15－E007

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

―国内のPKI推進状況―

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、国内の PKI 推進活動の状況を著したもので、電子政府の構築状況、民間での利用状況、国際的な活用の動き、及び国内の電子署名認証推進・活用団体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	新日本監査法人
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、国内における電子署名･認証の推進状況や利用状況をまとめたもので、運営委員・オブザーバのほかこの分野に関係する団体にも執筆していただいている。

第 1 章では、政府における PKI 利用に関する推進体制や推進状況を紹介する。

第 2 章では、民間における具体的な利用について事例を紹介する。

第 3 章では、PKI を国際的に利用する動きについて紹介する。

第 4 章では、国内の電子署名・認証の利用及び推進に係わる団体の紹介を行っている。

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．電子政府

1.1　電子政府推進体制

［http://www.kantei.go.jp/jp/singi/it2/cio/dai1/1gijisidai.html などより引用］

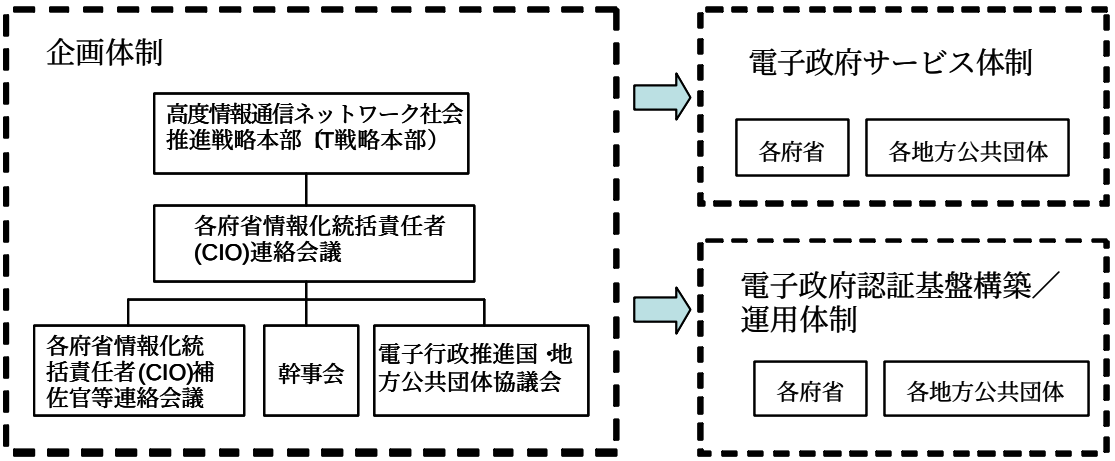


図 1-1 電子政府推進体制（JESAP 事務局作成）

（1）．高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）

メンバーは、内閣総理大臣を本部長、IT 担当大臣・内閣官房長官・総務大臣・経済産業大臣を副本部長とする他、それ以外の全ての国務大臣を本部員とする。民間有識者が本部員として参加。

（2）．各府省情報化統括責任者（CIO）連絡会議

・行政情報化に係る共通課題に対する基本方針等の検討、決定（業務改革、各府省情報化推進計画の策定等）
・各府省の情報化の進捗状況の把握・評価、総合調整
・各府省の情報化のうち、重要な事項の情報共有（先行事例の報告）
・e-Japan 重点計画に盛り込むべき課題の抽出

連絡会議の議長は内閣官房副長官補が、また、副議長は総務省行政管理局長が務める。連絡会議には各府省の CIO が参加するほか、オブザーバーとして、衆議院、参議院、最高裁、会計検査院、日銀などからも担当者が参加する。

（3）．各府省情報化統括責任者（CIO）補佐官等連絡会議

府省内の業務・システムの分析・評価、最適化計画の策定にあたり CIO 及び各所管部門の長（業務改革関係部門、情報システム統括部門）に対する支援・助言を行う CIO 補佐官を配置する。

（４）．幹事会

特定な事項について、専門的な検討を行う。

（５）．電子行政推進国・地方公共団体協議会

① 霞ヶ関 WAN と総合行政ネットワーク（LGWAN）を利用した情報の交換,及び共有の在り方
② 行政ポータルの連携の在り方
③ ①と②に関わるセキュリティ確保のあり方
④ IT を活用した業務改革に係わる相互の情報提供
⑤ その他国・地方公共団体が総合的・一体的に取り込むことが必要と認められる事項

1.2 中央政府における計画とその進捗状況

1.2.1 政府認証基盤（GPKI）の整備

(1) 電子政府と GPKI（Government Public Key Infrastructure）

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 の整備経緯

国の行政機関においては、政府全体として、整合性をもって総合的に GPKI の整備について、次のとおり取り組んできている。

- 1999 年（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 2003 年度（平成 15 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、2000 年（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。
- 2002 年（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、2002 年度（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、全府省において認証局が整備、運用が開始された。

(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、申請・届出等手続を行う国民等利用者側や地方公共団体における認証局の整備も進められた。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、地方公共団体の職責を認証する LGPKI（Local Government Public Key Infrastructure）が構築され、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る。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ことに留意することが必要である。

商業登記認証局については、2000 年度（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、2001 年度（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おり、2004 年（平成 16 年）１月現在で 14 認証局と相互認証を行っている。

地方公共団体による認証局については、LGPKI が 2003 年（平成 15 年）12 月に、住民を認証する公的個人認証サービスに基づく認証局は、2004 年（平成 16 年）１月に、それぞれ相互認証を完了している。

(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。

ブリッジ認証局の相互認証のための基準として、府省認証局等との間、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。府省認証局等については、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 Policy / Certification Practice Statement）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

国の行政機関等への電子申請や電子入札を目的として、今後においても民間認証局等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。

1.2.2 電子署名法に基づく認証業務

「電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）」（以下、「電子署名法」という。）は、電子署名及び認証業務について、法的な位置付けを明確にし、ネットワークを利用した社会経済活動の一層の推進を図り、国民生活の向上と国民経済の健全な発展に寄与することを目的として、平成 13 年 4 月 1 日に施行された。

電子署名法では、以下の３つの認証業務が定義されている。

「認証業務」：利用者が電子署名を行ったものである事を確認するために用いられる事項が、当該利用者に係るものであることを証明する業務。

「特定認証業務」：電子署名のうち、その方式に応じて本人だけが行うことができるものとして主

務省令で定める基準に適合するものについて行われる「認証業務」。

主務省令では、“その方式に応じて本人だけが行うことができるもの”として、一定の技術的信頼性を有する方式が規定されている。

「認定認証業務」：第４条で「特定認証業務」が認定を受けることができることとし、第６条で認定の基準が規定されている。

認定を受けるかどうかは、認証事業者の任意であるが、認定を受けた特定認証業務は、一定レベルの信頼性を有するものとして、利用者の目安となるものである。

認定の具体的基準は、主務省令で規定されており、以下の３つの内容で構成されている。

（１）特定認証業務の用に供する設備の基準

認証業務の安全性、信頼性を確保するために、特定認証業務を行おうとする者が採用する設備、装置等に関する規定

（２）利用者の真偽の確認基準

電子証明書を受け取った者への信頼性確保のために、特定認証業務を行おうとする者が、利用者の真偽を確認する方法に関する規定

（３）特定認証業務の管理・運用基準

電子証明書の発行及び利用に係る信頼性を確保するために、特定認証業務を行おうとする者が採用すべき認証業務手続きに関する規定

上記のすべての基準に適合するか調査を受けて認定され、または、１年毎に基準に適合しているか調査を受けて更新認定されて、平成 16 年３月現在サービスを行っている「認定認証業務」は、次の 20 業務である。

電子署名及び認証業務に関する法律に基づく認定認証業務一覧　（平成16年 3月26日現在）

特定認証業務の名称	業務を行う者の名称	認 定 日	認定の有効期限
Accredited Sign パブリックサービス	日本認証サービス株式会社	平成13年 7月13日	平成16年 7月12日
Accredited Sign パブリックサービス2	日本認証サービス株式会社	平成13年10月19日	平成16年10月18日
株式会社日本電子公証機構認証サービスiPROVE	株式会社日本電子公証機構	平成13年12月14日	平成16年12月13日
CECSIGN認証サービス	株式会社コンストラクション・イーシー・ドットコム	平成14年 3月26日	平成17年 3月25日
セコムパスポート for G－ID	セコムトラストネット株式会社	平成14年 7月 4日	平成16年 7月 3日
AOSignサービス	日本電子認証株式会社	平成14年 8月29日	平成16年 8月28日
e-Probatio PS サービス	エヌ・ティ・ティ・メディアサプライ株式会社	平成14年11月20日	平成16年11月19日
TOiNX電子入札対応認証サービス	東北インフォメーション・システムズ株式会社	平成14年12月10日	平成16年12月 9日
CWJ電子入札対応認証サービス	株式会社サイバーウェイブジャパン	平成15年 1月10日	平成17年 1月 9日
TDB電子認証サービスTypeA	株式会社帝国データバンク	平成15年 2月 5日	平成17年 2月 4日
ビジネス認証サービスタイプ1	日本商工会議所	平成15年 3月12日	平成17年 3月11日
電子入札コアシステム用電子認証サービス	ジャパンネット株式会社	平成15年 4月21日	平成16年 4月20日
信金中央金庫 電子認証サービス	信金中央金庫	平成15年 5月26日	平成16年 5月25日
全国社会保険労務士会連合会認証サービス	全国社会保険労務士会連合会	平成15年 6月10日	平成16年 6月 9日
CTI電子入札・申請届出対応 電子認証サービス	株式会社中電シーティーアイ	平成15年 9月29日	平成16年 9月28日
よんでん電子入札対応認証サービス	四国電力株式会社	平成15年10月 2日	平成16年10月 1日
Accredited Sign パブリックサービス1	日本認証サービス株式会社	平成15年11月 7日	平成16年11月 6日
MJS電子証明書発行サービス	株式会社ミロク情報サービス	平成15年12月 1日	平成16年11月30日
税理士証明書発行サービス	日本税理士会連合会	平成16年 1月16日	平成17年 1月15日
Secure Contract Support Service	リコーリース株式会社	平成16年 3月 1日	平成17年 2月28日

1.2.3 商業登記に基づく電子認証制度

（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、登記所に備える商業登記簿に記載して公示することで、取引の安全を図る制度である。

商業登記事務を取り扱う登記所は、全国に約６５０か所余あり、全国約３５０万の会社・法人に関する登記事務をつかさどっている。

（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。登記が会社の成立要件となる。

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ゆえんである。

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、登記の事由を証する書面の添付が必要である。

② 法人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制度

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、当該法人の法人格の存在の証明、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、登記上の法人代表者の電子証明書が発行される。

証明書には、法人代表者本人の氏名のほか、商号・本店・代表者の資格等が登記簿の記載内容に基づいて記録される。

この証明は、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、本店移転又は法人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となっていることである。

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、法人代表者からの使用廃止届・使用休止届の提出や変更登記の申請に基づく失効・保留等があり、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　電子証明書の取得手続

法人代表者が、当該法人の所在地を管轄する登記所に電子証明書の発行を申請すると、その登記所の窓口において電子証明書のシリアル番号が告知されるので、これに基づき、法人の事務所等において、インターネット経由にて電子認証登記所から電子証明書を取得する。

なお、発行申請に当たっては、あらかじめ、秘密鍵と公開鍵の鍵ペアを作成の上、公開鍵の値や申請情報等を格納したフロッピーディスクを用意する必要がある。

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、電子証明書の提出を受けた相手方は、当該署名の確認等をした後、電子認証登記所に電子証明書の有効性を確認することができる仕組みとなっている。

（５）現状と今後の予定

①　現状

平成１２年１０月に東京法務局と前橋地方法務局において商業登記に基づく電子認証制度の運用が開始された後、順次、運用実施庁が拡大され、現在では、全国ほとんどの会社・法人について制度の利用が可能となっている。

②　これまでの主な動き

・　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。

・　平成１３年６月から、GPKI との相互認証が実施されている。

・　平成１４年１月から、「公証制度に基礎を置く電子公証制度」との連携を図っている。

・　平成１４年４月から、会社関係書類の電子化（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、フロッピーディスクや 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したもの。）に対応している。

・　平成１５年４月１日から、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、電子証明書の発行手数料を大幅に引き下げた。

③　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

1.2.4 民間に対するサービス

（1）電子入札

①電子入札の背景

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おり、電子入札は CALS/EC の具体的な取り組みの一つである。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り、電子入札は、入札契約段階における CALS/EC 導入の一環と位置付けられる。

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､電子決裁システムの構築等が目標として掲げられている。

電子入札は、国土交通省における CALS/EC の取り組みの一環であるだけでなく、電子政府への取り組みにおいても「政府調達の電子化」の中核をなし、また、公共工事に対する国民の信頼の確保と建設業の健全な発達を目的とした「公共工事の入札及び契約の適正化の促進に関する法律」に基づく適正化指針にも位置付けられるなど、非常に重要な施策となっている。

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。

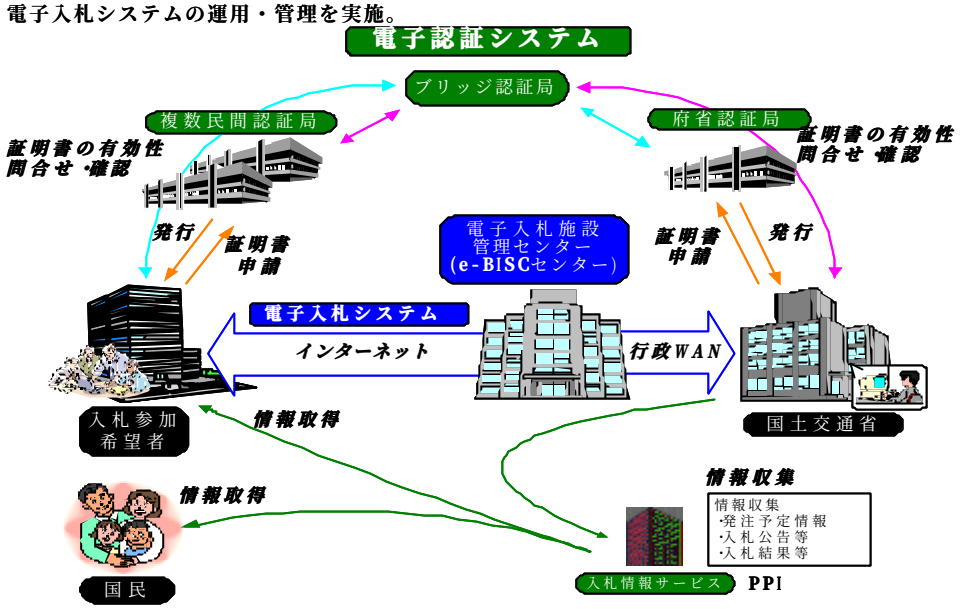
認証局は、国土交通省が導入している電子入札コアシステム（後述）においては、複数認証局対応となっており、現在、8 認証局がコアシステムに対応している（政府認証基盤のブリッジ認証局との相互接続完了認証局）。

電子入札導入効果としては、入札参加者の移動にかかるコストや移動時間等、入札に係る費用の縮減が大きいと考えられ、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。

■電子入札の仕組み

○電子入札は、入札に伴う資格審査確認申請から入札結果の公表に至るまでの行程をオンラインで行うもの。
また、電子入札を支援するためｅ－ＢＩＳＣセンター（電子入札施設管理センター：２００１年４月～）で、電子入札システムの運用・管理を実施。



