平成15年度　研究開発成果報告書

「次世代電子投票・アンケートシステムと その社会的利用に関する研究」

目次

1　研究開発課題の背景

本研究は、投票という重要な社会活動をサポートすることを課題としているが、そこには社会的、経済的、技術的な側面があるため、個別に説明する。

社会的な背景としては、先ず電子政府システムの実施があげられる。その中で旧自治省の電子・電子機器利用による選挙システム研究会中間報告（自治省2000年8月）を受けて、「電子機器利用による選挙システム研究会報告書」（総務省 2002 年 2 月）および、その機能要件定義である「電子投票システムに関する技術的条件及び解説」が総務省から発行された。さらに、地方選挙に限り電子投票を可能とする法改正もなされ、電子投票に向けた法制的基盤が固まりつつある。

しかしながら、これらの電子投票は、投票所における電子機器の利用を前提とするもので、前記研究中間報告における 3 段階の電子化の第一段階に過ぎない。因みに、電子化の段階としては、以下のように分類されている。

- 第一段階：投票所、開票所で電子機器を単体として導入する段階
- 第二段階：投票所間、投票所と開票所をネットワークで接続する
- 第三段階：任意の投票端末による投票

さらに、研究報告では最終的に第三段階が除かれており、近い将来の電子政府システムとしての電子投票は、任意の投票端末による投票という、高度にネットワーク化された社会における電子投票の枠組みが組み込まれていないことになる。

この方向性は、すでにパンチカードなどの選択方式を取り入れている米国でも同様であり、現在改版中の Federal Election Commission による Voting System Standards でも、attendee の存在しない、いわゆる network voting system は明示的に枠組みから外されている。しかし、インターネットが殆どの個人・家庭に普及した状況を想定して投票者の利便性を考えるとき、中央・地方の選挙を問わず理想的な電子投票の姿は、任意の投票端末から入力できる第三段階の形態であろう。様々な理由により投票所に出向けない人は、全国規模の選挙で現在約300万人いると言われている。こうした人々も含め第三段階の投票システムが導入されれば、天候等に左右されることなく投票率は大きく向上するものと期待される。国民あるいは住民に、行政側からアンケートして民意を聴く機会も今後増大すると思われるが、その際もプライバシー保護機能が備わったシステムに任意の端末から入力できることが望ましい。

第三段階の電子投票は、このように国民の政治への関心を高め、両者の間の距離を近づける効果があると同時に、長期的には行政経費を大幅に節減するものと予想される。

第三段階の電子投票・アンケートシステムは行政面に限らず、大学やマンション、医療ネットワーク等、様々な組織における選挙あるいはアンケート調査など多くの場面で必要とされよう。

次に、経済的側面から考えてみたい。インターネットの普及が進んでおり、総務省発表の通信利用動向調査では全人口の48%がインターネットに接続する環境を持つに至っている。この比率は世界的には16位ではあるが、絶対数では米国に次ぐ 2 位を保持している。また、インターネットへの接続も、電話回線（XDSL）、CATV や有線ネットワークなどのブロードバンド化が進んでおり、ネットワーク上のプライバシの保護メカニズムが解決されることで、利用形態の更なる多様化、拡大が図れる可能性がある。

これまでネットワーク上のプライバシは、e-mail や Web への送信データの暗号化を中心としたセキュリティ問題としての取り組みが進み、現状では暗号 e-mail や SHTTP さらには Socks などの技術が開発され、実用化に供されようとしている。しかし、市場調査などの情報収集におけるプライバシは単なる情報の秘匿ではなく、収集すべき情報は情報提供者名を伏せたまま情報収集者に知らされる仕組みが必要となる点で、これまでのセキュリティ問題とは異なった側面を持つものであり、今後ネットワークを利用した情報収集ビジネスが進展するために解決すべき新しい問題を提示している。電子投票自身非常に高度なプライバシの保護を必要とすることから、第三段階の電子投票が可能となれば、例えばファイナンス（投資相談）、バイオ分野（ゲノムベースでの情報収集）、教育分野（e-ラーニングにおける学生による教師の評価）、あるいは医療分野など多岐にわたる分野への応用が拓け、経済の活性化が期待される。

換言すれば、現在の e-mail やホームページの自発的情報提供による Push 型システムに加えて、回答を引き出す Pull 型システムも普及し、大きな経済効果を生むことが期待される。

最後に、技術的背景について述べることとする。

暗号研究者達は、過去 10 年以上に亘り、暗号理論応用の格好のテーマとして第三段階の形態を前提とする電子投票を研究対象として考察を重ねてきた。そこでは匿名性と二重投票等不正防止の両立性、公平性、公的検証可能性、耐買収性(レシートフリー性)等の要件を満たす方式が多数提案されてきた。しかし理論的興味が強かった故か、システム構成の簡易性、コンピュータシステムとしての信頼性、経済性(低コスト化)については余り考慮されていなかった。

本研究開発課題では、理論的諸要件に加えてシステム構成の信頼性や経済性も重視する方式として、研究分担者の一人、辻井により着想され、山口, 北澤, 黒澤等により検討されてきた準同型暗号方式による 2 センター方式(TYKK 方式)を提案し、実用化へ向けての研究開発を推進する。

また最近 ISO15408、即ちコンピュータシステム等の情報製品のセキュリティ評価基準の重要性が国際的に高まっているが、本課題では、電子投票システムを対象とするセキュリティ評価基準についても検討する。更に、運用状態に入った電子投票システムについて、ISO17799(我が国では ISMS, Information Security Management System)を考慮しつつ、セキュリティポリシーのガイドラインを作成する。電子投票システムを対象にしたセキュリティ評価基準やセキュリティポリシーはこれまで検討されていないが、実用化にあたって不可欠な課題である。

以上、社会的、経済的、技術的視点を総合し、21 世紀の IT 社会の基盤として効率的で低コストで信頼性の高い電子投票システムを提案することが本課題の目的である。

2　研究開発分野の現状

2-1　国内外における当該技術と競合する研究開発概要

国内外において当該研究開発課題と同一の目的においては目標に対して、さまざまなアプローチが行われている。他の研究例を記載する。

①　次世代電子投票・アンケート方式

理論的なアプローチとして、以下の3種類がある。

- ブラインド署名
- ミックスネット方式
- 準同型暗号方式利用方式

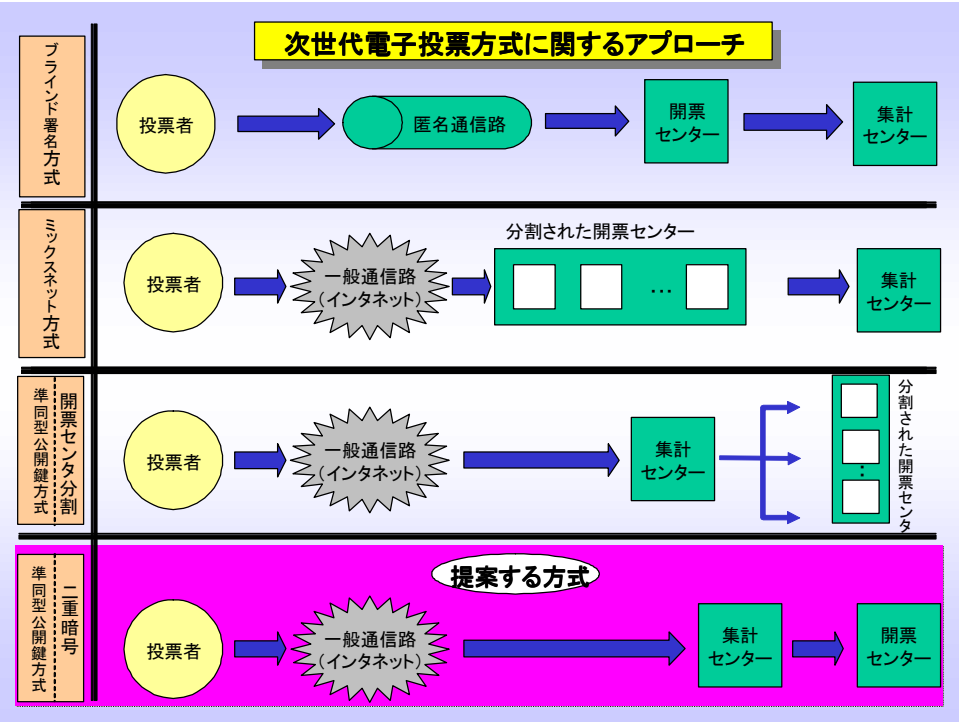


図 1　次世代電子投票方式に関するアプローチ

“ブラインド署名方式“は、票の内容を見せないままに、投票者は信頼される選挙管理センターに自分の名前を付けて送付する。選挙管理センターは名前とともに、有権性、二重投票のチェックを行い、合格すれば票に選挙管理センターの署名をつけて送り返す（この際、票の内容を見ないまま署名するため、ブラインド署名と呼ばれる）方式を利用する。投票者は、署名された票を匿名で集計センターに送り、集計センターは署名を確認して受理する。本方式は匿名であるため、票を秘匿する（暗号化する）手間が不要で、センター数も2個と経済的であるが、匿名通信路を必要とするため、インターネットなどの一般の通信路をそのまま利用することができない。このため、次に述べるミックスネット等の利用が必須となり、機器構成が増加するという欠点がある。

“ミックスネット方式”は図1に示す様に選挙センターを複数個カスケードにつなぎ、各センターは暗号化された票をシャッフル（入力と出力の関係がわからなくなる様に）する方式であり、投票内容が賛否、選択を基本とする投票システムのみならず、ブラインド署名と同様に文章形式をも扱うことができる。この方法の発想の原点は、多くの無記名の手紙をまぜて送られてきた順番との対応をつかなくす

る方法であった。この方式は、各センターの不正を防ぐ確度をあげるために、センター数を増やす必要があり、システム構成機器数が増大することおよび、公平性（選挙の途中結果をだれもが知りえないこと）を実現するために、投票締め切り後に開票し、集計する必要があり、開票の速報性上の問題がある。

“準同型暗号利用方式”は、暗号化された状態で、各票を掛け合わせることにより、中の票が加えられるという“準同型性”を利用した方式である。この方式には、センター同士の結託を防ぐ、あるいは何人かのセンター管理者が集まれば復号できるという開票センター分割方式（あるいは簡単に閾値方式）と、本提案の収集開票の2センター方式がある。閾値方式の問題としては、その閾値のセキュリティ強度を上げるために必要となるセンター数がセキュリティ強度に比例して増大することにある。

以上述べた3種類のアプローチ毎に主要な研究例を表 1 に示す。本提案は、表中のTYKK98に代表される方式である。

表 1 電子投票・アンケート研究代表例

ブラインド署名方式	**Chaum [Cha85] [Cha88]**	**太田[Oh88]**
	○ブラインド署名(個人の匿名性を守りつつ、確かな署名である事が検証できる署名方式)を提示。 ○[Cha88] では複数の選挙管理センターを必要とせず、単独の選挙管理センターで構成。 ○開票作業は投票者全員が協力して一斉に同時に行わなくてはならない。 ○自分以外のすべての投票者が結託しない限りにおいて、個人のプライバシは保たれる。 ○indevidually verifiable(個別検証可能)な方式。 ○RSA 暗号ベースのブラインド署名を利用。 ○anonymous channel を物理的仮定として設定。	○単独の選挙管理センターで構成できる方式の提案。 ○方式は、投票者、信頼できる選挙管理センター、集計センター、匿名通信路、および掲示板で構成される。 ○集計センターは著名確認後、掲示板に表示、各投票者は、掲示板で自分の票が存在する事を確認する事で individually verifiable(個別検証可能) な方式となっている。 ○投票者による 2 重投票を防止できる方式で、もし行われた場合は、誰が行ったかを特定できる方式。 ○計算量・通信量共に実用的な範囲に抑えた。 ○不正が起きた場合、クレームを挙げる場合の投票者のプライバシが無い。 ○RSA 暗号ベースのブラインド署名を利用。 ○選挙管理センターと集計センターが結託しても投票者の匿名性を保護可能。 ○大規模選挙向け。 ○anonymous channel を物理的仮定として設定。 ○同時期に Chaum も anonymous channel を利用した方式を提案。
ミックスネット方式	**Chaum[Cha81]**	**Park, 伊藤, 黒澤[PIK94]**
	○匿名通信路:Mix-net を最初に提案。 ○RSA 型暗号に基づいて Mix-net を構成し、匿名性を確保。 ○複数の mix-server がカスケードの配置。 ○全ての mix-server が正しく動かなくては正確な出力は出ない。 ○投票者は、各 mix-server が保有する公開鍵で多重に暗号化した電子メールを投票。 ○投票者が送信する暗号文は、mix-server の数に依存し、増加する。 ○各 mix-server は各電子メール同士の順番をシャッフルし入力との対応をなくし、且つ復号処理を行う。 ○individually verifiable(個別検証可能) な方式。	○ElGamal 暗号に基づいて構成。 ○暗号化されたテキスト長が mix-server 数に独立。 ○公平性を実現。 ○公平性を保つためには、各投票者の通信量は、ビット数 O(nk)ビット以上が好ましい。(ここで、n はビット長、k は mix-sever の数) ○全ての mix-server が正しく動かなくては正確な出力は出ない。 ○indevidually verifiable(個別検証可能) な方式。
準同型性暗号方式	**Benaloh,Yung [CY85][Ben86][Ben87]**	**佐古[SK94]**
	○投票者、n 個のセンター、掲示板で構成 ○投票内容は賛成、反対の二値方式(以降、準同型暗号方式)を用いた提案はすべてこの二値方式 ○各センターは r 次剰余暗号(確立的暗号)を構成 ○投票者は自分の票を定数項とするランダムな(t-1)次多項式を構成、各センターの公開鍵で暗号化して公開し(t-1)次の多項式であることを証明 ○票の内容が 0 または 1 であることを暗号カプセルプロトコルを用いて証明[Ben86] ○各センターは自分に送られてきたものを復号、(t-1)次の多項式である為、t 個以上のセンターが正しく処理していれば結果を復元可 ○集計値の正当性を零知識証明プロトコルで証明 ○以上の証明に対する検証は誰でも(投票者、センターに限らず)掲示板上の情報を元にして行うことが出来る:Universal Verifiability	○投票者、複数のセンター、掲示板で構成 ○[CY85]と同じ信頼性を保ちつつ処理量、通信量を大幅に減少([CY85]と比較して処理量 1/4、データ量を 1/80)投票時、投票者は仮投票に付加する情報を送付するのみ ○仮投票データ(1又は、-1)を事前に作成、提出し、正当性(暗号処理の正当性、仮投票内容の正当性)を零知識証明で誰でも検証可としている。重い計算やデータ転送は投票前に実施し実際の投票時に要する通信量、処理量を大幅に軽減 ○不正集計防止手段として、準同型暗号 E(X)=g^x mod q(X:平文、g,q 公開定数)を用い公表されたサブ集計とすべての投票文の一致性を準同型性を利用して暗号文のまま、誰でも検証可。[CY85]は準同型暗号として1対多に写像される確立暗号を用いるため零知識証明を使用

ブラインド署名方式	**浅野，松本，今井[AMI91]** ○公平性問題を解決 ○不正が起きた場合、クレームを挙げる場合の投票者のプライバシが無い。 ○選挙管理センターが不正行為を行った場合に、投票者のプライバシが犯される。 ○選挙管理センターが各投票文に対する総当りの計算により投票内容を求めるような攻撃をしない範囲において、その公平性を保てている。 ○選挙管理センターが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○anonymous channel を物理的仮定として設定。	**佐古[Sk92]** ○集計センターの不正に対し、自己の票の内容を公開することなしに異議申立てを行え、プライバシを保てる方式 ○異議申立ては有権者のみが提示できる Vote-tag を公開する事で行う。 ○賛成 or 反対 の 2 択の選挙において有効。 ○投票を破棄する投票者がいない事を仮定として設定。 ○RSA 暗号ベースのブラインド署名を利用。 ○署名は、投票内容を含まないメッセージに対してもらう。 ○選挙管理センターと集計センターが結託しても投票者の匿名性を保護可能。 ○集計センターが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○untappable channel(物理的に盗聴不可能な通信路)を物理的仮定として設定。
ミックスネット方式	**佐古, Killian[SK95]** ○[PIK93]の方式をベースに、ゼロ知識証明(Cut-and-Choose 方式)を利用しており、全体検証可能(universally verifiable) で公開検証可能な方式。 ○無証拠性の性質を実現。 ○匿名通信路を物理的仮定として設定。 ○全ての mix server が正しく動かなくては正確な出力は出ない。 ○攻撃(n-2 サーバの結託で anonymity が破れる)が示されているが、容易に修正可能である。 ○堅牢性の性質を付加した方式が、1998 年に尾形、黒澤、佐古、高谷らにより提案されている。その閾値は 1/2 であり、不正な mix-server の数が 1/2 以下の場合、正確な結果を出力可能とした。 ○更に、頑健性の性質に加え、検証者の計算量を軽減させた方式が 1998 年に阿部より提案されている。	**Jakobsen[J98]** ○閾値付き El Gamal 暗号に基づき構成。 ○効率の向上、各 Mix-Server の計算量は O(tN),(ここで、t 閾値) ○1/N の確率で cheating が成功してしまう。(ここで、N は投票者の数)。その為、N の大きな大規模選挙向けの方式である。 ○全体検証可能(universally verifiable)であるが、公開検証可能ではない為、検証して納得できるのは mix-server 自身のみ。 ○[J98]方式は、Euro2000 で Desmedt、Kurosawa により攻撃方法が示されている。改善方法は提示されていない。代わりに、[J98]とは全く異なる方式も提示されている。 ○99 年に新たに方式を提案したが、その方式に関しては、Asiacrypto2000 にて Mitomo, Kurosawa により攻撃方法と改良方法とが発表されている。
準同型性暗号方式	**Gramer,Franklin,Schoenmakers,Yung [CFSY96]** ○投票者、複数のセンター、秘密通信路、掲示板で構成 ○離散対数問題に基づく準同型な暗号系を適用 ○マスク票に秘密情報を付加したものを票とする ○秘密情報を定数項とする(t-1)次の多項式を構成 ○上記多項式の各定数を暗号化し公開 ○マスク票を定数項とする(t-1)次の多項式を構成し、秘密通信路を用いて管理センターに送る ○多項式の正当性を 3-move プロトコルで検証 ○集計;t 個までの正しいセンターが集まると正しい集計値を得ることが出来る ○センター数が 10 の場合、投票者に要求される通信量は約 10K ビット(離散対数方式における |P|=512 ビット,|q|=160 ビット)	**Gramer,Gennaro,Schoenmakers,[CGS97]** ○[CFSY96]ではセキュリティ強度の向上の目的等でセンターの個数を増加させる場合、投票者の作業量はセンター毎に分割した票を作成、検証する方式の為、センター数に比例して計算量、通信量が増加 ○本方式は投票者の計算量、通信量がセンターの個数に独立、投票者はシステムでただ一つの公開鍵で暗号化し、検証するのみ ○鍵生成 各センターが保有する分割秘密鍵 Sj を持ちより Lagrange 係数法により秘密鍵 S を生成(Shamir's(t-n)-Threshold secret sharing schem).$h=g^s$を公開鍵とする ○暗号系は ElGamal 暗号を適用、投票内容は G 又は 1／G ○票内容の正当性(G 又は 1/G)を検証する 3-move プロトコルを提案 ○票の集計に準同型性を利用 ○開票:指数部にある集計値をシーケンシャル検索法にて求める ○高次剰余暗号系も適用

ブラインド署名方式	**藤岡，岡本，太田[F0093]** ○公平性、匿名性を両立させた方式。 ○公平性実現にはビットコミットメントを方式に組み込む事で実現。 ○投票内容は、2 択以外の内容にも対応可能。 ○投票者の集計処理への参加が必要。 ○選挙管理センターと集計センターが結託しても投票者の匿名性を保護可能。 ○集計センターが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○大規模投票に向いている。 ○anonymous channel を物理的仮定として設定。 ○sensus や e- vote 等を筆頭に実装・公開実験などが実施されている。 ○分かりやすい構成であるため、広く実用化されている。	**大久保，三浦，阿部，藤岡[OMAFO99]** ○[FOO92]を改良。 ○walk-awayness(投票者は集計ステージに参加する必要がなく、投票の後は束縛されない性質)を実現。 ○公平性、匿名性を両立。 ○公平性を保つために用いられていたビットコミットの代わりに Threshold 暗号を用いている事により、公平性と匿名性の両性質を実現しつつ、ユーザの利便性を向上した方式。 ○選挙管理センターと集計センターが結託しても投票者の匿名性を保護可能。 ○集計センターが表示した掲示板で、自分の票があるか否かを確認する事で、individually verifiable な方式(個別検証可能な方式) となっている。 ○大規模投票に向いている。 ○anonymous channel を物理的仮定として設定。Mix-net による匿名通信路の実装も提示。
ミックスネット方式	**阿部[Ab00]** ○MIX への入出力数が N に対して、2 入力 2 出力の permutation を多段に組み合わせる構造。 ○2 入力 2 出力の permutation により、入出力が N である Mix-net を構成する最適な組み合わせについて解析。 ○全体検証可能(universally verifiable) であり、且つ公開検証可能である方式であり、且つ堅牢性を保持できる方式として、Cut-and-Chooose 方式を用いずに実現した初めての方式。 ○従来方式の多くは、mix-server 間の通信が頻繁に行われるものが多いが、この方式では各 mix-serbver のプロトコルへの参加を極端に抑える事が出来ている。 ○2 方式提案されており、各 mix-server の処理が 1 度の方式と 2 度の方式とがある。 ○Permutation Network の計算量は O(t N logN)。 ○N がそれほど大きくならない小・中規模の投票に適している。 ○修正と高速化が[AH01]で示されている。 ○2べき以外の入力数の効率的な扱いが[Su01]で示されている。	**大久保，阿部[OA01]** ○Hybrid 型暗号系を利用(ElGamal 暗号と共通鍵暗号とに基づく方式)。 ○各 mix-server の公開鍵の生成方法に工夫があり、前段の server の公開鍵を元に生成される。 ○投票者は平文(投票内容)を共通鍵暗号で n 多重に暗号化する。(ここで、n は mix-server の数) ○共通鍵暗号による平文の暗号化に用いる共通鍵は、各 mix-server の公開鍵に基づき生成。 ○暗号化されたテキストの長さが mix-server の数に独立。 ○ElGamal 暗号に基づく Mix-net では一度に処理できる平文の長さが公開鍵の長さによって制限されるが、この方式では固定任意長の平文を処理できる。 ○計算量・通信量共に効率的な方式。 ○投票者・閾値以下の mix-server の不正に対しては、堅牢性を保持できる方式。
準同型性暗号方式	**辻井、山口、北澤、黒澤 [TYKK98]** ○有権性確認・集計及び開票を行う二種の管理センター及び公開ボードで構成 ○準同型性特性を有する高次剰余暗号系を適用、暗号化されたままの各票を掛け合わせることにより集計 ○高次剰余暗号系の秘密鍵を保有する開票センターにより各個人各票を開票されるのを防ぐ目的で高次剰余暗号系で暗号化された票をさらに RSA 暗号系(有権性確認集計センターが秘密鍵保有)で暗号化したものを公開ボードに表示 ○二重暗号化された票が賛成、反対票の条件を満たしていることを Benaloh の暗号カプセルに機能追加して検証可とした。 ○正しく集計していることの検証プロトコルを提案 ○復合処理時間を実測し大規模選挙にも適用可の事を証明[YKT00] ○Biglobe を使用した実証実験を行い実用性の検証を行った[YKT00]	**Scheumaker[Sch99]** ○Public Verifiable Secret Sharing(PVSS,Stadler により提安)方式であり、藤崎、岡本[FO98]の効率向上版 ○投票内容 $V \in \{0,1\}$ に秘密情報 S を付加し Diffie-Herman 仮定の下 $U=G^{S+V}$ を公開 ○秘密情報 S を定数項とする(t-1)次の多項式を構成し、各センターの公開鍵で暗号化し公開 ○上記多項式の各定数 αj より $g^{\alpha j}$ を求め公開 ○多項式の正当性の正当性を検証する ○[CGS97]方式において、各センターが保有する分割秘密鍵を持ち寄って秘密鍵を生成する方式においてはセンター管理者、センター数の変更に伴い公開鍵の再生成が必要であるが本方式はこの再生成が不要 ○CFSY96 は分割秘密情報を秘密通信路を介して送る方式であるが、本方式は秘密通信路の必要はない ○CFSY96 は各票を一つ一つ復号するが本方式は加算(集計)された票を復号するのみ

2-2　国内における電子投票の現状

平成13年の12月に「電子式投票機を用いて行う投票方式等の特例に関する法律（電子投票法）」が施行された以降、下記に示すような複数のベンダーが第一段階の電子投票を実現してきている。しかし、これらのほとんどは第二段階、第三段階を考慮したものにはなっていない。従って、第三段階実現のためには、柔軟性・汎用性、安全性・信頼性、及び経済性に富むシステム構成を突き詰めて、運用面からも新たに生じる問題を解決していこうという段階である。

表 2 第一段階の電子投票システムの主な開発元とその特徴

開発元 「システム名称」	主な特徴	投票機の仕様、大きさ等
電子投票普及協業組合「電子投票機VT25」	全国初の新見市市長、市議会選挙で使用された 入力装置にはタッチペンを利用 電磁的記録媒体にはコンパクトフラッシュを採用	幅：350mm、奥行：350mm 高さ：　前面部102mm、背面部180mm(ポール部除く) 重量：約8.8kg、画面：15型 カード：ICカード
東芝「地方自治体向け電子投票箱」	候補者の選択画面は、候補者数に応じて「候補者名の一覧表示」「番号による選択」「50音からの選択」等のインターフェイスが可能 親しみやすいデザイン 電磁的記録媒体は1,000人まで対応可能	幅：450mm、奥行：600mm 高さ：　前面部100mm、背面部350mm(ポール部除く) 画面：15型 カード：磁気カード
NECシステムテクノロジー「選挙管理システム」	不在者投票システムなど、他の選挙事務管理システムとの連携 カードは非接触のICカードを採用 第2、第3段階も考慮した拡張性	幅：450mm、奥行：600mm、高さ：150mm、重量：約6kg、画面：10.4型、カード：ICカード
ムサシ／富士通「Tellac EM100 シリーズ」	富士通と選挙ビジネスのノウハウを持つ株式会社ムサシによる共同開発 投票所内はクライアント／サーバ方式、投票所のサーバにおいて、投票データを蓄積 電磁的記録媒体には専用メモリカートリッジを採用 カードはIC、磁気カードに対応 操作オプションとして、ヘッドホン音声ガイド、テンキー操作卓、タッチペン等が利用可能	画面：15型 カード：磁気、IC
NTT東日本「（電子投票システム）」	NTT独自の暗号技術を利用、選挙人のプライバシーを保護 開票作業は複数人の合意により実施 各投票所から集められた投票データをシャッフルする機能 電磁的記録媒体にはコンパクトフラッシュを採用	幅：420mm 高さ：230mm 重量：7kg 画面：15型 カード：ICカード

出展　：　EVS電子投票普及協業組合ホームページ

一方、平成17年4月施行予定の「個人情報の保護に関する法律」の観点から、電子投票やアンケートなど、インターネットを利用したサービスの本格化に伴い、情報セキュリティの重要性が増し、ネットワークにおけるより高度な暗号技術へのニーズが高まっている。これをターゲットに日本電気株式会社（NEC）は電子投票やインターネットなどにおける秘匿性を実現する業界初のミドルウェアを平成16年1月に発表している。
第三段階への対応を見据えた本製品は今後の進展に大きな期待が持てるものであるが、ミドルウェアの性格上、柔軟性・汎用性、安全性・信頼性、及び経済性に富むシステム構成や運用面に関しては個別に取り組む必要があり、方向が確立するまでには、まだ、時間が必要な状況である。
ただし、採用している暗号方式「digishuf」につきましては、有望な方式の一つであり、得意とする分野で本研究開発と連携したシステムとして今後協力していく可能性もある。

3　研究開発の全体計画

3-1　研究開発課題の概要

研究開発目標は、「任意の端末から入力できる、第三段階の電子投票システムを次世代電子投票・アンケートシステム」と位置付け、それを実現するための基盤技術を開発することである。より具体的には、本課題の目標は下記の通りである。

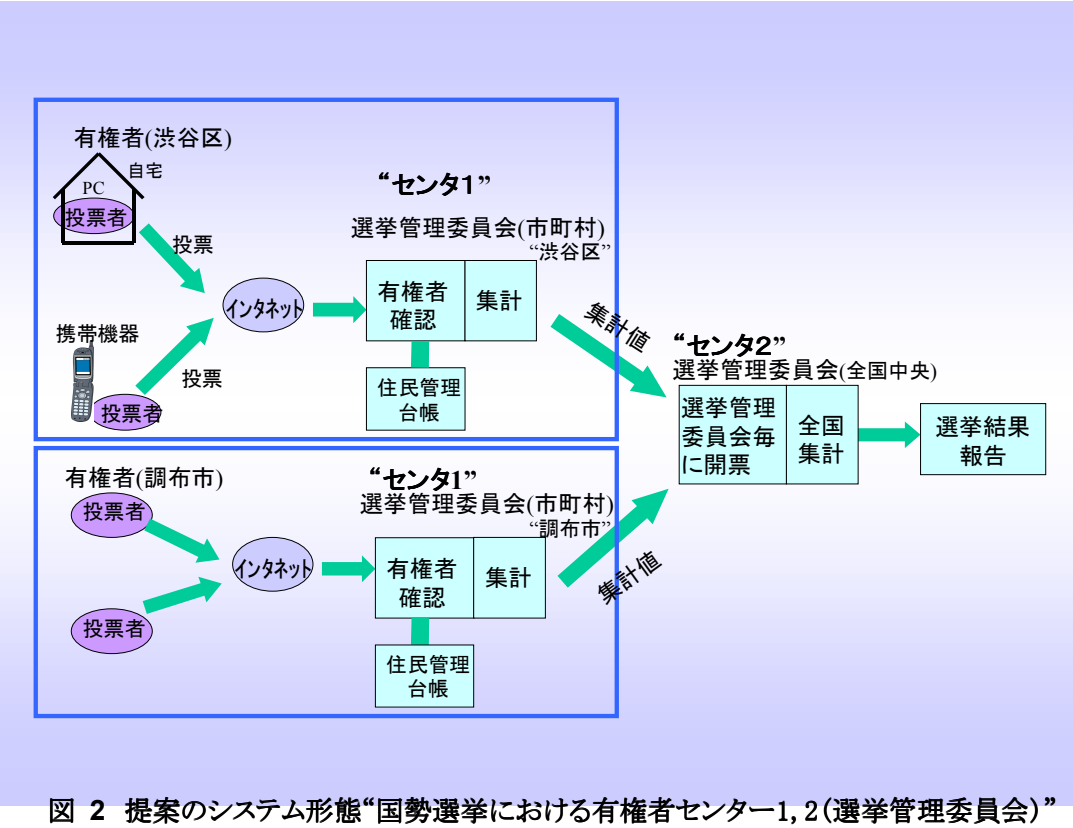


図 2　提案のシステム形態“国勢選挙における有権者センター1, 2（選挙管理委員会）”

・自宅のパソコンあるいは携帯端末から投票でき、従来の選挙システムを上回る確実性、安全性を保証することに加えて、従来の選挙では実質上不可能であった公的検証性を有する電子投票システムの構成法を検討する。ここで、公的検証性とは「自分の投票が集計結果に正しく反映されているか」を検証できること、および有権者の誰もが選挙のプロセスが定められたプロトコル通りに実行されていることが検証できることを意味している。上記システムを可能な限り簡易な構成とすることで、コンピュータシステムとしての信頼性が高く低コストで運用性の高いシステムを国政選挙レベルの規模で構築する方式を検討する。
・上記に述べた技術的ブレークスルーの達成により、プライバシーを守りつつ、ユーザの意見や要望を収集するという Pull 型情報システムを実現可能とし、潜在する巨大な市場を顕在化させ、経済活性化に寄与する。

上記の目標を達成するため、以下の図 3 に示す考え方に基づく 3 つのテーマについて研究開発を行う。

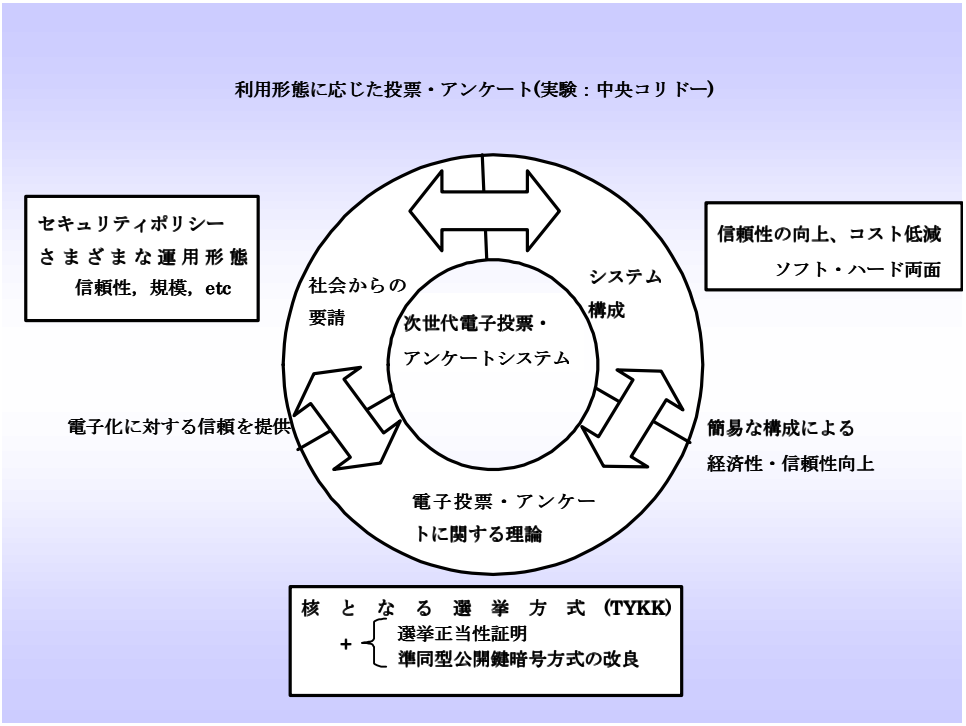


図 3 次世代電子投票・アンケート方式とその社会的利用に関する研究(概念図)

(1) システムに対する要件整理とシステム構成

(ⅰ)社会的利用分野の広がりを考慮しつつ、システムの全体の構成と要求される機能と安全性等の保障等の要件について検討する。当初想定していたシステム構成は図2の通りであり、その概要は次の通りである。

センター1の機能

① 投票者の有資格者認証
② 個々の投票内容を知ることなく、票の集計を行う。その集計値もセンター2の公開鍵暗号方式で暗号化されているため、センター1は知ることは出来ない。センター1は集計値の開票も出来ない。
③ 投票者の二重投票等の不正検出

センター2の機能

② 票の集計値を復号(個々の投票内容を知ることは出来ない)
③ センター1の不正検出

(ⅱ)以下の(2)で述べる要素技術の研究開発で得られた成果をハードウェアおよびソフトウェアを適宜組み合わせて実装する。

(ⅲ)参加企業を結ぶネットワークで諸性能を確認し、解決すべき課題を抽出して要素技術の研究開発に反映させる。その結果を踏まえた上で、東京都、山梨県、長野県の地方自治体と諸企業が参加する「中央コリドー高速通信実験協議会」のネットワーク上に実装して、課題の抽出と解決を図る。

(ⅳ)(ⅲ)と平行して、電子投票のためのコンピュータネットワークシステム(製品)を対象とするセキュリティ評価基準の検討、および運用システムに対して ISO17799(ISMS)に基づいたセキュリティポリシーガイドラインの検討を行う。

ただし、電子投票システムとしての機能要件は投票方式に依存しない形で進め、図 4 のような投票方式毎の実装への影響を極力吸収する様なシステムインターフェイスを検討することで、どのような投票方式でも対応できるように研究する。

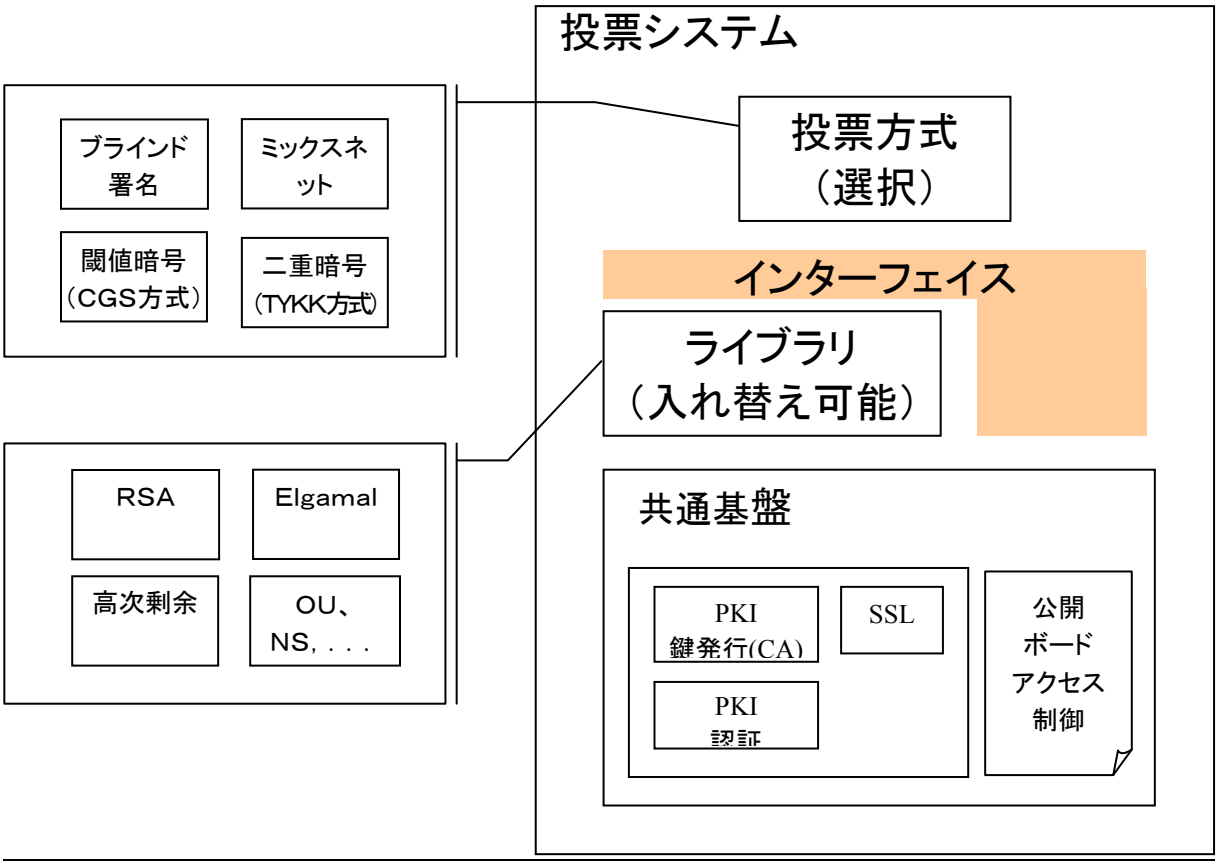


図 4 投票プロトコルと実装の関係

(2) 要素技術の研究開発

キーテクノロジーは

－1 準同型公開鍵暗号方式

－2 投票プロセスの正当性証明とその効率化

であるので、それらの研究課題について以下に説明する。

(2)－1 準同型公開鍵暗号方式

先ず、準同型公開鍵暗号方式について、そのイメージを簡単に説明する。平文を m_1 として、これを暗号化することを考える。素数を p，原始元を g として

$$y_1 = g^{m1} \bmod p$$

を計算し、y_1 を平文 m_1（投票者1の投票内容）に対する暗号文とする。P が 10 進で 300 桁程度の大きさの場合、p, g, y_1 を公開しても m_1 を求めることは計算量的に実際上不可能となる（離散対数問題の困難性）。このままでは正当な受信者も復号できず、暗号方式になっていないので、ある種の工夫が必要になるが、ここではその説明は省略する。2 番目の投票者の平文を m_2 とし、

$$y_2 = g^{m2} \bmod p$$

とする。このとき

$$y_1 y_2 = g^{m1+m2} \bmod p$$

となる。これが準同型の例である。2つの暗号文の積をとることによって暗号化された状態のまま2人の投票者の合計値（m_1+m_2）が暗号文 y_1y_2 の平文となっている。（m_1, m_2 が 0，1のような小さな数の場合には、乱数の利用などが必要となる。）

投票者が n 人の場合、$\sum_{i=1}^{n} m_i$ が $\prod_{i=1}^{n} y_i$ に対する平文となり、暗号化された状態のまま、平文が合算されていることになる。

以上の原理を暗号方式として具体化した方式として、高次剰余暗号、OU 関数，Paillier 等の諸方式が知られている。これらの方式を第 2 センターの公開鍵暗号方式として利用することにより、第 1 センターは投票内容を知ることなく（第 2 センターの秘密鍵を持っていないので復号できない）、暗号化された状態のまま合計値を平文とする暗号文となる。

暗号化を投票用紙を封筒に入れて密封することに喩えると、次のようなプロセスになる。

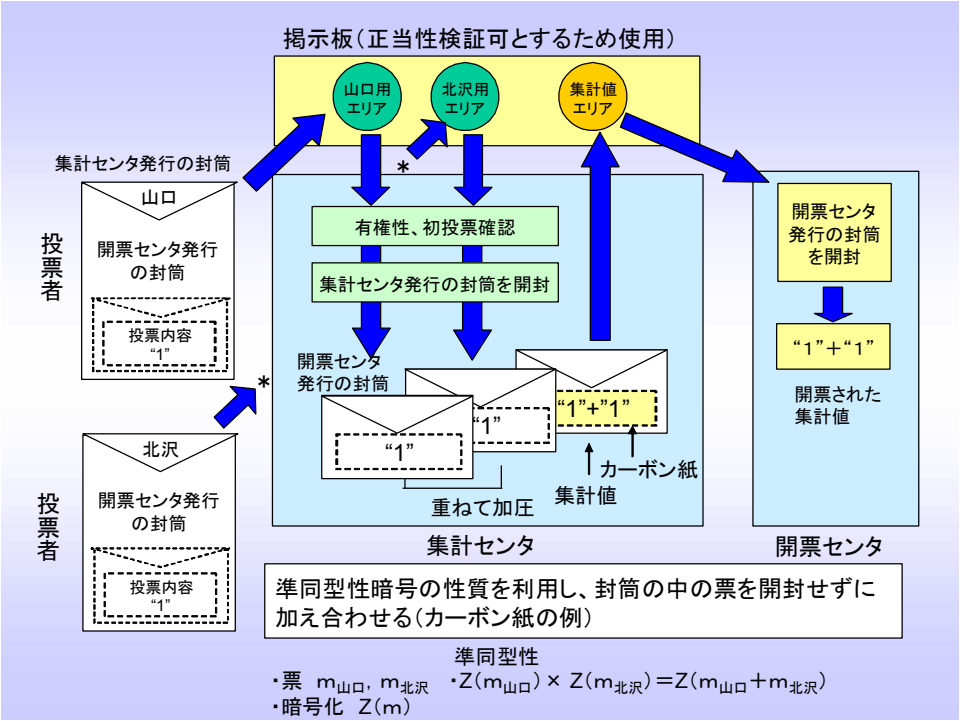


図 5 電子選挙:TYKK 方式のプロセス

(i) 投票者は投票内容を記した投票用紙を先ず第 2 センター宛ての封筒（内側封筒）に入れて密封し、次に第 1 センター宛の封筒（外側封筒）に入れて密封し、第 1 センターに送る。

(ii) 第 1 センターは、外側封筒のみを開封する（内側封筒は開封できない）。他の投票者についても同様の事を行う。

(iii) 全ての投票者の内部封筒を（密封されたまま）束ねる（$\prod_{i=1}^{n} y_i$ に相当）と、封をされた新しい封筒の中に、投票内容の合算値（$\sum_{i=1}^{n} m_i$）が記入された投票用紙が密かにすべり込んでいる。

このように一種の手品のような仕掛けが上記の離散対数問題の困難性を利用することによって実現された。

本課題では、高次剰余暗号, OU 関数, Paillier, Naccache-Stern 方式などの公知の諸方式について安全性、実装性、処理速度等の面から比較検討する。既に、申請者等は高次剰余暗号方式を実装の上、処理速度に関する実験を行っている。その結果、高次剰余暗号方式については、投票者が多い場合は処理に長時間を要するのではないかという専門家の予想に反して、1 億人程度でも数分間で処理できることが明らかになった。高次剰余暗号よりも高速化が期待できる, OU 関数, Paillier, Naccache-Stern 方式などについても、同一の安全性を確保するという条件の下、実装性、処理速度等の面から比較検討を進める。

(2)－2投票プロセスの正当性証明とその効率化

電子投票・アンケートシステムは、投票のプロセスに起こりうる次のような不正を想定して構築しなければならない。

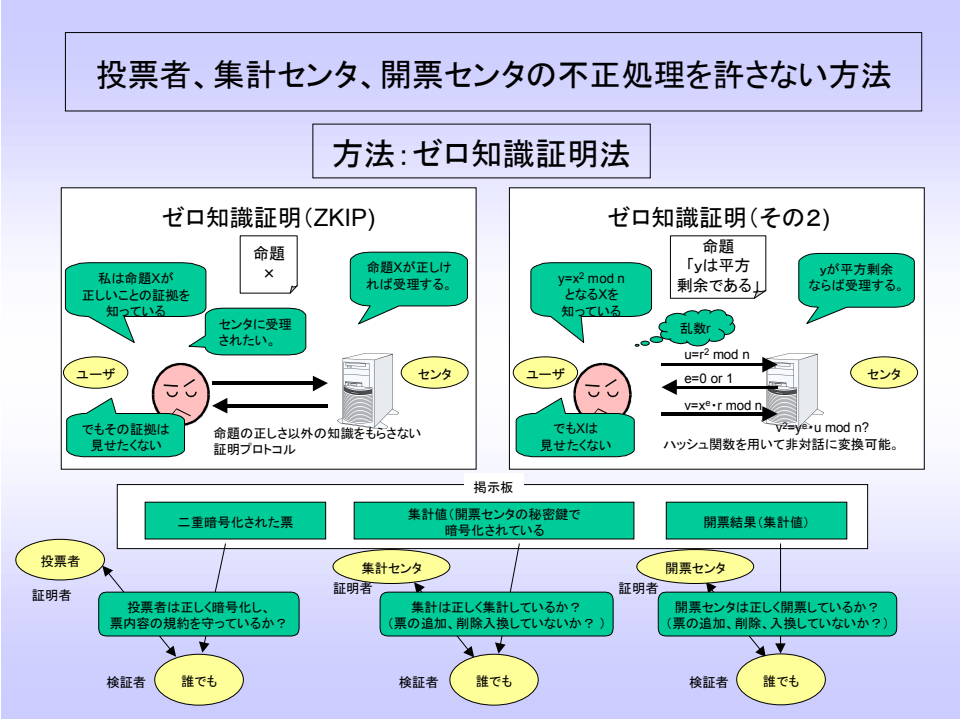


図 6 正当性証明

(i) 投票者が定められた手順で暗号化していない
(ii) 第一センターが、票の集計を手順どおりおこなっていない
(iii) 第二センターが開票を手順どおりおこなっていない
本課題ではこれらの不正を零知識対話型証明理論を応用して効率よく検証する方法を検討する。

レシートフリー性(自由意志での投票)については、理論的なアプローチと実装によるアプローチの併用で検討する。

(i) 理論的なアプローチ

理論的なアプローチとしては、SK95、Oka97、HS00、及びプロジェクト開始後に提案された JJ02 などの方法が知られている。TYKK 方式のレシートフリー機能実現のため、HS00 と類似の方式を適用できるようにする。

準同型方式に対しては、盗聴不可能な通信路の存在を仮定すれば、理論的にレシートフリー機能を実現できることがHS00により示されている。このとき、投票内容を暗号化した暗号文をセンターが作成して投票者に渡し、投票内容(平文)が何であるかを投票者のみに証明するという特殊な仕組み(designated verifier proof)を利用する。TYKK方式においては、センター2が暗号文の作成と投票者のみへの証明を受け持ち、投票者がそれを再暗号化して公開掲示板に掲示するという、HS00と類似の方式を適用することにより、理論的にレシートフリー機能を実現できる。

(ii) 実装によるアプローチ

投票データである暗号文をICカード内で生成する場合は、ICカード内で生成した「証拠となりうる一部のデータ」をICカード内で強制的に削除すること(JJ02で部分的に使われている方法)により、レシートフリー機能を実現する。

ただ、実装によるアプローチでレシートフリー機能を実現するためには、実装に対して利用者に信頼してもらうことが不可欠である。これは管理運用技術と連携しつつ達成を図る。

(3) 社会的利用形態の創造とシステムの運用管理

任意の端末から入力できるプライバシー保護が保証された電子投票・アンケートシステムは、電子行政分野はもとより、電子ビジネス、生活、ファイナンス、医療、教育等あらゆる分野においてニーズが潜在している。たとえば、個人個人の好みに合わせた商品開発におけるアンケート調査や、マンション立替の賛否をめぐるアンケート調査などが考えられる。

一般に、現在のところインターネットの利用形態は Push 型が主であるが、利用者がアンケート等に答える Pull 型の利用形態も潜在的には多いものと考えられる。本研究で提案する、さまざまな不正を防ぎつつ、プライバシーを守り、かつ、信頼性と経済性に優れた電子投票・アンケートシステムを利用することによる新しいインターネット利用の社会的形態を作り上げてゆきたい。

次に、これらの利用形態に対応して、電子投票・アンケートシステムの管理運用のありかたについて、ISO17799(ISMS)の観点から検討してガイドラインを作成する。

3-2　研究開発目標

3-2-1　最終目標（平成１７年３月末）

【研究開発課題】「次世代電子投票・アンケートシステムとその社会的利用に関する研究」

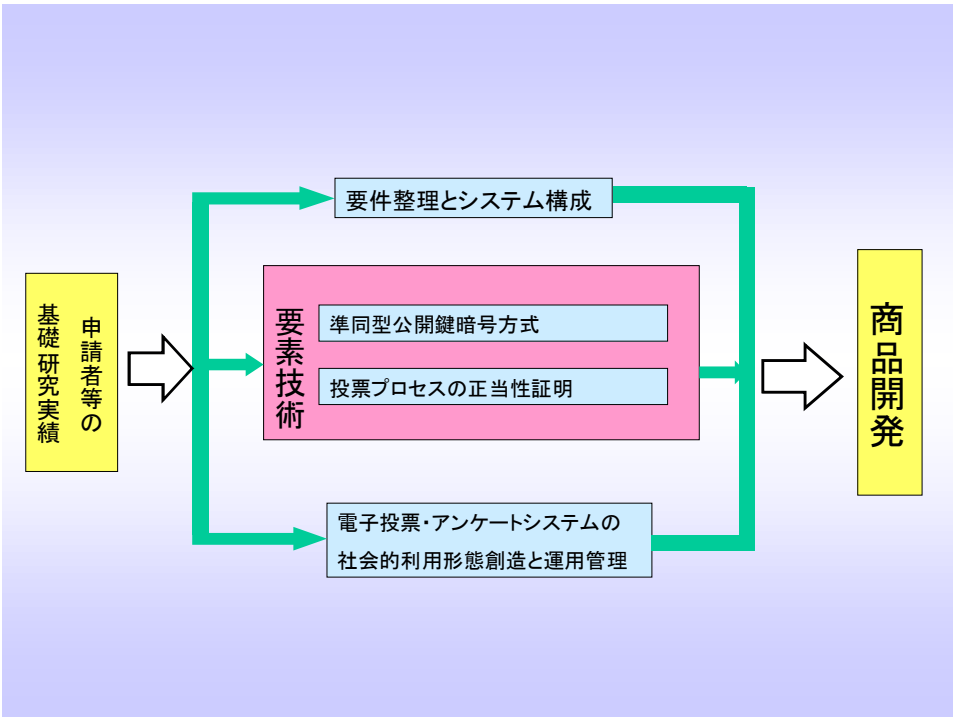


図 7　本研究開発の課題

（1）　社会的利用形態の創造とシステムの運用管理

次世代電子投票システムの法、社会制度への適合性を明確にし、明確な機能要件のもとに実現性を検証するとともに、アンケートなど、派生するさまざまな社会的利用を促進するために、以下のサブテーマを設定して研究を行うこと。

・利用分野と法・社会的制度の適合性
・運用利用形態ごとの要件整理
・効率的運用とリスク分析
・セキュリティポリシー

（2）　システム構成

信頼性と経済性を重視した構成方法（準同型―2センター方式）の諸性能に関する実証的研究を、以下のサブテーマで行うこと。

・システム構成
・モデル構築
・実験

（3）　要素技術

信頼性と経済性を重視した構成方法（準同型―2センター方式）の諸性能に関する理論的研究を、以下のサブテーマで行うこと。

・準同型公開鍵暗号方式
・選挙の正当性証明の理論

以下に(1)(2)(3)の各サブテーマについて述べる。

【サブテーマー1】利用分野と法・社会的制度の適合性

次世代電子投票を実現するにあたり解決すべき、法・社会制度を抽出し、その解決に必要な機能要件を導き出すこと。また、アンケートなど、投票に類似する利用分野を行政、電子商取引、教育、医療等の領域から最低5分野は開拓すること。

【サブテーマー2】運用形態ごとの要件整理

「次世代電子投票の満たすべき性質」が全て網羅された、「電子投票機能要件に関する標準」のドラフトが整備されること。このドラフトは、国政レベルで次世代電子投票要件に関する標準化が策定される際に、その入力として十分なものであること。具体的には、第一レベルの「電子投票システムに関する技術的条件及び解説」相当の内容を有するものであること。

【サブテーマー3】効率的運用とリスク分析

サブテーマー2で示される運用要件をもとに、性能上のボトルネックを解析し、解決策を提示すること。また、考えられるリスクとそれに対応するための指針を明示すること。

【サブテーマー4】セキュリティポリシー

次世代電子投票システムのセキュリティポリシーを、以下の観点から研究すること。

(i) 製造過程の観点(ISO15408)では、製造物のセキュリティ基本設計の核となる、セキュリティ設計ガイド(Protection Profile)のための指針を作成すること。

(ii) 運用の観点(ISO17799,ISMS)では、実際のポリシー、規定、手順のガイドラインを策定すること。

【サブテーマー5】モデル構築

TYKK 方式に基づく電子投票システムの参照モデルを構築すること。このモデルは、数万人から100万人程度までの利用者が利用できるだけのスケーラビリティを保証すること。なお、リファレンスモデルによる実験を想定して、その際に想定される性能のボトルネックを解消するために必要な計測方式を確立すること。

【サブテーマー6】システム構成

TYKK 方式に基づくシステム構築の元となる準同型性暗号方式の実装を準備し、性能測定を行うこと。特に開票性能が100万人レベルの投票で、10分以内であること。

【サブテーマー7】実験

参加企業および中央コリドー高速通信実験協議会の協力による電子投票実験を行い、性能、運用性の確認と、利用者の意識調査を行うこと。

【サブテーマー8】準同型公開鍵暗号方式

次世代電子投票システムに利用すべき暗号方式を、安全性と性能の対比のもとに策定すること。性能は理論値を用い、安全性は、定義の明確なものを尺度とすること。既存の諸方式の比較および、新方式の探求を行うこと。

【サブテーマー9】投票プロセスの正当性証明とその効率化

電子投票プロトコルに用いられる正当性の証明方式および監査履歴方式を、性能の観点から検討し、理論的に検証すること。なお、応答性能は、利用者の端末における処理性能と、選挙用サーバにおける処理性能を別に示すこと。選挙用サーバにおける処理性能は、投票者数に比例するレベルであること。また、監視下ではない投票端末を利用した場合の、買収や脅迫といった問題を解決する方法であること。

3-2-2 中間目標（平成１６年３月末）

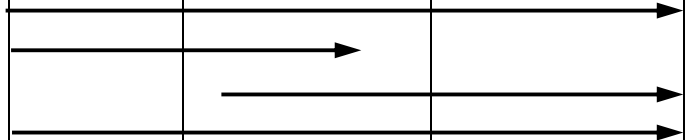
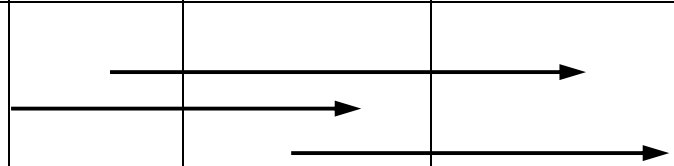
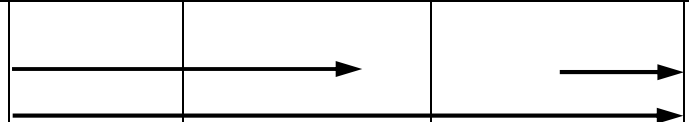
本研究の各サブテーマ毎のスケジュールは以下の通りである。中間目標は、要素技術のほとんどの研究が最初の成果を得ることを目標としており、下図の点線で示す、H15年度末を予定している。

大テーマ	サブテーマ	H14	H15	H16
社会的利用形態の創造とシステムの運用管理	1. 利用分野と法・社会的制度の適合性		調査研究 →	
	2. 運用形態ごとの要件整理	調査検討 →		
	3. 効率的運用とリスク分析		調査分析 →	
	4. セキュリティポリシー(ISO17799etc)		ポリシーガイドライン作成 →	
システム構成	5. モデル構築		構築 →	
	6. システム構成	準同型暗号方式の設計・実装 →		
	7. 実験		参加企業ネット・CCC利用実験 →	
要素技術	8. 準同型公開鍵暗号方式	諸方式の比較・新方式探求 →		→
	9. 投票プロセスの正当性証明とその効率化	ZKIP・耐買収性 →		

中間結果以降では、システム構成の実験を中心として、そこからの課題の発掘と研究へのフィードバックおよび、最終的な実験への反映を行う。

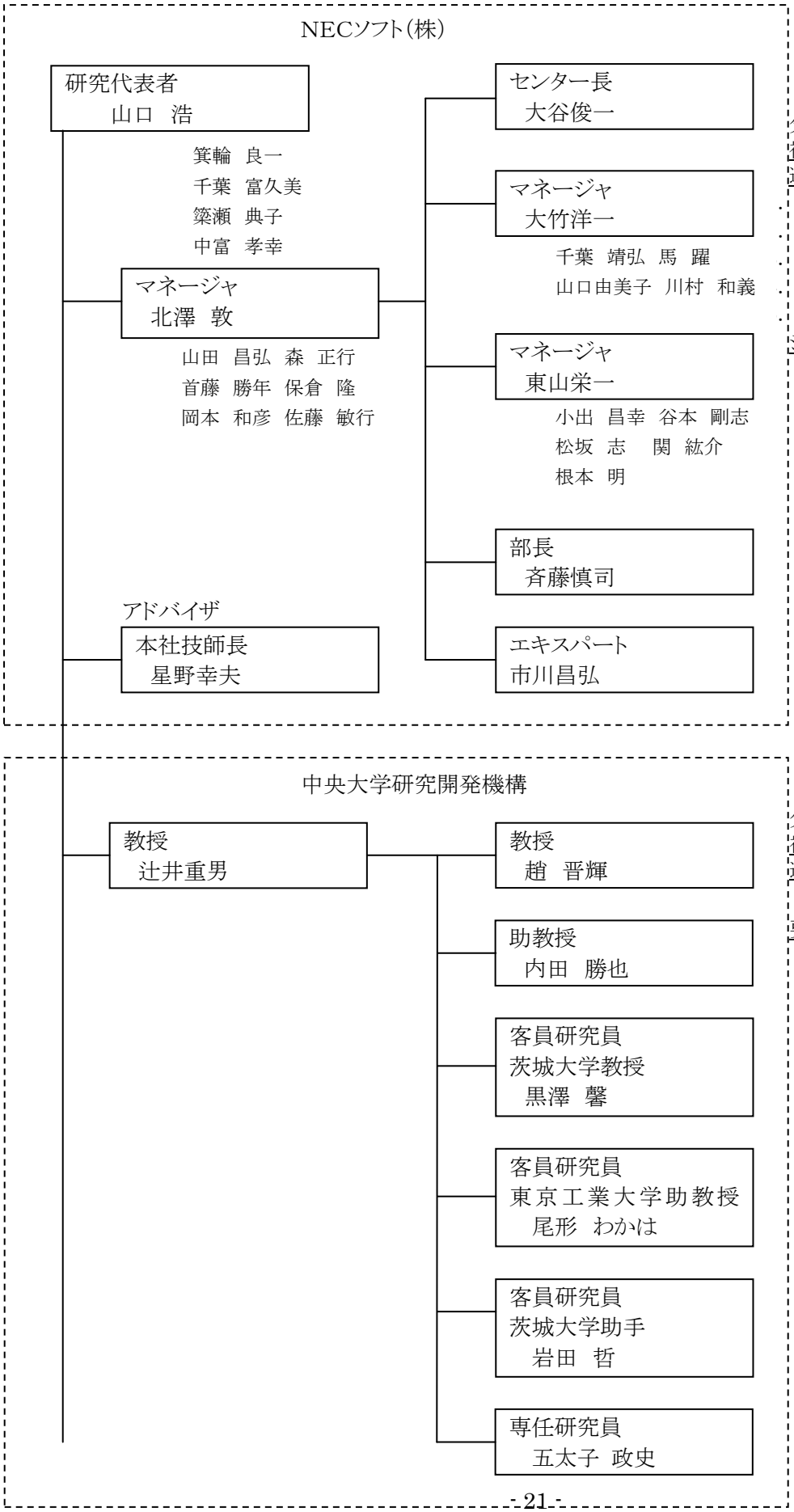
3-3　研究開発の年度別計画

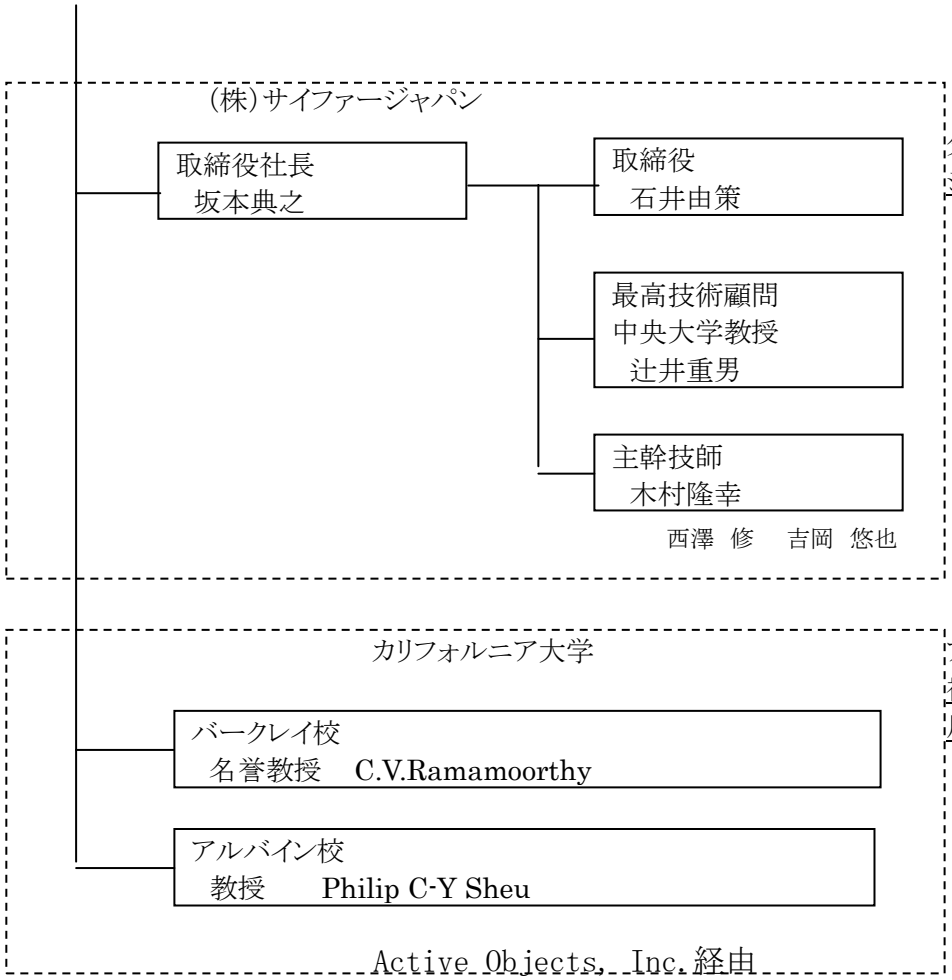
（金額は非公表）

研究開発項目	H14 年度	H15 年度	H16 年度	計	備　考
次世代電子投票・アンケート方式とその社会的利用に関する研究					
社会的利用形態の創造とシステムの運用管理 1. 利用分野と法・社会制度との整合性 2. 運用形態ごとの要件整理 3. 効率的運用とリスク分析 4. セキュリティポリシー（ISO17799etc.）					再委託先 （中央大学研究開発機構）
システム構成 5. モデル構築 6. システム構成 7. 実験（CCC21 協議会協力依頼）					再委託先 （サイファージャパン） （サイファージャパン）
要素技術 8. 準同型公開鍵暗号方式 9. 投票プロセスの正当性証明とその効率化					再委託先 （中央大学研究開発機構） （中央大学研究開発機構）
間接経費					
合　　計					

注）1　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の30％を上限として計上（消費税を含む。）。
　　2　備考欄に再委託先機関名を記載。

3-4　研究開発体制


NECソフト(株)
研究代表者
山口　浩
箕輪　良一
千葉　富久美
簗瀬　典子
中富　孝幸
マネージャ
北澤　敦
山田　昌弘　森　正行
首藤　勝年　保倉　隆
岡本　和彦　佐藤　敏行
センター長
大谷俊一
マネージャ
大竹洋一
千葉　靖弘　馬　躍
山口由美子　川村　和義
マネージャ
東山栄一
小出　昌幸　谷本　剛志
松坂　志　関　紘介
根本　明
部長
斉藤慎司
エキスパート
市川昌弘
アドバイザ
本社技師長
星野幸夫
分担:
社会的利用形態の創造とシステムの運用管理
1. 利用分野と法・社会制度との適合性
2. 運用形態ごとの要件整理
3. 効率的運用とリスク分析
システム構成
5. モデル構築
中央大学研究開発機構
教授
辻井重男
教授
趙　晋輝
助教授
内田　勝也
客員研究員
茨城大学教授
黒澤　馨
客員研究員
東京工業大学助教授
尾形　わかは
客員研究員
茨城大学助手
岩田　哲
専任研究員
五太子　政史
分担:
社会的利用形態の創造とシステムの運用管理
4. セキュリティポリシー
要素技術
8. 準同型公開鍵暗号
9. 投票プロセスの正当性証明とその効率化



分担:
<u>システム構成</u>
6. システム構成
7. 実験

アドバイザ:
<u>社会的利用形態の創造とシステムの運用管理</u>
1. 利用分野と法・社会制度との整合性
特に電子投票・アンケートシステムの社会的利用形態創造に関して

4　研究開発の概要（平成 15 年度まで）

4-1　研究開発実施計画

4-1-1 研究開発の計画内容

平成14年度および平成15年度の作業対象である以下のサブテーマ毎の計画を示す。

（ｉ）利用分野と法・社会的制度の適合性
（ii）運用形態ごとの要件整理
（iii）効率的運用とリスク分析
（iv）セキュリティポリシー
（ｖ）モデル構築
（vi）システム構成
（vii）実験
（viii）準同型公開鍵暗号方式
（ix）投票プロセスの正当性証明とその効率化

（ｉ） 利用分野と法・社会的制度の適合性

平成14年度

アンケートなど、投票に類似する利用分野について、行政、電子商取引、教育、医療等の領域におけるプライバシー保護のためのセキュリティの現状を調査する。

平成15年度

平成14年度提案中の、医療分野、教育分野での利用方法をさらに深更するとともに、新たな利用分野の検討を行う。また、「地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律」をベースとして次世代電子投票を実現するにあたり解決すべき、法・社会制度を抽出し、その解決に必要な機能要件を導き出す。

（ii） 運用形態ごとの要件整理

平成14年度

「次世代電子投票の満たすべき性質」が全て網羅された、「電子投票機能要件に関する標準」について、海外の動向調査を行い、それを参考にドラフトを作成する。

平成15年度

平成14年度作業中の米国 Federal Election Commission による Voting System Standards および、米国 Network Voting System Standard を参考とした海外動向調査を受けて、「次世代電子投票の満たすべき性質」が全て網羅された、「電子投票機能要件に関する標準」のドラフトを作成する。

（iii） 効率的運用とリスク分析

平成15年度

サブテーマ－ii で示される運用要件をもとに、性能上のボトルネックを解析する。

（iv） セキュリティポリシー

平成14年度

電子投票システムに対する ISO 15408 の視点からの調査を行う。

平成15年度

製造過程の観点（ISO15408）では、今年度調査中の、米国 IATF, HL7 用 Protection Profile を参考にして、電子投票システムに対する製造物のセキュリティ基本設計の核となる、セキュリティ設計ガイド（Protection Profile）のための指針を検討する。また、運用観点（ISO17799, ISMS）では、サブテーマ ii で示される運用要件を受けて、セキュリティポリシーガイドラインを構築する。

（ｖ） モデル構築

平成14年度

モデル構築のための基本設計を行う。

平成15年度

平成14年度作業中の基本設計を受けて、実際に電子投票実験を行うための参照実装を行い、参加企業内での実験を可能とする。

（vi） システム構成

平成14年度

TYKK 方式に基づくシステム構築の元となる準同型性暗号を実装する。

平成15年度

TYKK 方式に基づくシステム構築の元となる準同型性暗号を実装し、性能測定を行う。

（vii） 実験

平成15年度

参加企業による実験を行い、性能、運用性の確認を行う。また、中央コリドー高速通信実験協議会の協力による電子投票実験を準備する。

（viii） 準同型公開鍵暗号方式

平成14年度

次世代電子投票システムに利用すべき既知の暗号について、性能、安全性の理論的な特性を示す。

平成15年度

次世代電子投票システムに利用すべき新方式の暗号について、採用すべき暗号を決定する。

（ix） 投票プロセスの正当性証明とその効率化

平成14年度

既知の電子投票プロトコルに用いられる正当性の証明方式および監査履歴方式を、性能の観点から整理する。

平成15年度

TYKK方式(2センター方式)を前提とした場合の、正当性の証明方式および監査履歴方式を検討する。

なお，選挙用サーバにおける処理性能は、投票者数に比例するレベルを達成する。

また、レシートフリー方式の改良に関して検討する。

4-1-2 研究開発課題実施計画

平成14年度

（金額は非公表）

研究開発項目	第1四半期	第2四半期	第3四半期	第4四半期	計	備　考
次世代電子投票・アンケート方式とその社会的利用に関する研究						
社会的利用形態の創造とシステムの運用管理 1.　利用分野と法・社会制度との整合性 2.　運用形態ごとの要件整理 3.　セキュリティポリシー			→	→		再委託先 （中央大学研究開発機構）
システム構成 4.　モデル構築 5.　システム構成			→	→		再委託先 （サイファージャパン）
要素技術 6.　準同型公開鍵暗号方式 7.　投票プロセスの正当性証明とその効率化			→	→		再委託先 （中央大学研究開発機構） （中央大学研究開発機構）
間接経費						
合　　計						

注）1　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の30％を上限として計上（消費税を含む。）。
（合計の計は、「3－1の研究開発課題必要概算経費」の総額と一致）
2　備考欄に再委託先機関名を記載。

平成15年度

（金額は非公表）

研究開発項目	第1四半期	第2四半期	第3四半期	第4四半期	計	備　考
次世代電子投票・アンケート方式とその社会的利用に関する研究						
社会的利用形態の創造とシステムの運用管理 1. 利用分野と法・社会制度との整合性 2. 運用形態ごとの要件整理 3. 効率的運用とリスク分析 4. セキュリティポリシー	→	→	→	→		再委託先 （中央大学研究開発機構）
システム構成 5. モデル構築 6. システム構成 7. 実験	→	→	→	→		再委託先 （サイファージャパン） （サイファージャパン）
要素技術 8. 準同型公開鍵暗号方式 9. 投票プロセスの正当性証明とその効率化	→	→	→	→		再委託先 （中央大学研究開発機構） （中央大学研究開発機構）
間接経費						
合　　計						

注）1　経費は研究開発項目毎に消費税を含めた額で計上。また、間接経費は直接経費の30％を上限として計上（消費税を含む。）。
（合計の計は、「3－1の研究開発課題必要概算経費」の総額と一致）
2　備考欄に再委託先機関名を記載。

4-2　研究開発の実施内容

平成14年度および平成15年度の作業対象である以下のサブテーマ毎の実施内容を示す。
（ｉ）利用分野と法・社会的制度の適合性
（ii）運用形態ごとの要件整理
（iii）効率的運用とリスク分析
（iv）セキュリティポリシー
（ｖ）モデル構築
（vi）システム構成
（vii）実験
（viii）準同型公開鍵暗号方式
（ix）投票プロセスの正当性証明とその効率化

（i）　利用分野と法・社会的制度の適合性
平成14年度
- 第一段階および第二段階のわが国における電子投票に関する記事等を収集し、法的な問題点の洗い出しを実施。
- 実際に行われた電子投票を使用した地方選挙における特例法の適用と、その際の問題点分析を実施。
- 医療分野におけるシステムのセキュリティに関して、プライバシー保護の観点から必要要件の調査を実施。

平成15年度
- 電子投票に関しては以下の二点を中心に検討した
  ①　地方電子投票特例法に基づいた第一段階電子投票システムでの選挙実施実例を参考にした投票時の法的問題点の検討と、判例を中心とする過去投票の秘密侵害が問題となった事例の分析を実施し、憲法・公職選挙法に定められた投票の秘密原則の適用範囲を調査
  ②　諸外国（欧州を中心に）における公的電子投票の現状と電子投票に関する新たな法的取り組みの調査
  ③　第三段階の電子投票実現に向けて法制度変更の試案作成
- 医療分野、教育分野その他の分野での利用方法については以下の作業を実施した。
  ①　2003年5月に成立した個人情報保護法および医療関係ではHIPAA(米)、教育関係ではFERPA（米連邦法）に関して文献調査を実施
  ②　医療関係、教育関係および行政について、日本で想定される電子アンケート利用に関する調査を行い、関連諸法案・社会制度に関して整理を行った。

（ii）　運用形態ごとの要件整理
平成14年度
- NVSS（Network Voting System Standards）の理解およびNVSSをベースにした要件抽出作業を実施。
- NVSS 以外での有効な文献の追加調査の実施と日本における選挙制度・法律についての調査から、独自の要件抽出作業を実施。

平成15年度
- サブテーマ3の作業に先立ち、サブテーマ5で示される参照実装モデルで使用されているセキュリティ対策技術を含め、各運用要件の具体的な実装例の提示の充実を図った。
- サブテーマ3の検討結果をもとにフィードバックを行った。

（iii）効率的運用とリスク分析
平成15年度
- システムの性能において、特にボトルネックになると考えられる以下のポイントに関してサンプルケース（候

補者数4、投票者数2)で性能を測定し、投票者が多数の場合等の性能を予測し分析を開始した。

(1) センター1において、投票PCから送付された投票データの受付から、投票データの正当性を検証して登録するまでの性能

(2) センター1において、投票データを集計する性能

(3) センター1において、集計データの正当性を証明するデータを生成する性能

- また、サブテーマ5の参照実装モデルで使用されている具体的なセキュリティ対策技術を列挙し、それらの機能及びリスクに関する資料収集を行った。
- システムの票作成、投票、集計、開票の各プロトコル性能を最大構成(候補者数1000人、投票者数100万人)で割り出し、性能のボトルネックを分析した。
- サブテーマ5の参照実装モデルで使用されているセキュリティ対策技術の継続調査を行った。
- サブテーマ2で示される運用要件を元に、参照実装モデルでは実現されていない、あるいは他の実装手段が想定できる機能についてのセキュリティ対策技術を列挙し、調査を行った。

(ⅳ) セキュリティポリシー

平成14年度

- 電子投票システム用のISO15408 Protection Profileを一般化した「メタProtection Profile」、即ち、「投票の特性」・ISO15408のセキュリティ機能要件・システム構成の間のマッピングを定義し、ガイドラインを策定するアプローチを試行。
- モデルの正当性を検証するために、VSS(Voting System Standard)を分析。
- セキュリティ管理体制構築のため、センター1、2、及び個人利用場所で想定される運用ガイドラインの検討を実施。

平成15年度

- ISO15408では、ICカードに関するセキュリティ設計ガイド(PP)についての調査を実施し、実証実験等に利用するICカードへの対応を考察した。また、国内外で作成されているセキュリティ設計ガイド(PP)についていくつかの資料収集を実施している。
- ISO17799では、運営上の課題について、資料収集を行った。また、今年2月に行われた広島市長選挙などにおけるトラブルについて広島選管、総務省などにヒアリングを行い、今後の本プロジェクトでの実証実験で必要な情報を整理し、報告書を作成した。
- 米国国防総省が海外に居住する軍人や一般市民がインターネット経由で不在者投票を可能にするSERVE(the Secure Electronic Registration and Voting Experiment)の実験(最大10万人規模)への反対文書が発表されたため、本プロジェクト推進に対する参考(反面教師)にするため、その詳細の分析を行った。

