社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－CSEC－21 (13)
2003／5／16

公的連携ICカード導入のリスク評価における課題

山根信二† 村山優子†

2003年度に電子政府を実現するe-Japan計画に沿って，現在官公庁から地方自治体におよぶ全国的な取り組みが進められている．その過程で安全性証明のみならずリスク評価が重要な課題となっている．本報告では，政府調達システムに固有のリスク評価事例として特にスマートカート(多目的ICカード)に注目する．スマートカード導入において，仕様策定，国際技術標準の導入，端末のセキュリティといった個別の課題を取り上げ，最後に比較事例としてアメリカ，ドイツ，イギリスの関連動向についてもとりあげる．

Issues in Govermental Multi-application Smartcard Requirements

SHINJI YAMANE † and YUKO MURAYAMA†

Japanese government had proposed the single smartcard enough to run multiple applications. It is called "common IC card in public sector"(Kouteki Bun-ya ni okeru Renkei IC card). In 2001, the ministries agreed the adoption of operational policies and technical specifications for common IC card in public sector. This paper exmines the govermental requirements oo the smartcard from the view point of security engineering and risk analys. This paper also comment on the smartcard issues in US, Germany, and UK.

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)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，日本にそのような実績はない．また，日本の暗号モジュールの評価がアメリカのみならずイギリス・フランス・ドイツにくらべても遅れていることはかねてから指摘されている[2] [p. 30].

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，本報告では技術的なリスク(脅威，不確実性)に注目して検討を行なう．

1.1 スマートカードのセキュリティ

本発表では，公的機関においてスマートカードを導入する際のリスク評価に注目する．これは後に述べるように，不特定のアプリケーションを実行できるスマートカードでは仕様決定時と実地運用時との間でリスクの変動を考慮しなくてはならないためである．

このリスクを考察する前に，まずスマートカードの一般的なセキュリティ技術について述べる．スマートカードに対して，すでにいくつもの攻撃方法と防御手段が提案されている．それらは多岐にわたり，学術的な検証が行なわれているものだけでもTiming Attack, Power Analysis[8], Chosen Protocol Attack[1], Electromagnetic analyis[7], Optical Fault Induction Attack[16]といった手法があげられる．スマートカード製品にはこうした既知の攻撃を受けてもなお安全であるという試験が要求される．

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．たとえば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[2] [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約のために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は驚くに値しない．この現状を踏まえて，ECの第

† 岩手県立大学ソフトウェア情報学部
Faculty of Software Information Science, Iwate Prefectural University

3世代スマートカード計画をはじめとする新たなマイクロプロセッサや暗号アルゴリズムの研究開発も進められており，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製品化も期待されている (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[1) §14.6.3])，しかしながら現時点におけるスマートカードの導入には総合的なトレードオフの作業が必要であり，リスクを評価する観点が不可欠であると言える．

2. 連携 IC カード仕様決定の経緯および問題点

本節では，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「連携 IC カード」の導入における技術的課題について検討する．

2.1 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[4)]．

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，それが正式に決定したのは 2001 年 7 月 27 日の連絡会議においてである．そこでは，まず連携 IC カードがクリアすべき要件の基本方針が定められている．

(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

そしてこの方針に基づき，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連携 IC カードのベースとすること，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[9)]．

ここで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は**この時点ではまだ仕様が決定していなかった**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[10)] [§1.1])．このために連携カードの具体的な仕様の検討は先送りされている．

2.2 2002 年: 技術仕様

地方自治情報センターによって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」[10)] 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．この技術仕様は，政府にとって個人認証に必要な技術はどうあるべきか，そしてカード上で動作するアプリケーションはどのように動作するすべきか，というセキュリティの文化が反映されるべきものである．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．この仕様では，RSA 鍵長を 1024bit 以上に延長できず，DES, Skipjack, MD5 を使った既存のスマートカード製品も納入可能となる．この事は，技術仕様策定における専門的な分析を疑わしいものにしている．同時期には CRYPTREC 報告書は出されていなかったが，各省庁の代表が CRYPTREC の検討作業に注意を払っていればこの仕様は変更されていた可能性が高い．

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．

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」[11)] 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．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[11)] [§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なお信頼できる点にある．(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[1)] [§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．

2.3 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[17] という方針を決定していた．)

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．

2.3.1 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発生している[1] [§23.3.1]．

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[13]．しかしながら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，納入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．

また，各地方自治体が情報機器を調達する場合には政府の調達方針に制約されないという点にも注意が必要である．このために，各自治体はセキュリティ評価認証をうけないスマートカードを住基カードとして発行することが可能である．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．

2.3.2 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リスクの高い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[1] [§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．

2.3.3 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 3.1 節参照) は民間向け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[1] [§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．

2.4 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単体のセキュリティとは無関係に発生するリスクについて検討する．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．このために，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[1] [§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[19] [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が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には，カードのみならず，無数の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[1] [§2.5, §14.7–8]．こうした脅威に対しては，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 ブラウザは設定によって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報告されている[18]．この業務端末の脆弱性に関する脅威については，たとえば業務端末が利用者の合意を得ずにカードの製造 ID あるいはシステムパラメータへのアクセスを行なう場合，あるいは業務端末が暗証番号 (住民基本台帳アプリケーションの場合は 4 桁の数字) を入力するように WWW ブラウザ画面で利用者に指示する場合など，具体的な運用を通じた検証を行なう事が必要となる．また，技術的に中立な観点から，業務端末に汎用 PC 上の WWW ブラウザ以外のシステムを採用することも検討に値する．

