# 重み付き投票の電子化とその安全性に関する考察

税所哲郎[†] 齊藤泰一[††]
土井洋[†] 辻井重男[†,†††]

株主総会における議決権行使に代表されるように，1 人が複数票を投票可能な投票（重み付き投票）のニーズは少なくない．しかし，従来研究されてきた電子投票方式は，1 人が 1 票のみ投票可能であるという状況で設計されている場合が多い．本論文では，重み付き投票の電子化方法を提案し，その安全性について評価を行う．また，重み付き投票という点に注目すると，準同型暗号を利用した電子投票方式の拡張が，効率と安全性の点で優れていることを示す．

# On the Security of Electronic Weighted Voting Schemes

Tetsuro Saisho,[†] Taiichi Saito,[††] Hiroshi Doi[†]
and Shigeo Tsujii[†,†††]

A weighted voting scheme is applicable to several voting scheme, e.g., to the annual stockhodler's meeting. But ordinary electronic voting schemes are designed for same weight. In this paper, we propose electronic weighted voting schemes and evaluate their security. From the point of view of the weight, we show that an electronic voting scheme based on homomorphic cryptosystem is suitable to extend to weighted voting because of efficiency and security.

## 1. はじめに

株主総会における議決権行使は，経営方針に関する議案を決定する，会社にとって重要な意思決定手段である．議決権行使は，株主の所有株式数に比例して行えるので，1 人が複数票を投票可能な投票（重み付き投票）と見なすことができる．

また，ある一定の条件を課せられた投票（たとえば，国連安保理の決定）は重み付き投票を用いて実現できることが知られている[23]．

しかし，従来研究されてきた電子投票方式は，1 人が 1 票のみ投票可能という状況で設計されている場合が多い．これらを，重み付き投票へ拡張することは可能であるが，効率と安全性に関する研究[13),15),19),20)]は，十分とはいいがたい．

電子投票には，ブラインド署名[7)]を利用する方式[10)]，Mixnet[6)]を利用する方式[22)]，準同型暗号[14)]を利用する方式[8),9),12),21)]等があるが，重み付き投票を実現するために単純な拡張をすると，1 人 1 票という状況では浮かび上がらなかった無記名性に関する問題が生ずる場合もある．

本論文では重み付き投票という点に注目して，その電子化方法を提案し，安全性について評価を行う．以下，2 章で重み付き投票の定義とその応用例を示し，3 章でモデル化を行う．次に，4 章でブラインド署名を利用した投票方式の拡張，5 章と 6 章で準同型暗号を利用した投票方式の拡張を提案し評価を行う．さらに，7 章で改良と限界について述べ，最終章で結果をまとめる．

## 2. 重み付き投票と具体例

本章では，まず重み付き投票の定義と例を示す．特に株主総会における議決権行使については，日本の状況を中心に説明する．

### 2.1 重み付き投票

重み付き投票とは投票者が複数票を投票可能な投票であり，文献 23) に定義を含む詳細な記述がある．

**定義 1（重み付き投票）** ある閾値 $B$ と投票者ごとの重み $w_i$ が与えられており，賛成票を投じた投票者の重みの総和が $B$ 以上，かつそのときに限り可決と

† 中央大学研究開発機構
Research and Development Initiative, Chuo University
†† NTT 研究所
NTT Laboratories
††† 中央大学理工学部
Faculty of Science and Engineering, Chuo University

| 株主番号 0123 | 議決権行使株式数 | 200 |
|---|---|---|
| 第 1 号議案 | 賛 | 否 |
| 第 2 号議案 | 賛 [ただし　　を除く] | 否 |
| 第 3 号議案 | 賛 | 否 |

**図 1** 議決権行使書の例
Fig. 1 Ballot of stockholder's meeting.

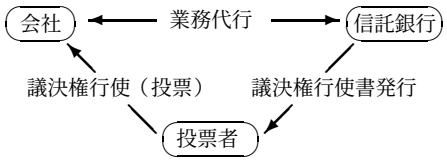


**図 2** 議決権行使の現状
Fig. 2 Model of the voting in stockholder's meeting.

なる投票を重み付き投票と定義する．∎

なお，ある一定の条件を課せられた投票は重み付き投票を用いて実現できることが知られている．たとえば，国連安保理は 5 カ国の常任理事国と，10 カ国の非常任理事国から構成されており，安保理の決定には
(1)　5 カ国の常任理事国すべての賛成と，
(2)　常任理事国を含む合計 9 カ国以上の賛成
という 2 つの条件を満たさなくてはならない．これは，常任理事国に重み 7，非常任理事国に重み 1 を与え，閾値を $B = 39$ とする重み付き投票として実現できる．実際，5 カ国の常任理事国と他 4 カ国が賛成すれば，賛成票を投じた投票者の重みの総和（以下，賛成総数）は 39 になるが，常任理事国 1 国のみが反対した場合は賛成総数が 38 にしかならない．閾値を $B = 39$ とすれば定義 1 を満たすことが分かる．

このように，重み付き投票の電子化を実現すると，様々な投票への応用が期待できる．

### 2.2 株主総会と議決権行使

株主総会は，会社の決算期の 3 カ月以内に開催することが，商法[11]234 条および 224 条の 3 により定められている．日本の場合，会社の決算期が 3 月に集中しているため，株主総会は 6 月に集中して開催される．そこで，経営に関する様々な議案に対して株主による議決が行われるが，それを議決権行使と呼ぶ．議案ごとの投票内容は**図 1** に示すように簡潔であり，議案に対する賛否，賛成時の除外事項等である．

議決権行使とは投票を意味しており，株主は議決権行使株式数（所有株式数から端数を除いたもの）分だけの投票を行うことができるので，重み付き投票である．もちろん，所有株式数が多い株主の投票全体に与える影響は大きい．たとえば，会社の発行株式数の 30%を所有する大株主は，事実上，会社の経営方針を決定できるといわれている．

また，商法 239 条の 4 により，株主の議決権不統一行使（たとえば議決権行使株式数のうち，30%は賛成，70%は反対とする議決権行使）は可能である．しかし，事前申請が必要であること，会社側で拒否できること等から，現状では個人株主による不統一行使は，事実上不可能と見なされる．

議決権行使は郵送によって行われることが多いが，郵送された議決権行使書（図 1）は商法 239 条に従って，株主総会実施後 3 カ月は閲覧または謄写が可能である．また，株主なら誰でも閲覧・謄写が可能であることから，現行の紙を利用する方式では，議決権行使結果は開示されていると考えてよい．

現状では，所有株式数の多い上位 10 人の大株主については，名義と所有株式数が会社の有価証券報告書や会社四季報[25] 等で公開されている．

なお，会社は株式に関する業務を行わない場合が多い．その場合，株主情報を信託銀行等に提供して，信託銀行が株式に関する業務を代行する．特に，**図 2** に示すように，議決権行使書の発行を信託銀行が代行することが多い．なお，会社によっては議決権行使の集計までを信託銀行が代行する場合もある．