(ⅴ) モデル構築

平成14年度

- 電子投票のモデルシステム構築に必要な製品の調査と、システム構成概要の検討を実施。
- システム構成要素を元に、必要な技術的項目の詳細について調査を実施。
- 既存製品と本電子投票の暗号化実装方法との連携について、投票者とセンター間の認証方式および投票データの暗号化方式を中心に検討を実施。
- ICカード内アプリケーションによる投票データ暗号化における技術的な方式等の検討を実施。
- PC上の投票用アプリケーション、ICカード内投票データ暗号化アプリケーション、各サーバのアプリケーション、電子認証局の設計を実施。

平成15年度

- 基本設計をもとに、実際に電子投票実験を行うためのシステムにおいて、以下のプログラムを実装。

(1) センター1

— 公開ボードプログラム

— 投票アプレット受信プログラム

— 暗号票受信プログラム
— 選挙実施プログラム
— 投票状況確認プログラム
— 暗号票集計プログラム
— 正当性検証データ生成プログラム

(2) センター2
— 準同型暗号鍵ペア生成プログラム
— 正当性検証パラメータ生成プログラム
— 投票アプレット定義プログラム
— 集計結果・正当性検証データダウンロードプログラム
— 正当性検証プログラム
— 集計結果開票プログラム

(3) 認証局
— 選挙人台帳登録プログラム

(4) 投票者PC
— 投票アプレット実行プログラム
— 投票データ暗号化プログラム

・ 実装した上記電子投票システムの正当性を確認するために、結合試験項目を約120項目列挙し、結合試験を実施。参加企業実験が可能な状態までシステムの品質を確保した。
・ 参加企業実験に向けて、電子投票システムのハウジング作業を実施した。
・ 参加企業実験用に、投票者向けのセットアッププログラムとユーザマニュアル、センター2管理者向けの運用マニュアル等を作成し配布した。
・ 2月に参加企業内で電子投票システムの実験を実施し、システムの運用性を確認した。
・ 参加企業実験後、投票者にアンケート調査し、システムの改善点の洗い出しを行った。自治体実験に向けて、現在システムの改修作業を実施中。

(vi) システム構成

平成14年度
・ 準同型性暗号方式に関して高次剰余暗号を投票者用サーバ用ともに実装。

平成15年度
・ ICカード用OU関数(暗号機能)の実装および性能評価を実施した。
・ サーバ用OU関数(鍵生成、復号、集計機能)の実装および性能評価を実施した。
・ 集計処理の正当性証明用関数の実装および性能評価を実施した。
・ 参加企業による実験および自治体による実験用のICカード発行に向けて準備を実施した。

(vii) 実験

平成15年度
・ 参加企業による小規模の実験を実施し、投票者操作性，システム運用性の確認を行った。
・ 中央コリドー高速通信実験協議会の協力の下、実験に関する説明書を作成し、下記2自治体に実験の説明を実施し、参加の意志を得た。(松本市，山梨市)
・ また、自治体殿からのヒアリングにより、実験企画の検討を進めた。

(viii) 準同型公開鍵暗号方式

平成14年度
・ 高次剰余暗号、NS暗号、OU関数、Paillier 暗号、CGS97 等で利用される離散対数を利用する方式について、暗号化コスト、鍵サイズ、データ量、復号速度、安全性証明に要するコストの分析を実施。

平成15年度
・ 準同型暗号方式(高次剰余暗号、OU関数、NS暗号、Paillier暗号、離散対数型暗号(CGS97等))の性

能に関する理論値を明らかにし、本プロジェクトで求められる投票に対する要件を条件とした理論値の比較を行った。この結果、複数候補に対する投票に適しており、暗号化時の演算コスト(法のサイズ)が小さいOU関数を準同型暗号として採用することに決定した。OU関数をTYKK方式に組み合わせることにより、本プロジェクトで求められる要件を満たす投票方式を実現できる。

- 複数候補に対する投票に適した準同型暗号(OU関数)について，要件定義に従い，投票者数，候補者数，選択肢タイプに応じて最も適切なパラメータを得るための方式に関する研究を行った。

（ix）投票プロセスの正当性証明とその効率化

平成14年度

- 二重暗号化された状態での集計処理の正当性証明の改良と、その証明及び監査履歴に要するデータ量について分析。
- 現状のコンピュータ性能を考慮して、実用に耐えうるように、証明の効率化の検討を推進。
- 従来の選挙方式(CGS97等)では安全性の根拠として離散対数問題の困難性を利用する場合が多いが、別の問題の困難性に根拠を置く方針の検討も推進。

平成15年度

- TYKK方式(2センター方式)における投票プロセスの正当性証明について検討を重ね、電子情報通信学会英文論文誌上で成果を発表した。上記方式は、選挙用サーバにおける処理性能は、投票者数に比例するレベルを達成している。
- TYKK方式(2センター方式)における監査履歴サイズと監査に必要な計算量について評価検討を進める。投票者のコスト削減を最優先し、監査履歴を作成するサーバ、監査するサーバのコストを削減する方法について調査検討した。
- また、監査履歴サイズと監査に必要な計算量について評価検討を進めるとともに、TYKK方式をレシートフリー方式へ改良する方式についても検討を進め、Hirt-Sako方式に準じた改良方式の実現を目指した。

5　研究開発実施状況（平成１５年度）

5-1 利用分野と法･社会制度との整合性

5-1-1 はじめに

2001 年 12 月に「電子式投票機を用いて行う投票方法等の特例に関する法律(電子投票法)」が制定されて後、2003 年度は、地方選挙における電子投票の取り組みが進み、表に示すような電子投票が行われてきた。2003 年 12 月には公職選挙法が改正され、期日前投票が電子投票可能となった。これら電子投票の実施とともに、可児市や海老名市における電子投票機の故障から、島根県松江市など電子投票の導入を断念する自治体がある一方、2004 年 2 月には超党派の国会議員連盟「電子式投開票システム研究会」が今夏の参院選で電子投票を試験的に導入できるよう公選法改正などの検討を行ったり（今回は見送り）、3/15～3/19 にかけて電子投票を使用した模擬投票を行ったりという動きをみせており、選挙の電子投票化への流れは確実なものとなっていると考えられる。

また、類似機能としてアンケートなどを想定した場合、匿名化という点で個人情報保護が重要になるが、2003年5月に個人情報保護法が制定され、2005年4月の完全施行に向けて、特定の個別分野に関しては指針がだされたり、個別法の制定が検討されたり等、官・民の対応が急がれている。

本節では、法・社会制度との整合性として、既に実施されている第一段階の電子投票に関して特例法実施例とその他現行法に対する評価を行い、諸外国の電子投票に対する取組みを調査し、第三段階の電子投票導入に向けての法改定の試案を提示する。また、類する利用分野として、医療・教育・行政に関して調査した結果をまとめる。

表 3　第一段階の電子投票により実施された地方自治体の選挙

・岡山・新見市長選・市議選（2002 年 6 月）
・広島市長選の一部　安芸区（2003 年 2 月）
・宮城　白石市議選（2003 年 4 月）
・福井　鯖江市議選（2003 年 7 月）
・岐阜　可児市議選（2003 年 7 月）
・福島　大玉村議選（2003 年 8 月）
・神奈川・海老名市長選・市議選(2003 年 11 月)
・青森県六戸町　　町長選(期日前投票も含む)(2004 年 1 月)
・京都市　京都市長選の一部　東山区で導入(期日前投票も含む) (2004 年 2 月)

なお、第一段階の電子投票とは、選挙人が指定された投票所において電子投票機を用いて投票する段階であり、総務省の「電子機器利用による選挙システム研究会」の報告書においてまとめられた電子投票の 3 段階のうちの一つである。第二段階は、指定された投票所以外の投票所においても投票できる段階であり、第三段階が投票所での投票を義務づけず、個人の所有するコンピュータ端末を用いて投票する段階をさす。

本研究では第三段階の電子投票を「次世代投票」と呼び、これをターゲットとして研究を行っている。

5-1-2 次世代電子投票の実現にむけての法･社会制度に関する研究

本項では、特例法実施例とその他現行法に対する評価として、国会論議の追跡と、過去の判例に関して憲法･公選法で保護されるべき投票の秘密の範囲、諸外国における電子投票の取組みを調査し、第三段階の電子投票の取組みとして、法制度改定の試案をまとめる。

5-1-2-1　特例法改正･電子投票法制定に関する国会論議の追跡

平成 14 年に施行された「地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律」（以下特例法と呼称）に基づき、電磁的記録式投票機を用いた6回の地方議会議員選挙と、5回の地方公共団体首長選挙が実施された。しかし、特例法は点字投票、不在者投票、郵便投票及び仮投票は対象としないものとして、電子投票の対象から除外されていたため、平成15年までに実施された電子投票では、点字、不在者、郵便、仮投票について、従来行われてきた通りの自書式の投票によって行われた。そのために開票にかかる時間的･人的コストを、電子投票方式を全く用いない従来の選挙と同等に要することとなり、選挙管理者[1]や総務省からは、むしろ不在者投票にこそ電子投票が必要ではないかとの指摘がなされた。昨年度の本研究においても、

> 電子投票においては、まず第一段階において、不在者投票所に電磁的記録式投票機を設置することができないかどうか検討する必要がある。特例法では全く考慮されていないが、可能となれば集計の際に自書式の不在者投票の開票と電磁的記録開票の二系統の開票が行われる必要が無くなり、指摘されている開票の速度の低下を防ぐことができる。しかしながら、不在者投票の場合、個々の不在者投票日から投票所での投票日との間に差があるため、その間に不在者投票者が選挙人資格を喪失する場合がある。不在者投票者の死亡や、選挙違反での有罪判決の言渡、国籍離脱や他の自治体への転出などが考えられる。その際には入力された投票結果から当該不在者投票者の投票データだけを選択して消去する技術的仕組か、不在者投票日の時点で投票の効力が確定したとする不在者投票の開票に関する考え方の制度的な転換のいずれかが要求される。
>
> 第二･第三段階においては、不在者投票を必要とする選挙人の数が激減することが考えられる。
> まず第二段階においては、業務等の事情があって選挙区を不在にしたとしても、選挙人名簿と投票機ネットワークシステムの結合がなされていれば、現に移動した先の投票所で投票が可能となるからである。但し、投票所開設時間内に投票所に出頭することのできない選挙人には依然として不在者投票制度が必用とされよう。（第三段階においては、選挙人の本人認証･本人の投票意思の確保･ネットワークセキュリティ･受信サーバの安定性などが確保されれば、不在者･洋上･在外各投票が発展的に解消されることはいうまでもない。）

と指摘したとおりである。

国会においても、特例法に基づく電子投票での不在者投票の取扱いについては論議の対象となり、総務省を中心に不在者投票制度の見直しが図られた。最終的に内閣提出法案として第156回国

[1] 岡山県地方自治研究会報告書,「電子投票システムの効果と課題　～電子投票導入に向けての考察～」(2002),p10 以下参照

会において「期日前投票制度の創設等を内容とする公職選挙法の一部を改正する法律」が成立し、平成15年6月11日に公布、平成15年12月1日から施行される運びとなった。この期日前投票制度において電子投票を利用可能とするために、同国会では特例法の改正も併せて議論され、改正特例法が同日に公布・施行された。

本項では、この期日前投票制度及び改正特例法の審議過程を追跡し、国会における電子投票に関する議論と国会議員の電子投票理解について整理を行う[2]。

2 不在者投票以外でも、第三段階電子投票におけるネットワーク化への対応など、本研究から見て興味深い議論も見られるが、今回は不在者投票関連の質疑のみに限定して、その要旨を箇条書きに要約する形で収集整理を行った。他の国会での争点（ALS 患者などへ向けた電子投票法バリアフリー条項や、郵便投票の拡張など）は、来年度の課題としたい。

表 4　国会における電子投票に関する議論と国会議員の電子投票理解状況

	日時	内容	
1	第 153 回国会　衆議院・政治倫理の確立及び公職選挙法改正に関する特別委員会第 2 号（平成 13 年 11 月 19 日（月曜日））	片山虎之助総務大臣より特例法案の提案理由および主旨説明	・本法案では、電磁的記録式投票機を用いた市町村の議会の議員または長の選挙の投票には、不在者投票等を除き、市町村は条例で定めるところにより、選挙人自ら投票所において電磁的記録式投票機を用いて投票を行う方法によることができることとした。
2	第 153 回国会　衆議院・政治倫理の確立及び公職選挙法改正に関する特別委員会第 3 号（平成 13 年 11 月 21 日（水曜日））	大幡基夫議員（共産党）より大竹邦実参考人（総務省自治行政局選挙部長）への質問	・自書式投票のみの場合、最終的に不在者投票も投票当日投票所での投票函に投函されたが、特例法案に基づく電子投票が実施されると、不在者投票は投票所の投票とは独立して集計が行われ、不在者投票者の人数によっては、第三者が事実上投票内容を知りうる場合もあろう。この点どう考えるか。
		大竹参考人の答弁	・点字・在外・洋上投票といった少数の投票について、従来から各選管に対してその投票の秘密の保持に十分留意するよう助言を行っている。今回の新制度ができた場合、不在者投票などについても同様の助言をしてまいりたい。 ・現行法上も、二重封筒の内封筒のみの混同で不在者投票者の特定ができないようになっている。 ・指定投票区制度を用いて、複数の投票区の不在者投票の一括開票ができる。投票の秘密保持にも資するのではないか。
		本法案（特例法案）に関する議決	・修正案（指定都市の区の扱いおよび投票機表示事項は候補者名・党派とすること）および特例法案のその他の部分について、総員起立で可決。本会議での報告は委員長に一任。
3	第 153 回国会　衆議院本会議(平成 13 年 11 月 22 日(木曜日))	・政治倫理の確立及び公職選挙法改正に関する特別委員長の報告の後、全会一致で委員長報告のとおり修正議決した。	
4	第 153 回国会　参議院・政治倫理の確立及び選挙制度に関する特別委員会第 2 号（平成 13 年 11 月 26 日（月曜日））	片山総務大臣より特例法案の提案理由および主旨説明	（上記（１）と同旨につき省略）
		中馬弘毅衆議院政治倫理・公職選挙法改正特別委員長より法案修正の説明	（上記（２）議決と同旨につき省略）
5	第 153 回国会　参議院・政治倫理の確立及び選挙制度に関する特別委員会第３号（平成 13 年 11 月 28 日（水曜日））	本法案（特例法案）に関する議決	特例法案について、総員起立で可決。
6	第 153 回国会　衆議院本会議(平成 13 年 11 月 30 日(金曜日))	・政治倫理の確立及び選挙制度に関する特別委員長の報告の後、全会一致で委員長報告のとおり可決した。(特例法成立)	
7	第 154 回国会　衆議院総務委員会　第 25 号（平成 14 年 6 月 27 日（木曜日））	松崎公昭議員（民主党）より片山虎之助総務大臣への質問	・新見市電子投票実行後の全体的な感想と今後の課題について大臣の意見を聞きたい。
		片山大臣の答弁	・電子投票の集計は約二十五分で、不在者投票が二時間かかった。 ・現地関係者の要望としては、不在者投票も電子投票にしてほしいとのこと。 ・不在者投票は、法律を直せば、若干の工夫をすれば可能になるのではなかろうか。

	日時	内容	
8	第 154 回国会　参議院・政治倫理の確立及び選挙制度に関する特別委員会 第９号（平成 14 年 7 月 22 日（月曜日））	広野ただし議員（民主党）より 片山総務大臣への質問	・新見市の電子投票について、総合的な評価を聞きたい。
		片山大臣の答弁	・若干問題は生じたが、全体としては順調に終わり、初めてとしては大変良かった。 ・新見市関係者によると、不在者投票数は千何百票の開票に二時間掛かり、電子投票数一万六〜七千の開票が実質十二分で終わっている。従って、不在者投票も是非電子投票でやらせてほしいということだ。 ・告示日当日に不在者投票を行おうとする者について、当日午後５時まで候補者が確定しないため、候補者の表示による情報提供が不十分になるという問題がある。 ・不在者投票を行った者が、選挙期日までに死亡した場合に、電子投票システムでその不在者投票を有効票から外すことができるかどうかの検討が必要だ。 ・いずれにせよ、不在者投票にも電子投票を導入するためには、技術上・法律上の検討を進める必要がある。
9	第 156 回国会　電子投票制導入に関する質問主意書 衆議院・質問第 12 号　（平成 15 年 1 月 31 日提出）	石井一議員（民主党）より 内閣への質問趣意書	・特例法の趣旨（第一条）「開票事務等の効率化及び迅速化」を実現するためには、同法第三条及び公職選挙法等の不在者投票に関する規定を早急に改正しなければならないと考えるが、改正するのかしないのか、政府の見解を示されたい。改正するのなら、その提案時期を提示されたい。改正しないのなら、その理由を回答されたい。
		小泉内閣総理大臣の答弁書	・地方公共団体の議会の議員及び長の選挙（以下「地方公共団体の選挙」という。）において、不在者投票を電磁的記録式投票機を用いて行う投票（以下「電磁的記録式投票」という。）の対象とすることについては、不在者投票制度の見直しと併せて検討を進めているところである。
10	第 156 回国会　衆議院・政治倫理の確立及び公職選挙法改正に関する特別委員会 第 2 号（平成 15 年 5 月 16 日（金曜日））	片山総務大臣より 公職選挙法の一部を改正する法律案の提案理由および主旨説明	・本改正法案では、選挙の当日に投票することが困難であると見込まれる選挙人について、当該選挙の期日の公示または告示があった日の翌日から選挙の期日の前日までの間、期日前投票所において、投票を行わせることができることとした。 ・また、地方公共団体の議会の議員及び長の選挙について、期日前投票所における投票を電磁的記録式投票機を用いて行うことができるようにするなど、所要の規定の整備を行うこととした。
11	第 156 回国会　衆議院・政治倫理の確立及び公職選挙法改正に関する特別委員会 第 3 号（平成 15 年 5 月 21 日（水曜日））	竹本直一議員（自民党）より 片山総務大臣への質問	・本法案は選挙人の投票環境を整えるため、不在者投票及び在外投票についてその投票方法の見直しを行うものと聞いている。改正法の主な内容について御説明をお願いしたい。
		片山総務大臣の答弁	（上記（10）と同旨につき省略）
		竹本議員より 若松謙維総務副大臣への質問	・今回の改正は不在者投票を見直して期日前投票を創設するということだと思うが、こういう改正を行う理由は何か。この改正をによってどんなメリットがあるのか。逆に、今までの制度のどの点に不都合があったのか。

	日時	内容	
		若松副大臣の答弁	・現行不在者投票制度は、当日投票主義の例外として投票日以外に投票の記載を行うことを認める制度である。選挙権の認定時期は選挙当日となり、投票の受理不受理は選挙期日に行う。このため投票の記載を行った投票用紙は内封筒及び外封筒に入れて封をして、外封筒に選挙人が署名をするという取扱をしている。 ・しかし、選挙人としては投票所同様、不在者投票日に投票を行っているとの認識が一般的であり、かつ不在者投票数も増加している。このような状況から三つ具体的な改善点を示したい。一点目は、不在者投票を直接投票箱に入れることができないこと。二点目として、不在者投票を内封筒及び外封筒に入れなければならず、手続が複雑であること、三点目が、外封筒に署名しなければならないことである。 ・今回の不在者投票制度の見直し、即ち期日前投票制度の創設は、このような意見等を踏まえて、選挙権の認定時期を期日前投票を行う日とし、従来の不在者投票の手続を簡素化して選挙期日前に投票を行わなければならない選挙人の投票環境の改善を図ろうとするものである。 ・導入のメリットは二点ある。一点目は選挙人にとり、選挙期日前の投票であっても選挙期日の投票と同様に直接投票箱に投票を入れることができ、投票を内封筒及び外封筒に入れて外封筒に署名するといった複雑な手続が必要なくなるという、投票の簡素化である。 ・二点目は、選挙管理機関にとり、不在者投票の受理不受理の決定・不在者投票用外封筒及び内封筒の開封などの事務作業がなくなるといった、選挙の事務負担の大幅緩和である。
		竹本議員より 高部正男参考人 （総務省自治行政局選挙部長）への質問	・期日前投票はすべての不在者投票について導入されるのではなく、名簿登録地選管における不在者投票のみ可能と聞いている。投票用紙を封筒に入れる必要のない期日前投票は大いに活用されてよいと思うが、なぜ名簿登録地選管での投票に限定されたのか、理由を聞きたい。 ・また、名簿登録地選管における不在者投票は不在者投票全体の中でどの程度の割合を占めているのかについても聞きたい。

	日時	内容	
		高部参考人の答弁	・現在の不在者投票制度は、名簿登録地の市町村で行うもののほかに、指定病院等の施設で行うもの、船員が船舶において行うもの、名簿登録地以外の市町村選管で行うもの、郵便投票、洋上投票が存在する。今回の期日前投票の対象は、名簿登録地市町村で行う不在者投票のみを対象としているが、理由は二つある。 ・一つは、名簿登録地以外の場所における不在者投票については、投票地に選挙人名簿が無いので、投票時に選挙権の有無を確認することができない。従って、投票時点において選挙権認定を行う期日前投票を採用することはできないからである。 ・二点目は、郵便投票や洋上投票については、個々の投票を（郵便やファックスを用いて）送致する仕組になっており、直接、投票箱に投函する仕組はとれないからである。また、指定施設等の不在者投票についても、その施設等において不在者投票を行う方は、施設の所在市町村の選挙人名簿に登録された選挙人に限られないため、個々の投票をそれぞれの名簿登録市町村選管へ送致することが必要となり、直接投票箱に投函する仕組をとることが困難となるからである。 ・名簿登録市町村における不在者投票の不在者投票全体の割合がどのぐらいかという点については、直近の衆議院選挙である平成十二年の衆議院総選挙においては八六・三%、平成十三年の参議院通常選挙においては八九・六%が名簿登録市町村での不在者投票になっている。不在者投票の約九割が名簿登録市町村での不在者投票という状況である。
		阿久津幸彦議員（民主党）より高部参考人への質問	・現行法で可能な、選挙期日の公示または告示の日当日の不在者投票が、本法改正により、翌日からしか期日前投票ができないことなる。それは従来可能だった貴重な投票機会が一日分奪われてしまうということである。当日投票を不可とする結論に至るまでにどんな議論があったのか聞きたい。 ・公示または告示の日当日だけでも、現行法のシステムによる不在者投票を残すことは可能か。残せないとすればその理由は何か
		高部参考人の答弁	・今回の期日前投票制度は、投票箱に投函する時点でもう投票行為が完結し、確定投票になるため、投票管理を厳格にする必要がある。 ・これまでは選管が立候補の受付と並行して不在者投票をすることになっており、選挙人の投票時点で候補者の氏名掲示等ができず、選挙人に対して十分な情報提供をすることができない。 ・電子投票の場合、電磁的記録式投票機の画面構成は候補者が出そろわないとできないため、公示・告示日には間に合わない。 ・以上のような理由から法案では期日前投票は公示・告示の翌日からとした。 ・今回の法改正で、現行法の二重封筒式の不在者投票制度が完全に消滅するわけではないので、議員の言うような公示・告示当日の不在者投票に現行法上の方式を用いることは理論的・政策的には可能である。しかし、翌日以降の期日前投票と異なり、確定投票にはならないことや、制度全体の整合性を考えると、徒に制度を複雑にするだけになると思われる

	日時	内容	
		阿久津議員に対して 片山総務大臣からの答弁	・投票期間が一日短くなるということが、大きな不利益を与えることは我々も承知している。公示・告示当日の不在者投票の問題は、総合的に様々な観点から、制度として成り立つかどうか十分検討させていただきたい。
		本法案に関する議決	・公職選挙法の一部を改正する法律案について、総員起立で可決。
		本法案に関する付帯決議	・自由民主党、民主党・無所属クラブ、公明党、自由党、日本共産党、社会民主党・市民連合及び保守新党の七派共同提案による附帯決議を付すべしとの動議が提出。
		・堀込征雄議員（民主党）より、趣旨説明（決議案文朗読）	公職選挙法の一部を改正する法律案に対する附帯決議（案） 本法の施行に当たり、政府は、次の事項について善処すべきである。 一　期日前投票及び不在者投票は、選挙の公示又は告示のあった日の翌日から選挙の期日の前日までの間とされたことに伴い、選挙人が投票機会を失することのないよう、その周知徹底を図ること。 二　期日前投票及び不在者投票の適正な管理執行に万全を期すること。特に指定病院等における不在者投票について、適正な管理執行に更に努めること。
		・本付帯決議について、総員起立で可決	
12	第 156 回国会　衆議院本会議（平成 15 年 5 月 22 日（木曜日））	・政治倫理の確立及び公職選挙法改正に関する特別委員長の報告の後、全会一致で委員長報告のとおり議決した。	
13	第 156 回国会　参議院・政治倫理の確立及び選挙制度に関する特別委員会第 2 号（平成 15 年 5 月 28 日（水曜日））	片山総務大臣より公職選挙法の一部を改正する法律案の提案理由および主旨説明	（上記(10)と同旨につき省略）
14	（14）第 156 回国会　参議院・政治倫理の確立及び選挙制度に関する特別委員会第３号（平成 15 年 5 月 30 日（金曜日））	福山哲郎議員（民主党）より 若松総務副大臣への質問	・期日前投票になると告示当日の不在者投票ができなくなることについては、当該選挙区が無投票当選を出す場合などもあり、正当性がある。 ・一方で、従前の制度を前提に告示当日に不在者投票に現れ、シャットアウトされる選挙人が生じないような対策を総務省は考えているのか。
		若松副大臣の答弁	・改正法成立の暁には、総務省を挙げて新制度の周知徹底に当たりたい。
		又市征治議員（社民党）より 高部参考人への質問	・期日前投票制度になると、確定票の入った投票箱が長時間保管されることとなり、首長など幹部から投票箱の管理者、職員に非常な圧力が掛かる可能性が生まれてくる。過去の事例に照らしてみると、投票箱のすり替えなどもおこりうる。投票箱の管理をどのように厳正に行っていくつもりか。
		高部参考人の答弁	・投票箱については複数の鍵による施錠や、投票管理者による日締の封印、立会人による封印など、チェック体制を整える。保管場所についても施錠ができるような場所を考える。従前の不在者投票では、選挙期日に不在者投票の投票箱への投函を忘れるなどの事件も起こっているが、そのようなミスが亡くなるというメリットもある。
		本法案に関する議決	・公職選挙法の一部を改正する法律案について、総員起立で可決。

	日時	内容	
		本法案に関する付帯決議	・自由民主党・保守新党、民主党・新緑風会、公明党、日本共産党、国会改革連絡会（自由党・無所属の会）及び社会民主党・護憲連合の各派共同提案による附帯決議を付すべしとの動議が提出。
		・福山議員より、趣旨説明 (決議案文朗読)	公職選挙法の一部を改正する法律案に対する附帯決議(案) 政府は、国民本位・政党本位の選挙制度を確立するため、本法の施行に当たり、次の事項についてその実現に努めるべきである。 一、期日前投票及び不在者投票の投票期間が、選挙の公示又は告示のあった日の翌日から選挙の期日の前日までの間とされたことに伴い、選挙人が投票機会を失することのないよう、その周知徹底を図ること。 二、期日前投票及び不在者投票について、本法の立法趣旨等を踏まえ、適正な管理執行に万全を期するとともに、特に指定病院等における不在者投票について、選挙の公正確保に配意しつつ、適正な管理執行の徹底に努めること。 三、在外投票制度の実施状況を踏まえ、できる限り速やかに衆議院小選挙区選出議員選挙及び参議院選挙区選出議員選挙を在外投票の対象とするための措置を講ずるものとすること。 四、候補者情報の充実、政治参加の促進、有権者と候補者の直接対話の実現、金のかからない選挙の実現等を図る観点から、ＩＴ時代の要請に即応し、インターネットを利用した選挙運動の早期導入に向け、積極的な検討を一層進めること。 五、民主主義の質的充実と活性化を促し、有権者の政治的関心を高める観点から、政党のマニフェスト等の導入の環境整備を検討すること。 右決議する。
		・本付帯決議について、総員起立で可決	
15	第 156 回国会　参議院本会議（平成 15 年 6 月 4 日（水曜日)）	・政治倫理の確立及び選挙制度に関する特別委員長の報告の後、全会一致で委員長報告のとおり可決した。(改正公職選挙法成立)	

5-1-2-2　憲法・公選法で保護されるべき投票の秘密の範囲

(i) 投票箱等の管理ミスで無効となった投票の取扱い

選挙管理者による、投票の管理執行に関る規定違反が原因で、有効票として計算されるべき投票が開票手続にかけられることなく無効票とされたまま当選者が決定された場合、当該投票をいかに取り扱うかという問題に関しては、判例の立場は概ね一貫していると言ってよい。

公職選挙法209条の2(潜在的無効投票)があった場合に、候補者の得票数に応じて按分比例した数を得票数から差し引く規定)を潜在的有効投票に準用し、按分して候補者の得票に加算することを主張する上告人に対し、上告人の主張を退け、潜在的有効投票を無効とした最二小判昭 32・5・31、本件原審が引用しているリーディングケースとして、不在者投票 31 票が投票所の閉鎖時刻までに投票管理者に送致されなかったために無効票となった際に、これをどの候補者の得票か帰属不明な潜在的有効投票と捉え、その総数が最下位の当選者と最高位の落選者との得票差を超えるかどうかを基準として公職選挙法 205 条 1 項に定める「選挙の結果に異動を及ぼす虞れ」の有無を判断した最一小判昭 46・4・15 が挙げられる。

(ii) 伊仙町事件

平成12年8月 27 日、鹿児島県伊仙町で町議会議員選挙が行われ、上告人らを含む 20 人が当選し、4人が落選した(最下位当選人と最高位落選人との得票差は20票)。ところが、選挙結果発表直後に、不在者投票合計 184 票中男子分 87 票は集計されたが女子分 97 票は投票箱に入れられないまま捨てられていたことが判明した。訴外落選人4人は、町選挙管理委員会に対して選挙の効力につき異議の申出をしたが、町選管はこれを棄却する旨決定した。これに不服の同異議申出人らは、次いで県選管に対して審査の申立てをしたところ、県選管は本件選挙を無効とする裁決を行った。

町議会は、臨時議会を招集して本件 97 票の点検を求める旨の議案を可決し、町選管は、これを受けて本件 97 票につき内封筒を開いて、その結果が部外者に知られるような状態で投票用紙の記載内容を点検した。この点検結果によれば、本件97票が適式に投票の集計に加わっていたとしても選挙結果に影響を及ぼすものではなかった。本件訴訟は、上告人(原告)らが、同点検結果を受けて県選管の選挙無効裁決の取消しを求めたものである。

原審(第1審)[3]は、原告らの請求を棄却した。上告審[4]は公職選挙法施行令 63 条 3 項に違反して投票箱に入れられなかったために無効票と確定された不在者投票の内容を、公職選挙法に定められた開票手続によらず取り調べて同法 205 条 1 項に定める選挙の結果に異動を及ぼす虞れの有無を判断することは許されないと述べ、やはり上告人(原告)らの請求を棄却した。

(iii)「異動を及ぼす虞れ」

本件原審・上告審ともに、結論として上記リーディングケースと全く同一の方法で「選挙の結果に異動を及ぼす虞れ」の有無を判断しているが、上告人は当該不在者投票につき、どの候補者に対する投票であるかの帰属を確定できる場合であるとして伊仙町選管に投票内容を点検させたうえで、その結果に基づいて「選挙の結果に異動を及ぼす虞れ」を判断すべきであると主張しており、このような方法が許されるかどうかについて初の最高裁の判断となった。

但し、下級審においては、本件と別の判断を下した裁判例(東京高判昭 53・8・15)がある。この東京高裁判決は、本件判決と全く逆の立場を取る。事実関係は、昭和 52 年 5 月 8 日に施行された鎌倉市議会議員一般選挙において、投票総数 76,175 票と開票された投票数 75,252 票との間に 923 票の差が発生した。そ

---

[3] 平成 13 年(行ケ)第 1 号、福岡高裁宮崎支部平 13・4・11 判決

[4] 選挙の効力に対する裁決取消請求、独立当事者参加申出事件、平成 13 年(行ヒ)第 205 号, 最高裁平成 13・12・18 第三小法廷判決,上告棄却(判時 1779 号 6 頁)

こで、本件選挙会は所在不明分 923 票を持ち帰り票（選挙人が投票用紙を投票箱に入れずに投票所外へ持ち帰った票）として処理し、30 名の当選人を決定した。

原告は、最下位の当選人と 1 票差をもって落選、鎌倉市選挙管理委員会に対して当該選挙の無効を主張して市選管に異議申出を行った。市選管はこの申出を審理するために投票の再調査を実施したところ、持ち帰り票として処理された 923 票は開票管理者の不注意で紛失したものであり、再調査時に偶然発見されたと発表した。そしてこの 923 票を全て有効票と認定して集計し直し、元の開票分 76,175 票の投票結果と合わせても当該選挙の結果に異動がない旨判定し、原告の異議申出を棄却した。続いて原告は神奈川県選管（被告）に対して市選管の異議申出棄却を不服として審査申立を行ったが、これも棄却された。
原告は、被告に対し、923 票は帰属不明の無効票であり、当該選挙の効力に関する審査申立棄却の裁決を取消し、選挙無効とする判決を求めたものである。

東京高裁は、当事者間に923票の紛失に関する事実関係の争いは無く、選挙の管理執行手続きに関する公職選挙法の規定に違反するとしたものの、923 票について用紙のすり替えや改竄、抹消など不正行為が行われていないという事実を認定し、現に点検、調査が可能な状況にあったとして、923 票の開票結果を各候補者の有効得票に加算して「選挙の結果に異動を及ぼす虞れ」を判断し、原告の訴えを退けたものである。

（iv）選挙の公正と公選法上の厳格な手続

本件最高裁判決においては、まず伊仙町選管の行った本件不在者投票 97 票の点検に関して上告人らが提出した証拠を、「無効票と確定された投票内容を選挙終了後に調査し、その投票内容いかんにより選挙の結果を左右するような手続は公職選挙法の予定していないところである…」として採用しなかった。また、公職選挙法の開票手続に関する規定を列挙した上で、「…個々の投票の効力判定や得票数の確定に関する判断に対する不服については、当選の効力に関する争訟（206 条ないし 209 条）により、開票手続や当選人決定手続の選挙無効原因については、選挙の効力に関する争訟（202 条ないし 205 条）により、それぞれ審理するものとされている。 以上の規定に照らせば、法は、開票手続、当選人決定手続及びその不服申立て手続について厳格な定めを設け、所定の手続により、選挙人が表明した意思が確定されることとして、選挙の公正を期しているものというべきである。」と述べ、公職選挙法の手続規定を参照することで、この厳格な手続から逸脱した無効票の点検をもって「選挙の結果に異動を及ぼす虞れ」を判断することは、選挙の公正を損ない許されないという立場を示そうとしている。

東京高裁判決はこの点、単に開票されなかった 923 票に対し、発見・点検・調査までの間に不正な働きかけが行われていなかった事実のみを重視し、また、この 923 票の点検・調査は開票手続そのものではないために、公職選挙法上の開票手続を逸脱しているからといってその効力を論ずる必用はないと判示している。この立場は、一旦投票結果によって表明された選挙人の意思を尊重するが故に「選挙の結果に異動を及ぼす虞れ」を非常に狭く解しているように見える。しかしこの 923 票の選挙人の投票意思だけが、運用の事実面はともかく、法的に根拠が存在しない方法で集計されるという結果の意味を軽視するものといわざるを得ない。地方議会とはいえ、立法従事者を選出する重大な手続である選挙において、選挙管理委員会の過失が原因で、形式的に異なった扱いを受けなければならない選挙人の投票が与えられた意味を考える必要がある。

その点、本件判決は、「…選挙の効力に関する争訟を審理する選挙管理委員会または裁判所が、無効票と確定された個々の投票の内容を取り調べて、いずれの候補者に対する投票であるかを明らかにし、それを選挙人が表明した意思であるとして候補者別の得票数に加算した上、その結果に基づいて法 205 条1項に定める選挙の結果に異動を及ぼすおそれの有無を判断することは、実質的には法の定める手続によらずに

投票を開票して候補者別の得票数を確定し直すに等しいといわざるを得ない。…」と述べ、無効票とされてしまった票と有効票との法的・手続的意味の平準化、ひいては選挙の公正に意を用いているといえよう。

(v) 秘密投票原則との関係

しかし、本件判決の論旨は、更に補強し得たのではないかと思われる。

それは、公職選挙法の定めた手続によらずして投票の内容が明らかになることそれ自体が投票の秘密を害すると考えることによって可能となる。通常、秘密投票の原則は、投票者と投票内容とが結びつけられないようにすることが主目的であると考えられるが、本来投票内容は適法な当該選挙の当選人選出のためだけに用いられるべきであって、他の目的で用いられることは原則としてあってはならないと考えるべきである。(最二小判平 9・3・28 では、泉佐野市議会議員選挙投票用紙差押え事件での警察による投票用紙差し押さえについて、何ら憲法判断することなく上告を棄却している)

本件において、上告人は外封筒と内封筒が離された後に内封筒を開封して点検・調査を行ったのであるから投票の秘密の侵害は起こらないと述べているが、無効となってしまった投票が、特定の投票箱・投票所に限られていた場合や、特に不在者投票の場合は、選挙人本人が通常の開票手続から外れて法定外の方式で自分の投票が点検されることを覚知しうるし、また公的機関その他の者が、点検・調査の結果からかなり特定された地域や集団における投票傾向を把握し得るし、当選人決定以外の目的で個人の投票内容を知ろうとする者にとっても相当有益な材料を、他ならぬ投票そのものから引き出すことができる危険性を指摘しておきたい。投票所外で任意に選挙人が投票の内容について陳述するのは自由であろうが、投票そのものから同様の情報を抽出できる可能性を開いておくことは、憲法 15 条 4 項に違反し、許されないと解すべきであろう。

(vi) 電子投票制度・電子投票システムへの示唆

電子投票を行う場合、上述の諸判例からは以下の3点が問題となるであろう。

①二重投票を防止するために、開票までの間、電子投票システムの記憶媒体内には投票者の投票内容の情報(α)および投票の有無の情報(β)が関連づけられて保存されていると考えられる。投票者以外の者が、βからαを引き出せるような状態はもちろん許されないし、βそのものも、当該投票への姿勢や政権に対する態度、棄権の意思などを示す可能性があるため、第三者から引き出されることの無いようなシステムが求められよう。

②第一段階の電子投票においては、投票データの入力された記憶媒体が開票所に搬送されるまでの間に、上で述べたような事故や管理ミス、あるいは意図的な選挙妨害等が発生し得る。(もっとも、システムの問題とは言えない。自書式投開票の持つ危険性が残存しているに過ぎない。)

③第二・第三段階の電子投票においては、開票センターのシステムに送信される過程での覗き見や改竄は暗号化で防ぐことができるとしても、意図的なデータの破壊や事故によるデータ喪失を防止ないしは早期に発見して防御および再送信が可能なシステムが求められよう。また、送信段階では既にβ情報はα情報と切り離されていることが求められよう。

5-1-2-3　諸外国の電子投票に対する取組み

＊電子投票制度の現状

①ベルギー[5]

- 1994年電子投票法により、国政選挙・地方選挙・EU 議会ベルギー代表改選ともに光学式ペンを備えたPC端末を用いた電子投票を実現した。
- ベルギー内務省は、1989 年から新しい投開票システムについての検討を始めた。検討を始めた理由としては、投票が義務であること、非拘束式名簿制による投票を行うため、これまでの紙による投開票では選挙時に膨大な時間と労力が必要とされていたことが、まず挙げられる。特に人口の集中しているブリュッセル首都圏・レジオンなどでは、リストと候補者の数が多くなるため、開票作業は困難を極め、関係者は日曜日から火曜日の朝まで作業を続けなければならない状況にあった。それゆえ、各投票所や開票所を管理する選挙人を確保することが次第に困難になり、各コミューンにとっては頭の痛い問題となっていた。
- ベルギーの選挙では 1 枚の投票用紙に、各政党リストの候補者名がすべて記載されているため、国政選挙では投票用紙1枚の大きさは1m四方（模造紙大という！）にもなっていた。この投票用紙の大きさは、記載される候補者名の確認作業、印刷経費、各コミューンまでの運送費、選挙日までの保管場所、投票時における秘密保持など様々な問題を生んでいた。投票所は学校や公民館などが使われているが、投票ボックスに十分なスペースが確保できず、大きな投票用紙を広げることができないため、投票者の中には床に広げて記入するようなケースもあり、投票の秘密が守れないだけでなく改ざんなどの問題も生じていた。
- 電子投票制を定めた法律には、連邦議会と各州の議会により任命された専門家会議による電子投票制に対する統制制度が規定されている。専門家会議はすべての選挙用ソフトウェアについて、内務省での準備段階や選挙管理事務所での使用段階において検査することができる。この統制は独立した形で実施され、専門家会議は独自の判断で検査を実施する選挙管理事務所を選択することができるようになっている
- 媒体は、開票用がFD、バックアップを磁気カードで取るようになっている。磁気カードは投票箱に回収する。

②オランダ[6]

- 1965 年王国選挙法により、機械式投票機が導入されていた。
- 1974 年王国選挙法により、電子投票機が導入されて以来の長い伝統を持つ。
- 1989 年現行王国選挙法により、適用する技術や機器の変更に法律がついていけなくなることがないように、技術や機器の運用については政令で定めることとした。
- 現行王国選挙法J33 条において、内務大臣の許可を得た技術を用いた場合に電子投票を限定し、その要件としてa,選挙人が望まなくとも投票の秘密を保持できること。b,電子投票を用いない場合と同等の投票結果と安定性・安全性を備えていること。c，候補者・名簿上の候補者番号・政党が明確に表示されること。d，二重投票を防止し、時に的な誤りを修正できること。を明文で定めている。

③ブラジル[7]

- 1994 年の選挙で連鎖方式の投票用紙持ち帰り不正投票事件が発覚、また以前から脅迫や買収が選挙に付き物とされてきた。こうした不正を排除するため、1996年連邦選挙法でテンキー入力方式の電子投票に踏み切った。

---

5 自治体国際化フォーラム 2001.06 月号（available at http://www.clair.or.jp/j/forum/)に全面的に依拠した。

6 Koninkrijk waarrijt(1989)(王国選挙法)

7 情報通信総合研究所,InfoCom ニューズレター（松原記事）に依拠

・ 媒体はFDを用い、投票終了後は開票点検委員会へ送致後、選挙裁判所へオンラインで送信し、開票する。また、FDに記録された投票内容は、同時に紙片に印刷され、バックアップ用に保存される。

5-1-2-4 第三段階の電子投票に向けて――――法制度改定の試案

現在、地方選挙において実施されている電子投票は、投票所に設置された投票専用の電磁的記録式投票機を用いて投票を行う方式に限定されているが、我々は、任意の場所から任意の投票用端末を用いて投票を行う「第三段階の電子投票」(以下「次世代電子投票」と記述する。)を可能とすべく研究を行っている。次世代電子投票において選挙人は投票所へ赴く必要がなくなり、また自書する必要もない。従って、様々な事由で投票所へ行くことのできない選挙人や身体故障等の理由により自書できない選挙人が、自宅などの任意の場所において、容易な端末操作で投票を行うことが可能となる。すなわち、投票の意思がありながら現在の投票制度では投票することが困難だった有権者が、容易に投票を実施することが可能となる。

また、文字判別に起因する投票数の不明確さや無効票の撲滅につながり、有権者の意思を明確に反映することができる。

既に第一段階の電子投票の導入において確認されているが、投票用紙を開票して集計する必要がなくなるので、開票作業の短縮に繋がり、開票作業に携わる職員の削減にも効果がある。さらに次世代電子投票になると、投票所の設置や投票用紙や投票データの運搬も不要となり、これらに必要な費用も削減できるようになる。

しかし、現在の法制度では次世代電子投票を用いた選挙を実施することができない。そこで、法律の改定案を検討することで、どのようにしたら次世代電子投票を用いた選挙が実施できるようになるかを検討し、さらにシステム上考慮すべきことの確認を行えるようにした。

(i) 選挙のための法律

『国』と『地方自治体』には選挙を実施可能とするために、それぞれ以下の法律が制定されており、国政のための選挙と地方自治体の選挙では、遵守すべき法律が異なっている。

(国) 憲法 → 地方自治法 → 公職選挙法 → 公職選挙法施行令 → 公職選挙法施行規則
(地) 条例 → 規則 → 要綱、規定、規程等

現在の電子投票は、公職選挙法(公選法)に特例法を付加することで実現可能になっている。実際の選挙においては公職選挙法も特例法も有効となるが、電子投票に関する部分については特例法が公選法よりも優先され、表示形式などの詳細については、自治体の条例に委任されている。

次世代電子投票を実現するためには、公選法もしくは特例法を改定する必要があるが、公選法を改定してしまうと、他の投票方式(紙による自書式投票、点字投票等)の扱いも含めて検討する必要があるため、さまざまな影響が出てしまう可能性がある。そこで、まず特例法を改定することで次世代投票を実現できるようにすることを考え、改定試案を作成した。また、現在の特例法の罰則規定だけでは、次世代電子投票において想定される犯罪行為を網羅しきれないため、罰則規定については公選法も含め全体的に検討し、特例法の罰則規定を強化する形をとった。

(ii) 選挙の基本原則と次世代投票

選挙制度については、もっとも基本的な原則は憲法に定められ、これを受けて公職選挙法で詳細に規定されている。日本国憲法は、国民主権主義を基調とし代議制民主主義を採ることを明らかにしている。その具体的手段である選挙については、法律に委ねることなく、表 5 に示すように憲法自体の中にいくつかの規定を設けている。

表 5　憲法に明記された選挙に関する記述

憲法　第 15 条 1 項	〈公務員の選定･罷免権, 全体の奉仕者性, 普通選挙･秘密投票の保障〉
公務員を選定し, 及びこれを罷免することは, 国民固有の権利である	
憲法　第 15 条 3 項	〈普通選挙主義〉
公務員の選挙については、成年者による普通選挙を保障する	
憲法　第 15 条 4 項	〈秘密投票主義〉
すべて選挙における投票の秘密は、これを侵してはならない。選挙人は、その選択に関し公的にも指摘にも責任を問われない（秘密投票は、各国共有の原則）	
憲法　第 44 条	〈平等主義〉
両議院の議員及びその選挙人の資格は、法律でこれを定める。ただし、人種、信条、性別、社会的身分、門地、教育、財産または収入によって差別してはならない	
憲法　第 14 条	
すべて国民は、法の下に平等であって、人種、信条、性別、社会的身分または門地により政治的、経済的又は社会的関係において、差別されない	
憲法　第 93 条	〈直接選挙主義〉
地方公共団体の長、その議会の議員及び法律の定めるその他の吏員は、その地方公共団体の住民が、直接これを選挙する	

上記、憲法における原則を受けて、公選法において7つの基本原則が定められている。各原則について、次世代投票においては次のような解釈をとることにした。

表 6　公選法の7つの基本原則と次世代投票における解釈

■ 投票主義（公選法 35 条）	
【条文】	選挙は、投票により行う
補足	次世代投票においても、この原則に変更は無い

■ 一人一票主義（公選法 36 条）	
【条文】	各選挙につき、一人一票に限る 比例代表, 小選挙区の二つが同時に行われる場合はそれぞれ一票
補足	・ハガキを用いた現行の本人確認に代わる、新しい本人認証システムが必要となるが、次世代投票であってもこの原則に変更は無い。現行の選挙と同じく、重複投票や詐称などが起こらないようにしなくてはならない。 ・特例法4条1項の1 『選挙人が一の選挙において 二以上の投票を行うことを防止できるものであること。』

■ 選挙人名簿登録主義（公選法 42 条）	
【条文】	選挙人名簿又は在外選挙人名簿に登録されていない者は、投票をすることができない。
補足	選挙人名簿は、現時点で殆どの選管において電子化されている。 次世代においては任意の場所からの投票となるため、ネットワーク経由で名簿との照合が行われて本人確認されるであろう。 確認のための手法は異なるが、次世代投票であっても原則に変更は無い 。

■ 投票当日投票所投票主義(公選法 44 条)	
【条文】	選挙人は、選挙の当日、自ら投票所に行き、投票をしなければならない。 選挙人は、選挙人名簿又はその抄本の対照を経なければ、投票をすることができない。
補足	【次世代を実現する場合】 ●基本・・「投票所」で　　「自ら」 ●例外・・「洋上、海外、自宅等」で「自ら」もしくは「代理人」によって ●次世代・・「任意の場所」で　　「自ら」もしくは「代理人」によって ・次世代においては、投票区・投票所といった投票する場所についての制限は必要なくなる。 ・選挙人名簿の対照は、原則どおり。 ・投票当日投票所投票主義の原則は、変更の必要あり。ただし、公選法の改定は行わない。
【改定案】	公選法44条は変更せず、特例法3条において、『選挙人が自ら、投票所において電磁的記録式投票機を操作する事により、』を、『選挙人が自ら、任意の場所において、任意の投票用端末を操作することにより』と書き換える。

■ 投票用紙公給主義(公選法 45 条)	
【条文】	投票用紙は、選挙の当日、投票所において選挙人に交付しなければならない。 2　投票用紙の様式は、衆議院議員又は参議院議員の選挙については総務省令で定め、地方公共団体の議会の議員及び長の選挙については当該選挙に関する事務を管理する選挙管理委員会が定める。
補足	→　次世代投票は紙を用いた投票ではないので、この原則の変更 もしくは同等の原則に置き換える必要がある。 ● 投票用紙　　⇒　投票用端末、本人確認用のトークン等 ● 投票所　　⇒　任意の投票場所 ● 投票用紙の様式　⇒　投票用端末の仕様
	ただし今回の法改定案の方針では、公選法をできるだけ改定せずに特例法の改定のみで対応するので、公選法45条の改定は行わない。特例法3条においては公選法45条を読み替えるという原則のままで問題ないと思われる。(特例法の4，5，6条において、公選法45条で定めた内容が置き換えられている)

■ 単記自書投票主義(公選法 46 条)	
【条文】	選挙人は、投票所において、投票用紙に当該選挙の公職の候補者一人の氏名を自書して、これを投票箱に入れなければならない。
補足	・この例外として代理投票や記号式投票、点字投票が挙げられる。 電子投票(次世代電子投票を含む)は、単記自書投票主義の例外とされ、記号式投票の一種と見なされている。よって原則の変更は必要ないが、条文を改定する必要はあると考えられる。 ・　投票所　⇒　任意の場所 投票用紙　⇒　投票用端末 自書　⇒　× 投票箱　⇒　× ・単記:複数人による記載　⇒　(次世代の場合は操作？)は不可 自書:自書　　⇒　(自ら端末を操作)は可
【改定案】	特例法の3条に46条を読みかえる記載がなされているため、公選法46条を改定したものを追加する必要はない。
補足	現在、国政選挙では記号式投票を導入していない。しかし、無効票の撲滅や開票作業の迅速化等のメリットの大きさを考えると、電子投票をはじめとする記号式投票を国政選挙に導入することは、効果が大きいと考えられる。

■ 秘密投票主義(公選法 46 条、52 条、68 条)	
【条文】	投票用紙には、選挙人の氏名を記載してはならない。 何人も、選挙人の投票した被選挙人の氏名又は政党その他の政治団体の名称若しくは略称を陳述する義務はない。
補足	⇒ 次世代電子投票においても投票の秘密は守られなければならないが、投票用紙を用いた投票ではないため、条文の改定が必要となる。 ⇒ ただしこれは秘密投票主義の原則を変更するものではない。 ⇒ 現在の特例法では電磁記録式投票機を想定しているため「投票の秘密が侵されないものであること」としか記載されていない。しかし、次世代電子投票の場合は投票システムだけでなく運用面でも、これまでに想定されていない部分がある。また、技術の進歩による影響を受けないためにも、罰則規定を追加もしくは強化し投票の秘密を守るべきと思われる。従って、現行の法では罰則規定が設けられていない分野いついても、新たにこれを厳密に禁じる法律の整備が必要である。 (例)227 条(投票の秘密侵害罪) 228 条(投票干渉罪)等 (例)投票用端末の改造の禁止、投票データの盗聴や改竄の禁止等
【改定案】	公選法46条における『投票用紙には、選挙人の氏名を記載してはならない』という一文を、以下のように書き換え、特例法の3条へ挿入する。 『電子投票の場合は、投票内容についての 秘密を確保するものでなければならない。』

(iii) 投票方法の分類とその対応

現在公職選挙法で認められている投票方法について分類したものを以下に示す。

表 7 投票方法の分類

	具体的な投票方法	特徴
自書式投票	投票用紙に候補者名などを自書する	
記号式投票	候補者氏名に〇印をつける	地方選挙のみ。不在者、期日前、点字は自書式
点字投票	点字投票である旨の表示をした用紙使用	
代理投票	代理者が投票用紙に代理で記載する	
期日前投票	投票日前に期日前投票所において投票	点字、代理投票が認められている
不在者投票 ・一般的 ・郵送等に ・洋上から	 不在者投票の事由に該当する選挙人が投票 投票所へ行けない場合、郵送で投票 洋上の船舶より FAX で投票	 点字による記載、代理人の代筆は不可 点字は不可。代理、代理の仮投票ＯＫ
在外投票 ・在外公館投票 ・郵便等投票 ・帰国投票 ・登録地における帰国投票 ・登録地以外の市町村における帰国投票	 大使館等で投票 大使館等へ郵送で投票 選挙人名簿に登録された選挙区で投票 選挙人名簿に登録されていない選挙区で投票	
仮投票	当該選挙人に仮に行わせる投票	代理投票が認められる
電磁的記録式	電磁的記録式投票機を用いて投票する	点字、不在者、仮投票は公選法適用

基本は投票当日、投票所における自書による投票だが、次の２つの例外が認められている。

（1）　投票当日投票所へ行くことができない

海外居住、指定船舶における遠洋漁業、身体故障などによる外出不能、投票日選挙区外へ行くなどがあり、それぞれ在外投票、洋上投票、郵便投票、不在者投票などが認められている。

（2）　自書できない

盲人の場合は点字の利用が、文盲や身体故障の場合は代筆が、身体故障により外出不能かつ自書不能な場合は郵便による代筆投票がそれぞれ認められている。

次世代投票を導入することで、投票所へ行く必要がなくなり、また自書する必要もなくなるため、(1)と(2)の問題は解決できる。つまり、公選法で定められている例外措置が不要となる。図 8 は、現状の投票方法の現状をまとめた図である。

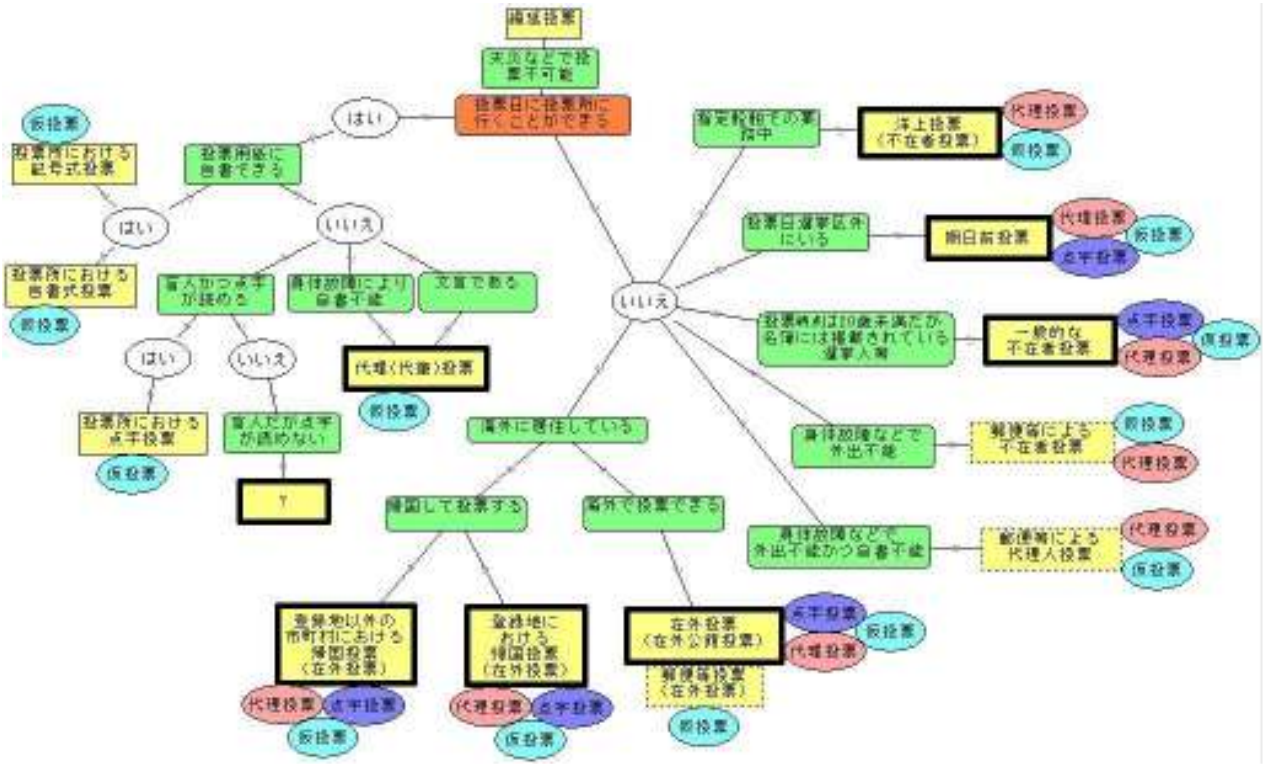


図 8　投票方法の現状

現在の公選法で定められた様々な投票方法は、次世代投票を導入することで図 9 のように統合される。

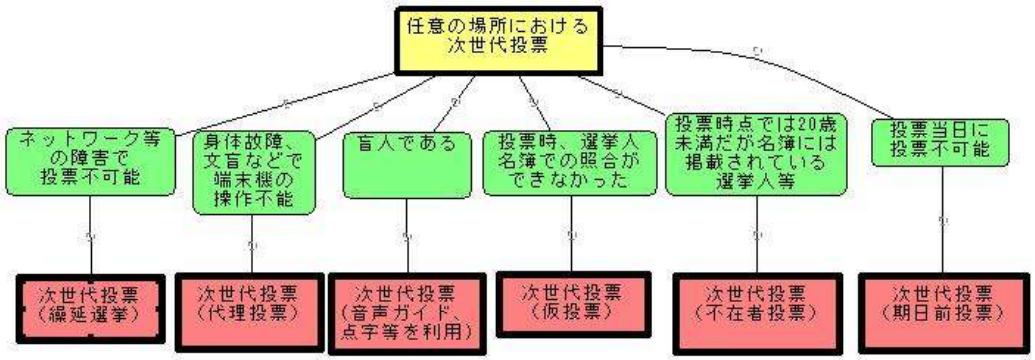


図 9　次世代投票での投票方法

表 8　次世代投票における現状の投票方法の適用方法

現在の投票方法	次世代との比較	次世代に適用するとどうなるか
投票所における自書式投票	投票所、自書式は無くなる	−
投票所における点字投票	投票用端末で点字の利用が難しい時は音声等を用いるべき	次世代投票（音声ガイド、点字などを利用）
投票所における記号式投票	電子投票は記号式投票の延長であると考えられる	−
投票所における代理投票（代筆による）	投票用端末の代理操作は認めるべき	次世代投票（代理操作）
帰国投票（在外投票）	任意の場所からの投票が可能なので、投票場所に拘らない	次世代投票
在外公館投票		
在外郵便投票		
在宅での代理人投票（郵便による）	任意の場所からの投票が可能なので、送信手段に拘らない	次世代投票
一般的な不在者投票	投票日前の投票は認めるべき	
不在者投票（郵便投票）	任意の場所からの投票が可能なので、送信手段に拘らない	次世代投票（不在者投票）
不在者投票（洋上投票）	任意の場所からの投票が可能なので投票場所に拘らない	次世代投票
期日前投票	投票日前の投票は認めるべき	次世代投票（期日前投票）
仮投票	次世代投票であっても仮投票は認めるべき	次世代投票（仮投票）
繰延投票	ネットワークなどの機器障害により投票日の投票不可能	次世代投票（繰延投票）

このように、次世代投票の導入により、公選法で定められている様々な投票方法は、ほぼすべて次世代投票でカバーすることが可能である。

（iv）特例法改定案

次世代投票の導入にあたり、次の観点で改定案をまとめた。

・公職選挙法の改定は行わず、特例法の改定のみを行う。

5-1-2-4 第三段階の電子投票に向けて――法制度改定の試案」において説明したように、公職選挙法を次世代投票にあわせて改定することで他の投票方法の実現が困難になる恐れがあるため、罰則規定以外は特例法のみの改定を行うこととした。

・特例法において、国政選挙における電子投票の利用を可能とする。

現在の電子投票は、地方選挙のみ利用可能である。しかし国政選挙においても導入の効果は大きいと考え、本改定案を作成した。

・公職選挙法の罰則規定を次世代投票導入に合わせ、特例法に取り入れる。

公選法の罰則は、選挙の基本原則に反した場合の犯罪行為及び自書式投票、その他公選法に定められた投票方式における不正行為について、詳細に規定されている。これに対して特例法における罰則は、

第十六条において、公選法四十八条における代理投票についての違反行為について定められているに過ぎない。現状の罰則規定だけでは次世代投票特有の犯罪行為についての違反行為すべてをカバーすることができないため、本改定案では、公職選挙法における罰則規定を次世代投票にあわせて改定して特例法に取り入れ、特例法改定案の21条から26条に記載した。これらの罰則規定は公選法における「職権濫用による選挙の自由妨害罪」「投票の秘密侵害罪」「投票干渉罪」「暴行罪、騒擾罪」「代理投票における記載義務違反」「選挙権及び被選挙権の停止」について、それぞれ次世代投票に合わせて内容を修正したものである。

・用語として、特例法で用いられている「電磁的記録式投票機」は、「電子投票システム」もしくは「投票用端末」と置き換える。

現在の電子投票では、投票も集計も、投票所に置かれた電磁的記録式投票機を用いる。しかし、次世代投票においては投票は投票用端末で、集計は電子投票システムで行うこととなる。そのため、文意に応じて用語を置き換えることとした。

表 9　次世代電子投票を導入するための法律の改定案

		現行			改定案	改定内容
第一条	趣旨	この法律は、情報化社会の進展にかんがみ、選挙の公正かつ適正な執行を確保しつつ開票事務等の効率化及び迅速化を図るため、**当分の間の措置として**、地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等について、公職選挙法（昭和二十五年法律第百号）の特例を定めるものとする。	第一条	趣旨	この法律は、情報化社会の進展にかんがみ、選挙の公正かつ適正な執行を確保しつつ開票事務等の効率化及び迅速化を図るため、**衆議院及び参議院における選挙及び**、地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等について、公職選挙法 （昭和二十五年法律第百号）の特例を定めるものとする。	・当分の間の措置として→削除 ・電磁的記録式投票機→電子投票システム ・国政選挙についての記述を追加
第二条	定義	この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。 一　電磁的記録媒体　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（次号において「電磁的記録」という。）に係る記録媒体をいう。 二　電磁的記録式投票機　当該機械を操作することにより、当該機械に記録されている公職の候補者のいずれかを選択し、かつ、当該公職の候補者を選択したことを電磁的記録として電磁的記録媒体に記録することができる機械をいう。	第二条	定義	この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。 一　電磁的記録媒体　電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの（次号において「電磁的記録」という。）に係る記録媒体をいう。 **二　投票用端末　選挙人が候補者の氏名もしくは党名を選択し、ネットワーク回線を通じて投票を行う装置を言う。** **三　電子投票システム　投票用端末を用いて候補者名もしくは党派別を選択し、ネットワーク回線を通じて投票を行うシステムを言う。**	投票用端末、電子投票システムという用語をここで定義。
第三条	**電磁的記録式投票機**による投票	**市町村**（地方自治法 （昭和二十二年法律第六十七号）第二百五十二条の十九第一項 の指定都市（以下「指定都市」という。）を除く。以下この項において同じ。）の議会の議員又は長の選挙の投票（公職選挙法第四十七条 、第四十九条並びに第五十条第三項及び第五項の規定による投票を除く。）については、市町村は、**同法第四十五条 、第四十六条第一項及び第四十八条の規定にかかわらず**、条例で定めるところにより、選挙人が、**自ら、投票所**（期日前投票所を含む。以下この条において同じ。）**において、電磁的記録式投票機**を操作することにより、当該**電磁的記録式投票機**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。	第三条	**電子投票システム**による投票	**市町村**（地方自治法 （昭和二十二年法律第六十七号）第二百五十二条の十九第一項 の指定都市（以下「指定都市」という。）を除く。以下この項において同じ。）の議会の議員又は長の選挙の投票については、市町村は、**同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず**、条例で定めるところにより、選挙人が、**自ら、任意の場所**（期日前投票所を含む。以下この条において同じ。）**において、任意の投票用端末**を操作することにより、当該**電子投票システム**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。	・同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず、」という記述を追加 ・公選法４７条、４９条並びに５０条３項及び５項の規定による投票を除く」の一文を削除 ・「自ら投票所において」→「任意の場所において」 ・「電磁的記録式投票機」→「電子投票システム」

		現行			改定案	改定内容
		２　**指定都市**の議会の議員又は長の選挙の投票（公職選挙法第四十七条 、第四十九条並びに第五十条第三項及び第五項の規定による投票を除く。）については、指定都市は、**同法第四十五条 、第四十六条第一項及び第四十八条の規定にかかわらず**、条例で定めるところにより、当該条例で定める当該指定都市の区の区域内の投票区を除き、選挙人が、**自ら、投票所において、電磁的記録式投票機**を操作することにより、当該**電磁的記録式投票機**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。この場合における同法第四十六条の二第一項 の規定の適用については、同項 中「第四十九条 」とあるのは、「第四十九条並びに地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第三条第二項及び第七条」とする。			２　**指定都市**の議会の議員又は長の選挙の投票については、指定都市は、**同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず**、条例で定めるところにより、当該条例で定める当該指定都市の区の区域内の投票区を除き、選挙人が、**自ら、任意の場所において、任意の投票用端末**を操作することにより、当該**電子投票システム**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。この場合における同法第四十六条の二第一項 の規定の適用については、同項 中「第四十九条 」とあるのは、「第四十九条並びに地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第三条第二項及び第七条」とする。	・同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず、」という記述を追加 ・公選法４７条、４９条並びに５０条３項及び５項の規定による投票を除く」の一文を削除 ・「自ら投票所において」→「任意の場所において」 ・「電磁的記録式投票機」→「電子投票システム」
		３　**都道府県**の議会の議員又は長の選挙の投票（公職選挙法第四十七条 、第四十九条並びに第五十条第三項及び第五項の規定による投票を除く。）については、都道府県は、**同法第四十五条 、第四十六条第一項及び第四十八条の規定にかかわらず**、前二項の条例を定めた市町村のうち当該都道府県の条例で定めるものの区域（指定都市にあっては、議会の議員の選挙に係る前項の条例及び長の選挙に係る同項の条例で定める区以外の区のうち当該都道府県の条例で定めるものの区域に限る。）内の投票区に限り、当該都道府県の条例で定めるところにより、選挙人が、**自ら、投票所において、電磁的記録式投票機**を操作することにより、当該**電磁的記録式投票機**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。この場合における同法第四十六条の二第一項 の規定の適用については、同項 中「第四十九条 」とあるのは、「第四十九条並びに地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第三条第三項及び第七条」とする。			３　**都道府県**の議会の議員又は長の選挙の投票については、都道府県は、**同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず**、前二項の条例を定めた市町村のうち当該都道府県の条例で定めるものの区域（指定都市にあっては、議会の議員の選挙に係る前項の条例及び長の選挙に係る同項の条例で定める区以外の区のうち当該都道府県の条例で定めるものの区域に限る。）内の投票区に限り、当該都道府県の条例で定めるところにより、選挙人が、**自ら、任意の場所において、任意の投票用端末**を操作することにより、当該**電子投票システム**に記録されている公職の候補者のうちその投票しようとするもの一人を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録する方法によることができる。この場合における同法第四十六条の二第一項 の規定の適用については、同項 中「第四十九条 」とあるのは、「第四十九条並びに地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第三条第三項及び第七条」とする。	・同法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず、」という記述を追加 ・公選法４７条、４９条並びに５０条３項及び５項の規定による投票を除く」の一文を削除 ・「自ら投票所において」→「任意の場所において」 ・「電磁的記録式投票機」→「電子投票システム」

		現行			改定案	改定内容
		（国政選挙について）			４　衆議院議員の議員及び参議院議員の選挙の投票については、**公選法第四十五条 、第四十六条第一項四十七条、第四十八条、第四十九条及び第五十条の規定にかかわらず**、選挙人が**自ら任意の場所**において**任意の投票用端末**を操作することにより、当該電子投票システムに記録されている公職の候補者のうちその投票しようとするもの一人、もしくは**一の衆議院名簿届出政党等（第八十六条の二第一項の規定による届出をした政党その他の政治団体をいう。以下同じ。）の同項の届出に係る名称又は略称を**選択したことを電磁的記録媒体に記録する方法によることができる。５　電子投票の場合は、**投票内容についての秘密を確保**するものでなければならない。	・国政選挙の場合の記述を追加・「公選法４７条、４９条並びに５０条３項及び５項の規定による投票を除く」の一文を削除・「５電子投票の場合は、投票内容についての秘密を確保するものでなければならない」の一文を追加
第四条	**電磁的記録式投票機**の具備すべき条件等	前条の規定による投票に用いる**電磁的記録式投票機**は、次に掲げる条件を具備したものでなければならない。 一　選挙人が一の選挙において二以上の投票を行うことを防止できるものであること。 二　投票の秘密が侵されないものであること。 三　**電磁的記録式投票機**の操作により公職の候補者のいずれを選択したかを電磁的記録媒体に記録する前に、当該選択に係る公職の候補者の氏名を**電磁的記録式投票機**の表示により選挙人が確認することができるものであること。 四　**電磁的記録式投票機**の操作により公職の候補者のいずれを選択したかを電磁的記録媒体に確実に記録することができるものであること。 五　予想される事故に対して、**電磁的記録式投票機**の操作により公職の候補者のいずれを選択したかを記録した電磁的記録媒体（以下「投票の電磁的記録媒体」という。）の記録を保護するために必要な措置が講じられているものであること。 六　投票の電磁的記録媒体を**電磁的記録式投票機**から取り出せるものであること。 七　権限を有しない者が**電磁的記録式投票機**の管理に係る操作をすることを防止できるものであること。 八　前各号に掲げるもののほか、選挙の公正かつ適正な執行を害しないものであること。	第四条	**電子投票システム**の具備すべき条件等	前条の規定による投票に用いる**電子投票システム**は、次に掲げる条件を具備したものでなければならない。 一　選挙人が一の選挙において二以上の投票を行うことを防止できるものであること。 二　投票の秘密が侵されないものであること。 三　**投票用端末**の操作により公職の候補者のいずれを選択したかを**電子投票システム**に記録する前に、当該選択に係る公職の**候補者の氏名及び党名**を**電子投票システム**の表示により選挙人が確認することができるものであること。 四　**投票用端末**の操作により公職の候補者のいずれを選択したかを**電子投票システム**に確実に記録することができるものであること。 五　予想される事故に対して、**投票用端末**の操作により**公職の候補者もしくは党名**のいずれを選択したかを記録した電磁的記録媒体（以下「投票の電磁的記録媒体」という。）の記録を保護するために必要な措置が講じられているものであること。 六　投票の電磁的記録媒体を**電子投票システム**から取り出せるものであること。 七　権限を有しない者が**電子投票システム**の管理に係る操作をすることを防止できるものであること。 八　前各号に掲げるもののほか、選挙の公正かつ適正な執行を害しないものであること。	・「電磁的記録式投票機」→「投票用端末」「電子投票システム」 ・「当該選択に係る公職の候補者の氏名」→「当該線k 宅に係る公職の選挙者もしくは党名」 ・「電気通信回線に接続してはならない」→「公衆回線及び閉域回線に接続する事を認める」「投票内容についての安全性を確保する為に必要な措置を講じなければならない」

		現行			改定案	改定内容
		２　**前条の規定による投票に用いる電磁的記録式投票機は、電気通信回線に接続してはならない**			２　**前条の規定による投票に用いる投票用端末は、公衆回線及び閉域回線である電気通信回線に接続することを認める。ただし、投票内容についての安全性を確保するために必要な措置を講じなければならない。**	
第五条	**電磁的記録式投票機**において表示すべき事項等	公職の候補者に関し**電磁的記録式投票機**において表示すべき事項は、公職の候補者の氏名及び党派別とする。この場合において、その表示の方法について必要な事項は、**都道府県**の議会の議員又は長の選挙については都道府県が、**市町村**の議会の議員又は長の選挙については市町村が、それぞれ、条例で定める。	第五条	**電子投票システム**において表示すべき事項等	公職の候補者に関し**電子投票システム**において表示すべき事項は、公職の候補者の氏名及び**党派別**とする。この場合において、その表示の方法について必要な事項は、**衆議院及び参議院の議員の選挙においては国が政令で、都道府県**の議会の議員又は長の選挙については都道府県が、**市町村**の議会の議員又は長の選挙については市町村が、それぞれ、条例で定める。	・表示方法について、国政選挙についての記述を追加 ・「電磁的記録式投票機」→「電子投票システム」 ・国政選挙については、「国が政令で」
第六条	**電磁的記録式投票機**の指定	**市町村**の選挙管理委員会は、第三条の規定による投票を行う選挙について、第四条第一項各号に掲げる条件を具備する**電磁的記録式投票機**のうちから、当該選挙の投票に用いる**電磁的記録式投票機**を指定しなければならない。この場合において、第三条第三項の規定による投票に用いる**電磁的記録式投票機**を指定しようとするときは、あらかじめ、**都道府県**の選挙管理委員会に協議し、その同意を得なければならない。 ２　**市町村**の選挙管理委員会は、前項の規定により**電磁的記録式投票機**を指定したときは、当該指定に係る**電磁的記録式投票機**の型式、構造、機能及び操作の方法を告示しなければならない。	第六条	**電子投票システム**の指定	**市町村**の選挙管理委員会は、第三条の規定による投票を行う選挙について、第四条第一項各号に掲げる条件を具備する**電子投票システム**のうちから、当該選挙の投票に用いる**電子投票システム**を指定しなければならない。この場合において、第三条第三項の規定による投票に用いる**電子投票システム**を指定しようとするときは、あらかじめ、**地方選挙の場合は都道府県の選挙管理委員会に、国政選挙の場合は、中央選挙管理委員会に協議し**、その同意を得なければならない。 ２　**市町村**の選挙管理委員会は、前項の規定により**電子投票システム**を指定したときは、当該指定に係る**電子投票システム**の**構成**、機能及び操作の方法を告示しなければならない。	・「電磁的記録式投票機」→「投票用端末」「電子投票システム」 ・形式、構造→構成 ・投票用端末の使用を決めてしまうと一種類の端末しか使用できなくなってしまうため、この条文はこれ以上の改定は不要

		現行			改定案	改定内容
第七条	**電磁的記録式投票機**による代理投票等	第三条の規定による投票において、身体の故障又は文盲により、自ら**電磁的記録式投票機**を用いた投票（**電磁的記録式投票機**を操作することにより、公職の候補者を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録することをいう。以下同じ。）を行うことができない選挙人は、同条の規定にかかわらず、投票管理者に申し立て、当該**電磁的記録式投票機**を用いた代理投票を行わせることができる。２　前項の規定による申立てがあった場合においては、投票管理者は、投票立会人の意見を聴いて、当該選挙人の投票を補助すべき者二人をその承諾を得て定め、その一人に当該選挙人が指示する公職の候補者一人に対して**電磁的記録式投票機**を用いた投票を行わせ、他の一人をこれに立ち会わせなければならない。３　第三条の規定による投票において、自ら**電磁的記録式投票機**を用いた投票を行うことが困難な選挙人（第一項に規定する選挙人を除く。）は、同条の規定にかかわらず、投票管理者に申し立て、当該**電磁的記録式投票機**の操作についての補助を行わせることができる。４　前項の規定による申立てがあった場合においては、投票管理者は、投票立会人の意見を聴いて、当該選挙人のために**電磁的記録式投票機**の操作を補助すべき者二人をその承諾を得て定め、その一人に**電磁的記録式投票機**の操作についての助言、介助その他の必要な措置（**電磁的記録式投票機**の操作により公職の候補者のいずれを選択したかを電磁的記録媒体に記録することを除く。）を行わせ、他の一人をこれに立ち会わせなければならない。	第七条	**電子投票システム**による代理投票等	第三条の規定による投票において、身体の故障又は文盲により、自ら**電子投票システム**を用いた投票（**任意の投票用端末**を操作することにより、公職の候補者を選択し、かつ、当該公職の候補者を選択したことを電磁的記録媒体に記録することをいう。以下同じ。）を行うことができない選挙人は、同条の規定にかかわらず、投票管理者に申し立て、当該**電子投票システム**を用いた代理投票を行わせることができる。 **２**　前項の規定による申立てがあった場合においては、投票管理者は、投票立会人の意見を聴いて、当該選挙人の投票を補助すべき者二人をその承諾を得て定め、その一人に当該選挙人が指示する公職の候補者一人に対して**任意の投票用端末**を用いた投票を行わせ、他の一人をこれに立ち会わせなければならない。 **３**　第三条の規定による投票において、自ら**任意の投票用端末**を用いた投票を行うことが困難な選挙人（第一項に規定する選挙人を除く。）は、同条の規定にかかわらず、投票管理者に申し立て、当該**任意の投票用端末**の操作についての補助を行わせることができる。 **４**　前項の規定による申立てがあった場合においては、投票管理者は、投票立会人の意見を聴いて、当該選挙人のために**任意の投票用端末**の操作を補助すべき者二人をその承諾を得て定め、その一人に**任意の投票用端末**の操作についての助言、介助その他の必要な措置（**任意の投票用端末**の操作により公職の候補者のいずれを選択したかを電磁的記録媒体に記録することを除く。）を行わせ、他の一人をこれに立ち会わせなければならない。	・「電磁的記録式投票機」→「電子投票システム」、「任意の投票用端末」 ・（保留）
第八条	投票の特例	第三条の規定による投票を行う選挙について、次の表の上欄に掲げる公職選挙法の規定を適用する場合においては、これらの規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句に読み替えるものとする。［表は別に記載］	第八条	投票の特例	第三条の規定による投票を行う選挙について、次の表の上欄に掲げる公職選挙法の規定を適用する場合においては、これらの規定中同表の中欄に掲げる字句は、それぞれ同表の下欄に掲げる字句に読み替えるものとする。［表は別に記載］	※別表に記載

