検証可能な匿名情報収集方式を用いた電子投票の実現と応用

1215098　安光 穂高　【 セキュリティシステム研究室 】

Realization and Application of E-voting using Secure Collection method of Anonymous Data with verifiability

1215098　Hodaka YASUMITSU　【 Security Systems Lab. 】

1　はじめに

投票用紙や人件費等のコスト削減および投票率向上を目的に，電子投票の研究が盛んに行われている．

表 1 に電子投票方式が満たすべき要件を示す．

表 1　電子投票方式が満たすべき要件

プライバシ保護	投票者の投票がいずれの参加者にも漏れないこと
有権者確認可能性	有権者のみが投票できること
二重投票不可能性	有権者が一回のみ投票できること
検証可能性	投票，集計，開票の正当性を検証可能なこと
堅牢性	何らかの誤りが混入した場合にそれを排除できること
公平性	投票の途中経過を誰も知りえないこと
無証拠性	投票者はどの候補者に投票したのか証明できないこと

公開鍵暗号をベースとした手法がいくつか提案されているが，要件を満たしている方式においても，投票内容が制限されている方式や実現するための構築・運用コストが高い方式，投票者の計算負荷が高い方式など要件とは別の問題が存在する．

携帯端末等の処理能力の低い計算機での投票を想定し，投票内容の制限を無くした比較的シンプルな方式として匿名情報収集方式 [1] がある．この方式は，共通鍵暗号とワンタイムパスワード認証方式 SAS(Simple And Secure password authentication protocol)[2] を用いた簡易で安全な投票プロトコルである．図 1 にプロトコルの概要を示す．エンティティは四つ存在し，投票者，保管サーバ，鍵サーバ，集計者である．投票者の送信するデータを二つに分け，投票と秘密鍵を別々に管理させることにより匿名性を維持しつつ投票を集計できる．

しかし，匿名情報収集方式では，全てのエンティティが手順通りに正しくプロトコルを実行し，単独での不正を行わないという前提条件がある．実際に運用する上では，不正者がいた場合でも正しく実行されるプロトコルが望ましい．そこで，本提案では，集計者が不正を行う可能性があることを前提とし，集計結果の改ざんがあった場合でも第三者が検証を行うことで，不正を検知できる仕組みを実現する．

2　提案方式

鍵サーバが集計結果の検証を行う．投票者が検証データを作成し，保管サーバを経由して鍵サーバに送信することで，匿名性を保ったまま集計結果の検証が可能となる．

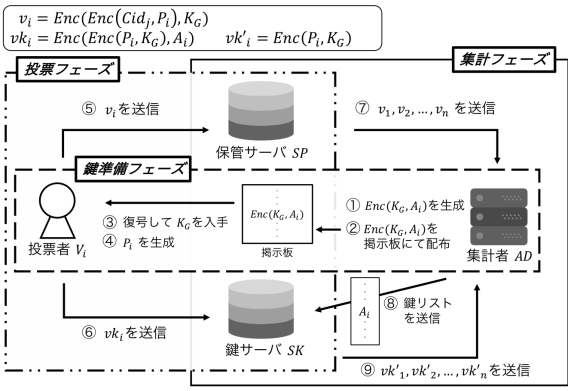

図 1　匿名情報収集方式のプロトコル概要図

以降では，表 2 に示す定義と記法を用いる．

表 2　提案方式における定義と記法

V_i	i 番目の投票者．ただし，$(1 \leq i \leq n)$
AD	投票を集計する集計者．
SP	投票を保管する保管サーバ．
SK	秘密鍵の保管と集計結果の検証を行う鍵サーバ．
Cid_j	j 番目の候補者を示す ID．ただし，$(1 \leq j \leq m)$
K_G	AD と投票者全員のグループ鍵．
P_i	V_i の秘密鍵．V_i 自身が生成する．
A_i	V_i と AD で共通の暗号鍵．投票者の認証情報を元に生成される．
$H(x)$	データ x をハッシュ関数 H によって変換した値．
$Enc(x, k)$	データ x を暗号鍵 k で暗号化した値．

2.1　前提条件

集計者は，集計結果の改ざんを行う可能性があり，その他のエンティティは決められた手順通りにプロトコルを実行するものと仮定する．

2.2　検証可能な匿名情報収集プロトコル

本投票プロトコルでは，登録，鍵準備，投票，集計，公表の 5 つのフェーズが存在する．登録フェーズにて，投票者の登録を行い，各サーバは SAS 認証方式による認証情報を保存する．鍵準備フェーズでは，投票者および集計者が暗号鍵を生成し共有する．投票者 V_i が所持する暗号鍵は，投票者全員のグループ鍵 K_G，自身の投票を暗号化する秘密鍵 P_i，集計者との共通鍵 A_i である．集計者 AD が所持する鍵は，グループ鍵 K_G およ