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、平成 13 年度は約 100 件、平成 14 年度は約 2,000 件で実施し、平成 15 年度からは直轄事業において全面的にスタートしている（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。

（２）公証制度に基礎を置く電子公証制度

①電子公証制度とは

電子公証制度は、公証人が紙の文書について行っている認証や確定日付の付与の事務に対応して、電磁的記録（電子文書）についても、電子公証業務を行う公証人である指定公証人が、認証や確定日付を付与する制度である。

電子取引・電子申請においては、インターネットを通じて情報が送受信されるため、情報の作成者を確認し、情報の内容の消失、改ざん等があった場合に、これに適切に対応する制度的な基盤が不可欠である。電子取引・電子申請に関する制度的な基盤のうち、電子署名や電子認証は、主として情報の作成者を確認するものであるが、電子公証制度は、情報の内容の改ざんや消失に備え、情報の内容を事後的に確認し、証明するための仕組みとして位置付けられる。すなわち、電子署名や電子認証だけでは、伝送途中での情報の消失等に対応することができないため、信頼することができる第三者機関に、作成された情報に関する記録（作成者に関する情報、作成された情報の同一性に関する情報）を作成・保管させ、これにより、後日紛争が生じた際に情報の

作成者及び情報の存在・内容を証明し、紛争の解決の手段となる制度が、電子公証制度である。このように、電子公証制度においては、公証人がTTP（Trusted Third Party）といわれる役割を担うことが期待されている。

②電子公証制度の概要

電子公証制度の内容は、（ｉ）電子私署証書、電子定款の認証、（ii）電子確定日付の付与、（iii）保存及び内容に関する証明の各サービスである。

（ｉ）電子私署証書、電子定款（電磁的記録）の認証

公証人法にいう「認証」とは、文書の成立・記載が正当な手続でされたことを証明することをいい、私署証書（署名又は押印のある私文書）の認証の場合、公証人の認証によって、当該私署証書の署名又は押印の真正（作成名義人の意思に基づいて署名又は押印がされたこと）が証明されたことをいう。

電磁的記録の認証についても、私署証書の認証と同様に、電磁的記録の作成名義人の意思に基づいて電子署名がされたことの証明を行うことになる。

（ii）電子確定日付の付与

私文書の確定日付の付与は、文書の存在を証明する制度として用いられているが、特に、債権譲渡の際には、確定日付のある証書による通知・承諾が債権譲渡の第三者対抗要件（民法第４６７条第２項）とされている。

今回導入された電子確定日付の付与の制度は、私文書の確定日付の付与の制度を電子化するものであり、具体的には、電子的な情報（データ）を指定公証人に送信し、指定公証人が当該情報を確認した上で、当該情報に日付を内容とする情報（日付情報）を付して、これに指定公証人が電子署名をした上で送信者に送り返すことになる。この場合、日付情報の付された情報は、「確定日付アル証書」とみなされる（民法施行法第５条第１項及び第２項）。これにより、日付情報が付された情報には、民法施行法第４条の「完全ナル証拠力」（実質的証拠力）が認められ、民事訴訟において一定の時期以前に当該情報が存在したことの強力な証拠となると考えられる。

（iii）保存及び内容に関する証明

従来の紙による私署証書の認証及び確定日付の付与では、認証又は付与の対象となった文書の保存及び保存された内容の証明（紙の文書における謄本に相当するもの）のサービスは行われていなかったが、私署証書の認証及び確定日付の付与の電子化に当たり、破損しやすいなどの電子的な情報の性質にかんがみ、後日その内容について証明することを可能とし、紛争を防止することができるように、これらのサービスを行うこととされている。

③おわりに

電子公証制度が、今後様々な方面で利用され、高度情報化社会を支える制度的な基盤として電子取引等の普及促進に資する制度となることを期待したい。

（３）電子申請（利用環境整備）

本項目においては、個別の行政機関への申請手続きの状況ではなく、電子申請を行うための基盤である電子申請システム整備の状況と手続電子化の大枠について説明する。なお、国の行政機関においては、前述の GPKI 同様、政府全体として、行政手続が電子的にインターネットを通じて行える電子申請システムの整備について、次のとおり取り組んできており、これにより、2003 年度（平成 15 年度）末までには、国が行う手続の約９７％が電子申請できる状況になることが予定となっている。

- 1999 年（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 2003 年度（平成 15 年度）までに、民間から政府、政府から民間への行政手続をインターネットを利用しペーパーレスで行えるシステムの整備を行う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、2000 年（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 省や個別の国税申告手続等のシステムの実用化を図ることとされた。
- 2002 年（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、2002 年度（平成 14 年度）までに全府省において電子申請システムを整備し運用を開始することが決定され、全府省において電子申請システムが整備、運用が開始された。なお、登記手続や国税申告などいわゆる大規模なシステムが関連しているものに関しては､現在も段階的に電子化が進められているところである。

さらに、2003 年（平成 15 年）７月には、各府省情報化統括責任者（CIO）連絡会議において「電子政府構築計画」が決定され、今後は、単なるオンライン化という「量」の追求から、手続の簡素化・合理化の徹底やワンストップサービスの拡大など利用者が便利で分かりやすいものとする「質」の向上への転換を図ることとしている。

1.3 地方自治体における計画とその進捗状況

1.3.1 公的個人認証サービスの整備状況

(1) 公的個人認証サービスの概要

① 行政手続のオンライン化に必要な、ネット社会の課題（成りすまし、改ざん、送信否認など）を解決する本人確認サービスを、全国どこに住んでいる人に対しても安い費用で提供する、電子政府・電子自治体の基盤。

② 従来、窓口に出向く必要があった行政手続が、家庭や職場からインターネットで可能となるもの。平成１６年１月２９日にサービス開始。

(2) 対象となる行政手続（＜　＞内は紙も含めた過去の年間実績）

① 当面の予定

（ｉ）２月２日～　：電子申告（国税庁＝東海４県先行）　＜約 2,000 万件＞

（ⅱ）２月１６日～：恩給関連申請の一部（総務省）　　＜約　　19 万件＞
（ⅲ）３月２９日～：社会保険関係手続（厚生労働省）　　＜約 4,900 万件＞
　　：無線従事者免許関連申請の一部（総務省）＜約 6 万件＞
（ⅳ）３月末～　　：旅券申請（外務省＝岡山県ほか順次）＜約　 580 万件＞
② 平成１６年度以降：６月より国税の電子申告が全国に拡大されるほか、国の機関の他手続・各地方公共団体の手続が順次追加される見込み。

(3) 利用方法
①サービスの利用に先立ち、電子証明書の発行を受ける必要がある。
（ｉ）お住まいの市区町村役場の受付窓口に、住民基本台帳カードなどの IC カードと、公的機関発行の写真付本人確認書類(写真付き住民基本台帳カード､運転免許証など)を持参。
（ⅱ）申請書に氏名、住所、性別、生年月日などを記入し、受付窓口に提出。
（ⅲ）受付窓口の担当者から本人確認を受ける（本人確認書類を提示)。
（ⅳ）受付窓口に設置された鍵ペア生成装置の案内に従い、鍵ペア（公開鍵＋秘密鍵）を生成（パスワードを設定)。
（ⅴ）鍵ペアが格納された住民基本台帳カードを受付窓口に提出。
（ⅵ）秘密鍵と電子証明書が格納された住民基本台帳カードなどを受け取る。
② 電子証明書を利用した行政機関等への申請・届出等（イメージ）
（ｉ）電子証明書の発行時に配布される利用者用クライアントソフト（CD-ROM）を、ご利用のパソコンにインストール。
（ⅱ）IC カードリーダライタを準備し、ご利用のパソコンに接続（各市区町村で発行される住民基本台帳カードにおける動作が確認された IC カードリーダライタの一覧を市区町村役場の受付窓口で提示)。
（ⅲ）行政機関等のホームページ等の案内に従い、申請書の必要事項を記入。
（ⅳ）住民基本台帳カードを IC カードリーダライタにセットし、暗証番号を入力。
（ⅴ）画面上の電子署名ボタンをクリックして、申請書に電子署名を付す。
（ⅵ）画面上の送信ボタンをクリックして、申請書、電子署名、電子証明書を送信。

(4) 電子証明書
① 発行者：都道府県知事
（４６都道府県が指定認証機関（財団法人自治体衛星通信機構）に委任）
② 発行手数料：平成１６年３月３１日まで無料。それ以降は原則５００円。
③ 有効期間：３年間

(5) 住民基本台帳ネットワークシステム（住基ネット）との関係
① 住基ネットは、公的個人認証サービスの受付窓口における本人確認に利用されるとともに、電子証明書の情報に異動等が生じた際、速やかに失効させることを実現。
② 住基ネットは公的個人認証サービスに不可欠の基盤であり、住基ネットに不参加の地方公共団体は、公的個人認証サービスを実施することができない。

2．民間での電子署名／認証の活用

2.1 特定認証業務を行う事業者の紹介

特定認証業務を行う事業者にアンケートを送った結果、回答のあった事業者について、以下に紹介する。

2.1.1 株式会社コンストラクション・イーシー・ドットコム

(http://www.construction-ec.com)

(1) 本社所在地

〒111-0042　東京都台東区寿 1-11-6　SMK ビル 7 階

(2) 設立年月日

２００年８月１日

(3) 主な事業内容

建設業界及び全産業の経済活動の新たな標準インフラとして、次の３つのサービスを提供する。

- CIWEB（CI-NET LiteS ASP サービス）
  建設業 EDI 標準に基づく、電子調達システム共同利用サービス
- CECSIGN 認定認証サービス
  特定認証業務の認定を受けた電子証明書発行。職務認証付きサービス
- CECTRUST（電子原本性保証サービス）
  電子契約による原本保管サービス
- CECMARKET（共通業者リスト掲載サービス・オープン調達サービス）
  建設マーケットプレイスの機能を利用した調達関連サービス

(4) 担当者連絡先

電子契約事業部　出本　浩

03-3842-0811　izumoto@construction-ec.com

2.1.2 株式会社中電シーティーアイ

(http://www.cti.co.jp/)

(1) 本社所在地

〒450-0003 名古屋市中村区名駅南一丁目 27 番 2 号

日本生命笹島ビル 5・7・8・9・13 階

(2) 設立年月日

2003 年（平成 15 年）10 月 1 日

(3) 主な事業内容

・システム開発、システム保守・運用

・ネットワークシステム・インテグレーション

・大規模システム開発・保守

・マルチメディアシステム・インテグレーション
・コンピュータグラフィックス企画・製作
・科学技術（環境情報・技術開発）
・バイオインフォマティクス
・建築設備 CAD の開発・保守、販売
・電力系統解析・炉心解析
・電子認証
・データセンター
・受託計算、アウトソーシング受託
・コンピュータ運転・運用管理
・データ授受・プリンタ等のコンピュータ周辺処理サービス

(4) 担当者連絡先

株式会社 中電シーティーアイ　中部認証センター
052-563-3990（事業運営に関する問合せ）　eigyo@cti.co.jp

2.1.3 株式会社帝国データバンク

(http://www.tdb.co.jp)

(1) 本社所在地

東京都港区南青山２－５－２０

(2) 設立年月日

創業：1900（明治 33）年 3 月 3 日、設立：1987（昭和 62）年 7 月 13 日

(3) 主な事業内容

企業信用調査、データベース提供、マーケティング、電子商取引サポート（電子証明書発行業務を含む）、出版

(4) 担当連絡先

営業推進部　電子認証課　臼井　治彦
03-5775-3135　　usui@tdb.co.jp

2.1.4 日本認証サービス株式会社

(http://www.jcsinc.co.jp)

(1) 本社所在地

東京都港区芝一丁目１０番１１号

(2) 設立年月日

１９９７年9月１１日

(3) 主な事業内容

電子証明書の販売、認証局業務のコンサルティング、アウトソーシング

(4) 担当連絡先

企画部長 町田 陽
03-5481-1391　machida@jcsinc.co.jp

2.2 民間での主要な用途

2.2.1 企業内利用

(1) 企業内情報システムの状況

インターネットは創生期を脱して、現在では日常の社会活動や企業活動に不可欠な道具として定着してきた。このように普及してきたインターネットの活用について、社会生活の中での普及度合い、企業活動の中での利用形態の変化に従って、その利用方法についても再考する必要があり、新しい企業内ネットワークのありかたと電子認証技術の適用について考察していきたい。

(2) 企業内情報システムの環境変化

平成１５年度は電子政府の成果による電子入札の実施、電子納税申告など政府や自治体の電子化が急ピッチで進んだ年である。またインターネットバンキングや株取引、インターネットオークション、インターネットショッピング、航空券の購入、新幹線の座席予約などがインターネットで簡単に利用できる環境が整ってきて、ごく一般の消費者が日常的・定期的に利用する機会が増している。それに応える情報システム対応として Web アクセス能力の強化、２４時間３６５日の安定したサービス、レスポンスの適正な動作保証が課題であり、携帯電話やモバイル PC からのアクセスに対する対応も欠かすことが出来ない。

企業の外から企業内情報システムに対する利用頻度の増加に伴い、従来社内インターネットと共有していたインターネット接続回線は、社外向け情報システムをインターネットデータセンタなど高速大容量の回線が得られる場所に設置して社内専用のシステムと分離する傾向にある。

インターネットを利用したサービスや業務が普及するに従いクローズアップされたのが情報セキュリティ対策への高い要望である。インターネットを利用したサービスが高度化される中、これを利用するクライアントの個人情報の保護は会社の存続をも左右する重大な経営課題であり、対策への高いニーズがある。情報セキュリティ対策として、ファイアウォール、不正進入検知、改ざん検知システムの設置の常識化、顧客情報を格納するデータベースの健全性の確保、万が一の事態に備えた原因探査システムと方策、再発防止のためのシステム、緊急対応制度の整備など情報セキュリティ対策への課題は多い。

一方、企業内ユーザの利用形態の多様化も進んでいる。もはや職場は自社事業所内だけではなく、出先からでも通常に業務をしたい、客先提案時に臨機応変の対応をしたいなどの要望や、企業グループ経営のニーズとして、構成企業の垣根をなくしたグループ内全社員を意識したネット利用の方法、事務・営業・開発・保守運用のそれぞれの部門に併せた最適なネットワークを構成したいなど、多様化するニーズに満足するネットワークを構成することは至難の業である。

情報セキュリティポリシーへの対応も忘れてはならない、企業内におけるウイルス感染はネ

ットワークからの感染経路より、持ち込み媒体や PC により引き起こされる事例が増えている。また、社内機密情報を移動媒体に格納し持ち出す事例もある。このような事例は社内にセキュリティポリシーを定めこれを実践することが肝要である。

(3) 企業内情報システムを守る技術

情報資源を守るために情報システムとして必要なことは、企業内情報資源に必要最低限度の人だけがアクセスできる個人認証の環境整備と途中経路での盗聴防止技術である。企業情報資源とはクライアント PC、ネットワーク、ネットワークサーバ上の各種データである。PC アクセス・ネットワークサーバへのアクセスは、通常 ID／パスワードを用いた認証を実施するが、電子証明書を格納した IC カードや USB トークンを用いたアクセス制御は現実的で効果のあるセキュリティソリューションとして利用されている。

