管理番号＃１４－０５

平成１６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

委託先：NEC ソフト㈱

平成１７年５月

情報通信研究機構

# 平成16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 研究開発の全体計画

## 2-1　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。

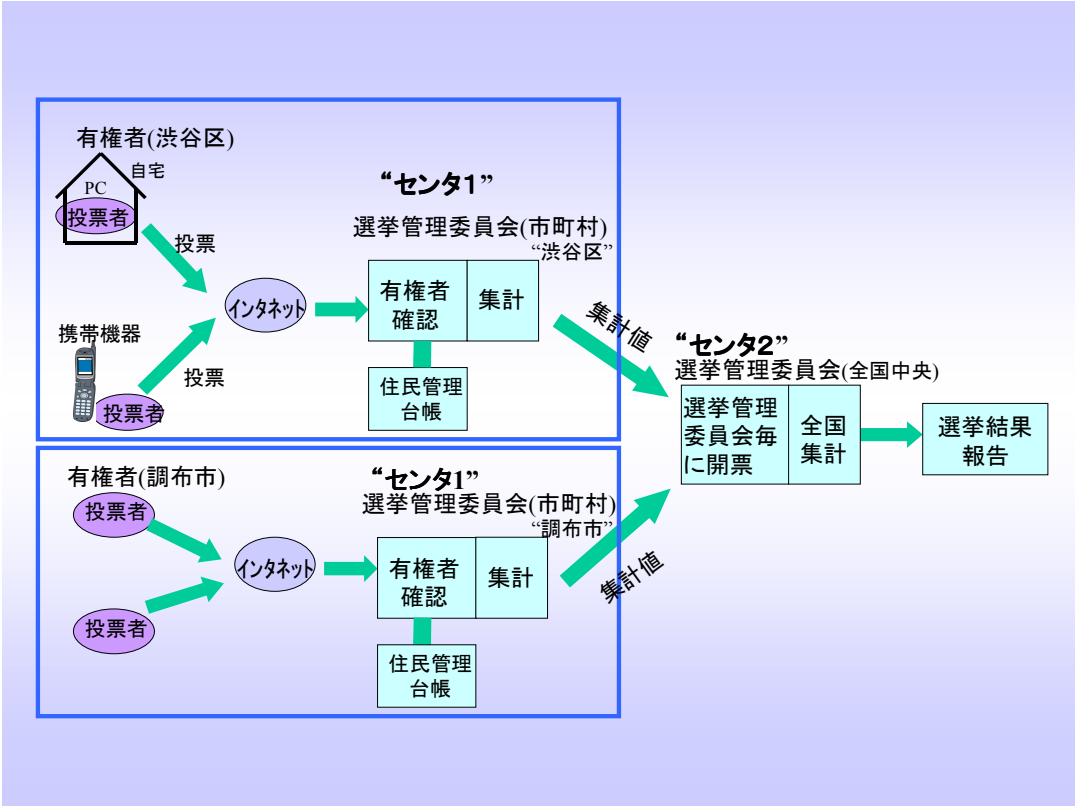



**図 1　提案のシステム形態“国勢選挙における有権者センタ 1, 2（選挙管理委員会）”**

・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 2 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。

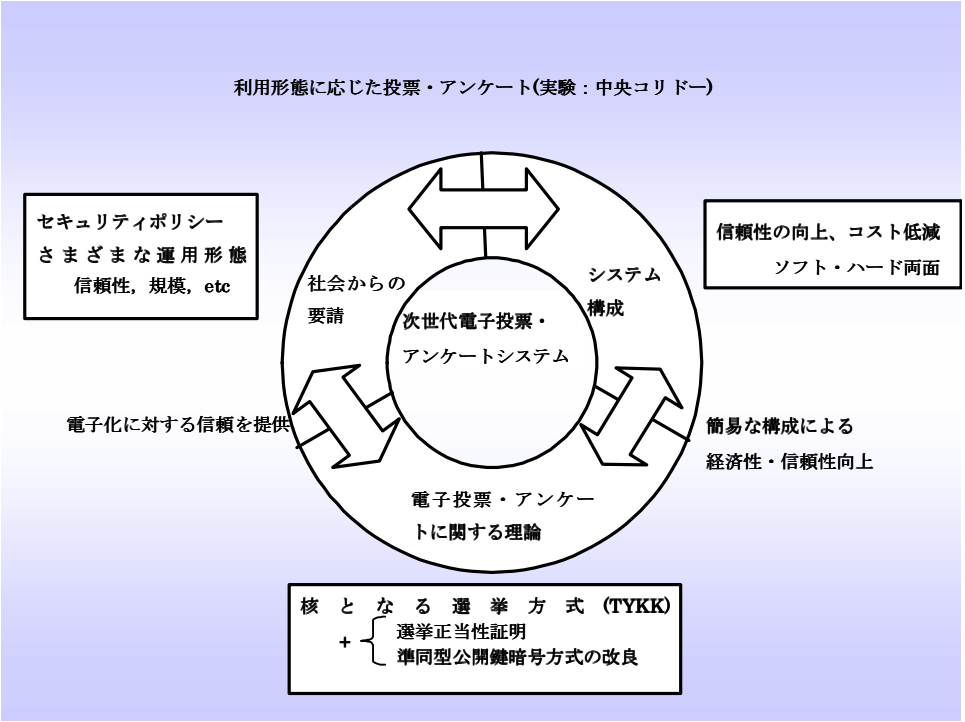



**図 2 次世代電子投票・アンケート方式とその社会的利用に関する研究(概念図)**

(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1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**

① 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)
② 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 3 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ー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。

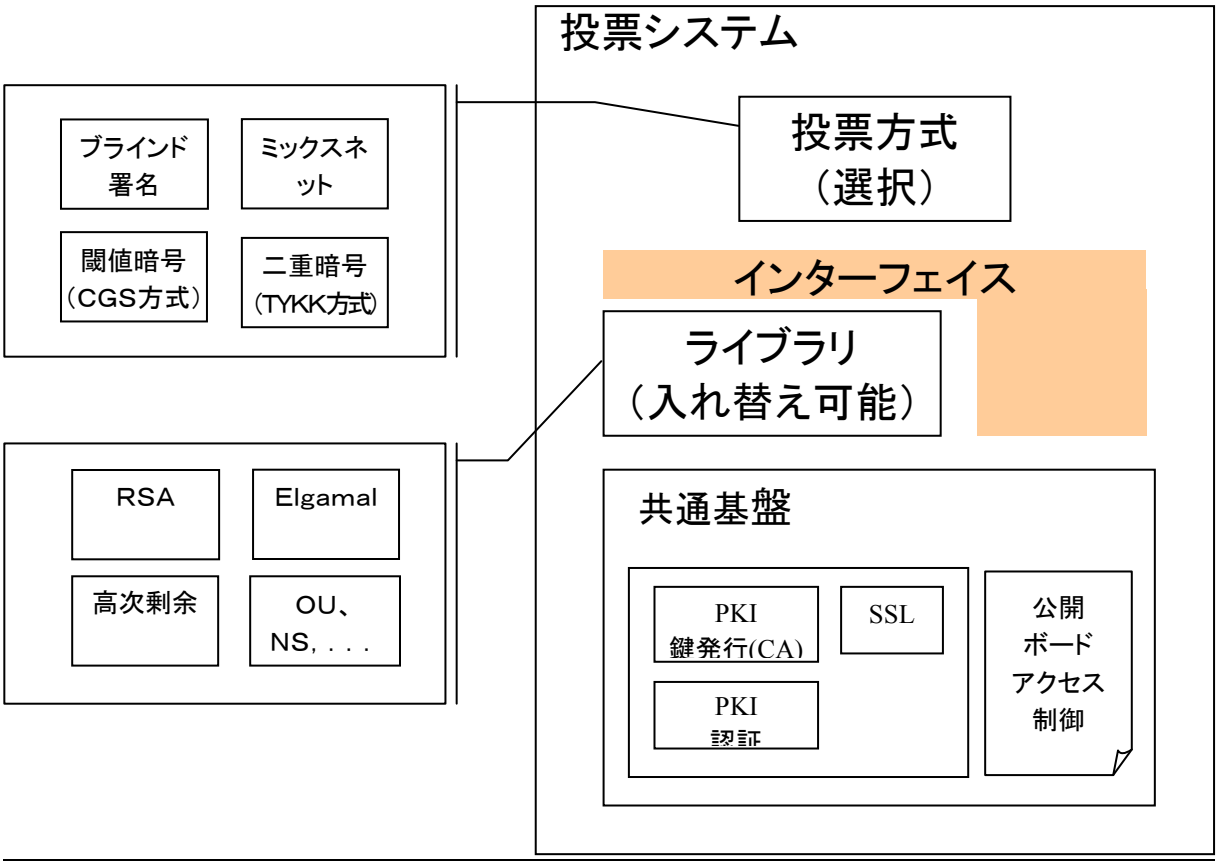



**図 3 投票プロトコルと実装の関係**

(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。

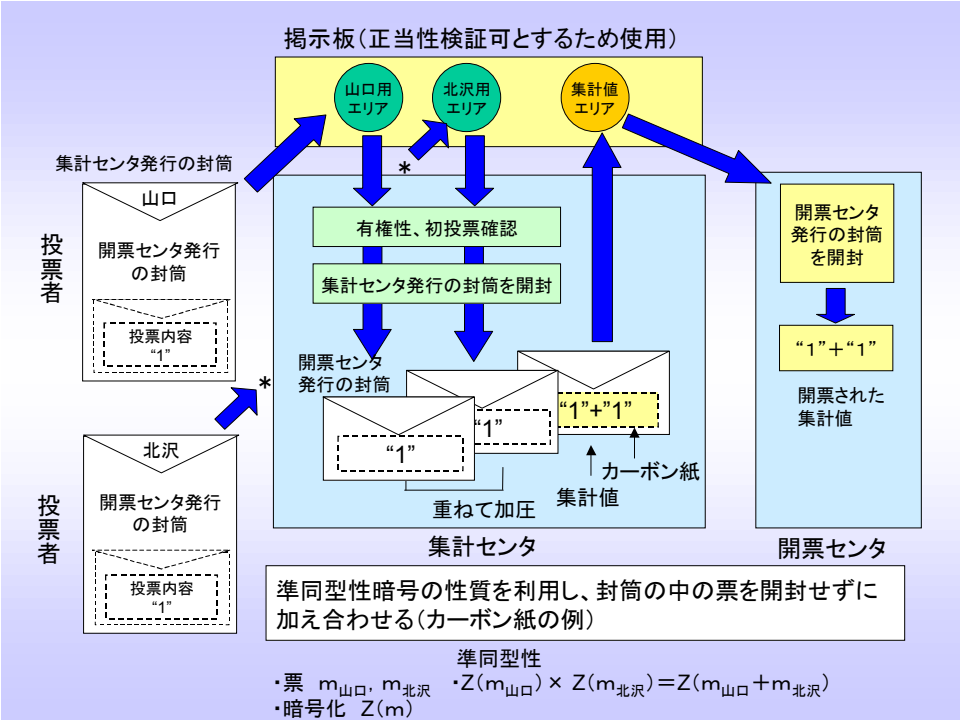



**図 4 電子選挙：TYKK 方式のプロセス**

(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。

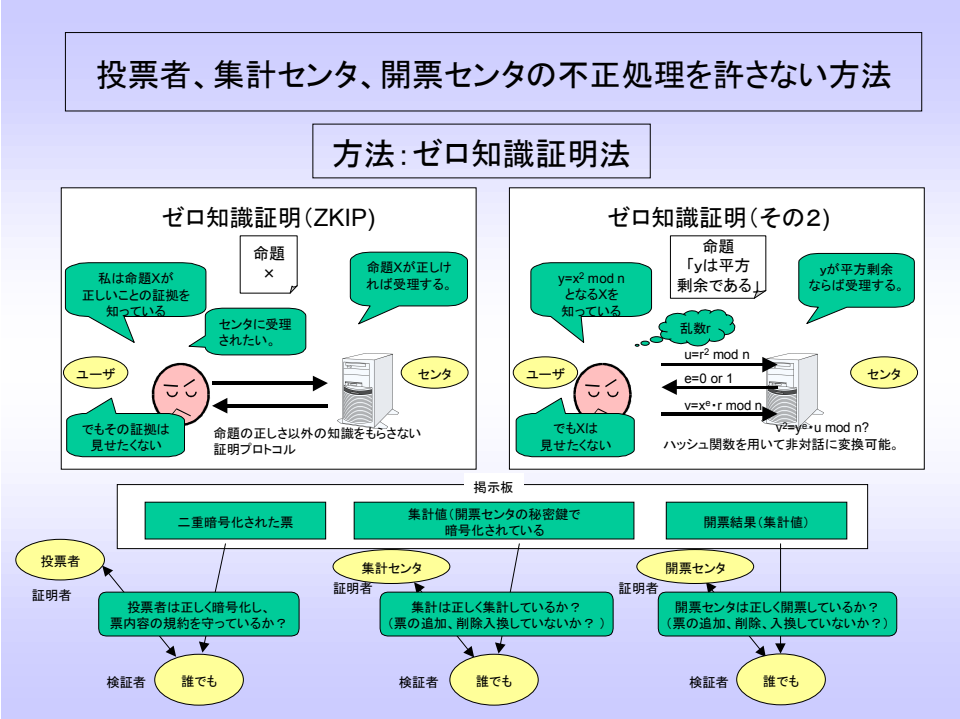



**図 5 正当性証明**

(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。

## 2-2　研究開発目標

### 2-2-1　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」**

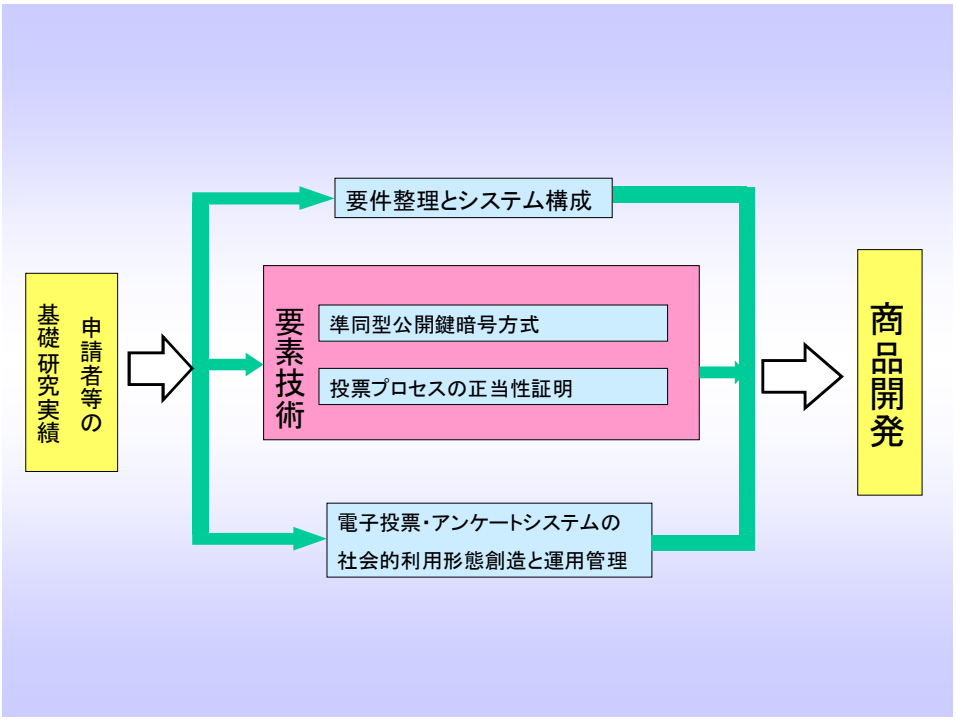



**図 6　本研究開発の課題**

（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。

## 2-2-2 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。

## 2-3　研究開発の年度別計画

平成14年度、平成15年度および平成16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。

平成16年度

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。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。

（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。

平成16年度

今年度整備した「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」のドラフトの見直しを行う。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ものとする。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にする。

（iii） 効率的運用とリスク分析

平成15年度

サブテーマー 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。

平成16年度

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。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。

（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。

平成16年度

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。

① 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。

② 運用の観点(ISO17799, ISMS)では、現在国内で行われている第一段階での電子投票における課題等の考察を通して、管理・運用体制に必要なセキュリティ管理システムを考察し、セキュリティポリシー、規定、手順のガイドラインを策定する。

成果の発表および妥当性の検証については、以下のように実施する。

① 電子投票システムやICカードのISO15408に関しては、日本セキュリティマネジメント学会(JSSM)全国大会(6月)での発表を予定している。
JSSMでの発表及び、実験にて得られた知見を含め、ICカードのPPのための指針の評価・作成を行う。

② 運用の観点(ISO17799, ISMS)では、
自治体での実験を通して、妥当性の検証を行う。
実験における環境を考察し、それを基に研究成果として作成したISMSを検証し、運用面における妥当性を評価・見直しを行う。
自治体における実環境および実験からの知見を総合的に検証し、電子投票・アンケートシステムにおけるISMS詳細基準を作成する。
ここで検討を行った調査・研究については、JSSMが今秋開催を計画している情報セキュリティ連合学会等での発表を予定している。

(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。

平成16年度

H15年度実装した電子投票システムの参照モデルについて、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できるようにする。

(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。

平成16年度

平成15年度の成果をもとにまとめを行う。

(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。

平成16年度

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。

(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。

平成16年度

平成15年度までの成果を元に、性能改善を行う。特に要件定義に従い、投票者数、候補者数、選択肢タイプに応じた適切なパラメータを得るための方式に関する研究を行い成果をまとめる。

(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。

平成16年度

要件定義、特にクライアントやサーバで仮定しうる条件を考慮した性能向上に関する研究と、レシートフリー方式に関する性能向上に関する研究を行い成果をまとめる。

**計画表**

（金額は非公表）

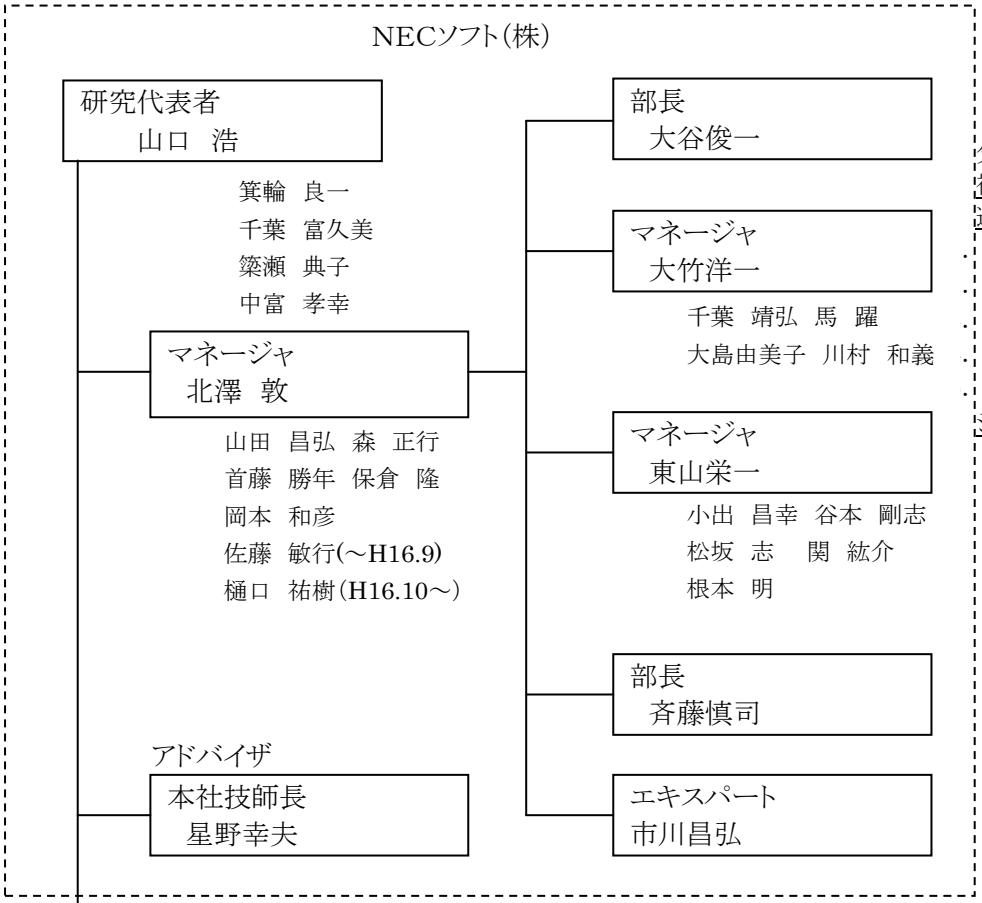
| 研究開発項目 | H14 年度 | H15 年度 | H16 年度 | 計 | 備　考 |
|---|---|---|---|---|---|
| 次世代電子投票・アンケート方式とその社会的利用に関する研究 | | | | | |
| 社会的利用形態の創造とシステムの運用管理<br>1. 利用分野と法・社会制度との整合性<br>2. 運用形態ごとの要件整理<br>3. 効率的運用とリスク分析<br>4. セキュリティポリシー（ISO17799etc.） | | | | | 再委託先<br><br><br><br>（中央大学研究開発機構） |
| システム構成<br>5. モデル構築<br>6.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

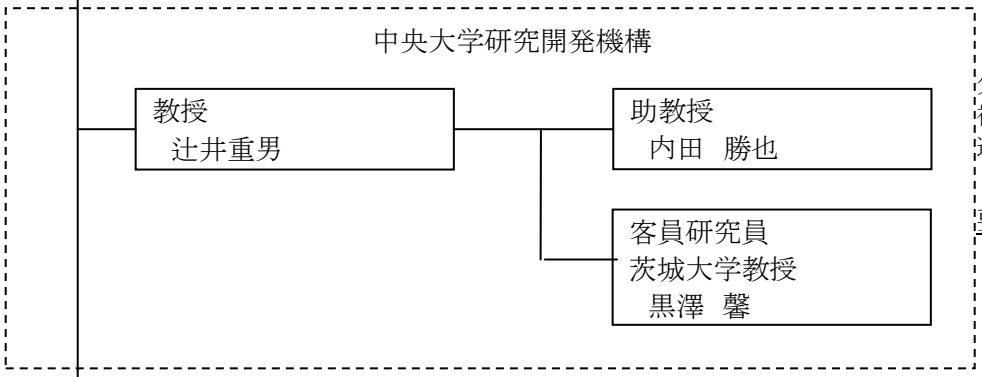
# 3 研究開発体制（平成１６年度）

## 3-1　研究開発実施体制



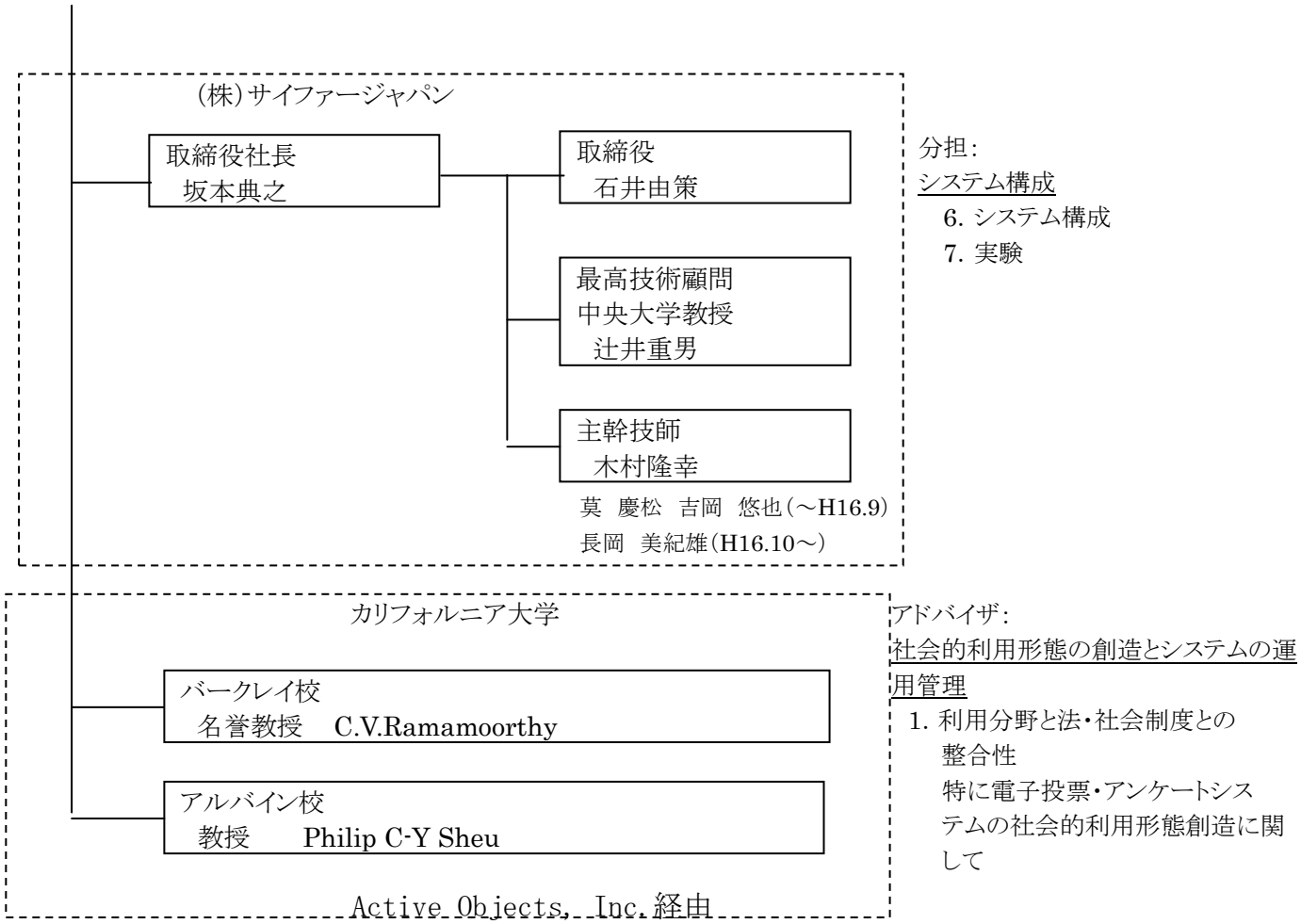

分担:
社会的利用形態の創造とシステムの運用管理
1. 利用分野と法・社会制度との適合性
2. 運用形態ごとの要件整理
3. 効率的運用とリスク分析

システム構成
5. モデル構築




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


(株)サイファージャパン
取締役社長
坂本典之
取締役
石井由策
最高技術顧問
中央大学教授
辻井重男
主幹技師
木村隆幸
莫 慶松 吉岡 悠也(～H16.9)
長岡 美紀雄(H16.10～)
分担:
システム構成
6. システム構成
7. 実験
カリフォルニア大学
バークレイ校
名誉教授 C.V.Ramamoorthy
アルバイン校
教授 Philip C-Y Sheu
Active Objects, Inc.経由
アドバイザ:
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
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

# 3-2 利用分野と法･社会制度との整合性

## 3-2-1 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 3 年、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り、地方自治体による電子投票はこれまでに 12 件に上る。2004 年度は新見市と白石市で 2 度目の電子投票が実施される一方、電子投票を実施した福井県鯖江市が財政を理由に条例の廃止を発表し、2005 年 3 月には、可児市の選挙に関して、選挙無効の名古屋高裁判決があった。また、新見市は、2005 年 4 月に町村合併に伴って行われる市長・市議選は、新市に加わる周辺町村の準備不足から電子投票を断念して手書きの投票に戻る。電子投票機のシステムトラブルに関連し、松江市は 2005 年 5 月の市長選を時期尚早として断念し、いまのところ 2005 年の電子投票の予定は立っていない。総務省は、危機管理対策の徹底を自治体に求める考えで、電子投票に関しては、理解を深めてもらうよう新マニュアルを作成し、夏までに自治体に配布する予定となっている[1]。しかし、自治体合併による新規導入の差し控えや、費用対効果を考えた国政選挙での電子投票導入の様子見状態でもあり、なんらかの推進策が必要な状態にあるといえる。他方、韓国では、2008 年の第 18 代国会議員総選挙から電子投票機による投票システムを導入し、2019 年の第 19 代国会議員総選挙ではインターネット投票を導入・実施するという計画を示している。

**表 1　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) |
| ・広島市長選の一部選挙区(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) |
| ・岡山　新見市　岡山県知事選挙・岡山県議会議員補欠選挙(2004 年 10 月) |
| ・宮城　白石市市長選(2004 年 10 月) |
| ・三重　四日市市長・市議議会議員補欠選挙(2004 年 11 月) |

本研究においては、初年度に電子機器利用による選挙システム研究会報告書において指摘された法的問題の整理と第一段階の電子投票導入に際して行われた法改正とその問題点について考察し、昨年度は期日前投票制度および改正特例法の審議を検討し、憲法・公選法で保護されるべき投票の秘密の範囲のまとめと、第三段階の電子投票に向けた法制度改定の試案をまとめた。

[1] 2005 年 5 末に配布予定

また、利用分野の研究に関しては、個人情報保護法制定前の医療における個人情報保護、個人情報保護法制定における個人情報のとりあつかいについて調査するとともに、医療分野、教育分野、行政分野に関していくつかの電子アンケートの可能性を検討した。

本年の報告書では、商法改正による株主総会議決電子投票制度創設後の議決権行使に関する問題の整理と、電子投票への示唆を行う。また、利用分野の検討としては、個人情報保護法が2005年4月から全面施行されるにあたり、各省から指針やガイドラインの制定や改版がなされ、アンケートなどの情報収集にあたり、個人情報に対して慎重な取扱が求められるようになったので、このまとめと、株主総会の電子投票制度と信用・金融分野、新しい分野としてSNSに関して研究の応用分野を検討する。

## 3-2-2 株主総会議決権電子化

### 3-2-2-1 株主総会における電子的議決権行使の法的性質をめぐる議論

平成13年11月28日の商法改正により、株式会社から株主に対しての株主総会開催通知等、株主からの株式会社への出欠等の通知や請求等の電子化、さらには株主総会会場を訪れないまま電子的に行う株主の議決権行使(商法の世界では、これを指して「電子投票」と呼んでいる。)といった、株主総会の電子化を実現するための法改正が実現した。

この電子投票をはじめとする、株主総会の電子化を進めるにあたって、商法学の観点から着目されたポイントは、「株主総会の会議体性」をめぐる議論であった。本稿は商法学上の株式会社の組織をめぐる議論を目的としたものではないので、以下その概略を記述するに留めるが、第2段階・第3段階の公職電子投票の実現においても、国や自治体と選挙民との関係性に着目してその是非を問う際に参考となる議論を含んでいるように思われる。

株主総会における議決権の行使は、資本多数決の観点から、株主は一株に対し一個の議決権を有することと定められている(商法第240条)。また、電子的な議決権行使の制度が導入される以前(昭和56年)から、総会に出席しない株主からの書面による議決権の行使の可否を、取締役会の裁量により決定できる旨の制度が整えられている(商法第239条ノ2)。このようないわば間接的な総会参加は、株主の総会に対するアクセス手段の拡充であって、株主の選択肢を増やすものとして積極的に評価されて制度化されてきた。一方で、「株主は直接会議体としての株主総会に参加し、対面で議案の説明を受けて質疑応答を行い、その上でなされた意思決定を議決権として行使するべき」であって、討論への参加をスキップして議決権の行使のみを許す書面投票は株主総会の形骸化を助長するもので望ましいものとはいえない、とする伝統的な株主総会観を持つ立場からの批判もみられる。この「争点について、会議の名にふさわしい討論・審議が株主総会の中では繰り広げられるべき」かどうかを問う論争を「株主総会の会議体性」の論争とよぶ。株主総会における不在者投票ともいいえる書面投票をめぐる上記の論争は、書面投票が制度化される前から、学界・実務界・議会を巻き込んで30年近く行われてきた。その成果は、電子投票の是非論にも妥当する。

このような意見の対立が起こる理由は、投票に参加する者(選挙人・株主)の投票すべき争点とその関連情報の認識方法が大きく異なっている所にある。株主総会では、審議過程への参加により充分な争点に関する情報を得た株主が、審議過程の締めくくりとして議決権行使を行うという一連の流れを重視する立場が書面・電子投票に対し批判的になる。一方公職選挙の投票は、争点(候補者)に関する情報の取得は個々の選挙人の関心に委ね、専ら候補者たる特定個人ないし得票政党の選抜に専従する。そのため投票日以前の選挙権者が選挙運動や政策討論といった争点の理解を促す場に参加しようがしまいが、選挙人の自由に委ねられる結果となる。

株主総会における議決権行使の対象は、総会での審議過程で提示された議題（争点）であり、その行使は複数ある争点のいずれかの優劣を判定する意思決定である。株主の議決権行使が、「争点に対する充分な理解に基づく意思表明」であることを重視する立場からは、総会の場に参加しないで議決権の行使のみを書面投票・電子投票のみで行うことは、上述のとおり本来的な株主総会の主旨を没却するものであって、望ましくないとされる。しかし、現実に行われている株主総会において、総株主の出席を必要条件とすることは求められておらず、委任状による議決権の間接的行使などの手法が用いられることは少なくない。株主総会において、議決権の行使にどのような意味づけを与えるか（投票者の争点に対する理解度が重要か否か、遠隔地からの投票行動は総会開催地に出席した株主の投票行動よりも軽いものか否か、委任状による議決権行使は望ましいか否か、等）は、各々の会社の組織文化に委ねられるべき問題であって、それは株主と経営者（取締役会）が最終的に決定すればよい問題であるとする「商法の私法性」[2]に基づく解釈が優勢となっている。これと同様に、株主総会の会議体性の主旨についても、抽象的に制度主旨を構築するのではなく、「商法の私法性」に着目し、当事者の私的自治に委ねるべきだと考えられるようになってきた。

### 3-2-2-2 株主総会における電子的議決権行使の問題点

この立場から、冒頭に述べた平成 13 年商法改正によって創設された、商法第239条ノ3では、取締役会の決議で電磁的方法により議決権の行使を可能とすることが出来る旨規定された(同第 1 項)。この条では更に、電子投票の利用株主に対して、招集通知・投票用紙に相当するものを電磁的方法により提供しなければならない(同第 3 項)としている。具体的には電子メール・磁気ディスク・光ディスク・携帯型メモリ媒体等が想定されるが、会社側の株主総会電子化のインセンティヴを考えると、少なくとも投票用紙に相当する電子的なデバイスとしては、会社が設置した株主総会用のサーバ上に立ち上げたウェブサイトにより議決権の行使を受け付けることが便宜であり、実際もこの方法が主流であろう。媒体を会社と株主との間で物理的に送り合うのでは、従来型の書面投票と比べてコストが低減しないからである。このウェブサイト上で提供しなければならない投票用紙に相当する議決権行使のためのウェブフォームの項目は、法務省の会社参考書類規則に定めがあり、次の3項目が掲げられている。

一、議案ごとの賛否の記載
二、取締役・監査役等の選任に関し、候補者ごとの賛否の記載
三、株主の氏名・議決件数・押印

このうち押印については電子署名または ID・パスワードの入力といった方法により、本人認証を行うことが出来るような機能をサイト上に設置し、置き換える必要があろう。

議決権行使の電子化に伴う問題として、議決権の二重行使が可能になる場合が挙げられる。株主総会の電子的議決権行使は、商法第232条第2項に基づき、電子的方法（e-mail 等）による招集通知を受け取る旨の意思表示を会社に対して行った株主に開かれるのが原則であるが、同法第239条ノ3第3項により、株主総会の招集通知が書面によって行われる株主も、総会会期の1週間前までに会社に対して電子的議決権行使を行いたき旨の請求を行えば、会社はそれを可能とすることを義務付けられている。このため、電子的議決権行使を希望する意思表示を会社に対して行った株主は、書面により送付された招集通知に添付された書面による議決権行使の用紙（投票用紙）を保持しながら、同時に電子的な議決権行使も可能な立場になるこ

[2] 商法の私法性とは、行政機関の監督などで、商法の「あるべき姿」「理想像」を押し付けるのではなく、可能な限り当事者間の合意によって自治的に何でも決めることが出来るようにするべきであるとする立場。規制よりも契約（その他の合意）で商事法関係を規律するべきとする。

とが想定される。この場合、議決権の行使として行われる意思表示として、2つの異なる意思表示が会社に到達した場合の取り扱いが問題となる。実務的には株主側の発信時点を基準とすることは不可能であろうから、会社到達時点の前後関係で決定するか、あらかじめ優先的に取り扱われる媒体を決定することで解決するかの2通りの方法が考えられる。いずれにせよ、これも会社と株主の私的自治により決定されるべき問題といえよう。また、事前の書面投票または電子投票による議決権行使のあった株主であっても、総会当日会場に足を運んで議決権の行使に及んだ場合は、当日の議決権行使が最終的なものとして取り扱われるべきことは当然であり、その範囲で、事前の書面投票または電子的議決権行使の内容は抹消されるような仕組みになっていなければならないと考えられる。

#### 3-2-2-3　公職電子投票との理論的相違と示唆

以上見てきたように、株主総会における議決権の行使（電子的なものを含む）は、資本多数決の原理、および私的自治から導き出される株主の議決権行使方法の選択権（といっても請求権的に解釈すべきではなく、会社が投票制度を設計する際に考慮すべき株主の利益と理解するべきであろう）がその基調となっている。これに対し、国や地方公共団体が実施する公職選挙が重視すべき基本的な価値は、立憲主義を支えるための普通・平等・秘密選挙権による多数決原理と、選挙制度の公平中立性である。したがって、株主総会の電子的議決権行使の際に株主が与えられる選択の幅は、公職電子投票にとって参考となる面もあるが、同時に投票の匿名性の維持や開票時のコスト増にもつながりかねず、慎重に取り扱うべき事項だといえる。

公職選挙における第2・第3段階の電子投票の導入に当たって、株主総会の電子議決権行使制度とその運用面で参考になると思われるのは、商法第239条ノ3が、招集通知・投票用紙及び投票の参考になる書類を、電子的議決権行使を求める株主に対して、同じく電子的方法により提供しなければならないとしている点にある。ネットワークを用いた公職選挙の電子投票については、本人認証を確実にし、また他の方法による投票と比較したメリットとデメリットを分かりやすく説明した情報を与えるために、電子投票の啓蒙情報（メリット・デメリットの告知および他の選挙人への委任の禁止等）の告知と本人認証の仕組（電子署名でも選挙人名簿番号 ID＆パスワードでも住民基本台帳カードでもバイオメトリクスでも良いのだが）および投票フォーム（またはそのURL）をセットにしたパッケージの交付を選管に義務付けるという方法に置き換えてみることが考えられよう。懸念されているなりすましを若干でも防ぐ方向にはたらくと考えられる。

また、二重投票対策の仕組も積極的に捉えることで、投票内容の投票本人による確認や、投票締切時間までの再投票を可能にする仕組みの構築の参考になるであろう。

現状、電子的議決権の行使は書面投票の一部として導入が進んでいる。次章で検討するように議決権行使の電子投票化はますます進むであろうし、その中で公職選挙における電子投票の導入に対するさまざまな示唆が得られることになると考えられる。

なお、現在、会社法制の現代語化、株式会社と有限会社の一体化、機関設計の柔軟化、最低資本金規制の撤廃、定款自治の範囲の拡大、等の改正を含む「会社法」と「会社法の施行に伴う関係法律の整備等に関する法律案」が第 162 回国会に提出され、審議されている[3]。

[3] 2005 年 5 月衆議院を修正通過し、参議院付託

平成 17 年 2 月 9 日に法制審議会から提出された「会社法制の現代化に関する要綱」において「電子投票」と記載されていた項目は、「会社法」では下記の記載になっている。

| |
|---|
| 第四章　機関<br>第一節　株主総会及び種類株主総会<br>第一款　株主総会 |
| （電磁的方法による議決権の行使）<br>第三百十二条　電磁的方法による議決権の行使は、政令で定めるところにより、株式会社の承諾を得て、法務省令で定める時までに議決権行使書面に記載すべき事項を、電磁的方法により当該株式会社に提供して行う。<br>2　株主が第二百九十九条第三項の承諾をした者である場合には、株式会社は、正当な理由がなければ、前項の承諾をすることを拒んではならない。<br>3　第一項の規定により電磁的方法によって行使した議決権の数は、出席した株主の議決権の数に算入する。<br>4　株式会社は、株主総会の日から三箇月間、第一項の規定により提供された事項を記録した電磁的記録をその本店に備え置かなければならない。<br>5　株主は、株式会社の営業時間内は、いつでも、前項の電磁的記録に記録された事項を法務省令で定める方法により表示したものの閲覧又は謄写の請求をすることができる。 |
| 第八款　債権者集会 |
| （電磁的方法による議決権の行使）<br>第五百五十七条　電磁的方法による議決権の行使は、政令で定めるところにより、招集者の承諾を得て、法務省令で定める時までに議決権行使書面に記載すべき事項を、電磁的方法により当該招集者に提供して行う。<br><br>2　協定債権者が第五百四十九条第二項の承諾をした者である場合には、招集者は、正当な理由がなければ、前項の承諾をすることを拒んではならない。<br>3　第一項の規定により電磁的方法によって議決権を行使した議決権者は、第五百五十四条第一項及び第五百六十七条第一項の規定の適用については、債権者集会に出席したものとみなす。 |
| 参考<br>（株主総会の招集の通知）<br>第二百九十九条　株主総会を招集するには、取締役は、株主総会の日の二週間（前条第一項第三号又は第四号に掲げる事項を定めたときを除き、公開会社でない株式会社にあっては、一週間（当該株式会社が取締役会設置会社以外の株式会社である場合において、これを下回る期間を定款で定めた場合にあっては、その期間））前までに、株主に対してその通知を発しなければならない。<br>2　次に掲げる場合には、前項の通知は、書面でしなければならない。<br>一　前条第一項第三号又は第四号に掲げる事項を定めた場合<br>二　株式会社が取締役会設置会社である場合<br>3　取締役は、前項の書面による通知の発出に代えて、政令で定めるところにより、株主の承諾を得て、電磁的方法により通知を発することができる。この場合において、当該取締役は、同項の書面による通知を発したものとみなす。<br>4　前二項の通知には、前条第一項各号に掲げる事項を記載し、又は記録しなければならない。 |

なお、「会社法の施行に伴う関係法律の整備等に関する法律案」では下記の電磁的方法による議決権の行使が定められている。

| |
|---|
| 第四節　機関<br>第一款　投資主総会 |
| （電磁的方法による議決権の行使）<br><br>第九十二条の二　電磁的方法による議決権の行使は、政令で定めるところにより、投資法人の承諾を得て、内閣府令で定める時までに議決権行使書面に記載すべき事項を、電磁的方法により当該投資法人に提供して行う。<br><br>2　投資主が第九十一条第二項の承諾をした者である場合には、投資法人は、正当な理由がなければ、前項の承諾をすることを拒んではならない。<br><br>3　第一項の規定により電磁的方法によつて行使した議決権の数は、出席した投資主の議決権の数に算入する。<br><br>4　投資法人は、投資主総会の日から三月間、第一項の規定により提供された事項を記録した電磁的記録をその本店に備え置かなければならない。<br><br>5　投資主は、投資法人の営業時間内は、いつでも、前項の電磁的記録に記録された事項を内閣府令で定める方法により表示したものの閲覧又は謄写の請求をすることができる。 |

## 3-2-3 電磁的議決権行使の実態

### 3-2-3-1 株主総会における電子投票

商法改正により平成 14 年度から開始されたインターネットを使用した議決権の行使は、2003 年度では上場企業の1割近くがパソコン経由で実施し、株主の投票者数も初年度から 2 倍に増えたという。

また、平成 16 年度は携帯電話をインターネットにつないで投票するシステムが中央三井信託銀行とUFJ信託銀行により開発され、6 月時点で 14 社が同システムを採用、うち NTT ドコモは議決権を行使した人の0.8%にあたる 774 人が利用したという。

2004 年の株主総会白書によると、株主総会の議決権行使について電磁的方法によるものを採用したと回答した会社は 211 社(回答会社全体の 11.0%、前年調査比 3.8 ポイント増)で、次回総会での採用予定も107 社となっており、着実に増加している。

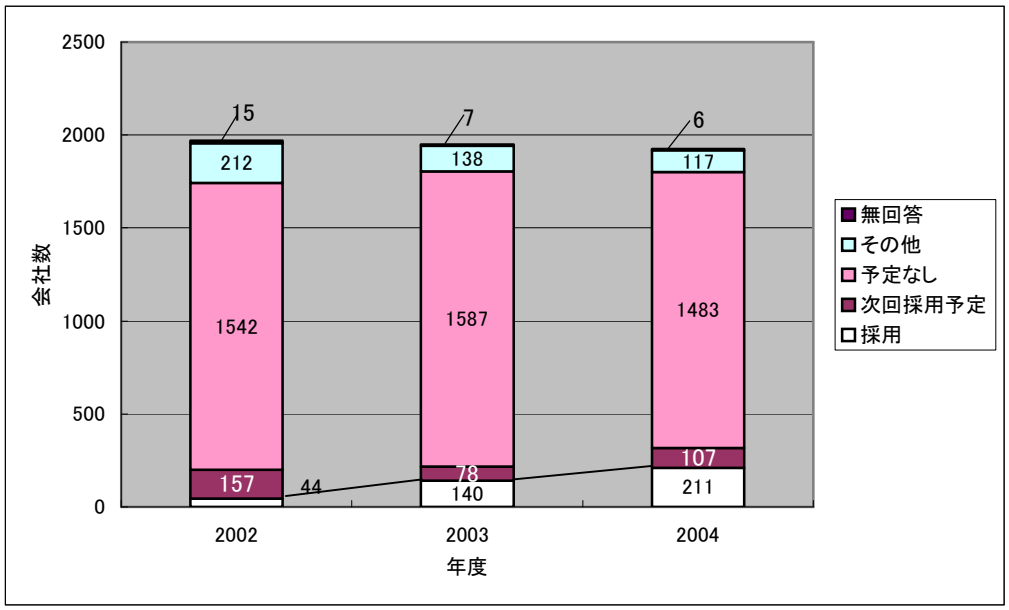



**図 7 電磁的方法による議決権行使の採用**[4]

電磁的議決権の行使は、株主が時間を気にせず投票でき、企業の側では株主の投票手段を増やすことにより、定足数の確保がしやすくなるというメリットがある。

日本では株式の相互持合いの解消に伴い、安定株主比率が低下し、機関化と国際化が進んできている(図2、図3)。こうした中、東京証券取引所と日本証券業協会は「機関投資家向け議決権電子行使プラットフォーム」の構築を進めている。当初は 2005 年 2 月決算銘柄からのサービス開始予定であったが、システム仕様の確定遅れから、2005 年 12 月期決算銘柄からサービスの本格的稼動を目指すようになった。

4 株主総会白書 2002 年度版、2003 年度版、2004 年度版から作成

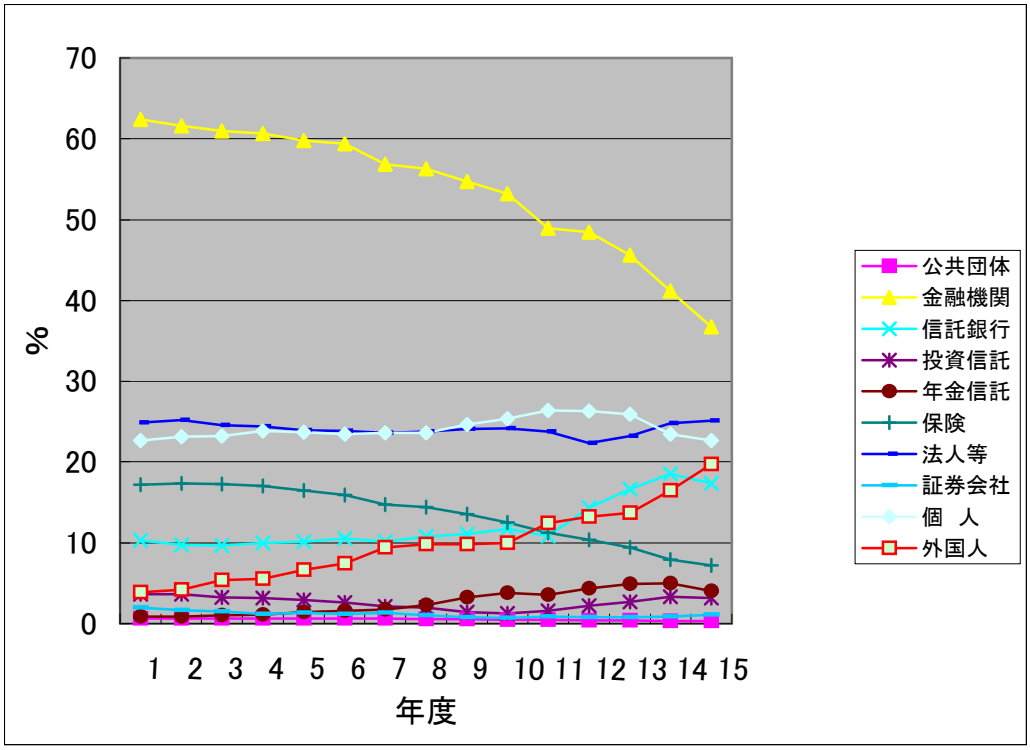



図 8 株主分布[5]

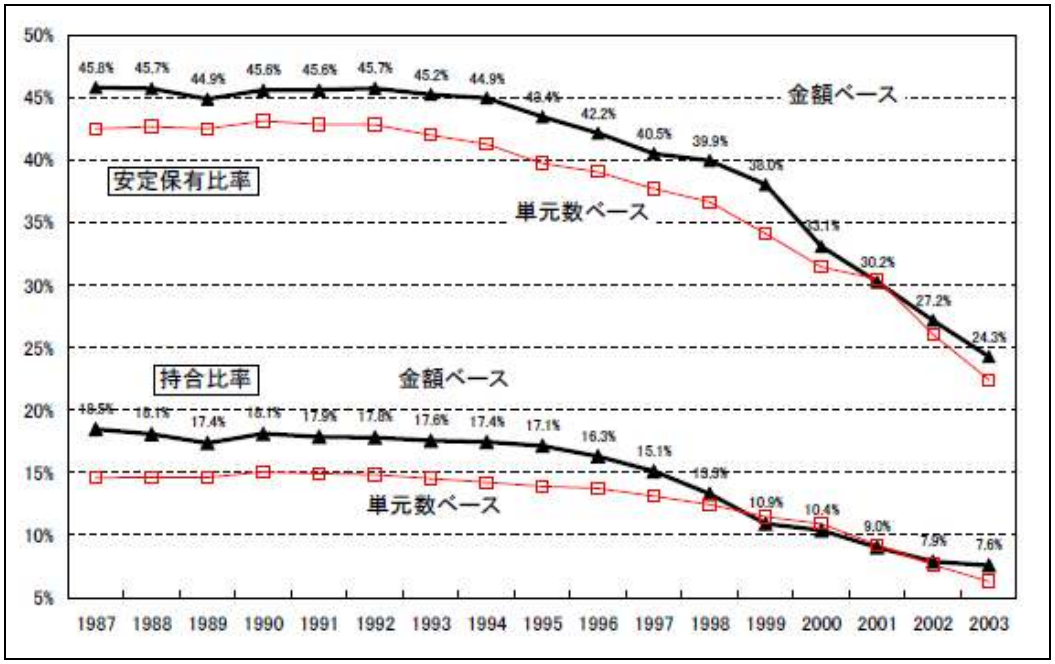



図 9 株式持合い状況調査(2003 年度版)[6]

5 「平成１５ 年度株式分布状況調査の調査結果について（全国証券取引所)」から作成
6 「株式持合い状況調査(2003 年度版)」 ニッセイ基礎研究所 より引用

### 3-2-3-2 機関投資家、外国人投資家の増加による議決権行使

日本では厚生年金基金連合会が 2003 年 2 月に「厚生年金基金連合会　株主議決権行使基準」を策定し、コーポレートガバナンス原則と具体的な行使基準を定めている。地方公務員共済組合連合会も 2004 年 4 月にコーポレートガバナンス原則と株主議決権行使ガイドラインを制定しており、今後、機関投資家による議決権行使の積極化に伴い、電子的議決権行使が本格化することが考えられる。2005 年 2 月に、厚生年金基金連合会と日本証券投資顧問業協会は、東京証券取引所・大阪証券取引所・ジャスダック証券取引所に対し、各取引所の上場企業へ、効率的・円滑な議決権行使のためのインフラ整備に向けた取組みを働きかけるよう「株主議決権行使に関するインフラ整備に向けた取組みへの要望書」を提出しており、この中には「機関投資家向け議決権電子行使プラットフォーム」への関係各社の協力を求める取組みを望む記述が含まれている。