		現行			改定案	改定内容
第九条	開票の特例	第三条の規定による投票を行う選挙について、公職選挙法第六十五条 及び第七十一条 の規定を適用する場合においては、同法第六十五条 中「投票箱」とあるのは「投票箱及び投票の電磁的記録媒体若しくは投票を複写した電磁的記録媒体」と、同法第七十一条 中「投票は、有効無効を区別し」とあるのは「投票、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は」と、「保存しなければならない」とあるのは「保存しなければならない。この場合において、投票にあつては、有効無効を区別して保存しなければならない」とする。 ２　第三条及び第七条の規定による投票については、公職選挙法第六十六条 から第六十八条の二 までの規定は、適用しない。 ３　公職選挙法第六十八条第一項第二号 又は第五号に規定する者に対する第三条 及び第七条 の規定による投票は、無効とする。 ４　開票管理者は、第三条及び第七条の規定による投票については、開票立会人とともに、投票の電磁的記録媒体に記録された投票を電子計算機を用いて集計することにより、各公職の候補者の得票数を計算しなければならない。この場合において、開票管理者は、開票立会人の意見を聴いて、投票の効力を決定しなければならない。 ５　開票管理者は、第三条の規定による投票を行う選挙については、公職選挙法第六十六条第三項 の規定にかかわらず、前項の計算の結果及び同条第二項 の規定により行った投票の点検の結果により、各公職の候補者の得票数を計算し、直ちにそれらの結果を選挙長に報告しなければならない。	第九条	開票の特例	第三条の規定による投票を行う選挙について、公職選挙法第六十五条 及び第七十一条 の規定を適用する場合においては、同法第六十五条 中**「すべての投票箱の送致を受けた」とあるのは「投票」と**、同法第七十一条 中「投票は、有効無効を区別し」とあるのは「投票、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は」と、「保存しなければならない」とあるのは「保存しなければならない。この場合において、投票にあつては、有効無効を区別して保存しなければならない」とする。 ２　第三条及び第七条の規定による投票については、公職選挙法第六十六条 から第六十八条の二 までの規定は、適用しない。 ３　公職選挙法第六十八条第一項第二号 又は第五号 に規定する者に対する第三条 及び第七条 の規定による投票は、無効とする。 ４　開票管理者は、第三条及び第七条の規定による投票については、開票立会人とともに、投票の電磁的記録媒体に記録された投票を電子計算機を用いて集計することにより、各公職の候補者の得票数を計算しなければならない。この場合において、開票管理者は、開票立会人の意見を聴いて、投票の効力を決定しなければならない。 ５　開票管理者は、第三条の規定による投票を行う選挙については、公職選挙法第六十六条第三項 の規定にかかわらず、前項の計算の結果及び同条第二項の規定により行った投票の点検の結果により、各公職の候補者の得票数を計算し、直ちにそれらの結果を選挙長に報告しなければならない。	

		現行			改定案	改定内容
第十条	投票を複写した電磁的記録媒体	投票管理者は、第三条及び第七条の規定による投票については、当該選挙に関する事務を管理する選挙管理委員会の定めるところにより、投票の電磁的記録媒体に記録された投票を他の電磁的記録媒体に複写しなければならない。 ２　開票管理者は、投票の電磁的記録媒体が破損し又は紛失したことにより、前条第四項の規定による集計を行うことが不可能であると認めるときは、開票立会人の意見を聴いて、当該投票の電磁的記録媒体に代えて、前項の規定により当該投票の電磁的記録媒体に記録された投票を複写した電磁的記録媒体（以下「投票を複写した電磁的記録媒体」という。）を使用して開票を行うものとする。	第十条	投票を複写した電磁的記録媒体	投票管理者は、第三条及び第七条の規定による投票については、当該選挙に関する事務を管理する選挙管理委員会の定めるところにより、投票の電磁的記録媒体に記録された投票を他の電磁的記録媒体に複写しなければならない。 ２　開票管理者は、投票の電磁的記録媒体が破損し又は紛失したことにより、前条第四項の規定による集計を行うことが不可能であると認めるときは、開票立会人の意見を聴いて、当該投票の電磁的記録媒体に代えて、前項の規定により当該投票の電磁的記録媒体に記録された投票を複写した電磁的記録媒体（以下「投票を複写した電磁的記録媒体」という。）を使用して開票を行うものとする。	修正なし
第十一条	選挙会の特例	第三条の規定による投票を行う選挙について、公職選挙法第七十九条第一項 、第八十条並びに第八十三条第二項及び第三項の規定を適用する場合においては、同法第七十九条第一項 中「第七章 」とあるのは「第七章 及び地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同法第八十条第一項及び第三項中「第六十六条第三項」とあるのは「地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同条第二項中「結果」とあるのは「結果及び地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第九条第四項の規定による計算の結果」と、同法第八十三条第二項中「第六十六条第三項」とあるのは「地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同条第三項中「投票の有効無効を区別し」とあるのは「投票、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は」と、「保存しなければならない」とあるのは「保存しなければならない。この場合において、投票にあつては、有効無効を区別して保存しなければならない」とする。	第十一条	選挙会の特例	第三条の規定による投票を行う選挙について、公職選挙法第七十九条第一項 、第八十条並びに第八十三条第二項及び第三項の規定を適用する場合においては、同法第七十九条第一項 中「第七章 」とあるのは「第七章 及び地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同法第八十条第一項及び第三項中「第六十六条第三項」とあるのは「地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同条第二項中「結果」とあるのは「結果及び地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第九条第四項の規定による計算の結果」と、同法第八十三条第二項中「第六十六条第三項」とあるのは「地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第九条第五項」と、同条第三項中「投票の有効無効を区別し」とあるのは「投票、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は」と、「保存しなければならない」とあるのは「保存しなければならない。この場合において、投票にあつては、有効無効を区別して保存しなければならない」とする。	「電磁的記録式投票機」→『電子投票システム』

		現行			改定案	改定内容
第十二条	立候補の特例	第三条の規定による投票を行う選挙（公職選挙法第四十六条の二第一項 の規定による投票を行う選挙を除く。）について、同法第八十六条の四 の規定を適用する場合においては、同条第五項 及び第六項 中「三日」とあるのは「四日」と、「二日」とあるのは「三日」と、同条第八項 中「三日」とあるのは「四日」とする。	第十二条	立候補の特例	第三条の規定による投票を行う選挙（公職選挙法第四十六条の二第一項 の規定による投票を行う選挙を除く。）について、同法第八十六条の四 の規定を適用する場合においては、同条第五項 及び第六項 中「三日」とあるのは「四日」と、「二日」とあるのは「三日」と、同条第八項 中「三日」とあるのは「四日」とする。	修正なし
第十三条	公職の候補者が死亡した場合等における電磁的記録式投票機の取扱い等	第三条の規定による投票を行う選挙について、公職の候補者が死亡した場合、公職選挙法第八十六条の四第九項の規定により届出を却下した場合又は同法第九十一条第二項 若しくは第百三条第四項 の規定により公職の候補者たることを辞したものとみなされた場合における**電磁的記録式投票機**の取扱いその他必要な措置については、政令で定める。	第十三条	公職の候補者が死亡した場合等における**電子投票システム**の取扱い等	第三条の規定による投票を行う選挙について、公職の候補者が死亡した場合、公職選挙法第八十六条の四第九項 の規定により届出を却下した場合又は同法第九十一条第二項 若しくは第百三条第四項 の規定により公職の候補者たることを辞したものとみなされた場合における**電子投票システム**の取扱いその他必要な措置については、政令で定める。	・「電磁的記録式投票機」→「電子投票システム」
第十三条の二		第三条の規定による投票を行う選挙について、第十二条の規定により読み替えて適用される公職選挙法第八十六条の四第五項 から第七項 までに規定する事由が生じた場合においては、第三条の規定にかかわらず、政令で定める期間、**電磁的記録式投票機**を用いた投票を行わないものとし、同法第四十五条 、第四十六条第一項、第四十八条及び第四十八条の二の規定により投票を行うものとする。	第十三条の二		第三条の規定による投票を行う選挙について、第十二条の規定により読み替えて適用される公職選挙法第八十六条の四第五項 から第七項 までに規定する事由が生じた場合においては、第三条の規定にかかわらず、政令で定める期間、**電子投票システム**を用いた投票を行わないものとし、同法第四十五条 、第四十六条第一項、第四十八条及び第四十八条の二の規定により投票を行うものとする。	・「電磁的記録式投票機」→「電子投票システム」
第十四条	公職の候補者が死亡した場合等の特例	第三条の規定による投票を行う選挙については、公職選挙法第十二章 の規定は、適用しない。ただし、市町村の議会の議員の選挙と市町村長の選挙をともに同条第一項又は第二項の規定による投票により行う場合（指定都市の議会の議員の選挙に係る同項の条例で定める区と当該指定都市の長の選挙に係る同項の条例で定める区が異なる場合を除く。）にあっては、この限りでない。 ２　地方自治法第七十六条第三項 、第八十条第三項、第八十一条第二項又は第二百六十一条第三項の規定による投票は、同法第八十五条第二項 又は第二百六十二条第二項 の規定にかかわらず、第三条の規定による投票を行う選挙と同時にこれを行うことができない。	第十四条	公職の候補者が死亡した場合等の特例	第三条の規定による投票を行う選挙については、公職選挙法第十二章 の規定は、適用しない。ただし、市町村の議会の議員の選挙と市町村長の選挙をともに同条第一項又は第二項の規定による投票により行う場合（指定都市の議会の議員の選挙に係る同項の条例で定める区と当該指定都市の長の選挙に係る同項の条例で定める区が異なる場合を除く。）にあっては、この限りでない。 ２　地方自治法第七十六条第三項 、第八十条第三項、第八十一条第二項又は第二百六十一条第三項の規定による投票は、同法第八十五条第二項 又は第二百六十二条第二項 の規定にかかわらず、第三条の規定による投票を行う選挙と同時にこれを行うことができない。	修正なし

		現行			改定案	改定内容
第十五条	同時選挙等の特例	第三条第一項又は第二項の規定による投票を行う選挙について、公職選挙法第百七十五条第八項 の規定を適用する場合においては、同項 中「第一項 又は」とあるのは「第一項 の掲示に関し必要な事項は市町村の選挙管理委員会が、」と、「事項は、」とあるのは「事項は」とする。	第十五条	同時選挙等の特例	第三条第一項又は第二項の規定による投票を行う選挙について、公職選挙法第百七十五条第八項 の規定を適用する場合においては、同項 中「第一項 又は」とあるのは「第一項 の掲示に関し必要な事項は市町村の選挙管理委員会が、」と、「事項は、」とあるのは「事項は」とする。	修正なし
第十六条	罰則	第三条及び第七条の規定による投票については、電磁的記録式投票機、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は投票箱と、第七条第二項の規定により選挙人の投票を補助すべき者及び同条第四項の規定により選挙人のために電磁的記録式投票機の操作を補助すべき者は公職選挙法第四十八条第二項 の規定により投票を補助すべき者とみなして、同法第十六章 の規定を適用する。 **2**　第七条第二項の規定により電磁的記録式投票機を用いた投票を行うべきものと定められた者が選挙人の指示する公職の候補者に対して電磁的記録式投票機を用いた投票を行わなかったときは、二年以下の禁錮又は三十万円以下の罰金に処する。 **3**　次に掲げる違反があった場合においては、その違反行為をした者は、二十万円以下の罰金に処する。 **一**　第七条第二項の規定により選挙人の投票を補助すべき者が同項の投票の補助の義務に違反したとき。 **二**　第七条第四項の規定により選挙人のために電磁的記録式投票機の操作を補助すべき者が同項の電磁的記録式投票機の操作の補助の義務に違反したとき。	第二十五条	代理投票における記載義務違反	第三条及び第七条の規定による投票については、電子投票システム、投票の電磁的記録媒体及び投票を複写した電磁的記録媒体は投票箱と、第七条第二項の規定により選挙人の投票を補助すべき者及び同条第四項の規定により選挙人のために電子投票システムの操作を補助すべき者は公職選挙法第四十八条第二項 の規定により投票を補助すべき者とみなして、同法第十六章 の規定を適用する。 ２　第七条第二項の規定により電子投票システムを用いた投票を行うべきものと定められた者が選挙人の指示する公職の候補者に対して電子投票システムを用いた投票を行わなかったときは、二年以下の禁錮又は三十万円以下の罰金に処する。３　次に掲げる違反があった場合においては、その違反行為をした者は、二十万円以下の罰金に処する。一　第七条第二項の規定により選挙人の投票を補助すべき者が同項の投票の補助の義務に違反したとき。二　第七条第四項の規定により選挙人のために電子投票システムの操作を補助すべき者が同項の電子投票システムの操作の補助の義務に違反したとき。	本条に掲載されている内容以外にも考慮する必要があるため、第二十一条以降として新規に設定する。 本条は特例法１６条の流用である。

		現行			改定案	改定内容
第十七条	選挙権及び被選挙権の停止	前条第二項又は第三項の罪を犯し罰金の刑に処せられた者は、その裁判が確定した日から五年間（刑の執行猶予の言渡しを受けた者については、その裁判が確定した日から刑の執行を受けることがなくなるまでの間）、公職選挙法 に規定する選挙権及び被選挙権を有しない。 ２　前条第二項の罪を犯し禁錮の刑に処せられた者は、その裁判が確定した日から刑の執行を終わるまでの間若しくは刑の時効による場合を除くほか刑の執行の免除を受けるまでの間及びその後五年間又はその裁判が確定した日から刑の執行を受けることがなくなるまでの間、公職選挙法 に規定する選挙権及び被選挙権を有しない。 ３　裁判所は、情状により、刑の言渡しと同時に、第一項に規定する者に対し同項の五年間若しくは刑の執行猶予中の期間について選挙権及び被選挙権を有しない旨の規定を適用せず、若しくはその期間のうちこれを適用すべき期間を短縮する旨を宣告し、又は前項に規定する者に対し同項の五年間若しくは刑の執行猶予の言渡しを受けた場合にあってはその執行猶予中の期間のうち選挙権及び被選挙権を有しない旨の規定を適用すべき期間を短縮する旨を宣告することができる。 ４　前三項の規定により選挙権及び被選挙権を有しない者は、公職選挙法第十一条第三項 、第二十一条第一項、第二十七条第一項、第三十条の四、第三十条の十第一項、第八十六条の八第一項及び第百三十七条の三の規定の適用については、これらの規定に規定する選挙権及び被選挙権を有しない者とみなす。 ５　第一項から第三項までの規定により選挙権及び被選挙権を有しないこととなる者に係る地方自治法第百二十七条第一項 、第百四十三条第一項及び第百八十四条第一項の規定の適用については、これらの規定中「第二百五十二条」とあるのは、「第二百五十二条、地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律第十七条第一項から第三項まで」とする。	第二十六条	選挙権及び被選挙権の停止	前条第二項又は第三項の罪を犯し罰金の刑に処せられた者は、その裁判が確定した日から五年間（刑の執行猶予の言渡しを受けた者については、その裁判が確定した日から刑の執行を受けることがなくなるまでの間）、公職選挙法 に規定する選挙権及び被選挙権を有しない。 ２　前条第二項の罪を犯し禁錮の刑に処せられた者は、その裁判が確定した日から刑の執行を終わるまでの間若しくは刑の時効による場合を除くほか刑の執行の免除を受けるまでの間及びその後五年間又はその裁判が確定した日から刑の執行を受けることがなくなるまでの間、公職選挙法 に規定する選挙権及び被選挙権を有しない。 ３　裁判所は、情状により、刑の言渡しと同時に、第一項に規定する者に対し同項の五年間若しくは刑の執行猶予中の期間について選挙権及び被選挙権を有しない旨の規定を適用せず、若しくはその期間のうちこれを適用すべき期間を短縮する旨を宣告し、又は前項に規定する者に対し同項の五年間若しくは刑の執行猶予の言渡しを受けた場合にあってはその執行猶予中の期間のうち選挙権及び被選挙権を有しない旨の規定を適用すべき期間を短縮する旨を宣告することができる。 ４　前三項の規定により選挙権及び被選挙権を有しない者は、公職選挙法第十一条第三項 、第二十一条第一項、第二十七条第一項、第三十条の四、第三十条の十第一項、第八十六条の八第一項及び第百三十七条の三の規定の適用については、これらの規定に規定する選挙権及び被選挙権を有しない者とみなす。 ５　第一項から第三項までの規定により選挙権及び被選挙権を有しないこととなる者に係る地方自治法第百二十七条第一項 、第百四十三条第一項及び第百八十四条第一項の規定の適用については、これらの規定中「第二百五十二条」とあるのは、「第二百五十二条、地方公共団体の議会の議員及び長の選挙に係る電子投票システムを用いて行う投票方法等の特例に関する法律第十七条第一項から第三項まで」とする。	特例法１７条の流用

		現行			改定案	改定内容
第十八条	**電磁的記録式投票機**の使用に要する費用の負担	地方公共団体の議会の議員又は長の選挙に関する**電磁的記録式投票機**の使用に要する費用については、当該地方公共団体の負担とする。	第十六条	**電子投票システム**の使用に要する費用の負担	**１　国政選挙に関する電子投票システムの使用に要する費用については、国の負担とする。** **２**　地方公共団体の議会の議員又は長の選挙に関する**電子投票システム**の使用に要する費用については、当該地方公共団体の負担とする。	・「電磁的記録式投票機」→「電子投票システム」 ・従来の条文を２に、国政選挙についての記述を１とする
第十九条	雑則	第三条の規定による投票を行う選挙について、公職選挙法第二百六十四条の二 から第二百六十六条 までの規定を適用する場合においては、これらの規定中「この法律」とあるのは、「この法律及び地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律」とする。	第十七条	雑則	第三条の規定による投票を行う選挙について、公職選挙法第二百六十四条の二 から第二百六十六条 までの規定を適用する場合においては、これらの規定中「この法律」とあるのは、「この法律及び地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律」とする。	・「電磁的記録式投票機」→「電子投票システム」
第二十条	国の援助	国は、第三条の規定による投票を行う選挙の円滑な実施に資するため、地方公共団体に対する助言その他の援助の実施に努めるものとする。	第十八条	国の援助	国は、第三条の規定による投票を行う選挙の円滑な実施に資するため、地方公共団体に対する助言その他の援助の実施に努めるものとする。	修正なし
第二十一条	命令への委任	この法律に定めるもののほか、この法律の施行に関し必要な事項は、命令で定める。	第十九条	命令への委任	この法律に定めるもののほか、この法律の施行に関し必要な事項は、命令で定める。	修正なし
第二十二条	事務の区分	この法律の規定及びこの法律の規定により読み替えて適用する公職選挙法 の規定により、都道府県の議会の議員又は長の選挙に関し、市町村が処理することとされている事務は、地方自治法第二条第九項第二号 に規定する第二号 法定受託事務とする。	第二十条	事務の区分	この法律の規定及びこの法律の規定により読み替えて適用する公職選挙法 の規定により、都道府県の議会の議員又は長の選挙に関し、市町村が処理することとされている事務は、地方自治法第二条第九項第二号に規定する第二号 法定受託事務とする。	修正なし
公職選挙法第二百二十六条	職権濫用による選挙の自由妨害罪	２　　国若しくは地方公共団体の公務員、特定独立行政法人若しくは日本郵政公社の役員若しくは職員、中央選挙管理会の委員若しくは中央選挙管理会の庶務に従事する総務省の職員、選挙管理委員会の委員若しくは職員、投票管理者、開票管理者又は選挙長若しくは選挙分会長が選挙人に対し、その投票しようとし又は投票した被選挙人の氏名（衆議院比例代表選出議員の選挙にあつては政党その他の政治団体の名称又は略称、参議院比例代表選出議員の選挙にあつては被選挙人の氏名又は政党その他の政治団体の名称若しくは略称）の表示を求めたときは、六月以下の禁錮又は三十万円以下の罰金に処する。	第二十一条	職権濫用による選挙の自由妨害罪	国若しくは地方公共団体の公務員、特定独立行政法人若しくは日本郵政公社の役員若しくは職員、中央選挙管理会の委員若しくは中央選挙管理会の庶務に従事する総務省の職員、選挙管理委員会の委員若しくは職員、投票管理者、開票**管理者又は選挙長若しくは選挙分会長、電子投票システムの作成者、電気通信回線の敷設に係る者、または投票当日及び開票当日に投票機（サーバ）を操作する者、投票用端末を代理操作する者**が選挙人に対し、その投票しようとし又は投票した被選挙人の氏名（衆議院比例代表選出議員の選挙にあつては政党その他の政治団体の名称又は略称、参議院比例代表選出議員の選挙にあつては被選挙人の氏名又は政党その他の政治団体の名称若しくは略称）の表示を求めたときは、六月以下の禁錮又は三十万円以下の罰金に処する。	電子投票システムの作成者、ネットワークを敷設するもの、投票機を操作する、端末を代理操作するものに分類し、選挙人の選挙の自由を妨害した場合の罰則とした

		現行			改定案	改定内容
公職選挙法第二百二十七条	投票の秘密侵害罪	中央選挙管理会の委員若しくは中央選挙管理会の庶務に従事する総務省の職員、選挙管理委員会の委員若しくは職員、投票管理者、開票管理者、選挙長若しくは選挙分会長、選挙事務に関係のある国若しくは地方公共団体の公務員、立会人（第四十八条第二項の規定により投票を補助すべき者及び第四十九条第三項の規定により投票に関する記載をすべき者を含む。以下同じ。）又は監視者が選挙人の投票した被選挙人の氏名（衆議院比例代表選出議員の選挙にあつては政党その他の政治団体の名称又は略称、参議院比例代表選出議員の選挙にあつては被選挙人の氏名又は政党その他の政治団体の名称若しくは略称）を表示したときは、二年以下の禁錮又は三十万円以下の罰金に処する。その表示した事実が虚偽であるときも、また同様とする。	第二十二条	投票の秘密侵害罪	**投票者の投票内容を知りえたものが当該投票者の意思によらず投票内容を表示した場合は、二年以下の禁錮又は三十万以下の罰金に処する。その表示した内容が虚偽である場合もまた同様とする。**	対象者が拡大するため、公選法２２７条の表記を変更
公職選挙法第二百二十八条	投票干渉罪	投票所（期日前投票所を含む。以下この章において同じ。）又は開票所において正当な理由がなくて選挙人の投票に干渉し又は投票内容を認知する方法を行つた者は、一年以下の禁錮又は三十万円以下の罰金に処する。 ２　法令の規定によらないで投票箱を開き又は投票箱の投票を取り出した者は、三年以下の懲役若しくは禁錮又は五十万円以下の罰金に処する。	第二十三条	投票干渉罪	正当な理由が無くて電子投票システムを利用して選挙人の投票に干渉し又は投票内容を認知する方法を行ったものは、一年以下の禁錮又は三十万以下の罰金に処する。 ２　法令の規定によらず**電子投票システムにアクセスしたもの**は、三年以下の懲役もしくは禁錮又は五十万円以下の罰金に処する	公選法２２８の改定
公職選挙法第二百二十九条	暴行罪、騒擾罪	投票管理者、開票管理者、選挙長、選挙分会長、立会人若しくは選挙監視者に暴行若しくは脅迫を加え、投票所、開票所、選挙会場若しくは選挙分会場を騒擾し又は投票、投票箱その他関係書類（関係の電磁的記録媒体（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られる記録であつて電子計算機による情報処理の用に供されるものに係る記録媒体をいう。）を含む。）を抑留、毀壊若しくは奪取した者は、四年以下の懲役又は禁錮に処する。	第二十四条	暴行罪、騒擾罪	投票管理者、開票管理者、選挙長、選挙分会長、立会人若しくは選挙監視者に暴行若しくは脅迫を加え、投票所、開票所、**電子投票システム**、選挙会場若しくは選挙分会場を騒擾し又は投票、**投票箱**その他関係書類（関係の電磁的記録媒体（電子的方式、磁気的方式その他人の知覚によつては認識することができない方式で作られる記録であつて電子計算機による情報処理の用に供されるものに係る記録媒体をいう。）、**本人認証の為の媒体**を含む。）を抑留、毀壊若しくは奪取した者は、四年以下の懲役又は禁錮に処する。	公選法２２９の改定

※第八条

特例法第八条記載の公選法適用時の読み替え内容			「改定案第八条」における公選法適用時の読み替え内容
公選法条項	読み替え前の字句	読み替え後の字句	読み替え後の字句
第四十八条の二第二項の表	第五十三条第一項	地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十三条第一項	地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十三条第一項
	閉鎖しなければ	状態にしなければ	状態にしなければ
	入れさせる場合	入れさせる場合又は当該**電磁的記録式投票機**を用いて投票させる場合	入れさせる場合又は当該**電子投票システム**を用いて投票させる場合
	開かなければ	開き、又は当該**電磁的記録式投票機**を投票できる状態にしなければ	開き、又は当該**電子投票システム**を投票できる状態にしなければ
	第五十三条第二項	地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十三条第二項	地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十三条第二項
	投票箱を開いた場合は	投票箱を開いた場合又は**電磁的記録式投票機**を投票できる状態にした場合は	投票箱を開いた場合又は**電子投票システム**を投票できる状態にした場合は
	第五十五条	地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十五条	地方公共団体の議会の議員及び長の選挙に係る**電子投票システム**を用いて行う投票方法等の特例に関する法律第八条の規定により読み替えて適用される第五十五条
第五十三条第一項	閉鎖しなければ	閉鎖し、かつ、**電磁的記録式投票機**（地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第二条第二号に規定する**電磁的記録式投票機**をいう。以下同じ。）を投票できない状態にしなければ	閉鎖し、かつ、**電子投票システム**（本法律第二条第三号に規定する**電子投票システム**をいう。以下同じ。）を投票できない状態にしなければ
第五十三条第二項	の閉鎖	が閉鎖され、かつ、**電磁的記録式投票機**が投票できない状態にされた	が閉鎖され、かつ、**電子投票システム**が投票できない状態にされた
第五十五条	投票箱	投票箱、投票の電磁的記録媒体（地方公共団体の議会の議員及び長の選挙に係る**電磁的記録式投票機**を用いて行う投票方法等の特例に関する法律第四条第一項第五号に規定する投票の電磁的記録媒体をいう。以下同じ。）、投票を複写した電磁的記録媒体（同法第十条第二項に規定する投票を複写した電磁的記録媒体をいう。以下同じ。）	投票箱、投票の電磁的記録媒体（本法律第四条第一項第五号に規定する投票の電磁的記録媒体をいう。以下同じ。）、投票を複写した電磁的記録媒体（同法第十条第二項に規定する投票を複写した電磁的記録媒体をいう。以下同じ。）
第五十六条	投票箱を送致する	投票箱､投票の電磁的記録媒体又は投票を複写した電磁的記録媒体を送致する	投票箱、投票の電磁的記録媒体又は投票を複写した電磁的記録媒体を送致する
	その投票箱	その投票箱、投票の電磁的記録媒体、投票を複写した電磁的記録媒体	その投票箱、投票の電磁的記録媒体、投票を複写した電磁的記録媒体

5-1-3 アンケートなど、投票に類似する利用分野の検討

2003 年は 5 月に個人情報保護関連5法が制定され、個人情報の取扱に関する包括的な道筋ができた。2005 年 4 月から完全施行されることになり、民間での教育や各種の施策対応や、各分野に対する個別法の検討も盛んになってきている。2003 年度はネットワークでの個人情報の流出に関しても耳目を集めた。今後アンケート等での個人情報の取り扱いは細心の注意を払う必要がある。本項では、個人情報保護法の概要に関してと、医療および教育分野、行政に関して法制度と利用分野に関する検討を行う。

5-1-3-1　個人情報保護関連 5 法

個人情報保護関連 5 法とは下記の 5 法を言う。

・個人情報の保護に関する法律
・行政機関の保有する個人情報の保護に関する法律
・独立行政法人等の保有する個人情報の保護に関する法律
・情報公開・個人情報保護審議会設置法
・行政機関の保有する個人情報の保護に関する法律の施行に伴う法律の整備等に関する法

上記のうち、「個人情報の保護に関する法律(個人情報保護法)」が個人情報保護についての基本法であり、基本理念、国と地方の責務、基本方針の策定などが記され、また、民間部門についての規定が行われている。残り 4 法が、基本法に基づき、公的部門における規定を定めている。個人情報保護法は包括法であり、現在、医療、通信、金融などいくつかの分野で指針あるいは個別法の制定に関して検討が進められている。

個人情報保護法は 2005 年春に完全施行予定であり、本法が施行されることにより、個人情報取扱業者に対する下記の規定が適応される。

- 本人からの開示要求に対する情報の開示
- 個人情報の漏洩に対する罰則

個人情報保護法では、基本法部分で、基本理念として個人情報の適切な取扱をあげ、国等の責務、政策として、政府が基本方針を作成して総合的かつ一体的に施策を推進することを述べている。一般法部分で、民間の個人情報取扱事業者の義務として対象情報を定め（一定規模以上のデータベースを中心）、個人情報の取扱と本人関与について定めている。事業者に対する監督や主務大臣の権限の行使の制限など、組織を対象とした法体系となっている。

5-1-3-2　医療分野

2003 年 6 月に厚生労働省の「診療に関する情報提供等の在り方に関する検討会」は最終報告書において、個人情報保護法などの制定により、ほとんどの医療機関が、本人からの求めに応じて、原則として診療記録を開示する義務を負い、診療記録の開示も含めた診療情報の提供が必要になることを示唆したが、独自の法制化は見送るとした。しかし、「個人情報保護法等で対象外となっている問題も含めて、まずは、診療情報の提供等に関して各医療機関が則るべき運用指針を策定するべきである。」として、「診療情報の提供に関するガイドライン（案）」を最終報告書に含め、厚生労働省はこれに基づき、「診療情報の提供等に関する指針」を策定し、各都道府県知事あてに 9 月 12 日付けで通知を出した（医政発 0912001 号）。

アメリカでは HIPAA（Health Insurance Portability and Accountability Act：健康保険のポータビリティとアカウンタビリティに関する法律）法が 2003 年 4 月以降施行されたが、本法はプライバシールールに関する詳細なルールと FAQ が付け加えられ、行動基準が詳細に明示されている。患者に情報取扱方針を通知する義務、患者の権利の明記、TPO（Treatment,Payment and HealtheCare Operations:診療・支払・医療業務管理）における患者の同意不要、情報取扱の具体的ルール、プライバシー保護担当者の必須設定が特徴となっている。HIPPA 法は患者個人をはじめとする個人に対する法体系であり、日本の個人情報保護法が組織中心であるのと対照的なものになっている。

昨年度に遺伝子関連の法制度に関する調査をまとめ、指針の中に暗号化が明確に定められていることを示したが、今後、カルテ開示や電子カルテ化の進展を考えると、個人情報保護の観点から、これらの中に暗号化が取り入れられることも考えられる。ここでは、個人情報を取り扱う（暗号化してデータ収集を行い、特定者にのみ特定の情報のアクセス権を与える）観点で、医療分野は（1）テーラーメード医療（2）電子カルテ開示　（3）患者満足度向上(4)後発医薬品の使用のための情報収集に関して取り上げる。医療行政に関しては、行政の分野でとりあげることにする。

(i) テーラーメード医療

テーラーメード医療とは、オーダーメード医療、個人別医療とも呼ばれる。近年のヒトゲノム解析の進歩に伴い、遺伝子の個人差によって医薬品の効果や副作用が異なることがわかり、患者にとって最も効果があり、副作用が発現する可能性が最小となるように、患者にあった治療方法を見出し、実践することをテーラーメード医療という。

米国食品医薬品局（FDA）は、2003 年 11 月 3 日に、薬理ゲノム（ファーマコジェノミクス）に関するガイダンス案を発表、企業の新薬臨床試験開始申請（IND）や、新たな販売認可申請（NDA）、生物製剤承認申請（BLA）において、必要となる薬理ゲノムのデータをまとめた。これにより、治験参加者の遺伝子解析が一般化すると考えられている。FDA は 2002 年末、特定薬剤に対し、遺伝子検査を推奨する文書を加えて市販するよう求めた（メルカプトプリン、日本では未販売）。これはある特定遺伝子を持つ人間には重篤な副作用を示すことが明らかになっている薬品であるが、それ以外の人間に対する有効性から薬品として認められた。アメリカでは実際にオーダーメード薬が市販されているのである。このようなオーダーメード薬市販されるようになれば、副作用を怖れる患者は遺伝子検査を求めることになると考えられる。

また、2003 年 10 月 10 日、米ゼネラル・エレクトリック（GE）は、英国の医療診断・解析システム大手アマシャムを買収した。その目的は GE が強い画像診断装置にアマシャムが得意な遺伝子解析システムや試薬を融合させ、遺伝子レベルで薬効を予測して薬を処方するテーラーメード医療をにらむためという。GE の医療機器部門とアマシャムを合わせた事業規模は年間 130 億～140 億ドル、日本では 15 億程度と試算している（日経新聞 2003 年 10 月24日）

日本においては、上記のようなファーマコジェノミクスに対する取組みはあまりされていないが、今後の世界の趨勢として、捉えておく必要がある。

日本では遺伝子と個人情報に関連する法案は特に無く、昨年度まとめたように倫理指針において、匿名化が定められている。しかし、厚生労働省は、医療分野の個人情報を保護するための個別法制定を検討する第三者機関を2004年4月中に設置し、今秋までに一定の結論を出すとの方針を個人情報保護関係省庁連絡会議に報告しており、特にその内容には遺伝子を巡る医療研究とプライバシー保護の兼ね合いなどが焦点になっているという。（日刊工業新聞 2004年04月08日 ）

厚生労働省は、「対がん10カ年総合戦略（昭和59年度～平成5年度）」及び「がん克服新10か年戦略（平成6年度～15年度）」により、「がんは遺伝子の異常によって起こる病気である」という概念が確立し、遺伝子レベルで病態の理解が進む等がんの本態解明の進展とともに、各種がんの早期発見法の確立、標準的な治療法の確立等診断・治療技術も目覚ましい進歩を遂げた」として、平成16年度からの新たな10か年の戦略について、がんの罹患率と死亡率の激減を目指して、「第3次対がん10か年総合戦略」を定めた。

「第3次対がん 10 か年総合戦略」の戦略目標の課題解決には癌治療の個別化「テーラーメード医療」の確立・普及がポイントになると考えられる。

遺伝子データと個人情報のリンクに関しては、現状は倫理指針において定められるもののみであるが、今後のオーダーメード医療の進展に伴い、研究段階から実際の医療の現場に入った際のデータ管理、データ収集、また、患者からの開示要求に対する対応などにおいて、データアクセス権限、暗号化と復号化、データ集計の処理に本研究が生かされると考えられる。

(ii) 電子カルテ

政府は「医療制度改革大綱（平成13年11月29日）」において、電子カルテに関して次のようなまとめを行っている。

- 電子カルテ・レセプト電算化などの医療のIT化の推進
- 電子カルテ等について目標と達成年次を年内に策定し、その実現に向けた支援措置を講じる。

2003年5月29日、厚生労働省医政局の「診療に関する情報提供等の在り方に関する検討会」は最終報告書（案）は、患者と医療従事者が診療情報を共有し、患者の自己決定権を重視するインフォームド・コンセントの理念に基づく医療を推進するため、患者に診療情報を積極的に提供するとともに、患者の求めに応じて原則として診療記録を開示すべきであるという基本的な考え方を示した。先に述べたように「診療情報の提供等に関するガイドライン」案は 9 月に「診療情報の提供等に関する指針」として通知されたが、同検討会では、カルテ開示についての個別法による法制化については、国会で成立した個人情報保護法等（公布後 2 年以内施行）により、患者本人からの請求に応じてカルテ開示などを義務付けているため、法制化については見送っている。本件に関しては、個別法制定に関する動きの中で、再度何らかの形で出ることも考えられる。

「診療情報の提供等に関する指針」では、医療従事者および医療機関の管理者ら医療従事者等と患者等とのより良い信頼関係を構築することを目的に、医療従事者等が本指針に則って積極的に診療情報を患者等へ提供することを促進するものであり、「診療情報の提供」と「診療記録の開示」を定めている。

「診療情報の提供」	医療従事者が診療の過程で知り得た患者の身体状況、病状、治療等の情報を、(1)口頭による説明、(2)説明文書の交付、(3)診療記録の開示等、具体的な状況に即した適切な方法により患者等に対して提供すること
「診療記録の開示」	診療録、処方箋、手術記録、看護記録、検査所見記録、X 線写真、紹介状、退院した患者に係わる入院期間中の診療経過の要約その他の診療の過程で患者の身体状況、病状、治療等について作成、記録または保存された書類、画像等の記録を患者等の求めに応じ閲覧に供することまたはそれらの写しを交付すること

上記の診療記録の開示を求め得る者は原則として患者本人であるが、本人以外でも開示を求めることができるケースがある。

(1) 患者に法定代理人がいる場合には法定代理人。(ただし、満 15 歳以上の未成年者については、疾病の内容によっては患者本人のみの請求)
(2) 診療契約に関する代理権が付与されている任意後見人。
(3) 患者本人から代理権を与えられた親族およびこれに準ずる者。
(4) 患者が成人で判断能力に疑義がある場合は、現実に患者の世話をしている親族およびこれに準ずる者。

医療従事者等は、診療情報の提供や診療記録の開示が患者本人または患者周辺の状況から好ましくないと判断した場合は、それを拒むことができるが、その場合、診療従事者等は、原則として、申立人に対して文書によりその理由を示す必要がある。

今後の電子カルテ推進の動きの中で診療記録の開示についても同時に考える必要があり、電子データの取扱として、行政からの要請による情報収集(疫病などの報告義務)、本人および代理人からの開示要求、研究データとしての情報集計など複数のレベルにおいて、個人情報の公開、匿名化の範囲を定めデータを運搬する必要があると考えられる。

先に述べたテーラーメード医療とのかかわりで、遺伝子情報を含む場合には、明確に定義された匿名化処理が必要になり、電子カルテと、それら遺伝子情報・個人情報のデータの取り扱いに、本研究が応用できると考えられる。

(iii) 患者満足度向上

企業における CS 向上と対応する PS(患者満足度)の向上、患者の生活の質(QOL)向上を掲げる医療機関がでてきている。

東京都では、「医療のより良い関係を考える会」が 2003 年 7 月「医療のより良い関係に向けた提言－納得と信頼の医療をめざして－」をまとめ、『患者中心の医療』を提言している。

患者自身の意識が大きく変わり、病院を自ら選択する方向に向かっており、雑誌のランキングやインターネットでの調査などを積極的に行うようになってきている。

医薬卸大手クラヤ三星堂の CS センターでは患者満足度調査を行っており、自社で作成した調査票を医療機関に送って患者に自宅で答えてもらい、この結果を分析して作成した報告書を医療機関に送り返すサービ

スを行っている。病院が実施している患者向け調査にくらべて客観性があり、評価結果を基に職員にサービス向上を促す医療機関も多いという。（日経産業新聞 2003/6/17）

自分がかかっている病院への評価は患者側の抵抗があり、なかなか本音が聞けないということもあり、上記 CS センターでの調査はなかなか人気であるという。匿名での収集・集計が簡単に可能にできれば、病院独自の PS のためのアンケートを行い、それを経営に役立てることができるようになると思われる。

患者満足度に関しては、各種コンサルタントでも分析サービスを含めてメニューとして出しているが、経営に反映させるのであれば、継続的に実施し、それを随時反映させる必要がある。また、病院での ISO9000 取得の流れを考えると、単発での実行ではなく、継続的に行うことがますます求められることになる。このためには、自システムにとりこむか ASP サービスなどで、セキュリティを確保しながら安価に手軽に導入できるシステムが必要になるだろう。

また、病院経営という立場から考えると、企業における「従業員満足度向上」と同様に施設に携わる医療従事者の職員満足度向上も考えていく施設が増えていくのではないかと考えられる。

（iv）後発医薬品

後発医薬品とは、先発医薬品の特許が切れた後に、先発医薬品と成分や規格等が同一であるとして、臨床試験などを省略して承認される医薬品（ジェネリック医薬品）のことを言う。

日本では、2002 年4月の診療報酬改定により，医療機関において後発医薬品を含んだ処方せんを発行した場合の処方せん料や、薬局において後発医薬品の調剤を行った場合の調剤料について、先発医薬品のみの場合よりも高い評価を行うことになった。これは医療保険財政の効率化を図るものである。患者の医療費負担が 2 割から 3 割に引き上げられ、負担が増加し、院外薬局を通して後発品を処方した場合に医療機関が診療報酬を受けられる（政府の後発医薬品使用促進政策）ことになったことから、後発医薬品へのシフトが進んでいる（2003 年 3 月末の国立病院・療養所の占める後発品の割合が 6.5%で、2002 年 9 月末にくらべ 1.2 ポイント増加している）。

世界ジェネリック医薬品協会によると 2002 年度の医薬品市場は、アメリカ、イギリス、ドイツではジェネリック医薬品の処方箋が医療用医薬品の 50%以上を占め、また、ジェネリック医薬品の後進国であったフランス、イタリア、スペインは政府の啓蒙キャンペーンもあり昨年から急速にシェアを伸ばしたが、日本のみ例外的に水準が低いとしている。医薬工業協議会によると日本の後発品のシェアは 1 割程度であるという。

アメリカでは、ほぼ完全な医薬分業で、法律により代替調剤（医師が処方した医薬品を、薬の専門家である薬剤師が品質とコストを考慮し、患者の同意の上で同一成分の他の名称の医薬品に替えることが認められている制度。欧米では一般化しているが日本では認められていない。）が認められているため、患者が先発医薬品と後発医薬品の選択を行うことができる。アメリカでは日本のような全国民を対象とする公的な医療保険制度は無く、大多数の国民は「マネジドケア」と呼ばれる民間医療保険に加入しているが、この民間医療保険で同一クラスの処方薬間で自己負担額に差を付ける「段階式自己負担制度」の導入が進んでおり、自己負担額が細分化されると後発医薬品への切り替えが進むというデータがある。

日本では代替調剤が認められていないが、病院によっては、患者が先発品か後発品かを選択できるようにしているところもあり（長野県下伊那厚生病院）、後発品の選択という意味で、医薬品メーカーや卸などによる医師・薬局・患者自身に対する後発医薬品選択のアンケートが考えられるだろう。

後発医薬品と先発品での選択基準の把握のほか、効果・満足度の把握にも使用できる。政府方針で健康保険料の低減のための後発品促進を行うのであれば、地方自治体など官側からの後発品使用状況確認が行われることも想定される。

5-1-3-3　教育分野

教育分野における個人情報の取扱に関しては、従来は各地方自治体の定める個人情報保護条例や地方公務員法第34条(守秘義務)等が関連する法であったが、今後、個人情報保護関連5法のうち「行政機関個人情報保護法」に従うものとなると考えられる。

アメリカでは、1974 年教育修正法で「家族の教育上の権利およびプライバシー法(Family Educational Rights and Privacy Act; FERPA)」が追加され、連邦の教育に関する法律の中で，親の権利が初めて明文化されたものとなっている。本法は学生の学歴記録の機密保持に関わる法律であり、下記が定められている。

- 教育機関が保持している記録の開示には生徒または親の同意が必要であることを明示
- 生徒が、自身の学歴記録へアクセスでき、訂正や個人情報の開示の中止を求める権利を認める
- 政府機関が学歴記録にアクセスする方針や複写を入手する権利を認める

日本の場合、内申書に関しては開示の方向にあるが、文部科学省はもともとこれらの情報は非公開であり、開示にあたっては慎重を期し、各自治体の判断にまかせるという態度を取っており、公開はあまり進められていないのが実情であった。個人情報保護法では、本人の開示要求に対しては公開するのが原則であり、今後の方針に関しては注目が必要である。

本分野での利用分野検討として、授業業評価とe-ラーニングを取り上げる。

(i) 授業評価

国立大学の大学法人化に伴い、独自の学部運営が重要になり、教員の評価が不可欠になると見られる。企業における「顧客満足」、先にみた医療における「患者満足」、また後に述べる行政における「市民満足」同様、学校においても学生を顧客と捉えた「学生満足」の観点が重要になってくると考えられる。近年は、サービスを受ける側の満足度向上からサービスを行う側の満足度、「従業員満足度」に関しても重視されるようになってきているが、ここではまず授業評価に関する現状と今後について検討してみたい。

大学、高専などの高等教育において、教育改革の一環として、FD活動が積極的に行われるようになってきている。FDとはファカルテイ・ディベロップメント(Faculty Development)の略で、「授業の改善等、教官の教育に対する資質の向上を図ること」を意味する組織的な取組みをさす。広義には教育機関の自己評価機能の開発や研究機能の開発、教育機能の開発、教員人事機能の適正化、管理運営機能の開発を含む多義的な概念であるが、日本では教育の質的向上を目指すものとして捉えられているようである。
(米国大学 Faculty Development 調査報告)

この FD の中に、授業評価も含まれる。

学生による授業評価に関しては、既にいくつかの大学では取り入れられ、ホームページでの公開も行われている。また、授業評価に関しては、評価作業を請け負う業者も現れているという。学生の満足度という尺度によって、授業の善し悪しを決めてしまう問題点に関しては、「学生による授業評価をどう見るか(2001、渡辺)」が、消費者モニターとの比較でまとめている。

アンケートの公開に関しては、熊本大学医療技術短期大学部の平成13年度授業に関するアンケート用紙等の一部開示決定に関する件(平成14年諮問第359号)において、「行政機関の保有する情報の公開に関する法律」3条の規定に基づく本件対象文書の開示請求に対して本大学長が行った不開示決定について，部分開示の変更を求める異議申し立てに対し、5条1号、6 号に基づく非開示情報として妥当であったという諮問委員会の見解を示している。「行政機関の保有する情報の公開に関する法律」5 条は、不開示情報とその例外を示している。

（行政文書の開示義務）
第五条　行政機関の長は、開示請求があったときは、開示請求に係る行政文書に次の各号に掲げる情報（以下「不開示情報」という。）のいずれかが記録されている場合を除き、開示請求者に対し、当該行政文書を開示しなければならない。
一　個人に関する情報（事業を営む個人の当該事業に関する情報を除く。）であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む。）又は特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの。ただし、次に掲げる情報を除く。
イ 法令の規定により又は慣行として公にされ、又は公にすることが予定されている情報
ロ 人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報
ハ 当該個人が公務員等（国家公務員法（昭和二十二年法律第百二十号）第二条第一項 に規定する国家公務員（独立行政法人通則法（平成十一年法律第百三号）第二条第二項 に規定する特定独立行政法人及び日本郵政公社の役員及び職員を除く。）、独立行政法人等（独立行政法人等の保有する情報の公開に関する法律（平成十三年法律第百四十号。以下「独立行政法人等情報公開法」という。）第二条第一項 に規定する独立行政法人等をいう。以下同じ。）の役員及び職員並びに地方公務員法（昭和二十五年法律第二百六十一号）第二条 に規定する地方公務員をいう。）である場合において、当該情報がその職務の遂行に係る情報であるときは、当該情報のうち、当該公務員等の職及び当該職務遂行の内容に係る部分
二　法人その他の団体（国、独立行政法人等及び地方公共団体を除く。以下「法人等」という。）に関する情報又は事業を営む個人の当該事業に関する情報であって、次に掲げるもの。ただし、人の生命、健康、生活又は財産を保護するため、公にすることが必要であると認められる情報を除く。
イ 公にすることにより、当該法人等又は当該個人の権利、競争上の地位その他正当な利益を害するおそれがあるもの
ロ 行政機関の要請を受けて、公にしないとの条件で任意に提供されたものであって、法人等又は個人における通例として公にしないこととされているものその他の当該条件を付することが当該情報の性質、当時の状況等に照らして合理的であると認められるもの
三　公にすることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあると行政機関の長が認めることにつき相当の理由がある情報
四　公にすることにより、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがあると行政機関の長が認めることにつき相当の理由がある情報
五　国の機関、独立行政法人等及び地方公共団体の内部又は相互間における審議、検討又は協議に関する情報であって、公にすることにより、率直な意見の交換若しくは意思決定の中立性が不当に損なわれるおそれ、不当に国民の間に混乱を生じさせるおそれ又は特定の者に不当に利益を与え若しくは不利益を及ぼすおそれがあるもの
六　国の機関、独立行政法人等又は地方公共団体が行う事務又は事業に関する情報であって、公にすることにより、次に掲げるおそれその他当該事務又は事業の性質上、当該事務又は事業の適正な遂行に支障を及ぼすおそれがあるもの
イ 監査、検査、取締り又は試験に係る事務に関し、正確な事実の把握を困難にするおそれ又は違法若しくは不当な行為を容易にし、若しくはその発見を困難にするおそれ
ロ 契約、交渉又は争訟に係る事務に関し、国、独立行政法人等又は地方公共団体の財産上の利益又は当事者としての地位を不当に害するおそれ
ハ 調査研究に係る事務に関し、その公正かつ能率的な遂行を不当に阻害するおそれ
ニ 人事管理に係る事務に関し、公正かつ円滑な人事の確保に支障を及ぼすおそれ
ホ 国若しくは地方公共団体が経営する企業又は独立行政法人等に係る事業に関し、その企業経営上の正当な利益を害するおそれ

本諮問においては、下記の論点で当該教官名、教科名に関しては不開示を妥当としている。

・授業評価に関するアンケート実施という事務の性質上，法5条6号の「その他当該事務又は事業の性質上，当該事務又は事業の適正な遂行に支障を及ぼすおそれ」があり不開示情報に該当する
・アンケートによる授業評価自体は，授業担当教官の個人に関する情報であって，個人を識別できる情報である。
・本件アンケートが試行的に行われたものであり当該教官の氏名を公表することを予定してされたものではない
・各大学における学生による授業評価については，現時点において，担当教員の氏名を一般に公表する慣行があるとまでは認められないことから，授業評価に係る教官の氏名は，慣行として公にされ又は公にすることを予定しているものとは言えず、当該教官の氏名は法5条1号ただし書イには該当せず，同号の不開示情報に該当する。
・授業科目名等に関しては、シラバス等から特定教官の個人氏名を識別できる情報である

本申し立てでは、アンケートに関する開示について異議申し立て人から「自己点検評価は結果が公表されることを前提としたものであり、調査事務に支障をおよぼすおそれのある内容が含まれるのであればアンケート調査自身が公正に実施されているとはいえない。回答者が不利益を被らないよう配慮されて実施されるべきでものであり、そのために無記名のアンケート調査を行っていると考えれば，学生の氏名の保護は行われているといえる。公表しないことを前提に実施しているのは学生の保護についてであり，その意味では学生が特定されなければ保護できるのである」としている。

ここでは、アンケート回答者についての個人情報に関しては、無記名であるという点で保護されているとし、アンケート内容に含まれる個人情報の取扱に関して問題が提示されている。アンケート内容に含まれる個人情報の取扱はアンケート調査票の作成方法に関わる問題であり、電子化を想定した場合にはアンケートシステムそれ自体の問題ではない。電子投票では、候補者自身が公知された内容であるからそれに対する当落は公開されて問題のないものであるが、そのシステムを特定多数による評価システムとして展開する場合、評価される対象が個人である場合に、その個人の評価をどこまで公表するか、という問題もでてくるということになる。

学生のアンケートによる授業の評価を大学での教授に対する業績評価のポイントとしている大学が欧米にはあり、授業評価の流れが日本でもそのような個人の業績評価につながるようになった場合、その内容の開示範囲については、十分検討する必要があると考えられる。

(ii) e-ラーニング

教育分野を市場として考えた場合、最も成長性の高い分野として e-learning があげられる。総務省のまとめた情報通信白書(平成 14 年)では、平成 13(2001)年度における e ラーニング市場は 290.0 億円と推計され、平成 18(2006)年度には、1,984.6 億円と、約 7 倍に増加すると予想している。白書では、e ラーニングを、代表的な運営形態である「インターネット(ここでは、TCP／IP プロトコルを活用したネットワーク通信の意味)を活用したネットワーク通信を使用するウェブベースのシステムを中心的に使用した教育／学習システム(WBT：WebBased Training)」と定義している。広義には、CD-ROM 等を活用するもの(CBT：Computer Based Training)やテレビ、ラジオ、通信衛星、携帯電話等を活用するものを含む場合がある。

gooリサーチでは、2002 年からビジネスにおける e ラーニングの利用に関する調査を行っており、2003 年度結果からは、e-ラーニングが企業研修として積極的に取り入れられている様子がうかがえる。

e-ラーニングは、高齢化にともなう、生涯学習や資格取得のためや、少子化にともなう幼児教育の進展に大いに関わるようになると考えられる。先の情報通信白書では、平成 13(2001)年度は、学校教育市場が 20.6 億円、企業内教育市場が 82.9 億円、生涯教育市場が 186.5 億円で、各市場の構成比では、生涯教育市場が 64.3%と全体の 3 分の 2 を占めており、生涯教育市場も順調に拡大するが、平成 18 年には生涯教育市場と学校教育市場が逆転すると予測している。

2002年10月に発表されたIDC Japan 株式会社の「国内IT教育・Eラーニング市場規模予測と動向」によると、今後 IT 教育サービス市場は安定して成長、中でも e-ラーニング市場は急成長する。 しかし、急激に拡大しつつある市場の中で生き残るには「通常の研修とe-ラーニングを組み合わせたブレンド型教育や、ユーザー企業、教育機関、専門学校との提携・共同開発が必要」で、「より踏み込んだコンサルティングやメンターサービス、教育業務のアウトソーシングサービスを取り入れることが発展のカギになるだろう」とも予測している。

e-ラーニングにおけるメンターサービスとは、受講者に対し学習サポートを行う要員がつき、学習指導を行うサービスを言う。受講者ごとに個別サービスを行う上で、満足度の向上や秘密保持が重要なファクターとなることは言を俟たない。

こうした個別サービスによる差別化、顧客満足の測定には、下記の技術が必要になると考えられる。

- インターネットを使用した個人認証と内容の暗号化技術
- アンケートにおける、回答者自身の個人情報の剥奪（回答者の心理的負担の軽減と、個人が特定されることにより回答内容に対してバイアスがかかることを防ぐ）

5-1-3-4　行政分野

政府の e-Japan 構想は平成 15 年度中の LGWAN 導入を求めており、地方自治体での電子化が進められている。「e-Japan 重点計画－2003」に掲げられた施策の推進状況の調査報告では、2003 年 11 月現在、都道府県 47、政令指定都市 13、市町村 2587 の計 2647 団体が接続済みという報告をだしている。平成 15 年 7 月に e-Japan 戦略 II が決定され、2004 年 1 月には e-Japan 戦略 II 加速化パッケージが策定された。ここでは、セキュリティ正確の強化とともに、電子政府・電子自治体の推進があげられている。

こうした電子化の流れの中で、自治体の中では、電子アンケートや投票システムにより、行政の政策形成、判断や行政評価のために不特定多数の住民に対し意識調査を行ったり、場合によっては明確な意思表示を求めようという動きがある。

自治体の財政再建や行政改革を進める必要性から、多くの自治体において『行政評価』への取組みが盛んになってきている。行政評価のシステム自体、確立されたものは無く、ISO9000 を行政評価のツールとして導入を検討する自治体が増えてきており、ここで市民満足度の向上が目標としてあげられるようになってきている。

また、急速な高齢化とがんや糖尿病など生活習慣病の増加などに対応するため、これまでばらばらだった健康診断の実施方法を統一するなど生涯を通じた健康管理のあり方などを規定した健康増進法が、2003年5月施行され、行政による健康情報の調査が定義され、地域福祉計画、医療制度改革とあわせ、将来的には広域の保健・医療ネットワークを想定した取組みが進められている。

ここでは、電子アンケート利用分野として、市民満足度調査と医療行政を取り上げる。

(i) 市民満足度調査

地方分権一括法が施行され、地方分権が実行の段階を迎え、地方公共団体の厳しい財政状況から、行政改革の推進手段として行政評価が導入されてきている。「平成14年度地方公共団体における行政評価についての研究会報告」によれば、平成 11 年度から 14 年度に地方自治体の行政評価導入状況は下表のように増加しており、市区町村では都道府県等と比べ取組みは緩やかであるが、「検討中」まで含めれば 1,025 団体から 2,086 団体に増加しているという。報告では、1) 予算、組織に反映させる等の行政評価の活用、2) 行政外の専門家や住民等の視点と協働、3) 評価システムの総合的、体系的な構築、という3点の課題への対処が今後の行政評価の普及、発展の鍵となるとしている。

表 10　地方自治体の行政評価導入状況

	「導入済み」又は「試行中」(H11 から H14)	平成 14 年取組み		
		政策	施策	事務事業
都道府県	26→46 団体	16 団体	33 団体	44 団体
政令指定都市	3→12 団体	5 団体	8 団体	12 団体
市町村	95→515 団体	79 団体	161 団体	491 団体

事務事業評価はゴミ収集、水道、道路メンテナンスなどのサービス行政について、コスト管理による業務の効率化を図ることであるが、これに比べると政策評価の実施状況が少ない。

政策評価とは、住民の満足度に注目し、満足度がどれだけ向上したかを具体的な指標に置き換えて、政策・事業の効果を測ることであり、道路整備における渋滞時間の減少や窓口サービスにおける待ち時間の減少などがあげられるが、こういった指標が実際に市民の満足度に合致したものであるか、その度合いがどれだけのものかというものが、行政がわの独りよがりにならないようにしなければならならない。満足度の向上という意味では、市民が最も求めているサービスを行うのでなければ、効果が得られない。このためには、市民に対するアンケートなどを行い、求められているものが何か、実際に効果がどうであったのかを測定する必要があるだろう。

行政評価システムが確立されたものでないため、その確立が今後の課題として上記報告にもあげられるれているが、その中で ISO9000 を行政評価のツールとして考える自治体も増えてきているという。JQA による地方自治体の ISO 導入状調査(「地方自治体と ISO マネジメントシステム及び行政評価について」平成 13 年 11 月調査)によれば、ISO9000 に積極的な自治体(「導入済み」「導入準備段階」及び「導入検討中」)はアンケート回答の 6.3%の 15 市であったが、上記行政評価の導入の増加を考えると、地方自治体における ISO9000 に対する取組みは増加していると思われる。JQA の ISO9001/JIS Q 9001 の登録「市役所」「町役場」の検索(1990～2004 年 4 月)では 16 件ヒットする。2002 年以降の登録が多く、導入準備・検討している市町村も多いのではないかと考えられる。

ISO9000 では PDCA サイクルによるマネジメントシステムや継続的改善、顧客満足を求めている。行政においては、市民満足度の測定が顧客満足にあたるものと考えられる。

アンケート方法に関しては、無作為抽出した市民に対し、郵送で調査票を送付・回収したり、市民モニターを設定して定期的なアンケートを行ったりというものがあり、アンケートの目的により方式を選択することになる。次世代の電子投票システムが転用できれば、全市民を対象して個人認証とセキュリティに考慮されたアンケートが可能となり、行政評価のシステムとして取り入れることができると考えられる。

(ii) 医療・健康行政

医療・健康行政においては、個人の診療情報や健康情報が流通するため、その情報の取扱に注意する必要がある。

たとえば、医療に対する法令に則って施行されているかの監督や、行政的な監査、感染症の届出、個別の疾患などによる報告などにおいて診療情報が使用されるケースがある。診療情報に関しては、電子カルテの導入と合わせて、その電子データ利用という観点で、個人情報保護法および医療関連法令に基づき、個人情報の保護と開示の両方で対応をとらなければならない。たとえば、「精神保健及び精神障害者福祉に関する法律 」における都道府県知事への届出、精神医療審査会への情報提供、医療機関の無断退去者に関する警

察への通報義務や「身体障害者福祉法」、「児童福祉法」における自治体の更正相談、療育指導、医療給付など、医療機関と自治体での診療情報の流通が存在する。

また、「感染症の予防及び感染症の患者に対する医療に関する法律」では感染症に関する情報収集及び公表について定められているが、行政では、感染症の他、大規模事故や天災などを含む傷病の把握・対応とともに、予防という観点からも対応が必要になる。

急速な高齢化とがんや糖尿病など生活習慣病の増加などに対応するため、これまでばらばらだった健康診断の実施方法を統一するなど、生涯を通じた健康管理のあり方などを規定した「健康増進法」が平成 14 年 7 月 26 日に法案が可決成立、平成 15 年 5 月 1 日に施行された。首都圏では、主な私鉄がホームを含めて全面禁煙にしたことで耳目を集めたが、この中には生活習慣の状況に関する調査を加え、国民健康・栄養調査を実施することや、調査に従事した公務員の秘密漏洩に関して罰則規定が設けられている。 生活習慣病の発生状況の把握に努めることが盛り込まれており、住民の健康情報の収集が行われることになる。

「健康増進法」は 21 世紀における国民健康づくり運動（健康日本 21）の法的根拠として提示されたものであり、運動期間は 2010 年度まで、運動の評価を 2005 年度に中間発表、2010 年度に最終評価を行うとしており、各自治体では、方針を決定して運動を推進している。

このような診療情報や健康情報の収集は、先の医療分野であげた、電子カルテやIT化と絡み、電子情報でのやり取りが考えられる。また、市民の健康情報の収集としては、アンケートによる生活実態調査やその集計が考えられ、これが継続的データ収集として地域特性の把握や健康行政への展開への反映に展開されるであろう。地域住民を対象とした場合、手軽に、継続的にデータが収集でき、かつ、健康にかかわるものである以上、本人のプライバシー保護には十分な注意を払う必要があることから、インターネットを利用した任意端末からの収集、データの匿名化が重要になると考えられる。

電子カルテを中心とした地域医療連携のモデルとしては、平成13年度の経済産業省モデル事業として構築された「わかしお医療ネットワーク」が、2003年7月、厚生労働省の「平成14年度地域診療情報連携推進事業成果発表会」で地域における糖尿病診療連携や在宅医療のレベルアップにおける成果を発表している。広域の保険・医療ネットワークとしての一つのモデルである。

以上、医療・教育・行政に関して電子投票に類するアンケート等の利用分野としていくつかのトピックを中心に概観してきた。これらは、選挙における投票の秘密保持という機能からアンケート回答者の個人情報保護および個人認証の部分と関連している。個人情報に関しては 2005 年 4 月に完全施行される個人情報保護法に関して、関連法案が検討されているため、それらに十分注意する必要がある。

今回検討していない信用分野に関しても個別の法制度の検討がされており、その状況により、対応すべき項目が変わってくると考えられる。ISO9000 や顧客満足度というものがどこの分野でも存在しており、電子化が進む現在、電子アンケートの領域の発展の余地はおおきいと考えられる。

5-2　運用形態ごとの要件整理

5-2-1 はじめに

旧自治省の電子・電子機器利用による選挙システム研究会中間報告（自治省 2000 年 8 月）を受けて、「電子機器利用による選挙システム研究会報告書」（総務省 2002 年 2 月）および、その機能要件定義である「電子投票システムに関する技術的条件及び解説」が総務省から発行された。さらに、地方選挙に限り電子投票を可能とする法改正もなされ、電子投票に向けた法制的基盤が固まりつつある。

電子化の段階としては、以下のように分類されている。

- 第一段階:投票所、開票所で電子機器を単体として導入する段階
- 第二段階:投票所間、投票所と開票所をネットワークで接続する
- 第三段階:任意の投票端末による投票

研究報告における機能要件定義では最終的に第三段階が除かれており、第三段階の電子投票の枠組みが組み込まれていない。

第三段階の電子投票システムの研究として、米国の VoteHere, Inc.から発表されている NVSS（Network Voting System Standards）がある。これは、VSS や他の研究プロジェクトの資料、カリフォルニア州の CalTech/MIT 投票技術プロジェクトの報告などをベースにした、VoteHere 社の独自の研究である。

本サブテーマでは、昨年度、この NVSS と「電子投票システムに関する技術的条件及び解説」をベースに調査検討を行い、日本の選挙制度に整合するような第三段階の電子投票システムの具体的なモデルを想定し、その電子投票システムとして有すべき性質についての標準（ドラフト）の策定を目指し、案を提示した。本年度はこの案をサブテーマ３「効率的運用とリスク管理」の成果をもとに見直しを実施している。

これに先立ち、サブテーマ３実施にあたり、サブテーマ５「モデル構築」で示される参照実装モデルで使用されているセキュリティ対策技術を含め、各運用要件の具体的な実装例の提示の充実を図った。（5-3-3 参照実装モデルのセキュリティ対策技術」参照）

5-2-2 要件定義について

5-2-2-1 構成

本標準において、次世代電子投票システムの要件の定義を、「機能要件」、「セキュリティ要件」、「ハードウェア要件」、「ソフトウェア要件」と大きく４つのカテゴリに分類している。それぞれのカテゴリの内容は以下の通りである。

表 11 電子投票システムの要件概要

カテゴリ	概　要
機能要件	次世代電子投票システムが投票の原則である、「公平性」、「可用性」、「完全性」、「投票の秘密性」の条件を満たし、また、投票者にとって投票システムが信頼に足りうることを可能とするための機能についての要件を示す。
セキュリティ要件	次世代電子投票システムに対する様々な脅威に対して、「公平性」、「可用性」、「完全性」、「投票の秘密性」を維持する為の要件を示す。
ハードウェア要件	次世代電子投票システムで用いられるハードウェアにおいて満たされるべき、または満たすべき「可用性」、「安全性」、などの要件を示す。
ソフトウェア要件	次世代電子投票システムを構成するソフトウェアの品質確保のための要件を示す。

次節の「要件定義」において詳説する各要件の解説における記述内容は、以下の内容である。

表 12 各要件の解説項目概要

解説項目	概　要
主旨・内容	本要件の背景、目的、内容などを示す。
実施例	本要件の実施の一例を示す。
法律上の条件との関係	「地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律」や公職選挙法等との関係を示している。解説中の略称については、以下のとおり。 特例法…地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律 特例令…地方公共団体の議会の議員及び長の選挙に係る電磁的記録式投票機を用いて行う投票方法等の特例に関する法律施行令 法…公職選挙法 令…公職選挙法施行令
留意事項	本要件を適用する際に留意すべき事項や、関係する他の要件について示す。
参考	他に参考とすべき資料などについて示す。

5-2-2-2 用語

本標準の要件定義において使用する用語の定義は以下のとおり。また、公職選挙法の条文の第ｘ条に関連する場合には、「法ｘ条」と表している。特例法についても同様に、「特例ｘ条」としている。

（1）人・組織関連

表 13 人・組織関連用語

用語	定義
選挙管理委員会	選挙実施の管理・運営をおこなう組織
選挙人	選挙当日に選挙権を有する者で選挙人名簿に登録されている者
選挙長／選挙分会長	候補の受付や選挙ごとに置かれる選挙会に関する事務を担任する者（法 75 条等）
投票立会人	投票所において投票に立ち会う者（法 38 条）
投票管理者	投票所において投票に関する事務を担任する者（法 37 条）
開票立会人	開票所において開票に立ち会う者（法 62 条）
開票管理者	開票所において開票に関する事務を担任する者（法 61 条）
選挙立会人	選挙会に立ち会う者（法 76 条）

（2）投票関連

表 14 投票関連用語

用語	定義
選挙人情報	選挙人名簿をもとに作られた情報。選挙人の確認や投票済みの記録などに利用する。
開票集計	投票データをカウントし選挙毎に候補者の得票数の集計を行うこと。白票が許容されるシステムでは、白票も白票としてカウントする。
投票データ	選挙人が投票用紙から候補の選択を行った内容を含む、システムで1票と認識される情報、または複数の投票データの総称
投票用紙	選挙人が投票を行う際の画面様式や候補者情報、候補者の選択方法などを含む情報
集計設定情報	投票データから集計を行う際に必要となる投票用紙の属性情報など
選挙人識別情報	選挙人がその人本人であることを識別することが可能である、PKI に基づく本人認証を行う為の情報
集計情報	投票データを開票集計した結果情報。
投票用紙の作成	議会等により規定された投票画面の様式をもとに、電子投票システムで処理可能な投票用紙を作成すること
投票用紙の承認	作成した投票用紙の画面様式などを確認し承認を与えること

(3) 共通、その他

表 15 共通、その他用語

用語	定義
電子投票システム	通信ネットワークを介し遠隔地の任意の場所の投票端末から電子的な投票を受け付け、開票集計を行うシステム。投票端末には一般のパソコンなどを使用する。
選挙人情報	選挙人名簿をもとに作られた情報。選挙人の確認や投票済みの記録などシステム内で利用する。
イベントログ	投票システムで発生したイベントの記録であり、後で訴追を受けた場合などで法律的に有効と認められるものであるもの
操作ログ	電子投票システムを誰がどのように操作したかが分かる記録
選挙データ	選挙において、電子投票システムの入出力が行われたデータや操作ログ、監査ログなど、後から選挙の再現が可能となる情報の総称
選挙データの写し	選挙データを複写したもの。障害時の復旧を目的としたものではなく、監査ログと同様な位置付けにある。
監査情報	イベントログ、選挙データの写しを含む、監査記録として有効な情報の総称
コミットメントデータ	投票データや集計値の正当性を証明するために使用される検証データ
電磁的記録媒体	電子的方式、磁気的方式、その他人の知覚によっては認識することのできない方式で作られる記録であって、電子計算機による情報処理のように供されるものに係る記録媒体をいう。
GUI（ Graphical User Interface）	ウインドウやアイコンなどの画像を表示し、マウスやタッチパネルなどでコンピュータを操作する初心者でもわかりやすいインターフェースのこと。
構造化プログラミング	プログラムを処理機能単位に分割して設計することにより、構造を明確にするプログラム設計手法。プログラムの構成がわかりやすくなり、デバッグ（プログラムの誤りを見つけ、修正すること）やアップデートしやすくなるというメリットがある。
モジュール	処理機能によって分割されたプログラム単位。
漏えい	情報の所有者が意図しない相手に情報を知らせること。
改ざん	投票データ、及び、管理上のデータを不正に書き換えること。
二重投票	同一の選挙人が、一つの選挙において、二つ以上の票を投じること。
暗号	復号鍵を所有する相手だけに情報が伝わるように、情報を交換すること。あるいは、そのように変換された情報のこと。
粉塵	機器に悪影響を与えるおそれのある微粒子。
UPS（無停電電源装置）	バッテリやコンデンサなどに蓄えられたエネルギーを使って、停電や電圧降下からコンピュータ等の機器を守る装置。
サージアブソーバ	異常電圧等を吸収し、電子機器を保護する装置・器具。
耐タンパ性記録媒体	改ざんなどの不正行為対策を施した記録媒体。
クラッキング	他人のコンピュータのデータやプログラムを盗み見たり、改ざんや破壊などを行なったりすること。
XML(eXtensible Markup Language)	W3C によって標準化されている拡張可能なマーク付け言語
DTD(Document Type Definition)	XML 文書の論理的な構造を定義する言語

5-2-3 要件定義

各カテゴリごとに、次世代投票システムに必要となる具体的な要件を定義した。

（1）機能要件

機能要件は、必要とされる機能についてそれぞれ投票前、投票中、投票後に分けて記述する。

（a）投票前要件

表 16 投票前要件

大項目	中項目	小項目	要件内容
1．システムテスト	1．システムテスト機能	1．システムテスト機能	1．電子投票システムは、システムが正常に動作することを確認できる機能を有すること
		2．テストの影響	1．システムテストは、選挙の結果にいかなる影響も与えてはならない
2．投票用紙形式の作成	1．投票用紙形式の作成機能	1．作成	1．投票用紙形式などの選挙毎に異なる情報は設定可能であること
			2．電子投票システムは、投票用紙　形式を作成する機能を有すること
		2．投票用紙の様式	1．定められたとおりの様式の投票用紙形式を作成できること
	2．アクセシビリティ	1．インターフェイス	1．投票用紙形式を表示するGUIは、投票者にわかりやすいインターフェイスであること
		2．バリアフリー	1．投票用紙形式は、アクセシビリティに関するオプションを指定できるべきである
3．投票用紙形式の承認	1．承認	1．レビュー	1．投票用紙形式のレビューおよび認証を行うことができること
		2．完全性	1．承認済みの投票用紙形式は、それが承認済みであることを反駁なしに証明可能でなければならない
			2．承認済みの投票用紙形式は、承認されてから変更されていないことを反駁なしに証明可能でなければならない
			3．承認済みの投票用紙形式を変更する場合は、再度承認されなければならない
	2．登録	1．投票用紙形式の登録	1．電子投票システムは、投票受付システムに投票用紙形式を登録する機能を有すること
			2．投票受付システムに登録できる投票用紙形式は、承認を受けたもののみであること

（b）投票中要件

表 17 投票中要件

大項目	中項目	小項目	要件内容
1. 投票	1. 投票受付の開始	1. 投票受付の開始	1. 票の受付を開始できること
		2. 投票前データの確認	1. 票の受付を開始する前に、ゼロ票確認を行うことができること(運用でも可)
	2. 選挙人識別情報	1. 妥当性確認	1. 電子投票システムは、選挙人識別情報の妥当性を確認する機能を有すること
	3. 選挙人名簿との対照	1. 選挙人名簿システムにアクセスする機能	1. 電子投票システムは選挙人名簿を対照するための機能を有すること
		2. 認証	1. 選挙人名簿アクセス機能は、選挙人名簿システムの真正性を反駁なしに確認できなければならない
		3. 扱う情報	1. 選挙人名簿アクセス機能は、投票を認可するかどうかを決定するのに十分な情報を選挙人名簿システムから取得できなければならない
			2. 選挙人名簿アクセス機能は、受け付けた投票処理が完了したことを選挙人名簿システムに通知できなければならない
	4. 投票の有効性の確認	1. 本人確認	1. 選挙人の本人確認を行なうことができること
		2. 選挙人の有効性	1. 選挙人の有効性を確認できること
			2. 投票資格のない者による投票を阻む手段を有すること
		3. 二重投票の防止	1. 二重投票を防止すること
	5. 有効な投票用紙の発行	1. 有効な投票用紙の発行	1. 複数選挙に対応できること(運用でも可)
			2. 選挙人の持つ権限に応じた投票用紙のみを選挙人に提示する機能を有すること
	6. 画面表示	1. 候補者情報の表示	1. 候補者は定められた様式に従い、表示されること
			2. 候補者情報を表示する際の文字スペースの割り当てやフォントなどを均一にすること
			3. 画面表示から選択する場合には表示画面には全ての候補者情報が表示されること

大項目	中項目	小項目	要件内容
		2. 画面のレイアウト	1. GUIなど利用者が利用しやすいインターフェースを用いること
			2. 投票時の画面上には、余計な情報を表示しないこと
			3. 投票時の画面は、指定した様式で表示されること
		3. 動作状態の確認	1. 投票操作による電子投票システムの動作状態を確認できる手段を有すること
	7. 投票のインターフェース	1. 投票の手順	1. わかりやすい投票手順であること
		2. アクセシビリティ	1. アクセシビリティを考慮したインターフェースを用いること
		3. 投票操作	1. いかなる候補者に対する投票も、操作回数や操作に要する時間に大きな差がないこと
	8. 候補者の選択	1. 選択の有無	1. 表示画面には、選択が行われたかどうかを表示する機能を有すること
		2. 選択の適正さ	1. 候補者の選択について、適正かどうか判断できること
		3. 不当な選択	1. 選挙人の選択が不当である場合、注意を促す機能を有すること
		4. 選択の完了	1. 候補者の選択されていない選挙について通知すること
		5. 最終確認	1. 票を送信する前に、選択内容が確認できること
		6. 選択の変更	1. 票を送信する前であれば、選択内容を変更することができること
		7. 投票しないで終了	1. 投票を実行しないで終了できる機能を有すること
	9. 投票データの作成	1. 選択の記録	1. 書き込み式投票をサポートする場合は、候補者を書き込むことができること
		2. 投票データの作成	1. 管理下にない場所にある投票端末で投票した場合でも、投票データが確実に作成されること
		3. 票の保護	1. 投票データを改ざん、破壊等から保護すること
	10. 投票データの送信	1. 送信の成否	1. 票データ送信の成否を投票者に通知する機能を有すること
		2. 票の保証	1. 票データ送信時、データが改変されないことを保証すること
		3. 票の秘密	1. 票データの送信時、投票内容の秘密・選挙人のプライバシーを侵さないこと
	11. 投票データの格納	1. 格納の成否	1. 票データ格納の成否を投票者に通知する機能を有すること

大項目	中項目	小項目	要件内容
		2. 完全性	1. 票データは格納されてから変更されていないことを証明できること
		3. 複写	1. 電磁的記録媒体に記録された票データを他の記録媒体に複写すること
		4. 投票内容の保存	1. 全ての投票者による投票内容を保存できるよう、電磁的記録媒体は十分な容量を有していること
			2. 電磁的記録媒体に記録される投票内容は、個々の票であること
	12. 投票受付の終了	1. 投票受付の終了	1. 管理者が投票終了の操作を加えた後には、追加的な投票が防止されること

