2F－01　個人の匿名性を考慮したアンケート集計方式の考察

小泉 泰則　　中山　賢一†
ＮＴＴ東日本 研究開発センタ‡

１．はじめに

現在、セキュリティー機能を有する電子アンケートシステムや電子投票システムが提供されつつあり、二重受付を防止し且つ受付情報に匿名性をもたせるために暗号を用いたいくつかの方式が取られている[1]、[2]。本稿では、アンケート回答者がどの程度匿名性を必要としているか、回答内容をどの程度個人情報として提供するかにより匿名回答範囲を制御するアンケート集計方式について考察する。

２．電子アンケートシステムの現状

今までの郵便や街頭での情報収集に比べ、簡単で迅速な情報収集を行うことが可能となることから、インターネットを使ってアンケートを収集することが多用されるようになっている。また、収集したユーザからのアンケートをもとに、個々の利用者の嗜好を抽出し、個人の嗜好にあった情報提供を行うことができ、このようなＷｅｂサイトも多くなってきている。

一般の利用者は、アンケートに回答し、商品を抽選でもらえる点や自分の嗜好に適した情報を提供される点から個人名を明記して回答をしたいと考えている。しかし、個人の趣味、支持政党、預金額などの情報は無記名では回答するが、個人を特定される回答には不安を抱いている。そのため、個人の情報として特定されたくない情報を空白として回答するか、アンケート全体の回答を止めてしまうことになり、多数の利用者からの回答が得られないという問題がある。

A Study of method for Collecting　User Information Considering　Concealment
† Yasunori Koizumi　　kenichi Nakayama
‡ Nippon Teregraph and Telephone East Corporation

３．プライバシを考慮した個人情報集計機能

前項の問題を解決するため、回答者それぞれが匿名とする条件を記述することにより、回答者の認証はするが、匿名条件に合致する回答内容は匿名回答として収集するアンケート収集機能を提案する。具体的には、回答者が匿名で送るべき回答の条件として回答項目と集計先での利用方法（以下、秘匿条件と呼ぶ）を記述し、回答者名を特定する回答とする条件として回答項目と集計先での利用方法（以下、公開条件）を記述することで、アンケート回答を収集するサーバに、秘匿条件に適合した回答は回答内容のみ送信し、公開条件に適合した回答は回答者名を付けて送信する。
（図１参照）

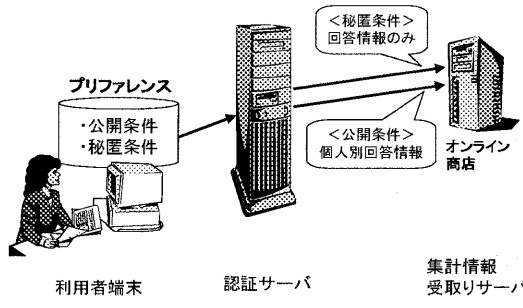

図１ プライバシーを考慮した集計機能

４．実現方式

上記機能を実現するためのシステムは、図１に示す利用者端末、認証サーバ、集計情報受取りサーバで構成される。

４．１ 利用者端末機能

利用者端末（クライアント）には、利用者の公開条件と秘匿条件を記述するプリファレンスファイルを用意する。本プリファレンスファイルは、個人のプライバシーを保護し個人情報を収集する

ための規約としてW３Cの標準として規定されているＰ３Ｐ（Platform for Privacy Preference project：）[3]を用いる。（図２参照）

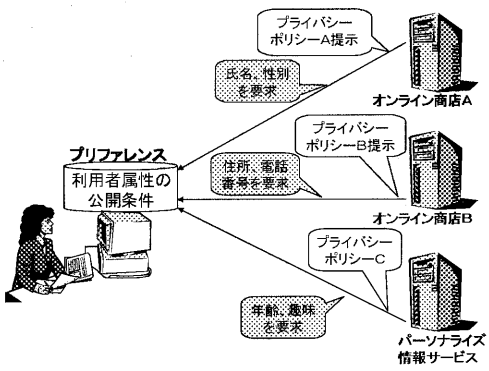

図 2. Ｐ3Ｐイメージ図

Ｐ３Ｐでは、利用者が情報をサーバに送信する時の条件をクライアント側のプリファレンスファイルに記述することになっており、サーバ側のプライバシーポリシと合致させ、合意が取れれば送信を許可する機能をもつ。

本システムでは、Ｐ３Ｐにおける「送信する」、「送信しない」の２条件に、「匿名で送信する」条件を付加する。そして、秘匿条件が合致する場合は、送信時に集計情報受取りサーバの公開鍵を利用して回答内容を暗号化し、認証サーバに配信する。

４．２ 認証サーバ機能

認証サーバでは、送信された利用者からの回答について、回答者認証を行い、二重回答を防止するとともに回答者情報を保存する。次に、秘匿条件の回答に対しては、回答者を識別する情報を削除し、認証サーバの署名を認証サーバの秘密鍵を使い暗号化し、その署名を付加し集計情報受取りサーバに送信する。それにより、集計情報受け取りサーバに対し回答者を認証したことを示す。公開条件の回答については、データに変更を加えず、集計情報受取りサーバへ送信する。

４．３ 集計情報受取りサーバ機能

受け取った、回答のうち、秘匿条件については、認証サーバの署名を認証サーバが公開する公開鍵を利用して複号化し、正当な回答であることを検証する。次に、回答内容を集計受取りサーバの秘密鍵で複号化する。処理の流れを図３に示す。

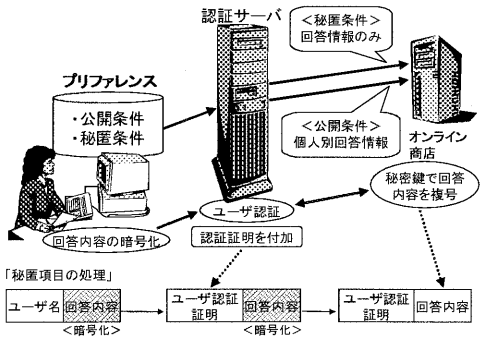

図 3. 秘匿項目処理の流れ

５．考察

本方式により回答者の指定に従った情報の配信が可能となるが、公開鍵暗号を用いているため、リアルタイム性を要求するサービスでは性能上の問題が生ずる可能性があり、リアルタイム性と安全性を考慮したシステムの検討を行う必要がある。

６．おわりに

本研究では、秘匿条件と公開条件を規定することにより、個人に適した情報の収集を行うシステムについて提案を行った。今後、集計サーバでの情報の利用方法を考慮した秘匿条件と公開条件の定義等、利用者の設定を簡単にし、利用者からはより抽象的な情報定義により端末エージェントが具体的な秘匿条件と公開条件を分類する機能について検討を進めていきたいと考えている。

参考文献

[1]小出，多田，他：関連付け可能な匿名オフライン電子マネー，ＤＰＳ研究会,2000 年 3 月

[2]北澤，双紙，他：匿名通信を記述するためのフレームワークについて，DPS 研究会，2000 年 3 月

[3]神場，古関：ｲﾝﾀｰﾈｯﾄﾏｰｹﾃｨﾝｸﾞの技術と応用，人工知能学会誌 15 巻 3 号，2000 年 5 月