# 電子署名普及に向けた調査報告書（２）
## ―海外及び国内金融分野での利用動向―

平成19年３月


次世代電子商取引推進協議会

# 序文

情報ネットワークを介した電子商取引の利用の拡大に伴い、信頼性・安全性確保は極めて重要な課題となっている。電子商取引の普及には電子署名（代理署名を含む）の利用により取引相手の信頼性保証（なりすまし及び改ざんの検知、否認防止）を行うことが必要であり、公開鍵基盤（PKI）による電子署名は、技術的にも利用環境としても利用可能な状況にあるが、その展開のスピードは遅く、特に民間分野ではまだほとんど利用されていない。

前年度は、これまで議論されてきた三文判 PKI（利用の制限を設けた電子署名）等の電子署名の運用の多様化に関する検討や、電子署名定着のための提言をまとめた。

今年度は、広く調査を行った。まず、電子署名の利用状況を中心に海外における PKI の利用状況について報告書あるいは Web による調査を行った。また、国内の金融関連機関に対して PKI 利用の状況調査及び意識調査を行った。それに加え、ドイツの著名な研究機関であるフラウンホーファー研究所にたいして「欧州における PKI および証明書の利用に関する調査」のテーマで委託調査を行った。調査結果は本報告書に付録として載せている。

本報告書は次の 2 部構成になっている。

第 1 部　海外での電子署名利用調査

第 2 部　金融業界（国内）における電子署名利用調査

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ある。

平成 19 年 3 月

次世代電子商取引推進協議会

# 目　次

# 第１部　海外での電子署名利用調査

# まえがき

2001 年 4 月に電子署名法が施行され、公開鍵暗号基盤（PKI）によるデジタル署名が法的な意味合いを持つことになった。また、2005 年 4 月 1 日には「e-文書法」という新しい法律が施行された。この e-文書法とは「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（通則法）及び「民間事業者等が行う書面の保存等における情報通信技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（整備法）という 2 つの法律をまとめた呼称のことである。各書類の保存方法等は、所管の各省庁から省令の形で指示される。

この法律は、民間においてこれまで法律によって紙による保存が義務づけられていた書類を、電子化したデジタルデータによって保存することを認めるものである。

このように、デジタル署名の利用は、政策的にも制度的にも利用を拡大する方向にあり、また、技術的にも利用環境としても利用可能な状況にある。

しかしながら、電子政府のサービス展開に伴って G2B において利用され始め、また B2B においても一部の業種で利用され始めているが、その展開のスピードは遅い。さらに、B2C や C2C では、多くのトラブルがすでに発生しているにもかかわらず、ほとんど利用されていない。

本調査研究では、電子契約などデジタル署名の利用の定着に焦点を絞り、社会が受け入れるための、社会的ニーズ、導入上の障害、実現のための技術的な成熟度、など多面的な視点から調査分析を進める。

本年度は、海外における電子署名の利用状況の調査を行った。この結果を第 1 部としてまとめる。

各章の概要は以下のとおりである。

第 1 章では、北米（米国、カナダ）における電子署名の利用状況について、報告書、Web を使って調査を行った。

第 2 章では、アジア、オセアニアから 9 カ国を選んで北米と同様の方式で調査を行った。

第 3 章では、欧州における電子署名の利用状況について、ドイツのフラウンホーファー研究所に委託研究を行った。

第 4 章では、利用拡大のための分析、提言をおこなった。

今後、この報告書に基づき、普及に向けた対策を検討していく予定である。

# 第1章　北米での電子署名活用調査

## 1.1　米国

(1) 背景／国の方針、法律、国民性

米国においては、1995 年のユタ州においてデジタル署名法（Digital Signature Act）が制定されている。ユタ州のデジタル署名法は、認証機関に関する免許制度を設け、細かい資格要件を定める一方で、認証機関の義務についても細目にわたる規定を置いている。「電子署名法の在り方と電子文書長期保管に関する現状調査報告書」では、世界各国の電子署名法を「規制モデル」「市場モデル」「ハイブリッドモデル」の 3 つに分類しているが、このユタ州のデジタル署名法は、「規制モデル」と分類されている。その後、アメリカでは、多くの州が電子署名関連立法を行ったが、そこでは、ユタ州法のように署名技術や認証機関を規制する立法は多くはみられない。これらは「市場モデル」と分類している。

米国連邦政府は、州毎にばらばらな法制になっている州法を統一するために制定された「グローバルなおよび国内の商取引における電子署名についての法律（Electronic Signatures in Global and National Commerce Act)」(E-Sign 法と略称される。）が、2000 年 10 月 1 日に施行されている。この「米国連邦政府の電子署名法（E サイン法)」も、「市場モデル」と分類されている。

「市場モデル」では、電子署名に対して特定の技術的規制をしておらず、認証局などの要件も定めていない。一般論として英米法の国々の電子署名法は「市場モデル」が多く、大陸法の国々の電子署名法は、「規制モデル」が多く見受けられる。

米連邦政府の E サイン法のような「市場モデル」の電子署名法の場合、その効力が曖昧な面もあり、電子署名を施すことを規制として利用されることは少ない。しかし、米国においても「電子署名」による規制を必要としている業界は存在する。個人情報保護法においては、ヨーロッパ諸国の多くは、オムニバス方式の立法であるが、米国は特にセクトラル方式である。電子署名法においても、その効力や規制と言った意味では似たところがある。

規制という意味では、医療の HIPAA(Health Insurance Portability and Accountability Act)、製薬業界における FDA（米国食品医薬品局）の「21CFR Part 11」などが、電子署名に関連する業界毎の規制と言える。規制による強制力を働かせるには、何らかの基準が必要になるが、米国の場合、アメリカ国立標準技術研究所（NIST）が米国連邦政府のブリッジ認証局との相互認証（Cross Certification）のための 4 つのレベルの基準を設けており、この基準が、米国における認証局の基準となっている側面がある。

電子署名に関係が深い IC カードは、米国は、欧州に比べ普及が遅れていた。しかし、2001 年 9 月 11 日の同時多発テロを契機にリアル ID 法の制定、大統領令 HSPD-12(Homeland Security Presidential Directive 12)「連邦政府職員と契約業者の共通識別基準のためのポリシー」の発令があり、これが電子的な身分証明書の普及を促がしている。これが、PKI の普及や電子署名の普及につながる可能性がある。

(2) インフラの状況／IC カード、eID、証明書発行主体

① 米国の PKI の概観

米国の PKI は、連邦政府の PKI を中心に構成されている。連邦政府の PKI と、業界毎の PKI が、連邦政府の PKI の定める 4 つの保証レベルのポリシーに従い、連邦政府のブリッジ認証局との相互認証（Cross Certificate）を行なうことで信頼関係の確立する方向にある。この業界毎の PKI には、以下のものがある。

- 学術系の HEPKI（Higher Education PKI）
- バイオ製薬業界の SAFE（Signature and Authentication For Everyone）
- 航空宇宙産業の Certipath

図 1.1-1 に米国連邦政府のブリッジ認証局と各業界の認証局との関係（相互認証：Cross Certification）の様子を示す。

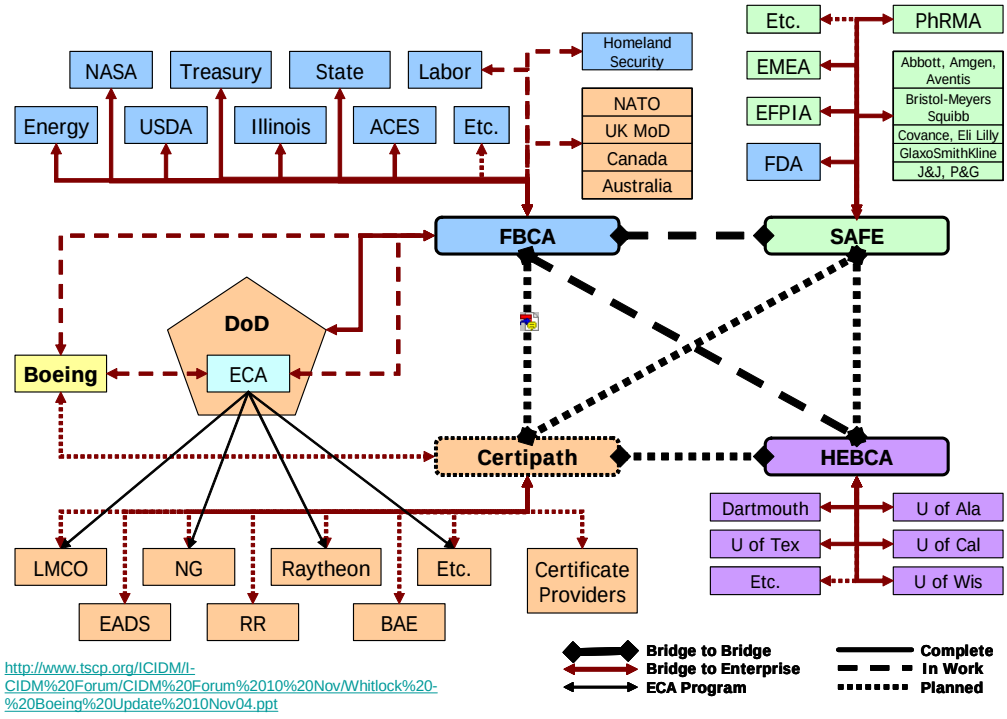



図 1.1-1 米国連邦政府のブリッジ認証局

② ID カードのプロジェクト

米国においては、市民向けに発行される電子的な身分証明書（eID）のプロジェクトは存在しないが、職業人ということに関しては、連邦政府職員と契約業者のための ID カード（PIV：Personal Identity Verification）の発行が始まっており、これが連邦政府以外も含め大きな影響をおよぼす可能性がある。PIV は、全連邦政府職員に配布され、PKI の証明書も格納されているため連邦政府の PKI に対しては多大な影響がある。

PIV は、2004 年 8 月に発令された大統領令 HSPD-12「連邦政府職員と契約業者の共通識別基準のためのポリシー」に基づき仕様が作成されている。HSPD-12 は、連邦政府施設への物理的・論理的アクセスのセキュリティ強化のため、身分証の標準を規定することを要求しているが、これは、政府機能の効率化のほか、連邦政府職員をテロから守り、また個人情報盗難も防止することを目的としている。この要求に応じた PIV プロジェクトでは、IC・ID カードの発行対象は、連邦政府職員だけでなく、契約業者にも含まれる。そのため非常に多くの枚数が発行されることが見込まれており、2009 年までに 2000 万枚が発行されると言われている。

米国立標準技術研究所（NIST：National Institute of Standards and Technology）は、HSPD-12 の指令に従い FIPS-201 呼ばれる基準を作成しさらに、この基準に適合する PIV カードの仕様（SP800-73）を作成した。NIST は、仕様を作成するだけでなく、FIPS-201 に準拠した PIV カードとミドルウェアを検証して、認定する NPIVP（NIST Personal Identity Verification Program）を立ち上げたが、NPIVP のような評価・認定制度がデファクトの標準を作り出す可能性がある。今後の米国連邦政府の PKI の成功の是非は、この PIV が鍵を握っていると考えて間違いない。

この PIV は、3 つの EE 証明書が格納できる。すなわち、認証用、署名用、暗号用の 3 つである。PIV の場合、認証用が必須であり、署名用、暗号用は、オプションである。しかし、署名が必要な権限者には、署名用の証明書が発行されると考えられることから、米国連邦政府機関における電子署名の普及は、やはり PIV の成功の是非にかかっていると考えられる。

(3) バイオ製薬業界の SAFE

Secure Access For Everyone（SAFE）は世界的なバイオ製薬（Bio-Pharma）業界において、規制や法に対応した電子署名用のクレデンシャルを提供するための PKI であるが、後述するように、電子署名が非常に重要な役割を果している。

SAFE は、米研究製薬協業協会（PhRMA）と欧州製薬団体連合会（EFPIA）の後援による世界的なプロジェクトであり、世界的な製薬企業より資金提供を受けている。

SAFE は以下のようなメンバーから構成されている。

(a) フルメンバー（Full Member）
営利・非営利を問わず、新薬の研究開発機関を含めた組織に所属する人

(b) 提携メンバー（Associate Member）
開業医や小規模研究機関の人

(c) 政府メンバー（Government Member）
監督機関や新薬発見・開発などの他の政府機関の人

(d) SAFE 発行者（SAFE Issuer）
PKI を運用していて SAFE メンバーの要求により SAFE 加入者へ証明書を発行する組織。これら Issuer は SAFE BCA と相互認証（Cross-Certify）を行なう。

(e) SAFE 薬剤協会（SAFE Bio-Pharma Association）
SAFE 標準の管理目的のために SAFE 創立メンバーよりつくられた非営利組織

SAFE は、当初はバイオ製薬業界主導で作られたが、後にヘルスケア関係や医療機器メーカも参加している。関連会社である SAFE-BioPharma、LLC が Identrus の協力のもとで CA を運営し、SAFE Credential（電子証明書）を会員企業及び薬品の治験を行う医師や研究者に配布している。薬品の治験結果に電子署名を施した電子データで処理することにより、研究開発コストの40%を占めるといわれている紙ベースでの処理コストを大幅に削減するとしている。現時点では、製薬企業と治験を行う病院や企業との間の BtoB や製薬企業と監督官庁との間の BtoR（R：Regulation）に関して利用されつつある。

製薬の治験などの報告に関しては、監督官庁である FDA が定めた医薬品の開発・製造における電子記録・電子署名に関する規制である FDA rule 21 Code of Federal Regulation（CFR）Part 11 Section 11.30（Controls for Open systems）が存在する。SAFE では、認証局運用基準は、この FDA CFR Part11 をクリアするように定められている。

SAFE では、認証局運用基準以外にも、署名のインターフェースなど、様々な基準や、相互運用性確保のための仕様も定めている。例えば、署名に関しては、USSI（Universal Safe Signing Interface）と呼ばれる文書を署名しアップロードするための Web ベースのインターフェースを定めている。既に、いくつかのベンダーが、この USSI に対応した SAFE 準拠ソリューションを提供している。

以下に、SAFE の主な役割を示す。

(a) バイオ製薬業界向けの証明書の発行
(b) SAFE-certified community 内での SAFE 認定アプリケーションのシームレスな認証連携
(c) FDA（米国食品医薬品局）、欧州 EMEA（the European Medicines Evaluation Agency）をはじめとした各国薬事行政関係機関 CA との相互認証（Cross certification）

SAFE の証明書を使ったプロジェクトとして、Firebird/SAFE プロジェクトがある。Firebird（Federal Investigator Registry of Biomedical Information Research Data）は、米国国立がん研究所（NCI National Cancer Institute）の CRIX（Clinical Research Information Exchange）の進めるパイロットプロジェクトのひとつである。CRIX は、新薬の開発、テスト、認可のプロセスを電子化するための標準を、様々な関係者を集め行なっており、Firebird は、FDA（米国食品医薬品局）のフォーム 1572 の提出プロセスを自動化する。フォーム 1572 は、臨床研究者が連邦政府規制に従って実施研究用新薬に、臨床試験に同意するための「治験担当医師誓約書」であり FDA から要求されている。

このように新薬の認可といった分野においては、様々な規制が必要であり、そのため電子署名は重要な役割を果す。

(4) その他

米国における SAFE 以外の業界の動きとしては、学術系 PKI の HEPKI、航空宇宙産業の Certipath がある。

Certipath は、米国連邦政府のブリッジ認証局と相互認証を行なっている Commercial Bridge CA（商業ブリッジ認証局）を運営している。CertiPath は、Exostar、ARINC、SITA（いずれも航空・防衛産業を対象に、IT ソリューション、エンジニアリングサービス等を提供）の 3 社が共同で設立した企業体である。3 社の共同設立（Exostar 中心）となった理由は、連邦政府が 1 社による商業ブリッジの独占を嫌ったためである。

参考

電子署名法の在り方と電子文書長期保管に関する現状調査報告書　平成 17 年 3 月（財）日本情報処理開発協会

https://www.japanpkiforum.jp/secure/kaiin/esign_k/2004/2004_e-sign_report.pdf

連邦政府における PKI 利用動向

http://e-public.nttdata.co.jp/f/repo/382_u0605/u0605.asp

先進アプリケーション事例調査報告

http://www.japanpkiforum.jp/hojo/shiryou/FY2005_report/03-appli.pdf

IC・ID カードの相互運用可能性向上に係る基礎調査

http://www.ipa.go.jp/security/fy18/reports/ICID/index.html

## 1.2　カナダ

カナダ連邦政府における PKI の構築は、1993 年に始まる。1993 年 8 月に、政府の通信セキュリティ機関（Communications Security Establishment）を中心とするワーキンググループは、カナダ国内における電子鍵の管理システムに対する要求をとりまとめ、その中で、連邦内での自動的な鍵管理に関するセキュリティ上の標準化とソリューション構築に向けた全省共通的なアプローチについての方針を定めた。その後 1993 年 11 月に、Nortel Secure Networks 社(現在の Entrust Technologies 社）と契約を行い、商用化可能な標準に基づく鍵管理システムの開発に着手した。

現在では、カナダは電子政府サービスの進捗度調査において、常にトップにランクされる先進 IT 国家である。この評価の主な理由はカナダ連邦政府総合サイト（www.canada.gc.ca）（カナダ通信省（Communication Canada）がサイトを管理）の充実度である。カナダ連邦政府における最初の優先事項の 1 つは、World Wide Web（WWW）上により効果的なポータルサイトを立ち上げることであった。2001 年 1 月、カナダ連邦政府はデザインを一新したカナダ連邦政府総合サイトを開設した。カナダ連邦政府総合サイトは、3 つの情報やサービスへのゲートウェイ（①国民向け、②企業向け、③世界のクライアント向け）を中心として設計されている。

電子政府達成度世界一の評価を得ているが、カナダ連邦政府オンライン（Government On-Line；GOL）構想をさらに実現するための鍵は、国民や企業と協議することである。このため多くの調査は、実際の提供手段や好ましい提供手段だけでなく、電子政府サービスに対する国民の期待に的が絞られている。

公開鍵証明書は政府内においては、セキュリティのユーティリティとして広く普及しており、CommonCA（CAを持たない省庁が共同で利用するCA）の活用や、ブリッジCAによる相互認証も進んでいる。

利用者視点からは、今後の多様なアプリケーションの展開に、EPassやG-passが期待されており、匿名性や導入容易性が評価されている。

官民連携による相乗効果が出ており、電子署名・認証の構築ベンダーを結果的に1社（Entrust Technologies社）に限定したことで、相互接続などの技術的課題も顕在化していない。

### 1.2.1　ePass

カナダ政府は、政府サービスへの安全なオンライン・アクセスをカナダ居住者に提供するため、ガバメント・オンライン（Government On-Line）サービスを実施している。政府省庁を通じて、個人および企業が、オンラインで書式に記入し、個人情報（たとえば住所）を更新できる領域まで、アクセスの提供を既に拡張している。

このレベルの個人セキュリティを可能にするために、政府は、“ePass”システムを導入実施した。ePassソリューションは、サーバ・ベースのPKIソリューションである。プライベート鍵とそれに対応する公開鍵証明書が中央サーバに保管されている。ユーザが政府サービスへのアクセスを希望するときに毎回、プライベート鍵と証明書が中央サーバから取り出される。この取り出しが行われるまえに、ユーザは、ユーザ名とパスワードによって認証を得なければならない。認証に成功すると、鍵のペアが自動的にユーザのローカルPCにインストールされる。トランザクション後、鍵のペアはローカル・システムから削除される。利用を希望するユーザは全員中央の認証局(CA)に登録してePassを取得する。このePass証明書に書き込まれている唯一の識別子は、それ自身には意味がないが一意である番号（MBUN：meaningless but uniquenumber）であり、この番号は基本的にランダムに生成される。各ユーザの識別子は一意であるため、複数のユーザが同じMBUNを所持することはない。番号自体に意味はないため、所持している番号からどのような種類の個人情報も推測されない。ユーザは、オンライン・アクセスを希望する各政府プログラムに（手続きとしては一度で）個別に登録する。ユーザのMBUNは、目的の政府プログラムの使用している各システム内でプログラム識別子にマッピングされる。各システムのプログラムでは、MBUNではなくて、このプログラムIDがユーザのインデックスとして継続的に使用される。実際、MBUN自体は、ユーザの裁量によりあとで変更される場合もある。

① ePassの利点

・各証明書に1つまたは複数のプログラムを関連付けることをクライアントが選択
・ユーザーフレンドリーな操作と効率的なセンタでの証明書管理
・クライアント側にソフトをインストール不要で、各セッション終了後に「痕跡」を抹消
・デジタル署名による否認防止とSSLによる機密性は確保

・プログラムごとにクライアント ID と権限を分散管理（プライバシー保護強化）
・「ローミング」（各証明書に任意のインターネット端末からアクセス可能）が可能
・ID／パスワードの復元は、匿名でセンタ側で実施（本人確認の繰り返しを回避）
・必要に応じて第二認証が本人確認の確実性を向上
・結果としてアプリケーション利用の簡素化と導入費用削減に寄与

② ePass の課題
・複数証明書を使用する場合、クライアントが複数のユーザ ID を記憶する必要がある
・ユーザ ID で認証局にアクセス可能

### 1.2.2 カナダ連邦政府ポータルサイト

カナダ連邦政府は、政府のプログラム・サービス・イニシアチブなどの行政情報をはじめとする様々な情報を提供する公式ポータルサイト「Canada Site（canada.gc.ca)」をいち早く 1995 年から運用している。

同ポータルを管理するカナダ公共事業・政府業務省（PWGSC：Public Works and Government Services Canada）は、行政情報・サービスのオンライン化の推進を目指す連邦政府イニシアチブ「Government On-Line（GOL)」を主導している。

2001 年 1 月には情報の再整理が行われ、カナダ市民・企業・外国人に向けたセグメント別ポータルが追加された。同年 2 月、ジャン・クレティエン首相は、セグメント向けポータルをはじめとするいくつもの新機能が追加された Canada Site は GOL イニシアチブにおける重要な成果であり、「カナダ市民はインターネットを利用してこれまで以上のことができるようになった」と述べている。

Canada Site のトップページには、カナダ市民向けポータル「Service Canada」、企業向けの「Canada Business」、外国人向けの「Canada International」という 3 つのゲートウェイが設けられている。このうち Service Canada は、オンラインだけでなく、電話や窓口なども含めた複数のチャンネルによる行政サービスへのアクセスを市民に提供するための政府横断プロジェクトの一環である。様々な行政サービスへの“ワンストップアクセス”をカナダ市民に提供することを目指す Service Canada には、すでに多数の連邦政府サービスが統合されており、州政府サービスの統合も進められている。

トップページは利用者別の情報提供を強く意識した構成となっているが、テーマや組織別に分類したページも用意されており、カナダについてのテーマ別ポータル「About Canada」、各州・準州政府の公式サイト、個々の政府機関の公式サイト、ウェブサイト以外の問い合わせ先情報などをまとめたページへのリンクも設けられている。

カナダには英語とフランス語という 2 つの公用語があるため、Canada Site のどのページも英語版とフランス語版が用意されている。また、二ヶ国語検索モジュール（Bilingual Query Module）と呼ばれる検索支援ツールによって、一度の検索で関連用語を含む英語文書とフランス語文書をすべて検索結果として抽出するといった幅広い検索が可能となっている。

同ポータルには「My Government Account」というパーソナライズ機能があり、利用者は Canada Site を介してアクセス可能なサイトの中から必要なリンクをまとめた独自のポータルを作成す

ることができる。リンクは情報種別またはアルファベット順に整理でき、必要なサイトにたどり着くまでに何度もクリックして進む必要がなくなる。また、特定の項目に新しいリンクが追加されたことを知らせる電子メール通知サービスに登録することも可能である。「My Government Account」を利用するには、ePass と呼ばれる本人認証のための情報（ユーザ名とパスワード）を作成する必要がある。ePass は、「My Government Account」以外にも、例えばカナダ歳入庁（Canada Revenue Agency）の「My Account」サービスなど、ePass を利用するその他の連邦政府のサービスへのアクセスにも共通で利用できる。

また、カナダ連邦政府は、携帯電話などのモバイル機器からアクセスできる「カナダ連邦政府ワイヤレスポータル」も開設している。ワイヤレスポータルを介してアクセスできる情報としては、カナダ国境サービス庁（Canada Border Services Agency）が提供するカナダ・米国間の国境を越えるための推定所要時間、カナダ産業省（Industry Canada）が提供するカナダビジネスサービスセンタの問い合わせ先情報、カナダ中央銀行が提供する為替レートなどがある。情報やサービスは今後も追加される予定となっている。

Canada Site は、オンラインフォーム「Tell Us What You Think（ご意見をお聞かせください）」・ユーザビリティ調査・アクセシビリティレビュー・展示会でのデモなどを通じて積極的にフィードバックを取得し、継続的に改善を行っている。

カナダの政府ポータルは、利用者別に情報を分類しているほか、州・地方政府の情報へのリンクも集約し、ウェブサイト以外の問い合わせ先情報も記載しているなど共通点が多い。これらは、利用者の視点を重視し、フィードバックを得ながら改善を繰り返してたどり着いた、政府ポータルのベストプラクティスといえそうだ。

また、存在しているのに見つけてもらえない政府の情報やサービスをなくし、検索機能で使い勝手を向上し、さらにはパーソナライズ機能などで国民一人一人にとっての利便性・有用性を高めるなど、利用者満足度の向上を徹底的に追求している点も見逃せない。

インターネット上の政府の正面玄関といえる政府ポータルは、単なる「顔」ではなく、電子政府の成否、すなわち国民が電子政府によってどれだけ恩恵を受けることができるかを左右する重要要素である。米国・カナダ両政府が利用者満足を重視して積極的な改善を行っているのも、この点を確信しているからだろう。

[1] 「電子認証分野における各国イニシアティブの概要」2005.6
[2] 米国マンスリーニュース　2006 年 4 月号
（http://e-public.nttdata.co.jp/f/repo/375_u0604/u0604.asp）

# 第2章　アジア・オセアニアでの電子署名活用調査

電子取引、電子申請において、当事者を認証（Authentication）し、関係する書類を保全するための電子認証・電子署名技術は、インターネットが普及した現在の社会において、必須の課題となっている。その中でPKIは電子認証・電子署名を行う為の基盤技術となっており、アジア・オセアニアの国々では、それぞれ独自のPKIアプリケーションを活用している。特に、韓国、シンガポール、オーストラリアでは国が主体的に情報インフラを整備し、先進的に導入が行われている。

今後、経済成長が見込まれるアジアの国については、Web サービスの拡大、ユビキタス社会の技術基盤の整備により、その重要性は一段と高まると思われる。

各国の電子署名に関連する法制度はばらつきがあるものの、既にPKIを利用したアプリケーションが、様々な分野で活用されており、今後も更に拡大され適用される可能性が大きい。

その中で今回の調査では、大きくヘルスケア、金融、B2B、B2C、政府・公共利用に分類し、それぞれ特徴があるアプリケーションの調査を行った。対象としては、中国、香港特別行政区、台湾、韓国、マレーシア、シンガポール、タイ、オーストラリア、ニュージーランドの 9 カ国、1 地域を対象に導入状況の調査を行った。

日本のIT関係の調達が、どちらかというと会計法等の観点から「公平性」「透明性」「低価格」を重視しているが、韓国では「技術」「スピード」を重視している等、アジアに・オセアニアおけるPKIに関連するビジョン、最近のPKI利用動向を紹介することにより、日本における今後のPKI利用促進を提起することができれば幸いである。

## 2.1　中国

(1) 背景／国の方針、法律

コンピュータが普及してその応用が進み、中国における電子商取引も日増しに広がっている。国際化の流れから、中国には発展や国際交流に適した制度の早急な整備が求められている。『電子署名法』はこうした状況から誕生した。

『電子署名法』は一朝一夕で誕生したわけではない。1999年の全国人民代表大会と全国政治協商会議期間中に、早くも電子商取引の法整備問題が提議され、当時の条件が未成熟で提案が直ちに実現することはなかったが、関係部門は研究に着手し始めた。しかし、電子商取引の法整備は難しく、関係部門は 2002 年から部分的な法整備を進めることを決定。その法律が今日の『電子署名法』である

『電子署名法』は何度か名称を変え、『電子印鑑法』、『デジタル署名法』と名付けられた後、技術中立の原則から、最終的に『電子署名法』になった。『電子署名法』の制定は2003年4月、国務院法制弁公室の主導で正式に起草段階に入った。『中華人民共和国電信条例』に基づき各方面が協力して、『電子署名法』は 2004 年 8 月 28 日、全国人民代表大会常務委員会を通過。胡錦涛国家主席が第 18 号の主席発令で公布した。正式名称は『中華人民共和国電子署名法』で、2005年4月1日に施行された。

(2) インフラの状況／証明書発行主体

●認証局について

2002 年より、情報セキュリティプロジェクト「CA 互聯互通模範工事」が国家計画委員会の許可を得て、始動している。同プロジェクトの内容は、(1)ブリッジ証明書機関（BCA）1ヵ所を設置すること、(2)国内の 6 社の典型証明書機関（CA）を相互接続すること、(3)選定した業務応用を通じて、異なる PKI のユーザに信頼関係を設けることの 3 点。また、BCA 運行、管理パターンの模索、管理体制整備、規格設定、多種技術体系共存のソリューションの開発を行う。国家 PKI 信頼体系の構築を推進する。同プロジェクトは国家情報センターとサービスセンターが実施する。相互接続する部門は、北京 CA（http://www.bjca.org.cn/）、上海 CA（www.sheca.com/asp/index.asp）、天津 CA（http://www.ectj.net/）、福建 CA（www.fjca.com.cn）、安信（吉林）CA（http://www.jlca.com.cn）、中国電信となっている。

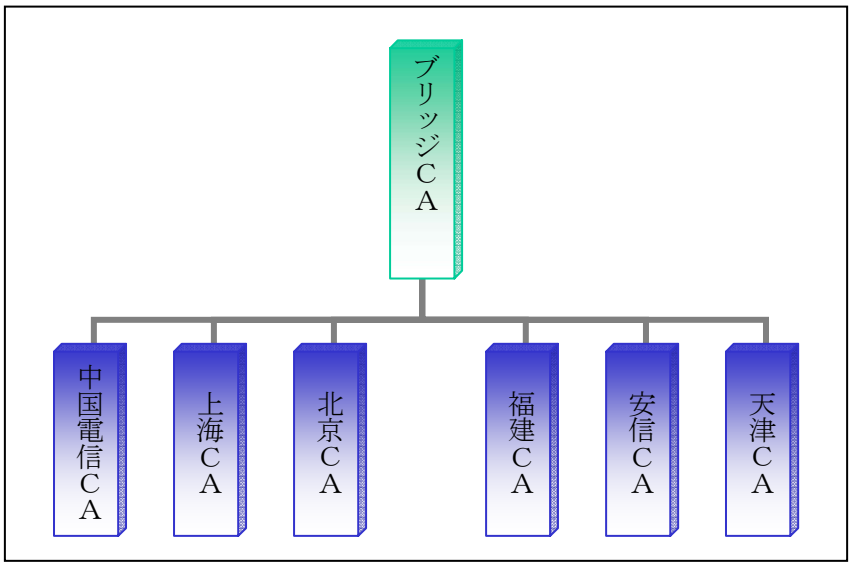



**図 1.2-1 認証局の相互接続**

●北京 CA

地方政府系認証局の代表として BJCA（北京 CA）が挙げられる。BJCA のサービスは大きく、国家レベルの認証局である「対外貿易認証センター」の運営、CIECC（中国国政電子商務センター）の運営する CIECC Net の構築・メンテナンス、中小企業向けの ERP システムの開発設計、IT サービスやシステム・インテグレーションサービスである。

(3) 金融部門

中国金融認証センター（http://www.cfca.com.cn）は PKI 証明書システムの安全性を確かめるため、2000 年 12 月より国家信息安全測評認証センターに検査を依頼していた。そして 2002 年 8 月、「国家信息安全認証システム安全証明書」が正式に授与された。中国金融認証センターはすでに 7 万枚の証明書を発行し、現在も月 5000 枚発行のペースで動いている。対象範囲は銀行、証券、通信、税務、保険、大型企業グループなど多岐に渡っている。2002 年のネット

銀行の取引額は現時点で1兆円を突破している。

中国金融認証センター（China Financial Certification Authority、略称 CFCA）は中国人民銀行を柱に、中国工商銀行、中国農業銀行、中国銀行、中国建設銀行、交通銀行など全国規模の商業銀行 14 行が共同で設立、ネット上の取引と支払いの安全性を保証する国家級の金融認証機構となっている。

中国金融認証センターでは、証明書の種類と用途について次の様に分類している。

・企業用高級証明書
企業に適用。比較的金額が大きいネット上 B2B 取引の場合利用し、安全ランクは高く、電子署名とデータの暗号化に使用する。

・企業用普通証明書
法人ユーザに適用。SSL、S/MIME で利用される。安全ランクは低く、比較的金額の小さいネット上の取引に用いる。

・個人用高級証明書
個人に適用。比較的金額が大きいネット上の取引の場合利用し、安全なランクは高く、電子署名とデータの暗号化に使用する。

・個人用普通証明書
個人ユーザに適用。SSL、S/MIME で利用される。安全ランクは低く、小額のネットバンクとインターネットショッピングに用いる。

・Web Server 証明書
ウェブサイトのサーバーに適用。比較的金額が小さい B2C 取引の場合利用する。B2B 取引を提供する時、Direct Server 証明書を申請するべきであり、Direct Server アプリケーションによりその安全性を保証する。

・Direct Server 証明書
電子署名とデータ用いて暗号化する。Direct Server 証明書は主に企業で利用され、B2B 取引を行う際に利用する。

(4) 公共（申請・納税）

●安全電子印章システム

中国電子商務協会と公安部物証鑑定センターが開発した「中国安全電子印章管理応用システム（http://www.esca.cn/index.action)」が 2004 年 11 月に北京で開通した。国旅集団出入境服務公司・中国国際経済諮詢公司・上海中泰実業公司の 3 社がこのシステムを通じて出国検査契約を行い、2004 年 8 月の中国電子署名法公布後初めての、安全電子印章署名による電子契約となった。

関係者によると、これは世界初の複数契約者による安全電子印章同時オンライン契約で、中国の印章史上に革命的な一ページを開くと同時に、2005 年 4 月の中国電子署名法実施に向けての助走ともなった

安全電子印章には電子スタンプと電子サインがあり、国家規格に合致する印章・印影を暗

号化して関連主管部門が認可した電子証書に使用、国家密碼管理委員会弁公室が授権した暗号のプライベート鍵を作成する。複号化はインテリジェントキーとパソコンの関連操作だけでよい。

●地方政府の取り組みー北京の「ディジタル・シティ」ー

北京は「ディジタル・シティ」構想を発表した都市の1つである。北京の場合、重要性が高いのは、実用的な電子政府プラットフォームを構築することとされた。北京の電子政府オンライン・サービス・プラットフォーム（eservice.beijing.gov.cn）は、2002年9月25日にサービス提供を開始した。この新しいサイトは、個人ユーザがこのウェブサイトからIDカード再発行を申請したり、入出国申請書をダウンロードしたりできる。企業も、このサイトを使って、多様な報告書を提出したり、展示会の座席を登録したり、取引の契約書を記入したりすることができる。北京の電子政府主要プロジェクトは以下のものである。

・E-ビジネス
・市民向け科学情報ネットワーク
・社会保障と地域サービスの情報化
・空間情報システム・エンジニアリング・プロジェクト


北京市政府調達センター・ログイン画面
http://www.bgpc.gov.cn/CALogin_Normal.aspx

●地方政府の取り組みー深圳市の電子政府ー

広東省・深圳市が中国初の「国家電子政府試験都市」となったことを受け、市民・企業向けサービス・外部ネットワークサイト「深圳市政府オンライン」と関連機関サイトとのリンクが進んでおり、サービス利用時の利便性が向上する見通しである。「深圳市政府オンライン」には47の政府機関の審査事項が掲載されており、500項目に及ぶ業務ガイドの閲覧や60種類のオンライン申告が可能になる。

電子政府化は今後も進められ、2010年までに深圳市の政務情報、行政手続きの問い合わせや申請がインターネット上でできるようになる。また、行政認可項目の6割以上でオンライ

ン処理が可能になる予定である。


深圳市電子証明書認証センター・デモ画面
http://www.szca.gov.cn/testca.htm

●参考文献

財団法人日中経済協会北京事務所　情報化協力室（CICC 北京）
http://www.ciccbj.org.cn

中国情報局 NEWS
http://news.searchina.ne.jp

株式会社 NTT データ　アジアマンスリーニュース　2002 年 10 月号
http://e-public.nttdata.co.jp/f/repo/49_asia200210/asia200210.asp

## 2.2　香港

(1) 背景／国の方針、法律

一国二制度の原則の下で中国に返還された香港では、返還後 50 年間にわたって、外交・防衛政策以外の分野では独自の政策・制度をとる自由が約束されている。情報政策、電子政府構築に関しても例外でなく、大陸とは別の動きをとってきた。返還直後の 1998 年に、香港特別行政区（HKSAR：Hong Kong Special Administrative Region）の政庁長官（Chief Executive）は“Digital 21 IT Strategy”を発表、2001 年、2004 年に戦略を見直すことにより、進歩を続けてきた。

●ESDLife

この戦略のもとで構築された市民向け公共サービスポータルである「生活易」(ESDLife)は、2000年末に開設されたが、早くもその翌年には、定評ある“Stockholm Challenging Award”を公共サービス部門で受賞している。また、香港では官民の緊密な協力関係のもとで電子政府の構築が進められていることも大きな特徴であり、「生活易」サイトも民間サービスとの相乗りサイトである。また、貿易EDIを支援するサービスも、民間の貿易関連企業と政府との合弁事業として行われたものである。

内容は行政手続のワンストップサービス、公的サービス情報へのアクセスなど、世界有数の高度性を有している。多数のサービスメニューには、税金支払などPKIに基づくアプリケーションも多い。

こうした手続きを行うための行政情報のキオスク端末は、香港各主要地点の駅や、スーパーマーケット、ショッピングモール、市民センターなどの施設や政府関係の施設などに設置されている。

「生活易ESD Life」の特徴は、政府と民間企業がポータルサイトを共有し、市民が政府のサービスと民間の電子商取引の両方を利用できることである。政府のサービスは、約200種のサービスを「生活易ESD Life」を介して提供している。また、政府との金銭的なやりとりは、電子的な支払いが可能となっている。一方、民間企業のサービスとしては、さまざまなオンラインショッピングが可能となっている。

表 1.2-1 ESD Lifeサービス一覧（抜粋）

| | 電子証明書 | 電子証明書もしくはパスワード |
|---|---|---|
| レジャーリンク | | |
| 香港スマートIDカードへのサービス予約手続き | | |
| 身分証明書の登録手続き | | |
| 運転免許試験予約および予約手続き | | |
| 結婚申請手続き | | |
| 住所変更 | | |
| 政府書籍 | | |
| 自動車証明書申請 | ○ | |
| 香港統計書籍 | | |
| 香港考試及評核局書籍 | | |
| 住所変更（運輸局） | ○ | |
| 住所変更（税務局） | | ○ |
| 税務申告 | | ○ |
| ボランティア計画申し込み | | |
| 有権者の住所変更 | ○ | |

| | | |
|---|---|---|
| 公衆審査登録 | | |
| 対話型税問合せ | | ○ |
| ビジネス登録の変更 | ○ | |
| 有権者登録申請 | ○ | |
| 誕生／結婚／死亡診断書の検索およびコピーの申請 | | |
| 住所変更（管選収益管理人） | ○ | |

○以外は ID・パスワードを利用

(http://www.esdlife.com)

(2) インフラの状況／IC カード、eID、証明書発行主体

●スマートカード

香港政府は、紙ベースの身分証明書を IC カードに切り替えるプログラムを 2003 年 8 月より開始し、4 年間で 11 歳以上のおよそ 700 万人の香港在住者を更新する予定である。新しい ID カードは、生まれた年次によって分けられたグループごとに発行されている。

このプログラムでは、IC カードへの切り替えをするだけでなく、インターネットで安全な電子商取引が行える「e-Cert」や、図書館カードなどの多機能な付加価値アプリケーションを導入することを主な目的としている。

またこの ID カードは、2004 年には、出入国の自動審査設備の利用、さらに 2006 年には、運転免許証の役割として利用できるようになった。これは、カード上の IC チップに他のアプリケーションを追加することのできるメモリ容量があるために、これらのサービスの実現を可能としている。

IC チップ内には、親指の指紋データが保管されているが、更にそれらのデータをより一層安全に保護するために、データ検索の際には必ずスマート ID カードと端末間での認証（Authentication）が求められる。

IC チップには耐タンパ性がある為、必要なアクセスキーや権限を持たない場合、チップ内のデータの参照、変更は一切できない。


スマート ID を利用すると、初年度は無料で香港ポスト e-Cert を選択することができる。香港ポスト e-Cert は、電子銀行サービスの他、電子政府サービス、オンラインエンターテイメント、株式取引および支払いのような商業目的にも使用することができる。例として大新銀行では、スマート ID 開発の支援、そして顧客が安全で信頼できる電子銀行業務の享受を可能にするために、e-Cert を利用した電子銀行サービスを導入している。

香港特別行政区政府に認定された認証局によって発行された電子証明書は PKI を適用し、

電子交易条令（ETO）によって法律上保証される。電子証明書は、オンライン処理での「身分証明書」となり、また、オンライン銀行取引で銀行と顧客双方の本人確認の証明となる。電子証明書で、安全で信頼できる環境でオンライン銀行取引することができる。

●認証局

電子証明書は以下の認証局で発行される。

・香港ポスト（HongKong Post）

格納媒体：スマートIDカード、フロッピーディスク、i-Key、他のスマートカード、USBトークン

・DisiSign

格納媒体：フロッピーディスク、スマートカード、USBトークン

○香港ポスト証明書のタイプと有効期間について

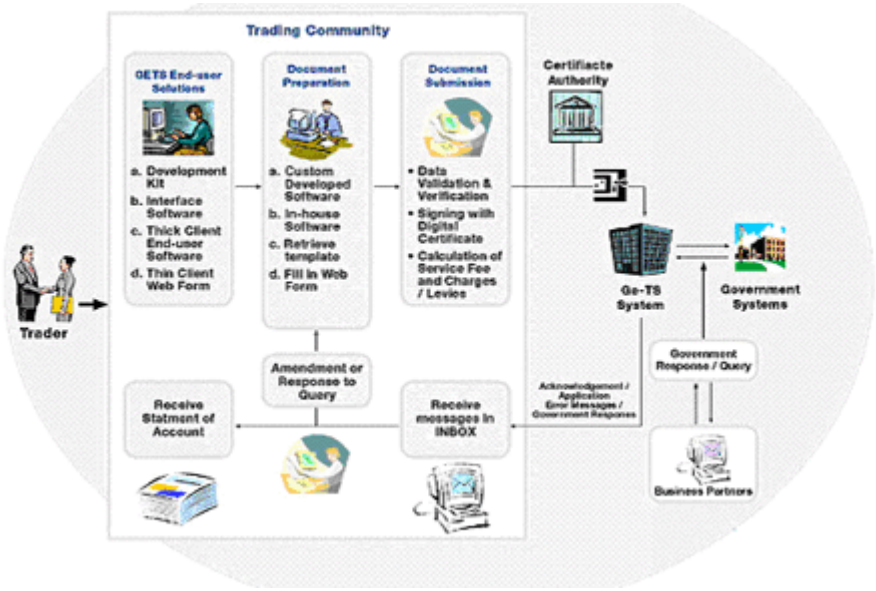
| 証明書タイプ | 有効期間 | 備考 |
|---|---|---|
| e-Cert（個人） | 3年 | |
| Bank-Cert（個人） | 3年 | |
| e-Cert（団体） | 1年もしくは2年 | |
| e-Cert（Encipherment） | 1年もしくは2年 | |
| e-Cert（サーバー） | 1年もしくは2年 | |
| Bank-Cert（法人） | N.A. | もともとの1年間有効期限の変更はなし |

（http://www.hongkongpost.gov.hk/product/ecert/type/index.html）

(3) 公共（申請・納税）

●政府電子貿易システム（GETS）

G2B分野でのPKI適用事例としては、政府電子取引サービス（GETS）が挙げられる。GETSは、輸出入に伴う関税申告などの申請・届出手続きをワンストップサービスで提供しているもので、Global e-Trading Services Limited、Tradelink Electronic Commerce Limitedが運営を請け負っている。




http://www.ge-ts.com.hk/en/service.html

●政府電子調達システム（ETS）

電子調達は、民間部門でｅジネスの採用を促進し、政府調達プロセスの効率を良くするために重要なイニシアチブとして開始された。この香港調達省が監督する電子入札システム（ETS）にもPKIが適用されている。ETSでは、政府調達関連の情報提供及び電子入札手続に関するワンストップサービスのアクセスに電子証明書が用いられている。香港調達省は2003年終わりまでに目標としていた電子入札80%を達成し、政府の電子調達戦略を推進ためのコンサルタント業務を2006年半ばに完了している。

ETSは、政府とオンラインで取引するため、世界中からサプライヤを集め、2005年には、30か国からの約3,000のサプライヤがETSユーザの登録を行った。

●参考文献

（財）国際情報化協力センター
http://www.cicc.or.jp/japanese/asiadenshi/hongkong.html

Dah Sing e-banking Service
http://www.dahsing.com/dsb/rbd/html/eb_main_01_e.htm

香港政府電子貿易システム
http://www.ge-ts.com.hk/en/service.html

香港政府電子調達システムサイト
http://www.info.gov.hk/digital21/e-gov/eng/init/procure.htm

マルトス推進協議会

www.multos.gr.jp/multos_intro/pdf/cs1_hong_kong_ID_j.pdf

## 2.3 台湾

(1) 背景／国の方針、法律

台湾政府では、1998 年に開始したオンライン税申請サービスから政府認証機関の設立を行ってきた。それから 3 年後、2001 年 4 月に発表された「電子化政府推進計画」(2001-2004 年)に基づいて、政府の強いリーダーシップの下、PKI を活用した安全性の高い電子政府実現をするため、環境整備が進められた。現在は PKI を利用した 900 近くのサービスが展開されている。

(2) インフラの状況／IC カード、eID、証明書発行主体

●スマートカード

「推進計画」では、身分証明証と健康保険証を一体化したスマートカードの導入が盛り込まれている。しかし、個人 ID を多目的に利用することについては、当初プライバシー保護の観点からの大きな批判があったが、2006 年 11 月 27 日現在 1,032,300 名の発行実績があり、2005 年には 2,132,650 件、3,782,096 件の利用が報告されている。

住民向け認証個人認証は 2003 年 4 月から開始されており、住民向けの内政部認証管理センター (MOICA) によると以下のサービスが適用されている。

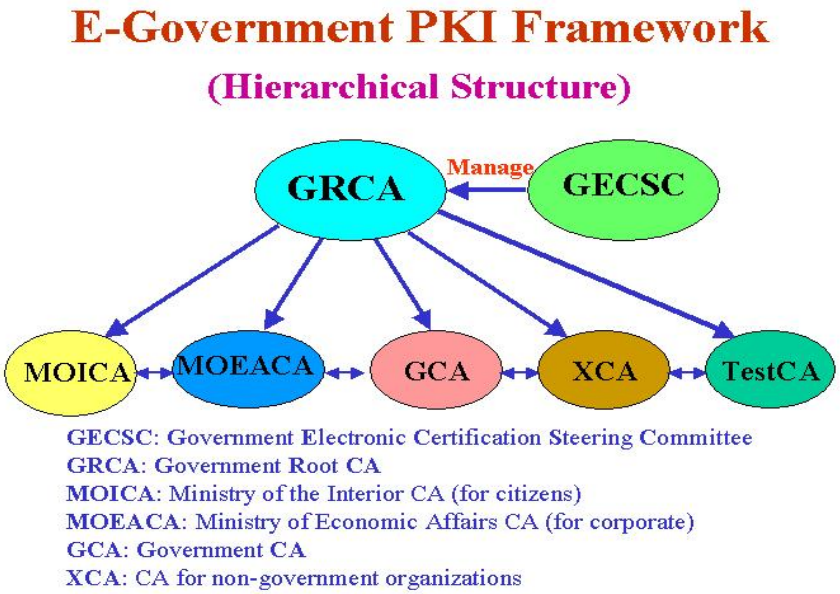
| サービス | 主管機関 |
|---|---|
| 土地管理申請サービス | 内政部 |
| オンライン戸籍登録サービス | 内政部 |
| 入国管理局出国制限問合せ | 入国管理局 |
| 農・労働保険オンラインサービス | 労工保険局 |
| 健康保険オンラインサービス | 中央保健局 |
| 自動車管理サービス | 交通部 |
| 個人税申請 | 財政部 |
| 財務部税ポータル | 財政部 |
| インターネットによる建築物安全検査 | 内政部 |
| 台北市民オンライン・サービス | 台北市政府 |

http://moica.nat.gov.tw/html/index.htm

●認証局

現在政府系の認証局は以下の通りとなっている。

| 名称 | 対象ユーザ | 主管機関 | 発行部数 2006 年 7 月迄 |
|---|---|---|---|
| GRCA | ルート CA | 行政院研究発展考核委員会 | |
| GCA | 政府機関 | 行政院研究発展考核委員会 | 75,082 |
| MOEACA | 法人 | 経済部 | 20,777 |
| MOICA | 一般市民 | 内政部 | 1,006,936 |
| XCA | 学校、財団法人、社団法人、行政法人等 | 行政院研究發展考核委員会 | 12,254 |
| GTestCA | GCA、MOEACA、MOICA、XCA のテスト用 CA | 行政院研究發展考核委員会 | |




http://grca.nat.gov.tw/より

民間認証局は以下の認証局が稼動中である。

| | |
|---|---|
| HiTRUST<br>http://www.hitrust.com.tw | ・主要株主は Acer、HSBC、AIG、ベリサイン等、準民間認証局。<br>・ターゲットは国内金融分野、ケーブルモデム、香港や中国など中華圏とのクロスボーダー取引。 |
| TWCA<br>http://www.twca.com.tw | ・主要株主は、政府系金融会社の 4 社。TSEC（台湾証券交易所）、FISC（財金資訊公司）、TISC（関貿網路公司）、TSCD（台湾証券集中保管公司）。金融分野（銀行・証券）ではほぼ寡占状態。<br>・電子公証、セキュア電子メール、電子株主公証、支払サービスなど付加価値向上に向けた新分野事業も推進。 |

| | |
|---|---|
| Chief Telecom<br>http://www.chiefca.com.tw | ・Chief Telecom が開設。RSA ルート配下の CA と、自社独自の CA の 2 種類を保有。 |

(3) 医療分野

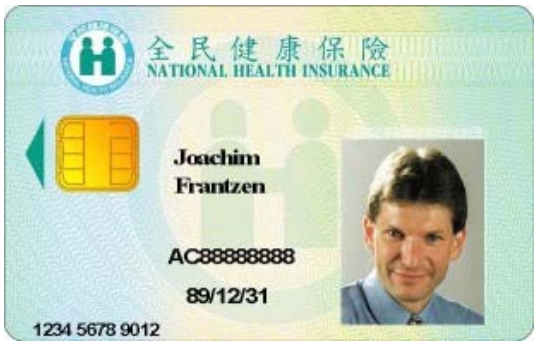
台湾においては、米国の医療政策やセキュリティポリシー (HIPPA など) の影響を受けつつ、ヘルスケア分野において PKI 導入が進みつつある。まず、健康保険カードが紙ベースから IC カード (NHI IC Card、仕様は Java Card) に全面的に変更されたことのインパクトが大きい。電子証明書や電子署名といった PKI アプリケーションは使用されていないものの、2002 年の開始からわずか 1 年あまりでほぼ全人口をカバーする 2200 万枚超の健康保険 IC カードが配布され、2004 年 1 月からは原則的に IC カードのみの運用となっている。

台湾の健康保険制度において、従来の紙のカードでは、母子用や高齢者用などの種類も多く、診療などを 6 回受けるたびに新しいカードと交換する必要があり、さらに他人に成りすまして医療サービスを受けるといった事態が発生していた。IC カードのねらいは、本人確認をしつつ個人情報の盗難を防止するというセキュリティ上の配慮と、有効期限の 5 年間は一枚の IC カードで更新すればよいといった利便性である。2004 年には、約 500 の病院全てと、17,000 超のクリニックの 99%が IC カードに対応した。

PKI が使われているのは、医師などのヘルスケア専門職 (約 20 万人) である。現在、HCA (Healthcare Certificate Authority) が DOH (Department of Health) によって設立されている。IC カード (HPC : Healthcare Professional Card) には電子証明書が格納されている。今後は、処方箋などの EMR (Electronic Medical Record : 診療情報の電子データ) にアクセスし、それを医療機関間で登録、参照する際の認証 (Authentication) と署名に用いられるという。

いわば日本で議論が始まった電子カルテである。

このように、PKI アプリケーションが格納可能な IC カードが普及している台湾のヘルスケアプロジェクトは、非 PKI と PKI の混合モデルであるといえよう




e-政府プロジェクトの目的を達成するために、中央健康保険局は、2006 年 1 月 12 日に電子証明書・SSL を利用したプラットフォームを更新し、サービス業務を拡大した。中央健康保険局は、新バージョンに個人情報検索、更新申請等、いくつかの新機能を加えることを発表した。市民はウェブサイト (http://eservice.nhitb.gov.tw/nhiweb) から市民電子証明書システム

もしくは、アプリケーション・サービス・センター（http://moica.nat.gov.tw）の市民電子証明書管理システムからリンクを行い、国民健康保険の申請、停止、入送金、支払の検索を行うことができる。また支払、更新申請の申請も可能である。国民健康保険局は保険団体、保健利用者に市民電子証明書システムを利用することを推進している。


中央健康保険局　国民健康保険ログイン画面

(4) その他

●B2B の活用

台湾で商取引を行うには政府に報告しなければならず、それを 5 年間保存しなければならない。この Invoice 自体は一般小売など B2C の領域においても使用されているが、e-Invoice は、まず B2B で電子化し、PKI プラットフォームを介して流通させようとするサービスである。現在、主として銀行業の B to B を中心とした SI ビジネスを展開する BankPro E-Service Technology 社では、B to B e-Invoice Added Values Services を提供している。これは、MOE（経済部）の CA を使い、センターを介して売り手と買い手間の Invoice が電子的にやりとりされるという仕組みである。

このモデルの背景には、税収を確実に上げるという政府の意向があり、e-Invoice の仕組みにおいては税務当局がセンターにアクセスすることができる。

●参考文献

行政院研究発展考加来委員会
e-Government Progress in Taiwan (2006/9)

アジア PKI フォーラム　2004 年台北
http://www.asia-pkiforum.org/sept_taipei/2_BankPro.pdf

中央健康保険局
http://www.nhi.gov.tw/english/e_00iccard.htm

内政部認証管理センター
http://moica.nat.gov.tw/html/en/index.htm

台湾イヤーブック 2006
http://www.gio.gov.tw/taiwan-website/5-gp/yearbook

## 2.4 韓国

(1) 背景／国の方針、法律

韓国は 1990 年代中盤から始まったインターネット環境下での情報化と、携帯電話をはじめとするワイヤレス通信の飛躍的普及により、2000 年代の現在、世界的な IT 大国としての地位を確固たるものとした。こうした成果は 1996 年から施行された情報化促進基本法に基づく第 1 次情報化促進基本計画（1996～1998）、サイバーコリア 21（1999～2001）、ブロードバンド IT コリアビジョン 2007（2003～2007）など、国家主導の中長期発展計画が適時、適切な形で打ち出され、体系的に、かつ一貫性を持って執行された結果であるといえる。

●電子商取引やインターネットバンキングなどでの活用

電子署名法の成立を受けて、まず行われたのが、電子商取引における電子署名の利用促進である。

電子署名法が施行された 1999 年には、「電子商取引法」が制定され、電子文書や電子署名の法的効力が認められることとなり、電子署名の応用領域が拡大した。また、消費者保護を目的として 2002 年に定められた「電子商取引消費者保護法」は、インターネット上の電子商店が証明書を取得して取引画面に表示することが義務付けられ、事業法人による証明書の取得が増加した。一方、インターネットにおいて未成年を対象にしたゲーム、成人対象のサイトなどにおいても、それらの利用にあたって成人証明を行う際に証明書が用いられている。

更に電子署名法が改正された 2002 年には、改正電子署名法が求めた政府の電子署名の安全性向上及び利用促進策の一つとして、行政自治部は、インターネットバンキングを利用する者に公認電子署名の利用を義務付けた。この公認証明書及び公認電子署名の詳細については後述する。

●韓国における電子署名制度の特徴

韓国の PKI は、認証機関の公認、公認証明書及び公認電子署名の有効性などにおいて、独自の特徴をもっている。

認証機関の公認

韓国で電子証明書を発行する認証機関は、電子署名法第 4 条に政府が公認したものである

ことが求められている。公認を受けない認証機関には、法的な規制や義務がないが、その証明書の利用範囲は実際には制限を受ける。

韓国における認証機関は、国における最上位の認証機関（ルート認証機関）として韓国情報保護振興院（KISA）があり、その下に公認認証機関が置かれる。

2006年11月現在、公認認証機関として認められているのは、以下の6機関である。

| 公認認証機関 | 公認日 |
|---|---|
| 韓国情報認証（SignGATE） | 2000年2月10日 |
| 韓国証券電算（SignKorea） | 2000年2月10日 |
| 金融決済院（YesSign） | 2000年4月12日 |
| 韓国電算院（NCA Sign） | 2001年3月13日 |
| 韓国電子認証（CrossCert） | 2001年11月24日 |
| 韓国貿易情報通信（TradeSign） | 2002年3月11日 |

●公認証明書及び公認電子署名の有効性

公認認証機関が発行する公認証明書を持つことで、公認された電子署名（公認電子署名）を生成することが可能となる。法令等において文書や書面に署名・記名や押印を要する場合、その電子文書に公認電子署名があればよいことが、電子署名法3条により定められている。

公認証明書には、公開鍵情報のほか、氏名、電子メール、住民登録制度に基づく住民登録番号（法人の場合は、登記された事業者番号）などが付加されている。

2005年11月末現在、公認認証機関が発行する公認証明書の発行枚数は、下表の通りおよそ1千万枚を超えている。

**表 1.2-2 公認認証機関が発行する公認証明書の発行枚数（2005年11月末現在）**

| 公認認証機関 | 公認証明書発行数 | 担当分野 |
|---|---|---|
| 韓国情報認証（SignGATE） | 584,000 | 政府関連 |
| 韓国証券電算（SignKorea） | 1,656,000 | 証券 |
| 金融決済院（YesSign） | 7,499,000 | 銀行 |
| 韓国電算院（NCA Sign） | 819,000 | 教育機関 |
| 韓国電子認証（CrossCert） | 81,000 | 一般企業、ISP |
| 韓国貿易情報通信（TradeSign） | 37,000 | 貿易分野 |
| 合計 | 10,677,000 | |

（出所）アイニュースより（http://security.inews24.com）

また、近年、公認電子署名を電子文書に付与する際に、タイムスタンプを付加するサービスの利用も増加している。タイムスタンプは、特定の電子文書および電子署名のデータ（情報）に人工衛星（GPS）から受信した国際標準時間情報（1/1,000～1/10,000秒単位）を偽造・変造が不可能な方法で結合することによって、該当電子文書や電子署名のデータが特定時点

に存在したという事実、および同電子文書等が変更されていないことを確認（保証）してくれるサービスのことである。「電子署名法」20 条は、利用者の申請がある場合、公認認証機関が、電子文書が当該公認認証機関に提示されたタイムスタンプを「確認」することができる旨を定めている。

(2) 金融分野

●電子売掛債権

B2B 電子商取引の活性化、IMF 通貨危機の経験から、2003 年 3 月に電子売掛債権システムが稼動した。このシステムでは、取引銀行が異なる場合での使用、オフライン商取引においても電子決済ができる様考慮され、偽造・紛失等、手形の短所を克服することに成功している。また、電子債権には、電子署名法第 2 条第 3 号の公認電子署名があることが求められている。

このプロジェクトは 2000 年 9 月に電子売掛債権の開発を金融情報化事業の一環として議決され、関連する法整備が行われてきた。

システム構成上の特徴としては、金融共同網（資金決済システム）と同一のネットワークを利用するが、業務処理のためのソフトウェアやハードウェアのみを別途構築した点である。

中央管理機関は銀行業界が共同出資した社団法人で資金決済システムの運営者である「金融決済院」が選定され、手形に準じて当座取引停止等の措置も可能となっている。

利用状況は以下の通りとなっている。

| 区分 | 2002 年 | 2003 年 | 2004 年 | 2005 年 |
|---|---|---|---|---|
| 件数（前年対比） | 9,774 | 37,000（379%） | 57,092（54%） | 105,689（85%） |
| 金額（億ウォン） | 4,430 | 19,460（439%） | 29,081（49%） | 36,384（25%） |
| 平均金額（万ウォン） | 4,500 | 5,300 | 5,100 | 2,900 |

（金融審議会金融分科会第二部会（第 31 回）情報技術革新と金融制度に関する WG（第 17 回）合同会合　資料 2）

(3) ヘルスケア

レセプトの電子化やオンライン請求など、韓国における医療分野の情報化はかなり進展しているようであるが、PKI の活用も始まっている。韓国で認証局 SignKorea を運営する Korea Securities Computer 社によれば総合医療情報システム：OCS（Order Communication System）、医療画像データベース：PACS（Picture Archiving & Communication Systems）、電子診療録：EMR（Electronic Medical Record）などの情報システムにおいて、医師用の電子証明書が用いられ、診療記録への電子署名が行われている。

2004 年、EMR の普及を促進するため、保健福祉部保健産業振興院は、医療機関、関連企業、研究所などの紙カルテ、電子カルテシステム、公認電子署名の専門家から構成された諮問委員会を立ち上げ、医療法への補完として EMR に対する公認電子署名の具体的な指針「電子カルテに対する公認電子署名適用指針」を作成した。同指針では、公認電子証明の主体、公認電子証

明のタイムスタンプ、公認認証書の有効性の確認、公認電子署名の管理責任、電子カルテの保管及び管理などについて、具体的な基準を定めている。

また、保健産業振興院は、医療分野における公認認証機関設立の必要性を唱え、EMR 普及の阻害要因を取り除く為、積極的に取り組んだ。

特に啓明大学校東山医療院では 2002 年医療法改正を受けて、全国の総合病院では初めて電子署名を付与する電子カルテの運用が開始された。これにより、改ざん等の危険から守られた安全な診療録管理が実現し、病院経営における事務処理コストの削減や、病院に対する信頼の向上などの効果を得ることが可能となった。このような医療情報化は、病院の経営陣が大きな関心を示し積極的に関与したことから成功したと言われている。現在は、特定の病院内で利用されているが、近い将来には、病院やクリニックなど医療機関間で診療記録や処方箋の検索、共有が可能になることを目標としている。

