

携帯電話による小規模会議用の無記名電子投票

小林 哲二 *

日本工業大学

1. はじめに

投票は投票者（有権者）の名前と投票内容を結びつけるか否かによって、記名投票と無記名投票に分類できる。選挙は無記名投票である。従来、選挙のために、投票所における投票の電子化を行う無記名電子投票が地方自治体で実現されている。選挙のためのネットワーク利用型電子投票は日本では実施されていないが、暗号技術を用いてネットワーク利用型電子投票を実現する方式が提案されている[1],[2]。

選挙のためでなく、数十名～100名程度の小規模会議においても、意思決定のために記名投票、及び無記名投票が必要になる場合があり、これを電子化できれば、会議時間の短縮が可能になり、会議の構成員にとっては、各自の時間を会議以外に有効利用できるため、仕事の生産性向上になる。この論文では、携帯電話とWebを用いて、数十名～数100名程度の小規模会議用のネットワーク利用型無記名投票を実現することを検討する。

2. 提案する無記名投票方式

(1) 構成要素

携帯電話による無記名投票システムは、投票者の携帯電話機、及び電子投票の集計サーバで構成する。

構成メンバーである複数の投票者は、同じ会議場において携帯電話を使用する場合と、別の場所において各自が携帯電話を使用する場合がある。投票者のほかに、議題の提示等の議事進行を行う投票管理者が存在する。

(2) 前提条件

携帯電話による無記名投票で使用する携帯電話の通信事業者は、1つだけとする。

携帯電話機のブラウザからのアクセスで、電子投票の集計サーバに送信されるIPアドレスは、携帯電話事業者のサーバがランダムに付与している。このために、電子投票の集計サーバは、IPアドレスだけでは1つの通信事業者に加入している個々の携帯電話機を特定できない。

携帯電話機と集計サーバの間の通信は、通信網の暗号化によって、安全である。集計サーバは不正を行わない。

(3) 投票者と集計サーバ

投票者は、投票者IDと投票者パスワードを個別に所有する。集計サーバは1つの投票議題ごとに新規に議題IDを生成して発行できる。議題IDは議題ごとに異なる。1つの議題について、議題IDと議題IDパスワードは、全部の投票者に共通である。

(4) 投票手順

図1に、携帯電話による無記名投票の手順概要を示す。詳細を以下に示す。

ステップ1（投票議題の宣言）：

投票管理者は、{議題、議題ID取得開始時刻、議題ID取得締切時刻、投票開始時刻、投票締切時刻、投票完了者申告時刻、投票完了者申告締切時刻}を宣言する。

集計サーバは、議題IDと議題IDパスワードを、新規に生成し、保存する。

ステップ2（議題ID取得開始時刻）：

議題ID取得開始時刻になり、議題ID取得のためのログインが可能になる。

ステップ3（議題IDの取得）：

個々の投票者は携帯電話機のブラウザによって、投票者IDと投票者パスワードを入力し、集計サーバにログインする。集計サーバは、議題IDと議題IDパスワードを投票者の携帯電話機に送信する。

ステップ4（議題ID取得終了時刻）：

議題ID取得終了時刻になる。集計サーバは、議題IDを取得した投票者のリスト（一覧表）である議題ID取得者リストを作成する。

ステップ5（投票開始時刻）：

投票開始時刻になる。集計サーバは投票受付を開始する。

ステップ6（無記名投票の実施）：

個々の投票者は、携帯電話機から、投票者IDを入力せずに、議題IDと議題パスワードによってログインし、投票を行う。

ステップ7（投票締切り時刻）：

投票締切り時刻になり、集計サーバは投票を締切り、実際の投票数を求める。

ステップ8（投票完了者申告開始時刻）：

投票完了者申告開始時刻になり、投票を完了した投票者は全員、携帯電話機から投票者IDと投票者パスワードによってログインを行い、投票完了を集計サーバに通知する。

ステップ9（投票完了者申告締切時刻）：

投票完了者申告締切り時刻になる。集計サーバは投票を締切り、投票完了者リストを作成する。

ステップ10（議題ID取得者リストと投票完了申告者リストの完全一致性をチェック）：

An Electronic Secret Voting Method for Small Meetings

* Tetsuji KOBAYASHI

Nippon Institute of Technology

Dept. of Computer and Information Engineering,

4-1-1 Joho-Building, Gakuidai, Miyashiro-machi,

Saitama-ken, 345-8501 Japan

集計サーバは、議題 I D 取得者リストと投票完了申告者リストを照合し、不一致の場合は、この議題 I D の投票は全部無効にする。これらのリストが完全に一致した場合は、次のステップに行く。

ステップ 1 1 (実際の投票数と投票完了申告者数の完全一致性チェック) : 実際の投票数と投票完了申告者リスト中の投票者数が不一致であれば、この議題 I D の投票は全部無効にする。これらが一致した場合は、次のステップに行く。

ステップ 1 2 (投票結果集計と公開) :

