社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26 (54)
2004／7／21

カメラ付き携帯電話を利用した電子投票システムの提案

本杉 洋† 桂川 健一‡ 佐々木 良一*

† 東京電機大学 情報セキュリティ研究室
〒101-8457 東京都千代田区神田錦町 2-2

E-mail: † motosugi@isl.im.dendai.ac.jp , ‡ katsuragawa@isl.im.dendai.ac.jp

あらまし 現在,投票率の向上や投票結果の正確で効率のよい集計のため,電子投票実現に関心が高まっている.しかし,インターネットを使った家庭からの投票では,買収や脅迫が考えられるため,実現は困難とされていた.本研究では,買収や脅迫がされていないことを証明するために最小限必要とされている,投票内容を見られなくする方式を提案している.具体的には,携帯電話のカメラで投票者を投票時に監視する電子投票システムを提案し,PC 上での実装とその評価を行った.その結果,将来,携帯電話の進歩と公的個人認証サービスを利用することで,システムを実現できる見通しを得た.

キーワード 電子投票,買収,脅迫,携帯電話,カメラ,ジェスチャ

Electronic Voting System Using Mobile Phone with Camera

Hiroshi Motosugi† Ken-ichi Katsuragawa‡ Ryoichi Sasaki*

† Information Security Laboratory, Tokyo Denki University

2-2 Kanda Nishiki-Cho Chiyoda-Ku Tokyo, 101-8457 Japan

E-mail: † motosugi@isl.im.dendai.ac.jp , ‡ katsuragawa@isl.im.dendai.ac.jp

Abstract Electronic Voting system is becoming to be widely used caused by the effective summing up function. However , there is a few problems , for example , Vote-buying and Voter coercion in Electronic Voting from home via internet. We propose the Electronic Voting system with counter-measures against vote-buying and voter coercion. This system make it possible to prevent the Vote-buying and Voter coercion by observing the voting process using Mobile Phone with Camera. We think that it is possible to carry out this system providing that improve in Mobile Phone and use the JPKI.

Keyword Electronic Voting, Vote-buying, Voter coercion, Mobile Phone, Camera, Gesture

1.はじめに

1.1.従来の選挙 (1)(2)

従来の選挙では,投票に紙を用いて投票者が記入をしていた.しかし,それでは集計に時間がかかり,判定ミスも起こることがある.

電子投票は,投票内容を電子化することで従来の選挙に対し,効率がよく正確な集計ができる.さらに,近年の低い投票率も向上させることが期待されている.

1.2.投票の 3 要件 (1)

従来の選挙では,以下 3 つのことを実現している.

(1)有権者の確認:現在では,有権者の確認は,有権者にはがきを送り,それを提出させることで行っている.

(2)有権者の無記名性:現在では,投票用紙に投票者を特定させるような氏名を書いていない.

(3)投票結果の正当性検証:現在の正当性検証では,

集計作業を一般の人に公開することで，不正がないことを証明している．

以上の機能を電子投票でも実行する必要がある．

1.3.電子投票の発展の3段階[1][6]

総務省では，電子投票の発展の3段階を示している．

第一段階では，有権者は国や地方自治体などによって指定された投票所で投票を行う．この段階は，2002年6月23日，岡山県新見市の市議会議員および市長選挙において実施された．従来に比べて，投票率は上がらなかったが，集計時間は約半分の速さになった．[7]

第二段階では，有権者は複数の投票所から一つを選択し投票を行うことができる．この段階になると，有権者は旅行先など離れた場所でも投票が可能となる．しかし，そのためには，各投票所間を繋ぐネットワークの構築が必要となる．

第三段階では，有権者はインターネットを使って家庭，職場などのコンピュータから投票が可能となる．この段階になると，第一段階，第二段階に比べて，投票できる範囲が格段と広くなる．

2.提案する電子投票システム

2.1.従来の問題と対応策

第三段階を実現するためのベースとなる方法として次の3つが考えられている．(1)ブラインド署名を使った方式，(2)準同型写像方式，(3)ミックスネット方式．この中で，ミックスネット方式が，正当性検証ができ，投票内容に関数する制約が小さいため，最も有効であるとされている．[1] したがって，ここでは，ミックスネット方式をベースに検討を行うことにする．

