

住民基本台帳カードをベースとした 連携ICカード導入の技術的問題点

Issues in Governmental Multi-application Smartcard*

山根 信二

岩手県立大学教員・CPSR/Japan

s-yamane@computer.org

2003年2月16日更新

目次

1	はじめに	2
2	スマートカード開発とセキュリティ	2
3	連携ICカード導入の経緯および問題点	3
3.1	2001年: 関係府省連絡会議	3
3.2	2002年: 技術仕様	4
3.3	ISO導入は改善策となるか	5
3.3.1	セキュリティ技術標準の課題	5
3.3.2	セキュリティ運用標準の課題	6
3.3.3	両者に共通する課題	6
3.4	カードの保護レベルと無関係に発生する問題	7
4	電子政府に関するセキュリティの比較検討	8
4.1	アメリカ合衆国のセキュリティ評価事例	8
4.2	ドイツ連邦のセキュリティ評価事例	8
4.3	英連邦のセキュリティ評価事例	9
4.4	比較と考察	9
5	おわりに	10

*本報告は2003年2月15日(土)に東京都国立市で開かれた「住基ネット第2次稼働へ向けての運動のためのワークショップ」第1分科会「住基ネットの制度的技術的問題点の解明と電子政府」にて発表された。本報告の一部はSymposium on Cryptography and Information Security 2003での発表[31]に基づいている。本報告にはいくつかのバージョンがあるため、引用の際には日付を明示されたい。本報告は2003年に出版されるCPSR/Japan報告書に収録される予定である。

1 はじめに

電子政府 / 電子行政サービスにおいて用いられる暗号製品 (暗号モジュール) が「信頼できる」ものか否かの評価は容易ではない。アメリカでは、連邦政府が調達する暗号モジュールの要件として連邦情報処理標準 FIPS140 が 1994 年 1 月に制定され、既に 10 年近い運用実績を持っているが、日本にはそのような実績はない。そしてアメリカのみならず、イギリス・フランス・ドイツに比べても暗号モジュールの評価において遅れをとっていることは総務省 / 経済産業省の暗号技術検討会も認めている事実である [3, p. 30]。2003 年初頭の時点で、暗号製品試験設備を備える評価機関で国際的な信頼を得ているものは日本国内には存在しない。

本報告では、暗号モジュールの中でも特にスマートカード (IC チップ搭載カードの中でも計算能力を持ったもの) について検討する。日本政府は行政サービスの一環としてスマートカードの配布を行なうが、そこには多くの問題がある。すでに法制の不備や運用面での問題が指摘されているが、本報告では特に情報セキュリティ対策面でのチェックに注目して検討を行なう。

2 スマートカード開発とセキュリティ

スマートカードに対して、すでにならぬ攻撃方法と防御手段が提案されている。それらはチップに対する攻撃、暗号プロトコルに対する攻撃、そしてカード偽造にいたる広い範囲にわたり、学術的な検証が行なわれているものだけでも Timing Attack, Simple Power Analysis, Differential Power Analysis, Chosen Protocol Attack [2], Optical Fault Induction Attack [17] といった手法があげられる。こうした攻撃に対して耐えられるセキュリティ機能がスマートカードには要求される。

スマートカードの開発においてセキュリティはかならずしも優先順位が高くない。CRYPTREC が国内のメーカーおよびベンダー 17 社に対して行なったアンケート結果によれば、スマートカードに用いる暗号の技術的要件として最も多い回答は、実装サイズ、実装可能性、処理速度だった。それらに比べて、セキュリティを保証する耐タンパ性や暗号強度の優先順位は低い [3, 資料 要件調査ワーキンググループ報告書 p. 10]。スマートカードの物理的制限を考慮した場合、現在のところ、サイズをセキュリティよりも優先した開発が行なわれること自体は驚くに値しない。この現状を踏まえて、3rd Generation Smart Card Project や新たな暗号アルゴリズムの研究開発を通じたスマートカードのサイズとセキュリティを両立させる試みも推進されており、そう遠くない将来にはさらに信頼性の高いスマートカードの一般製品化も期待される¹。だが、その時が来て「いままで使っていた製品は、本当は安全性が高くありませんでした。これからはもっと安全性の高い製品を使いましょう」と利用者には知らせるのでは遅い。手術を行なう医者が患者に対する説明責任 (アカウントビリティ) があるように、暗号製品を推進する者、そして採用する者は利用者へのアカウントビリティが要求される。特に公共サービスにおいてはこの原則を忘れてはならない。

¹ただし、経済的に引き合わないので実現しないだろうという見方もある [2, §14.6.3]

