マルチメディア通信と分散処理 75－13
（1996. 3. 1）

電子匿名アンケート機構の設計と実装

横川 典子
慶應義塾大学
norinori@sfc.wide.ad.jp

菊池 浩明
東海大学
kikn@ep.u-tokai.ac.jp

村井 純
慶應義塾大学
jun@wide.ad.jp

本稿は、インターネットにおいて「プライバシ侵害」「なりすまし」「多重回答」「改ざん/捏造」などの不正を防止し、匿名性を持った通信を提供するシステムについて述べる。本システムは、「回答エージェント」「認証エージェント」「匿名通信路」「集計エージェント」という4つのモジュールから構成される。RSA 公開鍵暗号に基づく Blind Signature を用いて、結託によるプライバシ侵害、回答の改ざん/捏造を防止し、認証機構を導入することにより、なりすましおよび多重回答を防止する。また、このシステムを用いた、電子匿名アンケート機構の設計とプロトタイプの実装を行ない、本システムの有効性を示す。本システム応用することにより、電子選挙等のプライバシ保護が必要なアプリケーションを実現することができる。

Design and Implementation of an Electric Anonymous Polling System

Noriko YOKOKAWA
KEIO University

Hiroaki KIKICHI
TOKAI University

Jun MURAI
KEIO University

This paper describes a system that eliminate four injustices: "privacy violation", "impersonate", "multi-polling" and "alteration/fabrication". This system is achived by four individual entities called "Agent"s. The mechanism of Blind Signature with RSA public-key encryption is used to detect privacy violation and alteration/fabrication. An authentication system prevents masquarade and multi-polling. A prototype of this system is implemented. This system fulfills the original definition of the term "communication" on communication using computers. With this system, opinions of users can be expressed as reliable anonymous messages on the Internet.

1 はじめに

インターネットは、異なる組織によって管理されるネットワーク同士を相互に接続することによって構築される開放的アーキテクチャを特徴とする大規模計算機網である。この特徴は接続が自由であるという利点の反面、経路上に悪意を持った者が不正行為を行なっていても分からない、という欠点も持つ。インターネットでは電子メールや電子ニュースなど、記名を前提とするアプリケーションが多く用いられて来た。しかし、匿名が必要となるアプリケーションも存在する。電子選挙や電子アンケートはその代表的なものである。これらのアプリケーションは、匿名と同時に認証が必要となる。しかし、認証を厳しいものにすればするほど、匿名性が失われ、匿名を提供すれば認証が不可能になる、という矛盾を持つ。またこれらのアプリケーションは、インターネット上で発生し得る不正行為を防止するものでなければならない。暗号化技術によって、1対1通信におけるインターネット上の不正を防止することが可能である。しかし、WWW (World Wide Web) に代表される「1対不特定な多」型の通信が中心的になりつつある。

本稿では、安全な匿名通信を提供するアプリケーションの一つとして、電子アンケート機構の設計と実装について述べる。本システムは Blind Signature [3] を利用した公開鍵暗号による電子署名を利用することにより、匿名を提供しながら、改ざん/捏造、なりすまし、多重回答といったインターネット上で発生し得る不正を防止する。

2章でインターネットで起こり得る不正行為の定義を行ない、3章でそれらの不正行為を防止しながら、匿名性を提供するためのシステムのモデル化を行なう。4章でモデル化に基づくプロトタイプの実装について述べ、5章でその評価を行なう。

2 インターネットで起こり得る不正行為

インターネットを統合的に管理する組織は存在しない。したがって、インターネットを介して情報を送る際、経路の途中に悪意を持つ者がいて、不正行為を行なう可能性もある。不正行為によって、インターネットユーザのプライバシが侵害される。

安全な電子アンケートを行なうためには、不正行為を防止しなければならない。本章では、安全な電子アンケートを妨害する可能性のある不正行為として、「プライバシ侵害」「回答の改ざん/捏造」「回答者へのなりすまし」「多重回答」の4つを挙げ、それぞれについて説明する。

プライバシ侵害

ある回答 A に関して、A からその回答を作成した回答者 V_A を推測、あるいは特定することを**プライバシ侵害**と定義する。

改ざん/捏造

ある回答 A に関して、その内容を書換えることを、回答の**改ざん**と定義する。また、ないはずの回答を作り上げ、本物の回答であるかのように見せかけることを、回答の**捏造**と定義する。集計者による集計結果の水増しや回答の破棄といった不正行為も、改ざん/捏造の一種として定義する。