第三段階において，インターネットを使った投票を実現する上で障害となる最大の問題が，選挙人が自分の意志によって投票したかわからないという点である．つまり，家で行われる投票だと，買収や脅迫がされるという可能性がある．この問題は上記の3つの実現方式でも対策がなされていない．そのため，この問題に対する対策も必要となる．

現在の選挙では，投票者は立会人の監視の下，1人で投票することにより，第3者から投票内容を見られることを防いでいる．これと同じように，提案する電子投票システムでは投票者をカメラで監視することで，第3者がいても投票内容を見れなくさせる方法を提案した．

2.1.具体的なアイデア

(1)秘密投票

投票者を監視するため，投票している様子を自分の携帯電話のカメラで自分を撮影してもらう．投票者以外の人が写っていたら，投票が無効となる．この判定は人が行い将来は自動化する．映像に写っていない範囲に脅迫者や買収者がいたとしても，投票画面が見えないものとすると投票者しか投票内容を知りえないので，秘密投票が成立する．

(2)ジェスチャ入りの動画

秘密投票であることの証明に動画で監視をすることが必要である．悪意のある第3者が動画をあらかじめ用意し監視を欺くことを防ぐため，動画に認証センタから指示されたジェスチャを入れることでその動画が事前に用意したものではなく，リアルタイムであることを意味する．

(3)投票後の処理

投票後，携帯電話の画面，メモリ内に誰に投票したかがわかるようなものがあると，買収の温床になりえるため投票内容を消去する．

2.2.携帯電話を用いる理由

カメラ付き携帯電話の契約数は図1のように年々増加してきているため，このシステムを実現すれば，投票率の向上が期待される．また，現在の携帯電話はインターネットに接続することができ，どこにでも持ち歩くことができるため，パソコンよりも自由度は増し，どこからでも投票ができるようになる．

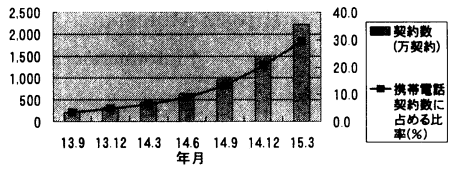


図1.携帯電話の契約数
（出典）「平成15年情報通信白書」

2.3.投票の流れ

ミックスネット方式を使うと，全体の流れは，以下の図2のようになる．投票者は認証センタに投票データを送り，認証センタはシャッフルセンタを通して，集計センタへ投票データを送る．

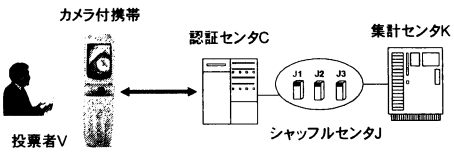


図2.全体の流れ

①投票者は認証センタへ携帯電話を用いて，投票要求する．

その際，携帯電話内のプログラムは，乱数 R_V を生成する．そして住民票コードと乱数 R_V を，認証センタ C の公開鍵 P_C で暗号化し認証センタに送信する．

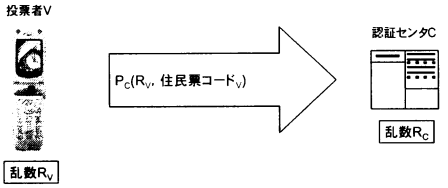


図 3.投票要求

②認証センタでは送られたデータを秘密鍵 S_C で復号化し R_V，住民票コードを得る．住民票コードから投票者を特定し，次に乱数 R_C，ジェスチャ指示を生成する．最後に候補者氏名，ジェスチャ指示，乱数 R_C，Rv を投票者の公開鍵 P_V で暗号化し送信する．