### 2.3 用語と記号

重み付き投票に関係するエンティティは $l$ 人の投票者 $V_i$，$n$ 人の管理者 $A_i$，$t$ 人の集計者 $T_i$ および確認者である．管理者や集計者が 1 人の場合は，単に $A$ や $T$ と記述する．各投票者 $V_i$ は投票内容 $v_i$ を $w_i$ 票だけ投票できる．$w_i$ が重みである．

## 3. 必要要件とモデル

本論文では，議論を簡単にするために，投票対象は 1 つで，投票者は賛成（投票内容 1）または反対（投票内容 $-1$）のいずれかの値を重み分だけ投票すると仮定する．また，重みを含めて集計した結果，賛成総数と反対総数が一致した場合は，可決と扱うことにする．すなわち，重み付き投票の定義（定義 1）における閾値は，$B = 0$ として議論を進める．

本章では，重み付き投票の電子化に向けての必要要件を示す．また，重みを公開情報と見なすか，秘密情報と見なすかの違いによる 2 つのモデルを示す．

### 3.1 投票の要件

重み付き投票の電子化を考える場合に満たすべき要件を，C1 から C10 に示す．これらの要件は，通常の電子投票に求められる要件（C1 から C7）と，重みの考慮による要件（C8 から C10）から構成される．
C1（完全性）不正がなければ正しく集計される．

C2（無記名性）投票者と投票内容の関連付けに関して，投票結果のみから得られる情報以上の情報を得ることができない．
C3（2 重投票不可能性）投票者は 2 度投票することはできない．
C4（未登録者の投票排除）登録された投票者以外は投票できない．
C5（公平性）投票に影響する途中経過が露呈しない．
C6（検証性）投票結果が正しいことを検証できる．
C7（無証拠性）投票内容が何かを第 3 者に証明できない．
C8（高効率性）重み付き投票を効率良く実現できる．
C9（不統一行使防止）投票者の投票内容はすべて同一である．
C10（重み情報の秘匿）重みを秘密情報と見なす場合，投票者の重みに関して，投票結果のみから得られる情報以上の情報を得ることができない．

さて，通常の（1 人 1 票の）電子投票方式を重み分だけ繰り返すことにより，重み付き投票の電子化を実現できる．しかし，株主総会の例（2.2 節）では，1 人が数万票を有する場合があり，効率が良いとはいいがたい．本論文では，既存の電子投票方式を重み付き投票に拡張する手法を採る．そこで，要件 C8 の定義を，方式を拡張する際の（計算量と通信量をあわせた）コストの増加が $\log w_i$ で抑えられることとする．

**定義 2（効率の良い重み付き投票）** 投票者 $V_i$ に与えられた重みを $w_i$ とする．投票者 $V_i$ の 1 人 1 票の電子投票方式のコストを $O(C_{1V})$，重み付き投票に拡張した場合のコストを $O(C_{WV}(w_i))$ とする．

$$O(C_{WV}(w_i)) \leq O(\log w_i \cdot C_{1V})$$

を満たすとき，重み付き投票方式の効率が良い（要件 C8 を満たす）と定義する． ∎

要件 C9 は不統一行使を認める場合[13),15)]と認めない場合[19),20)]では扱いが異なる．後者の場合，要件 C9 は投票を何度かに分けて行う際に問題となる．

**定義 3（不統一行使防止）** 投票者 $V_i$ に与えられた重みを $w_i$ とし，投票すべき内容は賛成，または反対のいずれかとする．投票者の投票できる内容が，重み $w_i$ の賛成，または重み $w_i$ の反対のいずれか一方に限られるとき，投票方式は不統一行使防止を実現できる（要件 C9 を満たす）と定義する． ∎

なお，要件 C9 は，国連安保理の決定のように，条件付き投票を重み付き投票として実現（2.1 節）するためには必須の要件であり，また，株主総会における議決権不統一行使に関する現況（2.2 節）とも一致する．

要件 C10 については，重みを秘密情報として扱う場合にのみ要求される条件である．これは，関係するエンティティの攻撃を認めるか否か，情報の漏洩度等により，様々な定義が考えられる．本論文では，重み付き投票に関係するエンティティの能動的な攻撃は考慮しない．また，情報の漏洩については次のように考える．従来の投票方式[4),6),8)~10),12),13),15),19)~22)]では，投票結果として必要な値は (賛成総数) − (反対総数) である．投票結果とは，投票を実現するために不可欠な値であり，投票結果のみから知られる情報は漏洩と考えない．しかし，投票に求められる要件を満たすためには，ほかに様々な情報が公開される．そこで，これらの情報から重みに関する情報が漏洩しないことを定義とする．

**定義 4（重み情報の秘匿）** $l$ 人の投票者とその重みの組を $\{(V_i, w_i)\}$ と記述する．重み付き投票が成立したときの結果のみの情報を $I_R$，投票にともない公開される（$I_R$ を含む）すべての情報を $I_V$ とする．$A$ を $I_V$ を入力とし $\{(V_i, \bar{w}_i)\}$ を出力する多項式時間アルゴリズムとする．任意の $i \in \{1, \cdots, l\}$ と，任意のアルゴリズム $A$ に対して，$I_R$ を入力とし $\{(V_i, \tilde{w}_i)\}$ を出力する多項式時間アルゴリズム $B$ が存在し，

$$\mathrm{Prob}(\bar{w}_i = w_i) < \mathrm{Prob}(\tilde{w}_i = w_i) + \epsilon$$

が成り立つとき，重み情報は秘匿される（要件 C10 を満たす）と定義する． ∎

次に，通常の電子投票に求められる要件について，注意事項を示す．まず，要件 C2 については，要件 C10 と同様，投票結果を除いた様々な情報から投票内容が漏洩しないことを定義とする．

**定義 5（無記名性）** $l$ 人の投票者とその投票内容の組を $\{(V_i, v_i)\}$ と記述する．重み付き投票が成立したときの結果のみの情報を $I_R$，投票にともない公開される（$I_R$ を含む）すべての情報を $I_V$ とする．$A$ を $I_V$ を入力とし $\{(V_i, \bar{v}_i)\}$ を出力する多項式時間アルゴリズムとする．任意の $i \in \{1, \cdots, l\}$ と，任意のアルゴリズム $A$ に対して，$I_R$ を入力とし $\{(V_i, \tilde{v}_i)\}$ を出力する多項式時間アルゴリズム $B$ が存在し，

$$\mathrm{Prob}(\bar{v}_i = v_i) < \mathrm{Prob}(\tilde{v}_i = v_i) + \epsilon$$

が成り立つとき，投票内容は秘匿される（要件 C2 を満たす）と定義する． ∎

重み付き投票では，投票者の重みが公開されている場合，投票結果のみから投票内容の情報が得られる場合がある（詳細は 7 章を参照のこと）．定義 5 は，(投票結果のみから得られる以上の）投票内容に関する情報が漏洩しないことを求めている．