このように、1990 年代後半から国立病院、大型病院、新設病院を中心に情報システムの導入が急速に拡大し、2000 年ごろから、EMR の導入も増加した。しかし、EMR の導入における医療機関別に個別化された情報システム開発は、国全体からみれば、重複投資となり、国全体の情報システム開発費用の上昇をもたらすとともに、医療機関間の情報共有が困難になってしまった。また、このような EMR の導入は病院あるいは医師中心のものであり、患者の医療情報の利用が難しいといった問題も顕在化されている。このような状況において、政府は、医療機関間の情報互換性を高め、EMR など医療情報システムの標準モデルを開発するとともに、患者中心であり、国家標準に準拠した電子健康記録（EHR：Electronic Health Record）の開発を医療情報化の重要な課題と定めた。

現在韓国政府は、2010 年までに全国範囲で E-Health サービスを提供する目標を定め、2005 年 12 月に保健福祉部は、実現に向けて「保健医療情報化事業推進団」を設立、今後数年間で研究チーム員総勢 205 人と事業費総額 140 億ウォンを投入する予定である。

EHR 開発事業は、三つの段階で推進していくと計画されている。

・第一段階（保健医療情報化インフラ構築　2004-2005）
　この段階では、主に関連専門家で構成されたワーキンググループ運営及び委員会の開催、EHR のコア技術に対する研究開発の推進、保健医療情報化ロードマップおよび推進計画の策定、関連法律制定案の準備などに取り組む。

・第二段階（公共保険医療機関の適用　2006-2008）
　この段階では、主に各種標準及び EHR コア技術を病院・保健所など公共医療機関での適用、各種標準及び EHR コア技術の民間シフト戦略の準備、国民へ健康情報提供のための基盤構築、保健医療情報化関連法律改正の推進などに取り組む。

・第三段階（民間へのシフト　2008-2010）
　この段階では、主に公共医療機関適用を通じて検証された標準及び EHR コア技術を民間へのシフト、民間シフトのための多様なインセンティブ提供方案の準備、民間における EHR システムの構築・活用に取り組む。

(4) 公共

●電子入札システム

電子調達システムである GePS (Government e-Procurement System) は、すべての政府調達に関わる情報提供と、公示から入札、開札、契約の支払いまでをインターネット上で行うことを目指し、2002 年 10 月からサービスが開始されている。入札参加者はこのシステムを利用するために、公認認証局から発行された電子証明書を使わなければならない。

現在、約 30,000 の公的機関、約 150,000 の企業が同システムに利用者登録しており、2005 年には 1800 万件の入札が 14 万件のプロジェクトおよび調達で実施され、年間の調達総額は約 43.4 億ドルに達した。このような実績を踏まえ、開発と運営を担当する調達庁では、GePS を世界最大の e マーケットプレイスと位置付けている。システムの導入効果としては、調達プロセスの公正性と透明化に加え、約 4.5 億ドルのコスト削減が得られた。

(韓国調達庁発行 An Introduction to the Korean Government's e-Procurement System : www.coti.go.kr/inter/img/8-eProcurement.pdf)

今後は更に利用者の満足度を向上させるため、ウェブコールセンターの設立、CRM (Customer Relationship Management) プログラムといったプロジェクトを立ち上げている。また、PDA を利用したワイヤレス環境からの接続については 2004 年 12 月より試験運用されていたが、2005 年 3 月より運用が開始されている。

●参考文献

株式会社 NTT データ　ワールドレポート　アジアマンスリーニュース　2006 年 12 月号
http://e-public.nttdata.co.jp/f/repo/426_a0612/a0612.asp

株式会社 NTT データ　ワールドレポート　アジアマンスリーニュース　2006 年 5 月号
http://e-public.nttdata.co.jp/f/repo/381_a0605/a0605.asp

株式会社 NTT データ　ワールドレポート　アジアマンスリーニュース　2004 年 11 月号
http://e-public.nttdata.co.jp/f/repo/249_a0411/a0411.asp

KOREA IT TIMES Special Report 2006/06/01
http://www.inkistar.co.kr/it/main_view.php?mode=view&nNum=3425&parts=Special

金融庁ホームページ　金融審議会・金融分科会
http://www.fsa.go.jp/singi/singi_kinyu/base_gijiroku.html#bunkakai

## 2.5 マレーシア

(1) 背景／国の方針、法律、国民性

マレーシアは、マレー系 (65.5%)、中国系 (25.6%)、インド系 (7.5%) などからなる人

口約 2600 万人の複合多民族国家である。立憲君主制（議会制民主主義）を採っている。1991 年、マハティール元首相により、2020 年までに先進国入りを目指すという長期計画「VISION 2020」が発表された。同国政府は、目標達成のためにマレーシアの産業構造を現在の製造業中心からサービス産業や知識集約産業中心の形態へ転換させていく必要があるとの認識から、1996 年 8 月より Multimedia Super Corridor（MSC：マルチメディア・スーパー・コリドール）計画に基づき戦略的に ICT 開発を進めている。なお、強力なリーダーシップを発揮して IT 政策を先導してきたマハティール元首相は、2003 年 10 月末に引退したが、新首相のアブドラ前副首相は、マハティール路線の継承を表明している。

●マルチメディア・スーパー・コリドー計画（MSC）

マレーシアの首都クアラルンプールのシティセンタとプトラジャヤ新行政首都サイバジャヤ・ハイテク都市、新空港を含む 15km×50km の地域に、世界的規模の情報通信産業、研究開発機関、ハイテク製造業およびサービス産業等を誘致して、21 世紀に向けた世界のマルチメディア拠点として発展させようとする国家プロジェクト。最先端の通信インフラ等ハード面での整備に加えて、電子署名法の制定や通信法の改訂などマルチメディアの利用を推進するための法制度や誘致企業への優遇措置等ソフト面での環境整備が用意されている。なお、プロジェクトの中核には、半官半民の企業が多くみられる。

MSC における基幹的な構想（Flagship Applications）として、以下のものがある。

1) Electronic Government：電子政府
2) Multipurpose Card：多目的カード
3) Smart Schools：遠隔教育
4) Telehealth：遠隔医療
5) R&D Clusters：研究開発重点地域
6) E-Business（World Wide Manufacturing Web & Borderless Marketing）
7) TechnopreneurDevelopment：ICT 中小企業、起業支援

マルチメディア開発公社（MDC）

MSC 計画の開発と実現のためにマレーシア政府が 1996 年に設立した国有企業。首相の直轄組織で、官僚政策に依存しない。MSC への企業誘致や、進出企業のニーズに対応する一元的窓口と位置付けられている。

マレーシア電子システム研究所（MIMOS）

科学・技術・イノベーション省（Ministry of Science, Technology and Inovations：MOSTI）の管轄下にある組織。IT に関連した活動を幅広く行う半官半民機関。また、1999 年からはマレーシア発のセキュア・インターネット・プラットフォーム製品として iVEST（internet Virtual Environment for Secure Transaction）の開発に取り組んでおり、この基盤のうえに国民 ID カード MyKad と連携した納税システム向けの e-Filing が構築された。

●電子政府構想

行政サービスの合理化、国民に対する行政サービスの質の向上を目指すものであり、現在は以下の９つのプロジェクトに取り組んでいる。

1) Project Monitoring System (PMS)
…プロジェクト監督システム、公共サービスにおける共通システム
2) Human Resource Management Information System (HRIMS)
…人材管理システム、公共サービスにおける共通システム
3) Generic Office Environment (GOE) …業務電子化による生産性向上
4) Electronic Procurement (EP) …電子調達
5) Electronic Delivery Services (E-Services++) …ワンストップ行政サービス
6) Electornic Labour Exchange (ELX) …電子職業安定所
7) E-Courts…電子法廷
8) E-Syariah…Syariah (イスラム法) における裁判の迅速化
9) E-Land…国土管理の効率化・有効化

●MyICMS 886

エネルギー・水道・通信省 (Ministry of Energy, Water and Communications) は、2005年12月､2006年から2010年までの通信とマルチメディアに関する青写真となるMy ICMS 886を発表した。My ICMSは、マレーシア情報通信マルチメディアサービス戦略 (The Malaysian Information, Communication and Multimedia Services strategy) を表しており、886は8つのサービス、8つのインフラ、6つの成長領域を示している。

【8つのサービス】高速ブロードバンド、3G携帯電話、モバイルTV、デジタルマルチメディア放送、デジタルホーム、RFIDを使った短距離通信、VoIPとインターネット電話、ユニバーサルサービスの提供
【8つのインフラ】統合ネットワーク (multi-convergence networks)、3G移動体通信ネットワーク、衛星通信ネットワーク、IPv6、情報ネットワークセキュリティ、など
【6つの成長領域】コンテンツ開発、ICT教育ハブ、デジタルマルチメディア受信機 (セットトップボックス)、VoIPなどの通信機器、RFIDなどの組込部品、海外ベンチャー

◆法律

●サイバー法 (Cyberlaws)

MSCの一環としてIT関連の法律が制定・改正されており、サイバー法と総称される。

1) Digital Signature Act 1997：電子署名法 (1998.10施行)
2) Copyright (Amendment) Act 1997：著作権法改正法 (1999.4施行)

3) Computer Crimes Act 1997：コンピューター犯罪法（2000.6 施行）
4) Telemedicine Act 1997：遠隔医療法（1997.6 制定）
5) Malaysian Communications and Multimedia Commission Act 1998：通信及びマルチメディア法（1999 年 4 月施行）
6) ELECTRONIC COMMERCE ACT 2006：電子商取引法

●電子署名法

電子署名法において、電子署名とは非対称（公開鍵）暗号システムによるものと規定されている。また、免許を受けた認証機関しか認証事業を営むことができない。認証機関及び認証書に関しても、詳細な規定が置かれており、認証書の発行・取消し、認証機関の保証、認証書の有効期間、認証機関の責任限度など、CPS（Certification Practice Statement：認証業務規程）で規定されるような事項まで言及されている。更に、電子署名の効果に関し詳細な規定を置いている。この他、タイムスタンプに関する規定や、刑事手続に関する規定が置かれている。

(2) インフラの状況／IC カード、eID、証明書発行主体

●電子署名法と認証局

マレーシアの電子署名法では、Establishment License と Operational License という 2 つのライセンスが定められており、Establishment License とは、建物や場所の権利などのインフラを持ち、認証局を建てるためのライセンスであり、Operational License とはエンティティを認証し、証明書を発行するなど、つまり認証局を運営するためのライセンスである。Operational License を取得するためには KPMG Malaysia などの監査法人から監査を受けなくてはならず、監査後に政府に対してレポートが提出される。また、その後も毎年監査が入る。

(i) Digicert Sdn. Bhd. (http://www.Digicert.com.my/)

Digicert 社は、マレーシアの郵政公社 POS Malaysia 社と通信マルチメディア省傘下のマレーシア電子システム研究所 (MIMOS) の合弁企業である。株式は POS が 55 パーセント、MIMOS が 45 パーセント所有。Digicert 社では Establishment License を 98 年に、Operational License を 99 年に取得した。電子政府関連の認証サービスを独占しており、ワイヤレス PKI、ID マネジメント、電子公証などの付加価値サービスを検討中。

(ii) MSC Trustgate.com Sdn. Bhd. (http://www.msctrustgate.com/)

トラストゲート社は、マルチメディア開発公社 MDC とベリサインが出資する企業である。

主な顧客基盤は金融（国内・外資系）、多国籍企業のマレーシア拠点であり、G2B 電子調達向けタイムスタンプ機能を担当事業者（e-Perolehan 社）に提供している。

(iii) Bank Negara Malaysia (http://www.bnm.gov.my/)
名前の通り、マレーシアにおける中央銀行である。

マレーシアでは半官半民系の認証局による寡占状態のため、認証局間の相互運用性確立に向けた動きは見られない。政府認証局が存在しないこともあり、Digicert 社の主な顧客基盤は公共分野で、ほぼ独占状態にある。一方、MSC Trustgate 社の顧客基盤は金融分野と多国籍企業である。両社とも現下の市場環境が思わしくないことから、Digicert 社はワイヤレス PKI やタイムスタンプ、電子公証、ID マネジメントなどの高付加価値サービスの提供を検討している。また、MSC Trustgate 社は既にタイムスタンプサービスを、政府向けの電子調達サービスプロバイダである ePerolehan 社に提供している。

●多目的カード (Multipurpose Card)
政府と民間で共用できるスマートカードプラットフォームの提供を目的とし、Government Multi-Purpose Card (GMPC) と Payment Multi-Purpose Card (PMPC) が開発された。MyKad は GMPC、Bankcard は PMPC の推進の為の製品である。

GMPC Applications (MyKad)
1) National ID
2) Driving License
3) Passport Information
4) Health Information
5) Touch N Go
6) MEPS Cash (電子マネー)
7) ATM
8) Public Key Infrastructure

PMPC Applications (Bankcard)
1) ATM
2) e-Debit
3) MEPS Cash

図 1.2-2 MyKad

MyKad は国民 ID カードとして配布され、表面には写真が貼付される。免許証、パスポート、電子マネー、カルテ、PKI など多様な機能を持っている。2005 末には、紙ベースの ID から MyKad への移行が完了した。技術についてはプロトン社、製造についてはアイリス社が請け負っているとのこと。
MyKad の申請費用は無料であったが、2006 年 1 月 1 日以降は費用が発生する。海外居住者を含めて全国民に申請義務があり、申請後三ヶ月以内にカードを受領しない者には、病気等正当な理由がある場合を除いて罰金が科せられる。なお、MyKad には PKI の鍵ペアを入れる

ことができるが、実際に鍵ペアを入れるかどうかについてはカード発行の際に、ユーザの意志で選択ができる。入れる場合には 50 リンギッド（1500 円程度）を支払う。また、証明書の発行を受ける認証局についても Digicert 社かトラストゲート社のどちらかを選択できる。しかし、これまでのアプリケーションメニュー5 種（国民 ID、運転免許証、パスポート、健康情報、電子マネー）は、いずれも非 PKI 仕様となっていた。最近では、電子申告の e-Filing にて PKI を利用しており、今後の MyKad は非 PKI モデルから非 PKI・PKI 混合モデルに移行が進む見通しである。

(3) 金融部門

マレーシアの国内銀行が約 10 行あり、その内の 2 行が PKI を用いたインターネットバンキングに参加している。また、保険会社では、顧客に PKI（スマートカード）を使用させているという例がある。

(4) 医療分野

マレーシア健康省 MOH（Ministry of Health）では、MyKad 活用を含めて遠隔ヘルスケアが計画されている。

(5) 公共（申請・納税）

●eProlehan（電子調達）

G2B の PKI の利用例として、電子政府構想の 1 つである電子調達システム（EP：Electronic Procurement）がある。政府電子調達システム ePerolehan の実装および運用の独占権を与えられている Commerce Dot Com Sdn Bhd と NTT データが共同で開発にあたった。

ユーザは MyeP スマートカードによりシステムを利用するが、このカードの中には、ユーザプロファイルと、マレーシア政府公認の CA により発行された証明書が格納されている。この証明書の使用により、全ての取引データが合法的かつ有効なものとして取り扱われる。

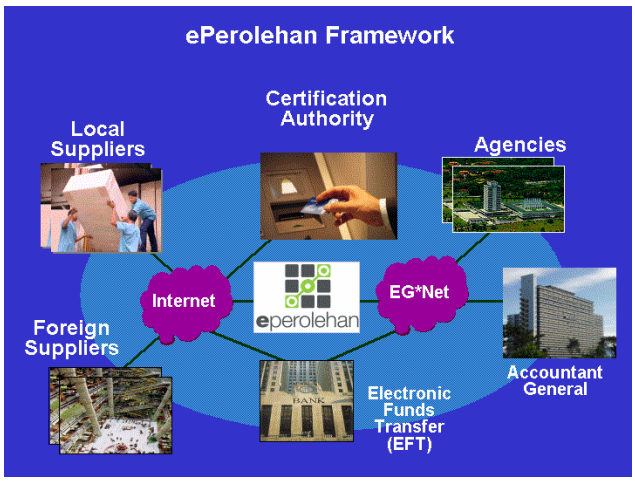



図 1.2-3 ePerolehan Framework


図 1.2-4 MyeP

●電子納税（MyKey + e-Filing）

2004年5月、LHDNM（Lembaga Hasil Dalam Negeri Malaysia：国税庁）は法人税申告のオンライン受付を開始した。まず、国税庁のウェブサイトより申告書をダウンロードし、記入後にMyKeyと呼ばれる証明書を使って電子署名し、e-Filingにより送信する。その際、スマートカードリーダにMyKadを挿入して認証をうける。また、2004年8月、MSC Trustgate社はMyKeyを含んだスマートカードをマレーシア国内の企業1000社に対して配布した。オンラインで税申告を行う企業は関連書類を国税庁に送信する必要はなく、国税庁による監査に備えて関連会計書類を保管しておくだけで済む。

2007年2月現在、一般市民もMyKadに格納したMyKeyを使ったオンライン税申告が可能になっている。MyKeyとして発行される証明書は2種類。1つは、電子署名および鍵暗号化用のAuthentication証明書。もう1つは否認防止用のNon-Repudiation証明書。納税者は、Borang CというExcel形式の申告ファイルをダウンロードし、必要事項を記入後MyKadの中のAuthentication証明書により署名し、e-Filingによりアップロードする。

2007年からはe-Bayaranが導入され、Bank Islam Malaysia Bhd, CIMB Bank（BCB account only）, Hong Leong Bank Bhd or Public Bank Berhadにインターネット・バンキングのアカウントがあれば、Financial Process Exchange（FPX）により支払いも可能になる模様。

●参考文献

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に関わる法制度及びビジネス環境の動向に関する調査報告書」、（財）日本情報処理開発協会、平成14年3月、
http://www.japanpkiforum.jp/shiryou/business_k/biz01_rep_all.pdf
平成14年度EC技術基盤の相互運用性に関する調査研究事業（普及阻害要因当の調査及び国際的ルールの検討）「PKI関連サービスビジネスの動向と今後の展望に関する調査報告書―欧米および日本・アジアでの展開―」、（財）日本情報処理開発協会、平成15年3月、
http://www.japanpkiforum.jp/shiryou/business_k/b02report.pdf
平成15年度EC技術基盤の相互運用性に関する調査研究事業（PKI相互運用のための動向調査およびガイドライン作成）「PKI利用モデルの現状と相互利用に関する調査報告書―欧米・アジアでの展開と日本への示唆―」、（財）日本情報処理開発協会、平成16年3月、
http://www.japanpkiforum.jp/shiryou/business_k/b03report.pdf
電子商取引推進協議会（ECOM）、「ベンチマーク報告Ⅱ」～アジア・オセアニア編～、2002年
電子商取引推進協議会（ECOM）、平成16年度　ECの国際化の推進に関する調査研究「海外におけるEC推進状況　調査報告書　2004」平成17年3月
電子商取引推進協議会（ECOM）、平成17年度　ECの国際化の推進に関する調査研究「海外におけるEC推進状況　調査報告書　2005」平成18年3月
（財）日本情報処理開発機構、経済産業省委託調査研究　平成16年度EC技術基盤の相互運用性に関する調査研究「PKI利用に関する動向調査報告書」、平成17年3月
MyKad、http://www.jpn.gov.my/kppk1/index.htm

JABATAN PENDAFTARAN NEGARA、http://www.jpn.gov.my/index.htm
Multimedia Super Corridor、http://www.msc.com.my/#intro=done
Cyberlaws and Intellectual Property Laws、http://www.msc.com.my/cyberlaws/
Flagship Applications Progress Status (as of 30th September 2006)、
http://www.msc.com.my/updates/flagships.asp
財団法人　国際情報化協力センター（CICC)、CICC　特別報告「ELECTRONIC GOVERNMENT IN MALAYSIA」、Salmah Khairuddin Malaysian Administrative Modernisation And Management Planning Unit　(MAMPU) Prime Ministers's Department, Malaysia、2005.11.21、
http://www.cicc.or.jp/japanese/kunibetsu/pdf_ppt/Malaysia-CIO_JAPAN%20version%202.pdf
財団法人　国際情報化協力センター（CICC)、「日機連17高度化-3　アジアにおけるIT産業の現状と今後の戦略に関する調査研究報告書」、2006年3月、
http://www.cicc.or.jp/japanese/tyousa/pdf_ppt/②-H17受託調査_アジアにおけるIT産業の現状と今後の戦略に関する調査研究報告書.pdf
財団法人　国際情報化協力センター（CICC)、「アジア情報化レポート2005　マレーシア」、2005年、http://www.cicc.or.jp/japanese/kunibetsu/pdf_ppt/マレーシア%20情報化レポート.pdf
政府調達（公共事業を除く）における契約の電子化のあり方に関する検討会（第7回)」資料「事例紹介　マレーシア電子調達システム」、株式会社　NTTデータ、2004.9.9、
http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/seifu_chotatu/pdf/040909_1_05.pdf
株式会社NTTデータ、アジアマンスリーニュース　2003年7月号「アジア・オセアニアで進む調達制度改革を通じた電子調達の実現」、2003年7月、
http://e-public.nttdata.co.jp/f/repo/153_a0307/a0307.asp、
Commerce Dot Com Sdn Bhd、http://www.commercedc.com.my/
ePerolehan、http://home.eperolehan.com.my/en/default.aspx
MyKey、https://www.mykey.com.my/Website/home.php
e-HASiL、https://ef.hasil.org.my/English/index.asp
Contactless News、Malaysia issues dual interface 'MyKad' ID card nationwide、
http://www.contactlessnews.com/library/2004/09/30/malaysia-issues-dual-interface-mykad-id-card-nationwide/、2004/09/30
INDUSTRY PERFORMANCE REPORT 2004、Malaysian Communications and Multimedia Commission、
http://www.cmc.gov.my/what_we_do/Research/ipr/IPR%202004.pdf、2004

## 2.6　シンガポール

(1) 背景／国の方針、法律

●シンガポールのICT政策

シンガポールの国家的情報化政策は、1980年から5年間を対象とした「国家コンピュータ

化計画（National Computerization Plan)」に始まる。以降、「市民サービス・コンピュータ化計画（CSCP：Civil Service Computerization Programme、1982～)」、「国家 IT 計画（NITP：National IT Plan、1986～1991)」、「IT2000（1992～1999)」、「Infocomm21（2000～2003)」、「Connected Singapore（2003～2005)」と次々と策定される計画に基づき情報化が推進されてきた。

現在、シンガポールは今後 10 年間を対象とした、ICT の次期国家的マスタープラン「Intelligent Nation 2015（iN2015)」の策定に取組んでいる。同計画は、2005 年 3 月に策定が発表され、シンガポールにおける全てのステークホルダーが ICT の恩恵に与ることができるよう、広く政府・市民・企業から意見を集め、2006 年施行開始を目指して策定作業が進行中である。

(2) 金融部門

●シンガポールの銀行間支払

銀行間取引での活用が顕著に見られる。例えば、銀行間での手形／小切手交換を行うクリアリングハウスシステムで 2003 年 7 月に稼動した CTS（Check Transfer System）では、手形／小切手の受け取り銀行、クリアリングハウス、手形／小切手の支払銀行間で、セキュアな環境下での完全電子化を実現している。銀行間で個口決済を行う eGIRO（電子送金）でも PKI 並びに VPN が適用されており、eGIRO（電子送金）のメンバー銀行は Web ベースで公共料金の振り替えなどを行うことが可能となっている。

(3) 公共

●政府調達の電子的統合（GeBIZ)

財務省は、政府とサプライヤとを電子的に結ぶことで、政府調達のバリューフォーマネー（VFM）を高めることができると考え、1990 年台中頃より電子調達システムの構築を進めており、1996 年には、電子調達システム（EPS）を完成させた。EPS は、政府調達に要する時間と費用を削減するとともに、政府調達に関わる予算統制を向上させた。一方、サプライヤにとっては、煩雑な事務の削減や支払いの迅速化を通じて、費用削減や資金運転の改善などの効果が得られたとされる。

その後、財務省は、EPS をさらに発展させ、サプライヤがワンストップで政府調達のすべての機会にアクセスできるようにする目的で、政府電子ビジネス（GeBIZ）システムの構築を進めてきた。本システムは、2003 年 6 月から本格的に稼動している（表 1.2-3)。

表 1.2-3 GeBIZ の概況

| 項目 | 概況 |
|---|---|
| 参加している政府機関 | 120 |
| 利用している政府職員 | 12,474 |
| 登録したサプライヤ数 | 14,529 |

| | |
|---|---|
| 入札金額の総計 | 年平均 100 億 SGD |

Government Electronic Business
Last updated on 01 October 2006
http://www.business.gov.sg/EN/ResourceLibrary/OnlineArticles/asme_sucess-gebiz.htm

GeBIZ では、サプライヤの事前登録、意見招請や公告、モール型調達、要求仕様（RFP）による調達、契約やサプライヤへの支払い、政府財産のオークション、財務システムへの連携など幅広い機能を提供している。

シンガポールでは、EPS や GeBIZ などの電子調達による効果が一層発揮されるよう、政府調達制度も改革されてきた。中でも、調達品目の金額に応じて調達手続きを柔軟に運用する方法が、電子調達、中でもモール型調達の利点を大いに引き出している。

それは、調達 1 件あたりの金額について、3,000SGD（1SGD を 75 円として、225 千円）以下、3,000SGD ドル超から 70,000SGD（同、5250 千円）以下、70,000SGD 超に区分し、区分毎に異なる調達方法を適用するものである。

3,000SGD 以下の調達は、少額調達と呼ばれ、公告や入札の手続きを省くことができる。GeBIZ では、少額調達に向けて、モール型調達を実現している。

3,000SGD 超から 70,000SGD 以下の調達では、調達官と監理官の職務牽制を通じて、簡易入札が実施される。70,000SGD 超の調達では、商品によって、公開入札、入札企業選択（要求仕様が複雑なもの）、入札企業制限（国家機密に関わるもの）の 3 種類が選択され、入札が実施される。GeBIZ ではこれらに要する政府とサプライヤの業務を電子化したワンストップサービスを提供している。

このような方法が合理性を持つのは、政府調達においては、調達件数の大部分を少額調達が占める一方、調達金額の多くを高額の調達が占めている現状がある。少額品は一般に、コモディティ（日用品）であり、要求仕様などの入札仕様書を詳細に作成する意味合いが薄い。また電子カタログでは、サプライヤが自由にいつでも価格を改定することができるため、商品やサービスの価格が市場の実勢を反映した価格に設定される利点が生じる。

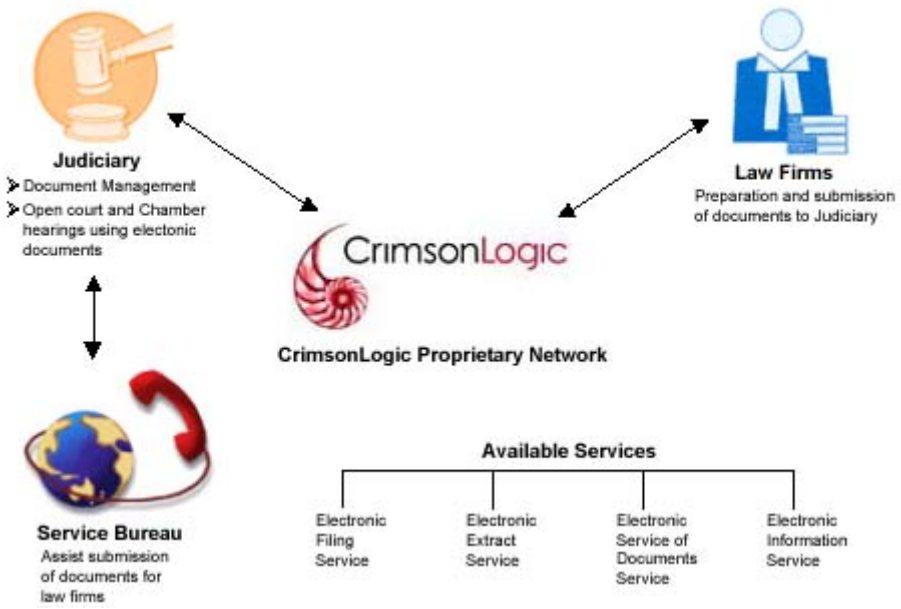
一方、調達官は、少額品の調達で削減された時間を使って、政府調達金額の多くを占める高額な調達をより効率的に実施することができる。

シンガポールでは、以上のような政府調達の改革を通じて、電子調達の効果を確実に獲得している。

●シンガポールの裁判所 e-filing

シンガポールでは、EFS（Electronic Filing System）という電子訴訟申し立てのシステムが 2000 年より稼動している。このシステムでは、民事・刑事を問わずインターネットから訴訟の申し立てが可能である。尚、EFS 利用の際に必要となる弁護士の電子証明書は最高裁判所が IC カードで発行している。訴訟の電子化は、検索、持ち出し、保管といった、紙のファイル管理から弁護士を解放するとしている。

EFSは2つの主なモジュールから成り立っており、フロントエンドシステムの利用により、法律事務所から電子的に法廷文書を保管することができる。所管官庁局は、同様なフロントエンドシステムを利用し、法律事務所用の文書を保管する。法律事務所の申請はワークフロー・システムに支援され、裁判所の職員の作業プロセスのために使用される。




http://info.efs.com.sg/default.htm

認可基準は次の様になっている。

1. EFS フロント・エンド・アプリケーションを導入していること。
2. 法律事務所の少なくとも 1 人が、LawNet トレーニング・センターによって実施されるトレーニングコースを受講していること。
3. 法律事務所から、少なくとも1回、EFS を経由して、申請を裁判所に提出し、受理されていること。
4. 法律事務所の少なくとも 1 人が有効な EFS 電子証明書を保有していること。

●電子建築確認申請

建築確認申請の業務を電子化した「コアネット（CORENET)」と呼ばれるシステムを政府が先行して3次元システムを導入した。

コアネットとは、大きく分けて、建築確認申請の(1)書類の電子提出（システム名：e-Submission)、(2)設計の法規チェック（同：e-PlanCheck)、(3)建設業務に関わる法規や企画などの情報提供（同：e-Info)、という 3 つのシステムからなり、このうち(2)の「e-PlanCheck」に3次元CADの技術を導入している。

この「e-PlanCheck」では、建築確認の申請者がビルの設計図を 3 次元 CAD で作り、それを「IFC」という建設業界向けの共通フォーマットで保存、そのデータをシンガポール政府

の建設局（BCA）のサーバーにアップロードする。

すると、そのデータを「e-PlanCheck」というシステムが設計上の制限事項や防災、バリアフリー、設備分野などについて法規チェックし、その結果をWEBブラウザやPDF形式の文書で申請者に知らせる。

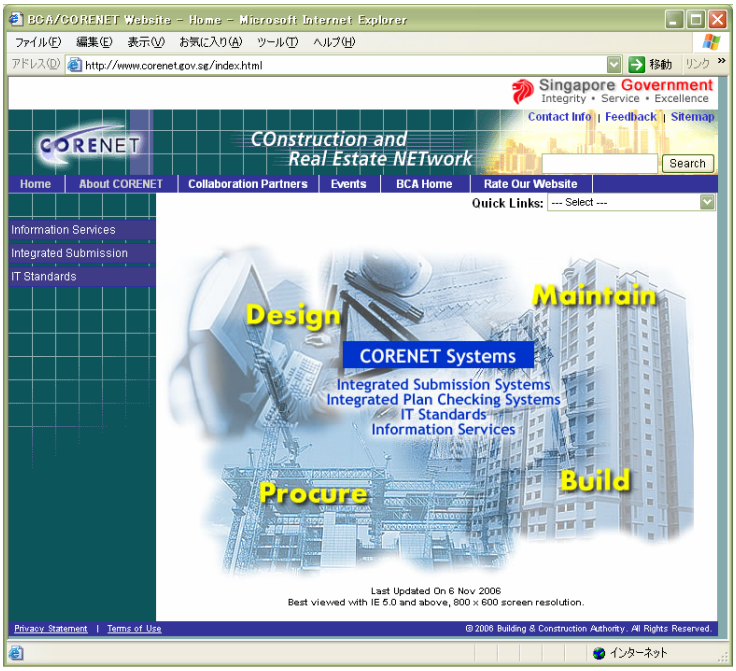
このシステムでは設計に法規や条例に矛盾した部分があると、画面に表示された3次元モデル上にその部分が目立つようにマーキングされる。また、正式申請の前にテスト的に設計データをサーバーにアップロードできる為、問題点がないかを事前にチェック、解決した後、正式な建築確認申請として提出が可能となっている。このことにより、申請者作業軽減が図られている。

この e-PlanCheck システムは、2000 年に開発が始まり、2004 年から実証実験や実展開準備のための運用が行われている。

しかし、e-Submission システムを通じての電子申請は、2 次元の図面や書類の方がまだ主流となっており、3 次元モデルを使った建築確認申請件数の伸びが期待されている。

建築確認申請での政府側の手続きは、複数の担当部門を経由して行われるため、電子化前では4週間程度要していたが、電子化により1週間に短縮された。

申請側の技術者はNetrust社が発行する、スマートカードもしくは、証明書ファイルの取得を行う必要があり、更に、図面、設計図書の電子化が必要である為、当初はこの手間が煩雑なことから不評であったが、上記のようにトータルのリードタイムが短縮されるというメリットを享受することにより、浸透している様である。




CORENET ログイン画面 www.corenet.gov.sg/index.html

●参考文献

Government Procurement Guide for SMEs
http://www.spring.gov.sg/Content/WebPage.aspx?id=a3028763-3cb9-42a4-b84f-06a9d726569a

株式会社NTTデータ　アジアマンスリーニュース　2003年7月号
http://e-public.nttdata.co.jp/f/repo/153_a0307/a0307.asp

EFSホームページ
http://info.efs.com.sg/default.htm

日経BP社建設・不動産専門情報サイト　KEN-Plats
http://blog.nikkeibp.co.jp/kenplatz/it/3taig/115690.html

## 2.7 タイ

(1) 背景／国の方針、法律、国民性

◆背景／国の方針

タイ王国は総人口 6120 万人の立憲君主制国家であり、国民の国王に対する支持率は非常に高い。タクシン政権は 2001 年 2 月の総選挙で誕生し、外資・外需と内資・内需のバランスをとりつつ発展を目指す「デュアル・トラック（複線型成長路線）政策」を導入し、観光、自動車、ファッション、食品、ソフトウェアなどが重点産業とされた。タクシン首相がコンピュータの輸入会社、ポケベル会社、タイ初の通信衛星打ち上げ、タイ最大の携帯電話会社などに深い関係をもっているという背景もあり、IT振興政策が積極的にとられてきた。しかし、2006年9月にはクーデターにより政権が交代しており、今後の状況に関しては不透明感が残っている。

情報技術（IT）振興の体制としては、まず1992年に、ITに関連する政府および民間代表により国家IT委員会（NITC：The National Information Technology Committee）が設立され、議長を務める首相のもと、タイの IT 発展、利用向上にむけた政策立案を行っている。IT の研究開発については、科学技術環境省の国家科学技術開発庁（NSTDA）の監督下にある半自治的政府研究開発機関である国家電子コンピュータ技術センター（NECTEC）が主導している。

2000年にはIT関連法規の制定、最高情報責任者（CIO）を介した諸官庁における IT 開発の進展を含む電子商取引の発展に関わる多くのプログラムや活動が推進されたが、この先頭に立ったのが NECTEC である。政府情報技術サービス（GITS）プロジェクトと連係して行なわれた政府 CIO プログラムは、統一された政府情報ネットワーク（GINet）を構築する試みであり、GINetは、すべての諸官庁のため、公開鍵インフラ（PKI）を運営している。

またNECTECでは、2001年から10年間を対象としたIT政策推進の基本方針が検討され、

2001 年 10 月に「IT2010」計画として採択、2002 年 3 月に閣議了解された。この IT2010 計画では、技術そのものではなく、知識集約型経済・社会に対応する IT 利用に主眼が置かれ、(1)人材育成、(2)技術革新、(3)情報インフラ投資および情報産業育成という 3 つのフレームワークが示された。更に IT2010 計画実現ため、2002 年にはその具体的なアクションプランとして、National ICT Master Plan (2002-2006) が NITC に認可された。この中では、特にソフトウェアにおける ICT 開発とビジネスの分野で東南アジア地域の中心となることが掲げられている。

◆法律

NECTEC が発案した重要な IT 関連法規としては、以下の六つがある。

- 電子取引法…Electronic Transaction Law
- 電子署名法…Electronic Signature Law
- 国家情報インフラ法（ユニバーサルアクセス法）…Universal Access Law
- データ保護（プライバシー）法…Data Protection Law
- 電子資金移動法…Electronic Funds Transfer Law
- コンピュータ犯罪法…Computer Crime Law

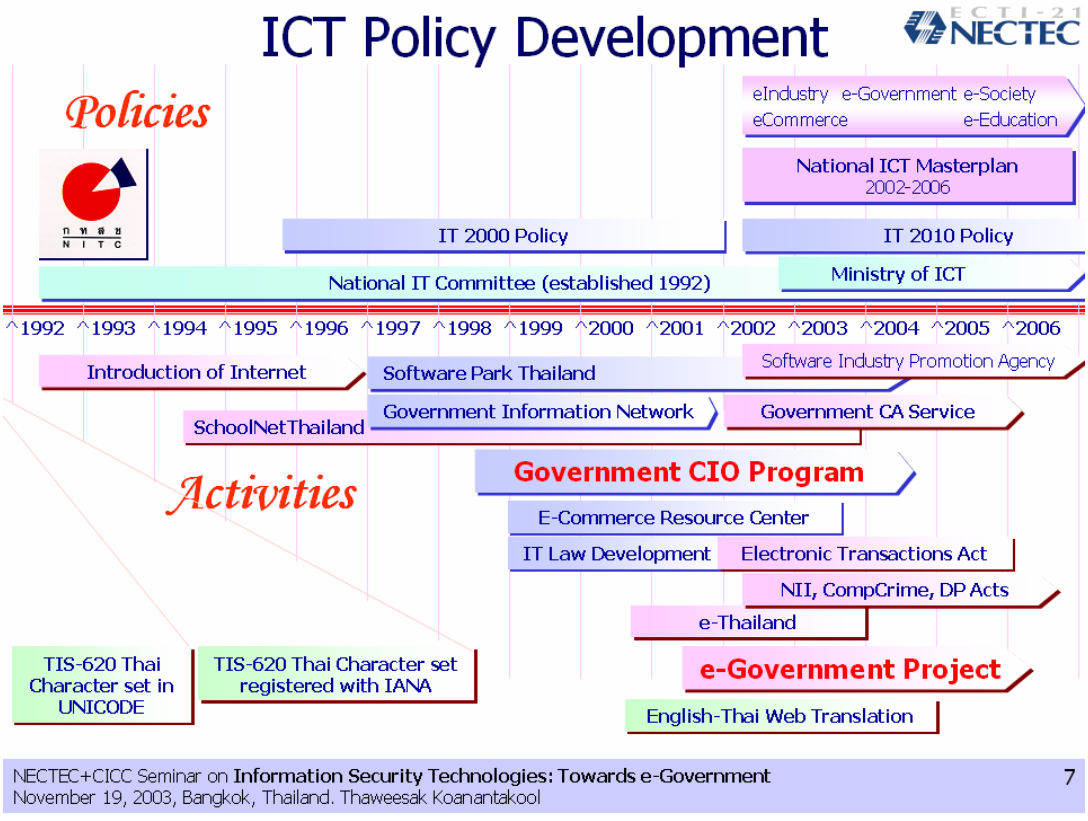



図 1.2-5 タイにおける ICT Policy Developmen

(a) 電子取引法

この法律では、適切に取り扱った電子記録を紙文書に等しいものと定義している。さらに、電子記録の送信・受信プロセスと、そのような送信が行なわれた日時と場所とを法的に認知する範囲も定義している。

(b) 電子署名法

電子署名を、「署名者の身元と、署名者が署名のついた文書内容を承認していることの証明」として定義している。この法律では、電子署名に使用する技術の選択に対しては、中立を保っているが、暗号技術に基づく公開鍵インフラ（PKI）を認知している。同時に、この法律により、取引の当事者は、独自の電子署名を選択できる自由も持つことになる。

上記二つの法案は、電子署名の主な原則を反映した「電子取引法案（Electronic TransactioAct B_E_2544)」と呼ばれる単一の法案にまとめあげられ 2001 年 12 月 2 日に公布された。

(2) インフラの状況／IC カード、eID、証明書発行主体

◆国内認証局の現状

現在の所、タイでは政府機関である GITS の他に 4 つの民間認証局が存在する。

それぞれのサービス開始は以下の通り。

- GITS（政府）：2002 年～
- ACERTs（民間）：2001 年～
- TaidigitalID（民間）：2001 年～
- TOT（民間）：2003 年 8 月～
- CAT Telecom Public Company Limited（民間）：2003 年 8 月～

TaidigitalID と ACERTs は、インターネットバンキングなどの財務ビジネスのための証明書発行サービスを目的としており、既にいくつかの銀行を顧客としているとのこと。GITS がルート認証局となるかどうかなど、将来的なタイにおける CA 構造は不明。また現在の所、公認認証局についての規定も定まっていない。

●GITS

政府機関向け CA として、2002 年からテスト運用を開始した。

GITS とは、各政府機関をネットワークにリンクし、また電子政府サービスを全国の国民に提供するためのサービスであり、その電子政府の電子的な仕事の流れを促すためには、政府情報ネットワーク（GINet）が中核と見なされている。しかしながら、PKI アプリケーション立ち上げの遅れに伴い、現状は政府内中心。

●ACERTs

ACERTs Co., Ltd は、Siam Commercial Bank PCL とのジョイントベンチャー企業であり、GITS に続くタイで 2 番目の CA として 2001 年 6 月に設立され、2001 年 12 月から業務を開始した。シンガポールの Netrust Pte. Ltd と協力関係にある。

iDC と認証局を基盤にしたセキュア通信サービスを提供しており、電子公証機能もサポートしている。主に、GITS の管掌外である国営企業などの公共市場に注力する方向。現在は Advanced Research Group の一部となっている。

●Thai Digital ID

主な顧客基盤は金融分野で支払決済ゲートウェイとあわせて PKI を提供している。

今後パブリック CA に注力する方向。http://www.thaidigitalid.com/

●TOT

TOT Corporation Public Company Limited 社（TOT）はタイの大手通信事業者であり、ISP やモバイルサービスプロバイダなどが対象だが、Baltimore Technologies 社と協力して、同社の UniCERT を導入し、2003 年 8 月 19 日に CA を設立した。http://www.ca.tot.co.th/

◆国民カード（Thai National ID Card）

Smart Card ID Project により、2004 年から IC カード内蔵の国民カードを配布している。

このカードの特徴は以下の通り。

- Secure biometric ID card
- Matching on-card function
- Multi-application card
- Public Key Infrastructure
- Free of charge to 64M citizens


図 1.2-6 Thai National ID Card

ICT 省と内務省（MOI：Ministory of Interior）では、2005 年 6 月末までに 1,200 万枚のスマート ID カードを発行し、2005 年末までに 2,600 万枚の発行目標を達成するべく協力していくと発表。タクシン首相も、現行の ID カードに替わってスマートカードが使える機会を 3 年以内に全タイ国民に対し提供すると公約している。

将来的には 18 省の情報が一つのカードに登録される方向だが、実際はまだ何も決まっておらず、まずは ID カードの機能のみでスタートする模様である。

なお、ICT 省の方針としては、将来的にスマートカードは国産化していく計画。初年度については国外企業から調達するが、3 年後には国内生産ができる体制を整え、年間 1,000 万枚のスマートカードチップ生産の実現を目指す。その中心となるのが、NECTEC 傘下のタイ・マイクロエレクトロニクス・センタ（TMEC：Thai Micro Electoronics Center）となる。しかし、2005 年には、一部の業者が発注仕様書を満たしていない欠陥品を納入したことが明らかになっており、大きな問題となっている。また、今後の ID カードには、RFID 機能を搭載することが情報通信技術省（ICT）により発表されている。

(3) 金融部門

Thai Digital ID は、タイの金融機関に対して IT サービスを提供する PCC グループのメンバであり、PCC グループの銀行間決済サービス「ePAY」への認証サービスを提供している。

また、銀行間決済分野では、Bank of Thailand が発行する証明書をベースに、地方銀行も含めた金融機関の間での資金の振替などが行われている。

2005 年 7 月には、バンコク銀行とタイ農民銀行が偽造防止のために EMV 方式の IC カードをクレジットカードとして導入すると発表しており、今後の展開が期待される。

(4) 医療分野

国民カードにヘルスケア情報を格納し、活用することも計画されているが、具体的な事例に関する情報は得られなかった。

(5) 公共（申請・納税）

電子政府サービスと国民カードの連携が検討されているが、PKI は利用されない模様。

(6) その他

◆交易 EDI

タイでは TradeSiam を通じた貿易関連 EDI システムが稼動している。現在は 2003 年 10 月に提案された「アセアン・シングル・ウインドウ」というアセアン全体の貿易関連業務効率化の構想に基づき、2008 年の完成に向けて対応がすすめられているが、ここでは PKI をベースとして ebXML を利用するシステムが検討されている。

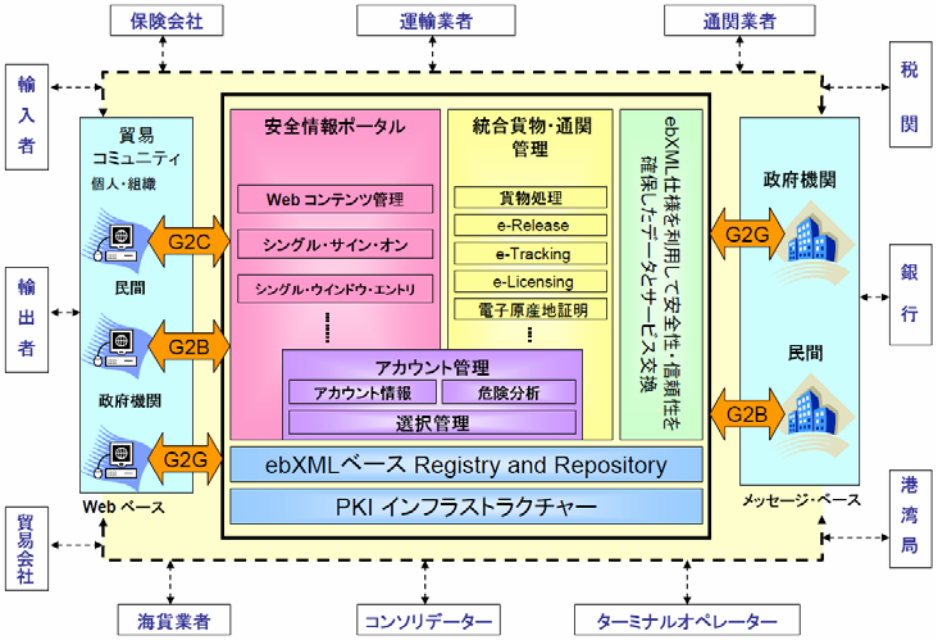



図 1.2-7 アセアン・シングル・ウィンドウのシステム構成案

参考文献


- 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 に関わる法制度及びビジネス環境の動向に関する調査報告書、平成 14 年 3 月(財)日本情報処理開発協会、
  http://www.japanpkiforum.jp/shiryou/business_k/biz01_rep_all.pdf
- 平成 14 年度 EC 技術基盤の相互運用性に関する調査研究事業（普及阻害要因当の調査及び国際的ルールの検討)、PKI 関連サービスビジネスの動向と今後の展望に関する調査報告書―欧米および日本・アジアでの展開―、(財) 日本情報処理開発協会、

http://www.japanpkiforum.jp/shiryou/business_k/b02report.pdf

- 平成15年度EC技術基盤の相互運用性に関する調査研究事業（PKI相互運用のための動向調査およびガイドライン作成)、PKI利用モデルの現状と相互利用に関する調査報告書―欧米・アジアでの展開と日本への示唆―、平成16年3月（財）日本情報処理開発協会、http://www.japanpkiforum.jp/shiryou/business_k/b03report.pdf
- Public Key Infrastructure [PKI] in Thailand, Assumption University Rear Admiral Prasart Sribhadung, http://www.nectec.or.th/cicc/download/04-pki.ppt , Information Security Technology Seminar, Nov. 19 2003
- Information Security Technologies Towards e-Government,Dr.Thaweesak Koanantakool,Director,NECTEC,http://www.nectec.or.th/cicc/download/01-keynote-speech.ppt, Information Security Technology Seminar, Nov. 19 2003
- Thailand ICT Indicators 2005, NECTEC, NSTDA, http://www.nectec.or.th/pld/documents_pris/ict_indicators2005_180705.pdf, Feb. 2005
- Smart Card Project in Thailand, Mr. Terdsak Pattayanun Inspector General / Ministry of Information and Communication, Thailand, http://www.asiaiccardforum.org/ENG/news/pdf_files_050720_21/DL18_Smart%20Card%20Project_in_Thailand.pdf、アジアICカードセミナー2005年7月21日、東京
- 日・タイ経済協力協会、日・タイ経済協力セミナー「中進国入りするタイと日本の新しいパートナーシップ」、経済産業省　通商政策局国際経済課長　黒田篤郎、http://www.jtecs.or.jp/pdf_seminar/s_pdf_seminar06-1.pdf、2006/09/25
- JETRO　日本貿易振興機構（ジェトロ)、調査レポートASEAN各国の発展戦略とビジネス環境の変化（2004年3月)、http://www3.jetro.go.jp/jetro-file
- /BodyUrlPdfDown.do?bodyurlpdf=05001134_001_BUP_0.pdf
- JETRO　日本貿易振興機構（ジェトロ)、調査レポート2004年2月10日「タイにおける近年のビジネス法制の変化と今後の展望」〈後編-1〉、日タイビジネスネットワーク代表　元田　時男、http://www.jtecs.or.jp/s-04-4.html
- 1　JETRO　ジェトロ・バンコクセンター、タイの法律　法制度　電子取引法、http://www.jetrobkk.or.th/japanese/pdf/3.7.4.5.pdf
- 科学技術振興機構、成清　正和.“アジアのIT人材育成―タイ：人材育成に貢献する日タイ大学間連携”、情報管理. Vol. 45, No. 12, (2003), 868-872、http://www.jstage.jst.go.jp/article/johokanri/45/12/45_868/_article/-char/ja
- 財団法人　国際情報化協力センター（CICC)、アジア情報化レポート2005　タイ、http://www.cicc.or.jp/japanese/kunibetsu/pdf_ppt/タイ%20情報化レポート.pdf
- National ID Cards Examples of Customers The Thai authorities、http://www.precisebiometrics.com/?id=223、
- 平成17年度　アジア産業基盤強化等事業　アセアン各国におけるICタグ（RFID）の活用可能性調査2　調査報告書、平成18年3月、次世代電子商取引推進協議会

- 平成 17 年度情報家電活用基盤整備事業「アジアにおける情報通信業界動向調査」報告書、平成 18 年 3 月、財団法人　国際情報化協力センター、http://www.cicc.or.jp/japanese/tyousa/pdf_ppt/②-H17 受託調査__アジアにおける IT 産業の現状と今後の戦略に関する調査研究報告書.pdf

## 2.8 オーストラリア

(1) 背景／国の方針、法律、国民性

●2010 年を目指す新たな電子政府戦略

オーストラリア政府は、2006 年から 2010 年までを対象とした新たな電子政府戦略の計画として「e-Government Strategy, Responsive Government：A New Service Agenda」を 2006 年 3 月に公表した。この中期計画では、次の 4 つの目標を戦略的優先課題としてあげている。

①Meeting users' needs（利用者ニーズの満足）

全ての国民が、ウェブ、電話、郵便、対面窓口など自分にあった方法で、政府のサービスを確実かつ効率的に受けられるようにする。

②Connected service delivery（結び合ったサービス提供メカニズム）

ウェブ、電話、郵便、対面窓口などのどの手段を用いる場合でも、統合したサービスをシームレスに利用者へ提供できるように、政府の組織と業務プロセスを再構築する。

③Value for money（バリューフォーマネー）

情報の共有、システムの連携や共有などを進め、シンプルでより効率的な政府を構築し、費用削減をいっそう進める。

④Public sector capability（公共部門の能力強化）

目標実現に向けて、政府の情報システムに関わる職員のスキルの向上や採用・昇進、ベストプラクティスの共有、政府調達の改革、知識管理、プロジェクトマネジメント、政府のアカウンタビリティや法令調整を進める。

●政府 ICT のためのガバナンスモデル

このような計画を推進するため、「政府 ICT のためのガバナンスモデル」と呼ばれる体制の整備が行われている。これは、これまでの電子政府推進体制と同じであるが、意思決定やサービス提供において、各機関間の連携・協働をいっそう強化することが予定されている。

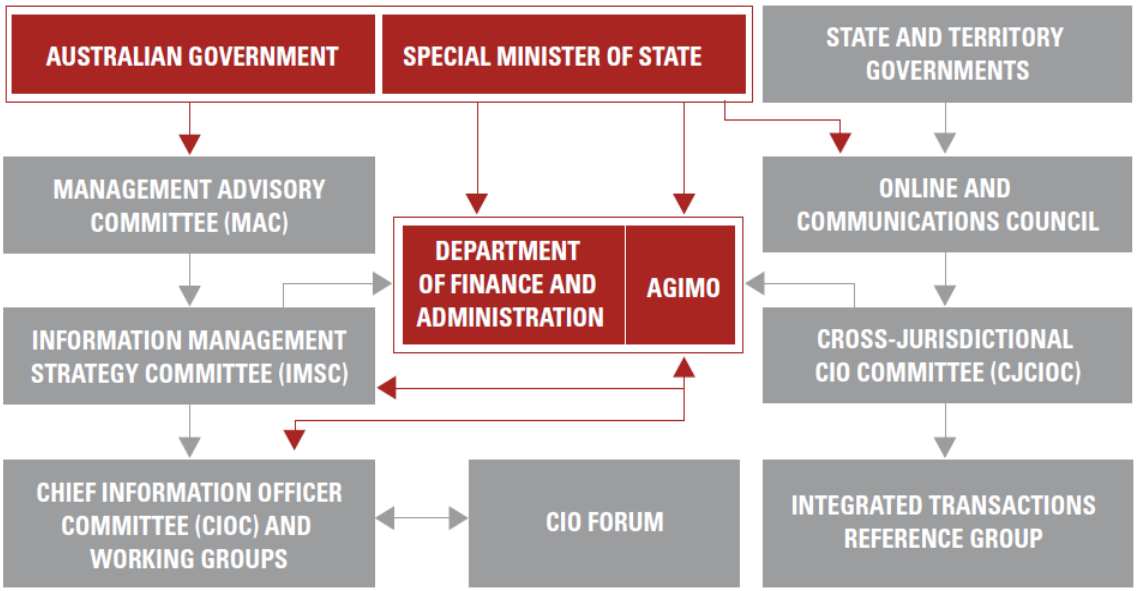



図 1.2-8 Governance model for government ICT（政府 ICT のためのカバナンスモデル）

http://www.agimo.gov.au/__data/assets/pdf_file/51499/e-gov_strategy.pdf pp.29

上記ガバナンスモデルにおいて、電子政府を推進する上で最も重要な職責は特別国務大臣（Special Minister of State）にある。特別国務大臣は、電子政府推進など政府の重要事業を進める専任の国務大臣であり、Department of Finance and Administration（予算・行政省）に設置されている。

しかし、その職務は、電子政府にとどまらず、選挙委員会、国有財産管理、映像管理（Film Australia）など複数の分野にまたがっている。そこで、特別国務大臣を支え、政府全体にわたる電子政府推進事業の中核として機能する実務上の組織として、AGIMO（Australian Government Information Management Office：オーストラリア政府情報管理局）が重要な役割を果たしている。

●AGIMO（Australian Government Information Management Office：オーストラリア政府情報管理局）

オーストラリアでは、さまざまな組織が上下関係または水平関係の網の目を張って、利用者志向・結果志向で統合度の高い最適化された電子政府の整備を進めている。そのような多数の異なる組織の運営は、原則として、行政改革の中心機関である予算・行政省に置かれたオーストラリア政府情報管理局（AGIMO）が管轄し、あるいは中心メンバとなって、実質的なリーダーシップを発揮し、施策の整合性の確保や、施策の確実な遂行を行っている。

このオーストラリア政府情報管理局（AGIMO）は、2004 年 10 月、電子政府推進において政府全体の企画や実行管理、評価を中心に行う組織として、特別国務大臣の管轄下に設置された組織である。それまで、オーストラリア政府情報管理局（AGIMO）は、全国情報経済局（NOIE：The National Office for the Information Economy）として、通信・情報技術・芸術省に

属する組織であった。しかし、電子政府の整備が進み、インフラやシステムの構築がおおむね初期の目的を達したことから、「情報経済分野が成熟してきたためNOIEの機能を省庁の業務責任及び活動と統合していくのが適当である」という通信・情報技術・芸術大臣の判断により、予算・行政省へと移管・再編されたのである。

オーストラリア政府情報管理局（AGIMO）の主な役割は、次世代の電子政府のあり方を、利用者である国民の視点から見直すことや、政府全体の IT 投資を評価し投資効果を高めていくことである。すなわち、オーストラリアでは、利用者志向と結果志向の2つのコンセプトを徹底することが新たな電子政府実現の重要成功要因と考え、そのためのマネジメントサイクルを政府全体で実施していく中心組織として、オーストラリア政府情報管理局（AGIMO）を位置づけているのである。

また、オーストラリア政府情報管理局（AGIMO）は、先のガバナンスモデルで示されている情報管理戦略委員会（ISMC)、情報化統括責任者評議会、管轄横断情報化統括責任者評議会（CJCIOC）の実質的な運営者となっている。また、先に述べたように、オーストラリア政府情報管理局（AGIMO）の情報化統括責任者は、政府全体の情報化統括責任者を兼ねている。

したがって、オーストラリア電子政府の新たな発展は、オーストラリア政府情報管理局（AGIMO）に委ねられているといっても過言ではない。

●オーストラリアの地方行政と法律

オーストラリア（以下、豪州）の政府は三層構造（連邦政府、州・特別地域政府（以下、単に「州政府」)、地方自治体）になっており、情報通信技術（ICT1）課題に対して統一的に取り組みにくい側面を持っていた。全国的なICT開発については部門レベル――例えば保健部門、教育部門など――で個別に展開されている。そのため、主な国家的なICT政策委員会であるオンライン協議会と通信協議会の役割は、各層の政府間での情報共有を促進することにある。豪州では、大都市周辺の大規模な自治体と地方部（へき地、遠隔地を含む）には小規模な自治体が数多く存在しており、その予算規模や人口規模等に大きな違いがある。小規模な地方自治体については、国内外のICTに関するプライバシー、認証およびセキュリティの事例を適用できない場合もある。

全国レベルで最も進展が見られる分野は、以下の2つである。まず、個人情報の保護の分野である。連邦政府によって制定された『1988年プライバシー法』の施行により、州政府および地方自治体は、市民等から得られた情報のプライバシーを保護するため、一貫した取組みをしている。次に、電子商取引の分野である。連邦政府の策定した『1999年電子取引法』により、すべての州・特別地域において電子取引の利用促進を図る法律等の制定が全国的に進展し、電子商取引のための法的枠組みが構築されている。

しかしながら、豪州には全国共通の身分証明カード（身分証明書）は存在しない。1980年

代に導入の検討がなされたが、猛烈な反対にあった。そのため、個人の身分確認の方法にはいまだ共通性がなく、個人の認証法においても脆弱性がある。現在取り組みがなされている医療 IC カード等の IC カード導入に向けての動きは、今後、個人電子認証をより効果的にするものとして期待されている。

一方、事業者認証の分野においては、個人認証を大きく上回る進展が見られる。連邦政府は、2000 年の物品およびサービス税（GST）の導入に伴い、豪州内のすべての事業者を対象とした新たな単一事業者番号／登記制度として、豪州事業者番号／豪州事業者登録簿（ABN/ABR）を義務づけた。以来、連邦政府による ABN/ABR 制度の発展、公開鍵インフラ（ゲートキーパー）の開発、および単一のデジタル署名証明書（ABN-DSC）の発行により、事業者は単一のデジタル証明書を利用してすべての政府系機関とのやりとりが可能になっている。ABN-DSC 技術の進展により、特に保健部門および輸出入部門において ABN-DSC を利用した事業者認証の導入に向けての大規模な取組みが進んでいる。

●オーストラリアでの電子取引きの認知度、普及の実態

オーストラリアの国土は広大で、国民は広く散在して住んでいる。このためオーストラリアでは電子取引の価値が理解され、きわめて短期間のうちにインターネットが使われるようになった。そしてオーストラリアは電子取引きの世界規模のプレーヤーである。ここはどの国からも遠く離れているので、インターネットがとても有効である。オーストラリアの殆んどの国民は、キャンベラ、メルボルン、アデレード、パース、ブリスベーンといった主要都市に住んでいる。これら都市部以外には人は殆んど住んでいない。そしてシドニーなどの主要都市のそれぞれに、非常に優れた通信インフラが整備されている。人工衛星による通信インフラ、州都を結ぶ光ファイバー網などである。通信業界は規制緩和により熾烈な競争下にある。通信の最大手 Telstra、オプタスだが、他にも数多くあり、かつそれぞれに技術的に優れた通信インフラを提供している。またそのそれぞれが独自の ISP も運営している。内陸部にはそれほど優れたインフラはないが、もちろん電話、電気はあるので、オーストラリアのどこででもインターネットは利用できる。日本とは 1 万マイル離れているが、インターネットにより日本の主要な貿易相手国になっている。食料、石炭、鉄などいろいろなものを輸出している。ブリスベーンは世界一面積の広い町だが、ここに住んでいる人は少数である。しかしインターネットによる商取引環境は整えられている。都市から外れた地域にも情報や通信のインフラを提供することで、そのデメリットを解消できる。インターネットがあれば、都市にいる必要はなくなる。これが重要である。

(2) インフラの状況／IC カード、eID、証明書発行主体

●電子政府の立ち上げ

政府機構は大きくて複雑である。そこで BEP（Business Entrance Point、総合受付）を利用して政府へのアクセスを集中し、政府の行政サービスを利用可能にし、政府の組織間のコミュニケーションを飛躍的に円滑化している。特にオーストラリアの税務署、検疫所、税関

は世界中と多くの取引を行っているが、その際、相手が何者なのかを常に知る必要がある。BEP により、貿易に伴う事務処理を大いに迅速化した。

オーストラリア政府は Government Online（オンライン政府）を省庁間、省庁と民間企業間で大いに推進させたいと考えている。これにより企業から政府へのアクセスが、時を選ばずにできるようになる。政府側も事務処理が軽減され、迅速化され、コスト軽減になる。その際、政府が重要だと考えたのが認証の問題である。相手が誰かという「署名」と、自分が確かにそれをやったと認めさせる「否認防止」である。このために PKI による電子認証を含む電子署名法を制定した。

次の問題は誰が CA になるか（誰がオーストラリアの PKI の権威になるか）であった。政府のある省が CA の役割を果たすことに名乗りを上げたが（つまりその省での取引の信頼性を引き受ける)、引き受ける責任がさらに広がることを恐れて放棄してしまった。理由は、政府が個人的なリスクを負うことはできないという立場からである。そこで Gatekeeper と呼ばれる戦略が提案された。

●Gatekeeper

Gatekeeper の実体は、民間の CA を評価し、一定の信頼性、基準を保証するための仕様である。だから Gatekeeper は銀行、官庁、その他の何れの業務、アプリケーションにも適用できる。そして政府が各 CA を直接に管理することはしない。Gatekeeper には「運用、技術要件、技術的な標準／方針、法律上の責任」が含まれ、とても具体的である。Gatekeeper の定める基準、仕様を守ることにより、信頼性と相互運用性の高い CA を運用することが可能になる。