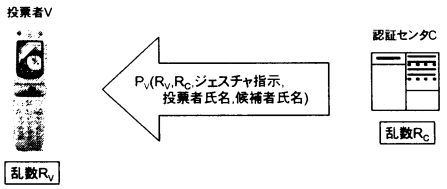


図 4.及びジェスチャ指示

③携帯電話内の投票プログラムは，認証センタから送られたデータを投票者の秘密鍵 S_V で復号化し，送られてきた乱数 Rv が①で送った Rv と同じであるかを確認しジェスチャを表示する．

投票者は，指示されたジェスチャを自分で撮影し，投票内容 M を選択する．

プログラムは投票内容 M を集計センタ P_K やシャッフルセンタの公開鍵 $P_{Jx(x=1,\ 2,\ 3...)}$ で多重に暗号化し，動画 D，乱数 R_C を共に電子署名 Sig_V をつけて認証センタに送信する．多重暗号する際，正当性検証のため投票内容を暗号化する毎にそのハッシュを控えておく．

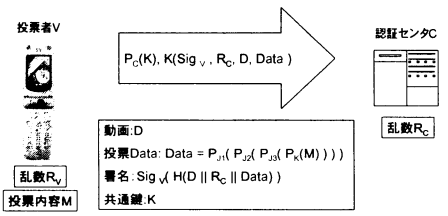


図 5.投票

④認証センタは，送られてきた乱数 R_C が①で送った R_C と同じであるかを確認し，電子署名の検証を行い，動画と投票データを分け，住民票コードと投票データそれぞれ投票時間が終わるまで控えておく．投票時間が終わったら，多数の投票者から送られてきた，多重に暗号化された投票データだけのリストをシャッフルセンタに送る．

⑤各シャッフルセンタは，投票データのリストを，自分の秘密鍵で復号化の後，シャッフル（順番入れ替え）を行い，次のシャッフルセンタに送る．ここで入出力のハッシュを正当性情報として公開する．投票者はこれを②で控えたハッシュと比較することで自分の投票データが届いたことを確認できる．

⑥集計センタは，シャッフルセンタから送られてきた投票データのリストを自分の秘密鍵で復号化し，全投票内容 M を取り出し，その結果を集計する．

3.安全性

(1)投票の 3 要件

次のようにすることにより，投票の 3 要件を満たしている．

① 投票者の確認

投票者の確認は PKI を使うことで確度の高い本人性が得られていると考えられている．

② 投票者の無記名性

投票者の個人情報は，認証センタで投票データと分け，投票データをミックスネットによる順番入れ替えすることにより投票者の匿名性を高めている．したがって集計センタに届いた投票内容から，投票者を特定させることはできない．

③ 投票結果の正当性検証

各シャッフルセンタは，投票データのリストを復号，シャッフルを行う前後に投票データのハッシュを公開している．投票者は自分の控えているハッシュが公開されたハッシュの中に入っていることを確認することで，正当性を行うことができる．

(2)投票内容の秘匿性

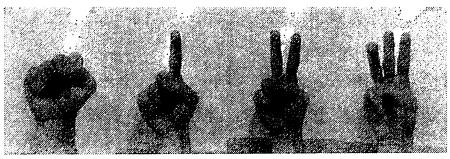
投票内容は，投票者側で集計センタ，シャッフルセンタそれぞれの公開鍵で多重に暗号化するため第 3 者が投票内容を盗み見るためには，全部の秘密鍵が必要となり秘密鍵を厳重に管理すれば安全性が保たれる．また携帯電話の画面自体を横から盗み見る行為に対してはカメラで監視することで防ぐことができる．携帯電話の電磁波から盗み見る行為に対しては電磁波シー

ルドを利用するなどにより，対応が可能であると考えられる．

(3)ジェスチャ動画の種類

上述のように投票が単独で行われているかを動画によって確認している．この動画を事前に撮影し単独投票を崩されないために動画にランダムなジェスチャを入れ，リアルタイムであるかを確認する方法を提案した．ジェスチャの種類を多く用意することによって，ジェスチャ入りの動画を事前に用意することが困難になる．多種類のジェスチャの方法として乱数をジェスチャとして要求し，投票者は片手で数字を表した手数字を用いて順番に出すことで，無限通りの表現が可能となる．

