Vol.2014-IS-127 No.1
2014/3/17

日本における安全なインターネット投票の導入に向けて

久保田 貴大[1,a)]

概要：選挙における投票を電子化することには以前から関心がもたれており, 実際に, 地方選に電子投票機が用いられたこともあった. 2013 年のネット選挙解禁とも相まってインターネットでの投票にも関心が高まっている. 本研究では, 日本におけるインターネット投票の実現の可能性や, その制度の導入までの課題について, 安全性, コスト, 法制度の三つの観点から調査・検討した. 特に, JCJ-Civitas 投票プロトコルを基にした, 「攻撃者が投票者と物理的に同じ場所にいて投票者の端末を監視する」という攻撃に対処するようなプロトコルを提案する.

1. はじめに

選挙における投票を電子化することには以前から関心がもたれており, さらに, 2013 年のネット選挙解禁とも相まってインターネットでの投票にも関心が高まっている. インターネット投票が導入されるためには, それが安全に行えることと, 導入によりコストが削減されることが必要である. 本研究では, 以下の 3 点について論じる.

(1) 従来方式とインターネット投票方式を併用すべきである. 理由は以下の 2 点である.
- すべての投票者がインターネットを使えるとは限らない.
- インターネット投票では, 攻撃者が投票者と物理的に同じ場所にいて, 投票者の端末を監視する可能性が常にある. この根本的な問題に対処するひとつの方法は, 「インターネット投票をしても, そのあと投票所で投票すると, インターネット投票が無効化され, 投票所での投票だけが数えられる」ようにすることである.

(2) 従来方式とインターネット投票方式を併用でき, かつ安全なプロトコルがある. ただし, 大規模な選挙には, 効率上の問題から適用は難しい.

(3) 単純計算により, インターネット投票によって削減されるコストを見積もった. 国政選挙ならば, 投票所および開票所の人件費の削減によって, コストが 100 億円規模で削減されるという見積りである.

[1] 東京大学大学院情報理工学系研究科コンピュータ科学専攻 113-0033 東京都文京区本郷 7-3-1
[a)] takahiro.k11_30@is.s.u-tokyo.ac.jp

1.1 諸外国でのインターネット投票

湯淺は, エストニアにおけるインターネット投票制度について調査と考察を行った [5]. エストニアのインターネット投票は, 再投票が可能である. さらに, 投票所でも再投票が可能であり, 投票所での投票は最終のものとなる. しかし, エストニアの投票プロトコルでは, そもそも検証可能性を視野に入れたものではない. 検証可能性があると, 集計の信頼度が従来方式よりも高まる. 本研究では, 検証可能性も成り立つようなプロトコルを考える.

1.2 関連研究

攻撃者が投票者と物理的に同じところにいて, 投票者の端末を監視するという危険性に対処するため, Clark らは偽のパスワードを設定するという方法を提案した [1]. この攻撃を受けている投票者は, 投票クライアントにパスワード入力を求められたとき, 偽のパスワードを入力する. パスワードが偽であっても, 投票クライアントには真のパスワードを入力したときと同じ画面が表示される. そのため, 攻撃者は何の情報も手に入れられない. この方法は, 本研究の方式に追加できる可能性がある.

2. インターネット投票プロトコル

2.1 安全性の定義

暗号理論では, インターネット投票プロトコルの安全性として, 以下の性質が挙げられている [3], [4].

(1) 匿名性... 自分の投票内容を他人に知られない.

(2) 公平性... 投票の結果は開票時までわからない. 投票の途中結果が露呈しないということである.

(3) 適格性... 有権者しか投票できない.

(4) 二重投票の防止
(5) 頑健性... 投票プロトコルの実行を妨害されない.
(6) 個別検証可能性... 投票のデータが公開掲示版に記録され, 有権者は自分の投票のデータが公開掲示版にあることを確認できる.
(7) 総合検証可能性... 公開掲示板のデータから, 開票と集計が正しく行われていることを誰もが確認できる.

JCJ-Civitas [2] は, 匿名性をさらに強めた耐買収性という以下の性質を満たす.