なお、アメリカでは、株主が株式総会で議決権を行使する際、無記名投票制度が一般的であるという。TIAA-CREF[7]の議決権行使ガイドラインでは 1 株1票の原則とともに「議決権行使の際には、匿名性が確保されなければならない」としている。UFJ 総合研究所が 2004 年に外資系を含む本邦投資家に対して行った日本株式の議決権行使方針のアンケートでも、自由意見欄に「無記名投票制度導入」を望む声があったとしており、株式市場のグローバル化と民主化とを合わせて検討すべき課題であろう。（日本の株主議決権行使ガイドラインでは、議決権行使における匿名性は特に求めていない）

### 3-2-3-3 株主総会当日における電子投票

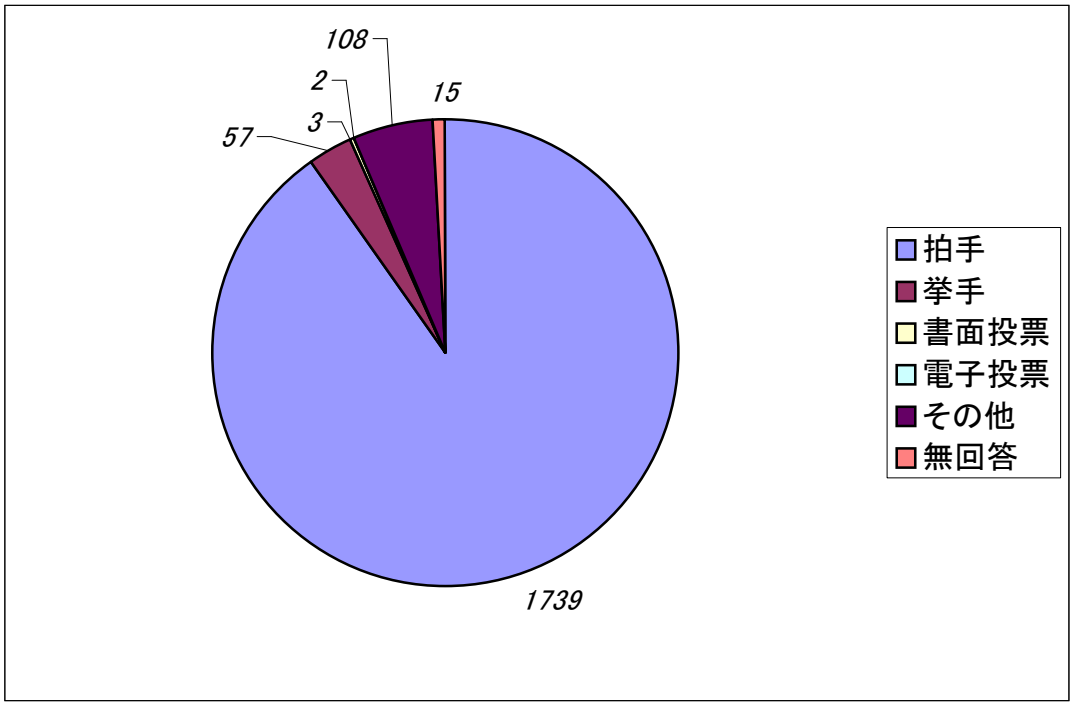
株式の相互持合いの解消に伴い、安定株主比率が低下し、総会前日までに各議案の定足数の充足や可決・否決が判明しないケースが増えてくると、総会当日に株主の同一性や保有議決権個数、賛否棄権の確認が必要になる。

2004 年度版株主総会白書によると、議場での採決方法は、拍手がほとんどであるが、書面投票は 3 社、電子投票も 2 社あった。その他に関しては「異議なし」や「賛成」「反対」などの発声、起立などによるものであり、簡易な採決方法をとっている。

今後テレビ会議などの仮想株式総会における議決権行使が認められるようになれば、電子投票もシステムとして必要になると考えられる。この場合、株主総会で、会社側からの働きかけを防いだり、経営者に対する責任追及や退職慰労金の支払い中止議題などに対し小額の社員株主が無記名投票でないために投票を棄権するというケースを防ぐためにも、無記名での投票システムが望ましい。議決権行使の匿名性をあげている TIAA-CREF は、企業経営者からの圧力が懸念されること、議案の表現を問題としているか内容を問題にしているかを明確にしないと行使結果に対する誤解が生じることなどをあげ、議決権行使内容の開示を拒否している。

---

[7] TIAA-CREF（Teachers Insurance Annuity Association . College Retirement Equities Fund）教職員保険年金協会大学退職株式基金　高等教育に携わる教職員向けの年金ファンドで、投資している企業に対して、コーポレート・ガバナンスに関する独自の基本指針“TIAA-CREF Policy Statement on Corporate Governance”を策定している。




（株主総会白書 2004 に基づきグラフ化）

**図 10 議場での採決方法**

### 3-2-3-4 株主総会以外の電磁的議決権行使

以上、株主総会での電子的議決権行使の実体と今後の展望について検討した。株主総会以外でも法的に電磁的な議決権行使を可能とした分野があるので、これについて簡単にまとめる。

(1)組合

IT 書面一括法（書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律 平成 12 年）は書面の交付や書面による手続きを義務付けている法律を改正し、電子メールなどの電子的手段も認めることで電子商取引の促進を狙い、中小企業等協同組合法など 50 本の法律を対象とした法律である。本法により、電磁的方法による議決権行使を可能としている。以下に組合員が電磁的方法により議決権を行使可能としている法律を示す。

**表 2 組合員が電磁的方法により議決権を行使可能としている法律**

| | |
|---|---|
| 財務省関係 | たばこ耕作組合法 |
| 厚生労働省関係 | 消費生活協同組合法 |
| | 生活衛生関係営業の運営の適正化及び振興に関する法律 |
| 農林水産省関係 | 農業災害補償法 |
| | 水産業協同組合法 |
| | 農業委員会等に関する法律 |
| | 漁船損害等補償法 |
| | 農業信用保証保険法 |
| | 漁業災害補償法 |
| | 森林組合法 |
| | 持続的養殖生産確保法(※) |
| 経済産業省関係 | 中小企業等協同組合法 |
| | 商工会議所法 |
| | 商工会法 |
| | 商店街振興組合法 |

※ 水産業協同組合法の電磁的方法による議決権行使を定款で定めている場合に、書面による同意を電磁的方法に代えることができる

(2)不動産

平成14年度の「区分所有法」改正により、電磁的記録による議事録作成や電磁的方法による決議が可能となり、平成16年1月には国土交通省により改訂された「中高層共同住宅標準管理規約」に「電磁的方法による議決権行使」が盛り込まれた。平成16年8月には電磁的方法による議決権行使を可能とした『マンションポータル イントラネッツ』を「イントラネッツ株式会社」と「コスモスライフ」が共同開発し販売開始している。

(3) その他総会議決権行使

政府は 2005 年 2 月 24 日に「IT 政策パッケージ 2005」を策定した。その中の「電子商取引」において、「(1)事業活動においてITの利用を阻害する残された課題への取組(内閣官房及び関係府省)」として、議決権に関する記載がある。

- 民法・中間法人及び NPO 法人の総会議決権行使等を電子的方法でも可能とするため、2005 年度末までに法制上の措置を講じる(内閣府及び法務省)。
- 信用金庫において電子的方法による総会議決権行使を可能とするため、2005 年度末までに法制上の措置を講じる(金融庁)。

このような議決権行使の場において電子投票のシステムが活用できると考えられる。

## 3-2-4 個人情報保護法

個人情報保護法が 2005 年 4 月から完全実施されるにあたり、「個人情報の保護に関する法律」（平成15年法律第57号）、「個人情報の保護に関する法律施行令」（平成15年政令第507号）及び「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）を受け、2004 年には各種指針等が政府から出された。セミナーが数多く設けられ、企業もいろいろな取組みを行っている。

次ページにガイドラインなどをまとめる。

## 表 3 個人情報保護法に関連するガイドライン等

| 分野 | | 所管省庁 | 先に定められていたガイドライン | ガイドライン等 | その他 |
|---|---|---|---|---|---|
| 医療 | 医療一般 | 厚生労働省 | 診療情報の提供等に関する指針 | 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」(12 月 24 日) | |
| | | | | 健康保険組合等における個人情報の適切な取扱いのためのガイドライン(12 月 27 日) | |
| | 研究 | 文部科学省・厚生労働省・経済産業省 | ・ヒトゲノム・遺伝子解析研究に関する倫理指針(平成 13 年 3 月) | ヒトゲノム・遺伝子解析研究に関する倫理指針(12 月 28 日全部改正) | |
| | | | ・遺伝子治療臨床研究に関する指針 (平成 14 年 3 月) | 遺伝子治療臨床研究に関する指針 (12 月 28 日全部改正) | |
| | | | ・疫学研究に関する倫理指針 (平成 14 年 6 月) | 疫学研究に関する倫理指針 (12 月 28 日全部改正) | |
| | | | ・臨床研究に関する倫理指針 (平成 15 年 7 月) | 臨床研究に関する倫理指針 (12 月 28 日全部改正) | |
| 金融・信用 | 金融 | 金融庁 | ― | 「金融分野における個人情報保護に関するガイドライン」 | 個人情報の保護と利用に関する自主ルール(全国銀行協会) |
| | | | | 金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針(告示) | 生命保険業における個人情報保護 のための取扱指針について(生命保険協会) |
| | | | | | 損害保険会社に係る個人情報保護指針について (日本損害保険協会) |
| | | | | | 生命保険業における個人情報保護のための安全管理措置等についての実務指針 (生保安全管理実務指針) (生命保険協会) |
| | 信用 | 経済産業省 | ― | 「経済産業分野のうち信用分野における個人情報保護ガイドライン」 | 全国銀行個人信用情報センターにおける個人情報保護指針 (全国銀行個人信用情報センター) |
| 情報通信 | 電気通信 | 総務省 | 電気通信事業における個人情報保護に関するガイドライン(平成 10 年 12 月) | 「電気通信事業における個人情報保護に関するガイドライン」 | |
| | 放送 | 総務省 | ・放送における視聴者の加入者個人情報の保護に関するガイドライン(平成 8 年 9 月) | 「放送受信者等の個人情報の保護に関する指針」 | |
| | | | ・通信衛星によるデジタル放送に係る有料放送役務標準契約約款(平成 9 年 11 月) | | |
| | | | ・衛星放送におけるプラットフォーム事業者の業務に係るガイドラインに関する指針(平成 15 年 4 月) | | |

| | | | | | |
|---|---|---|---|---|---|
| 事業全般 | | 経済産業省 | 民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン（平成 9 年 3 月） | 「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」 | 民間部門における電子商取引に係る個人情報の保護に関するガイドライン Ver.3.0<br>（電子商取引推進協議会（ECOM））<br>通信販売における個人情報保護ガイドライン(社団法人日本通信販売協会)<br>テレマーケティングにおける個人情報保護ガイドライン社団法人（日本テレマーケティング協会）<br>電子ネットワーク運営における「個人情報保護に関するガイドライン」（改訂第2版） |
| | | | | 「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」 | |
| 雇用管理 | 一般 | 厚生労働省 | 労働者の個人情報保護に関する行動指針（平成 12 年 12 月） | 「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」 | |
| | | | | 「雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項」※雇用管理における健康情報の取扱いについての留意事項をまとめたもの | |
| | 船員 | 国土交通省 | — | 「船員の雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」 | |
| 警察 | | 警察庁 | — | 「国家公安委員会が所管する事業を行う者等が講ずべき個人情報の保護のための措置に関する指針」 | |
| | | | | 警察共済組合が講ずべき個人情報の保護のための措置に関する指針について（局長通達） | |
| 法務 | | 法務省 | — | 「法務省が所管する分野における事業者等が取り扱う個人情報の保護に関するガイドライン」 | |
| | | | | 「債権管理回収業分野における個人情報の保護に関するガイドライン」 | |
| 外務 | | 外務省 | | 外務省が所管する事業を行う事業者等が取り扱う個人情報の保護に関するガイドライン（告示） | |
| 財務 | | 財務省 | — | 「財務省所管分野における事業者が講ずべき個人情報の保護に関する指針 | |
| 教育 | | 文部科学省 | — | 「学校における生徒等に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針」 | |
| 福祉 | | 厚生労働省 | — | 「福祉関係事業者における個人情報の適正な取扱いのためのガイドライン」 | |

| | | | | |
|---|---|---|---|---|
| 職業紹介等 | 厚生労働省 | ・職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針（平成 11 年） | 「職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針の一部を改正する告示」（厚生労働省告示第 391 号） | |
| 労働者派遣 | 厚生労働省 | ・派遣元事業主が講ずべき措置に関する指針（平成 11 年） | 「派遣元事業主が講ずべき措置に関する指針の一部を改正する告示」 | |
| 労働組合 | 厚生労働省 | | 個人情報の適正な取扱いを確保するために労働組合が講ずべき措置に関する指針（告示） | |
| 国土交通 | 国土交通省 | ― | 「国土交通省所管分野における個人情報保護に関するガイドライン」 | |
| 農林水産 | 農林水産省 | ― | 「個人情報の適正な取扱いを確保するために農林水産分野における事業者が講ずべき措置に関するガイドライン」 | |

http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

「個人情報の保護に係る関係省庁の検討状況」を元に作成

### 3-2-4-1 医療分野

昨年度報告書において、厚生省が個別法案の検討を行っていると述べたが、その後個別法は制定せず、ガイドラインの策定を行うこととなった(表 3 個人情報保護法に関連するガイドライン等 参照)。

医療分野で定められたガイドラインでは、匿名化を明示しており、個人情報のデータ管理、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電子投票に類する処理として本研究の成果を反映させることができると考えられる。そこで、ガイドラインおよび指針に現れる匿名化を中心としてここに示す。

| 医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン | |
|---|---|
| http://www.mhlw.go.jp/houdou/2004/12/dl/h1227-6a.pdf | 2004 年 12 月 24 日 |
| ・個人情報が研究に活用される場合、法による義務等の規定は適用されず、ガイドラインも適用外(医学研究分野の関連指針※を参照するが、本ガイドラインも留意のこと)<br>・治験及び市販後臨床試験における個人情報の取扱い<br>本ガイドラインのほか、薬事法及び関係法令(「医薬品の臨床試験の実施の基準に関する省令」(平成9年厚生省令第28号)等)の規定や、関係団体等が定める指針に従う<br>・医療機関等が企業から研究を受託して又は共同で実施する場合における個人情報の取扱い<br>本ガイドラインのほか、医学研究分野の関連指針や、関係団体等が定める指針に従うものとする。<br>・遺伝情報を診療に活用する場合の取扱い<br>遺伝学的検査等により得られた遺伝情報の取扱いについては、UNESCO 国際宣言等※※や医学研究分野の関連指針及び関係団体等が定める指針を参考とし、特に留意する必要がある | |
| 健康保険組合等における個人情報の適切な取扱いのためのガイドライン | |
| http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/kenkou.pdf | 2004 年 12 月 27 日 |
| ・政府管掌健康保険を管掌する国(社会保険庁)や市町村国民健康保険を運営する市町村等については個人情報の保護に関する法律が適用されず、他の法律や条令が適用されるため、ガイドラインの対象ではない<br>・個人情報取扱事業者としての法令上の義務を負う健保組合等に限らず、その規模等にかかわらず健保組合等を対象とする | |

※医学研究分野における関連指針[8]

| | |
|---|---|
| 「ヒトゲノム・遺伝子解析研究に関する倫理指針」 | 平成13年3月29日文部科学省・厚生労働省・経済産業省告示第1号 |
| 「遺伝子治療臨床研究に関する指針」 | 平成14年3月27日文部科学省・厚生労働省告示第1号 |
| 「疫学研究に関する倫理指針」 | 平成14年6月17日文部科学省・厚生労働省告示第2号 |
| 「臨床研究に関する倫理指針」 | 平成15年7月30日厚生労働省告示第255号 |

なお、上記指針は全て平成 16 年 12 月に改正されている。

※※UNESCO 国際宣言[9]

| | |
|---|---|
| 「ヒト遺伝情報に関する国際宣言」 | UNESCO October 16, 2003 |
| 「遺伝学的検査に関するガイドライン」 | 平成15年8月 遺伝医学関連10学会 |

8 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」別表 5

9 「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」別表 6

法律上は特に匿名化に関する記載は無いが、本ガイドラインでは、匿名化について、下記の項目で定めている。

(1)医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン

| | | |
|---|---|---|
| P6 | Ⅱ 用語の定義等<br>1．個人情報（法第２条第１項） | (例)下記については、記載された氏名、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ことから、**匿名化されたものを除き、**個人情報に該当する。(医療・介護関係法令において医療・介護関係事業者に作成・保存が義務づけられている記録例は別表1参照) |
| P6 | 2. 個人情報の**匿名化** | **当該個人情報から、当該情報に含まれる氏名、生年月日、住所等、個人を識別する情報を取り除くことで、特定の個人を識別できないようにすることをいう。**顔写真については、一般的には目の部分にマスキングすることで特定の個人を識別できないと考えられる。なお、必要な場合には、その人と関わりのない符号又は番号を付すこともある。<br>このような処理を行っても、事業者内で医療・介護関係個人情報を利用する場合は、事業者内で得られる他の情報や匿名化に際して付された符号又は番号と個人情報との対 応表等と照合することで特定の患者・利用者等が識別されることも考えられる。法においては、「他の情報と容易に照合することができ、それ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」についても個人情報に含まれるものとされており、**匿名化に当たって**は、当該情報の利用目的や利用者等を勘案した処理を行う必要があり、あわせて、本人の同意を得るなどの対応も考慮する必要がある。<br>また、特定の患者・利用者の症例や事例を学会で発表したり、学会誌で報告したりする場合等は、氏名、生年月日、住所等を消去することで匿名化されると考えられるが、症例や事例により十分な**匿名化が困難な場合**は、本人の同意を得なければならない。<br>なお、当該発表等が研究の一環として行われる場合にはⅠ9. に示す取扱いによるものとする。 |
| P13 | 【法の規定により遵守すべき事項等】 | 医療・介護関係事業者は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。なお、本人の同意を得るために個人情報を利用すること(同意を得るために患者・利用者の連絡先を利用して電話をかける場合など)、個人情報を**匿名化**するために個人情報に加工を行うことは差し支えない。 |
| P25 | ②同一事業者内における情報提供であり、第三者に該当しない場合 | このうち、医療・介護関係事業者内部の研修で診療録や介護関係記録等を利用する場合には、具体的な利用方法を含め、あらためて本人の同意を得るか、個人が特定されないよう**匿名化する**。 |
| P25 | (5)その他留意事項 | ・他の事業者への情報提供に関する留意事項<br>第三者提供を行う場合のほか、他の事業者への情報提供であっても、①法令に基づく場合など第三者提供の例外に該当する場合、②「第三者」に該当しない場合、③個人が特定されないように匿名化して情報提供する場合などにおいては、本来必要とされる情報の範囲に限って提供すべきであり、情報提供する上で必要とされていない事項についてまで他の事業者に提供することがないようにすべきである。<br>特に、医療事故等に関する情報提供に当たっては、患者・利用者及び家族等の意思を踏まえ、報告において氏名等が必要とされる場合を除き匿 |

| | | |
|---|---|---|
| | | 名化（Ⅱ2. 参照）を行う。また、医療事故発生直後にマスコミへの公表を行う場合等については、匿名化する場合であっても本人又は家族等の同意を得るよう努めるものとする。 |

(2)健康保険組合等における個人情報の適切な取扱いのためのガイドライン

| | | |
|---|---|---|
| P4 | Ⅱ 用語の定義<br>1. 個人情報（法第2条第1項） | ※ 記載された氏名、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は、匿名化されたものを除き、個人情報に該当する。 |
| P4 | 2. **個人情報の匿名化** | **当該個人情報から、当該情報に含まれる氏名、生年月日、住所等、個人を識別する情報を取り除くことで、特定の個人を識別できないようにすること**をいう。顔写真については、一般的には目の部分にマスキングすることで特定の個人を識別できないと考えられる。なお、必要な場合には、その人と関わりのない符号又は番号を付すこともある。<br>このような処理を行っても、健保組合等内で個人情報を利用する場合は、健保組合等内で得られる他の情報や匿名化に際して付された符号又は番号と個人情報との対応表等と照合することで特定の被保険者等が識別されることも考えられる。法においては、「他の情報と容易に照合することができ、それ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」についても個人情報に含まれるものとされており、**匿名化に当たって**は、当該情報の利用目的や利用者等を勘案した処理を行う必要があり、あわせて、本人の同意を得るなどの対応も考慮する必要がある。<br>また、特定の被保険者等の健診の結果や保健指導の事例を集団で行う保健指導で紹介したり、健保組合等の機関誌に掲載したりする場合等は、氏名、生年月日、住所等を消去することで匿名化されると考えられるが、健診の結果や保健指導の事例により十分な**匿名化が困難な場合**は本人の同意を得なければならない。 |
| P8 | 【法の規定により遵守すべき事項等】 | 健保組合等は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。なお、本人の同意を得るために個人情報を利用すること（同意を得るために被保険者等の連絡先を利用して電話をかける場合など）、個人情報を匿名化するために個人情報に加工を行うことは差し支えない。 |
| P15 | ②業務を委託する場合の留意事項 | ・なお、個人情報保護の観点から、可能な限り、個人情報をマスキングすることにより、当該個人情報を匿名化した上で、委託するよう努めること。 |
| P15 | ③業務を再委託する場合の留意事項 | なお、個人情報を含む業務の再委託や個人情報に関する処理の再委託をする場合には、個人情報保護の観点から、可能な限り、個人情報をマスキングすることにより、当該個人情報を匿名化した上で、委託先から再委託先へ個人情報が提供されないよう努めること。 |
| P21 | ②同一事業者内における情報提供であり、第三者に該当しない場合 | このうち、健保組合等内部の研修でレセプトや健診記録等を利用する場合には、具体的な利用方法を含め、あらためて本人の同意を得るか、個人が特定されないよう匿名化する。 |
| P21 | (5)その他留意事項 | 他の事業者への情報提供に関する留意事項<br>第三者提供を行う場合のほか、他の事業者への情報提供であっても、①法令に |

| | | |
|---|---|---|
| | | 基づく場合など第三者提供の例外に該当する場合、②「第三者」に該当しない場合、③個人が特定されないように匿名化して情報提供する場合などにおいては、本来必要とされる情報の範囲に限って提供すべきであり、情報提供する上で必要とされていない事項についてまで他の事業者に提供することがないようにすべきである。<br>また、被保険者等と医師等双方の二面性を持っている個人情報を第三者提供するに当たっては、双方の同意が必要となるが、一方の同意のみで第三者提供する場合は、他方の個人情報に係る部分をマスキングした上で行うこと。 |

個人情報の匿名化に関しては、いずれも「情報を取り除く」ことを明示しており、研究分野における暗号化に該当する記載は無い。

「ヒトゲノム・遺伝子解析研究に関する倫理指針」と「疫学研究に関する倫理指針」において、連結可能匿名化と連結不可能匿名化が定義されている。「遺伝子治療臨床研究に関する指針」「臨床研究に関する倫理指針」に関しては特に匿名化に関する記載はない。

(3) ヒトゲノム・遺伝子解析研究に関する倫理指針

| 頁 | 箇所 | 内容 |
|---|---|---|
| 6 | 3 保護すべき個人情報 | (2)個人情報を連結不可能匿名化した情報は、個人情報に該当しない。個情報を**連結可能匿名化**した情報は、研究を行う機関において、当該個人情報に係る個人と当該情報とを連結し得るよう新たに付された符号又番号等の対応表を保有していない場合は、個人情報に該当しない。 |
| 6 | | ＜**連結可能匿名化**された情報の取扱いに関する細則＞<br>**連結可能匿名化**された情報を同一法人又は行政機関内の研究部門において取り扱う場合には、当該研究部門について、研究部門以外で匿名化が行われ、かつ、その匿名化情報の対応表が厳密に管理されていること等の事情を勘案して適切な措置を定めるなど、当該機関全体として十分な安全管理が確保されるよう、安全管理措置を定めることができる。 |
| 11 | 6 研究を行う機関の長の責務 | (5)研究を行う機関の長は、個人情報に該当しない匿名化された情報を取り扱う場合は、当該情報を適切に管理することの重要性の研究者等への周知徹底、当該情報の管理(事故等の対応を含む。)、責任の明確化、研究者等以外の者による当該情報の取扱いの防止等、適切な措置を講じなければならない。 |
| 11 | | ＜匿名化した情報の取扱いに関する細則＞個人情報に該当しない匿名化された情報を取り扱う場合には、**連結可能**と**連結不可能**の区別に留意し、適切な措置を講じることとする。 |
| 11 | | (6)研究を行う機関の長は、ヒトゲノム・遺伝子解析研究の業務に係る情報の取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人情報の安全管理及び個人情報に該当しない**匿名化**された情報の適切な取扱いが図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。 |

| | | |
|---|---|---|
| 12 | | (10)研究を行う機関の長は、国内において共同研究を実施する場合は、それぞれの研究を行う機関に設置された倫理審査委員会において、他の共同研究機関における研究計画の承認の状況、インフォームド・コンセントの状況、**匿名化**の状況等を示した上で研究計画の承認を得なければならない。<br>ただし、複数の機関が参画する共同研究において、主たる研究を行う機関が研究全体の推進及び管理を担う場合は、当該主たる研究を行う機関においては、当該機関に設置された倫理審査委員会が研究計画全体について審査を行い、他の共同研究機関においては、第2の9(5)に従い、研究計画の実施について迅速審査を行うことができる。 |
| 18 | | (34)試料等の提供が行われる機関の長は、試料等を外部の機関に提供する際には、原則として試料等を**匿名化**しなければならない。<br>また、試料等の提供が行われる機関内のヒトゲノム・遺伝子解析研究を行う研究部門(以下「試料等の提供が行われる機関における研究部門」という。)に試料等を提供する際にも、原則として**匿名化**しなければならない。 |
| 18 | | ただし、次に掲げる要件のすべてを満たしている場合には**匿名化せず**に試料等を提供することができる。<br>ア提供者又は代諾者等が、匿名化を行わずに外部の機関又は試料等の提供が行われる機関における研究部門に提供することに同意していること。<br>イ倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において、**匿名化を行わ**ずに、外部の機関又は試料等の提供が行われる機関における研究部門に提供することが認められていること。 |
| 20 | ＜研究計画書に記載すべき事項に関する細則＞ | 研究計画書に記載すべき事項は、一般的に以下のとおりとするが、研究内容に応じて変更できる。 |
| | | ・研究の意義、目的、方法(対象とする疾患、分析方法等。将来の追加、変更が予想される場合はその旨。単一遺伝子疾患等の場合には研究の必要性、不利益を防止するための措置等の特記事項等。)、期間、予測される結果及び危険、個人情報の保護の方法(**匿名化しない場合**の取扱いを含む。) |
| | | ・試料等又は遺伝情報を外部の機関に提供する場合や研究の一部を委託する場合の**匿名化の方法**等の事項(契約の内容を含む。) |
| | | ・ヒト細胞・遺伝子・組織バンクに試料等を提供する場合には、バンク名、**匿名化の方法等** |
| | | ・試料等の廃棄方法及びその際の**匿名化の方法** |
| 20 | 7 研究責任者の責務<br>(5)<報告事項に関する細則> | 研究責任者が研究を行う機関の長に対して行う研究の実施状況の定期報告事項は、一般的に以下のと<br>おりとするが、研究内容に応じて変更できる。<br>・提供された試料等の数、試料等の保管の方法<br>・外部の機関への試料等又は遺伝情報の提供数、提供理由<br>・ヒトゲノム・遺伝子解析研究が実施された試料等の数<br>・研究結果、研究の進捗状況<br>・問題の発生の有無<br>・試料等の提供が行われる機関にあっては、上記のほか、**匿名化を行った試料等**の数 |

| | | |
|---|---|---|
| 21 | (7) | (7)研究責任者は、原則として、**匿名化**された試料等又は遺伝情報を用いて、ヒトゲノム・遺伝子解析研究を実施しなければならない。<br>ただし、提供者又は代諾者等が同意し、かつ、倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において認められている場合には、試料等又は遺伝情報の匿名化を行わないことができる。 |
| 21 | (8) | (8)研究責任者は、**匿名化されていない試料等又は遺伝情報**を原則として外部の機関に提供してはならない。<br>ただし、提供者又は代諾者等が**匿名化**を行わずに外部の機関へ提供することに同意し、かつ、倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において認められている場合には、**匿名化されていない試料等又は遺伝情報**を外部の機関へ提供することができる。 |
| 21 | (10) | (10)研究責任者は、ヒトゲノム・遺伝子解析研究の業務の一部を委託する場合において、試料等又は遺伝情報を受託者に提供する際は、原則として**試料等又は遺伝情報を匿名化**しなければならない。<br>ただし、提供者又は代諾者等が同意し、かつ、倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において認められている場合には、匿名化せずに試料等又は遺伝情報を提供することができる。 |
| 22 | 8 個人情報管理者の責務 | (1) 個人情報管理者分担管理者を含む。以下第2の8において同じ。)は、原則として、研究計画書に基づき、研究責任者からの依頼により、ヒトゲノム・遺伝子解析研究の実施前に**試料等又は遺伝情報を匿名化**しなければならない。<br>ただし、提供者又は代諾者等が同意し、かつ、倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において認められている場合には、試料等又は遺伝情報の匿名化を行わないことができる。 |
| 22 | | (2)個人情報管理者は、**匿名化**の際に取り除かれた個人情報を、原則として外部の機関及び試料等の提供が行われる機関における研究部門に提供してはならない。<br>ただし、提供者又は代諾者等が同意し、かつ、倫理審査委員会の承認を受け、研究を行う機関の長が許可した研究計画書において認められている場合には、個人情報を外部の機関及び試料等の提供が行われる機関における研究部門に提供することができる。 |
| 22 | | (3)個人情報管理者は、**匿名化作業**の実施のほか、匿名化作業に当たって作成した対応表等の管理、廃棄を適切に行い、個人情報が含まれている情報が漏えいしないよう厳重に管理しなければならない。 |
| 26 | 10 インフォームド・コンセント | (10)研究責任者は、提供者又は代諾者等からインフォームド・コンセントの撤回があった場合には、原則として、当該提供者に係る試料等及び研究結果を匿名化して廃棄し、その旨を提供者又は代諾者等に文書により通知しなければならない。また、提供者又は代諾者等が廃棄以外の処置を希望する場合には、特段の理由がない限り、これに応じなければならない。<br>ただし、次に掲げる要件のいずれかを満たす場合は、試料等及び研究結果を廃棄しないことができる。<br>ア当該試料等が**連結不可能匿名化**されている場合<br>イ廃棄しないことにより個人情報が明らかになるおそれが極めて小さく、かつ廃棄作業が極めて過大である等の事情により廃棄しないことが倫理審査委員会において承認され、研究を行う機関の長に許可された場合<br>ウ研究結果が既に公表されている場合 |

| | | |
|---|---|---|
| 27 | 〈説明文書の記載に関する細則〉 | 提供者又は代諾者等に対する説明文書に記載すべき事項は、一般的に以下のとおりとするが、研究内容に応じて変更できる。 |
| | | ・提供者又は代諾者等により同意が撤回された場合には、当該撤回に係る試料等及び研究結果が**連結不可能匿名化**されている場合等を除き、廃棄されること |
| 28 | | ・提供を受けた試料等又はそれから得られた遺伝情報についての**連結可能匿名化又は連結不可能匿名化の別**及び**匿名化の具体的方法**。**匿名化できない場合**にあっては、その旨及び理由 |
| 28 | | ・研究の一部を委託する場合の**匿名化の方法等** |
| 28 | | ・試料等から得られた**遺伝情報は、匿名化された上**、学会等に公表され得ること |
| 28 | | ・試料等をヒト細胞・遺伝子・組織バンクに提供し、一般的に研究用資源として分譲することがあり得る場合には、バンクの学術的意義、当該バンクが運営されている機関の名称、**提供される試料等の匿名化の方法**及びバンクの責任者の氏名 |
| 28 | | (13)研究責任者は、ヒトゲノム・遺伝子解析研究の実施前に、ヒトゲノム・遺伝子解析研究又は関連する医学研究に使用することを想定して、提供者又は代諾者等からインフォームド・コンセントを受ける場合には、その時点において予想される具体的研究目的を明らかにするとともに、個人情報が、**匿名化の可能性**を含めて、どのように管理され、かつ、保護されるかを説明し、理解を得なければならない。 |
| 32 | 13 研究実施前提供試料等の利用 | ＜A群試料等の利用に関する細則＞<br>研究を行う機関の長及び研究責任者は、A群試料等が提供された時点における同意が、当該試料を利用して新たに行おうとするヒトゲノム・遺伝子解析研究の研究目的と同じ研究目的に対して与えられたものであることを確認することとする。<br>また、他のヒトゲノム・遺伝子解析研究への利用に関し、そのヒトゲノム・遺伝子解析研究の意義、研究目的又は**匿名化等の方法**等に、どの程度言及された同意であったか、また、同意が得られた時期等にも配慮して判断しなければならない。<br>さらに、倫理審査委員会も、同様の事項に配慮して、その利用の取扱いを審査しなければならない。 |
| | | (4)B群試料等<br>ただし、次に掲げる要件のいずれかを満たすとともに、倫理審査委員会の承認を受け、かつ、研究を行う機関の長により許可された場合についてはこの限りでない。<br>ア**連結不可能匿名化**されていることにより、提供者等に危険や不利益が及ぶおそれがない場合<br>イ**連結可能匿名化**されており、かつ、B群試料等が提供された時点における同意が、ヒトゲノム・遺伝子解析研究の目的と相当の関連性を有すると合理的に認められる場合であって、ヒトゲノム・遺伝子解析研究の目的を提供者に通知し、又は公表した場合 |

| | | |
|---|---|---|
| | | (5)C群試料等<br>なお、B群試料等であって、提供された時点における同意がヒトゲノム・遺伝子解析研究の目的と相当の関連性を有すると合理的に認められないものはC群試料等とみなす。<br>ア**連結不可能匿名化**されていることにより、提供者等に危険や不利益が及ぶおそれがない場合<br>イ**連結可能匿名化**されており、かつ、次に掲げる要件のすべてを満たしている場合<br>(ア)ヒトゲノム・遺伝子解析研究により提供者等に危険や不利益が及ぶおそれが極めて少ないこと。<br>(イ)その試料等を用いたヒトゲノム・遺伝子解析研究が公衆衛生の向上のために必要がある場合であること。<br>(ウ)他の方法では事実上、ヒトゲノム・遺伝子解析研究の実施が不可能であること。<br>(エ)ヒトゲノム・遺伝子解析研究の実施状況について情報の公開を図り、併せて提供者又は代諾者等に問い合わせ及び試料等の研究への利用を拒否する機会を保障するための措置が講じられていること。<br>(オ)提供者又は代諾者等の同意を得ることが困難であること。 |
| 34 | 14 試料等の保存及び廃棄の方法 | (2)ヒト細胞・遺伝子・組織バンクへの提供<br>研究責任者は、試料等をヒト細胞・遺伝子・組織バンクに提供する場合には、当該バンクが試料等を一般的な研究用試料等として分譲するに当たり、**連結不可能匿名化**がなされることを確認するとともに、バンクに提供することの同意を含む提供者又は代諾者等の同意事項を遵守しなければな<br>らない。 |
| 34 | | (3)試料等の廃棄<br>研究責任者は、研究計画書に従い自ら保存する場合及びヒト細胞・遺伝子・組織バンクに提供する場合を除き、試料等の保存期間が研究計画書に定めた期間を過ぎた場合には、提供者又は代諾者等の同意事項を遵守し、**匿名化して**廃棄しなければならない。 |
| 36 | ＜本指針の対象とするヒトゲノム・遺伝子解析研究の範囲に関する細則＞ | 2．1．で示した本指針の対象としない研究を行う過程で、偶然の理由により遺伝情報（遺伝情報を得るに当たって使用された試料等を含む。）が得られた場合には、ヒトゲノム・遺伝子解析研究目的での使用、適切な管理（個人情報に該当する場合は安全管理措置、**個人情報に該当しない匿名化情報**の場合には適切な取扱い）、保存、**匿名化して廃棄**する等、その試料等の取扱いは、研究を行う機関の長が倫理審査委員会に諮った上で決定することとする。 |
| 36 | 16 用語の定義(5)**匿名化** | 提供者の個人情報が法令、本指針又は研究計画に反して外部に漏えいしないよう、その個人情報から個人を識別する情報の全部又は一部を取り除き、代わりに当該提供者とかかわりのない符号又は番号を付すことをいう。<br>試料等に付随する情報のうち、ある情報だけでは特定の人を識別できない情報であっても、各種の名簿等の他で入手できる情報と組み合わせることにより、当該提供者を識別できる場合には、組合せに必要な情報の全部又は一部を取り除いて、当該提供者が識別できないようにすることをいう。<br>匿名化には、次に掲げるものがある。 |
| 36 | ア**連結可能匿名化** | 必要な場合に提供者を識別できるよう、当該提供者と新たに付された符号又は番号の対応表を残す方法による匿名化 |

| | | |
|---|---|---|
| 37 | イ**連結不可能匿名化** | 提供者を識別できないよう、上記アのような対応表を残さない方法による匿名化 |
| 37 | 個人情報管理者 | 試料等の提供が行われる機関を含め、個人情報を取り扱う研究を行う機関において、当該機関の長の指示を受け、提供者等の個人情報がその機関の外部に漏えいしないよう個人情報を管理し、かつ、**匿名化する責任者**をいう。 |

(4)疫学研究に関する倫理指針

| 頁 | 箇所 | 内容 |
|---|---|---|
| 5 | 2 適用範囲 | ただし、次のいずれかに該当する疫学研究は、この指針の対象としない。<br>① 法律の規定に基づき実施される調査<br>② ヒトゲノム・遺伝子解析研究に関する倫理指針(平成16年文部科学省・厚生労働省・経済産業省告示第1号)に基づき実施される研究<br>③ 資料として既に**連結不可能匿名化**されている情報のみを用いる研究<br>④ 手術、投薬等の医療行為を伴う介入研究 |
| 5 | 研究事例 指針の対象外 | ・被験者(患者又は健常者)を2群に分け、一方の群は、特定の医薬品を投与し、他方の群には、偽薬(プラセボ)を投与することにより、当該医薬品の健康に与える影響を調べる行為。<br>(**連結不可能匿名化**されている情報)<br>・患者調査と国民栄養調査を組み合わせて、地域別の生活習慣病の受療率とエネルギー摂取量から、両者の関係を調べる行為。 |
| 20 | 10 資料の保存及び利用 | (2) 人体から採取された試料の利用<br>研究者等は、研究開始前に人体から採取された試料を利用する場合には、研究開始時までに研究対象者から試料の利用に係る同意を受け、及び当該同意に関する記録を作成することを原則とする。ただし、当該同意を受けることができない場合には、次のいずれかに該当することについて、倫理審査委員会の承認を得て、研究を行う機関の長の許可を受けたときに限り、当該試料を利用することができる。<br>① 当該試料が匿名化(**連結不可能匿名**化又は**連結可能匿名化**であって対応表を有していない場合)されていること。<br>② 当該試料が①の匿名化に該当しない場合において、試料の提供時に当該疫学研究における利用が明示されていない研究についての同意のみが与えられている場合は、以下の要件を満たしていること。<br>ア当該疫学研究の実施について試料の利用目的を含む情報を公開していること。<br>イその同意が当該疫学研究の目的と相当の関連性があると合理的に認められること。 |
| 20 | 11 他の機関等の資料の利用 | (2) 既存資料等の提供に当たっての措置<br>既存資料等の提供を行う者は、所属機関外の者に研究に用いるための資料を提供する場合には、資料提供時までに研究対象者から資料の提供に係る同意を受け、及び当該同意に関する記録を作成することを原則とする。ただし、当該同意を受けることができない場合には、次のいずれかに該当するときに限り、資料を所属機関外の者に提供することができる。<br>① 当該資料が匿名化されていること。(**連結不可能匿名化**又は**連結可能匿名化**であって対応表を有していない場合)<br>② 当該資料が①の匿名化に該当しない場合において、以下の要件を満たしていることについて倫理審査委員会の承認を得て、研究を行う機関の長の許可を受けていること。 |

| | | |
|---|---|---|
| 22 | 13 用語の定義<br>(7) **匿名化** | 個人情報から個人を識別することができる情報の全部又は一部を取り除き、代わりにその人と関わりのない符号又は番号を付すことをいう。資料に付随する情報のうち、ある情報だけでは特定の人を識別できない情報であっても、各種の名簿等の他で入手できる情報と組み合わせることにより、その人を識別できる場合には、組合せに必要な情報の全部又は一部を取り除いて、その人が識別できないようにすることをいう。 |
| 22 | (8) **連結可能匿名化** | 必要な場合に個人を識別できるように、その人と新たに付された符号又は番号の対応表を残す方法による**匿名化**をいう。 |
| 23 | (9) **連結不可能匿名化** | 個人を識別できないように、その人と新たに付された符号又は番号の対応表を残さない方法による**匿名化**をいう。 |

医療分野におけるアンケートの可能性としては昨年述べたように次のようなものがある。

① 患者満足度向上、従業員満足度向上を図る指針としてのアンケート
② 再生医薬品利用状況アンケート
③ 電子カルテ・オーダーメード医療における個人情報の削除とデータの収集

IT政策パッケージー2005 の「医療」の項目に、個人情報関連の項目があり、今後検討を要すべきものと思われる。

◆審査支払機関から保険者に提出されるレセプトの電算化の実現(厚生労働省)
・ 保険者等における個人情報保護の適正な取扱いを確保した上で、保険者の求めに応じ、審査支払機関から保険者への電子データによるレセプトの提出を 2005 年末までに開始する

◆レセプトデータ等の有効活用による医療の質の向上(厚生労働省)
・ 保険者等における個人情報保護の適正な取扱いを確保した上で、個人情報を除くレセプトの医療データについては、医療の質の向上を図る観点から、レセプト情報の電子化を前提として、簡易かつ有効に活用できる方法を研究・検討し、2005 年度末までに結論を得る。

◆ITを利用した医療情報の連携活用の促進(厚生労働省)
・ 患者等の要望と個人情報保護を前提とし、処方せんに記載されている情報の電子的共有等、関係機関が医療安全推進の観点から適切なネットワーク連携を行うための具体方策等に係る研究を 2005 年度に実施する。

◆遠隔医療の推進・ユビキタス健康医療の実現(総務省)
この項目に関しては、パッケージ内で個人情報についての記述は無いが、遠隔医療やユビキタス健康医療を考えた場合、情報の流通上での個人情報の取扱が問題になる。データ収集、集計と個人情報の切り離しといった技術に対するアプローチが必要になると考えられる。

■ 個人遺伝情報と事業

経済産業省は、2004 年 12 月 17 日、経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」を策定した。個人情報保護法では、施行令2条において個人情報の量を5000を超えない者を「個人情報取扱事業者」から除外しているが、本ガイドラインでは、「法の適用から除外されている個人遺伝情報、遺伝情報の数が 5000 人を超えない事業者についても、個人遺伝情報の特殊性にかんがみ、本ガイドラインの遵守に努めることとする。」としている(Ⅰ. 目的及び適用範囲(13)「遺伝情報取扱事業者」では「なお、その事業の用に供する遺伝情報の数が過去6月のいずれの日においても 5000 人を超えない者であっても、本ガイドラインを遵守することとする。」としている)。

個人遺伝情報に関しては、昨年の報告書に述べたオーダーメード医療、ゲノム創薬の点に関わってくる。2005 年 3 月 18 日厚生労働省は「医薬品の臨床試験におけるファーマコゲノミクスの利用指針の作成に係る行政機関への情報提供等について」(薬食審査発第 0318001 号)を通知し、ファーマコゲノミクスの指針の作成に備え、製薬企業より現状のゲノム検査を利用した臨床試験の実施状況に関する情報を求めた。アメリカでは米食品医薬品局(FDA)が、ファーマコゲノミクスのガイダンスの最終版を、2005 年 3 月 22 日に発表している。中国では 2003 年 10 月に、世界で初めて遺伝子治療製剤の製造、販売の許可がおりており、積極的に遺伝子治療が進められている。研究から臨床へと向かう中で、各種の病気と遺伝子の病態シミュレータなどの製品化も考えられている。ここで個人情報とデータの切り離し、収集といった観点で本研究の応用が想定される。

### 3-2-4-2 信用・金融分野

金融分野においては、信用情報機関が設置され、「名寄せ情報」として加盟各社の与信に関する個人情報を交換している。与信情報に基づき、消費者などへの過剰貸付の防止や審査事務の迅速化、消費者などの多重債務の防止などを図ることができる。

個人情報保護法が制定され、金融・信用分野に対しても、金融庁が「金融分野における個人情報保護に関するガイドライン」を、経済産業省が「経済産業分野のうち信用分野における個人情報保護ガイドライン」をそれぞれ 2004 年 12 月に策定している。

ガイドラインでは、個人の返済能力に関する情報の収集及び与信事業を行う個人情報取扱事業者に対する当該情報の提供を業とするものを「個人信用情報機関」とよび(第 2 条定義等)、個人信用情報機関に個人データが提供される場合の利用目的明示と本人同意(第3条4)とともに、個人情報取扱業者が個人信用情報機関から得た資金需要者の返済能力に関する情報について、当該資金需要者の返済能力の調査以外の目的に使用することのないよう、慎重に取り扱うよう求めている(第 13 条 3)。金融分野における個人情報取扱事業者が、与信事業に際して、個人情報を取得する場合の利用目的について本人の同意、与信の条件として、与信事業において取得した個人情報を与信業務以外の金融商品のダイレクトメールの発送に利用することを利用目的として同意させる等の行為を行うべきではないとしてしている(第3条3)。

本人同意に関しては、「原則として書面(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を含む。(第 4 条)」としている。

なお、ガイドラインでは「金融分野において個人情報データベース等を事業の用に供している者のうち、法第2条第3項第5号の規定により「個人情報取扱事業者」から除かれる者においても、本ガイドラインの遵守に努めるものとする。」としている(第1条3)。

海外の信用情報機関では、信用報告だけでなく消費者調査も行っている。個人の経済活動に関する詳細な情報を収集しており、個人のクレジットカードの決済時の与信情報の提供だけでなく、カードの利用状況と

それを利用した消費者調査を行ったり、個人信用情報をカードの利用者本人が入手できるようになっている。信用情報機関 Equifax と Lotus Development Corporation が Equifax 社の信用報告データベースと消費者マーケティングデータベースから個人情報を含む CD-ROM を販売しようとして苦情を受け、断念したというケースがあった。本件は、信用報告機関が保有する消費者報告から消費者に関する個人情報データベースの構築の可能性を示し、その情報の利用について考えさせる事件である。

日本においては、全国銀行個人信用情報センター、日本情報センター(JIC)、シー・アイ・シー(CIC)の3つの信用情報機関が提携し、CRIN(CRedit Information Network:クリン)という相互交流システムを構築している。これら3者は三者協指針として「信用情報機関における個人信用情報の保護に関する指針」[10]を平成11 年に定めており、個人信用情報の内容について、「情報主体の返済能力・支払能力を判断するために必要最小限のものでなければならず、かつ、取引内容、支払状況等の客観的な事実に基づくもの」でありかつ「情報主体の信教、政治的見解、保険医療等個人の機微に深く関わる情報収集・登録してはならない。」としている(第三章)。

金融機関において、与信の際に電子的に個人情報を収集するケースで、本人認証、情報の暗号化、収集、復号化が行われる。また、金融商品に対する各種アンケートを行うケースがあるが、近年の銀行や証券のネット化の増加、インターネット上での営業活動に特化した銀行・証券の出現に伴い、ネット上での取引において電子投票と同等の仕組みが利用できると考えられる。

なお、金融庁のガイドラインに基づき、生命保険協会と日本損害保険協会は2005 年 2 月に個人情報保護指針を改定している。

## 3-2-5 SNS と電子アンケートの可能性

2004 年度は、SNS と blog が大きな立ち上がりを見せた。SNS は、Sosial Networking Service の略で、匿名が原則であったインターネットの中で、名前や履歴などの個人情報を公開し、紹介制による参加、人脈作り・ネットワーク作りを特徴としている。日本における SNS の一つ「mixi」は、2005 年 1 月 21 日に 1 年で 30 万人を突破したと発表したが、「コミュニティを企業のマーケティングツールとして販売する」という明確な方針を持っていた「UUME」は 3 月 20 日を持って閉鎖されることになった。中国では成功したが日本ではビジネスモデルが立ちあがらなかったとされている。他の SNS「GREE」「mixi」「キヌガサ」なども、会員数は増加しているが、収益モデルを確立できていないようである。海外では、人材紹介形のビジネス系 SNS「LinkedIn」が存在するが、日本では主にパーソナル系の SNS が中心で、こうした形式の SNS は存在していない。

現在の SNS は、主に次のような機能を持っている。

- プロフィール管理(個人情報の登録と公開範囲の設定)
- 交友管理(友達の紹介や承認)
- コミュニティ管理(任意のコミュニティの作成、参加、脱退)
- Blog
- 掲示板
- スケジュール管理

[10] この指針は平成 17 年 4 月に「全国銀行個人信用情報センターにおける個人情報保護指針」に改められている

- メッセージ管理
- 検索
- 訪問履歴管理

拡張機能として、画像の管理やケータイ対応、RSS リーダ機能などがある。

いずれにせよ、インターネットの掲示板や Blog と異なり、ユーザを制限する機能があるのが特徴となっており、匿名が前提であったインターネットの世界で、記名のシステムが爆発的に伸びているという意味で、新しい潮流であるといえる。このような記名のコミュニティに対して、オフラインの世界同様、秘密投票や匿名のアンケートシステムは望まれるものと考えられる。電子的なコミュニティである以上、投票やアンケートも電子的なものとなる。個人の氏名や住所などの情報は消去され、性別や年齢などの属性情報とアンケートの集計結果のみが収集される安全性の高い電子アンケートシステムを導入することにより、UUME が果たせなかった企業のマーケティングツールとしてのネットワークが考えられる。

熊本県八代市では、自治体でははじめて SNS を使ったサービスを平成 14 年 12 月から開始し、SNS 化してからアクセスが急増し、登録者も増えて地域密着型のコミュニティサイトとして十分な手ごたえを感じているという。こうした自治体での取組みを考えると、昨年の報告書で出した市民満足度調査や行政評価と SNS、電子アンケートの組み合わせというモデルも考えられる。事業として不特定多数を対象にした SNS は現在「mixi」の一人勝ちのような様相を示しており、自治体や企業(従業員・ユーザ)など特定集団におけるコミュニケーションツールとしての活用が今後増加していくと考えられる。従業員を対象にしたケースなどでは個人情報は社員番号などで管理し、全員を対象としたシステムを構築できる。SNS にアンケートシステムをあらかじめ組み込むことにより、その都度アンケート用のプログラムを作成することなく、社員にとっては個人が特定されることなく、サブコミュニティ内の意見を抽出することが可能になるだろう。

従来、テレゴングのような、有線によるアンケート調査がテレビ・ラジオなどのマスメディアで使用されていたが、日本の携帯電話の広がりから、携帯電話による投票・アンケートシステムが開発されてきている。テレゴングに対応するシステムとして、携帯メール超高速受信リアルタイム集計システム「メルゴング」のサービスも株式会社インフォプラントによって 2003 年から開始されている。

メルゴングの特徴として、次のようなものがあげられている。

- メールによる視聴者参加型の生番組に連動させた、TV 画面への投票結果表示が可能
- 5 分間に 100 万通以上の投票メールを受信しリアルタイム集計が可能
- 応募メールの受付後、参加者に対してお礼のメール(サンクスメール)を送信可能
- 利用者がサーバ環境を考慮しなくても良い

携帯電話の場合、個人が特定されるという特徴があり、SNS もまた記名のシステムであり、個人が特定されるという特徴がある。個人情報が通知されないのなら、アンケートに答えても良いという層に対して、個人を特定される情報は切り捨てた上で、本人の属性(性差や年齢など)を勘案したアンケートシステムを提供するサービスが可能となる。

SNS の機能として、携帯電話からのアクセスも取り込む方向であり、アンケートシステムを SNS へ統合するサービスを考えると、次のようなものが考えられるだろう。

① SNS のサービス提供者

アンケートシステムをマーケットリサーチとして使用する。企業からの依頼を受けてアンケートを応募、回答した会員に対しポイントを付与するなどの形をとる。アンケート回答者はアンケートが必要とする属性情報はプロフィール機能から自動的に埋めこまれた情報を参照し、回答するかどうかを判断してアンケートに回答する。(個人情報保護法の観点から、不必要な個人情報をアンケートに含ませない)