要件 C7[4),12),22)]については，これを実現するとトータルとしてのコストが増大する．しかし，通常の選挙

**表 1** 電子投票方式の分類
Table 1 Classification of electronic voting schemes.

| 方式 | 分類 | 無記名性の実現方法 | 投票内容 |
|---|---|---|---|
| Mixnet | 投票内容掲示型 | Mixnet | 任意の値 |
| ブラインド署名 | 投票内容掲示型 | ブラインド署名，匿名通信路 | 任意の値 |
| 準同型暗号 | 集計結果掲示型 | 暗号化したままの集計 | 数値（0/1 等） |

やアンケートと違い，株主総会の例では会社（管理者）と株主（投票者）との間に複雑な利害関係が存在する．したがって，票の売買等が起こりやすい状況であると考える．そこで本論文では，要件 C7 も満たす方式の実現を目標とする．

### 3.2 モデル

#### 3.2.1 投票方式の分類

従来から提案されてきた電子投票方式は，Mixnet，ブラインド署名，準同型暗号を利用する方式に大別できる[16),24)]．後述するように，無記名性の実現方法が重み付き投票の安全性に影響するので，本節で分類を行う．

Mixnet やブラインド署名を利用する方式では，最終的に公開掲示板には各投票者の投票内容が無記名で掲示される．そして，掲示された結果を集計し，最終的な投票結果とする．本論文ではこれを投票内容掲示型と呼ぶ．

一方，準同型暗号を利用する方式では，暗号化した状態で各投票を公開掲示板に掲示した後，（暗号化したまま）集計を行う．そして，最後に復号を行うことにより，最終的な結果のみが掲示される．暗号化したまま集計（演算）を行う必要があるため，投票内容は $-1$ や 1 等の数値に限定される．本論文ではこれを集計結果掲示型と呼ぶ．

無記名性実現方法による分類を**表 1** に示す．

#### 3.2.2 重みの扱いによる分類

2 章で，重み付き投票の例を 2 つ述べた．この 2 つの例では重みという情報の扱いが異なる．前者（国連安保理の例）では各投票者の重みは公開されている．しかし，後者（株主総会の例）では各投票者の重みは公開されているとはいいがたい．一部の大株主を除き，株主の所有株式数は公開されないからである．

しかし，株主総会の例でも，重みを公開情報と解釈することは重要である．実際，投票者とその重みを知るエンティティ（会社）は必ず存在する．逆に，もしそのようなエンティティが存在しない場合は，ある投票者 $V_i$ が重み $w_i$ とは異なる重み $w_i'$ を用いて投票した場合に，不正を検出する手段はない．さらに，株主総会の例では，重みを知るエンティティ（会社）と投票者（株主）が敵対関係になることも少なくない．したがって，投票者の重みが公開されているモデル（重み公開モデル）で安全性を評価することは，重みを知るエンティティによる攻撃からの耐性を評価することになる．

一方，重みを個人情報としてとらえることも多いので，重みをつねに公開情報と見なすのも適切ではない．株主総会の例では，所有株式数（財産）が重みに相当するが，すべての株主がその公開を望むとは考えにくい．すなわち，

- 投票者とその重みを知る管理者 $W$ が存在し，
- その管理者 $W$ を信頼できる

というモデル（重み非公開モデル）が考えられる．株主の所有株式数は原則非公開であるが，信頼のおける信託銀行の存在を仮定している現状の株主総会の例（図 2）は，重み非公開モデルである．したがって，重み非公開モデルで（要件 C10 を含めた）安全性の評価を行うことも必要である．

本論文では，4 章と 5 章で重み公開モデルを扱った後，6 章で重み非公開モデルを扱う．

### 3.3 本研究の位置付け

従来の重み付き投票の電子化の研究[13),15),19),20)]は重み公開モデルでの研究であり，要件 C10 は考慮されていない．要件 C9 については，文献 19)，20) では必須とする方式を構築しているが，文献 13)，15) では投票者が重みを分割可能な方式を構築している．本論文では，要件 C9 を必須とし，重み公開モデルと重み非公開モデルでの投票方式を提案し，評価を行う．

## 4. 部分ブラインド署名を利用する方式

本章では，重み公開モデルに基づき，投票内容掲示型に属する FOO92[10)] に，部分ブラインド署名[2),3)]を応用する重み付き投票方式を提案し，その安全性を評価する．

### 4.1 部分ブラインド署名

管理者 $A$ の部分ブラインド署名を得るために投票者 $V_i$ が行うブラインド処理を $\chi$，アンブラインド処理を $\delta$ とする．$x_i$ を $A$ に署名させたい内容，$\sigma$ を $A$ の署名関数，$r_i$ を投票者が使用する乱数とし，$V_i$ と $A$ の共通情報を $c_i$ とする．$y_i = \delta(\sigma(\chi(x_i, c_i, r_i), c_i), c_i, r_i)$ とすると，$(x_i, y_i, c_i)$ が $A$ の部分ブラインド署名と

なる．

### 4.2 FOO92 を基にした重み付き投票方式

共通情報 $c_i$（重み $w_i$ とは限らない）分の投票を一度に行うプロトコルを示す．以下，FOO92 と同様に，匿名通信路の存在を仮定する．また，ビットコミットメント関数 $\xi(x,r)$ が公開されているとする．ここで $x$ はコミット内容，$r$ は乱数である．

**プロトコル 1** 投票者 $V_i$ と管理者 $A$ は重みに関する情報を共有し，$c_i$ 分の投票を一度に行う．

**登録** 投票者 $V_i$ と管理者 $A$ は $c_i$ を共通情報とする部分ブラインド署名を作成する．

(1) 投票者 $V_i$ は投票内容 $v_i$，乱数 $k_i$ を用い，$x_i = \xi(v_i, k_i)$ を作成する．次に $c_i$ と乱数 $r_i$ を使い，$e_i = \chi(x_i, c_i, r_i)$ と $V_i$ の署名 $s_i = \sigma_i(e_i)$ を作成し，$A$ に $(e_i, s_i, c_i)$ を送る．

(2) 管理者 $A$ は，まず，$(e_i, s_i, c_i)$ の正当性を検証する．次に，$V_i$ が $c_i$ 分の投票が可能であるか確認する．2 つの検証にいずれも合格したら，$d_i = \sigma(e_i, c_i)$ を作成し，$V_i$ に返す．

(3) $V_i$ は，$y_i = \delta(d_i, c_i, r_i)$ を計算し，部分ブラインド署名 $(x_i, y_i, c_i)$ の正当性を検証する．

**投票** 投票者 $V_i$ は匿名通信路を利用して，集計者 $T$ に部分ブラインド署名 $(x_i, y_i, c_i)$ を送る．$T$ は，$(x_i, y_i, c_i)$ の正当性を検証後，公開掲示板に掲示する．なお，掲示は投票番号 $m$ とのペア $(m, x_i, y_i, c_i)$ となる．

