方式の調査
- 院内感染対策サーベイランス

D．介護情報システムの基盤技術の開発と普及

E．コンサルテーション

F．教育・研修

③　PKI 推進状況

平成 13 年度は「先進的 IT 活用のネットワーク推進事業」として、26 地域において地域内の医療機関等が保有している診療録等を共通利用するネットワークシステムの開発・実験をおこなった。この中で、幾つかの CA 局を利用した地域があり、この中より、５地域を選択し、異なる CA 局に属する施設間で署名付紹介状を交換し、MEDIS-DC に仮のルート CA 局を立て、異なる CA ベンダー間の証明書および署名の運用互換性を検証した。

これと平行して、「保健医療福祉 PKI 研究会」を開催し、医療用の PKI 規格である ISO/TS17090 に従った「実証試験用医療用公開鍵基盤ガイドライン」および、その付属文書として、「実証試験用ヘルスケア PKI 認証局証明書ポリシー」を作成した。

平成 14 年度は、このガイドラインを実証し、ヘルスケア PKI の具体例を提供する為に、「保健医療福祉情報セキュリティ推進事業」を実施する。具体的には、認証センターが運営責任を持つ、ルート CA 局を上位とし、その下に CA 局全体を自地域におく場合と、RA（Registration Authority）のみを自地域におき、認証センターの IA（Issuing Authority）を共有する場合が混合したモデルを幾つかの地域の参加を得て、実運用に近い形で構築・運用し、今後の保健医療福祉 PKI 構築の検討に供する予定である。

(3) 連絡先

〒107-0052 東京都港区赤坂 2-3-4 ランディック赤坂ビル 10 階

TEL：03-3586-6321 FAX：03-3505-1996

MAIL：sysad@medis.or.jp

3.3.8 財団法人日本建設情報総合センター（JACIC）

(http://www.jacic.or.jp)

(1) 設立年月日

1985 年 11 月

(2) 電子入札に関する主な活動と成果

① 電子入札コアシステムの開発

複数の公共発注機関がバラバラに電子入札システムを構築すると、受注企業にとって、個々の発注機関毎に異なった対応を強いられる結果になるばかりか、国全体として見た場合に開発コストのムダが生じるため、これを解決する方法として、共通に利用可能な汎用性の高い部分をコアとして整理し、電子入札コアシステムとして開発を実施中である。

開発に際しては、仕様および提供条件等について検討することを目的として、(財)港湾空港建設技術サービスセンターとともに、電子入札コアシステム開発コンソーシアムを設立した。

② コアシステムへ適用する認証局体系の検討

コアシステムの開発趣旨に合致した認証のあり方を実現するには、複数の認証局対複数の入札システム（発注機関）が相互に共通的に適用できる認証の仕組みを構築する必要があり、これを実現するための枠組みを検討した。

検討結果を元に認証局に共通的に求める仕様を公開し、この仕様に則って運営する認証局の公募を実施した。

募集の前提として、各認証局は

・電子署名法による特定認証業務の認定取得

・GPKI のブリッジ認証局との接続

を満たす必要があることとした。

このイメージが実現すると、入札に参加する各企業は、いずれかの１つの認証局から取得した電子証明書があれば、コアシステムを導入した発注機関に対してアクセス可能となる。

③ マルチトラスト方式に関する検討

前述の方法の実現にあたり、GPKI または LGPKI に対応が実現していない時期の自治体等に対する過渡的な認証方法として、認証局間で相互に認証をする方法の 1 つとしてマルチトラスト方式を検討し、公募仕様に盛り込んだ。

④　成果物

電子入札コアシステム ver.1 をリリース（2002 年７月）

ver.2 をリリース予定（2002 年 10 月）

以降のバージョンを継続開発中

(3) 連絡先

財団法人日本建設情報総合センター CALS/EC 部

研究員 川崎 康

〒107-8416 東京都港区赤坂７丁目 10 番 20 号

アカサカセブンスアヴェニュービル５階

TEL：03-3505-0436（直通）　FAX：03-3505-8983

3.3.9 財団法人情報処理相互運用技術協会（INTAP）

(http://www.intap.or.jp/)