投票結果を集計し、投票結果を公開する。

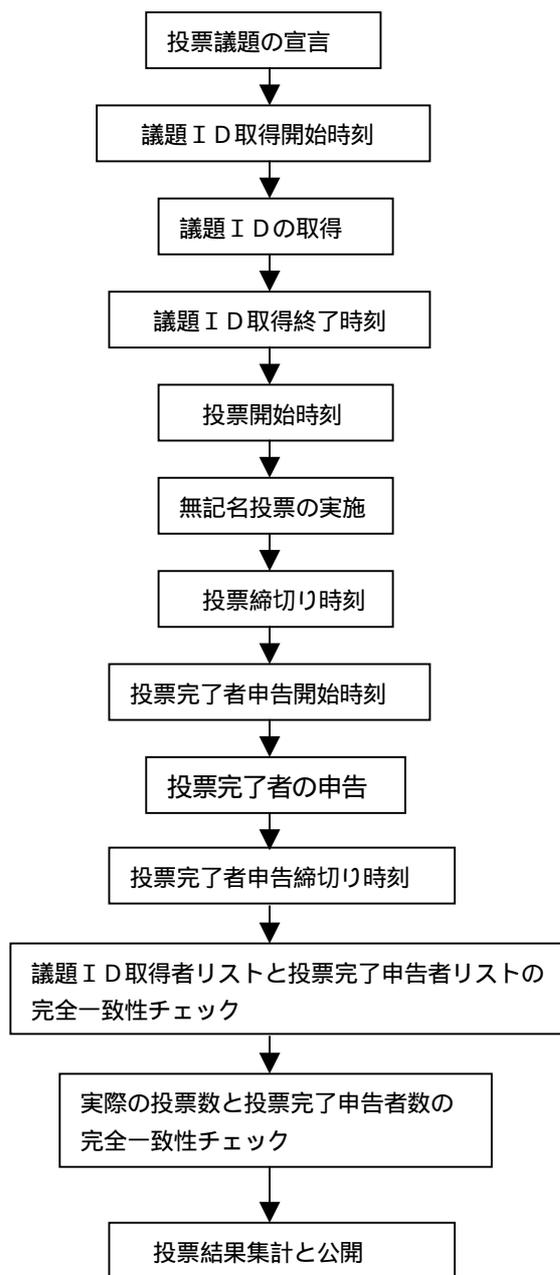


図 1 携帯電話による無記名投票の手順概要

3. 考察

(1) 投票結果の安全性

投票者の認証： 投票者 I D と投票者パスワードによって確保できる。

無記名性： 投票時には議題 I D、議題 I D パスワード、及び、投票内容しか入力しないことによって、無記名性を確保できる。

投票結果の正当性： 集計サーバのソフトウェアは、集計を行うだけであるので、バグがなければ投票結果の正当性を保証できる。

投票結果の検証： ログ情報として、議題 I D ごとに、投票受信時刻と投票内容を調べることによって、投票結果の集計の妥当性を検証できる。

投票の棄権数の検出： 議題 I D を取得した人が投票しなかった場合は、議題 I D 取得者リストと投票完了申告者リストが不一致になることで、検出できる。

多重投票の検出： 同じ投票者が複数回投票を行った場合は、実際の投票数と投票完了申告者数が不一致になることで、検出できる。

投票者の不正： 議題 I D を取得した人が投票を放棄し、且つ、投票完了申告を行った場合は、議題 I D 取得者リストと投票申告者リストが不一致になることで、検出できる。

(2) 他の電子投票方式との比較

無記名性について、他の電子投票方式との比較を行う。投票所における電子投票では、無記名性は、例えば、投票所入場券(投票所整理券)と引き換えに渡される投票トークン(例えば IC カード)を無記名にすること、及び、投票記録では投票者と投票内容の関係を無記名にすること等で実現できる。

暗号技術による電子投票の場合は、秘密鍵又は秘密情報を知っている人は、理論的には、すべての秘密鍵や秘密情報を集めれば、投票者の投票内容を特定できる場合が多い。

この論文で提案の無記名投票方式では、投票に関する秘密鍵や秘密情報はないため、前提条件の下では、集計サーバおよび投票管理者でも、投票内容と投票者を関連付けることができない。

(3) 記名投票との関係

提案の無記名投票方式において、記名投票は、投票時に投票者 I D も入力し、且つ、集計時に投票内容を公開することによって実現できる。

4. むすび

携帯電話による小規模会議用の電子投票方式を考察した。プロトタイプを試作を検討中である。

参考文献

- [1] 宮内宏, 尾花賢, 森健吾: 電子投票の実現, 電子情報通信学会誌, Vol. 86, No.5, pp.331-336 (May 2003).
- [2] 藤岡淳, 阿部正幸: 電子投票に対する情報セキュリティからのアプローチ, 電子情報通信学会誌, Vol. 86, No. 1, pp.33-35 (Jan. 2003).