② SNS サービス利用者

- SNS 機能の一部として、利用者が自由に項目を設定して利用する。
- SNS が企業や自治体などで、社員やユーザ、会員、地域住民などを対象にして、各種サービスの満足度を調査するために利用する。

総務省の予測によれば、2007 年 3 月末に SNS 参加者は延べ約 1,042 万人、アクティブ SNS 参加者数は約 751 万人に達するという。一般ユーザにサービスとして提供する専業事業者は収益モデルが確立されておらず、今後淘汰が進むとされているが、熊本県八代市の例に見るような会員組織でのコミュニケーションツールとしての導入はむしろ進むと考えられる。IP 接続業者やネットワーク関連サービスを行う企業などではユーザの流出を防ぐ意味で防衛的に SNS を拡充させることも想定される。こうした市場に対して、SI を含めた電子アンケート(投票)システムの導入が考えられよう。

# 3-3　運用形態ごとの要件整理

## 3-3-1 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。（3-4-3 参照実装モデルのセキュリティ対策技術」参照）

## 3-3-2 要件定義について

### 3-3-2-1 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 4 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 5 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。<br><br>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<br>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<br>法…公職選挙法<br>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。 |

### 3-3-2-2 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 6 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 7 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 |

（1）共通、その他

**表 8 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 |

## 3-3-3 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 9 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 |
| | | | 3．適切な権限を持つ管理者のみがインストール可能とすること |

（b）投票中要件

**表 10 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 11 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 12 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 13 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 14 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 |

## 3-3-4　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１３９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 15 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－<br>投票前要件 | ３ | ５ | ９ | １４ |
| 機能要件－<br>投票中要件 | １ | １２ | ３４ | ４２ |
| 機能要件－<br>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 | **１３９** |

# 3-4　効率的運用とリスク分析

## 3-4-1　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。

## 3-4-2　性能分析

### 3-4-2-1　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

### 3-4-2-2　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）

### 3-4-2-3　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 |

**表 16　性能測定結果(数値データ)**

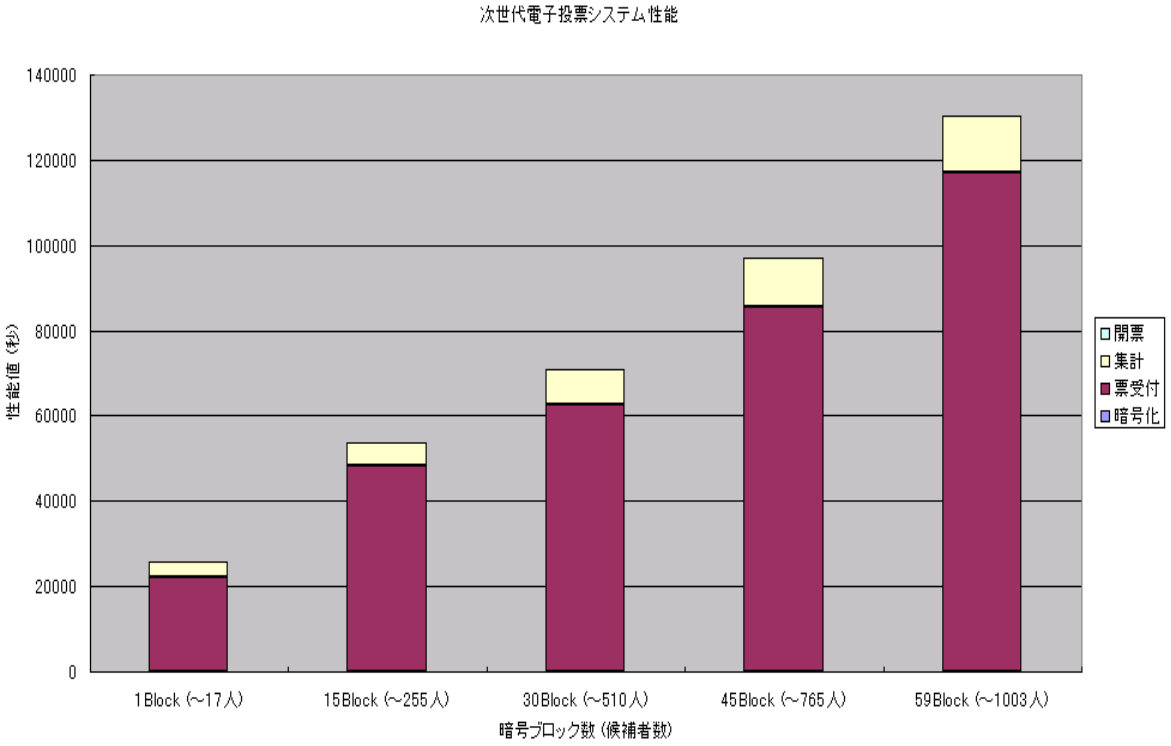



**図 11　性能測定結果（グラフ化）**

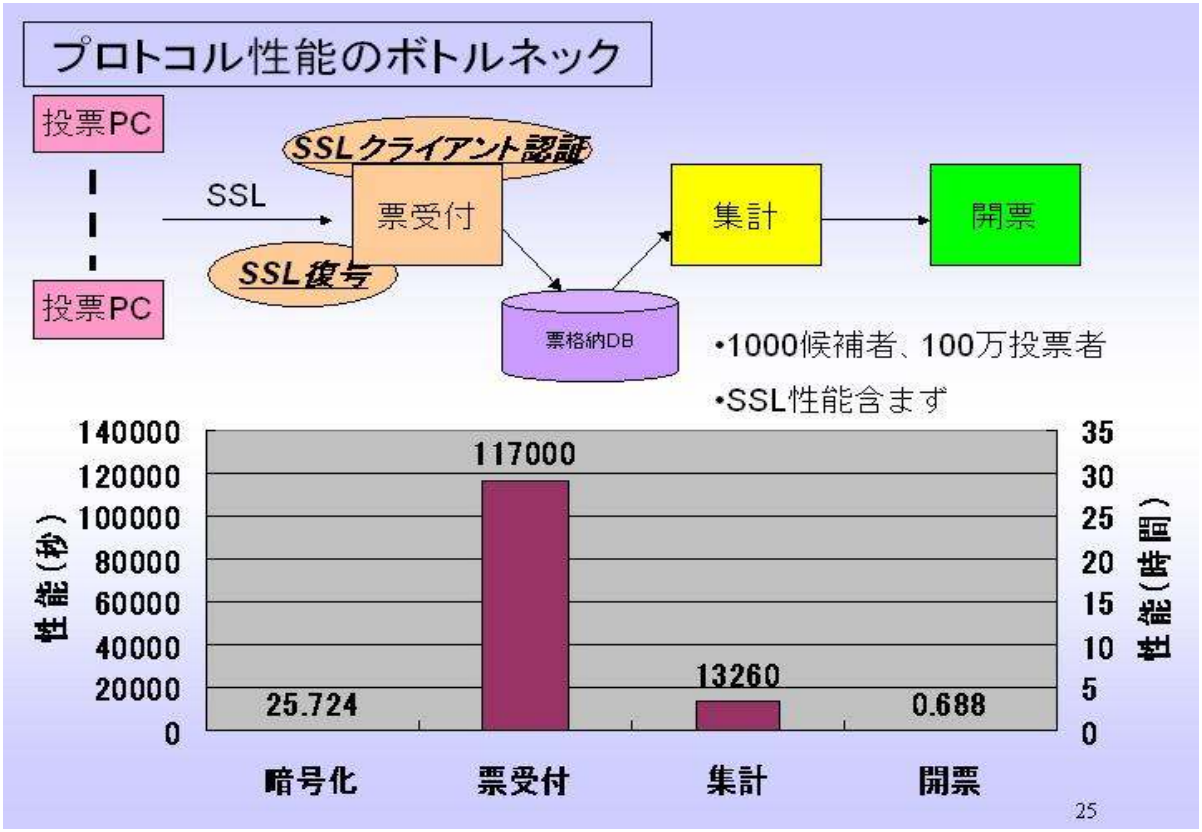



**図 12　プロトコル性能のボトルネック**

### 3-4-2-4　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**

## 3-4-3　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。

### 3-4-3-1　運用要件概要

サブテーマ２「運用形態ごとの要件整理」（3-3 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（3-3-2 要件定義について表 4　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「3-3-3 要件定義」表 12　セキュリティ要件に示す通りである。

### 3-4-3-2　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」（3-6 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。

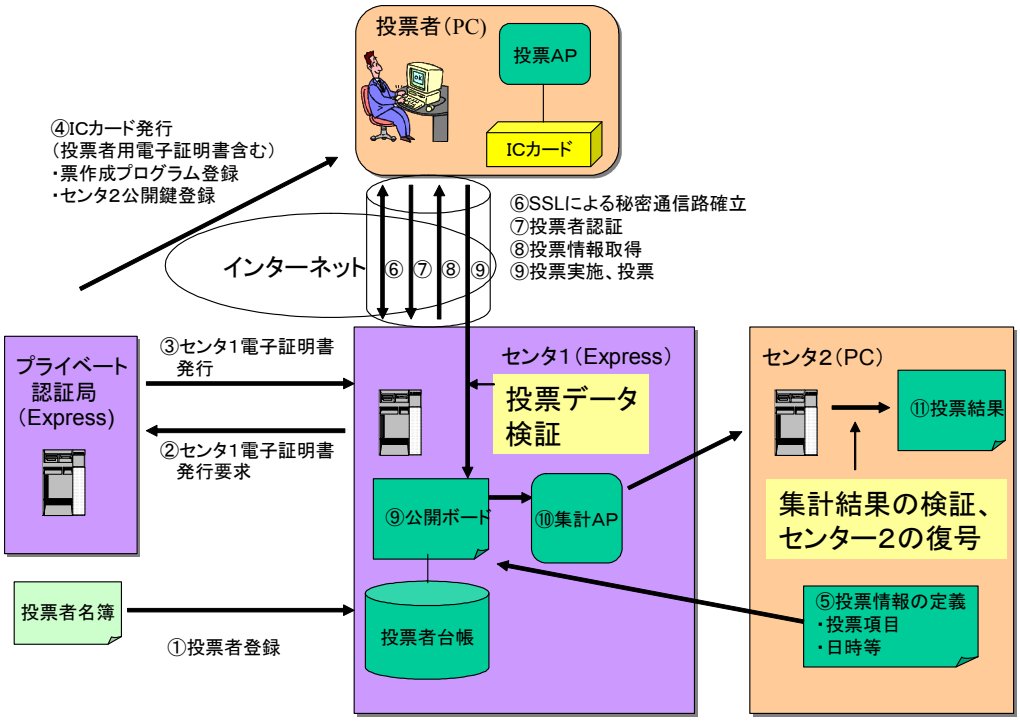



図 13　システム構成図

サブテーマ５「モデル構築」（3-6 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 17 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 18 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。 |

### 3-4-3-3　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」（3-3 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」（3-6 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 19 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<br>・ IPSec |
| 鍵管理 | 秘密鍵などを安全に秘匿する技術 | ・ HSM（Hardware Security Module）<br>・ 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)<br>・ 所持品による個人認証<br>・ 知識による個人認証<br>・ 身体的特徴および行動による個人認証<br>・ 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）<br>・ 物理的ネットワークの防御 ネットワーク機器の防御<br>・ 内部ネットワークへの不正接続の阻止<br>・ 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<br>・ ワクチンソフト導入<br>・ 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<br>・ サーバ上のファイルの改ざん検知<br>・ 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<br>・ ネットワーク上での不正アクセスの検知（NIDS）<br>・ 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<br>・ 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 20 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<br>（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 |

### 3-4-3-4　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。

### 3-4-3-5　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。

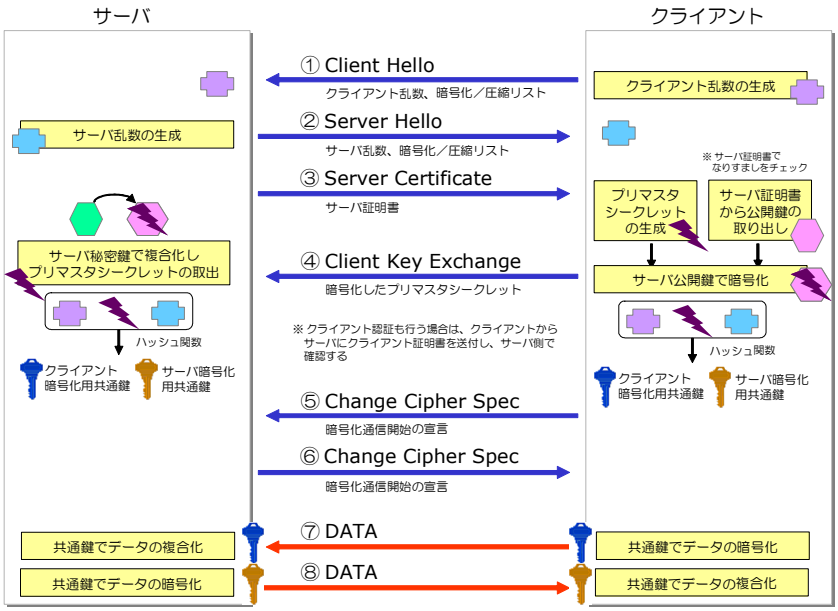



**図 14 SSLのやり取り**

(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。

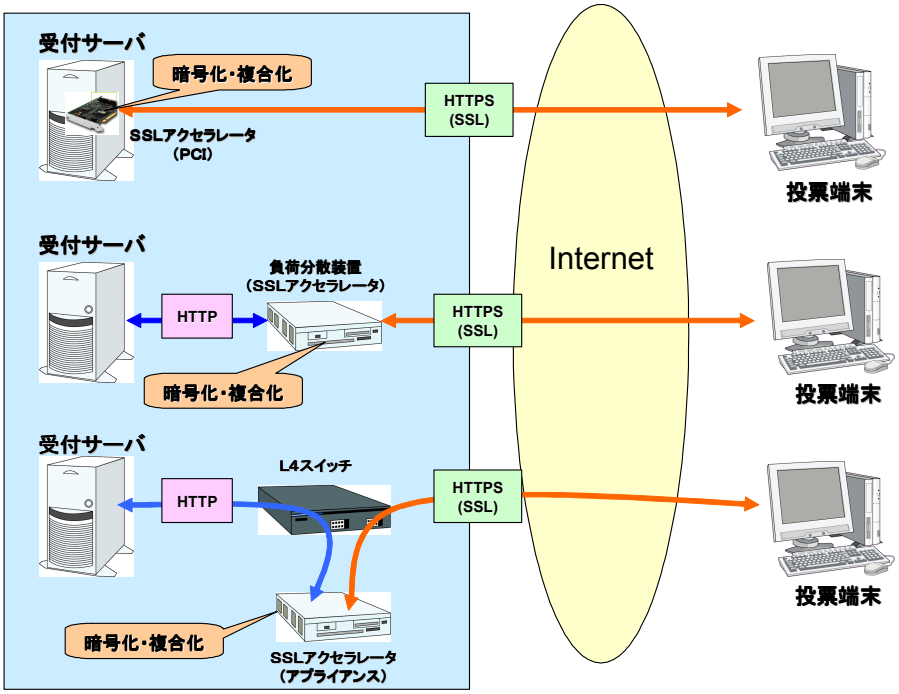



**図 15 SSLアクセラレータの利用形態**

(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。

### 3-4-3-6 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。

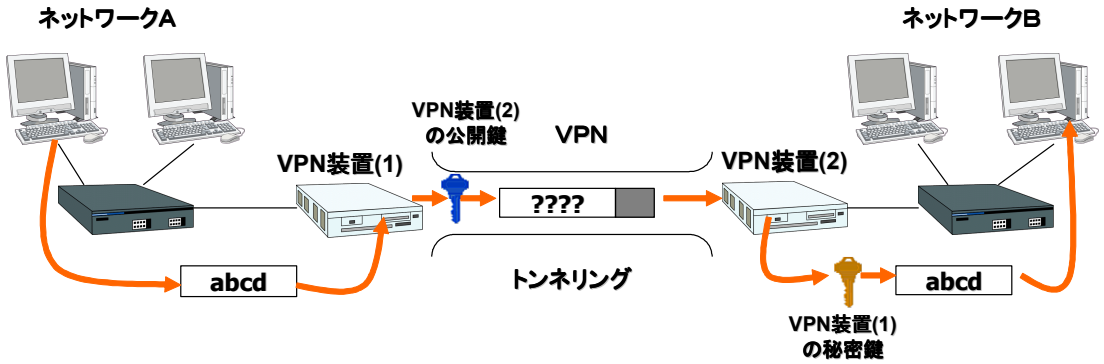



図 16 VPN接続の構成例

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。

### 3-4-3-7 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。）

### 3-4-3-8 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。

（1） 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。

（2） 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。

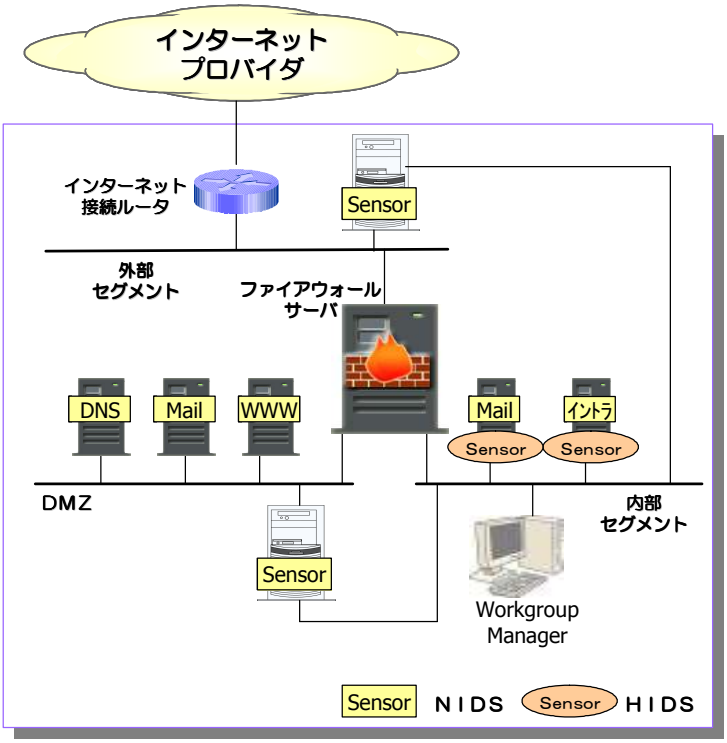



**図 17 ホスト型IDSとネットワーク型IDSの構成例**

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。

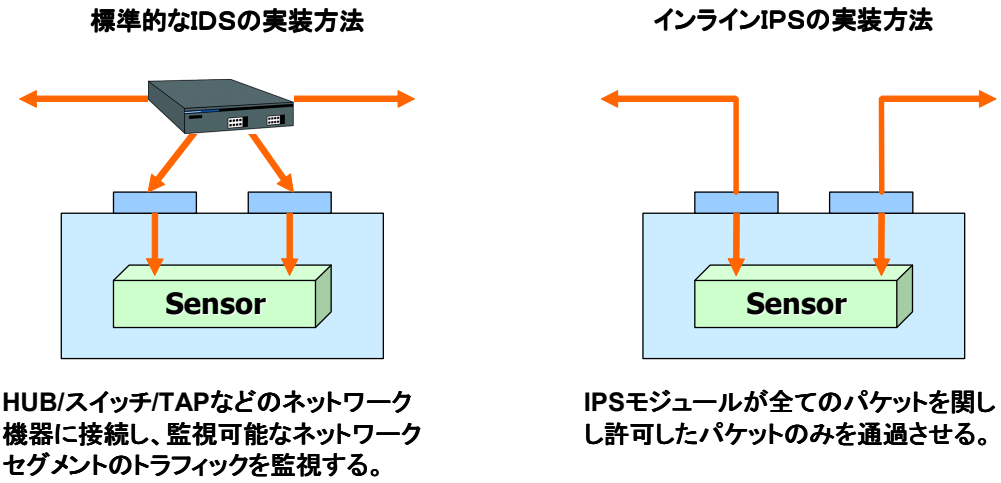



図 18 インライン型IDSの実装

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）。

### 3-4-3-9　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。

### 3-4-3-10 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。

### 3-4-3-11 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。

### 3-4-3-12 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。

### 3-4-3-13 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。

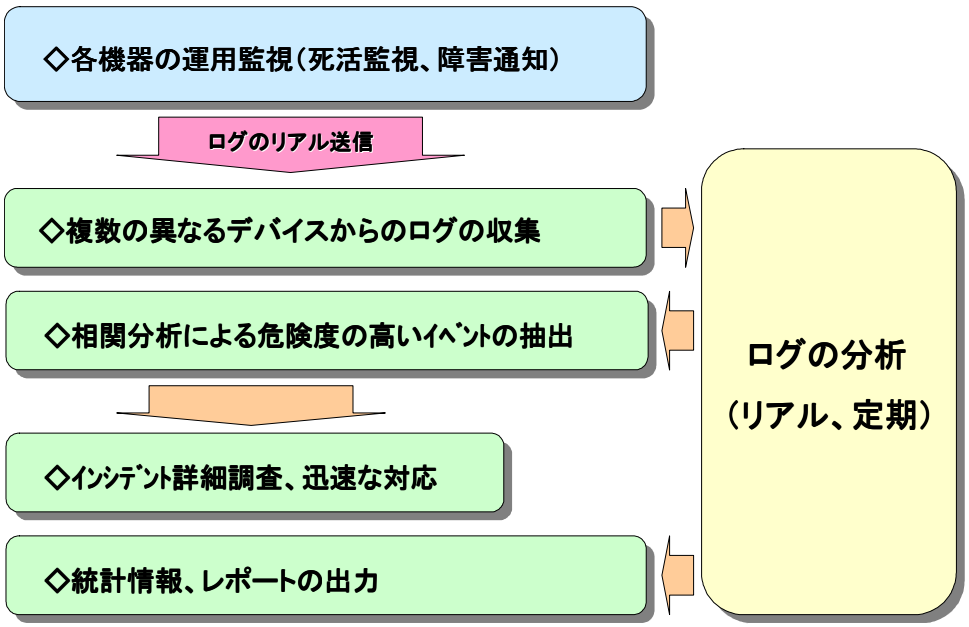



図 19 ログ分析の方法案

### 3-4-3-14 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）

### 3-4-3-15 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。

# 3-5　セキュリティポリシー

(1)ISO15408に関連する調査研究

ISO15408 では、「次世代電子投票・アンケートシステムの IC カードプロテクションプロファイルフレームワーク」に関する調査を行った。昨年度は、ウェブなどに公表されているプロテクションプロファイル(以下、PP)の調査を行った。

今年度は次世代電子投票・アンケートシステムに焦点を当てて検討を行った。特に、国内で利用されている住民基本台帳のICカードPPを基本にした。 電子投票システム全体のPPについて書いた事例は調査の限りでは存在しなかった。

また、本年度の調査ではシステムの PP に関しては世界の状況を調査すると共に、困難な状況になっている本質は何かを考察した。

最後に CC の国際会議である ICCC(International Conference on Common Criteria)の状況を整理し、世界の CC の検討状況と今後の方向性について整理を行った。

(2)ISMS(情報セキュリティマネジメントシステム)に関連する調査研究

ISMS では、今年度行われた電子アンケートを中心とした実証実験からの知見等を纏めた。

ISO15408 に関しては、以下に述べた。

3-5-1 次世代電子投票・アンケートシステムのICカードに関するPPフレームワーク

3-5-2 システムPPに関する内外の状況

ISMS に関しては、以下に述べた。

3-5-3 次世代電子投票・アンケートシステムのISMS

## 3-5-1　次世代電子投票・アンケートシステムのＩＣカードに関するＰＰフレームワーク

### 3-5-1-1　PPとは

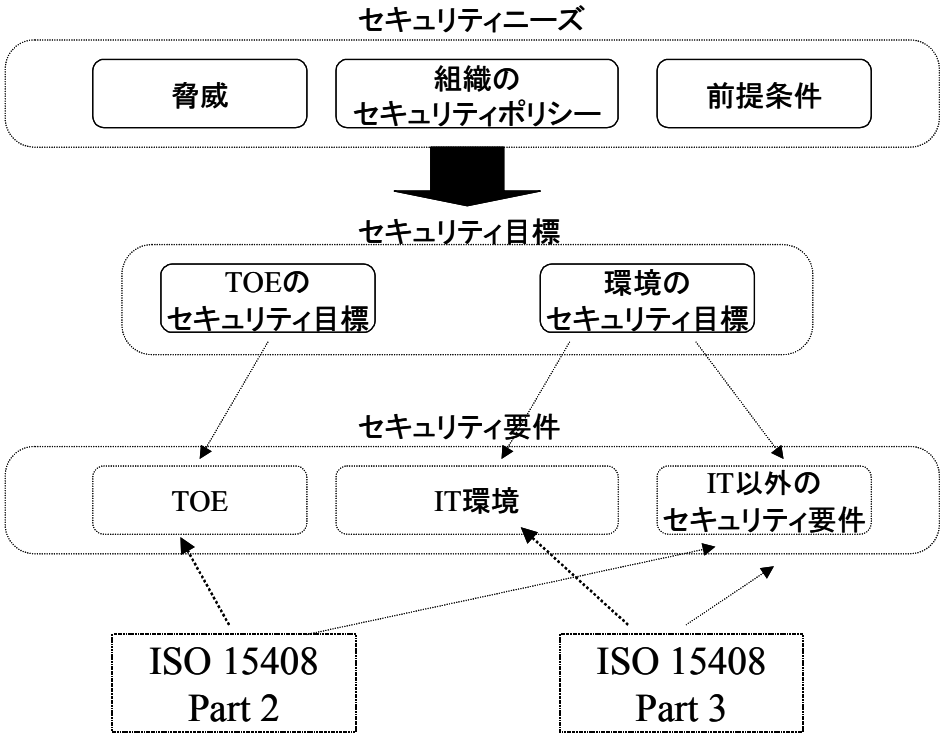
PPは、要は、セキュリティ要求条件であり、参考文献〔1〕にあるように例えて言うと、「作文」するの単語の辞書がCCであり、書かれる文章がPPであるという。辞書が共通であることによって、文章を共通言語として理解される。すなわち、セキュリティ仕様の共通化が図れるといえる。別の面で説明すると、PPはセキュリティ製品、システムを調達する側の要求仕様であり、ST(Security Target)はIT機能として実現した機能をさし、現実には製造業者あるいは開発が設計する製品の中のセキュリティ機能仕様である。

ここでの説明は、各工程を詳しく述べるのではなく、PP作成の流れを理解するという立場での留意点を中心に述べる。

### 3-5-1-2　PP作成作業の流れ

ISOの「PP／ST作成ガイドライン」におけるPP作成の流れは、図 20 であり、セキュリティニーズ、セキュリティ目標、セキュリティ要件という作業手順で行われる。すなわち、CCではトップダウンでセキュリティ

の要求条件が設計される。PPは本来的には、利用者が策定するものであるので「設計」という言葉は適切な表現とは思えない。「策定」というような表現の方が適当かもしれないが、現実には開発にかかわる技術者が、利用者からの依頼をうけて作成する場合が多く、PP開発などという表現が使われる。




〔出典:*1:ISO PDTR 15446Guid for the production of PPs and STs〕

**図 20 PP(および ST)の作成の流れ**

図 20 に示すように、PPの最終段階はセキュリティ要件であるが、その決定までの流れは次のようになっている。

（1） セキュリティニーズの決定

（ア） 環境に対する前提条件

（イ） 情報財（Ａｓｓｅｔ）に対する脅威

（ウ） 組織のセキュリティポリシー

分類(ア)、(イ)、(ウ)のキーワードは前提条件、脅威、セキュリティポリシーというのであるが、一見して、同一の要素による分類になっていないように思われ、網羅性の検証をする必要があろう。

検討すると、完全性が不安になる。(ア)と、(イ)、(ウ)の間は、(ア)が環境という言葉が境界と為って、IT システムとそれを取り囲む環境という分類であることがわかる。しかし、(イ)、(ウ)については、分類する要素になっていない。‘組織のセキュリティポリシーは、付加的条件と理解すべきである。とすれば、ITシステムに対するセキュリティニーズは情報財(Asset)に対する脅威のみでよいかを吟味する必要があろう。

IT システムは確かに情報処理が本来の機能である。かかわっている計算機本体(ハードウェなど)は処理を実現するための手段である。したがって、情報財(Asset)のみを挙げたというのも、理解はできるが、多少、この辺については議論の余地があるのではないだろうか。(このテーマは CC に対する研究課題として検討しているが、本論から外れてくるので言及を避ける)

分類学を問題にするなら、次の段階ではTOE内、外という論理で区別されるので完全性(網羅性)が確保されていると理解できる。

（2） セキュリティ目標の決定

（ア） ＴＯＥに対するセキュリティ目標の決定

（イ） ＴＯＥ環境に対するセキュリティ目標の決定

CCの基本的考え方は、TOEでセキュリティを担保できるものと運用などの人間系でガードするセキュリティの両輪で、システム全体のセキュリティを確保しようという考え方である。

この考え方は、情報セキュリティを現実に確保する上で、重要な観点である。えてして、日本文化の場合には、利用者は製造業者に機能に関する要求をだすが、自らが利用する(運用)規則については、なおざりになりがちであり、端的にはセキュリティ製品を購入すれば、情報セキュリティが保てるという錯覚に陥っている利用者が多いと思われる。

この考え方が、ITの世界でなければ、当然であるというのを、理解のために説明する。例として、家の鍵と安全性について考える。家の鍵と錠前があっただけで、果たして、家は安全に保てるだろうか。容易に考えられる最悪の事態は、鍵を無くして誰かに渡ってしまう場合であろう。これは、鍵を無くした人が悪いのであって、鍵システムを作った製造業者の責任ではない。

（3） セキュリティ要件の決定

このステップでは、CCPart2. およびPart3. に書かれているセキュリティ機能要件と保証要件をセキュリティ目標にあったものを拾い出して対応づけ、個別の機能を定めていく。

#### 3-5-1-3 作成フローにおける課題

PP／STはトップダウンで設計されるのがCCの流れになっている。しかし、現実には、STが出発点というのも多い。特に、現実のシステム設計の現場を考えれば、全ての製品をゼロから開発するのではなく、例えばOSは既存の製品を利用し、アプリケーションを開発するケースが多いと考えられ、その場合、OSのセキュリティ機能は、PPの検討の前にもう既に存在する。すなわちOSが既に、持つセキュリティを利用するというのが現実である。このような事態は、開発時点ばかりではなく、システムを一旦開発し、その後、改良をする場合に、通常生じる議論である。したがって、現実にはPPは全て最初から検討するというより、構成しようとする既存製品のセキュリティ機能がカバーする(あるいは解決する)脅威要素を洗い出しその脅威要素と利用者の考える脅威との対応関係を調べ、解決できるものはセキュリティの要求条件に組み入れることができ、解決できないものは、基本的には環境要件にするという作業手順になっている。

図 21 はこれらの関係を概念的に示した。要は、図の中央にあるように、セキュリティニーズと、既存製品との間で折り合いをつけるといったことが開発現場の現実である。(無論、新たにセキュリティニーズに基づく開発が全く行われないということではない)

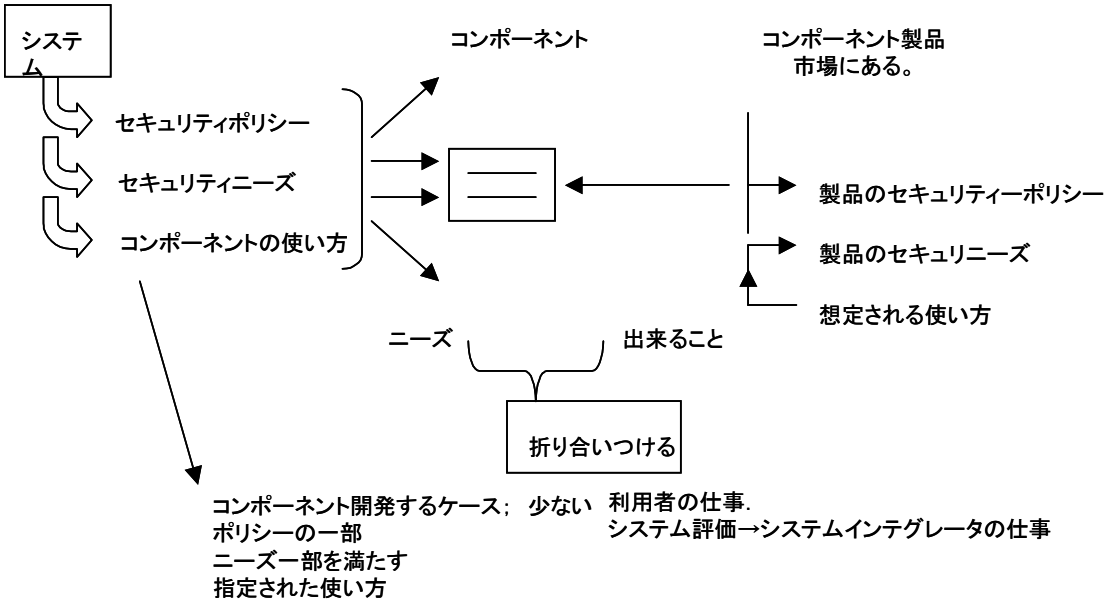



**図 21 既存のシステムコンポーネントと、PP の開発の関係**

### 3-5-1-4 参照モデル（住民基本台帳におけるICカードプロテクションプロファイル）の概要

本節では、電子投票の IC カードのプロテクションプロファイルの参照モデルとして、住民基本台帳の IC カードプロテクションプロファイルを選んだ。選択した理由としては、すでに開発されていることと、これを流用することを試み、関連する問題点の洗い出しと問題解決の検討を行うためである。プロテクションプロファイルを流用するというのはコモンクライティリアの基本的考え方の一つである。

（1）住民基本台帳の概要

住民基本台帳の IC カード（以下住基カード）は、住民負担の軽減、住民サービスの向上、行政改革のため、住民基本台帳法に基づき整備されつつある住民基本台帳ネットワーク(以下、住基ネットと略す)において、住民が市町村の提供する行政サービスを受けるために交付される IC カードである。

図 22 に住基カードの位置付けを示す。業務端末-サーバで構成される市町村システムでは、業務端末に提示さる住基カードを元に、様々な行政サービスが提供される。例えば、住基カードに格納された住民票コードに基づき、住民票写しが発行される。この市町村システムが住基ネットで相互接続されているので、居住する市町村以外でも住民票写しを入手出来るようになっていることが、大きな特徴である。

住民は、住基カードを利用し、市町村と言った空間的制約を越えた行政サービスが受けられると言う便利な反面、プライバシー侵害、各種の権利侵害、等に悪用される可能性も高くなる。そこで、市町村では、住基カードが装備すべき最低限の安全対策を PP(Protection Profile)と言う形にまとめ、カード製造事業者へ公表している。

住基カードは IC カードで、図 22 に示すように、

- 演算回路（CPU: Central Processing Unit）、記憶素子（ROM, RAM, F-RAM, EEPROM, etc）のようなハードウエア
- 記憶素子上に組み込まれるソフトウエア(ソフトウエアは業務用のアプリケーションプログラムやアプリケーションプログラムで共通に利用できる基本ソフトウエア)

から構成されている。この構成に合わせて、ハードウエア部分に対する要求仕様書 JICSAP(Japan IC Card system application council) part1 PP とソフトウエア部分に対する要求仕様書 住基用 IC カード PP が公表されている。

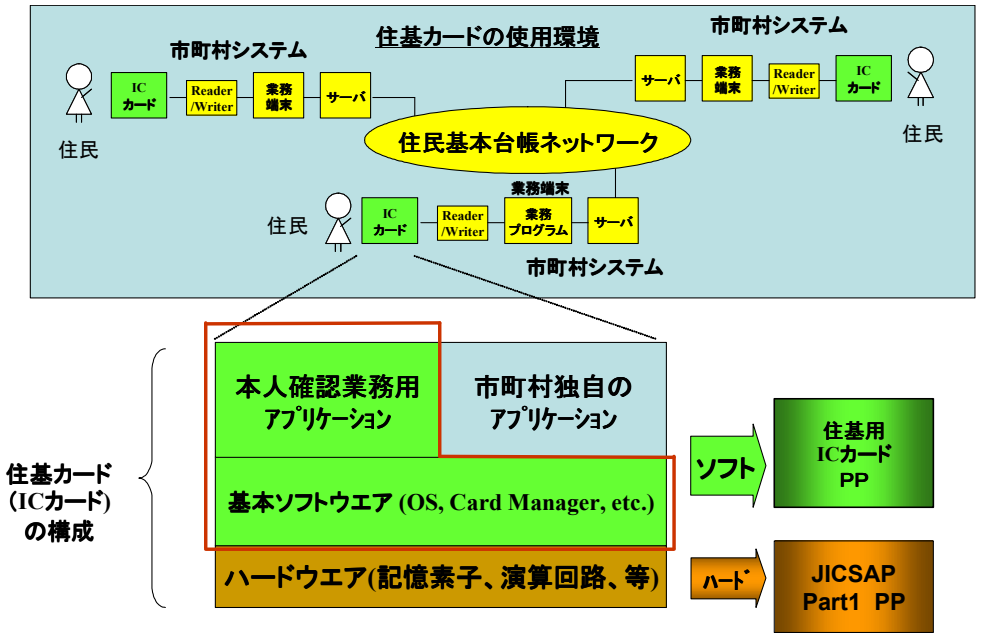



**図 22 住基カードの使用環境と構成**

(2) 住基用 IC カード PP の概要

住民基本台帳ネットワークシステム 住民基本台帳カード仕様書は、図 22 の IC カードと業務端末間の論理インタフェイスを規定している。住基用 IC カード PP は、この論理インタフェイスに関係すると思われる脅威を中心に、基本ソフトウエア及び本人確認業務用アプリケーションで必要とされるセキュリティ対策をまとめている。EAL(Evaluation assurance level)は、4+である。また、本 PP は、2003 年 5 月フランスの認証機関の承認を受けている。

① セキュリティ環境(Security environment)

住基カードが使われる環境において、住基カードのセキュリティ機能が守る資産(Assets)は、カード内に格納される以下のユーザデータ、

- 市町村が個別に設定する市町村初期化データ
- 住基カード製造者が設定するカード種別情報
- 本人確認業務用アプリケーションで使われる住民票コード

および、これらのデータを守るために使われる、以下の TSF(TOE Security Functions) データである。

- ユーザを認証(本人認証)するためのデータ:パスワード、輸送鍵
- 端末を認証するためのデータ:認証用の鍵
- 各種の権限を証明するデータ:アプリケーションプログラムのロード許可証明書

これらのデータに対し、

に示すように、7 つの脅威(Threats)、1 つの前提条件(Assumptions)、5つのポリシー(Policies)をセキュリティ環境として定義している。

表 21 セキュリティ環境

| | |
|---|---|
| **Threats** | **1) T.Logical_attack** |
| | **2) T.Illegal_Term_Use** |
| | **3) T.Disturb_APL** |
| | **4) T.Untrust_Path** |
| | **5) T.Enviroment** |
| | **6) T.Incomplete** |
| | **7) T.Hardware** |
| **Assumptions** | **1) A.TSF_Data** |
| **Policies** | **1) P.Authentication** |
| | **2) P.Secret_Setting** |
| | **3) P.Card_Activate** |
| | **4) P.PIN_Initialise** |
| | **5) P.Secure_Path** |

**表 21 セキュリティ環境**

これらのデータに対し、

に示すように、7つの脅威(Threats)、1つの前提条件(Assumptions)、5つのポリシー(Policies)をセキュリティ環境として定義している。

1) T.Logical_Attack 注1):

市町村に納入された住基カードは、住基カードの記憶素子へ、発行市町村初期化データや住民票コード設定、住基カードへの券面印刷等の工程を経て、市町村に住民に交付され、利用される。この一連の過程の住基カードに対し、IC カードの技術に詳しい攻撃者が、住民基本台帳カード仕様やカードが独自に規定する論理的インタフェイス(コマンド/レスポンス)を悪用し、ユーザデータや TSF データを改ざんしたり、盗んだりする。

注 1) PPでは一般的に、脅威を記号で識別している。T.Logical_Attack の T は、脅威(Threats)を表し、Logical_Attack は、脅威の内容を表す任意の文字列である。

2) T.Illegal_Term_Use:

住民基本台帳ネットワークで使われるカード関連機器の操作や技術に詳しい攻撃者が、住基ネットワークで使われる機器(カード関連機器)を悪用、あるいは、個人使用のパソコンの改造を行い、住基カードにアクセスし、ユーザデータや TSF データを改ざんしたり、盗んだりする。

3) T.Disturb_APL:

住基カードは、本人確認業務で使われるアプリケーションの他に、市町村が独自にロードするアプリケーションが存在する。このような複数のアプリケーションが存在する住基カード内で、市町村独自のアプリケーションがユーザデータ(本人確認業務用のアプリケーションデータ)を改ざんしたり、盗んだりする。

4) T.Untrust_Path:

IC カードの技術に詳しい攻撃者が、カードと Reader/Writer 間の通信中のデータを盗み、データフォーマットを分析し、ユーザデータや TSF データを推定する。住基カードの接続インタフェイスには接触型と非接触型がある。非接触型の場合、Reader/Writer とのデータ交換に電波が使われるため、データ盗聴のためのカード関連機器への細工が不必要となり、攻撃者にとって他人の住基カードへ攻撃する環境が作りやすくなる。

5) T.Environment:

住民が住基カードを使っている時に電源断が発生し、行政サービスが中断されることがある。その後、再度、行政サービスを受けようとした時、住基カード内のユーザデータやTSFデータが変わっていることがある。

6) T.Incomplete:

市町村に納入された住基カードが住民に交付されるまでに、様々なユーザデータや TSF データの設定が行われる。このような交付前の住基カードが悪用される。

7) T.Hardware:

半導体や暗号の技術に詳しい攻撃者が、住基カードのハードウエア(IC)に対し、以下の攻撃を行う。

- FIB (Focused Ion Beam) workstation, EBP (Electron Beam Prober), AFM (Automatic Force Microscope)を利用し、演算回路、記憶素子の物理的改ざん、盗聴(i.e. TOE 自体や TSF データの改ざん、TSF データの盗聴)
- ハードウエアの処理状況を分析することで、TSF データを推定
- IC カードを異常な状態で動作させ、その結果を分析し、TSF データを推定

1) A.TSF_Data [注2)]:

TOE(Target of Security)に設定されるTSF(TOE Security Functions)データには、TOEのライフサイクルを通して、様々な鍵、パスワード、等がある。設定されるそれらのデータは、ライフサイクルの各段階の責任で安全に管理されるものとする。また、設定時には、それらのデータは、Reader/Writer や端末といったIT(Information technology)装置内を通過する。従って、それらの機器の調達者はTSFデータが安全に管理できる IT 装置を採用する。

注 2) A.TSF_Data の A は、前提(Assumptions)を表す。

1) P.Authentication [注3]

住民基本台帳カード仕様書 第 2.1 版には、住民票コードの読出条件について、ポリシー的な記述は無い。しかし、7 章 住基カードアプリケーション仕様編 表 8.9 住基カード AP のセキュリティアトリビュート設定 から、以下の条件が暗黙的にポリシーとして設定されていると考えられる。

- ・PIN による本人認証が終わっていること
- ・全国センター発行の証明書による市町村認証が終わっていること

注 3) P.Authentication の P は、ポリシー(Policies)を表す。

2) P.Secret_Setting

1 章 概要 2.3 節 住民基本台帳カードの業務要件の (1)に、「カードに秘密鍵を設定する際に、安全な発行方式を採用する」との規定がある。

3) P.Card_Activate

1 章 概要 2.3 節 住民基本台帳カードの業務要件の (2) に、「住民がパスワードを設定することにより、カードが有効化する方式を採用する」との規定がある。

4) P.PIN_Initialise

1 章 概要 2.3 節 住民基本台帳カードの業務要件の (3)に、「パスワード忘却時にカード再利用に資する目的で、暗証番号初期化の後、利用者の新たなパスワード設定に対応する方式を採用する」との規定がある。

5) P.Secure_Path

7 章 住基カードアプリケーション仕様編 3.4 セキュアメッセージング機能について、「セキュアメッセージング機能は、IC カードと外部装置との間で授受される APDU(Application Protocol Data

Unit)を不正な盗聴から保護するための暗号化通信を行う機能である。住基カード AP において、本機能は住民票コード読み出し処理において利用される」との規定がある。

② セキュリティ設計目標(Security Objectives)

前節の Security environment に対して、の横軸に示すように、6つの TOE の設計目標(Objectives)、及び4つの TOE を取巻く環境(Environment)の設計目標で対抗している。

表 22 Security environment - Security objectives 対応表

| Environment \ Objectives | | Objectives for TOE | | | | | | Objectives for Environment | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1) O.Identification | 2) O.Authentication | 3) O.Domain | 4) O.Secure_Path | 5) O.Retention | 6) O.Forgry | 1) OE.TSF_Data | 2) OE.Term_TSF | 3) OE.Term_Mgt | 4) OE.Hardware |
| Threats | 1) T.Logical_attack | P | P | | | | | | P | | |
| | 2) T.Illegal_Term_Use | P | P | | | | | | P | P | |
| | 3) T.Disturb_APL | P | | P | | | | | | | |
| | 4) T.Untrust_Path | | | | P | | | | | | |
| | 5) T.Enviroment | | | | | P | | | | | |
| | 6) T.Incomplete | | | | | | P | | | | |
| | 7) T.Hardware | | | | | | | | | | P |
| Assumptions | 1) A.TSF_Data | | | | | | | P | P | | |
| Policies | 1) P.Authentication | P | P | | | | | | P | | |
| | 2) P.Secret_Setting | P | P | | | | | | P | | |
| | 3) P.Card_Activate | P | P | | | | P | | P | | |
| | 4) P.PIN_Initialise | P | P | | | | | | P | | |
| | 5) P.Secure_Path | | | | P | | | | | | |

~~表 22 Security environment - Security objectives 対応表~~

1) O.Identification [注4]

TSF は、カード発行者、住民、カード関連機器、住基カード内のアプリケーションを識別する機構を装備しなければならない。

注 4) O.Identification の O は、TOE の objectives を表す。

2) O.Authentication

TSF は、端末内の業務プログラムから TOE 内のユーザデータへのアクセス手段を論理インタフェイスに限定し、TOE が識別・認証したカード発行者、住民、カード関連機器のみが assets へアクセスできる機構を備えなければならない。

3) O.Domain

TSF は、住基カード内の個々のアプリケーションが管理できるファイル管理機構を装備し、他のアプリケーション管理下にあるファイルへのアクセスを防止しなければならない。

4) O.Secure_Path

TSFは、Reader/Writerとの通信データに対し、データフォーマットの分析を妨げる機構を備えなければならない。

5) O.Recovery

TSF は、住基カード使用中の電源断に対し、ユーザデータ、TSF データをリカバリーする機構を備えなければならない。

6) O.Forgery

TSF は、認証されたユーザから指示があるまで、行政サービスに使えない機構を装備すべきである。

1) OE.TSF_Data [注5]:

TOE に設定される TSF データは、TOE 外で安全に管理されるものとする。

注 5) OE は、Environment の objectives を表す。

2) OE.Term_TSF

カード関連機器は、住基カードが認証で用いるTSFデータを安全に扱い、認証処理が終わると消去する。

3) OE.Term_Mgt

カード関連機器は不正使用防止機構を備えていること。

4) OE.Hardware:

TOE は物理的に安全なハードウエア上で動作する。

PPには、更に、Security environmentの個々に対し、Objectivesの妥当性が詳しく説明されている。以下に、T.Logical_attack, T.Untrust_Path に対し記述されている Objectives の妥当性を示す。

1) T.Logical_attack に対する objectives の妥当性

T.Logical_Attack は、O.Identification、O.Authentication、OE.Term_TSF で対抗している。

O.Identificationにより、TOE外からアクセスしてくるユーザ(カード発行者、住民)やカード内のアプリケーションは識別される。

更に、O.Authentication によって、カード発行者、住民と認証されたユーザのみが利用可能な論理インタフェイスが明確になるので、ユーザデータの悪用が防止できる。また、端末の業務プログラムからTOE内のユーザデータへのアクセス手段はO.Authenticationによって、論理インタフェイスに限定されている。

また、ユーザを認証する際、外部から認証のためのデータがReader/Writerを経由して、TOEへ送られてくる。このようなデータの TOE 外(IT 機器)での安全性は OE.Term_TSF で保証される。

2) T.Untrust_Path に対する objectives の妥当性

T.Untrust_Path は O.Secure_Path で対抗している。

O.Secure_Pathにより、住基カードとReader/Writer間の通信データは、データフォーマット分析防止対策が施されるので、通信データを盗んでもユーザデータや TSF データを推定することは出来ない。

③ セキュリティ要件(Security requirements)

②で定義した Security objectives は、CC (Common criteria) Part2 で規定される機能要件、および part3 で規定される保証要件に展開される。表 23 に、住基用 IC カード PP が定義している機能要件と

の対応関係を示す。縦軸が Security objectives で、横軸がコンポーネントレベルの Functional requirements である。表中で、Pとあるのは直接関係する機能要件、Sとあるのは支援の機能要件、Dは依存関係から導かれる機能要件である。また、保証要件は EAL4+AVA_VLA.4 である。

| Objectives \ Functional Requirements | | 1) FCS_CKM.2 | 2) FCS_CKM.4 | 3) FCS_COP.1 | 4) FDP_ACC.1(1) | 5) FDP_ACF.1(1) | 6) FDP_ITC.1 | 7) FIA_AFL..1 | 8) FIA_ATD.1 | 9) FIA_UAU.1 | 10) FIA_UAU.4 | 11) FIA_UAU.5 | 12) FIA_UAU.6 | 13) FIA_UID.1(1) | 14) FMT_MSA.1(1) | 15) FMT_MSA.3(1) | 16) FMT_MTD.1 | 17) FMT_SMF.1(1) | 18) FMT_SMR.1(1) | 19) FPT_SRT.1 | 20) FPT_SEP.1 | 21) FPT_TST.1 | 22) FTP_ITC.1 | 1) FDP_RIP.1 | 2) FDP_ACC.1(2) | 3) FDP_ACF.1(2) | 4) FPT_PHP.3 | 5) FMT_MSA.1(2) | 6) FMT_MSA3(2) | 7) FMT_SMF.1(2) | 8) FMT_SMR.1(2) | 9) FIA_UID.1(2) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1) O.Identification | | | | | | | | P | | | | | S | | | | | | | | | | | | | | | | | |
| for TOE | 2) O.Authentification | D | D | S | P | P | S | S | P | P | S | S | S | D | D | D | P | P | P | | | | | | | | | | | | |
| | 3) O.Domain | | | | | | | | P | | | | | | | | | | | | P | | | | | | | | | | |
| | 4) O.Secure_Path | S | S | S | D | D | P | | | | | | | | | D | | | | | | | P | | | | | | | | |
| | 5) O.Retention | | | | | | | | | | | | | | | | | | | P | | D | | | | | | | | | |
| | 6) O.Forgery | | | | | | | | | | | | | D | | | | S | P | | | | | | | | | | | | |
| for Environment | 2) OE.Term_TSF | | | | | | | | | | | | | | | | | | | | | | | P | | | | | | | |
| | 3) OE.Term_Mgt | | | | | | | | | | | | | | | | | | | | | | | | P | P | | D | D | D | D | D |
| | 4) OE.Hardware | | | | | | | | | | | | | | | | | | | | | | | | | | P | | | | | |

**表 23 Security objectives - Functional requirements 対応表**


| Objectives \ Functional Requirements | | 1) FCS_CKM.2 | 2) FCS_CKM.4 | 3) FCS_COP.1 | 4) FDP_ACC.1(1) | 5) FDP_ACF.1(1) | 6) FDP_ITC.1 | 7) FIA_AFL..1 | 8) FIA_ATD.1 | 9) FIA_UAU.1 | 10) FIA_UAU.4 | 11) FIA_UAU.5 | 12) FIA_UAU.6 | 13) FIA_UID.1(1) | 14) FMT_MSA.1(1) | 15) FMT_MSA.3(1) | 16) FMT_MTD.1 | 17) FMT_SMF.1(1) | 18) FMT_SMR.1(1) | 19) FPT_SRT.1 | 20) FPT_SEP.1 | 21) FPT_TST.1 | 22) FTP_ITC.1 | 1) FDP_RIP.1 | 2) FDP_ACC.1(2) | 3) FDP_ACF.1(2) | 4) FPT_PHP.3 | 5) FMT_MSA.1(2) | 6) FMT_MSA3(2) | 7) FMT_SMF.1(2) | 8) FMT_SMR.1(2) | 9) FIA_UID.1(2) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1) O.Identification | | | | | | | | P | | | | | S | | | | | | | | | | | | | | | | | |
| for TOE | 2) O.Authentification | D | D | S | P | P | S | S | P | P | S | S | S | D | D | D | P | P | P | | | | | | | | | | | | |
| | 3) O.Domain | | | | | | | | P | | | | | | | | | | | | P | | | | | | | | | | |
| | 4) O.Secure_Path | S | S | S | D | D | P | | | | | | | | | D | | | | | | | P | | | | | | | | |
| | 5) O.Retention | | | | | | | | | | | | | | | | | | | P | | D | | | | | | | | | |
| | 6) O.Forgery | | | | | | | | | | | | | D | | | | S | P | | | | | | | | | | | | |
| for Environment | 2) OE.Term_TSF | | | | | | | | | | | | | | | | | | | | | | | P | | | | | | | |
| | 3) OE.Term_Mgt | | | | | | | | | | | | | | | | | | | | | | | | P | P | | D | D | D | D | D |
| | 4) OE.Hardware | | | | | | | | | | | | | | | | | | | | | | | | | | P | | | | | |