なりすまし

回答者ではない者が、回答者になりすましてアンケートに回答することを**なりすまし**と定義する。

多重回答

一人の回答者は1度しか回答することができないアンケートにおいて、回答者 V_A が2度以上回答をおこなうことを**多重回答**と定義する。

3 設計概要

本稿で提案するシステムは、2章で定義した不正行為を防止するものである。本章では、以下の4つのソフトウェアモジュールによって構成される、2つのモデルを定義する。

回答エージェント (Voter Agent)

人間である回答者とのインターフェース的役割を果たし、回答の作成にかかわる処理を担当するエージェント。

認証エージェント (Authenticater Agent)

回答者 A が有権者であるか、また、本当に A であるか、を認証するエージェント。

集計エージェント (Collector Agent)

回答を集め、集計し、その結果を公表するエージェント。

匿名通信路 (Anonymous Tunnel)

匿名通信路の目的は、集計エージェントおよび第三者による、回答者のプライバシ侵害を防止することである [4]。回答と回答者との結び付きを断つために、匿名通信路には以下の要素が必要となる:

- 集計エージェントによるプライバシ侵害の防止
- トラフィック解析からの回答者のプライバシ侵害の防止

回答の発信者が回答者本人であると、集計エージェントに回答と回答者との結び付きを知らせてしまうことになる。したがって、匿名通信路は、回答の発信者を匿名通信路自身に書き換えてから、集計エージェントへ中継する必要がある。しかし、匿名通信路が、送られてきた回答の発信者を書き換え、そのまま集計エージェントへ送るだけでは、匿名通信路の前後のトラフィックを解析し、匿名通信路へ送られてきた回答の順序を記憶しておくことによって、集計エージェントへ送られてきたどの回答がどの回答者/回答エージェントから発せられたものであるかを知ることが可能になる。匿名通信路は、トラフィック解析からも回答者のプライバシを保護しなければならない。

以上の要求を満たすためには、Chaum の提案した MIX-NET[3] による以下の方法がある:

1. 回答エージェントから情報を受け取ると、発信者を自分に書き換え、情報が入って来た順序とは無関係に、ランダムな順序で集計エージェントへ転送する。匿名通信路に必要な要素のうち、**トラフィック解析からの回答者のプライバシ侵害の防止**という要求を満たす

2. 回答エージェントから情報を受け取ると、発信者を自分に書き換え、任意の個数の匿名通信路をカスケードしたのち、集計エージェントへ転送する。匿名通信路に必要な要素のうち、**匿名通信路の結託の防止** という要求を満たす

3.1 モデル 1:認証エージェントと匿名通信路を用いたモデル

回答エージェントは作成された回答 A をもとに、Message Digest などの一方向性関数を用いて、数学的に回答の要約を計算し、認証エージェントへ送る。認証エージェントは認証を行ない、署名を返す。回答エージェントは署名と回答を匿名通信路経由で集計エージェントへ送る。集計エージェントは署名の検証を行ない、回答を公開する。

認証エージェントによる署名は、公開鍵暗号の秘密鍵を用いて行なわれるため、捏造することはできない。回答は匿名通信路を経由して送られるため、集計エージェントは、回答から回答者または回答エージェントを特定することはできない。また、集計エージェントによって署名の検証が行なわれる子とにより、認証エージェントの署名が正しいものであったか、また、回答が改ざんされていないかを確認することができる。

