不在者投票を考慮した電子選挙システム

許, 容碩
九州大学 システム情報科学研究院

櫻井, 幸一
九州大学 システム情報科学研究院

出版情報：コンピュータセキュリティシンポジウム2002. 1, pp.461-466, 2002-10. コンピュータセキュリティシンポジウム
バージョン：
権利関係：

不在者投票を考慮した電子選挙システム

許　容碩*　　櫻井　幸一

九州大学 システム情報科学研究院

〒812-8581 福岡市東区箱崎 6-10-1

あらまし 本研究では、不在者投票をも電子化した無記名型電子投票システムを提案する。日本の現行の選挙法では、不在者が投票後、開票するまでの間に死亡したり選挙権を喪失した場合には、無効票とみなして対応する必要がある。したがって、提案する電子投票システムでも、プライバシーを侵害することなく、如何にして、投票後に不在者投票を無効化するかが鍵となる。

キーワード　電子投票システム、不在者投票、安全性、プライバシー、２重公開鍵暗号

An Electronic Voting Scheme including Absentee
- A practical tallying that can the ballot – cancellation -

Yong-Sork HER*　　Kouichi SAKURAI

Dept.of Computer Science and Communication Engineering,　Kyushu University

6-10-1, Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan

ysher@tcslab.csce.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp

ABSTRACT　In this paper, we propose an unsigned electronic voting scheme to be electronic for an absentee voter. According to the existing election law of Japan, after an absentee voter enforces the voting, if absentee voter died or lost the right of casting the ballot before the tallying, the voting contents of this absentee are dealt with invalid. We should consider such these points in order to compose the e-voting system. So, our e-voting system can detect whether it infringes on the privacy or not, and we have an eye to make an invalidation of an absentee voting (after cast a vote).

Key Word　Electronic voting system, Election law, Privacy, the ballot-cancellation, Double encryption

1．はじめに

1.1 背景

暗号技術を利用したさまざまな電子投票システムが提案されている[PIK93][KJ95][CM96][RG97][TYKK98]．この中でもいくつかは、すでに実験システムなどで施行されている。我々の目標は実際選挙で使用することができる安全な無記名型電子投票システムである．

* 文部科学省科学研究費補助金学術創成研究課題番号14GS0218『社会基盤を構築するためのシステム LSI 設計手法の研究(研究代表安浦寛人九州大学システム LSI 研究センター長)の支援を受けている．

1.2 動機

-日本で最初の電子投票

2002 年 9 月 23 日，岡山で新見市の市場と市議員を選出するための最初の電子投票が施行された[MC1]．一般有権者は電子投票を使用したが,不在者投票に関しては、従来の自書式と同様に，郵便で投票紙を受けて手作業で開票したため，電子投票の開票に比べて，多くの時間がかかった．さらに，電子投票のみによる集計結果と不在者投票を含めた最終集計結果とが２段階に分けて公表され，従来の投票にはない新たなプライバシーの問題も指摘されている．表 1 は岡山の市議会選挙での候補群の得票率を表したものである．一般有権者と

不在者の支持度が政党別，候補者別に差が出たことが分かる．

候補群	得票率	
	電子式 **（ 一般有権者）**	**自書式** **（ 不在者）**
候補者 1	78.4 %	**69.6%**
候補者 2	9%	**11.5%**
候補者 3	5%	**13.3%**
候補者 4	7.6%	**5.6%**
合計	100% (14966 名)	**100%** **(1719 名)**

表 1. 候補群の得票率　(新見市の市議会)

1.3 貢献

本研究では、不在者投票をも電子化した無記名型電子投票システムを提案する．日本の現行の選挙法では，不在者が投票後，開票するまでの間に死亡したり選挙権を喪失した場合には，無効票とみなして対応する必要がある．

したがって，目標とする電子投票システムでも，プライバシーを侵害することなく，如何にして不在者投票を投票後に無効化するかが鍵となる．提案するシステムは，辻井らによる 2 重公開鍵暗号を用いた投票プロトコル[TYKK98]を基にし，投票後の投票値の無効化手法を導入した．