3 連携ICカード導入の経緯および問題点

パーソナルコンピュータで異なる複数のプログラムが動作するように、1枚のスマートカード上においても複数のプログラムやデータを格納し動作させることができる。そして近年では、政府機関・地方自治体・民間のサービスを1枚の共通カード上に相乗りさせる構想が「連携ICカード」として推進されてきた。本章ではその導入過程における技術的チェックについて検討する。

3.1 2001年：関係府省連絡会議

連携ICカードについて検討および決定を行なった機関は、「公的分野における連携ICカードの普及に関する関係府省連絡会議」（以下「連絡会議」と略す）である。この機関は2001年4月に初会合を行ない、具体的な検討は各府省の課長補佐クラスでつくる作業部会が担当している [6]。

当初より住民基本台帳カード上に複数の行政アプリケーションを搭載することが検討されていたが、それが決定したのは2001年7月27日の連絡会議においてである。この場で、2002年8月から市町村長が住民の申請により交付する住民基本台帳カードのスペックをベースとすること、また政府、地方自治体、民間組織のアプリケーションがカード上で実行できるようにすることが確認された [14]。基本方針では、連携ICカードがクリアすべき要件は以下のように簡潔に定められている [14, §2.(1)]。

1. 国民全体の利便性の網羅的な向上に資すること
2. 格納情報間の独立性を確保すること
3. 個人認証基盤として利用できること
4. 技術的スペックの柔軟性を確保すること
5. 高度な安全性を確保すること
6. 居住地移動にも適合するポータビリティを確保すること

まず問題となるのは、スペックのベースとなるはずの住民基本台帳カードの仕様はこの時点ではまだ決まっていなかったことである。（住民基本台帳カードの仕様書が財団法人地方自治情報センターによって策定されたのは、連絡会議で採用が決まった後の2001年10月のことである [15, §1.1]）。具体的なスペックの検討なしに、政府機関でもない組織の計画が政府調達システムに採択されるという事態は通常では考えにくい。もしも採択する理由があるとするれば、地方自治情報センターに確固たる実績があった場合である。しかしながら地方自治情報センターは住民基本台帳ネットワークの稼動においてセキュリティ・マネジメント能力および再発防止策の立案能力が欠如していることを示しており [19, 21]、要件の「高度な安全性を確保すること」についての実績がない。したがって採択にあたっては要件に含まれていない別の理由、たとえば「以前からやっていた」というだけの理由で住民基本台帳カードが採用されたと言わざるをえない。

3.2 2002年: 技術仕様

地方自治情報センターによってようやく策定された住基カードの技術仕様をベースとして、「公的分野における連携ICカード技術仕様」[15]が連絡会議において確認されたのは2002年3月のことである。しかしその内容は乏しく、セキュリティ専門家が貢献した形跡が見られない。以下に技術仕様のうちセキュリティに関わる点について分析を行なう。

暗号処理については必須仕様として「公開鍵の暗号処理機能」、推奨仕様として「RSA1024bit同等以上の強度」としか示されていない。認証機能を持つスマートカードは公開鍵暗号と共通鍵暗号とハッシュ関数というそれぞれ異なる暗号機能を組み合わせて設計されており、それらが欠けたものは「個人認証基盤として利用できる」ことが要件となっているスマートカードの技術仕様とは呼べない²。同時期にはCRYPTRECによって電子政府推奨暗号の評価作業が進められていたにもかかわらず、「公的分野における連携ICカード技術仕様」には暗号技術に関して明瞭な記述を示されていない。この事は、技術仕様策定における専門的な検討を疑わしいものに行っている。

また物理的仕様についての規定は「耐タンパ性を有する」ことが必須仕様にあるだけで、どのような試験に耐えられるのかという尺度をまったく規定していない。これでは物理的セキュリティはただの努力目標でしかない。

さらに、要件の一つである「格納情報間の独立性」についても具体的な保護手段が示されていない。データの独立性は製品テストだけで保証できるものではなく、請負業者のOS開発体制まで管理しないと努力目標に終わるおそれがある。たとえば、データの独立性が破られる欠陥の事例としては、2001年にNTTドコモの携帯電話機SO503i(ソニー製)で他のアプリケーションが格納していたデータにアクセスできた欠陥があげられる。この欠陥は一般の開発者によって指摘され、報道機関はメーカー、ベンダー、そして監督官庁に対して確認を求めたが、それらの関係者はいずれもデータの安全性は破られてはいないと回答した。その後、その回答は撤回され、該当機種は販売停止および42万台の無償交換に至っている[11]。スマートカードとはOSおよびデータの格納方式が異なるので一概に比較できないが、この事件はアプリケーションデータの独立性を保つことの難しさ、それをテストで発見することの難しさを示している。そしてこの種の事故は一部の問題業者だけではなく、日本の大量市販製品におけるソフトウェアのセキュリティ品質管理体制が決して高くないことを示す一例として考えるべきである[9]。