現状のネットワークへのアクセス管理にはかなり大きな問題がある。企業内 LAN の HUB に空きポートがあれば容易に LAN 接続することが可能になる場合が多いからである。無線 LAN を経由したアクセスも見逃してはならない。無線 LAN は電波が届けば事業所の外からでもアクセスすることが可能で、稚拙な設定では第三者の盗聴も容易な環境を簡単に構成してしまうことができるからである。また、社外からのネットワーク利用に対するニーズに応えながらセキュリティを確保することも必要である。

このようなネットワークアクセスへの解決策として認証 VLAN の適用が有効である。認証 VLAN は電子証明書技術を利用したアクセス認証を実施することが可能である。

例えば、認証 VLAN 対応のネットワークスイッチ機器を準備し、接続したいクライアントから電子証明書を利用して認証を行なうと、認証サーバからは接続できる VLAN 識別番号がネットワークスイッチに指示される。MAC アドレスと IP アドレスを固定的 DHCP 等で割り当てることにより、L3 フィルタリング機能にてアクセスが制御できるようなネットワークを構成にすることも可能である（機器により動作が異なる場合がある）。認証に失敗すればネットワークには接続されない。また、無線 LAN を構成する場合にも同様に認証することが出来る。無線 LAN の場合には暗号化機能を併用することが必要である。このように認証 VLAN 技術を利用するとネットワークレベルでのアクセス制御を木目細かく制御することが可能になる。また、副次的な効果としてウイルスに汚染されたクライアント PC をネットワークから切断するといったことも可能になり、管理された企業内ネットワークを構成する事ができる。なお、認証 VLAN は発展途上の技術でありベンダー間の互換性や相互接続性、仕様の相違など解決すべき問題も多い。

社内情報資源へのアクセス制御にも電子証明書技術が有効である。シングルサインオンと呼ばれる技術を利用して、一度の認証で許された情報資源へアクセスが可能になり利便性を向上できる。また、ワークフローなど社内文書への押印・回覧も電子証明書技術で達成可能である。

このように電子証明書技術は企業内ネットワークで活用可能な場面が多々あり、キーテクノロジーであるが、導入の難しさ、構築費用の問題などクリアしなければならない課題が多々あり、普及を阻害する要因になっている。

(4) 社員証 IC カードアプリケーション

企業内システムで最も有効な利用方法は電子証明書が入った IC カードを社員証として配布し利用することである。社員証は常に携帯し日常的に利用することから、個人認証手段として最も手軽であり受け入れやすいものである。また、前述の企業内情報システムにおける課題も電子証明書が格納された IC カードによりかなりの部分が解決可能である。また IC カードにクレジットカード機能、電子マネー機能、物理セキュリティー機能を兼ね備えることにより一層効果的な媒体になることが期待され、複数の大企業での導入事例が報告されている。最近では IC カードとともに USB トークンと呼ばれる媒体で利用されることも多い。電子証明書技術は企業内と同様に学校や病院など組織が運営するネットワーク環境に適用することが可能であり裾野が広い技術だと言える。

2.2.2 保険会社における利用例

損害保険の分野では、数年前から貿易 EDI の参加者として PKI を利用している実績がある。また、インターネットによる保険申し込みに際して保険申込書の原本性確保、否認防止等の目的で電子署名を利用している事例もある。背景としては、保険会社が扱う情報には機微情報が多く含まれているので、インターネットを利用する際には特に高度なセキュリティ確保が必要であり、PKI を利用したデータ通信が必要不可欠といえる業界の事情がある。

さらに、金融自由化の流れのなかでリスク細分型の保険契約が増えた結果、保険代理店は従来のポケット電卓等による見積もり作成が困難になり、ベストアドバイス義務の観点からも保険会社が保有する最新のデータベースを利用した保険料見積もりシステムが必要になってきている。保険会社としては各代理店が扱っている顧客の情報だけにアクセスする権限を与える必要があり、この制御に PKI を利用することによりセキュアーなサービスを提供することが可能になっている。

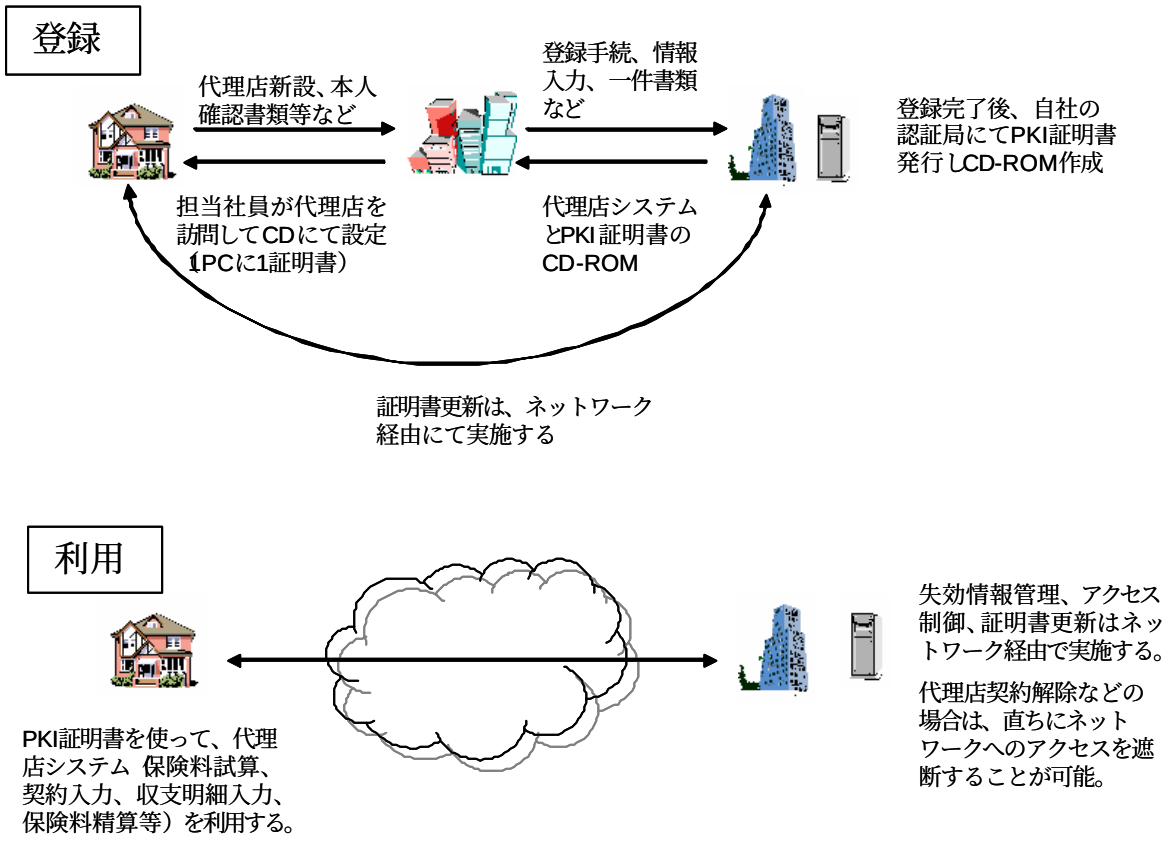


図 2-1 保険会社における利用例

2.2.3　リース会社における利用事例

大口取引先を対象として電子契約書システムの導入に取り組んでおり、電子契約書への署名に PKI を利用している。従来、紙で作成されていた契約書を電子化することで、契約書の保管コストならびに郵送などの配送コストの削減が可能になるという。現状の取り組みは大口取引先に限定されており、実験的な意味合いが強い。また、取引先に対する負担を軽減するという配慮から、セキュリティ上の観点からは取引先が行う方が望ましいにもかかわらず、登録機関が代行している業務プロセスが存在する。例えば、証明書の登録プロセスにおいて、登録機関が鍵ペアの生成を依頼する当事者となっており、生成された鍵ペアを IC カードに保管し、リーダ／ライタと共に取引先に渡している。

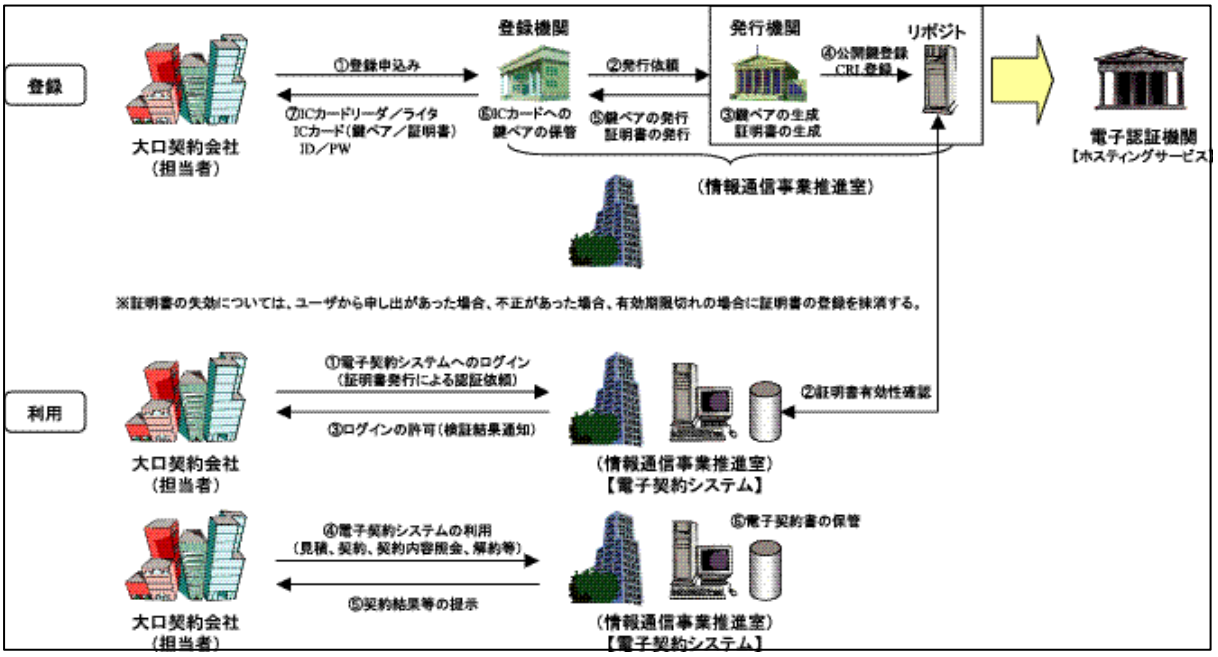


図 2-2 リース会社における利用事例

リース契約書などの債権証書を長期にわたって保管する必要がある。現在、2 万件の取引先があり、これまでは紙の契約書を大量に保管してきた。このシステムで、電子署名を利用することによって契約書を電子化し、保管コストを削減することを目標としている。また、契約書の電子化により、時間と場所を選ばずに電子署名が可能になり、紙の契約書で発生していた郵送や持ち込みなどのデリバリコストも同時に削減されることを見込んでいる。

2.2.4 証券会社での利用事例

［「電子署名及び電子認証の現状及び将来像に関する調査」
http://www.ecom.or.jp/ecit/report/mri_2002.pdf より抜粋］

社外の顧客向けに発信する電子メールへの署名に PKI を利用している。同社では、従来からフェイクメールによる風説の流布を危惧しており、株価操作の防止や顧客に対する信用確保を目的としたツールの導入を検討してきた。その中で PKI の機能が C 社のニーズにマッチしたことから、PKI を全社的に導入するに至っている。電子メールを利用する全社員（600 名）が利用しており、PKI の登録・利用フローは標準的なものとなっている。

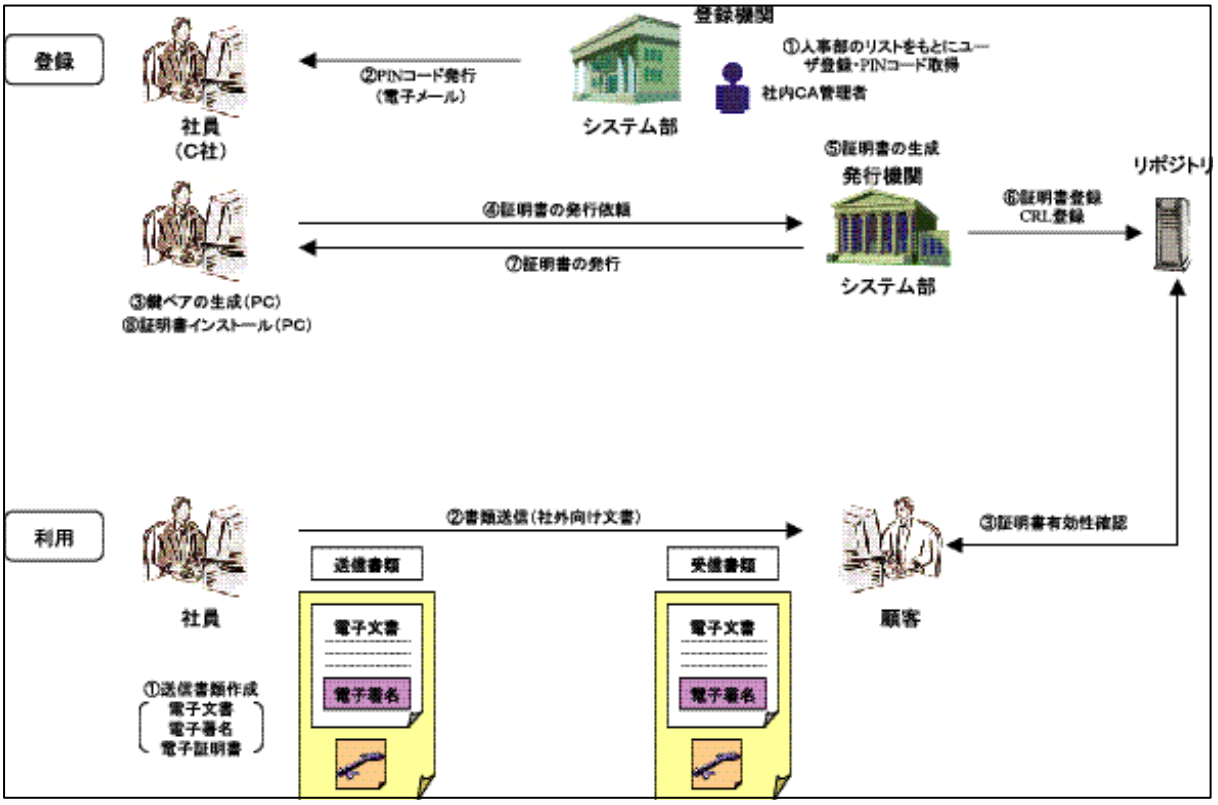


図 2-3 証券会社における PKI 登録・利用フロー

3．国際利用を目指す動き

3.1 アジア PKI フォーラムにおける相互運用試験

(1) はじめに

PKI インターネット上で電子商取引を安全にかつ確実に実現する技術として期待されているが、PKI を使用した国際間相互認証に関する分野において、特にアジア地域においては現在 PKI が構築されつつあるが、PKI の構築方法は各国の事情に応じて構築されることから、統一されていないのが現状である。