また、表 23 の対応関係の中で、O.Authentication に対して記述されている Functional requirements の妥当性を以下に示す。

1) O.Authentication に対する functional requirements 選定の妥当性

O.Authentication は、以下の 7 つの機能要件で実現される。

FIA_ATD.1 User attribute definition

FIA_UAU.1 Timing of authentication

FDP_ACC.1(1) Subset access control

FDP_ACF.1(1) Security attribute based access control

FMT_MOF.1 Management of security functions behaviour

FMT_MTD.1 Management of TSF data

FMT_SMR.1(1) Security roles

FIA_ATD.1 により、TOE へアクセスしてくるユーザ、すなわち、カード発行者、住民、カード関連機器、カード内のアプリケーションは識別される。FIA_UAU.1 により、TOE の識別、認証処理を行わないで、提供される TSF mediated-actions [注6]) が明確になる。すなわち、FIA_UAU.1 の [assignment:

list of TSF-mediated actions]に記述された以外の TSF mediated actions は識別、認証が必須となる。具体的なユーザ(カード発行者、住民、カード関連機器)、操作可能な operations、assets の一覧は FDP_ACC.1(1)で明確になり、その時に適用される rule は FDP_ACF.1(1)で示される。

また、FMT_SMR.1(1)により、住基カードの TOE に対する管理的役割(鍵設定、初期 PIN 設定、行政サービスに利用可能状態に設定)が明確になり、FMT_MOF.1 により、管理的役割と機能の関係が、また、FMT_MTD.1 により、管理的役割と TSF データの関係が明確になる。これらの要件は、TOE の Objectives をサポートする要件が、効率的に運用されるために必要な要件である。

注6) ここで言う TSF mediated action (TSF 調停アクション)とは、TOE が識別・認証処理の途中で出力する以下のメッセージ出力処理が該当する。

- 識別情報、認証情報の入力を督促するメッセージ
- 入力した識別・認証情報に関するエラーメッセージ等

以下は、O.Authentication を強化する 6 の supportive な要件である。

FIA_AFL.1 Authentication failure handling
FIA_UAU.4 Single-use authentication mechanisms
FIA_UAU.5 Multiple authentication mechanisms
FIA_UAU.6 Re-authenticating
FDP_ITC.1 Import of user data without security attributes
FCS_COP.1 Cryptographic operation

FIA_AFL.1 により、認証失敗時の TSF action が明確になり、攻撃者の攻撃チャンスを少なくする。FIA_UAU.5 により、TOE のサポートするユーザ認証の authentication mechanisms が明らかになる。また、それらの内、最低、住基カードの発行業務に使われる端末の authentication mechanisms には、FIA_UAU.4 により、再利用の出来ない authentication data(ex. Challenge data)の生成を要求しているので、発行用端末になりすますことを難しくしている。FIA_UAU.6 により、re-authentication を行うタイミングが明確になり、作業域へ展開した assets の漏洩が防止される。

FIA_UAU.5 のユーザ認証 mechanisms の中には、住基仕様に規定される external authentication mechanisms が含まれる。それらの実装においては、暗号の専門家による攻撃に耐えられるだけの標準のアルゴリズム、鍵サイズを採用する必要がある。これらの要件は FCS_COP.1 で明確になっている。また、鍵の初期設定には FDP_ITC.1 で指定されるポリシーに則り、外部から TOE 内に安全に設定される。

FCS_CKM.2、FCS_CKM.4、FIA_UID.1, FMT_MSA.1(1)、FMT_MSA.3(1)は dependency で必要となる要件である。

TOE が実装すべき、機能要件一覧を、エレメントレベルで付録に載せる。

住基用 IC カード PP では、脅威 T.Hardware に対して、環境の目標 OE.Hardware で対抗している。すなわち、T.Hardware への対抗策は、TOE のセキュリティ機能では無い。そのため、脅威等の詳細な説明はされていない。詳細な説明は、2003 年 5 月フランスで承認された JICSAP part1 PP に載っている。以下にその概要を示す。

(3) JICSAP part1 PP が定義する脅威

住基用 IC カード PP は、論理インタフェイスに着目したソフトウエア的なセキュリティ要求書である。住基カードの IC チップへの物理的な攻撃に対しては、JICSAP part1 PP が要求するセキュリティ要求事

項を満たすように推奨している。この推奨 PP では、半導体や暗号の専門化が、専用の装置を使い、素子レベルの攻撃を仕掛けてくることを想定している。以下に Security environment に記述されている脅威の概要を示す。

1) Micro_attack:

IC チップのパッケージ樹脂や絶縁膜を取り除いた IC に対し、FIB Focused Ion Beam、EBP(Electron Beam Prober)、AFM(Atomic Force Microscope)攻撃をかけ、

- 記憶素子の内容や回路を調べる(Reverse Engineering)
- 記憶素子や回路を変更する(test 回路の復元、保護セキュリティ回路の無効化)

2) Covert_channel:

Covert channel から出てくる IC の内部処理情報を分析し、データを推定するかもしれない。

IC の設計上の外部インタフェイスを i/o ports と言う。これに対し、内部処理を推測出来る可能性のある情報ルートを隠れチャネル(Covert channel, side channel)と呼ぶ。IC の場合、隠れチャネルへの攻撃手段として、以下が考えられる。

- SPA(Simple Power Analysis)/ DPA(Differential Power Analysis)攻撃: IC 内での消費電力の統計的分析により暗号化の鍵を推定する。
- Timing 攻撃:様々な入力データの IC 内での処理時間を比較・分析することで、暗号化の鍵を推定する。
- 漏洩電磁波攻撃:IC からの漏洩電磁波を分析し、復号されたデータを推定する。

3) Fault generation(Malfunction):

攻撃者は、異常な環境で IC を動作させることで、記憶素子や回路の動作を不安定にさせ、セキュリティ関連情報を推定する。

異常環境の発生方法には以下がある。

- DFA(Differential Fault Analysis)攻撃:IC 内の CPU に低レベルのイオンを照射する(exposing a processor to a low level of ionizing radiation)ことで、処理中のビットを強制変更し、正常処理の結果との差分を取る事で、暗号化の鍵等を推定する。
- 記憶素子の電気特性(例えば、time delay)を悪用するため、IC への供給電圧やクロックを急に変えたり(Glitch 攻撃)、異常な温度の基で IC を稼動させたりして、
- ソフト上意味をあるデータ(TSF データ)を漏洩させる。
- セキュリティ対策のため設けられたセキュリティ回路を動作不能にする。

4). Interface attack:

製造段階で、品質テスト、ソフトウエアのロード、暗号化の鍵設定等に使われたり、また、製品出荷後のメンテナンスに使われたりする、住基カードの運用に不必要な i/o ports を悪用し、データを漏洩・改ざんする。

(4) Composite ST

住基カードは、様々な企業(責任組織)を介在して作られることが多い。図 23 は、その一例を表している。

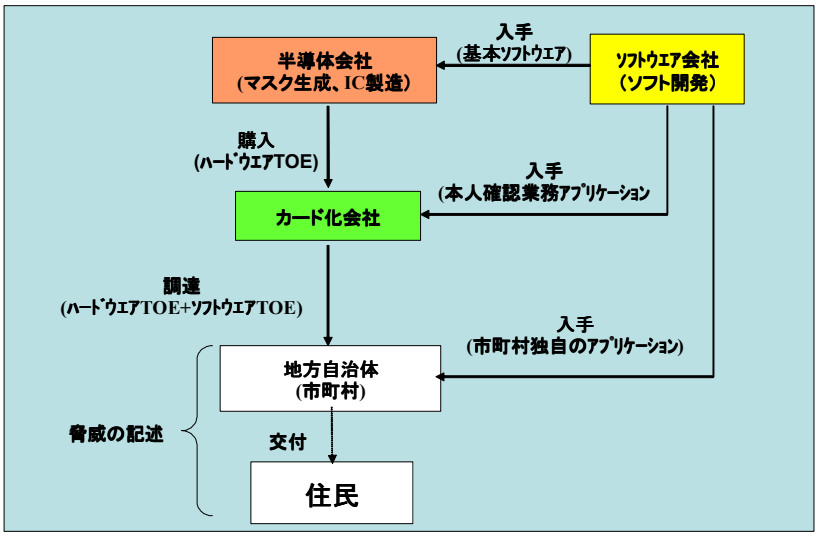



**図 23 住基カードの開発手順(例)**

半導体会社は、IC に焼付けるマスク用のソフトウエア情報をソフトウエア会社より調達し、IC の製造を行う。カード化会社は、モジュール化された IC を購入し、カードに仕上げる。本人確認業務アプリケーションが住基カードに設定されるのは、図では、カード化の段階であるが、IC 製造段階でもよい。カード発行は、住基カードの場合地方自治体である。地方自治体では、住基カードに市町村独自のサービスのためアプリケーションプログラムのロードやサービス環境を設定し、住民に渡される。住民は、渡されたカードでサービスを受けると同時に、新たなサービスを追加する(新たなアプリケーションプログラムのロード)こともできる。

このような一連の流れで作られ、利用される住基カードに対し、評価する必要のあるのは、カード化会社から地方自治体へ納入される時点のカードである。すなわち、納入する住基カードに対し、評価に必要な証拠資料(基本ソフトウエアに関する証拠資料、IC に関する証拠資料)を用意する必要がある。

半導体会社の製造する IC は色々な組織に販売される可能性がある。色々なカード化の組織が製品評価を受ける度に、同じ IC の評価を繰り返すのは、全体としての評価効率が悪くなる。これを解決しようとして、JIL(Joint Interpretation Library)の場で検討されている評価のプロセスを示したのが図 24 である。

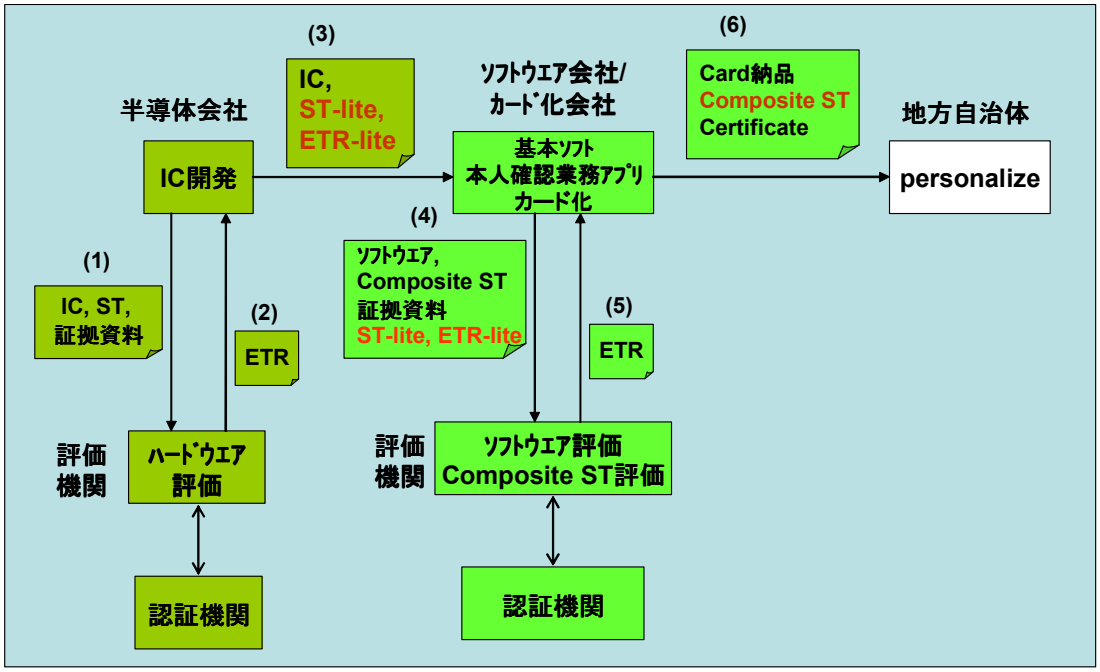



図 24 製品評価のプロセス

(1), (2)は、IC の評価プロセスである。このプロセスで ST や ETR(Evaluation Technical Report)が作成される。また、住基カード評価に必要なハードウエア資料を ST-lite, ETR-lite と呼ぶ。

(4), (5)は、地方自治体へ納入するカードの評価プロセスである。この場合、ST には、評価対象である IC、基本ソフトウエア、本人確認業務用アプリケーションが含まれる。このような複数の製造業者(異なる責任主体)からなる製品の ST を Composite ST と呼んでいる。

これが、Composite 製品の効率的な評価のアプローチであるが、未だ検討・試行段階にあり、以下のことを解決する必要がある。

・Composite 製品の認証

他国で認証を受けた製品(LSI chip)を包含する製品(住基カード)の認証方法。

・PP 準拠の Composite ST

準拠すべき PP が複数ある Composite ST で、個々の PP の要求事項に関連性がある場合の Composite ST での記述方法。

・ST-lite、ETR-lite の形式

Composite 製品評価に必要な ST-lite、ETR-lite の内容。

地方自治体における住基カードの調達においては、Composite ST の確認を基本とすべきである。しかし、Composite 製品の評価方法に関して国際的な合意が得られるまでには時間が掛かる。それまでの間は、ハードウエア、基本ソフトウエア、それぞれの ST を個別に確認するのが、現実的と思われる。

### 3-5-1-5 電子投票システムへの IC カード PP の適用

平成 14 年度の次世代電子投票・アンケートシステムとその社会的利用に関する研究によると、電子投票システムに必要とされる 11 の投票特性を定義している()。

表 24 電子投票システムの投票特性

| 投票特性 | 定義 |
|---|---|
| 完全性 | 不正が無ければ、正しく投票が行われること。 |
| 健全性 | 投票を混乱させることが不可能なこと。 |
| 有権者確認可能性 | 有権者のみが投票者になれること |
| 二重投票不能性 | 有権者が一回のみ投票できること |
| 無記名性 | 投票者の投票結果が秘密であること |
| 公平性 | 選挙が終了するまで、何人たりとも投票の途中経過を知ることが出来ないこと。 |
| 検証可能性 | 集計結果を検証できること。 |
| 買収不能性 | 投票者は投票結果を偽れること。 |
| 非待機性 | 投票者は投票後に拘束されないこと。 |
| 汎用性 | 様々な種類の投票に対応できること。 |
| 頑牽性 | 結託が出来ないこと。 |

（注）平成 14 年度‘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’P108 表 7 電子投票システムの投票特性の定義より

表 24 電子投票システムの投票特性

また、これらの投票特性を実現するために、システム構成要素（投票端末ハードウエア、投票端末ソフトウエア、管理者サーバハードウエア、管理者サーバソフトウエア、公開ボードソフトウエア、ネットワーク）が備える機能要件に展開できることを確認している。

そこで、今回は、投票システムのセキュリティ対策として IC カードが採用されるという前提で、有権者確認可能性、二重投票不能性に着目して、IC カードの PP を作成した。

図 25 に電子投票の想定手順を示す。有権者は、投票に先立ち、管理者サーバから投票用紙を入手し、投票端末に格納し、次に、公開ボードに載った立候補者名から特定の人を選び、投票用紙に氏名を転記し、管理者サーバに投票(送信)する。

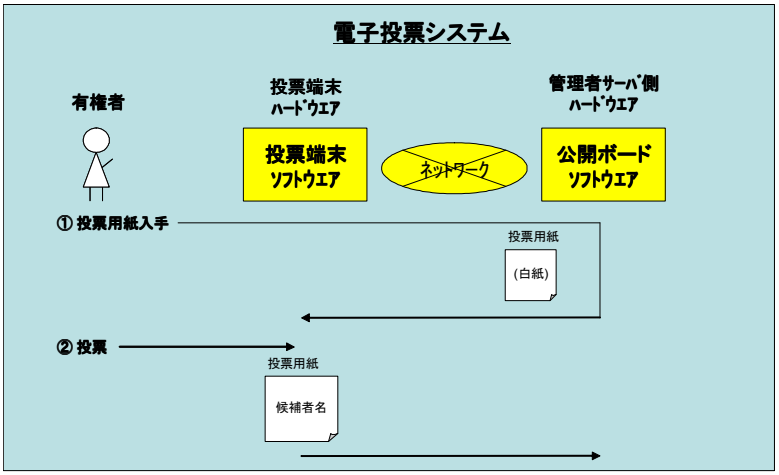



図 25 電子投票の想定手順

(1)有権者確認可能性への対応

図 26 は、有権者確認可能性‘有権者のみが投票者になれること’の意図することを表した脅威のイメージである。すなわち、有権者が管理者サーバから投票用紙を入手した後で、不正な人(攻撃者)が有権者に代わって、投票を行うと言うのが脅威である。

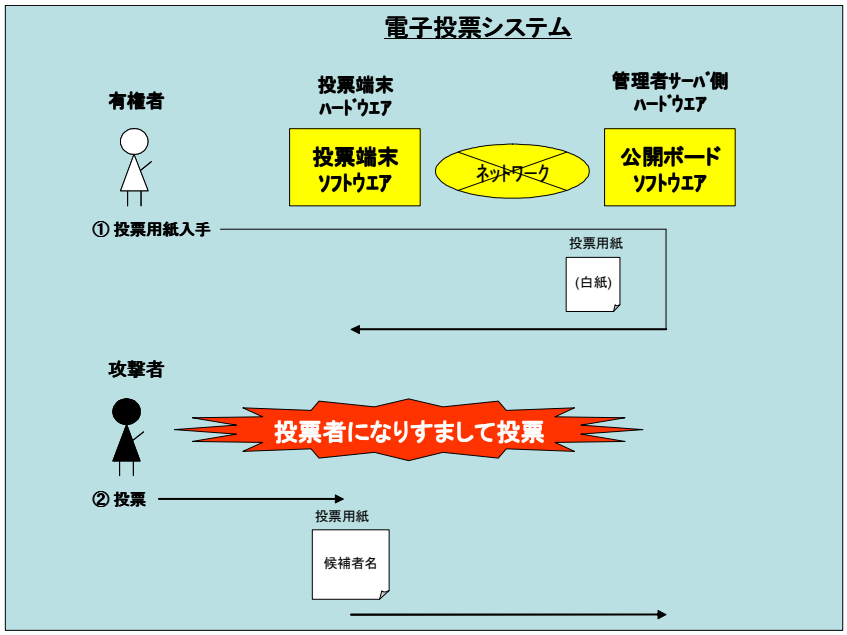



**図 26 有権者確認可能性の脅威イメージ**

この脅威に対し、電子投票システムとして、様々な対策が考えられる。IC カードが採用されるとした時の対策の一例を図 27 に示す。この例では、有権者に事前配布される IC カードに、投票という権利行使にはカードの所有者確認必要と言う条件が設定されているとしている。

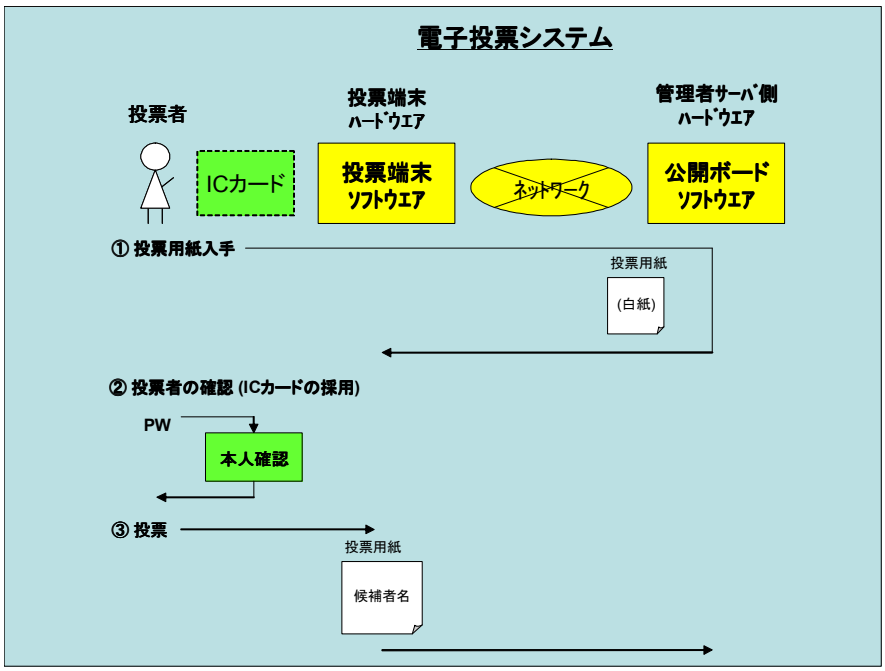


**図 27 電子投票システムでの対策例**

図 26 の脅威, 図 27 の対策例を CC の脅威(Threats) ⇒ 設計目標(Objectives) ⇒ 機能要件(Functional requirements)に展開すると、以下のようになる。

脅威: 不正な人が、投票権のあるひとになりすまし、投票を行う。

⇩

設計目標: TOEは、投票権のある人を特定する機構を備えなければならない。

⇩

機能要件: FIAクラス(パスワードによるユーザ認証機能等)が必要である。

⇩

セキュリティ機能: TOEは、本人(所有者)の確認機能を有する。

ただし、最後のセキュリティ機能は、製品に実装される内容なので、PP には表れず、ST(Security Target)で明確にされる。

(2) 二重投票不能性への対応

図 28 は、二重投票不能性 ‘有権者が 1 回のみ投票できること’の意図することを表した脅威のイメージ図である。すなわち、有権者が②で正規の投票をしたにもかかわらず、③で再度、投票を行うと言うのが脅威である。

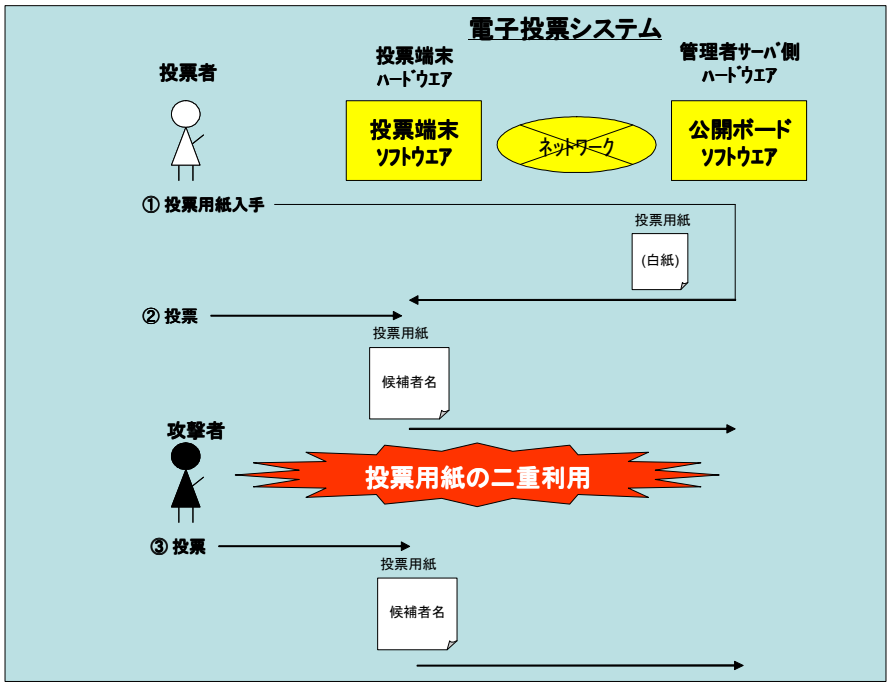



**図 28 二重投票不能性の脅威イメージ**

この脅威に対しても、電子投票システムとして様々な対策が考えられる。IC カードが採用されるとした時の対策の一例を図 29 に示す。この例では、IC カードと公開ボードソフトウエアの連携で対応している。IC カードでは、投票データに対し、電子署名を生成している。また、公開ボードでは、署名を利用し手、投票内容の改ざんチェックを行うと同時に投票内容の重複チェックも行っている。

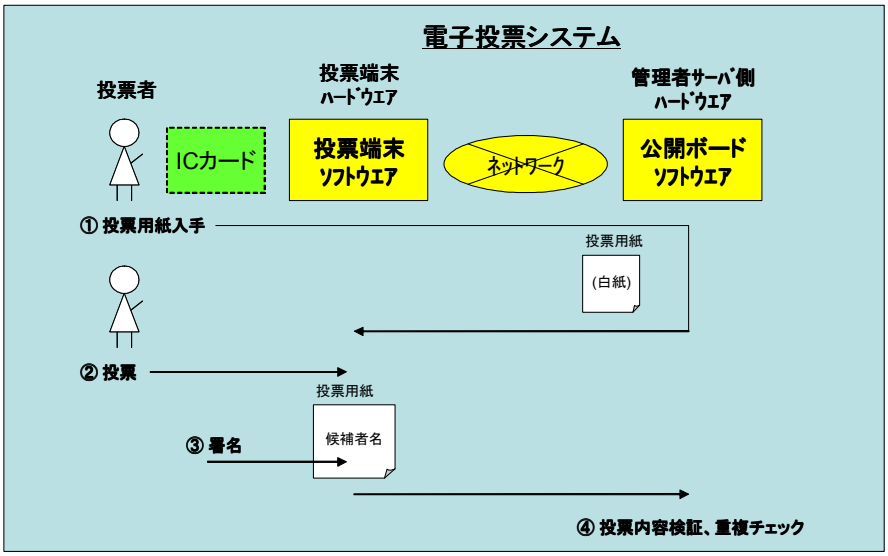



**図 29　電子投票システムでの対策例**

図 28 の脅威、図 29 の対策例を CC 的に書き直すと、以下のようになる。

Threats: 投票権のある人が、2回投票を行う(投票用紙を2回使う)。

⇩

Objectives: TOEは、投票事実を生成する機構を備えなければならない。

Objectives(環境): 環境は、投票事実の重複をチェックする機構を備えなければならない。

⇩

Functional requirements:
FCSクラス（投票事実の生成：ディジタル署名）が必要である。

### 3-5-1-6　次世代電子投票におけるPP設計の課題

本年度、11 の投票特性の中から、有権者確認可能性、2 重投票不能性の二つを例として取上げ、脅威エージェント、資産、攻撃方法を明快にしつつ、設計目標、必要な機能要件へと PP 的に展開した。残りの投票特性に対しても、同様のアプローチで、検討を進めれば、電子投票システムとしてのPP設計が可能と考える。

その際、以下の視点を配慮しつつ、電子投票システム用の PP 作成する必要がある。

・国際的に整合した投票特性

Internet voting については、多くの国や組織で検討されている。しかし、電子投票システムが持つべき特性について、統一された、まとまった考えは未だ無いようである。ヨーロッパで検討されている一例を以下に示す。

1) Votes cannot be intercepted nor modified,
2) Votes cannot be known before the official ballot reading,
3) Only registered voters will be able to vote,
4) Each voter will have one and only one vote,
5) Vote secrecy is guaranteed. It NEVER will be possible to link a voter and his/her vote,
6) The voting web site will resist any denial of service attack,
7) Voters will be protected against identity theft,
8) The number of cast votes will be equal to the number of received ballots,
9) It will be possible to prove that a given citizen voted,
10) The system will not accept votes outside the ballot opening period,
11) The system will be auditable.

(http://www.geneve.ch/chancellerie/E-Government/e-voting.html)

平成14年度の報告書で定義されている 11 の投票特性について、国際的な整合性の視点から、見直す必要がある。

・ IC カードの役割 (機能)の明確化

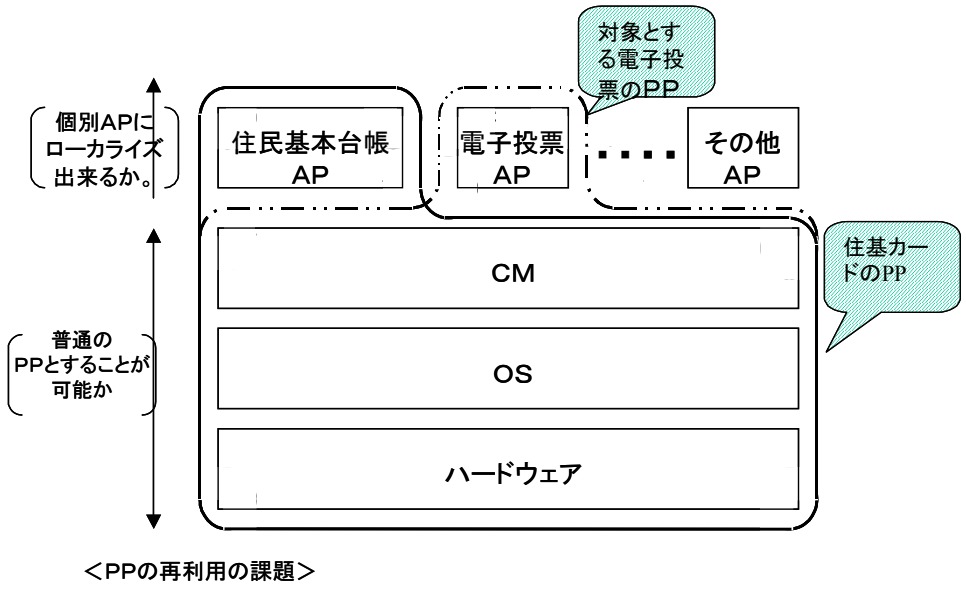
11 の投票特性を実現するため、電子投票システムの構成要素での分担方法について、脅威エージェント、情報資産、攻撃方法、等を明確にしつつ、IC カードの分担を明確にする必要がある。このための、セキュリティ要件からみて再度、検証すべきである。

・ PP の認証と利用者拡大の準備

住基カードでは PP の認証を取り、地方自治体の調達の公開性に貢献した。電子投票で使われる IC カードの PP も認証を取り、更に、英文版の PP を公開することで世界の組織で利用可能な環境を整えておくことも大切である。

### 3-5-1-7 電子投票システムとの差異

本節では、3-5-1-4 参照モデル(住民基本台帳におけるICカードプロテクションプロファイル)の概要で述べた住基カードの概要にもとづいてこれを、電子投票に適用する際の技術的問題点について考察を加える。検討の狙いは、出来るだけ既に開発された、住基カードの PP を電子投票に用いること(再利用)することである。




＜PPの再利用の課題＞

**図 30 住基カードPPと電子投票システムICカードのPPの関係**

上図に示すように、参照する住基の PP と、電子投票の PP とは、IC カードをともに使用するという意味で、IC カードのハードウエア、OS、CM（カード管理:ミドルウェア）は共通のセキュリティ要件が使えると考えられる。

しかし、当然のことながら電子投票と住民基本台帳は利用分野が異なるので、異なるようセキュリティ要求条件があると考えられる。したがって、その差異が PP の領域にどの様に影響してくるかを考察する

(1) PP 再利用の観点からの検討

脅威分析からPP及びSTも含めて一連の流れを、CCの機能要件を中心に整理してみると、図1．7．2のようになる。そこで、共通プラットフォームとマルチアプリケーションのPPについて、共通プラットフォームに要求されるPPの考察をすると次のようなステップで共通プラットフォームのPPの特性が明らかになる。

(イ) アプリケーションによって、脅威は異なる。

(ロ) 新たに加わるAPのPPは、APファイアウォールを前提とすべき

(ハ) AP独自のPPは、共通プラットフォームのセキュリティ機能とAPの機能との結合で作られる

(ニ) 共通プラットフォームの全体のPPは、各々のAPのPPの和集合である。

(ホ) 従って、新たなAPのPPの中を実現するために、それまでの共通プラットフォームのセキュリティ機能で実現が不可能な場合には共通プラットフォームに新たなセキュリティ要件としてPPを付け加える必要がある。

(ヘ) すなわち、自然に共通プラットフォームのPPは自然増殖するものであるが、現実のOSなどが現状の機能で充足しているように、共通プラットフォームのPPは飽和するであろう。

(ト) こうしてできた、共通プラットフォームの全体のPPはマルチアプリケーションに再利用可能なPPということができる。

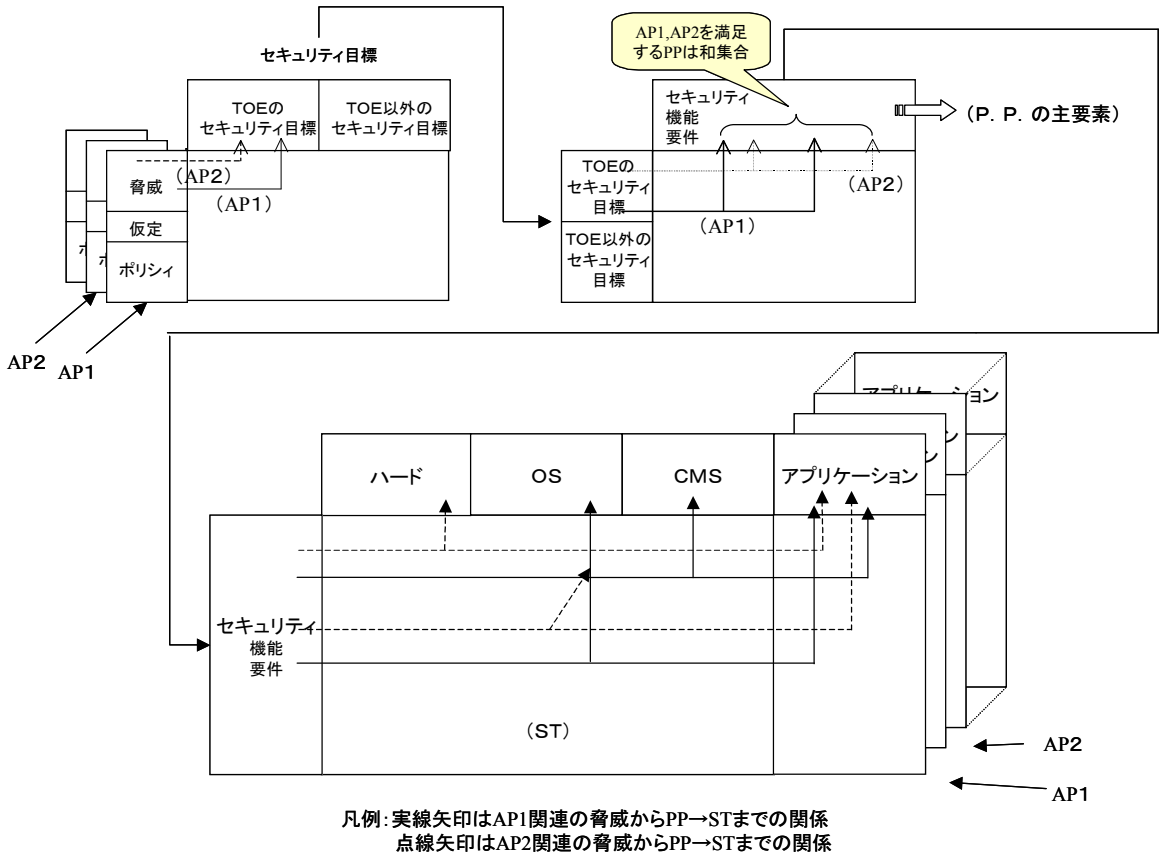



**図 31 マルチアプリケーションカード AP の脅威分析から PP/ST への流れ**

(2) 電子投票におけるICカードに蓄える情報資産について

平成14年度の検討では、CCの電子投票システムとしての検討が行なわれた。ここでの手法を分析すると、結論としてセキュリティの要件の中にICカードの必要性が生まれてこない。これは、情報資産の蓄積に関するセキュリティポリシーが設定されていないということに起因する。図 32 にその様子を示した。セキュリティポリシーによっては、電子投票をICカード無しで実現することも可能ということになる。現実に投票所で専用の端末から電子的に投票する電子投票もある。次世代電子投票として新たに、在宅で投票するという条件を加えて、初めて、ICカードの要求条件が個人認証をネットワークを介して行なうという機能要件が生じてくる

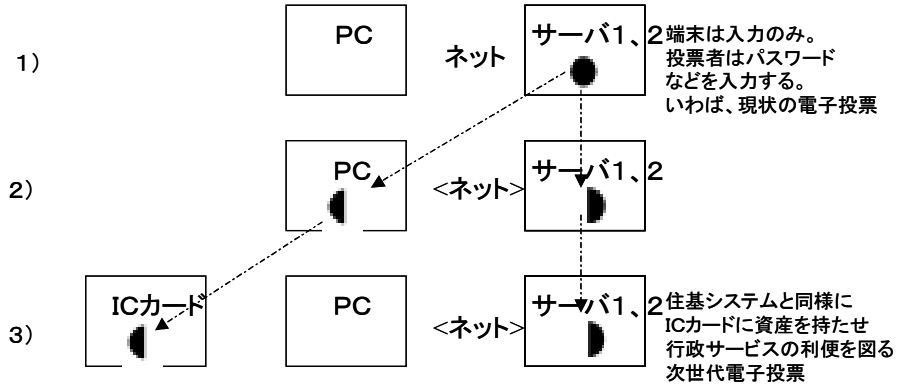



**図 32 情報資産の置かれる場所によることなる電子投票システム**

## 3-5-2　システムＰＰに関する内外の状況

### 3-5-2-1　システムPPに関する検討課題

PPは IS015408（以下、CCと略す）で書式や内容が定義されたセキュリティ要求仕様書であり、システムPP、即ちシステムを対象とする特別なPPの区分や規定はCCにはない[注7]。PPの対象（以下、TOEと略す）がシステムであっても製品であっても同じ基準でPPは書かれることとなる。

しかし公表されているPPの大部分は製品をTOEとしたもので、システムをTOEとするPP作成にあたってはいくつかの解決すべき事項或いは決断すべき事項のあることが現実である。

（1） システムの定義（システムの範囲）

JIS用語[注8]において、情報システムは「情報処理システムと、これに関連する人的資源、技術的資源、財的資源などの組織上の資源とからなり、情報を提供し配布するもの」と定義され、またCCにおいて、システムは「（IT）の特定の設置・設定を行ったもので、特定の用途と運用環境を伴うもの」としている[注9]。両方が共通して「複数のHW、SW、FWの結合体＋特定の用途設置設定条件＋運用環境（物理的、手続的、人的、等）」を包含したものとしている。

一方、PPを規定しているCC part1 では scope において、「CCは IT Products と System のセキュリティ特性の評価における基盤として使われることが意図されている」、「IT セキュリティ対策に直接関わらない管理的セキュリティ対策（組織的対策、人的対策、物理的対策、手続き的対策）に関するセキュリティ評価基準はCCに含まない。TOEの運用環境における管理的セキュリティ対策は前提条件として扱われる」と記述されている。これら二つの記述の整合には、明白な矛盾ではないものの疑問がある。実際に、評価対象としない管理的セキュリティ対策に関しては評価対象である技術的セキュリティ対策に必要なセキュリティ機能要件の記述に関するような詳細な規定がCCに含まれていない。

注7）米国 Digital Bond, Inc. が、システムを構成する製品の組み合わせ、実装、セットアップ詳細情報を記述する文書をシステムPP（SPP）としてCCに盛り込むようにインターネット上で提案している。

注8）JIS－X－0001

注9）CC用語定義（CC part1 の Definitions）

（2） システムPPの使われ方

PPの役割は周知のとおりITのセキュリティに関する要求事項（機能及び保証レベル）を記述した（ユーザからの）要求仕様書である。さらに、ベンダーが製品及びSTを開発する基盤としてそのPPが使われ、そのSTに基づいてその製品のセキュリティ評価・認証が行われることを想定している。

しかしながら、上述のとおりPPの規定やCCがシステムに不可欠な運用環境を含む管理的セキュリティ対策に関する詳細な規定や評価基準を含んでいないこと、及び後述するようにシステムのセキュリティ評価の大変さ等から、システムに対してCCが想定しているPP・ST・評価・認証の全行程を適用した例は殆どない。

その一方で、ITのセキュリティに関する要求事項を記述した要求仕様書規定としての完成度やセキュリティ仕様を記述する共通様式・用語としての利点、系統的なセキュリティ設計の指針となる利点を活用すべく、ST・評価・認証を切り離して仕様記述のためだけにPPを作成する動きがある。その場合、CCで詳細に規定していない運用環境を含む管理的セキュリティ対策の領域に対するPPの有効性を確保するためには、それらに関

する詳細な規定を何らかの方法（例えば、IS017799やFIPS SP800-53Draft等を併用するなど）で補うことが望ましい。

今後、CCが想定しているPP・ST・評価・認証の全行程をシステムに適用するためには、後述するシステム評価及びそのために必要となるシステムのSTの作成を念頭において、システムのPPに工夫を加える必要がある。

(3) システム評価

IT 利用者のニーズは、自分が使用するシステムの一部を構成している製品がセキュアであることよりは、システム全体がセキュアであることである。その意味で、ITセキュリティ評価においてシステム評価のニーズは大きい。システム評価が最終目標で、製品のセキュリティ評価はそこに至る通過点であり、システム評価を構成する部分評価として重要である。

しかしながら、人間系による運用管理を除外した IT 技術面だけに絞っても、CCに基づくシステムの評価には多くの作業が必要であり、システムのような大きな対象物を評価する効率的な評価方法は確立できていない。各国で提案し、チャレンジし、議論されている段階である。

システムの評価に関してのチャレンジは大きく3つの方向で取り組まれている。

ひとつはCCが評価対象外として詳しいセキュリティ要件を定義していないITの環境及び人間系による運用管理の部分、及びITの技術面であるが他の標準に預けて除外した暗号などに関して、他の標準を併用してシステム全体のセキュリティを確認しようとするもので、その方式が検討されている。（一方では、CCを拡張して運用管理を含めてCCでカバーせよという意見もある）

二つ目と三つ目は、運用等を除きITシステムの技術面に絞ってシステム評価をする試みである。これは大規模な評価対象の効率的な評価を行うためにシステムの持つ特性に着目した検討で、一つ目の取組みと補い合う取組みである。

まず、ライフサイクルの段階ごとにかかわる事業者が異なるスマートカードにおいて、下位のレイヤの評価結果を活用する形での評価が幾つか報告されており、CCに基づくシステム評価の例としてはもっとも先行している。このチャレンジの中から、ある評価結果を、それを包含するシステムの評価に利用するための報告書（ETR－LITE）が生まれてきたことは、システム評価への大きな足がかりである。

もうひとつのチャレンジは、構成要素が垂直につながって上位のものに下位のものが包含されるレイヤ構造が大部分のスマートカードとは異なり、構成要素が水平垂直両方向のつながりを持つ一般的なシステムの評価に対する取り組みで、幾つかのチャレンジが報告されている。さらに、後述する自国政府向けに限定して実施されている英国のシステム評価が実績もあり、制度の評価基準文書が公開されている段階に達している貴重なものである。このチャレンジにはいろいろなアプローチが見られるが、システムの構成要素それぞれに対する部分評価とそれらの繋ぎや機能分担に着目したシステム全体評価とを組み合わせるcomposite approachと呼ばれる方向に向かっているようである。

評価の元となるシステムのSTやPPに関して見ると、スマートカード評価においては現行のCCの規定がそのまま適用できている。一般的システムのSTやPPに関しては、ほとんど公開されている情報がない。防衛庁（技術研究本部）が行った調査[注10]では、英国のシステム評価においてはシステムの構成要素それぞれのSTに加えて、システムの構成要素の繋ぎや機能分担に着目したシステム全体のSTを作っている。

注 10）情報セキュリティ評価・認証に関する調査検討報告書（防衛庁技術研究本部　平成15年10月）

(4) スマートカードのPP

昨年度調査についての補足をする。

掲題の調査報告に含まれる Intersector Electronic Purse and Purchase Device Protection Profile(IEP&PD PP) Version1.3 March 2001 は、同報告の表 5-3-4 に示すとおりスマートカード(チップ及びカードOS)をプラットフォームとするアプリケーションに関するPPである。

同報告の図 5-3-8 Intersector Electronic Purse and Purchase Device に「上記範囲内に記述することは出来ない」とされていたが、下図に示すとおりR／WとMulti APのひとつをTOEの範囲としている。(下線部は引用文)

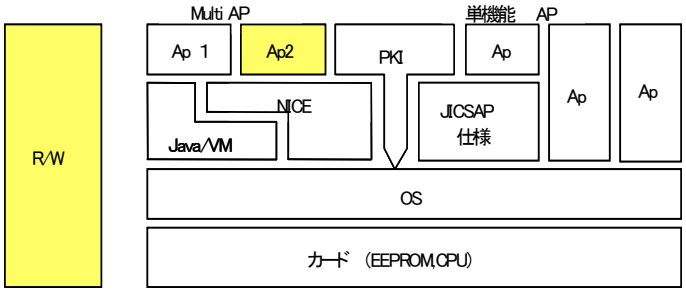



**図 33 平成15年度の E purse(電子財布)のプロテクションプロファイルの領域**

同報告の表 5-3-4 にこのPPの主要な内容が書かれているとおり、TOE の範囲は電子財布と POS の双方、対象資産は汎用の電子財布の支払いシステムとその環境、脅威として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、真正性の消失を挙げている。

TOE のセキュリティ対策目標として、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 を挙げている。

このPPのTOEの範囲と、プラットフォーム上の位置付け及びアプリケーションの社会的位置付けは、次世代電子投票システムの IC カードの TOE の範囲と類似しており、アプリケーションに関連する記述は異なるが、次世代電子投票システムの IC カードプロテクションプロファイル作成に当たって参考になり得る。

### 3-5-2-2 海外の状況(特に英国での検討状況)

(1) 英国国内基準によるシステム評価

英国におけるCCに基づくITセキュリティ評価の認証機関であり、政府機関であるCESG[注11]が、システム評価サービス(SYS Level Evaluations)を自国の政府機関向けサービスとして実施している。

このシステム評価はCCに基づくITセキュリティ評価とは別の仕組みとして行われており、相互承認協定であるＣＣＲＡ対象外である。しかしながら、公開されている評価基準 System Assurance Package Framework を見ると、基準はCCの評価基準である保証要件のサブセットに独自に強化した脆弱性評価が追加されたものであり、CCと無関係ではなく、関連性はかなり濃厚である。勿論、運用管理に関しては評価対象となっていない。

システム評価のためのシステム全体のつなぎに関する文書を作っていることは上述したとおりである。このシステム評価の実績や適用事例などはCCに基づくITセキュリティ評価とは対照的にインターネット上ではまったく入手できない。

注 11)http://www.cesg.gov.uk/

(2) 米国における(システム)PPと、C&Aの採用

米国においても、運用管理を除いたITシステムの評価に関する発表[注12]が行われているが、活発とは言えず、最近の情報もない。

ただ、システム評価を前提としないシステムのPP作成に関しては、継続的に検討成果がICCCなどで発表されている。

米国の医療情報システムの工業会であるHL7は、かなり早い時期にシステムのセキュリティ要件の記述にPPを用いる方針を打ち出した。理由はPPがセキュリティ要求仕様書の unify された基準である事だと聞く。

また、NISTからは、Process Control Security Requirement Forum と共同でCCに基づいた石油プラントなど Industrial Control 分野に対する IT セキュリティリスク低減の検討結果が発表されている。この発表では、セキュリティ要件記述の最終形をPPとしつつ、PPの書式に書き下ろす以前の検討結果が示されている[注13]。

同様に、CCを基盤としてPPに言及しつつ、米国の別のネットワークセキュリティ評価基準を併用してFAAのシステムのセキュリティ評価を検討した報告がMITRE社から出されている[注14]。

またCCとは別に、米国の政府機関においては、ITの運用許可のためのセキュリティ確認の手続きが、DITSCAP(国防省)、NIACAP(国防省以外の政府機関)として規定されている。これらの手続とCCに基づく評価認証の構造的な関係を明示する情報は入手できていないが、CCで評価された製品を採用することとDITSCAPやNIACAPの手続の両方を適用するようである。

注 12)http://niap.nist.gov/niap/events/pp-development-projectv2.pdf

注 13)http://www.isd.mel.nist.gov/projects/processcontrol/

注 14)http://www.mitre.org/work/tech_papers/tech_papers_03/abrams_faa/index.html

(3) ドイツ／フランスにおけるスマートカードPPと評価・認証

欧州はスマートカードの生産と利用で、日米より長い歴史を持ち、現時点で有している先行の利を維持するため、スマートカードのITセキュリティ評価に注力している。スマートカードはそのライフサイクルに対応したそれぞれのフェーズ(カードチップの製造、カードチップ上にカードOSを搭載、カードの形に成型、アプリケーションを搭載、所有者情報の書き込み、カードの使用、カードの廃棄)が異なった事業者により処理されるため、これをシステムと捉えた評価方法が欧州で工夫された。また、スマートカードをシステムとして捉える場合、前述したとおり構成要素が垂直につながって上位のものに下位のものが包含されるレイヤ構造が大部分であることが特徴である。従って、一つ前のフェーズの製品が次のフェーズのプラットフォームとなるので、次のフェーズで搭載される製品とプラットフォームを合わせたシステムとしてのセキュリティ評価が求められた。この場合、前の製品が評価認証されていれば、同じような評価を繰り返すことは効率的ではなく、関係者が工夫して前の評価結果を再利用するための文書としてETR－LITEが作られた。

2002のICCCでの発表[注15]によれば、ドイツで評価認証されたカードチップに、国境を越えたフランスでカードOSを搭載し、カードチップとカードOSを含めたシステムの評価認証がフランスで行われたと言うことである。

注 15)Composite evaluation best practice for Smart Card European Electronic Signature,
Jean-Marie ROUCAIROL & Wolfgang Pockrandt

(4) システム評価への提案・模索

今年のICCCは 9 月末にドイツで行われた。セッション総数63のうち、約20％にあたる12セッションの内容がシステム評価に関わるもので、発表者の国もいろいろであった。ITセキュリティ評価において、システム評価が求められ、各国がチャレンジしていることを示している。英国の制度に関しては、全く発表されなかった。

発表の内容は、運用を除いたシステムの評価方法の提案や独自の基準によるシステム評価の紹介、他の標準（BS7799やFIPS140-2等）との関連や併用、CC或いはBS7799を拡張する提案、システム評価の基本的なFrame Workに向けた提案など多岐に亘っている。

### 3-5-2-3　日本の状況

(1) JEITA電子政府PP

JEITA（当時はJEIDA）において、電子政府システムのPP作成プロジェクトが活動して、2000年10月にV0.2版、2002年2月にV1.0版のPPが発表された。これが日本のシステムに関するPPの最初のものである。これらのPP作成にあたって前項までに述べたいろいろな問題点に関する検討と判断がどのようになされたかは、PPそのものに明示される事項ではないため窺い知ることはできないが、PPの内容は、電子政府システム全体をひとつのTOEとして記述しており、それを構成する製品それぞれに関しての細分化やつながりに関する記述は見当たらない。また、運用管理に関する事項はPPの通常の記述方法どおり普通の文章で「環境によるセキュリティ目標」に書かれており、何らかの標準を併用した様子はなく、当然、評価対象外である。

(2) 防衛庁における調査

H13年度からH14年度にかけて防衛庁技術研究本部が中央大学に委託した調査検討*4 に研究において、システム評価に関しても調査報告が行われた。当時の世界各国から発表されているシステム評価に関する情報を先入観なく幅広く調査比較した報告は、その上に加えられた「有効と思われる方式」の考察と併せて、現在までのところわが国における唯一のものとして価値がある。

(3) 日立　永井氏の研究

永井氏は上記の防衛庁における調査で、システム評価に関する部分を主に担当し、それ以前からCC及びCCのシステムへの適用に関して研究している。2004年10月20日開催の情報処理学会セキュリティ研究会において、実際のシステムの構築される状況を踏まえてシステム評価を念頭においたシステムのPP作成方法を発表した。

