

携帯電話による無記名電子投票についての検討

An Electronic Secret Voting Method using Cell Phones

小林 哲二 *

Tetsuji KOBAYASHI

1. はじめに

投票は投票者（有権者）の名前と投票用紙記載内容を対応付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。投票所における無記名電子投票が地方自治体で実現されている[1]。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、実現する方式が提案されている[2], [3]。選挙のためでなく、数10名～100名程度の小規模会議においても、意思決定のために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ので、仕事の生産性向上になる[4]。この論文では、小規模会議用のネットワーク利用型無記名電子投票を、プライド署名[5], [6]と携帯電話などを利用して実現することを検討する。

2. 無記名電子投票の比較

表1に、無記名投票の比較を示す。小規模会議用無記名電子投票は大規模な電子投票と顕著な相違がある。

表1 無記名投票の比較

区分 比較項目	小規模会議用の 無記名電子投票	国や自治体の選挙の 無記名投票
投票者数	数10人～100人	数100人～数千万人
投票内容	議案への賛否	立候補者名
投票者の不正	不正は無い場合 が多い。	不正が発生する可 能性がある。
開票	即時	即日、又は翌日
投票場所	会議場	投票所
投票事項の公表 または公示	即時	投票日の数週間前
投票所入場券、又 は投票所整理券	不要	郵送
投票所における 本人確認	必要	必要
投票管理者	会議の議長	選挙管理委員会、及 び投票所立会人
不在者投票	無し	有り

3. 小規模会議用の無記名電子投票

3.1 構成要素

図1に、小規模会議用無記名電子投票における構成要素の概要を示す。構成員である複数の投票者は、同じ会議場に居て携帯電話を使用する場合と、別の場所に居て各自が携帯電話を使用する場合がある。投票者のかたに、議題の提示等の議事進行を行う議長（投票管理者）が存在する。

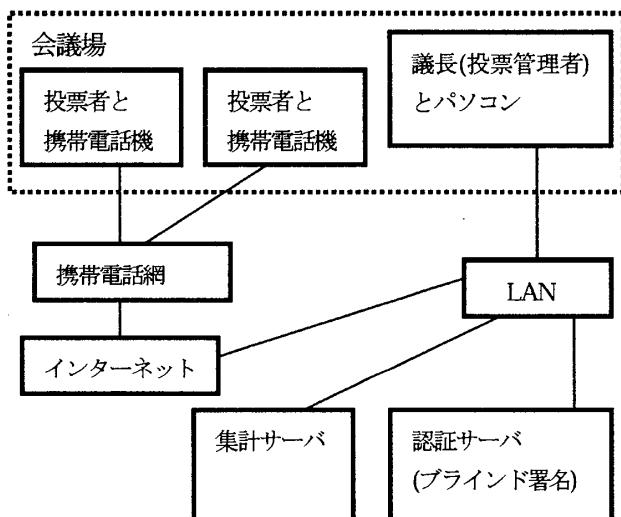


図1 小規模会議用無記名電子投票の構成要素の概要

3.2 前提条件

(1) 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。

(備考：携帯電話機のプ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。したがって、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。複数の携帯電話事業者の携帯電話機を利用可能にするためには、サーバに通知される携帯電話機の発信元アドレスが、通信事業者で共通化されている必要がある。)

(2) 1つの投票者集合で使用する携帯電話の機種は1つとする。

(備考：プロトコルのヘッダ情報で、機種が通知される場合がある。この制約をなくすには、機種を通知しないオプションを携帯電話機搭載ソフトで指定できる必要がある。)

(3) 携帯電話機と集計サーバ、及び認証サーバの間の通信は、通信網の暗号化と認証によって、安全である。

(4) 集計サーバと認証サーバの結託による不正はない。

* 日本工業大学工学部情報工学科、埼玉県宮代町学園台4-1-1

Nippon Institute of Technology,

Dept. of Computer and Information Engineering,

4-1-1, Gakuendai, Miyashiro-machi, Saitama-ken, 345-8501 Japan.

