個人嗜好反映型コンテンツ配送ミドルウェアの研究

4Q－3

相馬　浩之　田中 博樹
NTT 情報流通プラットフォーム研究所

1.はじめに

近年、予めサービス利用者（以下利用者と略す）の嗜好を調べ、配信コンテンツを選定して配送するプッシュ型コンテンツ同報配信サービスが注目されている。本稿では、プッシュ型コンテンツ同報配信サービスにおいて利用者の嗜好を反映しつつ利用者のプライバシーを保護することも可能とするコンテンツ配送方式について提案する。

2.コンテンツ配送に対する要求条件

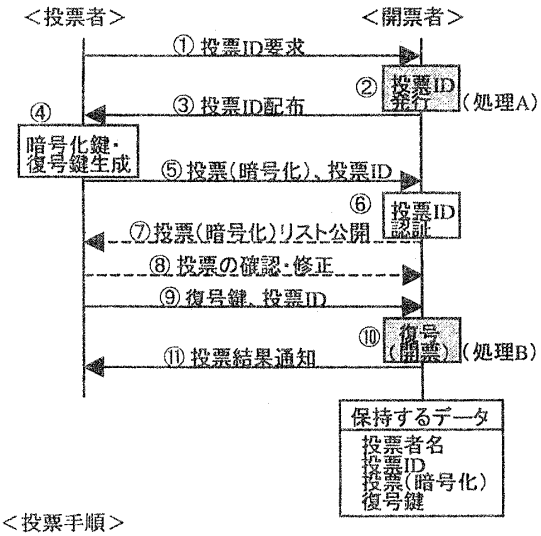
利用者にとって有用なコンテンツ配送サービスを実現するには、利用者の嗜好を反映するため、利用者の配送コンテンツの希望を調査する必要がある。しかし、全利用者の嗜好を反映したコンテンツを配送することは限られた時間の中では困難であり、また対費用効果の確保も困難である。多数の利用者の嗜好を反映するコンテンツの選定を容易にする一手段として、電子投票の適用が挙げられる。

電子投票を利用する場合、思想、嗜好、心身に関わることなど利用者自身のプライバシーをその利用者以外の者に知られないようにすることが重要である。特にコンテンツ選定の手段として投票を用いる場合は、誰がどのコンテンツを希望しているかを、コンテンツ流通業者など利用者以外の者に対して隠蔽できることが望ましい。

3.既存の電子投票方式

コンテンツ流通業者が多数の利用者の希望するコンテンツを調べるための電子投票方式として、Schneier の電子投票方式[1]が挙げられる（図 1）。この方式では、投票者と開票者の二者間で認証・開票し、投票者制限や二重投票防止などを実現する。

しかし、この電子投票プロトコルでは、開票者が投票者名と投票内容を入手できるため、投票者名と投票内容の対応を開票者が把握できてしまう。従って、前章で挙げた要求条件（プライバシー保護）を満たすことができない[2]。



<投票手順>
1.(投票者制限)有権者に対し投票ID(身分証明数)を与え、投票に対する権利を与える(②,③)。
2.(二重投票防止)投票IDにより、投票回数をチェックする(⑥)。
3.(漏洩防止)投票内容を暗号化する(④,⑤)。
4.(改竄防止)デジタル署名、デジタル署名を添付することにより、第三者からの攻撃を防止(⑤,⑧,⑨)
5.(追跡可能性)投票IDと投票者名をリストにして保持することにより、追跡が可能(②)。
6.(公開性)集計結果に対する投票IDの獲得を呈示することにより、投票の正当性を開示する(⑦,⑪)。

図 1　Schneier の電子投票フロー図

4.提案方式

提案方式で扱うコンテンツ配送サービスのシステム構成例を図 2 に示す。投票者、開票者、認証者はそれぞれ利用者、コンテンツ流通業者、認証局に対応する。

投票者のプライバシー保護を考慮した電子投票システムを検討するにあたり、(i)投票者と開票者の間の仲介者の設置と、(ii)投票内容の暗号化鍵の生成者の選定の2点について検討する必要がある。

Privacy-protection method on user's access to their desirable multimedia data
Hiroyuki Soma, Hiroki Tanaka
NTT Information Sharing Platform Laboratories
9-11, Midori-Cho, 3-Chome, Musashino-Shi Tokyo 180-8585, Japan

