要 旨

安全な匿名情報収集方式の提案

安光 穂高

情報化社会の発展に伴い，様々な情報がインターネットを通してやり取りされている．そうした中で，選挙における集計時のコスト削減や投票者の利便性向上による投票率アップを目的に，インターネット上で投票を行う電子投票に注目が集まっている．

既存方式として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．しかし，それらの既存方式では，投票内容が制限されているものや，構築コストが高く実現が難しい，復号処理に時間がかかるなどの問題がある．

本論文では，共通鍵暗号とワンタイムパスワード認証方式 SAS を用いた匿名情報収集方式を提案する．本方式は投票者，集計センタ，コンテンツサーバ，鍵サーバで構成される．投票者のプライバシを保証し，安全に投票者からの投票を収集することができる．処理負荷小さく，スマートフォン等の簡易通信端末上のアプリケーションとしても実現が可能である．また，電子投票に適用する場合に必要となる安全性要件を満たしていることを確認する．

キーワード　ワンタイムパスワード，SAS，匿名情報，電子投票，アンケート

Abstract

A Secure Collection method of Anonymous Data

YASUMITSU Hodaka

Along with a development of information society, various kinds of information are exchanged via the Internet. Under such circumstances, electronic voting which is voting on the Internet is drawing attention for a cost reduction and an increase voter turnout.

Several methods based on public key cryptography have been proposed as existing methods. However, these existing methods have problems that voting contents are restricted, construction costs are high, difficult to realize, and decryption processing takes time.

This paper proposes a secure collection method of anonymous data, using common key cryptography and one-time password authentication protocols SAS which apply a common key cryptography. The method consists of voter, an administration center, a contents management server and an encryption keys management server. A voter privacy is protected, and a vote from the voter can be securely collected. The method requires less processing load, so it can be applied to applications on popular communication terminals such as smart phones.

key words one time password, SAS, anonymous information, electronic voting, survey