そこで、日本 PKI フォーラムでは平成13年度にアジア圏の中でPKIの整備が進んでいる韓国、シンガポール及び日本の間で、PKI の相互接続の実証実験を実施し、PKI 相互接続に関する標準案の作成及び課題の抽出を行った。また、国際的な認証基盤として相応しい実験対象国・地域の拡大、PKI モジュールの API インタフェース等実験範囲の拡大、前年度の課題の検討・解決を図り、PKI 技術に関する国際間相互接続の基盤整備の一助とするため、日本、韓国、シンガポール、チャイニーズ台北、香港チャイナの５カ国／地域により、技術的な課題の解決、実験対象国／地域の拡大を図り、PKI 相互接続に関する標準の作成を目的として実験を行った。

(2) プロジェクト概要

① 体制

本実証実験の参加国／地域と推進組織を「表 2-2 体制」に示す。

表 2-2 体制

参加国／地域	組織
日本	日本 PKI フォーラム
韓国	Korea PKI Forum
シンガポール	PKI Forum Singapore
チャイニーズ台北	Chinese Taipei PKI Forum
香港チャイナ	Hong Kong PKI Forum

② 活動概要

相互接続基盤の整備にあたり、以下の活動を実施した。

- シンガポール、韓国、チャイニーズ台北、香港チャイナ、日本における PKI コンポーネント間接続に関する標準案、及び、PKI アプリケーションに関する標準案を作成
- PKI コンポーネント間接続に関する標準案について PKI Forum Singapore、Korea PKI Forum、Chinese Taipei PKI Forum、Hong Kong PKI Forum、及び日本 PKI フォーラムの参加団体のメンバを含む各国／地域技術者と調整
- PKI アプリケーションに関する標準案について PKI Forum Singapore、Korea PKI Forum、Chinese Taipei PKI Forum、及び日本 PKI フォーラムの参加団体のメンバを含む各国／地域技術者と調整

? 標準案の実用性及び有効性を、国内シミュレーションセンタ並びに各国・地域の現地実証実験環境にて検証
? 実証実験の成果を標準案にフィードバックし、標準を作成

(3) 標準作成

① PKI コンポーネント間接続に関する標準（相互接続インターフェース仕様）

認証局の設計担当者が、相互接続の設計作業における PKI コンポーネント間の接続インターフェースの要件を検討する際に使用する標準の策定を行った。

② PKI アプリケーションに関する標準（パス検証テストガイドライン）

認証局の設計担当者及びソフトウェア開発者がアプリケーションにおける証明書検証方法の設計作業において必要となる検証要件、及び評価作業におけるテスト項目を検討する際に使用する標準の策定を行った。

(4) シミュレーションセンタにおける認証局間の実証実験

相互接続のために認証局間で交換する証明書発行要求と相互認証証明書は、相手認証局が受け入れることができるものでなければならず、相手認証局が発行した情報を受け入れることができなければならない。また、相互接続を行った認証局ドメイン間ではエンドエンティティ証明書が相互に利用可能であり有効性検証が可能でなければならない。㆓実験では、認証局が「相互接続インターフェース仕様」に従って証明書のライフサイクル管理を行うことにより相互接続の関係を構築できることを確認することで、認証局の運用者にとっての標準の実用性を検証した。

(5) シミュレーションセンタにおける証明書検証の実証実験

国際間の電子商取引等を行うアプリケーションを利用するにあたって、利用者は相手方から受け取った証明書が有効なものであるかどうか、受け取った証明書が信頼できる認証局から発行されたものであるかどうかについて検証しなければならない。この証明書検証に、PKI コンポーネントのひとつである検証局へ問合せを行い検証する方式を適用するケースがある。本実験では、「相互接続インターフェース仕様」に則って、実際に証明書の検証を実施することで、「相互接続インターフェース仕様」が利用者にとって実用的であるか否かを検証した。証明書の検証には検証局を使用した。また、実験にはシミュレーション環境を利用した。

(6) シミュレーションセンタにおける国際間調達の実証実験

「相互接続インターフェース仕様」を、シミュレーションセンタにおける国際間調達の実証実験の観点から、利用者にとって実用的か否かについて現地環境を用いて検証した。

国際間調達業務における業務シナリオを設定し、日本のシミュレーションセンタ内で、利用者端末を使用し、日本国認証局が発行したエンドエンティティ証明書を保有するエンドエンティティ、日本のシミュレーションセンタ内のチャイニーズ台北認証局が発行したエンドエンティティ証明書を保有するエンドエンティティ、日本のシミュレーションセンタ内の香港チャイ

ナ認証局が発行したエンドエンティティ証明書を保有するエンドエンティティの間で買い手、売り手の立場を入れ替えて実験を行った。

各国／地域利用者端末と業務サーバで採取されるログ情報より検証内容を含むデータを収集し解析することで、「相互接続インターフェース仕様」の実用性を検証した。

(7) 現地環境における認証局間の実証実験

相互接続に係わる証明書のライフサイクル管理を通しての「相互接続インターフェース仕様」の有効性を、現地環境を用いて検証した。

(8) 現地環境における証明書検証の実証実験

「相互接続インターフェース仕様」に則って、実際に証明書の検証を実施することで、「相互接続インターフェース仕様」が利用者にとって有効であるか否かを、現地環境を用いて検証した。

(9) 現地環境における国際間調達の実証実験

「相互接続インターフェース仕様」を、現地環境における国際間調達の実証実験の観点から、利用者にとって有効か否かについて、現地環境を用いて検証した。

(10) 現地環境におけるパス検証テストガイドラインの実証実験

「パス検証テストガイドライン」の有効性を、現地環境を用いて検証した。

(11) 成果

① PKI コンポーネント間接続に関する成果

（ｉ）CC 及び CR ハイブリッドモデルの適用地域の拡大

昨年の実証実験で規定した Cross Certification（CC）と Cross Recognition（CR）のハイブリッドモデルを本年度実証実験の接続モデルとし、地域拡大に対するモデルの有効性検証を行った。本実証実験を通じてモデルの核である認証スキームや検証形態を崩すことなく、接続相手の拡大に適用できることを実証した。

（ii）相互接続における重点テスト項目の特定と共有

相互接続相手国の数を増やすことによって、相互接続を行う場合必ず陥るポイントやパターンを絞ることが可能となり、テストを行わなければならない範囲を明確にすることができた。そして、その対策として仕様への反映やテスト項目への盛り込み等を行った。

（iii）他国の政府認証基盤との親和性確保

今回採択したモデルは、相互認証技術に関して実績のある日本の GPKI 相互運用性仕様を参照しているが、本モデルとチャイニーズ台北側の GPKI との親和性を確保することができた。

（iv）ブラウザベースのサービスへの拡張

今回使用した証明書プロファイルは、ウェブブラウザベースの製品にも対応できるよう設計されている。本実証実験において、ウェブブラウザベースの制限された PKI 機能の環

境下においても、証明書プロファイルが適用できることを確認した。実際にはウェブブラウザに標準実装されているメーラーの S/MIME 機能を使い、そのサービスの有効性を確認することができた。

② PKI アプリケーションに関する成果

（ｉ）テストパターン最適化のための相互接続環境の体系化

パス検証テストガイドラインは、典型的な相互接続環境をモデルとして定義し、そのモデル毎に必要なテスト要件及び関連したテスト項目を定義したものである。

適切なテスト項目を抽出するには、適切な相互接続環境の選択/分析が重要となる。

X.509 や RFC3280 などの標準に記述されたパス検証ロジックは、そもそもどのような環境でも均一な検証結果を得られるように、非常に汎用的に記述されている。これは実装するベンダーにとっては大きな負担であり、多くの実装がサブセットにしかすぎないという現状がある。これは評価する側にとっても同じことであり、ある環境において評価すべきテスト要件を抽出することは非常に高度なスキルを要求される。

そのため本ガイドラインでは典型的な相互接続環境（モデル）を定義している。これらのモデルは、

- CA-CA 間の相互接続形態
- 失効・検証情報の提供方法
- 証明書を用いたサービス内容

といった 3 つの観点から体系化されている。複数の観点から体系化することで適用範囲を広げ、汎用的なガイドラインとすることができた。

（ii）パス検証機能に対する評価指標の確立

パス検証ガイドラインは、X.509 や RFC3280 などの標準に記述されたパス検証ロジックに基づいたテストケースの集合として設計した。

本実験では、今まで CA-CA 接続実験で使用してきた Cross Certification や Cross Recognition などについてガイドラインからテストケースを抽出し、CA-CA 接続実験で使用してきた各アプリケーションや検証局でそれぞれのテストケースを実行し、各アプリケーションや検証局が標準に忠実なパス検証機能を実装していることが確認できた。

（iii）署名・検証処理 API のインターオペラビリティ確保

昨今の PKI 推進活動は国の内外を問わず盛んであり、具体的な活動としてはアメリカにおける OASIS(旧 PKI フォーラム)、EU 圏における EESSI、国内における GPKI、LGPKI、JACIC、公的個人認証などが挙げられる。これらの状況において、PKI を活用する PKI アプリケーションの観点で見た場合、特定の仕様或いは特定の製品に依存した PKI アプリケーションとなることも多々見受けられる。このような場合、ある PKI アプリケーションサービスを利用するには利用者が PKI アプリケーションの要求を満たす署名・暗号機能をインストールする等の作業が必要となり、PKI アプリケーションごとにクライアント環境を構築する必要があるなどの煩雑さを増す要因となる。

1 国内で使用する場合にはこのような問題がある。また国際間で 1 つの PKI アプリケーションサービスを利用しようとした場合、クライアントで準備する必要がある署名・暗号

機能は輸出規制の対象となり、特定の製品に依存する PKI アプリケーションを構築することは実用的ではない。また、PKI アプリケーションが各国で使用可能な署名・暗号機能を使用するには、署名・暗号機能の仕様が統一されていないことから、PKI アプリケーションの構築が不可能となるという問題がある。

これらの問題は、国際間における PKI アプリケーションの普及を妨げる要因であり、国際間における PKI アプリケーションを普及させるにはこれらの問題解決を行うことが最大の課題であると言っても過言ではない。国際的な標準に基づいた上で、最低限の共通ルールを設定する必要がある。これらの課題を解決する目的で署名用トークンインターフェース仕様を策定した。

署名用トークンインターフェース仕様は、OS に関してオープンプラットフォームである PKCS#11 に基づいた機能仕様として設計した。具体的には、PKCS#11 で使用する機能の定義、各国の環境面の差異及び開発言語の差異を吸収する機能の定義、アプリケーション開発の容易性を高めるインターフェースの定義を行った。

本標準の有効性を確認するための実験では、テストアプリケーションを作成し、各国の PKCS#11 ライブラリを使用してテストアプリケーションへアクセスすることで本標準のすべての機能についての検証を行い、本標準の有効性を確認することができた。このことは、本標準が国際間のインターオペラビリティを確保していることを証明していると言うことができる。

本標準を使用することで、国際間の PKI アプリケーションを利用する上で各国の既存の PKCS#11 ライブラリをそのまま使用することができ、電子署名を有効的に活用することが可能となる。

以上より、本標準は、PKI アプリケーションの国際間での流動性を高め普及を推進するための 1 つの突破口を開いたという点で高く評価することができると考える。

3.2 Challenge PKI プロジェクト

(1) プロジェクト概要

Challenge PKI プロジェクトは、Challenge PKI は、NPO 日本ネットワークセキュリティ協会（JNSA）が、PKI の相互運用技術を取り巻く様々な問題に取り組んできた一連のプロジェクトである。プロジェクトは、PKI のインフラとしての必要性を社会にアピールし、その際ネックとなると考えられる PKI 相互運用性の問題を自ら解決していくこと等を目的とし、2001 年の夏にスタートした。2001 年度に Challenge PKI 2001 プロジェクト、2002 年度に Challenge PKI 2002 プロジェクト、そして現在は、Challenge PKI 2003 プロジェクトが進行中である。

PKI（公開鍵基盤）は、オープンなネットワーク上において、安全、安心を提供する有望な手段だと考えられている。しかし PKI が IT 社会における真の基盤となるためには、多くの課題がある。技術的な課題としては、PKI の相互運用性確保が挙げられる。PKI の相互運用技術の難しさは、広範囲 における認証、広範囲な応用、そして広範囲なセキュリティレベルへの対応が求められている点に起因する。そして、これらを実現するためには、標準化自体のあり方から、PKI アプリケーションを広く展開するまでのプロセスなども検討する必要がある。

Challenge PKI 2001 及び Challenge PKI2002 プロジェクトは、マルチドメイン・マルチベンダーでの PKI 相互運用フレームワークの確立を目指し活動を行ってきたが、Challenge PKI 2003 ではさらに範囲を広げ、PKI を利用した電子署名・認証フレームワーク全般の課題に取り組んでいる。

これらのプロジェクトの成果は、54thIETF 横浜、55 th IETF アトランタ、56 th IETF サンフランシスコ、57 th IETF ウィーンなどで発表している。また、これまでの成果を元にしたインターネットドラフトの発表も行っている。

現在の Challenge PKI プロジェクトは、実装レベルでの相互運用性の確保という側面だけではなく、世界レベルで広範囲に信頼関係を確立するための標準化やアーキテクチャのあり方を探るといったことをも念頭におき始めている。これに伴い、その活動の場も国内だけではなく、海外との連携を視野に入れたものになってきている。

ここでは、Challenge PKI プロジェクトのこれまでの活動を詳しく説明すると共に、今後の展望を紹介する。

(2) PKI の相互運用

PKI を様々なビジネスやサービスに適用するとき、また、異なった組織間や、国を超えての認証を行おうとした場合、現時点では、様々な課題がある。非技術面では、国や地域における法制度の違いや、ネットワークにおけるプライバシ保護の問題、また、複数の認証局間でのセキュリティポリシの違いなど、解決すべき問題はいくつもある。技術面においても、非常に複雑な問題がある。それが、PKI 相互運用性の確保である。PKI 相互運用の促進は、PKI が真の認証基盤となるための、最も重要な技術的課題だと考えられる。

冒頭でも述べたとおり、PKI の相互運用技術の難しさは、広範囲な認証、広範囲な応用、そして広範囲なセキュリティレベル等の対応が求められている点などにある。その他にも、PKI の相互運用技術自体が、法制度、プライバシなどと無関係ではなく、こうしたことが問題を複雑にしている。

PKI の相互運用性を確保するために必要な標準化作業は、ITU や IETF などの標準化団体において盛んに進められている。しかしこれらの標準化団体では標準化の作業を行っていても、これらの標準を実装したマルチベンダーの製品の相互運用性などを保証しているわけではない。また、ITU の X.509 や、IETF/PKIX RFC3280 といった PKI の標準に記述されている内容は、非常に広い範囲への応用を想定しており、これらだけで実際に相互運用性を確保した実装を行うことは困難である。現在、多くの PKI 製品が、X.509 準拠、RFC3280 準拠をうたっているが、実際の実装の多くは、X.509 や、RFC3280 のサブセット（一部分）を実装しているに過ぎない。そのため、サブセットの実装がなされた製品同士の組み合わせが複雑化し、相互運用が極めて分かりづらいものとなっている。

こういった問題に対処するため、北米やヨーロッパの様々な団体が PKI の相互運用性の問題などに取り組んでおり、各種の PKI に関連した相互運用仕様書や、標準への準拠性テスト仕様書の作成、そして相互運用テストが行われている。

(3) Challenge PKI 2001

Challenge PKI 2001 プロジェクトは、情報処理振興事業協会（IPA）の委託を受けて実施した PKI 相互運用実験である。実験では、９つの CA 製品やサービスの参加を得て、マルチドメイン・マルチベンダーの PKI 相互運用実験を行った。以下に、Challenge PKI 2001 プロジェクト開始時の目標を示す。