- 耐買収性... 攻撃者はリモートで有権者と通信するとする. 攻撃者が指定した秘密鍵や乱数を有権者に使うように指示しても, 匿名性が成り立つ. 耐買収性が成り立つならば, 有権者がこの指示に従ったかどうかもわからない. 攻撃者が, 有権者に選挙に参加しないよう指示しても, 有権者がその指示にしたがったかどうかわからないという安全性も含める.

2.2 提案プロトコル

JCJ-Civitas [2] は, 暗号理論的な安全性を満たすが, 以下の問題点がある.

(1) 同じ人が何度も投票できてしまうため, DoS 攻撃に弱い.
(2) 冒頭でも述べたように, 攻撃者が投票者と物理的に同じ場所にいて, 端末を監視するという攻撃への対処がない.

よって, 本研究では, JCJ-Civitas プロトコルの改変版を提案する. このプロトコルでは, 投票所においてクレデンシャルを確認することで, DoS 攻撃に対処する. また, 端末を監視された場合, 投票者は投票所でクレデンシャルを照合し, 端末を監視された投票を失効させるようになっている. また, これにより「インターネット投票を投票所での投票によって上書きする」ということが実現できる.

3. 法制度

前項の暗号プロトコルを用いて, コスト削減を目標とした, 投票所をできるだけ減らす案を考える. 各番号は制度の大まかな内容で, その下の箇条書きは備考である.

(1) 住民基本台帳カード (住基カード) に, 投票プロトコルで使う認証用と暗号化用の秘密鍵が格納される. 20 歳以上の国民には, 住基カードの所持が義務付けられる.
  - 本来, 住基カードは電子政府・電子自治体の基盤となるように作られた制度であった[*1]. 実際, 住基カードを利用して, 本人確認を必要とする行政手続のインターネット申請が可能である. ただし, 可能な手続きは納税などごく限られたものである. インターネット投票は, 現在の利用法の拡張であると考えることができる.
  - 住基カードを持っている人に限り, インターネット投票ができる.
  - 住基カードの盗難・紛失に備え, 本人確認用の秘密鍵には PIN が設定されているとする.
(2) 地方選挙・国政選挙のいずれにおいてもインターネット投票が可能である.
(3) 有権者は, ソフトウェアを認証されたウェブサイトからダウンロードして使う.
(4) 選挙告示日から, 開票日の前日まで, インターネット投票が利用できる. また, 期日前投票所で, 従来方式の投票ができ, ここでの投票はインターネット投票を上書きするものである. 選挙当日にも, 投票所で従来方式の投票ができる.

4. コスト見積り

国政選挙の予算から, インターネット投票の導入により削減できるコストを見積もる. 選挙執行委託費は, 国会議員の選挙等の執行経費の基準に関する法律によって決まっている. 国政選挙の予算額の推移は以下のようになっている. [*2]

- 平成 16 年度 参議院議員通常選挙 570 億円
- 平成 17 年度 衆議院議員総選挙 698 億円
- 平成 19 年度 参議院議員通常選挙 526 億円
- 平成 21 年度 衆議院議員総選挙 620 億円
- 平成 25 年度 参議院議員通常選挙 448 億円[*3]

開票区と投票区の制度は以下のようになっている.

- 開票区は原則, 一つの市区町村である.[*4] ひとつの開票区には, ひとつの開票所が設けられる.
- 投票区は各市区町村の選挙管理委員会が決める. ひとつの投票区にはひとつの投票所が設けられる.

平成 19 年度参院選の予算額の内訳では, 選挙当日の投票所, 開票所経費が 255 億円とされている. そのうち投票所経費は 197 億円[*5]である. 1 投票所のための予算は市, 区, 町, 村の種別と投票区における選挙人の人数によって決まっており, 主に人件費である. 例えば, 市において, 休日設けられる投票所経費の基本額は, 下の表のようになる.

表を見てもわかるとおり, この制度では, 選挙人の数を固定したとき, 投票所の数を少なくして, ひとつの投票所あたりに受け付ける選挙人を多くした方が経費を節約できるようになっている.