(1) 設立年月日/会員規模

1985 年 12 月 18 日

会員　19 社

(2) 主な活動と成果

(2.1)事業内容

次世代のコンピュータネットワーク情報基盤の確立を目指して、情報処理システムの相互運用技術に関する研究開発、調査研究、国際交流、試験検証およびこれらの成果に関する普及啓発等の活動を、インターネット分野の技術を核に推進しています。

①　研究開発事業

デジタル経済社会に向けた企業システム間の連携を可能とする技術基盤の確立のために、次の研究開発事業を行っています。

◆インターネット利用技術

◆次世代 Web コンピューティング技術

◆電子文書の交換／管理技術

◆システム運用管理の相互運用性技術

②　調査研究事業

次世代ネットワークシステム技術に関する調査研究として、複数ドメインにまたがる企業システム間の相互運用性確保の視点から次の調査研究を行っています。

◆コンテンツ配信技術

◆iDC の相互運用性・安全性技術

◆ユビキタスネットワーキング利用技術

◆オープン分散処理システムのモデリング技術

③　国際交流事業

インターネット関連の研究開発および標準化推進を目的として、次の国際交流事業を行っています。

◆インターネット技術の標準化

◆セマンティック Web、XML 暗号化等の標準化

◆システム運用管理技術

④　試験検証事業

運用管理システムおよび各種の標準仕様準拠についての相互運用性に関し、次の試験検証関連事業を行っています。

◆運用管理システムの相互接続試験

◆非 PC 系デジタル機器の相互接続試験

・情報家電等非 PC 系デジタル機器の相互接続試験

・標準仕様準拠に関する検証試験

⑤　普及啓発事業

これらの諸活動を支援するために、次の普及啓発活動を行っています。

◆シンポジウム、セミナーの開催

◆インターネット分野の最新技術に関する情報発信

(2.2)PKI、セキュリティ関連活動

①　非 PC 系デジタル機器のセキュリティ仕様策定と Plug&Play 機能の検証ソフトウェアの研究開発、非 PC 系デジタル機器がインターネット接続されて利用される場合のセキュリティモデルを検討し、その実現に必要な仕様策定とその標準化及び、検証ソフトウェア研究を行った。（平成 14 年度）

②　XML 暗号 API 仕様の策定

W3C で標準化された XML 暗号規格に基づいて XML 暗号 API 仕様に関する研究を行った。（平成 13 年度）

③　XML 電子署名 API 仕様の策定

IETF と W3C で共同して標準化が進んでいる XML 電子署名フォーマットに基づいて、XML 電子署名 API 仕様に関する研究を行った。（平成 13 年度）

(3) 連絡先

財団法人　情報処理相互運用技術協会（INTAP）

〒113-6591　東京都文京区本駒込二丁目 28 番 8 号

文京グリーンコート　センターオフィス 13 階

TEL：03-5977-1301　　FAX：03-5977-1302

MAIL： kambara@intap.or.jp（神原顕文）

3.3.10 社団法人日本防犯設備協会

（http://www.ssaj.or.jp）

(1) 設立年月日/会員規模

1986 年 4 月 30 日

259 社・団体（2003 年 2 月現在）

内訳　正 会 員：102 社

準 会 員：153 社

賛助会員：　9 社

特別会員：　5 団体

(2) 主な活動と成果

日本防犯設備協会は、防犯機器の性能や設置に関する調査研究を通じ、良質で、安価な防犯設備の普及を目的に昭和 61 年に設立された。以来、各種の委員会を組織し、防犯設備、システムの調査研究を継続的に行い、その性能や設置の基準についての基準や標準規格を定め、それらの成果を報告書・ガイドブックになどにまとめて、啓発活動を推進している。

平成８年には、インターネットの普及に伴い、情報セキュリティの重要性が認識されるようになり、情報セキュリティ調査特別委員会が設置され、この分野の調査研究への取り組みを開始した。平成 10 年からは常設の委員会とし継続的に活動を行い、調査研究報告書の発行、不正アクセス行為対策等の実態調査や技術開発状況の調査及び啓発用ビデオの作成、ガイドブックの発行などを行って来ている。