① 複数 CA 製品による相互運用性の検証
② マルチベンダーPKI の相互運用性実験方法の確立
③ マルチベンダー環境の PKI 構築技術の促進

実験の狭義の目標は、①の検証であったが、広義の目標である②③も重要な目標であった。プロジェクトは、実験参加者の協力を得て、非常に実り多いものとなった。その一方、PKI の相互運用を広く達成するためには、さらに多くの課題があることを学んだ。実験を通して明らかになった課題は、次の通りである。

① 実装の差異と標準の曖昧さ
② テストケース設計の困難さ
③ レファレンス実装の欠如

特に「①実装の差異と標準の曖昧さ」の問題は、標準化そのものに起因するものであった。こうした標準化に関する問題の発見は､後述する IETF での活動などにつながる貴重な成果であった。我々は当初、ある標準に基づき開発された製品間の実装の違いなどを明らかにすることで、相互運用性を確保するアプローチをとっていた。しかし ChallengePKI2001 以後では、そうした実装の違いを生む標準化自体の問題がクローズアップされた。IETF が進める標準化は「ラフ・コンセンサスとランニング・コード」と言われる思想の元に進められている。しかし複雑なセキュリティの要求は、その標準に準拠した「ランニング・コード」自体を開発することを困難にしている。このプロジェクトによって我々は、標準に対する準拠性が確認済みの、レファレンス実装の重要さを認識した。

Challenge PKI 2001 プロジェクトでは、相互運用テストのためのテストケースの設計を行ったが、この作業は非常に負担の大きいものであり、標準の作成と同程度に困難な作業だと思われた。Challenge PKI 2001 で構築した実験環境は、プロジェクト終了後に取り壊した。多くのリソースを費やして開発したテストケースは、この実験環境に依存したものであったため、再利用できないものになってしまった。

本プロジェクトでは、当初の目標に加え、レファレンス実装やテストケース再利用の重要性といった、今後 PKI 相互運用技術の普及啓発を行う上で多くの経験を得ることができた。これらの経験は、次の Challenge PKI 2002 プロジェクトに反映された。

(4) Challenge PKI 2002

Challenge PKI 2002 プロジェクトは、情報処理振興事業協会（IPA）の委託を受けて実施し

た、PKI の相互運用を促進するためプロジェクトである。前回の Challenge PKI 2001 で得られた知見や経験に基づき、PKI の相互運用における様々な問題を多角的にとらえ、解決手段を探るプロジェクトであった。

Challenge PKI 2002 プロジェクトでは、政府認証基盤（GPKI）の相互運用性を確保することに焦点をあてた。GPKI は広範囲な認証ドメインの顕著な構築例であり、PKI 相互運用の解決策を探るためには格好のターゲットでもあった。

一方、GPKI を認証基盤とした電子政府の成功の鍵のひとつとして、使いやすくセキュアな電子政府対応アプリケーションの流通が挙げられる。しかし、いざソフトウェアベンダーが GPKI に対応したアプリケーションを開発しようとしても、現状では色々な困難に遭遇すると思われる。それは、開発をする上で参考となる実装がない、テスト環境や開発環境がない、テストの方法が分からない等、そのほとんどは GPKI の高度な相互運用技術に由来する課題であると考えられる。GPKI の相互運用性を確保することで、GPKI に対応した電子政府アプリケーションの開発を促進することになり、結果として、GPKI を基盤とした広範囲なセキュリティを適正なコストで実現することができると考えられる。

Challenge PKI 2002 プロジェクトでは、以上に述べたとおり、GPKI の相互運用性の技術的な課題や、アプリケーション側での問題を解決することを大きな目標とした。プロジェクトでは、GPKI 相互運用性仕様書に準拠したアプリケーションの開発を促進するために、以下の成果物を作成した。これらの成果物全体を PKI 相互運用フレームワークと称している。

① GPKI の仕様の根拠となる標準の説明した報告書
② GPKI の開発環境
③ GPKI のテスト環境
④ GPKI のテストケース
⑤ GPKI に対応したパス検証のリファレンス実装

Challenge PKI 2002 プロジェクトにおいて中心的に扱った相互運用性の技術課題は、リライングパーティ（署名検証者）側における相互運用性、すなわち認証パス検証に関連した相互運用性に関するものであった。これは、おそらく PKI の相互運用を扱う上で最も高度かつ困難な課題である。認証パス検証は、リライングパティ側にとっては必須の機能であるため、ほとんどの電子政府アプリケーションにおいて実装されると考えられる。

これまで、PKI アプリケーションにおける認証パス検証機能は、X.509 や RFC3280 といった標準のサブセットに準拠した形で実装されてきた。標準のサブセットは、あくまで一部分を実装しただけのものであり、標準で想定されるどんな状況にも対応できるわけではない。特に電子政府のように広い PKI ドメインにおける認証や、更に様々な用途に応じた認証を行おうとした場合、認証パス検証は難易度を増す。

日本に限らず、各国の電子政府は、これまでにない広い範囲での認証が要求されている。すなわち PKI の標準に対しても、これまでにない要求が必要になるか、もしくは、これまでは実装・使用されていなかった部分が使われることになる。今回、標準で想定される様々な状況に

対応可能な PKI 相互運用フレームワークを作成したことで、国や地域などをまたがる広範囲な認証基盤における PKI アプリケーションの実現可能性が大いに増すことを期待できる。

(5) IETF での活動

Challenge PKI 2001、Challenge PKI 2002 などのプロジェクトを通して、標準化に対して何らかの関与する必要性が明確になってきた。こうした中、日本で初めて開催された 54thIETF 横浜においてプロジェクトの紹介を行ったのをかわきりに、プロジェクトの成果の発表、そして、これまでの成果から生まれたインターネットドラフトの発表等を IETF PKIX WG において行ってきた。以下に、IETF での活動の履歴を示す。

54th IETF 横浜での発表　-　2002 年 7 月 17 日
ChallengePKI2001 の成果の発表
http://www.jnsa.org/mpki/ChallengPKI2001-IETF-PKIX.pdf
http://www.jnsa.org/mpki/Interoperability_mPKI.pdf

55th IETF アトランタでの発表　2002 年 11 月 17 日
Challenge PKI 2001 で明らかになった問題点など報告
ChallengePKI2002 の紹介
http://www.ietf.org/proceedings/02nov/slides/pkix-5.pdf

56th IETF サンフランシスコでの発表　2003 年 3 月 20 日
ChallengePKI2002 の成果の発表
開発した相互運用テストスィートのデモ
http://www.ietf.org/proceedings/03mar/slides/pkix-2.pdf

57th IETF ウィーンでの発表　2003 年 7 月 17 日
インターネットドラフト Memorandum for multi-domain PKI Interoperability を発表
http://www.ietf.org/proceedings/03jul/slides/pkix-9/index.html

Challenge PKI プロジェクトでは、今後も、IETF のセキュリティ分野での標準化活動の一翼を担う活動を続けることを計画している。

(6) 今後の展開

Challenge PKI プロジェクトは、２年間に渡り PKI の相互運用に関する活動を行ってきた。

こうした活動の中で、海外との関係が急速にクローズアップされている。PKI の相互運用性の問題を取り上げて行く中で、数多く海外の動向・状況を調査し、プロジェクトの成果を IETF にフィードバックするといった普及・啓発活動を行ってきた。こうした取り組みの中、我々が注目している課題の多くに対して、海外でも同じような認識と取り組みがあることが徐々にわかってきた。

IETF などの標準化自体も様々な課題を抱えている。特に、複雑なセキュリティに関する標準化に関して行き詰っている側面が見受けられる。これにはいくつかの問題があるとおもわれるが、その中でも、IETF の標準化の基本的なコンセプトである「ラフ・コンセンサスとランニング・コード」だけではセキュリティの標準化は難しいということが挙げられる。こうした中で、標準化のプロセス自体として、標準・仕様作成と相互運用仕様やテスト仕様の作業を同時に進行させるための相互運用フレームワークが必要である、というのが現在の我々の結論のひとつである。すなわち、Challenge PKI 2002 プロジェクトのようなプロジェクト自身が標準化と同期して実施されるべきだと考えている。相互運用テストと標準化文書の作成、そしてランニングコードの作成は同時並行に進み、ランニングコードは、標準に対する準拠性テストにより評価されることが重要である。現在では、間違いなく、相互運用テストがなされていない、いい加減なランニングコードが標準化を阻害している。

ドッグイヤー時代の標準化は、ITU や、ISO/IEC などの標準化プロセスよりも、IETF のような組織の標準化プロセスが受け入れられる傾向にあったが、現在は、相互運用性の確立まで含んだ、更に新しい標準化スキームが求められているように感じられる。PKI の相互運用に対する上記のような取り組みは、米国 NIST や欧州の ETSI などといった広範囲に電子署名、電子認証を推進して行くミッションを持った組織において行われているように思われる。今後は、こうした海外の組織とも連携をはかっていくことが重要だと考えている。

PKI に限らず、基盤技術の相互運用を促進するためのプロセスや組織のあり方の重要性なども、もっと認識されるべきだと思われる。暗号技術等をネットワーク社会に生かすためのアイディアを論文などの文書にまとめる作業は多くの研究者などが行っている。こうしたアイディアの極一部が、標準化された技術となり、そして、この標準を実装した製品の開発などは企業等においてが行っている。しかし、これらの標準技術を幅広く展開し、真に IT 社会の基盤とするためには、相互運用性を確保するための努力が欠かせない。しかし、実際には、多くの場合、こうした相互運用を推進するプロセスは確立していないように思われる。例えば、日本の電子政府においても、電子政府のアーキテクチャを確立して相互運用を推進している組織はなく、ばらばらの実装がなされているのが実情に見える。

これまでのプロジェクトを通して、もうひとつ重要だと認識したことにセキュリティフレームワークや、それを実現するためのミドルウェアの重要性がある。最終的には、業務アプリケーションなどからは、複雑な相互運用技術を隠蔽する必要があり、何らかのセキュリティレイヤのミドルウェアが、実行時のネットワークの信頼と複雑な相互運用の問題を吸収する必要がある。

Challenge PKI プロジェクトは、PKI を IT 社会における真に基盤とするため、標準化への新たな取り組み、相互運用を推進するためのフレームワーク作り、そして、セキュリティフレームワークとミドルウェアのあるべき方向性などをテーマに今後の活動を計画している。

4．日本の電子署名認証推進・活用団体の活動紹介

4.1 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。17,500 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 c.簡易裁判所における民事事件の代理関係業務など）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基礎研究として取り組んできた。

近年は IT 化対策への具体的な対応のため執行部内に高度情報化対策部（平成 11 年から 15 年まで）、基盤整備対策部ならびに総合情報システム対策部（平成 15 年から）を設置し、担当副会長以下理事・部員を配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

＊上記は債権譲渡登記に対応するための限定機能の電子認証システムであるので、現在は、今年度から施行予定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から、電子署名法の特定認証業務の認定を受け、GPKI のブリッジ認証局との相互認証が可能となる電子認証局の構築を準備中であり、2004 年 6 月以降には稼動予定。

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きた。

・「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つき提言をしてきた。

C.基盤整備対策部

2003～2004

・「電子認証局構築ワーキングチーム」

平成 16 年 6 月から施行予定の商業法人登記のオンライン申請ならびに平成 17 年 3 月に施行予定の不動産登記のオンライン申請に対応するため、専門職代理人として司法書士の資格属性を証明する「日司連電子認証局」を電子署名法の特定認証業務認定を受けかつ政府のブリッジ認証局との相互認証の認定を受けるものに再構築するため基盤整備対策部内に専門のワーキングチームを設け、具体的な構築を担当している。電子証明書は、将来的には会員証を兼ねるものにすることも視野に入れ IC カード化することにして

いる。

D．総合情報システム対策部

2003～2004

連合会と全国 50 単位会と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、ならびに役員・委員のスケジュール管理・情報伝達、テレビ会議システムの導入、全国会員への情報通信網の構築を行っている。

事務局内部の個々の事務処理はかなり早くからコンピュータ化されてきているが、それぞれのシステムの統合化を図るため再構築の検討準備に入っている。

役員・委員総数 300 名余りのイントラネット構築を行い理事会はじめ各種委員会等の日程管理、会議資料の前送・保存、ネット会議等に活用。

全国会員の義務化研修のスケジュール、申し込み、単位取得の集計等のための研修システムを構築。

今後は、会員登録事務のネットワーク（Web）利用による一元化を図るための準備を進めている。

(3) 連絡先

日本司法書士会連合会

基盤整備対策部、総合情報システム対策部

担当副会長・対策部長 佐藤純通 jun2@ss.iij4u.or.jp

事務局担当職員　小野寺課長　hiroyuki.onodera@nisshiren.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

4.2 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 67，331 人

税理士法人会員 606（2003 年 11 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 接続した税理士の認証局を 2004 年１月に構築して、２月２日からの名古屋国税局管内の電子申告に取り組む税理士に電子証明書を発行している。税理士全員に電子証明書を発行する体制を整備している。

(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

4.3 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

27,805 名（2003 年 11 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なく、法律家として労働社会保険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た厚生労働省での電子申請受付業務に対応して、当会では、特定認証業務の認定を受け総務省ブリッジ認証局と相互認証を交わす士業界初の認証局を 2003 年 9 月 24 日に開局した。

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および研究会参加

（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）

・特定認証業務認定取得（2003 年 6 月 10 日）

・総務省ブリッジ認証局相互認証（2003 年 9 月 22 日）

・組織体制（電子化委員会）

(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：03-3813-4589　FAX：03-3813-4589
MAIL：河端　祐一　kawabatayu@shakaihokenroumushi.jp

4.4　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

37,654 名（2003 年 11 月 30 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。行政書士会の会員の品位を保持し、その業務の改善進歩を図るため、行政書士会及びその会員の指導及び連絡に関する事務を行うとともに、行政書士の登録に関する事務のほか、行政書士業務に係る調査・研究・推進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。

その後、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、新たな状況に対応するため、2003 年２月に一旦廃止し、次段階への準備を進めてきた。その結果、日本商工会議所とのタイアップにより、当会議所より発行される「ビジネス認証サービスタイプ１-Ｇ」の電子証明書を、当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とし、2004 年２月にもサービスの提供を開始するに至っている。

［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）

・「電子的代理申請・電子委任状研究会」報告書（2002.8）
・「電子申請研究会」報告書 ～代理申請、商取引公証基盤～（2003.3）

(3) 連絡先

日本行政書士会連合会
MAIL：黒川　久男　ngr-h-kurokawa@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　中西　豊（高度情報通信社会対策本部委員）
MAIL：fwjc6972@mb.infoweb.ne.jp

4.5 電気事業連合会

(1) 団体名／Web アドレス

電気事業連合会（http://www.fepc.or.jp）

(2) 設立年月日・会員規模

1952 年（昭和 27 年）11 月 20 日
会員　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

(3) 主な活動

電力業界大の情報高度化については、従来から EDI におけるビジネスプロトコルの標準化、業界共同データベースの構築及びソフトウェアの流通・共同開発など、共通課題の解決に取り組んできた。また、平成１３年に政府 IT 戦略本部が決定した「e-Japan2002 プログラム」で重点施策の一つに挙げられた“行政情報化の推進”を受け、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。