**集計** 投票締め切り後，投票者 $V_i$ は，投票番号 $m$ と投票内容および乱数，すなわち $(m, v_i, k_i)$ を匿名通信路を利用して集計者 $T$ に送る．次に，$T$ は，$(x_i, v_i, k_i)$ の正当性を検証する．この検証に合格した場合，公開掲示板に $(m, x_i, y_i, c_i, v_i, k_i)$ を掲示する． ∎

### 4.3 無記名性と重みの分割について

プロトコル 1 では，投票者が一度に複数票を投票するという目的は達しているが，投票結果と投票内容の関連付けが可能となる場合がある．実際，投票結果 $(m, x_i, y_i, c_i, v_i, k_i)$ は，公開掲示板に掲示される．この場合，「$c_i$ 票分の投票が行われ，その投票内容が $v_i$ である」ということが公開される．もし，$c_i$ と $V_i$ の関連付けが可能ならば，要件 C2（無記名性）を満足しない．

**例 1** 共通情報 $c_i$ を投票者 $V_i$ の重み $w_i$ とする．もし，重み $w_i$ を持つ投票者が $V_i$ しかいない場合は，公開掲示板に掲示される $(m, x_i, y_i, w_i, v_i, k_i)$ から，$V_i$ の投票内容が $v_i$ であるということが分かる． ∎

この問題は，投票内容とその重みという情報が公開されることに起因する．したがって，一度に重み $w_i$ 分だけ投票することをやめて，適切に分割して投票することによってある程度解決できる[19]．たとえば，重みを $2^j$（以下，分割単位．2 のべき乗である必要はない）に分割し，分割単位ごとに投票すればよい．この場合，投票者 $V_i$ の投票コストは $\log w_i$ となるので効率的である（要件 C8 を満たす）が，要件 C9 を満たすためには，分割して投票した内容がすべて同一であることを，投票内容を知られることなく証明しなくてはならない．零知識対話証明を使えば原理的には可能であるが，投票者の証明に要するコストが増加する．

また，各分割単位（たとえば $2^j$）を使う投票者が複数（多数）存在しなくてはならない．たとえば，1024 票以上の重みを持つ投票者が $V_i$ しかいない場合，分割単位 1024 とその投票内容 $v_i$ が掲示されれば，投票者 $V_i$ の投票内容が $v_i$ であることが分かる．したがって，重みの大きな投票者は，十分細かく分割しなくてはならない．

なお，分割を投票者任せにする場合，$V_i$ 以外の投票者の分割方法が，$V_i$ の投票内容の無記名性に大きく影響する場合がある．

**例 2** $V_i$ の分割単位が偶数値 $w_{i,k}$ を含むとする．$V_i$ 以外の全投票者の分割単位が，すべて奇数である場合，偶数の分割単位 $w_{i,k}$ とその投票内容 $v_i$ が掲示されれば，それが $V_i$ の投票であることが分かる． ∎

この問題は，分割の細分化だけでは解決できない．システムにより，分割単位に対してある程度のルール付けを与える必要がある．

なお，本節で議論した無記名性の問題は，投票内容掲示型の電子投票方式をプロトコル 1 に用いた手法で重み付き投票に拡張した場合は，必ず発生する．

## 5. 準同型暗号を利用する方式

本章では，重み公開モデルに基づき，集計結果掲示型に属する CGS97[9] および HS00[12] を利用する重み付き投票方式を提案し，その安全性を評価する．

### 5.1 原　　理

まず，準同型暗号 $f$ を用意する．$f$ は確率的公開鍵暗号であり，$f^{-1}(f(m_1) \times f(m_2)) = m_1 + m_2$ を満たす．準同型暗号を利用する投票は，準備の後，次の 2 つのフェーズで構成される．

**投票** 準同型暗号を利用した 1（賛成）または $-1$（反対）の暗号文を投票として掲示する．さらに，投

票が 1 または $-1$ の暗号文であることを証明する．

**集計** 投票をすべて乗ずる．結果は (賛成総数) − (反対総数) の暗号文になるので，それを集計者が復号し，可決（復号結果が 0 以上）か否かを示す．

準同型暗号を利用する方式を重み付き投票に拡張するためには，投票に重みを反映させる仕組みが必要となる．実現方法としては，次の 2 つの方法が考えられる．

**重み反映法 1** 投票時点で $w_i$ か $-w_i$ の暗号文を作り，これを投票として掲示する．また，投票が $w_i$ か $-w_i$ の暗号文であることを証明する．

**重み反映法 2** 投票時点では 1 または $-1$ の暗号文を作り，これを投票として掲示する．また，投票が 1 か $-1$ の暗号文であることを証明する．そして，集計までに暗号文を $w_i$ 乗する．

重み反映法 2 では，途中で $w_i$ 乗を行うコストが発生する．しかし，重み反映法 1 の場合も，(本章で述べる例では) 投票が $w_i$ または $-w_i$ の暗号文であることを証明しなくてはならず，この際 $w_i$ 乗を行うコストが発生するので，コスト的には大差はない．また，重み非公開モデルに適用する場合は，投票者の処理（証明に係わる処理を含む）が重みに依存しないほうがよい．よって，重み反映法 2 を採用する．

### 5.2 CGS97 を基にした重み付き投票方式

CGS97[9] を基にした重み付き投票方式を示す．複数の集計者 $T_i$ が集計に必要な情報を出力し，$(k,n)$ 閾値法で復号する．

**プロトコル 2** 投票フェーズで重みを反映させる点を除けば，CGS97[9] と同じである．

**準備** 公開された素数 $p$，$q|(p-1)$ と $g,G$（ただし $\mathrm{ord}(g)=\mathrm{ord}(G)=q$）に対し，各集計者 $T_i$ は乱数 $s_i$ を秘密に生成する．次に文献 18) に従い，閾値型 ElGamal 暗号の公開鍵 $h \equiv g^s \bmod p$ を生成する．

投票者 $V_i$ は乱数 $b_i \in \{1,-1\}$ をマスク値[8),9),21)] として選び，閾値型 ElGamal 暗号による $G^{b_i}$ の暗号文を生成する．$\alpha$ を乱数とすると，暗号文は $(\bar{x}_i,\bar{y}_i)=(g^\alpha \bmod p, h^\alpha G^{b_i} \bmod p)$ である．なお，これが $G$ または $G^{-1}$ の暗号文であることを投票者が証明する．

**投票** 次に，$e_i b_i = v_i \in \{w_i,-w_i\}$ となる $e_i \in \{w_i,-w_i\}$ を公開掲示板に掲示する．たとえば，乱数 $b_i$ が $-1$ であった場合，$v_i=w_i$ を投票するには，$e_i=-w_i$ を掲示する．