カードの表面加工については、別途「連携ICカード券面の偽造防止技術ハンドブック」[16]が出されており、カード偽造に対するセキュリティ対策は物理面や暗号技術面よりも比較的細かく規定されていると言える。しかしながらこのセキュリティ規定は、「誰から何を守るのか」というターゲットが的外れである。ハンドブックではセキュリティを高めるためとして試験技術についての詳細な記載を避けている[16, §7]。しかしながらアメリカの連邦政府調達基準をはじめとする現代的なセキュリティ基準の要点は、機構が暴露されてもお信託できる点にある。(ただし、試験方法を公開してもその実施理由を示さないことはあり得る。) それに対して上記ハンドブックでは大学専門課程の教科書[2, §12, §19.3.2]に出てくる程度のセキュリティ技術まで省略しており、時代遅れの印象が強い。(おそらく、専門機関で教育を受

² たとえば総務省/経済産業省の2001年度報告書では、当時の政府関係システムに用いられるICカードに利用されていた暗号として公開鍵暗号はRSA-1024、共通鍵暗号はDES, Triple-DES, Skipjack、ハッシュ関数はSHA-1, MD5が列挙されている[3, 資料 要件調査ワーキンググループ報告書 p. 4]。(なお、これらの暗号のうちいくつかは安全性に問題が指摘されており、今後の利用は推奨されていない。)

けた人物でなくても偽造防止技術の情報を入手することは可能である。住基ネットカードや連係 IC カードを発注する各自治体が納入業者に対してセキュリティ試験の結果を提出させないことは考えにくく、スマートカードがどのような試験を受けたのかは自治体への情報公開請求によって開示可能である。）

以上、セキュリティ技術の各点をとりあげて論じたが、技術仕様全体を通じて、日本政府がスマートカード、端末、基幹システムをどのように信頼できるものとして構築するのかという目的および全体像が見えてこない。（海外の事例については第 4 章で後述する。）日本の技術仕様には、誰が接続できて何をどのように守るのかというセキュリティ技術の知見に乏しく、スマートカード業者に丸投げの公共工事の発注書でしかない。

3.3 ISO 導入は改善策となるか

「公的分野における連携 IC カード技術仕様」には以上のような技術仕様としての不備があるが、同時にそれらの不備を補う可能性がある要求事項が盛り込まれていた。それがセキュリティ標準の採用である。

技術仕様の末尾には「ISO/IEC15408 の EAL4 以上の保障レベルを有する」「ISO17799 に準拠するセキュリティーポリシーを策定し運用する」ことが記されている。この ISO/IEC15408 EAL4 とは、ISO(国際標準化機構)と IEC(国際電気技術標準機関)によって認可されたセキュリティ技術に関する国際標準の評価保証レベル 4 を取得することを意味し、ISO17799 はセキュリティ運用に関する国際標準を満たすことを要求している。これによって、政府が発行する連携スマートカードには外部機関によって評価され認証されるプロセスが課せられることになった。（これに先立つ 2001 年に、政府は IT 製品の調達の際には、独立機関によって ISO/IEC15408 に基づいてセキュリティ評価・認証された製品等を調達すべきである [28] という方針を決定している。）

この外部評価には、評価機関による申請者（納入業者）へのコンサルテーションも含まれており、これらの措置によってセキュリティの技術面と運用面において大幅な改善が期待される。しかしながら、技術標準は万能ではない。以下の節では情報システムおよびスマートカードのセキュリティ評価における困難さについて検討する。

3.3.1 セキュリティ技術標準の課題

これまで 1 万円落札や業者への丸投げが横行していた日本の政府調達 [1, 13] にセキュリティについての技術的な条件が（法律に基づかない努力目標だとしても）加えられたのは評価できる。しかし実際に施行する上での課題も残されている。

セキュリティ評価機関の中にはスマートカードのセキュリティを評価するためのノウハウを豊富に持っているものもあれば持っていないものもある。このために海外ではスマートカードのノウハウがない機関が納入の抜け穴になった事例もすでに起こっている [2, §23.3.1]。国内ではいまのところスマートカード試験設備を持つ機関は限定されており、国際基準を実施しようとするこの立ち上げの時期にそれらの機関が評価機関としての看板に傷をつけるような評価を下すことは考えにくい。ただし、セキュリティ評価機関が増加した際に機関ごとの暗号モジュールの評価水準を一定にするための具体的なプランに乏しいのが現状である。