Gatekeeper は正式には官庁（電子政府）に適用するためのものである。従って官庁と付き合うためには、Gatekeeper による認証を受ける必要がある。しかし Gatekeeper がとても強力なので、他の幅広い分野の B2B で採用されている。この Gatekeeper の認証を受けるには、多くの時間と資金が必要である。

Gatekeeper の最初の認定を受けた CA のひとつである BaltimoreTechnologies では、施設を建設するのに 300 万ドル、認証を受ける書類の作成に 100 万ドルかかった。膨大な書類を提出して NOIE に承認の受け、さらに国防省、司法長官、そして諜報部の承認を受ける必要がある。Gatekeeper のエントリーレベルと呼ばれる認定を受けるまでに 9 ヶ月ほどかかった。そしてエントリーレベルから全面的な資格を受けるのに、さらに 15 ヶ月かかった。手続きの全体を網羅するのに 35 種類ほどの書類が必要となった。現在 Baltimore Technologies では、それらの書類の雛形を PKI 実装製品やサービスの一環として販売している。これを用いることにより Gatekeeper の認定を取得するのが容易になり、時間も半分くらいに短縮できる。Gatekeeper によって認定された最初の 3 システムは、Australia Tax Office (ATO)、Baltimore Certificates Australia Pty Limited (BCAPL、オーストラリアボルチモア認証会社)、Health e-Signature Authority (HeSA) である。

Gatekeeper には RCA (Root CA) や CA の仕様が定められている。たとえば下位レベルの CA をどう設定するか、あるいは両者の技術的または法律的な問題についてである。このうち技

術の問題は比較的簡単で、法律の問題の方がはるかに複雑である。

(Gatekeeper:http://www.agimo.gov.au/infrastructure/gatekeeper)

●オーストラリアにおけるPKIの普及度

①設置CA数

2006年9月現在、オーストラリアのPKI標準仕様であるGatekeeperの認定を受けている認証局は以下の通り。

| 認証局名 | 認定日 |
|---|---|
| Australian Taxation Office (ATO) (Tax PKI) | 16 June 2000 |
| Health eSignature Authority Pty Limited (Health PKI) | 19 January 2001 |
| VeriSign Australia Pty Limited | 5 April 2001 |
| Australia Post | 20 December 2001 |
| Betrusted Pty Ltd | 9 October 2002 |
| ANZ Banking Group Limited | 22 August 2003 |

なお、過去に認定を受けていた認証局は以下の通り。

| 認証局名 | 認定日 |
|---|---|
| Baltimore Certificates Australia Pty Ltd | 20 November 2000 |
| Telstra Corporation Limited | 9 October 2001 |
| PricewaterhouseCoopers | 7 March 2002 |

②証明書の料金

Verisignは証明書を販売していて、インターネットで価格表が公表されている。証明書のタイプは、ABN-DSC（オーストラリア事業者番号証明書)、デバイス（自動応答メールプログラム用など)、Type 3 HOST（輸入届出処理のホスト用)、個人、非個人（組織の担当者用)の5種類で、価格は85～540ドル。個人向けのIndividual(Type 1)Digital Certificateの価格は2年有効のもので115ドル。取得の際には、本人確認の為にAustralia POSTの運営するRAであるKeyPostに申請書と身分証明書を提示する必要がある。

銀行の証明書は、費用を銀行側で負担し顧客には無料で出している。その代わり取引きの手数料にチャージして回収している。

(3) 金融部門

●Project Angus

Project Angusは2001年に発表されたプロジェクトで、オーストラリアの銀行により発行されたビジネス用の電子証明書を、連邦政府機関が受け入れ可能とするものである。

このプロジェクトに参加した銀行は、世界中の銀行システムとの相互接続性を確立するた

めのIdentrusにも加盟していた。Identrusが扱う銀行は一定の規模以上でなければならず、オーストラリアでは Australia-New Zealand Bank (ANZ)、CBA、National Australia Bank (NAB)、WestPac の4行である。

Identrusでは、RCA (Root CA) はニューヨークやカナダであろうと、オーストラリア外のどこにあっても構わない。一方 Gatekeeper では、CA はオーストラリア内になければならない。ABN-DSC (オーストラリア企業番号ディジタル証明書) を発行したい銀行は、それを発行する CA がオーストラリアになければならない。すなわち RCA はオーストラリアになくてもいいが、発行する CA はオーストラリアになければならない。

(Identrus は2006年3月に Identrust に社名変更)

(4) 医療分野

●HIC (Health Insurance Commission)

オーストラリアでは、税金 (ATO) の次に PKI を利用しているのは健康保険である。オーストラリアの健康保険制度は国民皆保険制度で、年間約2億件の取引を行っている。健康保険の予算は60億ドル、毎年約30億ドルに相当する1億4000万通の処方箋が書かれている。HIC (健康保険委員会) は実際に電子証明書を発行する HeSA (Health e-signature Authority) を設立した。これは Gatekeeper の認定を受けている。

HIC で用いられる証明書は、患者と医療機関、患者と医者の間の本人認証に用いられる。

医療機関同士での医療記録 (カルテ) の交換はまだ行われていない。理由はプライバシー保護の観点と技術的な問題による。カルテは医者ごとにまちまちであり、まずそれを標準化する必要がある。技術的には HIC では、認証に十分の水準のセキュリティを備えるために、スマートカードによる認証とソフトウェア処理を組み合わせて用いている。

ヘルスケア専門職は約7,000枚のスマートカードと USB キーを持っている。このプログラムは今後2年間にさらに10万枚以上拡大する計画がある。

●Medicare Australia

メディケア・オーストラリアは、連邦機関の Human services 省の管轄の医療保険を運営する公的機関であり、すべての新しい電子データ交換 (EDI) および電子ビジネス・ソリューションに公開鍵暗号基盤を使用しており、向こう数年内に新たな電子ビジネス・ソリューションを展開することを目指して計画を進めている。従って、HeSA ではデジタル鍵および証明書への需要が、今後さらに高まるものと予想している。

●タスマニア州の健康保険証

2004年から2006年の間、少数ではあるが、「Megicare smart card」が試験的に発行されている (タスマニア州で1000枚ほど)。しかし、この結果は当初の予想を大幅に下回った模様。

2005年10月には、さらに大規模な行政サービスと電子保健衛生のための「the health and social services Access Card」プログラムが発表された。2007年から2008年にかけて発足し、1500万枚のカード発行が計画されている。

今後、「Megicare card」は「the health and social services Access Card」に置き換えられる予定。

(5) 公共（申請・納税）

●ABN-DSC（Australia Business Number Digital Signature Certificate）

オーストラリアではすべての企業がABN-DSC（オーストラリア企業番号）を持っている。企業の名刺や便せんのすべてに記載されている。以前はただの数字だったが、それが電子証明書つまりDSCに用いられるようになった。当初、これは政府が企業に義務づけるもの（企業からの納税申告書など)に使用されていた。すべての企業が1つの番号を持っているので、そのABNを用いて互いに連絡を取り合うことができる。

ABNは数年前にGST（物品サービス税）の一環として、ATOによって導入された。それまではオーストラリア法人番号（Australia Company Number, ACN）という別の会社番号が、別の政府機関によって発行されていた。ATOがGST（物品サービス税）を導入する際にそれまでのACNの末尾に数字を追加してABNを導入した。政府がGSTを導入したとき、ATOはGSTの納税申告を電子的に行うことを当初から推進したいと考えた。そこでATOはABNを設定し、事務処理の削減と税収拡大のために証明書の発行を開始した。そのためオーストラリアの大企業が、ATOによって発行される証明書が必要という状況になり、電子化が大いに促進されることになった。そしてこの証明書は一般のB2BおよびG2Bに利用することができる。当初、ATOはこれを許さなかったが（つまりGSTの納税申告だけに限定していた)、社会的な要求によりこれをPKIによる一般のB2B、B2Gの電子取引を利用できるように変更した。現在、ABN-DSCはATOだけでなく、Gatekeeperの認定を受けたe-Sign、PWC、Telstraによっても発行されている。ABN-DSCを共通化することにより、これらによって発行される証明書を共通に利用できるようになった。Gatekeeperを NIOEが制定したとき、6種類の証明書を設定した。このため例えば健康保険のための証明書を発行するHIC（健康保険委員会）と税金のための証明書を発行するATOでは、共通性はなかった。しかし共通のABS-DSCを用いることで相互に証明書を利用可能になった。

●ATO（Australia Tax Office）

オーストラリアの大半の人はその年度中に税金を支払う義務があって、年度末にe-tax（Electronic Tax）を利用して所得申告する。政府に有利なのは、すべての納税者が直接入力するので、入力処理が不要なことである。電子化によって、効率的で迅速かつ安価に処理される。書面なら約2ヶ月かかることを、約2週間で処理できるようになった。

e-tax以前には、所得申告には2通りの方法があった。1つは地域の郵便局か新聞雑誌取次店に行き、税金パックという小冊子を手に入れる。この書類にはすべてに手書きで記入する。オーストラリアの個人の所得税は、世界的にも最も複雑な税金体系の1つで、それによ

る問題が生じている。すなわち手書きの所得申告書に書き間違いが多いこと。そして書面を自動修正してくれるツール類がない。このため多くの納税者が公認会計士に申告を依頼していて、これに約200ドルがかかる。結局納税者にとって、オーストラリアの納税システムはとても高額なものになっている。そこで政府はその両方を解消するために、電子申告を奨励している。複雑な税金パックによる手続きをe-tax化し、納税者は税金パックに記入する代わりに、e-taxのアプリケーションをインターネットからPCに読み込み、オフラインで記入し電子署名して、直ちにアップロードすれば済むようになった。ただしその際オフライン処理が入るために、署名を保つためにPKIを利用する必要がある。

2001年11月現在、実績としてATO関連で30万件の証明書が発行され、PKIを利用して電子的に税務処理を行った企業は5万社であった。ほとんどの証明書はインターネットからダウンロードされたもので、CD-ROMやフロッピーディスクによる提供ではない。生成された鍵は301,000組、そのうち実際に使用されたものは72,000組である。この使用された鍵数が実態に近い。ABNを持っている企業は340万社。一定規模以上の企業はe-tax（従ってPKI）を利用しなければならない。従って上記の 30 万件には大手が含まれている。オーストラリアのほとんどの企業は従業員数が 1〜5 人の小規模会社だが、これらは e-tax を使う義務はなく書類申告で済ませることができる。一方、小規模であってもすべて企業がABNは持っている。

GSTの導入に伴い、企業ではない事業者もABNを持つようになった。それ以前は企業でなければABNは必要なく、例えば個人業主やタクシーの運転手にABNは必要なかった。GSTの導入によりすべての自営業者がこの税金を納める必要があり、このためにABNを持っている。

他のPKI応用の事例としては、老齢退職手当への応用がある。老齢退職手当の申告書の提出にPKIを利用している。それらにはやはり署名と認証が必要だが、税金ではないので同じ官庁でも応用が異なる。

●ATO PKIプロジェクトの経緯

ATOのPKIプロジェクトは1999年6月に始まった。スマートカードをデジタル化し、顧客向けアプリケーションとなる電子商取引インターフェイス（ECI）を決定した。これは顧客に送られ、PCに入れるとセキュリティが確立し、取引を始めるにあたって鍵と証明書を簡単にインポートすることができる。

Business activity statement（BAS）は改定され、Australian Business Number（ABN）を持つ企業はGSTの還付に改定されたBASを使うことになった。PKIを使ってインターネット上で安全にコミュニケーションするには GK の認定を受けた認証局を使うべきであると考え、自前の認証局を設立することになった。2000年5月25日にCAプロセスを開始。6月16日にはGatekeeperの完全認定を受けた。7月には最初の月次e-BASを発行。顧客はECIアプリケーションでBASをダウンロードし、emailを受け取る。顧客から最初のe-BASを受け取ったのは、7月27日であった。

●e-BAS による税務処理

BAS とは Business Activity Statement のことで、紙媒体でも電子媒体でも提出することができる（e-BAS の最初の「e」は electronic を意味する)。

オーストラリアの全企業／商業行為を行う組織は ABN に登録する。登録はインターネットから。年間売上高 2,000 万ドル以上の企業は全て電子的に BAS を ATO に提出することになっている。売上高がそれより少ない企業は、紙媒体でも電子媒体でもどちらでも選択できる。

ABN を申請し、電子的に提出するというオプションを選択すると（売上高 2000 万ドル以上の企業は必ず)、ATO から ECI アプリケーション CD-ROM と PIC メイラー（PIC は Personal Identification Code)、email が送られる。インターネットから PIC を入力すると鍵と証明書がダウンロードできる。鍵と証明書をダウンロードすると ECI アプリケーションにインポートされ、電子的な取引ができるようになる。取引きは、ECI アプリケーションを立ち上げてインターネット経由で新しいパスワードと PIC を入力する。

BAS の準備ができると、ATO システムはどのクライアントが準備できているかを認識し、「e-BAS を提出できる」、という email を受ける。ECI アプリケーションを稼動させてインターネット経由で e-BAS を入手し、ECI アプリケーションを使ってオフラインで e-BAS を仕上げてまたインターネット経由で作成した e-BAS を ATO に提出する。こうして鍵と証明書により、本人認証と暗号化を施しながら、税務処理を行うことができる。

2000 年 9 月 14,000 件（稼動開始直後）
2000 年 12 月 79,000 件
2001 年 10 月 400,000 件を見込んでいる。

●e-tax

個人向けには e-tax がある。これは 1 年に 1 度行われる。1999 年は約 60,000 件、2000 年は 150,000 件、2001 年は約 400,000 件の利用を見込んでいる。

●年金

BAS だけでなく superannuation（年金）もインターネットを介して行われ、ECI プラットフォームを利用しており、とてもうまくいっているが、オーストラリアの superannuation システムはとても複雑である。数字を見ると、2001 年 6 月末までに 180 万件が PKI を利用して記録され、2,526 件の還付が行われた。

(6) その他

●Telstra

Telstra は大手の電気通信会社／電話会社である。規制緩和までは唯一の電話会社だったが、現在は他にいくつか電話会社ができている。しかし最大手であることに変わりない。Telstra は自前の商業 CA を設立していて、今後 ABN-DSC の発行業務にも参入しようとしていた。Telstra が CA 事業に参入したのは、基本的に電話回線からの収益を伸ばすためである。

回線を使ってもらうための付加価値のあるサービスを提供しようとしていて、PKI はコンテンツ販売に必要な手段と考えている。Telstra にはオーストラリア中に何千という店舗があり、それらが RA になることができる。

しかしながら、2006 年 9 月現在では Gatekeeper の認定から外れている。

●オーストラリア郵便局

オーストラリア郵便局は、1996 年に証明書の発行事業を始め、2 年前に止めてしまった。オーストラリアには、全国に郵便局の窓口があるので、それを活用した CA ビジネスを始めようとした。その 1 つがパスポート申請の登録手続きである。パスポートを申請するには、郵便局に出掛けていって書類と身元確認の証拠を提出して申し込むと、書式に記入し刻印してそれを旅券事務所に送ってくれる。そして旅券事務所はパスポートを発行する。オーストラリア郵便局は、このパスポート申請に PKI を用いようとしたがうまくいかなかった。理由は、資金難と誰もオーストラリア郵便局の証明書は欲しがらなかったことによる。

●クイーンズランド州の運転免許証

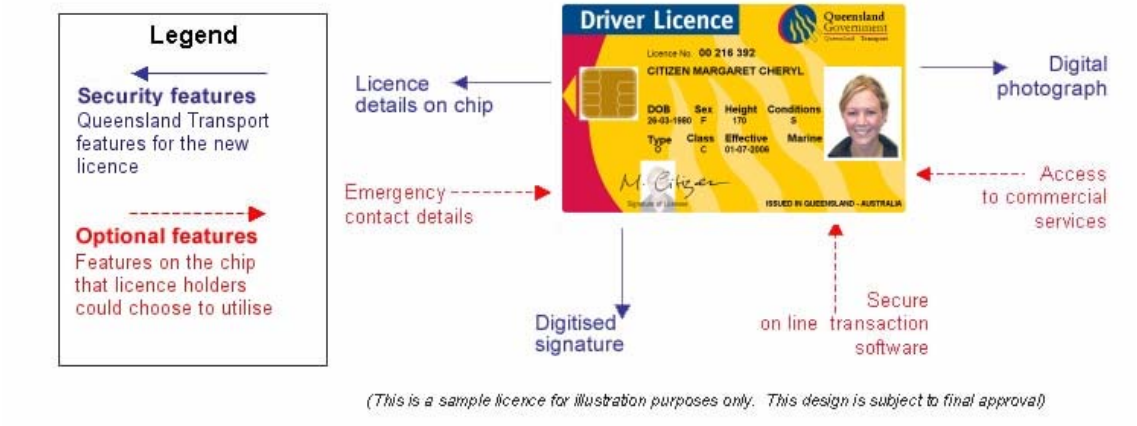
身元証明に関する犯罪との戦いや、電子商取引の支援のために、クイーンズランド州の新しい運転免許証のスマートカード化が 2007 年から計画されている（目標 200 万枚）。

このカードには、従来の免許証同様のライセンスに関する情報が含まれるだけでなく、電子化されたサイン（イメージ）と写真も含まれる。また、ユーザの意思により、緊急連絡先も含めることができ、これは緊急時に警察だけがアクセス可能となっている。

そして、行政機関との手続きの為に利用される電子証明書のソフトウェアも含まれる。

将来的に賛同が得られれば、商用サービスへのアクセスを提供することも計画しており、e-purse（電子財布）により駐車料金の支払いなども検討している。

ただし、この運転免許証のカードを銀行のカードとして利用可能とすることは無いとしている。




http://www.transport.qld.gov.au/qt/LTASinfo.nsf/index/NQDL_licence_features

●オーストラリア税関局

ここ 5 年間で、「貨物管理再エンジニアリング・プロジェクト」という大規模な統合プロジェクトがオーストラリア税関局により実施されてきた。このプロジェクトは、いくつもの申請書類を新制度に統合するもので、事業者はウェブサイトを基盤としたサービスを介して電子的に輸出入申告書を提出するよう法律で義務づけられている。新システムを利用する際には、ベリサイン証明書を購入するよう求められる。

●参考文献

アジアマンスリーニュース　2007 年 1 月号
「オーストラリアにおける医療の IT 化」
2007 年 1 月号
株式会社 NTT データ
http://e-public.nttdata.co.jp/f/repo/434_a0701/a0701.asp

Queensland driver licence
January 2007
The State of Queensland (Queensland Transport)
http://www.transport.qld.gov.au/qt/LTASinfo.nsf/index/NQDL_licence_features

The Integrated Cargo System (ICS)
Australian Customs Service
http://www.customs.gov.au/site/page.cfm?u=5523

各国の電子自治体の推進状況
第 7 章　オーストラリアの事例
平成 18 年 7 月 (2006)
財団法人　自治体国際化協会 (CLAIR)
http://www.clair.or.jp/j/forum/compare/pdf/0607-5.pdf
http://www.clair.or.jp/j/forum/compare/pdf/0607-1.pdf (表紙)

新しいセキュリティ技術と電子認証局のリスク管理に関する法的諸問題
平成 18 年 7 月
日本 PKI フォーラム　リーガルワーキンググループ
http://www.japanpkiforum.jp/shiryou/APKI-F/FY2005_LIWG_CA_Risk_Mng_J.pdf

アジアマンスリーニュース　2006 年 6 月号
「オーストラリアにおける IT ガバナンスの組織体制」
2006 年 6 月号

株式会社NTTデータ
http://e-public.nttdata.co.jp/f/repo/388_a0606/a0606.asp

アジアマンスリーニュース　2006年4月号
「オーストラリアの政府ポータル」
2006年4月号
株式会社NTTデータ
http://e-public.nttdata.co.jp/f/repo/376_a0604/a0604.asp

Gatekeeper Public Key Infrastructure (PKI) Framework
September 2006
http://www.agimo.gov.au/infrastructure/gatekeeper
http://www.agimo.gov.au/__data/assets/pdf_file/52243/Gatekeeper_PKI_Framework.pdf

「電子認証分野における各国イニシアチブの概要」
2005年6月2日
日本PKIフォーラム
http://www.japanpkiforum.jp/shiryou/e-auth_policy/overview_e-auth_v07_J.pdf

オーストラリア政府電子認証枠組　公開草案
2004年5月
日本PKIフォーラム
http://www.japanpkiforum.jp/shiryou/e-auth_policy/AU_Framework_J.pdf

E-commerce boosted by Government recognition of banking e-security system
August 2003
http://www.agimo.gov.au/media/2003/08/3025.html

ECOM調査レポート「ベンチマーク報告Ⅱ」～アジア・オセアニア編～
2002年
電子商取引推進協議会 (ECOM)
http://www.ecom.jp/ecit/report/e_gov/e_gov_4.pdf

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に関わる法制度及びビジネス環境の動向に関する調査報告書
2002/04
(財) 日本情報処理開発協会 (IPA)
http://www.japanpkiforum.jp/shiryou/business_k/biz01_rep_all.pdf

Australian Business Number Digital Signature Certificate Broad Specification
オーストラリア企業番号電子証明書仕様の大要（和訳）
2001年1月
日本PKIフォーラム
http://www.japanpkiforum.jp/shiryou/sankou/AU_ABNDSCv2_J.pdf

各国電子政府およびPKIプロジェクトの調査　調査報告書
平成13年（2001年）
（財）日本情報処理開発協会（IPA）
http://www.ipa.go.jp/security/fy13/report/foreign_pki/foreign_pki.html
http://www.ipa.go.jp/security/fy13/report/foreign_pki/foreign_pki.pdf

## 2.9　ニュージーランド

(1) 背景／国の方針、法律、国民性

ニュージーランドは人口約 409 万人、立憲君主制の国家で元首はエリザベス二世英国女王、議会は一院制となっている。

2006年11月、ニュージーランド政府は2000年から続く電子政府戦略を2003年に引き続き更新し、情報通信技術の環境変化を反映した“A strategy for e-government 2006”として発表した。この電子政府戦略の掲げるビジョンは以下の通り。

- サービスの提供と連携にむけた2010年までの改革の目標を明らかにすること
- 目標達成の成功度合いを公式サービスにむけた開発目標の指標と一致させること
- 戦略的目的の達成の為の、共同作業のキーとなる役割、標準や相互接続性、そして政府の業務構造を確認すること
- 目標達成にむけ政府横断で扱われる最新のハイレベルな仕事のアウトラインを提供すること
- 人々との関係を築くために政府がいかに技術を利用するのかという 2020 年に向けた新しい目標を制定すること

従来から電子政府戦略において重要視されているのがオンライン認証システムの構築であり、人々が電子環境で身元を明らかにできるような、一貫した方法を生み出すことが必要であるとしている。2002年4月、政府はオンライン認証の政策と実施原則を承認し、国家サービス委員会（State Services Commission）では、オンラインサービスの提供に伴うなりすましの発生率を減らすため、諸官庁がどのように認証ソリューションを構築すればよいかの指針の策定に取り組んできた。

また、システム共通の基盤整備や省庁間をまたがる調整・推進を担う部局として、国家サービス委員会配下の電子政府ユニット（EGU：E-Government Unit）が設置されており、以下の機能を通して各省庁の活動を支えている。

1. Webガイドライン、NZGLS（New Zealand Government Locator Service：ニュージーランド政府情報所在サービス）の規約の制定
2. ドメイン名の調停
3. 相互運用性（インターオペラビリティ）の枠組み
   （e-GIF：e-Government Interoperability Framework）策定
4. オンライン認証、セキュア電子環境（S.E.E.：Secure Electronic Environment）のルール化によるセキュリティ強化施策
5. 各省庁の電子政府プロジェクトの達成状況の監視・記録及び情報共有

2004年4月、EGUは行政機関向けに電子政府のための認証「認証のためのベスト・プラクティス・フレームワーク」を発表した。また、2004年10月、身元証明フレームワークを発表した。

●ニュージーランドの電子政府相互運用枠組み（NZ e-GIF）

e-GIFとは、Webサービス等の関連技術に基づいて各政府機関システム間の相互運用性を実現するフレームワークである。

e-GIFはログオンサービス（GLS：Government Logon Service）と身元検証サービス（IVS：Identity Verification Service）からなる。GLSを利用すれば、認証キーを1つ使うだけでオンライン行政サービスをうけることができる。またIVSを利用すれば、身元証明を一度ですませられるので、個々の官庁に対して手続きのたびに、改めて身元を証明する必要はない。2003年10月時点では、全体の省庁の45%が、情報システムを過去12ヶ月に導入または大幅機能改修し、そのうち33%の省庁が企画・入札段階でe-GIFを採用し、12%が採用しなかった。また、残りの省庁のうち45%は過去12ヶ月にシステム導入・大幅改修が無かったため、採用していない。なお、2006年11月に発表されたVersion 3.1が最新版となる。

●身元証明フレームワーク（EOI Framework：Evidence of Identity Framework）

本標準は、NZ e-GIFの認証標準の1つであり、取引相手のIDに信用性が求められるオンラインサービスの認証コンポーネントを設計するために有効な操作指針を概説している。本標準は、2004年10月に出版された「ID証拠の枠組み」を更新したものである。このフレームワークの開発理由は以下の通り。

・現在、省庁は、身元証明（EOI）に様々なアプローチを取れるようになったため、省庁ごとに様々な身元証明の組み合わせを要請される個人が混乱している。こうした混乱を回避するため、特定トランザクションに関連したリスクのレベルに準じて、プロセスに一貫性を持たせる必要がある。

・政府全体で身元証明にロバストで一貫した取組みをすることで、身元の不正使用、または身元詐称による個人もしくは公的な金銭損害からのユーザ保護を支援する。

・現在電子政府ユニット（E-Government Unit）は、身元のオンライン認証の問題に取り組んでいる。身元確認のためのロバストなフレームワークは、オンライン環境における全ての認証プロセスには不可欠な要素である。

・身元詐称は大きな問題になっており、EOI への一貫したアプローチの実装が身元詐称対策として有効であるようだ。海外の統計は、身元詐称により近年被害者数が非常に増加していることを示している。

このフレームワークの特徴的な内容を以下に示す。

◆信用レベル

オンラインサービスを利用しようとする個人の身元情報に要求される確信度が信用レベルであり、レベル０（匿名ユーザ）、レベル１（偽名ユーザ）、レベル２（識別されたユーザ）、レベル３（識別されたユーザと確認された処理）に分類している。

◆認証処理のコンポーネント

信用レベルは以下に示す３つの認証処理のコンポーネントにより分類される。

1. 身元証明強度（ユーザから提供された全ての身元情報に求める信頼度）
2. 認証強度（ある認証方法の使用を通じて示された信頼度）
3. 処理強度（オンライン処理に求める信頼度）

また、ロバストな認証の実現には、以下のようなコンポーネント間のバランスが重要であるとしている。

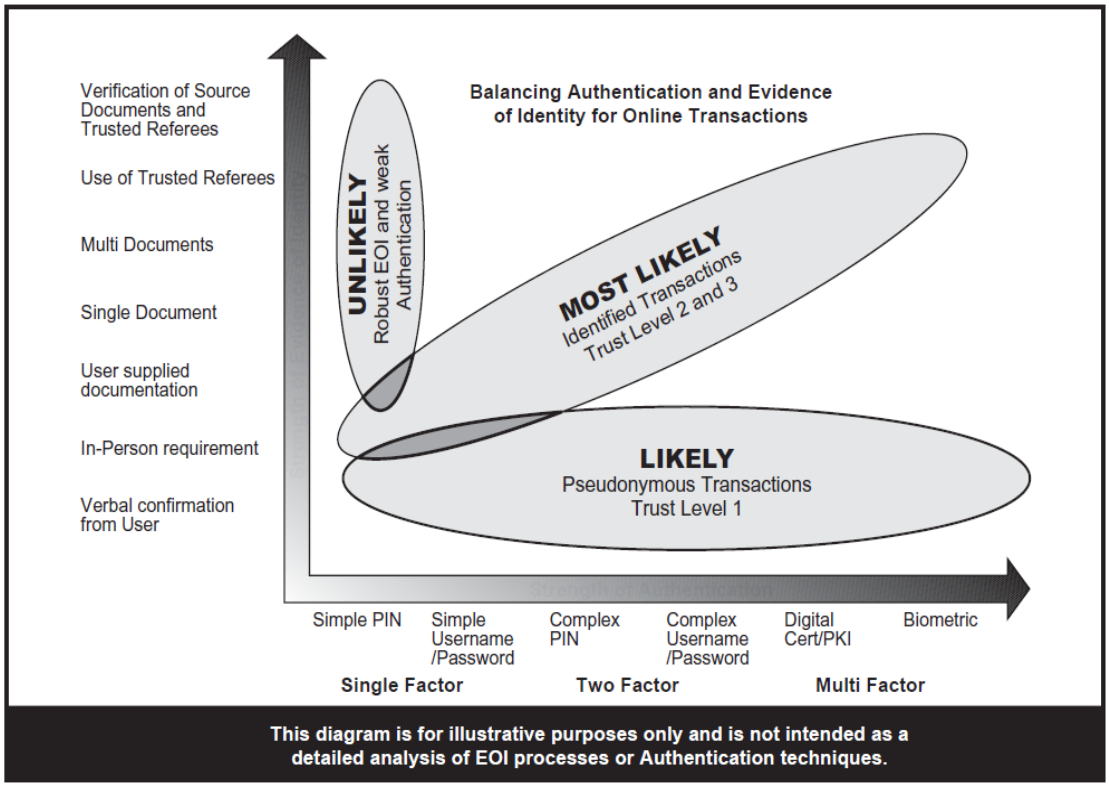



図 1.2-9 身元証明強度と認証強度の関係

●電子証明書の利用に関する指針

2004 年 4 月に発表された「Authentication for e-government：Best Practice Framework for Authentication」の中では、電子証明書の利用に関して以下の指針が示されている。

電子証明書の利用を避けるべきケース

・ユーザがコンピュータを理解出来ず、慣れていない場合
・サポートインフラストラクチャのないユーザーグループを担当している場合
・規模の巨大なユーザーグループをサポートしている場合

電子証明書の利用を考慮すべきケース

・強固な認証（価値のあるリソースを保護する）が必要な場合
・ユーザが、設定管理されているコンピュータから認証を行っている場合
・キーマネージメントとヘルプデスクインフラストラクチャを所有している場合

●E-awareness（電子政府の状況を認知する）プロジェクト

各政府機関を対象に、電子政府プロジェクトの進捗状況を調査しモニタリングする E-awareness（電子政府の状況を認知する）プロジェクトが継続的に実施されている。このプロジェクトは、各政府機関へのアンケート・ヒヤリングといった単なる情報収集にとどまらず、各プロジェクトの情報・ノウハウを共有することで各機関同士の協働を促す効果も期

待されている。ニュージーランドでは積極的な電子政府戦略のもと、様々な実験プロジェクトが精力的に行われてきたが、そこでの成功及び失敗を冷静に分析し、その後の展開へと着実に結び付けていることがうかがえる。

(2) インフラの状況／IC カード、eID、証明書発行主体

●安全な電子環境（S.E.E. ：he Secure Electronic Environment）

安全な電子環境（S.E.E.）構築プロジェクトは、政府サービス委員会、財務省、首相府の長官合同で実施している。このプロジェクト全体の主要な目的は、政府の電子メール交換（S.E.E. Mail)、権限のある公務員（S.E.E. PKI）向けの政府情報のリポジトリ（S.E.E. Directory）へのアクセスのための、安全な電子環境（S.E.E.）を開発・導入することであり、これが政府の省庁向けの安全なエクストラネットとなるということが重要なポイントである。この S.E.E.環境は、政府内部業務向けの共用のアプリケーション、業務プロセス、ワークフローシステム（例えば、政策立案プロセスである S.E.E. Workplace）を開発するためにも利用される。この環境は、データや情報の共有が容易となるように設計されており、また、将来は、守秘データについても安全に共有できるようになる。

●CA の廃業

2002 年当時、政府対応証明書の提供では大手であった BaycorpID が、2002 年 12 月にこの業界から撤退する意思を示した。既に証明書を利用していた政府機関は、自分で証明書の発行を行うことや他の業者を選定するなど、対応を迫られた。

この事件により、証明書の利用がリスク増大を招く一面もあると広く認識された。

(3) 金融部門

ニュージーランドでは、1999 年 12 月に CFISnet（Crown Financial Information System）という財務省と各省庁との財務・非財務情報の交換の為のオンライン・システムの運用が開始された。ここでは、ブラウザの認証に証明書を利用している。

(4) 公共（申請・納税）

●メールセキュリティ（SEEMail）

政府のセキュア電子メール交換システムとして SEEMail が導入された。このシステムでは、S.E.E. gateway と呼ばれるメールサーバ間で安全なメール交換が実現される。ベースとなる技術は S/MIME である。

●土地取引（Landonline）

国土情報省（LINZ：Land Information New Zealand）は、土地所有・調査情報 DB のオンライン提供サービスである Landonline おいて、証明書を利用している。

ここでは、弁護士が土地権利の委譲にともなう必要書類に電子署名することなどに利用されている。

(5) その他

児童、青年、家族機関（CYF：Department of Child, Youth and Family Services）と社会発展省（MSD：MINISTRY OF SOCIAL DEVELOPMENT）は1999年より独自にCAを構築し、アプリケーションへのログインセッションの暗号化と、ユーザ認証にPKIを利用している。

●参考文献


- E-government in New Zealand、State Services Commission、http://www.e.govt.nz/
- New Zealand E-government Interoperability Framework(NZ e-GIF) Version 3.1、New Zealand State Services Commission、Nov. 2006、http://www.e.govt.nz/standards/e-gif/e-gif-v-3-1
- Evidence of Identity Standard Version 1.0、New Zealand State Services Comission、June 2006、http://www.dia.govt.nz/diawebsite.nsf/Files/EOIStandard/$file/EOIStandard.pdf
- Authentication for e-government Best Practice Framework for Authentication、Authentication Team E-government Unit State Services Commission、http://www.e.govt.nz/services/authentication/authentication-bpf/bpf.pdf、APRIL 2004
- S.E.E. PKI Paper 14 - International and New Zealand PKI experiences across government, v 1.0、May 2003、http://www.e.govt.nz/services/see/see-pki-paper-14/see-pki-paper-14.pdf
- Technology Review, Individual-level encryption technology, Public Key Infrastructure (PKI) technology、New Zealand State Services Commission、http://www.e.govt.nz/services/securemail/securemail-options-2000406/chapter2.html#Toc74828128、June 2004
- アジアマンスリーニュース　2004年7月号　ニュージーランド:電子政府構築のプロジェクト進捗状況、http://e-public.nttdata.co.jp/f/repo/226_a0407/a0407.asp、2004年7月、株式会社NTTデータ
- 平成17年度情報基盤対策技術開発等推進費事業（次世代型電子認証基盤の整備）「電子認証ポリシーに関する調査報告書」、平成18年3月、財団法人日本情報処理開発協会、http://www.japanpkiforum.jp/hojo/shiryou/FY2005_report/04-policy.pdf
- 1 財政制度等審議会　財政制度分科会　法制・公会計部会　公会計基本小委員会(第9回)配布資料1「公会計に関する海外調査報告書（ニュージーランド)」、http://www.mof.go.jp/singikai/zaiseseido/siryou/zaiseig/g150530a.pdf、2003年5月30日、財務省
- 2005年度　経済産業省受託調査研究「電子認証フレームワークのあり方に関する調査報告書」(2006年3月)、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://202.12.30.115/ja/research/200604-CA/all.pdf
- 偽造キャッシュカード問題に関するスタディグループ（第9回）偽造キャッシュカード問

題と認証システムの考察、セコム株式会社 IS 研究所　松本　泰、2005 年 4 月 15 日、http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/03.pdf

- 本人認証技術の現状に関する調査、情報処理振興事業協会・セキュリティセンター、2003 年 7 月 29 日、http://www.ipa.go.jp/security/fy14/reports/authentication/
- 日本 PKI フォーラム電子認証ポリシー関連資料　和訳資料、http://www.japanpkiforum.jp/
- Guidance on Multi-factor Authentication Version 1.0 9.Trends 、http://www.e.govt.nz/standards/e-gif/authentication/guide-multi-factor-auth/chapter9.html、New Zealand State Services Comission、June 2006

# 第3章　欧州における PKI および証明書の利用

欧州における PKI および証明書の利用についてドイツの著名な研究機関であるフラウンホーファー研究所の調査結果「欧州における PKI および証明書の利用に関する調査」（付録に添付）から抜粋して紹介する。

## 3.1　概観

欧州委員会は、1999 年 12 月 13 日に電子署名の共通枠組みに関する指令である電子署名指令を発布した。この指令は欧州連合内で適用されるべきものであり、加盟国はこれを自国の法律に適合させなければならない。

しかし、相互運用上の問題が存在し、電子署名を必要とする応用分野は明確でないため、利用者への普及は進んでいない。とくに、クオリファイド証明書による電子署名の利用は予想よりもはるかに利用が少なく、市場はまだ十分に開拓されていないといえる。最近数年間では、これらの問題を克服するためにさまざまな国で標準化活動等の大規模なプロジェクトが遂行された。

しかし、アプリケーションとインフラストラクチャーに対する PKI ベースのサービス導入の進展状況は欧州内で大きく異なっている。しかも、電子署名指令の運営に関する EU の報告書によれば、e ガバメントおよび e バンキングは安全なインフラストラクチャーの推進力と考えられているが、銀行部門に関しては十分に利用することはできない。

署名媒体（スマートカードやその他の媒体）、技術的な実行方法、および電子署名、利用分野、登録方法、PKI の運営、相互運用性を必要とする行政手続きは各国でことなる。各国を比較した結果は、各国での普及に向けたさまざまな戦略（例えば、費用のかからない証明書、簡単な登録プロセス、USB やモバイルによる署名）にもかかわらず、電子署名はまだ広く利用されていない。

［Dumortier］の中では、電子署名のより広範囲な利用と受容に対する未解決の問題、ならびに欧州委員会の要求される活動はすでに特定されており、次のように簡単にまとめることができる。

- クオリファイド証明書およびそれに関連するサービスに対する自然状態での市場の需要は存在しない。欧州における電子署名の最大の応用分野は、限定された利用者環境の e-バンキングの用途に一般に結びついており、したがって指令の範囲外である。指令の範囲内では、応用は現在ごくわずかにしか行われておらず、ほぼ完全に e-ガバメントに限られている。
- 多くのアプリケーション・サービス・プロバイダーは、法律を順守するには利用では少なくともクオリファイド証明書による電子署名が必要であると誤って認識しており、これによって不必要な費用と複雑さがもたらされている。
- 国内と国外の両レベルにおける相互運用性の欠如は、電子署名の市場での受容と普及にとって障害となっている。
- 現在のところ EU 指令では SSCD（Secure Signature-Creation Device）に非常に高い要件が設定されていることもあって、このような装置を市場に提供する方法を見つけることはまだ非常にまれである。
- 署名に関する EU 指令の規制的な枠組みには、証明書のプロバイダーに対する極めて詳細な

規則が含まれているが、証明書のプロバイダーのその他のカテゴリーには対処していない。

［FIDIS-D41］によれば、2005 年時点ではまだ、デジタル署名、e-ID、または e-ガバメントの各サービスへの PKI システムの導入はほんの初期段階にあり、次の障害が確認されている。

- 複雑性、およびインフラストラクチャーを確立するために必要な初期投資。
- 消費者のイニシアティブ（e-アプリケーション、便利さ）の欠如 対 費用（カード・リーダー、ソフトウェア）。
- 特に証明書とサインド・エンベロップの相互運用性、第三者の認証局（CA）から発行された証明書の照合、アプリケーションによる証明書の利用、ディレクトリーが扱う証明書、およびタイム・スタンピングでの標準規格の欠如。標準規格がない中、デジタル署名への PKI の導入を進めているいくつかの国は独自の仕様を開発しており、相互運用性に将来問題を引き起こす可能性がある。
- CA 間および各国間での信頼性の相互認定（mutual trustworthiness recognition）の構築に関する法律面および手順面での規制、ならびにそれに関連する管轄区域。すなわち、（デジタル署名および契約上の法的責任に対する）方針、契約による合意、法的な枠組みの相互認定（mutual recognition）。
- アプリケーション水準での暗号技術、属性証明書、スマートカード技術、登録スキームの利用における技術的な相互運用性構築の困難が特に個々の CA 間において存在する。

## 3.2 欧州諸国の進展

アプリケーションとインフラストラクチャーに対する PKI ベースのサービス導入の進展は欧州内で大きく異なっている。ここでは、特徴のある国について紹介する。

### 3.2.1 オーストリア

オーストリア財務省、オーストリア国立銀行、グラーツ工科大学は、1999 年 5 月にオーストリア安全情報技術センター（A-SIT）を設立した。同センターは、技術的な情報セキュリティの分野における専門知識を発展させ、各種機関、経済、市民に貢献する使命を持った独立の非営利団体である。特にこの使命には、市民カード（*Bürgerkarte*）の導入および暗号方式の評価が含まれていた。また A-SIT は、デジタル署名の証明書を提供する権限を持った、最初であり現在唯一のオーストリアの組織である。

(1) eID

オーストリアの e-ガバメント戦略の基礎的な要素は市民カード（*Bürgerkarte*）である。これは電子署名とデジタル証明書が埋め込まれたスマートカードであり、これによって市民は電子公共サービスに安全にアクセスし、行政手続きを電子的に完了することができる。オーストリアの e-ID のコンセプトの独創性は、市民カードの種類が 1 つではない点である。「Bürgerkarte」は、パスポートのように各市民にとって同じ特性を持ったカードではなく、むしろ安全な電子行政サービスの設計を可能にするコンセプトである。そもそも「Bürgerkarte」は、追加の機能を組み込むことができる、手続きにおける署名ソリューションである。例えばこのカードは、公共部門においてオーストリア国民の身元を確認し、または

国の社会保障制度において国民を議員や行政機関の職員、学生として識別するために利用することができる。さらにこのカードは、支払機能を果たす。(いわゆる現金自動支払いカード(Bankomaten Karte))。原則的に、安全な形式で電子的に署名し、個人データを保存することを可能にするカードは市民カードとしての利用に適している。したがって、特定の団体(例えばオーストリア・コンピューター協会、連邦経済会議所など)が発行するメンバーシップ・カードやある種の銀行のクレジット・カードの機能を市民カードの機能に組み込むことができる。また、「簡単な」市民カード・サービスは携帯電話でも利用することができ、オーストリア国民は携帯電話を経由して文書にデジタルで署名し、政府に対する手続きを安全に行うことができる。したがって市民カードは特定の形式の技術に依存しておらず、自分の身分証明を電子的に行うためにどの技術を利用するかは完全に市民が選択することができる。IC カード、携帯電話、USB 機器のどれを使用するかにかかわらず、媒体が市民カードに不可欠な一定のセキュリティ要件(電子署名、身元確認、データ記憶)を満たすことが重要である。

自然人は、行政との電子的な通信において部門固有の個人識別子に基づいて身元が確認される。個人の固有の ID 番号(中央住民登録所に保存された ZMR 番号)から暗号化プロセスを経由して得られ、電子的に署名された形式で市民カードに保存された「ソース暗証番号」は、これらの部門固有の個人識別子を作り出す基礎として機能している。個人のソース暗証番号は、市民カードの正当な所有者のみが管理することができ、アプリケーションに直接保存することはできない。2 つの暗号化プロセスの適用(ソース暗証番号である ZMR 番号の暗号化およびソース暗証番号からの部門固有の個人識別子の取得)では、高水準のデータ保護が保証されている。

「Bürgerkarte」の立ち上げの主な動機は、オーストリアでの e-ガバメントの導入である。このイニシアティブを促進するために、オーストリアの「Bundeskanzleramt」(首相府)はすべての基本ソフトウェアおよび必要なライセンスを無料で提供している。認証局(CA)および登録局(RA)として、IC カード用署名の A-Trust やモバイル署名(いわゆる A1 署名)の Austrian Telekom 社などの民間プロバイダーが利用されている。

①費用:カードおよび署名の費用は A-Trust のウェブサイト[10]で見ることができる。価格構造は購入できるそれぞれのサービスによって異なる。一般には次の費用が適用される。

- 30 ユーロ－証明書なしの署名プレミアム・カード
- 12 ユーロ－登録および証明書の発行が 1 回
- 証明書の延長に対して毎年 15.6 ユーロ

②利用:オーストリアは e ガバメントの先導者と見なされているものの、経済的な視点から見れば発行されたデジタル署名の数はまだ限定されている。2005 年末までに発行された電子署名はわずか 70,000 件である。(オーストリアの人口の 0.7%)[11]。電子署名は、2006 年の最初の時点で依然としてあまりに高額、複雑で実用性が低すぎると考えられていた。初期の利用者は別のオペレーティング・システムを利用していることが極めて多かったため、Windows でしか利用できない点も欠点と考えられていた。

2006 年 1 月、A-SIT トラスト・センターは、クオリファイド証明書が売れなかったため、危うく支払不能[12]を発表しなければならなくなった。

**(2) e パスポート**：オーストリア政府は、2006 年夏からオーストリア国民が利用できる新たな電子パスポートを発表した。このパスポートには、冊子内表紙の 1 つのページにマイクロチップが埋め込まれている。この IC には、パスポートに書かれたほぼすべてのデータが含まれており、所有者の顔のスキャン・データも含まれている。このパスポートには、コピー防止のメカニズム、デジタル署名、暗号化伝送コードも備わっており、権限のない関係者はパスポートに含まれた情報を読み取ることができない。市民にとっては、新しい文書の導入はそれほど大きな変化をもたらしていない。有効な古いパスポートは有効期限まで提出する必要がない。新しいパスポートの価格は、大人は 69 ユーロ、子供は 26 ユーロで据え置かれる予定である。

**(3) 銀行**

オーストリアは、2005 年 1 月に、市民カードを銀行のクレジット・カードに統合する可能性を市民に提供する世界で最初の国となった。財務省と銀行クレジット・カードの発行者であるユーロペイの合意の後、オーストリアで発行されるマエストロ銀行のすべてのクレジット・カードに「市民カード」の機能を組み込むことが可能になった。利用可能な機能（銀行クレジット・カードのマイクロチップに保存されたデジタル署名）によって、すべての市民はマエストロ・カードを利用して自分の身分証明およびオンラインでの安全な取引を行うことができる。

①費用：マエストロ・カードの所有者は、2004 年 8 月 31 日まで、現在のカードをデジタル署名が含まれた新しいカードと無料で交換することができた。この日以降、この「プレミアム」機能には年間 12 ユーロの費用がかかる。このカードは、インターネットおよびカード・リーダーと接続された PC と併せて利用しなければならない。このサービスの理解を高めるため、200,000 台のリーダーが販促価格で提供された。取引に関連する e ガバメント・サービスの受容を促進することに加えて、銀行／市民の一体型カードでは、ビジネス間（e-ビジネス）およびビジネスと消費者の間（e-コマース）でのデジタル署名の利用を促進することになっていた。

**(4) e ヘルス**

**e カード**（電子健康保険カード）の全オーストリアでの普及キャンペーンは 2005 年 11 月に成功裏に完了し、ついに紙ベースの医療カード証明書に取って代わった。約 800 万枚の e-カードが作成された。e-カードでは、**市民カード**の機能を有効化することが可能であり（無料）、したがって追加的に e-ガバメント・サービスで利用することができる。この IC カードには、所有者の氏名、肩書き、生年月日、社会保険番号などの行政上のデータが含まれている。このカードには最新のデジタル署名機能も含まれており、認可を受けた所有者は政府機関に対する電子手続きにカードを利用することができるようになる。

①利用：2006 年 10 月までに約 820 万枚の e-カードが発行された。が、無料であるにもかかわらず、市民カードに対する最新の署名証明書によってこのカードの機能を強化する選択肢を選んだ人はわずか 8,500 人しかいない[13]。

**(5) モバイルによる身元確認**

2004 年 4 月、モバイル通信事業者である mobilkom austria 社は A1 SIGNATUR、*e-ガバメントのためのモバイル身元確認サービス*を立ち上げた。このサービスでは、e-ガバメントの利用者を携帯電話経由で身元確認／認証することが可能であり、またオーストリア国民は、市民カ

ードやソフトウェア・ベースのデジタル署名を所有する必要なく、文書にデジタルで署名し、政府に対する手続きを安全に行うことができる。

### 3.2.2　ベルギー

#### (1) eID

ベルギーの e-ID カードには、所有者の個人データとデジタル証明書が保存されたマイクロチップが埋め込まれており、リモート認証が可能である。2003 年から 2004 年に行われた約 70,000 枚のカードの 11 地方自治体（コミューン）への試験配布が成功した後、次にベルギーの残り 578 の地方自治体が 2009 年末までにこの移行を完了しなければならない。すべてのベルギー国民はこのときまでに電子 ID カードを所有することが求められる。ベルギーの e-ID カードと互換性のある数多くのアプリケーションとサービスが 2005 年にすでに利用可能だった。これには、オンライン所得申告、認定 E メール、オンラインでの公式文書の要求、インターネット・バンキング・サービス、電子図書館サービスなどがあった。

現在配布されているベルギーの e-ID カードは、第 1 世代のカードのみである。第 2 世代のカードは 2007 年末まで、第 3 世代のカードはその後発行される予定である。この 3 段階の展開に沿って、ADAPID（フランドル地方における電子 ID カードのための先進的アプリケーション）プロジェクトでは、第 1、第 2 世代の e-ID カードのセキュリティおよびプライバシーの問題を調査し、第 3 世代のためのより適切な設計および e-ガバメントと e-ヘルスのための先進的アプリケーションを提案する予定である。2009 年 6 月 30 日まで続くこのプロジェクトでは、数多くのプライバシー要件に取り組む予定である。

2006 年 11 月現在、約 400 万枚の eID カードが発行されており、350 万枚が有効化されている。市民は、e-ID カードの署名機能と認証機能の無効化を要求することができる。しかし 1 度無効化されると、再び有効化することはできない。

ベルギーの eID カードは、専門的には、異なる 3 つの 1024 ビット RSA 署名プライベート鍵（FIDIS-D36）を保持している。1 つは市民の認証、1 つは署名、1 つはカード自体の身分証明をベルギー政府に対して行うためのものである。eID カードは、3 つのプライベート鍵をすべて利用してデジタル署名を演算処理することができる。市民の認証鍵と否認防止署名鍵については、所有者が暗証番号を入力した後にのみこれが行われる。この暗証番号は市民が入力しなければならず、信頼できる何らかのハードウェア（例えば、独立型キーパッドが付属したスマートカード・リーダー）を利用するのが望ましいとされている。最初の 2 つの鍵ペアにはそれぞれ証明書が添付されている。これらの証明書は市民に対して発行される。すなわち 1 つの認証証明書は、例えば SSL/TLS に対する利用者の認証に使用するためのものである。2 つ目の証明書は、手書きの署名に等しい電子署名を生成するために使用できるクオリファイド証明書である。これらの証明書のいずれにも市民の E メール・アドレスは含まれていない。カードの第 3 の鍵ペアのプライベート鍵は、カードが相互認証のために国営登録所（RRN）と通信を行うときに利用される。（例えば、カード所有者の詳細（典型的には住所）、国の証明書などを更新するため）。RRN は、この第 3 の鍵によって算出された署名を照合するために、公開鍵のコピーをデータベースに保存している。それぞれの eID カードは、ベルギーのルート CA の証明書の真

正のコピーによって初期化されているため、このカードは「信頼できるソース」として利用できる。すなわち、各利用者は、ベルギーのルート CA の証明書を自分のスマートカードから読み込むことで、ベルギーの PKI システム内の信頼の連鎖を立証することができる。したがって eID プロジェクト全体は、発行段階で各市民が地方自治体に自ら出頭しなければならないので、確固たる利用者認証を行った全国的な PKI と見なすことができる。eID カードに関連するすべての証明書は、Belgian Post Group とベルギー最大の電気通信事業者である Belgacom 社の合弁事業である Certipost consortium によって発行される。

①費用：費用については、新しい ID カードの配布を担当するコミューンは、従来の ID カードが現在 5 ユーロから 7 ユーロであるのに対して、eID カード 1 枚につき 10 ユーロから 15 ユーロを市民に請求することができる。この新しい文書は 10 年ごとではなく 5 年ごとに更新しなければならなくなり、これによっても費用負担が増加して事実上価格が 4 倍になっている。コミューン自体は、従来の型で要求される 4 ユーロではなく 10 ユーロを連邦政府に支払わなければならなくなる。これらの費用を消費者に転嫁するかどうかは、個々のベルギー・コミューンの判断に任されている。すべてのベルギー国民は、2009 年末までに電子 ID カードを所有することが求められる。

②利用：ベルギーの最近の調査（2006 年）では、ベルギーのインターネット利用者の 43%は eID カードを現在所有しているものの、電子カード・リーダーを所有しているのはわずか 8%であることが明らかになった。その結果、eID カードが提供する可能性の多くは活用されていない。行政事務簡素化担当大臣は、ベルギーの電子 ID カードによって可能になったサービスの利用を増加させるため、行政事務簡素化の本部であるカフカ・コンタクト・ポイントと連絡を取って 5,000 台の eID カード・リーダーを無料でベルギー国民に配布することを発表した。eID カードに関連した試験プロジェクトを導入する地方の行政機関やコミューンも無料のカード・リーダーを受け取る。

**(2) e パスポート**

2004 年 11 月にベルギーは、国際民間航空機関（ICAO）の提言に準拠した電子パスポートの発行を世界で最初に開始した。このバイオメトリック・パスポートには、所有者の顔の画像が保存されたマイクロチップが埋め込まれている。欧州で適切な立法が行われた後、指紋が後の段階で追加される予定である。

### 3.2.3 チェコ共和国

チェコ共和国は、信頼性がありかつ安全な e ガバメント・サービスを市民に提供する試みの一部として、2006 年 7 月に電子署名とタイムスタンプサービスを導入した。チェコの IT 省は、すべての政府機関が法律で要求される要件（電子形式の提出物の受け取り、電子アドレスへの文書の送付、電子形式での行政活動の発表など）を満たすことができるように、すべての公共団体に効果的な認証システムを供給したいと考えている。市民、自然人、法人は同じ技術にアクセスできなければならない。現在、彼らは財政およびその他の行政手続きのためにそのシステムを利用している。

### (1) 電子署名

2006 年 7 月、次の 3 つの組織が新しい電子署名およびタイムスタンプの発行を委託された。認証局（První certifikační autorita a.s.）、eIdentity 社、Czech Post である。これらの機関は、単純な *PostSignum VCA* 証明書、クオリファイド *PostSignum QCA* 証明書などのいくつかの種類の認証証明書を発行する。

チェコの労働社会政策省は現在､数多くの IC カードを利用している唯一の国家機関である。同省の eID は、主に省の情報システムへのアクセスや省内の機密情報のやりとりに利用されている。

## 3.2.4　デンマーク

### (1) 電子署名

デンマークは電子 ID カードや電子身分証明書を提供しておらず、提供する意向もない。2003 年 2 月以降、デンマーク政府は利用者認証の手段として「無料のデジタル署名」を市民に提供している。そのコンセプトは一般に「公共のデジタル署名」と言われており、これによって市民はオンラインの公共サービスを安全な方法で利用することができる。

このデジタル署名プロジェクト[16]は、デンマークの e ガバメント・プログラムの一部として開始され、このプログラムは公共部門の近代化と発展への要求の高まりに応えるために立ち上げられた。デジタル署名プロジェクトの目標は、公開鍵基盤に基づく、オープンで拡張可能なセキュリティ・インフラストラクチャーを確立すること、またデジタル署名のための効果的な登録手続きおよび配布の仕組みを市民、企業、行政機関に対して確立することである。このデジタル署名プロジェクトは、科学技術革新省と TDC（デンマーク最大の電気通信企業）間の官民の提携として組織されている。TDC は、デジタル署名の確立、発行、維持管理を担当する認証局として活動している。TDC との官民の提携は、インフラストラクチャーと魅力的な電子サービスの維持管理および開発を確実に行うために確立された。

このデジタル署名はソフトウェア・ベースのデジタル署名であり、パスワードの使用が義務となっている。パスワードは、ウェブサイトへの入場管理、暗号化、および E メール、ウェブ・フォーム、ウェブ文書のデジタル署名に利用することができる。このデジタル署名は、個人の署名、被雇用者の署名、ビジネスの署名として発行されている。

①利用：デジタル署名の導入によって、2005 年 5 月時点で合計 375,140 件のデジタル署名の発行がもたらされた。その内訳は、321,753 件が個人のデジタル署名、50,999 件が被雇用者のデジタル署名、2,388 件が企業のデジタル署名だった。2005 年 2 月時点で、デンマークの行政機関の 90%近くがデジタル署名を導入しており、安全な E メールを送受信するための適切な方法を確立している。2005 年 5 月 25 日時点で、デジタル署名を利用する電子サービスが 400 超開始されている。

②費用：デンマーク政府は、約 4,000 万デンマーク・クローネ（570 万ユーロ）を費やしてデジタル署名の普及キャンペーンをサポートし、その一部は TDC が最初の立ち上げのパートナーを手助けするために利用した。証明書は無料である。

### (2) e ヘルス

デンマークには、市民ごとに生涯利用する単一の患者番号が存在する。すべての薬品、臨床所見、医師の処方箋は、公法で管理されているメドコムが運営する中央データベースに保存される。医師と薬剤師は、それぞれ読み書きすることが認められている。患者は自分のデータをインターネット経由で読み、そのデータに誰がアクセスしたか確認できるが、これはメドコムのデジタル署名証明書を持っている場合に限る。

## 3.2.5 エストニア

IDABC[17]の分析によれば、欧州全体における ICT および e-ガバメントの展開という点では、エストニアは 2003 年にすでに最も先進的な国の 1 つであると広く見なされていた。

### (1) eID

エストニアは 2002 年 1 月に国の ID カードを発行し始めた。このカードはエストニアのデジタル署名法の要件を満たしており、すべてのエストニア国民および 16 歳以上の永住権を持つ外国人にとって義務となっている。このカードは市民および居住者の身元を確認する主要な文書となるように作成されており、その機能はビジネス、政府関連または個人のあらゆる形式の通信に使用することができる。市民権・移民委員会（Citizenship and Migration Board）が発行するこのカードは、身分証明書および旅券（EU 内）として 10 年間有効である。このカードは、物理的な身分証明書であることに加えて、公共および民間のオンライン・サービスに対して安全な認証および法的拘束力のあるデジタル署名を手助けする高度な電子機能も備えている。

2003 年 3 月に立ち上げられたエストニアの e ガバメント・ポータル[18]は、公共のオンライン情報およびサービスに対する単一のアクセス・ポイントを提供している。このポータルは、国の ID カードによる認証を通じて、電子フォームを記入・提出し、個人データにアクセスし、手続きを行う可能性を利用者に提供している。

電子プロセッサーIC には個人データ・ファイルならびに認証のための証明書およびデジタル署名の証明書が含まれている。この証明書には、所有者の氏名と個人コード（国の ID コード）のみが含まれている。また、認証証明書には所有者固有の E メール・アドレス（公共部門との電子通信のための不変の E メール・アドレス名.*姓@eesti.ee* が伴う）が含まれている。このデータ・ファイルは ID カードと同じ期間有効である。デジタル証明書は 3 年間有効で、無料で更新することができるが、ID カードの有効期間より長くすることはできない。2006 年 10 月で 100 万枚の ID カードが発行されている。

2003 年、フィンランドとエストニアは、デジタル署名、文書形式および文書交換について 2 国間のコンセプトとプラクティスの調和を図る協定に署名した。OpenXAdES とコードネームを付けられた両国の署名プロジェクトは、「普遍的なデジタル署名」を促進するオープン・イニシアティブである。

**「コンピューター保護 2009 年」**のイニシアティブでは、エストニアを 2009 年までに世界で最も安全な情報社会の国にすることを目標としている。この目標を達成するために、数多くの副プロジェクトが立ち上げられる予定で、優先分野の 1 つは電子サービスの利用における ID

カード・ベースの認証の促進となっている。エストニアは、電子 ID ベースの認証およびデジタル署名において確立したプラクティスを持つ欧州国家である。エストニア国民は、2005 年 10 月の地方政府の選挙において、安全な ID カードを認証メカニズムとして使用して電子的に投票することができた。2009 年までには、電子認証（electronic authentication）における ID カードの利用が 20 倍増加すると予想されている。

①利用：国の ID カードに加えて、エストニア居住者はインターネット・バンキングの身分証明データを利用してオンラインの公共サービスにアクセスすることもできる（エストニア居住者の 70%超がインターネット・バンキングを利用しており、これは欧州で最も高い比率である。）。PIN コードの盗難や紛失があった場合は、サポート・ライン（1777）に電話することができる。

②費用：ID カードの発行費用は約 9.70 ユーロである。

### 3.2.6　フィンランド

#### (1) eID

フィンランドは電子 ID カード（*FINEID*[20] カード）を欧州で最初に発行した国である。1999 年 12 月 7 日、応用段階を開始する 1 つの方法として第 1 号カードがフィンランド首相に贈られた。このカードは公開鍵基盤（PKI）および証明書に基づいている。この ID カードは、フィンランドのあらゆる国民または永住者に与えることができる。FINEID プロジェクトは、オープンで無防備なネットワークにおいて公式の手続きを安全に行う手段を提供するインフラストラクチャーの構築を目標としていた。

また、市民証明書は、警察が発行する IC 式の ID カード、銀行のクレジット・カード、または携帯電話の SIM カードに組み込むことができる。市民証明書は、政府職員の証明書と同様、電子取引、E メール、文書の暗号化における確実な身分証明書、および電子署名として利用することができる。

技術的なデータに加えて、このカードの IC には住民登録センター[21]（PRC）のいわゆる認証局証明書およびカード所有者の身分証明書と署名証明書が含まれている。PRC は認証局の役割を果たしており、FINEID の証明書を発行している。PRC は現在のところ、フィンランドにおけるクオリファイド証明書の唯一のいわゆる認証局であり、電子署名に関する法律および関連する EU 指令で規定されたとおりに全欧州の証明書を発行することができる。PRC が発行した個人の証明書は、すべてクオリファイド証明書である。

カード所有者の証明書に含まれる唯一の個人データは、名、姓および利用者の固有の電子識別子（SATU）である。すなわち、所有者の個人 ID 番号、住所、生年月日またはその他同様の情報は IC に保存されていない。SATU は、個人の ID 番号とは異なり、所有者について何も表さないシリアル・ナンバーである。FINEID の証明書方針に従って発行される証明書は、証明書所有者の身元を認証し、デジタル署名およびデジタル文書の信頼性またはその他のデジタル・データを検証し、さらに電子通信、電子取引または電子データの転送の機密性を確保するためのものである。

PRC は PKI ベースの証明書を発行している。第 1 の鍵ペアは認証および暗号化のために、第

2の鍵ペアは電子署名のために利用される。鍵の使用は合致するPINコードでのみ可能である。PIN コードが鍵を有効化し、その後 IC は必要な計算オペレーションを提供できるようになる。プライベート鍵は証明書の所有者のみが（例えば ID カードの IC 上に）保有し、PIN コードを入力してはじめて利用することができるが、このときでもカードから読み取ることはできない。PIN コードを知るのはカード所有者のみであり、所有者は必要な場合にそれを変更することができる。PINコードの入力を3回間違えるとカードがロックされる。