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、直接又は日本経団連を通じて、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。日本経団連に於いては、電気事業連合会の要望を含めて「２００３年度日本経団連規制改革要望」の中で、本件に関する提言を政府総合規制改革会議等関係機関に対して行っている。

(4) 連絡先

情報通信部　副長　浜田　誓
hamadas@fepc.or.jp　Tel（03）3279-3744　Fax：(03) 3270-8085

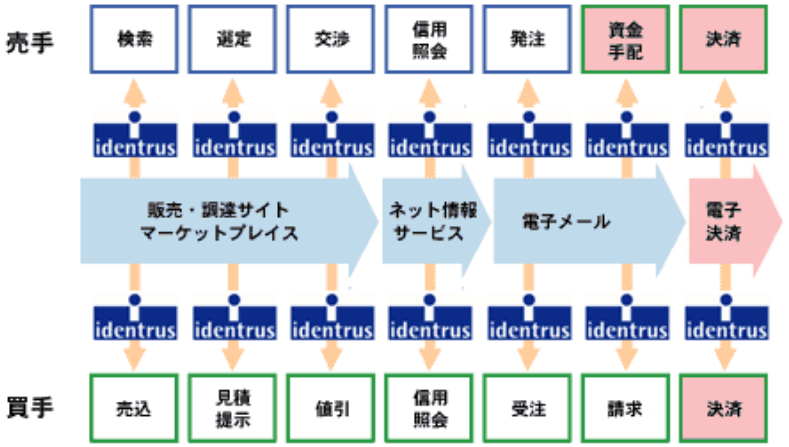
電気事業連合会
〒100-8118　東京都千代田区大手町１丁目９番４号　経団連会館

4.6　アイデントラス電子認証

(1) アイデントラス電子認証とは、

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）は、『世界共通の電子認証規格』を実現するために 1999 年 3 月に欧米の金融機関[1]が設立したアイデントラス社（Identrus，LLC 米国デラウェア州法に基づいて設立された有限会社）が推進する電子認証スキームであり、国際的な電子認証スキームである。

■ 電子商取引における銀行の新たな役割



その設立の目的は、インターネットにおける B2B 電子商取引を安全に行うために、銀行が企業の間に立って、『信頼される第三者』としての機能を提供しようとするものである。銀行が本来持つ『信用』を背景に、従来、商取引の一部でしか利用されていなかった『与信』『保証』の機能を、電子商取引の全ての場面で、生かすことができ、これにより、企業と銀行の新しいビジネス機会を創造することを狙いとしている。

アイデントラス認証スキームは、ベンダー中立なスキームであり、標準化されたの法的、技術的ルール（IC カードの仕様、本人確認基準等）の下に成り立っている。スキームの中心となるアイデントラス社は以下の役割を担っており、デジタル証明書が統一的なポリシーのもと発行されることを担保している。[2]

① 加盟金融機関共通の『認証局運営ルールを制定』
② 世界標準の技術に基づく『システム要件の策定』
③ スキーム、製品間の 『整合性の監視』

これにより、例えばアイデントラス電子認証を採用したマーケットプレースは、どの加盟金融機関から発行されたアイデントラス証明書であっても、顧客の認証手段として利用することができる。一方、顧客は Web サイト毎にデジタル証明書を保有する必要はなく、一枚の

1 ABN AMRO Bank, Bank of America, Bankers Trust (現 Deutsche Bank), Barclays, Chase Manhattan, Citigroup, Deutsche Bank , HypoVereinsbank の８行の出資により設立。現在、当スキームには 60 以上の金融機関(うち邦銀４行)が参加している。

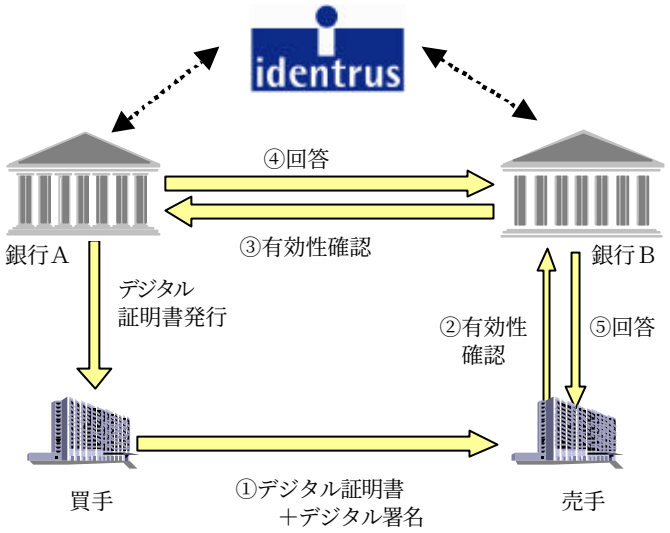
2 顧客サービスを開始した銀行は、毎年アイデントラス社の定めるガイドライン(Compliance & Control Assessment Guideline)に基づき監査を実施し、アイデントラス社に報告する義務がある。

アイデントラス証明書だけで価格交渉、受発注、決済といった商取引の様々な場面で安全に電子商取引を行うことが可能となる。

(2) アイデントラス認証モデル

アイデントラス・スキームでは、アイデントラス社と契約した金融機関（加盟金融機関）が運営管理する認証局が企業に証明書を発行し、さらに最上位にあるアイデントラス社のルート認証局が加盟金融機関に対して証明書を発行するという、階層型の信頼モデルが採用されている。

アイデントラス認証を特徴付けている基本的な仕組みは「４者間（４コーナー）モデル」と呼ばれている。そこでは、以下のような流れで、認証が行われる。



① 買手企業が売手企業にインターネットで物品購入の発注をする場合、デジタル署名とともに、買手企業は自分の取引銀行（銀行Ａ）から受けた証明書を同時に送る。

② 売手企業はその証明書が現在も有効なものかどうかを、自分の取引銀行（銀行Ｂ）に問い合わせる。

③ 銀行Ｂは、銀行Ａに、その証明書の有効性を問い合わせる。

④ 銀行Ａは、証明書の有効性を確認し、銀行Ｂに回答する。

⑤ 銀行Ｂは、売手企業に証明書の有効性を回答する。

銀行Ａと銀行Ｂ間メッセージには銀行が署名を行う。銀行の証明書の有効性については、銀行間メッセージのやりとりの都度、アイデントラス社のルート認証局が確認する。

(3) アイデントラス認証の利用例

これまで目立った利用実績がなかったが、昨年より一部の先進的な銀行で、アイデントラス認証を活用した顧客サービスを開始している。

例えば、UFJ 銀行は 2003 年 9 月、アイデントラス認証を使用して一部既存取引先企業との融資契約（金銭消費貸借契約等）を電子化するサービスを開始した。このサービスでは、UFJ 銀行が提供するシステムに顧客企業がインターネットでログインし、融資契約書にデジタル署名する仕組みである。電子契約書はサーバに保存され、顧客はいつでも保存された電子契約書を参照することができる。

また、海外では、ロイヤル・バンク・オブ・スコットランドがアイデントラス認証を利用した TrustAssured サービスを提供し、このサービスを採用したリース会社がリース契約の電子化を行っている。

今後、本格的な B2B での利用が期待される。

4.7 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 4-1 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 4-1 認証公証 WG 成果報告書/ガイドライン

1996～1999	2000～2001	2002
(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 (4)電子署名プログラム Protection Profile (5)証明書利用形態に関する考察 (6)電子署名文書長期保存に関するガイドライン	(1)属性認証の適用ガイドライン (2)電子認証利用形態に関する考察 (3)タイムスタンスサービスに関するガイドライン

(3) 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、検討を行っている。

① 電子認証システム仕様検討

・SAML による利用モデルの検討

② 属性情報利用検討

・属性情報を利用した認証システムを検討する際のガイドラインの作成

③　電子署名文書長期保存

・署名ポリシー

・長期保存におけるデータの保存性・見読性の利用者の視点での検討

(4) 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

4.8 電子商取引推進協議会（ECOM）：電子行政・ビジネス連携 WG（旧電子政府 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。

電子行政･ビジネス連携 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。

・政府ポータルのワンストップ化実現のための共通フレームワーク検討

・目的別行政関連ポータルモデルの検討

・官民連携ポータルビジネス促進のための共通基盤の整備

①　今年度の活動

今年度は、2 つのサブワーキンググループを立ち上げて活動を行っている.

・電子行政推進 SWG

政府ワンストップポータル実現のための共通フレームワークについて,特に経済産業活動に密接な関係を持つ「ビジネス総合サイト」をターゲットに、構築に向けた具体的なフレームワークの定期を活動の目標としている。

・電子行政関連ビジネス検討 SWG

目的別行政関連ポータルモデルの検討と、これらポータルを官民連携によって創設するために必要な要件の提起を目標としている。

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-
「電子政府活用に向けた提言　ビジネスと行政の連携の視点から」(2002 年度成果)

(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

4.9 日本 PKI フォーラム

(http://www.japanpkiforum.jp)

所在地　　143-0016 東京都大田区大森北１－２３－５　第一小田ビル
組織概要　アジア PKI フォーラムの活動を推進する日本国内の組織

(1) 組織概要

日本 PKI フォーラムは、アジア PKI フォーラム（アジアの PKI 推進機関、2001 年 6 月発足）の活動を推進する日本国内の組織として、2000 年 12 月に発足した。会員は現在約 80 社・団体となっており、企画部会、検討部会への参加を通じてフォーラムの活動に参加している。日本 PKI フォーラムは、アジアの国・地域が協力して PKI の相互運用性の確保や普及活動を行うことにより、アジアの電子商取引の活性化及び日本国内における PKI を利用したビジネス・アプリケーションの利用・促進を目標としている。

(2) 活動概要

① 検討部会活動 (a)ビジネス・アプリケーション検討部会

国内ならびにアジア／オセアニア各国の関係企業と連携をとりつつ PKI ビジネス／アプリケーションの典型的なケースの立ち上げについて特徴の分析・課題の検討・提言を行う。

(b) 相互運用技術検討部会・国際的相互認証実証実験

各国・地域間での認証局の連携の実現に向け、アジア圏共通の PKI に必要な技術的要件を抽出・調査することにより、アジア各国・地域での国際的な電子商取引の基盤整備を目指す。また今後各国・地域で実現されていく国際的な電子申請、電子通関、貿易金融 EDI、SCM、e-Marketplace など、電子政府から民間までの各種アプリケーションについて、PKI を利用する上での技術的、制度的、および運用面での課題につき検討・提言を行う。

また、インターネットを利用して国際的な電子商取引や電子情報交換を行う際の信頼性確保の基盤として、PKI による認証構造の整備が各国・地域で進められている。実証実験では、このような国際的な視野での PKI の適用を検討するにあたり、各国・地域の相互接続性を確認する。

(d)国際連携 アジア PKI フォーラムは、アジア域内における PKI の相互運用性の確保や PKI の普及活動を展開している。PKI の相互運用性の確保や普及は全世界共通の目標であり、

活動成果はアジア地域内に留まらず、広く世界規模に発展する事が期待され米国、欧州の国際組織との相互連携も極めて重要な活動となっている。日本PKIフォーラムはアジアPKIフォーラムの国際連携活動推進の議長国として、国際機関との連携を積極的に推進している。

(e)会員セミナー他

会員サービスの一環として会員からの要望を反映したセミナーを定期的に開催している。また会員向け国内・海外の PKI 関連情報を HP 上に提供している。

(3) 最近のトピックス

(a) 国際的相互認証実証実験

日本 PKI フォーラムは、アジア地域での PKI を利用した電子商取引の普及拡大のための基盤整備を推進するため、2001 年から経済産業省の支援を得て、アジア圏の中で PKI の整備が進んでいる韓国、シンガポール、およびチャイニーズ台北とともに PKI の相互接続に関する実証実験を行い、証明書・CRL の標準プロファイル、証明書パス検証に関するガイドライン、署名用トークンインターフェイスの共通仕様について報告書を発表している。また、実験の成果をアジア PKI 相互運用ガイドラインとして取り纏め中である。本ガイドラインの実ビジネスへの適用を目指し、PAA（Pan Asia e-commerce Alliance）と協同作業を行うことについて合意した。

（概要：http://www.japanpkiforum.jp/shiryou/exp02_rep_smr.pdf）

(b) PKI 関連サービスビジネスの動向に関する調査

欧米の PKI 先進国を調査対象として、社会性、経済性、地域性に基づいた PKI の活用事例と課題、解決に向けた取り組みを分析するとともに、日本・アジア諸国・地域との比較を行った。またこれらの分析結果に基づき、日本・アジア諸国にも適用可能と思われる PKI 普及・発展シナリオについて考察した。

（概要：http://www.japanpkiforum.jp/shiryou/biz02_rep_smr.pdf）

(c) 国際連携活動

欧州における電子署名標準化団体である EESSI は、アジアとの整合性を目指し、情報交換や標準案に対するコメントの提供に積極的な姿勢を示しており、アジア PKI フォーラムもそれに応えるべく、コミュニケーションを密にしている。一方米国を中心とした e ビジネス標準化団体 OASIS とも PKI の相互運用性や普及促進に向けた協力関係の強化について具体的なアクションプランを策定中である。

4.10 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

３４社

(2) 主な活動と成果

電子政府・電子自治体の実現に向けて、オンライン申請のモデル像や標準化技術などを民間レベルで協議・提言していくことを目的とした任意団体である。

ソフトウェアベンダー、ハードウェアベンダー、システムインテグレーターから印刷、出版業界にいたるまで幅広い企業が参画しており、ご後援いただいている学会等の知識層や行政への申請業務に深く関わっている各代理業の諸団体とのコラボレーション、さらに中央省庁や自治体とのコラボレーションを通じて、利用者にとって真に使いやすい電子申請の早期実現を目指す。現在、次の委員会、WG 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。

■電子申請インフラ委員会

使いやすくセキュアな電子申請の普及を目指し、基盤となる UI（ユーザインターフェース）、ハンドリングする XML データの構造（タグ）、及びセキュリティについて検討・提言をしていく委員会。

また、各種実証実験やプロジェクトと連携し、実用途での検証も行う。WG として以下のものがある。

【セキュリティ WG】

急速に普及しているセキュリティポリシー。しかし、その運用を助けるセキュリティ実装は理解されているでしょうか？

セキュリティ WG ではセキュリティポリシーの運用を助けるセキュリティ実装の具体的な提案をテーマに、実証実験への参加による実装と運用・結果報告や、セキュリティガイドマップの作成、セミナーによる普及活動等を行う。

【UI＆タグ検討 WG】

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利用者の状況に応じて適切なガイダンスが受けられる UI（ユーザーインターフェース）を目指して検討・普及と、複数の UI で共用する XML データの共通化を推進する WG。

■ビジネスモデル委員会

体系的な電子申請システム・ソリューションを構築し、電子自治体実現に向けた地方自治体に提供する。電子申請システムを核とするビジネスモデルを創出し、地域ベンダーの産業振興に貢献していく。

■登記オンライン申請検討委員会

司法書士の皆様と連携して、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する。

■実証実験推進 WG

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。

■成果物

異なる PKI システムでの電子署名相互認証の実現（2001 年 8 月）
セキュリティマップの公開（2002 年 5 月）
債権譲渡登記オンライン申請システムに対する提案書（2002 年 5 月）
商業登記オンライン申請システムへの提案書（2003 年 3 月）
電子申請におけるユーザーインターフェースガイドラインの公開（2003 年 3 月）
『インターネット電子申請』発刊（2002 年 6 月）
不動産登記オンライン申請システムにおける連件処理に関する提案書（2003 年 8 月）
岐阜県行政書士会・岐阜県との電子代理申請実証実験報告書（2003 年 8 月）
岐阜県電子申請実証実験報告書（2004 年 1 月予定）