関係者の説明によれば、住民基本台帳カードは、安全性に関する第 3 者による評価と確認

を2003年から行ない、4月に調達を開始し、8月に配布される予定である [22]。まずここで行なわれるであろうセキュリティ評価のプロセスについて概略を説明する。スマートカードのセキュリティ評価は、チップ、回路、カード本体、OS、アプリケーションといったカードの基本単位にまで及び、それらの設計から実装そしてテストにいたる各段階においてチェックが行なわれる。この作業を行なうには、経験豊富な海外の試験機関と納入業者でも何カ月もかかる³セキュリティをあとから追加することはできないという知見から、設計段階からセキュリティを重視した手続きをすすめることが要求されているが、多くの企業はセキュリティを重視した設計開発体制をとっていない。このために、評価機関は企業に対してコンサルテーションを行なう必要が生じる。こうした作業のために、業者が連携カードに必要な EAL4 以上の認証を取得するのは住基カード運用開始後になる可能性もある⁴。

また、自治体が情報機器を調達する場合には政府の調達方針の影響を受けない点にも注意が必要である。このために、セキュリティ評価認証を受けないスマートカードが住基カードとして納入されることは可能である。これは同じ住基カード互換のスマートカードでもセキュリティ認証を受けたカードと受けないカードの2種類が流通することを意味する。そしてどちらのスマートカードも技術仕様を満たしているため、公的連携スマートカード用のアプリケーションがセキュリティ認証を受けないカード上で動作することは避けることができない。したがってすべての自治体の情報セキュリティ担当者が(政府連絡会議の調達方針に従って)EAL4以上の取得を入札条件として要求することがセキュリティ対策上必要であると考えられる。

3.3.2 セキュリティ運用標準の課題

ISO17799 においては、リスク分析に基づいたセキュリティ対策を行なうことが定められている。ところがスマートカード上であらゆるアプリケーションが動作し、その用途が限定されない場合においては、納入当初はリスクが低かった環境が比較的高いリスクの環境に変わることがありうる。たとえば元々地方自治体の業務を省略化するためのカードが突然 ID カードの役目を担うようになったり、ショッピングカードの役目を担うようになった場合 [2, §14.7.4] については、リスク評価は低く見積もられたままでセキュリティ対策もそれに準じたものとなる。こうしたリスク変動を扱うようなセキュリティポリシーの形式化手法はいまだ存在しないため、スマートカードを発行する自治体およびシステムを納入する業者は対処できない。したがって、住基カードをベースとした連携カードが導入される際には、住民票サービスを想定したセキュリティポリシーの下で、実際にはそれよりもリスクの高い個人認証サービスや金融サービスが提供されることになる事態は避けることができない。

3.3.3 両者に共通する課題

ISO の技術標準と運用標準の両者に共通する問題としては、基準そのものがひとり歩きしてしまう場合が考えられる。たとえばアメリカ連邦政府の情報機器調達基準である FIPS140(第 4.1 節参照) は暗号モジュールの販売宣伝にも用いられることがあるが、「FIPS140 準拠」と示

³ 暗号モジュールの評価には一般の納入システムと比べてコストもかかり、暗号モジュールだけの評価をしては試験機関にとっては採算があわない [3, p. 30] ほどである。

⁴ ただし納入製品が海外の ISO 評価機関から EAL4 以上の認定を受けていれば、評価手続きを簡略化することが可能である。しかしながら、報告者の知る限り現時点で海外で EAL4 以上の認証を得た日本製のスマートカードは存在しない。

されるだけで、FIPS140-1 なのかそれとも FIPS140-2 なのか、評価保証レベルのうちどのレベルを取得したのか、そのレベルはどのようなセキュリティを保証しているのか [2, §14.4] が十分に周知されない事例がある。

このような事例を踏まえて、技術標準の尺度が一人歩きしたり、合格 / 不合格の尺度と混同されないよう注意するが必要である。具体的には、ISO/IEC15408 に相当する独自のセキュリティ評価、ISO17799 に相当する独自のセキュリティポリシーが国際技術基準の尺度と混同される場合が起こりうる。こうした尺度の混同を繰り返さないために、第 3 者による公正な評価が行なわれるよう注意すべきである。

3.4 カードの保護レベルと無関係に発生する問題

ここまではカードの技術仕様に即した分析を行なったが、本節ではスマートカードのセキュリティとは無関係に発生するセキュリティ上の問題について検討する。スマートカード以前のカード犯罪では、カードを個別に偽造するよりもむしろカードの接続先 (ATM やカード読み取り機、あるいは無人金庫や店舗そのもの) の偽造が行なわれてきた。現在でもカードを接続する機器のセキュリティを高めることは重要な課題とされている [2, §14.7.1]