2．TYKK 98

1998 年に，辻井，山口，北沢，黒澤により実際選挙で利用できる電子投票システムが提案された．彼らはゼロ知識証明，RSA と準同型暗号のための r-次剰余暗号を使用している[TYKK98]．このシステムの特徴は二つの独立的な機関を使用し，二重暗号化を行っている点である．それぞれの機関の公開鍵を通して投票内容を暗号化することで一つの機関が全体の選挙の責任を負う危険性を防ぐことができる．

また，二つの機関はお互い独立しているため投票内容や投票結果に対する偽造や内容変造を防ぐことができる．二つの機関はそれぞれの投票結果に対する不正を検出できる．

3．提案する電子投票のシステム

辻井らの研究では，不在者投票とその取り消し手段に関しては検討されていない．本研究では，この TYKK 投票プロトコルに対し，投票後の投票値の無効化手法を導入する．

3.1 基本的なアイディア

我々の目標は実際の選挙で一般投票者と不在者が共に投票できる電子投票システムを実現することにある．すなわち，開票時点における投票者の投票権に対する判断と集計計算に目標をおいて，投票結果の集計後にも無効化の計算をできる，すなわち，投票権利を喪失や不法投票などが起こった場合，投票を取消すことができるシステムを提案する．<図 1 参照>投票の集計計算する際，投票の無効化も可能である．

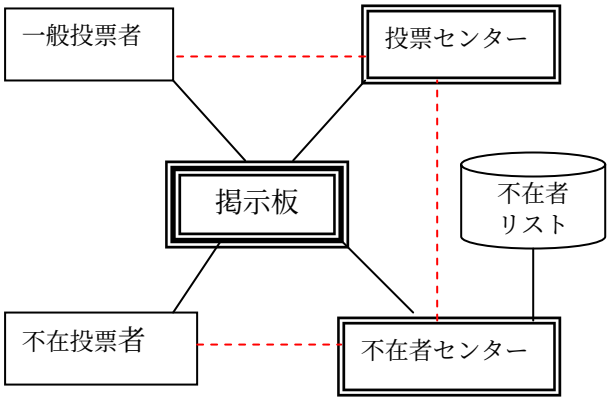

図 1. 我々の電子投票システム

3.2 システムの構成

提案するシステムは 4 部分で構成される．不在者，投票センター，不在者のリストを含む不在者センターと掲示板で構成する．

1)　不在者

不在者は，公務や健康等の理由で投票の当日に指定された投票所で投票を出来ない有権者を指す[VH]．特に，不在者には軍人が占める比率が最も多い．不在者に登録された有権者は，投票内容を暗号化するために投票システムと不在者システムからそれぞれの公開鍵を受け取る <表2 参考>．詳細な不在者の投票手順は次の通りである．

2) 不在者センター

不在者センターは適法な不在者のリストに対するデータベースをもっている．不在者の個人情報と ID を通し，有効票と無効票を判断でき，かつ投票可否も判断できる．不在者システムの役割は次の通りである．

- 暗号化された不在者の投票内容を不在者の公開鍵を利用して復号化する．

- 不在者が適法な有権者なのかどうか，また有効な投票であるかを判断する．
- 掲示板に判断結果を表明する．

3) 投票センター

不在者システムの不正行為があるかを確認し，最後の投票結果の集計を計算する． すなわち，投票センターは不在者センターの公開鍵を用いて不在者センターの計算結果を復号化した後,自身の計算結果と比較して異常有無を確認することができる．

4) 掲示板

掲示板では，有権者の投票内容は分からないが，投票の有無をあらゆる人々が知ることができる． また，投票内容の変造や削除はできない．掲示板の内容は<表2>のようになる．現在の投票制度で不在者投票の場合は投票内容の正確な送信と正確な集計可否を確認することが難しくなっている．不在者らは自身の投票内容が正確に転送されたのか，正確に集計に含まれたのかを最も心配している．本論文の電子投票では，これを満足するために掲示板を使用して正確な送信と集計を表明するため，現在の投票制度の問題を解決することができる．また，開票の時点で投票権の有無を公開して透明性を保障する．