(c)投票後要件

表 18 投票後要件

大項目	中項目	小項目	要件内容
1. 集計	1. 集計の原則	1. 開票所開票の原則	1. 投票受付が終了するまでは、何人も個々の票の内容を取得できてはならず、その他投票行動に影響を与えるいかなる情報も公開、公表されてはならない
		2. 集計漏れの防止	1. 妥当な票データはすべて集計結果に含まれていること
		3. 二重集計の防止	1. 1つの票を二回以上集計してはならない
		4. 仮投票	1. 仮投票をサポートする場合、仮投票による票を適切に集計できること
		5. 複数の集計システム	1. 集計システムが複数ある場合、すべての集計システムからの集計結果を統合できること
		6. 他の投票手段	1. 電子投票システム以外の投票手段からの集計結果と、電子投票システムからの集計結果を統合できること(運用でも可)
	2. 集計結果のレポート	1. 内容	1. 選挙結果に関するレポートを生成する機能を有すること
			2. レポートは、受理されたすべての票データを対象とすること
			3. レポートは、監査情報を含むこと
			4. レポート生成により、選挙データ及び監査情報を破壊・変更しないこと
			5. レポートは投票総数を含むこと
			6. レポートは選挙の結果及び各得票数を含むこと

大項目	中項目	小項目	要件内容
			7. レポートは得票数に含まれない票数を含むこと
		2. 完全性	1. レポートは生成されてから変更されていないことを確認できること
			2. レポートに含まれる項目を生成したシステムコンポーネントを確認できること
			3. 生成されたレポート内容に矛盾がないこと
2. 確認	1. 投票データの確認機能	1. 正確性	1. 格納された票データが投票者の意思を正確に反映していることを確認する機能を提供すること
		2. 投票の秘密	1. 票データの確認時、投票の秘密を侵さないこと

（2）セキュリティ要件

表 19 セキュリティ要件

大項目	中項目	小項目	要件内容
1. 秘密性	1. 投票の秘密	1. しきい値による保護	1. ネットワーク投票システムは、最低でも、しきい値による強度で投票の秘密を保護すべきである(運用でも可)
			2. 選挙管理委員会が、しきい値を指定することができること
			3. しきい値を超える共謀が起きない限り、投票の秘密が保護されること
		2. 信頼された個人の認証	1. しきい値を構成する信頼された個人も認証すること
		3. オープン性	1. 電子申請システムは、処理内容を明朗にするための機能を有するべきである
	2. 個人情報	1. 個人情報の保護	1. 選挙人識別情報を含む、個人情報を保護すること
2. 可用性	1. 可用性の設計	1. 管理下のシステム	1. 施設が管理下にある場合の可用性は、第一世代電子投票システムの可用性を比較の基準とすべきである
		2. 管理外のシステム	1. 施設が管理下にない場合の可用性は、不在者投票システムを比較の基準とすべきである
3. 完全性	1. 選挙データの完全性	1. 選挙データの保護	1. 電子投票システムは、選挙データの許可されない変更を防ぎ、もし許可されない変更が行われたら検出できる機能を提供すべきである。
		2. 改ざんの防止	1. 電子投票システムは、選挙データに対するいかなる改ざんも検出する機能を有するべきである

大項目	中項目	小項目	要件内容
	2. 投票データの原本性	1. 個々の票の保存	1. 投票データを記録する際は、受け付けた票そのものを保存しなければならない
		2. 選挙の特定	1. 投票データから、選挙種別および候補者名を特定できること
		3. 任期中の可読性の確保	1. 当該選挙に係る当選人の任期中、投票データの可読性を保証すること
4. 監査	1. 監査証跡	1. 監査情報の生成	1. 選挙が有効であったことの証拠となる監査情報（選挙データの写し、イベントログ）を生成し保持すること
		2. 監査情報の確認	1. 秘密性に関する要件を侵すことなく、独立して監査情報の正当性と正確性を試験し、確認できること
		3. 監査情報の保護	1. 監査情報は、変更・破壊・偽造から保護すること
		4. 秘密性の確保	1. 監査情報には、本標準の秘密性の要件を侵す情報を含めてはならない
		5. 監査情報の印刷	1. 全ての監査情報を人間が読める形式で印刷する機能を提供すること
	2. 選挙データの写し	1. 選挙データの写しの内容	1. 選挙データの写しには、選挙データとして必要な情報を含んでいること
	3. イベントログ	1. イベントログ	1. 投票システムは、システムが生成する主要なイベント情報を含むこと
		2. イベントログの生成	1. イベントログのレコードは、そのイベントが発生した時刻を特定できる情報を含むこと
			2. イベントログのレコードは、そのイベント発生の操作を実行した個人または個人達の識別情報を含むこと
			3. システムが運用中の間、イベントログ情報は使用可能であること
5. 脅威への対応	1. 人的脅威	1. アクセスコントロール	1. アクセス要求する各個人を識別すること
			2. アクセス要求する各個人の権限を識別すること
		2. アクセスコントロール機能の保護	1. アクセスコントロール機能への未許可アクセスを排除する機能を提供すること
		3. アクセスログの監視	1. すべてのアクセス要求のログをとり要求監視をすること
		4. 物理的なコントロール	1. システムコンポーネントへの物理的アクセスを制限する対策を提供すること（運用でも可）

大項目	中項目	小項目	要件内容
		5．秘密情報の保護	1．選挙の信頼性、投票の秘密を維持するための秘密情報は、可能な限り耐タンパ性を備えたハードウェアを使用すること
		6．通信保護の前提	1．選挙データ伝送時、非認可の変更・発見・暴露を防ぎ、選挙データのセキュリティとプライバシーを維持する設計をすること
		7．ネットワークセキュリティ	1．ネットワークに接続する機器をセキュリティ関連装置・ソフトウェアにより防護すること
		8．人的エラー、ミスの防止と検出	1．人的エラーを防止する対策を施すこと
		9．不正行為の防止と検出	1．不正行為からシステム、選挙データを保護すること
		10．堅牢性の維持	1．最新のセキュリティ対策を維持する機能を提供すること
		11．ソフトウェアの確認	1．システム運用中にソフトウェアの改変の有無を確認する機能を提供すること
		12．セキュリティ管理外のセキュリティ要素	1．システム管理外のセキュリティ要素に対するポリシーを定めること
	2．物理的脅威	1．システム障害	1．オペレーティングシステム及びアプリケーションソフトは安定性のあるものとすること
		2．選挙データ障害	1．システムダウンによる選挙データの消失を防止すること
		3．電源障害	1．停電等により電源供給が絶たれた際の対策を施すこと
		4．自然災害	1．落雷による装置故障及びその他想定される自然災害への対策を施すこと

（3） ソフトウェア要件

表 20 ソフトウェア要件

大項目	中項目	小項目	要件内容
1. 品質管理	1．開発・動作環境	1. 使用OS	1. 使用するオペレーティングシステムは安定性のあるものを採用すること
		2．使用OS、ソフトウェア	1. 使用するOS、ソフトウェアの品質が維持されていること
	2. 開発手法	1. 標準	1. 標準を定め文書化すること
		2. 処理フロー	1. 処理フローの明確化を図ること
		3．プログラミング、コーディング	1. 信頼性の高いプログラミング手法を採用すること
	3. テスト	1．ソフトウェアの正確性の証明	1. ソフトウェアが正確に動作することを保証するためにテストを実施すること
	4．ドキュメント管理	1．ソフトウェアアイテムの証拠書類の保存	1. ソフトウェアを構成する個々の要素（モジュール等）の信頼性を示す証拠書類を保存すること
		2．ソフトウェア開発プロセスの証拠書類の保存	1. ソフトウェア開発プロセスの証拠書類を保存すること
2. 構成管理	1. 構成管理計画	1．構成管理計画の策定と実施	1. 構成管理計画を策定し実施すること
	2．システム変更記録	1. システム変更記録の保存	1. システム変更記録を保存すること

（4） ハードウェア要件

表 21 ハードウェア要件

大項目	中項目	小項目	要件内容
1. 動作性能	1. サーバハードウェア	1. 処理能力	1. 投票受付システムおよび集計システムに使用するハードウェアは、支障のない処理速度を有していること
	2. 電磁的記録媒体	1．記録及び読出し速度	1. 票を記録する電磁的記録媒体は、支障のない記録及び読出し速度を有していること

大項目	中項目	小項目	要件内容
		2．記録及び読出し精度	1．票を記録する電磁的記録媒体は、支障のない記録及び読出し精度を有していること
	3．秘密情報を保持する装置	1．秘密保護	1．秘密情報を保持する装置は、秘匿されるべき情報を保護できるようなハードウェア的な機能を有すること
		2．不正防止の物理的対策	1．秘密情報を保持する装置は、物理的な不正アクセスに対して、十分な堅牢性を有すること
		3．秘密情報の復旧	1．票データを暗号化する場合、復号に使用する秘密情報を保持する装置は、万が一秘密情報が破壊されても復旧する手段を有すること
	4．専用投票装置	1．専用投票装置	1．投票装置として専用ハードウェアを使用する場合は、第一世代電子投票における投票装置のハードウェア要件に従うこと
2．動作環境条件	1．外部環境	1．停電対策	1．停電などにより電源供給が絶たれても、それまでに受け付けた票を消失しないこと
		2．落雷対策	1．落雷による装置故障を避けるための落雷対策を施すこと(運用でも可)
		3．温湿度対策	1．通常考えられる温度湿度条件で問題なく動作すること(運用でも可)
		4．粉塵対策	1．考えられる粉塵による影響への対策を施すこと(運用でも可)
3．保守性	1．故障対策	1．故障時の復旧の配慮	1．故障が発生した場合、迅速に復旧できるような対策をすること(運用でも可)
4．構成管理	1．構成管理計画	1．構成管理計画の策定と実施	1．ハードウェアの構成管理計画を策定し実施すること
	2．構成管理計画の実施に必要な情報	1．構成管理計画の実施に必要な情報	1．ハードウェアの構成管理計画の実施にあたって必要となるであろう情報を明らかにすること
5．装置間接続	1．装置間接続	1．システム内装置に関する技術の開示	1．装置同士が相互に直接または間接的に接続される部位に関する技術は、必要な場合には開示できるようにすること

5-2-4　要件定義内訳

要件には「主旨・内容」として各要件の背景、目的、内容などを示し、また、「実施例」の提示、及び「法律上の条件との関係」として公職選挙法、電磁記録投票法との関連を示した。

最終的に、次世代電子投票の満たすべき性質を表す、全１３８項目からなる要件定義を作成した。本要件定義項目の内訳を、次表に示す。また、各個別の要件の解説については「詳細・補足編」に記述する。

表 22 要件定義項目の内訳

カテゴリ	大項目数	中項目数	小項目数	要件項目数
機能要件－ 投票前要件	３	５	９	１３
機能要件－ 投票中要件	１	１２	３４	４２
機能要件－ 投票後要件	２	３	１０	１８
セキュリティ要件	５	１０	２１	４０
ハードウェア要件	２	６	１０	１０
ソフトウェア要件	５	９	１５	１５
合計	１８	４５	９９	**１３８**

5-3　効率的運用とリスク分析

5-3-1　はじめに

本節では、本年度実装したプロトタイプシステムで実施した性能測定結果をもとに分析した結果を報告する。

さらに、サブテーマ２に記載している運用要件及びサブテーマ５に記載している参照実装モデルのセキュリティ対策技術について調査した結果を報告する。

5-3-2　性能分析

5-3-2-1　性能測定ハードウェア環境

性能測定を実施したプロトタイプシステムのサーバマシンは、センター1サーバ1台とデータベースサーバ1台が互いにネットワーク接続されている環境で、マシンスペックはそれぞれ以下のようになっている。

① センター1 サーバ
- HW モデル名　NEC Express 120 Ra-1
- OS　Windows 2000 Server SP4
- CPU　1GHz × 2CPU
- メモリ　1179MB

② データベースサーバ
- HW モデル名　NEC Express 120 Ra-1
- OS　Windows 2000 Server SP4
- CPU　1GHz × 2CPU
- メモリ　1179MB

5-3-2-2　性能測定条件

今回の性能測定では、最終的に電子投票システムの最大構成要件（投票者数100万人、候補者数1000人）でどのくらいの性能値が出るか確認した。尚、候補者数に比例して暗号ブロック数、つまり暗号票データ容量が増えるため、以下のように候補者数を変化させて性能値の変化が正しいことを確認した。

① センター2OU 公開鍵サイズ
- 1024 ビット

② 投票者数
- 100万人

③ 候補者数
- ～17 名　（1暗号ブロック）
- ～255 名　（15 暗号ブロック）
- ～510 名　（30 暗号ブロック）
- ～765 名　（45 暗号ブロック）
- ～1003 名　（59 暗号ブロック）

5-3-2-3　性能測定結果

電子投票システムには、主として、票データ作成(暗号化)、投票、集計、開票の4つのプロトコルに分類される。そこで、今回それぞれのプロトコル性能を測定することでどこにボトルネックが存在するか分析を実施した。票データ作成(暗号化)、投票、集計、開票について、候補者数を変化させて測定した各プロトコル性能値は以下の結果となった。

暗号ﾌﾞﾛｯｸ数(候補者数)	1ﾌﾞﾛｯｸ(～17名)	15ﾌﾞﾛｯｸ(～255名)	30ﾌﾞﾛｯｸ(～510名)	45ﾌﾞﾛｯｸ(～765名)	59ﾌﾞﾛｯｸ(～1003名)
暗号化(秒)	0.436	6.54	13.08	19.62	25.724
票受付(秒)	22100	48500	62500	85400	117000
集計(秒)	3590	5160	8330	11750	13260
開票(秒)	0.011	0.173	0.349	0.519	0.688
総計(秒)	25690.447	53666.713	70843.429	97170.139	130286.412

図 10　性能測定結果(数値データ)

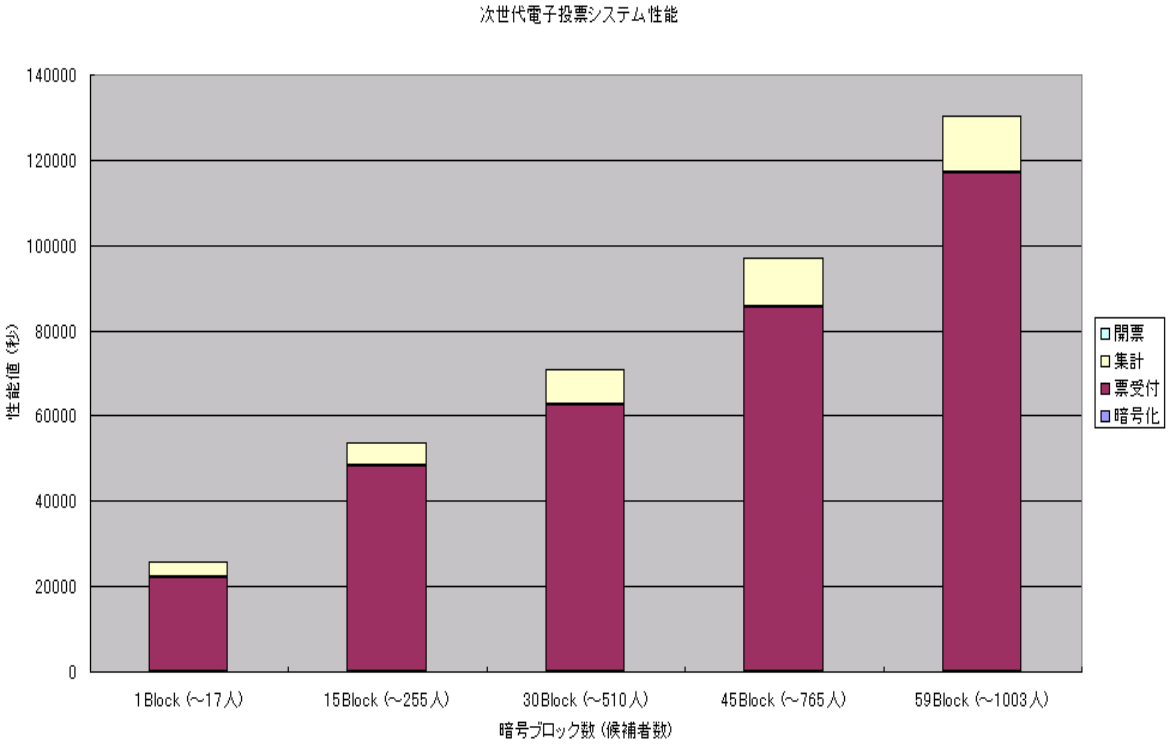


図 11　性能測定結果（グラフ化）

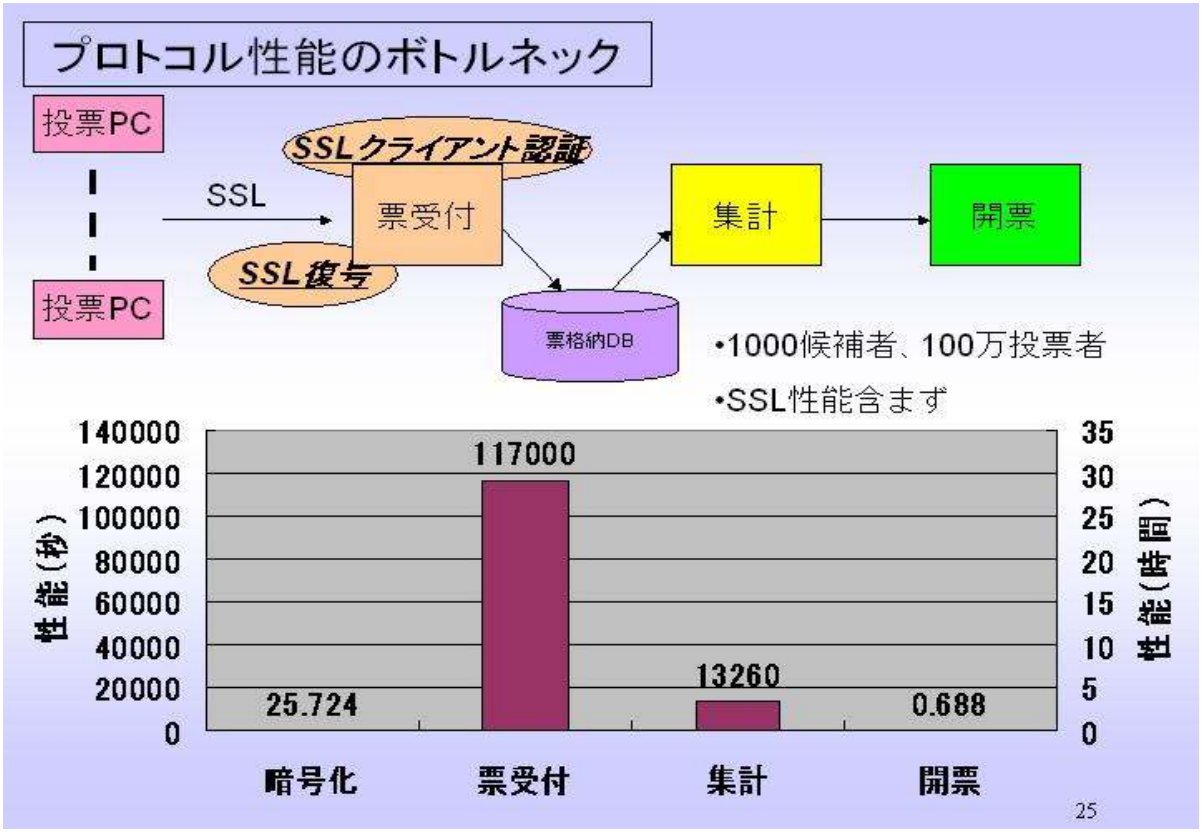


図 12　プロトコル性能のボトルネック

5-3-2-4　性能分析

前項の性能測定結果から、以下のことが判明した。

① 候補者数が増える（暗号ブロック数が増える）とそれに比例して性能値が大きくなる。つまり、電子投票システムの性能は、暗号文サイズに大きく左右される。
⇒ **【改善案】 暗号ブロック数の削減**

② 各プロトコル性能を分析した結果、特にセンター1 での暗号票を受付処理が突出して高コストである。
⇒ **【改善案】 センター1 サーバ（暗号票受付サーバ）の多重化**
⇒ **【改善案】 センター1 サーバ（暗号票受付サーバ）には、高性能 HW を採用**

5-3-3　参照実装モデルのセキュリティ対策技術

本節は、サブテーマ２に記載している運用要件及びサブテーマ５に記載している参照実装モデルのセキュリティ対策技術について調査した結果を整理したものである。

サブテーマ２に記載している運用要件に対して、参照実装モデルで実現していない又は今後実装が必要なセキュリティ対策技術について、現時点で適用できるセキュリティ技術について調査した。

またサブテーマ５に記載している参照実装モデルのセキュリティ対策技術について、現時点でのセキュリティ技術について調査した。

5-3-3-1　運用要件概要

サブテーマ２「運用形態ごとの要件整理」（5-2「5-2 運用形態ごとの要件整理」参照）では、、要件定義を、「機能要件」、「セキュリティ要件」、「ハードウェア要件」、「ソフトウェア要件」と大きく４つのカテゴリに分類している（「5-2-2 要件定義について」表 11　電子投票システムの要件概要　参照）。

要件定義に記載している「セキュリティ要件」は「5-2-3 要件定義」表 19　セキュリティ要件に示す通りである。

5-3-3-2　参照実装モデル

(i) 参照実装モデルのシステム構成

サブテーマ５「モデル構築」（「5-5 モデル構築」参照）に記載している参照実装モデルのシステム構成を以下に示す。

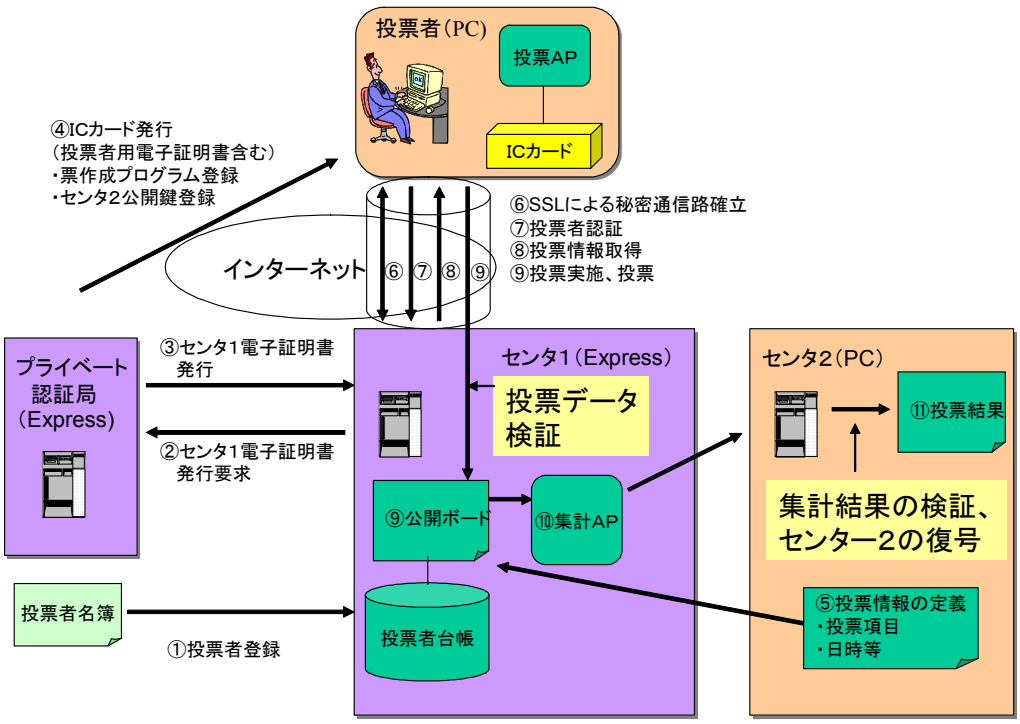


図 13　システム構成図

サブテーマ５「モデル構築」（「5-5 モデル構築」参照）では、システム構成を以下のように定義している。

表 23 参照実装モデルのシステム構成の定義

名称	定義
認証局	本システムにおいて、各センターの証明書や、投票者用 IC カードを発行する。
センター1	本システムにおいて、選挙情報(候補者情報も含む)の公開、投票データ収集、票の集計を行う。
センター2	本システムにおいて、選挙情報の定義、集計結果の開票を行う。
投票 PC	本システムにおいて、センター1から選挙情報を取得し、投票を行う。

表 24 参照実装モデルの構成要素の定義

構成要素	定義
投票端末ハードウェア	投票者の投票行為を実現するネットワークに接続されたハードウェア。
投票端末ソフトウェア	投票者の投票行為を実現するソフトウェア。
管理者サーバハードウェア	有権性の確認、集計、開票等の管理者側の行為を実現するネットワークに接続されたハードウェア。
管理者サーバソフトウェア	管理者側で行う全ての行為を実現するソフトウェア。
公開ボードソフトウェア	投票データ、および、集計結果等の公開可能なデータを公開するソフトウェア。
ネットワーク	投票端末と管理者サーバ側を電子的に接続するネットワーク。

5-3-3-3　参照実装モデルに必要なセキュリティ技術

サブテーマ２「運用形態ごとの要件整理」（「5-2 運用形態ごとの要件整理」参照）及びサブテーマ５「モデル構築」（「5-5 モデル構築」参照）に記載している、本研究で構築するシステムに必要なセキュリティ技術を以下に示す。

表 25 システム構築に必要なセキュリティ対策

分類	概要	個別技術
通信	安全でない通信路を用いて、認証・暗号化を実施し、完全性を持つ安全な通信を行うための技術	・ SSL/TLS ・ IPSec
鍵管理	秘密鍵などを安全に秘匿する技術	・ HSM（Hardware Security Module） ・ 鍵のバックアップ／リストア
認証・アクセス制御	システム利用者やサブシステム間で認証を行い、またアクセスを制限する技術	・ PKI (X.509) ・ 所持品による個人認証 ・ 知識による個人認証 ・ 身体的特徴および行動による個人認証 ・ 行動の特徴による個人認証
ネットワーク防御	ネットワークを、障害や悪意のある攻撃から防御する技術	・ ネットワークへの論理的な侵入の阻止） ・ 物理的ネットワークの防御 ネットワーク機器の防御 ・ 内部ネットワークへの不正接続の阻止 ・ ネットワーク上での不正アクセスの検知（NIDS）
ウィルス対策	ネットワーク経由や物理的メディアによる持ち込みなどによるウィルス感染からサーバ、クライアントを守る技術	・ HTTP, SMTP コンテンツフィルタリング ・ ワクチンソフト導入 ・ パターンファイルの配信・適用管理
サーバ防御	サーバを障害や悪意のある攻撃から防御する技術	・ サーバ要塞化 ・ サーバ上のファイルの改ざん検知 ・ パッチ適用
クライアント防御	開発者／システム管理者／選挙職員が使用する、選挙システムへアクセスする可能性のあるクライアント PC のセキュリティ確保	・ 利用者の認証 ・ ネットワーク上での不正アクセスの検知（NIDS） ・ 利用記録
物理的アクセスコントロール	サーバ、ネットワークなどを、悪意のある物理的アクセスから防御する技術	・ データセンターサービス ・ バイオメトリクス等認証技術

これらを整理し、運用面を考慮したセキュリティ対策としては、以下のものが必要になる。

表 26 システム構築に必要なセキュリティ対策具体例

分類	セキュリティ対策	具体低対策例
ネットワーク	不正アクセスの防止	・ ファイアウォール
	不正アクセスの監視	・ ＩＤＳ・ＩＤＰ
	ネットワークへの接続規制	・ ネットワーク監視
	機器へのアクセス制限	・ 機器のアクセス制限
	暗号化通信	・ ＳＳＬ
		・ ＩＰｓｅｃ
認証	利用者認証（外部）	・ ＰＫＩ
	利用者認証（内部）	・ 個人認証（所持品）
		・ 個人認証（生態）
アクセス制御	アクセス制御（利用者）	・ サーバでのアクセス権
	アクセス制御（ネットワーク）	・ （ファイアウォール）
ウィルス対策	外部からの侵入（ネットワーク）	・ ゲートウェイ型対策
		・ コンテンツフィリタリング
	内部からの侵入 （外部媒体、ネットワーク）	・ サーバ対策
		・ クライアント対策
	運用管理	・ 統合管理（状況管理）
		・ パターンファイル配信
サーバ対策	セキュリティ確保	・ サーバ要塞化
		・ 改ざん検知・自動復旧
クライアント対策	セキュリティ確保	・ クライアント要塞化
		・ 改ざん検知・自動復旧
運用管理	パッチ適用	・ 資産管理（状況管理）
	利用記録	・ ログ管理（監視）
鍵管理	秘密鍵などを安全に秘匿する技術	・ ＨＳＭ
		・ 鍵のバックアップ／リストア

5-3-3-4　セキュリティ対策技術の実態

参照実装モデルに必要なセキュリティ対策で重要なセキュリティ対策技術は、以下の通りである。

⑴ 暗号化通信（ＳＳＬ）
⑵ 暗号化通信（ＩＰｓｅｃ）
⑶ ファイアウォール
⑷ ＩＤＳ／ＩＤＰ
⑸ ウィルス対策
⑹ 認証
⑺ 鍵管理
⑻ ログ管理

以降このセキュリティ対策技術の実態の調査結果を示す。

5-3-3-5　SSL

⑴ 技術概要

ＳＳＬ（Secure Sockets Layer）は、Netscape Communications 社が開発した、インターネット上の通信データを暗号化して送受信ためのプロトコルである。現在インターネットで広く使われているＨＴＴＰやＦＴＰなどの通信データを暗号化し、プライバシー情報やクレジットカード番号、企業機密情報などを安全に送受信ためのものである。ＳＳＬは、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせて通信データの暗号化と復号化を行うものであり、データの盗聴や改ざん、なりすましを防ぐことを可能にしている。

ＳＳＬは、ＯＳＩ参照モデルの第４層であるトランスポート層にあたり、上記のプロトコルであるＨＴＴＰやＦＴＰなどのアプリケーションソフトからは、特に意識することなく透過的に利用することができる。現在は、ＳＳＬ３．０をもとに改良が加えられたＴＬＳ１．０がＲＦＣ２２４６としてＩＥＴＦで標準化されている。

ＳＳＬは、Ｗｅｂサーバのソフトウェアとクライアントで動作するＷｅｂブラウザの双方が対応することにより実現している。現在のサーバやクライアントのほとんどソフトウェアでは、ＳＳＬの機能に対応できている。

⑵ 技術詳細

実際のＳＳＬによって安全なやり取りが成立するまでの流れについてその詳細を説明する。

Ｗｅｂサーバは、ＳＳＬによる通信を行う時まず認証局による署名入りのデジタル証明書を、ブラウザに対して送信する。ブラウザは、この証明書を確認することでＷｅｂサーバの認証を行う。一方、ブラウザは、情報を安全にやり取りするために用いる暗号化方式から、対応できる暗号化方式をＷｅｂサーバに通知し、サーバと共に双方で実行可能な暗号化方式から、最も強固なものを選定する。また、ブラウザでは、暗号に用いる共通鍵を生成し、これをＷｅｂサーバからのデジタル証明書内にあるＷｅｂサーバの公開鍵で暗号化してＷｅｂサーバへ送信する。Ｗｅｂサーバでは、これを自らの秘密鍵で復号化することで、共通鍵を得ることとなる。 この段階において、双方が暗号化通信を行うための共通鍵を持つことになるため、認証が完了するとともに、それ以降はＨＴＴＰＳによるＳＳＬの安全な通信を実現することができる。

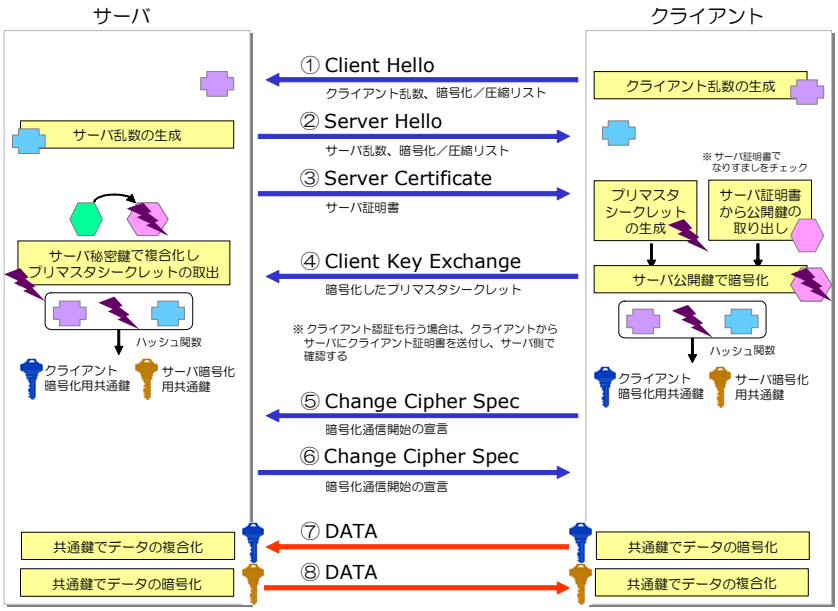


図 14　SSLのやり取り

(3)　技術に対する問題点と解決策

ＳＳＬによる通信は、認証と暗号化通信の実現により、「盗聴」「成りすまし」「改ざん」「否認」などのリスクを回避することが可能になる利便性の高い技術であることを説明したがその反面、認証や暗号化・復号化などがサーバのＣＰＵなどに負荷がかかるという問題がある。　現在パソコンのＣＰＵ能力は急速な進歩をしているため、クライアントではＳＳＬを実行するためのＣＰＵ負荷の問題はない。これに対してＷｅｂサーバでは、利用者がアクセスしてきた全要求に対して、同様の処理を行う必要がありＣＰＵ負荷が多大なものとなる。　現在のアクセスの多いＷｅｂのサーバ環境としては、負荷分散装置などによる複数のサーバで構成しているため、同時に多数のアクセスがあっても、パフォーマンスを低下させない構成を取ることができる。そこでＳＳＬに関係する一連の処理を、Ｗｅｂサーバから完全に分離することが可能であれば、Ｗｅｂサーバの負荷をさらに削減することができる。

現在の製品としては、ＳＳＬアクセレータと呼ばれるＳＳＬに特化した専用処理を行うのハードウェアが広く使われている。ＳＳＬアクセラレータは、ＳＳＬによる暗号通信で送受信されるデータの暗号化・復号化を高速に行なう専用ハードウェアである。ＳＳＬアクセラレータは、ＰＣＩカードなどサーバ内に設置する製品と、サーバとは別にネットワーク上に設置する製品の２つがあるが、原理は基本的に同じものである。

(4)　具体的な利用形態（ＳＳＬアクセラレータ）

現在ＳＳＬアクセラレータは利用形態による形態で分類することができる。以下に利用形態毎の概要を説明する。

（ア）　Ｗｅｂサーバへ実装するＳＳＬアクセラレータ

ＰＣＩ対応ボードとして製品化されたＳＳＬアクセラレータを、Ｗｅｂサーバ内に実装する形態である。Ｗｅｂサーバの送受信トラフィックは、サーバによってＳＳＬ対応処理を行うがその時のＳＳＬ対応処理を、ＰＣＩ対応ボード（ＳＳＬアクセラレータ）に要求し行う。

（イ） ネットワーク上に設置するＳＳＬアクセラレータ

現在最も利用されている形態で、ＳＳＬ処理を専用に行うネットワーク機器（アプライアンスサーバ等）をＷｅｂサーバとインターネットの間に配置する。Ｗｅｂサーバへの送受信トラフィックは、必ずＳＳＬアクセラレータを通過するので、その時に暗号化と復号化が必要なトラフィックをＷｅｂサーバに代わって処理を行う。また最近では、ＯＳＩ参照モデルのトランスポート層におけるトラフィック解析やスイッチングを行うレイヤ４スイッチを介することで、必要なトラフィックのみをＳＳＬアクセラレータで処理することも可能である。

（ウ） 負荷分散装置に実装するＳＳＬアクセラレータ

Ｗｅｂサーバのパフォーマンスを向上させる対策として、負荷分散装置(ロードバランサー)を利用しＷｅｂサーバを複数設置することが多いが、この負荷分散装置にＳＳＬアクセラレータを実装する形態で、負荷分散する時にＷｅｂサーバの選択をする情報としてＨＴＴＰＳの通信データ内の情報を使うために複合化が必要になるため、ＳＳＬアクセラレータを実装し高速に処理することを実現している。

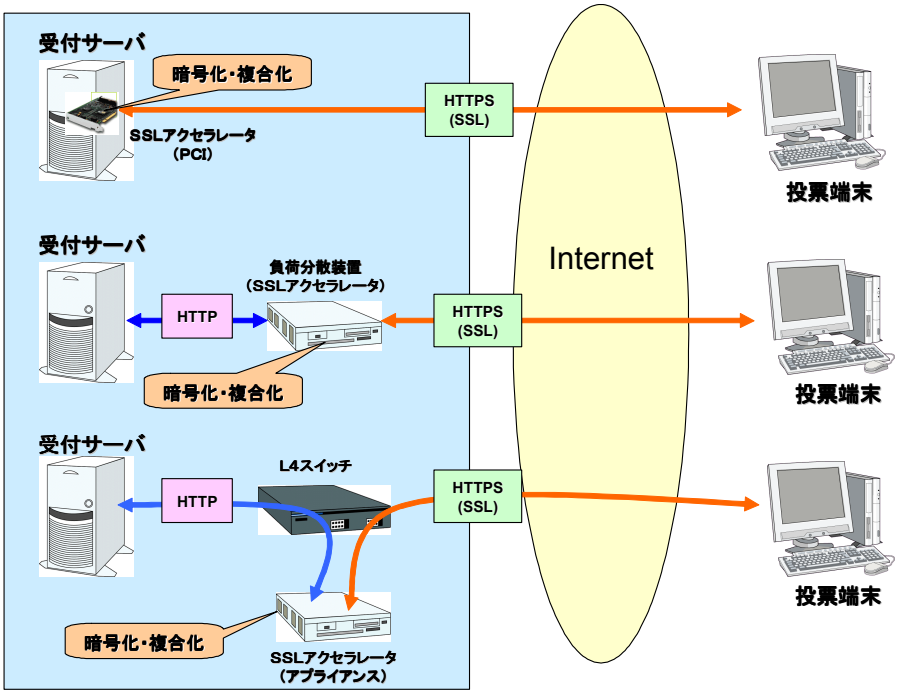


図 15 SSLアクセラレータの利用形態

(5) ＳＳＬアクセラレータの処理能力

ＳＳＬアクセラレータの処理能力について、現在の技術レベルでの状況を以下に示す。

ＲＳＡ の 1024 ビット公開鍵を用いる暗号化処理は、ＣＰＵ性能によって大きく異なるが、現在のクライアントで、毎秒 100 回程度である。これに対し、ＳＳＬアクセラレータでは、1 台当たり、毎秒 1,000 回程度のＳＳＬにおける暗号化と復号化を実現することができる。単純計算で、ＳＳＬに関わる処理パフォーマンスを、ＳＳＬアクセラレータ 1 台当たり、10 倍程度まで引き上げることができることになる。また、ＳＳＬアクセラレータは、カスケード接続やレイヤ４スイッチへの接続による複数台を設置することが可能で、これらの構成を取ることによりさらにパフォーマンスを向上させることも可能である。 さらに、ＳＳＬアクセラレータ

機能が持っている負荷分散装置を用いることで、Ｗｅｂサーバの負荷を分散させながら、ＳＳＬ処理のパフォーマンスを向上させるように、Ｗｅｂサーバ環境やトポロジを自由に設計することも可能である。

5-3-3-6 IPsec

⑴ 技術概要

ＩＰｓｅｃは、インターネットで暗号通信を行なうための規格である。ＩＰのパケットを、暗号化して送受信するため、ＴＣＰやＵＤＰなど上位のプロトコルを利用するアプリケーションソフトはＩＰｓｅｃが使われていることを意識する必要はない。現在インターネットで使われているＩＰｖ４ではオプションとして使用することができるが、次世代のＩＰｖ６では標準で実装される。

⑵ 技術詳細

ＩＰｓｅｃの具体的な仕組みを説明する。ＩＰｓｅｃは、暗号化通信を実現する複数のプロトコルの総称であり、大きく分けて以下の３つのプロトコルがある。

（ア） ＩＫＥ（Internet Key Exchange）

ＩＰｓｅｃによる暗号化通信は、まず鍵交換を含めたＳＡの合意をとることから始まるがこの合意は、あらかじめ手動で設定しておくことも可能である。しかしＳＡの合意を手動で設定するのはその作業が面倒であることと、通信相手となるコンピュータが遠隔地に設置されていたり、数が多かったりすると、手動で設定するのは事実上困難である。また、暗号化通信の安全性を向上させるため、使用する暗号鍵を定期的に交換することも必要となるため、なるべくこれらの管理を容易にするために、自動的にＳＡを交換することが必要となる。

そこでＩＰｓｅｃでは自動的にＳＡの合意をとることが可能な鍵交換プロトコルとして、ＩＫＥを規定している。ＩＫＥを使うことで、ＳASA の合意を自動的に行うことが可能になる。

（イ） ＥＳＰ（Encapsulating Security Payload）

ネゴシエーションが終了した後、通信を行う双方で暗号化されたパケットによる通信が開始される。ＩＰｓｅｃでは、パケットごとに暗号化がなされ、ＥＳＰと呼ばれる入れ物にパックされ送信される。ＥＳＰは、暗号化された通信内容にＳＰＩとシーケンス番号フィールド、そして認証データという３つの付加情報が付け加えられた構造をとっている。

（ウ） ＡＨ（Authentication Header。

ＡＨは、「完全性の保証」と「認証」のための仕組みである。ＡＨでは、データの暗号化は行わず、ＳＰＩ、シーケンス番号、そして認証データのみをパックして通常のＩＰパケットの中に加えるようにしている。

現在のＩＰｓｅｃの主な利用目的は、インターネットを使ったＶＰＮ接続である。これは今までのWAN接続は、専用線により実現する企業での本支店間の接続やＬＡＮ間接続といったものを、インターネットを使って実現する時に利用するものである。インターネットを利用した通信は、当然であるが不特定多数に通信内容がさらされることになるため、送信するデータを守る仕組みが必要になる。そこで、このＩＰｓｅｃを使用することにより、利用料金は専用線と比較してはるかに安価でありながら、専用線と同じような通信の秘匿性を実現することができる。現時点ではＩＰｓｅｃの大半が、ＶＰＮ接続を対象とするものが多い。製品としては、専用の暗号化装置（ＶＰＮ装置）としての形態と、ルータやファイアウォールなどの付加機能の形態の２つがある。このような製品をインターネットの接続部分に設置し、トンネル・モードのＩＰｓｅｃを

利用することで、拠点間のすべての通信を暗号化している。

(3) ＶＰＮ接続

現在インターネットを含め多種多様のネットワークがあるが、インターネットのような公衆のネットワークを利用する場合、情報の漏洩などセキュリティ面でのリスクが存在する。そこで、公のネットワークを利用しながらも高いセキュリティを保つ方法としてＶＰＮ接続がある。

以下にそのＶＰＮ接続の概要を示す。

ネットワークＡとネットワークＢをインターネットなどで接続し通信を行う場合、ネットワークＡに設置されたＶＰＮ専用機(1)とネットワークＢに設置されたＶＰＮ専用機(2)によってＶＰＮ接続が実現する。ネットワークＡからネットワークＢに送信したパケットはＶＰＮ専用機(1)で暗号化し、カプセル化されてネットワークＢに送信される。暗号化には、ＶＰＮ専用機(2)の公開鍵が用いられるが、これを復号化するためにはＶＰＮ専用機(2)だけが持つ秘密鍵が必要となるため、途中の盗聴や改ざんができない。ＶＰＮ専用機(2)では、受信したデータを復号化することで高度なセキュリティを実現することができる。

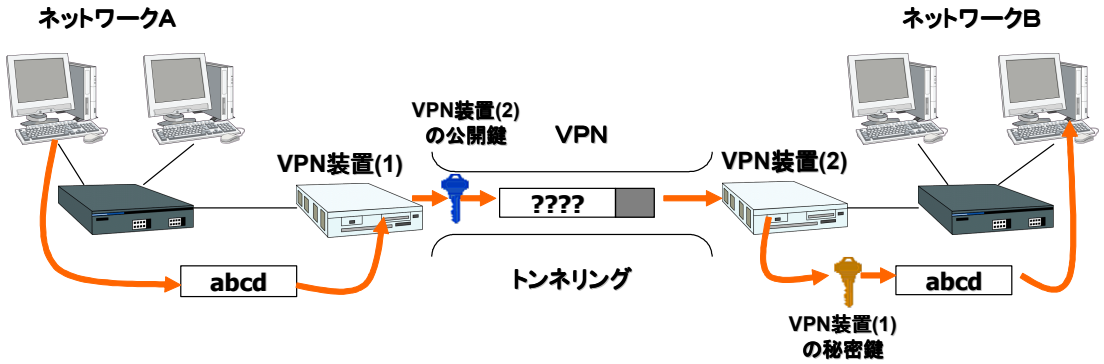


図 16 VPN接続の構成例

前述したように、ＶＰＮ接続でトンネリングを実現するためには、暗号機能、復号機能を含むパケットのカプセル化を実現する機能を持つ必要があるが、ＵＮＩＸ系ＯＳやＷｉｎｄｏｗｓ２０００などサーバで用いられているネットワーク専用ＯＳを用いることで実現することもできるが、一般的にはＶＰＮ機能を持ったネットワーク機器（ルータ等）を利用する。また高度なセキュリティを維持するとともに安定した通信を行うことのできるＶＰＮ接続を実現する場合には、ＶＰＮ専用機を用いることが多い。ＶＰＮ専用機は、ＶＰＮ接続に不可欠な機能のすべてを備えているが、さらに通信効率を上げるためのデータ圧縮機能や、企業内部のネットワークを守るためのパケットフィルタリングをはじめとするファイアウォール機能を備えたものや、暗号機能と複合機能を専用のチップ（ＡＳＩＣ）で高速処理するものが出てきている。

5-3-3-7 ファイアウォール

(1) 技術概要

ファイアウォールは、組織内のコンピュータネットワークへ外部から侵入されるのを防ぐためのシステムであり現在のインターネット接続には必須のものである。企業のネットワークでは、インターネットなど外部ネットワークから第三者が侵入し、データやプログラムの盗み見・改ざん・破壊などを防止するために、外部との境界を流れる通信データを監視し、不正なアクセスを

検出・遮断する必要がある。これを実現するための機能を備えているのがファイアウォールである。最近まではソフトウェアをサーバに組み込んで提供される形態が多かったが、現在は高い性能とセキュリティ強度がが要求されるため、専用のハードウェアが用いられることが多くなってきている。

なおファイアウォールは、一般的に以下の機能を備えている。

・アクセス制限
・アドレス変換
・ユーザ認証
・ログ収集／解析
・コンテンツフィルタリング
・ルーティング

⑵ 技術詳細

ファイアウォールには、以下の３つの方式がある。

（ア） パケットフフィルタリング

ルータなどが持っている機能で、送られてきたパケットを検査して通過させるかどうか判断する機能である。パケットフィルタリングは、ネットワーク層で動作するフィルタリングで、ファイアウォール製品だけでなくルータやサーバＯＳにも搭載されている機能である。ネットワーク層では、パケットの先頭にＩＰヘッダとＴＣＰ（ＵＤＰ）ヘッダが付いているが、パケットフィルタリングでは、これらのヘッダに含まれている「宛先ＩＰアドレス」、「送信元ＩＰアドレス」、「プロトコル」、「送信元ポート番号」、「宛先ポート番号」、「フラグ」などを調べることでセキュリティを確保している。

最も一般的かつ簡便なセキュリティ技術として知られているが、最近のルータでは大半が備えて機能であり、よく知られているだけに破る手段も多く、他の技術（不正侵入検知等）と併用することが必要である。

（イ） アプリケーションゲートウェイ

パケットフィルタリングがネットワーク層で動作するのに対し、アプリケーションゲートウェイはアプリケーション層で動作する。通常、アプリケーションゲートウェイはサーバに導入され「プロキシサーバー」と呼ばれる。プロキシサーバーは、クライアントとサーバの間で両者の通信を仲介する役目を担っていて、「クライアントとプロキシサーバー」および「プロキシサーバーとサーバ」という２つのセッションが張られて動作し、インターネットと社内ＬＡＮとの間のＴＣＰ／ＩＰは完全に切り離される形となるので、パケットフィルタリングよりもセキュリティは高くなる。

また、アプリケーションゲートウェイではデータ内容を元にアクセス制御するので、ウィルスやセキュリティホールを狙った攻撃を防いだり、詳細なログを保存したりすることができる。しかし、パケットフィルタリングよりも負荷が大きく、またアプリケーション（プロトコル）ごとに専用ソフトが必要になるため利用するアプケーションによって対応できないものがあり注意が必要である。

（ウ） ステートフルインスペクション方式

ファイアウォールを通過するパケットのデータを読み取り、その内容を解析・判断して動的に通信ポートを開放・閉鎖する機能である。パケットフィルタリング方式では、「データを送信したのがＬＡＮ側かＷＡＮ側か？」「アクセス先のポート番号は何か？」など、ＴＣＰやＵＤＰのヘッダを元に判断できる定型的な条件でパケットを遮断・通過させている。

しかし、パケットフィルタリング方式は正常に送信されたパケットに対しては適切に機能

することが可能であるが、特定のサーバを攻撃するために生成された不正なパケットなどは適切に処理できないことがある。

これに対して、ステートフルインスペクション方式は、ＬＡＮ側から送信したデータを管理テーブルで保管し、ＷＡＮ側から到着したパケットが管理テーブルと矛盾しないか確認する。

現在のファイアウォール製品は、ほとんどがこのステートフルインスペクション方式を採用しており、同時にパケットフィルタリング方式も利用可能になっている。

また実際のファイアウォールは、以下の２つの形態で構築されている。

（ア） サーバにソフトウェアを組み込む

ＵＮＩＸやＷｉｎｄｏｗｓ２０００などのＯＳで動作するサーバに、ファイアウォールのソフトウェアを組み込んでものである。サーバのＯＳの維持やサーバのカスタマイズが必要であり、またサーバでの処理のための能力不足などに注意が必要となる。

（イ） 専用機

専用機は、ＩＰフィルタリングやＮＡＴなどファイアウォールとしての必要な機能のみを備えている。そのため、サーバにソフトウェアを組み込んだファイアウォールに比べて高速に処理することができ、強固なセキュリティ機能を持つことができる。

現在、専用機を使うことで、従来型のサーバにソフトウェアを組み込んだ形態にはないメリットが生まれている。

１つめのメリットとしては、専用のＯＳを採用しており、汎用的なＯＳにあるセキュリティホール等の危険性から解放される。多くの専用機は、目的に適用するために十分なカスタマイズを実施したＵＮＩＸカーネルや独自ＯＳを採用している。

２つのメリットとしては、ＯＳとともにハードウェア上も目的に特化できるため、高速でかつ拡張しやすい作りにできることがある。とくにファイアウォール機能にＶＰＮ機能を同時に動作させると、とたんに処理が重くなり性能が低下する。ＶＰＮ機能では、暗号化や複合化やデータ圧縮、公開鍵処理などＣＰＵに負荷をかける処理が多数ある。このような場合でもアプ専用機では、、ＩＰｓｅｃアクセラレータなど重い処理するための専用ハードウェアの追加が容易にできる。インターネット回線が高速化されてきている現在では、ＬＡＮ側も含め高速な通信が可能となっており、ファイアウォールがボトルネックになるという結果も起きるため、「サーバにソフトウェアを組み込む」というファイアウォール形態は、既に臨界になっていると言われる。

３つめのメリットとしては、プラグ&プレイで設置でき、障害が発生した場合も機器ごと交換することが可能となる。従来型の「サーバにソフトウェアを組み込む」では、ファイアウォール専用機として構築していても、代替機を用意するとなるとＯＳのインストール、各種ドライバのインストールなど実施する作業が多い。また、周辺機器の多いサーバはそれだけ故障の発生する可能性も多く、不要な機器のない専用機の方がが故障しにくい。また、万が一故障したとしても、代替機に基本的な設定だけ移行すればすぐに復旧できる。

(3) 最新技術

現在のファイアウォールの最新技術概要を、以下に示す。

・ステートフルインスペクション方式を採用した専用機が、多数提供されており主流となっている。
・専用機として、高速に処理をするために一部の処理をチップ（ＡＳＩＣ）にしている製品が多数提供されている。

・１００MのＬＡＮだけでなくギガビットイーサネットにも対応できている。
・ゲートウェイ型だけでなく、最近ではＬＡＮの間に設置できるブリッジ型の専用機もあり、ネットワークに容易に接続できるようになってきている。
・専用機として、ファイアウォール機能たけで無く、ＶＰＮ機能、ウィルスチェック機能、ＩＤＳ機能、及びコンテンツフィルタリング機能を合わせて備えた製品が提供されている。（複数の機能を連携し、より強固なセキュリティ対策を実現することができる。）

5-3-3-8 IDS･IDP

⑴ 技術概要

ＩＤＳは、ファイアウォールとは異なり、通信パケットの中味を調べ、それぞれの企業におけるセキュリティポリシーに従い不正と思われるパケットを検知するものである。

製品により検知するためのしくみは異なるが、通信パケットを監視して安全なものと危険なものとを分類し、通過パケットの中で危険なものが発見されると事前に定義されたルールにしたがいアラート通知を行う。

基本機能としては、次の２つの機能がある。

（ア） シグネチャーによる攻撃の検知

過去の攻撃に使われたパターン（不正アクセスパターン）を「シグネチャー」として管理し、通過するパケットがこのパターンに一致した場合、攻撃を受けていると認識し、アラート通知を行う。該当製品に含まれるシグネチャーの数やの内容はメーカーにより異なるが、ＩＤＳメーカーは攻撃パターンを収集、分析し、シグネチャーに反映するための専門チームを有しており、このチームからの情報に基づきシグネチャーのアップデートを行なう。

（イ） プロトコル以上の検知

通常インターネットで使用されるプロトコルは、ＲＦＣにより定義されたプロトコルが用いられている。このＲＦＣでの定義に違反したプロトコルを不正とみなし、このような通信パケットを認識した場合、アラート通知を行う。

⑵ 技術詳細

ＩＤＳは、サーバなどを監視する「ホスト型ＩＤＳ」とネットワーク上に流れるパケットを監視する「ネットワーク型ＩＤＳ」の２つのタイプがある。

ホスト型ＩＤＳは、監視したいサーバにＩＤＳのソフトウェアをインストールし、ログの取得と追跡、重要ファイルの監視による改ざんチェック、不正なパケット検知と遮断などを行う。基本的には、重用なサーバに導入するのが一般的である。

ネットワーク型ＩＤＳは、監視対象となるインターネット接続部分や特定のセグメントにセンサーと呼ばれるＩＤＳを設置し、ネットワークを通過するパケットを全て監視する。センサーは、通信パケットがシグネチャーと一致、又は異常プロトコルを検知すると、アラート通知を行なう。

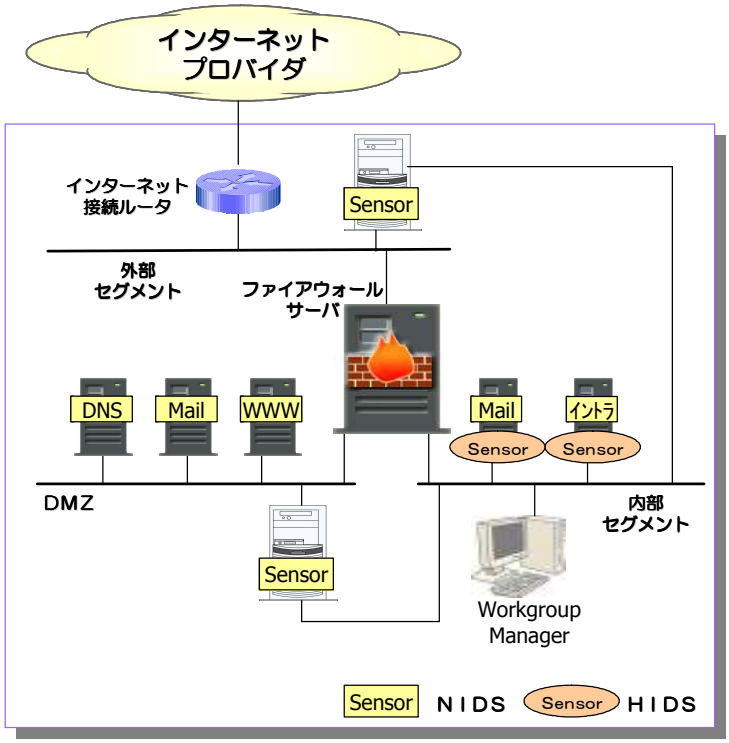


図 17 ホスト型IDSとネットワーク型IDSの構成例

ホスト型ＩＤＳ及びネットワーク型ＩＤＳは、不正アクセスを「検知」しても、その攻撃に対処するのはシステム管理者となる。ＩＤＳが検知した内容から対処を検討し、ファイアウォールなどの設定を変更する。よってシステム管理者の対処が遅くなると、その攻撃は続いてしまい大きな問題となる。このような状況に対処するために出てきたのが防御機能を持つIDSであるＩＤＰ（ＩＰＳ）である。

ＩＤＰ（ＩＤＳ）は、そのほとんどが「インライン型ＩＤＳ」という形態を採用している。インライン型にすることで、ネットワークに流れる不正パケットを防御することが容易にできるためである。　インライン型ＩＤＳは、ファイアウォールと同じにネットワーク上にゲートウェイとして設置し、ネットワークを通過する全てのパケットを監視する。ネットワーク型ＩＤＳではネットワーク上を流れているパケットをコピーしてパケットをチェックするのに対して、インライン型ＩＤＳはネットワーク上に設置されているため通過するパケットそのものをチェックする。

通過するパケットをチェックし異常を検知した場合、あらかじめ設定されているポリシーに従ってＩＤＳが自動的にパケットを遮断したり、攻撃を行っているＩＰアドレスからのパケットを破棄するとともに、セッションの切断を行なう。

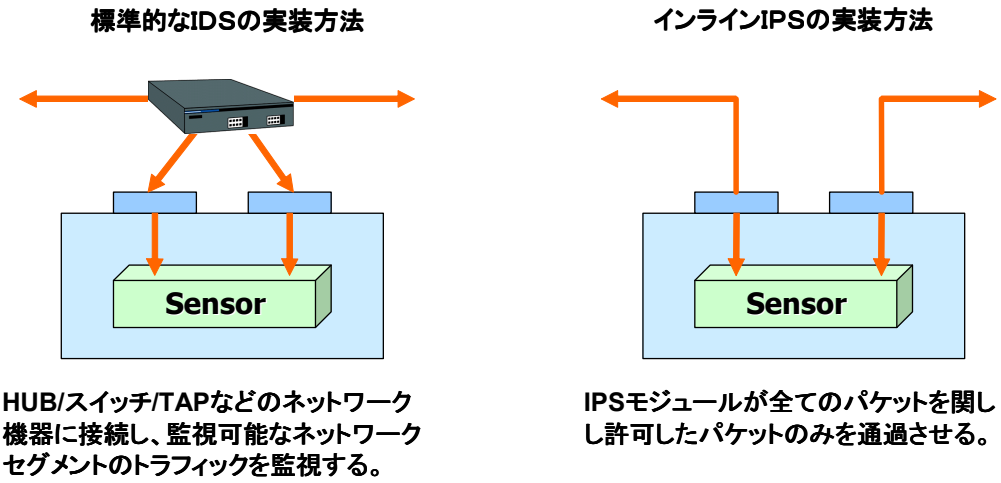


図 18 インライン型IDSの実装

また別な形態のＩＤＳとして「おとり型ＩＤＳ（別名：ハニーポット）」と呼ばれるＩＤＳもある。このおとり型ＩＤＳは、不正パケットを検知し、排除、または防御するといったＩＤＳの本来の形態ではなく、不正パケットを重要なサーバや特定のセグメントに行かないように誘い込み、その侵入パターンや攻撃パターンを解析するための情報収集を行うものである。

(3) 最新技術

現在のＩＤＳ・ＩＤＰの最新技術概要を、以下に示す。

・ＩＤＳ及びＩＤＰの専用機が、多数提供されており主流となってきている。
（しかし運用形態としては、まだ監視レベルの運用が主体である。）
・専用機として、高速に処理をするために一部の処理をチップ（ＡＳＩＣ）にしている製品が提供されている。
・１００Mだけでなくギガビットに対応した製品も出ており、高速なネットワークでも検知できるレベルになってきている。
・専用機として、ＩＤＳ機能たけで無く、ファイアウォール機能、ＶＰＮ機能、ウィルスチェック機能、及びコンテンツフィルタリング機能を合わせて備えた製品が提供されている。
（複数の機能を連携し、より強固なセキュリティ対策を実現することができる。）

なお不正検知の最新技術として、ＩＰＳがある。以下にＩＤＳの概要を示す。
ＩＰＳ（Intrusion Prevention System）とは、不適切なトラフィックがネットワークに流入するのを予防または防御してくれる機器であり、以下に示す機能を備えている、

・シグネチャ検知
・アノマリ（Anomaly：異常行動）検知
・DoS 攻撃検知
・偽装情報を利用した検知

またＩＰＳには、検知された悪意のあるトラフィックを回避したり遮断したりするために色々な防御機能が実装されている。以下に主な防御機能を示す。

・ＩＣＭＰ（Internet Control Message Protocol）やＵＤＰ、不正ＩＰパケットなどの TCP Reset で防御できない攻撃をパケット単位で破棄することができる。

・攻撃イベントを発生させたＴＣＰコネクションの全てのパケットを破棄したり、Reset パケットを送信してコネクションを切断したりすることができる。
・ファイアウオールルールを定義することによりトラフィックをフィルタリングできる。
・ファイアウオールルールを動的に変更することにより、該当する攻撃トラフィックを一定時間遮断することができる（このブロック方法は Drop Packet/Drop Connection と連携して利用され、一連の攻撃における最初の攻撃パケットを遮断することも可能である）。

5-3-3-9　ウィルス対策

⑴ 技術概要

現在、ウィルスの脅威は広く認知されており、ほとんどの企業などでは何らかの形で、ウィルス対策を行なっている。特に、エンドユーザが日常的に利用するクライアント向けのウィルス対策ソフトは、企業だけでなく一般家庭にまでも広く普及している。

一口にウィルスと言っても、ウィルス、ワーム、トロイの木馬などの種類があるが、ウィルス対策ベンダがワームの一種類と定義しているネットワーク型ウィルスには、特に注意が必要である。ネットワーク型ウィルスは、セキュリティホールを悪用してメールとファイル共有以外の経路で侵入し、ユーザの操作無しに自動的に感染活動を開始するものである。感染後には、ユーザの操作が無くても、自動的に活動を始めるため感染に気付きにくく、従来のウィルス対策ソフトでは防御が難しくなってきている。今後も、新種・亜種のウィルスが登場してくるのは、間違いなく、これら未知のウィルスによる被害を最小限に抑えるためには、単にウィルス対策ソフトを導入するだけでは充分な対策を取ることができない。

その理由として、企業ネットワークの内部実態あ、ＯＳなどのアップデート（パッチ適用）や新規のクライアントの追加などにより、随時変わっているかためである。企業のネットワークは日々変化を続ける“生き物”であり、ウィルス対策ソフトの運用・管理は、その変化に応じて続ける必要がある。特に、ウィルス対策ソフトのパターンファイル（ウイルス定義ファイル）は常に最新のものにする必要があり、そのために日頃からの継続的な運用・管理がウィルス対策のポイントとなっている。

⑵ 技術概要

一般的にウィルス対策ソフトは、「クライアント&ファイルサーバー」、「ゲートウェイ」、「グループウェア」等の製品がある。

これらは大きく分けると、「ローカルのハードディスクをスキャンするもの」と、「ローカルのハードディスクをスキャンするもの」の 2 つに分類される。「ローカルのハードディスクをスキャンするもの」には、「クライアント&ファイルサーバー」が該当し、「ローカルのハードディスクをスキャンするもの」には、「ゲートウェイ」、「グループウェア」が該当する。

（ア）クライアント&サーバ

クライアント向けの製品は、自宅のパソコンにも導入されているもので、企業向けの製品では、管理者が管理ツールを使いパターンファイルの配布など、複数のクライアントに対して一括で設定を行なえる機能を備えており、個人ユーザ向けのものとは管理面などで大きくことなっている

（イ）ゲートウェイ

ゲートウェイ向けの製品は、ＳＭＴＰ、ＨＴＴＰ、ＦＴＰといったゲートウェイを通過する通信パケット（プロトコルデータ）のトラフィックを監視し、スキャンを実施する。メールのリアルタイム検索では、「zip」や「exe」など検索対象に設定したファイルを検出すると、それらを一時的に別の場所にコピーし、そこでウィルス検索を実行する。そしてそのファイルがウ

ィルスに感染していなければ、コピーを削除して、オリジナルのファイルを宛先に配信し、ウイィスを検出した場合には、自動駆除、隔離、削除などを行ないメールの送信先や送信元に通知をする。

現在のウィルス感染経路の90%以上が電子メールだと言われており、ゲートウェイ型のウィルス対策ソフトは、現時点で非常に重要度の高いウィルス対策である。また最近では、ウィルススキャンに加え、コンテンツフィルタリングの機能を付加した製品も出てきている。

（ウ）その他

クライアント&サーバやゲートウェアイ以外では、ストレージ向けやＰＤＳ向けのウィルス対策ソフトの製品がある。例えばストレージ向けのものは、EMCなど特定のストレージに特化したものであり、ストレージ上にファイルが作成された場合などに、ストレージがサーバのウィルス対策ソフトにファイルを転送し、そこでウィルススキャンを行なうものである。

なおＰＤＡ向けのウィルス対策ソフトについては、まだ日本ではＰＤＡ自体の普及状況が高くないので普及もあまり進んでいない。

⑶ 最新技術

今後のウィルス対策で重要なキーワードの１つとして、「自己防衛型ネットワーク」がある。

「自己防衛型ネットワーク」は、ルータやスイッチなどのネットワーク機器に、ウィルス感染の可能性のあるパソコンからのアクセスや不正と考えられるアクセスを判断する機能を持たせ、ネットワークが自律的にセキュリティ対策を行なう仕組みを実現するというものである。現在さまざまなウィルス対策ベンダが、「自己防衛型ネットワーク」の実現に向けて製品の提供を始めている。また、日本では携帯電話の普及が進んでいるため、Ｊａｖａなどで開発されたプログラムを利用できる端末が一般化してきており、ウィルスの標的となることも充分に考えられるため、携帯電話向けアンチウィルスエンジンの開発が進められている。

さらに管理ツールの中には、他ウィルス対策ベンダのウィルス対策ソフトの管理も可能なｐものがる。これにより、グループウェア用はＡ社のウィルス対策ソフト、他はＢ社のウィルス対策ソフトを適用するといった使い方も可能にはなるが、まだ１社のウィルス対策ソフトで統一した方が、より効率的な運用・管理が可能になる。

5-3-3-10 認証

⑴ 認証技術状況

従来、本人を認証する方法としてパスワードやICカード、磁気カードなどが利用されてきた。しかし、広く利用されているパスワードの場合、キーストロークのログをとる「キーロガー」などで不正にインストールしてパスワードを盗み、本人になりすまして侵入した事件や、オンラインでの不正侵入の手口として、パスワード破りなど、現実に色々な事件が発生している。そこで、最近では人体に関わる特徴を用いたバイオメトリクス認証が注目されている。

バイオメトリクス認証の特徴は、指先にある「指紋」で認証を行うものや、本人の声である「声紋」によって確認するもの、手のひらにある「静脈」の形によって判別するものなど、一人ひとりが持っている生体の特徴をとらえてそれを情報として事前に登録しておき、その内容と照らし合わせて本人か否かを確認することができることである。以下にその主なものを示す。

- 指紋 指先の指紋を利用した認証方法
- 虹彩 瞳孔の薄膜組織模様を利用した認証方法
- サイン 筆跡、筆圧を利用した認証方法
- 声紋 発音時の声紋を利用した認証方法
- 網膜 網膜の表面血管パターンを利用した認証方法

・ 掌型 掌の幅、長さ、厚さなどの形状を利用した認証方法
・ 顔 顔形状を利用した認証方法
・ 手のひら静脈 手のひらの静脈パターンを利用した認証方法

現在では、これらの認証を使ってクライアントやサーバのログインなどに利用したり、データセンターなどの出入口などでの入退場の管理などで利用されている。

5-3-3-11 ネットワーク監視・管理

(1) 技術概要

ネットワーク監視ツールは従来、障害が起きた箇所を特定し、原因をつきとめる目的で利用されていた。今後もその機能の重要度が低下することはないが、最近では障害の起きる予兆を発見し、未然に防止し、将来のネットワーク構成改善に向けてのキャパシティプランニングを適切に行うために利用することが多くなってきている。現在のネットワーク監視・管理機能には、以下の機能がある。

（ア）構成管理

現在のネットワークの構成がどうなっているのか、またどのような機器が配置されているのかはを正確に把握する必要がある。

常に機器変更を含めた構成管理を自動的に行うのが、ネットワーク監視ツールの役割である。これを実現するためにＳＮＭＰという管理用の標準プロトコルがあり、ネットワーク機器それぞれがもっている管理情報（ＭＩＢという）から機器固有の管理情報を拾い、マネージャと呼ばれるコンソールでネットワーク全体の構成を管理する。　ＳＮＭＰベースのネットワーク監視ツールはこの機能に優れており、大規模ネットワークや重要なネットワークには必ず導入されている。

構成管理は、どの機器がどのポートに接続されているか、また特定の種類の機器のみを選んで視覚的に表示することが可能で、機器の変更や追加が行われても自動的にそれが捕捉できるようになっている。　構成管理はすべての管理のベースとなるものであり、トラフィック監視とともに用いることにより、障害対応をより迅速に行うことができる。

（イ）障害管理

障害管理機能は、機器のダウン（障害）時間を最小にするために重要な機能である。ＳＮＭＰベースの管理ツールの場合は、機器をポーリングして常に状況を把握しているため、機器に障害が発生すると、管理画面でその機器が障害の重要度に応じて特定色でアラート表示され、機器状態やトラフィック状況などをすぐに確認することができる。また担当者へのメール送信などのアクションを設定して自動的に対処が行える機能もある。さらに機器の障害で初めて通知するのではなく、障害の予兆となる動きが見られたときに警告を発するように設定も可能である。

イベント発生の判断は、機器状態の各種項目にしきい値を設け、それを超えた場合に段階に応じて必要な警告や対処を自動的に行うようにする。その設定には、統計的なしきい値は自動設定されるようになっていて、微調整程度で自由に利用できるようになっている（管理担当者が一定期間の稼働の後、適切な値に設定することも可能である。）

（ウ）性能管理

性能管理は通常、各機器のトラフィック状態を監視し、パフォーマンスを測定するところから始まる。ＳＮＭＰベースのツールでは定期的に送信/受信パケットを捉えて統計的な情報として表示する。トラフィック監視タイプのツールでは、監視対象のセグメントの概況をエージェントから取り込み、ほぼリアルタイムで表示することも可能である。。統計情報はどちらのタイプでもレポートが各種作成でき、詳細な分析と改善につなげられる。

以上、ネットワーク監視・管理の主要機能を説明したが、ネットワーク監視・管理ツール導入によって管理を実施するとき、他の管理ツールとの組み合わせ、将来の管理機能拡張に備えることが必要となる。

(2) 最新技術

最近多くなってきているセキュリティホールを攻撃するワームの発生は、企業のセキュリティ体制の見直しを迫る脅威となっている。ウィルス対策ソフトだけでは、最近のワームには対応できないのが現状である。

PCが1台感染しネットワークに接続すると、そのネットワークではたちまちウィルス感染が蔓延してしまう。この危険を防ぐには、セキュリティパッチを確実に、漏れなく全クライアントに適用することが大切で、社内へのパソコンの移動、持ち込み、持ち出しのルールを決め、遵守させるなど、セキュリティポリシーにのっとった運用ルールを確立し、遵守状況を絶えず検証できる仕組みが必須ウとなる。これに対応するために導入されるのが、資産管理ツールである。資産管理ツールでは、現在保有しているクライアントやサーバの各種情報を収集し管理し、パッチ適用やポリシー遵守を徹底させるための機能が充実している。

また、現状のシステム構成を把握していれば、新たに持ち込まれたパソコン及び不正に接続されたパソコンを検出することが可能となる。 ポリシー違反した接続やアプリケーション稼働を迅速に検知し、管理者への警告を行うことができるネットワーク監視ツールが出てきており、個人用のパソコンの接続や、ポリシー上許されていない機器接続、機器移動、アプリ稼働などを検知し、迅速な対処を行うことが可能である。最近の製品では、自動的にモバイルパソコンなどをネットワークに接続した時点でサーバに送信する仕組みで対応している。

5-3-3-12 鍵管理

(1) 鍵管理技術状況

認証局で発行する証明書(鍵)については、信頼性が必要となる。これに対応するために、認証局で鍵の生成、保管、署名操作や、ユーザの秘密鍵を保管する耐タンパ性を実現するハードウェアがある。通常これらの操作をコンピュータで行う場合、コンピュータ自身の損壊、不当な侵入による鍵の盗難、不正な複製などのリスクがある。

鍵管理の専用機(ハードウェア)であるHSMは、鍵生成や暗号化のロジックを隠し、不正行為を実質上、不可能にし鍵管理や信頼性の維持に万全を期すことができる。現在では、電子署名法関連法案にもその使用が義務付けられているものである。

またHSMでは、煩雑な操作や高度な物理的セキュリティ要件を伴わないことに加え、アクセラレーション(処理の高速化)機能も備えており、パフォーマンス面でも優れた性能を発揮することができる。

最近では、米国情報標準技術局(NIST)が政府調達の基準として定めたFIPS140－140-1(暗号モジュールのセキュリティ要件)に適用したHSM製品が日本でも提供(販売)されている。

5-3-3-13 ログ監視・管理

(1) 技術概要

システム内の各サーバのログは、常に採取し定期的に一元管理する必要がある。

ＵＮＩＸ系のサーバでは、ｓｙｓｌｏｇを利用して実現することが可能であるが、Ｗｉｎｄｏｗｓ系のサーバのログ、アプリケーションのログ、そして最近導入が進んでいる専用機（アプライアンスサーバ）の独自のログなどを統合的に管理することはできていないのが現状である。

なおアプリケーションのログについては、各アプリケーション（例：Ｗｅｂサーバやファイア

ウォール等）に対応した分析・レポートをグラフィックに編集・出力するソフトウェアが多数提供されている。

(2) 技術概要

最近では、ログを一元管理し定期的なバックアップをするだけで無く、ログを常に監視し管理者の設定により管理者へのメール通知などをするログ管理ツールが提供されている。このログ管理ツールを利用すれば、システム内で発生している状況をリスルタイムに確認することができシステム管理者は、効率的なシステム運用を実現することができる。

さらにこのログ管理ツールを機能アップした、ログ分析ツールも出現している。

前述したように、今までのログ分析ツールは、単一のアプリケーションに対応していた。しかし最新のログ分析ツールは、ある事象に対する他のログの相関関係を確認し統合的なログ分析を可能にしている。このツールを利用すれば、ＩＤＳでの検知した事象に対して該当サーバでの問題有無の確認やファイアウォールでの予兆などを自動的に確認しその結果をレポートしたり管理者に通知したりすることができる。

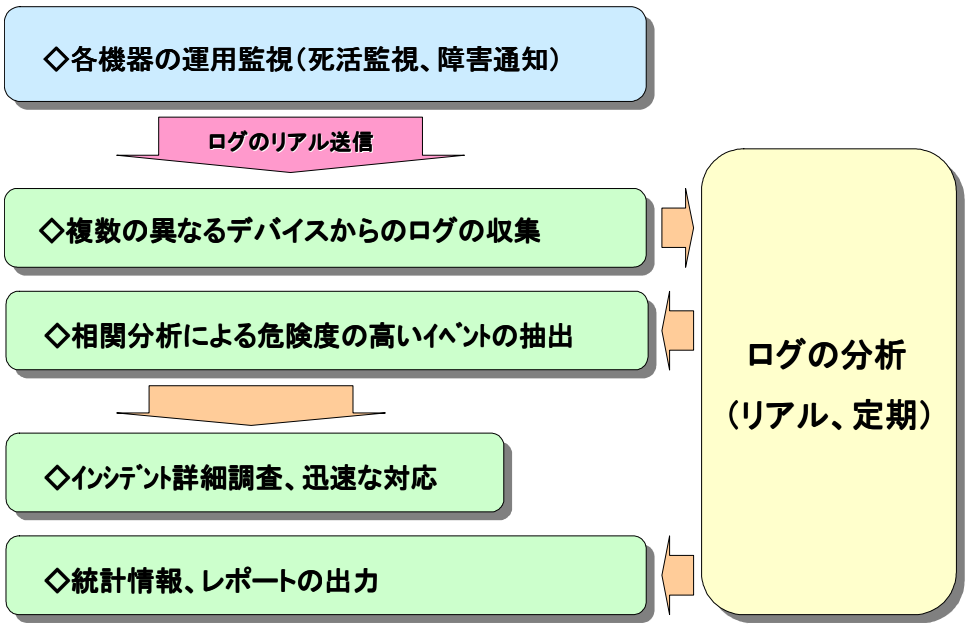


図 19 ログ分析の方法案

5-3-3-14 総評

本研究では、参照実装モデルについて現在適用可能なセキュリティ対策技術について調査したが、その結果を以下に示す。

◇クライアントとサーバ間の通信でSSLを採用し処理性能と信頼性を確保できるか？

・SSLアクセラレータ等を利用し処理性能を向上させる仕組みが必要
・負荷分散装置等により信頼性（処理性能）を向上させる仕組みが必要
・上記機器の組み合わせによる処理能力の評価が必要