現在までのところ、PKI を対象とした特段の活動はしていないが、これからの防犯設備、システムなどを検討するにあたって PKI の必要性、重要性を認識しており、具体的な取り組みへの検討を予定している。

また、平成４年からは防犯設備士養成講習・資格認定試験を実施し、現在では７千有余の防犯設備士が全国各地で防犯機器の施工や防犯診断などの分野で活躍している。

(3) 連絡先

社団法人 日本防犯設備協会

〒105-0013　東京都港区浜松町 1-12-4 第２長谷川ビル ４階

TEL:03-3431-7301　FAX:03-3431-7304　事務局　竹内　克彦

MAIL: takeuchi@ssaj.or.jp

3.3.11　東日本電子認証普及促進協議会

（http://www.pref.miyagi.jp/jyoho/mmc/epki/）

(1) 設立年月日/会員規模

2002 年 12 月 20 日

民間企業，国，北海道・東北６県，広域経済団体など 54 企業・団体（2003 年１月末現在）

(2) 主な活動と成果

電子商取引や電子自治体システム等における電子認証活用モデルについての調査・研究、電子認証の重要性やその活用についての普及啓発などの取組を進め，東日本における産業経済及び地域社会の活性化に寄与することを目的とする。

① 電子認証の普及・啓発

電子認証に関するセミナー等の開催，各種団体や自治体等へ訪問活動などを実施し，Ｅビジネス・電子自治体における電子認証技術の必要性や安全性などについての周知と利用の促進を図る。

② 電子認証活用モデルの調査・研究

電子認証を活用しようとする者，電子認証サービスを提供しようとする者及び各種のアプリケーションを提供しようとする者等の連携・協調によって，業務や取引などにおける電子認証活用モデルの調査・研究を進める。

③ 他地域との連携

東北地域内での連携を強化するとともに，他地域とも協調し，認証基盤やサービスコンテンツ（認証アプリケーション）の共同整備・共同利用などに取組み，地域連携による相乗効果の発現を図る。

(3) 連絡先

東日本電子認証普及促進協議会事務局（宮城県企画部情報政策課内）

〒980-8570 宮城県仙台市青葉区本町 3-8-1

TEL：022-211-2472　FAX：022-211-2495

MAIL：epki@pref.miyagi.jp

3.3.12 電子商取引安全技術研究組合（ECSEC）

(http://www.ecsec.org/)

(1) 設立年月日/会員規模：

2000 年２月 28 日設立　現構成員 49 組合員

(2) 主な活動と成果：

情報セキュリティ分野における日本の動きは、欧米に比べ大きく水を開けられ、国内のみの視点から国際的視点で積極的に取組む必要がある。これまでの我が国の製品品質の良さに加え、製品並びにシステムのセキュリティを併せ持つことにより、製品の付加価値増大に結びつく。特に、情報セキュリティについては製品提供者側のみではなく、製品を受け入れ運用する側もこのルールを充分に理解し活用することで、一層セキュアな環境を作り出すことができる。 その意味からも、情報セキュリティは一部の立場のものが対応・対処するのではなく、IT に関与する、すべてのプレーヤが関連するものであり、全関係者は情報セキュリティ保護と評価のスキームを充分に理解する必要がある。

この意向の基、平成 12 年２月通商産業省鉱工業技術研究組合法に基づき、メーカ・ユーザ・システムインテグレータ等 34 社が参加し、電子商取引安全技術研究組合 ECSEC を設立した。設立目的は、組合員共同による電子商取引に関する情報技術を用いた製品・システムのセキュリティに関する試験研究、並びに組合員の技術向上を図るための事業を行うこと。この試験研究のベース・ルールが、JIS X 5070（ISO/IEC 15408）情報技術セキュリティ評価基準である。 現在当組合は 49 社の参加をいただき、次の活動を行っている。

・Creator of PP：電子商取引と IC カードのセキュリティ分野での PP 作成（要求仕様）
・Developer of Implementation technology：セキュリティ実装技術の結集
・Instructor of ST creation technology：ST への理解と作成技術の指導普及（基本設計）
・Evaluator ：JIS X 5070 準拠の各種評価