JEITAのプロジェクト及び防衛庁の調査検討のいずれも継続されてない現在、継続的に検討を続け、また研究レベルの論文が学会に発表されたことは注目すべきことである。またこの論文は、実用を念頭においた具体的な提案である点でもCCに基づいたシステムのセキュリティ評価の実現に寄与すると考えられる。

(4) ISOへの提案活動

ISO／JTC1／SC27において、システム評価がNew Work Itemとされ、現在はSecurity Assessment of Operational Systemsとして、2006年10月にTRとする目標で検討されている。これに関して、国内のSC27委員会でどのような検討が行われているか不明だが、活発な組織的検討が行われているとの情報を得ていない。

### 3-5-2-4　専門家との会合によるヒアリング

(1) システムPPの必要性

前述したが、PPにはITのセキュリティに関する要求事項を記述した仕様書の役割と、PPに従って製品のSTを作成しセキュリティ評価・認証を受ける基盤としての役割がある。

システムのST作成、評価、認証は製品に関する評価ほど確立されておらず、事例も少ないので、少々先送りすることもやむを得ないが、電子投票・アンケートシステムのセキュリティの重要部分を受け持つICカードに

関してセキュリティ仕様を意識し、明確化し、共通的書式で記述することには大きな意義があり、将来のST作成、評価、認証へつながる第一歩となる。

「ICカードのPPは、是非作成すべきである」というのが、内山氏の意見である。

(2) システムの定義(システムの範囲)

システムのPPを作成する際に、システムの範囲として運用を含めるかどうかを決定する必要がある。内山氏の意見は、「管理運用は含めない」PPを推奨している。

その理由は、前述したようにPPとその基盤となるCCは技術規格であって人間系による管理運用は適用対象外とされ、それに関する規定は含まれていない。従って、システムの範囲としてPPに記述されてもCCによって評価できないことである。

また、運用に関する標準は別のもの(ISO17799 など)が存在し、その利用を検討すべきである。PPへ運用環境を含めた記述は可能であるが、電子投票・アンケートシステムは社会システムの一環をなす性格を持っており、組織内に設置・運用されるシステムより以上に運用環境に多くの考慮すべき事項があると推測でき、かつその重要度は大きい。その観点からも運用管理や運用環境に集中した検討を行い、その結果をPPとは別の形で記述すべきである。

(3) ICカードPP作成の留意事項

システムPPの作成にあたっては前述した永井・安細氏の論文が参考になる。

また、前述したとおり、アプリケーションがまったく異なるものの、Intersector Electronic Purse and Purchase Device Protection Profile(IEP&PD PP) Version1.3 March 2001 が、参考になるPPである。

電子投票・アンケートシステムにICカードを利用する1.5項の想定の場合、システムにはサーバ・クライアント・ICカードの3つのサブシステムが主要な構成要素として含まれている。実用上はこれに加えてインターネット網などがサーバとクライアント間に使われるし、クライアントにはICカードとのインタフェイス機器であるカードリーダライタも含まれると考えられる。電子投票・アンケートシステムのICカードは、それ自体が自己完結しているシステムではなく、他の2つのサブシステムと協働してシステムを構成している1つのサブシステムである。

このような場合、ICカードのPP作成にあたっては、システムの範囲の定義に加えて、他のサブシステムとのインタフェイス条件、即ち、他のサブシステムとのセキュリティ機能の分担、セキュリティ機能に関するインタフェイスの記述が重要である。

ICカードのPPに記述されるセキュリティニーズ(前提条件や対抗すべき脅威及び従うべきセキュリティポリシー)は、電子投票・アンケートシステムがICカードサブシステムに分担させるものと整合していなければならない。同様に、これらのセキュリティニーズを満たすためにICカードが装備すべきセキュリティ機能は、電子投票・アンケートシステムからICカードに分担させ配分されたものと整合していなくてはならない。他の2つのサブシステムとICカードが持つセキュリティ機能によって、電子投票・アンケートシステムが必要としているセキュリティ機能を満たしていることが確認できるべきである。

また、ICカードと他の2つのサブシステムとの間のセキュリティ機能に関するすべてのインタフェイス夫々について、ICカード側のインタフェイス条件と相手方のインタフェイス条件が正確に整合していることが確認できるべきである。

これらの点は、現時点でシステム評価に関する主流であると考えられるcomposite approachの視点に整合するもので、英国で実施しているシステム評価のSTに記述される内容とも整合している。

ICカードのPPだけが単独で存在しているのではなく、その前に電子投票・アンケートシステムのセキュリティニーズがあり、それが明確に文書化され、それらのうちICカードにどれを分担させるかの割り当てが必要である。セキュリティニーズを満たすためのセキュリティ機能についても同様である。可能であれば、電子投票・

アンケートシステムのセキュリティニーズとセキュリティ機能の明確化と文書化は、電子投票・アンケートシステム全体のPPとして書かれる事が最良の方法である。そうすれば、システム全体のPPの中に3つのサブシステムへの配分を記述することもできる。理想的な姿は、以下のとおりである。

① システム全体のセキュリティを考えた、システム全体のPPを作成

② 構成要素のつなぎや機能（特にセキュリティ機能）分担の明確化（①に記述する）

③ 構成要素夫々に対応するPPの1つとしてカードサブシステムのPP作成

電子投票・アンケートシステムのサブシステムとしての位置付けに加えて、クライアントとICカードは、他のアプリケーションシステムとも兼用する可能性が考えられ、専用で使用する場合より考慮すべき条件はさらに多いと考えられる。

ICカードに関して言えば、他のアプリケーションシステムと兼用する場合、マルチアプリケーションカードであると考えられる。マルチアプリケーションカードシステムは、カードチップ、カードOS、複数のアプリケーションソフトなどを構成要素にしている。マルチアプリケーションカードに搭載された電子投票・アンケートシステムは、マルチアプリケーションカードシステムの一部を構成する一つのサブシステムの位置付けである。

このような場合、ベースとなるマルチアプリケーションカードのアプリケーション分離機能が充実しているか否かで、作るべきPPの記述範囲やその後の評価プロセスが大きく変わる。

マルチアプリケーションカードのアプリケーション分離機能が充分な機能を有していない場合は、そのICカードに搭載されたソフトウエア全てをPP記述範囲とし評価対象としなければならず、PP作成やその後の評価は Composite approach を適用できない場合のシステムPPやシステム評価と同じく、規模によっては実行上評価不可能な作業量になる懸念があり、避けるべきである。

マルチアプリケーションカードを使用する場合、充分強力なアプリケーション分離機能を装備し、アプリケーション相互に影響しあうことの排除及びアプリケーションレベルのソフトウエアとそれを支えるOSまでのレイヤを完全に分離しそれらのインタフェイスを明確にすべきである。ICカード全体を視野に収めたPP構成の階層（レイヤ）構造をまず確立し、機能分担とインタフェイスの明確化をすることにより、アプリケーションの1つとして電子投票・アンケートシステムについてPPを作成できる。

この場合、電子投票・アンケートシステムとしてのセキュリティニーズ（前提条件や対抗すべき脅威及び従うべきセキュリティポリシー）はすべて記述される必要がある。そのセキュリティニーズを満たすために必要なセキュリティ機能は電子投票・アンケートシステムに装備するほか、プラットフォームであるICカードチップ、カードOS及びミドルウェアソフトに分担することが可能である。電子投票・アンケートシステムの持つセキュリティ機能を記述すると同様に、プラットフォームに求める機能をPPの「IT環境のセキュリティ機能」として明確に記述する必要がある。

現在発表されているICカードのPPの中には、マルチアプリケーション型であるにもかかわらず上述したようなアプリケーション間の分離やアプリケーションとOSなどのレイヤ構造が明確に分離されず、全体が渾然一体に書かれているものも見受けられるので、それらは再構成して書き直した上で利用されるべきである。なお、一見アプリケーションの1つに見えながら、他のアプリケーションにも利用されるPKIによる認証システムなどは、共通基盤的ソフトウエアとしてOS同様に他のアプリケーションとのインタフェイス条件を明確にすべきである

補足(1)　PPの評価認証は外国で

電子投票・アンケートシステムのICカードについて作成されたPPは、その内容が適切であるかITセキュリティの専門家により確認するためにPP評価・認証を受けることを推奨する。その場合、システムやICカードに関する評価・認証の経験、及び経験によるコストと時間の節約を考えると、海外で評価・認証を受けることを推奨する。

海外で評価・認証を受けるためにはPPを英訳する必要があるが、この英訳の過程で日本語にありがちな構文上の曖昧さが摘出され、日本語のPPを含めて精度が向上すると期待できるので、上記の経験によるコストと時間の節約と合わせれば、英訳に要するコストや時間のデメリットを相殺するだけの価値があると考える。

評価・認証を受ける国の候補は、国策としてスマートカードに注力し電子財布などスマートカードを含めたシステムPPの評価・認証経験の多いフランス、或いは同様にICカードに関する経験も多く電子投票システム評価も行っている可能性のある（今年のICCCにて発表あり。現在進行中か？評価認証済みの情報は掲載されていない）ドイツである。ITセキュリティに関しての経験とレベルでは世界のトップはアメリカ、次はイギリスの順と考えられるので厳格な評価を期待するならばこれらの国で評価を受ける選択肢もある。

日本のITセキュリティ評価・認証制度においては、システムPP評価やICカードの評価の経験が殆ど無いため、新しいジャンルの評価をはじめてやる場合、予期しない問題に遭遇して時間を費やしたり、国際的な判断と異なる判断をする可能性なしと言えない。

またCCの思想と求めるものは、製品が具備しているセキュリティ機能を過不足なく記述しそれにより対抗できる脅威を的確に記述することであるが、現状の日本の制度の運用においてはPPやSTにおいて考えられる脅威の記述に漏れがないことを重視しており、開発者の大きな負担と評価期間やコストが増大する一因になっている。このような日本の制度からの要求は、本件のPPのように社会システムにまで関わっていると難しい要素となる。

ただし、ここでの表現はあくまで、推奨ということである。日本には認証機関、評価機関があり、対応する機能はある。ここで述べたことは、日本と海外との現実の経験の差を直視した上での意見である。

補足(2)　システムのST、システム評価・認証へのチャレンジ（内山氏、永井氏、安細氏）

システムのPPやSTの書き方に大きな関連をもつシステム評価は、国際的に見て人間系による管理運用側面は評価対象から除外することと、ITシステム評価の方法として構成要素となる製品夫々とそれらの繋がりを評価する composite approach が主流と思われる。

Composite approach において、システム全体が対抗しようとする脅威及びシステムの前提条件や従うべきセキュリティポリシーと、そのために装備するセキュリティ機能は、夫々適切にシステムを構成する製品に配分されなければならない。しかしながら、一般的にはシステムとは独立に開発された製品を構成要素として使用するためその具体的方法は相当な検討を要する。この実用上の問題の解決のために、永井・安細両氏の論文は、システム全体から構成製品へトップダウンによる割り当てと、構成製品が具備しているセキュリティ機能のボトムアップによる積み上げとで整合を取る方法を提言している。

内山氏、永井氏、安細氏は、電子投票・アンケートシステムのICカードについて、PPが作成され評価・認証された後、是非STを作成し、ICカードサブシステムの評価・認証にチャレンジすることを希望し推奨している。

補足(3)　運用の記述と評価

システムPPの範囲から除外された人間系による運用管理は、情報セキュリティにとって重要度が小さいということではなく、CCに基づいて記述し評価することに馴染まないと考えるからである。

運用管理の記述と評価に関しては、情報セキュリティマネジメントに関する基準が幾つかあり、中でもJIPDECによるISMS、及び英国の標準であるBS7799は審査登録制度も運用されている。また、米国ではFISMAをサポートするFIPS200の制定に向けて、その準備段階の規格である FIPS SP800-37、-53、-53A が準備されつつある。

運用管理の記述と評価に関しては、上述するとおりCCのように世界唯一の標準は無いが、当面日本においてはJIS規格化もされている管理基準である ISO17799 を基盤とするISMS或いはBS7799に基づくことが適当と考える。

補足(4)　C＆A（Cirtfication&Acreditation）やIA(Information Assurance)などの全体構想

補足3で述べた運用管理の記述と評価に他の規格を併用すること以外にも、情報セキュリティのためには他の規格の併用が考えられる。

その１つはCCにも述べられているEMCがあり、また評価対象の物理的（機械的）セキュリティ対策に関しても現行のCCでは不十分でCCへの追加乃至は他の標準の併用が行われている。また、国内及びISOにおいても暗号モジュールの評価基準が検討されている。

以上の状況から分かるとおり、情報セキュリティをただ１つの標準で記述し評価できる状況ではない。

言うまでも無く情報セキュリティは、対象となる情報系全体が、どの側面に対しても一定し過不足ない漏れのないセキュアさを実現できなければ、その効果は激減する。

情報セキュリティをどのように捉え、セキュリティのいろいろな領域をカバーする標準をどのように利用するかを、統合的に制御する規範を持つべきときである。そのような規範は、セキュリティ向上とセキュリティ投資の効率化（知的作業と手続、人、物、金、時間）をもたらすと期待できる。

この領域で先行しているアメリカでは、Information Assurance について精力的に検討しつつ、国防省が1997年から採用していたDITSCAPをもとに、国防省以外の政府機関のNational securityに関わる情報システムに対して NIACAP の適用をしている。DITSCAP や NIACAP はＣ＆Ａ（Certification and Accreditation）と呼ばれる手続規定で、ITの技術的セキュリティと運用管理に関するセキュリティ評価等の結果に基づいてAccreditation（運用開始許可）を与える手続きを定め、そのために、どのような評価結果を揃えるべきかについても定めている。

わが国においてもIAやC＆Aの研究、理解、適用が増えることを望む。

## 3-5-3　次世代電子投票・アンケートシステムのＩＳＭＳ

### 3-5-3-1　背景

本項では、ISMS の基本的な考え方及びその電子投票への適用についてまとめる。ISMS は、元来、事業などを行っている組織が、継続的に行う情報セキュリティ管理のあり方についての枠組みである。したがって、電子投票、もしくは電子アンケートのように、一定の期間、実施される、いわゆるイベント的な行為に対して、どの程度適用可能か否か、もし適用可能であるならば、考慮すべき事柄などについてまとめる。

### 3-5-3-2　実証実験について

(1)実証実験の形態

図 34 に示すように、本実証実験では、集計センター、開票センターの2センター方式を採用している。投票者は、認証局により、発行された IC カードにより認証され、投票内容は暗号化されて送付される。

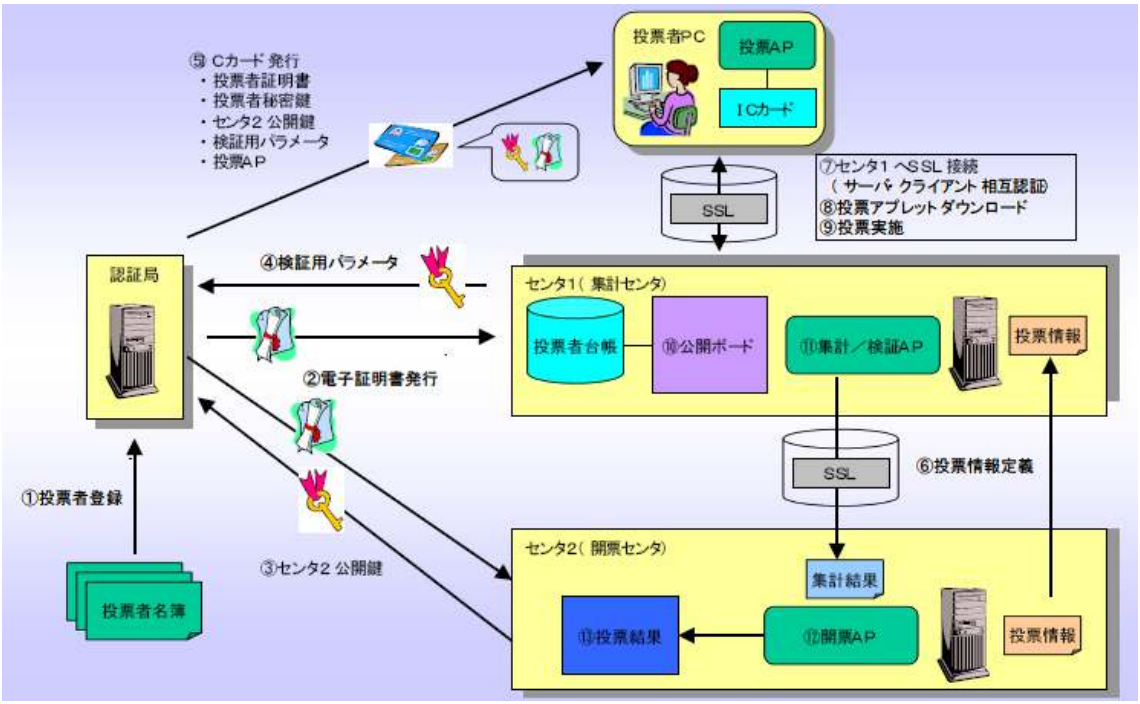



**図 34　全体構成**

(2)実証実験におけるセキュリティ管理策

セキュリティに関しては、図 35 に示すように、技術的セキュリティ管理策については、想定脅威に対する技術的管理策が、システム開発時に検討され、組み込まれた。

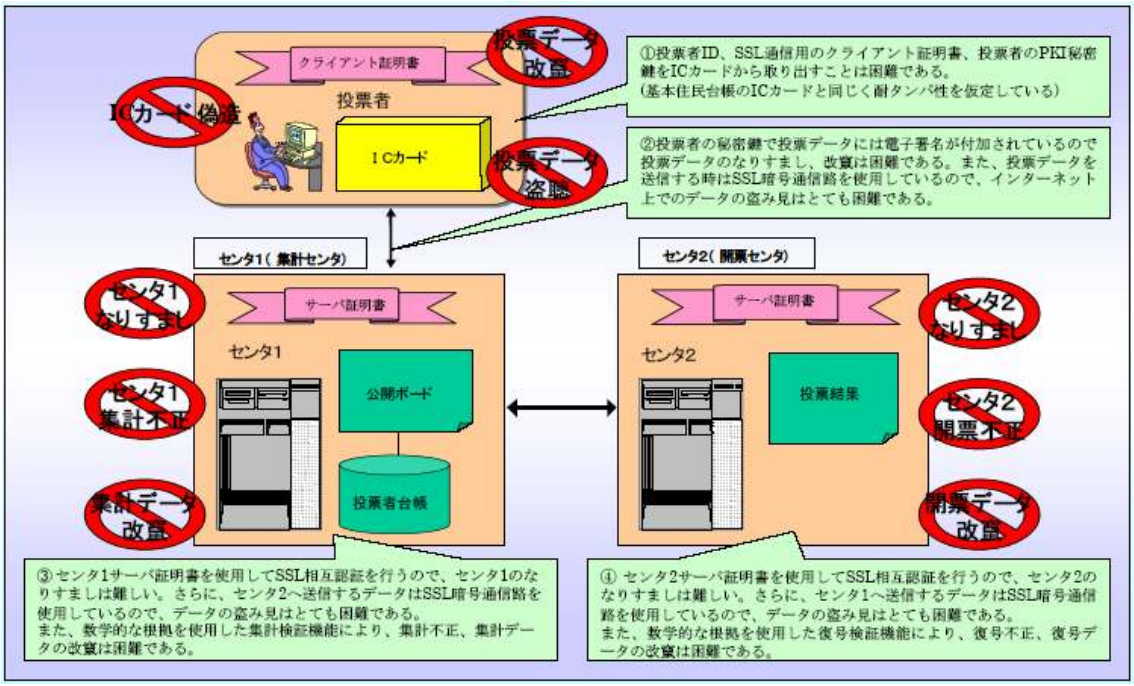



**図 35 想定脅威への技術的管理策**

また、ISMS において、要求されている物理セキュリティを含むその他の管理策については、特にリスクが高いと思われるセンター1については、データセンター内にサーバを設置することによる安全性の確保を行った。データセンターにおいて、実践されているオペレーショル・レベルの管理策についてヒアリングした結果は以下のようにまとめられる。

物理セキュリティ

- 入館者の確認およびカードによる入退館など 3 重のチェックを実施。
- 手荷物は全て、入り口ロッカーに入れる仕組み。係員が鍵を管理。
- 訪問者の移動は、全て帯同。
- 消化システムには、ハロンガスを使用。上下から。
- 監視カメラによる監視(出入り口、金庫室、作業エリアの 4 台)。
- 空調も上下左右から実施。
- 電源は、1 ラックあたり 2 系統の分電気盤。停電時は、自家発電。

ISMS 関連

- 127 項目中、開発のセキュリティは除外している。
- 適用範囲は、データセンターサービスを提供する全ての人員となっている。
- 最高責任者は、事業部長。適用範囲は、事業部。事業部内の ISMS 委員会は、全社の情報セキュリティ委員会の下部組織という位置づけである。
- 事業部の全従業員数は、300 名。そのうち、ISMS の対象者は 120 名。120 名中、約半数は、外部からの派遣である。
- 1 年目は、10 名体制で ISMS 構築に取り組んだ。その後、各セクションの担当者 4 名と事務局 3 名の 7 名体制で維持管理。全て、兼任している。
- 認証は 2002 年に取得した。
- 年 2 回の更新審査を体験して、現場に根ざした活動でないと回らないということを実感している。
- ISMS の目標として、インシデントを起こさない(0件維持)などの目標を設定している。
- 他社との差別化

- 経営者は、認証取得を販売促進につなげたいという考えである。
- 審査の中で、良かった点を「ストロングポイント」として明記してもらうことにした。
- ストロングポイントは、高度な技術の導入などではなく、管理上優れている点、たとえば、運用のノウハウを付加したなどの内容が中心である。

- ISMS 維持管理のポイントは、(あとで、まとめてではなく)「そのときに、注意する」ことである。
- インシデント報告
  - 障害対応一覧表などがある。
  - 月に 1 回、ヒヤリハット報告会を実施し、グループごとに提出させるようにした。
- 月に 1 度は、何らかの障害訓練を行っている。
  - シナリオは、ハードの故障、不審者の侵入、電話でパスワードを聞かれた、地震など。
  - 最初は、事前に知らせる方式を取っていたが、途中から、障害訓練のやり方を変え、「ブラインド訓練」にした。
  - 訓練の目標は、「xx分以内に復旧といったもの」

### 3-5-3-3　個別の管理策についての検証

本調査研究では、ISMS のベストプラクティスを基盤にした安全性確保に関する検討を実施した。その結果、電子投票に該当する管理策として ISO/IEC17799 からいくつかの管理策を抽出した。以下に、電子投票における ISMS のベストプラクティスと実証実験において実施された対策（管理策）との比較をまとめる。内容については別冊を参照されたい。

### 3-5-3-4　利用者アンケート結果の情報セキュリティ側面

実証実験で行われた利用者の意識アンケート調査の結果から、セキュリティや安全面について、使用者がどのような認識を持っているかについてまとめる。なお、意識アンケート調査は、使いやすさなどを中心とした内容になっており、その中でセキュリティや安全性にかかわるコメントなどを抽出した。内容については別冊を参照されたい。

### 3-5-3-5　管理策に関する考察

電子投票に適用する場合に検討を要する個別の管理策は、多岐に渡るが、今回の研究開発としての実験では、それが研究開発という位置づけで実施されたため、検証できた項目はかなり制限された。以下に、全体像を示す。

| 管理策 | 実験における適用 |
|---|---|
| セキュリティポリシー | 研究開発としての実験のため適用外 |
| セキュリティ組織 | ほとんど適用外（一部適合） |
| 情報資産の分類及び管理 | 研究開発としての実験のため適用外 |
| 人的セキュリティ | 研究開発としての実験のため適用外 |
| 物理的及び環境的セキュリティ | ほとんど適合（一部適用外） |
| 通信及び運用管理 | 研究開発としての実験のため適用外 |
| アクセス制御 | ほとんど適用外（一部適合） |
| システムの開発及びメンテナンス | 一部適合（一部適用外） |
| 事業継続管理 | 研究開発としての実験のため適用外 |
| 準拠 | 研究開発としての実験のため適用外 |

**表 25　管理策と実験における適用一覧**

（1）セキュリティ組織

- 情報処理施設への入退室管理は、指紋認証をもちいているため、「2.2 第三者アクセスのセキュリティ」の「第三者からの組織の情報処理施設及び設備へのアクセスを許可してはならない。」という要求項目には適合していると言える。

（2）物理的及び環境的セキュリティ

- 「第三者に対して、情報処理施設の場所を明らかにしないこと」という要求事項については、特定の実験関係者のみに開示しているという意味では、適合していると言えるが、次世代のシステム運用において、どのようにして実践するかについて、別途実験が必要であろう。
- 本実験では、情報処理施設として民間のデータセンターを使用しており、物理セキュリティは、そのセンターのセキュリティに依存している。「5.1 セキュリティ区画」の要求事項は、民間データセンターのオペレーションにより、適合していると言える。
- 「装置のセキュリティ」についても同様の理由により、要求事項を満たしていると言える。ただし、「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」という要求事項については、実験であることから、適用外とした。
- 「一般的な管理策」についても、ログオフの自動で入退室管理ログを保存するなどの管理策により適合している。ただし、「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」という要求事項については、実験であることから、適用外とした。
- 民間のデータセンター利用は、物理管理策の側面からは、有効と思われる。ただし、今回の実験で検証できなかった過負荷の問題や装置やソフトウェアの移動についての管理者の承認などのマネジメント上の問題などについては、さらなる検討が必要である。

(3) アクセス制御
- 「ネットワークのアクセス制御」の要求事項は、「共有ネットワークは使用していない」などの理由でいくつかの管理策が適用外になったが、それ以外は適合していた。

(4) システムの開発及びメンテナンス
- 「アプリケーションシステムのセキュリティ」については、SSL 通信路の利用やマニュアル作成などにより要求項目に適合していた。
- 「暗号による管理策」についても、TYKK 方式、ディジタル署名などの方法により要求事項に適合していた。

### 3-5-3-6 まとめ－技術革新における安全と安心

電子投票・アンケートを主催する者は、安全なシステムを提供する義務がある。ここでは、次世代電子投票・アンケートシステムの実施において、ISMS のコンセプトを活用し、安全なシステムを提供することを試みた本研究の結果をまとめる。

(1) “イベント”に対する ISMS の適用

電子投票・アンケートのように、一定期間で終了する“イベント[注17]”に対して ISMS を適用するためには、まず、リスク評価等を含む、所謂 PDCA を回す「リスクマネジメント・プロセス」が“イベント”に対して適用可能かという問題について考えなければならない。少なくとも、継続性がないと考えられる“イベント”へそのまま適用するのは困難であろう。

ただし、1年～数年の頻度で類似の電子投票・アンケートが繰り返されるなどの形式が取られている場合、前の回の“イベント”でセキュリティマネジメントの問題として明らかになった事柄については、その次の回の計画策定において検討するなどの方法で ISMS のリスクマネジメントサイクルのコンセプトを活用できる。

この場合、管理上の仕組みを規定しマニュアル化することが重要と考える。ISMS は、汎用的なフレームワークとしてそのコンセプトの活用は可能であるが、電子投票・アンケートの実用化と普及に向けては、最低限どのようなプロセスを踏む必要があるかについて規定した「ベースライン・マネジメント・プロセス・チェックリスト」などが整備されることが望ましい。

注17）投票などは、数年に一度行われるという意味では継続性があるが、オフィス業務や製造プロセスのような継続性はない

一方、個々の管理策について、ISMS では、ISO/IEC17799 などに、ベストプラクティスの管理策がまとめられている。今回の研究において、民間のデータセンターを使用し、調査結果のデータが集積・処理されるバックエンド・オペレーションのセキュリティマネジメントに該当する「物理セキュリティ、アクセス制御、システムの開発及びメンテナンス」などについて個々の管理策の実装状況を調査したところ、ISO/IEC17799 のベストプラクティス管理策の一部は、十分活用できることがわかった。今後、さらに異なる状況で利用可能性を検証し、「電子投票・アンケート向けベストプラクティス管理策」をまとめることが望ましい。

(2) 先進的技術を使用したプロセスの安全確保のリスク受容

電子投票・アンケートに対して、ISMS を適用する場合、主体となる組織（電子投票の場合は、自治体など）が、管理のための仕組みを構築することになる。昨年度、すでに実験的に電子投票を実施した自治体に対するヒアリング調査においても、その必要性が認識されていることが明らかになった。

しかしながら、今回の実験プロジェクトでは、先進的技術の利便性や実用可能性についての検証が主な目的であり、電子投票・アンケートの主催者は、実験のための場を提供する立場にあった。したがって、セキュリティポリシーの策定やセキュリティ組織構築など、セキュリティ管理のための仕組みづくりにおいて、重要な項目に関するISMS利用可能性の検証について、適用外となった項目があった。今回、適用外となった項目については、今後も引き続き実証実験などを通して検証する必要がある。

(3) 先進的技術を使用した機器の安全性

一方で、このような先進的な技術を使用するオペレーションの場合、使用される技術の安全性について、主体となる組織が理解し受容可能なリスクレベルにあるかどうかを判断するのは、非常に困難である。現在行われている実証実験等においても、機器の安全性については、ブラックボックスのまま、メーカーを信頼することにより実施しているというケースが少なくないようである。

したがって、機器やシステム等の技術セキュリティについては、公の機関や業界団体などで、一定レベルのセキュリティが確保されていることを保証する認証制度などが有用であろう。

(4) 次世代電子投票・アンケートの安全と安心のために

本研究における利用者アンケートの記述式回答では、“**あいまいな不安**”を表明したコメントが多く見られた。先進的技術である次世代電子投票・アンケートシステムを普及・推進するためには、利用者の“あいまいな不安”を減らしていくことが重要である。

今回の研究では、技術や機器の機能やユーザビリティの評価が中心であったが、今後の研究では、電子投票・アンケートを主体的に実施する主催者側の安全性確保についての意識についての調査が必要である。特に、機器の安全性とオペレーションを含む**システムやサービス全体の安全性確保**の考え方に基づく、具体的な安全性要求のあり方についてのフレームワークの確立が望まれる。ISMS の提示するベストプラクティスは、そのための参考になると考えるが、電子投票・アンケート実践の状況に即したより具体的な管理策の策定も有用であろう。

さらに、主催者が利用者に伝える安全情報と利用者の理解とのギャップを小さくする努力についての有効な方法論の開発が望まれる。安全情報の伝達については、リスク・コミュニケーションの研究において、インタラクティブ・コミュニケーションが重要であることが指摘されている。利用者は自ら実施すべき安全策についても、十分に理解しなければならないであろう。電子投票・アンケートの実践において、インタラクティブ・コミュニケーションを含む**有効なリスク・コミュニケーション方法**についてのさらなる実験や研究が望まれる。

# 3-6　モデル構築

## 3-6-1　電子投票共通基盤のサービス化について

第三段階の電子投票をコンピュータシステムで扱うためのアプローチとして、我々は、第三段階の電子投票を一般的にモデル化し、その範囲を明確にした上で、TYKK を具体例として実装を行い、問題点を解析するというアプローチを取ってきた。

しかしながら、電子投票の方式は TYKK の様な準同系性利用する方法に限らず、ミックスネット、ブラインド署名といった方式が検討され、それぞれ一長一短があることがわかっている。そこで、我々は、電子投票のさまざまなバリエーションを再度検討するとともに、バリエーションを吸収する実装方式を検討し、実際に実験で用いたコードをその方式で再度実装しなおすことで、リファレンスを提供することとした。

以下の図は、電子投票のソフトウェア（投票システムと呼ぶ）構造を模式化したものである。投票システムは、投票方式、投票方式で利用する暗号ライブラリ、認証および公開ボードといった基盤の組み合わせで構築される。

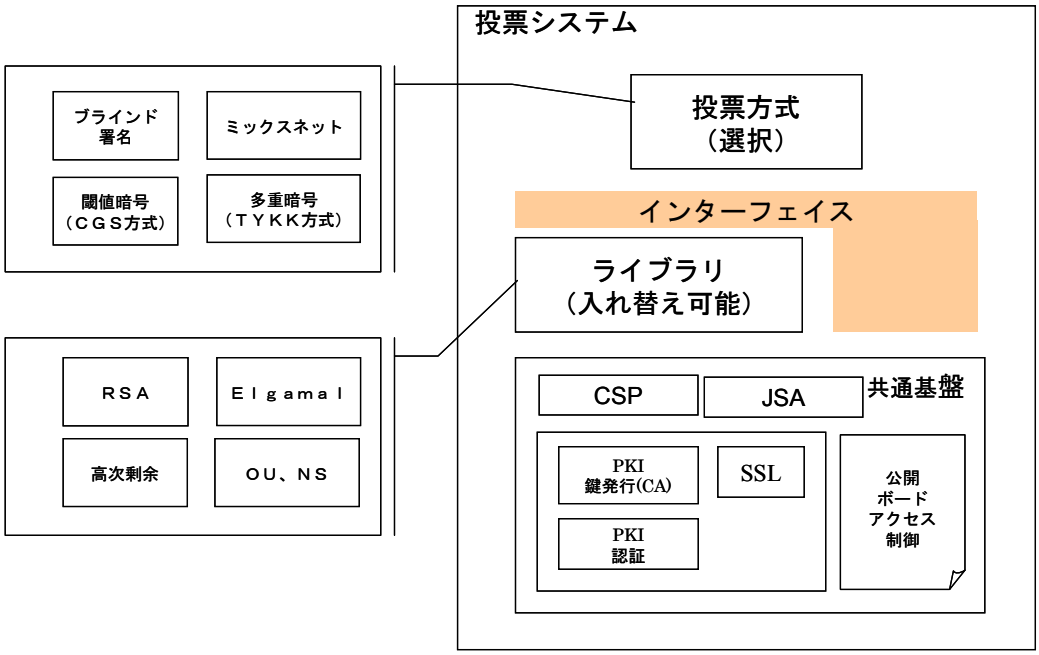



**図 36　投票プロトコルと実装の関係**

入れ替え可能な暗号ライブラリについては、別章で説明することとし、ここでは、共通基盤の実装をアプリケーションから隠蔽する方法と、投票方式の違いを吸収するためのソフトウェア構造について説明する。このために、サービス化という方法を取る。
サービス化により、アプリケーションと切り離すことで、アプリケーションのソースコードの変更を行わず、複数の電子投票実装を切り替えて利用できるようにする。サービス化することに伴い、例えば以下のようなことがアプリケーション本体の変更を行わずに実現可能となる。

・投票者の認証方式の変更（IC カード認証、パスワード認証、etc.）

・票暗号化方式の変更(TYKK、ミックスネット、etc.)
・公開ボード実装(票の保持等)の変更(DB、ファイルシステム、etc.)

たとえば、共通基盤のうち認証機能は、すでにある標準を用いることができ、この標準がサービス化の考え方を取り入れているため、認証のサービス化についてまず説明する。

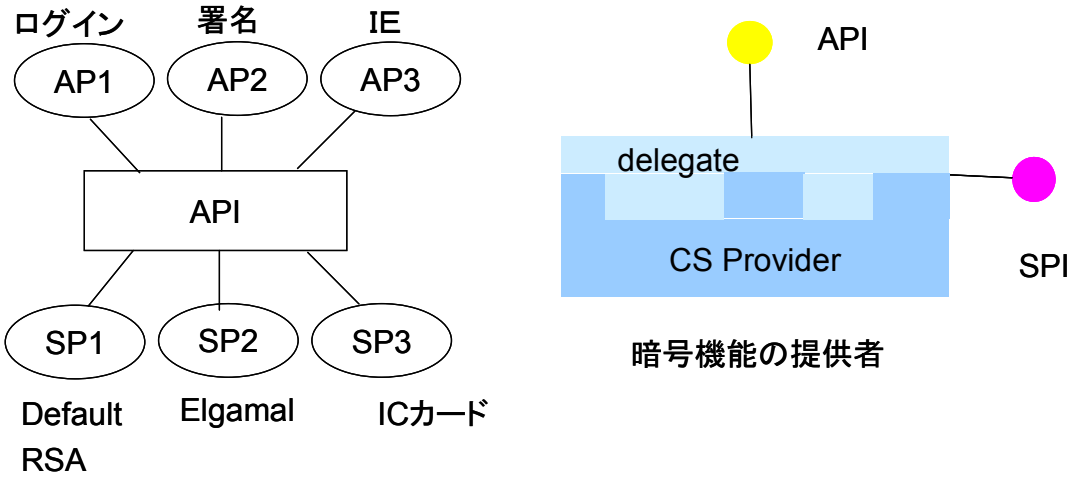



**図 37 本システムで利用しているマイクロソフトの CryptoAPI とそのサービス**

この図は、本システムで利用しているマイクロソフトの CryptoAPI とそのサービスを模式的に記述したものである。目的は、アプリケーションが IC カードを用いた認証を行う場合でも、通常の RSA を用いたプログラムでの認証を行う場合でも、上位のアプリケーションに変更を及ぼさないことである。このために、Crypto System Provider というサービス提供者のインターフェイスを準備し、各サービス提供者がそのインターフェイスを実装することで、API にはあたかも同じ提供者による機能が動いているかのように見せかける方法を取っている。

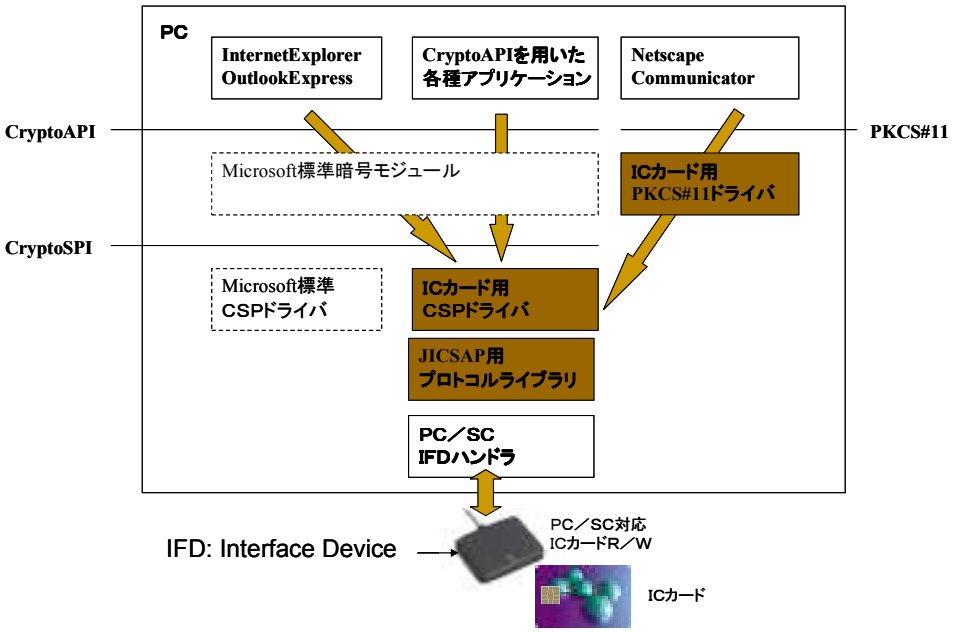



**図 38　IC カードを用いた CryptoAPI と、その CSP 実装の位置づけ**

たとえば、この図は、IC カードを用いた CryptoAPI と、その CSP 実装の位置づけを示したものである。このように、API がアプリケーションから実装を隠蔽するように、SPI を用いることで、複数のサービスの実装者が API に対してサービスを提供できるようになる。

一般に、サービスへのアクセスは API クラス（処理内容をいくつかひとまとめにしてクラス化）を介して行う。API クラスはサービスプロバイダ（サービスの実装）に対して処理を委譲する。
実装を行うサービスは、ServiceProviderInterface(SPI) 抽象クラスにより定義を行う。サービスプロバイダのクラスは SPI 抽象クラスを具象化したクラスとなる。API からサービスプロバイダへのアクセスは SPI を使用する。

共通基盤のサービス化を適用した電子投票システムの全体構図を図 39 に示す。

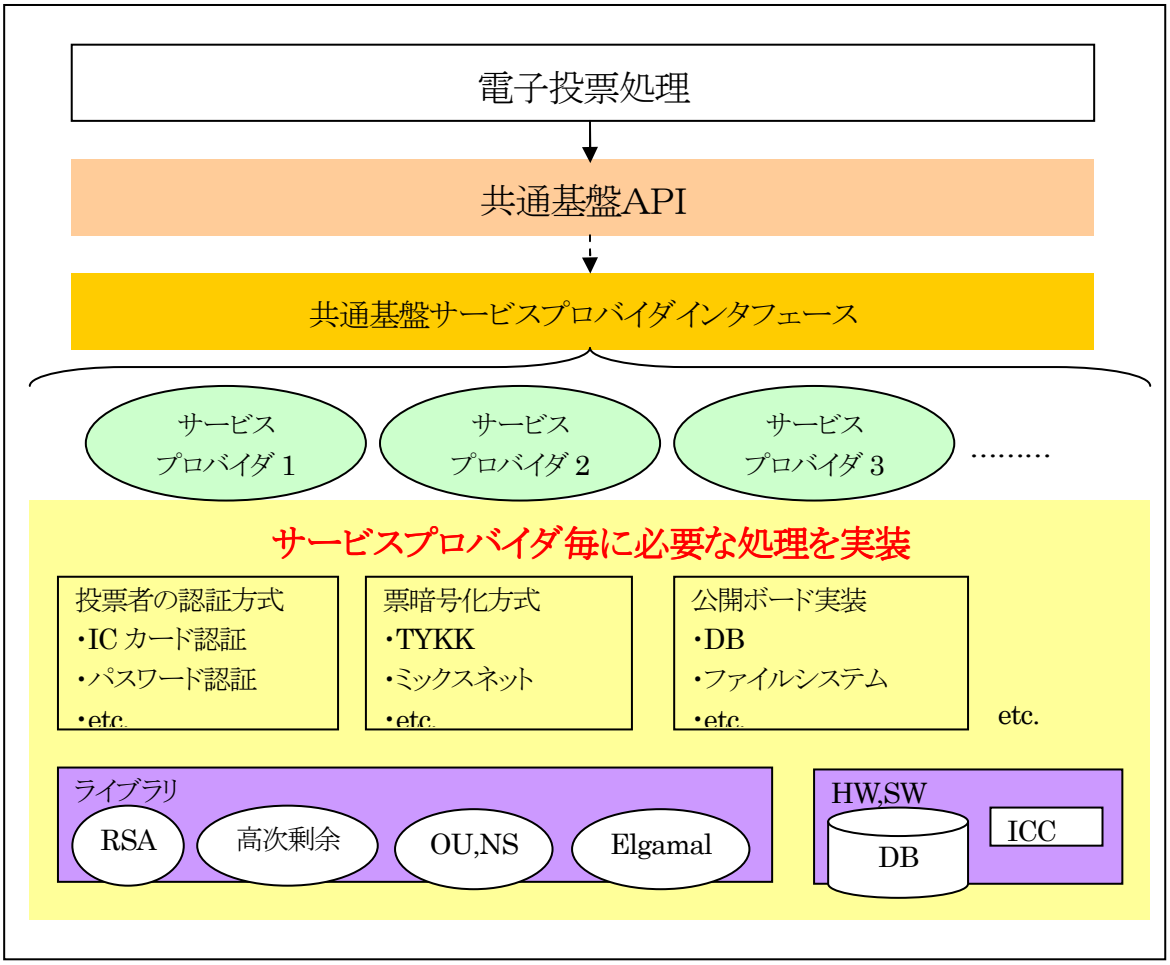



**図 39 共通基盤サービス化後の電子投票システムの全体構造**

## 3-6-2　サービス化対象処理

表 26 に示す処理内容をクラス化して、共通基盤のサービス化を行う。

**表 26　サービス化対象処理一覧**

| 処理内容(クラス) | API クラス | SPI クラス |
|---|---|---|
| 投票者の秘密処理 | nict.nvs.csp.VoterSecret | nict.nvs.csp.VoterSecretSpi |
| 選挙情報 | nict.nvs.csp.ElectionInfo | nict.nvs.csp.ElectionInfoSpi |
| 投票用紙 | nict.nvs.csp.Ballot | nict.nvs.csp.BallotSpi |
| 公開ボード | nict.nvs.csp.PublicBoard | nict.nvs.csp.PublicBoardSpi |

電子投票アプリケーションは、処理内容毎に定義された各 API クラスを介して、共通基盤サービスプロバイダの処理を呼び出す(図 40)。

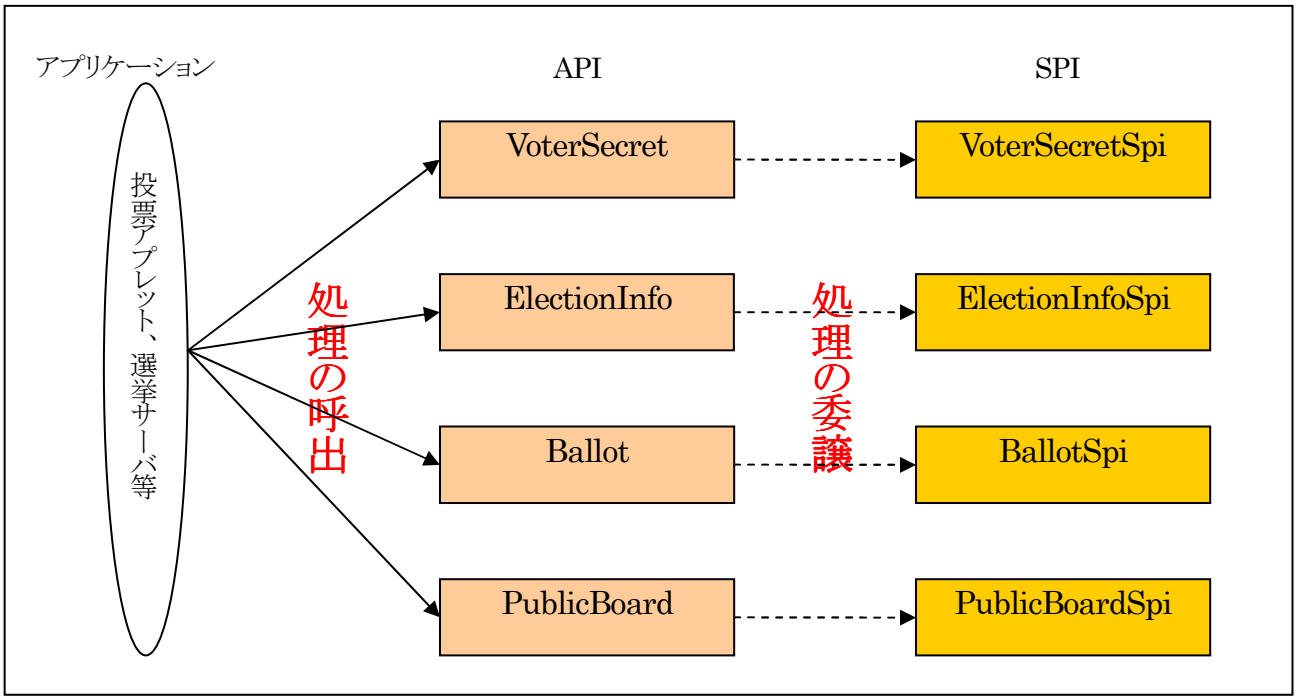



**図 40　API およびサービスプロバイダの呼出関係**

この構造を利用することで、以下に示すように、各投票方式の違いを吸収することができる。

## 表 27 各投票方式の違いを吸収する共通基盤サービスプロバイダの処理の呼び出し

| SPI | | 実装例 | | | |
|---|---|---|---|---|---|
| | | 投票方式 | | | |
| | | | | 準同形 | |
| | | ブラインド署名 | ミックスネット | 閾値暗号 | 二重暗号 |
| 対象 | 操作 | | | | |
| 有権者の秘密 | 投票者の認証 | | | | |
| vs | vs.load(from) | | | | |
| | from:証明先URL | | | | |
| | | | | | |
| 投票用紙 | 投票用紙の入手 | | | | |
| bt | bt.create(from) | bt.getAuthorityURL() | | bt.getAuthorityKey() | bt.getAuthorityKey() |
| | from: 入手元URL | | | | |
| | | | | | |
| 選挙情報 | 選挙情報の入手 | | | | |
| ei | ei.create(from) | ei.create() | ei.create() | ei.create() | ei.create() |
| | from: 入手元URL | | | | |
| | | | | | |
| 投票用紙 | 票の記入 | | | | |
| bt | bt.choose(ei) | bt.choose() | bt.choose() | bt.choose() | bt.choose() |
| | | | | | |
| 投票用紙 | 票の匿名化 | | | bt.encrypt() | bt.encrypt() |
| bt | bt.beAnonymous(with) | | | bt.addProof() | bt.addProof() |
| | with : 匿名化に利用するURL | | | | |
| | | | | | |
| 投票用紙 | レシートの作成 | commitment() | | digest() | digest() |
| bt | bt.prepareReciept() | | | | |
| | | | | | |
| 投票用紙 | 投票 | | | | |
| bt | bt.vote(vs,with) | vs.authenticate() | bt.HTTPSCSPost() | bt.HTTPSCSPost() | bt.HTTPSCSPost() |
| | with : 投票するURL | bt.requestBSignature() | | | |
| | | cm.anonymousChannel() | vs.authenticate() | vs.authenticate() | vs.authenticate() |
| | | bt.anonymousChannel() | | | |
| 投票用紙 | 票の検証 | bt.checkSignature() | | bt.verifyProof() | bt.verifyProof() |
| bt | bt.vefity(with) | | | | |
| | with : 検証に利用するURL | | | | |
| | | | | | |
| 公開ボード | 公開ボードの生成 | | | | |
| pb | pb.create(bt) | pb.create() | pb.create() | pb.create() | pb.create() |
| | | | | | |
| 公開ボード | 開票 | ei.wait() | ei.wait() | | |
| pb | pb.place(bt,el) | pb.place(bt,ei) | pb.place(bt,ei) | pb.place(bt,ei) | pb.place(bt,ei) |
| | | | | | |
| 公開ボード | 集計 | | | | |
| pb | pb.total(bt,el) | pb.getTallier().total() | pb.getTallier().total() | pb.getTallier().total() | pb.getTallier().total() |
| | | | | | |
| 公開ボード | 検証 | | | | |
| pb | pb.verify(bt,ei) | | | pb.getTallier().check() | pb.getTallier().check() |
| | | | | | |

### 3-6-3　サービスプロバイダの選択

各 API クラスはプロバイダ名を指定した「getInstance(provider)」静的メソッドでインスタンス化される。API クラスは、「sun.misc.Service.providers(SPIClass.class)」を利用して、インスタンス化可能なサービスプロバイダのインスタンス列挙を取得し、指定されたサービスプロバイダ名に一致するサービスプロバイダクラスインスタンスを含むAPIクラスのインスタンスを作成する。サービスプロバイダクラスには、サービスプロバイダ名を取得するための「getName()」メソッドを実装する。

図 41 に「getName()」メソッドの実装例を示す。図のように API.getInstance メソッドが呼び出された場合は、指定されたプロバイダ名"ServiceProvider2"に一致するプロバイダ名をもつ「サービスプロバイダ 2」プロバイダへ処理を委譲する API クラスインスタンスが返される。