時間	内容	機関	表明内容
投票	投票	不在者	投票可否
	適法な投票表明	不在者システム	不在者と投票の適法性可否
投票終了後	不在者の選挙権	不在者システム	不在者の選挙権をチェック
	蓄積値段	投票システム	暗号化になった形態の多重化になった適法投票
	投票システムの不正	不在者システム	投票システムの不正をチェック
	最終集計	不在者システム	投票結果の最終集計
	不在者システムの不正	投票システム	不在者システムの不正をチェック

表 2．掲示板の内容

3.3 投票の手順

この章では，提案する電子投票システムの投票手順を説明する．

記号定義

- 投票者: $v(i)$
- 投票者の ID: ID_i
- 投票者 $v(i)$ の投票内容: m_i (m_i = 0 or 1)
- 投票者の公開鍵 ：$<e_{v(i)}, N_{v(i)}>$ (RSA)
- 投票者の秘密鍵 ：$<d_{v(i)}, p_{v(i)}, q_{v(i)}>$(RSA)
- 不在者センターA の公開鍵 $<e_A, N_A>$ (RSA)
- 不在者センターA の秘密鍵 $<d_A, p_A, q_A>$ (RSA)
- $p_{v(i)}, q_{v(i)}, p_A, q_A$： large prime numbers
- x ： r-次剰余暗号の乱数
- r ： r-次剰余暗号の乱数 ($0 \le m_i < r$)
- 投票センターB の公開鍵 $<N_B, y>$ (r-次剰余暗号)
- 投票センターB の秘密鍵 $<p_B, q_B>$ (r-次剰余暗号)
- k_i： 不在者投票権の変数 (k_i =1 or 0)
- M ： 投票結果の合計

投票の手順は以下の通り（図 2 参照）

① 不在者 $v(i)$ は選挙管理委員会に不在者登録をする．

② 不在者 $v(i)$ は投票内容 m_i を投票する； m_i （m_i = 0 or 1)

③ 不在者 $v(i)$ は投票センターB の公開鍵$<N_B, y>$を利用して投票内容 m_i を暗号化する。

$$Z_i = y^{m_i} x^r \bmod N_B$$

④ 不在者 $v(i)$ は不在者センターA の公開鍵$<e_A, N_A>$を利用して Z_i を暗号化する。

$$C_i = Z_i^{e_A} \bmod N_A$$

⑤ 不在者 $v(i)$ は個人 ID(ID_i)を作る

⑥ 個人 ID(ID_i)と暗号化された投票内容 C_i を投票者の秘密鍵$<d_{v(i)}, p_{v(i)}, q_{v(i)}>$で暗号化する

$$(ID_i)^{d_{v(i)}}, C_i \bmod N_{v(i)}$$

⑦ 不在者 $v(i)$ は掲示板に暗号化になった上の投票内容と ID_i を掲示板に送信する．

< 投票終了後>

⑧ 不在者センターA は不在者の投票権が有効かどうかをチェックする．無効投票権は k_i =0，有効投票権 k_i =1 を表示される。

⑨ 不在者センターA は投票者 $v(i)$ の公開鍵の $<e_{v(i)}, N_{v(i)}>$で次の式を復号化して C_i を求める

$$(ID_i)^{d_{v(i)}}, C_i \bmod N_{v(i)}$$

⑩ 不在者センターA は自身の秘密鍵 $<d_A, p_A, q_A>$ を利用して C_i を復号化すれば Z_i を求めることができる。そして、次の式を計算する。