FINEIDカードの申請は、地域の登録局の役割を果たす警察当局または警察から権限を与えられた団体に本人が出向いて行いる。電子 ID カードは地域の登録局から本人が受け取らなければならず、このとき申請者の身元が再度確認される。

利用者の電子識別子は、例えば警察が ID カードを発行したときに市民証明書として有効化される。次に市民証明書がIDカードのICに埋め込まれる。市民証明書は銀行のデビット・カードおよび／またはモバイル機器のSIMカードに添付することもできる。どの市民も有効な市民証明書を同時に何枚か所有することができる。しかし、それらの証明書にはすべて同じ利用者電子識別子がついている。証明書の情報内容およびその信頼性は、認証局の電子署名によって検証される。住民登録センターの商標は、公共の市民証明書を利用するオンライン・サービスを利用者が発見・識別する上で役立つ。

①利用：FINEID カードの初期の受け入れ方は非常にゆっくりとしたものであり、2000 年の立ち上げ以来、2003 年中頃までに約 500 万人のフィンランド国民のうちわずか約 16,000 人しかカードを購入しなかった。12 月末までには合計で 96,100 人に市民証明書が発行された。このうち、81,300 の市民証明書が有効化された。14,900 人は健康保険の情報を自分の ID カードに組み入れた。フィンランド政府の目標は、2007 年末までに 200 の eID サービスが利用できるようにすることである。

市民証明書は2006年9月末までに合計で120,500人に発行された。このうち、104,100の市民証明書が有効化された。22,900人は健康保険の情報を自分のIDカードに組み入れた。

②費用：IDカードの費用は40ユーロで5年間有効である。

**モバイル**：市民証明書はSIMカードに組み入れることが可能で、これによって携帯電話利用者は単一のコードで簡単に身分証明を行うことができる。利用者の身分証明に加えて、この証明書によって、認証、交換されるデータの機密保持、および情報の整合とメッセージの送付を確実に行うことができる。

2005年以来、フィンランドの住民登録センターは、インターネット上で公式の手続きを行うための革新的なソリューションを市民に提供しており、これによって市民は、オンラインのサービスや要求のために確実な身分証明書が必要なときに携帯電話を利用できる。モバイル署名で必要なセキュリティ証明書が備えられた最初のSIMカードは、フィンランドで2番目に大きなモバイル・ネットワーク事業者であるElisa社から提供されている。この基礎となるのは、国際的な技術企業グループである Giesecke & Devrient 社（G&D）の署名機能および暗号化メカニズムが備えられたUniverSIM製品ラインである。Elisa社は、フィンランドの住民登録センターと協力して携帯電話経由で利用者の身元を確認するこの新しいサービスを提供する最初の事業者である。市民証明書はG&DのSIMカードに保存される。これはモバイル・セキュリテ

ィ・アーキテクチャー（公開鍵基盤）の一部であり、身元確認に要求されるセキュリティと独自性を確実に実現する。例えば市民が新しい住居へ引っ越したことをオンラインで登録したいときには、インターネットで該当するページを開き、フォームに記入して、オンラインの要求に対してモバイル署名の入力を求める登録事務所からのメッセージを携帯電話で受け取る。この市民は、個人の暗証番号を入力してデジタル署名の生成を許可する。デジタル署名はSIMカードによって生成され、暗号化された特別なメッセージとして登録事務所に返信される。公式の手続きに携帯電話でのデジタル署名の使用を望む市民は、地域の警察署で登録しサービスを申し込むことができる。統合的なセキュリティ証明書が備えられたG&DのSIMカードはJava™技術に基づいており、128Kb の記憶容量がある。このカードは現在、Elisa 社の指定販売店で入手できる。

**政府職員カード**：2006年、政府職員のためのIC式のIDカードがフィンランドの中央政府全体で採用されつつある。[22]。この写真付きのIDカードには、情報ネットワークにログインするための身分証明、ネットワーク利用者およびその利用権限の認証、E メールおよびその他の文書の暗号化、拘束力がありかつ疑いの余地のない電子署名の提供をフィンランドの法律で規定されたとおりに可能にするクオリファイド証明書が含まれている。これらの政府職員証明書はアクセス・コントロール・システム、在宅勤務、通行管理、物理的な身元確認にも利用できる。このIDカードと証明書はフィンランドの住民登録センター（PRC）で作成され、カードはSetec社が提供している。政府職員証明書は、国民が入手可能なクオリファイド証明書（または市民証明書）と同様に、フィンランドの証明書インフラストラクチャーの一部となっている。

**認証システム**：フィンランドは、フィンランドの地方自治体の ID 認証システム間の相互運用性の問題を解消するために、すべての中央政府および地方政府の機関のための安全な単一の認証標準規格への切り替えを 2006 年前半に準備している。以前は、地域の個々の機関が独自のID照合システムについて供給業者と交渉していた。その結果、それぞれのシステムは互換性がなかった。情報技術インテグレーターの Fujitsu Services 社がフィンランドの行政機関に電子認証ネットワークを提供している。この新しいシステムは、政府のあらゆる電子アクセス・サービスのための調和のとれたウェブ認証および支払機能を行政機関と市民の両方に提供し、さらには銀行支払の照合システムに接続される予定である。

(2) **e ヘルス**：*Kela Card*[23]（個人の健康保険カード）の目的は、薬局で薬品を購入するときにフィンランドの社会保障を受ける資格があるかどうかを証明することにある。もし望めば、健康保険に関する情報はIDカードに組み入れることも可能で、この場合IDカードは別のKela Cardに取って代わる。オンライン・サービスでは、この ID カードはコンピューターに取り付けられた読取装置およびカード・リーダー・ソフトウェアとともに使用される。

### 3.2.7　ドイツ

ドイツ連邦政府によって *e カード戦略*[25] が2005年3月9日に発表された。政府は、将来の電子健康保険カードおよびIDカードを単一の共通な文書に結合し、市民がe-ガバメント・サービスに簡単にアクセスできるようにすることを提案した。e カード戦略では、利用者の身元確認、社会保障に関する情報、健康保険サービスの分野における数多くのe-ガバメント・イニシ

アティブに共通の戦略的枠組みをもたらすことを目標としている。この共通戦略では、連邦政府のさまざまな e-カード・イニシアティブ（電子健康保険カード、e-ID カード、求職カードなど）ならびに重要なデータベースおよび社会保障と税務上の手続きの分野におけるサービスへのアクセスを協調させる。この戦略では特に、取引に関連する e-ガバメント・サービスの開発と受容を促進し、効率の向上と費用の節約を最大にするために、共通の基準を定めている。

ドイツの連邦政府による「*e ガバメント 2.0*」[26]プログラムは 2006 年 9 月に立ち上げられた。このプログラムでは現在と 2010 年の間の主要な活動が計画されている。e ガバメント 2.0 は、EU の i2010 イニシアティブの e ガバメント活動計画ならびにドイツ自身の BundOnline 2005 および Deutschland-Online の経験に基づいている。戦略的目標には、電子 ID カードの導入および eID のコンセプトの策定から構成される「身分証明書」、および市民、企業、行政のための安全な通信基盤で構成される「通信」が含まれている。

**電子署名**：T7 e.V.[27]は、E メールの安全な交換、電子署名の応用および IT セキュリティ管理（これらはすべて公開鍵基盤に基づくソリューションを必要とする。）を対象とした、デジタル署名のためのドイツのトラストセンター・ワーキング・グループである。これらを E-ガバメント・アプリケーション、および行政機関、産業、金融部門による利用のために導入するのをサポートするために、TeleTrust は T7 グループと共に相互運用可能なソリューションの開発および試験のための基礎的な要素を開発した。このワーキング・グループは、一般市民にとって包括的かつ調整がとれた形で公開鍵基盤の複雑なテーマを紹介する手段を考案している。この団体に加入するには、加入を希望する企業がすでに認定された証明書サービス・プロバイダーであるか、または 1 年以内にそれになることが求められる。

**PKI**：ドイツ署名法[28]、署名法令[29]、およびその他関連する文書と詳細では、セキュリティ・コンセプトが検証・確認されており、試験され確認された技術要素のみを利用する証明書サービス・プロバイダーだけが活動を開始することが確認されている。連邦ネットワーク局[30]は、マインツの事務所でクオリファイド証明書サービス・プロバイダー（トラスト・センター）を認定し、認定されたプロバイダーを監視し、これらに鍵の証明書を発行し（次に最終消費者に鍵の証明書を発行する必要がある。）、トップレベルの国営 CA すなわちルート CA を運営している。この機関は、証明書団体の認定だけでなく、すべての公認証明書サービス・プロバイダー（クオリファイド証明書／署名について）の監督にも責任がある。個々のサービス・プロバイダーの組織構造全体および業務の流れ、スタッフの資格および信頼性、そして財源（単に一時的な状態でない自立的運営が保証されなければならない。）が認定（認可）を与えられる前に調査され、調査はその後 3 年ごとに行われる。署名法が意味する範囲内での「クオリファイド」署名は、法的拘束力のある手書きの署名と同等であると見なされている。ドイツでは、IC カード自体（オペレーティング・システムなども含まれる。）だけでなく、例えば鍵の生成装置も認定の一部として調査・評価される。証明書サービス・プロバイダーのリストは連邦ネットワーク局によって公表される。[31]。

①利用：電子署名を促進するさまざまな戦略にもかかわらず、利用率はまだかなり低い状態である。この理由により、2005 年に認定トラスト・センター（TC トラストセンター）が支払不能を発表した。今のところ GeoTrust 社が TC トラスト・センターを引き継ぎ、業務を続け

ている。

②費用：クオリファイド証明書および先進的証明書は 3 年間有効で、D-Trust トラスト・センターでの費用は 160 ユーロである。トラスト・センターは、それぞれ独自の製品および価格戦略を持っている。

**銀行**：SparkassenCard[33]は、2005 年時点で、クオリファイド証明書による電子署名の証明書を組み込むことができる最初の銀行クレジット・カードだった。クオリファイド証明書の費用は、有効期限によって異なる。例えば 1 年以下の有効期限については 19.95 ユーロで、3 年を超えると 79.00 ユーロである。

**eID**：2006 年 9 月、証明書に基づいて認証およびデジタル署名をサポートする、2008 年に開始される電子 ID カードの発行をドイツが計画することが決定された。この決定は e ガバメント 2.0 戦略の一部である。

**外国人カード**[34]：2006 年 10 月に発表されたように、ドイツ国民のために計画された eID カードと同様、電子式「外国人カード」がドイツの在住許可証と間もなく取って代わる可能性がある。電子式外国人カードによって、電子 ID カードがドイツ国民に提供する機能と似た身分証明機能が計画されている。外国人カードは、デジタル式の在住許可証に相当するものになる。写真や指紋などのバイオメトリック・マーカーも組み込まれるだろう。

### (1) e パスポート

IC に保存された写真という第 1 段階のバイオメトリクスが組み込まれた 300 万の e パスポートが 2006 年までに発行された。連邦政府機関は現在、パスポートに組み込むためのデジタル指紋を取る第 2 段階に移行している。

### (2) e ヘルス

連邦社会保健省は、ドイツ市民のために e ヘルス・カードの導入を計画している。医師と薬剤師はヘルス・プロフェッショナル・カードを受け取る予定である。このカードには例えば処方箋に署名するための電子署名が備えられている。

このプロジェクトの主な目的は、医療部門のすでに確立されたプロセスをデジタルでサポートすることである。重要な例として次のものがある。

- 患者が健康保険の被保険者であることを医師の事務所や病院で確認する（現在すでに IC カードでサポートされている）
- 医師が必要とする場合、アレルギー・データ、長期的な薬物治療、血液型、免疫証明書などの現在は紙に保存されている情報を移転する
- 他の医師への照会
- 処方箋および薬局での薬品の購入

認証および緊急用のデータは別として、カードに保存されているすべてのデータは暗号化され、利用者が管理する暗証番号で保護されている。利用者は、自分のカードに保存されたすべてのデータに対して自由に読み取りのアクセスができる（例えば自分のカード・リーダーや公共の端末を使用してアクセスする。）。

照会や処方箋などのデータの移転に利用する場合、患者の e-ヘルス・カードのデータにアクセスするには*ヘルス・プロフェッショナル・カード*が必要である。e-ヘルス・カードの緊急用

データは暗号化されている。が、e-ヘルス・カードの暗証番号を必要とすることなくヘルス・プロフェッショナル・カードでアクセスすることができる。

### 3.2.8　EU

**市民カード・スキームの標準規格**

より迅速かつ広範囲な受容をもたらす意図の下、市民スマートカードの統合のためにすでに行われているあらゆる取り組みに条件を提供するために、複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化に関するCEN/ISSSのワークショップが立ち上げられた。このCENワークショップの合意では、市民サービス・スマートカード・スキームを構築する上で不可欠な組織面および運営面の規則、プロセス、技術的手法が導入されている。MMUSSTアプローチで特徴となっているのは、複数のアプリケーションおよび複数の発行者のスキーム間で地域レベルから国際レベルまでの相互運用性を可能にする点である。MMUSSTは、SmartCities（ISTプロジェクト12252）の活動を基礎としている。

その事業計画案は次の内容を含むCWA15535で明確にされている。

- CWA15535-1：複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化パート1－ビジネス・モデルの合意
- CWA15535-2：複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化パート2－スキームの構造および導入ソリューション

**欧州市民カードの標準規格**

欧州市民カードに対する標準規格も現在CENで承認が進められている。これはCEN/TS15480と呼ばれており、次の内容が含まれている。

- prCEN/TS15480-1 IDカード・システム－欧州市民カード－パート1：物理的プロトコル、電気的プロトコルおよびトランスポート・プロトコルの特性
- prCEN/TS15480-2 IDカード・システム－欧州市民カード－パート2：論理データ構造およびカード・サービス

**電子認証標準規格（eAuthentication Standard）**

2004年、電子認証に関するCEN/ISSのワークショップ［CEN/ISSS2004］では、3つの領域（スマートカード、バイオメトリクス、デジタル署名）について、すべての基礎的な要素が十分に整備されていると結論付けられた。しかし、電子認証を提供するためには、スマートカード、バイオメトリクス、デジタル署名の各標準基準を結合させる必要があった。CWA の電子認証はこのギャップを埋めるものであり、これら3要素の相乗効果について詳しく述べられている。「スマートカードおよびeガバメントのアプリケーションのための電子認証」に関するCENのワークショップは、この結論に従って次の複数のパートからなるCWA15264を作成した。[38]。

- CWA15264-1：スマートカード・インフラストラクチャー内の欧州の相互運用可能なeIDシステムのためのアーキテクチャー
- CWA15264-2：相互運用可能なIASサービスを組み込んだ複数アプリケーションのカード・スキームを作成するカード・スキーム運営者のためのベスト・プラクティスのマニュアル
- CWA15264-3：スマートカード・インフラストラクチャー内の欧州の相互運用可能なeIDシス

テムに対する利用者の要件

**公共調達**

2004 年 4 月 30 日に発効した公共調達に関する新しい指令［EU-RepDirSig］によって、公共調達で電子署名を利用するための法的な枠組みが完成した。電子署名の利用は、運営可能な電子調達システムを EU 全体で確立する上で中心をなすものである。電子調達は主要な応用分野の 1 つになることが期待されており、特により進んだ形態の電子署名が期待されている。電子調達では、電子署名の利用を促進する際に克服すべき課題が明らかにされている。公共調達に関する新しい指令では、電子入札にどの形式の電子署名を利用すべきかについて明らかにされていないが、指令 1999/93/EC を実行する国内法と一致していることを条件に加盟国にその選択を任せている。これは、EU の調達指令が入札申込みの署名および安全確保の様式を規制していない、紙の入札申込みに対する現在のやり方を反映している。

加盟国が異なる水準の電子署名を選択できるという事実は、国内で開発された製品を考慮して電子調達ソリューションが設計されるというリスクを示唆している。このリスクにより、調達市場が分断され、電子署名の国際的な市場に障壁がもたらされている。

現在の課題は、国際取引に障壁を築くことなく、電子調達のために欧州全体で電子署名を導入することである。この新しい指令は、電子調達を 2010 年までに欧州で確実に普及させるために、2005 年から 2007 年の目標を設定し、欧州委員会および加盟国にとって可能な活動を特定する活動計画によって補完されている。この活動計画では、相互認定（mutual recognition.）に基づく電子署名のための運営上のソリューションを必要としている。

**Porvoo Group**

Porvoo Group[39] は、欧州における公共部門および民間部門の安全な電子取引の確保に貢献するために、PKI 技術および電子 ID カードに基づいて、国際的に相互運用可能な電子身分証明書を促進することを主要な目標とする国際的協同ネットワークである。

2006 年 5 月 11 日および 12 日、国際 Porvoo Group の第 9 回会議がスロベニアのリュブリャナで行われた。この会議には、欧州 21 カ国、グルジア、日本、米国ならびに欧州委員会および国連の代表が約 100 人集まり、欧州の相互運用可能な電子身分証明書に向けた進展について検討した。この会議では、地球規模の調和、標準化、相互運用性に関連する問題が取り上げられた。アジェンダのその他の項目には、EU 内で行われている準備、欧州市民カードの開発、バイオメトリクスおよび電子 ID カードと電子パスポートにおけるバイオメトリクスの利用などがあった。

**EU 全体でのサービスへの安全なアクセスを要求する EU 活動計画 2010[40]**

市民は、旅行や移動をするときにサービスへの簡単なアクセスを望んでいる。EU 諸国の政府は、行政機関のウェブサイトおよびサービスに対して各国の電子身分証明書を相互認定（mutual recognition）するための安全なシステムを確立してこのプロセスを促進することに合意した。この活動計画では 2010 年までの完全な導入を予測している。欧州委員会は、2007 年中に電子 ID 管理の共通の仕様を特定する一方で、大規模で国際的な実行者を支援し、また電子署名の規則を 2009 年に見直すことでこれの実現を支援する予定である。

**IDABC PKI**

IDA（BC）の PKI[41] は、以前の IDA プログラムのために開発された、限られた利用者グループ（CUG）

のための公開鍵基盤（PKI）である。このPKIは、PKIの確立と関連する証明書方針（CP）を通じて、EU加盟国全体の行政機関とIDA（BC）の部門ごとのさまざまなプロジェクトに取り組んでいる欧州の各機関の最終利用者間の安全なデータ通信を促進している。IDA（BC）のPKIは現在、部門ごとの限られた利用者グループの最終利用者に個人向けの証明書と職務上の証明書を提供する一方で、他方ではサーバーの証明書を提供している。

sTesta

sTESTAは、行政機関間の安全な欧州横断テレマティクス・サービス（secured Trans European Services for Telematics between Administrations）の略語であり、欧州連合の機密用の電気通信ネットワークである。sTESTAは、欧州と各国の行政機関間の安全な情報交換に対するニーズの高まりに応えている。sTESTAは、行政機関全体にわたる要件に専念しており、保証された性能水準とセキュリティを提供している。2006年10月、いくつかのデータ通信インフラストラクチャーをEU規模で置き換えるこのインフラストラクチャーの提供について、Equant/Hewlett Packardの合弁企業との2億1,000万ユーロの契約に欧州委員会が署名したと発表された。この契約により、欧州と各国の行政機関は、いくつかの政策分野内で安全かつ信頼できる方法でデータ交換を行うことができるようになる。

## 3.3　デジタル証明書サービスにおける相違点

EU25カ国の80%近くが2008年までに自国の市民および企業にデジタル証明書サービスを提供することを提案した。欧州諸国での電子署名の導入は欧州指令99/93/ECに基づいているものの、その導入では大きなばらつきが示されている。

EU加盟国が各国の多様な身分証明書を共有し、相互連結し、利用できるようにするには各国の法律を調整する必要があるため、eIDの全欧州相互運用性の段階でさらなる問題が発生している。データ保護、プライバシー、情報の責任、アクセス権限、認証の質といった問題は大いに議論を招く問題である。

［FIDIS-D36］の結果を考慮して以下に主な相違点を検討する。

**署名媒体**

多くの欧州諸国は、スマートカードとタイプIIIのカード・リーダーを必ずしも必要としない署名スキームを導入した。（オーストリアやフィンランドなど）。これらの事例では、代わりに携帯電話やUSBメモリー・スティックを利用して署名手続きを行うことができる（オーストリアなど）。［FIDIS-D36］はこれを手続き用署名ソリューションとして分類している。これらの署名ソリューションは身分証明書に限定されない。

ベルギーやドイツなどのその他の国は、大部分のe-ガバメント・プロセスの電子署名において署名カードとタイプIIIのカード・リーダーを使用する傾向がある。［FIDIS-D36］はこれを*カード利用型署名ソリューション*として分類している。

EU電子署名指令によれば、クオリファイド署名はSSCD（secure-signature-creation device.）によって作成しなければならない。手続き用署名ソリューションにはこの機能が欠けている。すなわちアドバンス署名のみ作成することができ、これはドイツでは手書きの署名の代わりとして認められていない。

**技術的な導入**

重要な側面として、欧州指令 99/93/EU に基づいているものの、欧州における電子署名の導入では大きなばらつきが示されているという点がある。これまでのところ、欧州電子署名指令で定義された電子署名の４つの水準（単純な署名、先進的な署名、クオリファイド署名、認定された署名）の１つに達するために、どの技術的な実行方法を利用できるかについては合意が形成されていない。

**行政手続**

どのような種類の行政手続に対してどの種類の署名が必要であるかについて合意が形成されていない（単純な署名、先進的な署名、クオリファイド署名、認定された署名)。これは国のサービスについてすら明確でないことが多く、国際的な活動についてはさらに明確になっていない。

**利用分野**

もう１つの大きな相違点は、相互運用性に関する欧州の eID プロジェクトの大部分における共同アプローチである。多くの税金、医療、社会保障およびその他の政府機関が身元確認と認証のために国の eID を利用できるようになる一方で、過半数の国は eID ソリューションを商業組織に開放する予定である。

**登録方法**

証明書を入手するには登録手続きを行わなければならない。登録手続きも欧州諸国で異なっており、したがって認知される信頼度が異なる可能性がある。登録モデルには次の例がある。ノルウェー：外部委託、エストニア：官民の提携、ベルギー：行政機関内で実施。

**PKI の運営**

身分証明書と特に関連するのは、PKI の運営方法について欧州諸国間で観察される相違点である。例えばオーストリアやベルギーでは登録と証明が（企業のサポートを受けて）行政機関で行われているのに対して、例えばドイツやスウェーデンでは民間企業によって行われている。これらの相違点に加えて、欧州にはルート CA が存在しない。その結果、電子署名は、現在のところ欧州において技術的な水準では相互運用可能ではない。

世界中の認証局の大規模なリストはPKI のページhttp://www.pki-page.org/で見ることができる。

**相互運用性**

認証およびデジタル署名の相互運用性に対するアプローチは､現在次の２つが認識されている。ブリッジ認証局と GUIDE プロジェクトである。

- **ヨーロピアン・ブリッジ認証局**[42]：ヨーロピアン・ブリッジ認証局（EB-CA）は、主にドイツとオーストリアの認証局（CA）の主導により、欧州、米国、アジアのメンバー（民間と公共の組織）に PKI と電子署名の相互運用性を提供しているヨーロピアンブリッジ認証局は、組織間のリンクの中心として機能しており、また新しい参加者の融合および EB-CA の運営に対して広範なサービスを提供している。個々の組織は、自組織の通信パートナーすべてとの契約条項の交渉にこれ以上時間を費やす必要がない。他のすべての参加者との安全な電子ビジネス・プロセスを実現するには、ヨーロピアン・ブリッジ認証局との間で１つだけ契約を結べば十分である。

・ **GUIDE**[43]は連携ネットワークによるID管理アプローチを利用している。GUIDEプロジェクトで考慮されている一般的なシナリオは、本人が外国で全欧州政府サービス（PEGS）にログオンする状態である。これらの場合、PEGSには外国の利用者（本人）を認証する手だてがない。認証するには、本人の母国のIDプロバイダー（IP）が必要である。このIPは一般に2つの基本的なサービスを提供する。すなわち認証サービスと属性プロバイダー・サービスである。

発行された証明書の数は依然として限られているようである。が、これまで9年間、PKIは一部の欧州諸国で身分証明書システムに利用されてきた。それにもかかわらず、大きなセキュリティ問題は発表されなかった。[FIDIS-D36]によれば、証明書の情報を経由して行われる取引にはすでに連結性があるため、PKIは現在最適な方法でプライバシーを導入していない。

## 3.4 利用拡大のための検討課題

革新の普及に関する理論は、技術革新の普及過程という著書において1962年にすでにEverett Rogersによって形成されていた。

経済理論においてRogers［Rogers03］は、普及を「革新が特定の経路で時間と共に社会システムの構成員間で伝達されるプロセス」また「伝達内容が新しい考えに関係している特別な形式の伝達」と定義している。

Rogersによれば、革新は「(革新を）採用する個人またはグループによって新しいと認められた考え、プラクティス、または物」と定義される。

### 3.4.1 革新の特性

認知された5つの**革新の特性**が［Rogers03］で定義されている。これらは革新の採用速度を決定する。

1. **相対的優位性**は、ある革新がそれに取って代わられる考えよりも優れていると見なされる度合いである。革新に客観的な優位性がある場合、これはそれほど重要ではないが、むしろ個人がその革新を優位であると見なす場合は重要となる。優位性は経済的用語を用いて計測することができるが、社会的名声、便利さ、満足度も重要な役割を果たす可能性がある。
2. **両立性**は、革新が既存の価値、過去の経験、および潜在的な採用者のニーズと一致していると見なされる度合いである。既存の価値と一致している革新は、社会システムの基準および価値との両立性のない革新よりも速やかに普及する。
3. **複雑性**は、革新の理解・利用が難しいと見なされる度合いである。より簡単に理解できる革新は、新しいスキルを身につけ理解を高めることを採用者に要求する革新よりも迅速に採用される。
4. **試験可能性**は、革新を限られた条件で実験できる度合いである。潜在的な採用者が革新に多大な投資を行う前に試験できる新しい考えは、より迅速に採用される。
5. **観察可能性**は、革新の結果が他者の目に見える度合いである。個人が革新の結果を観察するのが簡単であれば、採用される可能性はそれだけ高くなる。

### 3.4.2　普及の段階

Rogers は革新の**普及**の 5 段階モデルも提案した。

1. **知識**：革新の存在と機能について知る
2. **確信**：革新の価値を確信する
3. **決定**：革新の採用を決定する
4. **導入**：革新を利用する
5. **確認**：革新の最終的な受容（または拒絶）

### 3.4.3　革新の採用者

Rogers は、新しい革新や考えの**採用者**は、認識、関心、評価、試験、採用に基づいて、革新を採用する意欲と能力に従って分類することができると述べた。採用者のカテゴリー別にいくつかの特徴を示す。

1. **革新的採用者**（2.5%）：冒険的、高い教育、複数の情報源、リスクを負う強い傾向、勇敢な人たち、変革を牽引する。革新的採用者は非常に重要な伝達者である。
2. **初期採用者**（13.5%）：社会的リーダー、有名、高い教育、尊敬される人たち、オピニオン・リーダー、新しい考えを試すがそれを注意深く行う。
3. **初期多数採用者**（34%）：慎重、非公式の社会的接触が多い、思慮深い人たち、注意深いが平均的な人たちよりも迅速に変化を受け入れる。
4. **後期多数採用者**（34%）：懐疑的、因習的、社会経済的な地位が比較的低い、懐疑的な人たち、大部分の人たちが利用しているときにのみ新しい考えや製品を利用する。
5. **採用遅滞者**（16%）：近所の人や友人が主な情報源である、借金を恐れる、因習的な人たち、「古いやり方」を好む、新しい考えに対して批判的で、新しい考えが主流または伝統にすらなったときにのみそれを受け入れる。

### 3.4.4　利用者の経験のライフ・サイクル

革新の受容にとって非常に重要なものとして、個人の経験プロセスと認知された革新の優位性もある。個人ベースの「利用者の経験のライフ・サイクル」と「認知されたシステムの質」の関係が「e ユーザーの検討評価の枠組み」[45]［eUser］で説明されている。最終利用者によって認知される（認知されるべき）特性と質は何であるか、または何である可能性があるか、またライフ・サイクルの次の段階に進む上でそれらのうちのどれが重大な決定要因となるかを評価／予測することが重要である。

利用者の経験のライフ・サイクルに関連するシステムの特性の基本的なカテゴリーは次のとおりである。[eUser]。

- **認知度**はシステムが個人の非利用者に知られるようになる度合いを指している。システムの実際の場所は、その認知度にとって明らかに重要な要素である。また、宣伝戦略によってプロバイダーがこれを高めることも可能である。しかし製品は、宣伝が行われなかったとしてもある程度は認知される。サービスを思いがけず見つけることから認識が生まれる可能性がある。例えば、ネットサーフィン中にサービスを見つけるなどである。

- **認知された実用性および使いやすさ**は、個人の非利用者の視点から見たシステム実用性およびアクセスと利用のしやすさを指している。これらはおそらく、利用者の特定の目的およびニーズを満たす製品の妥当性ならびに個人の環境への適合性から生じるだろう。さらに、(サービスが提供される方法ではなく）サービス自体によってもたらされる時間と費用の節約といったさまざまな具体的な側面も含まれる。最後に、これにはセキュリティといったそれほど具体的ではない側面も含まれる可能性がある。こういった側面はすべて、認知されるリスクと利用者の期待といった形で検討される。
- **利用可能性／アプローチのしやすさ**は、あらゆるタイプの利用意志のある個人の利用者がシステムのエントリー・ポイントに到達できる度合いを指している。確かに、サービス／システムのアクセスのしやすさ（例えば、誰でも、いつでも、どこからでも）は利用可能性／アプローチのしやすさにとって重要な要素である。この段階では、システムに到達するための利用可能な「経路」に関して、障害を持った人たちなどの多様な利用者集団の特定のニーズと要件が考慮される。
- **相互作用の経験の質**は、個人の実際の利用者が認知する相互作用の質を含み、有益かつ質の高い結果を得るためにシステムを利用できる（すなわち、客観的な満足に結びつく）度合いを指している。一般に、アクセスのしやすさ、使いやすさ、システムのユーザー・インターフェースの美しさが利用感の質の主要な決定要因となる。
- **関係の維持可能性**は、利用者がシステムに関わっていないときに、個人のシステム利用者との良好な関係が効果的に育成・維持される（例えば、利用者に新しい機能、コンテンツの更新、状況の変化などを知らせることによって）度合いである。プロバイダーは、この関係の持続可能性を確保するための具体的な戦略を導入する必要があるだろう。例えば、システム・プロバイダーは、個人の利用者の目的とニーズに最大限に適合するためにより豊富なサービス・パックを提供することができる。

### 3.4.5　結論

欧州のセキュリティ調査の目標は、欧州の産業競争力を高める一方で市民のために欧州をより安全にすることである。欧州全域での協力および調整の努力により、EU は常に変化する世界でリスクをより良く理解しそれに対応することができる。

電子署名指令が採用されたことに伴い、この指令が電子署名市場の急速な成長の初期段階を迎えるのに貢献することが一部で期待されている。[EU-RepDirSig] によれば、電子署名市場は予想されたほどにはまだ発展していない。市場が直面する技術的な課題には PKI 技術の複雑さが含まれている。もう 1 つの障害は、国内および国際的なレベルでの技術的な相互運用性の欠如によってもたらされている。また、証明書が単一のアプリケーションにのみ利用でき、サービス・プロバイダーが例えば銀行部門によって開発されたソリューションなど、独自のサービスのためのソリューションを提供する方がよいとしているところでは、一連の電子署名アプリケーションが存在する。これによって相互運用可能なソリューションの開発プロセスが減速している。

この報告書では、e-ガバメント・サービスでの電子署名の利用はすでにある程度の規模に達しており、おそらく将来の重要な推進力となるだろうと述べられている。e ガバメントのアプリケ

ーションの戦略的な役割はEUi2010イニシアティブで認識されている。このイニシアティブは、民間部門および公共部門によるICTの配備および効率的な利用を促進するためのものである。

このような理由により、この調査ではeガバメントのアプリケーションに焦点を当てて欧州諸国における電子署名の利用を分析した。この分析に基づけば、電子署名はe-ガバメントですらまだ利用されていないと結論付けなければならない。普及計画（例えば、負担ゼロ、簡単な登録、さまざまな署名機器）によっても広範な受容には結びつかなかった。

上記の発展（の欠如）についての考察は、技術革新の普及に関する経済理論および署名利用に対するその理論の適用に基づいて行われている。

デジタル署名の取り組みが遅いその他の理由は、[EU-RepDirSig]に対するTeleTrust[49]の反応[TeleTrust2006]においても特定されている。TeleTrustは、「自然人に対する意思表示」および自然人の間の電子上の法的相互関係（エンド・ツー・エンド）において利用するための電子署名の一方的な制限について、電子署名に関するEU指令を批判している。構成要素の署名およびプロセスの伝達の確保は、おそらくPKI利用のためのより重要な応用分野となる。

欧州委員会は、将来に向けて、eIDイニシアティブに高い優先順位を与え、電子署名のサービスおよびアプリケーションの開発を今後も促進し、市場を監視していく。eガバメントの活動を通じたサポートを超えて、電子署名の相互運用性および国際的な利用に対して特別な重点が置かれる予定である。クオリファイド証明書による電子署名のためのあらゆる種類の技術の相互運用性および利用をEU市場で促進するために、さらなる標準化活動が行われる予定である。

[参考文献]


[CEN/ISSS2004] CEN/ISSS Workshop eAuthentication, CEN/ISSS WS/eAuthentication Vision Document, Towards an electronic ID for the European Citizen, a strategic vision, October 2004, http://europa.eu.int/idabc/servlets/Doc?id=19132

[Dumortier] J. Dumortier, S. Kelm, H. Nilsson, G. Skouma, P. Van Eecke. The Legal and Market Aspects of Electronic Signatures, Study for the European Commission - DG Information Society, October 2003

[EU-RepDirSig] Report from the Commission to the European Parliament and the Council, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, 15.3.2006,

[eUser] EU IST eUser Project, Country Briefs and Country Backgrounds, http://www.euser-eu.org/euser_countrybrief.asp?MenuID=112 and http://www.euser-eu.org/SearchSpecial.asp?IDFocus0=3&CountryID=*&MenuID=109

[FIDIS-D36] EU FIDIS Project, Deliverable D3.6: Study on ID Documents, 31 March 2006, http://www.fidis.net

[FIDIS-D41] EU FIDIS Project, Deliverable D4.1: Structured account of approaches on Interoperability, 12 July 2005, http://www.fidis.net

[Rogers03] Rogers, E. M., "Diffusion of Innovation", Fifth Edition, Free Press, 2003.

[TeleTrust2006] TeleTrusT Recommendations for Further Action in Accordance with the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, Dated 15 March 2006,http://www.teletrust.de/fileadmin/files/publikationen/Stellungnahmen/TTT-StN_EC-Bericht-zur-Anwendg-1999-93-EG_en.pdf

# 第4章　分析・提言

## 4.1　電子署名の概要

前章までで、海外での普及、利用状況について説明した。この節では、我が国での状況を踏まえた上で、電子署名の概要を以下の項目について説明する。

(1) 共通基盤としての電子署名と電子認証
(2) 電子署名と電子認証の使い分け
(3) 否認防止の要件
(4) 否認防止の実装と電子署名法
(4) 2001 年施行の電子署名
(5) 2005 年施行の e 文書法
(6) タイムスタンプ

### 4.1.1　共通基盤としての電子署名と電子認証

IT 技術が社会に深く浸透していく中、これからの IT 社会の共通基盤として、ネットワーク基盤と認証基盤（電子署名と電子認証の基盤）が必要だと言う意見が多数見受けられる。例えば、2006 年夏に発表された e-JAPAN 重点計画 2006 でも、ネットワークと認証に関わる多くの記述があり、重点分野の最初に取り上げられている医療福祉分野においても、以下のような記述がある。

> これらの課題のもと、医療・健康・介護・福祉分野の情報化に関する横断的なグランドデザインを速やかに策定した上で、まず医療の情報化の共通基盤である安全かつ安価な大容量ネットワークの構築や、医療機関・従事者・患者等の認証の仕組みの確立等に着実に取り組む。

ここでは、医療情報等を高度に利活用するため、共通基盤としてのネットワークと認証の必要性を説いている。こうしたことは、医療福祉分野だけに限らず様々な分野でその必要性が議論されている。しかし、安全なネットワークとそのネットワークを利用するための認証基盤の構築ということに関しては、まだ大きな課題がある。

様々な分野で必要とされている認証基盤であるが、現時点において一般的に認証基盤のひとつと認識されている公的個人認証サービスの普及と利用は低迷しており、電子署名も普及しているとは言いがたい状況にある。

認証基盤の必要性の理解や、実際の認証基盤の構築、更に認証基盤の有効な利用を促進する上において、電子署名、電子認証（e-Authentication）、認証（Certification）といった用語の共通認識と的確な理解が欠かせない。現在のところ、これらの用語等の共通認識、ないし共通の理解が得られないまま「基盤を作る」という行為がなされているようにも見受けられる。

一般論として、電子署名は、作成した電子文書等の責任の所在等を明確にするために必要になり、電子認証は、こうした文書等を適切な権限を持った人が利活用するために必要になる。電子

署名と電子認証を理解する上で認証（Authentication）と認証（Certification)、2つの「認証」という用語は、多くの混乱の元になっている。多くの法律用語において「認証」は、英語のCertification を意味する。それに対して、サーバ等による利用者の真正性の確認を意味することも認証（Authentication）と呼ばれる。Certification は、何らかの権威者が発行する証明書により、何らかのことを証明する。公としての行政機関は、従来からこのCertificationを数多く行っており、その証としての証明書の発行を行なってきた。そのため法制度等において「認証」は、Certificationを意味することが多い。そのためCertificationの電子化自体も多くの場合、電子署名の技術を用いて実現される。

認証基盤のキーワードとなる用語を簡単に説明したところで、e-JAPAN重点計画2006にある「医療機関・従事者・患者等の認証の仕組み」を意訳して説明してみる。

| |
|---|
| 医療機関、医療従事者、患者を認証（Certification）する。結果として、医療機関、医療従事者、患者に電子的な証明書（Certificate）を発行する。医師や、医療機関等は、発行された証明書により医療記録等に（署名用証明書を使った）署名を行うことによって、この医療記録等の改ざん防止、記録の責任の所在の明確化にする。また、医療機関、医療従事者、患者は、発行された証明書による（認証用証明書を使った）認証（Authentication）により、インターネット等のネットワーク環境においても厳格な本人確認を行ない、センシティブな個人情報である医療情報の共有化を図る。 |

以上のように、電子署名は、電子文書等の生成段階、または、組織から外部に出る時において必要になり、電子認証は、電子文書等の利活用時に必要になる。この様に電子署名と電子認証は、認証基盤が提供するべき両輪であるが、現在のところ、電子署名と電子認証の状況は、大きく異なる。

電子署名については、電子署名法が 2001 年に施行され法制度の面からも整備されてきた。この法律において、民間に証明書を発行する認証業務の認定制度が導入されているが、この認定基準が非常に厳しく、厳しいが故に電子署名が基盤として定着、また普及しない原因にもなっている。

一方、電子認証（e-Authentication）は、インターネットや企業内のイントラネットで当たり前に利用されているにもかかわらず、社会の共通基盤として整備するに至っていない。また、電子認証におけるセキュリティレベルの基準といったものも整備されていない状況にある。これは、ネットワークにおけるリモートの電子認証（リモート認証）に対応する概念は、従来からの法制度にはないことにも起因している。

電子署名と電子認証を社会の共通基盤として構築し機能させるためには、用語等の共通認識、ないし共通の理解を深めた上で、技術、法制度、ビジネスのバランスのよい実装が必要になる。

### 4.1.2　電子署名と電子認証の使い分け

低迷する電子政府における電子申請の普及策として、これまで電子申請文書に施していた電子署名を省略し、ユーザ ID／パスワードで代替するといったことが検討されている。しかし、元来、

ユーザ ID／パスワードは、電子署名を代替できるというものではなく、また逆に、ユーザ ID／パスワードで可能なことが、電子署名で可能な訳でもない。電子署名が省略可能な電子申請は、元々、電子署名が必要でないものに電子署名を強制していたとも言える。

IT 社会において安全、安心を提供する電子署名は、どう言った場面で必要なのかを理解しなければ、電子署名の普及にもつながらない。これには、電子署名と電子認証の性格の違いを正しく認識して、その適切な使い分けが検討される必要がある。

欧州の電子身分証 IC カードは、一般的に eID と呼ばれているが、この eID は、IAS すなわち Identification、Authentication と electronic Signature と言ったコンセプトで仕様が作成されている。eID は、電子認証（Authentication）、電子署名（electronic Signature）、に利用できるものとなっているが、その使い分けを明確にしている。例えば、ベルギーの eID である BELPIC（Belgian Electronic Identity Card）は、カードに格納される（否認防止の）署名用の証明書の発行は、18 歳以上としている。BELPIC は、2009 年までに 12 歳以上の全国民に配布される予定であるが、責任能力の観点から 18 歳以下の国民には、IAS の「S」を提供していない。しかし 18 歳以下でも認証（Authentication）は必要としている。このように、署名は「責任の所在」を示すため責任能力が必要になる。

PKI を利用した認証（Authentication）では、この認証のメカニズムとして署名機能が利用される。しかし、これは否認防止の署名ではないことに注意する必要がある。BELPIC の例では、カードに格納された 2 つのプライベート鍵（Private Key）による署名を使い分け、「クライアント認証」と「電子文書への電子署名」を行っている。カード内の（認証用の）プライベート鍵による署名操作は、強い認証（Strong Authentication）機能を実現する。そして、この強い認証を利用することによってサーバへ電子文書をセキュアに渡すことができ、サーバ側では認証のアクセスログを残すことができる。しかし、それだけでは、電子契約などで要求される「実印での捺印」の代わりにはならない。

認証（Authentication）のみのシステムでは、電子文書というトランザクションと利用者の紐付けの関係をログという形で残すことができるが、これは、サービス提供者と利用者が利害関係にある場合、否認防止にはならない。また、誤認証などで引き起こされるリスクは、サービス提供者がより多くのリスク負うことになる。

一方、署名を利用したシステムの場合、サービス提供者が、利用者の否認防止の署名を付した電子文書受け受け取り、この否認防止の署名付き電子文書を保存することで、サービス提供者は、利用者の否認を合理的に防止することができる。

PKI では、この署名に使われるプライベート鍵に対応する公開鍵を証明するための電子的な証明書である公開鍵証明書が使われるが、IC カードを用いる際には、カード保有者のプライベート鍵と共に、このカード保有者の公開鍵証明書（以後、証明書）が格納される。このカード保有者の証明書には、この証明書に対応したプライベート鍵の使用目的が記述されている。否認防止目的で使用される証明書には、証明書に含まれる証明書拡張フィールドの鍵使用目的（Key Usage）に、否認防止用を示すための non-repudiation（否認防止）bit が設定される。この non-repudiation（否認防止）bit が設定されることにより、この証明書とこの証明書に対応したプライベート鍵が否認防止のために使われることを明確にしている。

non-repudiation bit が設定された証明書に対応するプライベート鍵で（否認防止のための）署名を行う場合、そのアプリケーションは必ず署名者、すなわちカード保有者に否認防止の署名する文書を提示する必要がある。

否認防止の署名と認証（Authentication）では、想定される脅威も異なる。ネットワーク社会において、なりすましや盗聴といった脅威が語られるが、否認防止の署名に対する脅威にもうひとつ、「内容を理解せず（させずに）否認防止の署名を行う（行わせる）」という脅威がある。

PKI 機能を利用した認証においては、その認証プロセスの中で乱数などに署名させて、その署名結果を検証することで認証を行なう。認証のための署名においては、利用者は署名対象（認証プロトコル中の乱数など）を確認することはなく、また、認証のプログラムも利用者に意識させずに署名操作を行うことが多い。それに対して否認防止の署名では、署名者が必ず否認防止の署名の対象となる文書を確認する必要がある。

IC カードに複数の証明書とプライベート鍵を格納して、否認防止の署名や認証などの用途に応じて使い分ける場合、このプライベート鍵を保護するためのメカニズム、すなわちアクセス制御ルールの設定も異なっている。

BELPIC の場合、認証用のプライベート鍵による署名では、カード保有者がカードの PIN を入力し保有者認証を行なった以降は、カードに格納された認証用のプライベート鍵が認証要求の都度自動的に署名する。こうしたことは、シングルサインオンなど、利用者に利便性を提供することもできる。正当な利用者の認証（Authentication）時の認証用のプライベート鍵による署名は、利用者に不利益をもたらすことはない。認証（Authentication）するのはサービス提供者側であり、利用者が認証されるためにプライベート鍵を使うことにより責任が生じると言うことはない。

これに対して否認防止の署名のプライベート鍵では、1 回の否認防止の署名操作、つまりひとつの文書の否認防止の署名毎に「カード保有者の同意確認」（User Consent）のための PIN の入力が必要な仕様になっている。これはカード自体が、「内容を理解せずに否認防止の署名してしまうこと」を防ぐ仕組みを有していると言える。署名は、利用者が行うものであり、この署名には、利用者の責任が生じる。

日本の公的個人認証サービスでは、証明書の non-repudiation（否認防止）bit が設定された否認防止目的の証明書のみが発行されている。従って、公的個人認証サービスの発行する証明書を、電子認証（Authentication）としての利用には注意が必要である。否認防止目的の証明書を安易に責任の生じない認証（Authentication）として利用することは、責任が生じる署名に対する利用者のリテラシーの低下につながる。

### 4.1.3　否認防止の要件

ここでは、電子署名と関連が深い、否認防止の要件をニュージーランドの政府の「電子政府のための認証・認証のためのベストプラクティスの枠組み」を参考に説明する。「電子政府のための認証・認証のためのベストプラクティスの枠組み」では、オンライントランザクションの信用のレベルとして、「身元証明［EOI］強度」、「認証強度（Authentication Strength）」、「トランザクション強度」の 3 つが、リスクに応じた形で求められるとしている。否認防止の要件ないし、電子署名と関係が深い「トランザクション強度」は、以下のように説明されている。

トランザクション強度：
行政機関があるオンライントランザクションに求める信用レベル（level of confidence）のことである。例えば、低強度トランザクションは、電子メールによる受理確認通知だけ求めるかもしれない。高強度オンライントランザクションは、あるトランザクションの否認防止要因を多く必要とするかもしれない。例えば、誰が依頼をしたかという証拠、メッセージの送信、受信証明、メッセージが改ざんされていないことなどの証明、これらの安全に保存など。

以後は、行政サービスにおける電子申請、電子契約をイメージして説明する。認証（Authentication）は、ある電子契約文書等のトランザクションを処理している時、その当事者の片方の身元を明らかにすることに関与する。否認防止は、身元を明らかにするだけでなく、以下の確立にもかかわるより広い問題である。

(1) 電子契約文書などのトランザクションが発生したこと
(2) そのトランザクション内に含まれる電子申請文書の信憑性
(3) 電子契約文書が行政機関へ送信され、受け取られたこと
(4) その電子契約文書の長期にわたる信憑性と、その電子契約文書が改ざんされていないこと
(5) 当事者のどちらも上記の点を否認できないこと

紙の契約文書と電子契約文書の双方において、否認防止への要件をあげることができる。ある行政機関とある人が一枚の紙の上で契約を結ぶ時、両者とも手書きの署名等によって自分を証明する。

こうすることで、当事者の署名は契約書に関連づけられ、この契約を取り消すことはできなくなる。こうした証明が、否認防止には要求される。これと同じ結果が、同様のことが電子契約文書でも望まれる。否認防止がなければ、この行政機関と契約者は次のようなもっと大きいリスクを負わなければならない。

(1) 契約上の義務は、当事者のどちら側にも法的強制力がない
(2) 当事者のどちらによる過失責任も、その行政機関の自己責任となる
(3) 行政機関の能力と信用に対する世間の信用が下がる
(4) 間違った人にサービスが提供される

多くのオンライン・システムは、否認防止要件を満たすような堅牢性を考慮して設計されていない。特に裁判所が望む、例えば詐欺の告訴などに関係するような高レベルの証明が考慮されていない。

否認防止の実現、発生した全てのトランザクションで、当事者どちらかによる否認に対抗できる否認防止を実現するには、オフライン（紙の契約文書）とオンライン（電子契約文書）環境の両方で同じレベルの堅牢性が必要になる。

### 4.1.4　否認防止の実装と電子署名

引き続きニュージーランドの政府の「電子政府のための認証・認証のためのベストプラクティスの枠組み」を参考に行政サービスにおける電子申請、電子契約をイメージした否認防止の実装と電子署名の関係を説明する。

以下に否認防止の実装の要件を挙げる。

(1) トランザクションと申請者とが強く結びついていること
(2) トランザクションは偽造が困難であるべき
(3) トランザクションは変更不可能であるべき
(4) トランザクションは検証可能であるべき

上記のようなことを満足する高い否認防止の実装を、電子認証（Authentication）のみのシステムで実現することは、非常に難しい。または、実現には、非常にコストがかかる。

偽造キャッシュカード問題に端を発した預金者保護法では、キャッシュカードにおける誤認証の立証責任を、サービス提供者側の金融機関に負わせることになった。認証するにはサービス提供者側で、利用者（預金者）は認証される側になるが、認証される側には、認証自体に対する責任は基本的に生じない。

預金者保護法は、預金者を保護する一方、偽装犯罪も誘発している。これは、キャッシュカードによる認証の否認防止性が低いことにも関係している。キャッシュカードのシステムにおいても、監視カメラ等を導入し、この画像を長期に保存することにより否認防止性を高めることは可能かもしれない。しかし、これらを長期に渡り検証可能とするには、非常に重いシステムになることが容易に想像される。

一方、電子署名を利用した場合、トランザクションに利用者の電子署名を付すことにより、簡易なシステムでも高い否認防止性を容易に実現することができる。更に受けて側でタイムスタンプを施せば、更に否認防止性が高まると考えられる。

現在の我が国の電子政府における電子申請の全てが高い否認防止性が必要なものばかりでないことは明らかである。しかし、否認防止が高い認証基盤の確立、すなわち電子署名が基盤として確立することは、将来において、様々な分野において透明性と効率の双方を提供できる可能性があることに注意する必要がある。

否認防止は、電子政府というよりは、むしろ利益相反の関係が多い民間の間の取引で重要になると考えられる。国家としてのIT戦略等が目指すべき事は、電子政府における電子申請の利用率を上げることが最終目標ではなく、IT 技術を駆使した安全・安心で効率的な社会のはずであり、そのためには、透明性と効率の双方を提供できる可能性がある電子署名の基盤の確立は非常に重要な意味を持つ。

### 4.1.5　2001年施行の電子署名

我が国の電子署名法（正式名称「電子署名及び認証業務に関する法律」）は2001年4月に施行された。電子署名法に主な内容は、「電磁的記録の真正な成立の推定」と「認証業務に関する任意

的認定制度の導入」である。対象は、自然人の電子署名が対象であり、逆に、法人、サービスサーバ、エージェントなどの署名などは対象外となっている。また、電子証明書により可能な、電子認証（Authentication）や暗号化も範疇ではないと考えられる。

電子署名法の「電磁的記録の真正な成立の推定」と「認証業務に関する任意的認定制度の導入」により、電子署名が利用できる環境が整備された。一方、「自然人」にしか証明書が発行できないという制約や、非常に厳しい認定基準が電子署名の普及を阻害している可能性もある。

「認定認証業務」の非常に厳しい認定基準は、電子署名のビジネス領域をニッチなものにしている。また、電子証明書はコストが高いものというイメージを植えつけている。

非常に認定基準が厳しいことは、結果として、電子署名が高コストになる原因となっている。

「認定認証業務」は、その証明書発行などに対して非常に厳しい制約がありビジネスの範囲を大幅に制限しているという問題もある。これらの非常に厳しい制約等は、技術の不理解が融通の利かない制度を作っているようにも見える。

例えば、「認定認証業務」の「認定認証業務と他の業務との誤認を防止」による制約と「自然人にしか証明書が発行できない」という制約の結果、人とサービス（ないしサーバ）、サービスとサービスの信頼関係を築けず、むしろ、人とサービス、サービスとサービスの信頼関係を分断している。

「非常に認定基準が厳しい」と「非常に制約が厳しい」は、民間におけるビジネスの創造を阻害している可能性がある。現実に純粋に民間のサービス向けの認証局は少なく、また減少傾向にある。これは本来の制度の目的を満たしていない。また、普及しないのであれば「制度」自体の意味をなさないともいえる。

電子署名法は、その条文において「政府は、この法律の施行後五年を経過した場合において、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする」（附則　第三条）としている。一般論として、現在の電子署名法は、完璧を求めすぎているところがある。施行当初、目指していた社会との齟齬も多いと考えられるが、電子署名の普及という観点を中心とした改正の検討が望まれる。

### 4.1.6　2005 年施行の e 文書法

電子署名は、法制度との結びつきが強いが、電子署名が重要になるのは、重要文書の保存が義務付けられる文書などであるが、電子署名が適合する業務は、これまでの紙前提とした法制度に阻まれている面もある。そうした問題のひとつに、法律で保存が義務付けられている文書の扱いの問題がある。

e 文書法（民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律）は 2005 年 4 月に施行された。この e 文書法は、電子署名に大きな影響を与えつつある。電子署名は、重要な電子文書に大きな意味を持つわけであるが、重要文書の電子化がなされなければ、電子署名自体もあまり意味をなさないという問題がある。そして、電子文書化には、既存の法制度による制約があるが、こうした典型的な例に、紙文書による保存義務を定めた多数の法令等の存在があった。

e 文書法は、法令で保存が義務付けられている文書の電子保存を大幅に認めている。これまでは、IT 基盤を利活用しようにも、その対象となる文書が紙文書では利活用のやりようがなかった訳である。また、これまで、電子署名は、単純にコストと見なされていた面があるが、紙から電子分文書へ移行することによりコスト削減が可能ということも理解されつつある。2001 年の電子署名法の施行当時は、ネットワークを介しての利用、それが便利になるという側面が強調されていた。しかしｅ文書法により、電子署名は、ネットワークを使ったサービスというよりは、(保存が必要な) 紙から電子データの移行にとって重要という認識が生まれつつある。

e 文書法の波及効果は大きなものがある。電子文書の保存には電子署名が重要であることを再認識させられ、紙文書依存の業界が e-文書法で刺激されているが、こうした中、電子文書の管理、保存に対して、様々なソリューションの製品化やサービスの提供が開始されつつある。そして、その中で電子署名が有効に利用される兆しが見える。電子署名は、法制度との関係が深く、署名文書は、長期の保存が必要な場合が多い。e 文書法は、文書の保存に署名が有効な技術であることを示した。そして、文書の長期保存について、電子署名だけでなく、タイムスタンプ（時刻証明）の重要性が認識されつつあることも大きい。

電子署名が付けられた電子文書が、更に、標準化が進めば、特定のシステムの依存性を大いに減らすことができる。こうしたことは、特に長期にわたる電子文書の保存には、非常に重要になる。情報システムのライフサイクルは短く、文書の保存期間は長くなる傾向がある。こうしたことも含め、電子署名、タイムスタンプを使った安定した長期署名フォーマットの出現が求められているが、これに対応した重要な動きに ECOM の「ECOM 長期署名フォーマット」がある。

### 4.1.7　タイムスタンプ

2005 年に施行された通称ｅ文書法に関連した動向としてタイムスタンプサービスの普及がある。電子署名を行う文書は、基本的に保存されるべき文書であり、その時刻証明などは、重要な意味を持つ。タイムスタンプサービスの主な方式のうちのひとつは、時刻が何らかの形で保証されたサーバが行う電子署名によって実現される。つまりタイムスタンプ自体も電子署名により実現された技術と言える。

電子署名法においては、自然人によるいわゆる否認防止の署名がその範疇であり、こうしたサービスサーバ（タイムスタンプサービスサーバ）による署名は、電子署名法の対象外となっている。そうしたこともあり、タイムスタンプにより時刻証明の法的有効性は、一部の省令（財務省令など）で認められたに過ぎない。とはいえ「タイムビジネス信頼・安心認定制度」が発足するなど、電子文書のセキュリティを確保するために大きな前進があった。

「タイムビジネス信頼・安心認定制度」が適切に運用されれば、タイムスタンプによる時刻証明は、非常に信頼のおけるものになる。従来は、こうした時刻証明は、信頼のおける人による作業として行われてきた。具体的には、公証人による確定日付の付与といった形で行われてきた。タイムスタンプによる時刻証明は、こうした公証人による確定日付の付与にくらべ、非常に低コストで、かつ自動的に行うことが可能で、社会全体としての大きなコスト削減が可能にする。こうしたことからも、タイムスタンプによる時刻証明が広く法的根拠を持つことが検討されるべきであるが、欧州においても、電子署名法にタイムスタンプが取り入れられている事例が多く見ら

れる。

参考

e-JAPAN 重点計画 2006

Authentication for e-government Best Practice / Framework for Authentication
http://www.e.govt.nz/services/authentication/authentication-bpf/bpf.pdf

「電子署名法の在り方と電子文書長期保管に関する現状調査報告書」

IC・ID カードの相互運用可能性の向上に係る基礎調査
http://www.ipa.go.jp/security/fy18/reports/ICID/index.html

## 4.2 分析

この節では、前章までの海外事例等から「電子署名の普及」についての分析を行なう。

### 4.2.1 普及している地域

電子署名の普及の兆しが見える地域は、一般論として、規制モデルの電子署名法を制定している地域が多い。しかし、電子署名法の規制モデルだけが、電子署名の普及の決め手ではないことは明らかで、紙文書から、電子文書への移行を可能とする柔軟な法制度、IT 技術の利用と強力に進める施策などが重要な要素となっている。

具体的には、アジアにおいては、韓国とシンガポール、欧州においては、エストニアなどにおいて、電子署名が基盤として様々な分野において、幅広く利用される兆しが見える。

エストニアにおいては、電子署名に普及の要素として以下のことが言える。

- トップダウンな施策
- 既存の基盤によるしがらみがなく、基盤が作り易い
- 国がコンパクト
- 法制度が柔軟
- T 国家を目指している

シンガポールもエストニアと似た性格を持つと考えられる。電子署名の普及には、法制度との関係が重要であり、法制度による後押しも必要だと考えられる。

韓国の場合、「トップダウンな施策」「IT 国家を目指している」などの条件が当てはまるが、更に、様々な分野において、電子署名の利用を適度に義務付ける政策を進めている。

欧州の規制モデルの電子署名法を制定している国において、必ずしも電子署名は普及していな

い。電子署名は、ある程度普及し基盤となり初めてその威力を発揮することができる。人口の大きい国ほど、普及させ基盤となるまでの紆余曲折が大きいのかもしれない。

人口の少ないコンパクトに国においては、トップダウンな IT 政策と法制度の柔軟な対応により、電子署名を基盤として機能させることにより、地域の中での全体最適の実現に電子署名の有効に利用する傾向がある。

柔軟な法制度も、非常に重要な要素である。電子署名が有効に働く領域は、「責任の所在」の明確化が必要な、何らかの規制が重要な役割を果す分野である。こうした規制が重要な分野ほど、硬直化した従来の法制度が、電子化を遅らせる原因となっていると考えられる。従って法制度の柔軟な対応が可能な国や地域ほど、電子署名が普及する可能性が高いと考えられる。

### 4.2.2　普及している分野（普及しそうな）

電子署名は、ある程度普及し基盤となり初めてその威力を発揮することができると考えられる。それは、地域というより業界分野という単位が重要になる。従って、地域として普及していない場合においても、業界分野としての普及が進められている場合もある。

この場合も、電子署名が、何らかの法制度による規制との関係があるが多い。規制が多い分野の典型として、医療や、製薬などの分野がある。英米法体系で市場モデルの電子署名法を採用している米国においても、医療や、製薬といった分野においては、多くの規制が存在する。そのため、これらの分野においての IT 化、電子文書化においても、規制が存在する。その規制に、ある基準を満たした電子署名が利用への強制力が働く。電子署名の普及には、こうした適度な強制力が必要だと考えられる。

我が国においても、電子入札における電子署名が似た状況がある。入札を行なう行政が強制力を働かせた結果、電子入札が普及したと動じに電子署名も広く普及した。こうした業界には、電子入札の次に更に高い否認防止性が求まれる電子契約において、電子署名を容易に利用することができる。

### 4.2.3　業務別整備状況

(1) 金融分野

一般顧客向けのインターネット金融としては、オンラインバンキング、オンライントレード、保険契約の締結などのリテールサービスや、不動産における抵当、支払代行や支払保証といった場面で利用されている。いずれも顧客の重要情報を取り扱い、トラブル発生時のリスクも大きいことから、PKI の適用が有効である。クレジットカードやキャッシュカードに秘密鍵（ないしプライベート鍵）を入れるケースも増えてきている。

また、企業向けとしては、銀行や証券会社など金融機関間の決済に加えて、SCM (Supply Chain Management) や eMP (e-Marketplace) 等、エンドユーザには直接サービス提供をせず、電子取引基盤を提供するサービスプロバイダが金融機能を提供する形態もある。

但し、金融機関による認証基盤の国際標準を目指した Identrus の様に多数の金融機関がメンバーとなり、複数の金融機関を接続した大規模な PKI 構築事例は見当たらない。

(2) 医療分野

医療分野では、カルテや診療録等の重要な個人情報の電子化が進みつつあり、その保存と検索、施設間連携などにおけるネットワークを介しての伝送・交換等において情報のセキュリティ確保や本人確認及びその資格と属性認証等がますます重要になっている。

個人向けでは、電子カルテや医療費請求・支払などが挙げられるが、健康保険証（健康保険 IC カード）に PKI を適用し、身分証明として活用する事例が増加すると考えられる。医師に対しては診断記録の否認防止、医師の身分証明として利用が行われると考えられる。

病院、診療所等の医療機関、医薬品企業等では、レントゲンや診断映像等の医療情報、カルテ等、個人の重要情報を取り扱う医療データ交換や、膨大な書類や投資を伴う医薬品調達などに、PKI が活用されると考えられる。

このように医療分野では、PKI の活用が最も期待される分野の 1 つと思われる。

(3) 政府分野（G2B、G2C）

EU では「電子署名に関する EU 指令」が実質的に PKI を推奨しており、さらに EU 以外の国でも電子署名法の整備が進められていることから、PKI 導入は更に拡大されることと思われる。

政府部門にとっての顧客である住民・企業向けでは、申請（住民票、企業登記、免許や認可の申請)、納税・税金還付（確定申告、決算申告）など、電子政府・電子行政が実現する多くのアプリケーションに PKI が用いられている。住民 ID カードなどの活用例も多い。

日本で偽装され問題となった建築確認申請では、シンガポールでは既に PKI を利用した電子建築確認申請導入しており、先進的な運用が開始されている。

(4) B2B、B2R

オンラインでのカタログ購入、eMP、e-Logistics、SCM、貿易金融 EDI、電子調達などが挙げられる。

しかしながら、実現させるには、ユーザのシステム間での相互運用が確立しなくてはならず、これには 2 つの課題がある。1 点目は PKI レベルでの相互運用性であるが、認証局間での相互認証が必要となり、アプリケーションに左右されない運用をしなくてはならない事、2 点目は業務プロセスの標準化を行うことである。