また、電子政府関連の情報セキュリティに対しても積極的に取組み、安全に安心して利用できる製品・システム構築に寄与すべく行動している。その結果、平成 14 年 12 月 20 日 日本で初めて当組合 ECSEC 研究所が評価機関認定を拝受した。

今後、電子政府/自治体・電子商取引等の分野を中心に、セキュリティに関するコンサルティング並びにセキュリティ評価等を基軸に継続して活動して行く。

(3) 連絡先

電子商取引安全技術研究組合：
〒104-0061　東京都中央区銀座 5-5-12　文藝春秋銀座別館５階
TEL：03-3569-0610　　FAX：03-3569-0606
Mail：office@ecsec.org

3.3.13　日本銀行金融研究所（IMES）ISO/TC68 国内委員会

（http://www.imes.boj.or.jp/）

(1) 設立年月日/会員規模：

(2) 主な活動と成果

ISO/TC68（「銀行業務、証券業務およびその他金融サービス（Banking, Securities and Related Financial Services）」を対象とする専門委員会）および SC2、SC6 の国内検討委員会事務局を日本銀行で担当し、ISO/TC68、国際標準に係る国内意見のとりまとめを行う。関連の情報を金融研究所ホームページで公開。金融の観点から、法律・会計制度・情報技術に関する研究を実施。

① 報告書の一部紹介

・「電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価」
（平成 13 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2001/kk20-b1-4.pdf

・「情報セキュリティ技術の信頼性を確保するために」（平成 13 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2001/kk20-2-2.pdf
・「情報セキュリティ技術の評価と信頼性」（平成 13 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2001/kk20-2-1.pdf
・「金融分野における情報セキュリティ管理の国際標準化動向」（平成 13 年２月）
http://www.imes.boj.or.jp/japanese/kouen/ko0102.html
・「金融業務と認証技術：インターネット金融取引の安全性に関する一考察」
（平成 12 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2000/kk19-b1-1.pdf
・「最近のデジタル署名における理論研究動向について」（平成 12 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2000/kk19-b1-3.pdf
・「デジタルタイムスタンプ技術の現状と課題」（平成 12 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2000/kk19-b1-4.pdf
・「金融業界における PKI・電子認証について―技術面、標準化に関する最近の動向を中心に」（平成 12 年４月）
http://www.imes.boj.or.jp/japanese/kinyu/2000/kk19-b1-2.pdf

(3) 連絡先

日本銀行金融研究所（IMES）ISO/TC68 国内委員会　事務局
〒103-8660 東京都中央区日本橋本石町 2-1-1
TEL：03-3279-1111　FAX：03-3510-1265

3.4 普及啓発を行っている団体

3.4.1 財団法人日本品質保証機構（JQA）電子署名・認証調査センター (http://jqa.jp/index2.html/)

(1) 設立年月日/会員規模

2001 年 3 月末設立

(2) 主な活動と成果

① 普及・啓発活動

ネットワーク環境が進む中、国民生活において電子署名の円滑な利用を促進するため「電子署名・認証ハンドブック」ビジネスユース編、パーソナルユース編の各小冊子を作成し一般に配布すると共に、PDF 形式にてホームページ上に公開している。また、全国各地においてセミナーを開催し、講演等による普及・啓発を行い、認証事業者へは、特定認証業務の認定基準について、設備、利用者の真偽の確認方法、業務の方法の適合性について普及活動をする。海外に対しては、電子署名・認証の国際間の相互承認に向けた活動を推進する。

② 調査研究の活動

諸外国の認定基準、制度、PKI 技術等の調査を行い、国際的な法的、制度的、技術的な状況に置けるわが国の位置付けについて評価するとともに、技術基準および標準化の最新動向の把握に努める。

③ 指定調査機関としての活動

財団法人日本品質保証機構は、電子署名法第 17 条第一項に基づき、特定認証業務の認定を申請した事業者に対して調査を行う「指定調査機関」として 2001 年 3 月 30 日、指定を受けた。指定調査機関とは、主務大臣の指定を受けて、主務大臣に代わって当該調査の全部もしくは一部を行う機関である。