**集計** $(X,Y)=(\Pi \bar{x}_i^{e_i} \bmod p, \Pi \bar{y}_i^{e_i} \bmod p)$ を公開掲示板上で計算する．次に，集計者 $T_i$ は部分情報 $a_i \equiv X^{s_i} \bmod p$ を公開する．$k$ 個の部分情報が集まれば，誰でも $X^s \bmod p$ を計算できるので，閾値型 ElGamal 暗号を復号して $G^M$ を得ることができる．ここで，$M$ は (賛成総数)−(反対総数) である．$M$ が小さいことから，$G^M \bmod p$ の離散対数問題を解くことによって $M$ を求めることができる．なお，部分情報 $a_i$ が正しいことを集計者 $T_i$ は証明しなくてはならない． ∎

### 5.3 無証拠性への拡張

次に，無証拠性（要件 C7）を有する HS00[12] への適用を考える．この際用いる準同型暗号は，文献 12) の 3.3 節に記述されている 6 つの性質を必要とするが，閾値型 ElGamal 暗号はこれらの性質を満たす．これらの性質のうち，重み付き投票（特に 6 章や 7 章）で利用するものの概要を示す．

**Random Re-encryptability** 平文 $m$ の暗号文 $E$ が与えられたとき，平文を知ることなく，別の暗号文 $E'$ を乱数 $r$ を用いて作成することができる．ElGamal 暗号の場合，$E=(x,y)$ とすると，$\xi$ を用いた再暗号化は $E'=(g^\xi x, h^\xi y)$ である．なお，$E'$ は $m$ の暗号文空間上に一様に分布する．

**1-out-of-L Re-encryption Proof** 暗号方式の公開鍵 $PK$，暗号文 $E=(x,y)$，その再暗号化が含まれる暗号文の集合 $\{E_1,\cdots,E_L\}$，および $E_i=(g^\xi x, h^\xi y)$ となる $\xi$ が与えられたとき，$i$，$\xi$ を知られることなく，$E_i$ が $E$ の暗号化であることを証明できる．以下，この証明を $P_{1L}(PK,E,\{E_1,\cdots,E_L\})$ と記述する．

**Designated-Verifier Re-encryption Proof** 暗号方式の公開鍵 $PK$ と検証者 $V$ の公開鍵 $PK_V$ が公開され，検証者は秘密鍵 $SK_V$ を保持しているとする．暗号文 $E=(x,y)$，$E'=(g^\xi x, h^\xi y)$，および $\xi$ が与えられたとき，その証拠 $\xi$ が存在することを，ある特定の検証者 $V$ のみに証明することができる．以下，この証明を $P_{DV}(PK,PK_V,E,E')$ と記述する．

さて，無証拠性を実現するためには，投票者は自らが作成した乱数を用いる証明を行うことができない（乱数生成方法を証拠として利用される場合がある[12]）．そこで，HS00 では，投票内容を $n$ 人の管理者 $A_i$ が作成することで解決している．

まず，管理者 $A_1$ は 1 の暗号文 $E_1$ を作成し管理者 $A_2$ に渡す．以下，管理者 $A_i$ は，管理者 $A_{i-1}$ から 1 または $-1$ の暗号文である $E_{i-1}=(x_{i-1},y_{i-1})$ を受け取り，それを再暗号化（Random Re-encryptability）した $\bar{E}_i=(\bar{x}_i,\bar{y}_i)$ を生成する．次に，$\bar{E}_i^{-1}=$

$(\bar{x}_i^{-1}, \bar{y}_i^{-1})$ として，$E_i \in_R \{\bar{E}_i, \bar{E}_i^{-1}\}$ を出力する．このとき，$E_i$ または $E_i^{-1}$ が，$E_{i-1}$ の再暗号化であるので，この証明 $P_{1L}(PK, E_{i-1}, \{E_i, E_i^{-1}\})$ を公開掲示板に掲示する．このようにして，$A_i$ が出力する $E_i$ が 1 または $-1$ の暗号文になること（ランダムに切り替わること）を証明できる．

一方，管理者 $A_i$ は投票者 $V$ へ，物理的に盗聴不可能な一方向性通信路（以下，PUOW 通信路）を使って $\bar{E}_i \in \{E_i, E_i^{-1}\}$ が $E_{i-1}$ の再暗号化であることの証明 $P_{DV}(PK, PK_V, E_{i-1}, \bar{E}_i)$ を行う．なお，投票者 $V$ はカメレオンコミットメント用の公開鍵 $PK_V$ を公開し，その秘密鍵 $SK_V$ を保持している．秘密鍵 $SK_V$ を知らない管理者 $A_i$ は $P_{DV}(PK, PK_V, E_{i-1}, \bar{E}_i)$ しか作ることができないが，秘密鍵 $SK_V$ を知る投票者 $V$ は，さらに $P_{DV}(PK, PK_V, E_{i-1}, \bar{E}_i^{-1})$ も作ることができる．したがって，PUOW 通信路を経由して得た証明を証拠として利用できないので，$V$ は入れ替えの有無に関する証明ができないことになる．この性質を利用して無証拠性を実現している．

**プロトコル 3** 準備フェーズで管理者による投票の作成を行うようにする．

**準備** 管理者 $A_1$ は 1 の暗号文 $(g^{\alpha} \bmod p, h^{\alpha} G^1 \bmod p)$ を生成し，これを $E_1 = (x_1, y_1)$ として管理者 $A_2$ に渡す．管理者 $A_2$ はランダムに $\beta_2 \in_R Z/qZ$ と $b_2 \in_R \{1, -1\}$ を選び，$((g^{\beta_2} x_1)^{b_2} \bmod p, (h^{\beta_2} y_1)^{b_2} \bmod p)$ を計算し，これを $E_2 = (x_2, y_2)$ として管理者 $A_3$ に渡す．以下，これを繰り返す．最終的には全員が $(x_n, y_n)$ を得ることができるが，それが 1 に対応する暗号文か $-1$ に対応する暗号文かを知ることはできない．ただし，PUOW 通信路を経由して，$\{b_2, \cdots, b_n\}$ を得る投票者は，$(x_n, y_n)$ が 1 に対応する暗号文か，$-1$ に対応する暗号文かを知ることができる．なお，再暗号化と入れ替えのみを行っていること等の証明は，各管理者 $A_i$ が公開掲示板上で行う．

**投票・集計** プロトコル 2 と同じである． ∎

### 5.4 安全性について

重み公開モデルの場合，基となる準同型暗号を利用した投票方式が安全な場合，重み付き投票方式も安全である．実際，違いは投票時の投票者の処理だけであり，投票フェーズで，$-1$ または 1 を掲示板に公開するのではなく，$e_i \in \{-w_i, w_i\}$ を公開する点のみが異なる．しかし，重み公開モデルでは，$w_i$ が公開されているため，セキュリティへの影響はない．

**定理 1** CGS97[9] が C1 から C6 を満たすならば，プロトコル 2 は，C1 から C6，C8，C9 を満たす．

**（証明）** C1 から C6 を満たすことは CGS97 より従う．投票者 $V_i$ の CGS97 に対する処理の違いは，重みを反映した $w_i$，または $-w_i$ のいずれかを掲示版に公開することだけであるから，C8 を満たす．また，投票は 1 回のみであるから，C9 も満たす． ∎