$$Z_c = \prod_{i=1}^{h} (Z_i)^{k_i} \bmod N_B$$

$$= \prod_{i=1}^{h} (y^{m_i} x^r)^{k_i} \bmod N_B$$

$$= \prod_{i=1}^{l} (Z_i)^1 \prod_{i=l+1}^{n} (Z_i)^0 = \prod_{i=1}^{l} (Z_i)$$

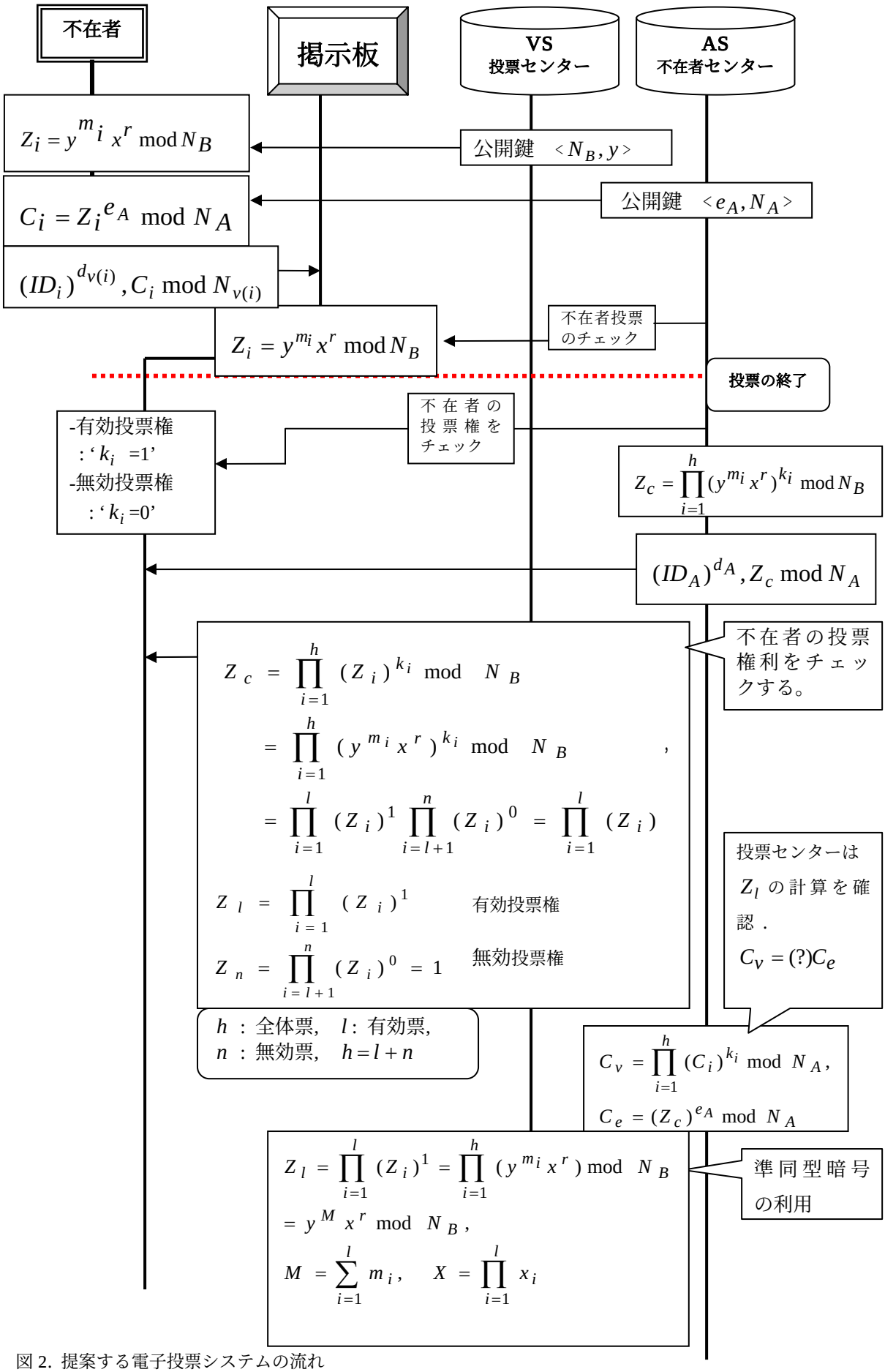

図 2. 提案する電子投票システムの流れ

< h = l + n , h:全体票, l:有効票, n:無効票 >

$Z_l = \prod_{i=1}^{l} (Z_i)^1$ ：有効投票権

$Z_n = \prod_{i=l+1}^{n} (Z_i)^0$ ：無効投票権

⑪ 不在者センターA は自身の ID_A を作る

⑫ 不在者センターA は自身の秘密鍵 $<d_A, p_A, q_A>$ で ID_A と Z_c を暗号化して掲示板に送信する.

$$(ID_A)^{d_A}, Z_c \bmod N_A$$

⑬ 投票センターB は不在者センターA の公開鍵 $<e_A, N_A>$ で $(ID_A)^{d_A}, Z_c \bmod N_A$ を復号化すれば Z_c を求めることができる。不在者センターA の Z_c の計算を確認するために次の式を計算する。

$$C_v = \prod_{i=1}^{h} (C_i)^{k_i} \bmod N_A,$$

$$C_e = (Z_c)^{e_A} \bmod N_A$$

C_v は 掲示板で 暗号化になった投票値の掛け算をしたのである. $C_v = C_e$ ならば不在者センターA の計算値がしく計算したのである.