現在の PKI を適用する動きでは、電子部品業界向けの EDI である RosettaNet の一部、北米でバイオ製薬業界主導に作られた SAFE の様に、PKI を適用する動きもあることから、活用する機会が徐々に広がる可能性もある。

(5) B2C

オンラインショッピングや電子オークションだけではなく、ソフトウェアやコンテンツの商取引である、映画・音楽・ゲームなどの配信にも用いられることが期待されている。しかしながら現在のところ、導入に向けた動きは殆どみられない。PKI の導入及び運用負担が軽減されず、一般消費者を対象とした PKI 関連のコンプライアンスがないこと、また、一般消費者のセキュリティに対する認識が PKI を利用する段階まで達していないことが要因となっている。

表 1.4-1 PKI を活用した業務別アプリケーションの例

| | アプリケーションの利用者（エンドユーザ） | |
|---|---|---|
| | 一般顧客 | 企業 |
| 金融 | ・オンラインバンキング、トレード、保険<br>・不動産取引 | ・銀行間決済／取引<br>・金融サービス（SCM/eMP への金融機能提供など） |
| 医療 | ・電子カルテ<br>・医療費請求・支払 | ・医薬品調達・医療データ交換 |
| 政府（G2B、G2C） | ・電子申請<br>・電子納税・還付 | ・電子調達・電子入札 |
| 企業間商取引（B2B） | ・オンライン購入<br>・eMP<br>・e-Logistics | ・SCM<br>・貿易金融 EDI<br>・電子調達<br>・機密情報交換（研究開発、提携／M&A 検討など） |
| 企業間商取引（B2C） | ・オンライン購入<br>・電子オークション<br>・コンテンツ配信 | |

●参考

（財）日本情報処理開発協会 IPA 2003 年 3 月 PKI 関連サービスビジネスの動向と今後の展望に関する調査報告書

（財）日本情報処理開発協会 IPA 2004 年 3 月 PKI 利用モデルの現状と相互利用に関する調査報告書

## 4.3 電子署名の提言

### 4.3.1 提言について

電子署名の提言を検討するにあたり、なぜ電子署名が重要かを説明する必要がある。本質的には、電子署名を普及させること自体は目的ではないかもしれない。電子署名は手段であるが、電子署名を普及させることにより、IT を駆使した「安全、安心で効率的な社会」、こうしたことを実現することが目的となる。ここで、電子署名は、必ずしも直接的に「便利」を提供するものではないことに注意すべきである。この「直接的に「便利」を提供するものではない」ことが、説明を難しくしている。電子署名は、むしろ「規制」的な意味が含まれる。

電子署名の必要性で、なりすまし、改ざん防止を説明されることが多いが、むしろ「責任の所在」を明確にするということが強調されるべきである。「責任の所在」を明確にするということは、サービスを受ける側（サービスの利用者）から自発的に行なわれることは、むしろ少ない。また組織内のような、ひとつの閉じた信頼の中において署名という要求は少ない。しかし、様々な連携、組織を超えた全体最適を実現する上で、各関与者の「責任の所在」の明確化が必要になる。

現時点において、組織を超えた全体最適を実現している分野は少なく、これをイメージすることは難しいところがある。

電子署名の普及は、結局のところ、「様々な連携、組織を超えた全体最適」を推進すると信じるが、電子署名の普及しないことは、「様々な連携、組織を超えた全体最適」の推進を阻害する、もしくは、社会システム全体を脆弱なものにしてしまう可能性があることが理解されるべきである。

以上の観点も踏まえ、本節では以下の項目の提言を行なう。

(1) 電子署名法の改正
(2) 自然人以外の署名の扱い
(3) 認定認証業務の制約の緩和
(4) タイムスタンプの法制化
(5) 適度な強制力とインセンティブの検討
(6) 保証クラスの明確化
(7) 電子政府における電子署名の普及
(8) 相互運用性確保のための施策

### 4.3.2 電子署名法の改正

2001 年 4 月 1 日に施行された電子署名法は、既に施行後 5 年を経過している。この電子署名法は、条文の中で、「政府は、この法律の施行後五年を経過した場合において、この法律の施行の状況について検討を加え、その結果に基づいて必要な措置を講ずるものとする（附則　第三条)」とされている。ドッグイヤーとも言われる急速に発展する IT 技術の世界において、5 年は非常に長い。IT 技術、IT 施策で大きく環境が変化しているが、電子署名法をはじめとする現行の IT 技術の関連した法制度は、こうした環境の変化に追随できていない側面がある。

また、5 年前、電子署名法などが当初目指していた IT 社会との齟齬は、既に数多く存在すると考えられる。IT 社会が健全に発展するために、大きな役割を果たすと考えられる電子署名の普及は大きな意味を持つ。こうしたことからも、普及という観点から電子署名法が見直されるべきである。ユビキタスネットワーク社会においては、認証を要するデバイスが人口よりもはるかに多く、またサーバによる署名が、人間が行うよりもはるかに多く想定される。このような今後の IT 社会に対する法制度は、これまでの法制度の延長上にある「電子署名法」などの枠組みだけではカバーできず、新たな枠組みも検討される必要があると考えられる。

現状は、電子署名法が機能していない故に、軽微な改正では根本的な問題の解決にならず、先送りされているようにも見受けられる。問題の先送りは、電子署名の基盤の整備を遅らせる結果となり、しいては、本来、電子署名の基盤の上に実装されるべき様々なアプリケーションが標準化されることなくバラバラに実装されていくことになる。こうした事態は避けられなければならない。

### 4.3.3　自然人以外の署名の扱い

電子署名法の改正の大きな論点のひとつに、証明書の発行対象の問題がある。現在の電子署名法では人（自然人）以外に対して発行した証明書に対して、法的根拠を与えることが出来ない。実体的に利用されている証明書に関して法的な効果を与えることが出来ないため、多くの利用用途に対して安全性を担保できないという問題がある。

具体的には以下のような発行対象が考えられる。

| 発行対象 | その問題 |
|---|---|
| 法人 | B2B 取引のオンライン受発注で利用されている証明書としては、自然人ではなく法人の証明書が必要だと言う議論がある。こうした場合、法人代表者や担当者が交代しても証明書の更新が不要になる。 |
| タイムスタンプ | TSA（Time-Stamping Authority）の証明書に関しては法的背景がない |
| サーバ証明書 | サーバ証明書は、インターネット上の商取引で最も有効に利用されているが、実質的には Web Trust for CA に依拠している |
| Machine to Machine | 今後最も需要が増加すると思われるユビキタス環境におけるデバイス等の認証(certification)については、電子署名法の効力が及ばない(Ipv6、医療機器、著作権管理、etc) |

以上の「発行対象」全てが電子署名法の範疇ではないかもしれないが、自然人以外の署名の効力について検討されるべきである。

### 4.3.4　認定認証業務の制約の緩和

認定認証局は、そのサービスにおいて多くの制約がある。現状、電子署名法が対象としている証明書の利用用途は「署名」のみであるが、実際には「認証」の用途で多くの証明書が利用されている。

- サーバ／クライアント間での認証
- 各種サービスへのログイン認証
- Machine to Machine 通信

これらの用途に対しては全く制度の整備がなされていないし、また認定認証局にとっては、これらの証明書が発行できないことがビジネス上の制約になっている。例えば、以下のようことに利用できない。

- 企業内システムへのログイン認証
- UPKI（大学 PKI）におけるクライアント認証
- 医療情報の開示制御における本人認証　等

認定認証局は、認証局に発行する CA 証明書に関しても制約がある。電子署名法における認定認証局には、誤認防止条項のため実質的に GPKI-BCA との相互認証（Cross Certification）しか許されていない。また、GPKI-BCA は、民間同士の利用を禁止している。このため認定認証局の信頼関係は孤立しており、結果として、利用者は、利用目的毎に証明書を持たなければならない等利便性が低下している（認定認証局同士の 1 対 1 での相互認証は可能であるが、非効率である)。認定認証局に対する制約は、そのまま、電子署名に対するビジネスの制約となっており、電子署名の普及を阻害している。以上のことから、認定認証業務の制約を緩和が検討されるべきである。

### 4.3.5　タイムスタンプの法制化

タイムスタンプは、自然人以外の署名、すなわちサービスによる署名のひとつとも捉えられる。タイムスタンプは、公証人による確定日付の付与と同様の機能を、IT 技術を駆使して実現したものとも言えるが、その効力が電子署名のように法制化され広く認められている訳ではない。タイムスタンプによる時刻証明は、公証人による確定日付の付与にくらべ、非常に低コストで、かつ自動的に行うことが可能なので、社会全体としての大きなコスト削減が可能になる。紙文書から電子文書への移行の中で、電子署名とタイムスタンプが適切に利用されるべきである。実際、欧州の電子署名が普及の兆しが見える国の場合、電子署名とタイムスタンプがセットになって法制度が作られている場合が多い。以上のことから、タイムスタンプによる時刻証明が広く法的根拠を持つことが検討されるべきである。

### 4.3.6　適度な強制力とインセンティブの検討

これまでの法制度で影響力が大きかったもの、例えば「個人情報保護法」これは、法律の施行により強制力が働いたため非常に影響力が大きかった。逆に「電子署名法」「e 文書法」は、電子署名や、電子文書での保存を強制したものではない。現状維持でよいとすると、これらは利用されない。普及を促がすためには、何らかの強制力やインセンティブが検討されるべきである。適度な強制力により、電子署名が社会基盤として成立すれば、その電子署名の基盤の上で様々な展開が可能になる。実際、韓国における電子署名は、適度な強制力により、実際に機能する社会基盤となりつつある。そして、様々な分野で電子署名が利用されつつある。

我が国においても、電子入札は同様のことが言える。電子入札は、入札を行なう行政が強制力を働かせた結果、電子入札が普及したと同時に電子署名も広く普及した。こうした業界には、電子入札の次に更に高い否認防止性が求まれる電子契約において、電子署名を容易に利用することができる。同様なことは、社会全体にも言える。電子署名は、利用者に広く普及して初めて基盤としての役割を果す。電子署名が基盤として機能することは、社会全体に対しての透明性と効率の双方を提供することになる。

以上のことから、規制が必要な業界の IT 化において、「規制モデル」としての認定認証局の証明書を利用する適度な強制力とインセンティブが検討されるべきである。

### 4.3.7　保証クラスの明確化

電子署名法では、認定認証業務認定といわれる認定制度を定めているが、この認定認証業務認

定では、認証局に対する認定の基準を定めている。内容としては認証局の設備や運用に関するものであり、特に、証明書を発行する本人身元確認と、証明書と鍵を本人に結びつける作業に関して非常に高いハードルを課している。

一般的にセキュリティの強度とコストとはトレードオフの関係にあり、さらに利用者の利便性ともトレードオフの関係にあることが多い。電子署名法の認定制度は、非常に高い基準のみが存在しており、結果として非常にコストのかかる構造になっている。

現実世界の印鑑は、大きく実印、銀行印、三文判と 3 種類があり、利用用途に応じて使い

分けを行っている。一方、現状の電子署名法では、最高のセキュリティレベルのもの（実印相当）のみしか定義されておらず、実際の印鑑において利用頻度の高い銀行印、三文判相当の証明書は定義されていない。最高のセキュリティレベルの証明書の発行は非常にコストを要し、結果として証明書の単価が下がらない。実際に銀行の取引であれば、銀行での本人確認で銀行用の証明書を出して良いはずである。

2007 年 1 月 4 日から、10 万円を超える 10 万円超の現金を振り込む際、身分証明証の提示による本人確認が必要となった。これは、金融機関の本人確認法の改正に基づく処置である。本人確認法は、2003 年に施行されているが、金融機関にとって、この「本人確認法」は非常に大きな意味を持つようになってきた。各金融機関は、「本人確認法」の遵守を義務付けられるが、これは規制だと考えられる。

電子署名法の認定認証業務認定では、「本人身元確認」について非常に厳しい基準が設けられている。この「本人身元確認」は、金融機関に対する「本人確認法」よりも厳しい。それにも関わらず、電子署名法の証明書を義務付けられている民間に対する規制は、ほとんど存在しない。電子署名法が要求する基準は、金融機関に要求される「本人確認」よりも厳しいことが、電子署名の応用分野をニッチなものにしている。

以上のことから、電子署名法においても、その利用のリスクに応じたセキュリティレベルの電子署名の基準が作成されるべきであるが、特に今後、社会的需要が大きい領域の基準作りに重きを置くことが検討されるべきである。

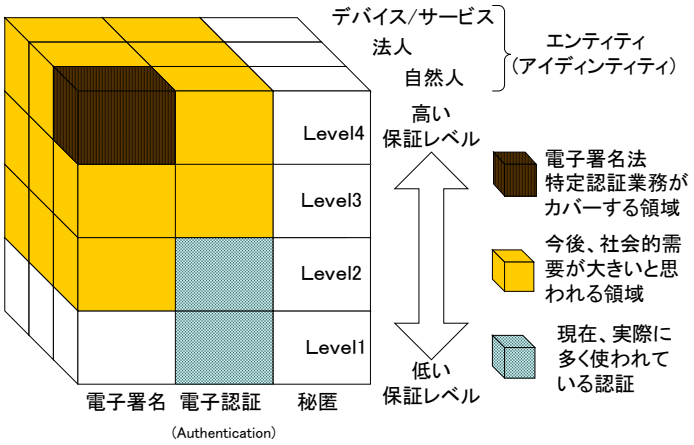



図 1.4-1 トラストキューブ

### 4.3.8　電子政府における電子署名の普及

電子政府では、電子申請、電子入札、電子申告などにおいて、電子署名が利用されている。しかし、強制力の働く電子入札以外は、利用率が極端に低いのが現状である。

電子申請、電子申告が普及していない理由は、様々な理由が考えられているが、少なくとも電子申請などを可能にすることが目標になっていたが、これらが利用されることに関しては目標となっていなかった。「IT 新改革戦略」では、利用率が目標として上げられており、そのための施策の検討が促されている。

その中で、電子署名の省略も検討されている。特に重要なのは、税理士、社会保険労務士などによる代理申請の場合、本人の署名が省略されると言うものである。この場合、本人の署名が省略されるが、逆に、税理士、社会保険労務士などの代理人が施す電子署名は、代理人としての責任を表す重要なものになるとも言える。

現在の我が国における電子申請が、高い否認防止性が必要なものばかりでないことは明らかである。しかし、否認防止が高い認証基盤の確立は、将来において、様々な分野において透明性と効率の双方を提供することにもつながることも考慮されるべきである。利益相反の関係が多い民間の間の取引でこそ電子署名が重要になると考えられるが、電子政府は、電子署名の普及も後押しすべきである。国家としての IT 戦略等が目指すべき事として、電子申請の普及だけではなく、電子署名の普及策が検討されるべきである。

### 4.3.9　相互運用性確保のための施策

電子署名の普及には、電子署名に関連した標準化と、その相互運用性の確保が欠かせない。電子署名に関連した標準化としては、署名に利用される証明書のプロファイルの標準化の他、IC カードなどの署名デバイス、署名検証、それから、署名フォーマット、署名対象の標準化などが考えられる。電子署名で重要なことは、その署名対象自体の標準化も欠かせない。標準化されたデータフォーマットを使い電子署名が施されたデータは、特定のシステムに依存しない独立したデータとしての普遍性を持つことになる。

電子署名法の施行依頼、こうした相互運用性確保のための施策は、ほとんど見られない。そのため、利用者は、利用目的毎に証明書を持たなければならない等利便性が低下している。利用促進という観点も含め相互運用性確保のための施策が検討されるべきである。

# 第２部　金融業界（国内）における電子署名利用調査

# まえがき

昨今のインターネット環境の普及と電子商取引の進展は目覚しいものがある。それに伴い、ネット利用や電子商取引における被害や不正行為も増大している。一方、なりすましや改ざんなどの電子社会でのリスクに対しては、電子署名技術が最も有効な対抗手段であるが、現状さほど普及しているとはいえない状況にある。

昨年度 ECOM では、電子署名利用上の問題点について幅広い視点から抽出し、普及を阻害する要因を整理した。その結果、主要問題を、

- 導入コストに対する投資効果が見えず、導入判断がしづらい
- 電子署名法に基づく運用は厳格で大変である
- PKI（電子署名）利用のガイドラインがない

の 3 つに絞込み、それに対する対策として業務分野に即した電子署名利用のガイドラインとベストプラクティスを示すことが有効と考えた。

今年度、署名普及対策としてのガイドライン作成につなげるため、特定の業界毎のビジネスでの利用状況を調査し､署名利用のモデルケースを検討することとした｡対象業界の候補としては、署名が有用になりそうな、医療業界、建築業界などが考えられたが、最終的に、金融業界を対象として調査することとした。金融業界は、経済面で産業界のハブであるとともに、一般人にとっても生活上係わりの深い業界であり、そこでの署名利用促進は社会全体への波及効果も大きいと考えられるためである。なお、医療や建築の分野では PKI 導入の検討も始まっている。

以下では、金融業界における署名利用の現状（1 章)、その調査結果の分析（2 章）とモデルの提案（3 章）について述べる。

# 第1章　現状調査

金融業界における電子署名利用の現状について、FISC（金融情報システムセンター：The Center for Finalcial Industory Information Systems）の協力を得て情報収集するとともに、いくつかの金融業界関連企業にヒアリングを行った。FISC では、電子署名を含む PKI の利用動向について 2006 年 3 月 FISC レポート[1]（ECOM 講演版を付録 3 に添付）としてまとめており、次節にその要約を示す。

ヒアリングは、当該企業における電子署名の利用状況から、今後の署名利用に関するスタンス、さらには公的な制度などへの要望など、多岐にわたる質問を用意して行った。結果については、企業名が特定できないよう、マージして述べる。

## 1.1　金融業界の PKI 利用動向（FISC レポートより）

従来、金融機関における電子取引の代表は ATM であったが、キャッシュカードとパスワードという、所持認証と記憶認証による電子認証が利用されてきた。その後、インターネットを利用した電子取引が開始されたが、インターネットバンキングを例にとると SECE（Secure Electronic Commerce Environment）と呼ばれるプロトコルを用いた公開鍵暗号基盤による電子証明書方式を採用して、サービスを提供する金融機関が数多く存在していた。しかし、専用ソフトウェアでサービスを行う形態であったため、利用者に相応の知識とパソコンへの導入が必要であり、その困難さと使い勝手の悪さから利用者数は伸び悩んだ。

そこで金融機関は、128 ビット SSL 暗号通信上で ID とパスワードを使って本人認証を行う方式の検討を行い、十分にセキュリティを確保できると判断して、この方式に順次切替えていった。この方式の導入により国内のインターネットバンキングは飛躍的に増加するようになった。

しかし、昨今、金融機関が提供するサービスに関して、スパイウエアやフィッシングメールなどを悪用し詐欺行為を働く犯罪が顕在化してきた。このため、電子認証等による対策の強化が急務となった。

法人向けサービスにおいては、三井住友銀行、東京スター銀行、愛知銀行等で PKI が利用されており、顧客の反応はおおむね良好で、特に複数の電子認証技術を組み合わせた、法人向けの複数のサービスを対象にした共通認証基盤を提供する三井住友銀行の取り組みが注目されている。一方、個人向けに導入している新銀行東京、野村證券では、法人向けにより先行して取り組んできたが、法人対象と比較して顧客の反応は現状でもまだ鈍いと評価されている。

## 1.2　金融業界へのヒアリング

### 1.2.1　ヒアリング項目

ECOM 電子署名・認証 WG では、国内での金融業界における電子署名利用状況の調査のために、いくつかの金融機関、リース会社等関連する企業等から直接、電子署名の利用の現状と取り組みについてヒアリングを実施した。本項では、まず、ヒアリングした項目を示す。

(1) 電子署名の利用状況について

①電子署名を利用するサービスを提供しているか、あるいは他社サービスを利用しているか。（例えば、電子契約、ネットバンキングなど）

②電子署名を利用する社内システムを持っているか。（例えば、電子決裁、文書管理など）

③上記①②で、利用している場合、電子証明書の発行や管理はどのように運用しているか（自社で認証局を運用、他社認証局を利用、など）。また、電子署名導入・利用にあたっての問題点、苦労したことはあるか。

④電子契約に関する取り組みと状況について。

⑤電子署名に対する行員や顧客の理解度や信頼度はどの程度か。

(2) 電子署名のニーズについて

①御社の提供サービスや社内業務で、電子署名が必要あるいは利用が望ましいシーン（利用者の厳格な認証、処理結果の証拠保存・事後否認防止、責任の明示など）はあるか。

②上記①でニーズはあるが未導入の場合、導入のネックになっていることは何か。あるいは、こうなっていれば導入するといったような条件はあるか。

③フィッシング対策としての発信メールへの署名、SOX 法対応としての署名利用などについて、どのように考えるか。

④電子署名と共に電子的な印影を表示するシステムもあるが、利用者や行員にとって印影が表示されることで理解度や信頼度は変わると思うか。リアルの判子と電子署名を組み合わせた利用方法を進めてはどうか。

(3) 電子署名の環境・インフラについて

①一企業にとじないで業界として、あるいは他業界と連携して電子署名を利用するシーンやニーズはあると考えるか。

②上記ニーズがある場合、その実現のためのネックになること、あるいは実現の条件は何か。（例えば、共通のプロファイル、ガイドラインなど）

③電子署名の社会インフラが整備されていれば、サービスや業務にも有用と考えられるか。例えば、公的個人認証が普及すれば活用することは考えられるか。（例えば、架空口座の撲滅、死亡した人の口座の凍結、相続トラブルの軽減等）

④金融機関で使用する証明書は、パブリックなものであるべきと考えるか。

（パブリックとは Windows の証明書ストアに認証局の証明書が格納されているもの）

(4) その他

①電子署名や PKI の技術、製品、インフラについて、現状の課題、今後の対応、今後の展開への期待などあるか。

②特定認証局の認定を取得することについての考え方。

③電子契約と電子署名の仕様及び課題。

### 1.2.2　ヒアリング結果

ECOM 電子署名・認証 WG にて実施した電子署名の利用の現状と取り組みについてヒアリングした結果について纏める。

(1) 電子署名の利用状況について

①電子署名を利用するサービスを提供しているか、あるいは他社サービスを利用しているか。（例えば、電子契約、ネットバンキングなど）

1) ビジネス用途

・ネットバンキングのログイン認証に利用している。

・国内取引の Web サイト、及び外為利用の Web サイトで、ID/PW から、証明書を利用して PKI を必須に変更した例がある（2 例）。

・電子契約や融資申し込みで電子署名利用（BtoB）。

・銀行自身が、第三者機関として証明書発行を実施。

・法人向けインターネットバンキングでの利用（他社 CA による SSL 認証）。

2) 個人（リテール）用途

・SSL のサーバ証明書程度の利用に限定。

・個人向けではそもそも署名のニーズが少なく、本人確認の認証のニーズはあるが、PKI でなくてもよく、ワンタイムパスワードや乱数表、携帯端末 ID 等で十分である。

②電子署名を利用する社内システムを持っているか。（例えば、電子決裁、文書管理など）

・行内で 10 以上のアプリで利用している。

・行員のログイン認証（USB トークンに入れてリモートアクセスでのログイン認証）。

・一部外部業者（IT ベンダー）のリモートアクセスにも使わせて、対価を取っている。

③上記①②で、利用している場合、電子証明書の発行や管理はどのように運用しているか。（自社で認証局を運用、他社認証局を利用）また、電子署名導入・利用にあたっての問題点、苦労したことなどはあるか。

・証明書はベリサインの ASP を利用している。

・他社 CA を利用している。（認証局名未開示）

・自社認証局ではなく、アウトソースしているため、あまり問題は出ていない。

・マス向け（インターネットバンキング）は他社 CA 利用で数十万枚発行の例あり。

・B2B 用と行内用は共通の行内セキュリティインフラを構築して利用。当初全て対面審査で発行していたが、運用が大変なのでレベル分けした。

④電子契約に関する取り組みと状況について。

・企業間電子契約と電子原本保管を提供した例あり。

・認証と署名は同一の証明書を利用している例あり。署名のニーズが少ないため。

・認証のレベルとして、高レベル PKI では、署名法を意識して対面で本人確認して証明書を発行するモデルで、本人も銀行も発行の負担が大きくなる。一方、低レベル PKI として、

企業の代表が申し込み一括して発行し、企業側で配付する方法もある。予め、署名法が適用されない可能性があると通告して利用してもらう。

・法人向け、ビジネス用途のインターネットバンキング（BtoB）では、100%PKI が利用されている（グループ内企業が多い。）

・リース業界の契約は、1 社で取引先数 10 万社、数 10 万通の契約を取り交わしている例もあるが、リース契約は一件あたり 3～5 年程度で、リース業界の取引先は中小企業が多く、一式で契約書一通の契約が多い。このため、1 社あたり数年に 1 通程度となるため、さほど大きな数の取引にならず、電子証明書の導入のニーズが低い。

⑤電子署名に対する行員や顧客の理解度や信頼度はどの程度か。

・一般の個人（行員含む）の理解は不十分である。サービスで使用している人はある程度理解しているかもしれない。

・技術の説明よりも、署名することの意味（行為責任）を理解させるべき。

(2) 電子署名のニーズについて

①御社の提供サービスや社内業務で、電子署名が必要あるいは利用が望ましいシーン（利用者の厳格な認証、処理結果の証拠保存・事後否認防止、責任の明示など）はあるか。

・オンライン申し込み等では、電子署名が必要と考えるが、実際のニーズが見えてきていない

・セキュリティ上、ログイン認証には意味があると考える

②上記①でニーズはあるが未導入の場合、導入のネックになっていることは何か。あるいは、こうなっていれば導入するといったような条件はあるか。

・書面の電子化においては、行内調整事項が多く、現時点では最初からオンラインで解決しているものが少ない。

・電子契約を計画中であるが、行内に認証局を構築するほどのニーズは無い。

・電子署名に対する理解度という観点では発想が逆。そもそも、PKI や署名を理解させる必要は無く、どういう効果があるというサービスの価値を示すべきであり、その中で電子署名を使うことを説明していくべき。

・PKI はインフラ（マス向け）とビジネス（クローズ）では用途が違うはずだが混在してしまっている。インフラとしては認証用途が主で、署名はビジネス用途。

・電子署名法では個人を認証するため、電子証明書の Subject には、法人間で利用する場合でも、個人名が格納されている。商業登記認証局では、会社代表者名が利用されるが、電子入札用などでは、代表者の委任を受けた者の名前が使われる。しかし、この場合、委任を受けた者の「役職名」が格納されるケースは殆どないが、現実の契約では、契約者の役職が部長以上でないといけないなど、役職に対する制約が多い場合があり、旨く利用しきれない場合が多い。

③フィッシング対策としての発信メールへの署名、SOX 法対応としての署名利用などについて、どのように考えるか。

・メールへの署名については、他行も実施しているので、実施する可能性がある。
・メール署名は解決すべき問題の一部にすぎない。署名があるだけでは安全とは言えず無意味との考え方もある。
・署名があるから安全という誤解を与えると困る。署名付きのスパムメールも出てくる。
・メールクライアントの制限があり、一律署名をつければ表示されるわけではないのが問題。

④電子署名と共に電子的な印影を表示するシステムもあるが、利用者や行員にとって印影が表示されることで理解度や信頼度は変わると思うか。リアルの判子と電子署名を組み合わせた利用方法を進めてはどうか。

・目に見えるかどうか以前の問題で、署名のニーズがあまり無いと思われる。当該製品もあまり流行っていないと聞いている。
・内部統制の機運が高まればニーズが出るかもしれない。そうなると、“部長”とか役職者に持たせるには良いツールかもしれない。

(3) 電子署名の環境・インフラについて

①一企業にとじないで業界として、あるいは他業界と連携して電子署名を利用するシーンやニーズはあると考えるか。

・建設業界では、入札先により別々の電子証明書が必要になる等問題になっている。電子証明書が共通に利用できるように統一が必要である。

②上記ニーズがある場合、その実現のためのネックになること、あるいは実現の条件は何か。（例えば、共通のプロファイル、ガイドラインなど）

・電子署名法の認定認証局はコスト的に高く、自行での運営等は難しく実現は困難。
・個人だけでなく、法人や役職に対する証明書を発行できるようにする必要がある。
・JPKI の利用に関して制約が大きく、広がらない原因となっていると考える。

③電子署名の社会インフラが整備されていれば、サービスや業務にも有用と考えられるか。例えば、公的個人認証が普及すれば活用することは考えられるか。（例えば、架空口座の撲滅、死亡した人の口座の凍結、相続トラブルの軽減等）

・全銀協でも検討したが、まず公的個人の普及が先である。
・大手銀行がやれば、利用が一気に増えると思われるので期待は出来るが、そのために特定認定を取得しないといけない等の制約が多く、話が進んでいない。
・普及の条件としては、本人確認方法として、金融の本人確認プロセスで、特定認証業務認定が取れること、銀行口座を作ればキャッシュカードに公的個人認証がついてくる（韓国モデル）、あるいは、銀行カードがインフラと認めてもらう（フィンランドモデル）などの対策が必要。

・国がPKIの利用を必須として義務付ける（例えば、口座を作るには公的個人証明書が必須）などが必要。
・相続等の対策は、お客様からの申告による事になっているので、問題はない。
・免許証のICカード化に伴い、証明書が付加されると良いが、現在はその方向ではない。

④金融機関で使用する証明書は、パブリックなものであるべきと考えるか。
（パブリックとはWindowsの証明書ストアに認証局の証明書が格納されているもの）
・一般顧客向けにはパブリックであるべき。
・ビジネス（電子契約など）の場合には、クローズな関係で使っており、問題ない。現にプライベートCAでやっていて、インストールの手間が1つ増える程度である。

(4) その他
①電子署名やPKIの技術、製品、インフラについて、現状の課題、今後の対応、今後の展開への期待などあるか。
・共通の CA とか標準のフォーマットは、ビジネスの観点からは制約になるので困る。ガイドラインよりもオプションとしての位置付けであり、各会社が個々のビジネスで判断することである。
・現状の署名法はビジネスのフレームワークに立ち入りすぎている。例えば電子契約に使えるようなリーガルフレームワークだけを作って欲しい。
・タイムスタンプのガイドラインも、ビジネスに立ち入りすぎている。ガイドライン作成時には十分注意が必要である。
・既存の紙文書を電子化するよりも、申し込みのところから電子化されたものの方が効果が高い。
・既存の紙文書のものを電子化した場合、セキュリティ的に低下してしまう印象を持つ人が多く、普及の妨げとなっている。
・金融機関での本人確認レベルに対応した電子署名について、法的な裏づけをつける事に意味がある。

②特定認証局の認定を取得することについて
・当初のねらいは他社との差別化、及び契約数が多いので、業務フロー改善に役立つ。
・三文判の使用により発行できるように規程を変更し、非特定認証の業務として、証明書発行を行っている。
・社内で契約業務は特定業務と判断。当時は特定認証局が一般的でなかったこと、証明書のカスタマイズ（プロファイルにサービス固有情報を入れる）を行いたかったことなどから自社で特定認証局を建てる判断をした。
・法律上、被証明者（＝顧客企業の社長）に実印を用意してもらう必要があるなど、証明書の取得の手間がかかるが、従来の紙による契約に比較してメリットが少なく、顧客の経営者に説明するのは困難。

③電子契約と電子署名の仕様及び課題。

- リース契約は私文書扱いとなっており、印紙も必要ないため印紙代節約というメリットが出ない。
- リース業界では1社あたりの契約書数が多くないため、コスト削減効果はあまりない。グループ会社等間で契約数も多ければ、それなりに効果はある。
- 電子契約用のアプリケーション（ワークフロー）が先にあればの前提であるが、契約書の作成が楽になる（時間短縮）という利点が考えられる。
- 契約後7年間（リースでは7年3ヶ月）保持しないといけないので、保管場所が不要という点についてはメリットがある。
- タイムスタンプをサポートしていないと、多重署名の方式が一本化されていないため、署名ファイルに上書きしたり、署名対象部分とリンクさせる方式などもあり、債務不履行時の訴訟を行う場合には問題になるかもしれない。

このヒアリングは、2006年7月から9月に掛けて実施している。現在では、ヒアリングを実施した時期に比べて、会社法、金融商品取引法等による内部統制に対する関心が高まっていることも事実である。

## 1.3 金融業界の現状

FISCレポートとヒアリング結果から推察される金融業界の現状を以下に纏める。

1) 金融機関においても、法人向けであるとか、ビジネス用途、及びクループ内企業といった範囲では、インターネットバンキングのログインで PKI を利用した認証がかなり一般的になっているが、個人向けに利用した例、特に電子署名を行う利用形態は殆どない。

2) 金融機関として、自社で認証局を運用している例は少ない。ASP サービス、他社 CA へのアウトソースが殆どの模様。特定認証業務に挑戦したところもあるが、コスト的にも見合わず、メリットも少なかった。

3) 一般の個人は電子署名に関する理解が不十分である。サービスで使用している人はある程度理解しているかもしれないという程度。そもそも、PKI や電子署名を理解させる必要は無く、どういう効果があるというサービスの価値を示し、その中で電子署名することの責任を理解させるべき。

4) 現実の契約では、契約者の役職に対する制約が多い場合があるが、電子証明書では、自然人が会社代表者の認証が多く、役職の認証がなされていない。電子契約で利用するには、この役職の認証が重要な意味を持つ。

5) 公的個人認証の活用については、現段階では否定的である。まずは、公的個人認証サービ

スの普及が先決である。

6) 大手銀行での採用や、本人確認方法として、金融機関の本人確認プロセスで、公的な証明書の発行ができたり、銀行口座や銀行カードに公的個人認証が付いてくるなど、銀行カードがインフラとして認めてもらうなどの対策が必要で、国が PKI の利用を必須として義務付ける（例えば、口座を作るには公的個人証明書が必須）などの後押しが必要である。

［参考文献］

［1］FISC　金融情報システム　平成 18 年春号 No.283　特集　p4　金融機関における電子認証の活用動向，調査部

# 第2章　分析

前章の調査結果からは、残念ながら現状の金融業界は署名利用に積極的ではないと言える。ヒアリングでは、例えば個人向けサービスでは署名の必要性を感じないとか、法律等による電子署名使用義務がない、等の意見が多く挙げられた。これは、昨年度の報告で列挙した問題点分類（①需要、②適用可能範囲、③法令・施策、④標準化・相互運用性、⑤安全性・信頼性、⑥導入容易性、⑦操作性・運用性、⑧保守性）のうち、最初の障壁である「需要」（導入のモチベーション）の部分が、ネックになっている状態と考えられる。

導入の阻害要因には一般に、電子署名の本質的な問題によるものと、個々の業界特有の状況によるものがあると思われるが、その要因を掘り下げて根本原因を明らかにする必要がある。

## 2.1　金融業界で電子署名が普及しない要因

まず電子署名導入のモチベーションを中心に、日本の金融業界の状況について議論し、阻害要因と思われるものとして以下の意見が出た。

- 金融業界は3大メガバンクに集約され、保守的になり、新技術導入の競争原理が働きにくい。かつて Identrus 構想があった頃は各社が世界を目指す雰囲気があった。今はアジアでも主導権を取れていない。金融分野に限らないが、欧米からのアジアでの PKI 導入視察は、日本を素通りして韓国等に向かうことが多い。
  ※Identrus：日米欧主要金融機関が出資・参加した電子認証プロジェクト。アイデントラス社（本社：ニューヨーク）が、共通の認証局運営ルール等を制定し、加盟金融機関を認証する最上位（ルート）認証局を運営した。（JEDIC ニュースレターより）
- 金融の業務は紙で最適化されている。金融は他業界とのハブだが、電子化が進まず、業界横断的な情報流通における電子署名のメリットが出ない。／コスト競争になれば電子化が進む可能性があるが、銀行法で公共性を重視されていて、海外に比べ銀行間の差（例えば金利など）が出ない（競争できない）。（逆に言うと ATM などのインフラは促進しやすかった。）
- 銀行業務の対称範囲として、口座のない人にはサービス提供できない。
- 電子的なやり取りが中心となるネットバンクは電子署名と親和性が高いと見られるが、どのように与信するかが問題。Identrus のように格付けする組織があるとよいかもしれない。メガバンクは自分で与信できるので必要ない。
- 地銀やネットバンクならニーズがあるかもしれない。／地銀はインターネットより地縁でのビジネスが中心。ネットバンクの PKI ニーズは署名より認証。
- BtoC では消費者は保護されているので署名のニーズは小さい。BtoB はありうる。特に銀行側が署名するニーズはある。
- SOX 法では署名も有効な方法だが、どの方法を利用するかは銀行の考え方次第。コストパフォーマンスで選択すると必ずしも署名利用にはならない。

Identrus は先進的・意欲的な取組みであったが、下記のような要因もあり、海外組織から破綻した。

- 使いみちが未定だった。e マーケットプレイスに期待していたが未だに流行らない。
- 技術も未成熟だった。Web アプリ相当を狙っていたが未完成。
- CP/CPS が厳しすぎた。

導入のモチベーション（動機）には、昨年度報告でも述べたとおり、積極的な動機（メリットやインセンティブがあるもの）と、消極的な動機（無いと困る、あるいは義務付けられているもの）がある。それを利用者と提供者の側面で次の表にまとめてみた。

**表 2.2-1 金融分野における電子署名利用・導入の動機の状況**

| | 積極的な動機の状況 | 消極的な動機の状況 |
|---|---|---|
| 提供者（金融機関）の視点 | ×コストダウンに繋がらない（競争の必要がない。競争できない）<br>×署名利用サービスを提供しにくい（本人確認法などの制約） | ×電子署名の利用義務はない<br>○フィッシング横行の状況に鑑み、正当な金融機関であることを示す署名の必要性は高まっている（バイオ認証が急速に普及した状況に通じる） |
| 利用者の視点 | ×魅力あるサービスがない<br>×慣れていない（普及していない）ため、効果が実感されない | ×署名が無くても困らない（特に個人ユーザは不正による事故があっても補償されるなど、保護されている）<br>○法人ユーザとしては、署名が求められれば利用せざるを得ない（組織であれば対応しやすい） |

凡例　○：プラス要因、×：マイナス要因

競争原理が働きにくいことや個人ユーザが保護される状況は、日本の金融業界に固有な要因と考えられるが、普及していない（インフラが整っていない）ことや、サービスが少ないことは PKI 技術の一般的な問題点でもあると言える。

## 2.2　電子署名普及のための条件

以上の状況に対し、他の業界の事例などを参考にして成功要因を議論し、電子署名が普及する条件として、以下の意見が出た。

- JACIC（財団法人日本建設情報総合センター）の電子入札コアシステムのように強制的に導入・普及すれば、電子契約など BtoB に発展する可能性がある。
- JPKI（公的個人認証サービス）や JACIC も官が受益者であるが、コンシューマに普及するには民間が受益者となり推進するモデルが必要。
- きわめて安価で、価格以上の利便性があり、使用頻度が高いこと（交通用のカード、キャッシュカードなど）（C の分野）

- B の分野では、使わざるをえない状況になること（建築士とか、資格を証明したり、文書の改竄がないことを証明する必要のあるケース）
- インセンティブも重要（韓国では、電子で納税すると割引あり）
- 入札や電子申請も行政側にメリットがあるが、インフラになれば利用者もメリットを感じるようになる（電子申請もまだ1%以下なので、50%以上にすることが目標）
- トップダウンの強制力が必要（韓国の電子債権モデル）

業界別の特徴（普及・推進の条件）としては以下があげられた。

- 医療業界は、技術的に詳しい医者など推進者がいる。
- 建築業界は偽造問題があり、対策として署名は有効。図面のチェックは大変なので、それを楽にする仕組みができるとよい。
- 士業（○○士など）も有望。
- 医療ではカルテなどを院外に流通するため署名が必要になる。金融ではそれに相当するのは、手形（電子債権）。

これらから、普及が促進される典型的なパターンを以下の 4 つと仮定し、その成功条件、成功例をまとめる。

**表 2.2-2 想定される普及パターン**

| | 普及パターン | 成功条件 | 成功モデル<br>（あるいは有望モデル） |
|---|---|---|---|
| 1 | トップダウンのインフラ整備や法制度の変更による普及 | ・強制力<br>・利用者のコストメリット（無料または極めて安価）<br>・利用者のインセンティブ（税金の軽減等） | ・韓国（金融）、エストニア（eID）、台湾（医療系）<br>・JACIC<br>・(非 PKI だが) 銀行 IC カード、生体認証 |
| 2 | 自由競争による導入促進 | ・規制緩和<br>・競争意識、横並びの意識<br>・魅力的アプリケーション、利用者の利便性 | ・(非 PKI の例では交通用や電子マネーの IC カード) |
| 3 | 影響力のある先進ユーザからの普及 | ・有資格者や大企業などの利用推進<br>・責任を明示する文化の醸成 | ・企業による署名メール<br>・○○士（建築士等）<br>・内部統制 |
| 4 | 情報流通や情報管理の必然性からの導入 | ・ドメイン間の文書流通<br>・BPR（業務改善）によるコストメリット | ・医療<br>・大学 |

項 1 と 4 は外的要因により利用しやすい状況が整うケースである。1 はまずトップダウンで証

明書が普及し、それを使う用途が徐々に広がっていく。4 は関連する業界で電子化が進めば相互流通時のデータの認証などでPKIの利用が必然化すると考えられる。項2と3は業界において自主的に導入が進むケースであるが、PKI については不正やトラブルの増大への反動として署名を使うことが常識となり、普及が進むというシナリオが期待される。

# 第3章　金融業界における利用モデルの提案

現時点の金融業界における PKI の利用状況としては、インターネット経由の B2B トランザクションにおいては大手行を中心に普及し始めているが、その他の分野については普及していない。特に個人を中心とした B2C での利用においては、ワンタイムパスワード等のキャラクタベースの電子認証の利用は進んでいるが、PKI についてはまだまだというのが現状である。しかしながら、今後は B2C でのインターネット取引の安全性確保の観点、更に他業界とのデータ交換や内部統制の観点等から普及が進んでゆくと思われる。そこで、以下に普及を促進するための、金融業界の内外での取り組みについて検討を行う。

以下では、前章での分析を踏まえて何らかの普及条件を仮定して、金融業界における PKI の利用モデルを検討・提案する。

## 3.1　PKI 導入モデル

PKI の一般的なモデルは、対等な当事者と、独立な第三者機関としての認証局という構成において、認証局の信頼性に基づき電子的なトランザクションを保証するモデル（三者モデル）である。しかし現在よく見られるモデルは、サービス提供側である行政機関や企業が認証局を持ち、市民や取り引き先に対して証明書を発行するモデル（二者モデル）である。また、認証局をアウトソースすることもあるが、証明書発行主体はサービス提供側であり、同様に二者モデルとなっていることが多い。

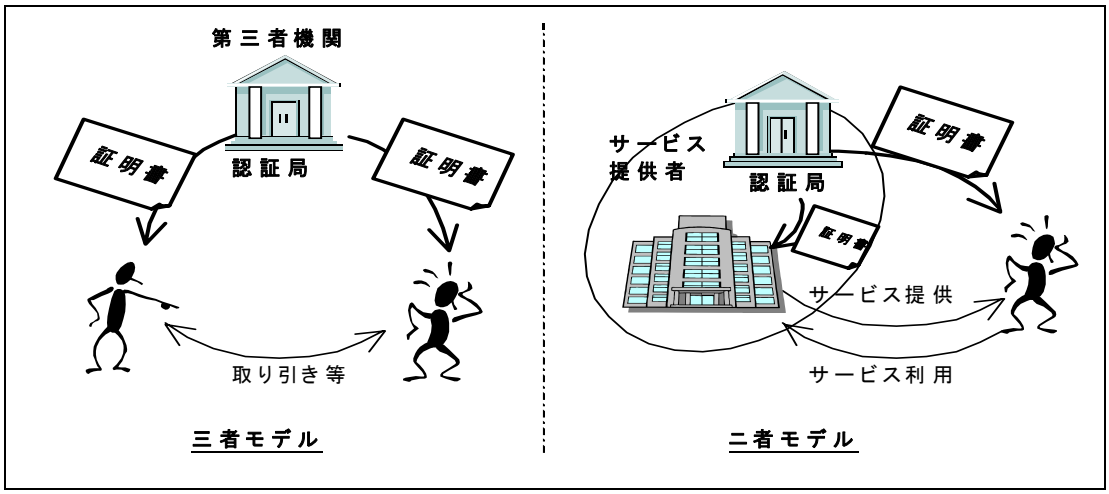



図 2.3-1 PKI 導入モデル

例えば、一般の認証機関の証明書を利用して取り引きする場合は三者モデルであり、銀行等が顧客に証明書を配布する場合は二者モデルである。三者モデルは、当事者間で共通に信頼できる第三者機関の選定に関して合意が難しいなどの問題があり、公的個人認証サービスや JACIC 認証局などを除き、あまり利用例は多くない。第三者機関としての認証局もビジネスモデルが成立し難いのが現実であり、業界全体で認証局の導入を考えるなど、Identrus のような構想を再構築す

ることが必要であろう。

一方、二者モデルはサービス提供者のクローズドなビジネスになることが多く必ずしもPKIが必須とは限らない。またPKIの利用は成りすましや改竄、否認を防ぐためであるが、サービス利用者が消費者であれば、消費者保護を目的とした法律により保護されるため、PKI のニーズは高くないのが現状である。従って、金融機関の発行した証明書が他の業界でも効力を持つようなオープンなビジネスモデルができ、積極的な利用の動機が喚起されることが必要であろう。

## 3.2 金融分野におけるPKI利用モデル

次に、前章の普及パターンを金融業界に当てはめて、それを可能とする（と思われる）施策と、利用モデルを以下にまとめてみた。

表 2.3-1 金融分野における普及パターンと利用モデルの想定

| 普及パターン | 施策の案 | 金融業界での利用モデル |
|---|---|---|
| トップダウンでのインフラ整備や法制度の変更による普及 | 一定額以上の金融取引での署名の義務化 | ・制度変更に対応した署名利用の金融アプリの普及・署名利用による利用者への利便性向上のための普及 |
| | 本人確認法における証明書利用の拡大（例：本人確認された電子証明書利用以外のインターネット取引の規制） | ・証明書入り銀行 IC カードの普及・公的個人認証の活用 |
| 影響力のある先進ユーザからの普及 | 金融機関証明書の普及 | ・金融機関による署名メール |
| 情報流通や情報管理の必然性からの導入 | SO法への対応 | ・内部統制ソリューションとしてPKI認証を導入 |
| | 電子債権法 | ・電子債権登録法対応サービス |

金融業界の場合、法的規制が多く、規制緩和や法的義務付けなど強制力の発動と、不正や被害の多発による世論の後押しが必要ではないかと考えられる。上記の例で言うと、「署名の義務化」や「証明書利用の拡大」が効果を発揮すると、次のようなシナリオで普及が進む可能性がある。

［普及シナリオの例1］：署名の義務化

①詐欺やウィルス等を原因とする不正取引で、金融機関の損害が増大

↓

②預金者個人からも、オンラインバンキングの安全性について問題視

↓

③政府が対策として、金融トランザクションにPKI利用を義務化

あるいは、金融機関が自己防衛のため、PKI利用を推奨

（例：現在のATMにおける資金移動の上限金額のように、PKIなしだと
小さくして、ICカードを使ったPKIだと制限無しにする等）

［普及シナリオの例2］：証明書利用の拡大
①韓国の様に1枚の証明書、それも認定認証局が発行したもので様々なサービスを利用可能
↓
②企業の業務が効率化されて、かつ金融機関側も電子化による恩恵を享受

その他、署名利用のハードルを下げるため、携帯電話による署名利用や、電子商取引のさらなる進展があると、普及を促進する要因になることが期待される。

# 付　録

１．欧州における PKI および証明書の利用に関する調査 2006 年

２．エストニア ID カードと電子署名の概念原則とソリューションホワイト・ペーパー

３．金融機関における電子認証の活用動向

# 欧州における PKI および証明書の利用に関する調査 2006 年

Fraunhofer Institute FOKUS

# 目　次

# 概要

欧州委員会は、1999 年 12 月 13 日に電子署名の共通枠組みに関する指令を発布した。この指令は欧州連合内で適用されるべきものであり、加盟国はこれを自国の法律に適合させなければならない。

しかし、利用者の受け入れ率は低く、相互運用上の問題が存在し、電子署名を必要とする応用分野は明確ではなかった。クオリファイド電子署名の利用に対する電子署名指令の運営に関する EU の報告書では、これらの署名は予想よりもはるかに利用が少なく、市場はまだ十分に開拓されていないとも述べられている。最近数年間では、これらの問題を克服するためにさまざまな国でイニシアティブおよび提携が組織され、標準化活動が行われ、大規模なプロジェクトが遂行された。

この調査の主な目的は、欧州における PKI 利用の現状と進展を調査し、浸透に向けた戦略と社会への影響を描き出すことにある。

アプリケーションとインフラストラクチャーに対する PKI ベースのサービス導入の進展状況は欧州内で大きく異なっている。この報告書では、したがって PKI ベースの証明書、スマートカード、署名の利用について、欧州諸国の状況をより詳細に分析する。電子署名指令の運営に関する EU 報告書によれば、e ガバメントおよび e バンキングは安全なインフラストラクチャーの推進力と考えられているため、これらのアプリケーション環境はさらなる情報検索のためのものであると考えられた。しかし、これらのインフラストラクチャーは通常、情報公開を目的として記述されているわけではないため、銀行部門に関しては十分な情報を利用することはできない。

観察された主な違いは、署名媒体（スマートカードやその他の媒体）、技術的な実行方法、および電子署名、利用分野、登録方法、PKI の運営、相互運用性を必要とする行政手続きに関するものである。各国を比較した主要な結果は、各国での浸透に向けたさまざまな戦略（例えば、費用のかからない証明書、簡単な登録プロセス、USB やモバイルによる署名）にもかかわらず、電子署名はまだ広く利用されていないというものであった。

電子署名と PKI が社会にもたらすことができる影響と経済的な側面を理解し予測するためには、全般的な革新のプロセスを理解することが重要である。この点は、革新に対して認識された 5 つの特性を定義した Everett Rogers の「技術革新の普及過程（Diffusion of Innovation）」の理論にしたがってさらに掘り下げて考える。5 つの特性とは、相対的な優位性、両立性、複雑性、試験可能性、観察可能性であり、電子署名に対するこれらの特性の関係が描かれている。

現在、PKI に関する活動では、法的な署名よりも認証特性が主に重視されている。認証はすべての人にとって第一の目標である。この目標は社会ではるかに広く認識されている。欧州委員会は、電子身分証明書に向けて進むために eID イニシアティブに高い優先度を与えた。

# 1. はじめに

長年、電子署名のブレークスルーが予測されていた。しかし、利用者の受け入れ率は低く、相互運用上の問題が存在し、電子署名を必要とする応用分野は明確でなかった。最近数年間では、これらの問題を克服するためにさまざまな国でイニシアティブおよび提携が組織され、大規模なプロジェクトが遂行された。この調査の主な目的は、欧州における PKI 利用の現状と進展を調査し、浸透に向けた戦略と社会への影響を描き出すことにある。

2 章では EU 電子署名指令（指令 1999/93/EC）を紹介する。この指令は、EU 加盟国内での電子署名の応用に対して基礎を提供している。PKI 利用の急増が長年予測されていたとはいえ、さまざまな障害が存在するのでその要点を説明する。欧州での PKI の利用を促進するために、いくつかのイニシアティブ、標準化活動、調査プロジェクトについて説明する。

3 章では PKI ベースのアプリケーション・サービス導入の進展について説明する。PKI ベースのサービスは欧州内でそれぞれ大きく異なった段階にあるため、証明書、スマートカード、署名の利用について、EU 加盟国および欧州委員会自体がより詳しく分析されている。デジタル証明書サービスのばらつきについて説明する。

4 章では社会への影響に注目する。電子署名と PKI が社会にもたらすことができる影響と経済的な側面を理解し予測するためには、全般的な革新のプロセスを理解することが重要である。Everett Rogers の「技術革新の普及過程」の理論に基づいて、PKI ベースのサービスの社会と個人への浸透を描く。

5 章ではこの調査の結論を下し、PKI の利用における将来の有望な分野について概要を説明する。

# 2. 欧州における PKI の利用

デジタル署名は、公開鍵基盤（PKI）スキームとの関連で利用されることが多く、そのスキームのなかで、通常は第三者によって運営される認証局が発行するデジタル ID 証明書によって、署名スキームで利用される公開鍵が利用者と結び付けられる。PKI システムでは非対称鍵暗号方式が利用される。

電子署名[1]では、あらゆる形式のプロセス、アプリケーション、インフラストラクチャーに必要なさまざまなセキュリティ対象がサポートされる。

[1] The terms ″electronic signature″ and ″digital signature″ are used equivalent in this report.

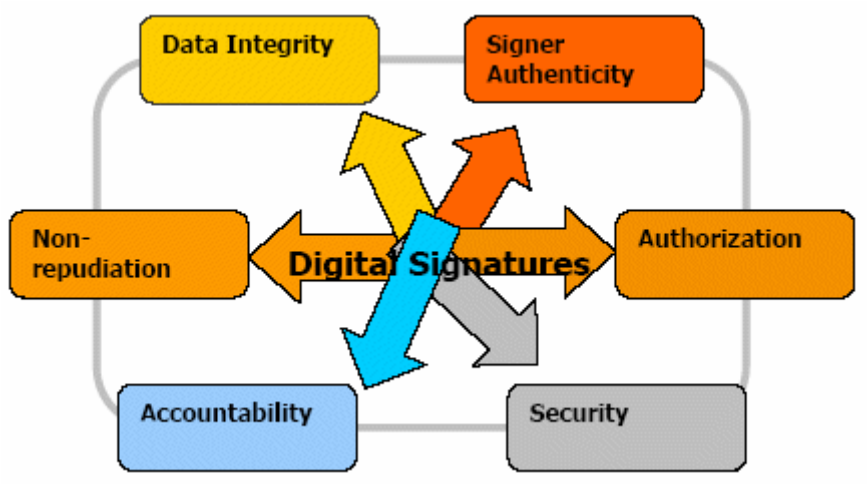



Figure 1 : Security Targets of Electronic Signatures (Source : www.arx.com)

電子署名の利用を促進し、その法的な認定に貢献するために、欧州議会は電子署名指令を発布した。この指令は、EU 内の市場を適切に機能させるために、電子署名および特定の証明サービスに法的な枠組みを確立する。

## 2.1 EU 電子署名指令

欧州での PKI の利用は EU 電子署名指令（欧州議会および電子署名の共通枠組み指令委員会による指令 1999/93/EC）から強い影響を受けている。

この指令では電子署名の 3 つの形式を取り上げている。第 1 の形式は最も単純な形式の「**電子署名**」であり、広い意味が与えられている。これはデータを識別・認証する機能を果たす。これは、人の名前や PIN コードを利用して E メール・メッセージに署名をするのと同じくらい単純になる可能性がある。認証が署名となるには、データと関連していなければならず、実体認証のためだけの方法や技術として利用されてはならない。

指令で定義された電子認証の第 2 の形式は「**アドバンスト署名**」である。署名のこの形式は、指令の第 2.2 条で定められた要件を満たさなければならない。この指令は技術的に中立の立場である。が、実際にはこの条項は、公開鍵基盤（PKI）に基づいた電子署名を主に指している。この技術では、暗号化技術を利用してデータに署名を行い、公開鍵またはプライベート鍵が必要になる。

最後に、第 5.1 条で言及された第 3 の形式の電子署名がある。指令ではこれ自体を指す言葉は与えられていない。が、一般に「**クオリファイド電子署名**」と呼ばれている。これは、クオリファイド証明書に基づき、安全署名生成装置（SSCD）によって作成されたアドバンスト署名で構成されており、付録 I、II、III の要件に適合している必要がある。

EU 加盟国の大部分は指令を国内の法律に組み込みた。また、EU 非加盟国の多くは、独自の電子署名および署名関連のサービス提供の法律を EU 指令の条項に基づかせている。指令は、技術的な面では、クオリファイド証明書に対する IETF の標準化作業などの国際的な標準化イニシアティブにさらに大きな影響を与えている。指令で導入された新しい専門用語（特に、クオリファイド

証明書、アドバンスト署名、証明書サービス・プロバイダー）は国際的な背景で採用されている。［Dumortier］。

とはいえ、「強固なセキュリティ」をもたらす（クオリファイド）電子署名の詳細に対する国ごとの解釈およびその結果の国ごとの具体的な規制ではばらつきが現れており、また電子署名の導入では大きな相違が現れて「共通枠組み」の形成を阻害している。署名に関する指令が欧州で制定されてから数年後の現在、特にクオリファイド電子署名はいまだに存在感が薄いままである。これまでのところ、欧州電子署名指令で定義された電子署名の４つの水準（単純な署名、アドバンスト署名、クオリファイド署名、認定された署名）の１つにたどり着くためにどの技術的な実行方法を利用できるかについて合意は形成されていない。また、どのような行政手続きと署名が必要であるかについての合意も形成されていない。

したがって、次のセクションではPKI利用の障害を説明する。

## 2.2 PKI利用の障害

このセクションでは、OASIS の PKI 技術委員会（OASIS PKI TC）と［Dumortier］が観察したPKI利用の障害を要約する。

OASIS PKI TC［OASIS-PKI］は調査を行い、PKIの展開と利用上の障害を特定し、優先順位をつけた。この調査は2003年に行われたとはいえ、調査結果は現在でも有効であると思われる。

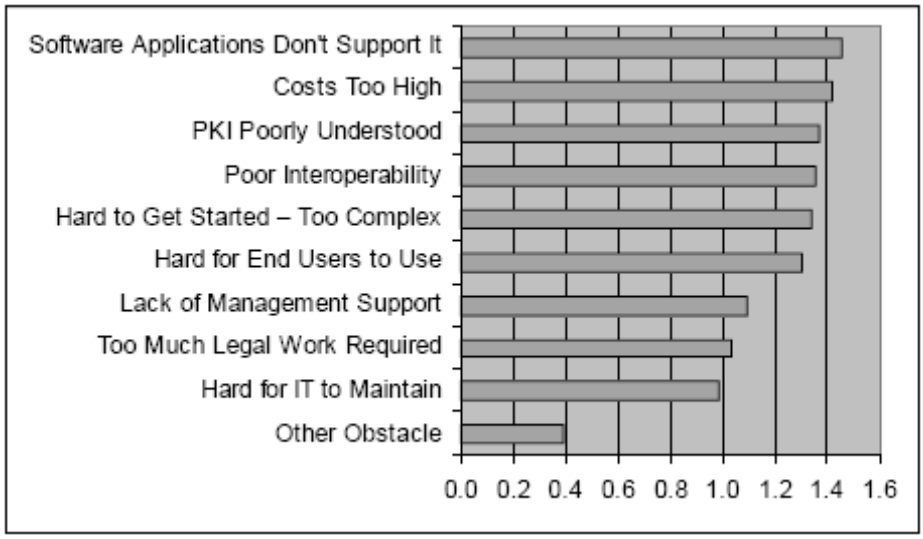



Figure 2：OASIS TC PKI Survey on PKI Obstacles（Source：[OASIS-PKI]）

［Dumortier］の中では、電子署名のより広範囲な利用と受容に対する未解決の問題、ならびに欧州委員会の要求される活動はすでに特定されており、次のように簡単にまとめることができる。

- クオリファイド証明書およびそれに関連するサービスに対する自然状態での市場の需要は存在しない。欧州における電子署名の最大の応用分野は、限定された利用者環境の e-

バンキングの用途に一般に結びついており、したがって指令の範囲外である。指令の範囲内では、応用は現在ごくわずかにしか行われておらず、ほぼ完全に e-ガバメントに限られている。

- 多くのアプリケーション・サービス・プロバイダーは、法律を順守するには利用では少なくともクオリファイド電子署名が必要であると誤って認識しており、これによって不必要な費用と複雑さがもたらされている。
- 国内と国外の両レベルにおける相互運用性の欠如は、電子署名の市場での受容と普及にとって障害となっている。
- 現在のところ EU 指令では SSCD に非常に高い要件が設定されていることもあって、このような装置を市場に提供する方法を見つけることはまだ非常にまれである。
- 署名に関する EC 指令の規制的な枠組みには、証明書のプロバイダーに対する極めて詳細な規則が含まれているが、証明書のプロバイダーのその他のカテゴリーには対処していない。

［FIDIS-D41］によれば、2005 年時点ではまだ、デジタル署名、e-ID、または e-ガバメントの各サービスへの PKI システムの導入はほんの初期段階にあり、次の障害が確認されている。

- 複雑性、およびインフラストラクチャーを確立するために必要な初期投資。
- 消費者のイニシアティブ（e-アプリケーション、便利さ）の欠如 対 費用（カード・リーダー、ソフトウェア)。
- 特に証明書とサインド・エンベロップの相互運用性、第三者の認証局（CA）から発行された証明書の照合、アプリケーションによる証明書の利用、ディレクトリーが扱う証明書、およびタイム・スタンピングでの標準規格の欠如。標準規格がない中、デジタル署名への PKI の導入を進めているいくつかの国は独自の仕様を開発しており、相互運用性に将来問題を引き起こす可能性がある。
- CA 間および各国間での信頼性の相互認定の構築に関する法律面および手順面での規制、ならびにそれに関連する管轄区域。すなわち、（デジタル署名および契約上の法的責任に対する）方針、契約による合意、法的な枠組みの相互認定。
- アプリケーション水準での暗号技術、属性証明書、スマートカード技術、登録スキームの利用における技術的な相互運用性構築の困難が特に個々の CA 間において存在する。

電子署名指令［EU-RepDirSig］の運営に関する EU の報告書によれば、クオリファイド電子署名の利用は予想よりもはるかに少なく、市場はまだ十分に開拓されていないとも述べられている。確認されている電子署名の有力な 2 つの応用分野は *e-ガバメント・サービス*と *パーソナル e-バンキング・サービス*に関連するものである。報告書では、市場の取り組みが遅い主な理由は経済的なものであると述べられている。すなわち、サービス・プロバイダーにはマルチアプリケーション用の電子署名を開発する誘因がほとんどなく、例えば銀行部門によって開発されたソリューションなど、独自のサービスのためのソリューションを提供する方を選んでいる。さらなる理由と

して、電子アーカイブのための包括的なソリューションなどのアプリケーションが依然として不足している点がある。このように受容が進まない状態が e-ガバメント・サービスの電子署名の利用によって克服されることが期待されている。e-ガバメント・サービスはすでにある程度の規模に達しており、おそらく将来の重要な推進力となるであろう。

e ガバメントのアプリケーションの戦略的な役割は i2010 イニシアティブ（http://europa.eu.int/information_society/eeurope/i2010/index_en.htm)でも認識されている。このイニシアティブは、民間部門および公共部門による ICT の配備および効率的な利用を促進するためのものである。

## 2.3 PKI 利用の促進

欧州における PKI 利用の障害を克服するために、いくつかのイニシアティブが組織され、標準化活動が遂行されている。

このセクションでは、例として次の最も関連性が高い戦略、イニシアティブ、標準化の取り組みの概要を紹介する。

- IDABC、すなわち、行政機関、企業、市民を対象とした欧州 e ガバメント相互配信サービスに関する共通プログラム
- 電子署名およびインフラストラクチャーを担当する ETSI の TC ESI
- ENISA、すなわち欧州ネットワーク情報セキュリティ局
- EU i2010 戦略－成長と雇用に向けての欧州情報社会

e ガバメントなどの一部の応用分野は他の分野よりも進歩している。したがって次の章では、EU および／または一部の欧州諸国で達成された e ガバメントと e ヘルスの進歩をより詳しく検討する。