**定理 2** HS00[12] が C1 から C7 を満たすならば，プロトコル 3 は，C1 から C9 までを満たす．

**（証明）** C1 から C7 は，HS00 より従う．C8，C9 は，定理 1 と同様に満たす． ∎

## 6. 重み非公開モデル

本章では，重み非公開モデルに基づき，重み情報の秘匿（要件 C10）を目的とする，集計結果掲示型に属する重み付き投票方式を提案する．

### 6.1 重み非公開モデルでのセキュリティ

3 章で考察したように，このモデルは投票者の重みを知る信頼のおける管理者 $W$ の存在を仮定する．また，5.1 節で言及したように，投票者 $V_i$ の処理から重みが露呈しないように，投票者の処理を重みに依存しないもの（重み反映法 2 を採用）とし，管理者 $W$ が重みを反映させるようにする．この場合，管理者 $W$ が票の重み付けを行うが，その処理に対しても信頼をおく．すなわち管理者 $W$ が，投票者の重みを暴露しないこと，投票者と結託して重みを操作しないこと，重み付けを間違えないことを仮定する．しかし，管理者 $W$ に対しても，重み情報の秘匿（要件 C10）以外の要件（C1 から C9 まで）は満たすべきである．もちろん，管理者 $W$ 以外に対しては，要件 C1 から C10 までを満たさなくてはならない．

### 6.2 提 案 方 式

**プロトコル 4** 投票者の重み $w_i$ の反映を投票者ではなく管理者 $W$ が行うように，プロトコル 3 から投票フェーズと集計フェーズを変更する．

**投票** $V_i$ は $e_i b_i = v_i \in \{1, -1\}$ となる $e_i \in \{1, -1\}$ を公開掲示板に掲示する．以下，$(x_i, y_i) = (\bar{x}_i^{e_i} \bmod p, \bar{y}_i^{e_i} \bmod p)$ とおく．

**集計** 管理者 $W$ は各投票 $E_i = (x_i, y_i)$ を再暗号化し，ランダムな置換 $\pi$ で入れ替えた $E'_{\pi(i)} = (x'_{\pi(i)}, y'_{\pi(i)})$ を対応する重みと一緒に $(E'_{\pi(i)}, w_{\pi(i)})$ として掲示する．さらに，置換のみを行っていることを文献 1) の方法を用いて証明する．

次に $(X, Y) = (\Pi {x'_{\pi(i)}}^{w_{\pi(i)}}, \Pi {y'_{\pi(i)}}^{w_{\pi(i)}})$ を計算する．以後の集計処理はプロトコル 3 と同じである． ∎

このプロトコルでは，掲示板上には $(E'_{\pi(i)}, w_{\pi(i)})$

が掲示されるが，$(x_i, y_i)$ との関連付けはできない．したがって次の結果を得る．

**定理 3** HS00[12] が C1 から C7 を満たすならば，プロトコル 4 は

(1) 管理者 $W$ に対しては C1 から C9 を満たし，
(2) 管理者 $W$ 以外に対しては C1 から C10 を満たす．

**（証明）** $W$ を含む全検証者に対して，C1 から C9 を満たすことは，定理 2 より従う．管理者 $W$ 以外に対して C10 を満たすことの証明は，付録 A.1 を参照のこと． ∎

投票者 $V_i$ が，自分の投票内容が（重み付けも含めて）投票結果に正しく反映されていることを確認できるようにするためには，Designated-Verifier Re-encryption Proof を用いて管理者 $W$ が $E_i$ と $E'_{\pi(i)}$ の対応を証明すればよい．

なお，プロトコル 4 では，管理者 $W$ に対し高い信頼を要求することを注意しておく．しかし，重み非公開モデルである株主総会の例（2.2 節）では，会社の株式業務を委託された（株式業務に関しては完全に信頼されている）信託銀行が存在する場合が多い．重みの管理と操作を行う管理者 $W$ への信頼を仮定することは，株主総会における現状と整合性がある．

## 7. 投票結果と重みの関係

本章では，投票結果と重みの関係について述べる．5 章で述べた重み公開モデル，6 章で述べた重み非公開モデルのいずれでも，重みを管理する（全投票者の重みを知る）エンティティは存在する．本章では，このようなエンティティの視点を考慮し，重み公開モデルに基づき，投票結果が無記名性（要件 C2）に与える影響について述べる．さらに，改良方式とその限界を示す．まず，無記名性に悪影響を与える例を 2 つ示す．

**例 3** $V_1$，$V_2$，$V_3$，$V_4$，$V_5$ の重みを各々4，3，8，4，8 とする．投票結果が $4k+1$ と公開された場合，$V_2$ が反対（$-1$ を投票）したことが分かる． ∎

**例 4** $V_1$，$V_2$，$V_3$，$V_4$，$V_5$ の重みを各々1，2，4，8，16 とする．投票結果が $-5$ と公開された場合，$V_1$，$V_3$，$V_4$ が賛成（1 を投票）し，$V_2$，$V_5$ が反対（$-1$ を投票）したことが分かる．この例では重みの分布が超増加数列であり，投票結果が分かれば，すべての投票内容が分かる． ∎

重み付き投票を実現する場合，実現方式として紙を利用しようと，電子化しようと，上記のように投票結果から投票内容が漏れる場合がある．これは電子化による問題ではなく，重み付き投票という仕組みと投票結果として (賛成総数) − (反対総数) を公開する仕組みを組み合わせることによる問題である．

これは，投票結果に誤差を与えるという方法である程度回避できる．集計結果掲示型に属するプロトコル 2，3，4 に対する拡張を示す．

**プロトコル 5** (賛成総数) − (反対総数) を公開することなく，投票結果を納得させるため，ある範囲内の誤差を複数の管理者 $J_i$ が発生させる．

**準備** 誤差を発生させる $n_J$ 人の管理者 $J_i$ を新たに選ぶ．誤差の範囲を $\{-E, \cdots, -1, 0, 1, \cdots, E\}$ とする．また，パラメータ $e = E/n_J$ を公開する．他の処理はプロトコル 2，3，4 と同じである．

**投票** プロトコル 2，3，4 と同じである．

**集計** $(X, Y)$ を公開掲示板上で計算した後，次の手順により誤差を発生させる．

(1) $J_i$ は $e_i \in_R \{-e, \cdots, e\}$ をランダムに選ぶ．次に $G^{e_i}$ の閾値 ElGamal 暗号文 $\hat{E}_i$ を作成して掲示版に掲示するとともに，その平文が $\{-e, \cdots, e\}$ に含まれていることの証明 $P_{1L}(PK, \hat{E}_i, \{-e, \cdots, e\})$ を行う．
(2) すべての $J_i$ が生成した暗号文 $\hat{E}_i$ を投票結果 $(X, Y)$ に乗ずる．
以下の手順はプロトコル 2，3，4 と同じである．最終的に，$\bar{M} = M + \sum e_i$ を得るが，$\bar{M} \geq E$ の場合は，可決と見なす． ∎