(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
Mail：info@e-ap.gr.jp

4.11 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) 設立の経緯

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（NPO Japan Network Security Association：JNSA）は、2000 年 4 月に任意団体として活動を開始した。社会インフラとして、インターネットを中心にした情報ネットワーク社会が形成されていく中で、ネットワーク・セキュリティは、必要不可欠のものになって行くはずである。セキュリティとは、「何か」、「誰が」、「どこまで」、「責任」をもつのか、その責任の保証範囲などは、まだ社会のコンセンサスが取れていないのが現状であった。それ以前にネットワーク・セキュリティとは、一体、何かということにおいても、様々な認識があるという状況を鑑み、ネットワーク・セキュリティ製品を提供しているベンダー、システムインテグレータ、インターネットプロバイダーなどネットワークセキュリティシステムに携わるベンダーが結集して、ネットワーク・セキュリティの必要性を社会にアピールし、かつ、諸問題を解決していく場として、JNSA が設立された。

最初の 1 年間の活動を踏まえて、内閣府へ NPO の申請を行い、7 月 12 日に NPO-JNSA としての移行を行う総会を開催し、正式に NPO としての活動を開始し、2004 年 2 月現在で会員数 181 社となっている。ネットワークセキュリティが想像以上の早さで身近な問題となる中、NPO としてJNSAが情報化社会へ貢献するのがこれからの命題である。これを実現するために、次のような活動を柱としている。

- 調査・研究活動
- 普及・啓発活動、情報提供
- セキュリティ技術者教育関連
- セキュリティに関する基準策定や認定
- 関連他団体との連携、国際協力
- 情報公開の推進

JNSA としての活発な活動を支えている、いくつかの特徴がある。

1.WG などの成果(報告書など)は、原則公開する。

2.実際の運営は、WG リーダーに任せる。

3.事務局は技術スタッフも擁し、WG などの活動を全面的に支援する。

これらは、実際の活動を行っていく中で、必要に応じて実現されていった面も多々ある。特に、成果物の公開は、参加するメンバーが実際に開発や営業などに使う際、非公開のものを内緒で見せられるよりは、私の所属している JNSA でこういう資料が公開されているので、ぜひご覧になってください、という方が、使いやすいし説得力もあるということで、割に自然に受け入れられたと思う。これは当初からの目的でもあったが、現代においては、人が知らないことを秘密にしておいて優位性を保つ時代ではなく、後から後から新しい情報を出すことの方が、優位性を維持できるということでもある。秘密を守るということは何か、という根源的なテーマを含んでいるが、技術的な問題や提案は、積極的に情報公開して、英知を集めて解決するのが、望ましい方向だということができる。

(2) 主な活動内容と成果

JNSA は、各部会毎に WG（ワーキンググループ）に分かれて活発な活動を行なっているが、成果物は基本的には公開情報とされていて、ダウンロードしてご利用いただける。ぜひご活用いただきたい。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、であるが、2004 年度は 2 月時点で総計 21 の WG が活動している。詳細は、http://www.jnsa.org/を参照して欲しい。

次に PKI 関連の活動を紹介しよう。これだけではないので、ぜひ実際の活動に参加してみていただきたい。

★★★――――――――――――――――――――――――

国際標準への貢献と活動

――――――――――――――――――――――――★★★

技術部会の PKI 相互運用技術 WG が中心になって、ChallengePKI プロジェクトが活動している。2001 年から 2002 年、2003 年と PKI に纏わる問題を実証実験し報告書にまとめて指摘してきている。独立行政法人 情報処理推進機構セキュリティセンター（IPA/ISEC）からのご支援の下、Challenge PKI 2001 年では、PKI の中核となる CA（認証サーバ）の相互運用性を 9 種類の CA について調査し、規格に明記されていない部分の実装の違いなどの問題を指摘した。特に multi domain 環境での問題については、報告書を英訳し国際的な議論を始めた。

翌年の Challenge PKI 2002 では、PKI アプリケーションを作る際のテスト環境を自由に作り出すためのテストベッドとテストスィートを開発した。これを使えば GPKI を含めた PKI 環境をエミ

ュレートでき、アプリケーションの開発環境が手軽に利用できるようになる。このソフトとデータはオープンソースとして公開され、ダウンロードして自由に利用できるようにした。

ChallengePKI 2003 では、更にタイムスタンプの技術的な調査と評価と ChallengePKI 2002 で開発したテストスィートにタイムスタンプの処理機能を組み込むと共に、政府と民間に対して実際にタイムスタンプへの期待や要求などをヒアリング調査し、これからの電子社会で必要となる機能について提言を含む報告書を作成した。更にソフトウエアを開発する際に重要となるセキュリティ API についても調査報告書を作成すると共に、サンプルプログラムを Windows 環境（CriptAPI）と Java 環境で作成し、これもオープンソースとして公開した。

ChallegePKI で得られた知見は、IETF（The Internet Engineering Task Force）へも報告し、multi domainPKI に関するインターネットドラフトの提案も行っている。PKIX-WG を中心にしたこの活動は大きな注目を集め、国際的にも規格の充実が認識され、新たな WG を作った方が良いのではないかという議論まで出てきている。また、米国の NIST や欧州の ETSI などとも連絡を取り合っており、PKI 関連の相互運用技術や標準化のレビューなどの相互協力を行っていく予定で活動している。これらの PKI 関連の活動は、下記の URL にまとめられているので、こちらをぜひ参照して欲しい。http://www.jnsa.org/mpki

◆◆◆ JNSA の課題 ◆◆◆

最後に、JNSA の今後の課題を考えてみたい。たくさんの課題があるのは間違いないが、その中からいくつかあげてみよう。

- ビジネスマーケットの形成
  基礎データの情報公開など
- 国際的な連携と標準化の貢献
  IETF（multi-domain-PKI）への参加など
- 脆弱性情報の取扱や周知に関する活動
  経済産業省や IPA などとの連携
  JNSA と TelecomISAC との協調活動
- 標準や製品の相互運用性の実証実験
  PKI 相互運用性実験
  無線 LAN の相互運用性
  IPv6 の IPv4 からの移行に関する実証実験
  電子政府関係の実証実験
  PKI アプリケーションのモデル開発
- サンプルポリシーの公開
  電子署名や暗号化への対応
- IT セキュリティ技術者教育
  スキルや評価方法に関する議論など
- 全国セキュリティ啓発キャラバン
  CD-ROM 作成

• 日本セキュリティ監査協会との協力関係

などなど、まだまだたくさんテーマがあるが、ここに全てを書き切れない。ご興味やご提案などがあれば、ぜひご連絡をいただきたい。ご一緒に活動できることを期待している。

(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　（JNSA）事務局
〒136-0075　東京都江東区新砂 1-6-35　T.T.ランディック東陽町ビル
TEL 03-5633-6061　FAX 03-5633-6062　sec@jnsa.org

4.12 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（JPNIC）

Japan Network Information Center（JPNIC）（http://www.nic.ad.jp/）

(1) 設立年月日／会員規模

1997 年 3 月　設立
318 会員（2004 年 2 月現在）

(2) 主な活動と成果

① 事業内容

国際的な運用・管理が必要とされる IP アドレス等のアドレス資源の管理、インターネットに関わる各種調査・研究や教育・啓発活動等を行っている。

（ｉ）IP アドレス事業

IP アドレスは IANA（Internet Assigned Numbers Authority）を頂点とする階層構造のインターネットレジストリによって管理されている。当センターは、日本における IP アドレスの管理を行っており、ISP（Internet Service Provider：インターネットサービスプロバイダ）に対する割り振りを行っている。

（ii）ドメイン名事業

ドメイン名に関する情報センター業務をはじめ、JP ドメイン名紛争処理方針の策定など各種 JP ドメイン名に関する業務を行っている。

また国際的なドメイン名管理のルール作りへの参加・協力なども行っている。

（iii）インターネット基盤事業

ENUM や IRR（Internet Routing Registry）をはじめ、様々なインターネットの基盤技術および運用に関する調査・研究と教育・啓発活動を行っている。

この他に、InternetWeek をはじめとするイベントや研究会の開催や共催を行っている。

② 電子署名・認証に関する活動

電子署名・認証の分野については、2002 年度下半期より調査研究を開始した。経済産業省より「IP アドレス認証局に関する調査研究」を受託し、インターネットレジストリにお

ける認証局と認証業務のあり方をはじめ、IP ネットワークの安全性に関する調査研究を行っている。この調査研究は 3 年間を予定しており、この期間に、あり方の調査、構築のための調査と方針策定、応用に関する調査と構築・実験等の活動を行う。

- 認証局のあり方と認証業務に関する調査

  国際的な地域インターネットレジストリである APNIC（Asia Pacific Network Information Centre）や RIPE NCC（RIPE Network Coordination Centre）における認証局の動向調査や、IETF（Internet Engineering Task Force）における情報交換を行っている。

- 認証技術と方針策定に関する調査

  CP/CPS（Certificate Policy / Certificate Policy Statement）策定や認証業務の検討のため、認証局監査に関する調査や、認証局と X.509 形式の証明書を扱うシステムに関する検討調査を行っている。

- 認証情報と IP ネットワークの活用に関する調査

  IP を用いたネットワークの分野の拡大に伴い、各種の利用分野におけるネットワークの安全性を検討することが課題となっている。安全性の確保の為に、当センターの認証局と認証情報を活用する手法について調査研究を行なっている。

調査研究の成果は各年度に、調査報告書としてまとめられる。またこの調査報告書は一般に公開され、調査・検討内容に関して議論できる資料となることも目指している。

電子署名・認証の分野においては、調査研究に関する発表や情報交換を通じて、技術および運用に関する知見が集約されることを目指している。

なお、「IP アドレス認証局のあり方に関する報告書（2002 年度実施）」は、JPNIC の Web（http://www.nic.ad.jp/ja/research/index.html）より入手可能である。

(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

4.13 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

（ⅰ）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

（ⅱ）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
- 遠隔医療システムの開発
- 認証局システムの開発・運用

（ⅲ）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
- IHE 等マルチベンダー医療情報システムの開発

（iv）介護情報システムの基盤技術の開発と普及

（v）コンサルテーション

（vi）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「医療用公開鍵基盤ガイドライン V1.0」および、その付属文書として、「ヘルスケア PKI 認証局証明書ポリシーV1.0」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」を実施した。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 のみを自地域におき、認証センターの IA を共有する場合が混合したモデル地域の参加を得て、実運用に近い形で構築・運用し、今後の保健医療福祉 PKI 構築の検討をおこなった。

平成１５年度はフイールドを公募し４件を採択し、今後のモデルシステムとして認証局の利用面を含め、ヘルスケア PKI の認証局運用の評価を実施している。

(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

sysad@medis.or.jp

4.14 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

4.15 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 18 社

(2) 主な活動と成果

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。

（ｉ）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。

◆次世代 Web コンピューティング技術

◆ユビキタスネットワーキング利用技術

◆ビジネス継続性技術

◆システム運用管理の相互運用性技術

（ii）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。

◆インターネット利用技術

◆Web サービス性技術

◆オープン分散処理システムのモデリング技術

（iii）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、分散システムのモデリング技術等の標準化

◆システム運用管理技術

（iv）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

（ｖ）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 PKI、セキュリティ関連活動

（ｉ）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）

（ii）「情報セキュリティに着目した電子自治体向け iDC 利用ガイド」を作成し、iDC イニシアティブと当協会の共催でセミナーを実施した。（平成 15 年度）

（iii）「Web サービス相互運用技術の調査研究報告書」を作成し、その中で Web サービスセキュリティに関して、Web サービスセキュリティ・モデル、サンプル・メッセージ等の調査、検討を行った。（平成 15 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）

4.16 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県の自治体、広域経済団体など 57 企業・団体
（2004 年１月現在）

(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。

・セミナー、公開勉強会の開催状況　2003 年 2 月（開催地：仙台市）
2003 年 6 月（同仙台市）
2003 年 10 月（同秋田市）
2004 年 2 月（同札幌市）

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。

・活動中の部会、研究会　電子認証普及促進部会
ビジネスモデル研究部会
次世代技術による住民指向型 WEB サービス研究会
地域多目的 IC カードの検討研究会
企業向インターネットサービスモデル研究会
行政モデル研究部会

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

4.17 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 ４６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、総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 日本で始めて当組合 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

4.18 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。

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

4.19 電子署名・認証センター（ESAC）

電子署名および認証業務に関する法律（略して電子署名法という）の施行に先駆けて平成１２年７月に財団法人日本情報処理開発協会に設置された。以降電子署名・認証に係る普及啓発活動を行っているが、平成１５年５月に電子署名法が定める指定調査機関の指定を受けて特定認証業務の認定に係る実地の調査をあわせて行っている。以下にそれぞれの活動内容を紹介する。

(1) 電子署名・認証に係る普及啓発活動

広く一般国民に対し、電子署名・認証についての普及啓発活動を展開することにより、電子署名・認証についての知識を広め、電子商取引等における電子署名・認証の利用促進を図ることを目的としている。

具体的には、オンラインオークション等のオンラインショッピングの利用者である消費者、オンライン電子申請等電子政府システム、企業間電子商取引等の利用者であるビジネスマン、及び電子認証サービスを提供する認証事業者に対して、下記の活動を実施している。

① 電子署名・認証普及啓発セミナー開催

電子署名法の主務官庁である総務省、法務省、経済産業省および電子署名・認証の普及に関心が深い団体等の協力を得て、東京、大阪、名古屋、札幌、仙台、広島、松山、福岡の８都市において開催している。

主なテーマは、電子署名法の概要と動向、安全な電子署名・認証の利用、商業登記に基づく電子認証制度、電子署名・認証の利用例等であり、都度時々のトピックスを加えている。

② 電子署名・認証ハンドブックの作成、配布

電子署名法に関する正しい知識の普及等を目的に、電子署名・認証に関する概略を知るための導入口として作成したもので、主にオンラインショッピング等の利用者である消費者をターゲットとした「パーソナルユース編」と、企業間電子商取引等の利用者であるビジネスマンにターゲットを当てた「ビジネスユース編」の２種類を用意している。なお、ハンドブックは PDF で Web サイトからも公開している。

③ 電子署名・認証関連　用語・技術標準集の作成、配布

電子署名・認証関連の調査研究活動を通じて得た情報をベースに、電子署名関連の用語及び標準化組織・機関についてまとめたもので、上記ハンドブックとあわせて見てもらえるように、また付録として、電子署名に関する法律及び電子証明書のプロファイル等を記載し、単独でも見られるようにした。

(2) 特定認証業務の認定に係る実地の調査

電子署名法における特定認証業務の認定制度に従って、認証事業者が申請する認証業務の調査申請を主務大臣に代わって調査を行うもので、新規認定のための調査と１年ごとに行う更新認定のための調査と設備、業務等の変更にともなう変更認定のための調査がある。

いずれの調査においても、規程類等ドキュメントの調査と認証業務に用いられる設備類の稼動調査を行って、その結果を主務大臣に通知する。主務大臣は調査結果の通知を受けて審査を行い適合であれば認定書を発行する。