・特定認証業務に係る認定の調査

調査申請書類の提出を受けて手続要件および内容要件の適合性を規則、指針、方針、適合例をもとに実地調査を行う。実地調査においては、特定認証業務における設備、システムおよび業務の運用状況の調査を行う。

実地調査の調査結果は、報告書として主務大臣に提出する。

(3) 連絡先

電子署名・認証調査センター

〒107-0052 東京都港区赤坂 1-9-15 自転車会館２号館４階

TEL：03-3583-9020 FAX：03-3583-9199

MAIL: info-esaec@jqa.jp

3.4.2 特定非営利活動法人電子認証局市民ネットワーク福岡 (CACAnet Fukuoka)

(http://www.cacanet.org/)

(1) 設立年月日/会員規模

1999 年９月 設立

2000 年９月 特定非営利活動法人の認証を取得

約 50 名参加

(2) 主な活動と成果

CACAnet Fukuoka は、PKI の普及を目的とした NPO である。CACAnet Fukuoka には、コミュニティスクールとコミュニティ CA という２つの顔がある。会員は合宿などの形で、電子認証システムのシステム構築や CPS の作成などの作業や議論を行っている。また、電子地域通貨システム Travecoup の開発と運用など、市民が PKI を日常的に利用し、楽しく親しむための応用サービスも行っている。

① コミュニティスクールとしての活動

CACAnet Fukuoka は、電子認証/電子署名に関連した知識や情報の提供を目的とするコミュニティスクール「CACAnet フリースクール」を主催している。CACAnet フリ

ースクールには、研究会と講習会があり、研究会は、PKIX 関連の RFC の輪講、電子認証署名法関連のパブリックコメントの作成、証明書発行システムの仕様検討などのテーマについて密度の濃い学習や議論をする場になっている。講習会は、多くの方を集めた集合教育として、インターネットを活用した安全な SOHO ビジネスのやり方や PKI 関連ツールの使用法の紹介などを行っている。

CACAnet フリースクールは、2002 年から東京でも開催するようになり、研究会は隔週の月曜に開催している。研究会や講習会の資料はインターネットで公開し、PKI に関連したインターネットセキュリティの情報の普及に貢献している。

② 電子認証機関としての活動

CACAnet Fukuoka には、多くの市民が低コストでカジュアルに PKI を利用できるようにすることを目的とした、コミュニティ CA としてのサービスを行おうとしている。すでに認証システムの構築および CPS の作成が完了し、市民が気軽に利用できる教育、介護、医療、ビジネス、行政サービスなどへ利用できるように環境の整備を行っている。

③ 成果物

- 証明書発行公開デモ（2000 年３月）
- 講習会「インターネットと電子認証」（2000 年６月）
- 講習会「インターネットによる SOHO 実践セミナー」（2000 年 10 月）
- インターネットフェスタ 2001 にてインターネットの盗聴公開デモ（2000 年 12 月）
- イムズ『e-生活のススメ』にてインターネットの盗聴公開デモ（2001 年５月）
- 情報処理学会全国大会にて「NPO による地域コミュニティを対象としたセキュリティ教育」を発表し奨励賞を得る（2001 年９月）
- 講習会「実習 電子認証システム入門」（2002 年５月）
- 講習会「電子認証 ? 電子認証実験に向けて? 」（2002 年５月）
- 他、研究会多数

(3) 連絡先

特定非営利活動法人 電子認証局市民ネットワーク福岡
理事長 山崎 重一郎
〒810-0004 福岡県福岡市中央区渡辺通 2-1-10 株式会社九州ビジネス気付
TEL：092-712-7003
MAIL:tonton@cacanet.org3

編集メンバー

前田　陽二	電子商取引推進協議会
松山　博美	電子商取引推進協議会
川松　和成	電子商取引推進協議会
小祝　香織	電子商取引推進協議会
中川　宏之	日本 PKI フォーラム
木村　吉博	経済産業省　リサーチャー

電子署名・認証利用パートナーシップ
報告書 2002
平成 15 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。）　14-E007