ネットワークを利用した無記名投票システムの開発

4G－8

花田 泰紀　乃村 能成　程 京徳　牛島 和夫
九州大学

1　背景と目的

近年の計算機技術の進歩によって、電子化された情報を扱うことが容易になってきている。一方、インターネットの普及に伴って、情報の伝達や共有が世界的規模で可能になってきている。

現在、選挙での投開票では、集計などの作業を除いて電子化されておらず、人間の労力によるところが大きい。そこで本研究では、投票から開票、集計までを一貫して電子化して行うことにより、人間の労力の軽減と投票の利便性の向上に繋がる、ネットワークを利用した無記名投票システムを開発する。

2　用語・概念の定義

ここで無記名投票に関する用語・概念を定義する。

有権者: 選挙に参加する権利を有する他から識別可能な主体。

選定情報: 有権者によって選定された候補に関する情報。

投票: 有権者によって行われる行為で、選定情報を伝えること。

電子投票用紙: 有権者が投票の際に、選定情報を知らせる媒体。

投票者: 有権者のうち、電子投票用紙を取得して、投票を行うことで選定情報を伝えた者。

選挙結果: 投票によって得られたすべての選定情報を処理して得られたもの。

選管: 選挙を遂行し、投票者から選定情報を受け取ることで、選挙結果を生じさせる組織。

さらにここで定義した用語を用いて、無記名投票を定義する。

- 選管は、投票者から投票によって渡された選定情報だけを受け取る。
- 投票によって渡された選定情報から、その投票を行った投票者を特定することは、誰にもできない。

上に示した条件を満たす投票を無記名投票として定義する。

3　設計

これまでに定義した用語と概念を基に、ネットワーク上での投票システムの設計を行う。

システムは、無記名性を保証しなければならない。また、投票に参加する人が有権者であることと、投票が投票者によって行われていることを、認証によって確認する必要がある。

無記名投票システムを設計する上での、制約条件を考える。

- 電子投票用紙を請求する段階では、誰によって請求されたのかを、選管は知らなければならない。また、電子投票用紙は、有権者１人に対して１度しか発行されない。
- 一旦発行された電子投票用紙には、有権者を特定する情報が含まれてはならない。また、一度投票に使われた電子投票用紙は、破棄されなければならない。
- 電子投票用紙は、簡単に偽造されてはならない。また、既に発行された電子投票用紙と同じ物が発行されてはならない。

Development of a Secret Voting System on Computer Network
Yasunori Hanada, Yoshinari Nomura, Jingde Cheng and Kazuo Ushijima
Dept. of Computer Science and Communication Engineering, Kyushu University

つまり、投票に対する認証を、正しい電子投票用紙を用いたものであるかの認証にすることで、有権者についての情報が含まれない電子投票用紙から、有権者を特定することはできない。このようにすることで、無記名性を保証している。

計算機上に実装する上では、無記名性を保証できなくさせる情報を、計算機に記録されないようにする必要がある。このため、投票を受けつけるサーバを2台構成とすることにし、電子投票用紙の発行を行う「選管サーバ」と、電子投票用紙を用いた投票を行う「投票サーバ」とした。サーバを2台とすることで、それぞれのサーバで記録されている情報が解析されたうえに、その相関関係がはっきりしない限り、無記名性が失われることはない。

このようにして設計された投票システムの構成は図1のようになっている。図中、投票者1、投票者2、…、投票者nは、任意の投票者が地理的に離れた場所から、任意の計算機を用いて投票に参加できることを示している。

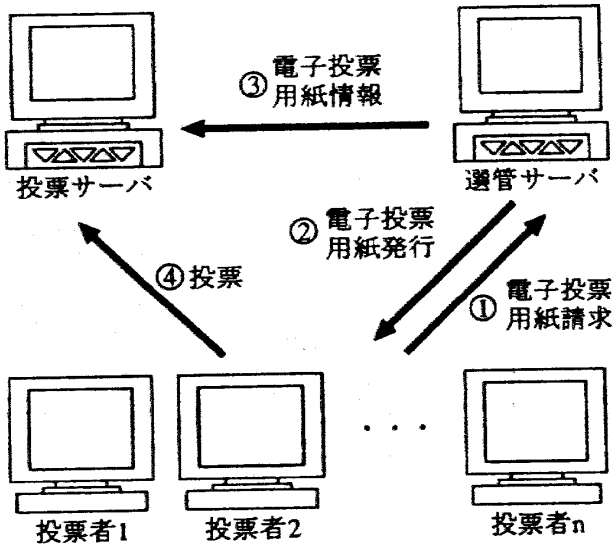

図1: 投票システムの構成図

以下で、設計した投票システムの説明を行う。

1. 電子投票用紙請求
   有権者は、選管に電子投票用紙を請求することにより、選挙に参加することができる。また、ここで有権者であることの認証を行う。
2. 電子投票用紙発行
   電子投票用紙請求が正しく行われたときには、電子投票用紙を発行する。
3. 電子投票用紙情報
   電子投票用紙の発行が正しく行われたときには、選管サーバから投票サーバに電子投票用紙情報が送られる。電子投票用紙情報には、電子投票用紙が発行されたという情報だけが含まれていて、誰に対して発行された電子投票用紙なのかは、わからなくなっている。
4. 投票
   電子投票用紙を用いて、投票を行う。

4 実装

構築には、FreeBSDの動作している2台のPCを用いた。利用者の利便を考慮して、Webベースの実装とした。Web上での処理にはPHP/FIを、データの管理にはpostgresを用い、それぞれのサーバでpostgresとPHP/FIを利用できるようにした。

有権者は、以下の手順で投票を行うことができる。

1. 認証サーバで、登録されている有権者名とパスワードを入力して、電子投票用紙を取得する。
2. 投票サーバで、取得している電子投票用紙と、候補を選定することで投票を行う。

Web上での実装のため、リンクをたどっていくだけで2つのサーバに接続されるので、サーバを2つに分けることでの利用者の利便は、サーバが1つであるときと、それ程変わらないと考えている。

5 今後の課題

- 今回構築したシステムでは、有権者を特定する際に、有権者が誰なのかを事前に登録しておかなければならないが、登録を簡便に行う手段を用意していない。
- 発行された電子投票用紙を無くしたときに、再発行することができない。また、無くさないようにする仕組みもない。
- Web上での実装のため、過負荷に対抗することができない。
- 現在、想定しているのは小規模の選挙だけで、2つのサーバだけで処理できる範囲に限られる。

これらの問題の解決をこれからの課題としたい。