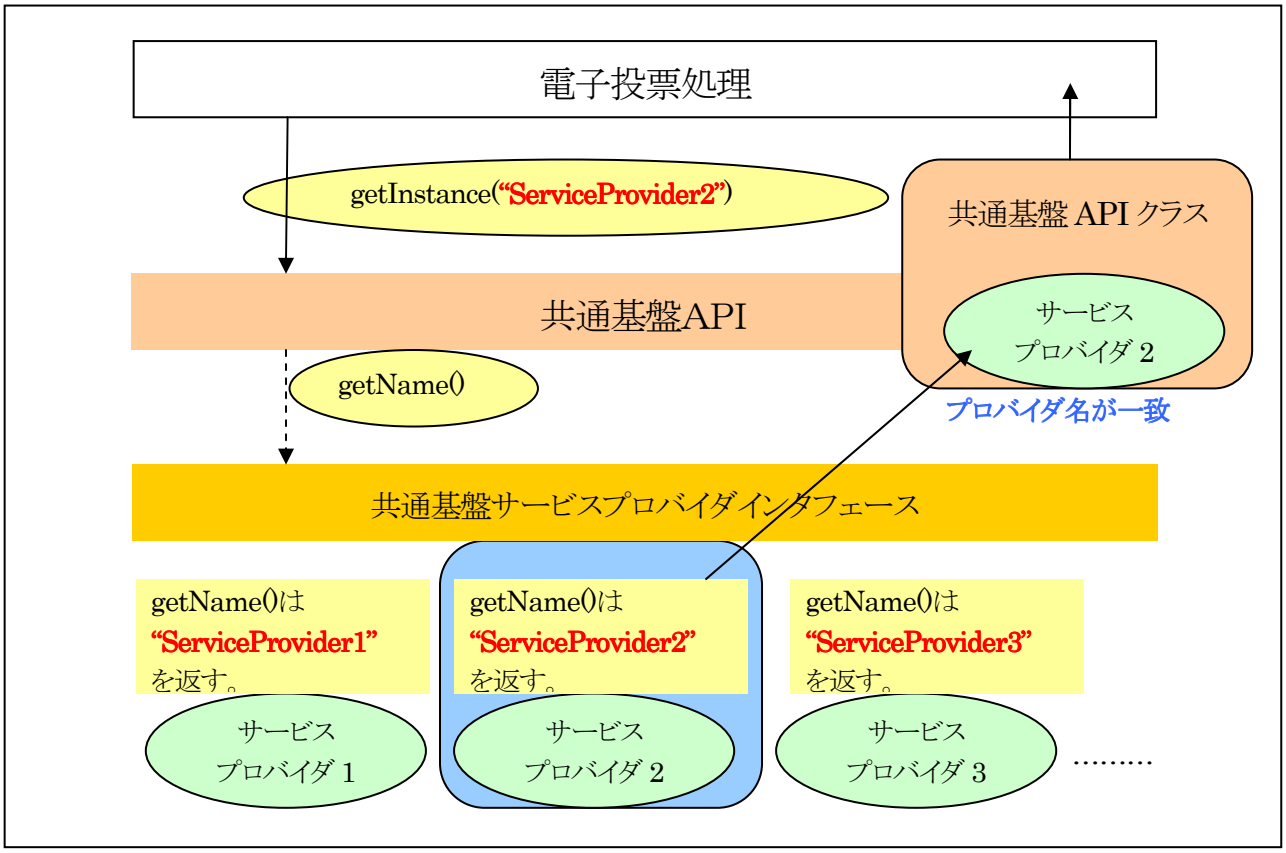



**図 41 サービスプロバイダの getName()メソッド実装例**

図 42 に API、SPI およびサービスプロバイダの実装例を示す。

```
/** API クラス */
class APIClass {
    private SPIClass spi;

    protected APIClass(SPIClass spi) {
        // SPI クラスインスタンスを内部保持する。
        this.spi = spi;
    }

    public static APIClass getInstance(String provider) {
        // 指定された型の SPI 実装を取得する。
        Iterator ps =
            sun.misc.Service.providers(SPIClass.class);
        while (ps.hasNext()) {
            SPIClass spi =    (SPIClass)ps.next();
            if (provider.equals(spi.getName())) {
                return new APIClass(spi);
            }
        }
        return null;
    }
}
```

```
/** SPI クラス 1 */
public abstract class SPIClass {
    // プロバイダ名取得。
    public abstract String getName();
    // SPI の実装処理実行。
    public abstract void execute();
}
```

```
/** サービスプロバイダクラス 1 */
public class SPIClass1 extends SPIClass {
    public String getName() {
        // プロバイダ名を返す。
        return “SPIClass1”;
    }
    public String execute() {
        return “クラス 1 の処理”;
    }
}
```

```
/** サービスプロバイダクラス 2 */
public class SPIClass2 extends SPIClass {
    public String getName() {
        // プロバイダ名を返す。
        return “SPIClass2”;
    }
    public String execute() {
        return “クラス 2 の処理”;
    }
}
```

**図 42 API、SPI の実装例**

クラス「APIClass」が API クラスの例、クラス「SPIClass」が SPI クラスの例である。また、クラス「SPIClass1」がプロバイダ名「SPIClass1」に対するサービスプロバイダクラスの例、クラス「SPIClass2」がプロバイダ名「SPIClass2」に対するサービスプロバイダクラスの例となる。

図 42 の API、SPI およびサービスプロバイダを利用したアプリケーションの例を図 43 に示す。クラス「Application」がアプリケーションクラスの例となる。

```
/** アプリケーションクラス*/
public class Application {
  public static void main(String[] args) {
    // プロバイダ名「SPIClass1」の実装をもつ API クラスを取得する。
    // ※SPIClass1 のインスタンスを内部に持つ API クラスインスタンスが返される。
    APIClass class1 = APIClass.getInstance( “SPIClass1” );

    // class1 処理実行結果の出力
    // ※「クラス 1 の処理」と出力される。
    System.err.println(class1.execute());

    // プロバイダ名「SPIClass2」の実装をもつ API クラスを取得する。
    // ※SPIClass2 のインスタンスを内部に持つ API クラスインスタンスが返される。
    APIClass class2 = APIClass.getInstance( “SPIClass2” );

    // class2 処理実行結果の出力
    // ※「クラス 2 の処理」と出力される。
    System.err.println(class2.execute());

    // プロバイダ名「SPIClass3」の実装をもつ API クラスを取得する。
    // ※指定プロバイダ名のサービスプロバイダが存在しないため、null が返される。
    APIClass class3 = APIClass.getInstance( “SPIClass3” );

    // class3 処理実行結果の出力
    // ※class3 実装は存在せず null のため、NullPointerException 例外となる。
    System.err.println(class3.execute());
  }
}
```

**図 43 API、SPI を利用したアプリケーションの例**

## 3-6-4 JAR サービスプロバイダの構造

サービスプロバイダを検索するための仕組みとして、JAR サービスプロバイダを利用する。(※前述の「sun.misc.Service.providers(SPIClass.class);」は JAR サービスプロバイダを利用している)
JAR ファイル内のリソースディレクトリ「META-INF/services」ディレクトリ内にプロバイダ構成ファイルを配置することで識別され、ファイル名に SPI 抽象クラス名(完全指定)、ファイル内に一意の具象サービスプロバイダクラス名(完全指定)の記述を含める。
(例)SPI クラス名(完全指定)が「nict.nvs.csp.VoterSecretSpi」、具象サービスプロバイダ名(完全指定)が「 nict.nvs.cipher.spi.NVSVoterSecretSpi 」の場合は、JAR ファイル内の「 META-INF/services/nict.nvs.csp.VoterSecretSpi」ファイルに、「nict.nvs.cipher.spi.NVSVoterSecretSpi」の記述を行う。

図 44 に JAR サービスプロバイダを利用した JAR ファイルの構成例を示す。

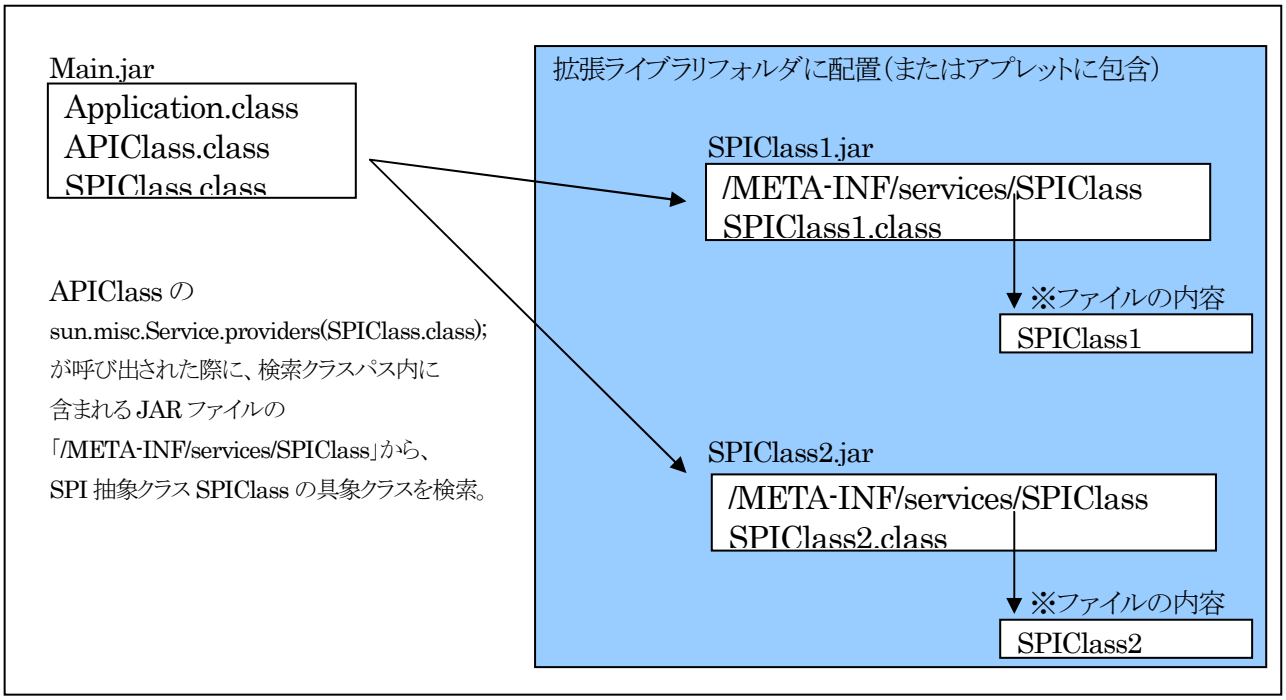



**図 44 JAR サービスプロバイダの構成例**

## 3-6-5　共通基盤 API、SPI のクラス図

共通基盤API、SPIのクラス図を図 45に示す。本クラス図には、サービスプロバイダクラスの実装例(NVS標準実装)を含む。

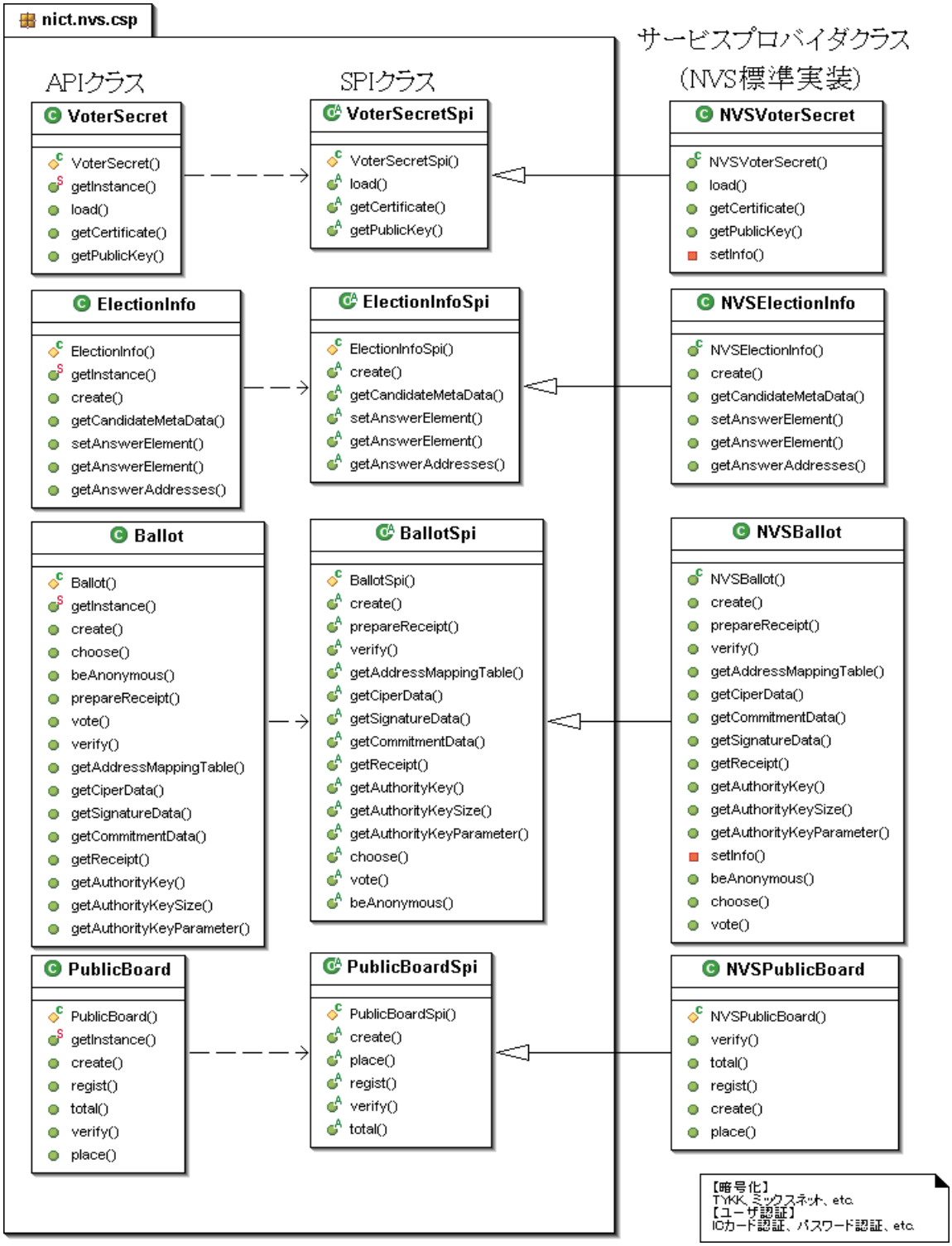



図 45　共通基盤 API、SPI(UML クラス図)

## 3-6-6 共通基盤 API 一覧

共通基盤の API 一覧を表 28 に示す。投票のメイン処理で呼び出される API、開票のメイン処理で呼び出される API、他クラスの API から呼び出される API（汎用 API）の3種類に分類される。

**表 28 共通基盤 API 一覧**

| | 項目 | 操作対象クラス | 呼出メソッド | 備考 |
|---|---|---|---|---|
| 投票 | 投票者の認証 | VoterSecret | load(from) | from:証明先URL |
| | 投票用紙の入手 | Ballot | create(from) | from:入手元URL |
| | 選挙情報の入手 | ElectionInfo | create(from) | from:入手元URL |
| | 選挙候補者情報の入手 | ElectionInfo | getCandidateMetaData() | |
| | 回答要素の保存 | ElectionInfo | setAnswerElement(IAnswerAddres, IAnswerElement) | 投票アプレットが使用 |
| | 票の記入 | Ballot | choose(ElectionInfo) | |
| | 票の匿名化 | Ballot | beAnonymous(with) | with:匿名化に利用するURL |
| | レシートの作成 | Ballot | prepareReciept() | |
| | 投票 | Ballot | vote(VoterSecret, with) | with:投票するURL |
| | 票の検証 | Ballot | vefity(with) | with:検証に利用するURL |
| 開票 | 公開ボードの生成 | PublicBoard | create(ElectionInfo) | |
| | 票の登録 | PublicBoard | regist(Ballot, ElectionInfo, VoterSecret) | |
| | 集計 | PublicBoard | total(Ballot, ElectionInfo) | |
| | 集計結果の検証 | PublicBoard | verify(Ballot, ElectionInfo) | |
| | 開票（復号） | PublicBoard | place(Ballot, ElectionInfo) | |
| | | | | |
| 汎用 | 投票者特定情報取得 | VoterSecret | getCertificate() | |
| | 票暗号化公開鍵取得 | VoterSecret | getPublicKey() | |
| | 回答要素の取得 | ElectionInfo | getAnswerElement(IAnswerAddress) | |
| | 回答要素アドレス列挙の取得 | ElectionInfo | getAnswerAddresses() | |
| | アドレス変換表の取得 | Ballot | getAddressMappingTable() | |
| | 暗号化票データ群の取得 | Ballot | getCiperData() | |
| | コミットメントデータ群の取得 | Ballot | getCommitmentData() | |
| | 電子署名データ群の取得 | Ballot | getSignatureData() | |
| | レシートデータ群の取得 | Ballot | getReceipt() | |
| | Authority公開鍵取得 | Ballot | getAuthorityKey() | |
| | Authority公開鍵サイズ取得 | Ballot | getAuthorityKeySize() | |
| | Authority公開鍵パラメータ取得 | Ballot | getAuthorityKeyParameter() | |

# 3-7　システム構成

## 3-7-1　システム構成の方針

### 3-7-1-1　背景、目的

電子投票方式に利用される暗号方式は、本プロジェクトで実際に実装した TYKK 方式を例にとっても各種の準同型公開鍵暗号方式が利用できる。また、ミックスネットで利用される共通鍵暗号，ブラインド署名で利用される公開鍵暗号など様々である。

サブテーマ「モデル構築」の「電子投票共通基盤のサービス化について」では、共通基盤の実装をアプリケーションから隠蔽する方法と、投票方式の違いを吸収するためのソフトウェア構造示している。ここで示されているサービス化という方法により、アプリケーションと切り離すことで、アプリケーションのソースコードの変更を行わず、複数の電子投票実装を切り替えて利用できる。

本サブテーマもこの手法を利用して暗号方式(暗号化アルゴリズム)の変更があった場合に暗号ライブラリを利用する側には実装の内容が変わったことを意識せずに実装する仕組みをまとめる。

### 3-7-1-2　H15 年度の研究内容

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。

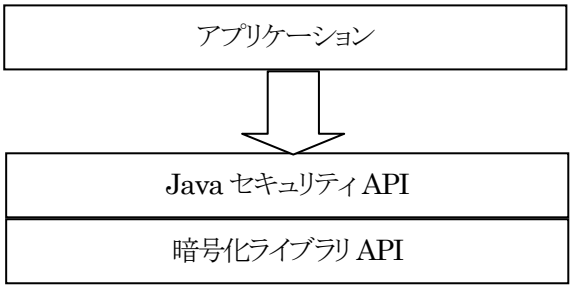
自治体実験に向けて改善が必要で有れば、対応する予定である。

## 3-7-2　暗号化ライブラリのサービス化

暗号化ライブラリをサービス化するためには、サブテーマ「モデル構築」で示す方法と Java セキュリティプロバイダの基盤を利用して提供する方法の 2 種類が考えられる。本章では、Java セキュリティプロバイダ基盤の概略を述べるとともに、H15 年度の成果である暗号コア機能からサービス化する機能を整理し、暗号ライブラリの再構成を示す。

### 3-7-2-1　Java アーキテクチャ・概念

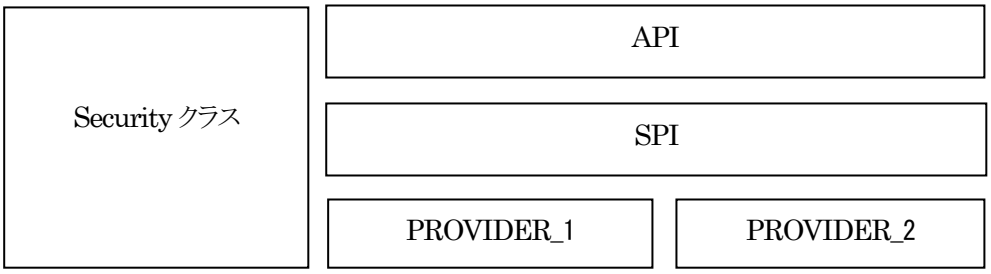
Java ではセキュリティプロバイダという概念があり、システムに用意されている複数の暗号系の実装を選択することができる。ユーザは特に指定をしなくてもシステムで標準の暗号化サービスプロバイダを Java のプログラム中から実行することが可能である。このアーキテクチャによって、実装の独立性と相互操作性が確保できる。




#### (i) セキュリティプロバイダ

セキュリティプロバイダは、Security API の暗号化に関するサブセットの固定実装を提供するパッケージ（またはパッケージセット）である。

プログラムは単に、特定サービス（たとえば DSA 署名アルゴリズム）用の特定型のオブジェクト（たとえば Signature オブジェクト）を要求するだけで、インストールされているプロバイダの 1 つから実装を獲得できる。あるいは、特定プロバイダのオブジェクトを要求することもできる。




#### (ii) エンジンクラスとアルゴリズム

エンジンクラスは、具体的な実装のない抽象的な方法で暗号化サービスを定義する。 暗号化サービスは、常に特定のアルゴリズムまたは型に関連付けられおり、暗号化の操作 の提供、暗号化の操作に必要なデータ・パラメータの生成や提供、あるいは暗号化の操作で使う暗号化鍵を安全にカプセル化するデータオブジェクト（キーストアまたは証明書）の生成が行われる。Java 暗号化アーキテクチャには、エンジンクラスなどの、暗号化に関連する Java 2 SDK Security パッケージが含まれている。API のユーザは、エンジンクラスを要求および使用して対応する処理を実行する。

エンジンクラスは、（特定の暗号化アルゴリズムに依存しない）特定の型の暗号化サービス機能へのインタフェースを提供する。これにより、Application Programming Interface（API）メソッドが定義され、API が提供する特定の種類の暗号化サービスにアプリケーションがアクセスできるようになる。

エンジンクラスが提供する API は、Service Provider Interface（SPI）として実装される。つまり、各エンジンクラスに対応する抽象 SPI クラスが存在し、この抽象 SPI クラスによって暗号化サービスプロバイダが実装しなければならない SPI メソッドが定義される。

エンジンクラスのインスタンスである API オブジェクトは、対応する SPI クラスのインスタンス SPI オブジェクトを private フィールドとしてカプセル化する。API オブジェクトのすべての API メソッドは、final

として宣言し、それらを実装することによって、カプセル化される SPI オブジェクトの対応する SPI メソッドが呼び出される。エンジンクラス（およびそれに対応する SPI クラス）のインスタンスは、エンジンクラスの getInstance ファクトリメソッドへの呼び出しによって作成される。

SPI クラスの名前は、対応するエンジンクラス名のあとに Spi を追加した名前になる。例えば、Signature エンジンクラスに対応する SPI クラスは、SignatureSpi クラスである。

各 SPI クラスは、抽象クラスである。指定したアルゴリズムに対する特定の型のサービスの実装を提供するには、プロバイダは、対応する SPI クラスをサブクラス化して、すべての抽象メソッドの実装を提供する必要がある。

**(iii) 実装とプロバイダ**

各種暗号化サービスの実装は、暗号化サービスプロバイダが提供する。暗号化サービスプロバイダとは、1 つまたは複数の暗号化サービスの実装を提供する基本パッケージである。エンジンクラスとアルゴリズムには、Java 2 SDK のデフォルトのプロバイダである SUN が提供する実装の一覧が記載されている。

その他のプロバイダは、各種サービスについて、独自の実装を定義できる。

### 3-7-2-2 暗号ライブラリの機能

暗号ライブラリとして提供する機能を整理し、共通化機能の洗い出しとインタフェースを検討する。

**(i) 投票方式の概要**

**a) TYKK 方式**

・システム構成:2 センタ構成(集計センタ, 開票センタ)
・暗号コア機能:鍵生成, 投票(暗号), 集計, 開票(復号), 検証
・暗号方式　:準同型性暗号方式, 2 重暗号用の暗号方式(共通鍵 or 公開鍵)
・検証項目　:投票正当性証明, 集計正当性証明, 開票正当性証明

**b) CGS97 方式**

・システム構成:n センタ構成(集計センタ, 開票センタ)
・暗号コア機能:鍵生成, 投票(暗号), 集計, 開票(復号), 検証
・暗号方式　:準同型性暗号方式
・検証項目　:投票正当性証明, 集計正当性証明, 開票正当性証明

**c) MIX-NET 方式**

・システム構成:n センタ構成(集計センタ, シャッフル／開票センタ)
・暗号コア機能:鍵生成, 投票(暗号), 集計, 開票(復号), 検証, シャッフル
・暗号方式　:共通鍵暗号
・検証項目　:シャッフル復号正当性証明

**d) ブラインド署名方式**

・システム構成:2 センタ構成(集計センタ, 開票センタ)
・暗号コア機能:鍵生成, 投票(暗号), 集計, 開票(復号), 検証, 匿名通信路
・暗号方式　:公開鍵暗号方式
・検証項目　:シャッフル復号正当性証明(匿名通信路で MIX-NET を利用した場合)

### (ii) H15 年度の成果

今回提供する暗号ライブラリの機能を整理する上で、H15年度までに実装した成果を例題として挙げる。

#### a) 暗号コア機能ブロック概要

暗号コア機能ブロックは、電子投票各方式に対応する共通機能，インタフェースを提供することを目的として検討，仕様化したが、特定の暗号化アルゴリズムに依存するインタフェースとなっている。現状の暗号コア機能の階層構成，ブロック構成を示す。

1)暗号コア機能階層構成

- 上位ＡＰインタフェース層
- アルゴリズムインタフェース層
- JNI インタフェース層
- C ライブラリ層

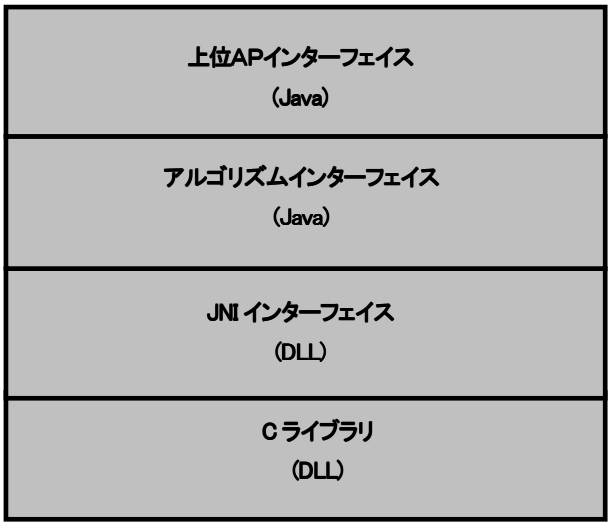



**図 46 暗号コア機能 階層イメージ**

上位 AP(選挙サーバプログラム等の上位アプリケーション)から、直接アクセスされる暗号コア機能ブロックは、「上位 AP インタフェース層」および「アルゴリズムインタフェース層」である。

JNI インターフェイス層、C ライブラリ層については隠蔽するものとし、上位側に意識させない作りとする。

2)暗号コア機能ブロック構成

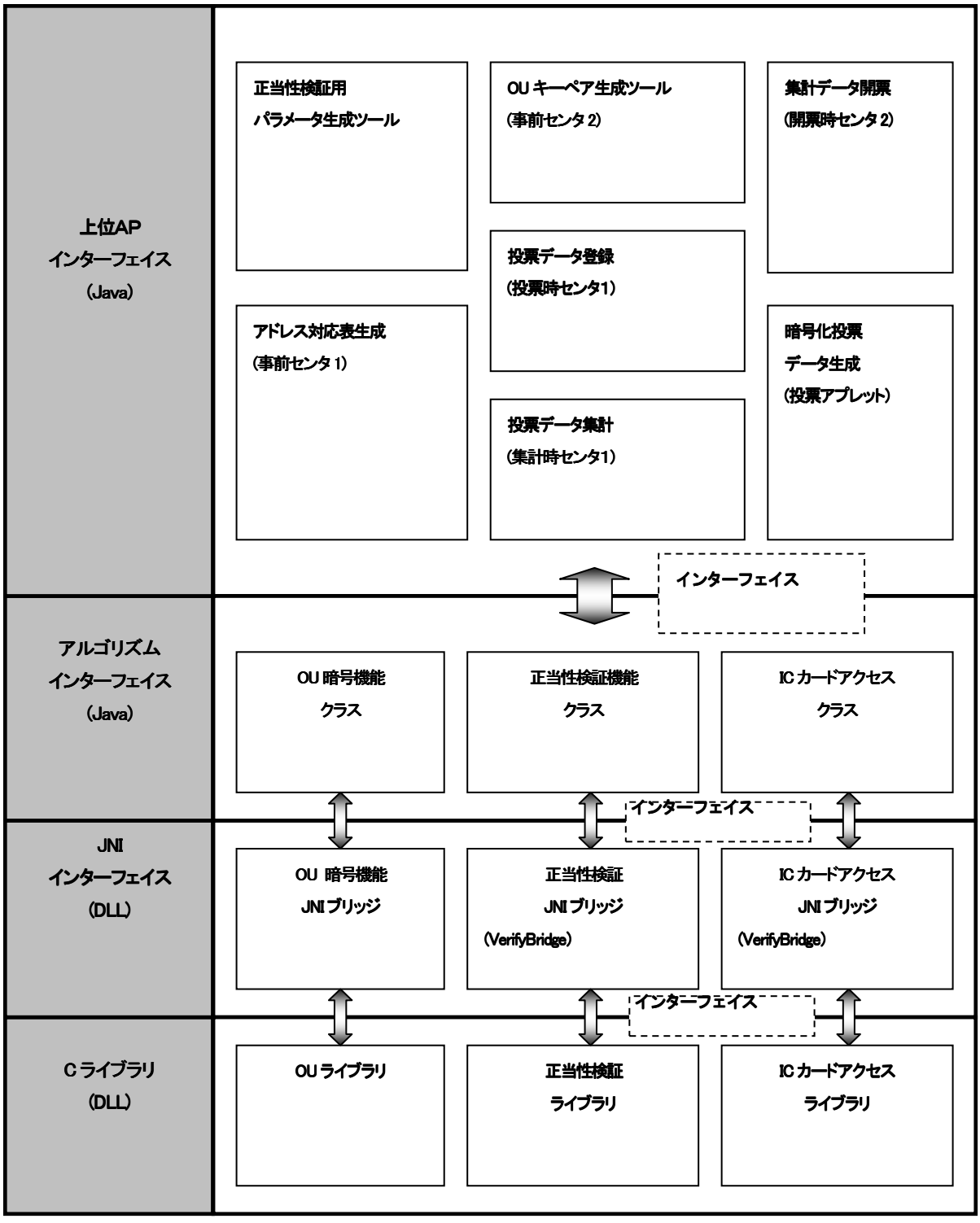



図 47 暗号コア機能 ブロック全体構成

**b) 暗号コア機能クラス図**

暗号コア機能のクラス図を以下に示す。

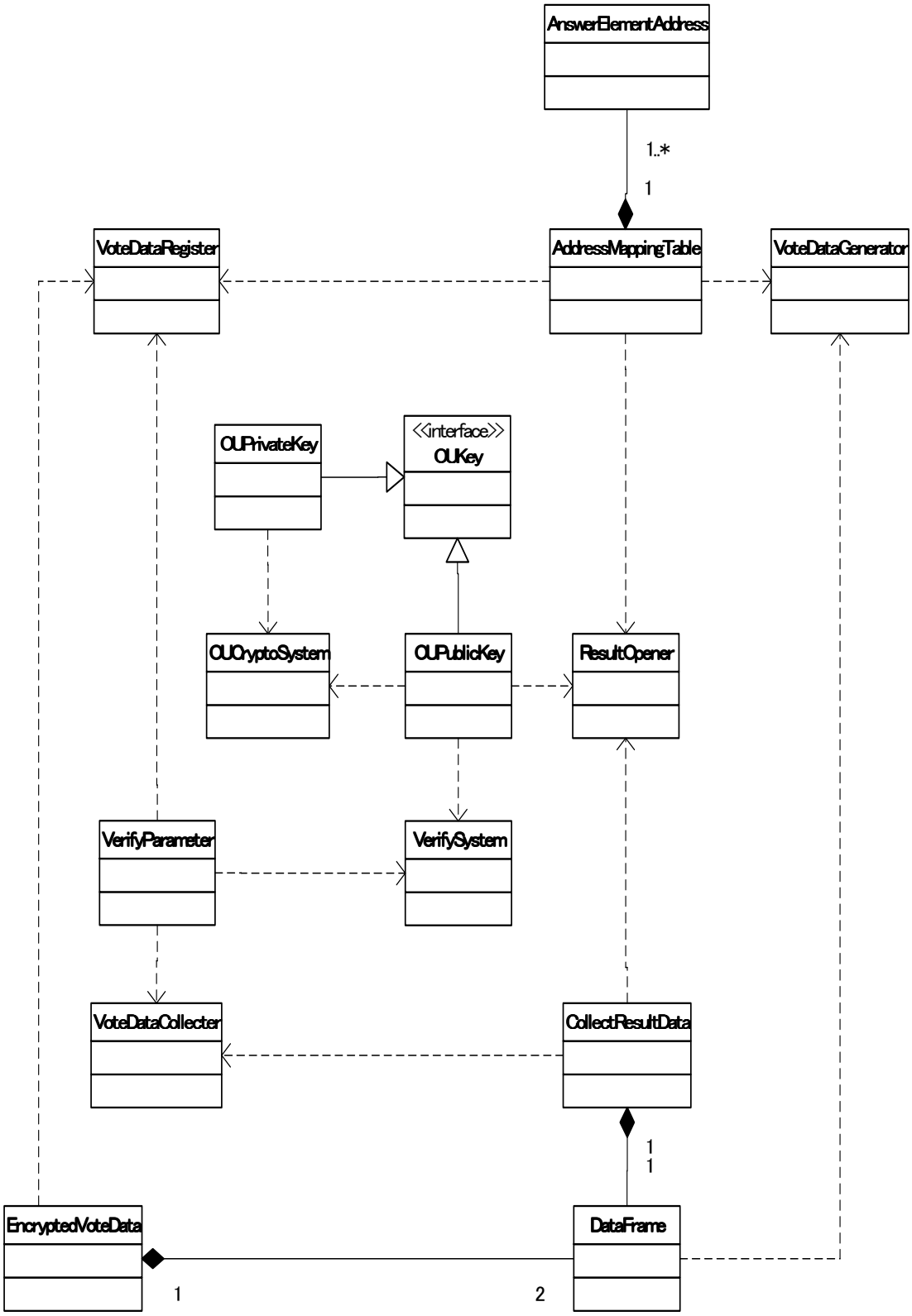



図 48 暗号コア機能 クラス図

暗号関連機能のクラス階層図を下記に示す。

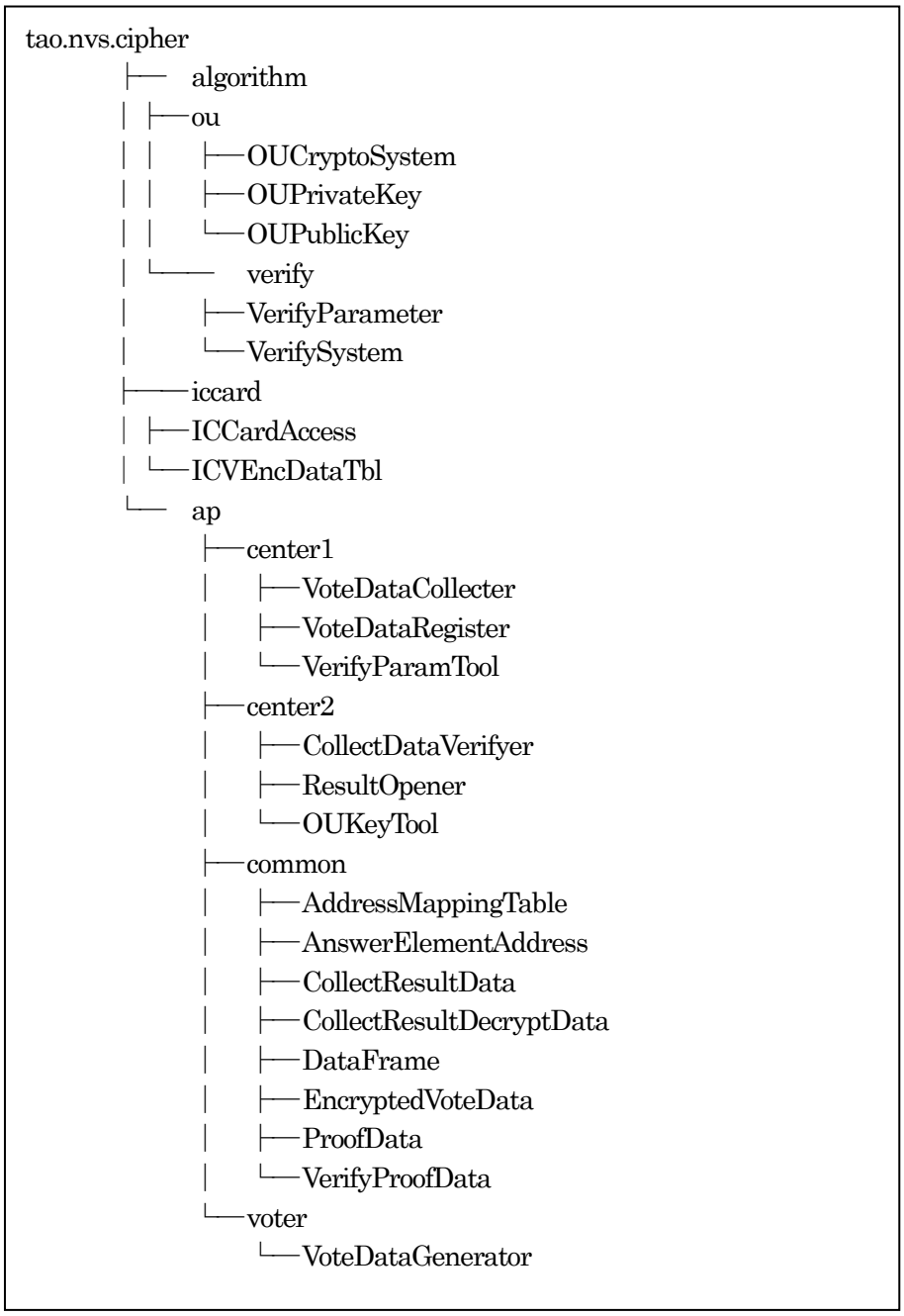



**図 49 暗号コア機能 クラス階層図**

**(iii) 共通化機能の整理**

H15年度実装した機能の中で共通化出来る機能は、アルゴリズムインタフェースとして提供している暗号化アルゴリズムに関する機能が挙げられる。以下にその機能をまとめる。

**a) 暗号システム機能**

本機能は、公開鍵暗号方式に関する各種の機能を提供する。

①鍵ペア生成機能
公開鍵・秘密鍵のリストを返す機能。
②暗号機能
平文データを暗号化し暗号データを返す機能。
③復号化機能
暗号データを復号化し平文データを返す機能。
④鍵ファイル読み込み機能
key オブジェクトを生成し返す機能。
⑤鍵オブジェクト保存機能
鍵をファイルへ保存する機能。
⑥暗号データ2つを加算する機能
暗号データを加算し加算結果暗号データを返す機能。

**b) 秘密鍵機能**

本機能は、秘密鍵データ・鍵サイズを設定・取得する機能を提供する。

①鍵データ取得機能
鍵データを返す機能。
②鍵サイズ取得機能
鍵サイズを返す機能。
③鍵データ設定機能
鍵データを設定する機能。
④鍵サイズ設定機能
鍵サイズを設定する機能。

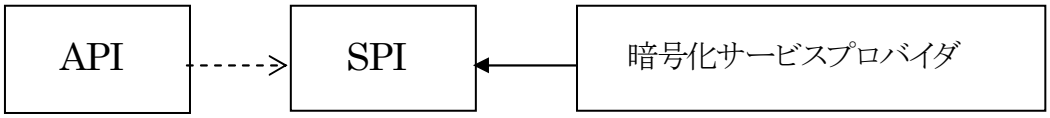
**c) 公開鍵機能**

本機能は、公開鍵データ・鍵サイズを設定・取得する機能を提供する。

①鍵データ取得機能
鍵データを返す機能。
②鍵サイズ取得機能
鍵サイズを返す機能。
③鍵データ設定機能
鍵データを設定する機能。
④鍵サイズ設定機能
鍵サイズを設定する機能。

**(iv) 共通化機能のサービス化**

共通化機能のサービス化手法としては、前述したようにエンジンクラスを用いて、具体的な実装のない抽象的な方法で暗号化サービスを定義する。 エンジンクラスは、特定の暗号化アルゴリズムに依存しない特定の型の暗号化サービス機能へのインタフェースを提供するため、API が提供する特定の種類の暗号化サービスにアプリケーションがアクセスできるようになる。




尚、サービス化の構成方法は、サブテーマ「モデル構築」を参照のこと。

暗号ライブラリ機能のクラス階層図を下記に示す。

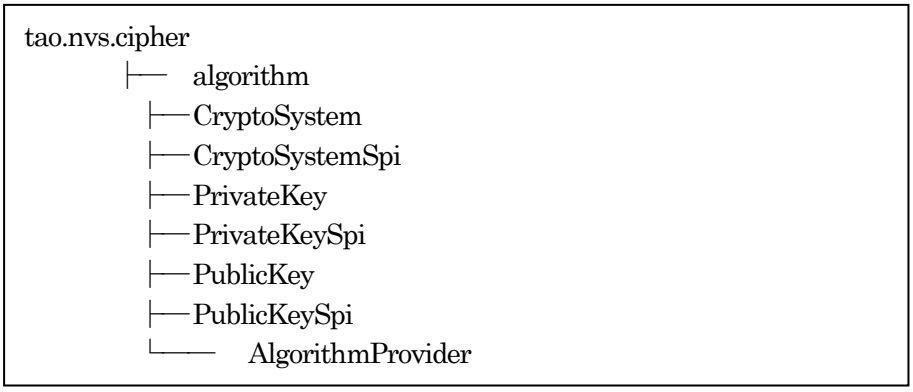
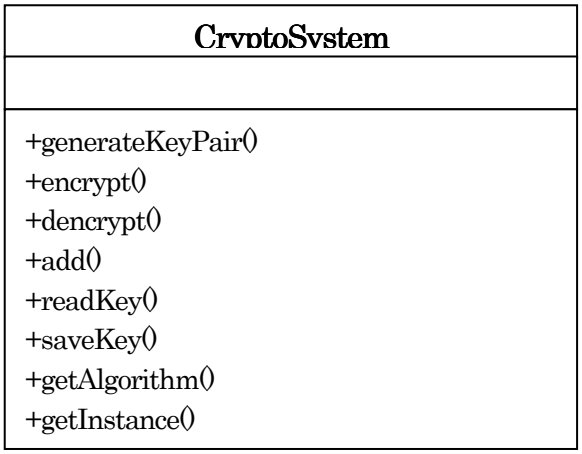



**図 50 暗号ライブラリ機能 クラス階層図**

### a) API クラス

1)暗号システムクラス

共通化機能を提供するクラスを示す。




①generateKeyPair():鍵ペア生成機能
公開鍵・秘密鍵のリストを返す機能。
②encrypt():暗号機能
平文データを暗号化し暗号データを返す機能。
③dencrypt():復号化機能
暗号データを復号化し平文データを返す機能。
④add()暗号データ2つを加算する機能
暗号データを加算し加算結果暗号データを返す機能。

⑤readKey()：鍵ファイル読み込み機能
key オブジェクトを生成し返す機能。
⑥saveKey()：鍵オブジェクト保存機能
鍵をファイルへ保存する機能。
⑦getAlgorithm() ：
実装の詳細に依存しない暗号化アルゴリズムを識別する文字列を返す機能。
⑧getInstance() ：
指定された暗号化アルゴリズムを実装するオブジェクトを作成する機能。
⑨getProvider() ：
オブジェクトのプロバイダを返す機能。

2)秘密鍵クラス
秘密鍵を保持するクラスを示す。

| PrivateKey |
| --- |
| |
| +getKey()<br>+getKeySize()<br>+setKey()<br>+setKeySize()<br>+toString()<br>+getAlgorithm()<br>+getInstance()<br>+getProvider() |

①getKey()：鍵データ取得機能
鍵データを返す機能。
②getKeySize()：鍵サイズ取得機能
鍵サイズを返す機能。
③setKey()：鍵データ設定機能
鍵データを設定する機能。
④setKeySize()：鍵サイズ設定機能
鍵サイズを設定する機能。
⑤toString()：鍵サイズ設定機能
鍵サイズを設定する機能。
⑥getAlgorithm() ：
実装の詳細に依存しない暗号化アルゴリズムを識別する文字列を返す機能。
⑦getInstance() ：
指定された暗号化アルゴリズムを実装するオブジェクトを作成する機能。
⑧getProvider() ：
オブジェクトのプロバイダを返す機能。

3)公開鍵クラス
公開鍵を保持するクラスを示す。

| PublicKey |
| --- |
| |
| +getKey()<br>+getKeySize()<br>+setKey()<br>+setKeySize()<br>+toString()<br>+getAlgorithm()<br>+getInstance()<br>+getProvider() |

①getKey():鍵データ取得機能
鍵データを返す機能。
②getKeySize():鍵サイズ取得機能
鍵サイズを返す機能。
③setKey():鍵データ設定機能
鍵データを設定する機能。
④setKeySize():鍵サイズ設定機能
鍵サイズを設定する機能。
⑤toString():鍵サイズ設定機能
鍵サイズを設定する機能。
⑥getAlgorithm() :
実装の詳細に依存しない暗号化アルゴリズムを識別する文字列を返す機能。
⑦getInstance() :
指定された暗号化アルゴリズムを実装するオブジェクトを作成する機能。
⑧getProvider() :
オブジェクトのプロバイダを返す機能。

### b) SPI クラス

各 API クラスに対応する抽象 SPI クラスを示す。

1)暗号システムクラス

このクラスは、CryptoSystem クラスの Service Provider Interface (SPI) を定義する。特定暗号化アルゴリズムの実装を提供する各暗号化サービスプロバイダは、このクラスのすべての抽象メソッドを実装する必要がある。

| CryptoSystemSpi |
| --- |
| |
| +generateKeyPair()<br>+encrypt()<br>+dencrypt()<br>+add()<br>+readKey()<br>+saveKey() |

2) 秘密鍵クラス

| PrivateKeySpi |
| --- |
| |
| +getKey()<br>+getKeySize()<br>+setKey()<br>+setKeySize()<br>+toString() |

3) 公開鍵クラス

| PublicKeySpi |
| --- |
| |
| +getKey()<br>+getKeySize()<br>+setKey()<br>+setKeySize()<br>+toString() |

**c) Provider クラス**

API クラスのプロバイダを表すクラスである。

| AlgorithmProvider |
| --- |
| |
| +getInfo()<br>+getName()<br>+getVer()<br>+toString() |

## 3-7-3 まとめ

本章では、暗号ライブラリとして提供する機能例を示し、サービスプロバイダというアーキテクチャを用いることで、暗号エンジンクラスのサービス化を検討した。

# 3-8　実験

## 3-8-1　実験の方針

### 3-8-1-1　背景、目的

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、自治体へ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。その結果、山梨市殿，箕輪町殿（以下、敬称略）の 2 自治体にご理解を得られ、実際に実験を実施することが出来た。

自治体実験の目的としては、下記を設定した。

- ◆ 性能，運用性の確認を行う。
- ◆ 有用性、安全性、利便性等に関する意識調を実施し、今後の課題とする。

## 3-8-2　自治体実験

中央コリドー高速通信実験協議会により、メンバーとなっている自治体など多方面に声をかけ、ご興味頂いた 3 自治体に実験の説明を実施した。実験で単発実施という位置づけのため、投票テーマ選定にかなり苦しみ、山梨市が決まったのみであったが、その後箕輪町に了解を得られ、結果的に 2 自治体で実施することとなった。実験の詳細については別冊を参照されたい。

### 3-8-2-1　実験イメージ

山梨市電子アンケート、箕輪町電子アンケートのイメージを記載する。

山梨市電子アンケートは投票は中学校のパソコンルーム PC（約 40 台）で実施し、東京データセンタに構築した集計センタで投票を受け付ける。投票期間終了後集計を実施して、山梨市の中学校に設置した開票センタより、集計データをダウンロードし、開票を実施する。

箕輪町電子アンケートは投票は各家庭，情報センタ，公民館で実施し、東京データセンタに構築した集計センタで投票を受け付ける。投票期間終了後集計を実施して、情報センタに設置した開票センタより、集計データをダウンロードし、開票を実施する。

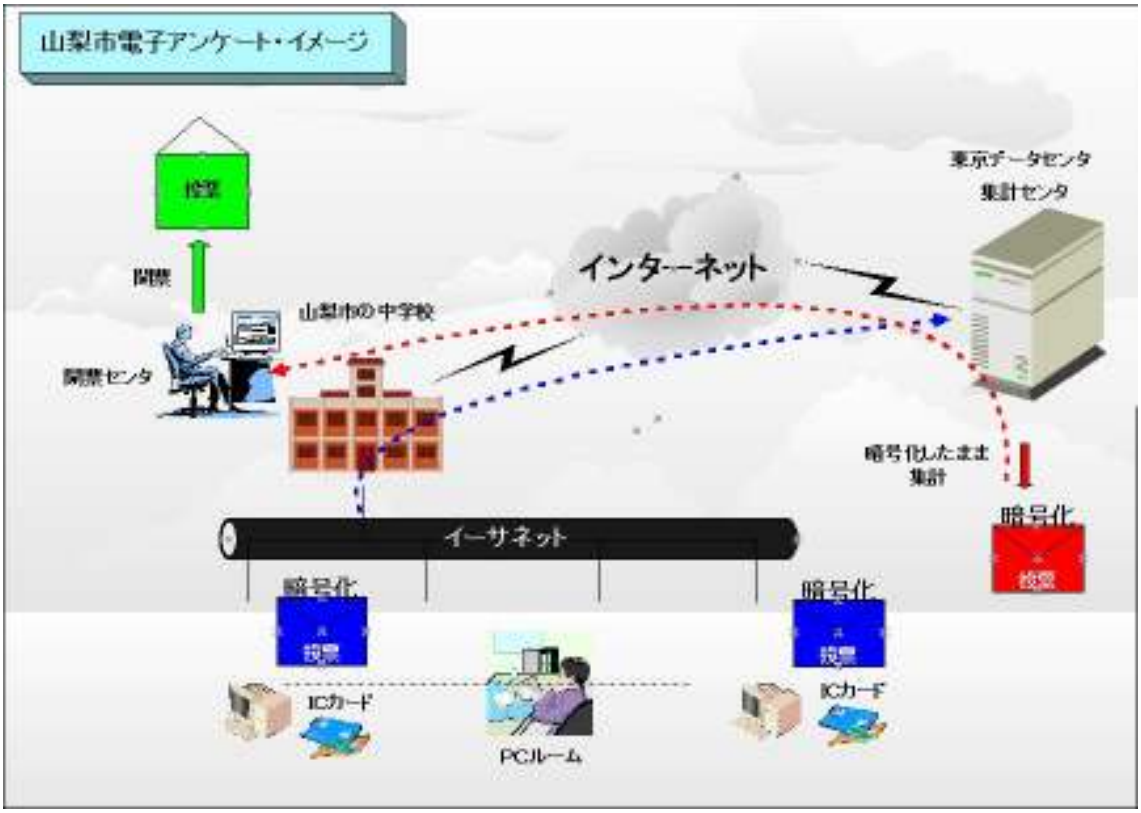



図 **51**　山梨市電子アンケート・イメージ

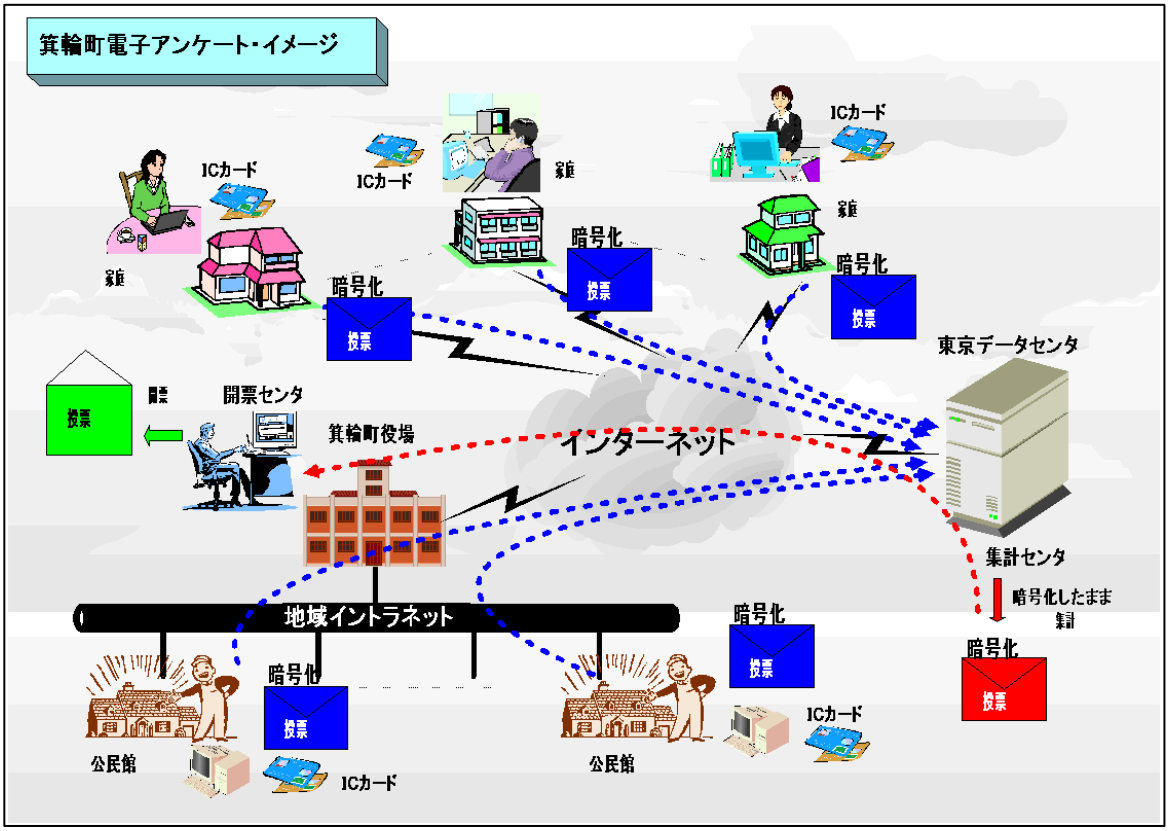
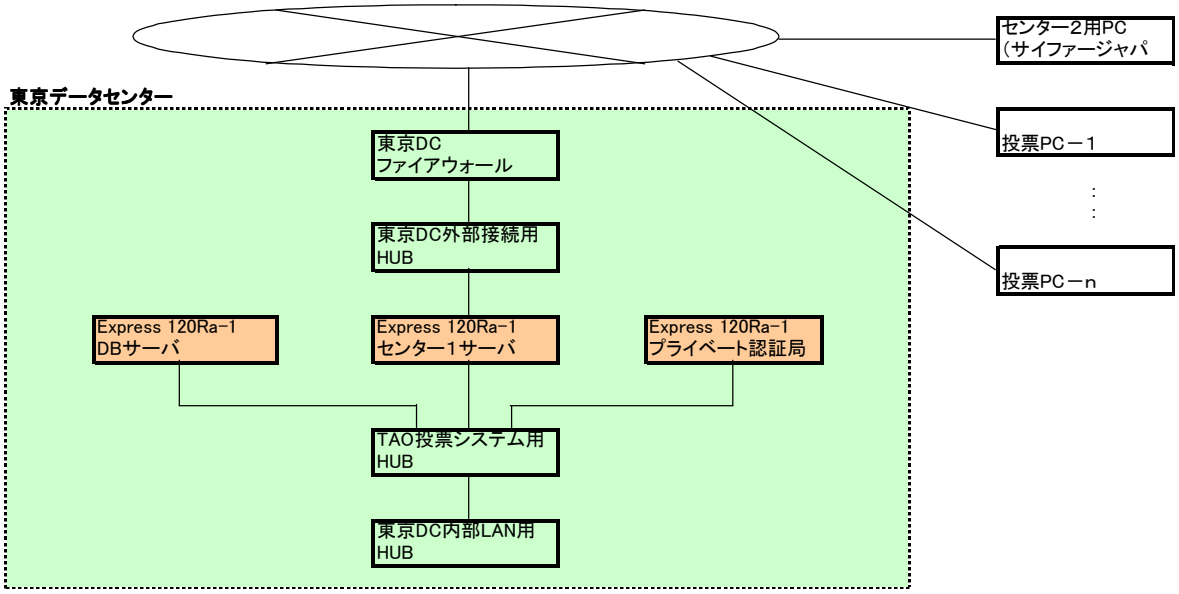