住基カードは、専用端末およびスマートカード読み書き装置をつないだ汎用パーソナルコンピュータ上の WWW ブラウザ (以下、「業務端末」と呼ぶ) からアクセスできるように設計されている。この業務端末用ソフトウェアは地方自治センターから希望する市町村に無償で提供され [30, pp. 4,7,9]、図書館や保健機関の PC を使って公共サービスに活用されることが計画されており、さらに連携カードサービス開始時には、公的サービスだけでなく商店街のポイントカードや有志でつくる地域通貨にも利用される可能性を持っている。したがって住基カードおよび連携スマートカードは、公的および私的な無数の業務端末とデータのやりとりを行なう状況を考慮したものでなければならない。

たとえスマートカード内部のデータが完全に他からアクセスできないと仮定しても、利用者が画面の指示に従って暗証番号 (住民基本台帳アプリケーションの場合は 4 桁の数字) を入力すればそのセキュリティは無効化される。これは古典的な偽 ATM の手口で可能である。だが、地方自治センターの住基スマートカードだけでなく、それをベースにした連携スマートカードの基本設計にもこの古典的な攻撃に対する配慮が一切見られない。

住基カードが公的個人認証サービス [20] とリンクした場合にはスマートカードはサインや実印やパスポートに近い効力を持つことも考えられるが、特にその際には業務端末のデータ格納が信頼できるかどうか、業務端末が表示するメッセージは信頼できるのか、業務端末でサービスを提供する者が信頼できるかどうかを確認することが必要となる [2, §2.5, §14.7-8]。こうした古典的なリスクに対しては、信頼すべき業務端末で悪意のあるコードが実行されないこと、誤動作が起こらないこと、あるいは信頼できない業務端末に接続しないこと、といった具体的なセキュリティ対策が必要となる。

しかしながら、業務端末に採用された汎用 PC 上の WWW ブラウザは悪意のあるコードを実行させることが可能であり、すでにスマートカード用の端末で任意のコードが実行可能だった事例も専門家によって報告されている [29]。このような業務端末のリスクにもかかわらず、無数に配置しようとする地方自治センターの構想は連携スマートカードの要件であるはずの安全性への配慮を欠いていると言える。この点で、地方自治センターによる標準システムは、汎用 PC 上の WWW ブラウザの指示を無条件に信用することを前提としており、業務端末の

セキュリティを無力化するものである。業務端末を無条件に信頼して電子署名の暗証番号を入力させるシステムは、利用者に対しても大きな責任を負わせるものである。技術的に中立な視点に立ってセキュリティに配慮すれば、さらに信頼できる業務端末を選ぶという選択肢もあったはずである。

4 電子政府に関するセキュリティの比較検討

最後に欧米諸国のセキュリティ評価事例について日本との比較を行なう。

4.1 アメリカ合衆国のセキュリティ評価事例

アメリカでは商務省の国家標準技術院 (NIST) が政府が調達する情報機器の規格を連邦政府標準規格 FIPS (Federal Information Processing Standard) として詳細に定義し、公開している。その中でも暗号モジュールに関する FIPS140 [18] では、設計から実装に渡る 11 の領域で 4 段階のレベルによる評価が要求され、その試験方法についても詳細に記されている。

FIPS の特筆すべき点として、NSA(国家安全保障局) が NIST に対して技術的な助言と支援を行なうよう連邦法で定められており [25, p. 303])、さらにその見直しはドラフト (草稿) 版として一定期間公開されてから改訂版に反映されるという仕組みを採用している点が挙げられる。これによって FIPS は他の政府専門機関からチェックされるだけでなくパブリックコメントでもチェックされることになる。

たとえば FIPS140-1 ではスマートカードはセキュリティレベル 1(最低限のセキュリティ)の暗号モジュールの例に挙げられていたが、2001 年の FIPS14-2 ではその例から除外された [18, §1.1]。この改訂はドラフト段階で公開され、スマートカードの位置づけが変わった点については通産省の外郭団体である情報処理振興事業協会の調査報告書 [10, IV.1.1] でも注目されている。この FIPS140-2 も 2002 年 12 月 3 日にはさらに改訂されており、また新たなセキュリティ要件が追加されている。