◇認証の処理どのようにするか？処理性能を確保できるか？（証明書による認証、バイオメトリックスなどによる認証？）

・センター接続時の認証方法（クライアント認証）の評価が必要
（クライアント証明書による認証、サーバ証明書による認証）
・各処理における認証方法（ユーザ認証）の評価が必要
（ICカードやバイオメトリックスによる認証）
・認証サーバの運用・管理方法の評価が必要（どのようにするか？）
（証明書の管理、鍵の管理）

◇センターのサーバ構成及びネットワーク構成をどうするか？

・処理能力（想定）に合わせたサーバ台数の確保
・負荷分散装置等により信頼性を向上させる仕組みが必要
・ファイアウォール、IDS、ウィルス対策等のセキュリティ機器の評価
・上記機器及び認証方法の組み合わせによる処理能力の評価

・ネットワーク構成（信頼性など含）の詳細な検討が必要
（インターネット回線の二重化。LANの分割、LANの二重化　等）

◇セキュリティ対策の運用形態をどのようにするか？（異常や障害をどうように検知し対処するのか？）

・各機器（サーバ、NW機器）でのログ採取は必須
・異常や障害をどのように検知し運用者に通知するかが不明確
・ログ分析（多種多様のログ）をどのように実施するか？
（分析方法、サイクル、報告方法など）

5-3-3-15 今後の課題

本研究では、サブテーマ２に記載している運用要件及びサブテーマ５に記載している参照実装モデルのセキュリティ対策技術について調査した。

現時点でのセキュリティ対策技術については、調査した結果、現時点では以下に示すセキュリティ対策技術が参照実装モデルに適用することが可能である。

・ファイアォールの適用（専用機の設置）
・ＳＳＬアクセラレータの適用（専用機の設置）
・ＶＰＮ装置の適用（専用機の設置）
・ＩＤＳ（ＩＤＰ）の適用（専用機の設置）
・ウィルス対策の適用（ゲートウェイ型専用機の設置）
・鍵管理の適用（ＨＳＭの設置）
・ネットワーク監視・管理の適用（構成管理、障害管理、性能管理）
・資産管理の適用（資産状況管理、不正接続管理、パッチ適用）

今後参照実装モデルへのセキュリティ対策技術の適用については、十分な検討をして実施する必要がある。また現時点でまだ十分な技術がされていないセキュリティ対策技術については、さらに調査をし検討が必要である。

セキュリティ対策技術は、常に変わっており今後も継続し調査をする必要がある。また適用可能であるセキュリティ対策技術については、具体的な導入検討を行い製品の選定をし、実際のシステムに組み込み評価をする必要がある。最終的には、適用すべきセキュリティ対策技術を決定し、製品としての評価を実施する必要がある。

5-4　セキュリティポリシー

本節では、「5-4-1背景・目的」から「5-4-5参考」までは「ICカードのプロテクションプロファイル」に関する報告を行い、「5-4-6 ISMSの基本的な考え方」から「5-4-7 まとめ」までは「ISMS」に関する報告を行い、「5-4-8 米国国防総省 SERVE(安全な電子登録および投票実験)のセキュリティ分析報告」は「SERVE」の概要の報告を行っている。また、「詳細・補足編」では国内で行われた電子投票(第一世代)に関連したインタビューをまとめた。

米国国防総省が推進しているSERVE(安全な電子登録・電子投票実験)に対するセキュリティ分析報告については、著作権の問題があるため、ここには概要紹介のみに限定している。

5-4-1 背景・目的

平成14年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」では、システム全体を俯瞰した際のセキュリティについての考察が行われた。本年はさらに踏み入って、より詳細なセキュリティ要件について考察する。ここでは、次世代電子投票におけるICカードの部位についてのプロテクションプロファイル(以下PP)について調査検討する。

ICカードは住基カード(住民基本台帳カード:2003年7月 発行枚数300万枚[8])やSUICAカード(2003年7月 発行累計668万枚[9])、ICテレホンカード(1999年の年間発行枚数 約800万枚[10])など、確実に我々の生活に浸透してきている。セキュリティが深刻な問題として唱えられる昨今、セキュリティと利便性の両方を向上させることが出来るICカードの存在意義はその重みを増してきている。世界規模での浸透を表すかのように、ICカードのPP作成は、国内外に少なくない事例を持つ。

PPが世の中に多く存在する現状から、次の課題が生まれてくる。ある製品に関係したPPが既に開発済みである場合、その製品のセキュリティターゲット(以下ST)作成時に開発済みのPPを参照、引用することができる。しかしながら、それでST作成が楽になったか、というと、必ずしもそうではない。多数のPPが存在する時、どのPPを適用するか、が課題となる。

更に、数多く存在する既存のICカードのPPについて、その特色、適用領域を比較した文献は稀少である。特に、日本の文献と海外の文献を同列に並べて比較対照したものは存在していないようである。従って、この調査結果は今般の次世代電子投票・アンケートシステムの構築にあたって、どのようなPPを用いるべきかの指針となることを想定する。今後、他のICカード関連システムにおいても、十分参考となる情報と考える。

具体的な調査方法として、現在オープンになっているPPについて、どのようなものがあるのか、どのような特徴を持っているのか、について調査を行う。特に、それぞれのPPが持つセキュリティの問題意識を中心に調べる。即ち、対象としている脅威とセキュリティ対策目標を比較する。その後、次世代電子投票・アンケートシステムに相応しいカードPPとは何か、について考察を行う。この調査・考察の結

8 Mainichi INTERACTIVE　http://www.mainichi.co.jp/digital/network/archive/200307/10/6.html
9 一枚の IC カード乗車券で関東圏の鉄道・バスをもっと便利に
http://www.jreast.co.jp/press/2003_1/20030712.pdf
10 IC カード利用促進協議会 | IC カード市場の動向 http://www.jicsap.com/sysintro/shijo.html

果、次世代電子投票・アンケートシステムに用いるICカードのPPについて、大まかな枠組みを提示することを、目的とする。

5-4-2 調査について

ここでは、今回の調査方法・調査対象および比較結果を示す。

5-4-2-1 調査方法

国内外のオープンになっているPPについて、想定しているTOEの定義及び範囲、それに対する脅威、セキュリティ対策目標の違いを比較する。Webでの情報収集を中心に行う。なお、PPの実態を深く知るため、専門家・関係者からのヒアリングも行った。

5-4-2-2 調査対象

先に触れたように、ICカードのPP作成の事例で、オープンになっているものは少なくない。しかし、次世代電子投票・アンケートシステムで用いるICカードのPPに適合するPPばかりではない。今回は調査対象のPPとして、比較的話題に登場するものを選んだ。しかしながら、TOEの範囲があまりに「ICカードを利用するシステム」という観点からかけ離れているものの幾つかを省略した(LSIチップのPPなど)。

住民基本台帳カードはオープンになっているPPの資料がないため、調査が困難であった。また、Suica、Eddyなどで馴染みが深いFelicaについても、ISO15408のEAL4の認定[11]を受けている(RC-S860)ため、調査対象としたかったが、問い合わせた結果、ソニー(株)としてはプロテクションプロファイルを保持していないことが判明し、そこで調査を断念した(本来、PPは調達者から発行するものであるから、ソニー(株)の責任で出せるものではない)。

具体的調査対象PPは以下のとおりである。

スタンダードなPPとして

- Visa Smart Card Protection Profile
- Smart Card Security User Group's Protection Profile
- Smart Card Integrated Circuit with Embedded Software Protection Profile(Eurosmart)
- Smart Card IC Platform Protection Profile(Eurosmart)
- ICカードプロテクションプロファイル(ICカード取引システム研究開発事業組合)

マルチアプリケーションのPPとして、

- The Smart Card IC with Multi-Application Secure Platform Protection Profile (Eurosmart)
- JICSAP ver2.0 Protection Profile part1 Multi-Application Secure System LSI Chip Protection Profile
- IT装備都市研究事業　アプリケーション・プログラム・ローディング機能付きICカードのセキュリティ要求仕様書

単体のアプリケーションのPPとして

- EMV ICC Credit & Debt Application Protection Profile
- PKIスマートカードプロテクションプロファイル(情報処理振興事業協会)

[11] Felica 概要　http://www.sony.co.jp/Products/felica/contents02_02.html

また、一部機能に特化したものとして

・Secure Signature – Creation Device Protection Profiles

・Intersector Electronic Purse and Purchase Device Protection Profile

・ICカード取引システム研究開発事業組合 ICカードリーダライタプロテクションプロファイル

5-4-2-3 比較結果

(i) 網羅的比較

比較調査結果は以下のとおりである。

対象とする正式名称、バージョン、発表日時、著者、PP認可番号、TOEの定義、TOEの範囲、対象資産、PPの脅威とセキュリティ対策目標、EALおよびSoF、EAL+の要因(EAL4+にするために加えるPP項目)を比較パラメータとした。以下にその比較結果を示す。

表 27 VSCPP,SCSUG PP,EMV-app PP, PP/9911 (1/2)

正式名称	Visa Smart Card Protection Profile (VSCPP)	Smart Card Security User Group's Protection Profile (SCSUG PP)	EMV ICC Credit & Debit Application Protection Profile(EMV-app PP)	Smart Card Integrated Circuit with Embedded Software Protection Profile
バージョン	Draft Version 1.6	Version 3.0	Draft Version0.4	Version 2.0
発表日時	May 4,1999	9 September 2001	14th December 2001	June 99
著者	Visa International Service Association	Smart Card Security User Group	EMVCo	Eurosmart Security Working Group
PP 認可番号		PP/0103		PP/9911
TOE の定義	スマートカード IC、OS、アプリケーション	IC、OS、CAD (Card Acceptor Device)	オンカードアプリケーションについて、EMV 仕様書に則ったEMVトランザクション処理が動作するもの	IC と組み込みソフトウェア
TOE の範囲	自動販売機、PC スマートカードリーダなど多くの種類のカード読み取り機を含む従来型のスマートカードの使用される環境	IC、OS、外界と通信する接触型 ISO-7816、非接触型 ISO-14443 メカニズムを含む	EMV の必須要求条件に限る。スマートカードハードウェアやカード OS ソフトウェアは含まない。	開発、環境構築、パッケージング、パーソナライズ、エンドユーザ環境での利用といった、スマートカードICのライフサイクルの全てのフェイズ
対象資産	明白に定義していない	カード所持者のデータ、セキュリティ属性、認証データ、アクセスコントロールリスト、TOE セキュリティプロセスにおける暗号鍵などのユーザデータ	1.EMV トランザクション処理を正しく行うアプリケーションの能力 2.アプリケーション実装とアプリケーションデータ	IC チップ自身、それと全ての仕様書、ソフトウェア、参照される文書、開発ツールと技術、アプリケーションデータ

表 28　VSCPP,SCSUG PP,EMV-app PP, PP/9911 (2/2)

正式名称	Visa Smart Card Protection Profile (VSCPP)	Smart Card Security User Group's Protection Profile (SCSUG PP)	EMV ICC Credit & Debt Application Protection Profile (EMV-app PP)	Smart Card Integrated Circuit with Embedded Software Protection Profile
脅威	・物理的および論理的な攻撃の脅威・不適切な仕様の脅威・セットアップ、ソフトウェア、ハードウェア設定時のエラーの脅威 ・ライフサイクル機能の相互作用を利用する、予期しない相互作用の脅威 ・暗号機能の脅威・データフローの脅威 ・TOE 設計、仕様、実装、秘密情報の発覚・露見・製品、IC マスク、ツールの盗難・設計、実装、秘密情報の(不当な)修正・干渉すること	・プロービングや TOE の変更(オルタネーション)など、TOE への物理的攻撃による脅威 ・間違いの挿入や繰り返しなど、TOE への物理的攻撃による脅威 ・不正アクセスや初回利用時の不正など、アクセスのコントロールによる脅威 ・許可されてない機能を用いるなど、予期せぬ相互作用による脅威 ・暗号機能についての脅威 ・情報漏洩など画面情報の脅威 ・環境ストレスやクローニングなど雑多な脅威・OS、特権ユーザの濫用などによる脅威 その他、環境への脅威が定義されている	TOE への間違い入力、数種類の通信失敗(情報漏洩、TOE のリセットへの直面、トランザクションデータへの脅威、TOE の干渉)	盗み、改変、資産の露見、部分的もしくは全部の許可無き複製といった悪戯を含み、Phase1(カードの要件定義) ～ 7(カードの有効期限切れ)までの TOE ライフサイクルのフェイズごとに脅威が定義されている。
TOE のセキュリティ対策目標	・TOE の物理的、論理的防衛 ・TOE データ、ファイルのアクセスコントロール ・情報漏洩への抵抗 ・ライフサイクル機能、セットアップシーケンス、複数アプリケーションのサポート ・暗号機能の安全な実装 ・ターミナルへの安全な通信手段 ・間違いデータの繰り返し探索 ・TOE メモリ整合性、チェック ・IT スタンダードに従順であること	・TOE 物理的及び論理的防衛 ・TOE データ、ファイルへのアクセスコントロール ・情報漏洩への抵抗 ・ライフサイクル機能、初期化、セットアップシーケンス、マルチアプリケーションのサポート ・暗号機能のセキュアな実装 ・カード読み取り機器との安全なコミュニケーション方法のサポート ・繰り返し攻撃や誤りのあるデータの繰り返しプロービングへの抵抗 ・セキュリティ関連イベント及び TOE ごとの同一性の監査	・データオブジェクトのアクセスコントロールとセキュリティポリシーの一致 ・TOE の間違い入力データへの繰り返しプロービングに対する抵抗 ・情報の漏洩を制限し、コントロールする手段の提供 ・全ての TOE が再起動した状態で、初期状態を維持する ・通信か電源が落ちても、セキュア状態を維持する ・不正入力からの自己防衛 ・TOE プラットホームの必要な暗号機能を提供し、物理的、論理的な脅威に抵抗する ・ターミナルは EMV 関連の機能をサポートして、それが証明されなければならない	タンパー耐性、複製防止、正常操作の保証、設計・実装・操作の欠陥の無いこと、情報漏洩の防止、メモリ内情報の保護。その他環境要件が別個に明示されている
EAL、SoF	EAL4+/SoF-medium	EAL4+/SoF-high	EAL4+/SoF-high	EAL4+/SoF-high
EAL+の要因	ADV_INT.1　開発方法 – TSF 内部構造 – モジュール構成 AVA_VLA.3　脆弱性アセスメント – 脆弱性分析 – 抵抗力中	ADV_INT.1 開発方法 – TSF 内部構造 – モジュール構成 AVA_VLA.3　脆弱性アセスメント – 脆弱性分析 – 抵抗力中	・ADV_IMP.2 開発 – 実装表現 – TSF の実装ほか ・AVA_VLA.3 脆弱性アセスメント – 脆弱性分析 – 抵抗力中	ADV_IMP.2 開発 – 実装表現 – TSF の実装 ALC_DVS.2 ライフサイクルサポート – セキュリティ開発-セキュリティ手法の十分さ AVA_VLA.4 脆弱性アセスメント-脆弱性分析 -抵抗力高

表 29　Smart Card IC Platform PP,PP/0010,IEP&PD PP(1/2)

正式名称	Smart Card IC Platform Protection Profile	The Smart Card IC with Multi-Application Secure Platform Protection Profile	Intersector Electronic Purse and Purchase Device Protection Profile(IEP&PD PP)
バージョン	Version1.0	Version 2.0	Version1.3
発表日時	July 2001	November 2000	March 2001
著者	Eurosmart Security Working Group	Eurosmart Security Working Group	Societe Financiere du Porte-Monnaie Electronique Interbancaire
PP 認可番号		PP/0010	PP/0101
TOE の定義	演算装置、セキュリティコンポーネント、I/O ポート(接触、非接触とも)、揮発性及び不揮発性メモリ、物理的にスマートカード IC に設置されるもの、ファームウェアなどの IC ソフトウェアを実装したスマートカード IC	(Java カードなどの)マルチアプリケーションがサポートされたスマートカードプラットホーム	電子財布と POS
TOE の範囲	ライフサイクルの全てのフェイズ	スマートカードプラットホームの従来型コンポーネント、アプリケーションシステムインタフェースとアプリケーションレイヤにロードされたネイティブもしくはコンパイルされたソフトウェア。ライフサイクルの全てのフェイズを対象とする。	電子財布と POS の双方
対象資産	ユーザデータ、組み込みソフトウェア、IC、ファームウェア、関連する文書だけでなく、TOE の操作、乱数についてなども含む	PPがアプリケーションを含まなくても、TOEはネイティブもしくはロードされたセキュリティメカニズムでユーザデータを守る。	汎用の電子財布の支払いシステムとその環境

表 **30　Smart Card IC Platform PP,PP/0010,IEP&PD PP(2/2)**

正式名称	Smart Card IC Platform Protection Profile	The Smart Card IC with Multi-Application Secure Platform Protection Profile	Intersector Electronic Purse and Purchase Device Protection Profile(IEP&PD PP)
脅威	・SC1-ユーザデータとスマートカード組み込みソフトウェアの誤魔化し操作 ・SC2-ユーザデータとスマートカード組み込みソフトウェアの露見 ・SC3-乱数の不完全性	盗み、改変、資産の露見、部分的もしくは全部の許可無き複製といった悪戯を含み、Phase1(カードの要件定義) ～7(カードの有効期限切れ)までの TOE ライフサイクルのフェイズごとに脅威が定義されている。PP/9911 に比べ Personalization およびライフサイクルの終了時に多くの脅威が挙げられている。	マネーロンダリング、IEP の自己同一性の強奪、繰り返し、トランザクション中で発生する障害、偽造、拒絶機能、真正性の消失
TOE のセキュリティ対策目標	・SG1-ユーザデータとスマートカード組み込みソフトウェアの完全性維持 ・SG2-ユーザデータとスマートカード組み込みソフトウェアの秘匿性維持 ・SG3-乱数の提供	PP/9911 に挙げたタンパー耐性、複製防止、正常操作の保証、設計・実装・操作の欠陥の無いこと、情報漏洩の防止、メモリ内情報の保護に加え、ロールバック時、アプリケーションの読み込みと削除、アプリケーション同士の隔離、リソースの管理が書かれている。その他環境要件が別個に明示されている	認証されない EV の生成と消失、変更を防ぐ方法、ユーザデータへの権限者以外のアクセスを防ぐ、正常な操作を保証する、タンパ耐性、電子財布が上限額を越えないことのチェック、IEP アプリが隔離されていること
EAL、SoF	EAL4+/SoF-high	EAL4+/SoF-high	EAL4+/SoF-high
EAL+の要因	ADV_IMP.2 開発-実装表現 - TSF の実装 ALC_DVS.2 ライフサイクルサポート - セキュリティ開発-セキュリティ手法の十分さ AVA_VLA.4 脆弱性アセスメント-脆弱性分析 - 抵抗力高 AVA_MSU.3 脆弱性アセスメント - 誤用 - セキュアでない状態での分析とテスト	ADV_IMP.2 開発 - 実装表現 - TSF の実装 ALC_DVS.2 ライフサイクルサポート - セキュリティ開発 - セキュリティ手法の十分さ AVA_VLA.4 脆弱性アセスメント-脆弱性分析 - 抵抗力高	ADV_IMP.2 開発 - 実装表現 - TSF の実装 ALC_DVS.2 ライフサイクルサポート - セキュリティ開発-セキュリティ手法の十分さ AVA_VLA.4 脆弱性アセスメント-脆弱性分析 - 抵抗力高

表 **31　SSCD-PP,IC** カード **PP,IC** カード **R/W PP (1/2)**

正式名称	Secure Signature – Creation Device Protection Profile (SSCD-PP)	ISO/IEC 15408 情報技術セキュリティ評価基準準拠 IC カードプロテクションプロファイル	ISO/IEC 15408 情報技術セキュリティ評価基準準拠 ICカードリーダライタプロテクションプロファイル
バージョン	Version1.05	1.1 版	1.1 版
発表日時	28 July 2001	平成 12 年 1 月 7 日	平成 12 年 1 月 7 日
著者	CEN/ISSS	IC カード取引システム研究開発事業組合	IC カード取引システム研究開発事業組合
PP 認可番号			
TOE の定義	スマートカードに限らないあらゆるタイプの署名生成機器の署名アプリケーションのセキュリティ要件	金融決済や公的 ID 管理システムなどセキュリティ確保が求められる様々な情報システムにおいて、アプリケーションプログラムを特定せずに IC カードを安全に使用するための一般的なセキュリティ要件	端末から ICC のセキュリティ確保に直接関係する部分を切り出した形。 アプリケーションプログラムは定義しないがファームウェアは搭載する
TOE の範囲	スマートカードに限らないあらゆるタイプの署名生成機器の署名アプリケーションのセキュリティ要件	CPU とメモリを持ついわゆるスマートカードを対象とし、チップカードやメモリカードは対象としない。外部端子付き、外部端子無しの双方を対象とする。カード OS も本 PP の範囲である。ICC 発行後は ICC 上で動作するアプリケーションプログラムは変更されないようなカード OS を対象とする。JICSAP Ver.1.1 の仕様に準拠して、ICC 発行後のファイルの創生、削除を許している。	スマートカードの読み書きを行うものであり、チップカードやメモリカードを読み書きするものではない。
対象資産	SCD、SVD、署名済みの文書、PIN やバイオメトリクスなどの参照情報、署名作成機能、作られた電子署名	不揮発性メモリに格納されるデータ、プログラムコード、キー	鍵（SM 内）、セキュリティ関連プログラム（SM 内）、ファームウェア、通過データ（KeyPad からのデータ、ユーザデータ、表示ユニット表示データ）、揮発性メモリ内データ

表 **32　SSCD-PP,IC** カード **PP,IC** カード **R/W PP (2/2)**

対象資産	Secure Signature – Creation Device Protection Profiles (SSCD-PP)	ISO/IEC 15408 情報技術セキュリティ評価基準準拠 IC カードプロテクションプロファイル	ISO/IEC 15408 情報技術セキュリティ評価基準準拠 IC カードリーダライタプロテクションプロファイル
脅威	・物理的プロービング ・SCD を引き出す攻撃 ・SVD か署名の偽造 ・ホストコンピュータにおける署名作成アプリケーションによって署名が行われるデータの改変	・コマンド・インタフェースを用いて、データやキーを不正に読み出す ・コマンド・インタフェースを用いて、データやキーを不正に変更する ・プロービングにより、データやキーを、不正に読み出す ・プロービングにより、データやキーを、不正に変更する ・インフォメーションリーク攻撃により、データやキーを、不正に読み出す ・環境ストレスを与えることにより、処理異常を起こさせデータやキーを、不正に読み出す ・プロービングにより、プログラムコードを、不正に変更する ・テストプログラムにより、プログラムコードを、不正に変更する ・物理的観察により、プログラムコードを、不正に読み出す	・物理的な攻撃により鍵を不正に読み出す ・物理的な攻撃により鍵を不正に変更する ・プロービング技術を応用して、セキュリティ関連プログラムを不正に変更する ・不揮発性メモリの空き領域にプログラムを組み込み,セキュリティ関連プログラムを不正に変更する ・不揮発性メモリ内のプログラムを不正に変更し、SM をスキップさせる ・製造過程で不正なプログラムを組み込み,利用時に・活性化させることにより TOE のセキュリティ機能を無効化する ・インタフェース間で盗聴することにより、Key–Pad から入力されたデータを不正に読み出す ・プロービングにより、Key–Pad から入力されたデータを不正に読み出すインタフェース間で盗聴することにより,ユーザデータを不正に読み出す ・インタフェース間でデータをすり替えることにより、ユーザデータを不正に変更する ・プロービングにより,ユーザデータを不正に読み出す ・プロービング技術を応用してデータをすり替え、ユーザデータを不正に変更する表示ユニットと MPU 間の通過データを不正に変更し,実データと異なる値を表示させる
TOE のセキュリティ対策目標	・物理的プロービング ・SCD を引き出す攻撃 ・SVD か署名の偽造 ・ホストコンピュータにおける署名作成アプリケーションによって署名が行われるデータの改変に対する防衛	・データが不正に読み出されない、変更されない ・プログラムコードが不正に読み出されない、変更されない ・キーが不正に読み出されない、変更されない	・TOE は機能の完全性を保障すること ・TOE は内部に保持されているデータの機密性・完全性を保障すること ・TOE は通貨データの機密性・完全性を保障すること ・TOE へのダウンロード時には相互認証をすること ・TOE にダウンロードされるデータの完全性を保障すること ・TOE は通信相手を認証できること、TOE は個別に識別可能なこと
EAL、SoF	EAL4+/SoF–high	EAL4/SoF–medium	EAL4/SoF–medium
EAL+の要因	AVA_MSU.3　脆弱性アセスメント – 誤用 – 分析とセキュアでない状態のテスト AVA_VLA.4　脆弱性アセスメント – 脆弱性分析 – 抵抗力高	AVA_VLA.3　脆弱性保証	ADV_IMP.2　TSF の実装 AVA_VLA.3　脆弱性保証

表 33　JICSAP2.0 PP、PKI スマートカード PP、AP ローディング機能付き IC カード PP (1/2)

正式名称	JICSAP ver2.0 Protection Profile part1 Multi-Application Secure System LSI Chip Protection Profile	PKI スマートカードプロテクションプロファイル	IT 装備年研究事業　アプリケーション･プログラム･ローディング機能付き IC カードのセキュリティ要求仕様書
バージョン	Version2.5	バージョン No.1.1	第 1.0 版
発表日時	June 6,2003	2002 年 2 月 20 日	平成 13 年 12 月 10 日
著者	(Issuers)Japan IC Card System Application Council (Authors)Electric Commerce Security Technology Research Association	情報処理振興事業協会	(財)ニューメディア開発協会
PP 認可番号	PP/0301		
TOE の定義	演算ユニット、メモリ、コプロセッサなどを搭載したシステム LSI チップ、ハードに依存したソフトウェア	PKI スマートカードとは、スマートカードに PKI 鍵ペア及びデジタル証明書を安全に格納するスマートカード上のセキュリティアプリケーションのことを指す。	演算回路、記憶素子、コプロセッサなどの集積回路を内蔵し、記憶素子に組み込まれたソフトウェアにより高度なセキュリティ機能を提供。アプリケーションプログラムがカード発行前または発行後にネットワークとリーダライタ等を通じて IC カード側にダウンロードして供給されることを想定。PP の対象は外部から電源が供給されるタイプに限る。
TOE の範囲	アプリケーションとは異なるメモリと回路の設定。暗号ライブラリや試験ソフトウェアの幾多のライブラリを含む。	本 PP の TOE には、PKI スマートカードのスマートカードアプリケーションだけが含まれる。PKI スマートカードに関連するその他の製品は、TOE に含まれない。PKI スマートカードアプリケーションと同じスマートカードにロードされた悪意を持つアプリケーションに関しては、考慮しない。	住民カードとして、各種の行政サービスが受けられるカード 銀行カードとして預貯金の預け入れ、引き出し、即時決済の出来るカード 安全なデータ蓄積媒体としての特徴を生かした電子財布用カード 高度な医療サービスが可能となる医療情報の格納カード
対象資産	ユーザデータ、TSF データ、ハード依存ソフトのプログラムコード	TOE が署名及び復号を行うため、最も重要となる情報資産はスマートカードに格納された PKI 秘密鍵である。加えて、ユーザの PC に返送される署名データ及び復号データは重要であり、情報資産とみなされる。これらの情報資産の機密性及び完全性は保護されなければならない。	1)ダウンロードされるアプリケーションが使用するデータやアプリケーションプログラムそのもの 2)TOE の生産過程で作られたり、また利用されたりする情報

表 **34　JICSAP2.0 PP、PKI** スマートカード **PP、AP** ローディング機能付き **IC** カード **PP (2/2)**

正式名称	JICSAP ver2.0 Protection Profile part1 Multi-Application Secure System LSI Chip Protection Profile	PKI スマートカードプロテクションプロファイル	IT 装備年研究事業　アプリケーション･プログラム･ローディング機能付き IC カードのセキュリティ要求仕様書
脅威	・半導体知識をもつ攻撃者による物理的攻撃 暗号と回路知識がある攻撃者による隠しチャネル探し ・暗号と回路知識がある攻撃者による特別な機器を用いてのメモリ内データの推定 ・回路知識のある攻撃者による特別な機器を用いての不要な I/O ポートの利用	・悪意を持つ者による繰り返し認証請求、TSF データ変更、認証試行の無制限化、認証情報の不正入手、不正ログオン、TOE に格納された秘密情報の改変、秘密情報削除後の残存データ盗難、TOE から PC 上のアプリケーションに返送する復号データを通信経路上で盗聴、署名の生成及び秘密情報の復号を行う ・正規ユーザが TOE を使用している間に、悪意を持つ者が不正なアプリケーションを使用して TOE にコマンドを送る ・悪意を持つ者や PC 上の不正なアプリケーションによる TSF 迂回 ・管理者による所有者のスマートカードを乱用 ・悪意を持つ者が署名データを通信経路上で改変しても、署名者は署名が改変されたことに気づかないこと ・大量のデータをスマートカードの通信路へ送信することによるデータオーバーフロー	・論理インタフェイスを悪用し、ユーザデータや TSF データの改ざん、漏洩 ・論理インタフェイスの繰返し攻撃で、TSF データを漏洩 ・TSF サービスの不完全な終了による、ユーザデータや TSF データの改ざん ・漏洩不正な人がアプリケーションプログラムをロードし、ユーザデータや TSF データの改ざん、漏洩 ・管理用端末を悪用し、ユーザデータや TSF データの改ざん、漏洩発行過程の TOE 悪用
TOE のセキュリティ対策目標	・TOE は物理的攻撃に対して演算ユニット、メモリ、電子回路の安全を確保する ・TOE は IC の内部演算への妨害を防ぐメカニズムの保持 ・TOE は物理的に危険な状態でさえセキュリティを維持することが出来なくてはならない ・TOE は IC を利用する環境に必要の無い I/O ポートが開発者にでさえ利用されるのを防ぐ	・TOE は、署名及び復号操作が可能となる前に、各ユーザの識別及び認証を実施し、連携する PC 上のアプリケーションも認証する。また、連続して認証情報の入力に失敗すると、TOE はロックされる ・利用できる操作を、ユーザの役割により制限 ・署名及び復号操作を行う都度、認証情報を使って識別及び認証 ・発行されたスマートカードは、TSF データを変更することはできない ・TOE とユーザの PC 上で起動するアプリケーション間で交換される秘密情報の保護 ・権限を持った者が適切なタイミングで認証情報の変更を行う。 ・削除時に秘密情報完全消去 その他、環境に対するセキュリティ要件が定義されている。	・TSF は、論理インタフェイス、利用出来るユーザ、利用できる Assets を明確にしなければならない ・TSF は Authorized User のみがユーザデータへアクセスできることを保証しなければならない ・TSF は、発行作業及び発行作業完了を明確にし、Administrator のみが行えることを保証しなければならない ・TSF は、Authorized User のみが Trouble Shooting を行えることを保証しなければならない ・TSF は、繰り返し攻撃に耐えうるセキュリティ機構を装備しなければならない ・TSF は、アプリケーションプログラムの resource 競合防止を保証しなければならない ・TSF は、TSF サービス時の異常を検出し、再起動時には異常検出前の状態からサービスを開始しなければならない ・TSF は、TSF サービスで利用する作業域にユーザデータや TSF データを残さないことを保証しなければならない
EAL、SoF	EAL4+/SoF-high	EAL4/SoF-medium	EAL4+/SoF-high
EAL+の要因	AVA_CCA.1　隠しチャンネル分析 AVA_VLA.4　脆弱性アセスメント-脆弱性分析-抵抗力高		AVA_VLA.3　脆弱性アセスメント － 脆弱性分析 － 抵抗力中

(ii) TOE の範囲の比較

ICカードシステムのセキュリティ範囲を明確に比較するため、以下の調査を行った。

ICカードシステムの構成は

- カード(EEPROM、CPU、RAM、コプロセッサなどのいわゆる基本ハードウェア)
- カードOS
- カードOS上のミドルウェアソフト(Java,NICE[12],JICSAP仕様など)
- 個別アプリケーション
- 関連するリーダライタ

という部品から成り立つ(図 20参照)。従って比較にあたっては、この図 20を基本テンプレートとした。

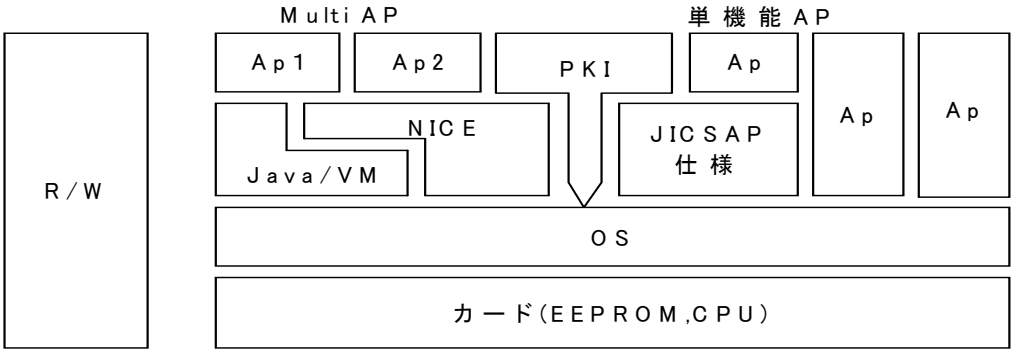


図 20 IC カードシステムの基本構成(IC カード自身とリーダライタのアーキテクチャ)

ICカードのPPは、カードのハードウェアやソフトウェアの何処までをPPの対象範囲とするかが、それぞれのPPの特色といえる。今回の調査対象であるプロテクションプロファイルについて、個別に図 20のテンプレートに基づき、対象範囲を明示した。それが図 21から図 33の各図である。

[12] NICE は、NTT が開発した IC カードプラットホーム(Network-based IC Card Environment)の略 NTT 情報流通プラットフォーム研究所 IC カード情報流通プラットホーム NICE
http://www2.pflab.ecl.ntt.co.jp/index/kenkyu/html/16.html

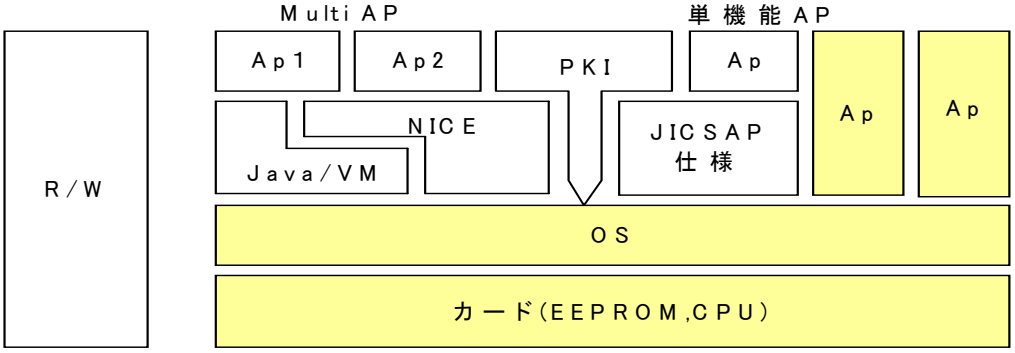


図 21　Visa Smart Card Protection Profile

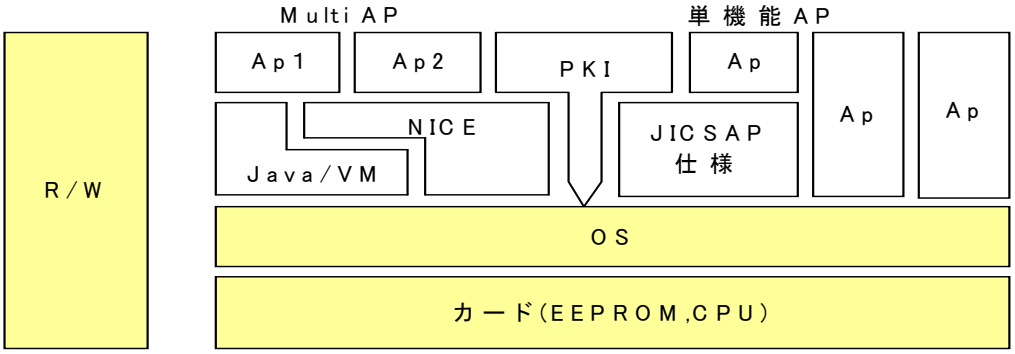


図 22　Smart Card Security User Group's Protection Profile

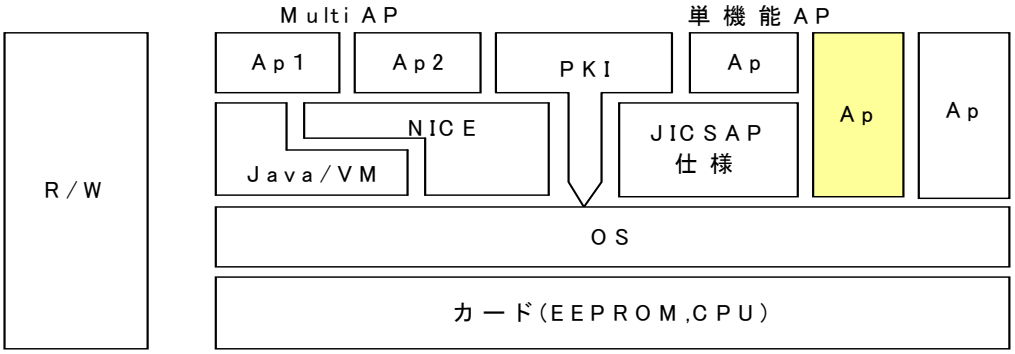


図 23　EMV ICC Credit & Debt Application Protection Profile

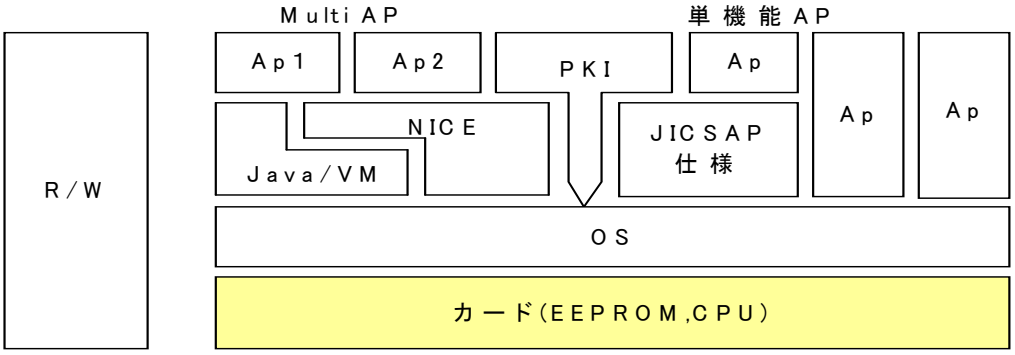


図 24　Smart Card Integrated Circuit With Embedded Software

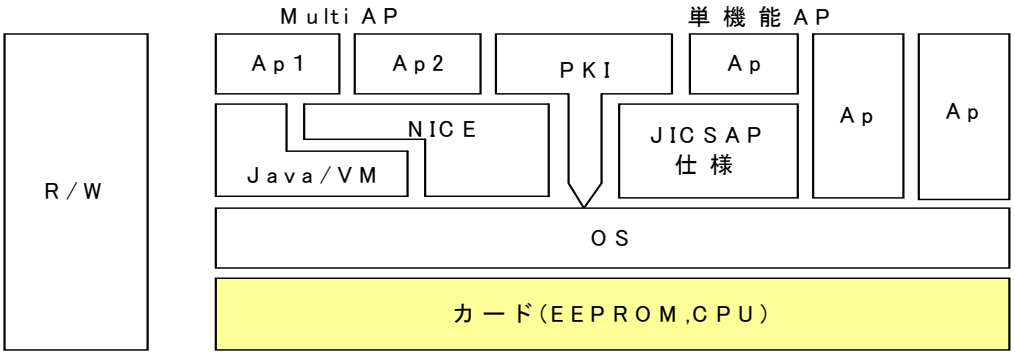


図 25　Smartcard IC Platform Protection Profile

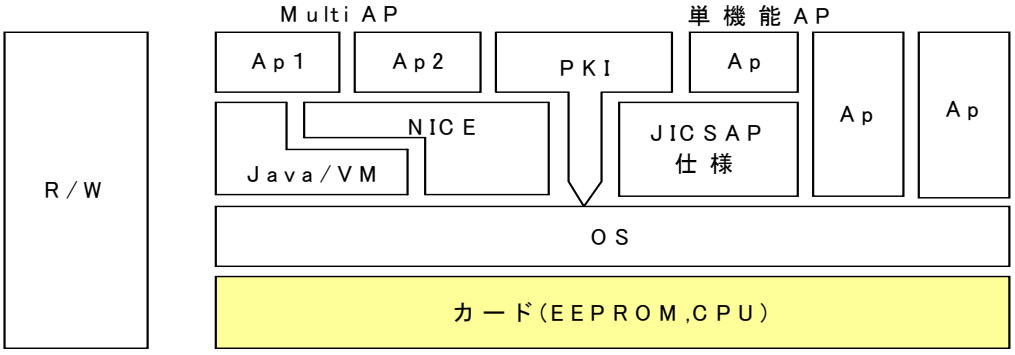


図 26　Protection Profile Smart Card IC with Multi-Application Secure Platform

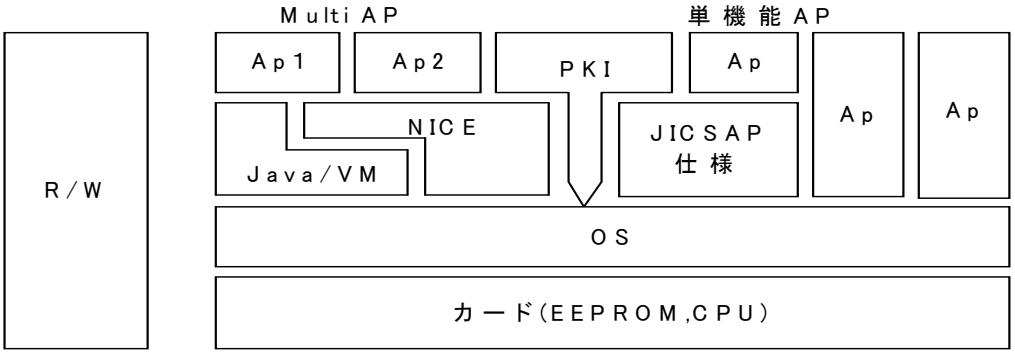


図 27　Intersector Electronic Purse and Purchase Device

上記範囲内に記述することは出来ない

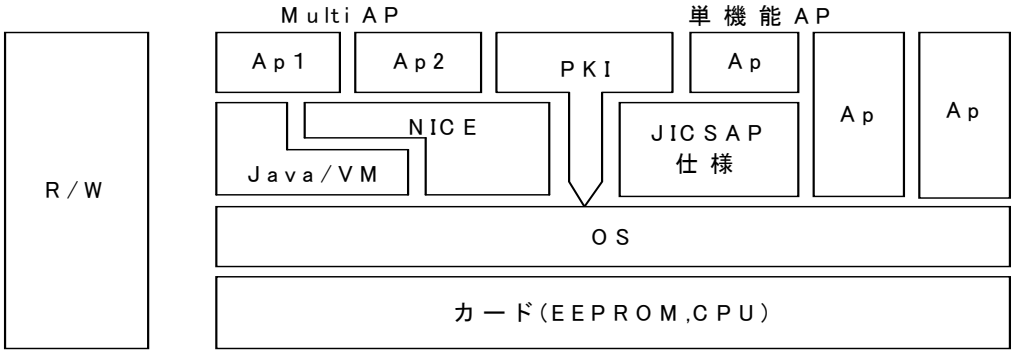


図 28　Secure Signature - Creation Device Protection Profiles

上記範囲内に記述することは出来ない

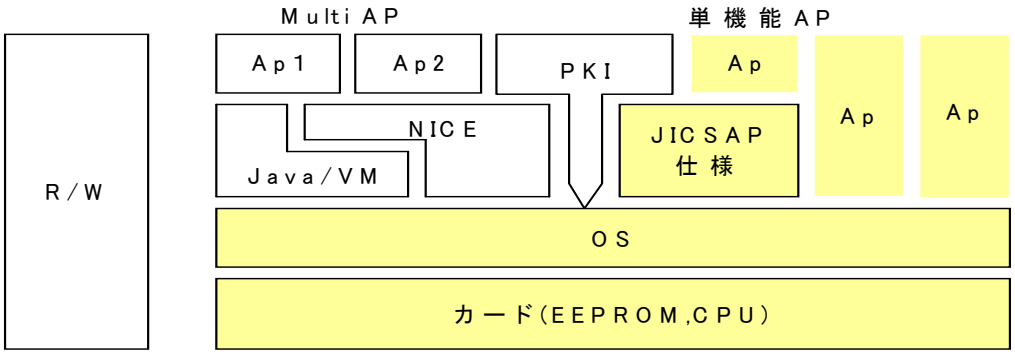


図 29　IC カード取引システム研究開発事業組合　IC カードプロテクションプロファイル

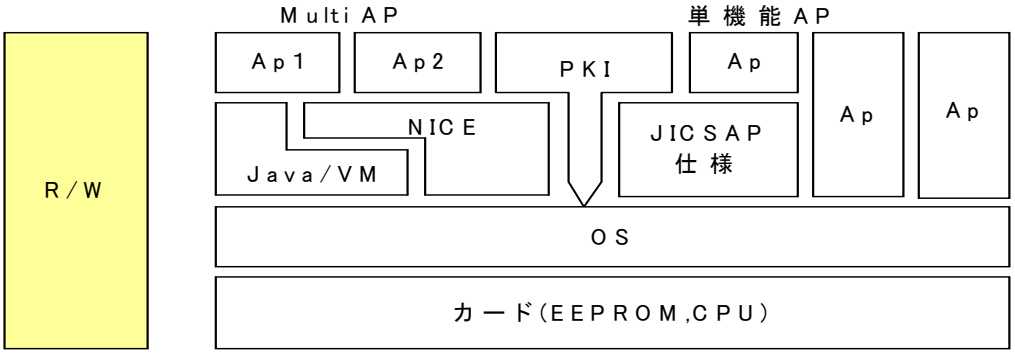


図 30 IC カード取引システム研究開発事業組合 IC カードリーダライタプロテクションプロファイル

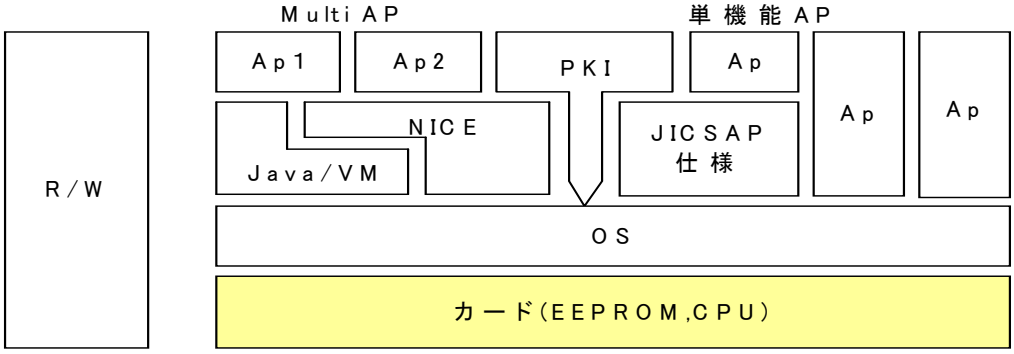


図 31 JICSAP ver2.0 Protection Profile part1 Multi-Application Secure System LSI Chip Protection Profile

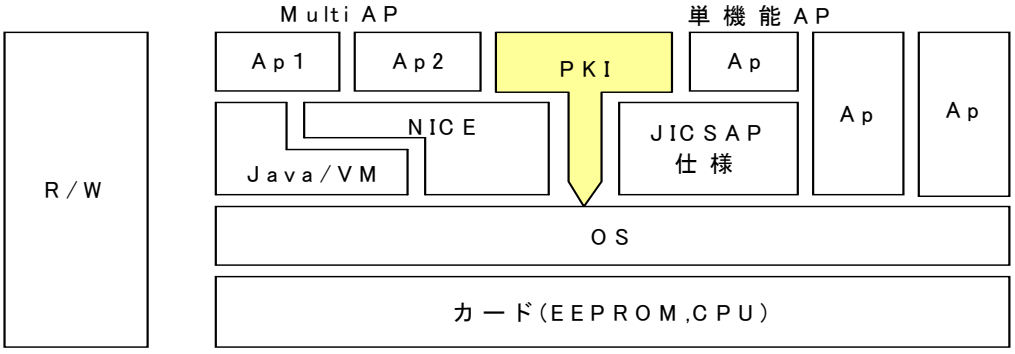


図 32 PKI スマートカードプロテクションプロファイル

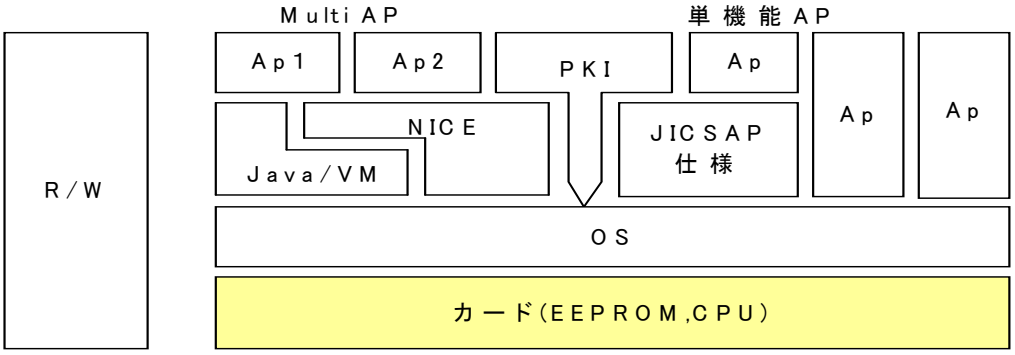


図 33 アプリケーション・プログラム・ローディング機能付き IC カードのプロテクションプロファイル

図 21から図 33のTOEまで、対象とする範囲を記述した。また、TOEの対象ではない範囲が明示されている場合は、それについても記述した。

Visa Smart Card Protection Profile

TOEの対象 ： IC、OS、(複数の)アプリケーション

TOEの対象でないもの ： 券面の印刷、磁気ストライプ、ホログラム、カードリーダライタ、ICカードインタフェースのネットワーク

Smart Card Security User Group's Protection Profile(SCSUG-PP)

TOEの対象 ： IC、OS、CAD(Card Accepter Device)

TOEの対象でないもの ： 特定のアプリケーション

EMV ICC Credit & Debt Application Protection Profile

TOEの対象 ： オンカードアプリケーションについて、EMV仕様書に則ったEMVトランザクション処理が動作するもの

Smart Card Integrated Circuit with Embedded Software Protection Profile

TOEの対象 ： 組み込みソフトウェアを搭載した集積回路

Smart Card IC Platform Protection Profile

TOEの対象 ： 演算装置、セキュリティコンポーネント、I/Oポート(接触、非接触とも)、揮発性及び不揮発性メモリ、IC設計/製造、ファームウェアなどのICソフトウェアを実装したスマートカードIC

TOEの対象でないもの ： その他全てのソフトウェア

The Smart Card IC with Multi-Application Secure Platform Protection Profile

TOEの対象 ： 開発段階～IC製造段階～スマートカード製造段階～パーソナライゼーション＆テスト段階～利用される段階に至るまでのマルチアプリケーションがサポートされたスマートカードプラットホーム

Intersector Electronic Purse and Purchase Device

TOEの対象 ： 電子財布と購入装置(POS)

TOEの対象でないもの ： 財布から財布への移動等の機能、オフラインでの再読み込み、電子財布、返済機能、通貨交換機能、自動読み出し機能、最新の購入のキャンセル

Secure Signature – Creation Device Protection Profiles

TOEの対象 ： SCDの作成の機能要件と保証要件

ICカード取引システム研究開発事業組合 ICカードプロテクションプロファイル

TOEの対象 ： 様々な情報システムにおいて、アプリケーションプログラムを特定せずにICカードを安全に使用するための一般的なセキュリティ要件を記述している。ハードウェア的にはCPUとメモリを持ついわゆるスマートカードを対象とし、いわゆるチップカードやメモリカードは対象としない、また、ICC外部インタフェースとして、金属端子を使用した外部端子付きICCと静電結合や電磁結合あるいは電磁波等を利用した外部電子端子なしICCがあるが、外部端子付き、無しの双方を対象とする。CPUを搭載したICCの機能は概ねカードOSに依存するため、当然ながらカードOSも本PPの範囲である。ICC発行後はICC上で動作するアプリケーションプログラムは変更されないようなカードOSを対象とする。JICSAP Ver1.1の仕様に準拠して、ICC発行後のファイルの創生、削除を許している。

TOEの対象でないもの ： アプリケーション。ICC発行後にICC上でアプリケーションをダウンロード、削除できるカード

ICカード取引システム研究開発事業組合 ICカードリーダライタプロテクションプロファイル

TOEの対象 ： ICCと直接に情報の送受信を行うICカードリーダライタ(ATM、CAT、POS等)のセキュリティ確保に直接関係する部分。アプリケーションプログラムは搭載しないがファームウェアは搭載し、必要に応じて、上位よりダウンロードによる変更を可能とする。

TOEの対象でないもの ： アプリケーションは特定しない。

JICSAP ver2.0 Protection Profile part1 Multi-Application Secure System LSI Chip Protection Profile

TOEの対象 ： LSIチップ(IC)、演算ユニット、メモリ、コプロセッサ、その他(テストソフトウェア、暗号ライブラリ)

PKIスマートカードプロテクションプロファイル

TOEの対象 ： PKIスマートカードのスマートカードアプリケーションだけが含まれる。
企業などの組織で用いられる。

TOEの対象でないもの ： PKIスマートカードに関連するその他の製品(例えば、PC上で起動し、TOEと連携して動作するアプリケーション)は、TOEに含まれない。TOEはスマートカード上で起動する。スマ

ートカードには、CPU及びメモリが搭載されており、また、オペレーティングシステムがある場合もあるが、これらのスマートカードコンポーネントは、TOEに含まれない。

アプリケーション・プログラム・ローディング機能付きICカードのセキュリティ要求仕様書

TOEの対象 ： 演算回路（CPU：Central Processing Unit）、記憶素子(ROM,RAM,F-RAM,EEPROM,etc)、Co-Processor等の集積回路を内蔵し、記憶素子に組み込まれたソフトウェアにより高度なセキュリティ機能を提供している。また、アプリケーションプログラムが、カード発行前または発行後に、ネットワークとリーダライタ等を通じて、ICカード側にダウンロードによって供給されることも想定している。本PPで対象とするのは外部から電源が供給されるタイプ(接触タイプと非接触タイプ)である。

TOEの対象でないもの ： 直接には、IT装備都市研究事業において使用されるアプリケーションロードが可能なICカードを対象とするものであるが、同事業のICカードシステムはアプリケーションを特定していない。電源内蔵タイプのICカード(接触タイプ非接触タイプは問わず)は対象ではない。

5-4-3 考察

これまでの調査はオープンになっている PP を対象にしているので、あくまで一般論としての PP の比較となっている。一方で、本題とする次世代電子投票・アンケートシステムの個別論として PP のあるべき姿を以下に考察する。

まず初めに次世代電子投票・アンケートシステムが利用する IC カードの要件を平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」に基づき次に整理する。

5-4-3-1 次世代電子投票・アンケートシステムが利用する IC カードの要件

次世代電子投票・アンケートシステムが利用するICカードの要件は、以下のように定められている。

○ICカードには、以下の内容が格納されている[13]

- ・センター1用共通鍵：C1-S
- ・センター2用準同型公開鍵：C2-P
- ・票作成プログラム
- ・投票者証明書(認証局の署名付き)

○票データの格納[14]

ICカードが作成する票データは「暗号化済み票データ[15]」である。これにより、票作成プログラムは票データの暗号化を行うものである、と考えることが出来る。

---

[13]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P187 5-4-2-7 投票者 PC の構成と役割

[14]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P220 5-4-7-2 票暗号化アプレット機能

[15]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P220 5-4-7-2 票暗号化アプレット機能

○ICカード上の実装　～べき乗剰余演算～

ICカードで用意されている機能を十分に活用して、べき乗剰余演算の性能アップを計る。べき乗剰余演算では多倍長演算やメモリの使用方法が性能に著しく影響を与えるため、この点に十分注意をする[16]

○ICカード上の実装　～高次剰余暗号関数～

投票者用であるICカード上の高次剰余暗号関数(暗号機能)の実装および性能評価を実施した[17]。

○ICカード上の実装　～コプロセッサ～

ICカードには、多倍長演算を最適に実行するための機能(コプロセッサ)を搭載しているタイプが存在する。従って、適したコプロセッサを搭載したICカードを選定する[18]。

これらの要件を満たすものとして、ICカードの選定が行われた。

○使用するICカードの要件

リーダ・ライタとの通信速度を考慮に入れ、接触型とする[19]。

○使用するICカードの要件

E社のICカード(CPU:16bit　周波数:3.5712Mhz,4.9152Mhz,コプロセッサ搭載(暗号強度は非公開)、メモリ:8KB、EEPROM:1MBのカード)を採用する[20]。

---

[16]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P224 5-5-1-3　現状の課題と研究

[17]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P224 5-5-1-4. 研究内容③H14 年度の効果

[18]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P231 5-5-2-2.演算ライブラリ調査　(ii)多倍長演算ライブラリの比較　b)IC カード実装

[19]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P232 5-5-2-3.高次剰余暗号実装検討　(ii)IC カードの高速化　a)IC カードの選定

[20] [20]平成 14 年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」 P232　5-5-2-3.高次剰余暗号実装検討　(ii)IC カードの高速化　a)IC カードの選定

表 35　次世代電子投票・アンケートシステムの IC カードに求められる要件

格納されているもの	・センター1用共通鍵：C1-S ・センター2用準同型公開鍵：C2-P ・票作成プログラム ・投票者証明書(認証局の署名付き)
べき乗剰余演算	行う
高次剰余暗号関数(暗号機能)	実装している
コプロセッサ	搭載
通信タイプ	接触型
CPU	16bit
周波数	3.5712Mhz, 4.9152Mhz
メモリ	8KB
EEPROM	1MB

5-4-3-2　考察(1) マルチアプリケーション IC カードを利用する場合のセキュリティ要件:アプリケーション間のファイアウォールの考察

平成14年度研究開発成果報告書「次世代電子投票・アンケートシステムとその社会的利用に関する研究」では、単機能のICカードが要件であった。しかし、将来性を考えれば、マルチアプリケーションのICカードを視野に入れておく必要がある。この観点から考察を加える。

マルチアプリケーションICカードの場合、ミドルウェアソフトにファイアウォールが必須であることを述べる。即ち、ファイアウォールが存在しないと仮定すると、アプリケーションが特定されない限りセキュリティ要件は割り出せない。例え、ある程度特定あるいは限定されているとしても、それぞれのアプリケーションの組み合わせの数のPPを検討しなければならなくなる。一方でファイアウォールが存在するとすれば、各アプリケーションとミドルウェアソフトの間のPPが存在すれば良い。すなわち、アプリケーションの数だけのPPを検討すれば良いことになる。従って、ファイアウォールは必須といえる。

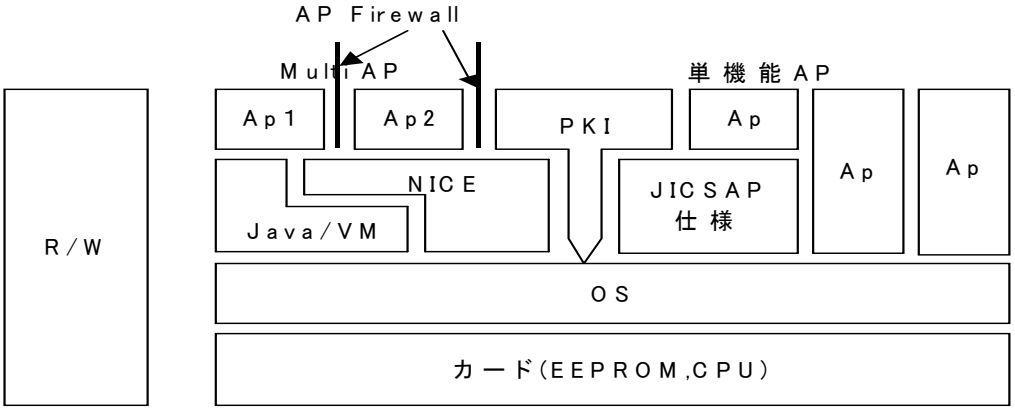


図 34　アプリケーション間のファイアウォール

アプリケーション間のファイアウォールに求められる要件は、住民基本台帳カードでは総務省が以下のように定義している[21]。

・情報を設定されたカードアプリケーション間は「アプリケーションファイアウォール」により、カード内でそれぞれ独立している。
  - 属性制御方式:属性情報に従ってメモリへのアクセス許可する方式(属性情報＝読み出し専用/読み書き可能/実行可能/アクセス不可などの属性を表す)。
  - ページ管理方式:ページ番号+論理アドレスでアクセス許可を行う方式(ページ＝メモリ上でのAPの論理的配置を表す単位)。
  - 仮想マシン方式:仮想マシンがAPのプログラムを解釈実行する方式(仮想マシン＝Java-VMなどにより実現されるアプリケーション実行環境) [22]。

アプリケーション間のファイアウォールは各社が実装しており、JavaCardの「アプリケーションファイアウォール」、Multosの「ファイアウォール」とFelicaの「アプリケーション・ファイアウォール」などがある。
JavaCardとMultosカードはソフトウェアで実装しているが、Felicaはハードウェアで実装している(詳細は「5-1.アプリケーション間のファイアウォールについて」を参照のこと)。
以上、マルチアプリケーションICカードのセキュリティを考える場合、現状ではアプリケーション間のファイアウォールは必須である。

5-4-3-3　考察(2)　PKI スマートカードの適用性について

次世代電子投票・アンケートシステムの機能要件からして「センター1用共通鍵」、「センター2用準同型公開鍵」をICカードに格納する要件があり、同様のセキュリティ要件はPKIスマートカードのPPに記述されている。従って、次世代電子投票・アンケートシステムで用いるICカードの、ことアプリケーション部位について、必要な要素を最も多く持つPPはPKIスマートカードのPPと言えよう。だが、現状のPKIスマートカードのPPでは、APIに関する記述はされていないため「票作成プログラム」をカバーできない。すなわち、PKIスマートカードに閉じたものとなっている。

[21]総務省　住民基本台帳カードの構造について（システム面のセキュリティ対策）
http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_card_01.pdf
[22] 総務省　住民基本台帳カードの構造について（システム面のセキュリティ対策）
http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_card_01.pdf

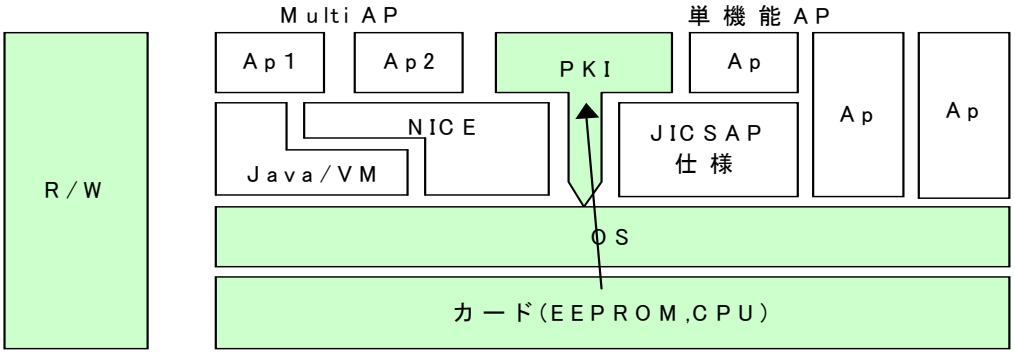


図 35　単機能の次世代電子投票・アンケートシステム用 IC カード(1)

電子投票のアプリケーションが載らないので使えない。

従って、次世代電子投票・アンケートシステムで用いられるICカードの要件としては、PKIスマートカードにAPIの記述、PKIスマートカードを利用するプレイヤーとの関係でセキュリティを定義・検討する必要がある。

単機能のICカードの場合、図 36のようにPKIスマートカードアプリケーションと電子投票・アンケートシステムで用いられるアプリケーションを繋ぐAPIが作成される、という解決法が考えられる。

マルチアプリケーションICカードの場合、図 37のようにPKI環境をミドルウェアソフトに吸収させるという解決法も考えられる(逆に、ミドルウェアソフトが票作成アプリケーションの機能を持つことも想定しうる)。

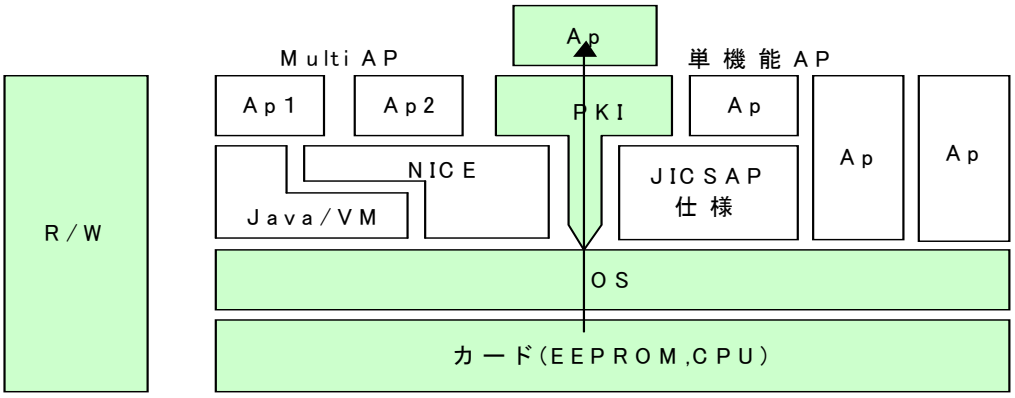


図 36　単機能の次世代電子投票・アンケートシステム用 IC カード(2)

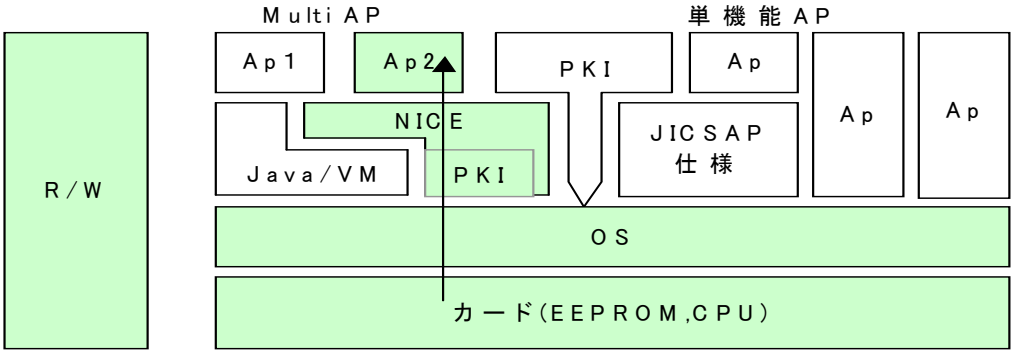


図 37　他のアプリケーションとの相乗効果がある場合（NICE を用いる場合）

5-4-3-4　考察(3) 現存する PP の課題の一般論「使われていない」こと

現存するPPは、ICカード業者、行政関係が多大な時間と労力を割いて作成している。しかしながら、現状ではそれらのPPは使われない場合がままある。その原因と対策を考察する。
最大の理由は、STを作成したことが無い人、あるいはSTを作成する能力が無い人が、PPを作ったことに依ると考えられる。
事例を挙げると「PPとして、ICカード内の秘密鍵を盗まれない様にすること」というSecurity対策目標を作ったとする。秘密鍵は公開鍵暗号方式、あるいはデジタル署名を作成するに当たってベースであり、これらの暗号システムのセキュリティを保つ為の根幹となるものである。これをICカードという物理的セキュリティの高いハードウェアに蓄積し、これが外部に盗まれない様にするという条件は、一見もっともらしい要求条件に思える。
しかし、この要求条件は設計する立場に配慮が欠けたものといえる。「盗まれない様にする」とは実現上どの様に具体化すれば良いか、が確定できないからである。即ち、上のPPは使えないPPの一例であろう。
図 38にあるように、PP作成者はST設計者と相互にフィードバックをかけあいながらPPを作成すれば、上のような事態を避けることが可能となる。従って、調達者は開発者からの何らかのフィードバックをかけられるプロセスが必要となる。参考として、カナダ政府は調達に関してRFP(Request For Proposal:調達仕様及びそれに対応する提案要求)、RFI(Request For Information:関連情報要求)、RFQ(Request For Quotation:見積もり要求)の三段階のプロセスを取っている。即ち、RFIでは開発業者から調達仕様(RFP)に関連する実現性の情報収集を行っている。このプロセスで、調達者は例えばPPに対するSTの実現性について開発者に問うことが可能になる。

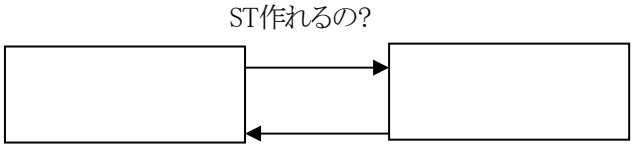


図 38　PP 作成者と ST 設計者

ある製品のPPに脆弱性について新たに条件が加わった時、対応するモジュールを付け加えての解決を行う。ある製品に既存モジュールA,B,Cがあった時(図 39参照)、既存モジュールA,B,Cを総合した全体＝Dと追加モジュールの整合性を検証するのでなく、既存モジュールAと追加モジュール、既存モジュールBと追加モジュール、既存モジュールCと追加モジュールの整合性を検証する。この時、既存モジュール同士の再チェックを行うことは状況により必要になるが、既存モジュールA,B,Cと追加モジュールの整合性がそれぞれ取れているときに、既存モジュール同士の再チェックを行う必要が無いようなモジュール構造が望ましい。
PPがモジュールと対応しているようなPP、STの要求の仕方と実装を理想形と考える。

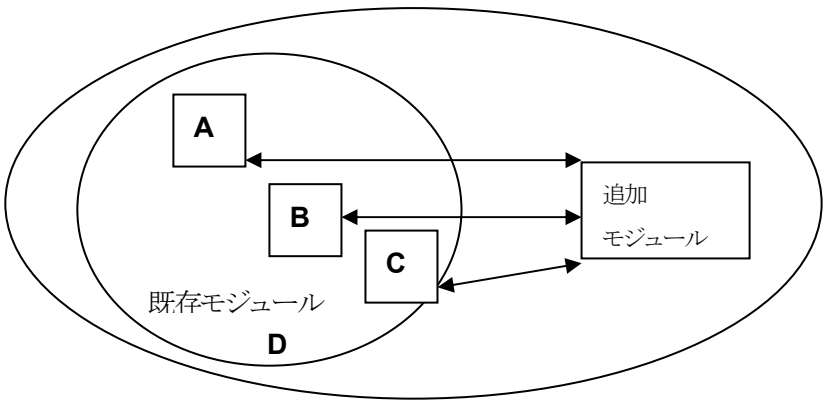


図 39　既存モジュール A,B,C に、新たにモジュールが追加された場合

STの要求の仕方については「Common Criteria for Information Technology Security Evaluation」を参照し、「セキュリティターゲットの作成/検討方法[23]」の所定の書式を用いて記述する。

主な記述項目は以下である。

①ST概要:ST識別、セキュリティ機能の概要など
②TOE記述:利用目的、構成、利用方法など
③セキュリティ環境:資産、前提条件、セキュリティ脅威、組織のセキュリティポリシなど
④セキュリティ対策方針:TOEとTOE環境のセキュリティ対策方針
⑤ITセキュリティ要件:TOEとTOE環境のセキュリティ機能要件、保証条件
⑥TOE要約仕様:ITセキュリティ機能と保証方法
⑦根拠:セキュリティ対策方針の根拠、セキュリティ要件の根拠、TOE要約仕様の根拠、保証方法の根拠

5-4-3-5　考察(4)　共通セットの議論

使われないPPについての考察を考察(3)で行ったが、使えるPPを作成するにあたっては、共通セットのPPを標準的に作成するという考え方がありえる。

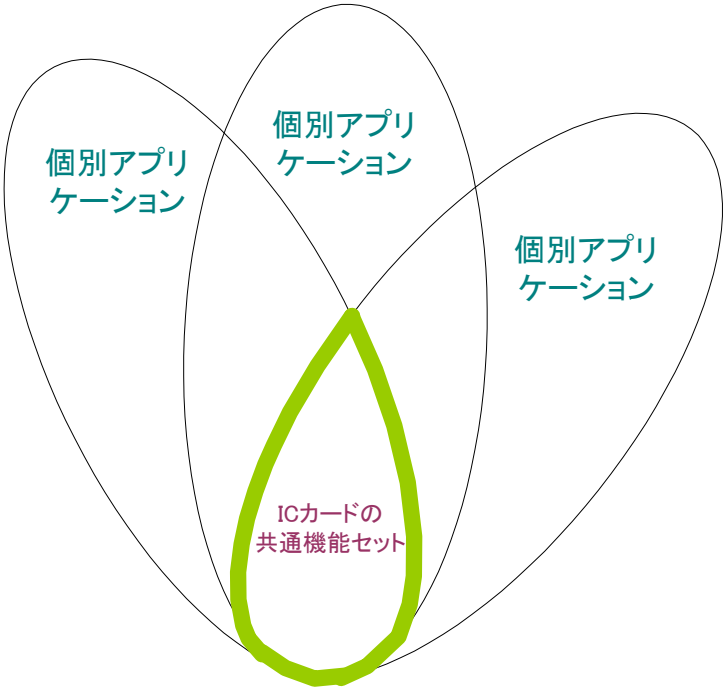


図 40　共通機能セットの絞り込み

[23] IC カードの普及等による IT 装備都市研究事業　開発事業(テーマ 1～6)報告書 4-57　ニューメディア開発協会　2002

ICカードはICカードの基本構成でも触れたように、OSや基本ハードウェアは共通であり、この分野のセキュリティ要件は共通であってしかるべきである。しかし、一方で個別分野(アプリケーション)からの要求条件に合わない部分が生じると想定できる。我々は、(理論的には)個別のPPを加えることで要求条件に見合うPPを作ることが出来ると考えている。但し、PPは加算的に条件を付加出来るが、対処すべきSTはその保証要件の充足性についても網羅的に試験する必要がある。

5-4-4 結論

以上、次世代電子投票・アンケートシステムにおけるPPについて調査検討を行った。検討の結果として、電子投票・アンケートシステムに直接適合するPPは世の中には存在していない。より近いPPとして、アプリケーションレベルではPKIスマートカードがありうるが、考察(2)で述べたように充分ではない。従って、適合するPPを既存のものに求めれば、既存のものの幾つかをピックアップして組み合わせたものになりそうである。

新たに、電子投票・アンケートシステムのPPを作成する場合には、

1)上記の組み合わせたPPをベースとする

2)さらに電子投票の個別アプリケーション(票作成プログラム、票データ)への脅威を分析し、対応するPPを検討する。

更に、実現性のあるPPにするため、考察(3)、考察(4)で述べた点を考慮することが望ましい。

5-4-5 参考

5-4-5-1 アプリケーション間のファイアウォールについて

(i) JavaCard のアプリケーションファイアウォール

松下電器(株)は自社の販売しているJavaCardのアプリケーションファイアウォールについて、以下のように記述している。

「Java Card™は多目的ICカードに最適化されたマルチアプリケーション実行環境を有し、カード発行後にサービス機能を追加できるアプリケーションダウンロード方式を採用する世界標準のカードプラットフォームです。

また、Java Card™の機能によってアプリケーションファイアウォールが無理なく構築でき、金融機関でも実績がある非常に高いセキュリティを有するマルチアプリケーション稼動環境が実現できます。[24]」

(ii) MULTOS カードのアプリケーション間のファイアウォール

雑誌FUJITSU 2000年3月号のマルチアプリケーションマネジメントシステムの特集で、MULTOSカードとJavaCardの双方についての記述に

「スマートカード上の各アプリケーションは、OSが提供するファイアウォール機能により、独立性が保証される[25]」とある。このことから、MULTOSカードのファイアウォールはソフトウェアによって実現されることがわかる。

(iii) Felica のアプリケーション・ファイアウォール

ソニー(株)は自社の販売しているFelicaのアプリケーション・ファイアウォールについて、以下のように記述している。

「FeliCaカードは、一枚のカードの中で多目的のデータを管理することができます。各々のデータには個別のアクセス権を設定することが可能で、これによってアプリケーション間の安全な相互運用が実現されています。ファイルシステムは、「エリア」と「サービス」によって階層状に構成されます。エリアとはフォルダに相当するもので、エリアの下にさらに階層的にエリアを作成することも可能です。サービスは、データに対するアクセスの種類や権限を定義します。