図 **52**　箕輪町電子アンケートイメージ

### a) 集計センタ（センタ１サーバ）構成

集計センタに設置したセンタ１サーバおよび構成機器のネットワーク構成を記載する。




東京データセンター内設置サーバスペック

| ｺﾝﾋﾟｭｰﾀ名 | 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 | 1GHz |
| メモリ | 1179Mbyt | 1179Mbyt | 1179Mbyt |
| 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 53 集計センタ(センタ1サーバ)構成図**

[センタ１サーバの仕様]

- コンピュータ　Express5800/120Ra-1
- OS　Windows2000Server　SP4
- CPU　PentiumⅢ　1GHz　×　2
- メモリ　1179Mbyte

[センタ１サーバのアプリケーション]

- IIS5.0
- Apache　Tomcat　4.1

[データベース（DB）サーバのアプリケーション]

- Oracle9i

[プライベート認証局のアプリケーション]

- CertWorker　1.0

**b) 開票センタ（センタ 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。

[センタ 2 サーバの仕様]

- コンピュータ　　ノート PC　VersaPro VY30Y/AG
- OS　　WindowsXP
- CPU　　PentiumⅣ　3GHz
- メモリ　　256Mbyte
- USB ポート
- CD-ROM ドライブ
- ネットワーク環境

[センタ 2 サーバのアプリケーション]

- j2re-1_3_1_09

**c) 投票者 PC 環境**

本実験で使用する投票者 PC 条件は以下の通りである。

[センタ 1 サーバの仕様]

- Windows98SE、WindowsME、Windows2000、WindowsXP
  ※Windows98SE、WindowsME では、「Microsoft Smart Card Base Components」の追加が必要
- Internet Explorer 5.5 以上
- USB ポート
- CD-ROM ドライブ
- ネットワーク環境
- Java ランタイムライブラリ 1.3.1_09

## 3-8-3 性能検証

### 3-8-3-1 目的

自治体実験で得られた投票, 集計センタ, 開票センタの性能を示し、H15 年度までの実装時性能測定と比較する。

また、投票性能に関してはシステム構成での性能測定結果と著しい差がみられたため、原因を調査し、改善方法を検討した。

### 3-8-3-2 投票性能

投票性能に関しては、意識調査アンケートで「投票にかかった時間」についての感想を頂いた。概ね、気にならなかったとの感想であったが、アンケートに回答している時間も含まれており、IC カードでの暗号化処理時間に関しては、かなり遅いと認識できた。これは、実装時の性能測定結果と比較して大きな開きがあり、この差を検証する必要がある。

### (i) 意識調査アンケートの感想

実施した意識調査アンケートの中で、投票性能に関する感想を示す。

#### a) 山梨市

表 29 投票時間に関する感想

| 投票時間の長さは気にならなかった。 | 少し時間がかかったと思った | 結構時間がかかったと思った。 | 非常に時間がかかったと思った。 |
|---|---|---|---|
| 110 | 39 | 7 | 0 |

山梨市殿では、この他に投票時間(アンケートに回答している時間含む)と投票機からの応答時間(IC 処理時間＋投票受付時間)にどれくらいかかったかの回答を得ている。

表 30 実際の投票時間に関する質問

| 時間(分) | 投票数 | 時間(分) | 投票数 |
|---|---|---|---|
| 1 | 4 | 11 | 0 |
| 2 | 14 | 12 | 1 |
| 3 | 21 | 13 | 0 |
| 4 | 9 | 14 | 0 |
| 5 | 27 | 15 | 6 |
| 6 | 1 | 16 | 0 |
| 7 | 1 | 17 | 0 |
| 8 | 0 | 18 | 0 |
| 9 | 0 | 19 | 0 |
| 10 | 37 | 20 | 8 |

表 31 投票時間のうち、投票機からの応答を待っている時間

| 時間(分) | 投票数 | 時間(分) | 投票数 |
|---|---|---|---|
| 1 | 23 | 11 | 0 |
| 2 | 32 | 12 | 0 |
| 3 | 30 | 13 | 0 |
| 4 | 4 | 14 | 0 |
| 5 | 24 | 15 | 0 |
| 6 | 0 | 16 | 0 |
| 7 | 4 | 17 | 0 |
| 8 | 2 | 18 | 0 |
| 9 | 1 | 19 | 0 |
| 10 | 3 | 20 | 0 |

投票機からの応答時間は、投票サポートしている状況で測定したレベルで、約 1 分 30 秒程度であり、アンケートに回答している時間に比べればそれ程待たされているとの感覚は持たなかった。但し、これが選挙などの短時間投票となれば、この応答時間が際だってくると考えられる。

次に箕輪町殿での意識調査結果を記載するが、この時間に関しては更に遅くなり、アンケート回答時間を考慮しても遅いと感じられる。

**b) 箕輪町**

**表 32 投票時間に関する感想**

| 投票時間の長さは気にならなかった。 | 少し時間がかかったと思った | 結構時間がかかったと思った。 | 非常に時間がかかったと思った。 |
|---|---|---|---|
| 90 | 101 | 28 | 6 |

箕輪町殿では、投票時間と投票機からの応答時間の回答を得られていないが、投票をサポートしている状況で測定したレベルで、約 2 分 30 秒程度であった。このため、非常に遅いとの感想も頂いている。

**(ii) H15 年度 IC カード処理の性能測定結果**

**a) 性能測定環境**

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

**b) 性能測定結果**

①暗号化処理結果

**表 33 1024bit 鍵の暗号処理結果**

| 平文ｻｲｽﾞ(bit) | 暗号化時間(ms) |
|---|---|
| 30 | 335 |
| 60 | 342 |
| 90 | 354 |
| 120 | 362 |
| 340 | 436 |

②コミットメントデータ生成結果

**表 34 1024bit 鍵のコミットメントデータ生成処理結果**

| コミットメントデータ生成時間(ms) |
|---|
| 143 |

③電子署名データ生成結果

**表 35　1024bit 鍵の電子署名データ生成結果**

| コミットメントデータ生成時間(ms) |
|---|
| 89 |

### (iii) 机上計算結果

#### a) 山梨市

山梨市殿で実施した電子アンケートの IC カード処理時間を H15 年度実施した性能測定結果を元に机上計算する。

1)暗号化条件
・鍵長 1024bit、投票者数 1000、設問 17、候補者数約 5

2)暗号化ブロック数
・暗号ブロック数:17 ブロック

3)机上計算
①1024bit 鍵の暗号処理結果
平文サイズ　　暗号化時間
(bit) (ms)
340　436
②コミットメントデータ生成時間:143ms
③電子署名データ生成時間:89ms
－－－－－－－－－－－－－－－－－－－－－－
合計　665ms×17 ブロック＝11.3s

#### b) 箕輪町

1)暗号化条件
・鍵長 1024bit、投票者数 1000、設問 28、候補者数約 6.1（171/28 平均）

2)暗号化ブロック数
・暗号ブロック数:28 ブロック

3)机上計算
①1024bit 鍵の暗号処理結果
平文サイズ　暗号化時間
(bit) (ms)
340　436
②コミットメントデータ生成時間:143ms
③電子署名データ生成時間:89ms
－－－－－－－－－－－－－－－－－－－－－－
合計　665ms×28 ブロック＝18.6s

**(iv) 実験データと机上計算値の比較**

下記の比較表によりはっきりと差異が確認できる。実験データは投票者認証や投票登録時間も含まれているが、極端な違いが見られるので、IC カード内処理を調査する必要がある。

**表 36 比較表**

| | 実験データ | 机上計算値 |
|---|---|---|
| 山梨市 | 約 1min30s | 11.3s |
| 箕輪町 | 約 2min30s | 18.6s |

**(v) IC カード性能調査**

IC カードの性能を調査するため、処理時間測定用機能を IC カード用 API に組み込み、IC カードに対する処理状態をモニタする。また、モニタした結果により、遅くなっている原因を掴み、対策を検討する。

**a) 処理時間測定機能**

①CPU 時間の取得

標準ライブラリである clock()関数を用いることで、プログラム起動後の CPU 積算時間を取得できる。今回の処理時間測定には本関数を使用する。

この関数で取得できる値が 1 増えると、(1/CLOCKS_PER_SEC)秒経過したことを表す。CLOCKS_PER_SEC=1000 なので、1ms 単位で計測可能である。

②LOG の保存

LOG の保存は CSV 形式で行う。ファイル名は「ICCLOG.csv」とし、必ず C ドライブ直下に保存する。

**(形式)　※1**

**[関数名],[処理概要],[開始],[終了]**

**(実例)**

**ICV_Initial,IC カード初期化,0,20**
**ICV_Write,投票テーブル格納,35,200**
**ICV_Write,投票データ格納,210,330**
**ICV_Final,終了処理,340,350**

**b) 測定手順**

①計測準備

IC カードにアクセスするためには、必ず ICV_Initial()関数を呼び出し、ハンドラを取得する必要がある。この関数は投票全体の流れの中で最初に呼び出される API である。この関数内で、計測結果を記録するためのファイルをオープンし、計測開始日時を書き込むものとする。

②計測結果の保存

各 API の先頭と末尾でタイマカウンタを取得し、②LOG の保存で述べた※1 の形式で処理時間の計測結果を記述していく。[開始]、[終了]欄には clock()関数によって取得できた値をそのまま記述する。

③計測完了

投票処理の最後には、必ず ICV_Final()関数が呼び出される。この関数内で、計測完了日時を書き込み、ファイルをクローズする。

④検証環境

検証を行うため、実際に箕輪町で実施されたアンケートと同じ投票作業を合計 10 回行い、

各処理にかかった平均時間を算出する。アンケートの設問数、使用した PC の性能は以下の通り。

⑤調査データ

箕輪町アンケート　：　暗号ブロック 28

⑥性能測定環境

CPU　：　Intel Pentium M 1.5GHz

メモリ　：　512 MB

OS　：　Microsoft Windows XP Professional Service Pack 1

**c) 測定結果**

**表 37　IC カード処理時間測定結果**

| Fanction | 処理時間(Sec) | | | |
|---|---|---|---|---|
| 初期化 | | | | 0.060 |
| 外部認証 | | | | 0.109 |
| Block | 投票回答テーブル書き込み | 投票データ書込み | 暗号処理 | 計 |
| 1 | 0.037 | 0.034 | 1.358 | 1.429 |
| 2 | 3.075 | 0.059 | 1.356 | 4.490 |
| 3 | 3.104 | 0.049 | 1.357 | 4.510 |
| 4 | 3.090 | 0.064 | 1.378 | 4.532 |
| 5 | 3.079 | 0.043 | 1.357 | 4.479 |
| 6 | 3.097 | 0.042 | 1.354 | 4.493 |
| 7 | 3.087 | 0.064 | 1.397 | 4.548 |
| 8 | 3.097 | 0.038 | 1.348 | 4.483 |
| 9 | 3.099 | 0.046 | 1.349 | 4.494 |
| 10 | 3.097 | 0.049 | 1.366 | 4.512 |
| 11 | 3.083 | 0.035 | 1.348 | 4.466 |
| 12 | 3.086 | 0.055 | 1.373 | 4.514 |
| 13 | 3.085 | 0.034 | 1.346 | 4.465 |
| 14 | 3.102 | 0.065 | 1.379 | 4.546 |
| 15 | 3.123 | 0.048 | 1.352 | 4.523 |
| 16 | 3.110 | 0.040 | 1.350 | 4.500 |
| 17 | 3.088 | 0.046 | 1.358 | 4.492 |
| 18 | 3.097 | 0.060 | 1.382 | 4.539 |
| 19 | 3.080 | 0.041 | 1.354 | 4.475 |
| 20 | 3.095 | 0.041 | 1.354 | 4.490 |
| 21 | 3.108 | 0.039 | 1.355 | 4.502 |
| 22 | 3.114 | 0.041 | 1.358 | 4.513 |
| 23 | 3.077 | 0.040 | 1.352 | 4.469 |
| 24 | 3.078 | 0.040 | 1.368 | 4.486 |
| 25 | 3.087 | 0.044 | 1.357 | 4.488 |
| 26 | 3.103 | 0.039 | 1.350 | 4.492 |
| 27 | 3.114 | 0.037 | 1.352 | 4.503 |
| 28 | 3.102 | 0.036 | 1.364 | 4.502 |
| 終了 | | | | 3.056 |
| トータル時間 | | | | 126.160 |

**d) 検証**

1)投票処理の流れ

投票データの暗号化が完了するまでの、IC カード内部の処理についてまとめる。

①PC－IC カード間通信の流れ

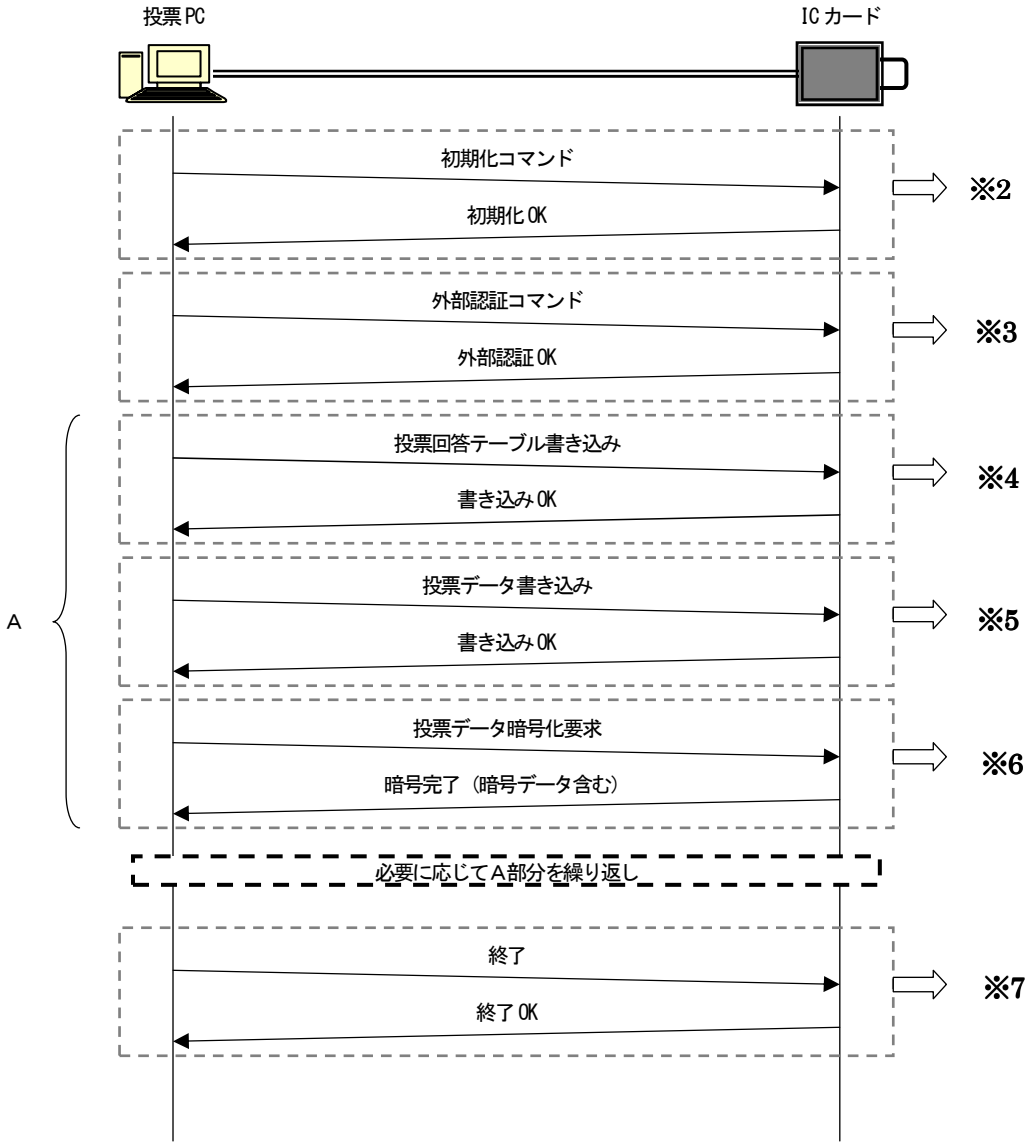



**図 54 PC－IC カード間通信の流れ**

②IC カード内処理詳細

●初期化　※2

IC カード内の投票アプリケーションを起動させ、投票やカード発行などの作業を行うための初期化を実行する。

●外部認証　※3

初期化完了後、投票作業を行うための認証を実行する。

●投票回答テーブル書き込み　※4

IC カード内で「投票回答テーブル書き込み」要求を受信すると、以下の動作が発生する。

・既に存在する投票回答テーブルと投票データの消去
・新しい投票回答テーブルの書き込みデータ作成
・投票回答テーブル書き込み

RAM 容量の関係上、投票回答テーブル及び投票データはフラッシュメモリ上に格納される。今回の実験のように、設問毎に投票回答テーブルの更新が行われる場合、その都度フラッシュメモリの消去処理が発生する。

●投票データ書き込み　※5

投票データも、投票回答テーブルと同じくフラッシュメモリ上に格納される。

また投票データの書き込みには、既に投票回答テーブルが書き込まれている状態でなければならない。上記、「投票回答テーブル書き込み」※4 にあるように、投票回答テーブルの書き込みを行った時点でフラッシュメモリ上に存在する投票データも消去されるため、この段階で再度消去処理が行われることはない。

●暗号処理　※6

IC カード内のアプリケーションでは暗号ブロックごとに完了フラグを設定し、投票データの２重暗号化を防止している。暗号処理実行時に、該当する投票ブロックに対応した完了フラグをセットする。

尚、この完了フラグはフラッシュメモリ上に存在する。

●終了処理　※7

全ての投票が完了すると、安全面を考えて投票に使用された投票回答テーブルと投票データの消去を行っている。

**e) 考察**

測定結果より、投票処理のボトルネックとなっているのは「投票回答テーブル書き込み」、「暗号処理」、「終了」の 3 箇所であることが判る。また、各処理時間の平均を比較してみると、「投票回答テーブル書き込み」と「終了」が約 3 秒とほぼ同じであり、暗号処理は約 1.3 秒と前述の 2 処理の半分以下となっている。

これらの処理に共通しているのはフラッシュメモリの消去処理が発生することである。そして

フラッシュメモリの消去処理が、投票全体のボトルネックになっているものと考えられる。根拠として、以下の 4 点が挙げられる。

①一般的にフラッシュメモリとはその消去に時間がかかる。
②上記 3 つの処理以外で、フラッシュメモリの消去を行っているものはいない。
③「投票回答テーブル書き込み」と「終了」では 2 回、「暗号処理」では 1 回消去処理が発生し、「投票回答テーブル書き込み」と「終了」がほぼ同じ処理時間になっている。
④1（block）の「投票回答テーブル書き込み」では処理に時間を要していない。これはフラッシュメモリ上に投票回答テーブルが存在しないので、消去を行っていないためである。

投票回答テーブルと投票データの格納先をフラッシュメモリとしたのは、IC カードの資源の問題からである。本来フラッシュメモリはセンタ 2 公開鍵やコミットメントデータ用パラメータ等、IC カード発行後に書き換えの必要が少ないデータのみを格納すべきであり、投票回答テーブルや投票データ等、頻繁に書き換えが行われるデータは RAM 上に専用の領域を確保すべきである。
しかし、IC カードの限られた資源では RAM 領域の確保が難しいため、容量に余裕のあるフラッシュメモリに格納し、必要に応じて読み出すよう処理を行っていた。

今回は設問ごとに投票回答テーブルと投票データの格納が行われており、また設問数も 28 と多いため、フラッシュメモリの消去が全体のパフォーマンスの低下に繋がっている。設問数が増えればそれだけ処理時間も延びるので、改善の必要性が極めて高いと判断する。

以下にフラッシュメモリの消去について説明する。

1)IC カードのフラッシュメモリ仕様

IC カードには、1Mbyte のフラッシュメモリが搭載されている。フラッシュメモリは 64Kbyte 単位の 16 ブロックで構成され、さらにその内の特定の 1 ブロックは 8Kbyte 単位の 8 ブロックに分割されている。

Block 1 は IC カードのシステムに予約された領域で、ユーザアプリケーションが使用することは出来ない。また、S-Block 1～3 もシステムに予約されている。さらに 64KByte 単位ブロックの内 1 ブロックは後述する消去処理用に予約されているため、使用可能な領域は Block 2～15 の内 13 ブロックとなる。

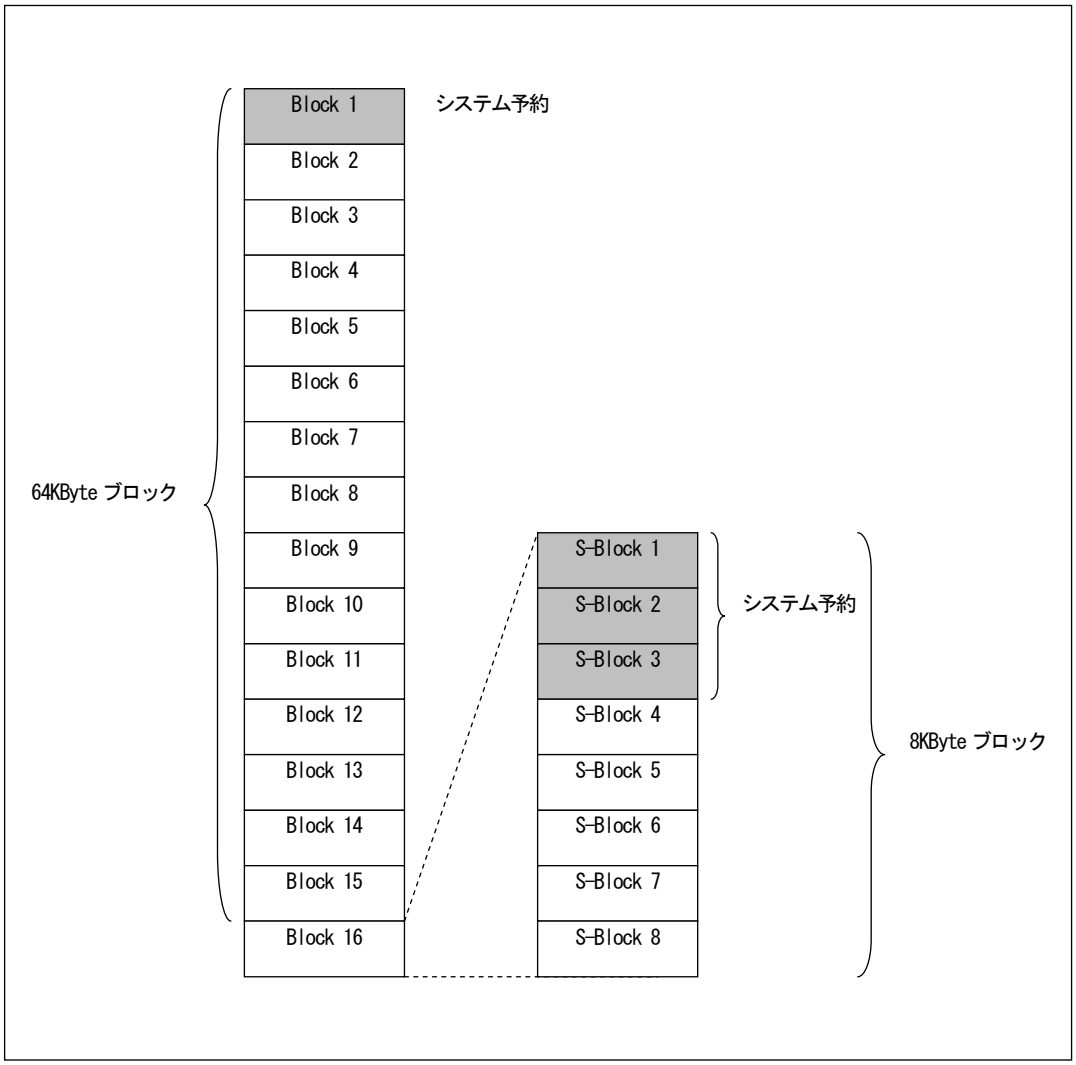



**図 55 IC カード フラッシュメモリブロック図**

2)データの書き込みと消去

IC カードのフラッシュメモリは、ユーザアプリケーションによって直接操作することが出来ない。これは書き込まれたデータをプロテクトするためで、直接 Read/Write を試みた場合プログラムが強制終了する仕組みになっている。

データの書き込みや消去にはシステム関数を使用する。この場合、書き込み先または消去するブロックを選択することは出来ず、各データにユーザ自身が割り振った ID を用いる。

書き込み関数では、対象のデータのサイズから格納できるブロックを自動的に選択し、そこに書き込むようになっている。サイズによっては他のデータが既に書き込まれているブロックが選択される。

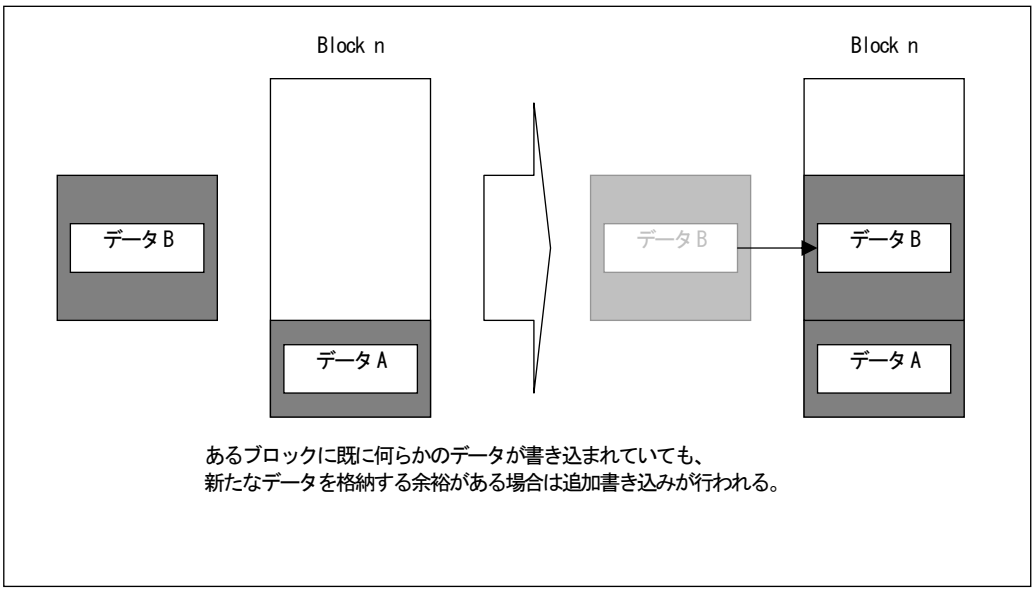



**図 56 IC カード フラッシュメモリ書き込み例**

前項の図のような同一ブロックに複数のデータが混在する状況下で消去を行う場合、本来消去したいデータ以外も消去してしまうことになる（フラッシュメモリはブロック単位でしか消去できない）。この時に、消去処理用に予約された領域が使用される。

消去要求があったデータを除いた他のデータを予約領域にコピーする。その後、元のブロックを消去し、新たな予約領域としている。

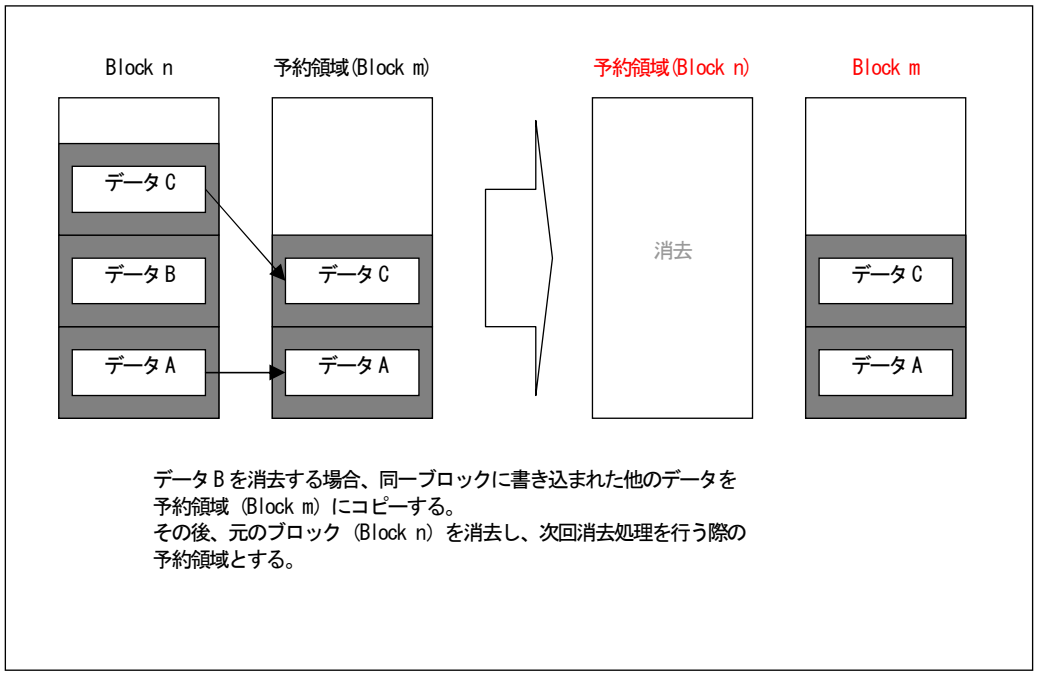



**図 57 IC カード フラッシュメモリ消去例**

3)投票処理の図解

●設問１の場合

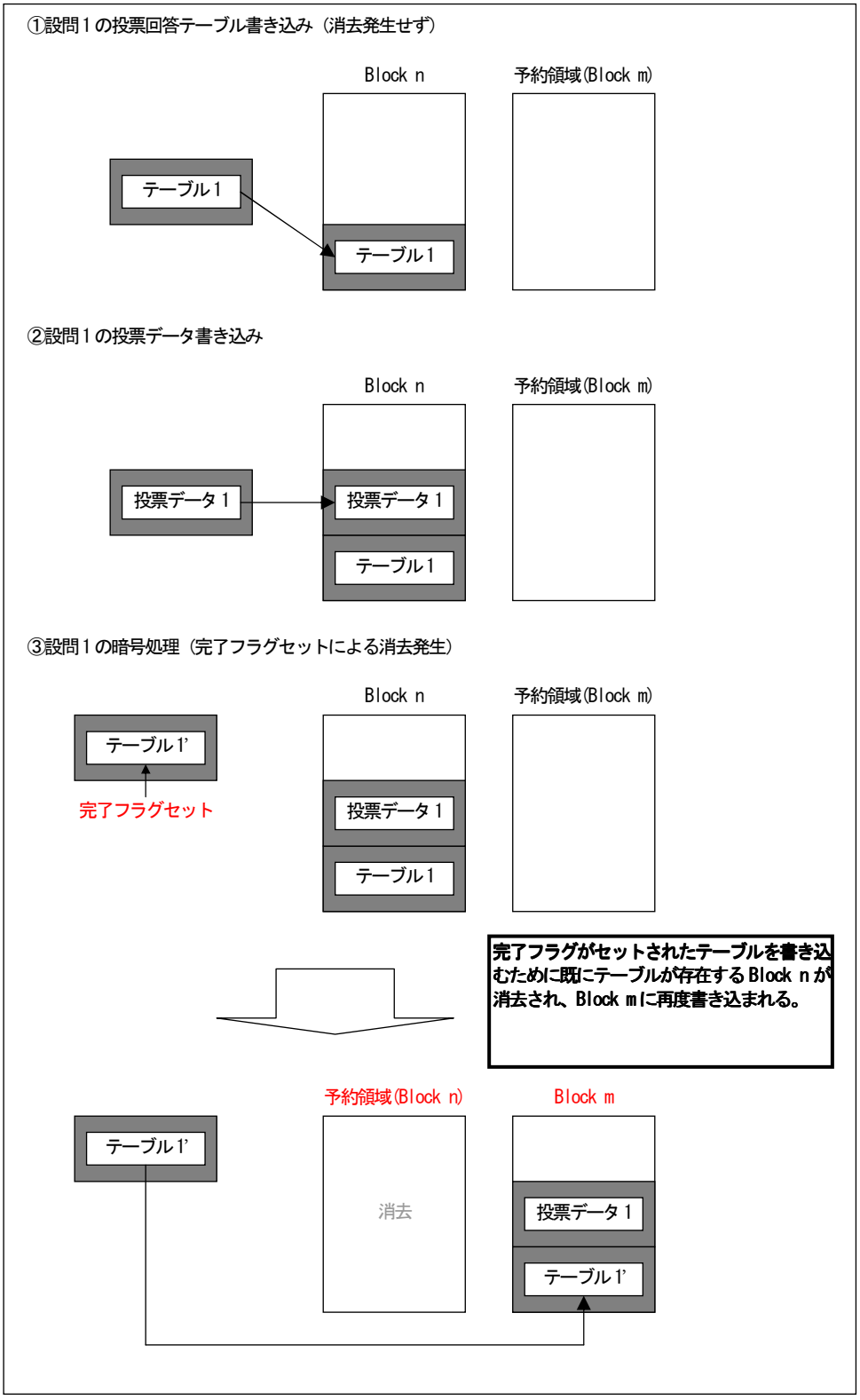



**図 58　投票処理　設問１の場合**

●設問２以降の場合

設問１との違いは投票回答テーブルの書き込み処理である。

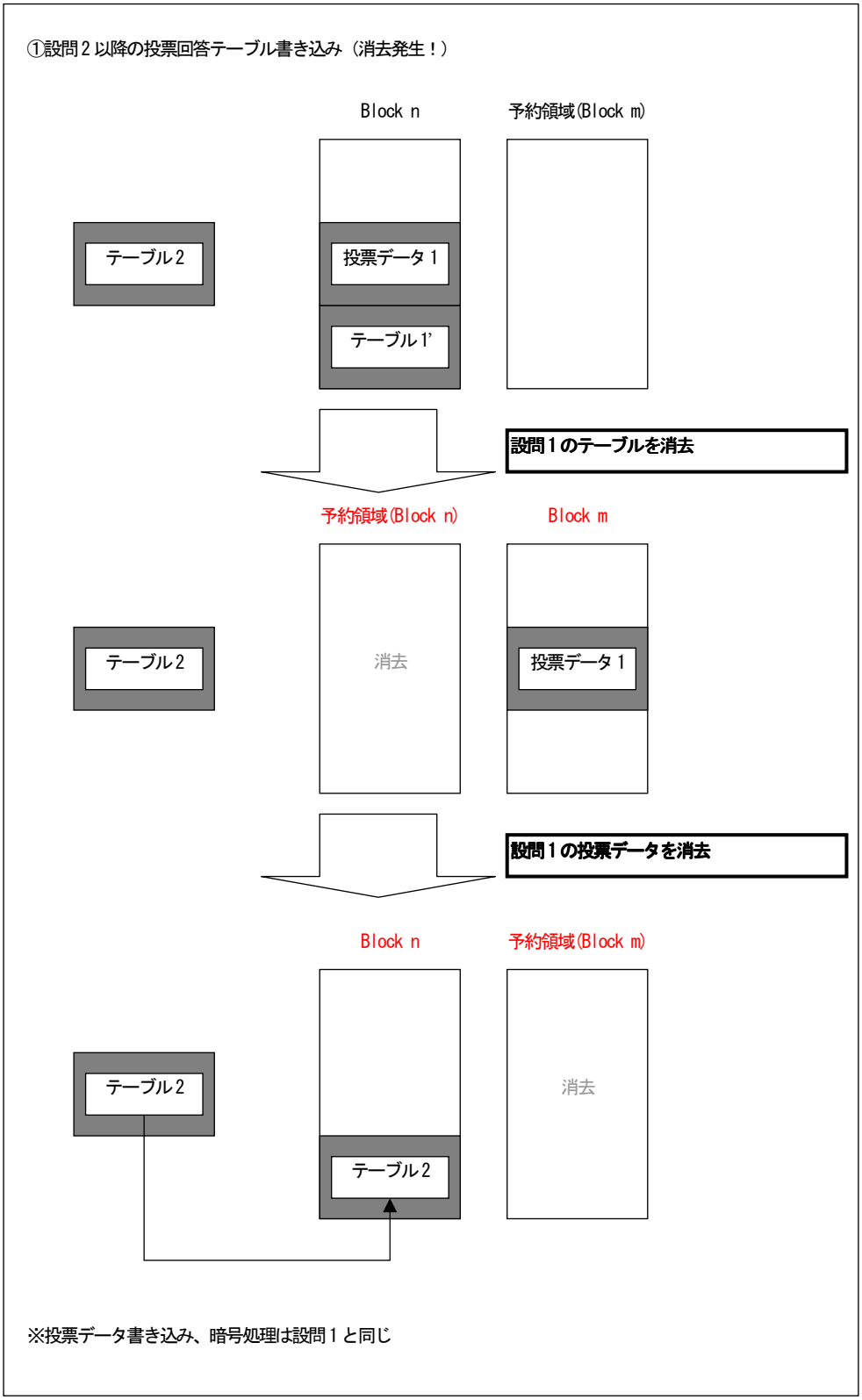



**図 59　投票処理　設問２以降の場合**

**f) 今後の対策案**

処理速度の向上のために、いくつかの対策案を示す。

①投票回答テーブル・投票データの削除

IC カードの機能を簡略化し、上位のアプリケーションで生成された暗号ブロックの暗号化処理のみを行う仕様に変更すれば、e)項で示したフラッシュメモリの消去処理が一切不要となるため、処理速度を向上させることができる。

投票回答テーブル及び投票データは、暗号ブロック生成のために必要なデータである。

IC カード内で暗号ブロックを生成する目的は、不正な投票を防止するためである。しかし外部認証が完了すれば、意図的に操作された投票回答テーブル及び投票データを格納し暗号化することも可能であり、十分に機能するとはいえない。上位アプリケーションの認証の方がより確実であると考える。

②投票回答テーブル・投票データの簡略化

IC カードでの暗号ブロック生成を維持したまま速度向上を図るには、フラッシュメモリに格納されているデータを簡略化し、RAM 上で操作できるように改善する。

現在の仕様では、投票回答テーブルの最大サイズは 1280 バイト、投票データの最大サイズは 765 バイトである。この２つを同時に RAM 上に保持すると暗号化処理を行うために必要な領域が確保できなくなるため、フラッシュメモリへの格納を行っている。

このテーブルをより簡略化し、必要最小限の情報のみで構成すればRAM 上に保持できるようになる。今回の実験のように設問ごとにグループを分けた形にすれば、投票回答テーブル及び投票データのサイズはかなり小さく出来る。

具体的にどのような形式にし、それに伴って生ずる制限事項などは未検討の段階であるが、IC カードアプリケーションを除いたほぼ全てのシステムを今のまま流用可能なため、最も現実的な改善方法と考える。

③IC カードの性能強化

現在使用している IC カードより、さらに性能が上位の IC カードを選択する。RAM 容量が増加されていれば、フラッシュメモリの使用頻度を抑えることが可能になる。

**(vi) 対策後の性能**

対策後の性能を算出する。この結果を基に大規模選挙に対する検証をまとめで実施する。

**a) 山梨市**

(v)IC カード性能調査の結果を元に対策後の性能を机上にて計算する。

1)初期化処理時間

・0.06s

2)外部認証時間

・0.11s

3)暗号ブロック処理時間
①1 暗号ブロック処理時間
・投票回答テーブル書き込み時間 0.04s
・投票データ書き込み時間 0.05s
・暗号処理時間 1.36s
－－－－－－－－－－－－－－－－－－－－－－
合計 1.45s

②17 暗号ブロック処理時間
・1.45×17＝24.65s

4)終了処理時間
・3.06s

5)投票処理トータル時間
・27.88s

**b) 箕輪町**

(v)IC カード性能調査の結果を元に対策後の性能を机上にて計算する。

1)初期化処理時間
・0.06s

2)外部認証時間
・0.11s

3)暗号ブロック処理時間
①1 暗号ブロック処理時間
・投票回答テーブル書き込み時間 0.04s
・投票データ書き込み時間 0.05s
・暗号処理時間 1.36s
－－－－－－－－－－－－－－－－－－－－－－
合計 1.45s

②28 暗号ブロック処理時間
・1.45×28＝40.60s

4)終了処理時間
・3.06s

5)投票処理トータル時間
・43.83s

### 3-8-3-3　センタ 1 性能

センタ 1 性能は、投票の受付処理と集計処理、および集計正当性検証データ生成処理に分けられる。これらの処理時間は、実験実施時にセンタ1で各処理に対するログを採取し、処理時間を計測した。

この値を元に、H15 年度実装時性能測定結果と比較し、改善が必要であるか検証する。

（性能測定環境）

[センタ 1 サーバの仕様]

- コンピュータ　Express5800/120Ra-1
- OS　Windows2000Server　SP4
- CPU　PentiumⅢ　1GHz　×　2
- メモリ　1179Mbyte

[センタ 1 サーバのアプリケーション]

- IIS5.0
- Apache　Tomcat　4.1

[データベース（DB）サーバのアプリケーション]

- Oracle9i

#### (i) 投票受付処理時間

##### a) 山梨市実験結果

表 38　20040901 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 35 名 | 7407 |

表 39　20040902 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 36 名 | 10803 |

表 40　20040903 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 36 名 | 75448 |

表 41　20040909 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 31 名 | 45669 |

表 42 20040913 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 26 名 | 13937 |

**b) 箕輪町実験結果**

表 43 20041206 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 18 名 | 11820 |

表 44 20041207 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 19 名 | 10972 |

表 45 20041208 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 11 名 | 9858 |

表 46 20041209 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 5 名 | 9903 |

表 47 20041210 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 6 名 | 8561 |

表 48 20041211 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 3 名 | 8516 |

表 49 20041212 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 13 名 | 9742 |

表 50 20041213 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 28 名 | 10786 |

表 51 20041214 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 19 名 | 11216 |

表 52 20041215 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 21 名 | 11839 |

表 53 20041216 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 20 名 | 12416 |

表 54 20041217 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 13 名 | 11929 |

表 55 20041218 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 13 名 | 12736 |

表 56 20041219 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 13 名 | 12875 |

表 57 20041220 投票受付処理平均時間

| fanction | 投票者 ID | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 40 名 | 18321 |

表 58 20041222 投票受付処理平均時間

| fanction | 投票者人数 | 平均時間 ms |
|---|---|---|
| 暗号票登録性能 | 49 名 | 22091 |

**c) H15 年度測定結果**

1)1000 候補/100 万人投票者(59,000,000 暗号ブロック)

・トータル時間:117000s(SSL 性能含まず)

・投票者一人あたりの時間:0.117s(59 暗号ブロック時)

(測定環境 : センタ 1 サーバの仕様)

- OS Windows2000Server SP4
- CPU PentiumⅢ 1GHz × 2
- メモリ 1179Mbyte

**d) 考察**

実験ログの測定結果で、山梨市「表 12 20040903 投票受付処理平均時間」,「表 13 20040909 投票受付処理平均時間」の 2 日が他測定結果より、飛び抜けて遅くなっている。この 2 日間は、35 名程度の投票者が PC ルームで、殆ど同時に電子投票の各操作を実施しており、投票者からセンタ1への同時アクセス数が多いためと考えられる。

・20040902(36 名):約 75.5s
・20040909(31 名):約 45.7s

大規模選挙を想定すれば、同時アクセス数は今回の実験の比ではないと予想され、同時アクセス数が増加した場合の応答の遅れを改善する方策は必要となる。

投票をサポートしていた限り、山梨市のその他や箕輪町の場合は、上記に比べて同時アクセス数が少ないと言える。投票者側のネットワーク・PC などの性能はほぼ同じと仮定すれば、「表 20 20041211 投票受付処理平均時間」の性能が、投票者個別の性能として有効であると判断できる。

・20041211(3 名):約 8.5s → 平均 2.8s(28 暗号ブロック)

H15 年度の投票受付処理性能は 59 暗号ブロックで 0.117s であり、大幅に遅くなっているように見える。

実験ログによる測定方法は、以下のようなパターン(関数毎と、それを呼び出す処理)で計測しているが、オーバヘッド部分がどうしても存在してしまう。

```
main() {
 性能測定開始();
   : ⇒ OverHead
 f1();
   : ⇒ OverHead
 f2();
   : ⇒ OverHead
```

```
  性能測定終了();
 }

 f1() {
  性能測定開始();
      :
  性能測定終了();
 }

 f2() {
  性能測定開始();
      :
  性能測定終了();
}
```

また、ログ情報をファイルに格納するなどのオーバヘッドも加算される。

実際の電子投票・アンケートは今回の自治体実験に近い処理となるため、実験測定結果を基に大規模選挙に対する検証をまとめで実施する。

### (ii) 集計性能

#### a) 山梨市実験結果

**表 59 母集団1集計処理平均時間**

| fanction | アンケートID | 投票者数 | 平均時間ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 15 | 4260 |

**表 60 母集団2集計処理平均時間**

| fanction | アンケートID | 投票者数 | 平均時間ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 21 | 5159 |

**表 61 母集団3集計処理平均時間**

| fanction | アンケートID | 投票者数 | 平均時間ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 20 | 4092 |

**表 62 母集団4集計処理平均時間**

| fanction | アンケートID | 投票者数 | 平均時間ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 16 | 5333 |

表 63 母集団 5 集計処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 15 | 4339 |

表 64 母集団 6 集計処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 16 | 4314 |

表 65 母集団 7 集計処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 301-317 | 35 | 8396 |

表 66 母集団 8 集計処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 401-417 | 26 | 6518 |

**b) 箕輪町実験結果**

表 67 集計処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 501-528 | 278 | 58621 |

**c) H15 年度測定結果**

1)1000 候補/100 万人投票者(59,000,000 暗号ブロック)

・トータル時間:3590000s

・1 暗号ブロックあたりの処理時間:0.061s

(測定環境:センタ 1 サーバの仕様)

- OS Windows2000Server SP4
- CPU PentiumⅢ 1GHz × 2
- メモリ 1179Mbyte

**d) 考察**

H15 年度測定結果に比べて大幅に処理時間が掛かっており、実験ログを基に検証する。

1)自治体実験集計要素数

自治体実験では、アンケート ID 単位での集計となるため、集計要素数は以下となる。

・1 アンケート ID あたりの暗号ブロック数:投票者数×1 暗号ブロック

(例)アンケート ID501

・278 暗号ブロック

2)机上計算

H15 年度測定結果の値を基に、自治体実験での集計時間を机上計算する。

・集計時間:1 暗号ブロックあたりの時間×1 アンケート ID あたりの暗号ブロック数

(例)アンケート ID501

・0.061s×278 暗号ブロック＝16.958s

3)集計処理手順

集計処理手順はおおよそ以下の流れとなっている。

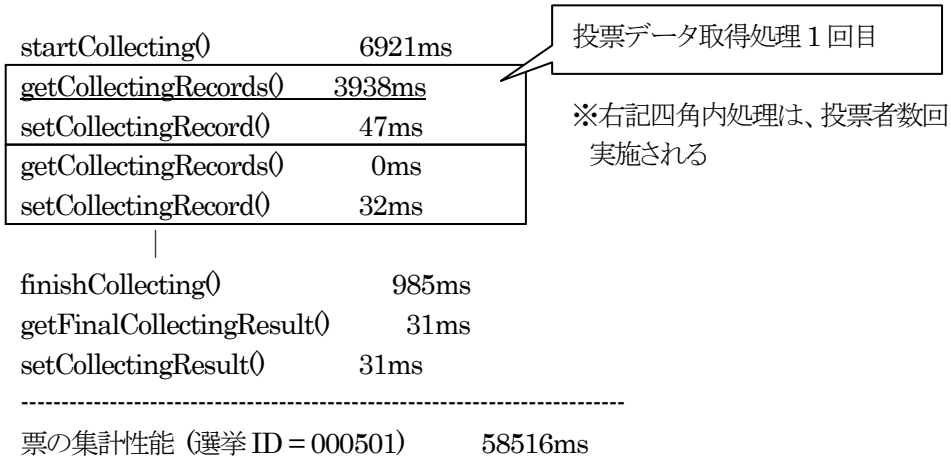
①step1:データベースから投票データ取得
②step2:集計処理
③step3:データベースに集計処理情報登録
③step4:投票者数分、step1～step3 を繰り返す
④step5:全投票者数の集計処理終了後、集計結果を登録する

実験ログでは、上記全処理の時間が採取されていないため、それぞれの処理時間は明確にはなっていない。また、(ｉ)投票受付処理時間の考察で記載したように、各処理にはオーバヘッドが存在するので、正確には各処理に対する処理時間を算出することは出来ないが、得られている情報を基に検証する。

4)各処理時間の概算

アンケート ID501 のログ情報は以下となっており、純粋な投票データ取得各処理時間の概算を算出する。

以下にログ情報の一部を抜粋する。




票の集計性能（選挙 ID＝000501） 58516ms

投票データ取得処理 1 回目のみ処理時間が掛かっているが、これはクラスをメモリにロードする時間が含まれていると予想される。

このログでは、集計処理時間そのものは表示されていない。但し、データベースからデータ取得・登録はおおよそ 30ms 程度となっているので、この値を基に集計処理を算出してみる。

・票の集計性能トータル時間:58516ms

---

・オーバヘッド:6921＋3938＋985＋31＋31＝11906ms
・データ取得:30×278＝8340ms
・データ登録:30×＝278＝8340ms
---
概算集計処理性能:29930ms

机上計算値に近い値とは言えないが、実際の電子投票・アンケートは今回の自治体実験に近い処理となるため、実験測定結果を基に大規模選挙に対する検証をまとめで実施する。

### (iii) 検証データ生成性能

#### a) 山梨市

表 68 母集団1検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 15 | 8013 |

表 69 母集団2検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 21 | 10476 |

表 70 母集団3検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 20 | 7962 |

表 71 母集団4検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 16 | 10955 |

表 72 母集団5検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 15 | 8561 |

表 73 母集団6検証データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 201-217 | 16 | 8544 |

表 74 母集団 7 検証データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 301-317 | 35 | 17983 |

表 75 母集団 8 検証データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 401-417 | 26 | 13521 |

**b) 箕輪町**

表 76 検証データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 票の集計性能 | 501-528 | 278 | 144587 |