< 有効票 : M>

⑭ 投票システムにより計算された投票結果を比較して, 計算結果が合えば掲示板に送信する.

$$Z_l = \prod_{i=1}^{l} (Z_i)^1 = \prod_{i=1}^{h} (y^{m_i} x^r) \bmod N_B$$

$$= y^M x^r \bmod N_B,$$

$$M = \sum_{i=1}^{l} m_i, \quad X = \prod_{i=1}^{l} x_i$$

5. まとめ

岡山の電子投票が成功したことによって, 不在者投票でも電子投票を実施するために, 現行の日本の公職選挙法と電子式記録式投票持例法(電子投票法)を改正するための作業が進行している[MC2].

不在者投票は重要な役割を担う. しかし, 大部分の電子投票システムが不在者投票について考慮していない. 岡山の電子投票でも一般有権者(電子投票)と不在者(磁石式)が別々の方式で投票を実施した結果, 従来の投票にはない新たなプライバシーの問題も指摘されている. 電子投票システムの現実化のためには不在者投票も含まれた, あらゆる有権者が平等に投票権をできるシステムが必要する. 本論文で, 我々は実際の選挙に近い状況の元で不在者と一般投票者が使用することができる電子投票のシステムを提案した. 特に, 本システムでは投票集計後にも無効票を処理することができる.

文 献

[PIK93] C.Park, K.Itoh, K.Kurosawa " Efficient Anonymous Channel and All / Nothing Election Scheme " EUROCRYPT '93, LNCS765, Springer-Verlag, Berlin Heidelberg 1994.

[KJ95] K.Sako, J.Kilian " Receipt -Free Mix-Type Voting Scheme " EUROCRYPT '95, LNCS921, pp393-403, Springer-Verlag, Berlin Heidelberg 1995.

[CM96] R.Cramer, M.Franklin, B, Schoenmakers, M.Yung "Multi-Authority Secret-Ballot Elections with Linear Work" EUROCRYPT '96, LNCS1070, Springer-Verlag, Berlin Heidelberg 1996.

[RG97] R. Cramer, R. Gennaro, B.Schoenmakers "A Secure and Optimally Efficient Multi-Authority Election Scheme" EUROCRYPT '97, LNCS1233, pp 103-118, Springer-Verlag, Berlin Heidelberg, 1997.

[TYKK98] S.Tsujii, H.Yamaguchi, A.Kitazawa, K.Kurosawa " A Method for Voting Protocols with regards to Privacy" ISEC98-42, 1998.

[OMAF099] M.Ohkubo, F.Miura, M.Abe, A. Fujioka, T.Okamoto "An Improvement on a Practical Secret Voting Scheme" ISW '99, LNCS 1729, pp225-234, 1999.

[BFPPS01] O.Baudron, P.-A. Fouque, D.Pointcheval, G.Poupard, J.Stern " Practical Multi-Candidate Election System" ACM 2001.

[CF95] J.Cohen, M.Fischer "A robust and verifiable cryptographically secure election scheme" In Proc.26th IEEE Symposium on Foundations of Computer Science(FOCS '85),PP372-382. IEEE Computer Society, 1985.

[CDS94] R.Cramer, I.Damagard, B.Schoenmakers "Proofs of partial knowledge and simplified design of witness hiding protocols" In Advances in Cryptology-Crypto94, Volume 839 of Lecture Notes in Computer Science, Berlin, Spring-Verlag, 1994.

[VH] http://www.votehere.com/

[AB] http://www.absenteeballot.net/

[MC1] http://www.mainichi.co.jp/ (June.24.2002)

[MC2] http://www.mainichi.co.jp/ (Aug.14.2002)

[BT] http://premium.nikkeibp.co.jp/biz/e-gov/sp0703b.shtml