EDD-21-063

電子メールと入力フォーム集計を用いて 匿名性と有効性を実用レベルで実現する簡易な電子投票方法の提案

平野　拓一*（東京都市大学）

Practical and Simple Electronic Voting Method Ensuring Anonymity and Validity With Practical Level Using Email and Input Form Aggregation

Takuichi Hirano*, (Tokyo City University)

Simple procedure for anonymous electronic voting using e-mail and input form aggregation is proposed. It is possible to use highly automated electronic system, but costs for system development and service usage are very high. The cost to verify the system is also very high. In this report, the author proposes a procedure to guarantee the anonymity and effectiveness of voting by using random number keys and data distribution, provided that the voting manager can be trusted.

キーワード：電子投票，匿名性，電子メール，入力フォーム集計，簡易
(Keywords, Electronic voting, Anonymity, E-mail, Input form aggregation, Simple)

1. まえがき

選奨投票や委員投票を行う際、多くの場合は秘匿性を確保した投票が望ましい。秘匿性を保証する投票には、投票者が集まって無記名で投票箱に投票用紙を入れる方法や投票権者に往復はがきを郵送して無記名で返信する方法が一般的に用いられる方法である。

しかしながら、人が移動したり郵便物を郵送したりすることはコストがかかり、インターネットが普及した現代では WEB や電子メールを用いた方法が渇望されている[(1)~(4)]。匿名電子投票を実現するために、ブラインド署名[(5)(6)]などの技術が開発されてきた。電子決済、電子商取引、オンライン予約など多くの決済やサービスが公開鍵暗号方式[(7)~(9)]の発明により高いセキュリティーで実現されているが、インターネットを利用した国政選挙は 2007 年にエストニアが世界で初めて行ったが、現在もセキュリティーに多くの懸念が持たれ[(10)]世界で普及していない。これは、記名電子投票の実現は容易であるが、無記名（匿名）電子投票の実現には多くの課題があることが理由である。

国政選挙のような大規模で非常に高い信頼性とセキュリティーが要求されるケースのみならず、研究会の論文賞・優秀論文発表賞の投票のような比較的少人数の投票で匿名性を保証した電子投票を行いたいケースもある。そこで、本稿では、セキュリティーの要求を現実的なレベルまで許容することで、匿名電子投票を実現する方法を提案する。提案する手法では現在普及している電子メールと個人でも簡易に構築できる入力フォーム集計を用いた簡易な手段を用いる。

2. 提案手法

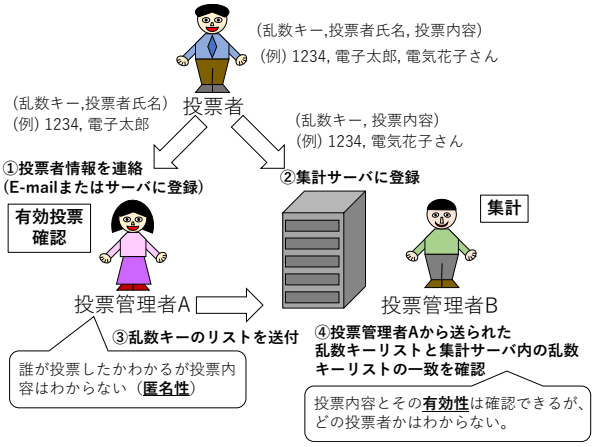

図１　匿名電子投票の手順

Fig. 1.　Procedure of Anonymous Electronic Voting.

図１に匿名電子投票の手順を示す。ここで扱う投票システムの要求としては、匿名性（誰による投票内容かわからないようにする）、有効性（投票権のある人による投票か確認。二重投票を排除）が求められる。これらの要求を満たすた

めに、投票者が適当に決めた乱数キーを用いて情報を紐付けると同時に、同時に知られたくない情報を分散して投票内容の匿名性と有効性を実現する。

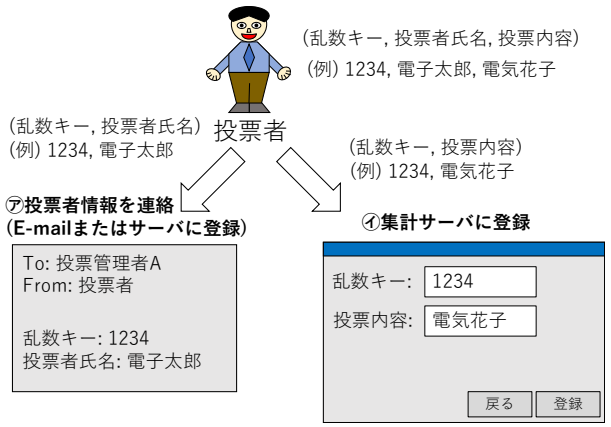

図 2　投票者の作業内容
Fig. 2.　Work Content of Voter.