**c) H15 年度測定結果**

1)検証データ生成処理時間

本処理時間は、関数単体の処理時間の測定値となり、1000 候補/100 万人投票者(59,000,000 暗号ブロック)分の性能測定は実施していない。

・Proof3 検証用データ(c,r)生成時間:576ms

(測定環境 : センタ 1 サーバの仕様)

- OS WindowsNT4.0 ServicePack6.0a
- CPU PentiumⅢ 733MHz
- メモリ 128MB

**d) 考察**

H15 年度測定結果と比べて若干早い結果となっている。集計処理性能と逆の結果となっており、実験ログを基に検証する。

1)自治体実験集計要素数

自治体実験では、アンケート ID 単位での集計となるため、集計要素数は以下となる。

・1 アンケート ID あたりの暗号ブロック数:投票者数×1 暗号ブロック

(例)アンケート ID501

・278 暗号ブロック

2)机上計算

H15 年度測定結果の値を基に、自治体実験での検証データ生成時間を机上計算する。

・検証データ生成時間:1 回あたりの時間×1 アンケート ID あたりの暗号ブロック数-1

(例)アンケート ID503

・0.576s×277=159.552s

3)検証データ生成処理手順

集計処理手順はおおよそ以下の流れとなっている。

①step1:データベースから検証データ作成用データ取得
②step2:検証データ生成処理
③step3:検証データ生成情報を登録
③step4:投票者数分、step1 と step2 を繰り返す

実験ログでは、上記全処理の時間が採取されていないため、それぞれの処理時間は明確にはなっていない。また、(ｉ)投票受付処理時間の考察で記載したように、各処理にはオーバヘッドが存在するので、正確には各処理に対する処理時間を算出することは出来ないが、得られている情報を基に検証する。

4)各処理時間の概算

アンケート ID503 のログ情報は以下となっており、純粋な投票データ取得各処理時間の概算を算出する。

以下にログ情報の一部を抜粋する。

```
getCommitmentRecords()          8844ms
getCommitmentForCollecting()    31ms
setVerifyRecord()               109ms
getCommitmentRecords()          0ms
getCommitmentForCollecting()    15ms
setVerifyRecord()               47ms
getCommitmentRecords()          0ms
getCommitmentForCollecting()    31ms
                |
setVerifyRecord()               47ms
getCommitmentRecords()          0ms
setVerifyData()                 31ms
---------------------------------------------------------------------------
検証データ生成性能（選挙 ID＝000501）      143047ms
```

コミットメントデータ取得
処理１回目

※右記四角内処理は、投票者数-1 回
実施される

投票データ取得処理 1 回目のみ処理時間が掛かっているが、これはクラスをメモリにロードする時間が含まれていると予想される。

このログでは、検証データ生成処理時間そのものは表示されていない。但し、データベースからのデータ取得・登録はおおよそ 30ms 程度となっているので、この値を基に処理を算出してみる。

・票の集計性能トータル時間:143047ms

---

・オーバヘッド:8844ms
・データ取得:30×2×278＝16680ms
・データ登録:30×＝278＝8340ms

---

概算集計処理性能:109183ms

机上計算値よりも大幅に改善されており、測定環境(サーバ性能)の違いが現れてきていると考えられる。

実際の電子投票・アンケートは今回の自治体実験に近い処理となるため、実験測定結果を基に大規模選挙に対する検証をまとめで実施する。

### 3-8-3-4 センタ 2 性能

センタ 2 性能に関しては、検証処理と開票処理に分けられる。これらの処理時間に関しては、実験実施時にセンタ 2 で各処理に対するログを採取し、処理時間を計測した。

この値を元に、H15 年度実装時の評価結果と比較し、改善が必要であるか検証する。

(性能測定環境)

[センタ 2 サーバの仕様]

- コンピュータ　ノート PC　VersaPro VY30Y/AG
- OS　WindowsXP
- CPU　PentiumⅣ　3GHz
- メモリ　256Mbyte
- USB ポート
- CD-ROM ドライブ
- ネットワーク環境

[センタ 2 サーバのアプリケーション]

- j2re-1_3_1_09

#### (i) 検証処理時間

#### a) 山梨市

表 77 母集団1Proof2 検証処理時間

| fanction | アンケート ID | 投票者数 | 時間 ms |
|---|---|---|---|
| Proof2 検証性能 | 201 | 15 | 438 |

表 78 母集団1Proof3 検証処理時間

| fanction | アンケート ID | 投票者数 | 時間 ms |
|---|---|---|---|
| Proof3 検証性能 | 201 | 15 | 1000 |

表 79 母集団1開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 15 | 59 |

表 80 母集団1復号検証用データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 15 | 9 |

表 81 母集団1復号正当性証明用データ生成処理時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201 | 15 | 391 |

表 82 母集団1復号検証処理時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201 | 15 | 328 |

表 83 母集団 2 開票処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 21 | 43 |

表 84 母集団 2 復号検証用データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 21 | 22 |

表 85 母集団 3 開票処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 20 | 43 |

表 86 母集団 3 復号検証用データ生成処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 20 | 23 |

表 87 母集団 4 開票処理平均時間

| fanction | アンケートID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 16 | 22 |

表 88 母集団 4 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 16 | 61 |

表 89 母集団 5 開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 15 | 48 |

表 90 母集団 5 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 15 | 9 |

表 91 母集団 6 開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 16 | 21 |

表 92 母集団 6 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 201-217 | 16 | 47 |

表 93 母集団 7 開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 301-317 | 35 | 46 |

表 94 母集団 7 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 301-317 | 35 | 6 |

表 95 母集団 8 開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 401-417 | 26 | 52 |

表 96 母集団 8 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 401-417 | 26 | 8 |

**b) 箕輪町**

表 97 Proof2 検証処理平均時間

| fanction | アンケート ID | 投票者数 | 時間 ms |
|---|---|---|---|
| Proof2 検証性能 | 501-528 | 278 | 89 |

表 98 Proof3 検証処理平均時間

| fanction | アンケート ID | 投票者数 | 時間 ms |
|---|---|---|---|
| Proof3 検証性能 | 501-528 | 278 | 38623 |

表 99 開票処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 開票性能 | 501-528 | 278 | 85 |

表 100 復号検証用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 復号検証用データ生成性能 | 501-528 | 278 | 59 |

表 101 復号正当性証明用データ生成処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 復号正当性証明データ生成性能 | 501-528 | 278 | 729 |

表 102 復号検証処理平均時間

| fanction | アンケート ID | 投票者数 | 平均時間 ms |
|---|---|---|---|
| 復号検証性能 | 501-528 | 278 | 77 |

**c) H15 年度測定結果**

1)各処理別性能測定データ

本処理時間は、関数単体の処理時間の測定値となる。

表 103 センタ 2 処理性能

| fanction | 時間(msec) |
|---|---|
| 復号性能 | 14 |
| Proof2 検証性能 | 144 |
| Proof3 検証性能 | 383 |
| 復号検証用データ生成性能 | 1919 |
| 復号正当性検証性能 | 9 |

（測定環境：センタ 1 サーバの仕様）

- OS　WindowsNT4.0　ServicePack6.0a
- CPU　PentiumⅢ　733MHz
- メモリ　128MB

**d) 考察**

5 種類の処理性能に関して、ログからの測定結果と H15 年度測定結果を比較する。実験データはアンケート ID501-528 の平均データを採用する。

1)机上計算

H15 年度測定結果の値を基に、自治体実験に当てはめた場合の机上計算する。

**①開票性能**

本処理時間は、集計された暗号ブロック単位の値となるため、実験データに換算すると以下となる。

・1 アンケート ID：14ms

**②Proof2 検証性能**

本処理時間は、集計された暗号ブロック単位の値となるため、実験データに換算すると以下となる。

・1 アンケート ID：144ms

**③Proof3 検証性能**

本処理時間は、センタ 1 で生成した各検証用データに発生するため、実験データに換算すると以下となる。

・検証データ生成数：1 アンケート ID あたりの暗号ブロック数-1
・Proof3 検証性能：0.383s×277＝106091ms

**④復号検証用データ生成性能**

本処理時間は、集計された暗号ブロック単位の値となるため、実験データに換算すると以下となる。

・1 アンケート ID：1919ms

**⑤復号正当性検証性能**

本処理時間は、集計された暗号ブロック単位の値となるため、実験データに換算すると以下となる。

・1 アンケート ID：9ms

2)比較

ログからの測定結果と H15 年度測定結果を比較する。処理時間の掛かる処理は、実験データの方が性能が良い結果となっており、測定環境（サーバ性能）の違いによるものと判断できる。机上計算の方が上回っている処理に関しては、オーバーヘッド部分が効いていると思われる。

**表 104 比較表**

| fanction | 実験データ | 机上計算値 |
|---|---|---|
| 開票性能 | 85ms | 14ms |
| Proof2 検証性能 | 89ms | 144ms |
| Proof3 検証性能 | 38623ms | 106091ms |
| 復号検証用データ生成性能 | 788ms | 1919ms |
| 復号正当性検証性能 | 77ms | 9ms |

### 3-8-3-5 まとめ

実際の電子投票・アンケートは今回の自治体実験に近い処理となる。センタ 2 性能以外の結果は、H15 年度測定結果より悪くなっているため、実験測定結果を基に大規模選挙に当てはめ検証する。

**(i) 投票性能**

大規模選挙（候補者 1000 人，投票者 100 万人）に想定した対策後の性能含め比較表を作成し、考察する。

**表 105 比較表**

| | 実験データ | 机上計算値 | 対策後計算値 |
|---|---|---|---|
| 山梨市<br>（17 暗号ブロック） | 約 1min30s | 11.3s | 27.9s |
| 箕輪町<br>（28 暗号ブロック） | 約 2min30s<br>（実測 126.2s） | 18.6s | 43.8s |
| 大規模選挙<br>（59 暗号ブロック） | | 39.2s | 88.8s |

この対策を施した場合の大規模選挙計算値は、約 88.8s となり、H15 年度の目標値最大 1 分を越えてしまう。問題となるのは、下記処理であり H15 年度評価時と比べて約 2 倍の数値となっており、事業化に向けては、この処理時間短縮が課題となる。

①H15 年度評価時暗号処理時間　0.665s
②対策後暗号処理時間　1.36s

※暗号処理時間：暗号処理＋コミットメントデータ生成＋電子署名データ生成

**(ii) センタ 1 性能**

大規模選挙（候補者 1000 人，投票者 100 万人）に想定した性能を計算し、考察する。

**a) 票受付性能**

実験データは、以下となる。

・投票者一人あたりの票受付時間：2.8s（28 暗号ブロック）

従って、大規模選挙に当てはめた場合は、以下となる。

・0.1s × 59 ブロック × 100 万人 ＝ 約 68.3 日

以上の結果から、サーバの性能向上や、サーバシステムを分散化することは必須であり、同時アクセス数増加した場合の応答の遅れなどは、投票者の負担増加や不信感をもたれる可能性もあるため、十分考慮してシステム構築する必要がある。

**b) 集計性能**

実験データは、以下となる。

・278 暗号ブロックあたりの集計処理時間：58516ms

この値をそのまま、大規模選挙に当てはめることは出来ない。暗号ブロック数が増加した場合のオーバヘッドは推定できないため、簡易的に実験で求められたオーバヘッド時間を上記値から削除した値を用いる。

・278 暗号ブロックあたりの集計処理時間：46610ms（オーバヘッド時間除く）

従って、大規模選挙に当てはめた場合は、以下となる。

・0.168s × 59 ブロック × 100 万人 ＝ 約 114.7 日

以上の結果から、サーバの性能向上や、サーバシステムを分散化することは必須である。

**c) 検証データ生成性能**

実験データは、以下となる。

・278 暗号ブロックあたりの検証データ生成処理時間：143047ms

この値をそのまま、大規模選挙に当てはめることは出来ない。暗号ブロック数が増加した場合のオーバヘッドは推定できないため、簡易的に実験で求められたオーバヘッド時間を上記値から削除した値を用いる。

・278 暗号ブロックあたりの検証データ生成処理時間：134203ms（オーバヘッド時間除く）

従って、大規模選挙に当てはめた場合は、以下となる。

・0.483s × 59 ブロック × 100 万人 ＝ 約 329.8 日

以上の結果から、サーバの性能向上や、サーバシステムを分散化することは必須である。

## 3-8-4 意識調査アンケート検証

### 3-8-4-1 目的

自治体実験では、実際に投票に参加していただいた投票者の方々から、有用性、安全性、利便性等に関する感想を頂いた。この意識調査アンケートの結果を検証し、今後の課題とする。

ここでは、操作性，運用性などの改善点を検証し、有用性・利便性に対する意見を抽出した。具体的な内容については別冊を参照されたい。安全性についてはサブテーマ4「セキュリティポリシー」で、性能面に関しては本サブテーマの 3-8-3 性能検証」にて記載する。

## 3-8-5 まとめ

各章にて、得られた改善点に関して整理し、今後の課題や提案をまとめる。

### 3-8-5-1 電子アンケート利用に関して

今回開発した電子投票・アンケートシステムは、大規模選挙を想定した仕様が中心となっており、電子アンケートとしてのユーザビリティ，集計の自由度などに若干配慮の欠けたものとなっていると言える。

本サブテーマ 1-1-4「意識調査アンケート検証」のまとめで記載しているが、以下を今後の課題として挙げる。

**(i) 自由記述の対応**

アンケートの設問に対して設定されている回答では、投票者の意思表示が出来ない場合があり、この様なケースに対応できる仕組みを検討する必要がある。

対応する最良の方法としては、以下の回答を用意するが考えられる。

●回答：その他（自由記述）

また、設定されている回答を選択しても、選択した理由を求めたい場合がある。このケースも自由記述が必要となり、自由記述の対応は本システムの課題として挙げられる。

自由記述に対応するためには、以下の検討が必要となる。

①設問・回答アドレスの付加

どの設問・回答に対する自由記述なのか判断できるためのアドレスヘッダを自由記述に付加する。

②自由記述の改竄・秘匿

自由記述も投票者の個人情報となるため、自由記述データの改竄検出や秘匿をおこなうための仕組みが必要となる。

③投票者との関連付け排除

集計できるデータは、準同型性を利用した暗号系によって投票者との関連付けを排除できるが、自由記述データではこの仕組みを利用できない。このため、他方式などを利用して投票者と自由記述の関連付けを排除する。

尚、自由に付加できる選択肢を複数用意して、投票者に意味づけをしてもらう事も考えられなくはないが、選択肢が増えることによる集計・開票性能への影響が心配される。この方策の実現性も検討の余地があるのではと思われる。

**(ii) 集計の自由度に関して**

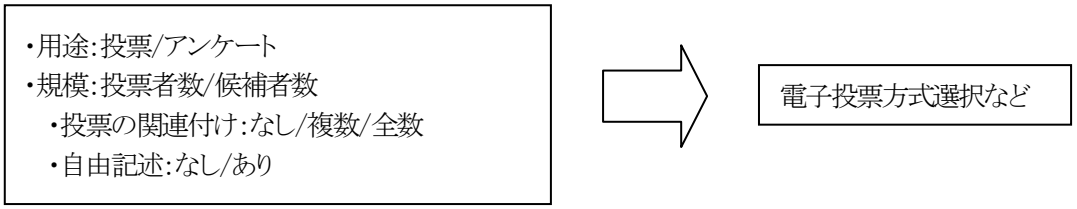
アンケート情報を活用する側としては、他回答との関連付けをした集計情報が必要となる。この様なケースに対応できる仕組みを検討する必要がある。

現在の電子投票・アンケートシステムで対応する場合は、各設問や回答を関連付けるための情報を平分に組み込むことで、対応可能である。この関連情報は、最大設問・回答数の組み合わせだけになると考えられるため、暗号ブロック数が極端に増え、投票受付や集計に多大なる負荷を与えることになり、本システムのメリットが薄れてしまう可能性がある。

a)自由記述の対応と同じく、集計の自由度が容易に確保できる他方式を利用することも解決策のひとつである。

a)，b)の課題を考えた場合、電子投票・アンケート主催者による実施条件入力により、入力条件にあったシステムの自動構築などが出来るモデルとすることは、事業化の意味では有益となるかもしれない。

例えば、下記のような入力などが考えられる。




**(iii) 投票アプレット生成仕様**

アンケートを実施する場合には、設問・回答が長文となったり、設問に対する説明文を入れたりするケースがある。また、画面デザインにより、操作に時間が掛かったり、間違った操作の元になる。このため、投票画面をデザインするための xml 仕様を改善する必要がある。

**3-8-5-2 投票実施形態に関して**

今回開発した電子投票・アンケートシステムは、家庭で投票出来ることを目的として研究・開発したが、不特定多数の投票者全てに投票操作などが受け入れられない可能性があることが判った。

**(i) 複数の投票場所を設定**

不特定多数の投票者が対象となるような投票・アンケートの場合、さまざまな理由により家庭からネットワークを介して投票することが出来ないケースがある。この様なケースに対応できる仕組みを検討する必要がある。

箕輪町実験で実際に体験したように、投票者の状況に合わせ投票実施形態を複数用意する方法が考えられる。

・家庭から投票
・指定場所で投票

家庭から投票する場合、投票期間に自由度を設けやすいので、仮に投票できなかった場合でも指定日に指定場所で投票するリカバリーが可能である。また、指定場所で投票する場合、専用端末を用意することも可能であり、操作性の改善にも繋がる。

**(ii) 現行システムとの併用**

現行システムとの併用も考えられるが、電子投票・アンケートの利便性が半減したり、システムコスト・運用コストが増加するなど主催者側の利点は見出せ難いが、不特定多数の投票者全てに対応することを想定すれば、検討に値するのではと思われる。

例えば、選挙案内はがきに該当選挙用投票者個別シリアル番号(セキュリティシールで保護)などを付加しておき、投票所では選挙案内はがき＋身分証明書で投票用紙に交換・投票する。家庭からは該当選挙用投票者個別シリアル番号＋IC カード＋投票者認識情報で電子投票するなどが考えられる。

### 3-8-5-3 操作性に関して

本サブテーマ 1-1-4「意識調査アンケート検証」のまとめで記載しているが、以下を今後の課題として挙げる。

**(i) 手順の簡略化**

参加企業実験を通じてかなり改善はされたと認識していたが、投票アプリケーションなどのインストール作業や投票までの操作は、もっと簡略化しないと PC 操作に不慣れな投票者にとって負担が大きくなる。負担が大きくなれば、電子投票・アンケートに参加する割合も減ってくることが予想される。

**(ii) 手順のガイダンス機能**

参加企業実験を通じて、インストールマニュアル・操作マニュアルはかなり改善したが、PC 操作に不慣れな投票者には、音声ガイダンスや映像などによる手順の説明方法も可能性として認識する必要がある。また、マニュアルにない状況に対応するためのヘルプディスクの整備も必須である。

**(iii) マウスフォイール機能**

選択式の本システムでは、殆どの操作がマウスのみで実行可能であるため、操作性が良いとの意見を頂いている。但し、設問・回答が１投票画面で入りきらない場合、横方向に関しては文章を改行することで対応可能であるが、上下方向のスクロールは、マウスフォイールが使用できないためかなり不便であり、使用出来るように改善する必要がある。

### 3-8-5-4 性能に関する課題

本サブテーマ 1-1-3「性能検証」のまとめで記載しているが、以下を今後の課題として挙げる。

**(i) IC カード処理性能調査と改善**

今回調査し、提案した対策を施したとしても、大規模選挙（候補者 1000 人，投票者 100 万人）に想定した目標値はクリアできない。処理性能としては以下となり、この違いを調査するとともに改善策を施す必要がある。

①H15 年度評価時暗号処理時間　0.665s
②対策後暗号処理時間　1.36s

※暗号処理時間：暗号処理＋コミットメントデータ生成＋電子署名データ生成

**(ii) センタ 1 性能**

検証結果では、サーバの性能向上や、サーバシステムを分散化することは必須と結論付けた。また、票受付性能には SSL 処理性能が加味されていない数値での検証である。従って、以下調査・検証する必要がある。

・SSL 処理性能調査
・大規模選挙を想定した場合のサーバ構成

### 3-8-5-5 ユーザ教育に関する課題

山梨市での情報リテラシー授業や箕輪町での公民館操作サポートを通じて、投票者に対する情報セキュリティ・安全面の啓蒙の必要性，投票操作説明や訓練の必要性を痛感した。

以下に、「電子アンケートの正しい操作や手順についての説明や訓練は必要か」の問いに対する回答結果を記載する。インストール作業のなかった山梨市でも、説明または訓練が必要と回答した割合は 90%以上となっており、ユーザ教育の計画など十分配慮して検討すべきであろう。

**表 106 山梨市 設問 4-3 投票結果（全体）**

| 説明・訓練とも必要だと思う。 | 説明は必要と思う。 | 訓練は必要と思う。 | 必要と思わない。 |
|---|---|---|---|
| 54 | 77 | 2 | 6 |

**表 107 箕輪町 設問 4-3 投票結果（全体）**

| 説明・訓練とも必要だと思う。 | 説明は必要と思う。 | 訓練は必要と思う。 | 必要と思わない。 |
|---|---|---|---|
| 85 | 90 | 12 | 9 |

# 3-9　準同型公開鍵暗号方式

## 3-9-1　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。

## 3-9-2　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 60 に示す．

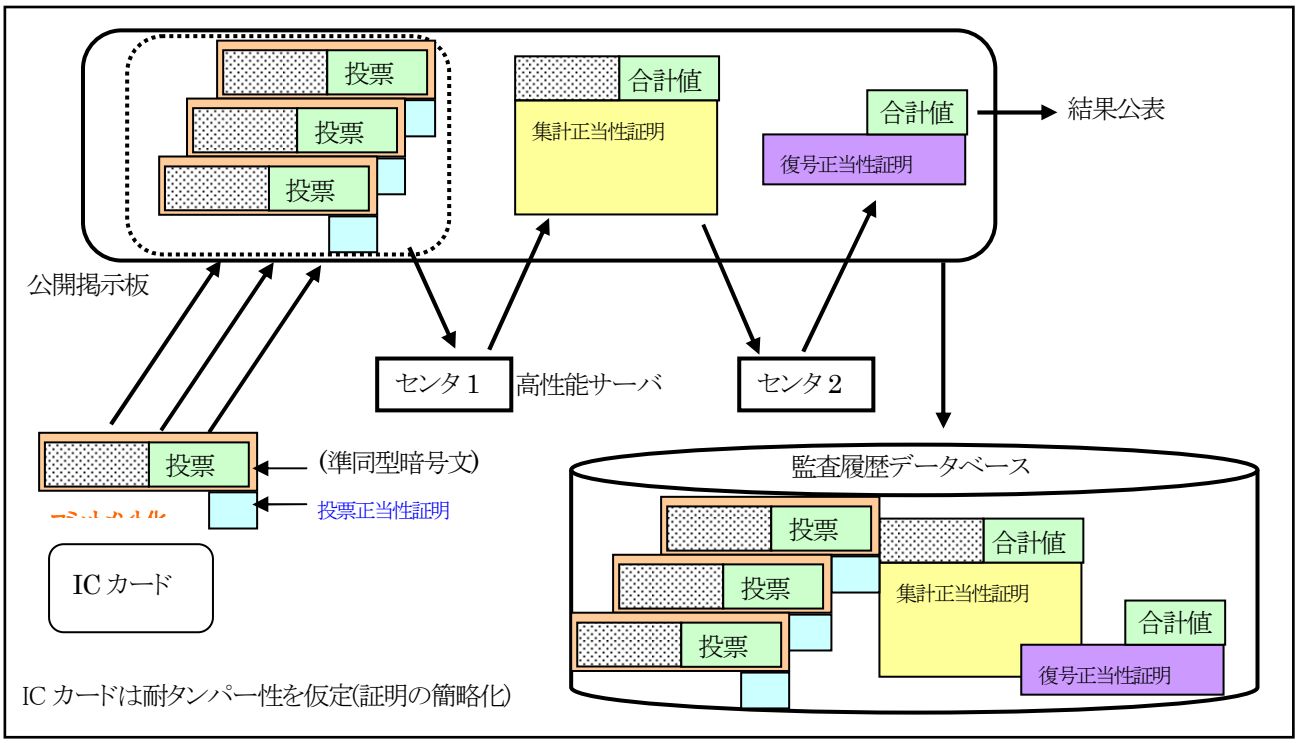



**図 60　投票プロセスにおける処理とデータの流れ**

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 1 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 108** に示す．

**表 108** 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 1 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．OU 関数と閾値法を利用する枠組み(CGS97 や Paillier 暗号を用いる方式と同様な枠組み)を組み合わせることは困難であるが，OU 関数と TYKK 方式を組み合わせるという新しい枠組みにより，高性能・高安全性を有する電子投票方式を実現できる．

## 3-9-3 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2-1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。

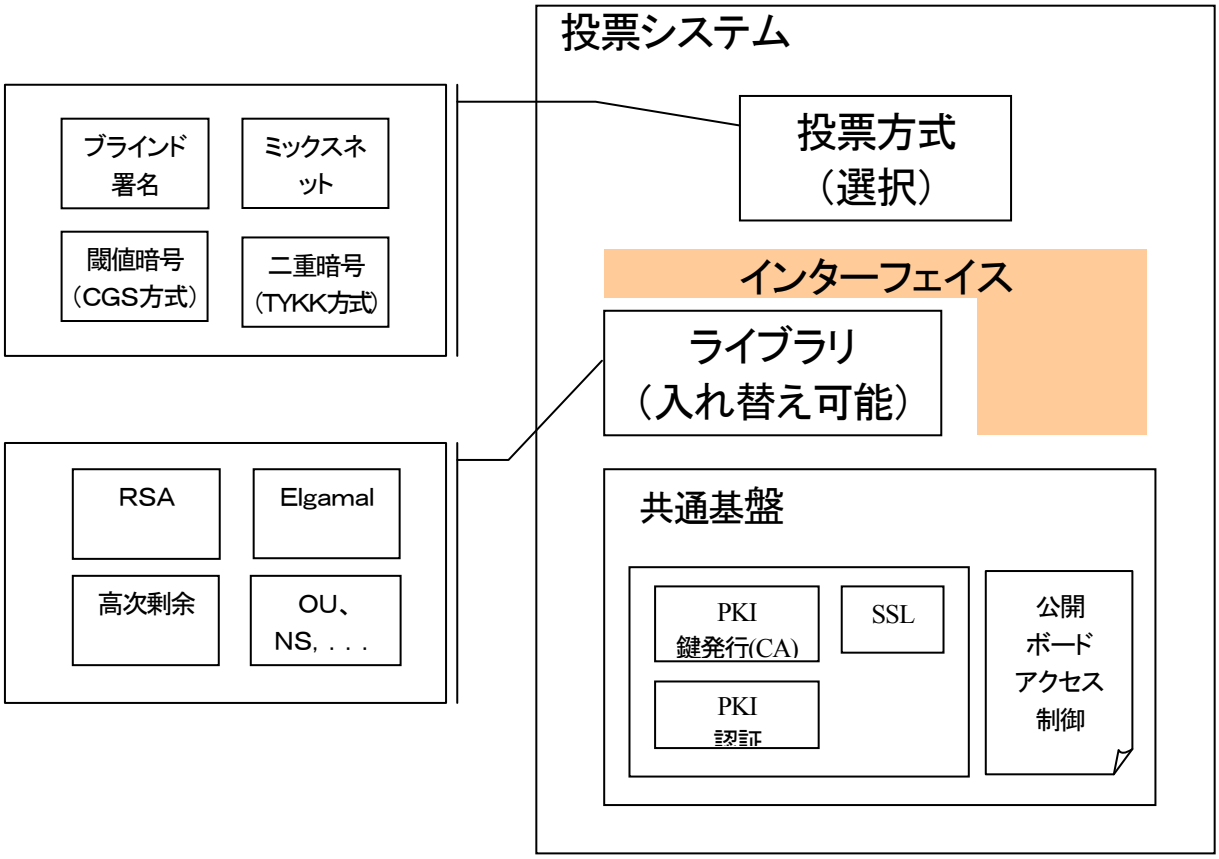



**図 61　投票プロトコルと実装の関係**

## 3-9-4 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。

# 3-10 投票プロセスの正当性証明とその効率化

## 3-10-1 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、理論的に検証した。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を条件とした。

## 3-10-2 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” [109] 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 62 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.

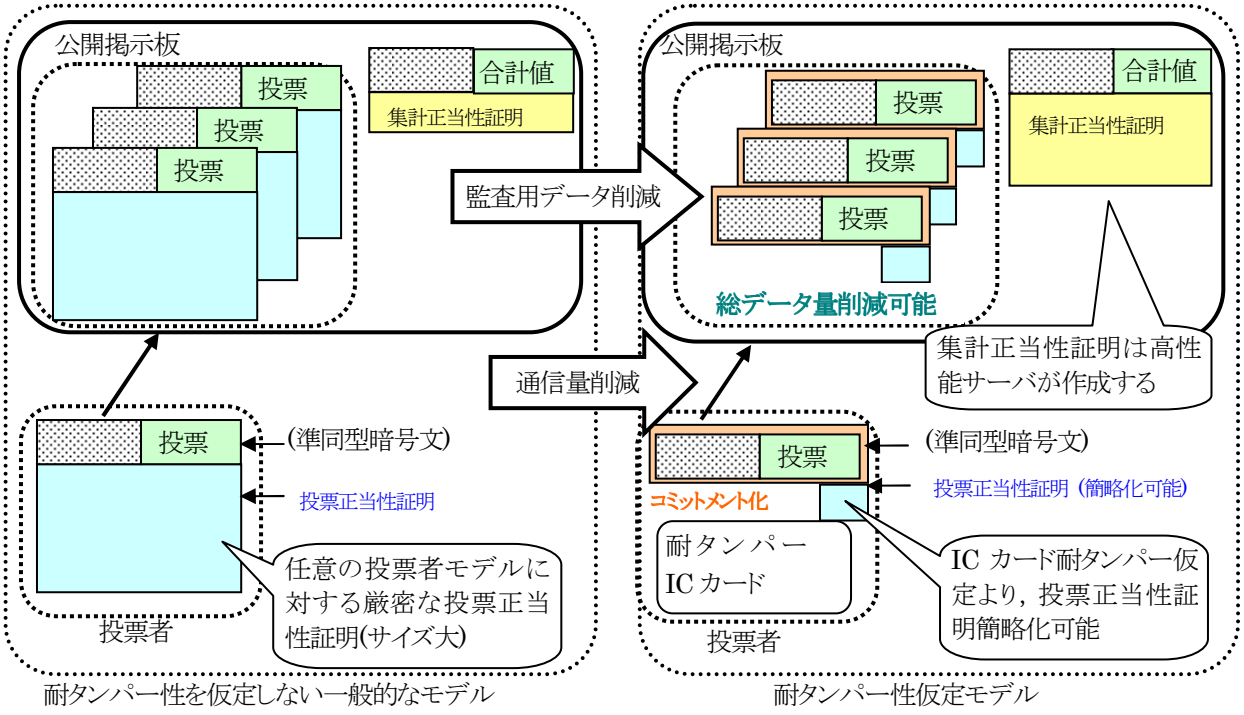



**図 62** 安全性証明に関するモデルの比較

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 109 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 109** 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 109 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。

## 3-10-3 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]、[Oka97]、[HS00][110]、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、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) 提案方式の実現**

**TYKK方式を一部変更し、レシートフリー機能を追加した。主な機能を以下に示す。**

- 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(賛成票、反対票).
- 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し，投票者はこれを通して公開された票の中身を知る.
- 秘密通信路を通して得た情報から投票者は自分の投票したい方を選び，自ら乱数を生成して，票を再暗号化して投票する.
- 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.

投票者に秘密情報を持たせることで，買収・脅迫者に対し偽りの証明が可能となる．これを利用することで，投票者がセンター2 から得た情報には証拠能力が無いとすることができる.

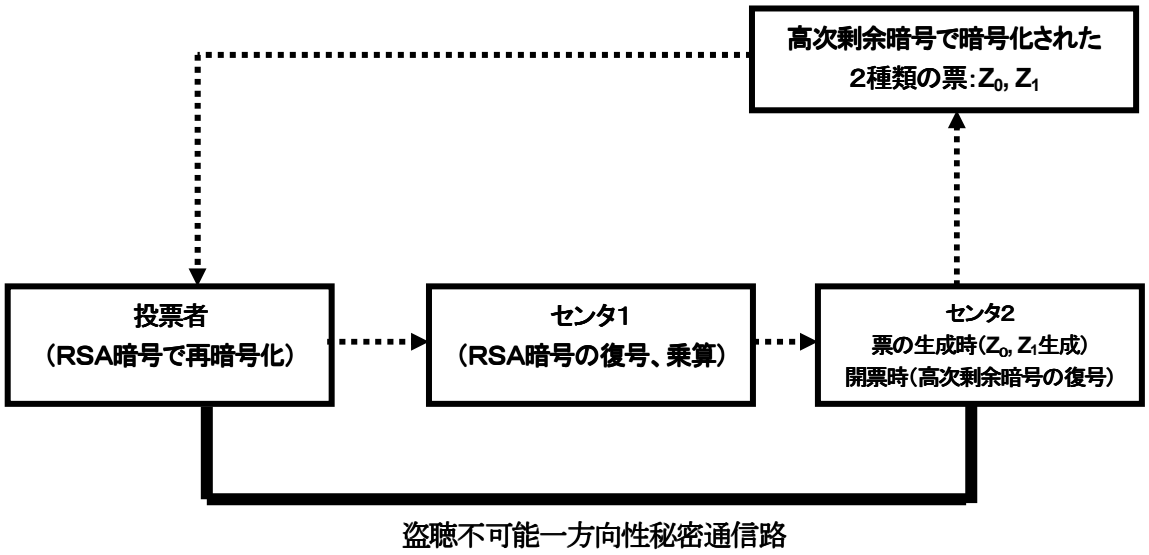



**図 63　TYKKプロトコルにおける レシートフリー方式**

### (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 が投票内容;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表示する.

$Z_0 \equiv y^0 x_0^r \bmod N_2$ , $Z_1 \equiv y^1 x_1^r \bmod N_2$ $(x_0, x_1 \in_R Z_{N_2})$

$Z_0$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. (**特定検証者用暗号化の正当性証明;**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. (**再暗号化の正当性証明;**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.

第5 章において,「投票者が乱数を生成したのではレシートフリーにならない」と述べた. この乱数$x_{v_i}$ はレシート(証拠)となるかが問題となる.

買収・脅迫者に対し，投票者$v_i$ が乱数$x_{v_i}$ $i$ をレシートとして提示したとする. 買収・脅迫者は投票者が$Z_0$もしくは$Z_1$ のどちらか一方を投票したことは確認できるが$Z_0$ および$Z_1$ の中身までは分からないので0 と1 のどちらを投票したかまでは確認できない. つまり，この乱数だけではレシートにはならない.

あとは, Step3. における証明がレシートとなる可能性があるが，この証明はHS2000 と同じように，投票者が第3 者に対して証明する場合には2 通りの証明ができる. (「ごまかし」が可能である)
(詳細は「電子投票:2003 年度に発表された TYKK 方式の Recipt-free の実現」参照)).

(iii)正当性証明

レシートフリー機能における各種処理の正当性証明を可能にした。

(a)票の正当性証明 (STEP2 の証明)

センター2 が票内容が0である票と、票内容が 1 である票を、それぞれ高次剰余暗号で暗号化する。, その二つの暗号化された値 $Z_0, Z_1$を公開掲示板に表示する。 センター2 は投票内容が 0 あるいは 1 であることを、そのどちらかの値であることは知られること無く、証明する。

証明プロトコルは　Benaloh [Ben86] が提案したゼロ知識証明法 “暗号カプセル”手法を適用する。また、ゼロ知識証明法において必要とされる健全性、ゼロ知識性の証明も行っている。

(b) 特定検証者用暗号化正当証明 (Designated verifier encryption proof ：STEP3)

センター2 は$Z_0$が投票内容:0 を,$Z_1$が投票内容:1 を暗号化したものであること

($Z_0 \equiv y^0 x_0^r \bmod N_2$ , $Z_1 \equiv y^1 x_1^r \bmod N_2$　)を秘密通信路を用いて特定の投票者に伝える. その際, 証明も付加する. (Designated verifier encryption proof)

センター2 が証明者となり, 特定投票者が検証者となる.

投票者は買収者・脅迫者に対して本当の証明とごまかしの証明の2 通りの証明が可能となる.

買収者・脅迫者にとっては, 投票者が正直に証明しているのか, それとも偽りの証明をしているのか区別がつかない.

したがって, Designated Verifier encryption Proof から得られる情報には証拠能力がないといえる. よって, レシートフリーを満たしているといえる.

このDesignated Verifier encryption Proof はHS2000 で提案されたCGS97 方式の Designated Verifier Re-encryption Proof を参考にしてTYKK2003 方式に考案したものである. 以下にこの考案したDesignated Verifier encryption Proof が健全性とゼロ知識性を満たすことも証明している。

(c).再暗号化の正当性証明( Re-encryption proof)

投票者は自分の投票したい値を$Z_0$ または$Z_1$ から選び, 乱数$x_{v_i}$ を用いて再暗号化し, それをRSA 暗号で暗号化してから投票する. ここで, $Z_0$ または$Z_1$ を選び乱数$x_{v_i}$ を用いて正しく再暗号化していることを証明する. つまり,

$Z_i \equiv Z_0 (x_{v_i})^r \bmod N_2$ or $Z_i \equiv Z_1 (x_{v_i})^r \bmod N_2$

であることを証明する. 投票者が証明者(prover)となりセンター1 が検証者(verifier)となり、健全性とゼロ知識性を満たすことも証明している。

ただ、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。

## 3-10-4 まとめ

投票対象を１つ(0 または１を投票)に限定し, 準同型暗号を利用する投票方式に対して, 投票の正当性証明, 集計の正当性証明, 復号の正当性証明に分けて証明生成コスト, 検証コストを評価した.

従来の TYKK 方式の証明(投票, 集計, 開票)では, 対話証明を用いていた. これに対し, 本研究で提案する改良 TYKK 方式では, 集計の正当性証明は非対話化を実現し, 効率向上を達成した. また, TYKK 方

式の証明(投票, 集計, 開票)については, 投票者数に比例する証明方法を得ることができた. 従って, 理論的には現実的な方法とみなすことができる. しかし, 閾値法を利用する方式(CGS97)では集計の証明は不要である. このため, 証明生成と検証を含めたトータルの処理性能は, 改良 TYKK 方式よりも閾値法を利用する方式のほうが優れている.

さて, 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.

## 3-10-5 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.

## 3-11 総括

2年半におよぶ研究開発期間において、9つのサブテーマに対して行った研究開発で、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

- 現行法と特例法の対応と実施された選挙における問題点が明確になった。
- 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。
- 平成15年度会社法改正による株主総会議決電子投票制度創設後の議決と、公職電子投票との制度上の差異と問題点の指摘が完了した。
- 現行特例法制定過程(国会審議)の評価を付す事ができた。
- 電磁的方法による議決権行使および決議を可能とした法制度と分野が明らかになった。
- 株主総会における電磁的方法による議決権行使の現状と利用可能性を示せた。

サブテーマ2:運用形態ごとの要件整理

- NVSS および関連文献の調査を推進し、これを元に日本の投票制度や第1世代電子投票の実績を加味した上で、「電子投票機能要件」をまとめ上げた。
- 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。
- H14年度およびH15年度にまとめた「電子投票機能要件」において、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った。

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。
- 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、必要な対策を検討できた。
- 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整理できた。

サブテーマ4:セキュリティポリシー

- 電子投票システムに要求される「投票の特性」に対してどの様なセキュリティ機能要件が必要か、に関してISO15408の視点でまとめた。
- 次世代電子投票・アンケートシステムにおけるセンター等で想定される情報セキュリティ管理策をまとめた。

・ 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
・ PC上の投票用アプリケーション、各サーバ(センタ1、センタ2)のアプリケーション、電子認証局の基本設計を完了した。
・ データベースのテーブル定義、候補者メタデータ定義を完了した。
・ 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。
・ サーバ用高次剰余暗号関数(鍵生成、復号、集計機能)の実装および性能評価を実施した。
・ サーバ用0U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、要求仕様(投票規模、投票対象、安全性の仮定)毎のコストを明らかにした.
・ ICカード用0U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。
・ 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
・ 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した。
・ 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し, 一定の成果を得た。
・ 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] 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
[12] 「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
[13] 「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
[14] 「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
[15] 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
[16] 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
[17] 疫学研究に関する倫理指針(2002)
http://www.niph.go.jp/wadai/ekigakurinri/index.htm
[18] 「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
[19] 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
[20] 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
[21] 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)
[22] 東尾正・石川善朗『公職選挙法』ぎょうせい(1992)
[23] 野中俊彦『選挙法の研究』信山社(2001)
[24] 東浩紀(2003)「情報自由論」(中央公論 4 月号)
[25] 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)
[26] 岩村・神田編『電子株主総会の研究』弘文堂(2003)
[27] あさひ法律事務所他『株主総会 IT 化の法務と実務』中央経済社(2002)

[28] 選挙制度研究会編『わかりやすい公職選挙法』ぎょうせい(2001)
[29]「レポート　前年比 2．3 倍の 161 社が利用　動画配信には抵抗感も　株主議決権のネット投票が急伸」日経インターネットソリューション(2003.8)
[30]「株主総会の投票がケータイで可能に　14社が採用」(2004/6/20　朝日ニュース)
[31] 株主総会白書　2004 年版　商事法務　1715 号(2004 年)
[32] 株主総会白書　2003 年版　商事法務　1681 号(2003 年)
[33] 株主総会白書　2004 年版　商事法務　1640 号(2002 年)
[34]「株式市場のグローバル化と株主対応の留意点」関　孝哉　商事法務　1625 号(2002 年)
[35]「株主総会の IT 化」弥永真生　ジュリスト　No.1271(2004)
[36] 株式持ち合い状況調査　2003 年度版　ニッセイ基礎研究所(2004)
[37] 議決権行使方針に関する機関投資家アンケート調査結果(2004 年 6 月 23 日)
http://www.ufji.co.jp/publication/report/press/040623.pdf
[38] 厚生年金基金連合会 株主議決権行使基準 平成 15 年 2 月 20 日策定, 厚生年金基金連合会 http://www.pfa.or.jp/jigyou/pdf/gov_01.pdf
[39] 株主議決権行使に関するインフラ整備に向けた取組みについて　平成17年2月14日
（東京証券取引所・大阪証券取引所・ジャスダック証券取引所 にあて、社団法人 日本証券投資顧問業協会、厚生年金基金連合会 連名）
[40] TIAA-CREF、年金基金の議決権行使内容開示に反対
http://www.e-associates.co.jp/jp/magazine/backnumber/irgovernancenews011.htm
[41] 中国で遺伝子治療薬承認、世界初　p53腺ウイルス注射液　(中国通信社)
http://www.china-news.co.jp/culture/2003/10/cul03102501.htm
[42] イー・マーキュリー　プレスリリース「イー・マーキュリーの SNS『mixi（ミクシィ）』、ユーザ数が 30 万人を突破」 http://www.emercury.co.jp/press/050121.html
[43] コミュニケーションサイト「meetme.jp」が 3 月末でサービス終了
http://internet.watch.impress.co.jp/cda/news/2005/01/31/6283.html
[44] グローバル・フレックス・プランニング　プレスリリース
ビジネス向けのソーシャルネットワークとして「biji」が 2004 年 11 月 1 日オープン
http://www.gfplan.co.jp/press20041012.html
[45] 個人情報の保護に係る関係省庁の検討状況
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html
[46]「金融分野における個人情報保護に関するガイドライン」
http://www.fsa.go.jp/siryou/siryou/kj-hogo/01.pdf
[47] 電子ネットワークと個人情報保護　岡村久道・新保史生(2002)　経済産業調査会
[48] 全国銀行個人信用情報センター　http://www.zenginkyo.or.jp/pcic/
[49] IT政策パッケージー2005　―世界最先端の IT 国家の実現に向けてー
http://www.kantei.go.jp/jp/singi/it2/kettei/050224/050224pac.html
[50] infoPLANT　サービス　メルゴング
http://www.info-plant.com/service/media/mailgong/index.html
[51] ブログ・SNSの現状分析及び将来予測　総務省（2005）
http://www.soumu.go.jp/s-news/2005/050517_3.htm

サブテーマ2：運用形態ごとの要件整理

[52]「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）
[53] VoteHere, Inc., “Network Voting System Standards”

サブテーマ3：効率的運用とリスク分析
[54] キーマンズネット http://www.keyman.or.jp/
[55] IT 用語辞典 e-Words http://e-words.jp/
[56] 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
[57] Mainichi INTERACTIVE
http://www.mainichi.co.jp/digital/network/archive/200307/10/6.html
[58] 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
[59] 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
[60] Felica 概要 http://www.sony.co.jp/Products/felica/contents02_02.html
[61] 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
[62] 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
[63]「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
[64] 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
[65] Felica 概要 Felica のしくみ
http://www.sony.co.jp/Products/felica/contents02_02.html
[66] **Visa Smart Card Protection Profile** Draft Version 1.6, Visa International Service Association, May 4,1999
[67] **Smart Card Security User Group's Protection Profile** Version 3.0, Smart Card Security User Group, 9 September 2001
[68] **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
[69] **Smartcard IC Platform Protection Profile** Version 1.0, Atmel Smart Card ICs, Hitachi Europe Ltd, Infineon Technologies AG, Philips Semiconductors, July 2001
[70] **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
[71] **P rotection Profile Intersector Electoronic Purse and Purchase Device** Version 1.3 March 2001
[72] **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
[73] **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
[74] **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
[75] 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
[76] **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
[77]「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
[78]「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
[79] **A Comparative Study of the Major Smartcard Platforms** Dr Brian McKeon Director,Smartcard Technologies Keycorp Limited　2001/11
[80]「雑誌 FUJITSU 2000 年 3 月号」 2000/4
[81] **Smart Card Protection Profiles :An Overview** , Mikhail Gordeev, Vesna Haasler, Martin Manninger 2002
[82] 吉川肇子著「リスク・コミュニケーション」、（福村出版、1999）
[83]「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）
[84] 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
[85] Eric Maiwald、「**Network Security**」、Osborne/McGraw-Hill、2001
[86] 'ISO 15408 情報セキュリティ入門'　内山政人著、東京電機大学出版局
[87] '次世代電子投票システムの IC カードプロテクションプロファイルの考察' 日本情報セキュリティマネジメント学会 JSSM 大阪全国大会鈴木幹夫、内田勝也
[88] 第5回 International Conference on Common Criteria 講演集

サブテーマ5：モデル構築

サブテーマ6：システム構成

[89] 岡本栄司　著　暗号理論入門[第 2 版]　共立出版株式会社
[90] 暗号技術評価報告書 「CRYPTREC Report 2002」
[91] IC カードシステム利用促進協議会　http://www.jicsap.com/index.html
[92] JR 東日本　http://www.jreast.co.jp
[93] 日本道路公団　http://www.jhnet.go.jp
[94] 総務省　http://www.soumu.go.jp
[95] NTT 東日本　http://www.ntt-east.co.jp
[96] NTT 西日本　http://www.ntt-west.co.jp/
[97] Scott Oaks　著　島田秋雄　監訳　JavaTM セキュリティ　株式会社オライリー・ジャパン
[98] サンマイクロシステムズ　http://java.sun.com

サブテーマ7:実験

サブテーマ8：準同型公開鍵暗号方式

[99] 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).
[100] Benaloh, J.: "Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols," Advances in Cryptology-CRYPTO'86, LNCS263, pp.213-222 (1986).
[101] 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).
[102] Fouque, P.A., and Stern, J.: "One Round Threshold Discrete-Log key Generation without Private Channels", Proc. Of PKC2001, LNCS1992, pp.300-316, (2001)
[103] 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).
[104] Okamoto, T., and Uchiyama, S.: "A New Public-Key Cryptosystem as Secure as Factoring," Advances in Cryptology-EUROCRYPT'98, LNCS1403, pp.308-318 (1998).
[105] Naccache, D., and Stern, J.: "A New Public Key Cryptosystem Based on Higher Residues," Proc. 5th Conf. on CCS, pp.59-66 (1998).
[106] Paillier, P.: "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," Advances in Cryptology-EUROCRYPT'99, LNCS1592, pp.223-238 (1999).
[107] Pedersen, T.:"A threshold cryptosystem without a trusted party", Advances in Cryptology-EUROCRYPT'91", LNCS547, pp.522-526 (1991).
[108] 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.

[109] [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.
[110] [HS00]M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," EUROCRYPT'00, pp.539-556, Springer-Verlag LNCS 1807, 2000
[111] [JJ02]A. Juels and M. Jakobsson, "Coercion-Resistant Electronic Elections," Cryptology ePrint Archive 2002/165, IACR, 2002
[112] [Oka97]T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," Security Protocols Workshop, pp.25-35, Springer-Verlag LNCS 1361, 1997.
[113] [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.
[114] 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).
[115] Tsujii, S., Yamaguchi, H., Kitazawa, A., and Kurosawa, K.: "A Method for Voting Protocols with regards to Privacy," 信学技報 ISEC98-42 pp.45-52 (1998).
[116] 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).
[117] 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)
[118] [BEN86] j. bENALOH, "cRYPTOGRAPHIC CAPSULES: a DIS JUNCTIVE PRIMITIVE FOR INTERACTIVE PROTOCOLS," PROC. OF CRYPTO '86, LNCS263, PP. 213-222, 1986.
[119] [YKDKT03] H.Yamaguchi, , A.Kitazawa, H.Doi, K.Kurosawa, AND S.Tsujii "An Electronic Voting Protocol Preserving Voter's Privacy , "IEICE TRANS. INF. & SYST., VOL.E86-D, NO.9 , PP. 1868-1878, 2003.

[120] [TYKK98] S.Tsujii, H.Yamaguchi, A.Kitazawa, K.Kurosawa, “A METHOD FOR VOTING PROTOCOLS WITH REGARDS TO PRIVACY,” TECHNICAL REPORT OF IEICE, ISEC98, PP. 45-51, 1998.

全般:.

[121] 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」

[122] 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

[123] 「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 |
|---|---|---|---|---|
| 1 | 山口　浩<br>北澤　敦<br>Sheu, Phillip<br>石井　千洋 | Bridging Biomedical Application and IT－A Case Study | Integrated Design & Process Technology | 2003/06 |
| 2 | 山口　浩<br>北澤　敦<br>黒澤　馨<br>辻井　重男 | An Anonymous Survey Protocol Preserving Privacy. | IDPT2002 Conference, Society for Design and Process Science | 2002/12 |
| 3 | 山口　浩<br>星野　幸夫<br>鈴木　健嗣<br>Chittoor V. Ramamoorthy | The design of new service system based on the interdisciplinary research, | Transaction of Society for Design and Process Sciences | 2003/9 |
| 4 | 鈴木　幹夫<br>内田　勝也 | 次世代電子投票システムのICカードプロテクションプロファイルの考察 | 日本セキュリティ学会 | 2004/06 |

論文

| 項番 | 著者名 | 表題 | 誌名 | 掲載年月 |
|---|---|---|---|---|
| 1 | 山口　浩<br>星野　幸夫<br>Chittoor V. Ramamoorthy<br>石井　千洋 | Creating a New Service on the Web | International Journal on Artificial Intelligence Tools | 2003/06 |
| 2 | 山口　浩<br>北澤　敦<br>土井　洋<br>黒澤　馨<br>辻井　重男 | An Electronic Voting Protocol Preserving Voter's Privacy. | IEICE TRANSACTION on Information and Systems. | 2003/09 |
| 3 | 山口　浩<br>鈴木　健嗣<br>Chittoor V. Ramamoorthy | The Humanization, Personalization and Authentication ISSUES in the Design and Interactive Service System | Transaction of the SDPS | 2003/09 |

| 項番 | 著者名 | 表題 | 誌名 | 掲載年月 |
|---|---|---|---|---|
| 4 | 鈴木　幹夫<br>内田　勝也 | 次世代電子投票システムの IC カードプロテクションプロファイルの考察 | 日本セキュリティ学会 | 2004/06 |
| 5 | 鈴木　幹夫<br>内田　勝也 | セキュリティ評価基準における脅威分析に関する一考察 | 第1回 学際的情報セキュリティ総合科学シンポジウム論文集 | 2004/11 |

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 |
| 6 | 鈴木　幹夫<br>内田　勝也 | 電子投票システムのセキュリティ評価 | I 情報セキュリティ人材育成公開講座 | 2004/08 |
| 7 | 北澤　敦 | 電子投票・アンケートシステムの構成と技術的課題 | 情報セキュリティ人材育成公開講座 | 2004/08 |
| 8 | 千葉　富久美 | 電子投票と法制度 | 情報セキュリティ人材育成公開講座 | 2004/08 |