### 2.3.1 IDABC[2]

IDABC は欧州委員会の企業産業総局によって運営される共通プログラムであり、欧州の民間部門を近代化するという eEurope の目標に貢献している。IDABC は、行政機関、企業、市民を対象とした欧州 e ガバメント相互配信サービス（Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens）の略語である。

*IDABC e ガバメント観測所* [3]は欧州全体の e ガバメントの問題点と進展に関する参考情報ツールである。このツールは、独特な情報資源一式、および欧州内外の e ガバメント戦略、イニシアティブ、プロジェクトに対する価値ある見識を e ガバメントの意思決定者および専門家のグループに提供している。

[2] IDABC http://ec.europa.eu/idabc/en/home

[3] IDABC eGovernment Observatory, http://ec.europa.eu/idabc/en/chapter/140

### 2.3.2 ETSI[4]

欧州電気通信標準化協会（ETSI）は非営利組織であり、ETSI の活動プログラムの特定の分野を担当する数多くの技術団体で構成されている。TC ESI は ETSI 内で電子署名およびインフラストラクチャーの標準化を担当している。ETSI の活動は［ETSI06］に記述されている。

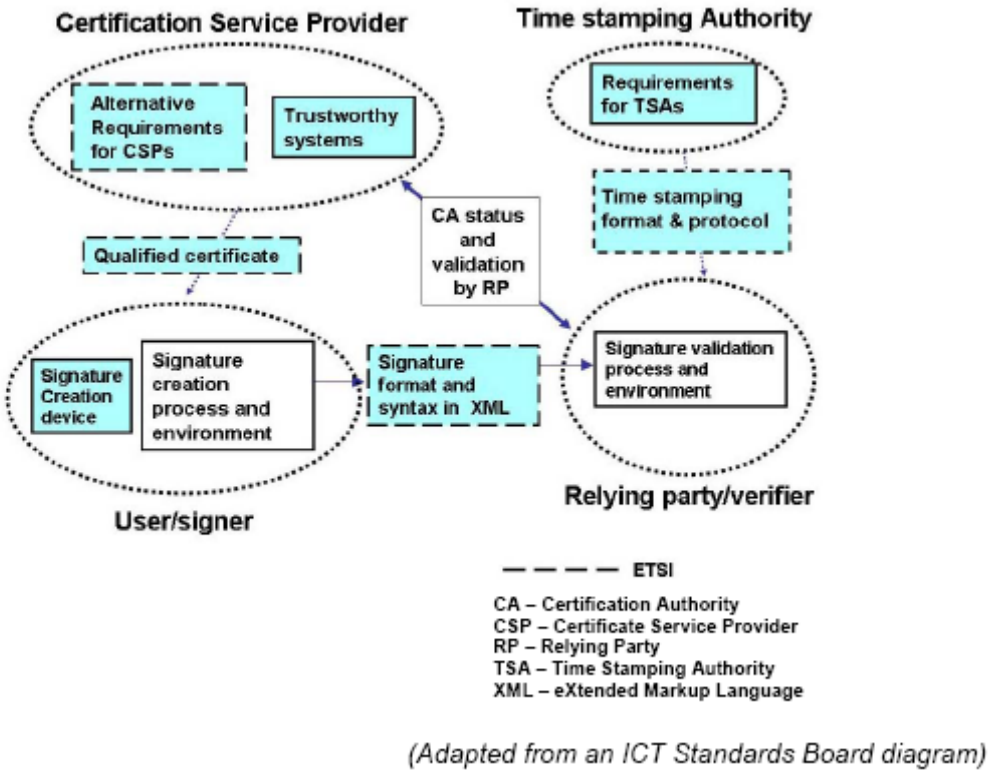



Figure 3：ETSI Work on Electronic Signature Standardization（Source：ETSI）

図 3 では、電子署名およびインフラストラクチャーに対して行われた ETSI のすべての活動が要約されている。設定された標準規格を以下にリストアップする。

- TR 102 044　電子署名およびインフラストラクチャー（ESI）；役割および属性証明書に対する要件
- TR 102 045　電子署名およびインフラストラクチャー（ESI）；大規模なビジネス・モデルに対する署名の方針
- TR 102 046　電子署名およびインフラストラクチャー（ESI）；EESSI フェーズ 2 および 3 の ETSI 標準規格の維持管理
- TR 102 047　電子署名およびインフラストラクチャー（ESI）；電子署名フォーマットの国

[4] ETSI, TC ESI is responsible for Electronic Signatures and Infrastructures standardization http://portal.etsi.org/Portal_common/bottom.asp?Register=&tbid=607&SubTB=607&TAB_ID=&Param=

際的調和

- TR 102 040　電子署名およびインフラストラクチャー（ESI）；証明書を発行する CA に対する方針要件の国際的調和
- TR 102 231　電子署名およびインフラストラクチャー（ESI）；委託サービス・プロバイダーのステータス情報の調和に関する規定
- TR 102 158　電子署名およびインフラストラクチャー（ESI）；クオリファイド証明書と利用可能な属性証明書を発行する証明書サービス・プロバイダーに対する方針要件
- TR 102 153　電子署名およびインフラストラクチャー（ESI）；証明書プロファイルの予備調査
- SR 002 176　電子署名およびインフラストラクチャー（ESI）；安全な電子署名のためのアルゴリズムおよびパラメーター
- TS 101 733　電子署名およびインフラストラクチャー（ESI）；CMS フォーマットのアドバンスト署名 CAdES）
- TS 102 280 X.509 V.3　自然人に発行された証明書のための証明書プロファイル
- TR 102 272　電子署名およびインフラストラクチャー（ESI）；署名方針のための ASN.1 フォーマット
- TS 101 456　電子署名およびインフラストラクチャー（ESI）；クオリファイド証明書を発行する認証局に対する方針要件
- TS 102 042　電子署名およびインフラストラクチャー（ESI）；公開鍵証明書を発行する認証局に対する方針要件
- TR 102 317　電子署名およびインフラストラクチャー（ESI）；ETSI の成果を管理するためのプロセスおよびツール
- TS 101 903　電子署名およびインフラストラクチャー（ESI）；XML フォーマットのアドバンスト署名（XAdES）
- TS 101 862　電子署名およびインフラストラクチャー（ESI）；クオリファイド証明書プロファイル
- TS 102 176-1　電子署名およびインフラストラクチャー（ESI）；安全な電子署名のためのアルゴリズムおよびパラメーター（パート 1）：ハッシュ関数および非対称アルゴリズム
- TS 102 176-2　電子署名およびインフラストラクチャー（ESI）；安全な電子署名のためのアルゴリズムおよびパラメーター（パート 2）：署名生成装置のための安全なチャネル・プロトコルおよびアルゴリズム
- TR 102 041 SEC ESI；署名方針の報告書
- TS 102 023　電子署名およびインフラストラクチャー（ESI）；タイム・スタンピング機関に対する方針要件
- TS 101 861 SEC ESI；電子署名およびインフラストラクチャー（ESI）；タイム・スタンピング・プロファイル
- TR 102 038　署名方針のための XML フォーマット
- TR 102 030 SEC ESI；委託サービス・プロバイダーのステータス情報の調和に関する規定

- TR 102 438　電子署名およびインフラストラクチャー（ESI）；欧州における電子署名標準規格の応用
- TR 102 458　電子署名およびインフラストラクチャー（ESI）；米国連邦 PKI から EU クオリファイド証明書方針（TS 101 456）へのマッピング

現在、ETSI での電子署名に対する活動では、特定の e-ビジネスのニーズのためのプロファイルの仕様に焦点を当てており、一方で TC ESI も次の関心領域（例えば e-インボイスや登録 E メール）の特定を進めている。

### 2.3.3　ENISA[5]

ENISA（欧州ネットワーク情報セキュリティ局）は、2005 年に発足した欧州連合の新しい局であり、EU の各機関と加盟国のために活動している。ENISA は欧州連合、EU 加盟国、経済界がネットワークと情報のセキュリティ問題を阻止し、これに取り組んで対応する能力を高めるために設立された。ENISA は、この目標を達成するために、ネットワークと情報のセキュリティのセンター・オブ・エクセレンス（中核的組織）となり、公共部門と民間部門間の協力を促進している。

ENISA は次のように述べている。「包括的なセキュリティには、安全な技術、安全な組織的プロセス、必要な経歴とスキルを持った人たちが必要である。これらすべてが、明確なインターフェースとあらゆる関係者に理解される専門用語を使用して協力的に活動しなければならない」。現在、ENISA は、欧州で利用されている知識、技術、組織の証明書に関する情報を収集している。ENISA はこの情報に基づいて「情報セキュリティ証明書」[6]のイベントを準備しており、証明書スキームの設定とその利用に関わる人たちが 2006 年末に集まる予定である。関係者が招待され、証明書スキームとその利用について紹介する予定である。ENISA は、共通点と相違点を明確にするために討論会を主催する予定である。証明書スキームを改善し、その利用を促進する計画がそのすぐ後に続く。証明者と証明書の最初のリスト[7]が作成された。

### 2.3.4　EU i2010 戦略[8]

「i2010－成長と雇用に向けての欧州情報社会」のイニシアティブは、情報社会およびメディア部門の 2010 年までの主な課題と成長に取り組むための枠組みとして、2005 年 6 月 1 日に欧州委員会によって立ち上げられた。このイニシアティブは、開かれた競争的なデジタル経済を促進するもので、一体化および生活の質の推進力として ICT が重視されている。i2010 は次の 3 つの柱で構成されている。

- 情報社会およびメディア・サービスの開かれた競争的な EU 市場を促進する、欧州の単一

[5] ENISA http://www.enisa.europa.eu/
[6] ENISA event "Information Security Certificates"
http://www.enisa.eu.int/pages/IS_certificates.html
[7] ENISA initial list of certifiers and certificates,
http://www.enisa.eu.int/doc/pdf/deliverables/enisa_list_of_certifying_orgs.pdf
[8] i2010 - A European Information Society for growth and employment
http://europa.eu.int/information_society/eeurope/i2010/i2010/index_en.htm

情報空間の創出
- ICT の革新と研究への投資の増加
- ICT の利用による一体化、より良い公共サービス、生活の質の促進

欧州の政策における「ネットワークと情報のセキュリティ（NIS）」の重要性はさまざまな形ですでに認識されている。i2010 戦略では、手ごろかつ安全な高帯域での通信を提供するための前提条件として、セキュリティの問題が強調された。

対話、協力、権限委譲に基づく NIS への新たな戦略的アプローチが欧州委員会によって提案された。[EU-NIS]。EU 加盟国は、ENISA と緊密に協力しつつ、セキュリティ技術のメリット、実践、行動を促進することを明確に依頼されている。e-ガバメント・サービスは、後にその他の部門に拡大される優良なセキュリティ・プラクティスを伝達・促進する手段であると見なされている。

## 2.4 EU プロジェクト

このセクションでは、さまざまなビジネス領域における電子身分証明書および証明書の利用に関連する重要な欧州のプロジェクトについて簡単な概要を紹介する。

### Digital Passport (http://www.eudigitalpassport.com)

Digital Passport（安全で便利な国境通過のためのバイオメトリック・データを利用した欧州の次世代デジタル・パスポート）によって、標準規格の一貫した適用、一連の技術の開発、新たな国境管理および空港のプロセスへの連結を行う方法が示される予定である。Digital Passport プロジェクトによって、従来の冊子と、カード所有者の個人データおよびバイオメトリック・データを所蔵・処理する大容量の IC マイクロ・コントローラーとの結合に基づいた新世代のデジタル・パスポートが実現される予定である。RSA マイクロプロセッサーによって、暗号化およびデジタル署名のための PKI ベースのセキュリティおよび能力へのサポートが提供される予定である。端末では、空港プロセスのモデルを含む、バイオメトリクス、パスポートへの非接触型接続、アプリケーションへの接続がサポートされる予定である。

### eEpoch (http://www.eepoch.net/)

eEpoch（eEurope スマートカード憲章の概念実証および包括的なソリューション）は 2004 年にすでに終了している。eEpoch の狙いは、各国内の電子 ID カードを地域および各国間の e-ガバメント・アプリケーション・サービスの領域で使用して、法的拘束力のある安全なインターネットベースの電子取引のために拡張可能な全欧州環境が実現できることを証明することであった。

### eGov-Bus (http://www.egov-bus.org/)

eGov-Bus（先進的 e ガバメント情報サービス・バス）の目的は、データ・アクセスの抽象化を提供する、安全性、利用可能性、拡張性の高い分散アーキテクチャーをベースにしたウェブ・サービス、プロセス、リポジトリー管理プラットフォームに依存して、技術の受容を促進し信

頼できるシステムの有効性および否認防止を確立する電子署名の高度なアプリケーションを作り出す能力を持った、政府および政府間のシステムのためのプロセスおよびコンテンツ管理の領域において研究と標準規格を統合・拡大することである。川下への主要な効果は、多くのeガバメント・プロジェクトの統合費用を削減することである。

eUser (http://www.euser-eu.org)

eUser（利用者中心のオンライン公共サービスの設計および実現に対する実証的サポート）の調査は、eガバメント、eヘルス、eラーニングの提供に関する利用者の真のニーズについて確かな証拠を提供し、また最新のオンライン公共サービスに対する利用者の姿勢および理解度に関するデータを提供するために開始された大規模な調査およびサポートのプロジェクトである。このプロジェクトでは、EUのISTプログラムが利用者と利用者のニーズをIST開発の中心に据えるという主要な目的を達成するためのサポートを行っている。このプロジェクトでは、欧州理事会が優先事項と認めた主要な公共電子サービスの領域（eガバメント、eヘルス、eラーニング）に関する経験的な情報を提供し、またこれらの領域での需給バランスを評価している。

GUIDE (http://www.guide-project.org)

GUIDE（欧州における政府の利用者 ID-e ガバメントのための相互運用可能かつ安全な ID 管理アーキテクチャーに対する欧州の標準規格の作成）は、欧州連合（EU）が資金を提供する調査プロジェクトであり、欧州における安全かつ相互運用可能なeガバメントの電子身分証明書サービスおよび電子取引のための技術的、制度的、政策的、社会経済的アーキテクチャーを構築する目的を持った調査および技術開発を行っている。認証と ID 管理自体は市民にとってサービスとはならない。むしろGUIDEは、その他数多くのeガバメント・サービスが認証を基礎として開発されるための触媒および基盤として機能している。GUIDE は、e ガバメントの認証のためのオープン・アーキテクチャーを構築することで、欧州をeガバメント・サービスの世界的なリーダーとする長期的なビジョンを持っている。

FIDIS (http://www.fidis.net/)

FIDIS（情報社会におけるIDの将来）は次の項目に対する技術に関する欧州の調査を統合するネットワーク・オブ・エクセレンス（中核ネットワーク）である。すなわち、身元と身元確認、身元と身元確認のコンセプトの相互運用性、ならびに個人情報の盗難、プライバシー、セキュリティ、プロファイリング、犯罪科学上の意味合いといった領域をサポートする技術である。FIDISのビジョンは、適切なIDとID管理が公正な、または（より）公正な欧州の情報社会への道筋をどのように前進させることができるかについて欧州が理解を深めることである。

NETC@RDS (http://www.netcards-project.com/index.php)

NETC@RDS プロジェクトは、IT システム、スマートカード、または両方の組み合わせのいずれかに基づく高度なウェブ指向のアプリケーションを利用することで、欧州横断的な医療サー

ビスへの市民のモバイル・アクセスを改善することを目標としている。また、このプロジェクトでは、欧州の健康保険カードの電子化、および欧州内の医療費の清算／請求処理などの追加サービス改善のための技術的解決策を導入・評価することを目標としている。NETC@RDS のサービスは、スマートカードおよび／またはネットワーク構築ソフトウェア・アプリケーションを含む既存の医療情報システムの延長として、オーストリア、フランス、ドイツ、ギリシャ、イタリア、フィンランドの試験運用地域で技術的に導入される。

PRIME (http://www.prime-project.eu)

PRIME（欧州におけるプライバシーと ID の管理）は、プライバシーを向上させる ID 管理システムの実用見本を開発することを目標としている。市場での導入を促進するために、例えばインターネット通信、航空会社および空港の乗客処理、位置ベースのサービス、共同 e-ラーニングなど、現実の世界の困難なシナリオにおいて ID 管理の斬新なソリューションが実演される予定である。

SecureE-Justice (http://www.secure-justice.org)

SecureE-Justice（司法の協力環境のための安全な通信・コラボレーションの枠組み）のプロジェクトは、複数の司法現場を持った分散的な通信・コラボレーションの枠組みに組み込まれる革新的で安全な技術の設計および開発に関連するものである。このプロジェクトは、セキュリティ市場全般を指向しており、特に分散環境および司法の協力におけるセキュリティ管理の市場に専念している。このプロジェクトで取り組んでいる調査活動項目には、確実な利用者管理（利用者の身元確認、認証、認可)、PKI、デジタル証明書、バイオメトリクスによる身元確認技術、確実な通信管理などがある。

## 3. 欧州諸国の進展

アプリケーションとインフラストラクチャーに対する PKI ベースのサービス導入の進展は欧州内で大きく異なっている。この報告書では、したがって PKI ベースの証明書、スマートカード、署名の利用について EU 諸国の状況についてより詳細に分析している。

この分析に対する多大な情報を次の資料から得た。

- IDABC 報告書「欧州諸国における e ガバメント－第 6 版」2006 年 9 月 29 日［IDABC-eGov06］
- IDABC e ガバメント観測所[9]
- Cap Gemini による EU の調査「公共サービスのオンラインでの利用可能性：欧州はどのように進展しているか」第 6 回調査の報告 2006 年 6 月［EU-eGovOnline］

e ガバメントおよび／または e ヘルスの分野で PKI ベースのソリューションに対する優良なア

[9] IDABC eGovernment Observatory http://ec.europa.eu/idabc/en/chapter/140

プローチや戦略を持った国を以下に選び出して説明し、それとともに普及計画と証明書の費用に関する情報を掲載した（情報が確認された場合)。

## 3.1　国の概要

e ガバメントおよび e バンキングは安全なインフラストラクチャーの推進力と考えられており［EU-RepDirSig]、すなわち、PKI、電子署名、電子認証が利用されているため、これらのアプリケーション環境はさらなる情報検索のためのものであると考えられている。とは言うものの、銀行部門には利用できる情報がほとんどないことをはっきりと述べなければならない。通常これらのインフラストラクチャーは、一般からのアクセスを目的として記述されているものではない。

e ガバメントにおいて欧州で先導的と考えられている国についてさらに詳しく説明する。いくつかの国については情報がほとんど収集できない。これらの国は先導的と考えられていないこと、および／または情報が現地の言語でしか手に入らなかったことが主な理由である。注目すべき結果を達成していない国がリストに含まれているが、記述は非常に短くなっている。

### 3.1.1　オーストリア

オーストリア財務省、オーストリア国立銀行、グラーツ工科大学は、1999 年 5 月にオーストリア安全情報技術センター（A-SIT）を設立した。同センターは、技術的な情報セキュリティの分野における専門知識を発展させ、各種機関、経済、市民に貢献する使命を持った独立の非営利団体である。特にこの使命には、市民カード（*Bürgerkarte*）の導入および暗号方式の評価が含まれていた。また A-SIT は、デジタル署名の証明書を提供する権限を持った、最初であり現在唯一のオーストリアの組織である。

**eID**：オーストリアの e-ガバメント戦略の基礎的な要素は**市民カード**（*Bürgerkarte*）である。これは電子署名とデジタル証明書が埋め込まれたスマートカードであり、これによって市民は電子公共サービスに安全にアクセスし、行政手続きを電子的に完了することができる。オーストリアの e-ID のコンセプトの独創性は、市民カードの種類が 1 つではない点である。「Bürgerkarte」は、パスポートのように各市民にとって同じ特性を持ったカードではなく、むしろ安全な電子行政サービスの設計を可能にするコンセプトである。そもそも「Bürgerkarte」は、追加の機能を組み込むことができる、手続きにおける署名ソリューションである。例えばこのカードは、公共部門においてオーストリア国民の身元を確認し、または国の社会保障制度において国民を議員や行政機関の職員、学生として識別するために利用することができる。さらにこのカードは、支払機能を果たする。(いわゆる現金自動支払いカード（Bankomaten Karte))。原則的に、安全な形式で電子的に署名し、個人データを保存することを可能にするカードは市民カードとしての利用に適している。したがって、特定の団体（例えばオーストリア・コンピューター協会、連邦経済会議所など）が発行するメンバーシップ・カードやある種の銀行のクレジット・カードである。ら市民カードの機能を組み込むことができる。また、「簡単な」市民カード・サービスは携帯電話でも利用することができ、オーストリア国民は携帯電話を経由して文書にデジタルで署名し、政府に対する手続きを安全に行うことができる。したがって市民カードは特定の形式の技術に依存しておら

ず、自分の身分証明を電子的に行うためにどの技術を利用するかは完全に市民が選択することができる。IC カード、携帯電話、USB 機器のどれを使用するかにかかわらず、媒体が市民カードに不可欠な一定のセキュリティ要件を満たすことが重要である。(電子署名、身元確認、データ記憶)。

自然人は、行政との電子的な通信において部門固有の個人識別子に基づいて身元が確認される。個人の固有の ID 番号（中央住民登録所に保存された ZMR 番号）から暗号化プロセスを経由して得られ、電子的に署名された形式で市民カードに保存された「ソース暗証番号」は、これらの部門固有の個人識別子を作り出す基礎として機能している。個人のソース暗証番号は、市民カードの正当な所有者のみが管理することができ、アプリケーションに直接保存することはできない。2 つの暗号化プロセスの適用（ソース暗証番号の ZMR 番号の暗号化およびソース暗証番号からの部門固有の個人識別子の取得）では、高水準のデータ保護が保証されている。

「Bürgerkarte」の立ち上げの主な動機は、オーストリアでの e-ガバメントの導入であった。このイニシアティブを促進するために、オーストリアの「Bundeskanzleramt」（首相府）はすべての基本ソフトウェアおよび必要なライセンスを無料で提供している。認証局（CA）および登録局（RA）として、IC カード用署名の A-Trust やモバイル署名（いわゆる A1 署名）の Austrian Telekom 社などの民間プロバイダーが利用されている。

*費用*：カードおよび署名の費用は A-Trust のウェブサイト[10]で見ることができる。価格構造は購入できるそれぞれのサービスによって異なる。一般には次の費用が適用される。

- 30 ユーロ－証明書なしの署名プレミアム・カード
- 12 ユーロ－登録および証明書の発行が 1 回
- 証明書の延長に対して毎年 15.6 ユーロ

*利用*：オーストリアは e ガバメントの先導者と見なされているものの、経済的な視点から見れば発行されたデジタル署名の数はまだ限定されている。2005 年末までに発行された電子署名はわずか 70,000 件である。（オーストリアの人口の 0.7%）[11]。電子署名は、2006 年の最初の時点で依然としてあまりに高額、複雑で実用性が低すぎると考えられていた。初期の採用者は別のオペレーティング・システムを利用していることが極めて多かったため、Windows でしか利用できない点も欠点と考えられていた。

2006 年 1 月、A-SIT トラスト・センターは、クオリファイド証明書が売れなかったため、危うく支払不能[12]を発表しなければならなくなった。

**e パスポート**：オーストリア政府は、2006 年夏からオーストリア国民が利用できる新たな電子パスポートを発表した。このパスポートには、冊子内表紙の 1 つのページにマイクロチップが埋め込まれている。この IC には、パスポートに書かれたほぼすべてのデータが含まれており、所有者の顔のスキャン・データも含まれている。このパスポートには、コピー防止のメカニズム、デジタル署名、暗号化伝送コードも備わっており、権限のない関係者はパスポートに含まれた情報を

[10] Costs of certificates and cards in Austria http://www.a-trust.at/html/preisinfo.asp
[11] Signature usage in Austria http://www.heise.de/newsticker/meldung/68944
[12] Heise News, 27.1.2006,
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/68944&words=%D6sterreich%20Signatur

読み取ることができない。市民にとっては、新しい文書の導入はそれほど大きな変化をもたらしていない。有効な古いパスポートは有効期限まで提出する必要がありません。新しいパスポートの価格は、大人は 69 ユーロ、子供は 26 ユーロで据え置かれる予定である。

**銀行**：オーストリアは、2005 年 1 月に、市民カードを銀行のクレジット・カードに統合する可能性を市民に提供する世界で最初の国となった。財務省と銀行クレジット・カードの発行者であるユーロペイの合意の後、オーストリアで発行されるマエストロ銀行のすべてのクレジット・カードに「市民カード」の機能を組み込むことが可能になる。利用可能な機能（銀行クレジット・カードのマイクロチップに保存されたデジタル署名）によって、すべての市民はマエストロ・カードを利用して自分の身分証明およびオンラインでの安全な取引を行うことができる。

*費用*：マエストロ・カードの所有者は、2004 年 8 月 31 日まで、現在のカードをデジタル署名が含まれた新しいカードと無料で交換することができた。この日以降、この「プレミアム」機能には年間 12 ユーロの費用がかかる。このカードは、インターネットおよびカード・リーダーと接続された PC と併せて利用しなければならない。このサービスの理解を高めるため、200,000 台のリーダーが販促価格で提供された。取引に関連する e ガバメント・サービスの受容を促進することに加えて、銀行／市民の一体型カードでは、ビジネス間（e-ビジネス）およびビジネスと消費者の間（e-コマース）でのデジタル署名の利用を促進することになっていた。

**e ヘルス：e カード**（電子健康保険カード）の全オーストリアでの普及キャンペーンは 2005 年 11 月に成功裏に完了し、ついに紙ベースの医療カード証明書に取って代わりた。約 800 万枚の e-カードが送付された。e-カードでは、**市民カード**の機能を有効化することが可能であり（無料）、したがって追加的に e-ガバメント・サービスで利用することができる。この IC カードには、所有者の氏名、肩書き、生年月日、社会保険番号などの行政上のデータが含まれている。このカードには最新のデジタル署名機能も含まれており、認可を受けた所有者は政府機関に対する電子手続きにカードを利用することができるようになる。

*利用*：2006 年 10 月までに約 820 万枚の e-カードが発行された。が、無料であるにもかかわらず、市民カードに対する最新の署名証明書によってこのカードの機能を強化する選択肢を選んだ人はわずか 8,500 人しかいない[13]。

**モバイルによる身元確認**：2004 年 4 月、モバイル通信事業者である mobilkom austria 社は A1 SIGNATUR、*e-ガバメントのためのモバイル身元確認サービス*を立ち上げた。このサービスでは、e-ガバメントの利用者を携帯電話経由で身元確認／認証することが可能であり、またオーストリア国民は、市民カードやソフトウェア・ベースのデジタル署名を所有する必要なく、文書にデジタルで署名し、政府に対する手続きを安全に行うことができる。

### 3.1.2　ベルギー

**eID**：ベルギーの e-ID カード[14]には、所有者の個人データとデジタル証明書が保存されたマイク

[13] Heise Online News, 17.10.2006, http://www.heise.de/newsticker/result.xhtml?url=%2Fnewsticker%2Fmeldung%2F79618&words=elektronische%20Signatur

[14] Belgian e-ID card http://www.belgium.be/ and http://www.rijksregister.fgov.be/

ロチップが埋め込まれており、遠隔認証が可能である。2003 年から 2004 年に行われた約 70,000 枚のカードの 11 地方自治体（コミューン）への試験配布が成功した後、次にベルギーの残り 578 の地方自治体が 2009 年末までにこの移行を完了しなければならない。すべてのベルギー国民はこのときまでに電子 ID カードを所有することが求められる。ベルギーの e-ID カードと互換性のある数多くのアプリケーションとサービスが 2005 年にすでに利用可能であった。これには、オンライン所得申告、認定 E メール、オンラインでの公式文書の要求、インターネット・バンキング・サービス、電子図書館サービスなどがある。

現在配布されているベルギーの e-ID カードは、第 1 世代のカードのみである。第 2 世代のカードは 2007 年末まで、第 3 世代のカードはその後発行される予定である。この 3 段階の展開に沿って、ADAPID（フランドル地方における電子 ID カードのための先進的アプリケーション）プロジェクトでは、第 1、第 2 世代の e-ID カードのセキュリティおよびプライバシーの問題を調査し、第3世代のためのより適切な設計およびe-ガバメントとe-ヘルスのための先進的アプリケーションを提案する予定である。2009 年 6 月 30 日まで続くこのプロジェクトでは、数多くのプライバシー要件に取り組む予定である。

現在、約 400 万枚の eID カードが発行されており、350 万枚が有効化されている。市民は、e-ID カードの署名機能と認証機能の無効化を要求することができる。しかし 1 度無効化されると、再び有効化することはできない。ベルギーの PKI インフラストラクチャーおよび署名と認証の証明書に関する詳細は、「ベルギーの eID カードの専門事項」[15]に関するプレゼンテーションでいくつか見ることができる。

ベルギーの eID カードは、専門的には、異なる 3 つの 1024 ビット RSA 署名プライベート鍵（FIDIS-D36）を保持している。1 つは市民の認証、1 つは署名、1 つはカード自体の身分証明をベルギー政府に対して行うためのものである。eID カードは、3 つのプライベート鍵をすべて利用してデジタル署名を演算処理することができる。市民の認証鍵と否認防止署名鍵については、所有者が暗証番号を入力した後にのみこれが行われる。この暗証番号は市民が入力しなければならず、信頼できる何らかのハードウェア（例えば、独立型キーパッドが付属したスマートカード・リーダー）を利用するのが望ましいとされている。最初の 2 つの鍵ペアにはそれぞれ証明書が添付されている。これらの証明書は市民に対して発行される。すなわち 1 つの認証証明書は、例えば SSL/TLS に対する利用者の認証に使用するためのものである。2 つ目の証明書は、手書きの署名に等しい電子署名を生成するために使用できるクオリファイド証明書である。これらの証明書のいずれにも市民の E メール・アドレスは含まれていない。カードの第 3 の鍵ペアのプライベート鍵は、カードが相互認証のために国営登録所（RRN）と通信を行うときに利用される。（例えば、カード所有者の詳細（典型的には住所）、国の証明書などを更新するため）。RRN は、この第 3 の鍵によって算出された署名を照合するために、公開鍵のコピーをデータベースに保存している。それぞれの eID カードは、ベルギーのルート CA の証明書の真正のコピーによって初期化されているため、このカードは「信頼できるソース」として利用できる。すなわち、各利用者は、ベルギ

[15] Technical information on the Belgian ID card, http://homes.esat.kuleuven.be/～decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf

ーのルート CA の証明書を自分のスマートカードから読み込むことで、ベルギーの PKI システム内の信頼の連鎖を立証することができる。したがって eID プロジェクト全体は、各市民が地方自治体に自ら出頭しなければならないので、発行段階で確固たる利用者認証を行った全国的な PKI と見なすことができる。eID カードに関連するすべての証明書は、Belgian Post Group とベルギー最大の電気通信事業者である Belgacom 社の合弁事業である Certipost consortium によって発行される。

*費用*：費用については、新しい ID カードの配布を担当するコミューンは、従来の ID カードが現在 5 ユーロから 7 ユーロであるのに対して、eID カード 1 枚につき 10 ユーロから 15 ユーロを市民に請求することができる。この新しい文書は 10 年ごとではなく 5 年ごとに更新しなければならなくなり、これによっても費用負担が増加して事実上価格が 4 倍になっている。コミューン自体は、従来の型で要求される 4 ユーロではなく 10 ユーロを連邦政府に支払わなければならなくなる。これらの費用を消費者に転嫁するかどうかは、個々のベルギー・コミューンの判断に任されている。すべてのベルギー国民は、2009 年末までに電子 ID カードを所有することが求められる。

*利用*：ベルギーの最近の調査（2006 年）では、ベルギーのインターネット利用者の 43%は eID カードを現在所有しているものの、電子カード・リーダーを所有しているのはわずか 8%であることが明らかになった。その結果、eID カードが提供する可能性の多くは活用されていない。行政事務簡素化担当大臣は、ベルギーの電子 ID カードによって可能になったサービスの利用を増加させるため、行政事務簡素化の本部であるカフカ・コンタクト・ポイントと連絡を取って 5,000 台の eID カード・リーダーを無料でベルギー国民に配布することを発表した。eID カードに関連した試験プロジェクトを導入する地方の行政機関やコミューンも無料のカード・リーダーを受け取る。

**e パスポート**：2004 年 11 月にベルギーは、国際民間航空機関（ICAO）の提言に準拠した電子パスポートの発行を世界で最初に開始した。このバイオメトリック・パスポートには、所有者の顔の画像が保存されたマイクロチップが埋め込まれている。欧州で適切な立法が行われた後、指紋が後の段階で追加される予定である。

### 3.1.3　チェコ共和国

チェコ共和国は、信頼性がありかつ安全な e ガバメント・サービスを市民に提供する試みの一部として、2006 年 7 月に電子署名と電子スタンプの認証サービスを導入した。チェコの IT 省は、すべての政府機関が法律で要求される要件（電子形式の提出物の受け取り、電子アドレスへの文書の送付、電子形式での行政活動の発表など）を満たすことができるように、すべての公共団体に効果的な認証システムを供給したいと考えている。市民、自然人、法人は同じ技術にアクセスできなければならない。現在、彼らは財政およびその他の行政手続きのためにそのシステムを利用している。

**電子署名**：2006 年 7 月、次の 3 つの組織が新しい電子署名および電子スタンプの発行を委託された。認証局（Prvni certifika?ni autorita a.s.）、eIdentity 社、Czech Post である。これらの機関は、単純な PostSignum VCA 証明書、クオリファイド PostSignum QCA 証明書などのいくつかの種類の認証証明書を発行する。

チェコの労働社会政策省は現在、数多くの IC カードを利用している唯一の国家機関である。同省の eID は、主に省の情報システムへのアクセスや省内の機密情報のやりとりに利用されている。

### 3.1.4 デンマーク

**電子署名**：デンマークは電子 ID カードや電子身分証明書を提供しておらず、提供する意向もありません。2003 年 2 月以降、デンマーク政府は利用者認証の手段として「無料のデジタル署名」を市民に提供している。そのコンセプトは一般に「公共のデジタル署名」と言われており、これによって市民はオンラインの公共サービスを安全な方法で利用することができる。

このデジタル署名プロジェクト[16]は、デンマークの e ガバメント・プログラムの一部として開始され、このプログラムは公共部門の近代化と発展への要求の高まりに応えるために立ち上げられた。デジタル署名プロジェクトの目標は、公開鍵基盤に基づく、オープンで拡張可能なセキュリティ・インフラストラクチャーを確立すること、またデジタル署名のための効果的な登録手続きおよび配布の仕組みを市民、企業、行政機関に対して確立することである。このデジタル署名プロジェクトは、科学技術革新省と TDC（デンマーク最大の電気通信企業）間の官民の提携として組織されている。TDC は、デジタル署名の確立、発行、維持管理を担当する認証局として活動している。TDC との官民の提携は、インフラストラクチャーと魅力的な電子サービスの維持管理および開発を確実に行うために確立された。

このデジタル署名はソフトウェア・ベースのデジタル署名であり、パスワードの使用が義務となっている。パスワードは、ウェブサイトへの入場管理、暗号化、および E メール、ウェブ・フォーム、ウェブ文書のデジタル署名に利用することができる。このデジタル署名は、個人の署名、被雇用者の署名、ビジネスの署名として発行されている。

*利用*：デジタル署名の導入によって、2005 年 5 月時点で合計 375,140 件のデジタル署名の発行がもたらされた。その内訳は、321,753 件が個人のデジタル署名、50,999 件が被雇用者のデジタル署名、2,388 件が企業のデジタル署名であった。2005 年 2 月時点で、デンマークの行政機関の 90%近くがデジタル署名を導入しており、安全な E メールを送受信するための適切な方法を確立している。2005 年 5 月 25 日時点で、デジタル署名を利用する電子サービスが 400 以上開始されている。

*費用*：デンマーク政府は、約 4,000 万デンマーク・クローネ（570 万ユーロ）を費やしてデジタル署名の普及キャンペーンをサポートし、その一部は TDC が最初の立ち上げのパートナーを手助けするために利用した。証明書は無料である。

**e ヘルス**：デンマークには、市民ごとに生涯利用する単一の患者番号が存在する。すべての薬品、臨床所見、医師の処方箋は、公法で管理されているメドコムが運営する中央データベースに保存される。医師と薬剤師は、それぞれ読み書きすることが認められている。患者は自分のデータをインターネット経由で読み、そのデータに誰がアクセスしたか確認できる。が、これはメドコム

[16] Digital signature project in Denmark
http://www.egov-goodpractice.eu/gpd_details.php?&gpdid=1786#descriptionsection

のデジタル署名証明書を持っている場合に限る。

### 3.1.5　エストニア

IDABC[17]の分析によれば、欧州全体における ICT および e-ガバメントの展開という点では、エストニアは 2003 年にすでに最も先進的な国の 1 つであると広く見なされていた。

**eID**：エストニアは 2002 年 1 月に国の ID カードを発行し始めた。このカードはエストニアのデジタル署名法の要件を満たしており、すべてのエストニア国民および 16 歳以上の永住権を持つ外国人にとって義務となっている。このカードは市民および居住者の身元を確認する主要な文書となるように作成されており、その機能はビジネス、政府関連または個人のあらゆる形式の通信に使用することができる。市民権・移民委員会（Citizenship and Migration Board）が発行するこのカードは、身分証明書および旅券（EU 内）として 10 年間有効である。このカードは、物理的な身分証明書であることに加えて、公共および民間のオンライン・サービスに対して安全な認証および法的拘束力のあるデジタル署名を手助けする高度な電子機能も備えている。

2003 年 3 月に立ち上げられたエストニアの e ガバメント・ポータル[18]は、公共のオンライン情報およびサービスに対する単一のアクセス・ポイントを提供している。このポータルは、国の ID カードによる認証を通じて、電子フォームを記入・提出し、個人データにアクセスし、手続きを行う可能性を利用者に提供している。

電子プロセッサーIC には個人データ・ファイルならびに認証のための証明書（公共部門との電子通信のための不変の E メール・アドレス*名. 姓@eesti.ee* が伴う）およびデジタル署名の証明書が含まれている。この証明書には、所有者の氏名と個人コード（国の ID コード）のみが含まれている。また、認証証明書には所有者固有の E メール・アドレスが含まれている。このデータ・ファイルは ID カードと同じ期間有効である。デジタル証明書は 3 年間有効で、無料で更新することができる。が、ID カードの有効期間より長くすることはできない。2006 年 10 月で 100 万枚の ID カードが発行されている。

2003 年、フィンランドとエストニアは、デジタル署名、文書形式および文書交換について 2 国間のコンセプトとプラクティスの調和を図る協定に署名した。OpenXAdES とコードネームを付けられた両国の署名プロジェクトは、「普遍的なデジタル署名」を促進するオープン・イニシアティブである。

「コンピューター保護 2009 年」のイニシアティブでは、エストニアを 2009 年までに世界で最も安全な情報社会の国にすることを目標としている。この目標を達成するために、数多くの副プロジェクトが立ち上げられる予定で、優先分野の 1 つは電子サービスの利用における ID カード・ベースの認証の促進となっている。エストニアは、電子 ID ベースの認証およびデジタル署名において確立したプラクティスを持つ欧州国家である。エストニア国民は、2005 年 10 月の地方政府の選挙において、安全な ID カードを認証メカニズムとして使用して電子的に投票することができした。2009 年までには、電子認証における ID カードの利用が 20 倍増加すると予想されている。

---

[17] IDABC eGovernment Factsheet - Estonia - National Infrastructure, http://ec.europa.eu/idabc/en/document/5900/391

[18] Estonia eGovernment portal eesti.ee

*利用*：国の ID カードに加えて、エストニア居住者はインターネット・バンキングの身分証明データを利用してオンラインの公共サービスにアクセスすることもできる。（エストニア居住者の 70%超がインターネット・バンキングを利用しており、これは欧州で最も高い比率である。）。PIN コードの盗難や紛失があった場合は、サポート・ライン（1777）に電話することができる。
*費用*：ID カードの発行費用は約 9.70 ユーロである。[19]。

### 3.1.6　フィンランド

**eID**：フィンランドは電子 ID カード（*FINEID* [20]カード）を欧州で最初に発行した国であった。1999 年12月7日、応用段階を開始する1つの方法として第1号カードがフィンランド首相に贈られた。このカードは公開鍵基盤（PKI）および証明書に基づいている。この ID カードは、フィンランドのあらゆる国民または永住者に与えることができる。FINEID プロジェクトは、オープンで無防備なネットワークにおいて公式の手続きを安全に行う手段を提供するインフラストラクチャーの構築を目標としていた。

*市民証明書*は、警察が発行する IC 式の ID カード、銀行のクレジット・カード、または携帯電話の SIM カードに組み込むことができる。市民証明書は、政府職員の証明書と同様、電子取引、E メール、文書の暗号化における確実な身分証明書、および電子署名として利用することができる。

技術的なデータに加えて、このカードの IC には住民登録センター[21]（PRC）のいわゆる認証局証明書およびカード所有者の身分証明書と署名証明書が含まれている。PRC は認証局の役割を果たしており、FINEID の証明書を発行している。PRC は現在のところ、フィンランドにおけるクオリファイド証明書の唯一のいわゆる認証局であり、電子署名に関する法律および関連する EU 指令で規定されたとおりに全欧州の証明書を発行することができる。PRC が発行した個人の証明書は、すべてクオリファイド証明書である。

カード所有者の証明書に含まれる唯一の個人データは、名、姓および利用者の固有の電子識別子（SATU）である。すなわち、所有者の個人 ID 番号、住所、生年月日またはその他同様の情報は IC に保存されていない。SATU は、個人の ID 番号とは異なり、所有者について何も表さないシリアル・ナンバーである。FINEID の証明書方針に従って発行される証明書は、証明書所有者の身元を認証し、デジタル署名およびデジタル文書の信頼性またはその他のデジタル･データを検証し、さらに電子通信、電子取引または電子データの転送の機密性を確保するためのものである。

PRC は PKI ベースの証明書を発行している。第 1 の鍵ペアは認証および暗号化のために、第 2 のペアは電子署名のために利用される。鍵の使用は合致する PIN コードでのみ可能である。PIN コードが鍵を有効化し、その後 IC は必要な計算オペレーションを提供できるようになる。プライベート鍵は証明書の所有者のみが（例えば ID カードの IC 上に）保有し、PIN コードを入力してはじめて利用することができる。が、このときでもカードから読み取ることはできない。PIN コードを知るのはカード所有者のみであり、所有者は必要な場合にそれを変更することができる。

---

[19] Estonia rates of state fees http://www.mig.ee/eng/state_fees/
[20] FINEID technical information www.fineid.fi
[21] Finnish Population Register Centre,
http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/index_eng

PIN コードの入力を 3 回間違えるとカードがロックされる。

FINEID カードの申請は、地域の登録局の役割を果たす警察当局または警察から権限を与えられた団体に本人が出向いて行いる。電子 ID カードは地域の登録局から本人が受け取らなければならず、このとき申請者の身元が再度確認される。

利用者の電子識別子は、例えば警察が ID カードを発行したときに市民証明書として有効化される。次に市民証明書が ID カードの IC に埋め込まれる。市民証明書は銀行のデビット・カードおよび／またはモバイル機器の SIM カードに添付することもできる。どの市民も有効な市民証明書を同時に何枚か所有することができる。しかし、それらの証明書にはすべて同じ利用者電子識別子がついている。証明書の情報内容およびその信頼性は、認証局の電子署名によって検証される。住民登録センターの商標は、公共の市民証明書を利用するオンライン・サービスを利用者が発見・識別する上で役立つ。

*利用*：FINEID カードの初期の受け入れ方は非常にゆっくりとしたものであった。[FIDIS-D36]。2000 年の立ち上げ以来､2003 年中頃までに約 500 万人のフィンランド国民のうちわずか約 16,000 人しかカードを購入しなかった。12 月末までには合計で 96,100 人に市民証明書が発行された。このうち、81,300 の市民証明書が有効化された。14,900 人は健康保険の情報を自分の ID カードに組み入れた。フィンランド政府の目標は、2007 年末までに 200 の eID サービスが利用できるようにすることである。

市民証明書は 2006 年 9 月末までに合計で 120,500 人に発行された。このうち、104,100 の市民証明書が有効化された。22,900 人は健康保険の情報を自分の ID カードに組み入れた。

*費用*：ID カードの費用は 40 ユーロで 5 年間有効である。

**モバイル**：市民証明書は SIM カードに組み入れることが可能で、これによって携帯電話利用者は単一のコードで簡単に身分証明を行うことができる。利用者の身分証明に加えて、この証明書によって、認証、交換されるデータの機密保持、および情報の整合とメッセージの送付を確実に行うことができる。

2005 年以来、フィンランドの住民登録センターは、インターネット上で公式の手続きを行うための革新的なソリューションを市民に提供しており、これによって市民は、オンラインのサービスや要求のために確実な身分証明書が必要なときに携帯電話を利用できる。モバイル署名で必要なセキュリティ証明書が備えられた最初の SIM カードは、フィンランドで 2 番目に大きなモバイル・ネットワーク事業者である Elisa 社から提供されている。この基礎となるのは、国際的な技術企業グループである Giesecke & Devrient 社（G&D）の署名機能および暗号化メカニズムが備えられた UniverSIM 製品ラインである。Elisa 社は、フィンランドの住民登録センターと協力して携帯電話経由で利用者の身元を確認するこの新しいサービスを提供する最初の事業者である。市民証明書は G&D の SIM カードに保存される。これはモバイル・セキュリティ・アーキテクチャー（公開鍵基盤）の一部であり、身元確認に要求されるセキュリティと独自性を確実に実現する。例えば市民が新しい住居へ引っ越したことをオンラインで登録したいときには、インターネットで該当するページを開き、フォームに記入して、オンラインの要求に対してモバイル署名の入力を求める登録事務所からのメッセージを携帯電話で受け取る。この市民は、個人の暗証番号を入力してデジタル署名の生成を許可する。デジタル署名は SIM カードによって生成され、暗号化さ

れた特別なメッセージとして登録事務所に返信される。公式の手続きに携帯電話でのデジタル署名の使用を望む市民は、地域の警察署で登録しサービスを申し込むことができる。統合的なセキュリティ証明書が備えられた G&D の SIM カードは Java™技術に基づいており、128Kb の記憶容量がある。このカードは現在、Elisa 社の指定販売店で入手できる。

**政府職員カード**：2006 年、政府職員のための IC 式の ID カードがフィンランドの中央政府全体で採用されつつある。[22]。この写真付きの ID カードには、情報ネットワークにログインするための身分証明、ネットワーク利用者およびその利用権限の認証、E メールおよびその他の文書の暗号化、拘束力がありかつ疑いの余地のない電子署名の提供をフィンランドの法律で規定されたとおりに可能にするクオリファイド証明書が含まれている。これらの政府職員証明書はアクセス・コントロール・システム、在宅勤務、通行管理、物理的な身元確認にも利用できる。この ID カードと証明書はフィンランドの住民登録センター（PRC）で作成され、カードは Setec 社が提供している。政府職員証明書は、国民が入手可能なクオリファイド証明書（または市民証明書）と同様に、フィンランドの証明書インフラストラクチャーの一部となっている。

**認証システム**：フィンランドは、フィンランドの地方自治体の ID 認証システム間の相互運用性の問題を解消するために、すべての中央政府および地方政府の機関のための安全な単一の認証標準規格への切り替えを 2006 年前半に準備している。以前は、地域の個々の機関が独自の ID 照合システムについて供給業者と交渉していた。その結果、それぞれのシステムは互換性がありませんであった。情報技術インテグレーターの Fujitsu Services 社がフィンランドの行政機関に電子認証ネットワークを提供している。この新しいシステムは、政府のあらゆる電子アクセス・サービスのための調和のとれたウェブ認証および支払機能を行政機関と市民の両方に提供し、さらには銀行支払の照合システムに接続される予定である。

**e ヘルス**：*Kela Card* [23]（個人の健康保険カード）の目的は、薬局で薬品を購入するときにフィンランドの社会保障を受ける資格があるかどうかを証明することにある。もし望めば、健康保険に関する情報は ID カードに組み入れることも可能で、この場合 ID カードは別の Kela Card に取って代わる。オンライン・サービスでは、この ID カードはコンピューターに取り付けられた読取装置およびカード・リーダー・ソフトウェアとともに使用される。

### 3.1.7　フランス

**eID**：CNIE（Carte Nationale d'Identite Electronique）と呼ばれる eID カードの計画は、INES プログラム（Identification Nationale Electronique Securisee）の一部として 2003 年に初めて発表された。

プロジェクト INES（「Identite Nationale Electronique Securisee」すなわち「安全な国営電子身分証明書」）は 2005 年 4 月 11 日に公式に承認された。INES プロジェクトでは、とりわけ、ID カードおよびパスポートを要求する手続きを統合、保護、簡素化し、身分証明書の管理を改善し、e-ガバメントおよび e-コマースのサービスの受容を促進することが期待される電子署名を市

[22] Finnish Government Employees get chip ID card, October 2006, http://www.fineid.fi/vrk/bulletin.nsf/HeadlinesFineidEng/A25EC94E8F7395B0C22571FD004232A4)
[23] Kela Card, http://www.kela.fi/in/internet/english.nsf/NET/171203103605MH?openDocument

民に提供する予定である。将来の e-ID カードと e-パスポートの両方が、「非接触」無線 IC タグ（RFID）のマイクロチップに保存された所有者の個人情報およびバイオメトリック識別子を組み込む予定である。将来の ID カードおよびパスポートに含まれた個人情報は、新しい共通のデータベースに保存され、一方バイオメトリック・データは別のファイルに匿名で保存される。このプロジェクトの調達活動は、2005 年中にカードを開発・試験し 2006 年に配布を開始する見通しの下、もともとは 2004 年末よりも前に開始される予定であった。報道によると、e-ID カードの配布は現在では 2007 年に開始される予定である。

政府が 2008 年までに「電子行政」に移行することを支援して、2005 年 12 月 6 日に法令が発布された。この法令ではまた、すべての行政機関が電子情報の交換のために安全で相互運用可能なシステムに移行するという要件が定められている。

**e ヘルス**：電子健康保険 ID カードの Vitale は 1998 年に導入され、現在は最新版に更新されているところである。最近、フランスの医療サービス組織である SESAM-Vitale は、すでに確立された Vitale 医療「スマート」カードの新規かつ最新版の製作を 3 社の工業会社に委託した。新しいカードは、カード所有者の写真およびサービスとデータの新しい管理特性を組み込んで、今後 2 年間で少なくとも 2,400 万枚作成される予定である。フランスの健康保険パートナーが、メンバーのために技術的なソリューションを開発するために設立した SESAM-Vitale は、次世代の健康保険カードを供給する契約を Gemplus 社、Axalto 社、Oberthur Card Systems 社に発注した。現在流通している 5,300 万枚のカードと段階的に置き換わる新しいカードは、より使いやすく、データ管理がより安全になるように設計されている。最初の新世代カードは 2006 年 11 月から入手できるようになる予定である。

### 3.1.8　ドイツ

**戦略**：連邦政府のイニシアティブにおいて、ドイツでの電子署名の利用促進を目標に、官民の「*署名連合*」[24]が 2003 年 4 月 3 日にベルリンで設立された。連合のパートナーは、共同宣言において、特にアプリケーションおよび製品の技術的な標準規格、複数の機能を持った IC カードの利用、共通のセキュリティ基準、先進的かつクオリファイドな電子署名の利用について合意した。

ドイツ連邦政府によって e カード戦略[25]が 2005 年 3 月 9 日に発表された。政府は、将来の電子健康保険カードおよび ID カードを単一の共通な文書に結合し、市民が e-ガバメント・サービスに簡単にアクセスできるようにすることを提案した。e カード戦略では、利用者の身元確認、社会保障に関する情報、健康保険サービスの分野における数多くの e-ガバメント・イニシアティブに共通の戦略的枠組みをもたらすことを目標としている。この共通戦略では、連邦政府のさまざまな e-カード・イニシアティブ（電子健康保険カード、e-ID カード、求職カードなど）ならびに重要なデータベースおよび社会保障と税務上の手続きの分野におけるサービスへのアクセスを協調させる。この戦略では特に、取引に関連する e-ガバメント・サービスの開発と受容を促進し、

[24] German "Signature Alliance": http://www.signaturbuendnis.de/englisch/index.htm

[25] German eCard-Strategy
http://www.bmwi.de/BMWi/Redaktion/PDF/E/ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf and http://www.heise.de/english/newsticker/news/57333

効率の向上と費用の節約を最大にするために、共通の基準を定めている。

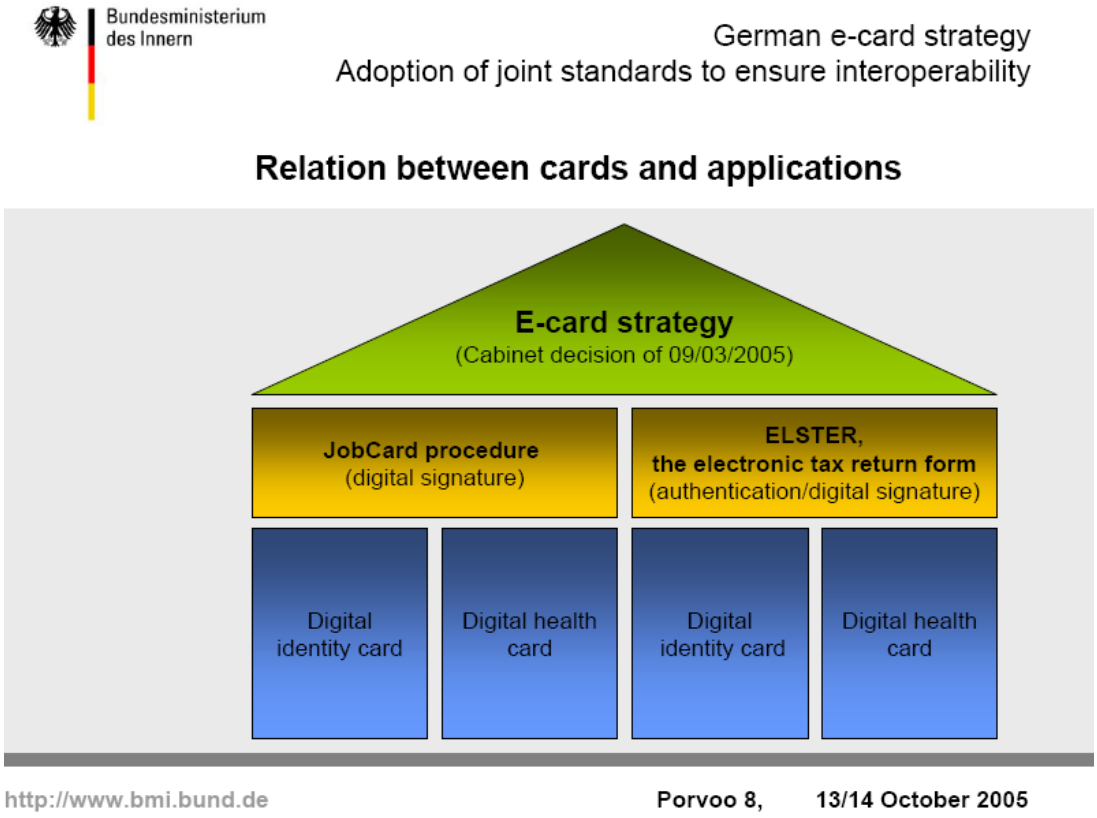



Figure 4：German E-card strategy (Source：www.bmi.bund.de)

ドイツの連邦政府による「*e ガバメント 2.0*」[26]プログラムは 2006 年 9 月に立ち上げられた。このプログラムでは現在と 2010 年の間の主要な活動が計画されている。e ガバメント 2.0 は、EU の i2010 イニシアティブの e ガバメント活動計画ならびにドイツ自身の BundOnline 2005 および Deutschland-Online の経験に基づいている。戦略的目標には、電子 ID カードの導入および eID のコンセプトの策定から構成される「*身分証明書*」、および市民、企業、行政のための安全な通信基盤で構成される「通信」が含まれている。

**電子署名**：T7 e.V. [27]は、E メールの安全な交換、電子署名の応用および IT セキュリティ管理（これらはすべて公開鍵基盤に基づくソリューションを必要とする。）を対象とした、デジタル署名のためのドイツのトラストセンター・ワーキング・グループである。これらを E-ガバメント・アプリケーション、および行政機関、産業、金融部門による利用のために導入するのをサポートするために、TeleTrust は T7 グループと共に相互運用可能なソリューションの開発および試験のため

[26] eGovernment 2.0
http://www.kbst.bund.de/cln_011/nn_998588/SharedDocs/Publikationen/Themen/eGovernment/egov__2__0,templateId=raw,property=publicationFile.pdf/egov_2_0.pdf (in German) and
http://ec.europa.eu/idabc/en/document/5887/194

[27] T7 e.V. http://www.t7-isis.de/index.php?id=190&L=1

の基礎的な要素を開発した。このワーキング・グループは、一般市民にとって包括的かつ調整がとれた形で公開鍵基盤の複雑なテーマを紹介する手段を考案している。この団体に加入するには、加入を希望する企業がすでに認定された証明書サービス・プロバイダーであるか、または 1 年以内にそれになることが求められる。

PKI：ドイツ署名法[28]、署名法令[29]、およびその他関連する文書と詳細では、セキュリティ・コンセプトが検証・確認されており、試験され確認された技術要素のみを利用する証明書サービス・プロバイダーだけが活動を開始することが確認されている。連邦ネットワーク局[30]は、マインツの事務所でクオリファイド証明書サービス・プロバイダー（トラスト・センター）を認定し、認定されたプロバイダーを監視し、これらに鍵の証明書を発行し（次に最終消費者に鍵の証明書を発行する必要がある。）、トップレベルの国営 CA すなわちルート CA を運営している。この機関は、証明書団体の認定だけでなく、すべての公認証明書サービス・プロバイダー（クオリファイド証明書／署名について）の監督にも責任がある。個々のサービス・プロバイダーの組織構造全体および業務の流れ、スタッフの資格および信頼性、そして財源（単に一時的な状態でない自立的運営が保証されなければならない。）すらが認定（認可）を与えられる前に調査され、調査はその後 3 年ごとに行われる。署名法が意味する範囲内での「クオリファイド」署名は、法的拘束力のある手書きの署名と同等であると見なされている。ドイツでは、IC カード自体（オペレーティング・システムなども含まれる。）だけでなく、例えば鍵の生成装置も認定の一部として調査・評価される。証明書サービス・プロバイダーのリストは連邦ネットワーク局によって公表される。[31]。

*利用*:電子署名を促進するさまざまな戦略にもかかわらず、利用率はまだかなり低い状態である。この理由により、2005 年に認定トラスト・センター（TC トラストセンター）が支払不能を発表した。[32]。今のところ GeoTrust 社が TC トラスト・センターを引き継ぎ、業務を続けている。

*費用*：クオリファイド認定書および先進的証明書は 3 年間有効で、D-Trust トラスト・センターでの費用は 160 ユーロである。トラスト・センターは、それぞれ独自の製品および価格戦略を持っている。

| | Issue of a certificate | Basic fee per year | Sum of a 2-year usage |
|---|---|---|---|
| D-Trust GmbH | 41 € | 29 € | 99 € |
| Deutsche Post Signtrust | 0 € | 39 € | 78 € |
| TC Trust Centre | 8 € | 62 € | 132 €[33] |
| T-TeleSec | 23,57 € | 42,95 € | 109,47 € |

[28] Signatures Act, http://www.bundesnetzagentur.de/media/archive/3612.pdf
[29] Signature Ordinance, http://www.bundesnetzagentur.de/media/archive/3613.pdf
[30] Bundesnetzagentur
http://www.bundesnetzagentur.de/enid/8d729ce18edfa60e990fa549b004f713,0/Technical_Telecoms_Regulation/Electronic_Signature_z2.html
[31] Certification Service Providers in Germany,
http://www.bundesnetzagentur.de/enid/8d729ce18edfa60e990fa549b004f713,0/Electronic_Signature/Certification-Service_Providers_2u2.html
[32] http://www.heise.de/newsticker/meldung/64224

Figure 5 : Price strategy of four major German trust centers (Source [FIDIS-D32])

**銀行**：SparkassenCard[33]は、2005 年時点で、クオリファイド電子署名の証明書を組み込むことができる最初の銀行クレジット・カードであった。クオリファイド証明書の費用は、有効期限によって異なる。例えば 1 年以下の有効期限については 19.95 ユーロで、3 年を超えると 79.00 ユーロである。


Figure 6 : Banking Card with qualified certificate (Source : S-Trust)

**eID**：2006 年 9 月、証明書に基づいて認証およびデジタル署名をサポートする、2008 年に開始される電子 ID カードの発行をドイツが計画することが決定された。この決定は e ガバメント 2.0 戦略の一部である。

**外国人カード**[34]：2006 年 10 月に発表されたように、ドイツ国民のために計画された eID カードと同様、電子式「外国人カード」がドイツの在住許可証と間もなく取って代わる可能性がある。電子式外国人カードによって、電子 ID カードがドイツ国民に提供する機能と似た身分証明機能が計画されている。外国人カードは、デジタル式の在住許可証に相当するものになるだろうが、写真や指紋などのバイオメトリック・マーカーも組み込まれるだろう。

**e パスポート**：IC に保存された写真という第 1 段階のバイオメトリクスが組み込まれた 300 万の e パスポートが 2006 年までに発行された。連邦政府機関は現在、パスポートに組み込むためのデジタル指紋を取る第 2 段階に移行している。

**e ヘルス**：連邦社会保健省は、ドイツ市民のために e ヘルス・カードの導入を計画している。医師と薬剤師はヘルス・プロフェッショナル・カードを受け取る予定である。このカードには例えば処方箋に署名するための電子署名が備えられている。

このプロジェクトの主な目的は、医療部門のすでに確立されたプロセスをデジタルでサポートすることである。重要な例として次のものがある。

- 患者が健康保険の被保険者であることを医師の事務所や病院で確認する（現在すでに IC カードでサポートされている）
- 医師が必要とする場合、アレルギー・データ、長期的な薬物治療、血液型、免疫証明書などの現在は紙に保存されている情報を移転する
- 他の医師への照会

[33] SparkassenCard, http://www.s-trust.de/index.htm
[34] eID and Foreigners' Card announcement, http://www.heise.de/english/newsticker/news/78862

・　処方箋および薬局での薬品の購入

認証および緊急用のデータは別として、カードに保存されているすべてのデータは暗号化され、利用者が管理する暗証番号で保護されている。利用者は、自分のカードに保存されたすべてのデータに対して自由に読み取りのアクセスができる。(例えば自分のカード・リーダーや公共の端末を使用してアクセスする。)。

照会や処方箋などのデータの移転に利用する場合、患者の e-ヘルス・カードのデータにアクセスするにはヘルス・プロフェッショナル・カードが必要である。e-ヘルス・カードの緊急用データは暗号化されている。が、e-ヘルス・カードの暗証番号を必要とすることなくヘルス・プロフェッショナル・カードでアクセスすることができる。