調査に係る手続き、必要書類等について、http://www.jipdec.jp/esac/jipdectejyun.pdf、http://www.jipdec.jp/esac/syorui1.htm に詳細を記述している。また、電子署名法の施行後、２つの指定調査機関（日本情報処理開発協会、日本品質保証機構）によって調査され、認定された認証業務については、主務省庁のホームページ例えば経済産業省の場合は、http://www.meti.go.jp/policy/netsecurity/digisign_ninteiitiran.htm に記載されている。ちなみに、2003 年１月末現在において認定されている認証業務は１９業務である。

(3) 連絡先

財団法人　日本情報処理開発協会（JIPDEC）電子署名・認証センター
〒105-0011　東京都港区芝公園 3-5-22　機械振興会館　別館　２階
TEL：03-3432-6597　　FAX：03-3432-6201
MAIL：info@ac.jipdec.jp

4.20 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

電子認証局市民ネットワーク福岡は、市民がカジュアルに利用できる PKI の普及を目的とした NPO である。電子認証局市民ネットワーク福岡は、コミュニティスクールとコミュニティ CA の二つを主な事業としている。ただし CA としての活動は本格化していないのが現状である。

電子認証局市民ネットワーク福岡は、カジュアルな PKI の普及を促進するために、PKI の応用システムの構築にも取り組んでいる。その例として、電子署名に基づいた電子地域通貨システム Travecoup の開発や PKI ベースの VPN 構築キットの作成などがある。また、コミュニティが独自の PKI を構築するためのパッケージソフトである「コミュニティ PKI ビルダ」の開発なども行っている。

コミュニティスクールとしての活動は、地域通貨の研究会やコミュニティ PKI を実現するためのシステム構築のためのソフト開発手法の研究会や PKI を使って VPN を構築方法についての研究会などを行っている。

(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:yamasaki@cacanet.org

4.21 信金中央金庫

（http://www.shinkin-central-bank.jp/）

(1) 本店所在地　東京都中央区京橋 3 丁目 8 番 1 号

(2) 設立年月日　昭和 25 年 6 月 1 日

(3) 主な事業内容

［当金庫の概要］

信金中央金庫は、全国の信用金庫を会員とする協同組織形態の金融機関で、信用金庫の中央金融機関として、信用金庫業界の発展につとめると共に、わが国経済社会の繁栄に貢献することを目的として設立された。会員数は 314 信用金庫（平成 15 年 12 月末現在）である。

当金庫は、「個別金融機関」と「信用金庫のセントラルバンク」という 2 つの役割を主な事業としている。具体的な内容は次のとおりである。

①個別金融機関としての役割

機関投資家、総合的金融サービス提供機関、地域金融機関

②信用金庫のセントラルバンクとしての役割

信用金庫の資金需給の調整等、信用金庫の資金・為替の集中決済、信用金庫の業務機能の補完、信用金庫業界の信用力の維持・向上

［認証局の設置］

信金中央金庫では、平成 15 年 5 月 26 日、特定認証業務の認定を金融機関として初めて取得した。この特定認証業務により、当金庫が別に提供する「電子手形サービス」において、取引内容の改ざん防止や取引行為の否認防止を可能とした。

当金庫では、信用金庫業界の中央金融機関として、全国の信用金庫に本電子認証業務を展開し、我が国の中小企業のインターネットを通じた電子商取引の活発化、各種申請手続の効率化の実現を図ることとしている。

(4) 連絡先

総合企画部電子手形企画室　高橋秀充・佐藤真哉
TEL : 03-6202-7170
MAIL: aed87190@star.odn.ne.jp

4.22 モバイル IT フォーラム（mITF）

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

(1) 設立年月日・会員規模

平成１３年６月２５日

一般会員１０９、個人会員１１、特別会員２　（平成１５年５月２３日現在）

(2) 主な活動

- 第４世代移動通信システム及びモバイルコマース等の新世代モバイルに関する研究開発及び標準化の調査研究
- 新世代モバイルに関する情報の収集、交換及び提供
- 新世代モバイルに関する関係機関との連絡調整
- 新世代モバイルに関する普及啓発
- その他本会の目的を達成するために必要な事業

① フォーラムコーディネーショングループ（F-CG）

フォーラムコーディネーショングループは、各部会が任務を遂行するために必要な部会間の調整、及び運営委員会の会合間の執行方法策定を行います。

② 第 4 世代モバイル部会

（ｉ）第 4 世代モバイル部会

当面の活動内容

◆新しい（１０年後の）ビジネスマーケット創出に向け研究開発、標準化の枠組みを構築

－ 第４世代システムのあるべき姿、開発シナリオの検討
（システムへの要求条件、システムモデルおよびオープンにすべきインタフェースの明確化）

－ 国内外関係機関との連携
（フォーラム、研究機関、標準化機関、等）

－ 移動通信以外のシステムとのインターワークの検討
（他システムとの相互接続、シームレスな運用法、等）

◆第４世代モバイルシステムの研究開発に向けて、新たな要素技術研究テーマの抽出、検討を行い、本部会としての評価を実施

（ii）システム専門委員会

当面の活動内容

◆世界最先端のモバイル IT を実現する第４世代移動通信システムのシステム構成法の明確化

◆必要な要素技術の調査・検討・評価

◆国内外の関係機関と連携し、標準化の枠組みの検討

◆伝送速度や必要な要素技術など、技術的要求条件の検討

（iii）アプリケーション専門委員会

当面の活動内容

◆第 4 世代システムにおけるアプリケーションがもたらす未来の想定

◆コンテンツ・サービス、及びビジネスキームの検討／分析

◆社会・産業界からの第 4 世代システムに対する要望の検討／分析

◆アプリケーション実現のための要求条件の検討

◆対外的な提言のとりまとめ

③ モバイルコマース部会

当面の活動内容

◆携帯電話、モバイル網に関連する範囲を対象とした、モバイルコマースの開発・標準化の推進

－ 原則、インターネットにおける標準技術を採用

－ モバイル EC に特化した標準化の必要性を検討し､標準技術をベースにしたプロフ

ァイリングを実施

④ 技術専門委員会

当面の活動内容

◆モバイルコマースで広汎に利用される基盤技術に関する検討を行う。

－ 共通的に利用される認証技術の検討

－ 技術的検討結果に基づく実現性の実証実験の検討

⑤ 推進専門委員会

当面の活動内容

◆モバイルコマース実現のためのビジネス要件の検討及び提案

－ ローカル環境におけるモバイルコマースのビジネス要件の整理と検討

－ モバイルコマースのインフラについての検討

◆モバイルコマースの商用化・実用化の障害となり得る課題の検討

－ 制度的課題の検討

－ 法的課題の検討

◆市場に導入されつつあるビジネスモデルの調査

⑥ OMA 部会

当面の活動内容

OMA の本会議等の報告ならびに情報交換の実施を行います。

(3) 連絡先

モバイル IT フォーラム事務局

〒100-0013 東京都千代田区霞が関 1-4-1 日土地ビル 14 階 社団法人電波産業会内

TEL：03-5510-8594 FAX：03-3592-1103

E-mail：smitf@arib.or.jp http://www.mitf.org

4.23 特定非営利活動法人 日本セキュリティ監査協会（JASA）

Japan information Security Audit association

(http://www.jasa.jp)

(1) 設立年月日/会員規模

2003 年 10 月 10 日 特定非営利活動法人（NPO）として設立

会員数 94 社、後援団体 12 団体（2004 年 1 月現在）

(2) 設立の背景

コンピューター利用の一般化、インターネットの普及により、行政機関や民間企業の多くの活動に於いて、インターネットに接続された情報システムの利用は急激に拡大しています。ま

た、家庭からのインターネット利用も増加しており、社会活動と国民生活などの情報システムとインターネットに依存する割合は増加の一途を辿っています。

その一方で、情報システムや組織体におけるセキュリティ対策の不備に起因する様々な問題も生じています。このようなセキュリティインシデントは、個人情報の漏洩による人権侵害、企業の機密情報の漏洩による経済的損害や情報システム全体のダウンといった被害をもたらし、経済社会に与える影響は深刻なものとなりつつあります。

こうした環境の変化を受けて、IT セキュリティ評価認証スキームの創設、暗号技術の評価、ISMS 適合性評価制度の創設、インシデント情報共有・相談体制の整備など、情報セキュリティに関する制度整備は着実に進んできています。

しかしながら、独立かつ専門的知識を有する専門家による、情報セキュリティ対策の有効性を評価する「情報セキュリティ監査」の制度整備が遅れていることが喫緊の課題として浮上しました。そこで、経済産業省は「情報セキュリティ監査研究会」を設置し、情報セキュリティ監査のあり方について検討を行ない、情報セキュリティ監査研究会報告書と情報セキュリティ監査のための基準等を２００３年３月に公表しました。また、この報告書の提言を受け、２００３年４月１日より「情報セキュリティ監査制度」が開始されました。

(3) 設立の目的

「情報セキュリティ監査制度」を社会に普及・浸透するためには、情報セキュリティ監査の普及啓蒙活動のみならず、監査主体による「公正かつ公平な情報セキュリティ監査」が欠かせません。

そのためには、標準的な監査手法や監査技術を確立し、監査の質（高い倫理観、高い専門的な能力）が一定水準以上であることを担保する仕組み作りが必要となります。このような背景のもと、監査企業や監査人、一般企業や団体などの内部監査実施部門等が一同に会し、「公正かつ公平な情報セキュリティ監査」の確立と普及・浸透を目的とした「特定非営利活動法人日本セキュリティ監査協会」を設立しました。

本協会では、この目的を達成するために、監査技術の向上、監査主体の質の向上（監査人スキルアップ、行動規範の確立、監査人資格のあり方の検討）の他、各種団体との連携、監査制度の国際標準の調査研究や改善提言、並びに監査などについての相談窓口の開設など、幅広い活動を行い社会に貢献できる「公正かつ公平な情報セキュリティ監査」の普及・浸透に努めてまいります。

(4) 主な活動

本協会は前述の設立目的に鑑み、主な活動は以下の５項目となります。

① 情報セキュリティ監査制度の普及促進

- セミナーの開催、会報や書籍の出版による啓蒙活動など
- 各種業界団体などに対する普及活動
- 相談窓口の開設

② 情報セキュリティ監査の質の向上

（ｉ）情報セキュリティ監査技術の向上

- 監査手法の調査研究
- 監査ノウハウの蓄積
- 監査マニュアルの作成

（ⅱ）情報セキュリティ監査主体の質の向上

- 監査人のスキルアップ支援
- 監査企業ならびに監査人の行動規範の確立
- 監査人資格のあり方の検討

③ 情報セキュリティ監査制度の研究

- 国際標準など他関連監査基準の研究
- 情報セキュリティ監査制度の検討ならびに提言
- 業界別ガイドラインの作成支援など

④ 相談窓口の開設

- 監査制度の案内
- 監査企業の紹介
- その他監査に関する諸問題の相談受付

⑤ 審査委員会の設置

- 倫理制度の検討
- 監査事例の適正性審査
- 監査主体/監査人の倫理審査

＜お問い合わせ先＞

◇ NPO 日本セキュリティ監査協会 事務局 ◇

住所：〒136-0075 東京都江東区新砂 1-6-35 T.T.ランディック東陽町ビル１階

担当：沓澤（くつざわ）、青柳

TEL：03-5634-7808、FAX：03-5634-1040、e-mail：office@jasa.jp

URL ： http://www.jasa.jp

◇ 関西地区オフィス ◇

住所：〒531-8577 大阪府大阪市北区豊崎 5-4-19（インテック大阪ビル内）

TEL：06-6376-3536

付録　JESAP 運営委員会活動概要

回数	開催日時	議題
第１回	2003 年 6 月 2 日（月） 14：00～17：00	1.委員長挨拶 2.平成１５年度計画案 3.公的個人認証（個人証明証）に関する講演と議論 ①「公的個人認証の今後の展開」 ②「個人向け証明書の検討 4.その他事務局連絡
第２回	2003 年 7 月 3 日（木） 14：00～16：00	1.委員長挨拶 2.事務局からの連絡 3.教育分野における証明書の利用
第３回	2003 年 8 月 5 日（火） 14：00～17：00	1.委員長挨拶 2.事務局からの連絡 3.電子認証における属性情報の活用 4.医療分野における証明書の活用 5.認証における属性情報の活用 6.属性証明に関する代理士業のあり方について 7.教育分野における証明書の活用
第４回	2003 年 11 月 14 日(火) 14：00～17：00	1.委員長挨拶 2.事務局からの連絡 3.「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」 ②「国税電子申告・納税システム」 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」
第５回	2003 年 12 月 10 日(水) 14：00～17：00	1.委員長挨拶 2.事務局からの連絡 3.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 4.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

		5.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－ 6.平成１５年度 JESAP 報告書 2003 目次案の検討
第６回	2003 年 1 月 22 日（木） 14：00～17：00	1.委員長挨拶 2.事務局からの連絡 3.平成１５年度 JESAP 報告書 2003 提言について

執筆者一覧（敬称略、順不同）

	氏名	所属	担当
委員	西谷　研次	(株)UFJ 銀行	4.6
委員	鈴木　春洋	(株)中電シーティーアイ	2.2.1
委員	立川　雅章	(財)国際研修協力機構	2.2.2
委員	山崎重一郎	近畿大学	4.20
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	4.19
委員	喜多　紘一	（財）医療情報システム開発センター	4.13
委員	大野　　実	全国社会保険労務士会連合会	4.3
委員	石幡　吉則	電気事業連合会	4.5
委員	池谷　千尋	電子申請推進コンソーシアム	4.10
委員	寺川　　陽	(財)日本建設情報総合センター	4.14
委員	田中　一志	日本税理士会連合会	4.2
委員	佐藤　純通	日本司法書士会連合会	4.1
委員	中西　　豊	日本行政書士会連合会	4.4
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	4.12
委員	安田　直義	日本ネットワークセキュリティ協会	4.11
ｵﾌﾞｻﾞｰﾊﾞ	澤田　稔一	総務省 行政管理局	1.2.1
ｵﾌﾞｻﾞｰﾊﾞ	山碕　良志	総務省 自治行政局	1.3.1
ｵﾌﾞｻﾞｰﾊﾞ	印南　朋浩	経済産業省 商務情報政策局	1.2.2／1.2.4(3)
ｵﾌﾞｻﾞｰﾊﾞ	中垣　治夫	法務省 民事局	1.2.3／1.2.4(2)
ｵﾌﾞｻﾞｰﾊﾞ	星加　　司	国土交通省 総合政策局	1.2.4(1)
企画委員	松本　　泰	セコム（株）	3.2
事務局	前田　陽二 小祝　香織	電子商取引推進協議会	1.1／2.1／2.2.3／2.2.4／4.7／4.8／4.18／4.22
事務局	中川　宏之	日本 PKI フォーラム	3.1／4.9
協力	（財）情報処理相互運用技術協会（INTAP）事務局		4.15
協力	東日本電子認証普及促進協議会　事務局		4.16
協力	電子商取引安全技術研究組合（ECSEC）事務局		4.17
協力	信金中央金庫		4.21
協力	日本セキュリティ監査協会（JASA）事務局		4.23

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報告書 2003
―国内の PKI 推進状況―
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-E007

ISBN4-89078-613-9 C2055

定価 5,000円（本体4,762円＋5％税）