① 投票者は自分で決めた乱数キーと投票者の氏名を図 2㋐のように投票管理者 A に電子メールで送る（入力フォーム集計でも構わないが、本人確認には注意を要する）。ここで、投票管理者 A は投票資格があるかどうか、また二重投票していないかどうか確認し、乱数キーの有効性を判断する。乱数キーは、全投票者に対して必ずしも一意である必要はない。同じ乱数キーがあっても投票管理者 A 側と投票管理者 B 側で数が一致すればよいからである。全投票者に対して一意に乱数キーを割り当てたい場合は、すでに登録された乱数キーがある場合は変更させたり、投票者が乱数を登録する代わりに投票管理者 A がハッシュ関数で乱数キーを生成したり、投票管理者 A が事前に乱数キーを投票者に割り当てたりする方法で実現可能である。

② 投票者は①と同じ乱数キーを用いて、乱数キーと投票内容を図 2㋑のように入力フォーム集計サーバに登録する。ここで、電子メールによる連絡が使えないのは、電子メールを用いた場合はアドレスで投票者と投票内容の対応付けが得られてしまうからである。

③ 投票管理者 A は有効な投票者の乱数キーのリストを投票管理者 B に送付する。投票者の氏名は送付しない。

④ 投票管理者 B は集計サーバの投票内容を集計する。その際に、③で投票管理者 A から届いた乱数キーのリストと集計サーバの乱数キーの対応を確認することで投票の有効性を確認できる（有効であることは事前に投票管理者 A が確認している）。投票管理者 B は集計作業において誰が投票した内容であるかわからない（匿名性）。

3.　匿名性・有効性・信頼性・透明性に関する条件

本節では匿名性・有効性・透明性実現のための条件について述べる。

3.1　匿名性

ネットワーク通信の傍受対策などは RSA 暗号など[7]~[9]を用いるものとする。投票管理者 A が乱数キーと投票者氏名の対応情報を漏らさければ、投票内容の匿名性を確保することができる。

3.2　有効性

投票の有効性は投票管理者 A が電子メールアドレス（場合によっては携帯電話番号）など、一意に投票者と紐付いた連絡方法で実現できる。また、無効投票や二重投票も確認できる。

3.3　信頼性・透明性

本手法は、少人数（10～20 名程度）の信頼できるメンバー同士による投票で、投票管理者 A および投票管理者 B は人間が行うことを想定している。投票管理者 A および投票管理者 B の処理はプログラムを構築して自動化することも可能ではあるが、コストがかかる上に動作の検証が必要となる。投票管理者 A および投票管理者 B を人間が行う場合、それぞれ 1 名で行うと不正しやすく透明性が低くなる。そこで、投票管理者 A,B それぞれの役割を複数名にすることで、信頼性・透明性をより高めることができる。ただし、あまり多くの人数を割り当てると、例えば投票管理者 A の誰かが、例え間違いであっても投票者を特定できる乱数キーと投票者氏名の組み合わせを投票管理者 B に送信してしまう可能性があるので、実用上は信頼できる 2～3 名程度がよいと考える。人間が行うと完全な信頼性・透明性は保証できないが、より信頼性の高い大規模な投票に適用する場合はプログラムによる自動化で対応することが可能である。

4.　むすび

電子メールと入力フォーム集計を用いた実用的なレベルで簡易な匿名電子投票方法の手続きを提案した。投票管理者の人間が信頼できるという前提で投票の匿名性、有効性を保証する手順を示した。本手法は現在普及している電子メールと個人レベルでも簡易に構築できる入力フォーム集計を用いて実現可能な実用的で簡易な匿名電子投票方法であり、研究会の選奨投票など比較的少ない投票者数の場合に有効な方法である。

文　　献

（1） 岡本学, 田中良明, “匿名配布を用いた無記名電子投票,” 電子情報通信学会論文誌 A, vol.J87-A, no.7, pp.958-966, July 2004.

（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. 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. 著書名・著書名・著書名：「タイトル」, 雑誌名, Vol.巻数, No.号数 pp.ページ数（発行年）

（4） J. Epstein, “Electronic Voting,” in Computer, vol. 40, no. 8, pp. 92-95, Aug. 2007.

（5） D. Chaum, “Blind signatures for untraceable payments,” In: D. Chaum, R.L. Rivest, A.T. Sherman (eds) Advances in Cryptology. Springer, Boston, MA., 1983.

（6） D. Chaum, “Security without identification: transaction system to make big brother obsolete,” Comm. of the ACM, vol.28, no.10, pp.1030-1044, Oct. 1985.

（7） W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Trans. Information Theory, vol.22, no.6, pp.644-654, November 1976.

（8） R.L. Rivest, A. Shamir and L. Adelman, “A Method for Obtaining Digital Signature and Public-key Cryptsystems,” MIT-LCS-TM-082, 1977.

（9） W. Diffie, “The first ten years of public-key cryptography,” in Proc. IEEE, vol.76, no.5, pp. 560-577, May 1988.

（１０） Independent Report on E-voting in Estonia
https://estoniaevoting.org/