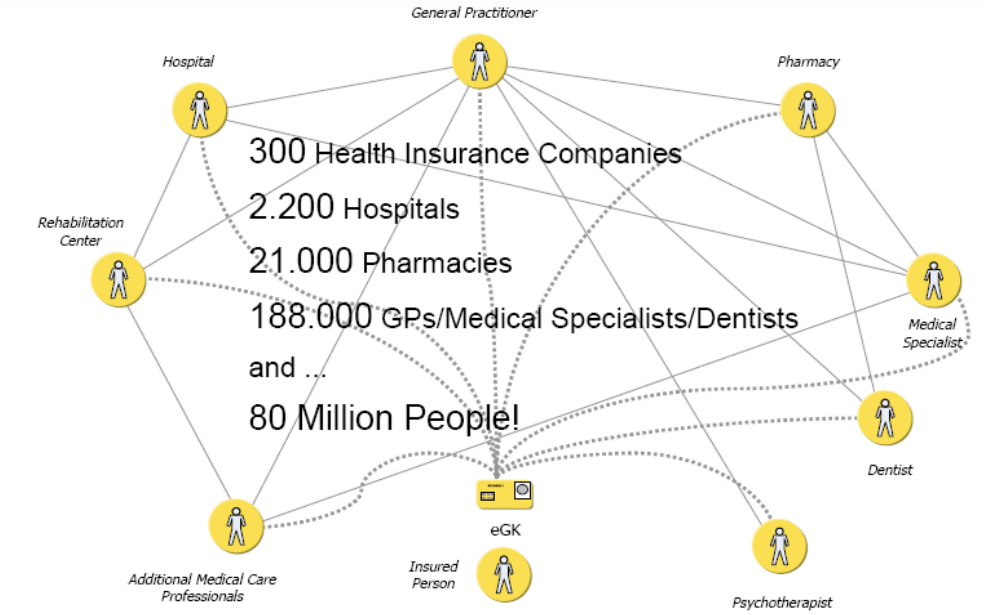



Figure 7 : Challenge eHealth (Source : Gematik)

e-ヘルス・カードの X.509 証明書の仕様に関するさらなる詳細は次のウェブサイトで見ることができる。

http://www.gematik.de/(S(utvcgh4515vgehassgaif1zf))/upload/gematik_PKI_X509_Zertifikate_des_Versicherten_eGK_V1_2_0_951.pdf (ドイツ語)。

### 3.1.9　ギリシャ

現在のところギリシャには e-ガバメントのための中心的な e-ID インフラストラクチャーは存在しません。特に、e-ID カードに対する計画は発表されていない。

### 3.1.10　ハンガリー

**電子署名**：ハンガリーでは、現在のところ中心的な ID インフラストラクチャーは整備されていない。しかし共通の身元確認／認証の枠組みが整備されている。この多層的なセキュリティの枠組

みは、身元確認および認証のための適切なメカニズムをさまざまなアプリケーションに提供している。ハンガリーの行政手続法およびその実行命令では、行政機関のさまざまなサービスのための身元確認および認証のプロセスが規定されている。異なる 2 つの場合を特定することができる。すなわち、パスワードによる認証、またはデジタル証明書による認証である。

2006 年 7 月、ハンガリーは新しい電子署名管理を立ち上げた。ネットロック KFT は、「上級証明書を発行する」権限、すなわち外国の電子証明書プロバイダーにライセンスを発行する権限を与えられた。このプロバイダーは、ライセンスを受けた後、有効な電子証明書をハンガリーで発行することができる。国立通信局が適切な登録命令を発すれば、ネットロックは行政事務で利用できる電子証明書を発行する最初の企業になる。

### 3.1.11 アイスランド

**電子認証**:電子身分証明書は、市民に電子サービスを提供する上で鍵となる役割を果たしている。したがってこのプロジェクトには高い優先順位が与えられており、2004 年から 2007 年の情報社会に対するアイスランド政府の方針である「すべての国民に役立つ資源」では、2007 年までに電子証明書を全面的かつ広範囲に利用することを目指している。

### 3.1.12 アイルランド

アイルランド政府の電子身分証明書管理体制は、現在核となる 2 つのコンセプトを中心に構築されている。すなわち公共サービス個人番号 (PPSN) と公共サービス・ブローカー (PSB) である。PPSN は、アイルランド人の子供が生まれたときに現在全員に強制的に割り当てられている固有の識別子である。PSB の職務は電子的なブローカー／ヘルパー／アシスタントである。PPSN を利用した公共サービス・カード (PSC) の普及キャンペーンも計画されており、これによって医療カード、社会サービス・カードなどのいくつかのカードの機能が 1 つにまとめられる予定である。

### 3.1.13 イタリア

**eID**：一連の e-ガバメント・サービスへのアクセスを提供しているスマートカードは、イタリアでこれまでに 1,310 万枚超発行された。国営サービス・カード (NSC) はすでに 930 万枚発行され、さらに 300 万枚発行されようとしている。が、政府関連のサービス利用のためのこれらのスマートカードが最大の割合を占めている。e-ガバメント・サービスへの安全なアクセスを利用者に提供するように設計された NSC は、イタリアの e-ID カードの「姉妹」カードである。NSC は、所有者の写真が含まれていないことを別とすれば e-ID カードと同じ特性を持っている。

イタリアの電子 ID カード（「Carta d'identita elettronica」または CIE）は、次の 3 つの主要な務めを果たする。すなわち、紙ベースの ID カードに取って代わるだけでなく、国際的な旅券となり、e ガバメント・アプリケーションにおける認証や身元確認を可能にする。

2005 年 4 月以降、Carta Regionale dei Servizi がロンバルディア地方で利用されている。このカードはデジタル署名をサポートし、銀行のクレジット・カードおよび e ヘルス・カードにもなる。とは言うものの、この地方の医師が導入したカード・リーダーはわずか数台である。

### 3.1.14 ラトビア

**eID**：ラトビア郵便局が認定電子署名カードの発行を開始した 2006 年 10 月 4 日、「電子署名」が正式にラトビアに到着した。この新しいカードを利用して、文書に電子的に署名し、さまざまなオンライン電子サービスにアクセスすることができる。ラトビアの e ガバメント事務局は、開発中のすべての電子サービスが立ち上がった後、このカードが広く利用されることを期待している。いくつかの機関ではすでに電子サービスを提供している。

税務省は、市民および企業が特別な契約に署名することを条件に利用できる独自の電子署名を持っている。しかしこれからは、全国的に安全な電子署名を代わりに利用することができるようになる。現在のところ、必要な申告と税金申告の約 90%が電子署名を利用して電子的に提出することができる。

*費用*：2006 年 9 月、ラトビアの e ガバメント担当大臣は、新しい電子署名カードのより広い利用を促進し、電子サービスの利用可能性を向上させるために、電子署名を導入した結果市民が負担する費用の一部に対して国の予算から資金提供することを提案した。民間人の 2 年間有効な新しい電子署名カードの費用は約 34 ユーロになり、一方個々のタイム・スタンプの費用はさらに 0.5 ユーロかかると見積もられている。

### 3.1.15 リトアニア

リトアニア政府は電子 ID カードをまだ発行していない。電子署名インフラストラクチャーは、民間部門で電子文書交換をサポートするために利用されている。

### 3.1.16 ルクセンブルク

市民およびルクセンブルクで設立された法人には固有の識別子が発行され、市民は従来の ID カードも所有している。現在のところ、特筆すべき段階に到達した電子 ID プロジェクトは存在しない。

### 3.1.17 マルタ

**eID**：マルタの「電子身分証明書」は 2004 年 3 月に開始され、個人の身分証明書を必要とするオンライン・サービスに安全にアクセスするために利用できる安全な**ネットワーク鍵**となっている。電子身分証明書の目的は、柔軟性と便利さを利用者に継続的に提供しながら、取引に関連する付加価値のある電子サービスの安全な提供を可能にすることである。政府はまた、個人データおよび機密データの送信を必要とするオンラインでの行政手続きに関する一般市民の疑念を減らす上でこれが役立つことを期待している。

「鍵」は各市民に発行され、これによって所有者が有効化したときにデータおよびサービスへのアクセスが可能になる。鍵がとり得る形態はさまざまであり、クレジット・カードやデビット・カードに見られるものと同様の暗証番号や長い番号などがある。機密性と責任を保証するために、鍵は政府ではなく民間団体によって発行・管理される。鍵の管理者は、各市民への鍵の割り当ておよび国内のすべての電子身分証明書のリポジトリー管理を担当する。

市民は、紙の ID カードのコピーおよび有効な E メール・アドレスを持って社会保障省の地区

事務所に本人が出頭することで、電子身分証明書を申請できる。職員は市民の詳細を登録し、それを電子身分証明書管理者に提出する。電子身分証明書管理者は、妥当性の調査を行い、登録されたEメール・アドレスを通じて申請者に初回のパスワードを送付し、起動番号を郵便で送る。市民は、これらのパスワードおよび起動番号によって電子身分証明書およびサービス・アカウントを有効化できる。

電子身分証明書システムは、もともとはMicrosoft 社によって開発され、その後国有 IT サービス企業であるMitts 社によってカスタマイズされた。e-ID の発行および管理に対する責任は、法律事務所であるFenlex と地元のICT 企業であるDataTrak 社およびComputime 社で構成される合弁企業であるAccerta 社に与えられた。

**e パスポート**：マルタのパスポート事務所は、市民がいつどこでもパスポートを申請することができるようにするオンライン・サービスを2005 年8 月に立ち上げた。パスポート事務所のウェブサイトで利用できるこのオンライン・サービスは、有効なマルタのID カードを所有する19 歳以上のすべてのマルタ国民が利用できる。サービスの利用者は、事前にe-パスポート・サービスの登録を行い、e-ガバメントの電子身分証明書（e-ID）を所有しなければならない。

### 3.1.18 オランダ

2003 年、オランダでDigiD の開発が開始された。このシステムにより、インターネット上で個人の電子的な身元確認が可能になる。オランダ政府は、別の水準において、いわゆる市民サービス番号（CSN）の導入に向けて最初のステップを踏み出した。市民サービス番号は、各自然人に固有のID 番号を割り当てることを目的としている。（現在の社会保障番号である「ソフィ番号」に相当する。）。

### 3.1.19 ノルウェー

ノルウェーでは、標準化された PKI（公開鍵基盤）ソリューションによって、民間部門と公共部門の両方においてさまざまな関係者が市民の間で広まりつつあるサービスの開発に関心を持つようになった。新しいサービスは社会保障部門および医療部門に導入され、学生は政府の奨学金に電子的に申し込むことができる。スマートカードを利用した投票が地方選挙で試され、2005 年の総選挙では従来の投票に代わるものとなった。ノルウェーの宝くじにより、210 万枚のスマートカードを発行することに成功した。次の2 つの選択肢を選ぶことができる。与信枠、電子財布が付いたカードと純粋な「宝くじカード」である。

ノルウェーのe ガバメント戦略「e ノルウェー2009」の目標の1 つは、ワンストップ・サービスのポータルhttp://norge.no/の安全な個人向けバージョンを2005 年末までに作り出すことであった。

### 3.1.20 ポーランド

ポーランドは現在、電子 ID カードやデジタル証明書の形式のデジタル身分証明書を利用しておらず、将来にも計画していないようである。

### 3.1.21 ポルトガル

ポルトガルの新しい ID カード（Cartao do Cidadao）の最初の試験結果が 2006 年 3 月 8 日、公式の式典で発表された。この Cartao には、身分証明書で見ることができるすべてのデータをはじめ、カード所有者の電子的な身元確認および電子認証に必要なデジタル署名を含む電子チップが組み込まれる予定である。したがって、この新しいカードは、オンラインで利用できる数多くの行政サービスへのアクセスを提供する eID カードとして利用できる。このカードはまた、他の既存の ID カード 5 枚を統合し、これらに取って代わる予定である。5 枚のカードとは、社会保障カード、公共医療サービス・カード、納税者カード、有権者カード、そして当然ながら現在の ID カード、すなわち Bilhete de Identidade である。

### 3.1.22 スロバキア

数多くの e-ガバメント・サービスが 2005 年の早い時期からスロバキアで立ち上げられてきた。この新しいシステムでは、認証のための固有に発行された PIN コードを利用して、安全な通信を使用する。

### 3.1.23 スロベニア

**eID**：すべてのスロベニア国民は、スロベニアの中央住民登録所（CRP）に登録され、固有の個人登録番号（PRN、スロベニア語の略語は EMŠO）を受け取る。スロベニアは 2003 年 2 月に eID カードの開発を開始した。この eID カードは強制ではない。そのコンセプトは、署名カードと従来の視覚的な ID カードを結合することである。政府の認証局である SIGEN-CA は、個人にクオリファイド証明書を発行している。

### 3.1.24 スペイン

**eID**：スペイン政府の最近の e ガバメント戦略は「Conecta 計画」と呼ばれており、最初のバージョンは 2004 年 9 月に発表された。この計画の鍵となる要素は、DNI Electronico という国の電子 ID カードを導入することであり、この ID カードはスペインの従来の ID カードに段階的に取って代わる。このスペインの eID には 2 つの証明書が含まれる予定である。1 つは認証用、もう 1 つは署名用である。この新しいカードの普及キャンペーンは 2006 年 3 月に始まった。

この新しい eID カードには電子認証システムおよび電子署名システムが含まれており、これらは電子取引における利用者のセキュリティを向上させ、プライバシーを保護することを目的としている。国家警察総局もまた、新しいカードに対するスペイン国民の関心を高めるために、「Identíficate con él」（これで自分の身分証明をする）というスローガンの下で情報キャンペーンを展開している。

*利用*：[Millard04] によれば、スペイン市民の所得税務サービスは、所得税申告を納税者に代わって提出する仲介人を認めているため、インターネット経由の申告数の大幅な増加に貢献している。これは、多くの普通の市民にとっては阻害要因であるデジタル署名を使用する必要があることを考えると、特に有益である。したがって、有効化されたデジタル署名はわずか 300,000 である。が、170 万件を超える申告が提出されている。この差異は、個々の専門の所得税仲介人が自

分のデジタル署名を使用して数多くの市民の代わりに所得税申告を行っていることが大きな理由である。デジタル署名は電子サービスを利用している多くの人にとって依然として障害であるようである。このような仲介人を利用しなければ、オンラインでの申請数はそれほど多くなかっただろう。この方法を利用することで市民の数を増やすことが可能である。

### 3.1.25 スウェーデン

**eID**：電子 ID カードは、認証局の役割を果たしているスウェーデンの郵便局が販売している。(郵便局の CA 業務は 2003 年 9 月に電気通信企業である TeliaSonera 社が引き継ぎた。)。スウェーデンの公的部門管理局とデジタル署名供給業者の間で枠組み協定が署名されたことを受けて、ソフトウェア・ベースの電子 ID（特にスウェーデン最大の銀行が開発した銀行 ID）も一部の e-ガバメント・サービスに利用できるようになった。政府は、将来に向けて、バイオメトリック識別子が含まれた公式の電子 ID カードの導入を計画している。

### 3.1.26 スイス

電子署名に関する法律が 2003 年 12 月 2 日にスイスの下院で承認され、2005 年に発効した。電子署名で締結された契約は、書面によるものと同じ法的地位が与えられる。電子取引の関係者は、公認認証局から得た電子署名を利用してオンラインで契約書に署名することができるようになる。しかし、遺言や建物売却の捺印証書など一部の公式文書は従来の方法で署名しなければならない。

*利用*：請願、立候補、国民投票のイニシアティブにおける電子署名はスイス当局が意図するもう 1 つの応用である。しかしこれは、電子署名設備が現在よりも広く利用可能になるかどうかによって左右されるだろう、とスイス当局は 2006 年 9 月に述べている。

### 3.1.27 英国

**eID**：英国の最も一般的で中心的な身分証明書プラットフォームは Government Gateway（http://www.gateway.gov.uk）である。利用者は、このポータル上で利用者 ID／パスワードやデジタル証明書の申請を選択できる。これらの証明書が受理されれば、利用者は希望の e ガバメント・サービスに登録することができる。(有効化 PIN コードを受け取った後の場合もある。)。

2004 年 5 月、政府は、中央政府のサービスへの市民のアクセスを可能にし、地方政府のサービスへのリンクを提供するために、e ガバメント・サービスの中心的なポータル（www.direct.gov.uk）を立ち上げた。このポータルには、総合案内とともに、自動車運転者、父母、障害者、キャリアのためのコンテンツが豊富に掲載されている。Government Gateway（www.gateway.gov.uk）ポータルは、e ガバメント・サービスのための中央登録サービスである。登録プロセスが完了すれば、Government Gateway のすべてのサービス全体で単一の利用者 ID やデジタル証明書を利用することができる。適切な政府のウェブサイト、ポータルまたは第三者のソフトウェア・パッケージを利用して手続きを行うことができる。

*利用*：eGovernment Gateway にアクセスしてサービスを利用することにすれば、オンラインで証明書を申請することができる。

*費用*：証明書はEquifax[35]およびChamber SimplySign[36]からインターネット上で申請することができる。(政府認証レベル 2 のためのブラウザー・ベースのデジタル証明書)。Equifax と Chamber SimplySign の証明書費用は、どちらも 25.00 ポンド＋付加価値税である。

### 3.1.28 EU

**市民カード・スキームの標準規格**

より迅速かつ広範囲な受容をもたらす意図の下、市民スマートカードの統合のためにすでに行われているあらゆる取り組みに条件を提供するために、複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化に関する CEN/ISSS のワークショップが立ち上げられた。この CEN ワークショップの合意では、市民サービス・スマートカード・スキームを構築する上で不可欠な組織面および運営面の規則、プロセス、技術的手法が導入されている。MMUSST アプローチで特徴となっているのは、複数のアプリケーションおよび複数の発行者のスキーム間で地域レベルから国際レベルまでの相互運用性を可能にする点である。MMUSST は、SmartCities (IST プロジェクト 12252) の活動を基礎としている。

その事業計画案は次の内容を含む CWA15535[37]で明確にされている。

- CWA15535-1：複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化パート 1－ビジネス・モデルの合意
- CWA15535-2：複数のアプリケーションおよび複数の発行者の市民カード・スキームの標準化パート 2－スキームの構造および導入ソリューション

**欧州市民カードの標準規格**

欧州市民カードに対する標準規格も現在 CEN で承認が進められている。これは CEN/TS15480 と呼ばれており、次の内容が含まれている。

- prCEN/TS15480-1 ID カード・システム－欧州市民カード－パート 1：物理的プロトコル、電気的プロトコルおよびトランスポート・プロトコルの特性
- prCEN/TS15480-2 ID カード・システム－欧州市民カード－パート 2：論理データ構造およびカード・サービス

**電子認証標準規格**

2004 年、電子認証に関する CEN/ISS のワークショップ［CEN/ISSS2004］では、3 つの領域（スマートカード、バイオメトリクス、デジタル署名）について、すべての基礎的な要素が十分に整備されていると結論付けられた。しかし、電子認証を提供するためには、スマートカード、バイオメトリクス、デジタル署名の各標準基準を結合させる必要があった。CWA の電子認証はこのギャップを埋めるものであり、これら 3 要素の相乗効果について詳しく述べられている。「スマート

[35] Equifax, http://www.equifaxsecure.co.uk/ebusinessid/
[36] British Chambers of Commerce, Chamber SimplySIgn, http://www.simplysign.co.uk/
[37] CEN CWA 15535:
http://www.cenorm.be/CENORM/BusinessDomains/BusinessDomains/ISSS/activity/ws-mmust.asp

カードおよびｅガバメントのアプリケーションのための電子認証」に関する CEN のワークショップは、この結論に従って次の複数のパートからなる CWA15264 を作成した。[38]。

- CWA15264-1：スマートカード・インフラストラクチャー内の欧州の相互運用可能な eID システムのためのアーキテクチャー
- CWA15264-2：相互運用可能な IAS サービスを組み込んだ複数アプリケーションのカード・スキームを作成するカード・スキーム運営者のためのベスト・プラクティスのマニュアル
- CWA15264-3：スマートカード・インフラストラクチャー内の欧州の相互運用可能な eID システムに対する利用者の要件

**公共調達**

2004 年 4 月 30 日に発効した公共調達に関する新しい指令［EU-RepDirSig］によって、公共調達で電子署名を利用するための法的な枠組みが完成した。電子署名の利用は、運営可能な電子調達システムを EU 全体で確立する上で中心をなすものである。電子調達は主要な応用分野の 1 つになることが期待されており、特により進んだ形態の電子署名が期待されている。電子調達では、電子署名の利用を促進する際に克服すべき課題が明らかにされている。公共調達に関する新しい指令では、電子入札にどの形式の電子署名を利用すべきかについて明らかにされていない。が、指令 1999/93/EC を実行する国内法と一致していることを条件に加盟国にその選択を任せている。これは、EU の調達指令が入札申込みの署名および安全確保の様式を規制していない、紙の入札申込みに対する現在のやり方を反映している。

加盟国が異なる水準の電子署名を選択できるという事実は、国内で開発された製品を考慮して電子調達ソリューションが設計されるというリスクを示唆している。このリスクにより、調達市場が分断され、電子署名の国際的な市場に障壁がもたらされている。

現在の課題は、国際取引に障壁を築くことなく、電子調達のために欧州全体で電子署名を導入することである。この新しい指令は、電子調達を 2010 年までに欧州で確実に普及させるために、2005 年から 2007 年の目標を設定し、欧州委員会および加盟国にとって可能な活動を特定する活動計画によって補完されている。この活動計画では、相互認定に基づく電子署名のための運営上のソリューションを必要としている。

**Porvoo Group**

Porvoo Group[39]は、欧州における公共部門および民間部門の安全な電子取引の確保に貢献するために、PKI 技術および電子 ID カードに基づいて、国際的に相互運用可能な電子身分証明書を促進することを主要な目標とする国際的協同ネットワークである。

2006 年 5 月 11 日および 12 日、国際 Porvoo Group の第 9 回会議がスロベニアのリュブリャナで行われた。この会議には、欧州 21 カ国、グルジア、日本、米国ならびに欧州委員会および国連の代表が約 100 人集まり、欧州の相互運用可能な電子身分証明書に向けた進展について検討した。この会議では、地球規模の調和、標準化、相互運用性に関連する問題が取り上げられた。アジェ

---

[38] CWA 15264 (2005) eAuthentication:
http://www.cenorm.org/CENORM/BusinessDomains/businessdomains/isss/cwa/eauthentication.asp
[39] Porvoo Group,
http://www.vaestorekisterikeskus.fi/vrk/home.nsf/pages/20710B02C6C5B894C2256D1A0048E290

ンダのその他の項目には、EU 内で行われている準備、欧州市民カードの開発、バイオメトリクスおよび電子 ID カードと電子パスポートにおけるバイオメトリクスの利用などがあった。

**EU 全体でのサービスへの安全なアクセスを要求する EU 活動計画 2010**[40]

市民は、旅行や移動をするときにサービスへの簡単なアクセスを望んでいる。EU 諸国の政府は、行政機関のウェブサイトおよびサービスに対して各国の電子身分証明書を相互認定するための安全なシステムを確立してこのプロセスを促進することに合意した。この活動計画では 2010 年までの完全な導入を予測している。欧州委員会は、2007 年中に電子 ID 管理の共通の仕様を特定する一方で、大規模で国際的な実行者を支援し、また電子署名の規則を 2009 年に見直すことでこれの実現を支援する予定である。

**IDABC PKI**

*IDA (BC)の PKI*[41]は、以前の IDA プログラムのために開発された、限られた利用者グループ (CUG) のための公開鍵基盤 (PKI) である。この PKI は、PKI の確立と関連する証明書方針 (CP) を通じて、EU 加盟国全体の行政機関と IDA (BC) の部門ごとのさまざまなプロジェクトに取り組んでいる欧州の各機関の最終利用者間の安全なデータ通信を促進している。IDA (BC) の PKI は現在、部門ごとの限られた利用者グループの最終利用者に個人向けの証明書と職務上の証明書を提供する一方で、他方ではサーバーの証明書を提供している。

**sTesta**

sTESTA は、行政機関間の安全な欧州横断テレマティクス・サービス (secured Trans European Services for Telematics between Administrations) の略語であり、欧州連合の機密用の電気通信ネットワークである。sTESTA は、欧州と各国の行政機関間の安全な情報交換に対するニーズの高まりに応えている。sTESTA は、行政機関全体にわたる要件に専念しており、保証された性能水準とセキュリティを提供している。2006 年 10 月、いくつかのデータ通信インフラストラクチャーを EU 規模で置き換えるこのインフラストラクチャーの提供について、Equant/Hewlett Packard の合弁企業との 2 億 1,000 万ユーロの契約に欧州委員会が署名したと発表された。この契約により、欧州と各国の行政機関は、いくつかの政策分野内で安全かつ信頼できる方法でデータ交換を行うことができるようになる。

## 3.2 デジタル証明書サービスにおける相違点

EU25 カ国の 80%近くが 2008 年までに自国の市民および企業にデジタル証明書サービスを提供することを提案した。2005 年の状況が図 8 に示されている。

---

[40] EU Press release: eGovernment: Commission calls for ambitious objectives in the EU for 2010, 25 April 2006, http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/523&format=HTML&aged=0&language=EN&guiLanguage=en

[41] IDABC PKI, http://ec.europa.eu/idabc/en/document/2316/5644

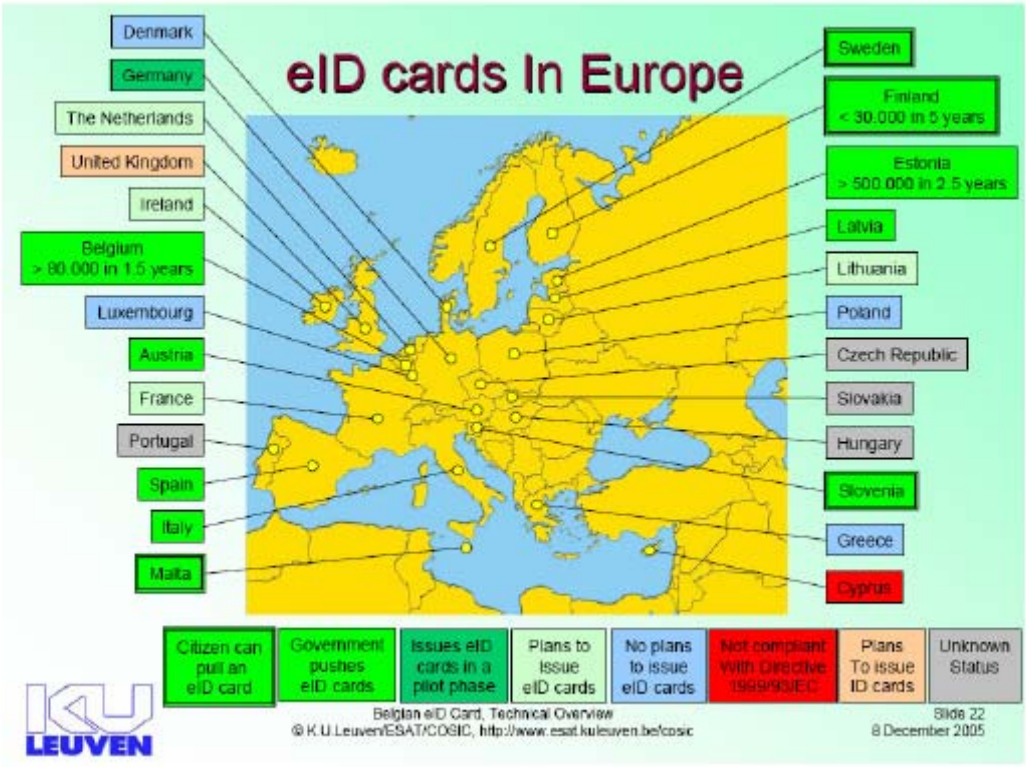



Figure 8：eID cards in Europe（Source：KU Leuven）

欧州諸国での電子署名の導入は欧州指令 99/93/EU に基づいているものの、その導入では大きなばらつきが示されている。

EU 加盟国が各国の多様な身分証明書を共有し、相互連結し、利用できるようにするには各国の法律を調整する必要があるため、eID の全欧州相互運用性の段階でさらなる問題が発生している。データ保護、プライバシー、情報の責任、アクセス権限、認証の質といった問題は大いに議論を招く問題である。

［FIDIS-D36］の結果を考慮して以下に主な相違点を検討する。

**署名媒体**

多くの欧州諸国は、スマートカードとタイプ III のカード・リーダーを必ずしも必要としない署名スキームを導入した。（オーストリアやフィンランドなど）。これらの事例では、代わりに携帯電話や USB メモリー・スティックを利用して署名手続きを行うことができる。（オーストリアなど）。［FIDIS-D36］はこれを手続き用署名ソリューションとして分類している。これらの署名ソリューションは身分証明書に限定されない。

ベルギーやドイツなどのその他の国は、大部分の e-ガバメント・プロセスの電子署名において署名カードとタイプ III のカード・リーダーを使用する傾向がある。［FIDIS-D36］はこれをカード利用型署名ソリューションとして分類している。

EU 電子署名指令によれば、クオリファイド署名は安全署名生成装置によって作成しなければならない。手続き用署名ソリューションにはこの機能が欠けている。すなわちアドバンスト署名の

み作成することができ、これはドイツでは手書きの署名の代わりとして認められていない。

**技術的な導入**

重要な側面として、欧州指令 99/93/EU に基づいているものの、欧州における電子署名の導入では大きなばらつきが示されているという点がある。これまでのところ、欧州電子署名指令で定義された電子署名の４つの水準（単純な署名、先進的な署名、クオリファイド署名、認定された署名）の１つに達するために、どの技術的な実行方法を利用できるかについては合意が形成されていない。

**行政手続**

どのような種類の行政手続に対してどの種類の署名が必要であるかについて合意が形成されていない。(単純な署名、先進的な署名、クオリファイド署名、認定された署名)。これは国のサービスについてすら明確でないことが多く、国際的な活動についてはさらに明確になっていない。

**利用分野**

もう１つの大きな相違点は、相互運用性に関する欧州の eID プロジェクトの大部分における共同アプローチである。多くの税金、医療、社会保障およびその他の政府機関が身元確認と認証のために国の eID を利用できるようになる一方で、過半数の国は eID ソリューションを商業組織に開放する予定である。

**登録方法**

証明書を入手するには登録手続きを行わなければならない。登録手続きも欧州諸国で異なっており、したがって認知される信頼度が異なる可能性がある。登録モデルには次の例がある。ノルウェー：外部委託、エストニア：官民の提携、ベルギー：行政機関内で実施。

**PKI の運営**

身分証明書と特に関連するのは、PKI の運営方法について欧州諸国間で観察される相違点である。例えばオーストリアやベルギーでは登録と証明が（企業のサポートを受けて）行政機関で行われているのに対して、例えばドイツやスウェーデンでは民間企業によって行われている。これらの相違点に加えて、欧州にはルート CA が存在しません。その結果、電子署名は、現在のところ欧州において技術的な水準では相互運用可能ではない。

世界中の認定機関の大規模なリストはPKI のページhttp://www.pki-page.org/で見ることができる。

**相互運用性**

認証およびデジタル署名の相互運用性に対するアプローチは、現在次の２つが認識されている。Bridge CA と GUIDE project のソリューションである。

- **European Bridge CA**[42]：European Bridge CA（EB-CA）は、主にドイツとオーストリアの認定機関（CA）の主導により、欧州、米国、アジアのメンバー（民間と公共の組織）に PKI と電子署名の相互運用性を提供している。European Bridge CA は、組織間のリンクの中心として機能しており、また新しい参加者の融合および EB-CA の運営に対して広範なサービスを提供している。個々の組織は、自組織の通信パートナーすべてとの契約条項の交渉に

[42] European Bridge CA, http://www.bridge-ca.org/eb-ca2/index.php?lang=en

これ以上時間を費やす必要がありません。他のすべての参加者との安全な電子ビジネス・プロセスを実現するには、European Bridge CA との間で 1 つだけ契約を結べば十分である。

- GUIDE[43]は連携ネットワークによる ID 管理アプローチを利用している。GUIDE のプロジェクトで考慮されている一般的なシナリオは、本人が外国で全欧州政府サービス（PEGS）にログオンする状態である。これらの場合、PEGS には外国の利用者（本人）を認証する手だてがありません。認証するには、本人の母国の ID プロバイダー（IP）が必要である。この IP は一般に 2 つの基本的なサービスを提供する。すなわち認証サービスと属性プロバイダー・サービスである。

発行された証明書の数は依然として限られているようである。が、これまで 9 年間、PKI は一部の欧州諸国で身分証明書システムに利用されてきた。それにもかかわらず、大きなセキュリティ問題は発表されない。[FIDIS-D36] によれば、証明書の情報を経由して行われる取引にはすでに連結性があるため、PKI は現在最適な方法でプライバシーを導入していない。

## 3.3 国の概要の評価

国の概要および電子署名指令［EU-RepDirSig］の運営に関する EU 報告書の結果に基づけば、クオリファイド電子署名の利用は予想よりもはるかに少なく、**市場は現在まだ十分に開拓されていない**。EU 報告書では、電子署名の有力な 2 つの応用分野は *e-ガバメント・サービスとパーソナル e-バンキング・サービス*に関連するものであると述べられている。インターネットに投資を行ったため、e-ガバメント／e-ID の分野での証明書／PKI の戦略的利用に関する情報は豊富にある。対照的に銀行部門では、技術面と利用者の受容に関する点の両方で公の情報はそれほど見つからない。

EU 報告書とレイキャビクで行われたポルボー7 セミナーの資料[44]に関して得られた教訓を以下に提示する。

- ［EU-RepDirSig］：サービス・プロバイダーには複数のアプリケーションによる電子署名を開発する誘因がほとんどなく、独自のサービスのためのソリューションを提供する方がよいとしている。
- ［EU-RepDirSig］：電子アーカイブのための包括的なソリューションなどのアプリケーションが不足している。
- オーストリア、ポルボー：全欧州的な協力（特にデジタルで署名・認証されたオーストリアの文書を外国で認定する点について）を拡大する必要がある。また Bridge CA の利用から制限および法的責任に関する疑問が生じる可能性がある。
- ノルウェー、ポルボー：一般市民の PKI プログラムが、市民や公共サービスの経済的ニーズによってではなく技術的教条主義者によって推進される傾向がある。
- ベルギー、ポルボー：市民へのコミュニケーションが重要である。また、カード・リーダーが利用可能であることが不可欠である。

---

[43] EU IST GUIDE project, http://www.guide-project.org)

[44] Materials of the Porvoo 7 Seminar in Reykjavik, Iceland, 26-27 May 2005, http://vrk.fineid.fi/default.asp?path=E%2CeEurope%2F9%2CReykjavik&template=

- フィンランド、ポルボー：成功の必須条件は、簡単な利用、広範な行政間の協力、民間部門との協力、サービス・プロバイダーのサポートおよび指導である。
- スウェーデン、ポルボー：市場（特に政府）は市民が eID を所有しない場合サービスを開発しないため、市場がより多くの電子サービスを提供できるようになるまで市民の負担はゼロでなければならない。

国の評価について以下の意見が追加された。

- オーストリア：この国は e-ガバメントの先導者の 1 つではあるものの、証明書の利用があまりに高額、複雑で実用性が低すぎるため、2005 年末までに発行された電子署名はわずか 70,000 件（すなわちオーストリア人口の 0.7%）であった。また A-SIT トラスト・センターは 2006 年に危うく支払不能を発表しなければならなかった。
- ベルギー:現在、ベルギーのインターネット利用者の 43%は eID カードを所有しているが、電子カード・リーダーを所有しているのはわずか 8%である。
- デンマーク：デンマークの人口は 5,450,661 人である。デジタル署名の導入によって、2005 年 5 月時点で合計 375,140 件のデジタル署名が発行された。これは人口のわずか 6%である。証明書は無料である。
- フィンランド:2006 年 9 月末までに、フィンランド国民 5,231,372 人のうち合計で 120,500 人に市民証明書が発行された。これは人口の 2.41%である。
- ドイツ：電子署名を促進するさまざまな戦略にもかかわらず、利用率はまだかなり低い状態にある。このため、認定トラスト・センター（TC トラストセンター）は 2005 年に支払不能を発表した。
- スペイン：有効化されたデジタル署名はわずか 300,000 件であるが、所得税申告のために行政機関に提出された署名は 170 万件を超えている。この差異はビジネス・モデルが原因である。すなわち、利用者に代わって仲介者（人）がこの署名に関与している。

総合すると、電子署名は e-ガバメントである。らまだ利用されていないと結論付けなければならない。普及計画（例えば、負担ゼロ、簡単な登録、さまざまな署名機器）によっても広範な受容には結びつかなかった。

上記の発展（の欠如）についての結論では、技術革新の普及に関する経済理論および署名利用に対するその理論の適用を考慮に入れなければならない。

これは次の章で行う。

# 4. 社会への影響

電子署名と PKI が社会にもたらすことができる影響と経済的な側面を理解し予測するためには、全般的な革新のプロセスを理解することが重要である。

この章は、Everett Rogers の「技術革新の普及過程」の理論［Rogers03］、電子署名の普及に関する成果 D3.2 の「PKI およびバイオメトリクスの調査」［FIDIS-D32］において EU プロジェクト FIDIS で行われたこの理論の評価、および e ユーザー［eUser］プロジェクトの結果に大きく依存している。これらの評価は、3 章の結果および Fraunhofer FOKUS の経験によって補足されている。

## 4.1 革新の普及

革新の普及に関する理論は、*技術革新の普及過程*という著書において 1962 年にすでに Everett Rogers によって形成されていた。

経済理論において Rogers［Rogers03］は、普及を「革新が特定の経路で時間と共に社会システムの構成員間で伝達されるプロセス」また「伝達内容が新しい考えに関係している特別な形式の伝達」と定義している。

Rogers によれば、革新は「(革新を) 採用する個人またはグループによって新しいと認められた考え、プラクティス、または物」と定義される。

### 4.1.1 革新の特性

認知された 5 つの**革新の特性**が［Rogers03］で定義されている。これらは革新の採用速度を決定する。

1. **相対的優位性**は、ある革新がそれに取って代わられる考えよりも優れていると見なされる度合いである。革新に客観的な優位性がある場合、これはそれほど重要ではありませんが、むしろ個人がその革新を優位であると見なす場合は重要となる。優位性は経済的用語を用いて計測することができる。が、社会的名声、便利さ、満足度も重要な役割を果たす可能性がある。
2. **両立性**は、革新が既存の価値、過去の経験、および潜在的な採用者のニーズと一致していると見なされる度合いである。既存の価値と一致している革新は、社会システムの基準および価値との両立性のない革新よりも速やかに普及する。
3. **複雑性**は、革新の理解・利用が難しいと見なされる度合いである。より簡単に理解できる革新は、新しいスキルを身につけ理解を高めることを採用者に要求する革新よりも迅速に採用される。
4. **試験可能性**は、革新を限られた条件で実験できる度合いである。潜在的な採用者が革新に多大な投資を行う前に試験できる新しい考えは、より迅速に採用される。
5. **観察可能性**は、革新の結果が他者の目に見える度合いである。個人が革新の結果を観察するのが簡単であれば、採用される可能性はそれだけ高くなる。

### 4.1.2　普及の段階

Rogers は革新の**普及**の 5 段階モデルも提案した。

1. **知識**：革新の存在と機能について知る
2. **確信**：革新の価値を確信する
3. **決定**：革新の採用を決定する
4. **導入**：革新を利用する
5. **確認**：革新の最終的な受容（または拒絶）

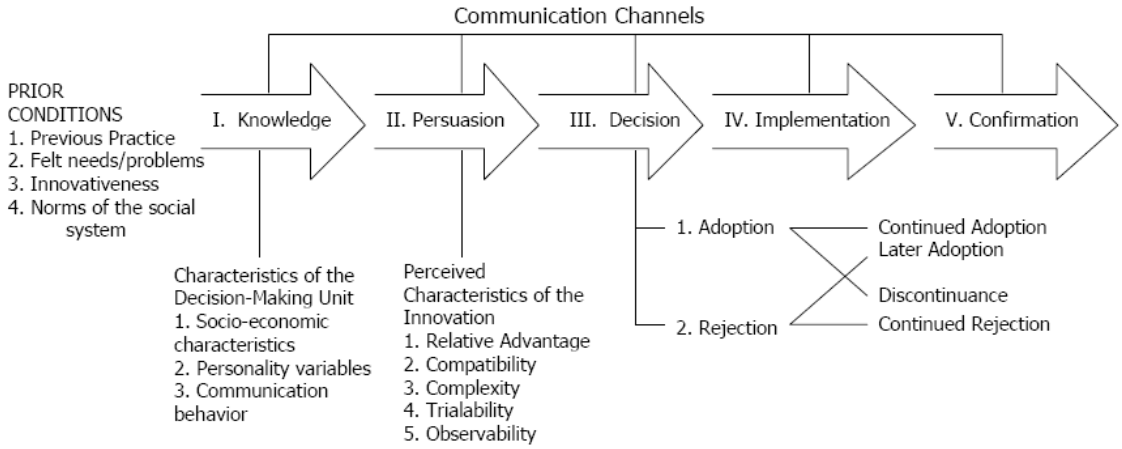



Figure 9：Rogers Innovation-Decision Process（Source：fr.cfans.umn.edu/courses/ESPM3251）

### 4.1.3　革新の採用者

Rogers は、新しい革新や考えの**採用者**は、認識、関心、評価、試験、採用に基づいて、革新を採用する意欲と能力に従って分類することができると述べた。採用者のカテゴリー別にいくつかの特徴を示す。

1. **革新的採用者**（2.5%）：冒険的、高い教育、複数の情報源、リスクを負う強い傾向、勇敢な人たち、変革を牽引する。革新的採用者は非常に重要な伝達者である。
2. **初期採用者**（13.5%）：社会的リーダー、有名、高い教育、尊敬される人たち、オピニオン・リーダー、新しい考えを試すがそれを注意深く行う。
3. **初期多数採用者**（34%）：慎重、非公式の社会的接触が多い、思慮深い人たち、注意深いが平均的な人たちよりも迅速に変化を受け入れる。
4. **後期多数採用者**（34%）：懐疑的、因習的、社会経済的な地位が比較的低い、懐疑的な人たち、大部分の人たちが利用しているときにのみ新しい考えや製品を利用する。
5. **採用遅滞者**（16%）：近所の人や友人が主な情報源である、借金を恐れる、因習的な人たち、「古いやり方」を好む、新しい考えに対して批判的で、新しい考えが主流または伝統にすらなったときにのみそれを受け入れる。

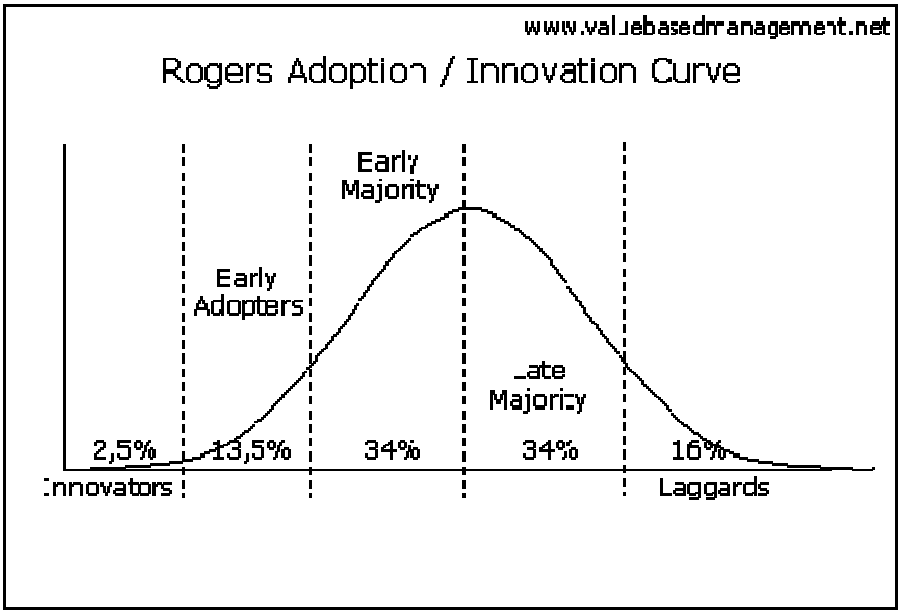



Figure 10：Rogers Adoption/Innovation Curve (Source：www.valuebasedmanagement.net)

## 4.2　利用者の経験のライフ・サイクル

革新の受容にとって非常に重要なものとして、個人の経験プロセスと認知された革新の優位性もある。個人ベースの「利用者の経験のライフ・サイクル」と「認知されたシステムの質」の関係が「e ユーザーの検討評価の枠組み」[45]［eUser］で説明されている。最終利用者によって認知される（認知されるべき）特性と質は何であるか、または何である可能性があるか、またライフ・サイクルの次の段階に進む上でそれらのうちのどれが重大な決定要因となるかを評価／予測することが重要である。（図 11 を参照）。

[45] eUser Inspection Evaluation framework, http://www.euser-eu.org/Document.asp?MenuID=124

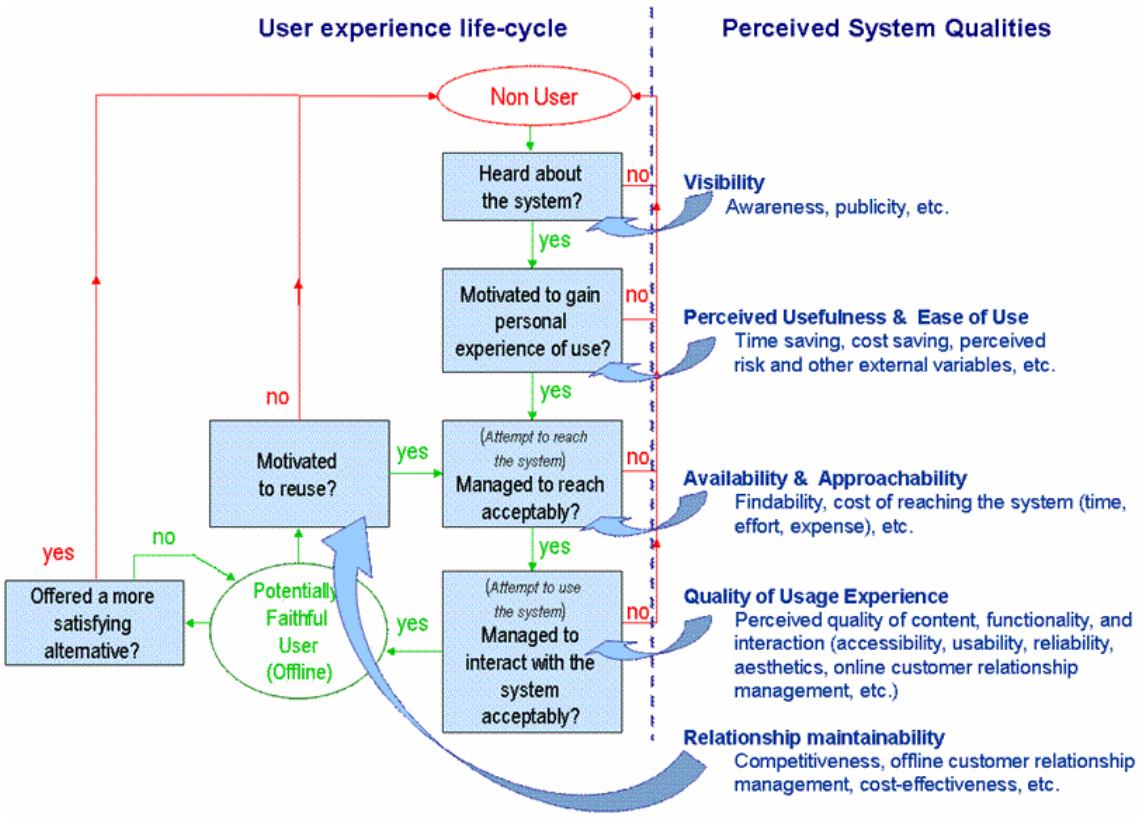



Figure 11 : eUser project : Lifecycle vs. perceived system qualities [Source eUser www.euser-eu.org]

利用者の経験のライフ・サイクルに関連するシステムの特性の基本的なカテゴリーは次のとおりである。[eUser]。

- **認知度**はシステムが個人の非利用者に知られるようになる度合いを指している。システムの*実際の場所*は、その認知度にとって明らかに重要な要素である。また、宣伝戦略によってプロバイダーがこれを高めることも可能である。しかし製品は、宣伝が行われなかったとしてもある程度は認知される。サービスを思いがけず見つけることから認識が生まれる可能性がある。例えば、ネットサーフィン中にサービスを見つけるなどである。
- **認知された実用性および使いやすさ**は、個人の非利用者の視点から見たシステム実用性およびアクセスと利用のしやすさを指している。これらはおそらく、利用者の特定の目的およびニーズを満たす製品の妥当性ならびに個人の環境への適合性から生じるだろう。さらに、(サービスが提供される方法ではなく) サービス自体によってもたらされる時間と費用の節約といったさまざまな具体的な側面も含まれる。最後に、これにはセキュリティといったそれほど具体的ではない側面も含まれる可能性がある。こういった側面はすべて、認知されるリスクと利用者の期待といった形で検討される。
- **利用可能性／アプローチのしやすさ**は、あらゆるタイプの利用意志のある個人の利用者がシステムのエントリー・ポイントに到達できる度合いを指している。確かに、サービス／システムのアクセスのしやすさ（例えば、誰でも、いつでも、どこからでも）は利用可能性／アプローチのしやすさにとって重要な要素である。この段階では、システムに到達す

るための利用可能な「経路」に関して、障害を持った人たちなどの多様な利用者集団の特定のニーズと要件が考慮される。

- **相互作用の経験の質**は、個人の実際の利用者が認知する相互作用の質を含み、有益かつ質の高い結果を得るためにシステムを利用できる（すなわち、客観的な満足に結びつく）度合いを指している。一般に、アクセスのしやすさ、使いやすさ、システムのユーザー・インターフェースの美しさが利用感の質の主要な決定要因となる。
- **関係の維持可能性**は、利用者がシステムに関わっていないときに、個人のシステム利用者との良好な関係が効果的に育成・維持される（例えば、利用者に新しい機能、コンテンツの更新、状況の変化などを知らせることによって）度合いである。プロバイダーは、この関係の持続可能性を確保するための具体的な戦略を導入する必要があるだろう。例えば、システム・プロバイダーは、個人の利用者の目的とニーズに最大限に適合するためにより豊富なサービス・パックを提供することができる。

## 4.3 普及の実現

革新の普及および利用者の経験のライフ・サイクルに関する経済理論の基礎的な要素を紹介したので、次にこれらの理論を PKI／電子署名の採用／利用に関連付ける。システム／サービスの特性に関して、採用の速度はその特性の「客観的な価値」に左右されませんが、利用者に認知される特性／質が重要な側面となる。潜在的な採用者が認知する革新について、PKI／証明書／署名の各システムの特性を以下に分析する。

### 4.3.1 認知度

Rogers が「予防的革新」と特徴付けた革新の典型的な欠点は、採用の速度が比較的遅い点である。予防的革新とは、何らかの将来の好ましくないイベントが発生する可能性を下げるために、ある時点で個人が採用する考えである。この革新を採用しなくとも好ましくないイベントが発生しない可能性があるため、予防的革新の採用は徐々に行なわれる。予防的革新を市場に投入するには、例えばHIV の予防やシートベルトの利用などの他の予防的革新で行われたように、啓蒙戦略を採用して大規模なマーケティング・キャンペーンを行わなければならない。重要な予防的革新は法律と罰則によって強制されることすらある。(例えば、ドイツにおけるシートベルトの利用)。

初期採用者は最も影響力が大きい潜在的採用者グループであるため、認知度を上げるには、特に彼らを最初のターゲットにしなければならない。したがって、クリティカル・マスに達するためには、製品をこのグループ内に提供することが極めて重要である。

これまでのクオリファイド電子署名の市場浸透率に基づけば、今までのところ革新的採用者のごく一部しかこの革新を採用していないと推測される。また、非公式的には、潜在的な採用者の大部分は知識段階にすら到達しておらず、この技術が存在することすら認識していないと思われる。

### 4.3.2 相対的優位性

電子署名はセキュリティを強化する。しかし、セキュリティと電子署名の関係は、社会全般に

とっては明らかになっていない。このことは、セキュリティと署名にはさまざまな水準があること、どのアプリケーションにどの署名を使用すべきか、という点を考慮するとさらに難しくなる。さらに難しいのは、多くの人が「関係がない」と見なしているさまざまなアプリケーションに同じ技術（証明書）が適用されていることを理解することである。（すなわち、ポータルにログオンして契約に署名すること）。

通常、電子署名に関して次のメリットが利用者にもたらされる。[FIDIS-D41]。

- 政府機関内で情報を処理する時間を節約し、市民にとっては応答時間が短縮される
- 手続きの時間と費用が削減される結果として費用が節約され、精度と生産性が向上し、紙ベースの維持運営費が削減され、提供されたサービスに対する利用者の支払方法を改善して信頼性を高めることができる
- 内部の利用者、公共団体およびその他の団体に対するサービスが向上する
- 紙ベースのシステムと比較してデータの質と統合性が改善される

FIDIS のプロジェクトで評価されたように、たいていの場合これらのメリットは行政機関にとってのメリットであって市民のためのものではありません。したがって、相対的優位性の認知度はかなり低い状態である。したがって、利用者にとっての真のメリット、および認識を高め市民に「PKI の利用」を提供する方法に関するマーケティング戦略に労力を費やすことが極めて重要である。

潜在的な採用者に認知される相対的優位性を判断するためには費用に目を向けることが重要である。が、これは署名を市場に導入する上で最も重要な要素ではない（デンマークでは費用のかからない証明書でも広範な受容を推し進めることはできない）。その他の予防的革新に見られるように、単に存在して利用できるだけでは必ずしも革新の採用に結びつかない。

一般に、費用とメリットも均一に配分されていないことに注意しなければならない。行政機関は、主な利得者である一方で、このインフラストラクチャーの費用に対してはわずかにしか貢献しない。他方、民間の利用者は、ほとんどメリットを得ることがない一方で費用の大部分を負担しなければならない。クオリファイド電子署名のためのアプリケーションがほとんど存在しないことを考慮すると、価格はかなり高いと見なされる可能性がある。これは相対的優位性の認知度のさらなる低下をもたらす。

クオリファイド電子署名の受容は、利用者に金銭的なメリットを提供することで増加する可能性がある。例えば、クオリファイド電子署名を利用してオンラインで手続きを行うことを選択する利用者に対して行政機関の手続き費用を免除することも可能である。価格の差別化を利用して、特にさまざまな利用者グループをターゲットにすることもできる。また、新しい価格モデルの調査も行わなければならない。例えば、署名者が署名照合の費用を徴収し、年間の費用を削減するという提案がある。

### 4.3.3　認知された実用性および使いやすさ

認知された実用性は、上記で得られ説明された相対的優位性と密接に関連している。市民に親

切な PKI サービスの利用を実現するには、利用の必要が定期的に発生しなければならない。[46]。概算によれば、週に 1、2 回が目標になるはずである。これは年間で 80 回の利用になる。ドイツにおける行政機関のサービス、税金または社会福祉に関する電子的なニーズを数えると、年間で必要とされる利用回数は平均してわずか 5 回以下である。e ヘルスについては、電子署名の利用が増加するかどうかは現在まだ確認されていない。

医師、公証人、弁護士は日ごろから法的拘束力のある文書に署名しなければならないため、特定の専門家による電子署名の利用がもっと増加することが期待されている。オンライン取引は、窓口の取引のわずか 10%の費用しかかからず、文書による取引の 13%しかかからないという銀行部門の通則を適用してみると、大きな経済的可能性が考えられる。市民は、クオリファイド署名が行われたこれらの文書（例えば、行政の通知、判決、法的強制力のある文書など）に対して、署名を検証するための照合ソフトウェアがあれば十分だろう。これは費用をかけずに行うことができる。

欧州のビジョンでは、電子身分証明書つまり eID を最優先としている。この優先付けとともに、電子認証への移行が現在行われている。多くの人がいろいろなユーザー名／パスワードを組み合わせて持っているので、認知された実用性がかなり向上する可能性があるため、ID カード（証明書を含む）による電子認証は公開鍵利用の推進力となる可能性がある。採用にとって重要なのは、当然ながら、政府関連の分野に限定されないサービス・プロバイダーの大部分がこの電子認証証明書を広く受け入れることである。これには、これらの官民ネットワーク間の相互運用可能な PKI インフラストラクチャーが必要である。

### 4.3.4　両立性

署名プロバイダーの大部分は、暗証番号を利用して署名者の認証を行っている。暗証番号はオンライン・バンキングや ATM などで金融取引を認可するために一般に利用されているため、暗証番号の利用には高い両立性がある。しかし、実際に法的拘束力があるにもかかわらず、クオリファイド電子署名によって署名された契約をそのような取引として見なさない人がいるかもしれない。したがって、クオリファイド電子署名の利用の法的重要性を潜在的な採用者に知らせなければならない。前にも述べたように、暗証番号と電子署名の関係は、潜在的採用者について明らかでない。暗証番号と電子認証の間に心理的な連結を確立することの方が簡単かもしれない。なぜなら、パスワードを暗証番号に関連付けることの方がはるかに簡単だからである。

単純なソリューションが既存の認証システム（例えば、オーストリアの携帯電話サービス・プロバイダーやオランダの SMS メッセージ）上に構築された場合の方が一般に受容率は高くなる傾向がある。

### 4.3.5　複雑性

平均的な利用者が公開鍵の暗号方式の原理を理解できるようになることは期待できない。しか

[46] TeleTrusT-Stellungnahme zur eCard-Initiative, April 2005,
http://www.teletrust.de/fileadmin/files/TTT-StN_eCard-Initiative_final.pdf

し、これは必要ではないかもしれない。電子署名を利用することで認知されるセキュリティは（一度採用されれば）かなり高くなり、基礎となる原理の完全な理解は必要ない。例えば、大部分の利用者は ATM の基礎となるプロセスおよびセキュリティ対策を理解していない。が、ATM は極めて普及している。

当然ながら、署名アプリケーションが簡単に利用・理解でき、利用者に自分のプライベート鍵を他人に教えさせないことが非常に重要である。他方では、IC カード・リーダーの利用は大部分の潜在的採用者にとって新しいことになる可能性が高く、設置と維持管理によって問題が引き起こされる可能性がある。複雑性を減らすには、モバイルクオリファイド電子署名［Rossnage105］が大いに役立つ可能性がある。

### 4.3.6　利用可能性／アプローチのしやすさ

潜在的な採用者がクオリファイド電子署名に好意的な姿勢を持ち、採用を決定したとしても、登録局の職員は十分に情報を伝えられておらず、これらの商品を提供することすら認識していないことが多いため、潜在的な採用者を獲得することは実際には非常に難しい状態である。（少なくともドイツにおいて）。

このギャップは、政府が ID カードの証明書をサポートし、証明書をカードに組み込めばおそらく解消されるだろう。

### 4.3.7　試験可能性

クオリファイド電子署名が現在提供されている方法では、潜在的な試験可能性は存在しません。利用者は、クオリファイド電子署名を生成できるようになる前に、最初の費用を請求され、証明サービスに対して支払を行わなければならない。したがって潜在的な採用者は、この革新の潜在的なメリットを試験できるようになる前にかなりの金額を投資しなければならない。しかし、無料の証明書やプリティー・グッド・プライバシー（PGP）などの無料のソフトウェアを利用して電子署名を試験することは一般に可能である。しかしどちらの場合でも、試験するのは実際の環境ではありません。すなわち、どちらのサービスも先進的署名とともに利用することができず、PGP の場合は最終的に採用されるものではなく、異なる外観と雰囲気、さらには異なる証明書構造の別のソフトウェアを試験することになる。

無料の試験用証明書を発行するなどして、試験可能性を高めなければならない。また、市民の ID カード上で電子証明書を発行しようとするいくつかの国の意向によって、さらに多くの試験が行われる可能性がある。この目的のために試験環境および試験サービスが利用できるようにならなければならない。

### 4.3.8　観察可能性

採用者は、自分の署名を検証できるようになることで、自分の署名の有効性を確認し他の人たちに実演してみせることができる。しかし、自分で電子署名を取得していない人たちは署名を検証することができず、観察可能性を失いる。また、予防的革新であることから、予防された好ましくないイベントは、その定義により発生せず、したがって観察を行ったり回数を数えたりする

ことができない。

## 4.4 電子身分証明書

公共サービスへのアクセスおよびその利用のための、身分証明の安全な電子的手段に対するニーズは市民および企業にとって不可欠であり、またこのニーズによって電子署名の利用が促進されることが期待されている。さまざまな形態の eID が現れ、ある程度の相互運用性が求められるようになる。

e ユーザー・プロジェクトでは、e ガバメントにおける身分証明方法について人口調査が行われた。それを以下に示す。

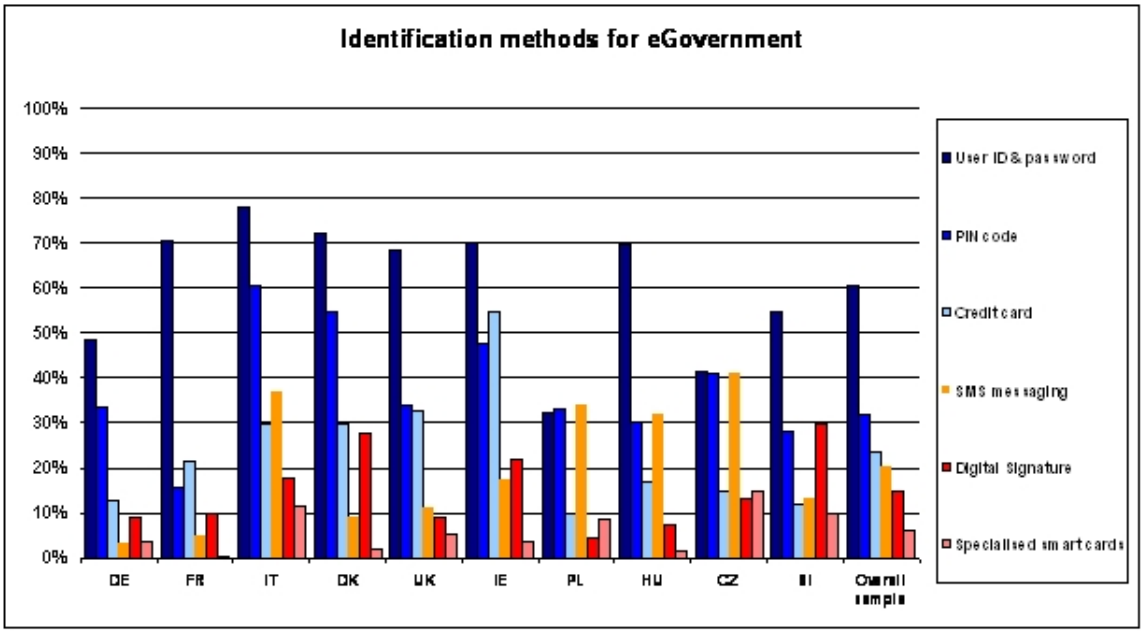



Figure 12：Identification methods for eGovernment [Source：eUser Project[47]]