エリアやサービスに設定される「アクセスキー」は、権限の無い者がサービスにアクセスすることを防ぎ、アプリケーション・ファイアウォールを実現しています。また、複数のアクセスキーを合成して作られる「縮退鍵」の技術によって、アクセス対象が複数に渡る場合でも、一回の相互認証で複数のファイルをオープンすることができます[26]。」

---

24 松下電器株式会社　総合的な IC カードシステムソリューションを提供する Java Card™対応非接触 IC カードと IC カード発行・運用管理システムを発売
http://www.matsushita.co.jp/corp/news/official.data/data.dir/jn030609-1/jn030609-1.html

25 雑誌 FUJITSU 2000 年 3 月号 104-108　マルチアプリケーションマネジメントシステム：MAM
http://magazine.fujitsu.com/vol51-2/paper05.pdf　兵藤義以、山手康正　2000 年 4 月

26 Felica 概要　Felica のしくみ　http://www.sony.co.jp/Products/felica/contents02_02.html

Felicaのアプリケーション・ファイアウォールを満たす技術はハードウェア実装であり、インフィニオンテクノロジー社の「SLE66CLX320P」および「SLE66CL80P」などのチップによってアプリケーション・ファイアウォールが実現されているという。

「可能な最高度のセキュリティ要件を満たすため、多様なレベルの物理的保護（アクティブ・シールドなど）と、業界最強のDPA/SPA（Differential Power Analysis/Simple Power Analysis）アタック対策を含む暗号サポートとが組み合わされています。オンチップMMU（メモリ管理ユニット）には、複数のアプリケーションをセキュアに分離するためのハードウェア・ファイアウォールが組み込まれています[27]。」

以上、マルチアプリケーションICカードでのアプリケーション間のファイアウォールには、ソフトウェアでの実装とハードウェアでの実装の両方の手段があることがわかる。

[27] インフィニオンテクノロジーズジャパン株式会社ニュースルーム　2002年11月5日
http://www.infineon.jp/news/press/p0211012.htm

5-4-6 ISMS の基本的な考え方

ISMS は、電子投票において要求される情報セキュリティを実現するための、有効な手段の一つである。その特徴は、大きく2つにまとめられる。ひとつは、リスクマネジメントサイクルの考え方に沿って、手順を踏んだ対策の策定が可能になることである。その結果、各自治体が、それぞれの状況に合致した管理手法を構築できる。もうひとつは、機器の安全性やネットワーク上の技術セキュリティだけでなく、物理的に外部から侵入される脅威や内部者による不正行為など、幅広い脅威を対象として考えられるようになることである。これまでの情報セキュリティにおいても、物理的な対策などを考慮していなかったわけではないが、ISMS では、BS7799 もしくはISO/IEC17799 といった世界的規模で受け入れられている規格が存在するため、網羅的に情報セキュリティの必要事項を検討できるという利点がある。以下、この 2 つの特徴について簡単に説明する。

5-4-6-1 リスクマネジメントサイクル

ISMS は、基本的に組織が情報セキュリティに関する対策を、手順を踏んで策定し、継続的に実践するための枠組みである。したがって、多くの場合、企業や団体などの組織が、自分の組織が情報セキュリティを日常的に実践できるようにするための拠り所として採用する。

ISMS では、リスクマネジメントサイクルの考え方が導入されている。これは、組織が保護すべき情報資産を明確にし、それに対するリスク評価を実施した後、適切な管理策を策定し実践するというものである。さらに、ISMS では、実践した結果を見直し、改善していくことが規定されている。

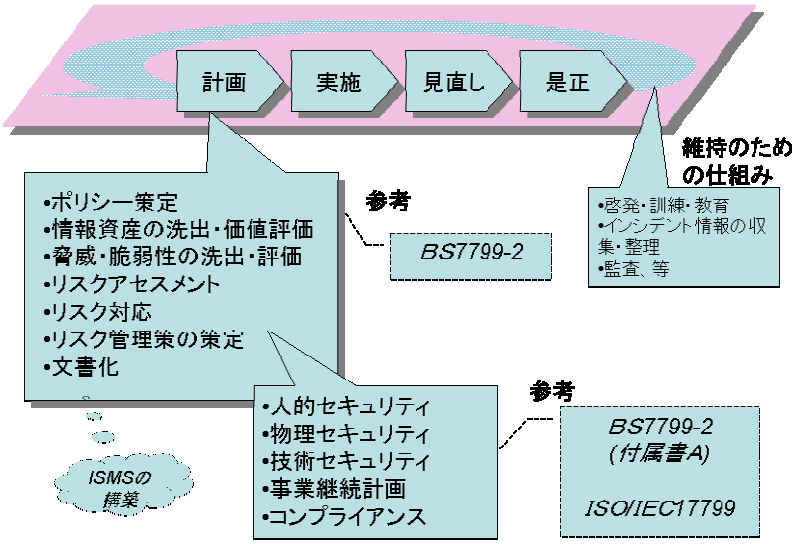


図 41　ISMS の概念図

以下、電子投票に ISMS を適用した場合における、リスクマネジメントサイクルの流れを概説する。

(i) スコープ

ISMS を導入する場合には、まず、スコープと呼ばれる適用範囲を定める。たとえば、電子投票について考えると、それを運用管理する“組織”がひとつの適用範囲の要素として考えられる。また、電子投票の運用管理という“業務”もこの適用範囲に入るであろう。さらに、物理的な側面では、投票や開票が行われる場所、及び電子投票のための準備が行われる場所がその対象となりうる。また、保護すべき情報資産としては、投票機、開票機の他にも、日常的に選挙人の個人情報を保管している選挙人名簿なども検討すべき要件として含まれる。

(ii) 組織体制の確立

選挙の運営等の実務を行っている組織として、選挙管理委員会がある。地方自治体では、通常、自治体の一部門として存在し、職員が構成メンバーとなっている。選挙管理委員会は、日常的には選挙人の名簿管理などを実施し、選挙が実施される場合にはその運営管理に係わる実務を行う。

ISMS の実践においては、基本的に 3 つの組織が必要となる。ひとつは、ISMS を構築するための組織である。これは、ISMS 導入の最初の段階で必要となる組織で、脅威や脆弱性の洗い出しや管理策の策定などを行い、組織の中に ISMS を導入する基盤を作るための作業グループと考えるとよい。一旦 ISMS が組織に導入されると、それを維持管理するための作業を行うグループが必要となる。このグループは、リスクに関連する情報を収集したり、管理策を見直すための一連の作業を行う。これらの 2 つのグループは、同じひとつのグループが継続して行うことが多い。

もうひとつのグループは、組織の責任者などから構成される、最高責任期間である。電子投票の場合、選挙の運営管理に最終的に責任を持つ「最高責任者」が情報セキュリティ管理においても最高責任者となり、関連組織の長などからなる委員会（ISMS 委員会）を構成し、採用すべきセキュリティ管理策などについて、最終の意思決定を下す。

(iii) ポリシーの策定

情報セキュリティについて、組織が示す基本方針、すなわち情報セキュリティポリシーを定める。ポリシーは、ISMS 委員会により決定され、情報セキュリティに関する最高責任者により、組織全体に周知徹底される。電子投票におけるポリシーには、個人情報の保護や正確性の確保などが要件として含まれると思われるが、個々の主体者により、十分議論され、まとめられなければならない。

(iv) リスク評価とリスクマネジメント

ISMS におけるリスク評価は、以下の要件を満たすことが要求されている。

(i) 資産の洗出し
(ii) 資産価値の評価
(iii) 脅威の洗出し
(iv) 脆弱性の洗出し
(v) 脅威と脆弱性の評価
(vi) リスク評価

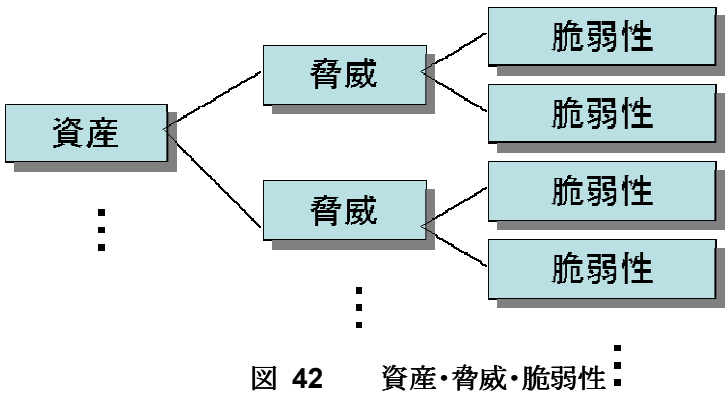


図 42　資産・脅威・脆弱性

図 42 に示すように、個々の(情報)資産を洗い出した後、それぞれに関連する脅威と脆弱性を明確にしていく。たとえば、電子投票機が輸送途中に盗まれた場合、電子投票機が(情報)資産で、盗難が脅威となる。脆弱性は、警備体制の不備などが想定される。

情報資産の洗出しは、通常、関係者等にヒアリングシートなどを配布し情報収集するなどの方法により行われる。ハードウェア、ソフトウェア、紙文書などに分類される資産が考えられる。一般的に考えられる項目としては、DISC PD 3002 や ISO/IEC13335-3 などを参考にできるが、電子投票の場合、さらに検討が加えられる必要がある。

情報資産価値の評価方法のひとつとして、定性評価がある。定性評価では、たとえば、「その情報資産が、機密性・完全性・可用性を喪失した場合に、どのくらいのダメージを受けるか」という視点から、3 段階や 5 段階等で評価する。

脅威と脆弱性の特定も、関係者等にヒアリングシートなどを配布し情報収集する。
脅威の例としては、地震、空調故障、盗難、記憶媒体の不正使用。捜査員のエラー等があげられる。また、脆弱性の例としては、建物・ドアおよび窓の物理的保護の欠如、ソフトウェアの不充分なテスト、保護されない文書の保管、不充分なセキュリティ訓練等が考えられる。一般的に考えられる項目としては、DISC PD 3002 や ISO/IEC13335-3 などを参考にできるが、電子投票の場合、さらに検討が加えられる必要がある。

リスクマネジメントでは、法的要求事項や業務上の要求事項を鑑み、リスクの受容レベルを決めていくが、電子投票の場合、かなり高いレベルが要求される項目もあると予想される。

(v) 管理策の選択

ISMS では、英国の国家規格 BS7799-2 の付属書 A　及び国際規格 ISO/IEC17799 に管理策が提示されており、実践上の参考となる。必ずしも提示されているすべての管理策を採用する必要はない。逆に、提示されていないが導入する必要がある管理策もあると思われる。特に、電子投票の場合、法的要求事項に関しては、慎重な検討が必要であろう。また、日常、選挙人名簿などを行っている選挙管理委員会、投票所、開票所等、個別に管理策を検討する必要があると思われる。

(vi) ヒアリング調査に基づく現状の考察

電子投票の実施において、手順を踏んだリスク評価などのリスクマネジメントサイクルを意識した形で実施されているものはなかった。情報セキュリティ管理の最高責任者も特に意識した形で任命しているケースはなく、電子投票の実施母体の最高責任者がその任を負うというのが一致した結論であった。

しかしながら、情報セキュリティ対策については、どの自治体も慎重な検討を重ねており、落雷・停電・電力供給ストップについての検討をし、対策を打つなど、個別の具体的な対策は取られていた。

ISMS については、おおむねその概要を把握していたが、コストが発生するなどの懸念から採用していないなどの話があり、ISMS の内容について、若干の誤解があるように感じ

た。

全般的に、機器の技術面について、不明な部分が多く、この点を懸念している自治体がほとんどであった。

5-4-6-2 ベースライン管理策の策定

ISMS の基本的な考え方に基づくと、管理策は個々の組織（たとえば、自治体）が、リスク評価などの一連のリスクマネジメントプロセスを経て、決めることになっている。しかしながら、最低限のセキュリティ・レベルを確保したり、個々の組織での作業量を軽減するために、ベースライン管理策を設定することは、一つの有効な手段と考えられる。そこで、ここでは、ISO/IEC17799 に沿って、電子投票に適用する管理策を、昨年度の報告書をベースにまとめる。

(i) 人的セキュリティ

4.1 職務定義及び採用におけるセキュリティ

管理目的: 人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため。

- ♦ 情報セキュリティポリシーに定義した情報セキュリティに関する役割及び責任を職務定義書に明記すること。
- ♦ 採用する人員、請負業者及び臨時職員に求める資質や職能を明確にすること。
- ♦ 人員の採用条件の一部として、被雇用者から機密保持合意書への署名を得ること。
- ♦ 雇用条件には、被雇用者に対し情報セキュリティに関する責任を明示すること。
- ● 機密保持合意は、関係する全ての者に対して、毎年１回、確認書を送付し、関係者全てから署名を得ること。
- ● 業務を外部に委託する場合においても、上記項目全てについて同様の対応を行うこと。

ISMS

管理目的: 人による誤り、盗難、不正行為、又は設備の誤用のリスクを軽減するため。

1. 情報セキュリティポリシーに定義した情報セキュリティに関する役割及び責任を職務定義書に明記すること。
2. 採用する人員、請負業者及び臨時職員に求める資質や職能を明確にすること。
3. 人員の採用条件の一部として、被雇用者から機密保持合意書への署名を得ること。
4. 雇用条件には、被雇用者に対し情報セキュリティに関する責任を明示すること。

4.2 利用者の教育・訓練

管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。

- ♦ 情報セキュリティポリシーの対象者に対し、情報セキュリティポリシー及び関連する手順等に関する教育・訓練を定期的に実施すること。

ISMS

管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。

1. 情報セキュリティポリシーの対象者に対し、情報セキュリティポリシー及び関連する手順等に関する教育・訓練を定期的に実施すること。

4．3 セキュリティ事件・事故及び誤動作への対処

管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。

- ♦ セキュリティ事件・事故は、経営陣を含めた連絡網を通じてできるだけ早く報告すること。
- ♦ セキュリティ事件・事故やそれに準ずる出来事を発見した場合の報告義務を、その義務を有する者に対し周知徹底すること。
- ♦ ソフトウェアが誤動作した場合の報告手順を定めること。
- ♦ 発見したセキュリティ事件・事故や誤動作の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にすること。また、その結果を組織の情報セキュリティに反映させる態勢を整えること。
- ♦ 情報セキュリティポリシー及び関連する手順に違反した場合の処置は、正式な懲戒プロセスに従うこと。
- ● セキュリティ事件・事故の対応を行うための組織を作り、事件・事故への対応が十分できるように普段から訓練・教育を行っておくこと。
- ● システム上の変更後は勿論のこと、定期的に脆弱性検査などを行い、既知の脆弱性や設定ミスの発見に努めること。

ISMS

管理目的: 情報セキュリティの脅威及び懸念に対する利用者の認識を確実なものとし、通常の仕事のなかで利用者が組織のセキュリティポリシーを維持していくことを確実にするため。

1. セキュリティ事件・事故は、経営陣を含めた連絡網を通じてできるだけ早く報告すること。
2. セキュリティ事件・事故やそれに準ずる出来事を発見した場合の報告義務を、その義務を有する者に対し周知徹底すること。
3. ソフトウェアが誤動作した場合の報告手順を定めること。
4. 発見したセキュリティ事件・事故や誤動作の種類や規模、事業への影響度の大きさ、復旧のための関連費用等を明確にすること。また、その結果を組織の情報セキュリティに反映させる態勢を整えること。
5. 情報セキュリティポリシー及び関連する手順に違反した場合の処置は、正式な懲戒プロセスに従うこと。

(ii) 物理セキュリティ

5．1 セキュリティ区画

管理目的: 業務施設及び情報に対する許可されていないアクセス、損傷及び妨害を防止するため。

- ♦ 情報処理施設及び設備を含む領域の保護のために、セキュリティ境界を導入すること。
- ♦ セキュリティ区画は、許可されない者がアクセスできないよう入退管理を行うこと。
- ♦ セキュリティ区画は、特別な管理を要求される作業場所や施設を保護する目的で設置されること。
- ♦ セキュリティ区画において作業をするために必要な措置を講じ、作業ガイドライン等を整備すること。
- ♦ 納品及び積荷場所は、許可されないアクセスを避けるため管理され、情報処理施設及び設備から分離されること。
- ● セキュリティ区画の入退管理は自動的に記録が取れる仕組みを採用する。

ISMS	管理目的: 業務施設及び情報に対する許可されていないアクセス、損傷及び妨害を防止するため。 1. 情報処理施設及び設備を含む領域の保護のために、セキュリティ境界を導入すること。 2. セキュリティ区画は、許可されない者がアクセスできないよう入退管理されること。 3. セキュリティ区画は、特別な管理を要求される作業場所や施設を保護する目的で設置されること。 4. セキュリティ区画において作業をするために必要な措置を講じ、作業ガイドライン等を整備すること。 5. 納品及び積荷場所は、許可されないアクセスを避けるため管理され、情報処理施設及び設備から分離されること。

5. 2 装置のセキュリティ

管理目的: 資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため。

- ♦ 装置の設置場所における環境上の脅威を軽減するための措置を講ずること。
- ♦ 装置を許可されないアクセスから保護すること。
- ♦ 装置を停電やその他の電源異常から保護すること。
- ♦ データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。
- ♦ 装置の可用性及び完全性を確実に維持するために、装置の保守を正しく実施すること。
- ♦ 装置を処分あるいは再利用する際、装置に格納された情報を事前に消去すること。
- ● ネットワークへの過負荷が発生しないような措置を講ずること。
- ● 組織の敷地外で情報処理装置を利用してはならない。

ISMS	管理目的: 資産の損失、損傷又は劣化、及び業務活動に対する妨害を防止するため。 1. 装置の設置場所における環境上の脅威を軽減するための措置を講ずること。 2. 装置を許可されないアクセスから保護すること。 3. 装置を停電やその他の電源異常から保護すること。 4. データ伝送や情報サービスに使用する電源及び通信ケーブルの配線に対し、傍受や損傷等を防止するための措置を講ずること。 5. 装置の可用性及び完全性を確実に維持するために、装置の保守を正しく実施すること。 6. 組織の敷地外で情報処理装置を利用する場合は、管理者による承認を受けること。 7. 装置を処分あるいは再利用する際、装置に格納された情報を事前に消去すること。

5. 3 一般的な管理策

管理目的: 情報及び情報処理設備の損傷又は盗難を防止するため。

- ♦ 離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。
- ♦ 離席時や帰宅時には、ログオフを徹底し、他人による情報システムへのアクセスを防止するための措置を講ずること。
- ♦ 組織が所有する装置や情報、ソフトウェア等を管理者による承認なしに移動させないこと。
- ● 必要な作業は、可能な限りセキュリティ区画にて行い、一般の場所での作業を行わない。
- ● また、セキュリティ区画への入退室は、全て記録（ログ）が残る仕組みを構築する。
- ● 離席時にはログオフ状態に簡単にできる機器などを利用し、スクリーンセーバの利用はしない。

ISMS	管理目的: 情報及び情報処理設備の損傷又は盗難を防止するため。 1. 離席時や帰宅時における、机上やその他の場所への情報の放置を禁止すること。 2. 離席時や帰宅時には、パスワードで保護されたスクリーンセーバの使用やログオフを徹底し、他人による情報システムへのアクセスを防止するための措置を講ずること。 3. 組織が所有する装置や情報、ソフトウェア等を管理者による承認なしに移動させないこと。

(iii) 技術セキュリティ

a) センター間の結託について

次世代電子投票・アンケートシステムにおいて、センター１とセンター２の間で結託が行われることにより、セキュリティ上の脆弱性が発生する可能性がある。

センター間での結託としては、それらの運用を行う要員間で結託が発生しない仕組みを考えることで、セキュリティポリシー上の問題として捉えることにした。

現行の公職選挙法では、投票所の監視権限を持った者がいたり、開票管理者や開票立会人(注３)を選定し、開票時の不正に対処する仕組みが作られている。

注３）開票管理者は、それぞれの選挙ごとに置かれ、その選挙の開票に関する事務（投票の点検、投票の効力の決定、開票の結果の報告、開票録の作成、開票所の取締りなど）を行う。開票管理者は、その選挙の有権者の中から、区市町村の選挙管理委員会によって選任される。

開票立会人は、開票に立ち会い、開票管理者が行う投票の効力の決定に際して意見陳述などを行う人を言う。 その選挙の候補者や名簿届出政党等が各開票区の選挙人名簿の中から本人の承諾を得て１人を定め、区市町村の選挙管理委員会に届け出ることができる。届け出が１０人を超えたときはくじで１０人にし、３人に満たない場合は、選挙管理委員会が選挙人名簿に登録された者から３人になるまで、補充選任する。

本研究でも、現行の方法と同じように、集計センター、開票センターの２つのセンターに開票管理者や開票立会人的な機能を持った者を立会させることも想定できる。 通常の投票日だけであれば、投票から開票までの期間が高々１日程度と想定されるため、立会させることは不可能ではないであろう。

しかしながら、不在者投票を含めた期間やシステム実装時から開票終了までの全期間について立会を行う必要がある場合には、これらの人々が立会するだけでは対応できない可能性もあると考えるのが一般的であろう。

b) 建設業界における談合の研究

結託を考える場合、「ゲーム理論」における囚人のジレンマの問題を発展させ、建設業界の談合問題へ適用した論文がある。[70]

この事例では、ゲームが無限回行なわれることを想定しており、以下の結論を導きだしている。

（１） 談合が発覚したときのペナルティをいくら大きくしても，談合は起こり得る。

（２） 発覚確率がある値以上ならば，談合は起きない。

（３） 談合をしたときの利得は，大きければ大きいほど談合が起きやすくなる。

投票での問題が、建設業界における談合の問題と同列に論じられるかの問題はあるが、結託の問題に対しても大いに参考になる研究であると考えている。

c) ネットワークセキュリティでの考え方

ネットワークシステムに対する攻撃に対抗するための手段として、セキュリティサービスとして、「機密性・完全性・可用性」（ＣＩＡ： Confidentiality、Integrity、Availability）が良く知られているが、この他に「説明責任」(Accountability を訳したもので、ログ等を取ったり、必要な記録を保存することで、証拠を保全すること）を考えることが重要であるとの指摘がある。[71]

「説明責任」機能自体は単独で攻撃に対して効果を発揮するものでなく、ＣＩＡ単独で対応するよりも、強化できるものであるとしている。　下表に示すように、ＤｏＳ攻撃（Denial of Service：サービス妨害攻撃）以外の攻撃に対しては、他の機能を強化する役割を果たしている。

結託を考える場合、上記の2つの論点をよく整理してみると、考え方が同じであることに気づく。即ち、談合しても簡単に発覚してしまえば、談合を行うことをあきらめることになり、談合が簡単に発覚する仕組みとして、「説明責任」機能を導入することが、談合を見いだすための情報を保存することであると言える。

この考え方をセキュリティポリシーの中で考えていくことが、次世代電子投票・アンケートシステムにおける管理・運用面での結託を防止することになるものと思われる。

「説明責任」として考えることは、ログ・記録を取ることが基本になっており、そのような対応を行うことになるが、それらは、単にセンター内のシステムだけでなく、システムが設置してある物理的な面、建物・部屋などへの入退館・入退室の面でのログの記録も「説明責任」の一部分であることは言うまでもない。

建物への入退館記録、センターシステムの設置場所への入退室記録等については、必ず個人レベルで記録し、また、センターシステム設置場所については、最高度のセキュリティを確保するためには、操作などを行う場合には、1人で行うことができない仕組みを考慮することも必要になる。

表 36　攻撃に対応するセキュリティサービス機能

	セキュリティサービス			
攻撃の種類	機密性（Confidentiality）	完全性（Integrity）	可用性（Availability）	説明責任（Accountability）
アクセス攻撃	●			●
修正攻撃		●		●
DoS攻撃			●	
否認攻撃		●		●

(iv) 通信及び運用管理

6.1 運用手順及び責任

管理目的: 情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。

- ♦ セキュリティポリシーに従い特定した操作手順を文書化し、維持すること。
- ♦ 情報システムや情報処理施設等に対する変更を管理すること。
- ♦ セキュリティ事件・事故の対応を迅速、効果的、整然と行うために、また関連するデータ（監査証跡、監査ログなど）の収集を行うために、セキュリティ事件・事故を管理する責任体制及び手順を定めること。
- ♦ 情報やサービスへの許可されない変更や誤用の機会を低減するため、職務の分離及び責任の範囲を明確にすること。
- ♦ 情報システムの開発及びテストの環境を運用施設及び設備から分離すること。また、運用ソフトウェアについて、開発段階から運用段階へ移行の手順を定めること。
- ♦ 外部の施設管理サービスを利用する場合、評価されたリスクに基づき、適切な措置を定め、内容を明記した正式な契約を締結すること。
- ● 必要な操作は出来る限り単純化し、操作を行う場合には、２人体制で行うなどを考慮する。　外部へ処理作業を委託する場合も同じとする。

ISMS

管理目的: 情報処理設備の正確、かつ、セキュリティを保った運用を確実にするため。

1. セキュリティポリシーに従い特定した操作手順を文書化し、維持すること。
2. 情報システムや情報処理施設等に対する変更を管理すること。
3. セキュリティ事件・事故の対応を迅速、効果的、整然と行うために、また関連するデータ(監査証跡、監査ログなど)の収集を行うために、セキュリティ事件・事故を管理する責任体制及び手順を定めること。
4. 情報やサービスへの許可されない変更や誤用の機会を低減するため、職務の分離及び責任の範囲を明確にすること。
5. 情報システムの開発及びテストの環境を運用施設及び設備から分離すること。また、運用ソフトウェアについて、開発段階から運用段階へ移行の手順を定めること。
6. 外部の施設管理サービスを利用する場合、評価されたリスクに基づき、適切な措置を定め、内容を明記した正式な契約を締結すること。

6.2 システム計画の作成及び受け入れ

管理目的: システム障害によるリスクを最小限に抑えるため。

- ♦ 情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。
- ♦ 情報システムを新規導入あるいは変更する際の受け入れ基準を確立し、情報システムの本番利用を容認する前に適切なテストを実施すること。
- ● ネットワークの輻輳（DoS 攻撃なども含め）に対応できるシステム構成を事前に確認し、ネットワークの輻輳でシステムの可用性を損なわれないようにする。

ISMS

管理目的: システム障害によるリスクを最小限に抑えるため。

1. 情報システムの処理能力及び記憶容量を十分に確保するため、利用状況を監視し将来に必要な処理能力や容量を予測すること。
2. 情報システムを新規導入あるいは変更する際の受け入れ基準を確立し、情報システムの本番利用を容認する前に適切なテストを実施すること。

6．3　不正ソフトウェアからの保護

管理目的: ソフトウェア及び情報の完全性を保護するため。

- ♦　情報や情報システムを不正ソフトウェアから保護するための検出及び防止策を講じ、適宜利用者の教育・訓練を実施すること。

ISMS

管理目的: ソフトウェア及び情報の完全性を保護するため。

1. 情報や情報システムを不正ソフトウェアから保護するための検出及び防止策を講じ、適宜利用者の教育･訓練を実施すること。

6．4　情報システムの管理

管理目的: 情報処理及び通信サービスの完全性及び可用性を維持するため。

- ♦　重要な情報及びソフトウェアのバックアップコピーを定期的に取得し、定期的にテストすること。
- ♦　情報システムの操作担当者の作業履歴を記録すること。　また、操作担当者以外の者が作業履歴を定期的にチェックすること。
- ♦　障害が報告された情報システムを確実に修正すること。
- ●　バックアップは安全な場所に保管し、それらの入出を記録できるようにしておくこと。

ISMS

管理目的: 情報処理及び通信サービスの完全性及び可用性を維持するため。

1. 重要な情報及びソフトウェアのバックアップコピーを定期的に取得し、定期的にテストすること。
2. 情報システムの操作担当者の作業履歴を記録すること。 また、操作担当者以外の者が作業履歴を定期的にチェックすること。
3. 障害が報告された情報システムを確実に修正すること。

6．5　ネットワークの管理

管理目的: ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため。

- ♦　ネットワークにおけるセキュリティを確保し維持するための措置を講ずること。

ISMS

管理目的: ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため。

1. ネットワークにおけるセキュリティを確保し維持するための措置を講ずること。

6．6　媒体の取扱い及びセキュリティ

管理目的: 情報資産に対する損害及び事業活動の中断を回避するため。

- ♦　テープ、ディスク、カセット等の移動可能な記憶媒体や書類等を適切に管理すること。
- ♦　不要になった媒体を処分する際、情報漏洩を防止するための措置を講ずること。
- ♦　情報の、許可されない開示及び改ざん、誤用等を防止するため、媒体の取扱い及び保管に関する手順を定めること。
- ♦　情報システムに関する文書を許可されないアクセスから保護すること。

ISMS	管理目的: 情報資産に対する損害及び事業活動の中断を回避するため。 1. テープ、ディスク、カセット等の移動可能な記憶媒体や書類等を適切に管理すること。 2. 不要になった媒体を処分する際、情報漏洩を防止するための措置を講ずること。 3. 情報の、許可されない開示及び改ざん、誤用等を防止するため、媒体の取扱い及び保管に関する手順を定めること。 4. 情報システムに関する文書を許可されないアクセスから保護すること。

6.7 組織間における情報及びソフトウェアの交換

管理目的: 組織間で交換される情報の紛失、改ざん又は誤用を防止するため。

- 取引先や協業相手等と情報やソフトウェアを交換（電子的、人手にかかわらず）する場合、必要に応じて情報交換の実施に関する正式な契約を締結すること。
- 移送中の媒体を許可されないアクセス、誤用及び破損から保護すること。
- 電子取引を行う場合、不正行為、契約紛争、情報の許可されない開示及び改ざんを防止するための措置を講ずること。
- 電子メールの使用に関するポリシーを定め、電子メールの使用により発生しうるリスクを軽減するための措置を講ずること。
- 電子オフィスシステムの使用に関するポリシー及びガイドラインを定め、電子オフィスシステムの使用に関連したリスクを抑制すること。
- 組織の情報を一般に公開し利用可能にする場合の正式な承認プロセスを定めること。
- 組織の情報を一般に公開し利用可能にする場合、その情報を許可されない変更から保護すること。
- 電話やファクシミリ、ビデオ通信等を使用して情報を交換する場合、そのポリシーと手順を定め、必要な措置を講ずること。

ISMS	管理目的: 組織間で交換される情報の紛失、改ざん又は誤用を防止するため。 1. 取引先や協業相手等と情報やソフトウェアを交換(電子的、人手にかかわらず)する場合、必要に応じて情報交換の実施に関する正式な契約を締結すること。 2. 移送中の媒体を許可されないアクセス、誤用及び破損から保護すること。 3. 電子取引を行う場合、不正行為、契約紛争、情報の許可されない開示及び改ざんを防止するための措置を講ずること。 4. 電子メールの使用に関するポリシーを定め、電子メールの使用により発生しうるリスクを軽減するための措置を講ずること。 5. 電子オフィスシステムの使用に関するポリシー及びガイドラインを定め、電子オフィスシステムの使用に関連したリスクを抑制すること。 6. 組織の情報を一般に公開し利用可能にする場合の正式な承認プロセスを定めること。 7. 組織の情報を一般に公開し利用可能にする場合、その情報を許可されない変更から保護すること。 8. 電話やファクシミリ、ビデオ通信等を使用して情報を交換する場合、そのポリシーと手順を定め、必要な措置を講ずること。

(v) アクセス制御

7.1 アクセス制御に関する事業上の要求事項

管理目的: 情報へのアクセスを制御するため。

- ♦ 情報へのアクセス制御に関する事業上及びセキュリティ上の必要性を明確にし、それに従いアクセス制御ポリシーを定めること。
- ♦ 情報へのアクセスは、アクセス制御ポリシーに従い制限されること。

ISMS

管理目的: 情報へのアクセスを制御するため。

1. 情報へのアクセス制御に関する事業上及びセキュリティ上の必要性を明確にし、それに従いアクセス制御ポリシーを定めること。
2. 情報へのアクセスは、アクセス制御ポリシーに従い制限されること。

7.2 利用者アクセス管理

管理目的: 情報システムへの許可されていないアクセスを防止するため。

- ♦ 情報システム利用者の登録及び登録抹消の手順を定めること。
- ♦ 特権の割当て及び使用を制限し管理すること。
- ♦ 情報システム利用者に対するパスワードの割当ては、確立された管理プロセスに従い実施されること。
- ♦ 経営陣・管理者は情報システム利用者のアクセス権を定期的に見直すように指示すること。
- ● 利用者の認証には、認証の３要素（SYK: 知っているもの、SYH： 持っているもの、SYA：身体的な特徴）の２つ以上を利用することが望ましい。 例えば、利用者は、IC カードとパスワード、指紋認証とパスワードと言った複数の認証要素を利用した方法を採用する。

ISMS

管理目的: 情報システムへの許可されていないアクセスを防止するため。

1. 情報システム利用者の登録及び登録抹消の手順を定めること。
2. 特権の割当て及び使用を制限し管理すること。
3. 情報システム利用者に対するパスワードの割当ては、確立された管理プロセスに従い実施されること。
4. 経営陣・管理者は情報システム利用者のアクセス権を定期的に見直すように指示すること。

7.3 利用者の責任

管理目的: 許可されていない利用者のアクセスを防止するため。

- ♦ パスワードの選択及び使用に際して、正しい情報セキュリティ慣行を参考に、利用者に情報セキュリティ上の問題を考慮することを要求すること。
- ♦ 利用者の領域にある装置を常時監視することが不可能な場合、当該装置を適切に保護するよう利用者に要求すること。

ISMS

管理目的: 許可されていない利用者のアクセスを防止するため。

1. パスワードの選択及び使用に際して、正しい情報セキュリティ慣行を参考に、利用者に情報セキュリティ上の問題を考慮することを要求すること。
2. 利用者の領域にある装置を常時監視することが不可能な場合、当該装置を適切に保護するよう利用者に要求すること。

7．4　ネットワークのアクセス制御

管理目的: ネットワークを利用したサービスの保護のため。

- 利用者に、明確に許可された以外のサービスへのアクセスを防止するための措置を講ずること。
- 情報システムの利用者がコンピュータにアクセスする場合のネットワークの経路を制御すること。
- 情報システムに対する遠隔地からのアクセスを許可する場合、利用者認証を行うこと。
- 遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。
- 診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。
- 情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。
- 共有ネットワークへのアクセス権限は、アクセス制御ポリシーに従い付与されること。
- 共有ネットワークへのアクセスを許可する場合、アクセス制御ポリシーに基づき、可能な限り経路を制御すること。
- ネットワークに関連するサービスを使用する場合、そのサービスに施されたセキュリティに関する情報について、明確な説明をうけること。

ISMS

管理目的: ネットワークを利用したサービスの保護のため。

1. 利用者に、明確に許可された以外のサービスへのアクセスを防止するための措置を講ずること。
2. 情報システムの利用者がコンピュータにアクセスする場合のネットワークの経路を制御すること。
3. 情報システムに対する遠隔地からのアクセスを許可する場合、利用者認証を行うこと。
4. 遠隔地のコンピュータに対するアクセスを許可する場合、接続の認証を行うこと。
5. 診断用の通信ポートへの許可されないアクセスを防止するための措置を講ずること。
6. 情報システムに対する許可されないアクセスを防止するため、ネットワークを適切に分離すること。
7. 共有ネットワークへのアクセス権限は、アクセス制御ポリシーに従い付与されること。
8. 共有ネットワークへのアクセスを許可する場合、アクセス制御ポリシーに基づき、可能な限り経路を制御すること。
9. ネットワークに関連するサービスを使用する場合、そのサービスに施されたセキュリティに関する情報について、明確な説明をうけること。

7．5 オペレーティングシステムのアクセス制御

管理目的: 許可されていないコンピュータアクセスを防止するため。

- 接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。
- 情報サービスへのアクセスは、安全なログオンプロセスを使用すること。
- 情報システム利用者は、個人を特定できる一意の識別子（利用者 ID）を有すること。また、正当な利用者であることを認証するための適切な技術を選択すること。
- パスワード管理システムは、情報システム利用者に有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を管理すること。
- システムユーティリティプログラムの使用を制限し管理すること。
- 情報へのアクセスに際して、脅迫の対象となり得る利用者のため、脅迫に対して警報を発信する機能を備えること。
- 取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末を一定の活動停止時間の経過後、システムから遮断すること。
- リスクの高いアプリケーションシステムへの接続時間は、制限されること。

ISMS

管理目的: 許可されていないコンピュータアクセスを防止するため。

1. 接続が許可された特定の場所や携帯装置に対する認証を行うため、端末を自動的に識別する機能を備えること。
2. 情報サービスへのアクセスは、安全なログオンプロセスを使用すること。
3. 情報システム利用者は、個人を特定できる一意の識別子（利用者 ID）を有すること。 また、正当な利用者であることを認証するための適切な技術を選択すること。
4. パスワード管理システムは、情報システム利用者に有効なパスワードを設定させるための対話式の機能を備え、パスワードの内容や文字数、文字の種類、変更の頻度等を管理すること。
5. システムユーティリティプログラムの使用を制限し管理すること。
6. 情報へのアクセスに際して、脅迫の対象となり得る利用者のため、脅迫に対して警報を発信する機能を備えること。
7. 取扱いに慎重を要する情報システムに接続された端末が活動停止状態にある場合、その端末を一定の活動停止時間の経過後、システムから遮断すること。
8. リスクの高いアプリケーションシステムへの接続時間は、制限されること。

7．6 アプリケーションシステムのアクセス制御

管理目的: 情報システムが保有する情報への許可されていないアクセスを防止するため。

- 情報及びアプリケーションシステムへのアクセスは、アクセス制御ポリシーに従い制限されること。
- 取扱いに慎重を要する情報システムは、隔離した環境に設置されること

ISMS

管理目的: 情報システムが保有する情報への許可されていないアクセスを防止するため。

1. 情報及びアプリケーションシステムへのアクセスは、アクセス制御ポリシーに従い制限されること。
2. 取扱いに慎重を要する情報システムは、隔離した環境に設置されること

7．7　システムアクセス及びシステム使用の監視

管理目的: 許可されていない活動を検出するため。

- ♦　例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。
- ♦　情報処理施設及び設備の使用を監視するための手順を定めること。
- ♦　情報処理施設及び設備の監視活動の結果を定期的に検証すること。
- ♦　正確に記録をするために、コンピュータ内のクロックを同期化すること。

ISMS

管理目的: 許可されていない活動を検出するため。

1. 例外事項やその他のセキュリティ関連イベント等の監査ログを記録し、定められた期間において保存すること。
2. 情報処理施設及び設備の使用を監視するための手順を定めること。
3. 情報処理施設及び設備の監視活動の結果を定期的に検証すること。
4. 正確に記録をするために、コンピュータ内のクロックを同期化すること。

7．8　モバイルコンピューティング及び遠隔地勤務

管理目的: 移動型計算処理及び遠隔作業の設備を用いるとき、情報セキュリティを確実にするため。

- ●　モバイルコンピュータは利用してはならない。

ISMS

管理目的: 移動型計算処理及び遠隔作業の設備を用いるとき、情報セキュリティを確実にするため。

1. モバイルコンピュータを用いる場合、評価されたリスクに基づき、モバイルコンピュータ使用の方針を定めた上で必要な措置を講ずること。
2. 遠隔作業を許可し、管理するためのポリシー、手順及び基準を策定すること。

(vi) システムの開発及びメンテナンス

8．1　システムのセキュリティ要求事項

管理目的: 情報システムへのセキュリティの組み込みを確実にするため。

- ♦　情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要求事項を明確にすること。

ISMS

管理目的: 情報システムへのセキュリティの組み込みを確実にするため。

1. 情報システムを新規導入あるいは変更する際、事業の要求事項に基づいたセキュリティ要求事項を明確にすること。

8．2　アプリケーションシステムのセキュリティ

管理目的: 業務用システムにおける利用者データの消失、変更又は誤用を防止するため。

- ♦　アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能を整備すること。
- ♦　アプリケーションシステムで処理されたデータに対する改変を検出する機能を備えること。
- ♦　メッセージの完全性を保護する必要がある場合、メッセージ認証機能を備えること。
- ♦　アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。

ISMS	管理目的: 業務用システムにおける利用者データの消失、変更又は誤用を防止するため。 1. アプリケーションシステムに入力されるデータが妥当なものであることを確認するための機能を整備すること。 2. アプリケーションシステムで処理されたデータに対する改変を検出する機能を備えること。 3. メッセージの完全性を保護する必要がある場合、メッセージ認証機能を備えること。 4. アプリケーションシステムから出力されるデータが妥当なものであることを確認するための機能や手順を整備すること。

8.3 暗号による管理策

管理目的: 情報の機密性、真正性又は完全性を保護するため。

- 情報を保護するために、評価されたリスクに基づき、暗号の使用についての方針を定めること。
- 取扱いに慎重を要する情報や重要な情報については、機密性を保護するため暗号化すること。
- 電子情報の真正性および完全性を保護するため、デジタル署名を用いること。
- 取引に関わる紛争を解決するため、電子情報による取引事実の否認を防止するための措置を講ずること。
- 情報を保護するために暗号を用いる場合、関連する対策基準類や手順等に準拠し、適切に鍵管理を行うこと。

ISMS	管理目的: 情報の機密性、真正性又は完全性を保護するため。 1. 情報を保護するために、評価されたリスクに基づき、暗号の使用についての方針を定めること。 2. 取扱いに慎重を要する情報や重要な情報については、機密性を保護するため暗号化すること。 3. 電子情報の真正性および完全性を保護するため、デジタル署名を用いること。 4. 取引に関わる紛争を解決するため、電子情報による取引事実の否認を防止するための措置を講ずること。 5. 情報を保護するために暗号を用いる場合、関連する対策基準類や手順等に準拠し、適切に鍵管理を行うこと。

8.4 システムファイルのセキュリティ

管理目的: IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため。

- 稼動中の情報システムへのソフトウェアの導入は適切に管理されること。
- テスト用のデータは適切に保護され管理されること。
- プログラムソースライブラリへのアクセスを厳格に管理すること。

ISMS	管理目的: IT プロジェクト及びその支援活動をセキュリティが保たれた方法で実施されることを確実にするため。 1. 稼動中の情報システムへのソフトウェアの導入は適切に管理されること。 2. テスト用のデータは適切に保護され管理されること。 3. プログラムソースライブラリへのアクセスを厳格に管理すること。

8．5　開発及びサポートプロセスにおけるセキュリティ **管理目的:アプリケーションシステムソフトウェア及び情報のセキュリティを維持するため。** ♦　情報システムの正式な変更管理の手順を定め、変更を厳格に管理すること。 ♦　オペレーティングシステムを変更する場合、アプリケーションシステムの見直し及びテストを実施すること。 ♦　パッケージソフトウェアの変更は原則として行わないこと。 ♦　やむを得ずパッケージソフトウェアの変更が必要になった場合、変更を厳格に管理すること。 ♦　ソフトウェアの購入の際、プログラムにトロイの木馬やコバート通信路等が懸念される場合、事前に検査し、また使用及び変更を厳格に管理すること。 ♦　ソフトウェア開発をアウトソーシングする場合、評価されたリスクに基づいた正式な契約を締結すること。	
ISMS	管理目的:アプリケーションシステムソフトウェア及び情報のセキュリティを維持するため。 1. 情報システムの正式な変更管理の手順を定め、変更を厳格に管理すること。 2. オペレーティングシステムを変更する場合、アプリケーションシステムの見直し及びテストを実施すること。 3. パッケージソフトウェアの変更は原則として行わないこと。 4. やむを得ずパッケージソフトウェアの変更が必要になった場合、変更を厳格に管理すること。 5. ソフトウェアの購入の際、プログラムにトロイの木馬やコバート通信路等が懸念される場合、事前に検査し、また使用及び変更を厳格に管理すること。 6. ソフトウェア開発をアウトソーシングする場合、評価されたリスクに基づいた正式な契約を締結すること。

（vii）事業継続管理

9．1　事業継続管理 **管理目的: 事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務プロセスを保護するため。** ♦　ISMS 適用範囲全体を含む組織の事業継続を検討し策定、維持するための管理プロセスを整備すること。 ♦　事業継続に取り組むため、リスクアセスメントに基づいた戦略計画を策定すること。 ♦　重要な業務プロセスに関連した中断又は障害の際、事業の運営を維持し、許容時間内に復旧させるため、必要な計画を立案すること。 ♦　全ての計画の整合性を保証し、また、試験や保守の優先順位を明確にするため、事業継続計画全体を統括する枠組みを維持すること。 ♦　事業継続計画は定期的に試験され、常時有効であることを確実するために内容の見直しにより維持されること。

ISMS	管理目的: 事業活動の中断に対処するとともに、重大な障害又は災害の影響から重要な業務プロセスを保護するため。 1. ISMS 適用範囲全体を含む組織の事業継続を検討し策定、維持するための管理プロセスを整備すること。 2. 事業継続に取り組むため、リスクアセスメントに基づいた戦略計画を策定すること。 3. 重要な業務プロセスに関連した中断又は障害の際、事業の運営を維持し、許容時間内に復旧させるため、必要な計画を立案すること。 4. 全ての計画の整合性を保証し、また、試験や保守の優先順位を明確にするため、事業継続計画全体を統括する枠組みを維持すること。 5. 事業継続計画は定期的に試験され、常時有効であることを確実するために内容の見直しにより維持されること。

(viii) コンプライアンス

10.1 法的要求事項への準拠 **管理目的: 刑法及び民法、制定法、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため。** ♦ 個別の情報システム毎に関連する全ての法令、規制及び契約上の要求事項を明確にし、これを文書化すること。 ♦ 知的財産権に関わる法的制限事項を遵守した手順を整備すること。 ♦ 組織の重要な記録を紛失、消失、破壊、改ざん等から保護すること。 ♦ 個人情報保護に関する法令に従い、個人の情報を保護すること。 ♦ 情報処理施設及び設備の悪用を防止するための措置を講ずること。 ♦ 暗号の使用に関する法令を遵守すること。 ♦ 訴訟に提示する証拠は、関連する法令に定められた規則に準拠すること。
ISMS	管理目的: 刑法及び民法、制定法、規制又は契約上の義務、並びにセキュリティ上の要求事項に対する違反を避けるため。 1. 個別の情報システム毎に関連する全ての法令、規制及び契約上の要求事項を明確にし、これを文書化すること。 2. 知的財産権に関わる法的制限事項を遵守した手順を整備すること。 3. 組織の重要な記録を紛失、消失、破壊、改ざん等から保護すること。 4. 個人情報保護に関する法令に従い、個人の情報を保護すること。 5. 情報処理施設及び設備の悪用を防止するための措置を講ずること。 6. 暗号の使用に関する法令を遵守すること。 7. 訴訟に提示する証拠は、関連する法令に定められた規則に準拠すること。

10.2 セキュリティポリシーと技術標準への準拠性のレビュー **管理目的: 組織のセキュリティポリシー及び関連する対策基準や手順書等へのシステムの準拠を確実にするため。** ♦ 組織の経営者・管理者は、責任範囲における全てのセキュリティ手続きが正しく実行されていること確実にする措置を講じ、組織内のすべての範囲においてセキュリティポリシー及び関連する対策基準や手順書等への準拠を定期的に見直すこと。 ♦ 情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的に確認すること。

ISMS	管理目的: 組織のセキュリティポリシー及び関連する対策基準や手順書等へのシステムの準拠を確実にするため。 1. 組織の経営者・管理者は、責任範囲における全てのセキュリティ手続きが正しく実行されていること確実にする措置を講じ、組織内のすべての範囲においてセキュリティポリシー及び関連する対策基準や手順書等への準拠を定期的に見直すこと。 2. 情報システムが情報セキュリティポリシー及び関連する対策基準や手順書等に準拠していることを定期的に確認すること。

10.3 システム監査の考慮事項 **管理目的: システム監査プロセスの有効性を最大に、また監査プロセスと業務の間でおよぼしあう影響を最小にするため。** ♦ 稼動中の情報システムに対する監査を実施する場合、業務が中断するリスクを最小限に抑えるよう計画し、被監査部門と合意すること。 ♦ システム監査ツールに対する誤用又は悪用等を防止するための措置を講ずること。	
ISMS	管理目的: システム監査プロセスの有効性を最大に、また監査プロセスと業務の間でおよぼしあう影響を最小にするため。 1. 稼動中の情報システムに対する監査を実施する場合、業務が中断するリスクを最小限に抑えるよう計画し、被監査部門と合意すること。 2. システム監査ツールに対する誤用又は悪用等を防止するための措置を講ずること。

(ix) ヒアリング調査に基づく現状の考察

人的セキュリティについては、ほとんどの自治体が、「自治体職員は不正行為を行わない」という前提に基づいてセキュリティ対策を実施していた。いくつかの自治体担当者は、この問題を懸念しているという意見を持っていたが、現状、特に内部犯罪の可能性を考えた対応策を重視する傾向は見られなかった。

オペレーショナル・ミスについては、どの自治体もかなりの研修を行っており、エラーが出たときの対処方法などの訓練を重ねている自治体が多くあった。

物理的セキュリティについては、投票結果が入ったコンパクト・フラッシュの輸送について、施錠した箱にいれ、複数の担当者が運ぶなどの方法が取られていた。投票所や開票所は、衆人環視の環境にあり、これまでの紙による投票と同様の管理方法であった。

技術セキュリティ、通信及び運用管理、アクセス制御などにおける、機器の技術的要件については、メーカーに対する信頼性に依存しているケースがほとんどで、担当者によっては、その点に不安を感じているということであった。自治体独自で、プログラムや機能、不正操作の可能性などについて、チェックを行うのが難しいため、監督官庁などに、セキュリティ要件を定め、認証するなどの制度を設けてほしいといった要望があった。

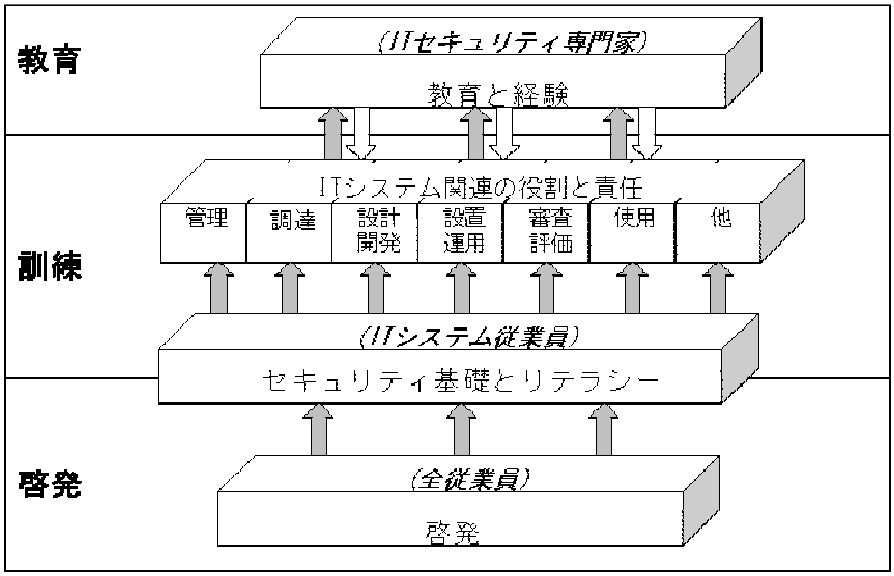
事業継続管理については、事故が発生した場合に備えて予備機を準備するなど慎重な対処が取られていた。

コンプライアンスについては、当然、各自治体で必要な法整備を行っていた。

多くの自治体で、機器の機能の部分がブラック・ボックスになっており、その点を問題視している。しかしながら、個々の自治体でチェック機能を持つのは、現実的には困難であり、所管している官庁もしくは業界によるガイドラインの策定などの対応策の検討が必要であろう。

5-4-6-3 維持継続のための要件

(i) 実施者及び投票者に対する教育・訓練・啓発



*「米国におけるコンピュータ・セキュリティ・インシデントとその対策としてのセキュリティ教育」, (財)防衛調達基盤整備協会

*SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model (supersedes NIST Spec. Pub. 500-172)

図 43　教育・訓練・啓発

組織の中に、情報セキュリティリスクに対する感性を定着させるためには、継続的な教育・訓練・啓発が必要である。教育は、情報セキュリティの専門家を育成するために行われるもので、自ら組織外の専門家等と情報交換し、常に新しい技術や知見を身につけられるだけの能力を有する者の育成を目標とする。訓練は、日本で一般的に‘教育’と呼ばれているものに近い。情報セキュリティ関係者が、それぞれの役割とそれにあった情報セキュリティの知識を身につけ実践できるようにするものである。啓発は、すべての従業員に対して行われるもので、ポスターなどを使って、情報セキュリティの感性を高めることをいう。情報セキュリティの感性は、時間が経過すると劣化するため、常にさまざまな方法を駆使して継続的に行わなければならない。

電子投票においても、選挙期間はもとより、日常的な作業においても啓発を実施することにより、関係者のセキュリティの感性が維持される。その結果、事故発生を未然に防いだり、事故や事件が発生した場合でも、適切な行動が取れるようになる。

(ii) 事故・事件情報の収集と反映

過去の事故や事件の情報を収集し、リスク評価やセキュリティ管理策の策定に活用できるような仕組みづくりが重要である。通常の組織では、当初から適切な管理策が策定でき

るとは限らない。したがって、定期的に見直す必要がある。過去の事故や事件の情報は、この際に、考慮すべきことや注意すべきことの情報を提供する重要な役割を担っている。このような情報は、自分の組織で発生した事柄だけでなく、他の組織において発生した事件・事故情報も役に立つ。さらに、事件・事故にまでならなくとも、それにつながりそうな出来事（インシデントという）についての情報も有用である。

組織内に、これらの情報を収集し分析する体制を整え、継続することが重要である。当然のことであるが、他の組織とはさまざまな事情や目標が異なるため、他の組織で起きた事件や事故、インシデントの情報を活用する場合は、その違いを十分に検討する必要がある。

(iii) 投票者とのリスクコミュニケーション

電子投票の実用化に向けては、その利便性やリスクについて、自治体と投票者が十分に情報交換する必要がある。ここでは、リスクコミュニケーションの一般的な定義から、どのような情報が、どのような形で交換される必要があるかを考察する。

リスクコミュニケーションの定義は、「個人、機関、集団間での情報や意見のやりとりの相互作用的過程」と定義される[28]。この定義によると、「リスクの性質についてのさまざまなメッセージ」を「リスク・メッセージ」という。「リスク・メッセージ」は、たとえば、「リスクを低減するためにはどのような行動をとればよいのか」などを含む伝達情報で、「(主たる)送り手から(主たる)受け手への一方向的に伝えられるもの」とされている。さらに、リスクコミュニケーションでやりとりされる情報には、住民から自治体へ伝えられる意見などの逆方向の流れも含まれるというのがこの定義の特徴である。

これを電子投票にあてはめると、まず、電子投票導入の利便性とともに、それに伴い発生するリスクを住民に伝達することが重要といえる。たとえば、遺伝子組み替え食品などのように、先進的な科学技術に係る情報は、専門家が、リスクを含む情報を住民に伝えているが、住民が遺伝子組み替え技術のリスクを充分に理解して受け入れているかどうかは疑わしい[29]。従って、自治体や専門家は、電子投票のリスクを住民に伝える方法を、注意深く検討する必要がある。

平川氏は、PABE の研究を引用し、遺伝子組み替え生物を例として、専門家が陥りやすい 10 神話を提示している。

---

[28]「リスク・コミュニケーション」、吉川肇子著、福村出版、1999 年

[29] 同上

表 37 専門家が陥りやすい神話―遺伝子組み替え生物(GMO)を例として(PABE, 2001)

神話 1	根本的な問題は、一般市民が科学的事実に無知だということである。
神話 2	人々は、GMO に対して「賛成」か「反対」かのどちらかである。
神話 3	消費者は医療用の GMO は受け入れているが、食品・農業に利用される GMO は拒絶している。
神話 4	欧州の消費者は、貧しい第三世界に対して利己的に振舞っている。
神話 5	消費者は、選択の権利を行使するために遺伝子組み替え表示を欲している。
神話 6	一般市民は、誤って、ＧＭＯは不自然なものだと考えている。
神話 7	市民が規制機関を信用しなくなってしまったのは、BSE(狂牛病)危機の失策が原因である。
神話 8	一般市民は「ゼロリスク」を要求しているが、これは不合理である。
神話 9	GMO に対する一般市民の反対は、倫理的または政治的な、「他の」要因によるものである。
神話 10	一般市民は、事実を歪曲する扇情主義的なメディアの従順な犠牲者である。

資料:「不確実性・価値・公共性をめぐるリスクコミュニケーションの諸問題― リスクガバナンスの非公共化に抗して」、平川秀幸（京都女子大学現代社会学部）、日本公共政策学会 2003 年度研究大会 第 15 セッション「環境問題におけるリスク・コミュニケーション」、2003 年 6 月 (http://www.cs.kyoto-wu.ac.jp/~hirakawa/sts_archive/regulatory/PPSA/hirakawa20030615.pdf)

この遺伝子組み替え技術に関する観察は、電子投票の社会的受容を促すための方法論の検討にも充分役に立つと考える。

自治体が実施するリスクコミュニケーションを考える際に考慮すべき点として、住民の「リスク認知」があげられる。神奈川県自治総合研究センターがまとめた「自治体のリスクコミュニケーション[30]」では、人々のリスク認知の特徴として、以下の点をあげている。

(1) 人々は、出来事の記憶しやすさや想像のしやすさに影響を受けやすい。
(2) 単にリスクがあることを指摘するだけでは、人々は、かえってリスク認知を高めて必要以上に恐怖を感じることがある。
(3) 人の強固な信念は、容易に変え難い

考え方や意見がはっきりしない段階では、リスク情報の表現の仕方を少し変えるだけで、リスク認知をかえることができる。

先進的な技術に関するリスクコミュニケーションにおいては、「一般の人々の認知が「高すぎる」と判断する送り手（たとえば企業、専門家、政府など）が、それを「適正な」程度に引き下げようとするものが多い[31]」という意見もある。自治体や企業のリスク認知と住民

[30]「自治体のリスクコミュニケーション」、神奈川県自治総合研究センター、2001 年 3 月
[31]「リスク・コミュニケーション」、吉川肇子著、福村出版、1999 年、pp.31

のリスク認知のギャップを考えた上で、適切な方法を取ることが重要である。

また、住民が電子投票について、どのような意見を持っているかが、自治体側に十分に伝えられなければならない。今回のヒアリング調査においても、自治体と住民の間でさまざまなコミュニケーションが図られていた。もっとも典型的なものはパンフレットによる情報伝達であるが、模擬投票やアンケートという形で、住民がどのように感じているかを調査している事例もあった。特に模擬投票は、実際のオペレーションを体験することにより、不要なリスク認知を避けるといった形で、過去に遺伝子組み換え食品やBSEの事例に見られたように、不可解なものに対して大きなリスクが潜んでいるシグナルと捉えるといったリスクを低減させ、比較的抵抗の低い導入を実現した事例もあった。この模擬投票によるフィードバックの反映は、住民からのリスクコミュニケーションと捉えることができ、今後、より高度な技術を使用する電子投票システムを導入する場合は、さらにこの種の情報伝達手法における工夫が必要になると思われる。

5-4-7 まとめ

調査結果を踏まえたわが国の電子投票に ISMS を適用する場合のポイントをまとめる。

5-4-7-1 リスクマネジメントプロセスの必要性

電子投票において、ISMS のコンセプトを活用する際に重要なのは、リスクマネジメントサイクルと言われる、一定の手順を踏んで管理策を策定することである。これにより、あらゆる脅威について、網羅的に検討することができるようになる。また、リスクマネジメントサイクルの考え方を導入することにより、継続的な改善が可能になり、過去の経験が次の投票時に生かされるというメリットがある。

特に、組織体制について、情報セキュリティに関する最高責任者や担当部署（または担当者）を決めて取り組むのが適切である。現状、多くの自治体では、組織体制が明確にされていない。また、現状、個々の自治体で、リスクについての検討やさまざまな管理策が取られているが、ISMS を導入することによりさらに統制された情報セキュリティ管理が行われるようになる。

5-4-7-2 ベースライン対策の必要性

電子投票を実施するに当たって最低限必要と考えられるベースラインのセキュリティ対策について、何らかのガイドラインが策定されることが望ましい。これは、今後、実施されるすべての電子投票が、一定のセキュリティ・レベルを実現することに役立つと考えられる。また、個々の自治体で、一から個別の管理策を策定する労力を削減することにも繋がる。ただし、ベースライン対策の活用については、情報セキュリティは、個々の実施主体(自治体)でリスク評価をし、管理策を決めるのが基本であり、ベースライン対策として策定された管理策をただ守ればよいという形にならないように注意が必要である。

ベースライン対策は、専門家などにより慎重に検討され、実証実験で適用するなど十分な検討プロセスを経て、策定されることが望ましい。

5-4-7-3 リスクコミュニケーションの必要性

自治体と住民との間で、電子投票に関する情報交換が双方向で行われなければならない。現状、パンフレットや模擬投票という形で行われているが、技術が高度になり、理解がより難しくなった場合を考えた工夫が必要であろう。

電子投票は、特に、住民のリスク認知にバラツキや誤解が発生した場合、投票結果に影響する恐れがあるため、自治体が住民のリスク認知を把握する手段などについても研究が必要と思われる。

5-4-8 米国国防総省 ＳＥＲＶＥ（安全な電子登録および投票実験）のセキュリティ分析報告

5-4-8-1 SERVE（安全な電子登録、投票の実験）についての概要

米国国防総省が推進しているSERVEのセキュリティ分析報告書に関して、その概要をまとめたものである。報告書の英文とその翻訳については、著作権の問題もあるため、プロジェクト内での利用のみとした。

ここには、その概要と本プロジェクトでの考察点をまとめた。

本報告書は、米国国防総省のFVAP（Federal Voting Assistance Program；米国選挙支援事業）の援助を受けて構築したインターネット上での投票システムSERVE（Secure Electronic Registration and Voting Experiment；セキュア電子登録、電子投票の実験装置）におけるコンピュータシステム情報のセキュリティを評論したものである。（参照：http://www.serveusa.gov/）。本システムは現時点で実験段階とは言え、近い将来の総選挙使用する予定となっている。本報告はSPRG（the Security Peer Review Group；セキュリティピア評価団体コンピュータによる投票の安全をFVAPにより集められSERVEを評価する団体）のメンバーによって書かれた。主なテーマは、システムの脆弱性を検査することと、多方面からのサイバーアタックの可能性の確認と選挙の安全性と課題の摘出、解決策の提示である。

SERVEシステムは2004年度の予備選挙と最終選挙に展開する予定である。有権者は選挙区への登録をし、どこからでもインターネットを通じて選挙可能になる。現時点で参加ができるのは、米国外在住の投票者で7つの州（アーカンソー、フロリダ、ハワイ、ノースカロライナ、サウスカロライナ、ユタ、ワシントン）の50郡に住む有権者や軍関係者である。今回の予備・最終選挙において10万人のSERVEシステム参加が見込まれている。2000年度の最終選挙の全投票者数は約1億人であった。目標は海外に住む全ての有権者、軍関係者とその扶養家族にSERVEを使用することである。その数は約6百万人に及び、2004年度のSERVE計画で将来のプロトタイプとなることが期待されている。

結論は以下にまとめられる。

ＤＲＥ（direct recording electronic：直接電子式記録）投票方式には多々なる欠点と攻撃されやすいセキュリティの問題があった。そのプログラムは完全に閉鎖的・独占的であり、セキュリティ評価を受けておらず、脆弱なものであった。特に内部攻撃（プログラマー）の標的となりえるものだ。ＤＲＥは投票者認証記録が物理的に残されないという問題と、有権者からの信頼性の点で問題があった。ＳＥＲＶＥにも同様の課題があると言える。

それだけではなく、ＳＥＲＶＥはインターネットやＰＣを利用するシステムである為、たくさんの根本的なセキュリティ問題がある。例えば、内部攻撃、サービス妨害攻撃、なりすまし、投票権売買、コンピュータウイルスなどなど、大災害をもたらす可能性がある。

このような攻撃は大規模に発生し、影響は個人ばかりではなく米国の法治外の国々まで広がる可能性がある。そして、投票システム加入者以外への影響、個人のプライバシー侵害、投票権の売買、投票結果の混乱を引き起こす。いうまでもなく、大統領選にも影響する。完全犯罪も可能であり、そうでなくとも、社会的混乱は避けられない。

選挙に対するサイバー攻撃の成功率を憶測するのは困難である。しかし、本報告で私たちは何故に容易にシステムに侵入できるかを示す。インターネット上には既にいくつかのキットがでており、これで選挙システムへの変更や直接的攻撃が可能である。かくして、米国総選挙はインターネットのサイバーアタックの歴史な標的になっていることを念頭に置かなければならない。たとえ、その動機が攻撃者の個人的興味であろうと、政治的理由であろうと。

ここで示す脆弱性はＳＥＲＶＥのバグ修正や更改ですむような問題ではなく、今日のユビキタスネットをもたらしているインターネット、ＰＣなどの構造的な欠陥である。これらの課題は今のところ抜本的に改善しなければ解決の見通しがないといえる。すなわち、インターネットに接続されているすべてのハード、ソフトのセキュリティ機能を置き換えなければならない根本的課題といえる。

我々は、SERVE 以外にもインターネット選挙システムについて多くの調査をした。選挙者にとって利便性のあるシステムやセキュリティ上もっと脆弱なものあるいは中程度のものがあった。しかし、他の例すべてについて、ＳＥＲＶＥのもつ脆弱性について基本的な問題が存在し、ＳＥＲＶＥの代替案として提唱できるものはなかった。ここでは、ＳＥＲＶＥの目的に沿うものとして、Ｋｉｏｓｋ構造を持つ選挙システムを提唱する。しかし、これはインターネットベースではないし、一般の安全でないＰＣソフトで構成されるものではない。

ＳＥＲＶＥは２００４年の選挙において無事運用されていると見なされている。しかし、大統領選挙で一見成功したようである。しかし、ＳＥＲＶＥが信頼性があり、堅牢で安全なシステムと評価されることは、ある意味で不幸な事象である。ますます、この影響が拡大し、将来このような類の選挙システムが普及した後に、巧妙な手口で壊滅的打撃を受ける可能性があるからである。

ＳＥＲＶＥのようなシステムが海外の軍隊における選挙をサポートすべきであることを認めるが、現在のＳＥＲＶＥは残念ながら実用にはまったく耐えられるものではない。それは、攻撃が成功したときの影響があまりに大きすぎるからである。我々は、何度も言うようだがＳＥＲＶＥに対し基本的に設計しなおし、セキュリティ上の抜本的解決が図られるまでは現状のＳＥＲＶＥを直ちに適用を中止すべきであることを切に要望する。

我々は、現プロジェクトを否定しているのではない。本当の問題は、関係者の見識が甘いとか、技術に問題があるとか、リソースの問題、検討姿勢ということではなく、FVAPの企画した全電子的に遠隔からおこなう投票システムの安全性の要求条件が現状のインターネットとPCのセキュリティ技術では本質的に実現不可能であるということなのだ。このようなことは、現状のインターネットやPCを根本から変えなければならい。あるいは、将来セキュリティの抜本的解決があれば別だが。SERVEプロジェクトは現時点では先を行き過ぎており、セキュリティインフラが整備されるまでは再検討すべきものである。

5-4-8-2　本論文に対する評価

以下に、本論分の評価を行う。

①　インターネット電子投票はサイバー攻撃の対象

インターネット電子投票は本論文にあるようにサイバー攻撃の対象となりやすいので、適用には十分配慮すべきである。

すなわち、インターネットを利用した電子投票などの行政活動に対しては、ハッカーなどの攻撃対象としての興味をそそるものがある。愉快犯や反体制派などの攻撃目標になりやすいといえよう。

②　特に、サイバー攻撃は考慮すべき

次の米国の動きは参考になり、国レベルで積極的な検討が進められている。また、同報告には、日本と連携についても言及している。

http://www.glocomnet.or.jp/okazaki-inst/700tamura.cyber1.html
http://www.glocomnet.or.jp/okazaki-inst/cyber2.tamura.html

上の URL には、「米国のサイバー攻撃対策の現状と課題」(著者:田村重信（慶應義塾大学大学院講師）がのべられており、次の項目が書かれている。

(上)の内容:

安全保障専門議員の動き、米国におけるサイバー攻撃の現状　、サイバーセキュリテイ政策の変遷　、国防省・国防情報システム庁のコンピュータ網防護統合任務部隊

(下)の内容

情報保証概念の導入　、インサイダーによる脅威　、国防省の対応　、FBI国家インフラ防護センター(NIPC)　、民間企業へのアプローチ　、ジョン・カイル上院議員が日米の協力を強調　、米国が直面する課題

③　サイバー攻撃について

「サイバー攻撃」については、過去 10 年位、多くの議論があり、”サイバー攻撃＝サイバーテロ”と考える議論がある一方、米国国防総省(DoD)や CERT/CC の調査に基づいた議論[注]がある。

ただ、最近の有害プログラムなどの蔓延をみていると、インターネットに対するサービス妨害(Denial of Service)が行われる可能性はゼロではないため、どの様な問題が発生するかを冷静に見極め、本プロジェクトで考察を行うことは必要であると考えている。

(注)2002 年 7 月に米国大統領重要基盤保護委員会(the president's Critical Infrastructure Protection Board)の副委員長、Howard Schmidt は、「昨年、米国国防総省は DoD への侵入の 97、98%は既知の脆弱性へのパッチプログラムの未適用や不適切なシステム設定が原因であるという調査結果を発表している。ネットワーク侵入を防御するために必要な技術は『何かの技術である』との誤解があるが、これは技術の問題ではない。」と述べている(http://www.govtech.net/magazine/sup_story.phtml?id=18492)。また、CERT/CC でも同様な調査結果がある。

④　研究プロジェクトでの考え方

(イ) 本論文は、『次世代電子投票・アンケートシステム』と同一の環境でのシステムではないため、そのまま本論文での結論が適用されるわけではない。

(ロ) しかしながら、この論文で行われた検討を十分吟味し、情報収集や実証実験などを通じて、本プロジェクトの方向性を見出すことが大切である。

(ハ) ICカードを利用している点の有効性を再評価すべきであろう。

(ニ) MobileVPNの導入の提案:

環境によっては、VPNで擬似的な専用線ネットワークを構成し、安全性を高めることも考えられる。また、どこからでもアクセスを可能にするには動的に割り付けるMobileVPNは有効と思われる。

(ホ) セキュリティ運用の重要性

セキュリティを確保するには、管理・運用の重要性は本プロジェクトでも当初から考えてきており、今後とも、人間系がどのようにかかわって全体システムとして安全を担保できるかを検証する必要がある。

⑤ その他

大統領選挙を控え、軍からの投票が正確に行われたときに現在の体制で不利になるほうが、この論文を書いているという見方も出来る(不在者投票にはすでに偏りがあるという表現がある)。 しかしながら、本プロジェクトではこの様な意見も含め、広範囲に検討を進めていきたい。

5-5　モデル構築

5-5-1　プロトタイプシステムの実装

本節では、昨年度の概要設計をもとに実装したプロトタイプシステムについて説明する。実装したプロトタイプシステムのイメージは以下のとおりである。

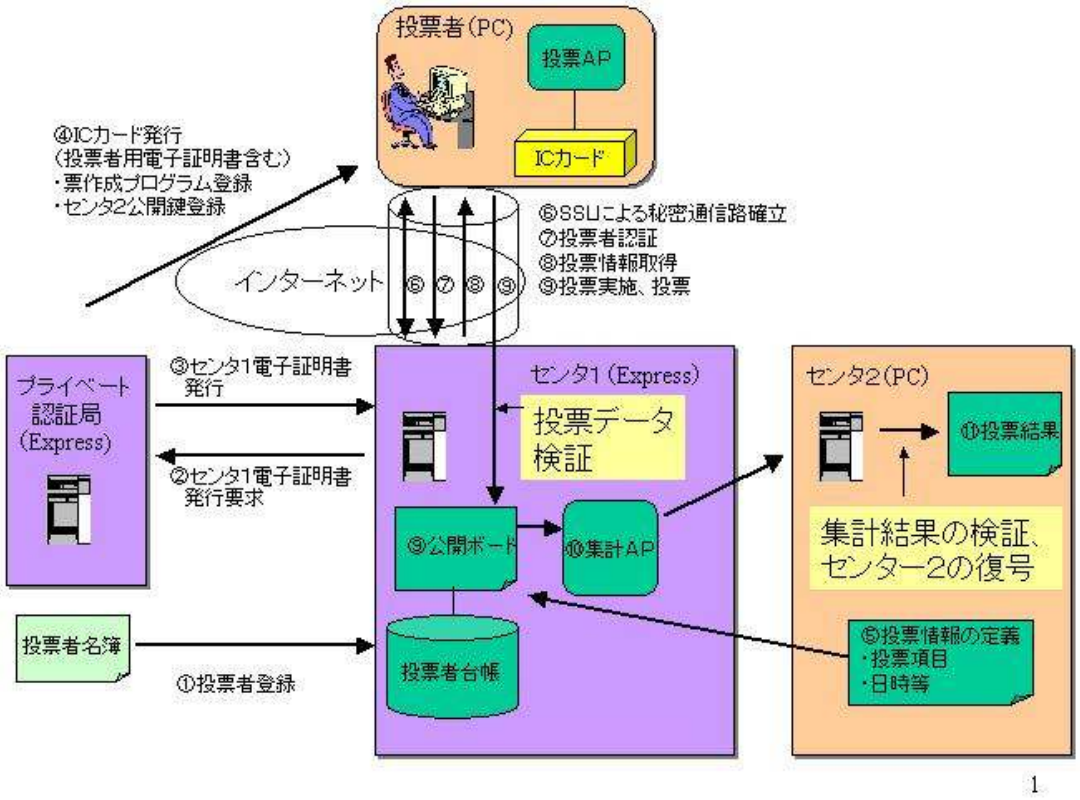


図 44　電子投票プロトタイプシステムイメージ

5-5-1-1　プライベート認証局

プライベート認証局では、主として電子証明書を発行する。電子証明書の発行には、CertWorker という認証局ミドルウェアを使用し、投票者に配布する投票用 IC カードの発行には、独自ツールを開発してそれを使用した。

① 投票者 IC カード発行ツール

本ツールは、SHARP からリリースされた独自投票アプリケーション書込み済みの IC カードに、センター2公開鍵、センター2公開鍵パラメータ、投票者クライアント証明書を書き込む機能を有する。画面イメージを以下に示す。

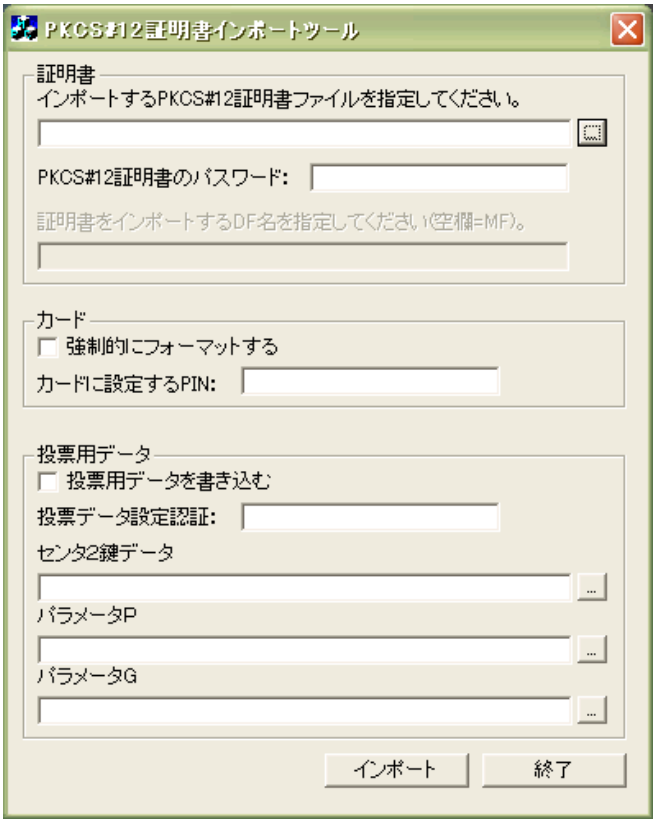


図 45　投票者 IC カード発行ツール画面イメージ

5-5-1-2　センター1

センター1では、主として投票データの受付、集計等を行う。実装したセンター1のプログラムを以下に示す。

① 公開ボードプログラム

公開ボードプログラムは、センター1の公開ボードに格納されている各種コンテンツを容易にアクセスする手段を提供するライブラリ群である。以下に提供する主な API を挙げる。

投票データ登録
投票データ取得
投票アプレット登録
候補者情報取得
集計結果データ登録
集計結果データ取得
集計証明データ登録
集計証明データ取得

② 投票データ受信プログラム

投票データ受信プログラムは、投票者 PC から送信されてくる暗号化投票データを受信し、公開ボードに登録するプログラムである。本プログラムは、WEB アプリケーションとして動作し投票データを登録する際に以下検査を実施し、エラーを検出した場合は、投票者 PC にその旨を報告する。

投票期間内の投票
二重投票
投票データの正当性検証(コミットメントデータ検証)

③ 集計プログラム

集計プログラムは、公開ボードに収集された暗号化投票データを取り出して集計し、求まった集計結果を公開ボードに登録するプログラムである。本プログラムは、スタンドアロンアプリケーションとして動作し、投票データが暗号化されたままの状態で集計可能な特徴を有する。