こうした厳しい調達基準のためにアメリカ連邦政府がスマートカードを全面導入する見込みはいまのところ立っていないが、州によってはスマートカードを使った個人認証の導入が検討されている。たとえば 2002 年カリフォルニア州の公聴会で、専門家団体 CPSR がセキュリティ事例分析の第一人者 Peter Neuman らの協力を得て、州に対して慎重な対応を求める証言 [27] をおこなっている。

4.2 ドイツ連邦のセキュリティ評価事例

ドイツでは、認証局の基幹システムに情報機器を調達する場合や、銀行間のネットワークに加入する場合には認証評価レベル 5 の取得が要求されている。このセキュリティ要件については、電子署名法に基づいて内務省の情報技術保安局 (BSI, Bundesamt für Sicherheit in der Informationstechnik) が定めている。

ドイツの BSI がアメリカの NSA と異なる点は、連邦政府や商務省への助言でなく、全省庁のセキュリティポリシーや端末まで対象としている点である。たとえばドイツで電子署名を認証するための最上位の認証局は電気通信・郵便規制庁が担当しているが、その評価・監

査はBSIが行ない、また認証局を監督するだけでなく認証に用いる暗号アルゴリズムを決定し、また実際の電子認証に用いる政府調達電子メールクライアントとしてS/MIMEおよびOpenPGP/MIMEに対応したオープンソースソフトウェアを採用したのもBSIである [5] .

4.3 英連邦のセキュリティ評価事例

イギリスはドイツのBSIやアメリカのNSAのように電子政府のセキュリティについて、他省庁に対して一元的に評価・助言を行なう権限を持つ機関は法律上は常設されていない。(現在もイギリスでは国民IDカードが提案されているが [4] , これに対してセキュリティ機関が公式に参与したという発表は見当たらない。) しながらセキュリティ評価の国際標準化や認証技術・暗号技術の管理についてはGCHQ(Government Communications Headquarters) 内の(CESG (Communications-Electronics Security Group) が担当していると考えられる。

イギリスにおける特長としては、セキュリティ評価にあたっては政府機関よりもパブリックコメントや議会の果たす役割が大きい点があげられる。イギリスでは国民IDカードが提案され実験運用されては廃案になってきた歴史がある。その際に中立的なセキュリティ評価を提出してきたのは政府機関ではなくむしろ非政府系機関である。

たとえば、1999年に中央コンピュータ技術庁(CCTA, Central Computer and Technology Agency) が法案提出前にパブリックコメントを募集し、それに対してFoundation for Information Policy Research(FIPR) が批判的なコメントを提出しており [7] , 2003年にもIDカードの導入に対してコメントを公表している [8] . このFIPRは、セキュリティエンジニアリングの第一人者としてECの第3世代スマートカード計画⁵にも携わっているケンブリッジ大学のRoss Andersonがとりまとめを行っており、暗号製品に限定されない幅広い提言を行なっている。

4.4 比較と考察

以上の欧米の事例をもとに、比較と考察を行なう。

日本の現状の体制は、政府のセキュリティ評価機関が法律に基づいて各省庁に対して監査を行なうアメリカやドイツよりも、強力な監査機関を明文化しないイギリスに近い。しながら、イギリスのように監査機関以外の組織によるセキュリティ評価がパブリックコメントや議会制を通じてとりいれられない点が異なっている。住民基本台帳法ネットワークにおいても、法案提出においてパブリックコメント募集は行なわれず、法案の強行採決 [26] から仕様決定、業者入札、そして納入運用 [12, 23, 24, 1] にいたるまで、専門的な外部評価を求める機会が存在せず、詳細は府省や外郭団体からの通達によって決定されてきた。

日本が他国に先駆けて多目的の住民スマートカードを発行できるのは、日本の電子政府/電子自治体の先進性を示すものではなく、むしろ技術的知見に基づいて積み重ねられるべきセキュリティ文化の欠如と開かれた民主制の不在を示すものである。

⁵ ECで開発が推進されている第3世代スマートカードは、日本で現在導入が推進されている「次世代スマートカード」 [22] とは異なる。日本のいわゆる次世代スマートカードは欧州では第2世代に該当すると考えられる。

5 おわりに

本報告ではスマートカードを中心として、日本の電子政府 / 電子自治体におけるセキュリティ評価体制の不備、そして今後のリスク評価の課題について検討した。さらに欧米のセキュリティ評価体制との比較を行ない、日本に欠如している要素について分析した。

セキュリティ技術の粋を集めてもリスク (脅威, 不確実性) は存在する。そして、それを評価する手法を獲得すればなるべくリスクの低い選択肢を選ぶことも可能である。しかしその手法を確立するには、政府機関、自治体、企業、大学、国際機関、および非政府系団体にまたがる我々の社会の知見を結集して取り組むべきである。