このプロトコルでは，投票結果は誤差 $\sum e_i$（ただし $|\sum e_i| \leq E$）を含む．この重み付き投票における閾値は $B = 0$ であり，投票結果が閾値 0 から離れている場合は，プロトコル 5 で可決か否決かを確認できる

**定理 4** 管理者 $J_i$ すべてが結託しないと仮定する．$|M| > 2E$ の場合，プロトコル 5 は

(1) 可決か否決かを誰もが確認でき，
(2) 開示された投票結果には誤差が含まれており，その誤差の値を知ることはできない．

**（証明）** $|M| > 2E$ の場合は，明らかに投票結果が可決または否決であることを確認できる．すべての管理者 $J_i$ が誤差の値 $e_i$ を開示しない限り，$M$ の値を知ることはできない（誤差の値を知ることはできない）． ∎

投票結果は，誤差 $\sum e_i$ を含むので，投票結果を誤差なく公開する場合と比較して，個々の投票内容を知ることは困難になる．現実の投票では投票結果が数票差の接戦になることは少ないので，ある程度の効果が期待できる．しかし，小規模な投票や，賛成総数と反

**表 2** 各方式の特長
Table 2 Properties of proposed schemes.

| 方式 | 基本方法 | 達成した要件 | 安全性の仮定 * |
|---|---|---|---|
| プロトコル 1 | 部分ブラインド署名，FOO92 | C1〜C6，C8，C9 | 分割の安全性 |
| プロトコル 2 | CGS97 | C1〜C6，C8，C9 | |
| プロトコル 3 | HS00 | C1〜C9 | |
| プロトコル 4 | HS00 | C1〜C10 | 重みを知る管理者への信頼 |

* 基本となる投票方式に含まれない仮定

対総数がきわめて近い場合には，$|M| \leq 2E$ となる確率が高くなるので，適用できない．たとえば，誤差の範囲 $E$ を小さく設定して，この確率を小さくするすることは可能であるが，誤差が小さくなると，大きな重みを持つ投票者の投票内容を得ることができる確率が大きくなるといった問題が発生する．

誤差を含む集計結果を開示するのではなく，可決または否決のみを示すプロトコルを構築できれば，投票結果として公開する情報が最小になり，投票結果から個々の投票内容を類推することは最も困難になる．可決または否決のみを開示するプロトコルは，$M$ の値を開示しないということに関して信頼のおける集計者 $S$ の存在を仮定すれば，構成できる．

**プロトコル 6** 集計者 $S$ と閾値型 ElGamal 復号を行う集計者 $T_i$ との間の秘密通信路の存在を仮定し，集計者 $S$ が可決または否決であることのみを証明する．重みの総和を $w_T \ll q$ とする．プロトコル 2，3，4 に対して，集計処理を次のように変更する．

**集計** $(X, Y)$ を計算する．次に，集計者 $T_i$ は閾値型 ElGamal 復号を行うために必要な部分情報 $a_i \equiv X^{s_i} \bmod p$ を $S$ に秘密に送る．$S$ は集まった $a_i$ を用いて復号結果 $M$ を得る．$M \in \{0, \cdots, w_T\}$ であれば可決，$M \in \{-1, \cdots, -w_T\}$ であれば否決である．そこで，可決であるか否決であるかという 1 ビットの情報を公開する．次に $S$ は集計結果の正当性，すなわち $M$ が対応する区間に入っていることを，たとえば Boudot の手法[5] 等によって証明する（付録 A.2 を参照のこと）．∎

このプロトコルを使うと，投票結果に関する最小の情報のみを公開する投票方式が実現できる．

**定理 5** 管理者 $S$ が，$M$ の値を開示しないことに関して信頼できると仮定する．プロトコル 6 は

(1) 可決か否決かを誰もが確認でき，
(2) 投票結果に関する情報は可決または否決の 1 ビットのみ開示される．

**（証明）** プロトコル 6 の構成方法と Boudot の手法から明らかである．∎

なお，$S$ は，$M$ に関する情報を漏らすという不正はできるが，投票結果を左右すること（可決を否決と主張すること）はできない．

さて，重みの分布が超増加数列（例 4）の場合は，可決または否決という 1 ビットの情報のみから，重みが最大の投票者（例 4 の場合は $V_5$）の投票内容が分かる．これは，重みの分布が超増加数列の場合は，重みが最大の投票者以外の投票は投票結果に影響しないからである．重み付き投票の場合は，重みにより投票が結果にどの程度影響を与えるかという指標として Shapley-Shubik Index や Banzhaf Index が知られている[23]．そして，ある程度の重みを持つ投票者の投票内容が，投票結果のみから類推されることは防ぎえない．

## 8. ま と め

本論文では，重み付き投票の電子化方法について提案した．本論文で提案した方式は，従来の電子投票方式を重み付き投票へと拡張するものである．投票内容掲示型の電子投票方式の拡張の場合，重み情報がセキュリティ（特に無記名性）に悪影響を与えうることを示した．一方，投票結果掲示型（準同型暗号を利用）の電子投票方式の場合，重み付き投票への拡張が安全かつ効率良く実現できることを示した．結果を**表 2** にまとめる．

しかし，株主総会等では，議案数がたかだか 10 件程度であることから，一度に複数議案について投票できる効率の良い方式の実現が望まれる．それに適した FOO92[10] を応用したプロトコル 1 では安全な重みの分割が必要であり，その研究は今後の課題である．また，高速復号可能な準同型暗号[17] を利用した複数議案対応への拡張とその評価も今後の課題である．