④ 集計証明生成プログラム

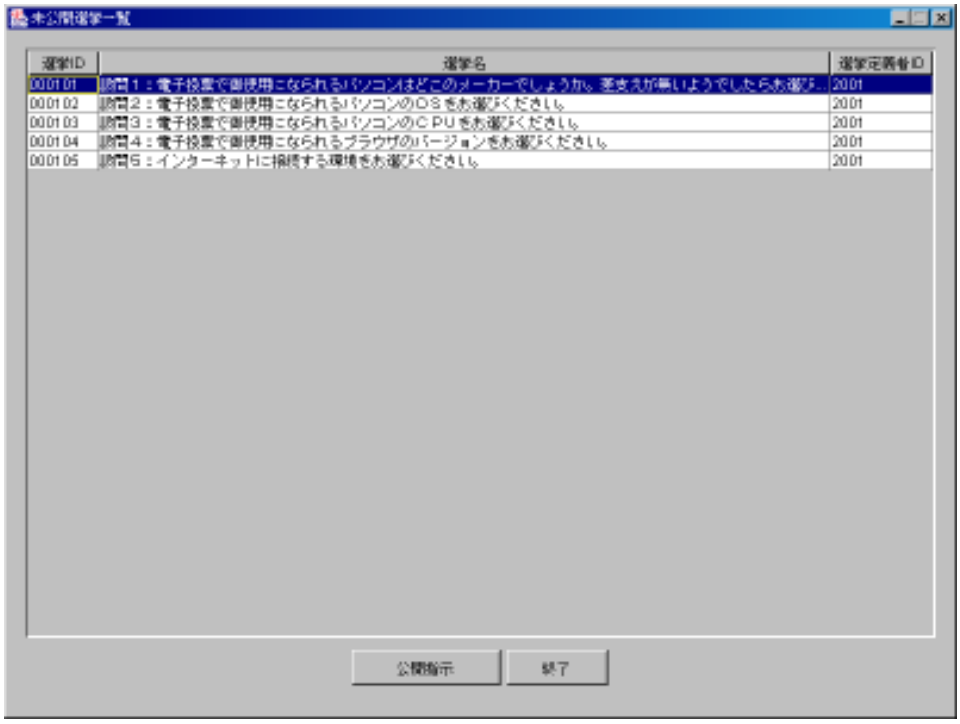
集計証明生成プログラムは、公開ボードに収集された暗号化投票データを取り出して集計結果の正当性を証明するデータを生成し、生成した集計証明データを公開ボードに登録するプログラムである。本プログラムは、スタンドアロンアプリケーションとして動作する。

⑤ 投票アプレット受信プログラム

投票アプレット受信プログラムは、センター2から送信されてくる投票アプレットを受信し、公開ボードに登録するプログラムである。本プログラムは、WEB アプリケーションとして動作し、投票アプレットの登録が完了すると、センター2にその旨を報告する。

⑥ 選挙公開プログラム

選挙公開プログラムは、センター2から投票アプレットが登録された後に、選挙の公開期間を設定するプログラムである。選挙の公開日が設定された時点で、投票者はその選挙にアクセスして投票可能となる。本プログラムは、スタンドアロンアプリケーションとして動作する。以下に選挙公開プログラムの画面イメージを示す。



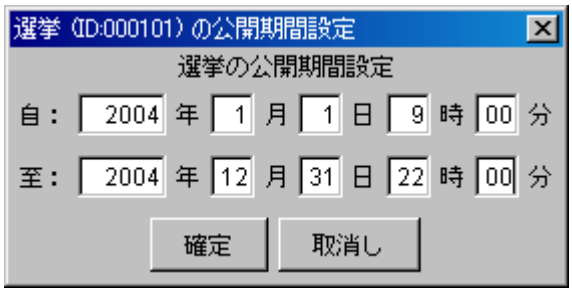


図 46　選挙公開プログラム画面イメージ

⑦　投票ページ生成プログラム

投票ページ生成プログラムは、各選挙の投票期間をチェックし現在投票可能な選挙をリストアップして投票者に提供するプログラムである。本プログラムは、WEB アプリケーションとして動作する。以下に本プログラムが生成する投票ページの画面イメージを示す。

図 47　投票ページ画面イメージ

⑧ 投票者認証プログラム

投票者認証プログラムは、投票者がその選挙に対して投票権があるかどうか認証するプログラムである。本プログラムは、投票ページから投票する選挙の投票ボタンを押したときに起動されるWEBアプリケーションであり、投票権がある場合は、投票アプレットがロードされて投票可能となるが、投票権がない場合は、エラー表示されて、投票不可能となる。以下に投票者認証開始画面と投票権が無く、認証に失敗した場合の画面イメージを示す。

図 48　投票者認証画面イメージ

⑨ 投票状況確認プログラム

投票状況確認プログラムは、各選挙の投票状況（投票済、投票未の情報や投票時間等）を各投票者に提供するプログラムである。本プログラムは WEB アプリケーションとして動作する。以下の投票状況確認プログラムが提供する画面イメージを示す。

図 49　投票状況確認画面イメージ

5-5-1-3　センター2

センター2では、主としてセンター2 鍵ペア生成、投票アプレットの定義、開票等を行う。実装したセンター2のプログラムを以下に示す。

① センター２OU 鍵ペア生成プログラム

センター2OU 鍵ペア生成プログラムは、OU 秘密鍵と OU 公開鍵のペアを生成するプログラムである。OU 公開鍵は、投票データを暗号化するために使用され、各投票者の IC カードに格納されて配布される。OU 秘密鍵は、センター2で暗号化された集計結果を復号するために使用される。本プログラムはスタンドアロンアプリケーションとして動作する。以下にセンター2OU 鍵ペア生成プログラムの画面イメージを示す。

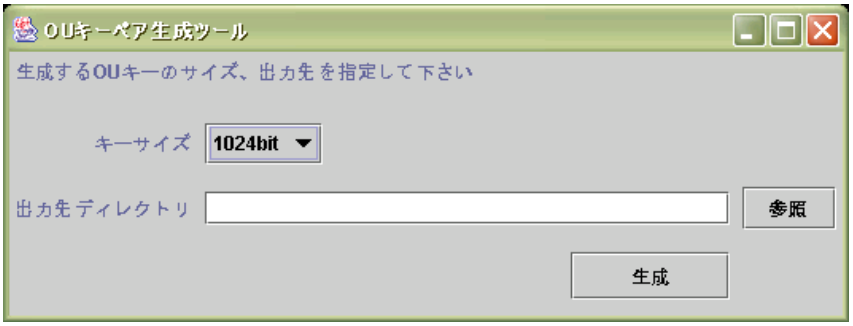


図 50　センター2OU 鍵ペア生成プログラム画面イメージ

② センター２OU 公開鍵パラメータ生成プログラム

センター2OU 公開鍵パラメータ生成プログラムは、OU 公開鍵からパラメータ(p、G)を生成するプログラムである。OU 公開鍵パラメータは、各投票者の IC カードに格納されて配布される。OU 公開鍵パラメータは、投票 PC から投票データと共にセンター1に送信され、センター1 で受信した投票データの正当性を検証する際に使用される。本プログラムはスタンドアロンアプリケーションとして動作する。以下にセンター2OU 公開鍵パラメータ生成プログラムの画面イメージを示す。

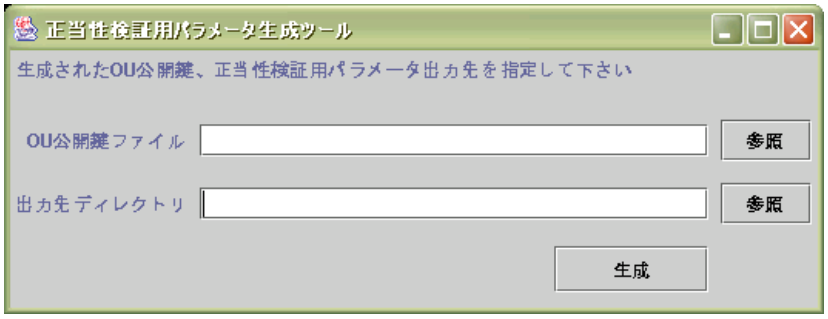


図 51　センター2OU 公開鍵パラメータ生成プログラム画面イメージ

③ 投票アプレット定義プログラム

投票アプレット定義プログラムは、エディタで編集した候補者メタデータ XML ファイルを読み込み、センター1に登録する投票アプレットを生成するプログラムである。本プログラムはスタンドアロンアプリケーションとして動作する。以下に投票アプレット定義プログラムの画面イメージを示す。

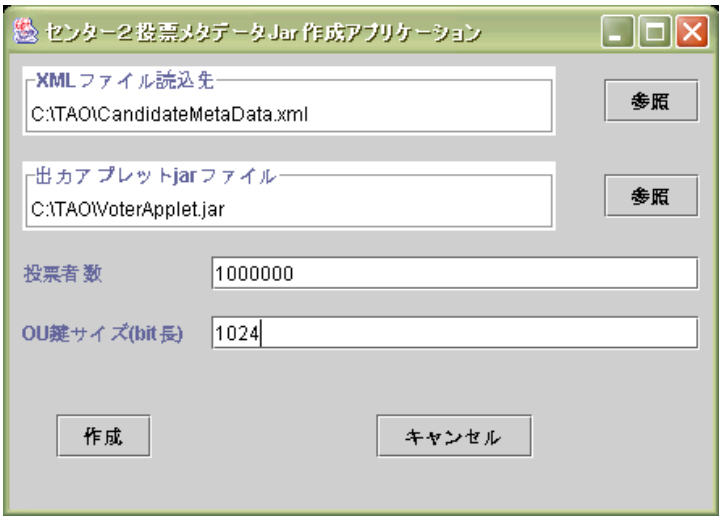


図 52　投票アプレット定義プログラム画面イメージ

④ 投票アプレット登録プログラム

投票アプレット登録プログラムは、投票アプレット定義プログラムで作成した投票アプレットを最大5つまでセンター1 に登録するプログラムである。本プログラムはセンター1 の投票アプレット受信プログラム（WEB アプリケーション）にアクセスすることで動作し、SSL のクライアント認証を必要とする。以下に投票アプレット登録プログラムの画面イメージを示す。

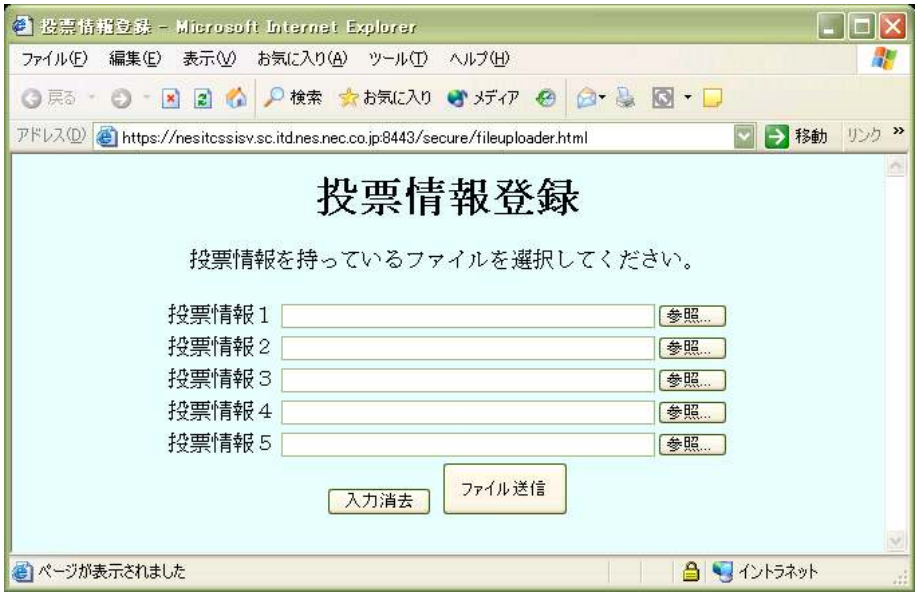


図 53　投票アプレット登録プログラム画面イメージ

⑤ 公開ボードコンテンツダウンロードプログラム

公開ボードコンテンツダウンロードプログラムは、ある選挙 ID の公開ボードコンテンツをセンター2 にダウロードするプログラムである。本プログラムはセンター1 の公開ボードにアクセスすることで動作し、SSL のクライアント認証を必要とする。以下に公開ボードコンテンツダウンロードプログラムの画面イメージを示す。

図 54　公開ボードコンテンツダウンロードプログラム画面イメージ

⑥ Proof2 集計結果正当性検証プログラム

Proof2 集計結果正当性検証プログラムは、公開ボードからダウンロードした暗号化集計結果を対象に正当性の検証をするプログラムである。本プログラムは、スタンドアロンアプリケーションとして動作する。以下に Proof2 集計結果正当性検証プログラムの画面イメージを示す。

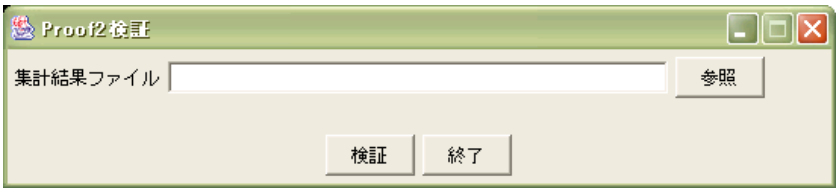


図 55　Proof2 集計結果正当性検証プログラム画面イメージ

⑦ Proof3 集計結果正当性検証プログラム

Proof3 集計結果正当性検証プログラムは、公開ボードからダウンロードした暗号化集計結果の正当性検証データを対象に正当性を検証するプログラムである。本プログラムは、スタンドアロンアプリケーションとして動作する。以下に Proof3 集計結果正当性検証プログラムの画面イメージを示す。

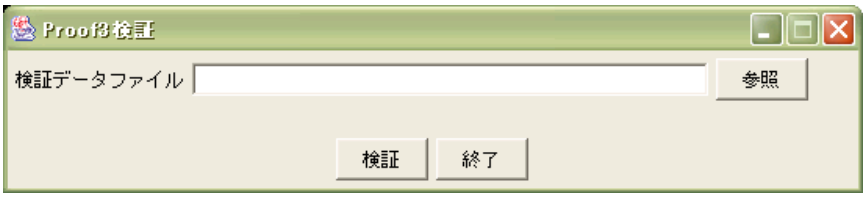


図 56　Proof3 集計結果正当性検証プログラム画面イメージ

⑧ 集計結果開票プログラム

集計結果開票プログラムは、公開ボードからダウンロードした暗号化集計結果を OU 秘密鍵で復号する。また、投票アプレット内の候補者メタデータと突き合わせて、開票結果をCSVファイルに出力する。本プログラムは、スタンドアロンアプリケーションとして動作する。以下に集計結果開票プログラムの画面イメージと、集計結果の開票 CSV イメージ例を示す。

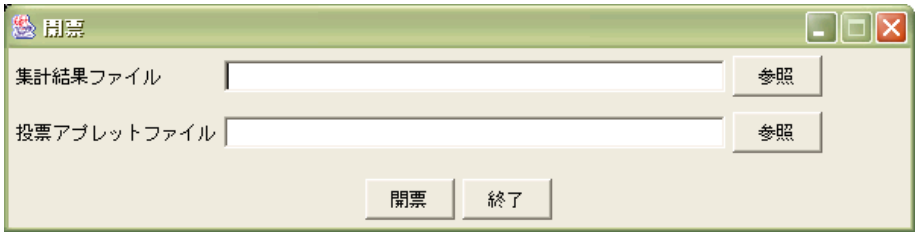


図 57　集計結果開票プログラム画面イメージ

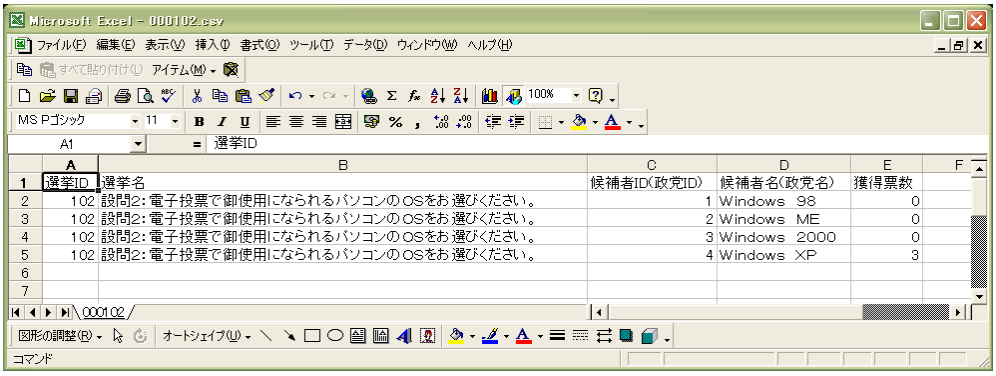


図 58　集計結果の開票 CSV イメージ例

5-5-1-4　投票者 PC

投票者 PC では、センター1 から選挙情報を取得し、投票を行う。実装した投票者 PC のプログラムを以下に示す。

① 投票アプレット

投票アプレットは、センター1に配置される小さな Java プログラムで投票者 PC にダウンロードされて WEBブラウザ上で実行される。投票アプレットは、センター1から選挙情報を取得し、投票者ICカードに格納されている投票データ作成アプリケーションにアクセスして投票データを生成し、センター1に送信する。以下に投票アプレットの画面イメージを示す。

図 59　投票アプレット画面イメージ

② 投票データ作成プログラム（投票者 IC カードアプリケーション）

投票データ作成プログラムは、投票者 IC カードに格納される小さなプログラムで、投票データを生成し、投票者 IC カードに格納されている OU 公開鍵、OU 公開鍵パラメータ p,G で投票データの暗号化、投票データのコミットメントデータの生成を実施する。暗号化された投票データと、生成した投票データのコミットメントデータは、投票データフレームにラップし、投票アプレットに出力する。

③ 投票者クライアント証明書管理プログラム

投票者クライアント証明書管理プログラムは、投票者 IC カードの IC カード装置への挿入を監視する常駐プログラムである。投票者 IC カードが IC カード装置に挿入されると、PIN 番号認証を実施し、WEB ブラウザが IC カードからクライアント証明書を取得できる状態にする。以下に投票者 IC カード挿入時に起動される PIN 番号認証画面イメージを示す。

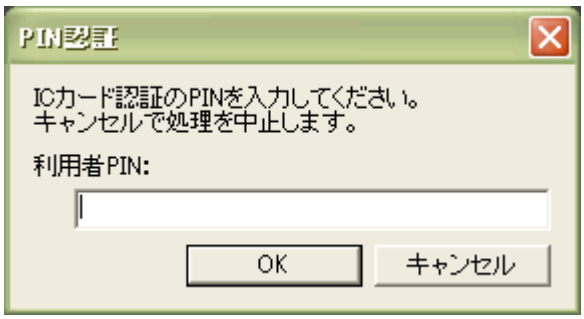


図 60　PIN 番号認証画面イメージ

5-5-2　プロトタイプシステムのハウジング作業

本節では、電子投票実験を実施するために行った電子投票プロトタイプシステムのハウジング作業について説明する。ハウジング作業を実施したのはセンター1サーバ、データベースサーバ、プライベート認証局サーバの 3 台のサーバで、以下詳細に説明する。

5-5-2-1　電子投票プロトタイプシステムの HW・SW 構成

電子投票プロトタイプシステムの各サーバ側の HW 構成ならびに SW 構成は以下のようになっている。

① プライベート認証局サーバ
HW 構成
Express 5800 / 120 Ra-1
1GHz×2CPU
1179MB メモリ
HDD×2　RAID1　総容量 36GB
SW 構成
Microsoft Windows 2000 Server SP4
CertWorker 1.0

② センター１サーバ
HW 構成
Express 5800 / 120 Ra-1
1GHz×2CPU
1179MB メモリ
HDD×2　RAID1　総容量 36GB
SW 構成
Microsoft Windows 2000 Server SP4
Microsoft Internet Information Server 5.0
Apache Tomcat 4.1

③ データベースサーバ
HW 構成
Express 5800 / 120 Ra-1
1GHz×2CPU
1179MB メモリ
HDD×2　RAID1　総容量 36GB
SW 構成
Microsoft Windows 2000 Server SP4
Oracle 9i Database Server

5-5-2-2　電子投票プロトタイプシステムの NW 構成

電子投票プロトタイプシステムのネットワーク構成を説明する。プライベート認証局サーバ、センター1サーバ、データベースサーバは、NECソフトが管轄する東京データセンター内に設置され、厳重なセキュリティ管理のもと運用され、インターネットを経由して各投票者PC、センター2にサービスを提供する。以下に電子投票プロトタイプシステムのネットワーク構成を示す。

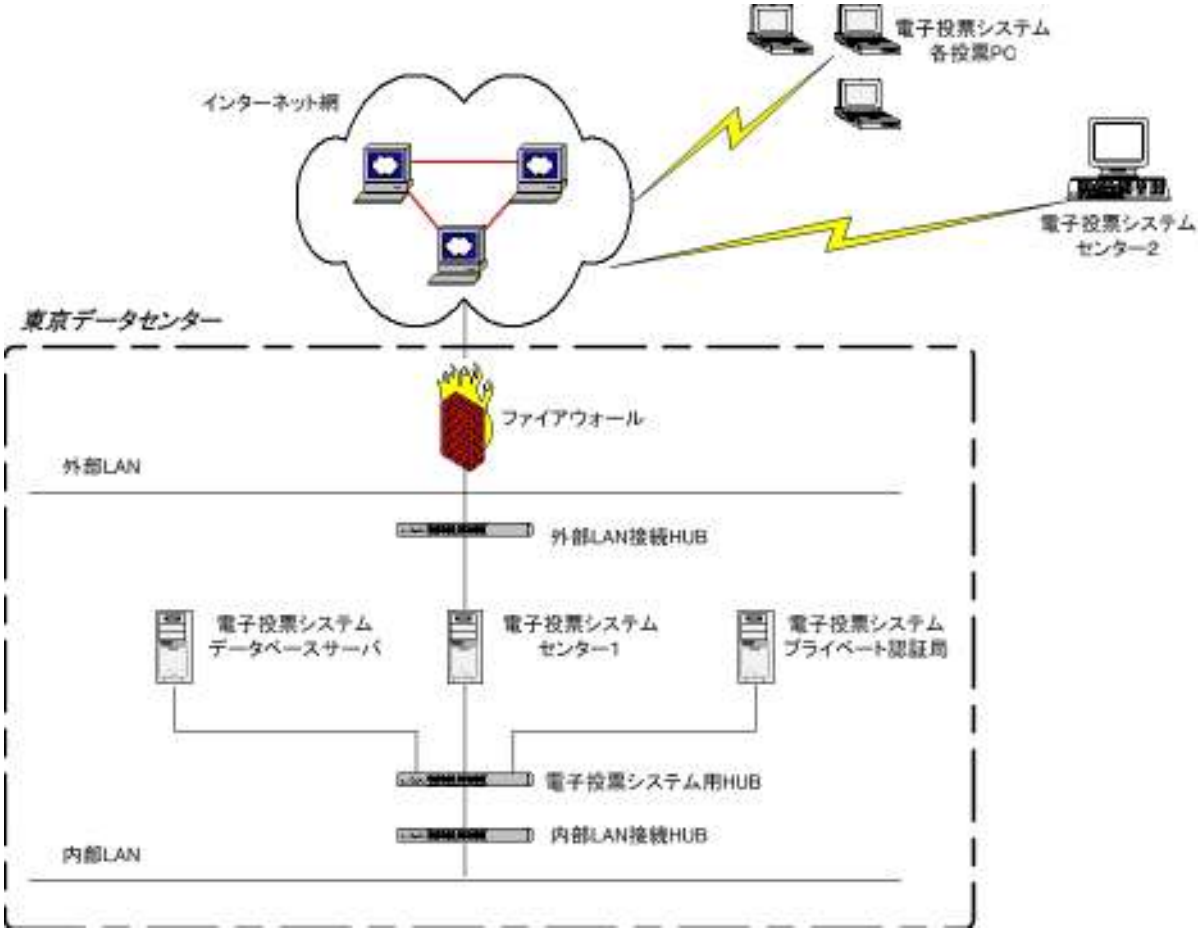


図 61　電子投票システムネットワーク構成図

5-5-2-3　電子投票プロトタイプシステムのセキュリティ管理

電子投票プロトタイプシステムのプライベート認証局サーバ、センター1サーバ、データベースサーバは、NEC ソフトが管轄する東京データセンターに設置される。東京データセンターは、厳重なセキュリティ管理のもと運用されている。以下に主なセキュリティ施策について説明する。

① 東京データセンタービルの入出管理

東京データセンタービルは、24時間365日、警備員による厳重なセキュリティが実施されている。また、入館の際は、入館記録簿を記入することで、入出管理が徹底されている。

② 東京データセンター内マシン室の入出管理

東京データセンター内のマシン室も厳重なセキュリティが実施されている。具体的には、東京データセンター機密保持合意書への署名、セキュリティカードの利用、監視カメラによる監視が行われている。

③ 東京データセンター遠隔保守マシン室の入出管理

東京データセンター内のマシンには、内部の専用 LAN を経由して遠隔保守が可能になっている。遠隔保守端末は、NEC ソフト内のマシン室に設置されている。NEC ソフト内マシン室は、指紋認証による厳重なセキュリティが実施されている。

5-5-2-4 電子投票プロトタイプシステムの障害管理

電子投票プロトタイプシステムが設置されている東京データセンターには、保守オペレータが常時システムの障害を監視している。システムの障害が検出されると保守オペレータから電子投票システムの管理者に対して電話・電子メールで通報される。通報を受けた電子投票システム管理者は、適切な処置を施し、処置完了報告を保守オペレータに対して行う。以下に監視内容を挙げる。

① サーバ死活監視

ping によるサーバ機器活性状態を監視。

② サーバ状態監視

サーバリソース(CPU 使用率、DISK 使用率、ネットワーク使用率)の閾値監視

③ HTTP 監視

外部公開 URL に対して、GET リクエストを送り、その応答コードを監視

④ ハードウェア稼動監視

ESMPRO/ServerAgent が検出する障害情報を監視

5-5-2-5 電子投票プロトタイプシステムの運用管理

電子投票プロトタイプシステムは、東京データセンターの保守オペレータにより運用される。運用方法については、電子投票システム管理者が運用手順書を作成し、保守オペレータはその運用手順書に従ってシステムを運用する。以下に作成した電子投票システムの運用手順書を示す。内容については、別冊を参照されたい。

① 運用手順書

運用仕様書.doc

② サーバ起動・シャットダウン手順書

サーバ起動・シャットダウン手順書.doc

5-5-3 参加企業実験

前項のハウジング作業を実施した電子投票プロトタイプシステムで、研究参加企業（中央大学、NEC ソフト、サイファージャパン）内の模擬実験を実施し、システムの運用性を確認した。実験の詳細や、結果の分析については別で述べることとし、ここでは、モデル構築として実験の為に準備したことについて述べる。

5-5-3-1 電子証明書の発行

電子投票システムのセンター1と投票者 PC 間、センター1とセンター2間は、インターネット網を通じて SSL 通信でアクセスされる。SSL 通信は、通常のサーバ認証だけでなく、クライアント認証も実施することとした。従って、プライベート認証局サーバの認証局ソフトである CertWorker を使って以下の電子証明書を発行した。

① プライベートルート証明書
発行数は1通。センター1サーバ、センター2PC、各投票 PC にインストールする。

② センター１サーバ証明書
発行数は1通。センター1サーバにインストールする。

③ 投票者クライアント証明書
発行数はセンター2と各投票者数分。センター2PC と各投票者 IC カードにインストールする。

④ 投票アプレットの署名用証明書
発行数は1通。センター1サーバに配置する投票アプレットを署名するのに使用する。投票アプレットは、投票 PC で投票時に署名付アプレットとしてダウンロードされ、その時に正当なものかどうか検査される。

5-5-3-2 投票者 IC カードの発行

投票者ICカードは、電子投票プロトタイプシステムで投票する時に必要となる。投票者ICカードは「投票者 IC カード発行ツール」で発行する。投票者 IC カードに書き込まれる情報には以下のものがある。

① 投票データ作成アプリケーション（iccap.a60）
投票データ作成アプリケーションは、投票PCの投票アプレットからアクセスされるICカードアプリケーションで、投票データを生成して暗号化する。本アプリケーションは、カード製造会社（SHARP）で書き換え不可の状態で書き込まれて出荷される。アプリケーション ID は、”03 00”が設定される。

② センター2 公開鍵（ou_pubkey.bin）
投票 PC で作成する投票データを暗号化するのに使用される。

③ センター2 公開鍵パラメータ（P.bin, G.bin）
投票 PC で作成する投票データが正当なものか検証するために使用される。センター1 が投票データを受付ける際、投票 PC から送信されてきた本パラメータで投票データの正当性を検証する。

④ 投票者クライアント証明書（シリアル番号.p12）
投票 PC がセンター1 にアクセスするときの SSL クライアント認証で使用される。

5-5-3-3　インストーラの作成

参加企業実験用に作成したインストーラを以下に示す。

① 投票 PC 用インストーラ（InstallAnywhere 形式）

N3NVSS.exe

② センター２用インストーラ（ZIP 形式）

Center2.zip

5-5-3-4　マニュアルの作成

参加企業実験用に作成したマニュアル類を以下に示す。内容については別冊を参照されたい。

① 投票者 PC インストール手順書

投票者PCインストール手順書.pdf

② 投票者 PC 操作説明書

投票者PC操作説明書.pdf

③ センター２インストール手順書

センター2インストール手順書.txt

④ センター２操作説明書

センター2操作説明書.rtf

5-6　システム構成

5-6-1　システム構成の方針

5-6-1-1　背景、目的

平成14年度成果報告書「5-6 準同型公開鍵暗号」で示された、通信の効率と復号性能で優位性のある OU 関数の実装を行い、データ量・処理速度の考察を行った。

また、平成14年度成果報告書「5-7 投票プロセスの正当性証明とその効率化」において研究された「集計の正当性証明」および「復号の正当性証明」を実装し、データ量・処理速度の考察を実施した。

5-6-1-2　方針

以下の方針に従って準同型公開鍵暗号を実装する。

1)　プラットフォームの想定

投票者・集計センター・開票センターの機能を実装するプラットフォームは、H14 年度と同様に以下を想定する。

①　投票者機能

投票者機能は投票作成用プログラム、パラメータおよび個人認証用パラメータを投票者(PC)に配布する事で実現する。このプログラムおよびパラメータを配布する方法として、一般的に安全とされている IC カードを選択した。IC カードには高い耐タンパー性があり、改竄等が非常に困難であると言われている。この特徴により、IC カード内に組み込んだプログラムおよびパラメータの健全性を確保する。

②　センター機能

センター1 およびセンター2 機能である鍵生成・集計・復号に関しては、一般的なサーバマシン上にて実現する。

2)　OU 関数の性能測定

①　処理時間の測定

鍵生成処理、暗号化処理、集計処理、復号処理の性能測定を行う。

②　データ量

平文サイズの違いによるデータ量を比較し、投票者 PC、センター1、センター2 のデータ量の概算を求め比較を行う。

3)正当性検証機能の性能測定

①　集計検証処理

検証パラメータ生成処理、コミットメントデータ検証処理、Proof2 検証処理、Proof3 検証用パラメータ生成処理、Proof3 検証処理

②　復号検証処理

復号検証データ生成処理、復号検証処理の性能測定を行う。

③ 電子署名検証処理

電子署名データ生成処理、電子署名検証処理の性能測定を行う。

④ 検証用データのサイズ

実際の投票を想定場合の集計検証用データ、復号検証用データ、電子署名検証用データの概算を行う。

5-6-1-3 現状の課題と研究

OU 関数の実装に当たり、高速化を図るために IC カード、サーバそれぞれのプラットフォームに適した実装が必要となる。

① IC カード上の実装

IC カードで用意されている機能を十分に活用して、べき乗剰余演算の性能アップを計る。べき乗剰余演算では多倍長演算やメモリの使用方法が性能に著しく影響を与えるため、この点に十分注意をする。

② サーバ上の実装

サーバ実装処理を高速化するために、多倍長演算ライブラリを使用する。

また、関数単体で最適な高速化手法を検討し、実装する。

5-6-1-4 研究内容

H15 年度の研究内容の概要に関して以下に示す。

① H15 年度の目標

TYKK 方式に基づくシステム構築の元となる準同型性暗号を実装する。

② H15 年度の実施内容

準同型性暗号方式に関して OU 関数を投票者用，センター用ともに実装および性能評価を実施した。

また、集計処理，復号処理の正当性証明用関数の実装および性能評価を実施した。

③ H15 年度の効果

IC カード用 OU 関数（暗号機能）の実装および性能評価を実施し、100 万人規模の大規模選挙においても問題なきことを確認した。サーバ用 OU 関数（鍵生成、復号、集計機能）に関しても実装および性能評価を実施し、100 万人規模の大規模選挙においても問題なきことを確認した。

また、集計処理，復号処理の正当性証明用関数を実装し、不正な集計処理を検出できることを確認した。

④ 取り組み状況

システム構成としての実装・評価は完了し、システム構成として全機能・実装・評価結果を盛り込んだ成果報告書を執筆開始。

自治体実験に向けて改善が必要で有れば、対応する予定である。

5-6-2 基本仕様

5-6-2-1 OU 関数・正当性検証機能実装検討

(i) IC カード実装処理の高速化

a) コプロセッサメモリの使用

暗号化処理の高速化には、多倍長演算処理をいかに短時間で実施するかが鍵である。IC カード上での多倍長演算処理の速度は、IC カード上でべき乗剰余を行うコプロセッサの性能に依存する。

今回採用する IC カードには、コプロセッサの性能を最大限に発揮するための二つの機能が用意されている。一つはデータセット制御機能、もう一つは COPY 制御機能である。

データセット制御機能は、コプロセッサ RAM にデータを設定する時に、前回のコプロセッサ演算で使用したデータを再度利用することを可能とする機能である。

COPY 制御機能は、コプロセッサ RAM に格納された演算結果を別のコプロセッサ RAM にコピーする機能である。

いずれの機能も RAM を介さずにダイレクトにコプロセッサ RAM を使用することで高速化が図れ、同時に RAM メモリの節約に繋がる。

実装に当たっては、この2つの機能を使用するものとする。

b) 内部関数化による実装

IC カードに実装するのは暗号化機能だけであり、その規模は小さく内部関数化が可能である。

一般的に、ライブラリ化による実装よりも内部関数化による実装の方が、処理速度の観点からは有利と考えられる。

(ii) サーバの高速化

a) Crypto++5.1 の採用

サーバ上での多倍長演算処理の速度は、実装する多倍長演算ライブラリの性能に依存する。OU 関数の実装では、高次剰余暗号と同じライブラリを使用することにした。

5-6-2-2 基本仕様

本研究で実装を行う機能の概要を記す。

(i) 暗号化処理

IC カード内に実装する機能。IC カード内の投票者の投票データを準同型公開鍵で暗号化処理を行う。IC カードという限られた CPU 性能、メモリ容量を考慮した実装が必要となる。

(ii) 公開鍵、秘密鍵の鍵生成処理

サーバ上で実装する機能。準同型公開鍵暗号の公開鍵、秘密鍵の生成を行う。鍵生成処理の際に素数、擬似乱数を使用する場合には 5-6-2-2 (v) 準同型公開鍵暗号アルゴリズムの条件を満たす必要がある

(iii) 集計処理

サーバ上で実装する機能。準同型公開鍵暗号文同士をべき乗演算する事で求められる。

(iv) 復号処理

サーバ上で実装する機能。準同型秘密鍵で復号処理を行う。サーバ実装ということで CPU 性能、メモリ容量は IC カードより条件が緩和される。計算結果を保持したテーブル実装が可能な場合は、メモリ容量を計算し高速実装をする。

(v) 準同型公開鍵暗号アルゴリズム

a) OU 関数

本年度実装する OU 関数のアルゴリズム概要を示す。

b) 鍵生成(1024bit の場合)

(1) p,q を 340 ビット奇素数として, ランダムに選び, $n=p^2q$ を公開する.

(2) 次の条件を満たす g をランダムに選ぶ.

(ア) g を Z/nZ からランダムに選ぶ,

(イ) $g_p=g^{p-1} \bmod p^2$ を計算する.

(ウ) g_p の$(\mathbf{Z}/p^2\mathbf{Z})^*$上での位数が p であるか, チェックする. 実際には, $g_p \neq 1$ の場合は, この条件を満たすはず.

(3) $L(g_p)=\dfrac{g_p-1}{p} \bmod p$ を計算し, 秘密に保持する(秘密鍵のひとつ).

(4) 公開鍵(k,n,g,h)を公開する. 秘密鍵は, $(p,q,k, L(g_p))$

c) 暗号化

(1) 平文 m を平文空間 $\{0,1\}^{k-1}$ から選ぶ.

(2) 乱数 $r,(0 \le r < n)$ をランダムに選択する.

(3) 暗号文 C を $C = g^m h^r \bmod n$ を計算することにより得る.

d) 復号処理

(1) $C_p = C^{p-1} \bmod p^2$ を計算する. 次に, $L(C_p)=\dfrac{C_p-1}{p}$ を計算する.

(2) $D(C)=\dfrac{L(C_p)}{L(g_p)} \bmod p$ を計算する. D(C)が平文空間 $\{0,1\}^{k-1}$ にあれば, 復号成功.

(vi) 集計の正当性検証アルゴリズム

センター1 は, $Z_1, Z_2, \cdots, Z_n$ を得ることができる. センター1 は, 各々を乗じた $Z=\prod_{i=1}^{n} Z_i \bmod n_A$ を公開掲示板上に公開することになるが, そこで, 集計の正当性証明(乗算の正当性証明)を与えなくてはならない.

コミットメント $C_1, C_2, \cdots, C_n$ は公開掲示板上に掲示されているので, 積算の途中経過(コミットメント)を掲示すればよい. 実際には, $C_1 \equiv g^{Z_1}, C_2 \equiv g^{Z_2}$ が与えられたとき, $C_{(1,2)} \equiv g^{Z_1 Z_2}$ を出力し, 計算が正しいことを証明する. これは, 次の離散対数が等しいことを証明するプロトコル $EQ_{DL}(x,y,g,h)$ を使って実現できる.

プロトコル 1　$\log_g x = \log_h y$ を示すプロトコル $EQ_{DL}(x,y,g,h)$

(g,h,x,h) が与えられたとき, 下記のプロトコルを 1 回行う.		
証明者	通信	検証者
$w \in_R Z_n, (a,b)=(g^w,h^w)$	$(a,b) \rightarrow$	
	$\leftarrow c$	$c \in_R Z_n$
$r \leftarrow w+\alpha c$	$r \rightarrow$	$g^r = ax^c, h^r = by^c$

なお, このプロトコルを非対話すると次のようになる.

① $a \equiv g^w \bmod p, b \equiv h^w \bmod p, c = H(x \| y \| a \| b), r = w + \alpha c$ を計算する.

② 証明は (c, r) となる.

③ $c = H(x \| y \| g^r / x^c \| h^r / y^c)$ の検証を行うことにより, 検証できる.

さて, 最終的には, $\log_g C_1 = \log_{C_2} C_{(1,2)}$ の証明(つまり, $\log_g g^{Z_1} = \log_{g^{Z_2}} g^{Z_1 Z_2}$ の証明のプロトコル)が必要である. このプロトコル $PM_{COM}(C_1, C_2, C_{(1,2)}, g)$ は $EQ_{DL}(C_1, C_{(1,2)}, g, C_2)$ により実現できる. n 投票者の集計結果 $g^Z \bmod p$ を得たら, Z を公開する.

なお, $PM_{COM}(C_1, C_2, C_{(1,2)}, g)$ を用いて, 離散対数部分の積を証明する $PM_{DL}(C_1, C_2, Z)$ を構築することができる. 実際、$PM_{DL}(C_1, C_2, Z) = \{PM_{COM}(C_1, C_2, C_{(1,2)}, g), C_{(1,2)}, Z\}$ が証明となる. 検証は、次の手順となる.

① $PM_{COM}(C_1, C_2, C_{(1,2)}, g)$ を検証する.

② $C \equiv g^Z$ を検証する.

(vii) 復号の正当性検証アルゴリズム

OU 関数の場合, 乱数 r が指数部にあるため, これを直接求めることは困難である. 従って, 暗号文 $E(m, r) \equiv g^m h^r \bmod n$ を $g^m (h_0^n)^r \equiv g^m (h_0^r)^n \bmod n \equiv g^m \tilde{r}^n \bmod n \equiv E(m, \tilde{r})$ と解釈し, $t = \tilde{r}^n \bmod n^2$ から, $\tilde{r}$ (n 乗根)を求めることで, 上記の証明を実現する.

$n = p^2 q$ であるので, 問題を次のように分割し, 中国人の剰余定理を用いて最終的に $\tilde{r}$ を求める.

$$t \equiv r_p^{\,n} \bmod p^2$$

$$t \equiv r_q^{\,n} \bmod q$$

後者の式は $(n, q-1) = 1$ より, r_q を容易に得ることができる.

前者の式は $(n, \phi(p^2)) = p$ であるため, 与えられた x に対して法 p^2 での p 乗根を解かなくてはならない. しかし, 与えられた x が既に p 冪の場合 $(x = w^p \bmod p^2)$ は,

$$x^p \equiv w^{p^2} \equiv w^p \equiv x \bmod p^2$$

となることから, x そのものが p 乗根の解の1つとなる. 従って次のように解くことができる.

① $t_1 \equiv t^{1/q} \bmod p^2$ を解く($(q, \phi(p^2)) = 1$ より容易).

② $t_2 \equiv t_1^{\,1/p} \bmod p^2$ を解く(上記の議論より容易).

③ $t_3 \equiv t_2^{\,1/p} \bmod p^2$ を解く(上記の議論より容易). これが, r_p となる.

最後に, r_p, r_q から, 中国人の剰余定理を用いて, r を求めればよい.

(viii) 実装上の注意事項

公開鍵暗号方式では素数、乱数の扱い方が安全性に大きく依存する。TYKK で使用する素数、擬似乱数の条件を記述する。

a) 素数の条件

TYKK では以下の３つの条件を全て満たす事で、素因数分解に強い素数と判断する。

⑴ 乱数(素数候補)p は、「p-1 が小さな素数(17863 以下の素数)で割り切れない」こと。

⑵ Miller-Rabin テストを(何回か)通ること。

⑶ RSA の素数の条件と同じ。参考文献[72]参照

b) 擬似乱数の条件

擬似乱数を発生させる場合、毎回同じ乱数を出力するような実装はしない。例えば、初期値(SEED)などを設定して乱数を出力する、乱数生成ライブラリを利用する場合は、初期値に「時刻」、「IP アドレス」、「プロセス番号」等のサーバ固有の情報を利用して SEED が決して同じにならないようにする。

(ix) 実装環境

本研究で使用する IC カード、サーバを想定した PC の仕様を記す。

a) IC カード

IC カードは 16bitCPU を内蔵したものを使用する。 (JICSAP2.0 対応)

b) リトルエンディアン

IC カードへの I/O のインターフェースはビッグエンディアンである。しかし、IC カード内部ではリトルエンディアンで処理される。

c) IC カード実装環境

OS : AP 実行環境 Ver2.20X
端末 PC : Windows2000 ServicePack4

(x) サーバ(PC)

a) ビッグエンディアン

サーバで扱うデータは全てビッグエンディアンである。

b) サーバ実装環境

OS : WindowsNT4.0 ServicePack6.0a
CPU : IntelPentiumⅢ 733MHz 以上
RAM : 128MB 以上

(xi) 高速化実装する関数

実装を行う際には事前に高速化手法の検討を行い、より効率的に最適化実装をおこなうものとする。

a) IC カード実装

(1) 暗号化関数

- OU 関数の実装
- IC カードに適した関数の実装(AP、LIB)
- 暗号コプロッセッサ
- E 社の提供している暗号ライブラリの使用

b) サーバ実装

(1) 公開鍵、秘密鍵の鍵生成関数

- OU 関数の公開鍵、秘密鍵の生成
- 公開鍵は IC カード格納用に適した鍵構造(リトルエンディアン)
- 秘密鍵はビッグエンディアン
- サーバに適した多倍長演算ライブラリの使用

(2) 集計関数

- OU 関数暗号文のべき乗演算
- サーバに適した多倍長演算ライブラリの使用

⑶ 復号関数

- OU 関数暗号文の復号処理
- サーバに適した多倍長演算ライブラリの使用

⑷ 集計の正当性検証機能関数群

- サーバに適した多倍長演算ライブラリの使用

⑸ 復号の正当性検証機能関数群

- サーバに適した多倍長演算ライブラリの使用

⑹ 電子署名検証関数

- サーバに適した多倍長演算ライブラリの使用

(xii) その他実装するプログラム

正しく処理が行えている事を確認するためのテストプログラムの実装及び、速度性能を計測するプログラムの実装を行う。

a) テスト用プログラム

⑴ 鍵生成テスト

- サーバ上で、OU 関数の公開鍵、秘密鍵が正しく生成されることをテストする

⑵ 暗号化テスト

- IC カード上で、OU 関数の暗号処理が正しく行われることをテストする。

⑶ 復号テスト

- サーバ上で、OU 関数の復号処理が正しく行われていることをテストする。

⑷ 集計テスト

- サーバ上で、OU 関数が正しく集計されていることをテストする。

b) 速度測定プログラム

⑴ 鍵生成の処理時間

- サーバで OU 関数の鍵生成の処理時間を測定する。

⑵ 復号の処理時間

- サーバで OU 関数の復号の処理時間を測定する。

⑶ 集計の処理時間

- サーバで OU 関数の集計の処理時間を測定する。

⑷ IC カード上の暗号の処理時間

- IC カード上の IC カード版性能測定用 AP に対して各種コマンドを発行し、IC カード上の OU 関数の処理時間を測定する。

⑸コミットメントデータ検証処理時間

- サーバでコミットメントデータの検証処理時間を測定する。

⑹Proof2 検証処理時間

- サーバで Proof2 検証時間の測定する。

⑺Proof3 検証用データ(C,R)生成時間

- サーバで Proof3 検証用データ生成時間の測定する。

⑻Proof3 正当性検証時間

- サーバで Proof3 検証時間の測定する。

⑼復号の検証用データ(ST)生成時間

- サーバで復号の検証データ生成時間の測定する。

⑽復号の正当性検証時間

- サーバで復号の検証時間の測定する。

⑾電子署名検証時間

- サーバで電子署名の検証処理時間を測定する。

（xiii）性能目標値

以下に性能目標値を記載する。

⑴ 暗号化処理

下記に暗号化処理の性能目標値、目標値設定条件、目標値設定の理由を示す。

目標値：全候補者（1000）回答データ要素　30s 以下
　　１候補　30(s)／1000＝0.03s 以下
条件　：最大候補者数を 1000 とする。
理由　：投票者が実施する処理である。準同型公開鍵暗号による暗号化処理の後に、正当性検証用データの生成処理が実施される。投票時間の増加は投票者に負担をかける事になると予想される。従って今回、投票に費やす時間を最大１分と想定し、準同型公開鍵暗号の暗号化処理時間をその半分の 30s 以下と設定した。

⑵ 復号処理

下記に復号処理の性能目標値、目標値設定条件、目標値設定の理由を示す。

目標値：全暗号ブロック　10 分以下
条件　：最大暗号ブロック数を 1000 とする。
理由　：復号時間は平文サイズによって決まる。したがって、平文サイズの大きさをファクターにして、処理時間を測定する。

⑶ 鍵生成

下記に鍵生成処理の性能目標値、目標値設定条件、目標値設定の理由を示す。

目標値：12 時間以下
条件　：なし

理由　：1回の投票に対して、センター2で選挙実施事前準備段階に、一度だけ実施される処理である。
通常、マシンが稼働していない時間帯に処理すれば良いと考え、12時間以下と設定した。

⑷ 集計処理

下記に集計処理の性能目標値、目標値設定条件、目標値設定の理由を示す。

目標値：全暗号ブロック　1時間以下
条件　：最大暗号ブロック数を1000000×1000とする。
理由　：投票締め切りから集計、開票までの時間を1時間程度とした場合、復号処理を10分以下と想定し、集計処理を1時間以下と設定した。

（xiv）準同型公開鍵暗号の詳細評価項目

a) OU関数

⑴ 暗号化関数（ICカード）

- 鍵サイズ1024bit、平文サイズ15、30、45、60、75、90、105、120、128、340bitの速度測定。

⑵ 復号関数　（サーバ）

- 鍵サイズ1024bit、平文=10、20、30、40、340bitの速度測定。

⑶ 鍵生成　　（サーバ）

- 1024bit鍵生成時間の測定

⑷ 集計関数　（サーバ）

- 鍵サイズ1024bit、暗号文の数量1万、10万、100万の速度測定。

5-6-3 OU 関数評価結果報告

5-6-3-1 評価方針

(i) 公開鍵サイズ

CRYPTREC Report2002[73]によると、合成数nの素因数分解問題に関しては、2002年時点で、n=pq及びn=p^2qについては、(pのbit数)=(qのbi数)かつ、(nのbit数)≧1024あれば、今後10年程度の使用に関しては安全であると報告されている。

従って、公開鍵サイズは1024bitとする。

5-6-3-2 評価項目

評価項目は以下の通りである。

- 鍵生成時間 :サーバ上での公開鍵と秘密鍵の生成処理時間。
- 暗号化時間 :ICカード上での平文の暗号化処理時間。
- 復号時間 :サーバ上での暗号文の復号処理時間。
- 集計時間 :サーバ上での暗号文の集計処理時間。

5-6-3-3 パラメータ

(i) 鍵生成処理

鍵生成処理はサーバ上に実装される。

鍵処理は、以下の条件毎に処理性能を測定する。

- 鍵サイズ:1024bit。

(ii) 暗号化処理

暗号化処理はICカード上に実装される。

暗号処理は、以下の条件毎に処理性能を測定する。

- 鍵サイズ:1024bit。
- 平文サイズ:15～128bit以下、及び当該鍵で扱える最大平文サイズ。

(iii) 復号処理

復号処理はサーバ上に実装される。

復号処理は、以下の条件毎に処理性能を測定する。

- 鍵サイズ:1024bit。
- 平文サイズ:10bit～40bit、及び当該鍵で扱える最大平文サイズ。

(iv) 集計のパラメータ

集計処理はサーバ上に実装される。

集計処理は、以下の条件毎に処理性能を測定する。

- 鍵サイズ:1024bit。
- 暗号文の数量:1万、10万、100万。

5-6-3-4　評価環境

評価を行う環境を以下に示す。使用するプログラミング言語は、IC カード版がC、サーバ版が C＋＋である。

(i) IC カード評価環境

IC カード	接触型 IC カード(JICSAP2.0 対応)
IC カード　OS	AP 実行環境 Ver2.20X
端末用 PC　OS	Windows2000　ServicePack4
端末用 PC　CPU	IntelPentiumⅢ
端末用 PC　ｸﾛｯｸ	667MHz
端末用 PC　ﾒﾓﾘ	64MB

(ii) サーバ評価環境

OS	WindowsNT4.0　ServicePack6.0a
CPU	IntelPentiumⅢ
ｸﾛｯｸ	733MHz
ﾒﾓﾘ	128MB

5-6-3-5　評価結果

(i) 鍵生成処理結果

以下に、鍵生成処理結果を示す。処理結果は 50 回の計測を行った平均値である。また、生成した鍵は、特定の平文を使用して、暗号化・復号に問題ないことを確認した。

表 38　鍵生成処理結果

1024bit 鍵生成時間
(ms)
633

(ii) 暗号化処理結果

以下に、暗号化処理結果を示す。

なお、測定では、IC カード上で暗号処理を行って端末 PC にレスポンスを返した時間と、暗号処理を行わずに端末 PC にレスポンスを返した時間を計測し、両者を差し引いたものを暗号処理時間とした。また、平文は乱数値である。

処理結果は 50 回の計測を行った平均値である。

表 39　1024bit 鍵の暗号処理結果

平文ｻｲｽﾞ (bit)	暗号化時間 (ms)
15	333
30	335
45	340
60	342
75	346
90	354
105	362
120	362
128	365
340	436

(iii) 復号処理結果

以下に、復号処理結果を示す。なお、平文は乱数値である。
処理結果は 50 回の計測を行った平均値である。

表 40　復号処理結果

	OU 関数
	1024bit
平文ｻｲｽﾞ (bit)	復号時間 (ms)
10	14
20	13
30	13
40	14
max	14
平均	13

注:
表 40 中の「max」は当該鍵サイズで扱える最大の平文サイズである。1024bit 鍵では 340bit である。

（iv）集計処理結果

以下に、集計処理結果を示す。なお、処理結果は 50 回の計測を行った平均値である。

表 41 集計処理結果

暗号ブロック数量	鍵ｻｲｽﾞ (bit)	集計結果 (ms)
10000	1024	1,121
100000	1024	11,126
1000000	1024	111,039

5-6-4　正当性検証機能評価結果報告

鍵長 1024bit を想定した検証処理時間結果を示す。また、各処理結果は 50 回の計測を行った平均値である。

5-6-4-1　集計の正当性検証機能

表 42 正当性検証機能測定結果

概要説明	時間(msec)
検証用パラメータ P,G 生成時間	11930
コミットメントデータ生成時間	143
コミットメントデータ検証時間	142
Proof2 検証時間	144
Proof3 検証用データ(c,r)生成時間	576
Proof3 検証時間	383

5-6-4-2　復号の正当性検証機能

表 43 復号正当性検証機能測定結果

概要説明	時間(msec)
復号検証用データ生成時間	1919
復号正当性検証時間	9

5-6-4-3　電子署名検証機能

表 44 電子署名検証機能測定結果

概要説明	時間(msec)
電子署名データ生成時間	145
電子署名データ検証時間	1

5-6-5 考察

5-6-5-1 OU 処理時間に関する考察

＜条件＞
・OU 公開鍵長は 1024bit とする。
・平文サイズは 340bit とする。

(i) 大規模選挙(投票者数 100 万人, 候補者数 1000 人)

a) 暗号化

投票者数 100 万人を想定した場合、1 候補者あたり 20bit の平文が必要となる。OU 関数の平文サイズは 340bit なので、1 暗号ブロックに最大 17 候補者をのせて暗号化処理が行える。1000 候補者全ての平文を暗号化するために必要な暗号ブロック数は 59 となる。(1000／17＝59 ブロック)

【OU 関数:暗号処理時間】
鍵長 1024bit、平文 340bit の暗号化処理時間は約 436ms。
436ms × 59 ブロック ＝ 約 26 秒

大規模選挙を想定した場合、十分問題ない処理時間といえる。

b) 復号処理

OU 関数の復号の特徴として、1 度に復号する bit 数が増加しても、1 回の復号処理時間の増加が殆ど見られない事である。従って、1 度に処理する bit 数を多くし復号回数を少なくする事が高速な実装になる。

【OU 関数:340bit の復号処理時間】
14ms × 59 ブロック ＝ 約 1 秒

大規模選挙を想定した場合、十分問題ない処理時間といえる。

c) 集計処理

【OU 関数:集計処理時間】
1024bit 鍵長の場合の、暗号ブロック数量 1,000,000(100 万)の集計処理時間は 111,039ms となる。平文を 340bit とした場合、1 暗号ブロックに 17 人の候補者が載せられるので以下のようになる。(1000／17＝59 ブロック)

111,039ms × 59 ブロック ＝ 約 1.8 時間

以上の結果から、集計処理時間の目標値 1 時間以内は満たせていない。しかし、サーバの性能向上や、サーバシステムを分散化することでさらに処理時間が短縮できると思われる。

(ii) 中規模選挙(投票者数 10 万人, 候補者数 100 人)

a) 暗号化

大規模選挙結果より、中規模に置いても問題ないと言える。

b) 復号処理

大規模選挙結果より、中規模に置いては問題ないと言える。

c) 集計処理

1024bit 鍵長の場合の、暗号ブロック数量 100,000(10 万)の集計処理時間は 11,126ms となる。平文を 340bit とした場合、1 暗号ブロックに 20 人の候補者が載せられるので以下のようになる。
(100／20＝5 ブロック)

11,126ms × 5 ブロック ＝ 約 55.6 秒

以上の結果から、集計処理時間の目標値 1 時間以内を十分に満たしている。

(iii) 小規模選挙(投票者数 1 万人, 候補者数 10 人)

a) 暗号化

中規模選挙結果より、小規模に置いても問題ないと言える。

b) 復号処理

中規模選挙結果より、小規模に置いても問題ないと言える。

c) 集計処理

中規模選挙結果より、小規模に置いても問題ないと言える。

5-6-5-2 正当性検証処理時間に関する考察

＜条件＞
・OU 公開鍵長は 1024bit とする。
・RSA 公開鍵長は 1024bit とする。
・平文サイズは 340bit とする。

(i) 大規模選挙(投票者数 100 万人, 候補者数 1000 人)

a) 検証用パラメータ P,G 生成時間

この処理は、投票準備段階で 1 回だけ行われる。
この検証用パラメータは個準同型公開鍵サイズに依存して生成される。公開鍵サイズが大きくなるほど処理時間が増加する傾向にある。

【検証用パラメータ生成時間】
11930ms ＝ 約 11.9 秒

大規模選挙を想定した場合、十分問題ない処理時間といえる。

b) コミットメントデータ検証時間

IC カード内で生成したコミットメントデータの検証を行う。また、コミットメントデータは準同型暗号文と同じ数になる。投票者数 100 万人を想定した場合、1 候補者あたり 20bit の平文が必要となる。OU 関数の平文サイズは 340bit なので、1 暗号ブロックに最大 17 候補者をのせて暗号化処理が行える。1000 候補者全ての平文を暗号化するために必要な暗号ブロック数は 59 となる。(1000／17＝59 ブロック)

【コミットメントデータ検証時間】
143ms × 59 ブロック × 100 万人 ＝ 約 97.6 日

現在の PC の主流になりつつある CPU（インテル Pentium4 3.0GHz HT 対応）では、約 1/6 の処理時間で済み、用途に合わせて複数台での分散処理が有効である。また、最近のサーバマシンでは、64bit 化や複数 CPU でのマルチスレッド処理が可能であり、高性能機器であれば数時間での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

c) Proof2 検証時間

開票する直前に行う検証処理。集計値と集計値のコミットメントデータの検証を行う。

【コミットメントデータ検証時間】
142ms × 59 ブロック ＝ 約 8.4 秒

d) Proof3 検証時間

センター1(証明者)が検証用データを作成した後に、センター2(検証者)が実際検証を行うので、処理時間(日数)はセンター1＋センター2 となる。

センター1(証明者)

集計の正当性検証用データ(C,R)を生成する。

【検証データ(C,R)生成時間】
576ms × 59 ブロック × 100 万人 ＝ 約 393.3 日

現在の PC の主流になりつつある CPU（インテル Pentium4 3.0GHz HT 対応）では、約 1/6 の処理時間で済み、用途に合わせて複数台での分散処理が有効である。また、最近のサーバマシンでは、64bit 化や複数 CPU でのマルチスレッド処理が可能であり、高性能機器であれば数時間での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

センター2(検証者)

センター1 の生成した(C,R)を検証する。

【Proof3 検証時間】
383ms × 59 ブロック × 100 万人 ＝ 約 261.5 日

現在の PC の主流になりつつある CPU（インテル Pentium4 3.0GHz HT 対応）では、約 1/6 の処理時間で済み、用途に合わせて複数台での分散処理が有効である。また、最近のサーバマシンでは、64bit 化や複数 CPU でのマルチスレッド処理が可能であり、高性能機器であれば数時間での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

e) 復号の正当性検証時間

センター2(証明者)が検証用データを作成した後に、センター1(検証者)が実際検証を行うので、処理時間はセンター1＋センター2 となる。

① センター2(証明者)
復号の検証データ(ST)を生成する。

【検証データ(ST)生成時間】
1919ms × 59 ブロック ＝ 約 113.2 秒

② センター1(検証者)
センター2 の生成した検証データ(ST)を検証する。

【復号検証時間】
9ms × 59 ブロック ＝ 約 0.5 秒

f) 電子署名検証時間

IC カードでは、投票時に作成した準同型暗号文とコミットメントデータのペアに対して、電子署名データを生成する。従って、電子署名データは準同型暗号ブロック数となる。

【電子署名検証時間】
1ms × 59 ブロック × 100 万人 ＝ 約 16.3 分

(ii) 中規模選挙(投票者数 10 万人, 候補者数 100 人)

a) 検証用パラメータ P,G 生成時間

大規模選挙結果より、中規模に置いても問題ないと言える。

b) コミットメントデータ検証時間

IC カード内で生成したコミットメントデータの検証を行う。また、コミットメントデータは準同型暗号文と同じ数になる。投票者数 10 万人を想定した場合、1 候補者あたり 17bit の平文が必要となる。OU 関数の平文サイズは 340bit なので、1 暗号ブロックに最大 20 候補者をのせて暗号化処理が行える。100 候補者全ての平文を暗号化するために必要な暗号ブロック数は 5 となる。(100／20＝5 ブロック)

【コミットメントデータ検証時間】
143ms × 5 ブロック × 10 万人 ＝ 約 19.8 時間

現在の PC の主流になりつつある CPU(インテル Pentium4 3.0GHz HT 対応)では、約 1/6 の処理時間で済み、用途に合わせて複数台での分散処理が有効である。また、最近のサーバマシンでは、64bit 化や複数 CPU でのマルチスレッド処理が可能であり、高性能機器であれば数十分での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

c) Proof2 検証時間

開票する直前に行う検証処理。集計値と集計値のコミットメントデータの検証を行う。

【コミットメントデータ検証時間】
142ms × 5ブロック ＝ 約0.7秒

d) Proof3 検証時間

センター1(証明者)が検証用データを作成した後に、センター2(検証者)が実際検証を行うので、処理時間(日数)はセンター1＋センター2となる。

① センター1(証明者)
集計の正当性検証用データ(C,R)を生成する。

【検証データ(C,R)生成時間】
576ms × 5ブロック × 10万人 ＝ 約3.3日

現在のPCの主流になりつつあるCPU(インテル Pentium4 3.0GHz HT対応)では、約1/6の処理時間で済む。また、最近のサーバマシンでは、64bit化や複数CPUでのマルチスレッド処理が可能であり、高性能機器であれば数十分での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

② センター2(検証者)
センター1の生成した(C,R)を検証する。

【Proof3 検証時間】
383ms × 5ブロック × 10万人 ＝ 約2.2日

現在のPCの主流になりつつあるCPU(インテル Pentium4 3.0GHz HT対応)では、約1/6の処理時間で済み、用途に合わせて複数台での分散処理が有効である。また、最近のサーバマシンでは、64bit化や複数CPUでのマルチスレッド処理が可能であり、高性能機器であれば数十分での処理時が可能であると予想される。このため、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

e) 復号の正当性検証時間

大規模選挙結果より、中規模に置いても問題ないと言える。

f) 電子署名検証時間

大規模選挙結果より、中規模に置いても問題ないと言える。

(iii) 小規模選挙(投票者数1万人, 候補者数10人)

a) 検証用パラメータ P,G 生成時間

中規模選挙結果より、小規模に置いても問題ないと言える。

b) コミットメントデータ検証時間

ICカード内で生成したコミットメントデータの検証を行う。また、コミットメントデータは準同型暗号文と同じ数になる。投票者数1万人を想定した場合、1候補者あたり14bitの平文が必要となる。OU関数の平文サイズは340bitなので、1暗号ブロックに最大24候補者をのせて暗号化処理が行える。10候補者全ての平文を暗号化するために必要な暗号ブロック数は1となる。

【コミットメントデータ検証時間】
143ms × 1ブロック × 1万人 ＝ 約23.8分

c) Proof2 検証時間

開票する直前に行う検証処理。集計値と集計値のコミットメントデータの検証を行う。

【コミットメントデータ検証時間】
142ms × 1ブロック ＝ 142ms

d) Proof3 検証時間

センター1(証明者)が検証用データを作成した後に、センター2(検証者)が実際検証を行うので、処理時間はセンター1＋センター2となる。

① センター1(証明者)
集計の正当性検証用データ(C,R)を生成する。

【検証データ(C,R)生成時間】
576ms × 1ブロック × 1万人 ＝ 約1.6時間

② センター2(検証者)
センター1の生成した(C,R)を検証する。

【Proof3 検証時間】
383ms × 1ブロック × 1万人 ＝ 約1時間

e) 復号の正当性検証時間

中規模選挙結果より、小規模に置いても問題ないと言える。

f) 電子署名検証時間

中規模選挙結果より、小規模に置いても問題ないと言える。

5-6-5-3 処理性能に関する考察

正当性の証明処理性能で問題となるのは、平成14年度成果報告書「5-7 投票プロセスの正当性証明とその効率化」において研究された「集計の正当性証明」であるが、この処理はセンター側のサーバで実施されるため、「5-6-5-2 正当性検証処理時間に関する考察」の各項目で記載しているとおり、サーバの性能向上やマルチCPUによるマルチスレッド処理、HPC(高性能コンピューティング) テクノロジによるクラスタ・コンピューティングなどにより、リアルタイムでの検証や第三者が開票後に検証する場合でも問題ない程度となる。

5-6-5-4 データ量に関する考察

＜条件＞

- OU公開鍵サイズは1024bitとする。
- RSA公開鍵サイズは1024bitとする。
- 平文サイズは340bitとする。
- 投票者数は100万人とする。
- 候補者数は1000人とする。

(i) 投票者 PC のデータ量

投票者数 100 万人を想定すると使用する平文は 1 候補者あたり 20bit 必要となる。OU 関数の平文サイズは 340bit なので 1 暗号ブロックに 17 候補者を載せる事ができる。したがって、1000 候補者を全て暗号化するためには、準同型暗号分は 59 ブロックになる。

同様に、コミットメントデータ、電子署名データも 59 ブロックになり、投票データ量は以下のようになる。

表 45　投票者 PC のデータ量

	投票データ量	暗号ブロック数
準同型暗号文	7.6Kbyte	59
コミットメントデータ	7.7Kbyte	59
電子署名データ	7.6Kbyte	59

投票者 PC ではこのデータをインターネット経由でセンター1 へ送信をする。従って投票データ量は少ない事が好ましい。

(ii) センター1 のデータ量

センター1 には投票者人数分のデータが集まる事になる。(i)の結果から、センター1 のデータ量は以下のようになる。

また、Proof3 検証用データ(C,R)とは、センター1 が集計処理の不正をしていない事を示すデータであり、センター1 が作成するデータである。

表 46　センター1 データ量

	データ量
準同型暗号文	7.6Gbyte
コミットメントデータ	7.7Gbyte
電子署名データ	7.6Gbyte
Proof3 検証用データ(C,R)	10Gbyte

(iii) センター2のデータ量

センター2 で集計されたデータ量は投票者 PC で生成した、準同型暗号文と同じになる。従って、OU 関数の場合は 7.6Kbyte となる。

また、復号の検証用データ(ST)とは、センター2 が復号処理の不正をしていない事を示すデータであり、センター2 が作成するデータである。

表 47　センター2 データ量

	データ量
準同型暗号文	7.6Kbyte
復号の検証用データ(ST)	513.3Kbyte

5-6-6　システム構成のまとめ

5-6-6-1　まとめ

(i) OU 関数処理性能に関して

暗号化処理

投票者 100 万人程度、候補者 1000 人程度の選挙であっても問題ないと判断する。

復号処理

投票者 100 万人程度、候補者 1000 人程度の選挙であっても問題ないと判断する。

集計処理

投票者 100 万人程度、候補者 1000 人程度の選挙の場合、目標値を達成できない結果となったが、より高性能なサーバ、複数の PC を使用して分散集計を行うことで大幅に処理時間を削減できるため、問題ないと判断する。

(ii) 正当性検証処理に関して

①集計の正当性検証処理

投票者 100 万人程度、候補者 1000 人程度の選挙の場合、センター1 の処理時間は非常に大きくなることが判明した。しかし、将来的により高性能なサーバ、複数の PC を使用して分散処理を行うことで大幅に処理時間を削減できると判断する。

②復号の正当性検証処理

投票者 100 万人程度、候補者 1000 人程度の選挙であっても問題ないと判断する。

③電子署名の検証処理

投票者 100 万人程度、候補者 1000 人程度の選挙であっても問題ないと判断する。

5-7　実験

5-7-1　実験の方針

5-7-1-1　背景、目的

各サブテーマの研究開発成果により、以下の特徴，メリットを持ち合わせたシステム構築が進んでいる。その中で、「目に見える・わかりやすいセキュリティ」を実現するために、IC カード内での暗号化を含む票作成に取り組み、市販のICカードを用いた試作に成功している。これにより、ICカードの耐タンパー性を利用することで、投票者端末にとって最大の負担となる投票内容の正当性証明コスト(処理時間)を大幅に削減することが可能となった。

●特徴
- ・投票・アンケートの対象となるユーザの本人認証が可能
- ・本人のプライバシーを秘匿した上での投票の有資格者であることを認証
- ・投票の有効性についての証明等安全性、健全性が保証されるシステム
- ・広域での大規模投票・アンケートにも対応できるシステム構成

●メリット(インターネット電子匿名投票・アンケート方式)
- ・匿名性
  →本音の回答がし易い
- ・実施場所、期間設定の自由度
  →回収率の増加が見込まれる
- ・実施有無の秘匿
  →地域におけるプラバシー保護(隣近所への配慮)が可能

本サブテーマでは、次世代電子投票・アンケートシステムの社会的利用の研究を目的にして地方自治体での実験を予定しており、この準備のため参加企業による模擬実験を実施し、自治体での実験準備を進めている。

5-7-1-2　研究内容

H15 年度の研究内容の概要に関して以下に示す。

① H15 年度の目標

参加企業による実験を行い、性能、運用性の確認を行う。また、中央コリドー高速通信実験協議会の協力による電子投票実験を準備する。

② H15年度の実施内容

参加企業による小規模の実験を実施し、投票者操作性，システム運用性の確認を行った。また、中央コリドー高速通信実験協議会の協力の下、実験に関する説明書を作成し、松本市，山梨市の 2 自治体に実験の説明を実施し、参加の意志を得るとともに、自治体からのヒアリングにより、実験企画の検討を進めた。

③ H15年度の効果

参加企業による小規模の実験の中で、ヘルプディスク，投票者意識調査を実施し、インストール作業，操作性に対する改善項目が明確になった。

実際に電子投票システムを利用したユーザ意見として「インターネットを利用した投票は便利である」,「次世代の社会基盤として有効」の割合が多いことが確認された。

④ 取り組み状況

参加企業実験で要望のあった投票者インストールマニュアル，操作マニュアル等の改善を実施中である。

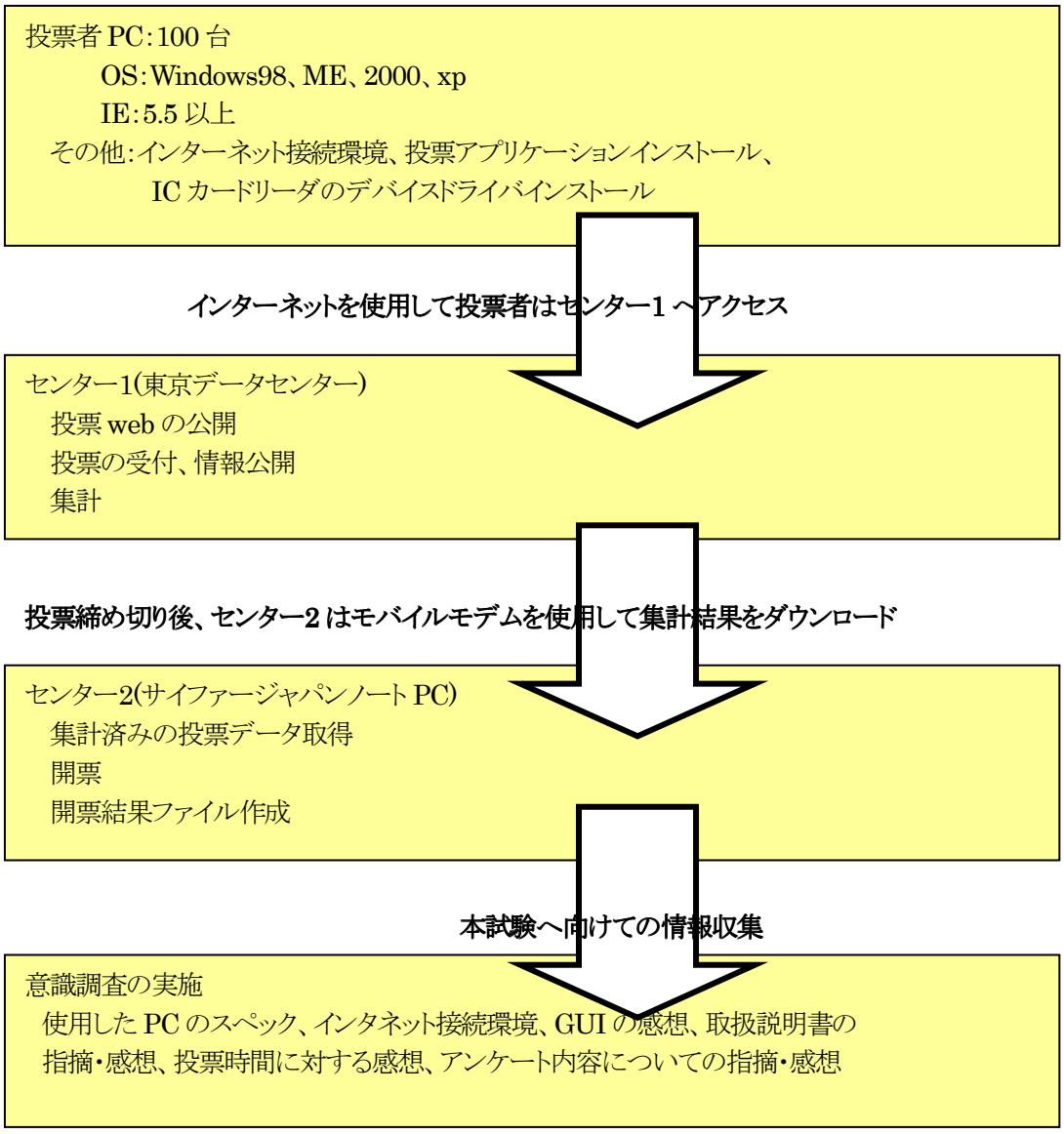
また、自治体実験に向けた準備を継続する。

5-7-2 参加企業による模擬実験

参加企業による小規模の実験を実施し、投票者操作性，システム運用性の確認を行った。

5-7-2-1 実験計画

(i) 全体の流れ



(ii) 作業項目

作業項目は以下の通りである。

a) 事前準備

(1)　投票者 PC セットアップ

- インターネット接続環境を構築する。
- Java SDK1.3.1_09 のインストールする。(VM を使用できる環境)
- IC カードリーダ/ライタドライバのセットアップする。

(2)　センター2 セットアップ

- モバイルモデムの設定を行う。
- アンケート定義する。
- アンケートの内容を登録する。

(3)　センター1 セットアップ

- アンケート内容を登録する。
- アンケート内容を公開する。
- 投票 web 画面を作成し、公開する。

(4)　公開鍵、検証パラメータ、投票回答テーブル作成

- アンケート定義をもとに公開鍵を作成する。
- 公開鍵をもとに検証パラメータを作成する。
- アンケート定義をもとに投票回答テーブルを作成する。

(5)　IC カード発行

- 投票アプリケーションを登録する。
- PKI アプリケーションを登録する。
- 公開鍵、検証パラメータを登録する。

b) アンケート投票作業

(1) 投票者 PC とセンター1 の通信

- 投票者 PC に IC カードを接続しセンター1 へアクセスし投票を行う。

c) アンケート集計、検証データ作成作業

(1)　アンケートの集計

- 投票されたアンケートの集計開始を指示する。
- 集計の検証データを作成し、公開ボードへ反映する

d) アンケート集計検証作業

(1)　集計処理の検証

- 投票終了後にセンター1 より検証データを受け取り検証を行う。

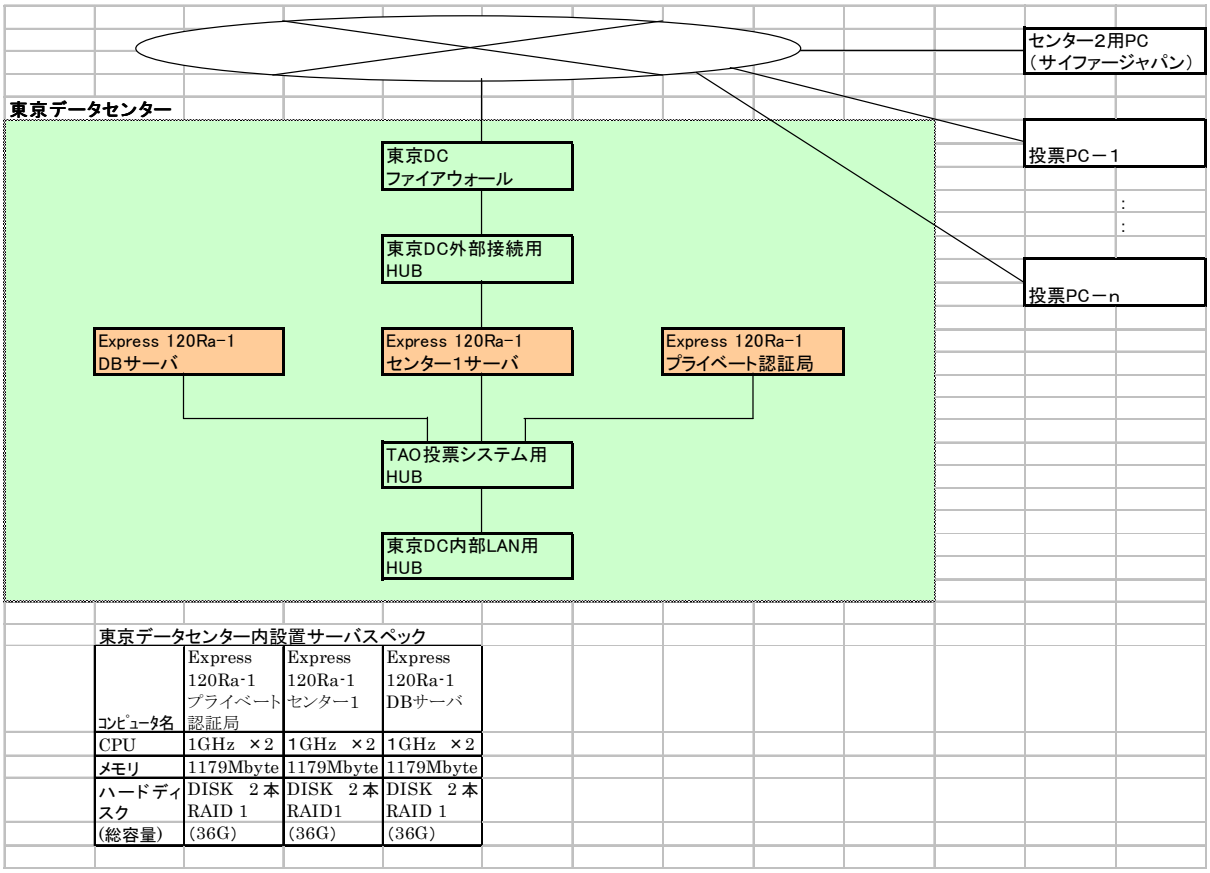
e) アンケート開票作業

(1)　アンケートの開票

- アンケートの復号を行い結果を公開する。

(iii) ネットワーク構成

本実験で使用するネットワーク構成は、下記の通りである。



東京データセンター内設置サーバスペック

コンピュータ名	Express 120Ra-1 プライベート認証局	Express 120Ra-1 センター1	Express 120Ra-1 DBサーバ
CPU	1GHz ×2	1GHz ×2	1GHz ×2
メモリ	1179Mbyte	1179Mbyte	1179Mbyte
ハードディスク (総容量)	DISK 2本 RAID 1 (36G)	DISK 2本 RAID1 (36G)	DISK 2本 RAID 1 (36G)