3. 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．

3.1 米連邦政府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) として公開している．その中でも暗号モジュールに関する FIPS140[12] 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[14] [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．

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 FIPS140–2 ではその例から除外された[12] [§1.1]．この改訂はドラフト公開時点で注目を集め，IPA による調査報告でも報告されている[8] [IV.1.1]．さらにこの FIPS140–2 も 2002 年 12 月 3 日に改訂され，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．こうした議論の一つとして，2002 年カリフォルニア州の公聴会において専門家団体 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意見陳述[15] をおこなっている．

3.2 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) 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が行なっている．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，電子署名に関わる政府調達電子メールクライアント[3]の採択も行なっている．またオープンソースソフトウェアの導入による信頼性確保のような独自の試みも行なっている[20]．

3.3 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に類似する情報セキュリティ機関としてGCHQ(Government Communications Headquarters)内のCESG (Communications-Electronics Security Group)が存在するが，他の省庁に対して一元的に評価・助言を行なう権限は法律で明記されていはいない．

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．この議論における特長としては，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．そして，技術的に中立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．技術的なコメント[5),6)]を提出してきた代表的な団体であるFoundation for Information Policy Research(FIPR)は，ECの第3世代スマートカード計画☆にも携わっているケンブリッジ大学のRoss Andersonがとりまとめを行なっており，暗号製品に限定されない幅広い提言を行なっている．

3.4 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，強力な監査機関を法律上定めないイギリスに近い．しかしながら，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議会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は，法案の強行採決から仕様決定，業者入札，そして納入運用にいたるまで，専門的な外部評価を求める機会が存在せず，詳細は審議された法令ではなく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，日本の電子政府の先進性を示すものではなく，むしろリスク評価の不在であると言うこともできる．

☆ 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」[13)]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．

4. まとめ

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検討を行なった．

セキュリティ技術の粋を集めてもリスク(脅威，不確実性)は必ず存在するが，その上でリスクの低い選択肢を選ぶことも可能である．しかし技術的に中立な評価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する取り組みが必要である．その際に諸外国の取り組みが有益な参考事例となる．

参考文献

1) Anderson, R. J.: *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.

2) 暗号技術検討会: 暗号技術検討会2001年度報告書，総務省／経済産業省 (2002). Available online at `http://www.meti.go.jp/policy/netsecurity/downloadfiles/cryptrec2001report.pdf` (visited February 4, 2003).

3) Bundesamt für Sicherheit in der Informationstechnik: Projekt SPHINX, Online document. `http://www.bsi.de/aufgaben/projekte/sphinx/index.htm` (visited December 3, 2002).

4) 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 (2001). 2001年4月26日. `http://www.mainichi.co.jp/digital/netfile/archive/200104/26-1.html` (visited January 4, 2003).

5) 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).

6) Foundation for Information Policy Research: FIPR response to the UK Entitlement Card consultation, Online document (2003). Availabele online at `http://www.fipr.org/cards/entitlementresponse.html` (visited February 4, 2003).

7) Gandolfi, K., Mourtel, C. and Olivier, F.: Electromagnetic analyis: Concrete results, *Cryptographic Hardware and Embedded*

Systmes - CHES 2001, LNCS 2162, pp. 251–262 (2001).

8) 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` (visited February 5, 2002).

9) 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 (2001). 平成 13 年 7 月 27 日. `http://www.kantei.go.jp/jp/singi/it2/others/kihon.pdf` (visited January 4, 2002).

10) 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 (2002). 平成 14 年 3 月 26 日. `http://www.kantei.go.jp/jp/singi/it2/others/siyou.pdf` (visited January 4, 2002).

11) 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 (2002). 平成 14 年 7 月 20 日. `http://www.kantei.go.jp/jp/singi/it2/others/ichb.pdf` (visited January 4, 2002).

12) National Institute of Standards and Technology: Security Requirements for Cryptographic Modules, FIPS PUB 140–2, U.S. Department of Commerce (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).

13) 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 (2003). 特集: IC カード技術の基礎と応用 第 6 章.

14) Schneier, B. and Banisar, D.(eds.): *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons (1997).

15) Siegel, L.: Proposed Identification Schemes Should Be Carefully Evaluated, Online document (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.

16) Skorobogatov, S. P. and Anderson, R. J.: Optical fault induction attacks, *Cryptographic Hardware and Embedded Systmes - CHES 2002*, LNCS 2523, pp. 2–12 (2002).

17) 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 (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.

18) 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 (2002). Archive is available at `http://www.st.ryukoku.ac.jp/~kjm/security/ml-archive/memo/2002.07/msg00138.html` (visited February 13, 2003).

19) 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 (2002). `http://www.lasdec.nippon-net.ne.jp/rdd/icc/gaiyo/gaiyo.pdf` (visited February 4, 2003).

20) 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, 電子情報通信学会情報セキュリティ研究専門委員会, pp. 487–489 (2003). 7A-4.