本報告ではテクニカルなセキュリティ評価を主に扱ったために、運用現場でのリスク、法律制度面でのリスク、そしていわゆるプライバシー保護技術や匿名化技術の利用についても扱っていない。それらの分析については他の指摘に譲りたい。

謝辞 SCIS2003 参加者および CPSR 日本支部メンバーからは具体的なコメントをいただいた。ここに感謝する。

更新履歴 2003.02.07, 1st draft. 2003.02.09, 2nd draft. 2003.02.10, 3rd draft. 2003.02.11, final draft, 第 3.4 節を追加。2003.02.13, updated version. 文章の推敲。2003.02.15, 参考文献 [29] 追加。2003.02.16, 文章の推敲。

参考文献

- [1] 秋山訓子. 政府の IT 戦略「電子政府」にムダ. 朝日新聞, 2002. 2002 年 11 月 04 日総合面 時時刻刻. Another version is available at <http://www.asahi.com/tech/asahinews/K2002110400250.html> (visited February 10, 2003).
- [2] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001. 邦訳はトップスタジオ訳『情報セキュリティ技術大全—信頼できる分散システム構築のために』日経 BP 社, 2002. Sample chapter is available at <http://www.cl.cam.ac.uk/~rja14/book.html> (visited January 4, 2003).
- [3] 暗号技術検討会 2001 年度報告書. 総務省 / 経済産業省, March 2002. Available online at <http://www.meti.go.jp/policy/netsecurity/downloadfiles/cryptrec2001report.pdf> (visited February 4, 2003).
- [4] 東浩紀. 自由と交換される匿名性. 中央公論, Vol. 108, No. 1, pp. 310–319, January 2003. ‘情報自由論: データの権力, 暗号の倫理’ 第 7 回.
- [5] Bundesamt für Sicherheit in der Informationstechnik. Projekt SPHINX. Online document. <http://www.bsi.de/aufgaben/projekte/sphinx/index.htm> (visited December 3, 2002).
- [6] 臺宏士. 共通 IC カード 1 枚で行政サービス: 住基カードを軸に政府が導入を検討. 毎日インタラクティブ DIGITAL トゥデイ, April 2001. 2001 年 4 月 26 日. <http://www.mainichi.co.jp/digital/netfile/archive/200104/26-1.html> (visited January 4, 2003).
- [7] Foundation for Information Policy Research. Framework for Smart Card Use in Government. Online Document, 1999. <http://www.cl.cam.ac.uk/users/rja14/cards.html> (visited December 3, 2002).
- [8] Foundation for Information Policy Research. FIPR response to the UK Entitlement Card consultation. Online document, February 2003. Available online at <http://www.fipr.org/cards/entitlementresponse.html> (visited February 4, 2003).