本論文では，要件 C10 については，受動的攻撃しか考慮していない．投票者や管理者による能動攻撃に対する安全性の研究も今後の課題である．

**謝辞** 本研究に関し熱心に討論いただいた辻井研究室の鈴木昭正氏に感謝します．なお，本研究において，土井，辻井は TAO（通信・放送機構）の支援を一部受けました．

## 参 考 文 献


1) Abe, M.: Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers, *EUROCRYPT'98*, LNCS 1403, pp.437–447, Springer-Verlag (1998).
2) Abe, M. and Fujisaki, E.: How to Date Blind Signatures, *ASIACRYPT'96*, LNCS 1163, pp.244–251, Springer-Verlag (1996).
3) Abe, M. and Okamoto, T.: Provably Secure Partially Blind Signatures, *CRYPTO2000*, LNCS 1880, pp.271–286, Springer-Verlag (2000).
4) Benaloh, J. and Tuinstra, D.: Receipt-Free Secret-Ballot Elections, *Proc. STOC'94*, pp.544–553 (1994).
5) Boudot, F.: Efficient Proofs that a Committed Number Lies in an Interval, *EUROCRYPT 2000*, LNCS 1807, pp.431–444, Springer-Verlag (2000).
6) Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).
7) Chaum, D.: Blind Signatures for Untraceable Payments, *CRYPTO'82*, pp.199–203, Plenum Press (1983).
8) Cramer, R., Franklin, M., Schoenmakers, B. and Yung, M.: Multi-authority secret ballot elections with linear work, *EUROCRYPT'96*, LNCS 1070, pp.72–83, Springer-Verlag (1996).
9) Cramer, R., Gannaro, R. and Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme, *EUROCRYPT'97*, LNCS 1233, pp.103–118, Springer-Verlag (1997).
10) Fujioka, A., Okamoto, T. and Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections, *AUSCRYPT'92*, LNCS 718, pp.244–251, Springer-Verlag (1993).
11) 平井宜雄，青山善充，菅野和夫（編集代表）：六法全書平成 14 年版，有斐閣 (2002).
12) Hirt, M. and Sako, K.: Efficient Receipt-Free Voting Based on Homomorphic Encryption, *EUROCRYPT2000*, LNCS 1807, pp.539–556, Springer-Verlag (2000).
13) 石田夏樹，尾形わかは：準同型暗号系に基づいた分割可能な複数票電子投票方式，2003 年暗号と情報セキュリティシンポジウム（SCIS2003）予稿集，Vol.I of II, pp.197–202 (2003).
14) Kurosawa, K. and Tsujii, S.: A General method to Construct Public Key Residue Cryptosystems, *Trans. IEICE*, Vol.E73, No.7, pp.1068–1072 (1990).
15) 松尾真一郎，尾形わかは：分割可能な複数票電子投票方式，信学技報，ISEC2002-96, pp.1–6 (2002).
16) 岡本龍明, 山本博資：現代暗号, 産業図書 (1997).
17) Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, *EUROCRYPT'99*, LNCS 1592, pp.223–238, Springer-Verlag (1999).
18) Pedersen, T.: A threshold cryptosystem without a trusted party, *EUROCRYPT'91*, LNCS 547, pp.522–526, Springer-Verlag (1991).
19) 税所哲郎，齊藤泰一，土井 洋，辻井重男：1 人複数投票可能な電子投票に関する一考察，情報処理学会コンピュータセキュリティ研究会，CSEC17-3, pp.13–18 (2002).
20) 税所哲郎，齊藤泰一，鈴木昭正，土井 洋，辻井重男：準同型暗号を利用した 1 人複数投票可能な電子投票方式，コンピュータセキュリティシンポジウム 2002（CSS2002），pp.467–472 (2002).
21) Sako, K. and Kilian, J.: Secure voting using partially compatible homomorphisms, *CRYPTO'94*, LNCS 839, pp.411–424, Springer-Verlag (1994).
22) Sako, K. and Kilian, J.: Receipt-Free Mix-Type Voting Scheme, *CRYPTO'95*, LNCS 921, pp.393–403, Springer-Verlag (1995).
23) Taylor, A.D.: *Mathematics and Politics*, Springer-Verlag (1995).
24) 山口 浩，大久保美也子，北澤 敦，辻井重男：電子投票・アンケート諸方式に対する比較考察，情報処理学会コンピュータセキュリティ研究会，CSEC17-4, pp.19–24 (2002).
25) 会社四季報 2002 年 1 集新春号，東洋経済新報社 (2002).


## 付 録

### A.1 重み情報の漏洩に関して

重み非公開モデルにおける $l$ 人の投票者による重み付き投票を考える．プロトコル 4 を実行後，投票者とその重みの対応を無視できない確率で得ることができる（攻撃者が存在する）のならば，重み同一の通常の ElGamal 暗号ベースの匿名通信路（たとえば文献 1)）の匿名性を無視できない確率で破ることができることを示す．問題として投票者 $V_i$ と投票の組 $\{(V_i, E_i)\}$，それを Re-encryption してランダム置換を施したもの $\{E'_j\}$ が与えられるとする．そして，攻撃者に，重み付き投票の管理者 $W$ への入力データとして $\{(V_i, E_i)\}$ を，出力データとして $\{(E'_j, w_j)\}$ を入力するとする．すると，攻撃者が出力する投票者と重みの対応 $\{(V_k, w_k)\}$ より置換による対応 $\{(j, k)\}$ を無視できない確率で得ることができる．

### A.2 投票結果（可決か否決）のみを示す方法

投票結果 $M$ が 0 以上，または 0 未満であることを示す効率の良い零知識対話証明は，Boudot の手法[5]を利用して構成できる．これは，$Y \equiv h^{\alpha} G^{M} \bmod p$ が与えられたとき，$M$ の範囲（たとえば 0 以上であること）を効率良く証明する手法であるが，Boudot の手法を利用するためには，$M$，$\alpha$ の両方の値が必要である．しかし，プロトコル 6 では，ElGamal 暗号文の閾値復号より $M$ を得ることはできるが，$\alpha$ を知ることはできない．そこで，集計者 $S$ は暗号文を次のように変換する．

(1) 任意に $\beta$ を選び，ElGamal 暗号文 $(\bar{X}, \bar{Y}) = (g^{\beta} \bmod p, h^{\beta} G^{M} \bmod p)$ を公開する．

(2) $(X, Y)$ と $(\bar{X}, \bar{Y})$ が同一平文の暗号化であることを証明する．たとえば，$(X/\bar{X}, Y/\bar{Y})$ を公開掲示板上で集計者 $T_i$ に閾値復号してもらい，復号結果が $G^0 \equiv 1 \bmod p$ であることを示せばよい．

このようにして得た $\bar{Y}$ に対して，Boudot の手法[5]を適用すればよい．

(平成 14 年 11 月 29 日受付)
(平成 15 年 6 月 3 日採録)

**税所 哲郎**

平成 14 年中央大学大学院理工学研究科情報工学専攻博士後期課程修了．同年より中央大学研究開発機構客員研究員．研究テーマは，経営情報システム，金融情報システム，情報セキュリティ，情報社会論．博士（工学）．経営情報学会，日本社会情報学会，情報通信学会，情報文化学会，日本オペレーションズ・リサーチ学会，日本セキュリティ・マネジメント学会等の各会員．

**齊藤 泰一**

平成元年早稲田大学理工学部数学科卒業．平成 3 年早稲田大学大学院理工学研究科修士課程数学専攻修了．同年日本電信電話株式会社へ入社．平成 13 年中央大学理工学研究科情報工学専攻博士後期課程修了．博士（工学）．電子情報通信学会会員．

**土井 洋**（正会員）

平成 12 年岡山大学大学院自然科学研究科システム科学専攻博士課程修了．同年より中央大学研究開発機構助教授．暗号理論，情報セキュリティの研究に従事．博士（理学）．電子情報通信学会会員．

**辻井 重男**（正会員）

昭和 33 年東京工業大学工学部電気工学コース卒業．中央大学教授，東京工業大学名誉教授．工学博士．電子情報通信学会会長，総務省電波管理審議会会長等歴任．現在，IEEE Japan Council Chair．著書「暗号—ポストモダンの情報セキュリティ」（講談社メチエ選書),「暗号と情報社会」（文藝春秋社）ほか多数．