欧州委員会は、eID イニシアティブに高い優先順位を与えている。例えばそれは、電子調達活動計画や旅券のセキュリティ特性の調和、全欧州 e ガバメント・サービス、IST、eTen プログラムのための eID の相互運用性の側面に対する IDABC プログラムの活動などを通じて行なわれる見込みである。e ガバメントの活動を通じたサポートを超えて、電子署名の相互運用性および国際的な利用に対して特別な重点が置かれる予定である。欧州委員会は、電子署名のためのあらゆる種類の技術の相互運用性および利用を促進するために、さらなる標準化活動を促進する予定である。

IT の専門家、企業、政府のための欧州の独立団体である EEMA は、デジタル身分証明書は 2020 年までに世界の人々の日々の生活に多大な影響を与え、また**電子身分証明書**の運営は次の 10 年間

[47] eUSER population survey 2005
http://www.euser-eu.org/eUSER_PopulationSurveyStatistics.asp?KeyWordID=1&CaseTitleID=850

の主要な課題となるだろうと予測した。[48]

PKI は、電子認証／身分証明書のあらゆる管理インフラストラクチャーにおいて不可欠の要素である。連携 ID 管理は PKI の内部利用をサポートすることができる。が、利用者には見えない。サーバー・ベースの署名などの展開によっても、市民が自分で証明書を取得する必要がないアプリケーションが育成されている。

現在、PKI に関する活動では、法的な署名よりも認証特性が主に重視されている。認証はすべての人にとって第一の目標である。パスワードの利用がすべての人にとって負担になりつつあるため、この目標は社会ではるかに広く認識されている。したがって、証明書による安全な認証方法は、広い範囲で証明書の利用を導入するための有効な方法であると思われる。

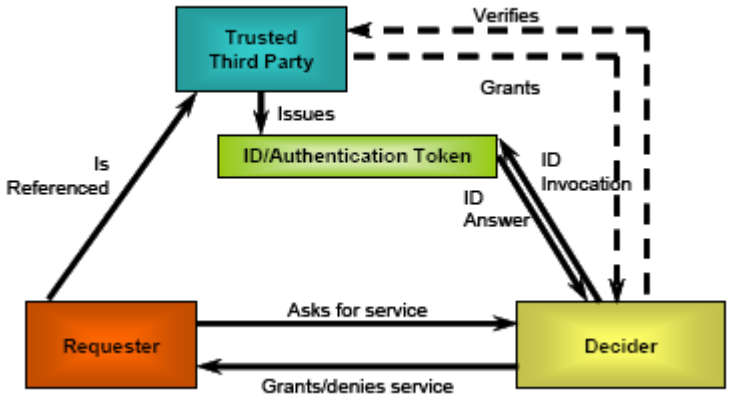



Figure 13 : Trust model of eID card according to CWA 15535-1

電子身分証明書の発展を促進し、それによって PKI 関連のサービスを育成するために、EU は欧州の相互運用可能かつ相互に認定された eID をサポートするためのロードマップに従って活動している。

[48] Eema, European e-Identity Conference eema's Annual Conference 2006, http://www.eema.org/downloads/eema06/eema06_report.pdf

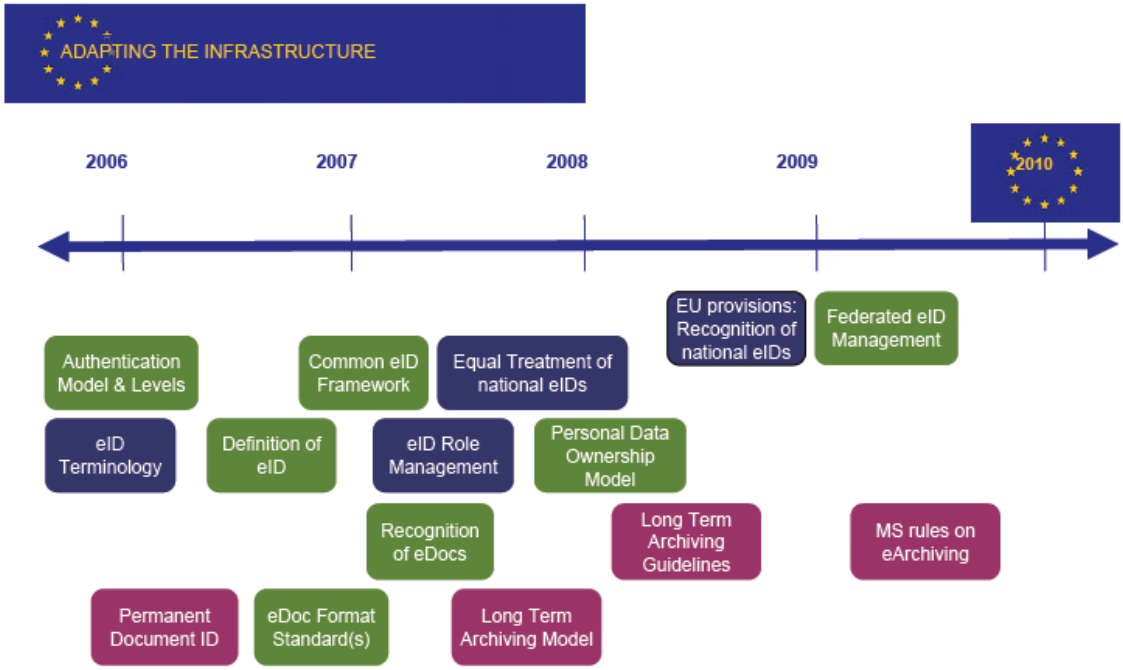



Figure 14：EU eIDM/eDoc roadmap [Varghese06]

セキュリティ分野における具体的なニーズについて、欧州セキュリティ調査諮問委員会（ESRAB）の最終報告書「課題の達成」[EU-ESRAB2006]が発行された。この報告書は、調査および技術開発のための第７次フレームワーク・プログラムに対する欧州委員会の要件を満たすだけでなく、この他にも国、地域さらには民間の多くの調査プログラムを調整できる強固な参照枠組みを提供している。

この報告書では、欧州のセキュリティ調査の目標は、欧州の産業競争力を高める一方で、市民のために欧州をより安全にすることであると述べられている。取り組むべき主要な問題には、安全な状態と安全でない状態の市民の認識、緊急時および通常時の当局と市民の間の連絡および指示が含まれている。

推奨される調査項目には、特に、市民の安心感および危機感をもたらす要因の理解、さらにはそれを判断する方法が含まれている。調査プロジェクトでは、適用性、利用のしやすさ、手ごろな価格に関する市民の具体的なニーズを満たすことを目指さなければならない。セキュリティ技術の調査および開発に最終利用者をうまく取り込むためには、非常に数が多く、複雑で多様な公共の利用者組織の組織構造および独特の文化を理解する必要がある。

また、市場を創出するためには、国際的な開発プログラムのイネーブラー（促進要因）および調達におけるツールとして標準規格が重要であることが確認された。欧州標準化委員会(CEN)は、セキュリティ分野における欧州の標準化を調整しており、標準化の新たなニーズを具体的に特定することを目標としている。

## 5. 結論

欧州のセキュリティ調査の目標は、欧州の産業競争力を高める一方で市民のために欧州をより安全にすることである。欧州全域での協力および調整の努力により、EU は常に変化する世界でリスクをより良く理解しそれに対応することができる。

電子署名指令が採用されたことに伴い、この指令が電子署名市場の急速な成長の初期段階を迎えるのに貢献することが一部で期待されている。[EU-RepDirSig] によれば、電子署名市場は予想されたほどにはまだ発展していない。市場が直面する技術的な課題には PKI 技術の複雑さが含まれている。もう 1 つの障害は、国内および国際的なレベルでの技術的な相互運用性の欠如によってもたらされている。また、証明書が単一のアプリケーションにのみ利用でき、サービス・プロバイダーが例えば銀行部門によって開発されたソリューションなど、独自のサービスのためのソリューションを提供する方がよいとしているところでは、一連の電子署名アプリケーションが存在する。これによって相互運用可能なソリューションの開発プロセスが減速している。

この報告書では、e-ガバメント・サービスでの電子署名の利用はすでにある程度の規模に達しており、おそらく将来の重要な推進力となるだろうと述べられている。e ガバメントのアプリケーションの戦略的な役割は EUi2010 イニシアティブで認識されている。このイニシアティブは、民間部門および公共部門による ICT の配備および効率的な利用を促進するためのものである。このような理由により、この調査では e ガバメントのアプリケーションに焦点を当てて欧州諸国における電子署名の利用を分析した。この分析に基づけば、電子署名は e-ガバメントですらまだ利用されていないと結論付けなければならない。普及計画（例えば、負担ゼロ、簡単な登録、さまざまな署名機器）によっても広範な受容には結びつかない。

上記の発展（の欠如）についての考察は、技術革新の普及に関する経済理論および署名利用に対するその理論の適用に基づいて行われている。

デジタル署名の取り組みが遅いその他の理由は、[EU-RepDirSig] に対する TeleTrust[49]の反応 [TeleTrust2006] においても特定されている。TeleTrust は、「自然人に対する意思表示」および自然人の間の電子上の法的相互関係（エンド・ツー・エンド）において利用するための電子署名の一方的な制限について、電子署名に関する EU 指令を批判している。構成要素の署名およびプロセスの伝達の確保は、おそらく PKI 利用のためのより重要な応用分野となるだろう。

欧州委員会は、将来に向けて、eID イニシアティブに高い優先順位を与え、電子署名のサービスおよびアプリケーションの開発を今後も促進し、市場を監視していく。e ガバメントの活動を通じたサポートを超えて、電子署名の相互運用性および国際的な利用に対して特別な重点が置かれる予定である。クオリファイド電子署名のためのあらゆる種類の技術の相互運用性および利用を EU 市場で促進するために、さらなる標準化活動が行われる予定である。

[49] TeleTrust is a German non-profit organization for the Promotion of Trustworthiness of Information and Communication Technology.

## Appendix

## References


[CEN/ISSS2004] CEN/ISSS Workshop eAuthentication, CEN/ISSS WS/eAuthentication Vision Document, Towards an electronic ID for the European Citizen, a strategic vision, October 2004, http://europa.eu.int/idabc/servlets/Doc?id=19132

[Clarke] Clarke, R.: A Primer in Diffusion of Innovations Theory, http://www.anu.edu.au/people/Roger.Clarke/SOS/InnDiff.html

[Dumortier] J. Dumortier, S. Kelm, H. Nilsson, G. Skouma, P. Van Eecke. The Legal and Market Aspects of Electronic Signatures, Study for the European Commission - DG Information Society, October 2003

[ETSI06] Charles Brookson and Dionisio Zumerle: ETSI White Paper No. 1, Security for ICT - the Work of ETSI, Revision 1, February 2006

[EU-DirSig] Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures, published in the Official Journal of the European Communities (OJ L 13, 19.01.2000, p. 12)

[EU-RepDirSig] Report from the Commission to the European Parliament and the Council, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, 15.3.2006,

[EU-eGovOnline] EU: Study "Online Availability of Public Services: How Is Europe Progressing?", Web Based Survey on Electronic Public Services, Report of the 6th Measurement June 2006, http://www.de.capgemini.com/m/de/tl/EU_eGovernment-Studie_2006.pdf

[EU-ESRAB2006] European Communities, European Security Research Avisory Board: "Meeting the Challenge: The European security research agenda", September 2006, http://ec.europa.eu/enterprise/security/articles/article_06_09_25_tc_en.htm

[EU-NIS] Euroean Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society - "Dialogue, partnership and empowerment", 2006, http://ec.europa.eu/information_society/doc/com2006251.pdf

[eUser] EU IST eUser Project, Country Briefs and Country Backgrounds, http://www.euser-eu.org/euser_countrybrief.asp?MenuID=112 and

http://www.euser-eu.org/SearchSpecial.asp?IDFocus0=3&CountryID=*&MenuID=109

[EIF] European Interoperability Framework for pan-European eGovernment Services (EIF), Version 1.0, 2004, http://ec.europa.eu/idabc/en/document/2319/5644

[FIDIS-D32] EU FIDIS Project, Deliverable D3.2: A study on PKI and biometrics, 4 July 2005, http://www.fidis.net

[FIDIS-D36] EU FIDIS Project, Deliverable D3.6: Study on ID Documents, 31 March 2006, http://www.fidis.net

[FIDIS-D41] EU FIDIS Project, Deliverable D4.1: Structured account of approaches on Interoperability, 12 July 2005, http://www.fidis.net

[IDABC-eGov06] EU, Editorial Team of European Dynamics for the IDABC eGovernment Observatory: eGovernment in the European Countries - 6th Edition, Report, 29 September 2006 http://ec.europa.eu/idabc/en/document/5094/254

[Millard04] Millard, J., Kubicek, H., Westholm, H., Cimander, R., Iversen, J.S. (2004) Reorganisation of government back-offices for better ePS - European good practices (back-office reorganisation), prepared for the European Commission eGovernment Unit, Brussels, January 2004.

[OASIS-PKI] OASIS PKI TC, Analysis of June 2003 Survey on Obstacles to PKI Deployment and Usage, August 3, 2003 http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf and www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf

[Rogers03] Rogers, E. M., "Diffusion of Innovation", Fifth Edition, Free Press, 2003.

[Rossnagel04] Heiko Rossnagel: Mobile Qualified Electronic Signatures and Certification on Demand, Lecture Notes in Computer Science, Volume 3093/2004, in book "Public Key Infrastructure", pp 274-286

[Rossnagel05] Heiko Rossnagel and Denis Royer: Making Money with Mobile Qualified Electronic Signatures, Lecture Notes in Computer Science, Volume 3592/2005, in Book "Trust, Privacy and Security in Digital Business", pp 110-118.

[TeleTrust2005] Teletrust, TTT-Stellungnahme zur eCard-Initiative der Bundesregierung, April 5, 2005 http://www.teletrust.de/fileadmin/files/TTT-StN_eCard-Initiative_final.pdf

[TeleTrust2006] TeleTrusT Recommendations for Further Action in Accordance with the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, Dated 15 March 2006, http://www.teletrust.de/fileadmin/files/publikationen/Stellungnahmen/TTT-StN_EC-Bericht-zur-Anwendg-1999-93-EG_en.pdf

[Varghese06] Aniyan Varghese: Achieving the Interoperable and Mutually recognised eID in EU: eGovernment Action Plan. eGovernment Unit, Directorate General Information Society & Media, European Commission, Presentation World e-ID 2006 conference, Sophia-Antipolis, France, 20-22 September 2006.

## Acronyms／Abbreviations

| | |
|---|---|
| CA | Certification Authority |
| CRL | Certificate Revocation List |
| CSP | Certification Service Provider |
| CWA | CEN Workshop Agreement |
| DSS | Digital Signature Standard |
| EC | European Commission: The European Commission embodies and upholds the general interest of the European Union and is the driving force in the Union's institutional system. Its four main roles are to propose legislation to Parliament and the Council, to administer and implement Community policies, to enforce Community law (jointly with the Court of Justice) and to negotiate international agreements, mainly those relating to trade and cooperation |
| EESSI | European Electronic Signature Standardization Initiative |
| ETSI | European Telecommunication Standards Institute |
| EU | European Union: The European Union (EU) is a family of democratic European countries. |
| IETF | Internet Engineering Task Force |
| ITU-T | International Telecommunications Union Telecommunications Sector |
| PKI | Public Key Infrastructure |
| SSCD | Secure Signature-Creation Device |
| TTP | Trusted Third Party |

# エストニア ID カードと電子署名の概念
# 原則とソリューション
# ホワイト・ペーパー
# バージョン：2003 年 6 月 5 日

# 目　次

### 文書の状態

この文書は、AS Sertifitseerimiskeskus（www.sk.ee）によって作成されており、何も変更が加えられていない元のままの形式であれば自由に配布できる。このホワイト・ペーパーの最新バージョンを含むエストニア ID カードのプロジェクト情報は、http://www.id.ee からオンラインで入手可能である。筆者への連絡は info@id.ee にお願いしたい。

### はじめに

エストニアは、国民や国内に居住する在留外国人を識別するための主要な文書として ID カードを実装している。このカードは、物理的な身分証明書であるだけでなく、全国的なオンライン・サービスに関連した安全な認証（Authentication）および法的拘束力のある電子署名を促進するための高度な電子的機能を備えている。

このホワイト・ペーパーでは、このプロジェクトの背景にある原則の概要を示し、このカード・プロジェクトの遂行中に行われた選択や決定について説明する。また、関連するサービスおよびアプリケーションの実装方法の概要についても説明している。

### 対象読者

このホワイト・ペーパー前半の「原則」は、法律および経済的な観点から、意志決定者や潜在的な一般ユーザー向けに書かれている。後半の「ソリューション」は、実装者向けの内容になっており、基本的な PKI の概念に関する知識を前提にしている。

### 現在のプロジェクトの状態

最初のエストニア ID カードは、2002 年 1 月に発行された。1 年間で 130,000 枚を超えるカードが発行され、2003 年末までに、その総数は 350,000 枚（人口全体の約 25%）を超える増加が見込まれている。

このカードは汎用性が考慮されており、その機能は、企業、行政機関、または個人による任意の形式の通信に使用される見込みである。このカードは既に、ユーザーの日常的な通信をより便利なものにするのに役立っている。以下、その実装およびアプリケーションについての詳細について説明する。

## 1. 原則

### 1.1 電子署名に関する規定

エストニア議会（Riigikogu）は、電子署名法案（Digital Signature Act、以下 DSA）を 2000 年 3 月 8 日に通過させ、2000 年 12 月 15 日に施行した。この法律は、全国的な PKI および電子署名のインフラストラクチャーの実装に不可欠な事項について規定している。この法律は、http://www.legaltext.ee/text/en/X30081K3.htm からオンラインで参照できる。

### 1.1.1　電子署名の概念

エストニア DSA によると、電子署名は DSA で定義された要件に準拠し、かつ他の法律で別に規定されていない限り、手書きの署名と等価である。したがって、原則として、電子署名と手書きの署名は公共部門と民間部門の両方の文書管理において等価である。DSA はまた、公共部門の組織が電子署名された文書を受け付ける義務があることも規定している。

DSA で定義された電子署名の要件では、電子署名が署名者を一意に識別できること、いったん署名した後はその署名を無効にしない限りデータを変更できなくなるような方法で署名済みのデータに結びつけられていること、および、署名の時間を識別できること（タイムスタンプまたは同等の時間確定技術が使用されている場合）が必要であると規定されている。

EC 指令 1999/93/EC の点から見ると、DSA はアドバンスト電子署名のみを規定している。その他の種類の電子署名も当然使用できるが、DSA はこれらに法的な権限は与えていない。

### 1.1.2　証明書サービス・プロバイダー（CSP）

DSA はエストニアにおける CSP の業務を規定しており、CSP の要件を設定し、その運営と管理について規定している。CSP は、規定された最小の株式資本を保有している場合にのみ合法的な組織になることができ、国家証明書サービス・プロバイダー登録機関（後述を参照）に登記される必要があり、さらに組織とシステムの信頼性を保証するために年次監査を実行する必要がある。CSP はまた、サービス提供中に発生する補償責任から保護されるように損害賠償保険にも加入する必要がある。

DSA によると、CSP による証明は名前と ID コードで識別可能な実在の人物に限られており、現在、仮名に対する証明書の発行は DSA の対象範囲外であることに注意する必要がある。この問題は法律の採択プロセスで議会において議論されたが、不必要なリスクを増加させることになると判断された。これまでのところ、その必要性は見られない。

### 1.1.3　タイムスタンプ・サービスプロバイダー（TSP）

DSA はまた、TSP の業務と、TSP 間のタイムスタンプの比較についても規定している。一般に、これらのサービス・プロバイダーの要件も CSP の場合と同じである。DSA によると、タイムスタンプは単純に、特定のデータが特定の時点に存在していたことを証明するデータ単位である。DSA はタイムスタンプをこれ以上詳細には定義していないが、タイムスタンプは、タイムスタンプされたデータに結びつけられ、そのタイムスタンプを無効にしない限りいったんタイムスタンプされたデータを変更できないような方法で発行される必要があると規定している。

### 1.1.4　管理－登録機関と担当省庁

証明書発行サービス・プロバイダーの国家登録機関には、エストニアのすべての CSP と TSP に関するデータが記録されている。この機関は CSP の公開鍵を確かめるが、厳密に言えばエストニアにおけるルート CA ではない。代わりに、管理機関として機能し、とりわけサービス・プロバイダーの年次監査の結果を確認する。登録作業を管轄している経済通信省には、監査結果を確認したり、サービス・プロバイダーの敷地および関連情報を調査したりする権限がある。

### 1.1.5　外国の証明書

DSA は外国の証明書の承認（recognition）についても規定しており、外国の証明書が、エストニアの CSP によって発行された証明書と等価であると承認（recognition）されるには、登録された CSP によって確かめられるか、DSA の要件に明示的に準拠しているか、国際協定の対象範囲に入っているかのいずれかが必要であると規定している。

## 1.2　身分証明書に関する規定

エストニアにおける身分証明書は、身分証明書法によって規定されている。この法令は、http://www.legaltext.ee/text/en/X30039K7.htm からオンラインで参照できる。

### 1.2.1　義務付けられた文書

この法令によると、すべてのエストニア在住者、および、少なくとも 1 年の有効期間がある有効な在住許可証に基づいてエストニアに永続的に居住するすべての在留外国人に対して、ID カードの所有が義務付けられている。カードの不所持に対する罰則はないが、最初のエストニア・パスポートが 1992 年に 10 年の有効期間で発行されており、その期限が切れつつあることから、ほとんどの住民が 2002～2006 年の間のこの文書の更新時に、ID カードのみ、またはパスポートと一緒になった ID カードのどちらかを申し込むと予測されている。2006 年末までには、100 万枚のカードが発行される見込みである。

この文書の種類は単一であり、ユーザーが選択または除外できる異なるオプション機能は存在しない。すべての文書に、電子データと証明書を含むチップが装備されている（後述を参照）。一部のユーザーがカードの電子的な使用について疑念または恐れを抱く可能性があることは理解されており、それに対する対応策も提供されている。ユーザーがカードの電子的機能の使用を希望しない場合、そのユーザーは証明書の有効性を一時停止することにより、そのカードの電子的な使用を不可能にすることができる。証明書の一時停止または失効によって、ユーザーのデータは公的な証明書ディレクトリからも削除される。

### 1.2.2　カードの外観とレイアウト

カードの外観を次に示す。


エストニア ID カードの表面


エストニア ID カードの裏面

カードの表面にはカード所有者の署名と写真が掲載され、また次のデータも含まれている。

- カード所有者の名前
- カード所有者の個人コード（国家 ID コード）
- カード所有者の誕生日
- カード所有者の性別
- カード所有者の市民権
- カード番号
- カードの有効期限

裏面には、次のデータが含まれている。

- カード所有者の出生地
- カードの発行日付
- 在住許可証の詳細およびその他の情報（該当する場合）
- マシン読み取り可能な（ICAO）形式でのカードおよび所有者のデータ

### 1.2.3　カード上の電子データ

各 ID カードには、さまざまなデータが含まれている。また、上に示したデータのうち、写真と手書きの署名を除くすべてのデータが、特殊な公的に読み取り可能なデータ・ファイルとして電子的な形式でカード上に記録されている。さらに、このカードには、2 つの証明書と、PIN コードで保護され、証明書に関連付けられたプライベート鍵が含まれている。これらの証明書には、所有者の名前と個人コード（国家 ID コード）のみが含まれている。さらに、認証用の証明書には所有者の一意の電子メール・アドレスが含まれている。以下、これらの証明書と電子メール・アドレスの詳細について説明する。

### 1.2.4　証明書

発行された各 ID カードには、認証用と電子署名用の 2 つの証明書が含まれている。また、カード上には 2 つの個別の PIN コードで保護され、証明書に関連付けられた 2 つのプライベート鍵も存在する。これらの証明書には使用の制限は存在しない。この証明書は本質的に汎用であり、個人間や組織間、またはカード所有者と行政機関の間など、任意の形式の通信に使用されるように考慮されている。また、この証明書には役割や認可は含まれていない。役割や認可が必要な場合は、何らかの帯域外の方法を使用して管理する必要がある（後述の「役割、認可、および組織の検証」も参照)。

証明書には、カード所有者の名前と国家 ID コードが含まれている。エストニアでは、このデータは本質的に公的なものであることが承認されている。名前は重複している可能性があるが、国家 ID コードは一意であるため、証明書によってカード所有者が一意に識別される。さらに、認証証明書にはカード所有者の電子メール・アドレスも含まれている。

欧州理事会および議会の電子署名指令 1999/93/EC の点から見ると、エストニア ID カード上の証明書はすべてクオリファイド証明書である。

### 1.2.5　電子メール・アドレス

各 ID カード上の認証証明書には、行政機関によって割り当てられたカード所有者の電子メール・アドレスが firstname.lastname_NNNN@eesti.ee の形式で含まれている。ここで NNNN は 4 つの乱数であり、これらの乱数は同じ名前を持つユーザーにも一意の電子メール・アドレスを提供するために必要である。このアドレスは、それ以降の証明書またはカードの発行でも変更されず、そのユーザーの「生涯の」アドレスであることが保証されている。

このアドレスに関連付けられた実際の電子メール・サービスは存在しない。このアドレスは単に、電子メールをそのユーザーの「実際の」アドレス（電子メール・アカウント）に転送するための中継アドレスである。各ユーザーは、その目的に利用可能なオンライン・サービスを使用して転送先アドレスを設定する必要があり、このアドレスは任意の頻度で再設定することができる。最大 5 つの転送先アドレスを指定できる。

このアドレスは、行政機関からユーザーへの通信に使用されると想定されているが、個人間の通信や、企業と個人の間の通信でも使用できる。これらのアドレスは、CSP の証明書ディレクトリを介して、だれでもオンラインで入手できる。

このアドレスは単純な電子メール・アドレスとして使用できるが、このアドレスとカード上の認証証明書を使用すると、ユーザーは自分の電子メールへの電子署名や暗号化も可能になる。電子メールの電子署名には法的拘束力がなく、DSA の対象範囲に含まれていないが、これによって、送信者の正当性に関する追加の認証が受信者に提供される。スマートカード上の証明書を使用した電子メールの暗号化や署名は、各種の電子メール・アプリケーションの標準の機能である。

転送サーバーにはスパム対策の手段が実装されている。さらに、エストニアではスパムの発信は違法であり、スパム発信者はそれに応じて起訴される。

### 1.2.6　データ保護

エストニア ID カードについては、カードの発行とそれ以降の利用プロセスに関連した個人データがほとんど存在しないため、データ保護はほとんど問題にならない。エストニアでは、個人データおよび個人データを含むデータベースの国家機関や民間団体による使用を規制する幅広い個人データ保護法が施行されている。この法令の要件が満たされていることを監督し、必要に応じてその遵守を強制する行政機関がエストニア・データ保護監察機関である。

カード上の証明書は、ディレクトリ・サービスから公的に入手可能であり、カード所有者の名前と個人 ID コードのみが含まれている。これらのデータは、エストニアでは本質的に公的なデータと見なされている。さらに、認証証明書内の電子メール・アドレスもディレクトリから入手できる。このディレクトリには、有効な（アクティブな）証明書のみが含まれている。個人が自分の証明書を一時停止または失効するとその証明書がディレクトリからも削除されるため、これらのデータは入手できなくなる。

公的なデータ・ファイルは、オンライン上にはどこにも公開されていない。視覚的および電子的な形式のカード上の個人データには、カード所有者がそのカードを物理的に渡した相手だけがアクセスできる。

エストニアにおける ID カードおよびデータ保護に対する一般的見地は、カードに含める個人データをできるだけ少なくすべきであるというものである。代わりに、データは関連機関に存在するデータベースに保持すべきであり、個人はカードを鍵（認可方法）として使用してデータベース内の自分のデータにアクセスできる。

### 1.2.7　組織の構造、カードの発行と運用

カードの発行とそれ以降の運用は、公共機関と民間機関の緊密なパートナーシップで実行される。ID カードの発行と運用、およびそれに関連付けられたインフラストラクチャーに関連する主な組織には、次の 3 つがある。

エストニア市民権・移民委員会（Estonian Citizenship and Migration Board、以下 CMB）は、エストニア国民および在留外国人への身分証明書の発行に責任を負う政府機関であり、これは身分証明書法で規定されている。CMB は、エストニア内務省の管轄にある。CMB は、国民からのカードの申込みを受け付ける。

エストニアの 2 つの主要な銀行である Hansapank と Eesti Uhispank、および 2 つの電気通信会社である Eesti Telefon と EMT によって設立された AS Sertifitseerimiskeskus（「証明書センタ

ー」、以下 SK）は、CA として機能し、カードの発行と使用のために必要な電子的インフラストラクチャーを維持すると共に、関連したサービスやソフトウェアを開発する。SK はまた、Hansapank と Eesti Uhispank の銀行支店を介した所有者へのカードの配布も担当している。

Swiss TRUB AG の子会社である TRUB Baltic AS は、カードを個別化する企業である。

カードの発行プロセスは、個人が CMB にカードの申込みを提出した時点で始まる。この申込みは本人が直接提出することも、郵送することもできる。CMB の要求に従って、TRUB がカードを個別化し、SK がカードに対する証明書を発行する。SK はまた、カードとその PIN コードを、カード所有者が申込み時に指定した銀行支店でカード所有者に発行する業務も行う。

カードを個別化するときに、カード上にプライベート鍵が生成される。この鍵がカードから出ることはない。また、セキュリティ上の理由から、いずれの鍵にも鍵供託システムは含まれていない。認証用の鍵と証明書を暗号化に使用することは可能であるが、これは主に、暗号化された電子メールなどの安全な伝送のためのツールとして使用されている。これらの証明書の有効期間は 3 年しかないため、この ID カードが長期にわたる文書の暗号化に使用されることは想定されていない。

さらに広いカード運用のために、SK では、LDAP ディレクトリ・サービス、OCSP 検証サービス、および有効性や電子署名のオンラインでの検証に必要なその他のサービスを含む関連した電子サービスを整備している。SK はまた、カードや電子署名に対するアプリケーションの作成に関心を持つすべてのユーザーにソフトウェアを提供すると共に、電子署名の実現や検証を行うための既製のクライアントおよび Web ポータルも提供している（後述の「文書形式と DigiDoc」を参照)。さらに、SK は、カードの紛失や盗難が発生した場合に直ちに証明書の有効性を一時停止するために使用できる 24 時間の電話ホットラインを開設している。

## 2. ソリューション

以下では、エストニア ID カードおよび電子署名インフラストラクチャーの実装中に解決されたいくつかの問題点や疑問点について説明する。

### 2.1 証明書プロファイルと電子メール・アドレス

エストニア ID カード上の証明書は、標準の X509v3 証明書である。認証用の証明書には、カード所有者の電子メール･アドレスが含まれている。証明書プロファイルは別の文書で入手できる。

### 2.2 証明書の有効性の検証方法

エストニア DSA によると、CSP は「証明書の有効性をオンラインで検証するための方法」を提供する義務がある。SK は、ID カードに対する証明書の発行者として、証明書の有効性を検証するための 3 つの方法をユーザーに提供している。

一時停止および失効された証明書の一覧を含む CRL が提供されている。CRL は標準の方法ではあるが、2003 年 1 月の時点で、CRL のサイズが 1 年間で 1MB 以上に増大して利便性が低下してい

るため、現在では時代遅れの方法になっている。CRL は主に、下位互換性および規格の遵守のために提供されている。SK は CRL を 1 日に 2 回更新している。デルタ CRL は提供されていない。

2 番目の方法は、すべての有効な証明書を含む LDAP ディレクトリである。このディレクトリはリアルタイムに更新される。証明書が有効になると、その証明書はこのディレクトリにアップロードされ、一時停止または失効されると、このディレクトリから削除される。何よりも、これによって、任意の ID カード所有者の電子メール・アドレスを検索する機会がすべての人に提供されている。サーバーを過負荷から保護するために、1 つの LDAP クエリーに対して返される応答の最大数についての制限が設けられている。

証明書の有効性を検証するための最も便利な方法が、SK の OCSP サービスである。この方法は、証明書の有効性の単純な検証だけでなく、電子署名に対する有効性の検証（「公証人認証」）にも使用できる。SK は、RFC 2560 に準拠した標準の OCSP サービスを提供している。この RFC 準拠の詳細部分で重要な点は、OCSP 応答は CRL に基づくと想定されているため、必ずしも実際の証明書の状態が反映されないことである。これに対して、SK では、マスターCA 証明書データベースから切り離された、CRL を使用しない運用方法で OCSP サービスが実装されている。そのため、SK の OCSP 応答には、実際の（リアルタイムの）証明書の状態が反映される。

## 2.3 OCSP、タイムスタンプ、および電子署名の証拠となる値

法的拘束力のある電子署名にとって、時間はきわめて重要な要素である。エストニア DSA および常識では、有効な証明書を使用して指定された署名のみが有効であると見なされる。しかし一方では、署名デバイス（ID カード）が PIN と共に盗まれ、ユーザーに成り代わった他の何者かによって電子署名が行なわれる可能性がある。こうしたリスクへの対応策を提供するために、ユーザーには、SK によって運営されている 24 時間の電話ホットラインを使用して自分の証明書の有効性を一時停止する機会が与えられている。この 2 つの概念を組み合わせると、ユーザーは、有効な証明書を使用して指定された署名と、一時停止または失効された証明書を使用して指定された署名を明確に区別できる必要がある。したがって、署名、時間、および証明書の有効性を結びつけるタイムスタンプおよび有効性の検証サービスが必要になる。

署名の有効性に関する別の重要な概念に、既に証明書の期限が切れていたり、証明書が失効されたりした場合でも署名は有効でなければならないという点がある。証明書がカード所有者または他の何者かによって一時停止されても、カード所有者は、銀行支店でその証明書を再び有効にすることができる。

SK は、タイムスタンプを標準の OCSP に基づいて実装することを選択した。これにより、サービス・プロバイダーは、証明書の有効性と時間の情報を 1 つの便利なクエリー応答で適切に配信できるようになる。OCSP プロトコルのクエリー形式には、反射攻撃（リプレイ・アタック）から保護するための Nonce フィールドが含まれている。この Nonce フィールドは、暗号的な乱数データではなく、署名されるデータのハッシュを含むように設定される。このデータも単なる乱数として解釈できるためである。OCSP レスポンダは、RFC に従って応答に署名する。SK の場合、この応答には、元の Nonce（文書ハッシュ）、応答の提供／署名時間、および署名の提供に使用される証明書の ID が含まれており、この 3 種類のデータが結びつけられて電子署名の有効性の検証が実

現される。SK は、署名された応答を証拠資料としてログに格納する。

上で説明した概念の主な機能は次のとおりである。

- 電子署名および文書の長期にわたる有効性を保証する。
- 標準のプロトコルと規格に基づいている。
- 検証プロセスが軽量で、文書が自己完結型であるため、追加の検証サービスを必要としない。

SK は、その DigiDoc 電子署名アーキテクチャーに、クライアントとサーバーの両方の部分を含む、これらの機能のすべてを実装している。

## 2.4 文書形式と DigiDoc

電子署名を日常的なものにするには、共通の理解および署名の処理方法が必要になる。さらに、互換性のあるアプリケーションを作成するには、ソフトウェアや技術が、関心を持つすべてのユーザーにとって利用可能でなければならない。最終的に、電子署名の潜在的な利点を解放するための鍵は、1 つの組織内ではなく、組織間の通信に存在する。そのため、特定のコミュニティー内のすべての組織が電子署名を同じ方法で解釈し、理解することがきわめて重要である。エストニアの場合は、このコミュニティーが国全体である。

市場には電子署名に関する利用可能な実装やアプリケーションが多数存在しており、それらのすべてが特定の目的に適していると謳っている。しかし、エストニア・プロジェクトのニーズに適すると考えられる、最新の標準に基づいた既知のアプリケーションや実装を見つけることはできなかった。また、電子署名に頼る一国の日常生活の機能を保証している外国のソフトウェア・プロバイダーへの依存も、戦略的なリスクと見られる場合がある。そのため、まったく新しいアプローチ、および、まったく新しいソフトウェア・アーキテクチャーが必要とされた。

2002 年、SK はパートナーと共に、DigiDoc と呼ばれる総合的な電子署名アーキテクチャーを作成した。この名前が示すように、DigiDoc は電子署名の作成、処理、および検証に関してユーザーが必要とする可能性のあるすべてのニーズを満たすことを目的にしている。

サーバー側では、DigiDoc は RFC2560 に準拠した OCSP サーバーを提供する。このサーバーは、マスターCA 証明書データベースを直接操作して、証明書や署名に対する有効性の検証を実現する。また、クライアント側ではいくつかのコンポーネントを提供する。

最も重要なコンポーネントは、電子署名の一般的な実装および実施にとって重要なデジタル文書形式である。2002 年の時点では、いくつかの標準が採択または準備されていた。SK は、DigiDoc 文書形式を XML-DSIG 標準に基づいて実装した。2002 年 2 月、ETSI は XML-DSIG に対する拡張機能を ETSI TS 101 903（XAdES ともいう）として公開した。DigiDoc 文書形式は、そこで提案された拡張機能のサブセットを含む、XAdES のプロファイルである。DigiDoc 形式は仕様書に記述されている。

この文書形式に基づいて、次のコンポーネントを結びつけるライブラリが C 言語で開発された。

- DigiDoc 文書形式
- SK の OCSP 検証サービス
- Windows のネイティブな CSP インターフェースまたはクロス・プラットフォーム PKCS#11

を使用した、ユーザーの ID カードとのインターフェース

DigiDoc ライブラリでは、上のすべてのコンポーネントに対する使い勝手の良いインターフェースが提供されているため、アプリケーション開発者はOCSP プロトコルの詳細やDigiDoc(XAdES、XML-DSIG) 形式の内部を理解している必要はない。このライブラリを任意のアプリケーションの内部またはアプリケーションの上に組み込むことができる。COM インターフェースが実装されているため、DigiDoc サポートを、COM 技術をサポートしている任意の Windows アプリケーションに追加することが容易になっている。また、Java 実装も提供されている。

ただし、実際のアプリケーションがなければエンド・ユーザーにとって価値は生まれないため、ライブラリと形式を提供するだけでは不十分である。DigiDoc サポートは、文書などを扱うエストニアのほとんどの文書管理システムや Web サイト内で最終的に実現されることになると予測されているが、いくつかの例または「参照」アプリケーションも提供されている。DigiDoc クライアントは、ユーザーが文書への署名や文書の検証を簡単に行うことができる Windows アプリケーションである。一方、DigiDoc ポータルは、ユーザーがスタンドアロン・ソフトウェアをインストールしなくても、それと同じ操作をオンラインで実行できるアプリケーションである。当然ながら、どちらも同じ DigiDoc ライブラリに基づいているため、完全に互換性がある。クライアントで指定された署名はポータルで検証することができ、その逆も可能である。

これらのライブラリ、仕様、およびアプリケーションはエストニア国民に無料で提供されており、日常生活や、企業および行政機関の通常業務での電子署名の使用は 2003 年には大幅に増加していると予測される。エストニアにおける最初の公式の電子署名は、2002 年 10 月 7 日に DigiDoc クライアントを使用して提供されたが、国家的な規模での電子署名の実装には必然的に時間がかかる。

## 2.5 役割、認可、および組織の検証（Roles, authorizations and organizations' validations）

PKI や電子署名の実装に関連して、役割と認可に関する問題がさまざまなプロジェクトで発生してきた。前提になっているのは、電子署名のための証明書は特定の目的でのみ発行できること、および個人の役割を役割証明書（role certificates）に埋め込み、次にその役割証明書を使用して別のシステムに対して証明書所有者を認証したり、別の役割の電子署名を生成したりできることである。したがって、ユーザーは自分が持っている各役割に対して追加の役割と署名証明書が必要になるため、証明書の数が増加し、それによって相互運用性や拡張性に関する重大な問題が発生してきた。

エストニア DSA でも規定されているように、エストニアのアプローチでは、電子署名用の証明書を使用して指定された電子署名は手書きの署名とまったく等価であると規定している。個人の手書きの署名には、その個人の役割は含まれていない。この役割と認可は、何らかの帯域外（証明書との関連における帯域外）の方法を使用して確立される。これと同じアプローチが、認証時の認可にも適用される。個人の証明書には、その個人の認可資格情報は含まれていない。代わりに、すべての個人に同じ汎用的な鍵（認証用の証明書）が与えられ、個人の役割と認可は、オンライン・データベースなど、その鍵に基づく何らかの他の方法を使用することによって決定でき

る。

このような概念を示す実際的な例として、組織での委任状による文書への署名がある。従来の PKI 環境では、この処理は、既述の問題が発生するような何らかの形式の属性証明書を使用して実行されてきた。エストニアおよびPKI の環境では、実生活における委任状の作成方法を明らかにし、電子的な文書管理にそれと同じ原則を使用する方法が考えられる。従来、委任状は、その認可を与えた人物によって署名された文書の形式で許可されてきた。この文書は次に、認可を受ける人物に与えられ、その人物は必要に応じてその文書を関係者に提出できる。これと同じ処理を電子的に実行することが可能である。つまり、委任状を与える人物は、自分の汎用の個人用証明書を使用して文書に署名し、その文書を認可が与えられた人物に転送することができる。次に、この人物はこのデジタル委任状に、自分が署名するその他の文書を同封できる。その後、この文書を受け取った人物は元の署名された文書と、その人物がこれらの文書に署名する権限を実際に持っていたことを確認する同封された委任状の両方を確認できる。

当然、既述した汎用の証明書や文書に関連して属性証明書を使用することもできるが、エストニアの概念はどちらかといえば汎用の証明書を対象としている。

上の説明の例外は、組織の検証である。デジタル文書は、他の組織がその文書を発信した組織の ID を確認できるように、元の組織による検証が必要な場合がある。これは、たとえば、銀行取引明細書など他の組織に提供されるデータベースにオンラインで署名する場合に有効である。この目的に合わせ、SK は文書への電子署名に使用できる証明書を組織に発行している。事実上、この証明書はすべての人の ID カード上の個人の署名証明書と等価であるが、法律的には署名とは見なされず、エストニアの法律によると、署名を提供できるのは実在の人物だけであるため、法律の対象範囲に含まれる必要はない。したがって、「組織の署名」は単純に（それが実際に特定の組織から発信されているという）情報の正当性を証明するための追加のツールと見なす必要がある。この情報には、その組織で作業している実在の人物の電子署名が添付されている場合もあれば、添付されていない場合もある。ただし、PKI の複雑さはここまでであり、個人および組織の署名用の証明書を除けば、個人の役割証明書やそれより複雑なものは何も必要がない。

## 2.6 さらなる開発：臨時カードと代替カード

2003 年当初の時点で、エストニアにおける電子署名の可用性と操作性を向上させるためのアイデアがいくつか議論されている。その 1 つが、「臨時 ID カード」すなわち予備カードである。ここでの主な関心事として、既述のカード発行プロセスがきわめて複雑であり、現在の規定に従うと、個人がカードを申し込んだ時点からカードを受け取るまでに最大 30 日かかる場合がある。カードを紛失したり損傷したりして個人が新しいカードを取得する必要が発生した場合、30 日間も電子署名を提供できなくなることがあり、これは競争の激しいビジネス環境では受け入れられない可能性がある。そこで、このような問題の範囲を最小限に抑えるために、現在の ID カード所有者が「予備カード」を取得できるようにすることも考えられる。ただし現在この対策は実装されておらず、この問題に対する別の対応策として、料金は高いが「通常の」方法で ID カードをより速く取得できる「至急サービス」だけを既述の組織が実装するというものがある。

今後予定されている別のサービスに「代替カード」がある。国家 ID カードが、電子署名用の

証明書の唯一の運搬媒体であるとは限らない。また SK は、エストニアに居住しておらず、エストニア ID カードを持つ必要がないユーザーにも証明書を発行できる。この対応は、多国家間の業務における社内サービス用として既にスマートカードを使用しており、SK によって発行された電子署名用の証明書を社内のカードに追加することによって複数の国にわたる共通のインフラストラクチャーを作成したいと考えている大企業にも必要である。この企業自体が登録機関として機能し、SK は通常の ID カードの場合と同様に、証明書の要求に応えて証明書を発行する役割を果たす。ただし、この「代替カード」はニッチ・ソリューションにとどまるであろう。一般大衆にとっては、各人の役割にかかわらず、エストニアの国家 ID カードが汎用の署名ツールである。

## 2.7 電子署名の国際的な有効性

国際的な通信において法的拘束力のある電子署名は、新たに出現しつつある領域である。ほとんどの国ではまだ国内の習慣や法律が、電子署名が日常的な通信で広範に使用される状況に対応できるほどには実現化していないため、このような習慣の調和が今後数年間の課題として残っている。

標準の拡張によって、相互運用性ではなく多様性が生まれてきた。現在の標準は、また、ある程度までは法律も同様に、PKI や証明書に関連する可能性のあるすべての取引を対象範囲に入れ、それらに異なった内容の法的権限を与えようとしている。これがまた、複雑さや混乱に拍車をかけている。

この点に関して、エストニア ID カードの実装者は、デジタルの世界は従来の文書管理に類似しており、文書や通信には次の 2 つの基本的な種類が存在するという見解を示している。

1) 法的拘束力のある署名された文書。電子署名か手書きの署名かは問わない。
2) それほど厳密に規定する必要のない、その他の任意の形式の通信。

公証文書（従来の意味で公証人制度に関連付けられているもの）は、1）の特殊な事例である。

たとえば、エストニア行政規則では、文書または管理法への署名が必要とされていないすべての事例において、署名または暗号化された電子メール、FAX、電話、口頭の会話など、双方にとって便利なその他の任意の通信手段によって解決できると規定されている。役人が行う必要があるのは、文書管理システムで事例の解決方法に関する適切な通達を作成し、適切な連絡先やその他の詳細情報を追加することだけである。ただし、文書への署名が必要な場合は常に、電子署名か手書きの署名のどちらかが必要である。

国際的に相互運用可能な電子署名の場合は、双方（両国）が相手国の規則によって発行された署名を認める必要がある。ここで考慮すべき主な技術的側面として次の 3 つがある。

- 発行された証明書の品質。1999/93/EC の点から見ると、法的拘束力のある電子署名を提供するために使用される証明書は、署名人を明確に示しているクオリファイド証明書でなければならない。
- 署名および文書自体に使用されている形式。前述の DigiDoc システムは間違いなく有効なオプションである。なぜなら、現在のところ電子署名とそれに関連した技術情報のための最も高度な標準と考えられる XAdES 標準に基づいているためである。ここで重要な側面は、

この形式やソフトウェアが、公共の監査、確認、綿密な調査向けに、できればオープン・ソースで利用可能でなければならないということである。XAdES 標準と DigiDoc ソース・コードはどちらも、任意の当事者が利用できる。

- システムの信頼性と署名の有効性を保証するために、署名および認定に関連付けられているインフラストラクチャー・サービスの内容。ここでは、エンド・ユーザーへの署名デバイスの配信や、証明書の一時停止のための緊急ヘルプデスクの利用可能性、あるいは証明書や電子署名の有効性の検証のために CA によって提供されるサービスなどの、特定の品質の証明書関連サービスを想定している。1 つのオプションとして、DigiDoc に関連して既に説明したように、すべてのオンライン有効性検証に標準の OCSP ベースのサービスを使用する方法がある。

別の重要な問題は、紛争がどの司法権の下で解決されるかという点である。これは、一般的な国際協定の司法権の場合と同じである。契約では通常、どの司法権の下で決定されるか、および紛争がどこで解決されるかが定義される。そのため、契約自体でも、紛争が発生した場合に、証明書や署名に対してどの法律の要件が考慮されるかが示されることがある。当然、契約のみの場合は電子署名は使用されず、おそらくより汎用的なアプローチが必要になる。

## 2.8 OpenXAdES プロジェクト

2002 年初めのエストニア ID カード・プロジェクトが開始当初から、電子署名を提供するためにすぐに利用可能なソリューションの調査が始まったが、既述の通り、エストニアのすべてのニーズに適したソリューションは見つからなかった。そこで、そのようなニーズに適したシステムが必要であるという判断から、DigiDoc が開発された。

エストニア ID カード・プロジェクトは国際的な注目を集め、現在も引き続き注目されている。「汎用の電子署名／文書」という概念をエストニア国境を超えて促進するために、OpenXAdES というコード名のプロジェクトが必要であると判断した。この名前は、オープンな通信とそれに伴う国際標準に対する我々の取り組みを示している。この技術は現在、www.openxades.org で他の国やコミュニティーから利用できるようになっている。このサイトでは、プロジェクトの背景にある我々の動機について説明し、ダウンロード用にマニュアルおよびソフトウェア・ライブラリを提供している。2003 年の夏には、このサイト上でいくつかのテスト・サービスを稼働させる予定である。これらのサービスは、電子署名用の証明書を含むスマートカードを所有している人ならだれでも無料で使用でき、それにより文書への署名や文書の検証を行うことができる。

我々の目標は、OpenXAdES を異なる法律や技術標準に準拠させながら、法的拘束力のある電子署名および文書に引き続き焦点を絞ることである。OpenXAdES は、異なる法律および異なる規則の下で発行されたスマートカードやその他の署名トークンと連携することができる。このプロジェクトの最終目的は、法的拘束力のある電子署名やペーパーレスの文書管理を日常的な生活、ビジネス、および通信に導入することにある。エストニアではこのような状況が既に実現しており、この技術によって各種の関係が変貌を遂げている。我が国で経験しているものと同じ利点を他の国でも実現できるように支援したいと考えている。

OpenXAdES は、その名前が示すように、だれもが自由に参加できるオープン・イニシアティブ

である。2003 年 5 月、AS Sertifitseerimiskeskus と Finnish Vaestorekisterikeskus（住民登録センター、PRC）は、デジタル文書をフィンランドとエストニアの国内および両国間で実現化することを目標に、両国間での電子署名の相互運用性を向上させるための契約に署名した。他のコミュニティーの他の関係者にもこのプロジェクトへの参加を求め、それによって「デジタル国家」のネットワークを拡張していきたい。

# 金融機関における電子認証の活用動向

# 金融機関における電子認証の活用動向

平成18年6月21日

財）金融情報システムセンター

調査部

1

## 金融機関における電子認証の活用動向

＊電子認証の導入

1）インターネットバンキング等非対面取引の増加

2）フィッシング等ネット犯罪の急増

3）セキュリティ強化の必要性

国内金融機関の電子認証の導入事例

| 金融機関名 | 提供対象 | 導入機能 | 導入サービス | 導入方式 |
|---|---|---|---|---|
| 三井住友銀行 | 法人 | 本人認証<br>電子署名 | 共通認証サービス<br>（インターネットバンキング、外国為替など） | ウェブブラウザもしくはICカードに格納の<br>電子証明書方式による本人認証および電子署名 |
| 東京スター銀行<br>（NTTデータ） | | 本人認証 | インターネットバンキング | 電子証明書方式による本人認証 |
| 愛知銀行 | | 電子署名 | 電子メール送信 | 電子証明書方式による電子署名 |
| 新銀行東京 | 個人 | 本人認証<br>暗号通信 | インターネットバンキング | ICカード＋パスワードによる2要素本人認証<br>ICカード＋共通鍵暗号方式による暗号通信 |
| 野村證券 | | 本人認証 | インターネットトレーディング | 電子証明書方式による本人認証 |

2

## 金融機関における電子認証の活用動向

### ①三井住友銀行（自営型）

・提供サービス 「Value Door」（法人向け）

**導入経緯**

・顧客サービスの向上

・信頼される銀行

・インターネットサービスの本人認証の強化の必要性

・グループサービスの効率化

**サービス概要**

・本人認証方式

Ⅰ）ダウンロード方式 ・・・利用料無料、エクスポート禁止

Ⅱ）ICカード方式 ・・・要初期契約料・月額基本使用料、要専用機材

Ⅲ）ID・PW方式 ・・・資金移動を伴わない場合のみ

3

## 金融機関における電子認証の活用動向

**サービス概要**

・有効期限1年間（有効期限の1ヶ月前から電子証明書の更新可能）

・EBサービス内容

主銀行取引以外を含めたEBサービスの窓口となっている

| ValueDoorでは、 | | |
|---|---|---|
| 国内振込・振替、口座照会等 | ＜法人向けインターネットバンキング＞ パソコンバンクWeb21 | パソコンバンクナビWeb |
| 外為取引 | Global e-Trade サービス | i-Deal(アイディール) |
| 手形事務合理化 | e-パッケージ | e手形レス・e手形発行サービス |
| 関連会社サービス | SMBC経営懇話会 (SMBCコンサルティング株式会社提供) | PAYWEB (SMBCファイナンスサービス株式会社提供) |
| | FinancialLink (フィナンシャルリンク株式会社提供) | |

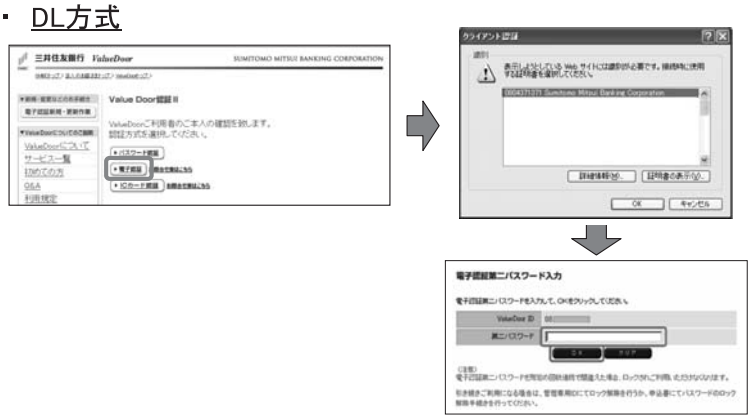
4

## 金融機関における電子認証の活用動向

**利用**

・本人確認 ・・・ DL方式 （法人名義にて発行）
ICカード方式 （法人役職員に発行）

・利用方法 ・・・ DL方式




IC方式

・事前に設定した端末のICカードリーダーにICカードを挿入し、「ICカード用のパスワード（ユーザーPIN）」を入力することにより認証する。
・ICカードを読み取るためのカードリーダーとICカードが必要。
（ICカード方式の場合初期費用が必要で、約1年毎にICカードの更新が必要）

5

## 金融機関における電子認証の活用動向

**現状及び今後の展開**

・大企業等での利用が活発
・外国為替取引のインターネット取扱いが増加
・ドキュメンタリー取引の利用者及び銀行の事務効率化
・他行や他社への認証代行サービス提供によるビジネス化

法人トップ画面
（2006年2月現在）


出所）三井住友銀行HPより

6

## 金融機関における電子認証の活用動向

### ②東京スター銀行（共同センター型）

・提供サービス

インターネットバンキング「スターBB」（法人向け）で電子認証を利用

**導入経緯**

・法人用ネット取引における高セキュリティの必要性

・都市銀行と同レベル以上の高セキュリティのアピール

・NTTデータの共同センターにおける認証局代行サービスの開始

・導入コストの低下　（「ANSER－WEB（AAC）」のオプションサービス）

**サービス概要**

・本人認証方式

Ⅰ）ダウンロード方式

・・・利用料無料、エクスポート禁止、1契約20ID

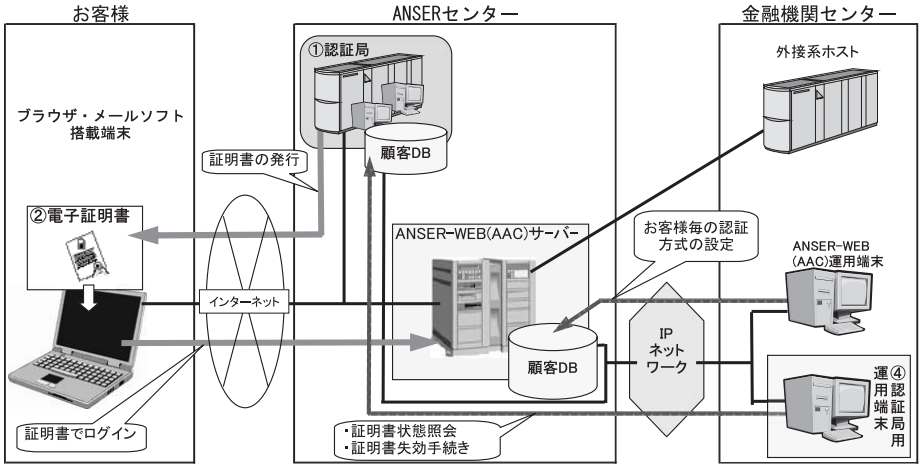
Ⅱ）ID・PW方式　　・・・Ⅰ及びⅡの併用は不可

7

## 金融機関における電子認証の活用動向

**サービス概要**

・NTTデータの共同センター利用




（注）金融機関の認証局用運用端末は，ANSER－WEB運用端末と共用利用が可能「ANSER-WEB（AAC）」

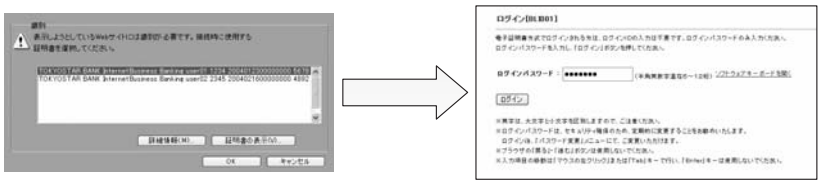
（出所）NTTデータ

8

## 金融機関における電子認証の活用動向

**利用**

・DL後は電子証明書を提示し、ID・PWを入力することで利用可能となる



出所：東京スター銀行

・有効期限366日（有効期限の30日前から電子証明書の更新可能）

**現状及び今後の展開**

・法人取引であるため、新規利用者の8割が電子証明書方式を採用

・関東のみならず広域で採用

・顧客需要の対応（利用環境の改善等）

・共同センターを活用したビジネスモデルの構築

9

## 金融機関における電子認証の活用動向

### ③新銀行東京

・提供サービス

個人向けインターネットバンキングでICキャッシュカードによる電子認証を利用

**導入経緯**

・店舗網の補完

・ICキャッシュカードの活用

・NTTコミュニケーションズの「セーフティパス」

・導入コストを抑えられる （業務委託、開発不要等）


出所）新銀行東京HPより

**サービス概要**

・本人認証方式

Ⅰ）セーフティパス方式

・・・初年度無料、ICカードリーダーは無償貸与

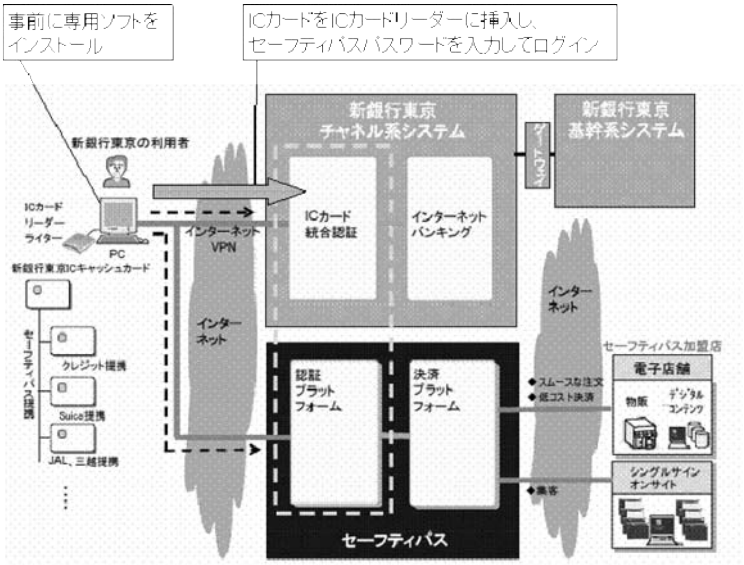
Ⅱ）ID・PW方式 ・・・Ⅰ及びⅡの併用可能

10

## 金融機関における電子認証の活用動向

### サービス概要

・NTTコミュニケーションズが提供するICカード総合認証基盤を利用




（出所）新銀行東京資料をもとにFISCにて一部追記

11

## 金融機関における電子認証の活用動向

### 現状及び今後の展開

・セーフティパスの顧客利用は低迷

・ネット犯罪の未然防止のため安全性をよりアピール

・法人サービスへの採用

同行のインターネットバンキング画面


出所）新銀行東京HPより

### ④その他

・野村證券等の証券会社では一部導入が見られる。

・ネット証券会社ではほとんどが、ID・PW方式を採用

12

## 金融機関における電子認証の活用動向

### 金融機関における電子認証導入の現状と今後

・金融分野を取り巻くネット犯罪が増えたために、セキュリティの強化に取組む金融機関は増えている。
・主に法人向け取引で電子証明書による本人認証が採用されている。
・共同センターを利用している金融機関では、今年度中に多く採用されるものと思われる。
・個人向けサービスでも、本人認証の強化の必要性が高まっているものの、現状では従来通りのID/PW方式やワンタイムパスワード方式のような簡便な方式が普及している。
・セキュリティに対する認識が高まっていることから、業界での共通認証基盤を導入したり、他の認証基盤との相互認証を行ったりと、より広範囲での連携が重要。
・金融に限定しないさまざまな場面での活用ができるモデルが必要。

13

## 金融機関における電子認証の活用動向

ご清聴ありがとうございました

財）金融情報システムセンター
調査部

14

# メンバリスト

事務局

| | |
|---|---|
| 前田　陽二 | 次世代電子商取引推進協議会（ECOM） |

顧問

| | |
|---|---|
| 大山　永昭 | 東京工業大学 |
| 菅　　知之 | 関西大学 |
| 平田　健治 | 大阪大学　大学院 |

幹事

| | | |
|---|---|---|
| 幹事（第１部担当） | 松本　　泰 | セコム株式会社 |
| 幹事（第１部担当） | 榎本　　尚 | 花王インフォネットワーク株式会社 |
| 幹事（第２部担当） | 政本　廣志 | 日本電信電話株式会社 |
| 幹事（第２部担当） | 高塚　　肇 | NTT コミュニケーションズ株式会社 |

編集メンバ（上記幹事以外）

| メンバ名 | 団体名 |
|---|---|
| 小林　信博 | 三菱電機株式会社（第１部） |
| 中村　克巳 | 三菱電機情報ネットワーク株式会社（第２部） |

オブザーバ

| メンバ名 | 団体名 |
|---|---|
| 安西　慶修 | （財）金融情報システムセンター（FISC） |
| 高津　岳志 | （財）金融情報システムセンター（FISC） |
| 堀田　康裕 | （財）金融情報システムセンター（FISC） |

メンバ（上記以外）

| メンバ名 | 団体名 |
|---|---|
| 出本　　浩 | 株式会社エヌ・ティ・ティ・データ |
| 西田　　梢 | シヤチハタ株式会社 |
| 長島　健一 | 大日本印刷株式会社 |
| 柴田　和充 | 電気事業連合会 |
| 千葉　昌幸 | 株式会社三菱総合研究所 |
| 田中　　稔 | 三菱電機株式会社 |
| 伊藤　正剛 | 株式会社帝国データバンク |
| 斉藤　敦久 | 株式会社リコー |
| 寺尾　雄一 | 株式会社リコー |

電子署名普及に向けた調査検討報告書（２）
―海外及び国内金融分野での利用動向―

平成 19 年 3 月発行

発　行　　次世代電子商取引推進協議会

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
東京都港区芝公園三丁目 5 番 8 号
機械振興会館　3 階
TEL：03(3436)7500

この資料は再生紙を使用しています。