ジェスチャの例として，図6のように片手で6通りの数を表すことができる．



0　1　2　3

4　5

図 6.ジェスチャの例

(4)二重投票

投票者が二重投票しないように，認証センタでは，投票された投票者の住民票コードを控え，同じ住民票コードがないかを調べることで安全性は保たれる．

(5)認証センタへのなりすまし

不正なプログラムを使い，違う認証センタへ投票される恐れがある．投票者が投票要求時に生成した乱数 R_V を確認することでなりすましを確認できる．

なお，電子投票をパソコンで行うと，ハードウェア面，ソフトウェア面で次のような問題があった．

ハードウェア面での問題として，複数のモニタへの出力することで，別の場所から投票内容を除き見ることが可能であるということ．

ソフトウェア面の問題として，買収者がリモート操作ツールを使い，投票者になりすまし投票できるということ．

この2つの問題は，パソコンでは解決することが困難である．しかし，提案システムでは，携帯電話を用いるため，このような問題が発生しない．

以上より使用上，大きな問題はないと言ってよいだろう．

4.実装と評価

提案方式の実装として java を用い表1の PC 環境の下で開発し，現状の携帯電話との比較検討した．プロトタイプとして暗号方式は RSA 公開鍵方式を採用し，動画を使わず静止画を用い，単独投票の確認を人が判定することとした．

表1. 開発･評価環境

CPU	Intel Celeron766MHz (1450.86MIPS)
MEMORY	184MB
HDD	20GB
OS	Windows XP Professional
言語	Java2 SDK, Standard Edition 1.4.1

4.1.処理速度

暗号化処理速度についてプロトタイプシステムで10回計測したところ，暗号化の処理速度は平均0.28[秒]であった．au の CDMA1xWIN シリーズに搭載されている SH-Mobile の MIPS 値は 173[MIPS]であり評価 PC の約8分の1である．単純に CPU 性能だけで暗号化速度を推定すると携帯電話では約 2.35[秒]であり，利用可能な範囲である．ただし，処理速度は CPU 性能だけでは決定しないので実際は時間がかかる可能性がある．

4.2 通信速度

au の携帯電話で作成できる動画の画像サイズは最大 QCIF(176×144)，データサイズが 150[KB]までとなっている．現在でも表2に示すように QCIF サイズなら 8.33[秒]で送ることができる．認証処理等を自動化するには高精彩な動画が必要となる可能性があり，今後の課題である．

表2. 通信時間[秒]

		携帯電話 144 [kbps]
動画(15fps) VGA	29300 [KB]	1627.78
動画(15fps) QCIF	150 [KB]	8.33

4.3.今後の課題

今回は，PC 上で実装を行ったが，今後，携帯電話で実装し，評価をしていく予定である．

5.まとめ

今回提案したカメラ付き携帯電話を使った電子投票システムでは，電子投票で問題となっていた買収，脅迫への対策を行った．

提案システムを実現するには，動画を用いるため携帯電話の処理速度，通信速度などを進歩させなければならないが，公的個人認証サービス開始しているので，実現させることは難しいとは言えない．このシステムが実現することができれば，投票率低下が解決され，投票全体の効率が上がることにつながる．

また，広い範囲でのアンケート調査などに使うことも利用方法の１つとして考えられる．

参考文献

[1] 宮内宏，尾花賢，森健吾「電子投票の実現」電子通信学会誌 Vol.86 No.5 pp.331-336 2003 年 5 月

[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」電子通信学会誌 Vol.86 No.1 pp.33-35 2003 年 1 月

[3] Alexandros Xenakis，Ann Macintosh 「Procedural Security in Electronic Voting」37th Hawaii International Conference on System Sciences 2004

[4] 佐々木良一，内田勝也，岡本栄司，菊池浩明，寺田真敏，村山優子「情報セキュリティ事典」共立出版 2003 年 7 月 10 日

[5] 電子投票普及協同組合
http://www.evs-j.com/

[6] 総務省「電子機器利用による選挙システム研究会報告書」
http://www.soumu.go.jp/s-news/2002/pdf/020201_2.pdf

[7]総務省　情報通信白書
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/html/F30Z2000.html