[*1] 総務省 住民基本台帳カード総合情報サイト http://juki-card.com/about/index.html
[*2] 平成 21 年度予算執行調査の調査結果の概要, http://www.mof.go.jp/budget/topics/budget_execution_audit/fy2009/sy210703/2107d_06.pdf
[*3] 国会議員選挙経費基準法が 2013 年 4 月に改正され, 予算が減らされたため. 改正前の計算だとすると, 514 億円であった.
[*4] 二つの小選挙区に分かれているときは, それぞれが開票区となる
[*5] 期日前投票所の経費は含めない.

選挙人の数	投票所経費の基本額
500 人未満	190,711 円
500 人以上 1000 人未満	203,793 円
1000 人以上 2000 人未満	307,498 円
2000 人以上 3000 人未満	314,298 円
3000 人以上 5000 人未満	355,103 円
5000 人以上 10000 人未満	465,573 円
...	...

4.1 投票所・開票所経費の削減

インターネット投票制度においては, なるべく多くの人がインターネット投票を利用したほうがコストが削減される. 削減の大きさを, 小さめに見積もるため, インターネット投票制度下において, 投票者のうち 70 パーセントがインターネットを利用するとする. 平成 25 年度のインターネットの普及率は 79 パーセントであるため, 将来インターネットの普及が進むことを考慮すると, 低めの見積りであるといえるだろう. 他方, 30 パーセントが投票所で投票をするとし, 人数に比例した費用がかかると仮定する. そして, 現在, 期日前投票の利用率が 18 パーセントを超えていることから, 期日前投票費用 26 億円から, 30 パーセントの人数のための費用を計算すると, 26 億円 $\times \frac{30}{18}$ =43.3 億円となる. また, 開票所にも人数に比例した費用がかかるとすると, 開票所費用は 58 億円 $\times \frac{30}{100}$ =17.4 億円となる.

4.2 インターネット投票のための費用

JCJ-Civitas の実験結果によると, 3.0 GHz Xeon プロセッサ, 1GB RAM, 1Gb LAN のサーバに対し, Emulab クライアントを用いてシミュレーションを行った結果, 10 時間以内に処理できたのが 1000 人という結果であった. 国政選挙の投票者を 7000 万人とすると, 7 万台のサーバが必要であり, このままでは実現することは難しい. ただし, 費用の点からのみ以下の考察を行う. たとえば 3.1 GHz Xeon プロセッサ, 4GB SDRAM 2 枚というマシンで, 2013 年 11 月における価格が 80550 円というものがあった. 仮にこのマシンを 7 万台購入したとしても, 70 億円である.

また, 選挙期間 17 日に予備日 3 日を加えて 20 日間として, 1 選挙区を 10 人から 20 人の技術者が担当するとすると, 合計約 800 人の技術者が必要となる. 技術者 1 人の人件費を 1 日 40,000 円とすると, 6.6 億円となる.

4.3 コスト見積りのまとめ

投票所・開票所経費以外の条件は同じとする. ここまでの見積りによると, 投票所経費, 開票所経費, サーバマシン経費, 技術者人件費の合計は 143.3 億円となる. 従来の投票所・開票所経費は 255 億円であったので, 111.7 億円の削減になっている.

5. 結論

本研究では, 投票所方式とインターネット投票方式を併用できるような投票プロトコルを提案した. また, 単純計算によってコストを見積もると, 投票所・開票所経費が 100 億円以上節約されるということであった. ただし, JCJ-Civitas の効率上の問題から, 直ちに実現することは難しい. 今後の課題としては, 本研究の安全性を満たす投票システムの実験による評価, 提案した投票プロトコルの安全性を暗号学的に厳密に解析すること, 投票者のコンピュータ環境の安全性についての検討, 国政選挙だけでなく他の条件におけるコスト見積りなどが挙げられる.

参考文献

[1] Jeremy Clark and Urs Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In *Financial Cryptography and Data Security*, pages 47–61. Springer, 2012.
[2] Michael R Clarkson, Stephen N Chong, and Andrew C Myers. Civitas: Toward a secure voting system. Institute of Electrical and Electronics Engineers, 2008.
[3] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. A practical secret voting scheme for large scale elections. In *Advances in Cryptology—AUSCRYPT'92*, pages 244–251. Springer, 1993.
[4] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70. ACM, 2005.
[5] 湯淺 墾道. エストニアの電子投票. **九州国際大学社会文化研究所紀要**, (65):39–71, 2009.