び投票者との共通鍵 $A_1, A_2, ..., A_n$ である．以下に，投票，集計，公表の 3 つのフェーズについて記述する．

2.2.1　投票フェーズ

以下，投票者 V_i が候補者 Cid_j に投票する場合の処理手順を示す．

1. P_i および K_G で候補者 ID を暗号化し，投票 v_i を生成する．
   $v_i = Enc(Enc(Cid_j, P_i), K_G)$
2. P_i にハッシュ関数を適用し，投票 v_i を暗号化して検証データ f_i を生成する．
   $f_i = Enc(Cid_j, H(P_i))$
3. v_i および f_i を SP に送る．
4. P_i を K_G および A_i で暗号化し，投票鍵 vk_i を生成する．
   $vk_i = Enc(Enc(P_i, K_G), A_i)$
5. vk_i を SK に送る．

2.2.2　集計フェーズ

SP は投票者から受け取った投票 $v_1, v_2, ..., v_n$ をランダムに並べ替え，投票者を特定できないようにした上で，AD に送る．以下に，SK と AD との処理を示す．

1. AD は，投票者との共通鍵リスト $A_1, A_2, ..., A_n$ を SK に送る．
2. SK は，共通鍵リストを用いて $vk_1, vk_2, ..., vk_n$ を復号し，投票鍵 $vk'_1, vk'_2, ..., vk'_n$ を算出する．
   $vk'_i = Enc(P_i, K_G)$
3. $vk'_1, vk'_2, ..., vk'_n$ をランダムに並び替えた後，AD に送る．

以上までの手順完了後，AD は投票鍵 $vk'_1, vk'_2, ..., vk'_n$ を K_G で復号し，秘密鍵 $P_1, P_2, ..., P_n$ を得る．このとき，どの投票鍵に関しても K_G で復号可能であるため，得られた秘密鍵がどの投票者のものであるかは特定できない．投票 $v_1, v_2, ..., v_n$ も K_G で復号可能であるため，同様に投票者の特定は不可能である．全てのデータを復号することで，各候補者の得票数を集計できる．

2.2.3　公表フェーズ

集計結果の公表前に，SK が検証を行う．以下に検証の手順を示す．

1. AD は，秘密鍵 $P_1, P_2, ..., P_n$ にハッシュ関数を適用し，検証鍵 $fk_1, fk_2, ..., fk_n$ を生成する．
   $fk_i = H(P_i)$
2. AD は，集計結果と検証鍵 $fk_1, fk_2, ..., fk_n$，候補者 ID $Cid_1, Cid_2, ..., Cid_m$ を SK に送る．
3. SK は，fk_i を用いて $Cid_1, Cid_2, ..., Cid_m$ を一つずつ暗号化し，検証データ $f_1, f_2, ..., f_n$ と比較して一致するものがあるかどうかを検証する．
4. 検証データと一致した fk_i と Cid_j の組み合わせにより，候補者 ID 毎の得票数を計算し，集計結果と等しいことを確認する．検証に成功した場合，SK は集計結果を公表する．

3　評価

集計者が集計結果を改ざんした場合，検証によって改ざん検知できることを示す．集計結果の改ざんは以下の二通り存在する．

1. 票数の水増し，もしくは無断削除
2. 候補者の各得票数入れ替え

鍵サーバの検証では，投票者が作成した検証データを保管サーバ経由で入手するため，全候補者の得票数と一致する．したがって，1 の改ざんを検知できる．また，鍵サーバは検証鍵 fk_i で候補者 ID を暗号化して，検証データと一致するものを探索するため，候補者 ID 毎の得票数が計算できる．したがって，2 の改ざんも検知できる．

既存の匿名情報収集方式と提案方式の計算量を比較する．表 3 に投票者 V_i，集計者 AD，鍵サーバ SK それぞれが行うハッシュ関数，暗号化，データの平均比較回数を示す．

V_i は検証データを作成するため，V_i が行う暗号化回数が既存方式より 1 回多くなっている．AD は検証鍵を作成するが，計算量は既存方式と同じである．SK が集計結果の検証を行うため，既存方式に比べ暗号化およびデータの比較が必要である．

表 3　計算量の比較（単位：回）

	既存方式			提案方式		
	ハッシュ関数	暗号化	比較	ハッシュ関数	暗号化	比較
V_i	1	4	1	1	5	0
AD	n	0	0	n	0	0
SK	0	0	0	0	mn	$\frac{m(n^2+n)+2n}{4}$

4　まとめ

シンプルな電子投票方式である匿名情報収集方式において，集計者が集計結果の改ざんを行う可能性がある場合でも，集計結果の正当性を検証可能なプロトコルを示した．投票者の代わりに鍵サーバが集計結果の検証を行うため，投票者の処理負荷は小さく抑えられる．

今後の課題として，実際の運用を考えると，投票者も不正を行う可能性があるため，投票行為の正当性も保証する必要がある．

参考文献

[1] 安光穂高，”匿名情報収集方式の提案”，高知工科大学学士学位論文，2017.

[2] T.Tsuji，T.Kamioka，A.Shimizu，”Simple And Secure password authentication protocol Ver.2(SAS-2)”，IEICE Technical Reports，OIS2002-30，2002.