- [9] 今井拓司, 三宅常之. ケータイ・ソフト開発 人海戦術の破綻. 日経エレクトロニクス, No. 795, pp. 117-137, 2001. 2001年5月7日号. Sample article is available at <http://ne.nikkeibp.co.jp/NE/2001/010507/tokushu.html> (visited February 4, 2003).
- [10] 情報処理振興事業協会. 平成11年度スマートカードの安全性に関する調査 調査報告書. 平成11年度セキュリティセンター活動報告, 2000. 平成12年2月29日. Available online at <http://www.ipa.go.jp/security/fy11/report/contents/crypto/crypto/report/SmartCard/sc.html> or <http://www.ipa.go.jp/security/enc/smartcard/sc-survey.pdf> or (visited February 5, 2002).
- [11] 笠島達也. ドコモ最新型携帯相次ぐ欠陥. 西日本新聞, 2001. 2001年5月17日. Also available online at http://www.nishinippon.co.jp/digiQ/html/main/01_5_17.html (visited February 4, 2003).
- [12] 切込隊長. 管理すれども機能せず～サイバネティック社会への道. 俺様キングダム出張所, No. 14, June 2002. Online article available at <http://www.tanteifile.com/rensai/taichou/14.html> (visited December 1, 2002).
- [13] 岸本周平. 政府調達システムとITシステム-“ITゼネコン”を育てたのはだれか, February 2003. RIETI政策シンポジウム だれのための電子政府? 第2セッション基調講演. <http://www.rieti.go.jp/jp/events/03020501/info.html> (visited February 4, 2003).
- [14] 公的分野における連携ICカードの普及に関する関係府省連絡会議. 公的分野における連携ICカードの実現に向けた基本的考え方, July 2001. 平成13年7月27日. <http://www.kantei.go.jp/jp/singi/it2/others/kihon.pdf> (visited January 4, 2002).
- [15] 公的分野における連携ICカードの普及に関する関係府省連絡会議. 公的分野における連携ICカード技術仕様, March 2002. 平成14年3月26日. <http://www.kantei.go.jp/jp/singi/it2/others/siyou.pdf> (visited January 4, 2002).
- [16] 公的分野における連携ICカードの普及に関する関係府省連絡会議. 連携ICカード券面の偽造防止技術ハンドブック, July 2002. 平成14年7月20日. <http://www.kantei.go.jp/jp/singi/it2/others/ichb.pdf> (visited January 4, 2002).
- [17] Simon Moore, Ross Anderson, Robert Mullins, George Taylor, and Jacques J. A. Fournier. Balanced Self-Checking Asynchronous Logic for Smart Card Applications. Online paper, 2002. <http://www.cl.cam.ac.uk/~swm11/tmp/micromicro.pdf> (visited February 4, 2003). To be appear in *Microprocessors and Microsystems Journal*.
- [18] National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. FIPS PUB 140-2, U.S. Department of Commerce, May 2001. Updated on December 03, 2002. Supercedes FIPS PUB 140-1, 1994 January 11. Also available online at <http://csrc.nist.gov/cryptval/140-2.htm> (visited January 4, 2002).
- [19] 日本セキュリティ・マネジメント学会. セキュリティ・マネジメントの視点から見た住民基本台帳ネットワーク接続問題に関する提言, December 2002. <http://www.jssm.net/jssm/20021218Teigen.html> (visited January 14, 2003).
- [20] 公的個人認証サービス. 日経コンピュータ, No. 563, p. 36, December 2002. 2002年12月16日号.
- [21] 太田阿利佐. 「もっと情報公開を」住基ネットのセキュリティーで学会が初提言. 毎日インタラクティブ DIGITAL トゥデイ, December 2002. 平成14年12月18日. <http://www.mainichi.co.jp/digital/netfile/archive/200212/18-1.html> (visited January 4, 2003).
- [22] 大山永昭. 次世代スマートカードの技術と応用. インターフェース, Vol. 29, No. 3, pp. 91-98, March 2003. 特集: ICカード技術の基礎と応用 第6章.
- [23] 斎藤貴男. プライバシー・クライシス. 文春新書 023. 文藝春秋, 1999.
- [24] 櫻井よしこ, 伊藤穰一, 清水勉. 「住基ネット」とは何か?: 国民と自治体のための脱「住基ネット」論. 明石書店, September 2002.

- [25] Bruce Schneier and David Banisar, editors. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. John Wiley & Sons, August 1997.
- [26] 「世界」編集部(編). ストップ!自自公暴走: 日本の民主主義の再生のために. 岩波書店. 「世界」別冊 No. 668, 1999.
- [27] Lenny Siegel. Proposed identification schemes should be carefully evaluated. Online document, January 2002. <http://www.cpsr.org/program/natlID/natlIDcal-jud-8.1.02.html> (visited January 4, 2002). Prepared for California State Assembly Judiciary Committee Hearing.
- [28] 総務省行政管理局. 各省庁の調達におけるセキュリティ水準の高い製品等の利用方針, March 2001. http://www.soumu.go.jp/gyoukan/kanri/010425_9.htm (visited January 4, 2003). 平成 13 年 3 月 29 日 行政情報化推進各省庁連絡会議了承.
- [29] 高木浩光. [memo:4491] 宝塚市、伊丹市、川西市、猪名川町の IC カード利用者に任意コード実行攻撃の脅威 (was Re: ブラウザのセキュリティ設定を安全性を下げるよう指示しているサイト). セキュリティホール memo メーリングリスト, July 2002. Archive is available at <http://www.st.ryukoku.ac.jp/~kjm/security/ml-archive/memo/2002.07/msg00138.html> (visited February 13, 2003).
- [30] 地方自治センター. IC カード標準システムの概要「未定稿(抜粋)」. Online document, September 2002. <http://www.lasdec.nippon-net.ne.jp/rdd/icc/gaiyo/gaiyo.pdf> (visited February 4, 2003).
- [31] 山根信二, 村山優子. 電子自治体のシステム調達におけるリスク評価の課題. 2003 年暗号と情報セキュリティシンポジウム予稿集, pp. 487-489. 電子情報通信学会情報セキュリティ研究専門委員会, January 2003. 7A-4.

Copyright©2003 Shinji R. Yamane.

本報告は, GNU Free Documentation License 1.1(GNU フリー文書利用許諾契約書)の条件下で自由に利用可能である. 詳細については <http://www.gnu.org/copyleft/fdl.html> から入手可能である.