モデル 1 の概要を図 1 に示す。

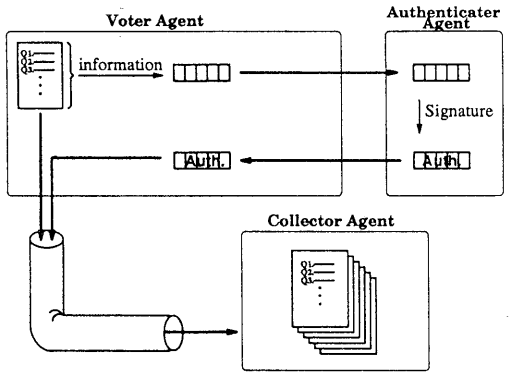

図 1: 認証エージェントと匿名通信路を用いたモデル

結託問題

回答エージェントは、回答者の認証情報と回答の要約を認証エージェントへ送る。認証エージェントは、回答そのものの内容は知ることができないが、認証情報から回答者を特定することが可能であり、要約と回答者との対応をすることができる。一方、集計エージェントでは認証エージェントの署名つきの要約と、回答から直接計算した要約が一致するかを確認することによって署名の検証を行なっており、回答者そのものを知ることこそできないが、回答と回答の要約を知ることができる。したがって、集計エージェントが、ある回答の要約をもって認証エージェントへ問い合わせを行なった場合、その回答の回答者が集計者に露見し、回答者のプライバシ侵害が起こる可能性がある。

集計エージェントと認証エージェントが結託して回答者のプライバシを侵害することを**結託問題**と定義する。認証エージェントと匿名通信路を用いたモデルは、新たに結託問題を生むことになる。

3.2 モデル 2: Blind Signature を用いたモデル

結託問題を解決するためには、回答の要約の内容を知られることなしに、認証エージェントの署名をもらう必要がある。Blind Signature を用いることにより、この機能を提供することが可能である。Blind Signature は、プライバシを保護したまま 電子署名を行なうための方法であり、Chaum によって提唱された方法である。Blind Signature の概要を以下に示す:

1. ユーザは、各秘密にしたい要素 (メッセージなど) X に対し、秘密の乱数 R を設定し、記録する。Rを認証者の公開鍵 e で暗号化する (R^e)。そして Xに Rをかけ、$X \cdot R^e \pmod n$ として認証者に送る。R はユーザしか知らない秘密の要素であるので、認証者は $X \cdot R^e$ から X を知ることはできない。

2. 認証者は送られて来たもの $(X \cdot R^e)$ に自分の秘密鍵 d で署名をし、$(X \cdot R^e)^d \pmod n$ としてユーザに送りかえす。

3. ユーザは $(X \cdot R^e)^d$ に乱数 R の逆数を掛け、X^d を得る $((X \cdot R^e)^d \cdot \frac{1}{R} \pmod n = X^d \cdot (R^e)^d \cdot \frac{1}{R} \pmod n = X^d)$。

集計エージェントが要約から回答者を特定しようと思っても、認証者と結託することはできない。秘密の乱数 R の上から署名を行なうため、認証エージェントはその回答者がどのように要約された回答を持っているのかを知ることはないからである。この方式は、結託問題を解決している。Blind Signature を用いたモデルの概要を図 2に示す。

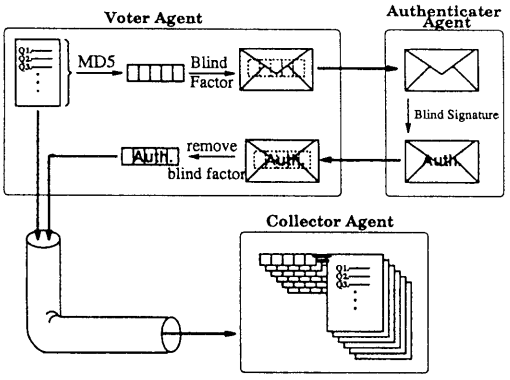

図 2: Blind Signature を用いたモデル

3.3 モデル化のまとめ

認証エージェントと匿名通信路を用いたモデルでは、プライバシ侵害、改ざん/捏造、なりすまし、多重回答の全ての問題を解決することができる。しかし、新たに認証エージェントと集計エージェントによる**結託問題**が発生する。結託問題は、Blind Signature の概念を導入することにより、解決できる。

4 プロトタイプの実装

3 章で定義した 2 つのモデルのうち、モデル 2 に基づいてプロトタイプの実装を行なった。実装したのは回答エージェント、認証エージェント、匿名通信路、集計エージェントの 4 つである。設計の概要を図 3に示す。

それぞれのエージェントおよび匿名通信路は perl を用いて実装し、Blind Signature 手続きは RSA[2] のパッケージを用いて C 言語によって実装した。各エージェント間プロトコルには HTTP[5] を利用し、認証エージェントおよび集計エージェントは WWW の CGI スクリプトとして実現した。

4.1 回答エージェント

回答エージェントは、回答者によって起動されるエージェントであり、以下の 2 つのモジュールによって構成される:

- ユーザインターフェースモジュール
- プロセスモジュール

ユーザインターフェースモジュールは、回答エージェントを構成する機関のうち、回答者と直接やりとりを行なう部分である。ユーザインターフェースモジュールとして、WWW クライアントを利用した。

プロセスモジュールは、Blind Signature 手続きで、その回答エージェント固有の秘密要素を計算する。これらの秘密要素を第三者、あるいは認証エージェント、集計エージェントが知ることにより、回答者のプライバシ侵害が起こる。以上の理由から、プロセスモジュールを全ての回答者に共通するサーバにはせず、回答者がそれぞれの権限で立ち上げることのできるサーバとして実装した。プロセスモジュールはユーザインターフェースモジュールを起動するほか、Blind Signature 手続きの処理や、認証エージェントおよび集計エージェントとの通信を行なう。プロセスモジュールの行なう処理を以下に示す:

1. 回答から MD5 を用いて要約を計算する
2. Blind Signature 手続きを行ない、認証情報をユーザインターフェースモジュールへ送る
3. 認証エージェントから認証結果を受け取る
4. 回答を匿名通信路へ送る
5. 匿名通信路からレシートを受け取る

集計エージェントが回答を公開する際、認証エージェントの署名を識別子として同時に公開する。プロセスモジュールが、認証エージェントから署名を受け取ると、それをファイルとして保存しておくことにより、回答者は署名を識別子として公開された回答を検索し、自分の回答が正しく公開されていることを確認することができる。

4.2 認証エージェント

認証エージェントは、回答エージェントから回答の要約と認証情報を受けとり、その結果を返す役目を果たすエージェントである。認証エージェントは以下の 2 つのリストをもつ:

- 有権者リスト
- パスワードリスト

有権者リストとは、ある回答者に対して、その回答者が未回答であるかどうかをチェックするために用いられるリストである。パスワードファイルは、回答エージェントから送られてきた認証情報 (パス

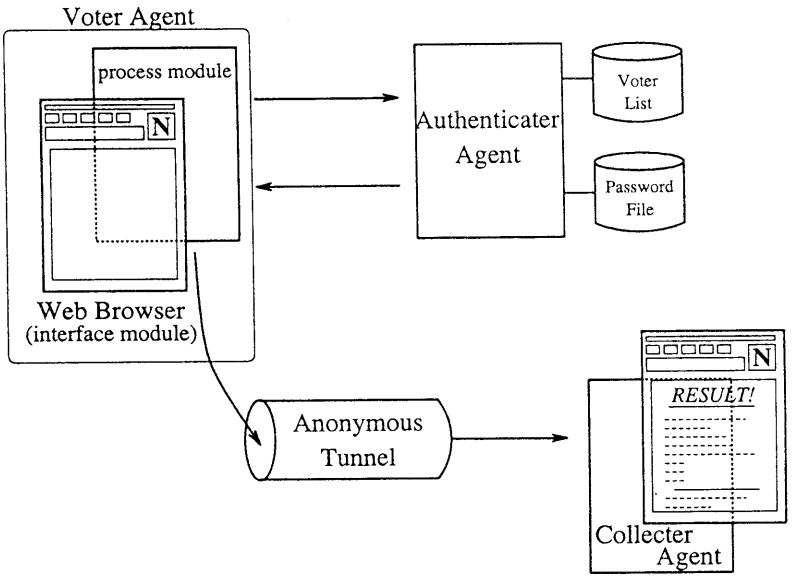

図 3: システム実装概要

ワード) が、正しいものであるか検証する際に参照される。

有権者リストによって多重回答を、パスワードファイルによってなりすましを防止することが可能になる。

4.3 匿名通信路

匿名通信路の目的は、回答エージェントのプライバシを保護したまま、回答を集計エージェントへ送り届けることである。プロトタイプでは、以下に示す方法で 3章で定義した匿名通信路の必要条件のうち、**集計エージェントによるプライバシ侵害の防止**を満たす実装を行なった。

1. 回答エージェントから情報を受けとる
2. 回答エージェントへ受けとり証明を返す
3. ランダム時間待つ
4. 自分を発信者として、回答を集計エージェントへ送る

4.4 集計エージェント

集計エージェントは、回答エージェントから匿名通信路を経由して、回答を受けとり、集計結果を公表する役目を果たすエージェントである。集計エージェントは認証エージェントの署名の検証を行ない、正しいものであると確認したのち、回答を公表する。署名の検証は以下の手順で行なわれる:

1. **認証エージェントの署名の復号化**: 認証エージェントの公開鍵で署名を復号し、回答の要約 p を得る
2. **回答の要約の計算**: 匿名通信路経由で受け取った回答から要約 q を得る
3. **署名の検証**: p と q を比較する。一致すれば、改ざんが行なわれていないことがわかる

回答の公開は、WWW で行なわれる。この時、認証エージェントの署名を回答の識別子として、同時に公開する。

5 評価

本システムは、ユーザ (回答者) の直接的な行動 (ボタンをクリックする、アンケート用紙に記入する、など) が状態変化の要因となるため、システム全体を評価するのではなく、ユーザの直接的な行動

表 1: 必要とされる処理時間

(単位:秒)

時間	回答エージェント			認証エージェント	匿名通信路	集計エージェント	
	認証		BS			署名の検証	
	なし	あり				あり	なし
実経過時間	0.1	0.1	0.3	0.9	0.6	0.3	0.1

によって区切られる、各要素についての定量評価を行なった。

必要とされる処理時間の測定をおこなった(実行した計算機:Sun Sparc Station 20)。なお、これらの値は一度に1つの回答しか処理しない場合の値であり、ユーザの直接的な行動に必要とされる時間は含まれない。測定はコマンド `time` を用い、各50回実行して1回の回答あたり必要な処理時間の平均をとったものである。それぞれに必要とされた処理時間を表1にまとめる。

各モデルが必要とする処理時間の予測値は、モデル1で1.9秒、モデル2で2.2秒である。Blind Signature処理を入れても0.3秒多く必要になるのみである。また、ここで示す時間は、あくまで1つ回答が終了するまでに必要な処理時間の合計である。ひとつひとつの処理の間にはユーザの直接的な行動が必要とされるため、ユーザが実際に体感する時間は分割される。

また、表1から、認証エージェントの認証処理に多く処理時間を必要としていることがわかる。これは認証エージェントが、2つのファイルに基づく2つの認証を行なっていることに起因する。また、匿名通信路にかかる処理時間も大きいが、匿名通信路は回答エージェントから回答を受け取るとすぐに受け取り証明を返すため、匿名通信路および集計エージェントが必要とする処理時間は、ユーザである回答者には体感されない。

プロトタイプの実装では、認証エージェント、匿名通信路、集計エージェントをそれぞれ一つずつしか置いていない。したがって、全ての回答がこれらのエージェントへ集中することになる。システムの規模性および耐久性の向上のためには、それぞれのエージェントを複数置くことによる負荷分散が必要になる。

6 結論

インターネットにおける「1対不特定の多」型通信で起こり得る不正行為を防止しながら、匿名通信を提供するシステムを構築した。本システムでは、問題点を以下のように解決した。公開鍵暗号とメッセージダイジェストによる署名を用いて、回答者による回答の改ざん/捏造を防止した。認証エージェントを認証を行なう専門のエージェントとして独立させ、回答者へのなりすましや、多重回答を防止した。また、匿名通信路が回答と回答者の関係を隠蔽し、回答者をプライバシ侵害から保護した。さらに、集計エージェントと認証エージェントの結託を防止するため、RSA 公開鍵暗号に基づく Blind Signature を導入した。

本研究によって、回答者はアンケート用紙を集計する組織および人間の存在を気にすることなしに、自由に意見を表現できるようになり、「自由な発言が可能な社会」をインターネット上に築くことが可能になる。

プロトタイプシステムとして、単一の認証エージェントおよび単一の集計エージェントを用いたモデルを実装した。規模性や耐久性を提供するために、複数のエージェントによるシステムの構築は今後の課題である。

参考文献

[1] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[2] Rivest, R. L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptsystems", Communications of the ACM, Vol21, No.2, pp.120-126, Febrary, 1978

[3] D.Chaum, Security without Identification: Transaction systems to Make Big Brother Obsolete, Communications of the ACM, Vol.28, No.10, pp.1030-1044, 1985

[4] 菊池 浩明, 飯島 良行: "かきまぜるネットワーク ~PEMを応用した匿名選挙の試み~", WIDE 11月研究会 (1994)

[5] T.Berners-Lee, *Hypertext Transfer Protocol - HTTP/1.0*, INTERNET-DRAFT, December 1994.