3.3 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。

3.4 投票手順

携帯電話とブラインド署名による小規模会議用無記名電子投票の手順概要を示す。

ステップ0 (初期設定) : 投票管理者は、投票管理者 ID と投票管理者 ID パスワードを集計サーバに設定する。

認証サーバは、ブラインド署名用の秘密鍵と公開鍵を生成し、公開鍵を公開する。

ステップ1 (投票議題の宣言) : 投票管理者（議長）は、投票者に {議題、議題 ID 取得の開始時刻・終了時刻、ブラインド署名取得の開始時刻・終了時刻、投票の開始時刻・終了時刻} 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 取得のためのアクセスが可能になる。

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、集計サーバにアクセスする。

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。

ステップ5 (ブラインド署名取得開始時刻) : 認証サーバはブラインド署名の受付を開始する。

ステップ6 (投票用紙データへのブラインド署名発行) :

個々の投票者は、携帯電話機から、投票者 ID と投票者パスワード、および議題 ID と議題 ID パスワードによって認証サーバにアクセスし、投票用紙電子データに投票内容 A を記入して、乱数を乗じる等のブラインド署名作成に必要な処理を行ったデータを認証サーバに送信して、ブラインド署名を依頼する。

認証サーバは依頼されたデータにブラインド署名を行って、投票者に返却し、投票者はブラインド署名の正当性を検証する。

ステップ7 (投票用紙データへのブラインド署名発行終了) :

投票用紙へのブラインド署名発行終了時刻になり、認証サーバはブラインド署名発行を終了する。

ステップ8 (携帯電話の匿名性を利用した無記名投票の実施) :

投票者は、投票者 ID を入力せずに、議題 ID と議題パスワードでログインし、投票内容 B とブラインド署名の付加された記入済み投票用紙データを集計サーバに送信する。

集計サーバは、投票内容 B とブラインド署名（ブラインド署名取得時の投票内容 A を含む）によって、ブラインド署名の正

当性を検証する。

ステップ9 (集計サーバにおける集計) : 集計サーバは、有効な全部の投票について、投票内容 B を集計し、集計結果、および有効な投票内容 B とそのブラインド署名を、全部について、同時公開する。

ステップ10 (投票者による検証) : 投票者は、集計サーバの公開する有効な投票内容とそのブラインド署名が、自己の投票内容およびブラインド署名と一致することによって、自己の投票が集計に含まれていることを確認する。もしも含まれていない場合は、集計サーバに全員の再投票を申請する。

3.5 考察

投票の安全性などについての考察を以下に示す。

- (1) 投票者の正当性認証：投票者 ID と投票者パスワードによって確保できる。
- (2) 無記名性：投票時には議題 ID、議題 ID パスワード、投票内容 B、およびブラインド署名しか入力しないことによって、無記名性を確保できる。
- (3) 投票結果の正当性：集計サーバは、集計を行うだけであるので、投票結果の正当性を保証できる。
- (4) 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、投票時のブラインド署名の重複によって、検出できる。
- (5) 自己の投票内容：投票者によって検証が可能である。
- (6) 認証サーバが、ブラインド署名を作成時の情報を保存すると認証サーバの情報と集計サーバの情報から、投票が匿名通信路で実施されても、誰の投票かが分かり、かつ投票内容と対応づけられるので好ましくないため、認証サーバでは、ブラインド署名を作成時の情報を廃棄する。
- (7) 認証サーバがブラインド署名作成時の投票内容 A と、投票者が集計サーバへの投票実施時の投票内容 B が異なっている場合は、集計サーバにおけるブラインド署名の検証が不一致になるので、無効投票になる。

4. むすび

小規模会議用の無記名電子投票の処理を、ブラインド署名と携帯電話の匿名性などによって実現することを考察した。今後は、代替方式との比較や改良の検討などを行う。

参考文献

- [1] <http://www.evs-j.com/>
- [2] 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).
- [3] 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).
- [4] 小林哲二：携帯電話による小規模会議用の無記名電子投票、情報処理学会 67 回全国大会講演論文集、pp. 3-395～3-396, (March 2005).
- [5] 岡本龍明、山本博資：現代暗号、産業図書、(1997).
- [6] 電子情報通信学会：情報セキュリティハンドブック、(2005).