図 62 ネットワーク構成図

(iv) センター1 サーバ構成

本実験で使用する集計サーバ(Web サーバ)、データベースサーバ、認証局サーバのハードウェア構成は下記の通りである。

- コンピュータ　Express5800/120Ra-1
- OS　Windows2000Server SP4
- CPU　PentiumⅢ 1GHz × 2
- メモリ　1179Mbyte

[集計サーバのアプリケーション]

- IIS5.0
- Apache Tomcat 4.1

[データベースサーバのアプリケーション]

- Oracle9i

[認証局サーバのアプリケーション]
（1） CertWorker 1.0

（v）センター2 サーバ構成
本実験で使用する開票サーバのハードウェア構成は以下の通りである。

- ■ コンピュータ 汎用ノート PC
- ■ モバイルモデム AirH”
- ■ OS WindowsXP SP1
- ■ CPU PentiumⅢ 933MHz
- ■ メモリ 256Mbyte

（vi）想定する環境
a) 投票者 PC 環境

≪パソコン本体の環境≫
- メーカー製
- 自作パソコン
- デスクトップ型パソコン
- ノート型パソコン

≪パソコン内部の環境≫
- オペレーティングシステム(以後、OS と称す)の種類、バージョン
- ブラウザ環境
- パーソナルファイアーウォールの有り／無し
- 常駐型ウィルス監視ソフトの有り／無し(有りの場合はそのソフトを名を調査)
- Java ランタイムライブラリ 1.3.1_09 以外のインストール有り／無し(有りの場合は Ver 情報)

※ TAO 投票用アプリケーションの必須環境は Windows98 以降、IE5.5 以降

（vii）投票者 PC のネットワーク環境
- ファイアーウォールの有り／無し
- Proxy の有り／無し
- 通信路(光、ADSL、ISDN、アナログ、ケーブル、無線、携帯端末、専用線)
- LAN、モデム、ルーター、TA の使用の有り／無し

※ 投票者の認識している範囲の情報で良い。

（viii）実施手順
手順１ 事前準備作業
- ■ アンケート定義ファイル作成
- ■ センター2 へアンケー定義ファイルを設定
- ■ IC カードアプリケーションの設定、IC カードの発行
- ■ 投票用 web 画面作成
- ■ 各種プログラムのインストール、設定等

■ アンケート定義に適した投票回答テーブル作成
■ 公開鍵、検証データ作成パラメータの生成
■ IC カードへ投票回答テーブル、公開鍵、検証データ生成パラメータの書き込み(IC カードの発行)
■ IC カード、IC カードリーダライタの配布

手順2 アンケート公開作業
■ センター1 へアンケート定義ファイルを設定
■ アンケートをセンター1 の Web サーバに公開
■ 公開ボードのアクセスを許可

手順3 アンケート集計作業
■ アンケート集計
■ 集計の検証データ生成

手順4 アンケートの開票作業
■ 投票締め切り要求をセンター1 へ通知(CJ から NES へ電話で通知)
■ 集計済みデータをセンター1 からダウンロード
■ 集計の検証
■ 集計結果を開票、結果ファイルの作成
■ 結果ファイルをセンター1 がダウンロードを行い、web へ公開する

手順5 模擬実験に対する意識調査の実施
■ 意識調査内容の決定、作成、配布する
■ 意識調査の集計、結果を配布する

手順6 データ解析・報告書の作成
■ 実際の測定値からデータを解析し、報告書を作成する

(ix) 準備機材

・モバイルモデム(AirH")	1 枚
・IC カード	100 枚
・CD-ROM	100 枚
・CD ラベル	100 枚

5-7-2-2　アンケート内容

今回の模擬実験アンケート内容は、自治体で実施される可能性のある環境をテーマにアンケート内容を作成する。

「平成１５年　環境にやさしいライフスタイル実態調査　環境省」から抜粋

1.あなたが関心のある（興味がある，心配している）環境問題は何ですか。あてはまるもののを選んでください。いくつ選んでも構いません。

①大気汚染（空気が汚くなること）
②水質汚濁（海や川などの水が汚染されること）
③騒音（周りの音がうるさいこと）
④森林減少（森や林が少なくなること）
⑤有害化学物質（危険な化学物質があること）
⑥廃棄物（ゴミが近所に捨ててあること）
⑦生物多様性が失われること（野生の動物や昆虫等の生き物の種類が減少すること）
⑧地球温暖化（地球の気温が上がること）
⑨砂漠化（土地に草や木が生えなくなること）
⑩酸性雨（酸性の有害な雨が降ってくること）
⑪その他（①～⑩以外に関心があれば選んでください）

2.みなさんにお聞きします。あなたは、今後、つぎのようなことを行おうと思いますか。
あてはまるものをすべて選んでください。

①使わないときは、テレビや部屋などのあかりを消す
②使わないときは、水道の蛇口をきちんと閉める
③家で花や木を育てる
④ごみを、燃えるごみ，燃えないごみ，資源ごみ（空き缶，ペットボトル，古新聞など）に、きちんと分別する
⑤地域の人たちが、地域の掃除や、木や花を植えるときには参加する
⑥ものは長く使えるように大切に使う
⑦家族や友達などと環境について話し合う
⑧鉛筆やノートは、環境に良いものを買う
⑨買い物のとき、レジ袋をもらわないように気をつける

3.環境を守るためにはいろいろな立場の人が協力しなくてはなりませんが、では、次のうち、誰が一番重要な役割を持っていると思いますか。どれか一つを選んでください。

①わたしたち自身
②大人たち
③学校
④企業
⑤地方自治体
⑥日本の政府
⑦わからない

⑧その他

4.あなたは、環境問題に関することを何から知りましたか。あてはまるものをすべて選んでください。

①テレビ・ラジオから
②新聞や学習雑誌から
③マンガから
④本から
⑤学校の授業や先生から
⑥学校の遠足や見学から
⑦臨海学校・林間学校や自然教室で
⑧部活や課外活動で
⑨友達から
⑩家族・親戚から
⑪塾で
⑫講演会や展示会で
⑬家族旅行などで
⑭インターネットで
⑮地域の団体で
⑯動物園・水族館や博物館で
⑰市役所・区役所などで作った本で
⑱児童館・コミュニティで
⑲その他

5.あなたの学校では、次のような勉強をしたり、行事に参加したことはありますか。あてはまるものをすべて選んでください。

①環境問題について、先生の話を聞いた
②みんなで環境問題に関して話し合った
③地域の掃除やごみ拾いなどに参加した
④山や川などで自然の観察をした
⑤ごみ処理場や下水処理場などの施設を見学した
⑥川や湖の水、空気や雨の状態について見学した
⑦夏休みなどの自由研究で環境のことを調べた
⑧牛乳パックやケナフなどで紙づくりをした
⑨植物の栽培や動物の飼育・観察をした
⑩特にない
⑪その他

■アンケート制約条件

上記 1～5 のアンケート回答の制約条件は以下の通りとする。

アンケート 1.　必須回答・複数選択可
アンケート 2.　必須回答・複数選択可
アンケート 3.　必須回答・八者択一　(オンリーワン)
アンケート 4.　必須回答・複数選択可
アンケート 5.　必須回答・複数選択可

5-7-2-3　アンケート結果

参加企業実験アンケート集計結果
「環境にやさしいライフスタイル実態調査」

■期間:2004年02月16日9時00分～02月20日17時30分

投票有効数:　66票　/　100票

結果は「詳細・補足編」を参照されたい。

5-7-2-4　意識調査アンケート内容

(i) インストール・操作性に関する調査

投票者によるアプリケーションのインストールおよび投票の操作性に関して意見を収集し、自治体実験ならびに製品化の改善点を調査する。

●投票者 PC 環境に関する調査

設問1－1:電子投票でご使用になられるパソコンはどこのメーカーでしょうか？
差支えが無いようでしたらお書き下さい。
また、自分でパソコンを組み立ている方は自作とお書き下さい。
例)DELL、IBM、HP、SOTEC、COMPAC、松下、日立、ソニー、シャープ、
エプソン、富士通、NEC、自作等

設問1－2:電子投票でご使用になられるパソコンの OS をお書き下さい。
例)Win98、WinME、Win2000、WinXP 等

設問1－3:電子投票でご使用になられるパソコンの CPU とその性能をお書きください。
例) PentiumⅢ 1GHz

設問1－4:電子投票でご使用になられるブラウザのバージョンをお書き下さい。
例)IE5.5、IE6.0、IE6.0SP1

設問1－5:インターネットに接続する環境をお書き下さい。
例)ADSL、ケーブル、光、会社の LAN、学校の LAN、ISDN、ダイアルアップモデ　ム、モバイルモデム、無線 LAN 等

設問1－6:USB のポート数をお書き下さい。
例)1,2,3,4

設問1－7:日本語変換辞書は通常何をお使いでしょうか？
例)ATOK**, IME**

●投票者 PC インストール作業に関する調査

設問2－1. インストール作業は正常に完了出来たと思いますか？
例)出来たと思う, できていないと思う。

設問2－2. 証明書管理ツール(N3NVSS.exe)のインストール時にエラーが発生しましたか？
例)はい, いいえ, わからない, 覚えていない

設問2－3. 2－2で”はい”とお答えしたかたは、どのようなエラーかお書き下さい。

設問2－4. Java ランタイムライブラリ(j2re-1_3_1_09-windows-i586-i.exe)のインストール時にエラーが発生しましたか？
例)はい, いいえ, わからない, 覚えていない

設問2－5. 2－4で”はい”とお答えしたかたは、どのようなエラーかお書き下さい。

設問2－6. IC カードリーダライタ・ドライバーのインストール時にエラーが発生しましたか？
例）はい，いいえ，わからない，覚えていない

設問2－7. 2－6で”はい”とお答えしたかたは、どのようなエラーかお書き下さい。

設問2－8. その他、インストール作業に関するご意見が御座いましたらお書き下さい。

●インストールマニュアルに関する調査

設問3－1.「投票者 PC インストール手順書」に記載されているインストール手順は判りやすかったでしょうか？
例）はい，いいえ

設問3－2. 3－1で”いいえ”とお答えしたかたはどのようなところがわかりにくかったでしょうか？率直な感想をお書きください。
例）見出し，専門用語，ことばの言い回し，重要な記載がない

設問3－3. インストールマニュアルの全般の取扱についてお答えください。
以下(A1～A4)の選択肢より、一つ選んでください。

A1. マニュアルに一通り目を通した。
A2. 基本的にはマニュアルをみないでインストールを行い、問題が発生した時に活用した。
A3. マニュアルを全く見ていない。
A4. その他

設問3－4. その他、インストールマニュアルに関するご意見が御座いましたらお書き下さい。

●投票画面に関する調査

設問4－1. 電子投票の画面全般について率直な感想をお答えください。
例） 色が単調，配色が見づらい，このままでも良い

設問4－2. 今回の電子投票の画面で、改善する必要があると思う箇所を具体的にご指摘ください。、
例）アンケートの文字を大きくして欲しい。
IC カード処理時間の待ち時間を表示して欲しい。
背景の灰色に赤色文字は読みづらいので変更して欲しい。

設問4－3. 電子投票結果のグラフについて率直な感想をお答えください。
例）見やすい，見にくい，レイアウトが悪い，円グラフはやめた方が良い。

●投票実施に関する調査

設問5－1. 実際に最後まで投票が行えましたでしょうか？
投票が最後まで行えなかった方は、どのようなことが理由だったのでしょうか？
例）投票する時間がなかった
インストールが面倒で、拒絶してしまった。
インストールしたが、動作しなくてあきらめた

●ヘルプデスク対応に対する調査

設問6－1. ヘルプデスクをご利用した方にお聞きします。
ヘルプデスクスタッフの対応はどのような感じだったでしょうか？
例）満足している
満足していない(理由：レスポンスが遅い，説明が足りない)

●その他、改善要求

設問7－1. 今後の電子投票を進めていく上で、ここは是非とも改善すべきという点がございましたら、具体的にご記入をお願い致します。

（ii） 次世代電子投票・アンケートシステムを利用した感想

次世代電子投票・アンケートシステムとはどのようなものか、体験していただいた参加企業のメンバーの意識を調査する。また、今後の課題とする。

●第三世代を実際に使用した感想、有用性、安全性、利便性等に関する意識調査
（地方自治体殿対応プレ意識調査）

設問8－1. インターネットを利用した電子投票の安全性に疑問を持たれましたか？
例）はい、いいえ、わからない

設問8－2. 8－1のお答えの理由を分かる範囲で結構ですので、具体的に内容をお書き下さい。

設問8－3. インターネットを利用した電子投票は便利であると思われましたか？
例）はい、いいえ、わからない

設問8－4. 8－3のお答えの理由を分かる範囲で結構ですので、具体的に内容をお書き下さい。

設問8－5. インターネットを利用した電子投票は今後の社会基盤として有効と思われますか？
例）はい、いいえ、わからない

設問8－6. 8－5のお答えの理由を分かる範囲で結構ですので、具体的に内容をお書き下さい。

設問8－7. この他、インターネットを利用した電子投票に関して、ご意見等がありましたらご記入をお願い致します。

5-7-2-5　意識調査結果

調査結果は「詳細・補足編」を参照されたい。。

5-7-2-6　模擬実験の結果を反映させたシステムの改善提案

模擬実験のヘルプディスク実施，意識調査結果より、以下の点の改善が必要と考える。自治体実験までに対策を実施する予定である。

(i) インストール関する改善

採用した IC カードが IC カードリーダ・ライタのドライバに関するインストールに起因するインストールエラーやミスが多かったため、メーカに対して改善要求を実施する。

また、Java プラグインのバージョンに起因するインストールエラーが多かったため、最新版を適用することとする。

(ii) 操作性に関する改善

画面の色彩やデザインを改善する。

(iii) マニュアルに関する改善

インストールマニュアル・操作マニュアルが判りづらいとの意見が多かったため、以下の説明を追加したマニュアルを作成する。

・インストールフローの追加
・投票フローの追加
・１枚にまとめたクイックマニュアルの追加
・電子投票の安全性・暗号化のシステムの説明追加
・サーバ内部で発生したエラー画面の追加。

5-7-3　自治体実験

中央コリドー高速通信実験協議会の協力の下、実験に関する説明書を作成し、松本市，山梨市，大町市の 3 自治体に実験の説明を実施し、参加の意向を打診すると共に、自治体からのヒアリングにより、実験企画の検討を進めた。

5-7-3-1　自治体でのヒアリングによる可能性

以下に自治体における利用の可能性について、ヒアリング内容から得た内容も含め記載する。

(i) 公共組織における情報化の流れ

【行政情報化の世代の推移】

第一世代:内部事務の機械化
第二世代:行政サービスの電子化（現状）
第三世代:民意主導の政策形成支援（本システムの利用ターゲット）

公共組織の情報化の流れはいまや政策形成支援へのシステムに進化しつつある。第三世代の行政情報化では以下のシステムが望まれている。

【第三世代行政情報化】

行政情報化の目的:マーケティングの支援、行政サービス効果の測定

情報システムの目的:住民対話ルートの電子化による地域協働態勢の実現
施策/事業の評価処理の電子化による意思決定支援
主なシステム:行政評価システム、住民アンケートシステム(電子会議室)

(ii) 自治体における利用の可能性

第三世代の地方自治体情報化に有用な基本システムとして、本システムによる電子投票・アンケートが利用される可能性は非常に大きいと判断される。

【例】

●政策アセスメントシステムとしての利用(山梨県山梨市)

a. システム概要

・市における実際の政策への評価・民意収集を目的とする電子投票・アンケートシステムを構築する。
・今回は対象を市立の中学校とし中学生向けの政策説明に対し意思確認の電子投票、政策評価のアンケートを実施する。
中学生の政策への関心向上も期待する。
・ネットワーク母体は学校イントラネットを使用する。

b. システム活用への期待

・投票者、アンケート母体を特定でき得るシステムの構築。
・様々な投票・アンケート形態が実現できる(自宅、公共の端末からのアクセスも可能)。

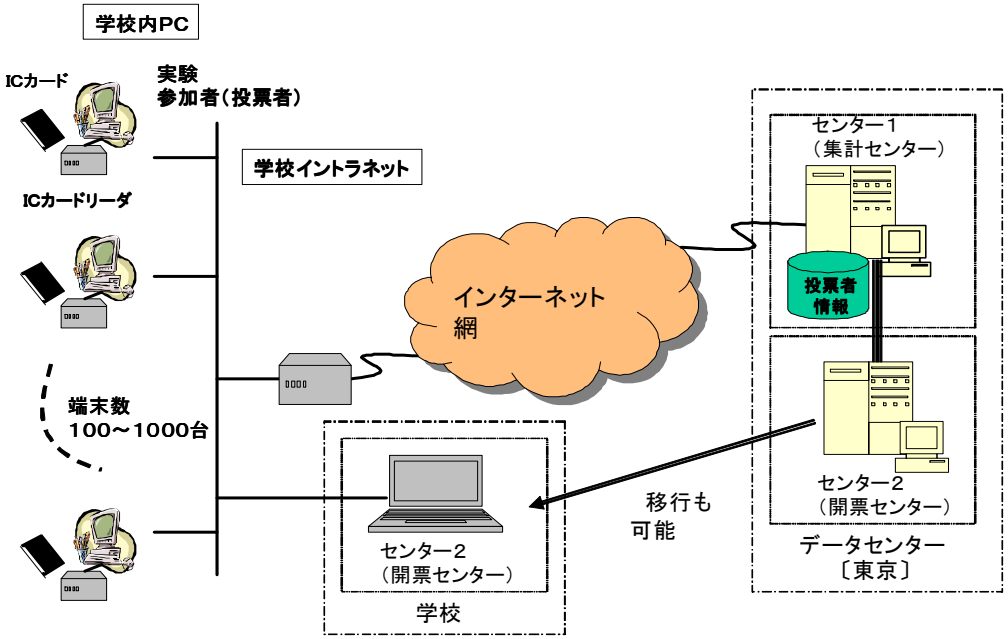


図 63　学校内PCを対象とした実験イメージ

【民意主導政策形成支援システムとしての利用】

CCC21 協議会の協力の下に実験を持ち込んだ地方自治体との接触の中で、下記の実用化の可能性が顕在化しつつある。

・今後更に重要となる政策アセスメントの基本ツールとして利用できる。
・調査母体(有効投票者)の信憑性を担保した民意収集が望まれている。
・住民参加のイベントツールとしても有用である。

【本システムの利用用途】

a. 地域利害関係に直結する事業計画に対するオピニオンサーベイ
・ごみ、産廃処理現場建設
・道路建設にともなう用地交換
・区画整理事業
・宅地造成事業(山林の開墾のよる)
・市町村合併

b. 個人の状況・趣味・嗜好に関する調査
・性感染症に関しての調査(AIDS)等
・特定疾病に関する調査
・結核、B 型、C 型肝炎
・障害者に対する調査

(iii) 事業化へのポイント

自治体における利用の可能性自治体における利用の可能性iii)事業化へのポイント

地方自治体でのヒヤリングより、下記が重要な事業化へのポイントと判断される。

a. 運用性

開票センターを自治体内部に置きたいとの意見をいただいた。本システムの開票センターは非力な PC でも実現可能な機能構成としているため、ご要望にお応えできる。

b. コスト

システム構築, 運用を継続的に地方自治体で維持するのはコスト的に無理がある。本研究開発実験で実施する集計センターサービスを提供する ASP モデルが有用である。

5-7-3-2 自治体実験の計画

候補に挙がっていた3自治体の内、松本市, 山梨市の2自治体より、参加の意志を得ることが出来、H16 年度実験実施に向け、準備を開始している。

実施時期に関しては、自治体それぞれの諸事情により

(i) 松本市

地方自治体殿における情報通信技術活用の課題先取実験として提案し、ご担当部署により、実験テーマを検討していただいている。

【実験の位置づけ】

民意主導の政策形成支援サービスの提供実験

・行政サービス電子化に続く民意収集サービスへの取り組み

住民の新システム体験

・地方自治体と住民が電子自治体構想の将来を疑似体験

自治体殿懸案の民意収集案件の事前情報入手

・母集団を特定して（個人認証）の投票・アンケートの実施

・投票者の匿名性を確保しますので「本音」の意見の収集を期待

(ii) 山梨市

地方自治体殿における教育分野での課題先取実験として提案し、ご担当部署ならびに教育委員会のご担当により、実験テーマを検討していただいている。

【実験の位置づけ】

民意主導の政策形成支援サービスの提供実験

・電子投票，アンケート，パブリックコメントを活用

・民意収集による行政，学校教育への反映

インターネットを利用した先進的技術研究の模擬体験

・情報リテラシーの学習

・ネットワーク社会の近未来の姿やセキュリティ問題に関する啓蒙

5-8　準同型公開鍵暗号方式

5-8-1　はじめに

次世代電子投票システムに利用すべき暗号方式の決定を、安全性と性能の対比のもとに策定する。。この際、性能は理論値を用い、安全性は、定義の明確なものを尺度とする。また、既存の諸方式の比較および、新方式についても検討する。

5-8-2　目標の達成状況

高次剰余暗号、OU 関数、NS 暗号、Paillier 暗号、離散対数型暗号(CGS97 等)の 5 種類の準同型暗号方式について，特に本プロジェクトに求められる要件の一つである複数候補者に対する投票を視野にいれ，利用者端末・管理者サーバ毎に処理性能，通信(データ長)性能の理論値を導出し比較した．本プロジェクトの投票プロセスにおける処理と(通信を含む)データの流れを図 64 に示す．

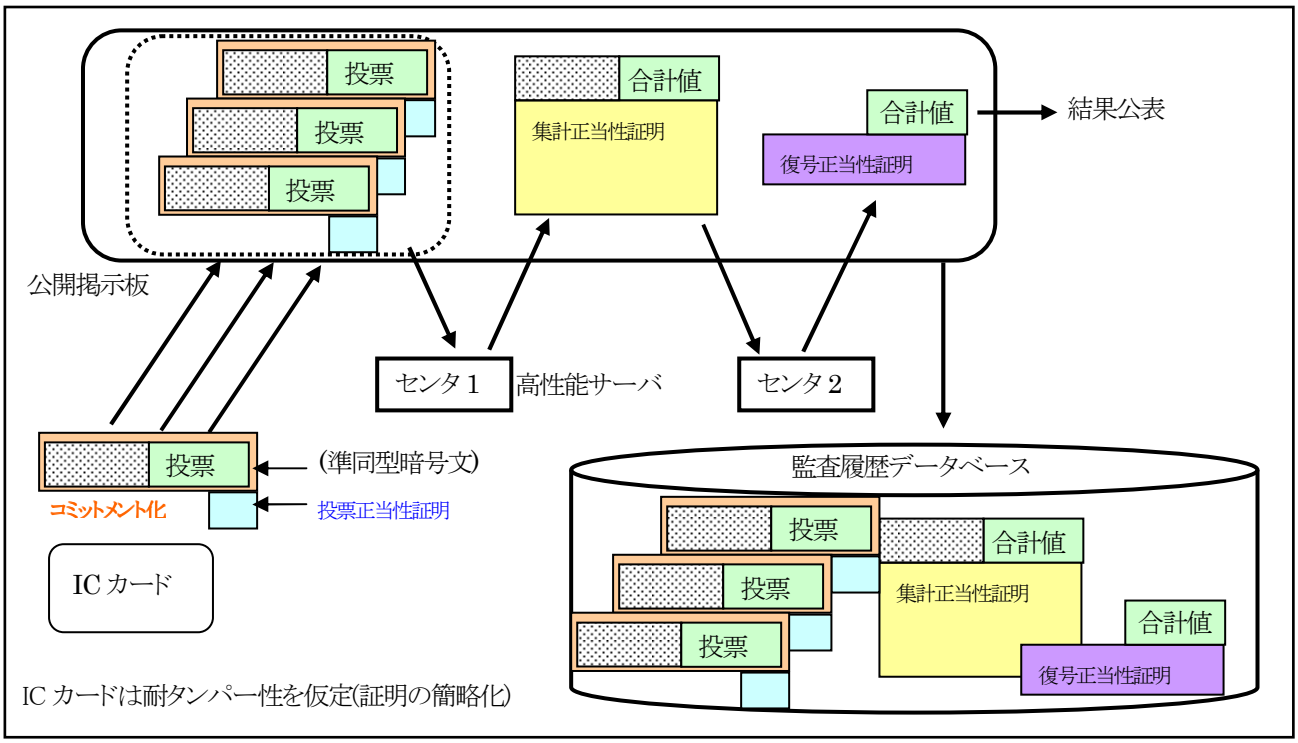


図 64　投票プロセスにおける処理とデータの流れ

本プロジェクトでは，準同型暗号を用いることにより復号処理の簡略化を図るとともに，投票者認証機能を兼ねた耐タンパー性を有する IC カードを利用する．また，投票データを IC カード内で生成するので，投票内容が適切か(例えば，投票データが 1(賛成)または 0(反対)に限られるか)という証明は大幅に簡略化できる．このモデル(耐タンパー性仮定モデル)では，準同型暗号を利用する全ての電子投票方式において，投票者端末にとっての最大の負担となる投票内容の正当性証明コスト(処理時間及びデータサイズ)を大幅に削減できる．以下，主に耐タンパー性仮定モデルにおける準同型公開鍵暗号方式の比較を行う．

まず，準同型暗号を用いて電子投票を実現する場合，同一の投票データ(例えば，賛成=1)が異なる暗号文データに暗号化される必要があるため，確率暗号を用いなければならない．また，準同型暗号の中には復号性能が低速なものも多く，暗号文 1 つあたりの平文サイズが小さいものも多い．さて，候補となる 5 種類

の暗号方式はいずれも確率暗号であり，暗号文には投票データ以外に乱数部分(図 64 の灰色の部分)が含まれる．耐タンパー性仮定モデルを採用する場合は，通信量の削減，監査履歴データベースの容量削減の観点から，1 つの暗号文にできる限り多くの投票データを詰込める方式が有利であり，これは単純に「平文長/暗号文長」として評価できる．また，大規模かつ複数候補者に対する投票に適することも必要であるので，やはり「平文長/暗号文長」が大きい方式が望ましい．

更に，計算資源(CPU パワー，メモリ)に制限がある IC カードの利用を前提とするので，暗号化時の演算コスト(特に法のサイズ)が小さいことも準同型暗号を選択するための条件となる．

さて，5 種類の暗号方式は，いずれも安全性は素因数分解や離散対数問題に関するある種の判定問題(DH 判定問題，e次剰余判定問題，n次剰余判定問題等)に帰着される．これらの問題が困難であることを保証するためには，演算を行う法のサイズを大きくすればよい．従って，安全性を有するための(すなわち素因数分解や離散対数計算が困難となる)法のサイズを，CRYPTREC 暗号技術評価報告書を参考にして決定した．次に，データサイズと処理性能に関連が深い「平文長/暗号文長」，「最大規模での暗号化回数」を評価した．結果を**表 48** に示す．

表 48 準同型暗号方式の比較

暗号方式	安全性仮定	法サイズ	平文長/暗号文長	最大規模での暗号化回数
e次剰余暗号	e次剰余判定問題	1024	8%	250
OU関数	p部分群判定問題	1024	33%	59
NS 暗号	複数の p_i次剰余判定問題	1024	22%	91
Paillier 暗号	n次剰余判定問題	2048	50%	20
CGS97	DH 判定問題	1024	2%	500
楕円 CGS97	楕円 DH 判定問題	160	6.3%	500

*)最大規模での暗号化回数は投票者 1,000,000，投票対象 1000 を想定

大規模投票に適し複数候補者への対応が容易な方式は，「平文長/暗号文長」が大きい方式である．また，「最大規模での暗号化回数」が小さいほうが有利である．この条件と計算能力に制限があるICカード等への実装が可能であること(法サイズは1024ビット程度が上限となること)を考慮すると，表 48よりOU関数やNS暗号が有力な候補であることがわかる．

さて，本プロジェクトでは，認証機能を含む全体的な性能，利便性を考慮し，本プロジェクトで採用する準同型暗号方式として，「平文長/暗号文長」がより大きい OU 関数を採用することとした．

5-8-3 TYKK 方式以外の方式の優位性

一方、TYKK方式以外の方式の優位性について述べる。まず準同型方式における既知の方式として米国のCGS方式がある。当プロジェクトは実験を進める中で、CGS方式の大きな欠点に気づいた。それは、投票結果を格納する際のハードデスクへの書き込みに膨大な時間を要し、投票者が多い場合には、集計・開票に支障を来たすという点である。その理由は、CGS方式はエルガマル暗号を用いている為、平分ー暗号文効率が極端に悪いことによるものであり、投票者による正当性の証明を避ける方式(センターが証明を代行する方式あるいはICカードの耐タンパーを利用する方式)を採用した場合、この点が我々の方式の優位性になると考える。

次に、準同型以外のブラインド署名およびミックスネット方式であるが、ブラインド署名の場合、投票時に複数のサーバとの通信を必要とするため、サーバによるブラインド署名から投票までの間に、署名された票が通信エラーによって投票者に届かなかったり、投票者のPCの電源が落ちてしまったりといった障害を考慮する

必要がある。実際、我々の準備実験においても、投票用プログラムをダウンロードする際に、セキュリティの設定等で失敗するケースが見受けられた。これに対して、準同型方式では投票はサーバとの1回の通信で完了し、後の処理はサーバに任せることができるため、システムの信頼性は格段に向上する。

ミックスネット方式では通信回数は1回で完了するためこういった問題は発生しないが、選挙完了まで最後のミックスの復号および集計ができないことが問題として知られている。準同型を用いた我々の方式では、選挙完了後の開票は、ノートPCでも可能であり、金庫に保管するなど運用が容易である。また、当プロジェクトのこれまでの研究で明らかになった、票のサイズとその書き込み性能についての検討はミックスネットについては行われていない。サーバ間で情報をやり取りし、公開情報が多いミックスネットの場合、検討が必要と考える。

以上のように、代表的な3方式は、各々、システム構築方式や運用と関連して一長一短があると考えるが、独自性(特許出願中)という観点も考え、当プロジェクトの考案方式であるTYKK方式を用いて、松本市、山梨市、などと連携して、平成16年に実験を行うべく準備を進めている。

他方、研究では、電子投票システムとしての機能要件は投票方式に依存しない形で進めてきている。今後、投票方式毎の実装への影響を極力吸収する様なシステムインターフェイスを検討する。たとえば、以下の図 65は投票方式と実装の関係を示したが、各投票方式で利用するインターフェイスを定義し、投票方式を変更した場合でも入れ替えが容易にする方式などを検討する。

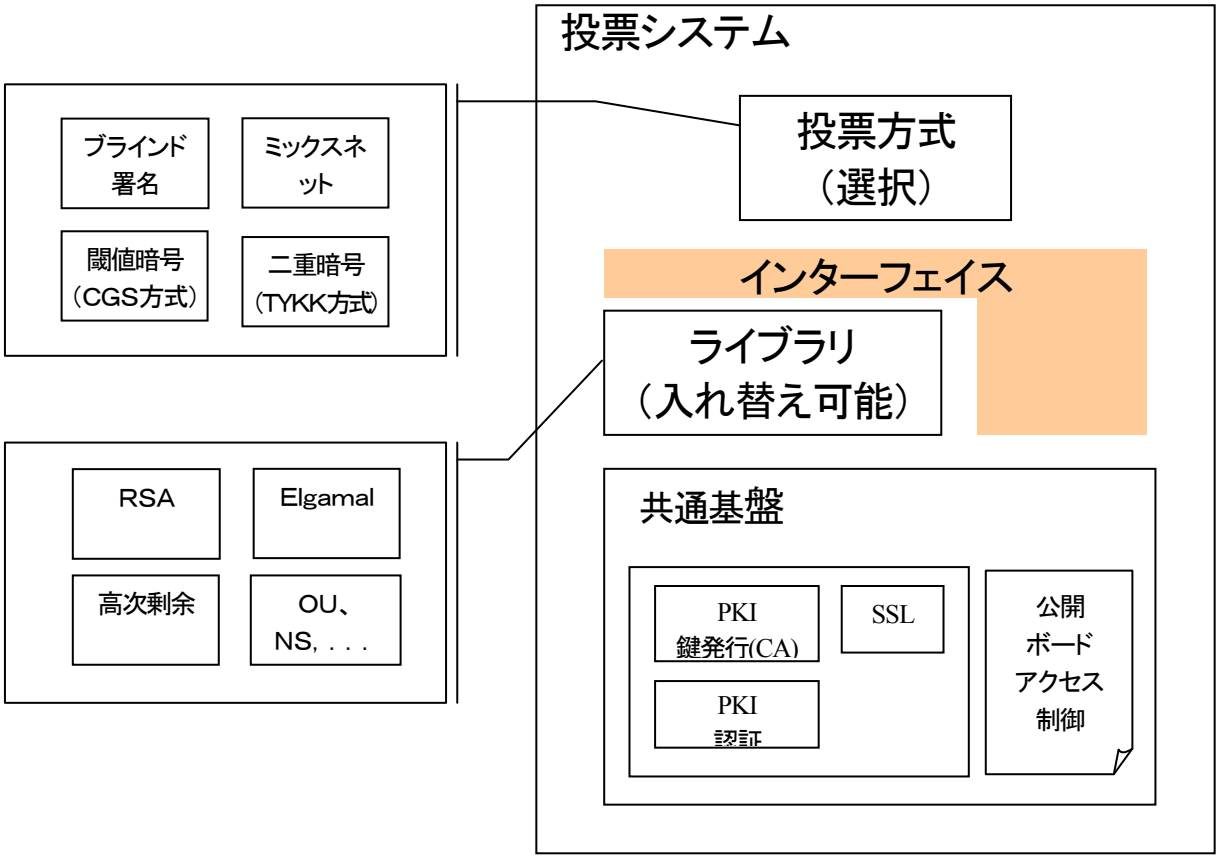


図 65　投票プロトコルと実装の関係

5-8-4 まとめ

複数候補者を考慮する投票用途，特に中～大規模投票を考慮する場合，高次剰余暗号，(楕円)離散対数型(CGS97)のように，テーブル参照を用いて離散対数を解く必要がある方式は，復号性能の観点から，平文サイズを大きくとることができない．実際，暗号文サイズに対して平文のサイズを大きくすると，復号性能の劣化に直結する．これらの暗号も，平文サイズを小さくした場合は，十分高速に復号可能だが，投票の作成(暗号化)回数と通信量が増大する．従って，投票クライアント(例えば，ICカード)への負担が大きくなり，投票を保存するサーバの性能も劣化するため，中～大規模投票には適さない．

一方，Paillier暗号は中～大規模投票においては，復号性能，通信の効率(平文サイズ/暗号文サイズ)の面では最適である．ただし，法のサイズは 2048 ビットとなる．すなわち，クライアントは暗号文を作成する際，2048 ビットの法でべき乗剰余演算を行わなくてはならない．これは，現時点の IC カードに搭載されているべき乗剰余関数の仕様(1024 ビット程度までのべき乗剰余演算が可能)を考慮すると，現実的ではない．もちろん，IC カード上で多倍長演算関数を実装すれば実現できるが，プログラムが複雑・大規模になり，開発コストはもとより，投票者の負担となる暗号化性能(=投票性能)に悪影響を与える。

この結果，中～大規模投票も含めた投票方式として有望なのは，OU関数とNS暗号である．通信の効率(平文サイズ/暗号文サイズ)と復号性能を考慮すると，OU 関数を用いた方式が若干優れている．

なお，OU 関数は，法が pq^2 という特殊な形式であることに注意すべきである．一方，NS 暗号は，合成数である法が pq という RSA 暗号型であるが，$p-1, q-1$ が多くの小さな素数を因子として持つということは注意すべきである．これらの暗号の(特殊な)法に対する効率のよい素因数分解アルゴリズムが発見された場合には，法のサイズ等の見直しが必要である．

従って，OU 関数(暗号化処理は NS 暗号，高次剰余暗号とほぼ同じ)を実装し，性能評価を行うべきと結論する．

また、電子投票に要求させる要件は電子選挙の種類、目的、規模、など多様であるため、TYKK 方式以外の方式の優位性について検討をした。まず準同型方式における既知の方式として米国のCGS方式、のブラインド署名方式、ミックスネット方式各方式などの、TYKK 方式以外の方式の優位性について検討をした。

5-8-5 今後の課題

高次剰余暗号、NS暗号、OU関数、Paillier暗号、(楕円)CGS97等で利用される離散対数を利用する方式について、暗号化コスト、鍵サイズ、データ量、復号速度、安全性証明に要するコストの分析を実施した。

しかし，与えられた要求仕様に対し、現実的かつ効率のよい投票方式を実現するためには、サブテーマ「投票プロセスの正当性証明とその効率化」と連携して要求仕様毎の性能比較をすることが必要である．H16年度も継続してコスト分析の研究を継続する。

5-9　投票プロセスの正当性証明とその効率化

5-9-1　はじめに

電子投票プロトコルに用いられる正当性の証明方式および監査履歴方式を、性能の観点から検討し、理論的に検証する。なお、応答性能は、利用者の端末における処理性能と、選挙用サーバにおける処理性能を別に示し、選挙用サーバにおける処理性能は、投票者数に比例するレベルであること、および、監視下ではない投票端末を利用した場合の、買収や脅迫といった問題を解決する方法であること。

5-9-2　目標の達成状況

TYKK 方式(2 センター方式)における投票プロセスの正当性証明, 監査履歴方式について検討を重ね, 電子情報通信学会英文論文誌上で“An Electronic Voting Protocol Preserving Voter’s Privacy” [90]として発表した. 詳細は論文を参照のこと.

この論文では核となる準同型暗号方式の例として高次剰余暗号を用いているが, 準同型暗号方式に対しての制限(例えば, 閾値法を適用可能などの条件)がないという汎用的な性質も有している. したがって, 準同型暗号方式として OU 関数などを用いてもよい. また, 上記方式では, 選挙用サーバにおける処理性能が投票者数に比例するレベルを達成するとともに, 投票・集計プロセスの正当性証明が可能であるなど, 理論的な安全性も有している.

TYKKを用いたときの、投票プロセスの正当性の検証について述べる。

① ICカードの耐タンパー性の利用

② 暗号プロトコルによる方式

の2つが考えられる。

本プロジェクトにおいては、住民基本台帳システム、及び公的個人認証システムの法制度化を考慮し、耐タンパー性に依存するのが、実用的かと考えており、公的個人認証では、個人にとって最も大事な秘密鍵がサイバーパスポートとして住基カードに内臓されますので、国が耐タンパー性を前提としている以上、投票でもそれを前提とするのは妥当と考える。

本プロジェクトでは, 投票者端末は耐タンパー性を有する IC カードとして実現し, さらに管理者サーバはある程度厳格に管理された高性能コンピュータとなる. この結果, 投票者端末の処理能力は小さいが, 管理者サーバ(集計用コンピュータ)の能力は格段に大きいことを仮定してよく, これは従来の電子投票で考えられているモデルとも一致する. また, 管理・運用技術を併用することにより, 各プロセスでの不正混入の確率を小さくすることは可能である. このため, 耐タンパー性を有する IC カードで作成する投票内容の正当性証明は大幅に簡略化できる.

これらの条件の下, 投票者端末のコストを小さくし, 投票結果をすばやく公開することが可能で, リアルタイムまたは事後に投票プロセスの正当性の証明を監査履歴データベースに格納することが求められる. 図 66 に安全性証明に関して, 耐タンパー性を仮定しない一般的なモデルと耐タンパー性仮定モデルとの差異を示す.

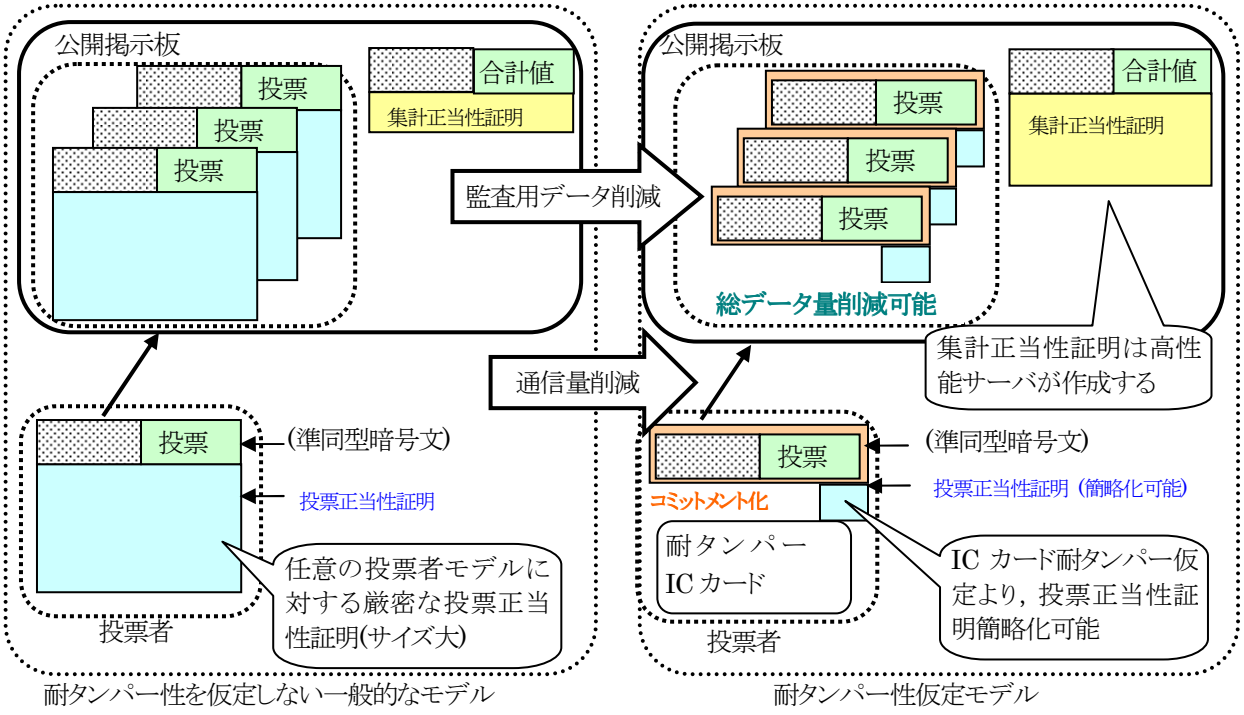


図 66 安全性証明に関するモデルの比較

耐タンパー性仮定モデルでは，データ(暗号文)に多数の投票データを詰め込むことができれば，結果として，投票者の処理コストの削減(つまり，暗号化処理の削減と通信データの削減)を実現できる．

また，公開掲示板に掲示されるデータが最終的に監査履歴データベースに格納されるので，掲示されるデータサイズが小さいほうがサーバや監査履歴データベースの観点からは有利である．すなわち，投票データのサイズ，投票の正当性証明サイズ，集計や開票などに要する証明サイズの和を小さくできることが望ましい．

次に，正当性証明の性能を評価するために，安全性を理論的に証明しうる電子投票方法(CGS97 や TYKK)を選び，更にシステム全体からの視点も考慮して，最終的な評価を行った．表 49 に理論的安全性が証明可能な準同型暗号を利用した電子投票方式の各処理の特長を示す．

表 49 理論的安全性が証明可能な準同型暗号を利用した電子投票方式の特長

方式 (枠組み)	準同型暗号方式	正当性証明コスト			正当性証明以外のコスト			IC カード対応
		初期化	集計	開票	投票作成	集計履歴	開票処理	
閾値法 (CGS97)	ElGamal 暗号	$O(k^2)$	$O(1)$	$O(km)$	$O(\log(n^m))$	$O(n)$	$O(n^m)$	容易
	Paillier 暗号	$O(k^2)$	$O(1)$	$O(km)$	$O(\log(n^m))$	$O(n)$	$O(\log(n^m))$	困難
TYKK	e 次剰余暗号	$O(1)$	$O(n)$	$O(m)$	$O(\log(n^m))$	$O(n)$	$O(n^m)$	容易
	NS 暗号	$O(1)$	$O(n)$	$O(m)$	$O(\log(n^m))$	$O(n)$	$O(\log(n^m))$	容易
	OU 関数	$O(1)$	$O(n)$	$O(m)$	$O(\log(n^m))$	$O(n)$	$O(\log(n^m))$	容易

*)複数候補者に対する投票を前提にコストを評価した．

**)コストの単位はべき乗剰余回数．k は管理者数，n は投票者数，m は候補者数．

本プロジェクトでは，投票作成(暗号化処理)は耐タンパー性を有する IC カードで行う．したがって，投票者端末にとっての最大の負担となる投票内容の正当性証明コストはわずかなので，表 49 には記載していない．

投票者端末の観点からは，複数候補者に対する大規模投票を効率よく実現するためには，投票作成コストが優れていることが望ましい．投票作成コストは全て同一のオーダであるが，準同型公開鍵暗号の評価で示したように，$O(\log(n^m))$の定数部分は大きく異なる．一般に投票者端末の計算能力が小さいことから，$O(\log(n^m))$の定数部分がより小さいことが望ましく，暗号方式としては OU 関数，NS 暗号が優れている．

さて，OU 関数や NS 暗号を利用する場合は，TYKK 方式と組み合わせることにより，理論的安全性を達成できるが，TYKK 方式は集計正当性証明に多くのコストを必要とするという欠点がある．しかし，集計正当性証明を行うのは高性能サーバであり，集計正当性証明を作成するコストは投票者数に比例するレベルを達成していることから，現実的な問題はないと考える．

電子投票方式の広範囲な利用を目標とする本プロジェクトでは，集計時に発生するコストより，投票コストや実装可能性(法が 1024 ビット程度)を重要視すべきである．次に，サーバや監査履歴データベースが現実的な性能を達成できるかどうかを考慮しなくてはならない．システムに求められるこれらの要件を考慮すると，耐タンパー性仮定モデルでは，OU 関数を TYKK 方式に組み合わせる方式が現実的なシステムであると評価できる．ただし，どのモデルを採用するかについては投票に求められる要件などに依存する．このことを考慮しながら実用化に向けて今後も柔軟に対応する．

また、②暗号プロトコルによる方法、においては[YKDKT2003]においてその内容が発表されているが、候補者数が多い場合は、投票者に負担をかけることになります。その対策としては、センター2の協力により、投票者に負担をかけない方式の着想を得ている。

なお、この方式を用いる場合でも、IC カードはレシートフリーに対する事実上の対抗策として重要と認識して、このように、採用すべきモデルは投票に求められる要件などにより異なるので、このことを考慮しながら実用化に向けて今後も柔軟に対応する。

5-9-3 レシートフリー方式の実現

また、上記の評価・研究と平行して、レシートフリー方式実現に関しての研究も進めている。

レシートフリー機能は、投票者が投票内容に関する証拠(レシート)を脅迫者や買収者に提供できなくなれば実現できまる。そこで、本プロジェクトでは、理論的なアプローチと実装によるアプローチの併用で実現する。

(1) 理論的なアプローチ

理論的なアプローチとしては、SK95[91]、Oka97[92]、HS00[93]、及びプロジェクト開始後に提案された JJ02[94]などの方法が知られている。TYKK 方式のレシートフリー機能実現のため、HS00 と類似の方式を適用できるように、プロトコルを一部拡張する。

準同型方式に対しては、盗聴不可能な通信路の存在を仮定すれば、理論的にレシートフリー機能を実現できることが HS00 により示されている。このとき、投票内容を暗号化した暗号文をセンターが作成して投票者に渡し、投票内容(平文)が何であるかを投票者のみに証明するという特殊な仕組み(designated verifier proof)を利用する。TYKK 方式においては、センター2 が暗号文の作成と投票者のみへの証明を受け持ち、投票者がそれを再暗号化して公開掲示板に掲示するという、HS00 と類似の方式を適用することにより、理論的にレシートフリー機能を実現できる。

(i) 提案方式の構成

TYKK方式のレシートフリー実現のための構成として，現状の方式と提案方式の大きく異なる点を挙げる．

- 投票者が票を作成するのではなく，センター2 が票を作成し公開する．投票者は自分の投票したい方を選んで投票する
- センター2 と投票者の間に盗聴不可能一方向性秘密通信路を仮定する.(HS00 と同じ仮定)
- 投票者に秘密情報を持たせ，それに対応した投票者の公開鍵を設定する.

(ii) 票の作成の流れ

TYKK方式の拡張版であるYKDKT2003に関してレシートフリー方式における票の作成の流れを記述する。

使用する暗号パラメータは以下の通りである。

センター2（高次剰余暗号）

【秘密鍵】 p_2, q_2

【公開鍵】 $r, y, N_2 (= p_2 q_2)$

ただし， $N_2 < N_1$ である.

コミットメントデータに使用する鍵は以下の通りである.

【秘密鍵】 なし

【公開鍵】 p_0, g, G

センター2 が票を作成し，投票者が投票をするまでの流れを以下に示す.

Step1. センター2 が0 と1 をそれぞれ高次剰余暗号で暗号化した値を作成し，その値を公開掲示板に送る.

$Z_0 \equiv y^0 x_0^r \bmod N_2$, $Z_1 \equiv y^1 x_1^r \bmod N_2$ $(x_0, x_1 \in_R Z_{N_2})$

Z_0 は0 を,Z_1 は1 を暗号化したものであるが，ここではセンター2 以外は票の対応関係はわからない.

Step2. センター2 は投票内容0 と1 を正しく暗号化したことを証明する．(Proof of validity of ballot)

Step3. センター2 は Z_0 が0 を,Z_1 が1 を暗号化したものであることを秘密通信路を用いて投票者に伝える．その際，証明も付加する. (Designated verifier encryption proof)

Step4. 各投票者は Z_0 or Z_1 から投票したいほうを選び，（Z_k （$k = 1; 0$）とする）乱数 $x_{v_i} \in_R Z_{N_2}$ を生成し，

$Z_i \equiv Z_k x_{v_i}^r \bmod N_2$

を計算する. さらに

$E_i \equiv Z_i^e \bmod N_1$

と再暗号化して公開掲示板に投票する.

Step5. コミットメントデータとして用いる $C_i \equiv G^{Z_i} \bmod p_0$ を作成.

Step6. Z_k を乱数 $x_{v_i} \in_R Z_{N_2}$ を用いて正しく再暗号化したことを証明する．(Re-encryption proof)

(**Step7.**）以下，集計・開票は現状のYKDKT2003方式と同様.

ここで**Step4.** において，投票者 v_i は乱数 x_{v_i} を用いて Z_k を再暗号化している． Z_k をそのままRSA暗号で暗号化して投票したのでは，センター2 にとっては投票者がどちらを投票したのか分かるのでプライバシーが保たれない.(Z_k をセンター1 の公開鍵を用いて暗号化して公開掲示板の値と比較すれば，確認できてしまう)そこで，投票者 v_i は乱数 x_{v_i} を用いて Z_k を再暗号化して Z_i とし，これをRSA 暗号で暗号化して E_i として投票する.

理論的なアプローチでレシートフリー機能を実現するためには、物理的に盗聴不可能な通信路[SK95、HS00]や盗聴不可能な匿名通信路[Oka97]が必要な上、センターから投票者への証明を検証するコストが必要になるなど、投票者を含むシステム全体に多くの負担が発生する。この負担増加は、(現時点では)理論的なアプローチだけでレシートフリーを実現する場合の限界と認識している。

(2) 実装によるアプローチ

投票データである暗号文を IC カード内で生成する場合は、IC カード内で生成した「証拠となりうる一部のデータ」を IC カード内で強制的に削除すること(JJ02 で部分的に使われている方法)により、レシートフリー機能を実現する。

ただ、実装によるアプローチでレシートフリー機能を実現するためには、実装に対して利用者に信頼してもらうことが不可欠である。これは管理運用技術と連携しつつ達成を図ることになる。

これら二つのアプローチを基本アイデアとし、利用者のレシートフリー機能に対する要求に柔軟に対処しうる方式を提供する。

5-9-4 まとめ

現実の投票では，投票対象が複数であることが多く，本研究も投票対象の最大値を1000と設定している．このような複数投票対象を考慮する電子投票を実現するためには，サブテーマ「準同型公開鍵暗号方式」より，OU 関数か NS 暗号といった，平文サイズ／暗号文サイズが大きな準同型暗号を採用する必要がある．従って，TYKK 方式を採用するのが最良の選択となる．さもないと，クライアント(投票)コスト，投票内容を管理するサーバの管理コストが膨大になる．

さて，TYKK のサーバ問題点となる集計正当性証明の処理は，クライアント側ではなく，サーバ側で発生する．サーバはクライアントとは異なり，高性能 PC/WS を仮定することが可能である．従って現実問題としては集計の正当性証明の問題点は緩和できる可能性もある．そのためには，投票規模の分割，複数集計サーバによる処理分散の可能性を実装・実証し，現実的な状況の下で適切な投票規模の分割サイズを調べる必要がある．この際，ネットワークを利用するので，コネクション確立に要するコスト，データ転送コストや，応答性能などについての実証実験や評価を行う必要がある．

また，モデルとして，「IC カードの耐タンパー性を仮定する」というモデルや，「全ての証明は，投票時間内ではなく，投票後のある一定の時期までに作成・検証できればよい」というモデルも考えられる．後者の場合 TYKK 方式の問題となる「集計の正当性証明」をリアルタイムで行う必要がなくなる．例えば乗算結果のみを掲示した後に，集計の証明を与えるというモデルも採用可能である．そのようなモデルでの実証・評価も必要と考えられる．

5-9-5 今後の課題

現状のコンピュータ性能を考慮して，実用に耐えうるように証明の効率化を推進し，一定の成果を得た．今後は，証明に必要な対話回数の削減の検討を含めた，更なる効率向上を中心に研究を継続する．

また，従来の選挙方式(CGS97 等)では安全性の根拠として離散対数問題の困難性を利用する場合が多いが、別の問題の困難性に根拠を置く方式の検討も推進した．この方式についても，更に研究を継続する．

5-10 総括

平成15年度は研究開発全体に亘る9つのサブテーマに対して研究開発を行い、以下の成果を得ることができた。

サブテーマ1:利用分野と法・社会制度の適合性

- 現行法上の「投票の秘密」の範囲を過去の判例から特定し、各段階の電子投票に当てはめた場合の整合点および問題点を明らかにした。
- 外国の選挙および争点投票に関する制度・学説・実例を整理した。
- 第二・第三段階の電子投票の実現に伴って生ずると思われる、憲法上の議会制民主主義原理への影響とその制度化(住民投票・選挙区制など)のモデルを提示した。
- 現行法および特例法を基に、第三段階電子投票向けの法制度改革案を検討できた。
- 医療・教育・行政における利用分野の可能性をいくつかピックアップできた。

サブテーマ2:運用形態ごとの要件整理

- H14年度にまとめた「電子投票機能要件」において、具他的な実装例を追記することで、本要件の参照者にとって、より理解し易いものとなった。また、サブテーマ3の検討結果から、実際的な課題や考慮されていなかった点が明確になり、より充実された。

サブテーマ3:効率的運用とリスク分析

- システムの票作成、投票、集計、開票の各プロトコル性能を最大構成(候補者数1000人、投票者数100万人)で割り出し、性能のボトルネックを分析した結果、他プロトコルに比べ、「投票プロトコル」にボトルネックがあることが判明した。
- 電子投票システムの参照実装モデルに必要なセキュリティ対策技術を現時点で有効かつ適用可能な技術についてまとめた。

サブテーマ4:セキュリティポリシー

- 本プロジェクトでも利用するICカードについて、13種類のものを本プロジェクトのICカードのPPとして、あるべき姿などを検討し、選定に当たっての留意点を明確にした。
- 現在、国内で公表されているPPについては、本プロジェクトを想定した場合には必ずしも十分でないことが明確になった。
- 現在、国内で実施されている電子投票は第一世代の投票システムであるが、いくつかの問題も発生しており、それらについて関係者からのヒアリングを行うことにより、次世代電子投票を行う際に運用上の課題についての情報収集を行い、その整理をした。

サブテーマ5:モデル構築

- 参加企業実験後の投票者アンケート結果から、以下のようなシステムの改善点が明らかになった。
  - (ア) 投票者PC用のインストーラの簡略化
  - (イ) 投票者用ユーザマニュアルの明瞭化
  - (ウ) 投票者用プログラムのユーザインターフェイス改善
- 投票データのデジタル認証、復号化された集計データの正当性証明といったセキュリティ機能の必要性

サブテーマ6:システム構成

- ICカード用OU関数(暗号機能)の実装および性能評価を実施し、100万人規模の大規模選挙においても問題なきことを確認した。
- サーバ用OU関数(鍵生成、復号、集計機能)の実装および性能評価を実施し、100万人規模の大規模選挙においても問題なきことを確認した。
- 集計処理の正当性証明用関数を実装し、不正な集計処理を検出できることを確認した。

サブテーマ7:実験

- 参加企業による小規模の実験の中で、ヘルプディスク, 投票者意識調査を実施し、インストール作業, 操作性に対する改善項目が明確になった。

・ 実際に電子投票システムを利用したユーザ意見として「インターネットを利用した投票は便利である」,「次世代の社会基盤として有効」の割合が多いことが確認された。

サブテーマ8:準同型公開鍵暗号方式

・ 暗号方式ごとの暗号化コスト、データ量、安全性証明に要するコストを分析し、明らかになった要求仕様(投票規模、投票対象、安全性の仮定)毎のコストをもとに、投票者数, 候補者数, 選択肢タイプに応じた適切な方式が確認できた。

サブテーマ9:投票プロセスの正当性証明とその効率化

・ TYKK方式(2センター方式)における投票プロセスの正当性証明について、選挙用サーバにおける処理性能は、投票者数に比例するレベルを達成できた。
・ 投票者のコスト削減を最優先し、監査履歴を作成するサーバ、監査するサーバのコストを削減する方法について一定の成果を得た。
・ TYKK方式をレシートフリー方式へ改良する方式についても検討を進め、Hirt-Sako方式に準じた改良方式に関して理論的に実現可能となる目処がついた。

参考資料・参考文献

サブテーマ1:利用分野と法・社会制度との整合性

[1] 電子機器利用による選挙システム研究会報告書(平成 12 年 4 月)
http://www.soumu.go.jp/s-news/2002/pdf/020201_2.pdf
[2] 岡山県地方自治研究会報告書,「電子投票システムの効果と課題　～電子投票導入に向けての考察～」(2002),p10 以下
[3] 「自治体国際化フォーラム 2001.06 月号」
(available at http://www.clair.or.jp/j/forum/)
[4] 「Koninkrijk waarrijt(王国選挙法)」(1989)
[5] 「実務と研修の為のわかりやすい公職選挙法[第十三次改訂版]」(選挙制度研究会編　, 2003/10)
[6] 伊藤正己、加藤一郎編「現代法学入門(第3次版補定番)」(有斐閣双書、1999/12)
[7] 榎並利博「自治体の IT 革命」(東洋経済新聞社、2000/06)
[8] 「IT　社会における選挙運動、選挙管理」(IT　選挙運動研究会、国政情報センター、2003/10)
[9] 奥平康弘、川添利幸、丸山健「テキストブック憲法[第二十版]」(有斐閣ブックス、1989/6)
[10] 在外選挙制度研究会　岡沢憲芙、戸羽江二「在外選挙｜外国の制度と日本の課題」(株式会社インフォメディアジャパン、1998)
[11] 開原成允, 樋口範雄編「医療の個人情報保護とセキュリティ」(有斐閣、2003/8)
[12] 個のメール医療マガジン　第 20 号 2003/11/10
(バックナンバー:http://biotech.nikkeibp.co.jp/pm/mail_itiran.jsp)
[13] 医療のより良い関係に向けた提言　東京都健康局　2004/7/14
(http://www.kenkou.metro.tokyo.jp/isei/yoi/iseipress030714-6.pdf)
[14] 電子政府・電子自治体のプライバシーに関する調査研究報告書　(株)ネオテニー編　2003/3　(http://joi.ito.com/joiwiki/PrivacyReport)
[15] 学生による授業評価をどう見るか　渡辺　勇一　生物科学　52 巻 4 号(2001.4.1)
[16] goo リサーチ　第 3 回 ビジネスにおける e ラーニングの利用に関する調査
(http://research.goo.ne.jp/Result/0311cl07/01.html)
[17] 情報通信白書　総務省　平成 14 年度版　平成 15 年度版
(http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm)
[18] 地方公共団体における行政評価の導入の実態と今後の展開について(概要)－平成14年度地方公共団体における行政評価についての研究会報告－
(http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm)
[19] 行政評価をダブルクリック！　(http://www.soumu.go.jp/click/)
[20] 日本ジェネリック医薬品研究会(http://www.generic.gr.jp/)
[21] 医薬工業協議会(http://www.epma.gr.jp/index.htm)
[22] 薬剤費の「段階式自己負担」導入に功罪、後発品への切り替え進むが治療中断も－－米研究　2003.12.8　(http://medwave2.nikkeibp.co.jp/wcs/med/leaf?CID=onair/medwave/mdps/280346)
[23] 保健医療分野の情報化にむけてのグランドデザイン(2001)
http://www.mhlw.go.jp/shingi/0112/dl/s1226-1.pdf
[24] 「高度情報通信社会推進に向けた基本方針」
http://www.kantei.go.jp/jp/it/981110kihon.html
[25] 「わが国における個人情報保護システムのあり方について(中間報告)」(高度情報通信社会推進本部,1999)http://www.kantei.go.jp/jp/it/privacy/991119tyukan.htm

[26]「わが国における個人情報保護システムのあり方について」(中間報告)に対する意見書(日弁連,2000)
http://www.nichibenren.or.jp/jp/katsudo/sytyou/iken/00/2000_6.html
[27] 医療におけるプライバシー保護ガイドライン(1999)
http://www.mi-net.org/privacy/p_guide.html
[28] ヒトゲノム・遺伝子解析研究に関する倫理指針(2001)
http://www.meti.go.jp/policy/bio/rinri-shishin/rinrishishin-hontai.pdf
[29] 疫学研究に関する倫理指針(2002)
http://www.niph.go.jp/wadai/ekigakurinri/index.htm
[30]「ヒトES細胞の樹立及び使用に関する指針」(2001)
http://www.mext.go.jp/a_menu/shinkou/seimei/2001/es/010901.htm
[31] ヒトに関するクローン技術等の規制に関する法律」及び「特定胚の取扱いに関する指針
http://www.mext.go.jp/a_menu/shinkou/seimei/2001/hai3/011201.htm
[32] 精子・卵子・胚の提供等による生殖補助医療のあり方についての報告書
http://www.mhlw.go.jp/shingi/2003/01/s0109-2h.html
[33] 選挙制度研究会編『実務と研修のためのわかりやすい公職選挙法』ぎょうせい,第 12 次改訂版,(2001)
[34] 東尾正・石川善朗『公職選挙法』ぎょうせい(1992)
[35] 野中俊彦『選挙法の研究』信山社(2001)
[36] 東浩紀(2003)「情報自由論」(中央公論 4 月号)
[37] G. アナス「プライバシーと守秘義務」(情報倫理学研究資料集 III,2001)
サブテーマ2:運用形態ごとの要件整理
[38]「電子機器利用による選挙システム研究会報告書」(総務省 2002 年 2 月)
[39] VoteHere, Inc., "Network Voting System Standards"
サブテーマ3:効率的運用とリスク分析
[40] キーマンズネット http://www.keyman.or.jp/
[41] IT 用語辞典 e-Words http://e-words.jp/
[42] アットマーク・アイティ http://www.atmarkit.co.jp/fsecurity/
サブテーマ4:セキュリティポリシー
[43] Mainichi INTERACTIVE
http://www.mainichi.co.jp/digital/network/archive/200307/10/6.html
[44] 一枚の IC カード乗車券で関東圏の鉄道・バスをもっと便利
http://www.jreast.co.jp/press/2003_1/20030712.pdf
[45] IC カード利用促進協議会 | IC カード市場の動向
http://www.jicsap.com/sysintro/shijo.html
[46] Felica 概要 http://www.sony.co.jp/Products/felica/contents02_02.html
[47] NTT 情報流通プラットフォーム研究所 IC カード情報流通プラットホーム NICE
http://www2.pflab.ecl.ntt.co.jp/index/kenkyu/html/16.html
[48] 総務省 住民基本台帳カードの構造について(システム面のセキュリティ対策)
http://www.soumu.go.jp/c-gyousei/daityo/pdf/juki_card_01.pdf
[49]「IC カードの普及等による IT 装備都市研究事業 開発事業(テーマ 1～6)報告書」4-57 ニューメディア開発協会 2002
[50] 兵藤義以、山手康正「雑誌 FUJITSU 2000 年 3 月号 104-108 マルチアプリケーションマネジメントシステム」(MAM、2000/04)
http://magazine.fujitsu.com/vol51-2/paper05.pdf
[51] Felica 概要 Felica のしくみ
http://www.sony.co.jp/Products/felica/contents02_02.html
[52] Visa Smart Card Protection Profile Draft Version 1.6, Visa International Service Association, May 4,1999

[53] Smart Card Security User Group's Protection Profile Version 3.0, Smart Card Security User Group, 9 September 2001
[54] Smart Card Integrated Circuit with Embedded Software Protection Profile Version 2.0, ATMEL Smart Card ICs, BULL-SC&T, DE LA RUE - Card Systems, EUROSMART, GEMPLUS, GIESECKE & DEVRIENT GmbH, HITACHI Europe Ltd, INFINEON Technologies, MICROELECTRONICA Espanola, MOTOROLA-SPS, NEC Electronics, OBERTHUR Card Systems, ODS, ORGA, Philips Semiconductors, SCHLUMBERGER Cards Division, SECRETARIAT GENERAL DE LA DEFENSE NATIONALE Direction Central de la Securite des Systemes d'Information, ST Microelectronics, June 99
[55] Smartcard IC Platform Protection Profile Version 1.0, Atmel Smart Card ICs, Hitachi Europe Ltd, Infineon Technologies AG, Philips Semiconductors, July 2001
[56] Protection Profile Smart Card IC with Multi-Application Secure Platform Version 2.0, ATMEL Smart Card ICs, BULL-CP8, EUROSMART, GEMPLUS, GIESECKE & DEVRIENT GmbH, HITACHI Europe Ltd, INFINEON Technologies, MICROELECTRONICA Espanola, MOTOROLA-SPS, NEC Electronics, OBERTHUR Card Systems, ODS, ORGA, Philips Semiconductors, SCHLUMBERGER Cards Division, SECRETARIAT GENERAL DE LA DEFENSE NATIONALE Direction Centrale de la Securite des Systemes d'Information, ST Microelectronics, November 2000
[57] Protection Profile Intersector Electoronic Purse and Purchase Device Version 1.3 March 2001
[58] Protection Profile Smartcard Integrated Circuit Version 2.0 Motorola Semiconductors, Philips Semiconductors, Service Central de la Securite des Systemes d'Information, Siemens AG Semiconductors, STMicroelectronics, Texas-Instruments Semiconductors September 1998
[59] IC カード プロテクションプロファイル 1.1 版 IC カード取引システム研究開発事業組合 2000/1
[60] IC カードリーダライタ プロテクションプロファイル 1.1 版 IC カード取引システム研究開発事業組合 2000/1
[61] JICSAP Ver2.0 Protection Profile Part 1 Multi-Application Secure System LSI Chip Protection Profile Version2.5, Japan IC Card System Application Council, June 6,2003
[62] PKI スマートカードプロテクションプロファイル バージョン No.:1.1 情報処理振興事業協会 2002/2
[63]「IT 装備都市研究事業 アプリケーション・プログラム・ローディング機能付き IC カードのセキュリティ要求仕様書 第 1.0 版」(財)ニューメディア開発協会 2001/12
[64]「IC カードの普及等による IT 装備都市研究事業 開発事業(テーマ 1～6)報告書」財団法人 ニューメディア開発協会(代表:NTT コミュニケーションズ株式会社) 2002/4
[65] A Comparative Study of the Major Smartcard Platforms Dr Brian McKeon Director,Smartcard Technologies Keycorp Limited 2001/11
[66]「雑誌 FUJITSU 2000 年 3 月号」 2000/4
[67] Smart Card Protection Profiles :An Overview , Mikhail Gordeev, Vesna Haasler, Martin Manninger 2002
[68] 吉川肇子著「リスク・コミュニケーション」、(福村出版、1999)
[69]「自治体のリスクコミュニケーション」、(神奈川県自治総合研究センター、2001/3)
[70] 島崎敏一、「ゲーム理論による談合の分析」、建設マネジメント研究論文集, 土木学会, Vol.4, pp.21-28, 1996.12.12-13
[71] Eric Maiwald、「Network Security」、Osborne/McGraw-Hill、2001

サブテーマ5:モデル構築
サブテーマ6:システム構成
[72] 岡本栄司 著 暗号理論入門[第 2 版] 共立出版株式会社
[73] 暗号技術評価報告書 「CRYPTREC Report 2002」
[74] IC カードシステム利用促進協議会 http://www.jicsap.com/index.html
[75] JR 東日本 http://www.jreast.co.jp
[76] 日本道路公団 http://www.jhnet.go.jp
[77] 総務省 http://www.soumu.go.jp
[78] NTT 東日本 http://www.ntt-east.co.jp
[79] NTT 西日本 http://www.ntt-west.co.jp/
サブテーマ7:実験
サブテーマ8:準同型公開鍵暗号方式
[80] Baudron, O., Fouque, P., Pointcheval, D., Stern, J., and Poupard, G.: "Practical Multi-Candidate Election System," Proceedings of the 20th ACM Symposium on Principles of Distributed Computing (PODC2001), pp. 274-283 (2001).
[81] Benaloh, J.: "Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols," Advances in Cryptology-CRYPTO'86, LNCS263, pp.213-222 (1986).
[82] Cramer, R., Gennaro, R., and Schoenmakers, B.: "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology-EUROCRYPT'97, LNCS1233, pp.103-118 (1997).
[83] Fouque, P.A., and Stern, J.: "One Round Threshold Discrete-Log key Generation without Private Channels", Proc. Of PKC2001, LNCS1992, pp.300-316, (2001)
[84] Kurosawa, K., and Tsujii, S.: "A General Method to Construct Public Key Residue Cryptosystems," Trans. Of IEICE, Vol. E73, No.7, pp.1068-1072 (1990).
[85] Okamoto, T., and Uchiyama, S.: "A New Public-Key Cryptosystem as Secure as Factoring," Advances in Cryptology-EUROCRYPT'98, LNCS1403, pp.308-318 (1998).
[86] Naccache, D., and Stern, J.: "A New Public Key Cryptosystem Based on Higher Residues," Proc. 5th Conf. on CCS, pp.59-66 (1998).
[87] Paillier, P.: "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Advances in Cryptology-EUROCRYPT'99, LNCS1592, pp.223-238 (1999).
[88] Pedersen, T.:"A threshold cryptosystem without a trusted party", Advances in Cryptology-EUROCRYPT'91", LNCS547, pp.522-526 (1991).
[89] 暗号技術評価報告書(2001 年度版), 情報処理振興事業協会, 通信・放送機構 (2002)
サブテーマ9:投票プロセスの正当性証明とその効率化.
[90] [YKDKT2003]H.Yamaguchi, A.Kitazawa, H.Doi, K.Kurosawa and S.Tsujii. An Electronic Voting Protocol Preserving Voter's Privacy. IEICE TRANSACTION on Information and Systems. Vol. E86-D, No.9, pp1868-1878,2003.
[91] [SK95] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth," EUROCRYPT'95, pp.393-403, Springer-Verlag LNCS 921, 1995.
[92] [Oka97]T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," Security Protocols Workshop, pp.25-35, Springer-Verlag LNCS 1361, 1997
[93] [HS00]M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," EUROCRYPT'00, pp.539-556, Springer-Verlag LNCS 1807, 2000

..
[94] [JJ02]A. Juels and M. Jakobsson, "Coercion-Resistant Electronic Elections," Cryptology ePrint Archive 2002/165, IACR, 2002
[95] Cramer, R., Gennaro, R., and Schoenmakers, B.: “A Secure and Optimally Efficient Multi-Authority Election Scheme”, Advances in Cryptology-EUROCRYPT’97, LNCS1233, pp.103-118 (1997).
[96] S. Tsujii, H. Yamaguchi, A. Kitazawa, and K. Kurosawa,. “A Method for Voting Protocols with regards to Privacy,” IEICE Technical Report, ISEC98-42 pp.45-52 (1998).
[97] 辻井重男, 山口浩, 北澤敦, 長井雅紀, 黒澤馨: “VCA モデルによる電子投票システムの提案,” Proc. of SCIS’99, pp.29-34 (1999).
[98] Yamaguchi, H., Kitazawa, A., Kimura, T., Takahashi, H., Kurosawa, K., and Tsujii S.: “A Method for Voting Protocols with regard to Privacy – NO.3 Experimental Results –,” 信学技報 ISEC2000-77, pp.163-169 (2000)

全般:.
[99] 平成14年度研究成果報告「次世代電子投票・アンケートシステムとその社会的利用に関する研究」
[100] 平成14年度研究成果報告「次世代電子投票・アンケートシステムとその社会的利用に関する研究」～詳細・補足編
[101] 「電子投票システムに関する技術的条件及び解説」(総務省)

（添付資料）

1 研究発表、講演、文献等一覧

研究発表、論文等の状況は、以下のようになっています。

研究発表

項番	発表者名	表題	発表会名	発表年月	備考
1	山口 浩 北澤 敦 Sheu, Phillip 石井 千洋	Bridging Biomedical Application and IT - A Case Study	Integrated Design & Process Technology	2003/06	14-001
2	山口 浩 北澤 敦 黒澤 馨 辻井 重男	An Anonymous Survey Protocol Preserving Privacy.	IDPT2002 Conference, Society for Design and Process Science	2002/12	―
3	山口 浩 星野 幸夫 鈴木 健嗣 Chittoor V. Ramamoorthy	The design of new service system based on the interdisciplinary research,			―

論文

項番	著者名	表題	誌名	掲載年月	備考
1	山口 浩 星野 幸夫 Chittoor V. Ramamoorthy 石井 千洋	Creating a New Service on the Web	International Journal on Artificial Intelligence Tools	2003/06	14-002
2	山口 浩 北澤 敦 土井 洋 黒澤 馨 辻井 重男	An Electronic Voting Protocol Preserving Voter's Privacy.	IEICE TRANSACTION on Information and Systems.	2003/09	15-001
3	山口 浩 鈴木 健嗣 Chittoor V. Ramamoorthy	The Humanization, Personalization and Authentication ISSUES in the Design and Interactive Service System	Transaction of the SDPS	2003/09	―

講演

項番	講演者	表題	講演会名	講演年
1	山口　浩	An example of applicants' qualifications	IEEE-International Conference on Tools with Artificial Intelligent	2002
2	山口　浩	Accelerated migration to Collaborative Intellectual Activities – Bioinformatics and Knowledge Society	IEEE Fifth International Symposium on Multimedia Software Engineering	2002
3	山口　浩	Toward a digital knowledge services on cyberinfrastructure	The 8th IEEE International Symposium on High Assurance System Engineering	2004
4	山口　浩	An anonymous polling scheme exploring a new community on web	The 21st International Conference on Conceptual Modeling	2002
5	山口　浩	Creating a knowledge-based service on the web	Formal Opening of Distance Learning Laboratory College of Engineering	2002