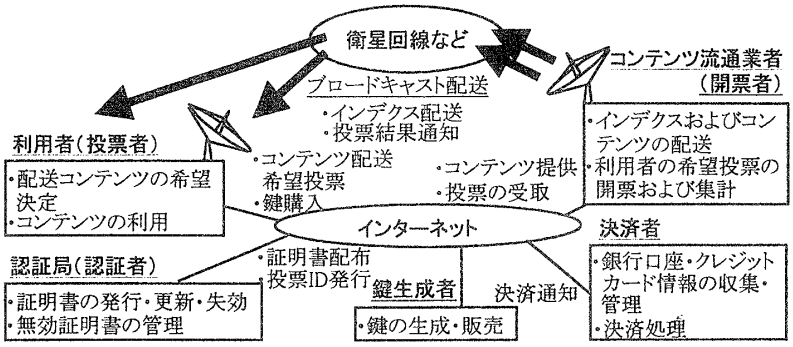


図 2　本コンテンツ配送サービスのシステム構成例

(i) 投票者と開票者の間の仲介者の設置

Schneier の投票システムでは、開票者が投票者名と投票内容を扱うため、投票者名と投票内容の対応が把握できてしまう。ここで、仲介者として認証者を設け、投票者名を扱う認証を認証者に行わせ、投票内容を扱う開票を開票者に行わせる方式を採用する。**投票者と開票者の間に認証者を設けることで開票者に対する投票者名と投票内容の対応の隠蔽が可能になり、開票者に対する利用者のプライバシー保護が実現できる。**

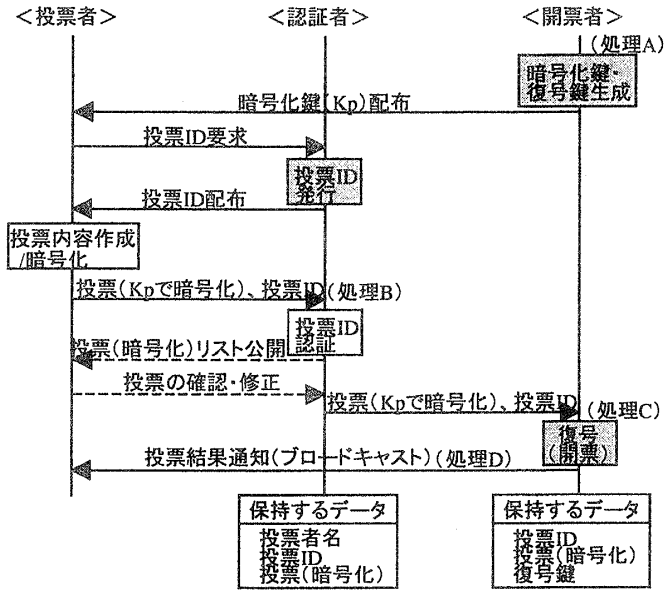


図 3　本提案方式による電子投票方式のフロー図

(ii) 投票内容の暗号化鍵の生成者の選定

(i)の検討結果より仲介者として認証者を設けた場合、認証者は個々の票の投票者を認識できるため、認証者が票の復号鍵を入手できないようにして認証者に投票内容を隠蔽する必要がある。そこで、**開票者が暗号化鍵を生成し、開票者以外の者にはその暗号化鍵を開示しないようにする。これにより認証者に対して投票者名と投票内容の対応の隠蔽が可能となる。**

上記2点の検討結果をふまえた電子投票方式を図 3 に示す。

まず、開票者は公開鍵暗号方式での暗号化鍵（公開鍵）と復号鍵（秘密鍵）を生成する（図 3 処理 A）。投票者は開票者から入手した暗号化鍵（公開鍵）を用いて投票内容を暗号化し、認証者へと配送する。認証者は投票者の認証を行い（処理 B）、開票者へと票を転送する。票を受け取った開票者は、復号鍵（秘密鍵）を用いて開票し（処理 C）、開票結果を全投票者へ同報の形態で通知する（処理 D）。

これにより、利用者以外の全ての者に対して投票者の投票内容を隠蔽でき、プライバシー保護が可能となる。

5.まとめ

多数のサービス利用者の希望コンテンツを調べるために、コンテンツ提供前に予め投票を行うサービスにおいて、配送コンテンツの希望投票時に、投票者を認証しつつ、投票者のプライバシーを保護する方式を明らかにした。投票者と開票者の間に仲介者（認証者）を設け、さらに投票に対する暗号化鍵を開票者が生成することで投票者名と投票内容の対応を利用者以外の者に対して隠蔽できることを示した。

今後、不特定多数の利用者の配送希望を反映したコンテンツ配送サービス向けミドルウェアの実現に向け、提案方式の詳細化を行う。

[参考文献]

[1] Bruce Schneier:, "Applied Cryptography", John Wiley & Sons Inc., 1995

[2] 相馬、田中、小林:「プライバシー保護を考慮した個人嗜好反映型コンテンツ流通方式の提案」、信学会 NA ワークショップ、1998.12