ウェブベースドな匿名認証システム
– プログラミング・シンポジウムでのアンケート収集 –

疋田敏朗[†] 副田俊介[††] 繁富利恵[††]

匿名認証を用いたウェブベースドなアンケートシステムの開発について検討を行う．筆者らは従来から匿名認証ライブラリ SENSU を用いたアンケートシステムを開発しており，プログラミングシンポジウム等でデモを行ってきた．SENSU を含め，匿名認証技術は利用者の匿名性を守りつつ，権利の有無を確認を行うことが可能な仕組みである．こういったシステムの多くは，利用者側での計算と秘密の保持を必要とする．これを実現するため，従来のプログラミング・シンポジウムでのアンケートシステムは，認証およびアンケートの集計を行うサーバと，アンケートシステム利用者の端末で動作する専用クライアントソフトウェアから構築されていた．しかし，アンケート専用のソフトウェアをインストールすることは利用者にとって心理的な負担となる．また，サービスを提供する側から見ても，各プラットフォーム（Windows, Mac OS, Linux 等）ごとに専用のアプリケーションを準備するのは負担となる．一方，通常のウェブベースドなアンケートシステムは構築・利用は容易であるものの，利用者のプライバシへの配慮はほとんどなされていない．これは，利用者の安全性が犯されていると言うことに他ならない．そこで，本論文では匿名認証を用いたウェブベースドなシステムを実現する方法を複数提案し，それらの比較を行った．また， SENSU を用いたウェブベースドなアンケートシステムを構築する方法について述べ，利用者のプライバシを守りつつ容易に利用できるシステムの構築を行うことが可能であることを示した．

Anonymous Authentication for Web-based Systems: Its Application in Questionnaire of Programming Symposium

Toshiro Hikita,[†] Shunsuke Soeda[††] and Rie Shigetomi[††]

In this paper, we discuss how anonymous authentication can be used together with web-based systems. The authors have been developing the SENSU anonymous authentication system, and been using it in the electronic questionnaire system of the Programming Symposium. By using SENSU, the user can authenticate himself without revealing his identification. As with many other cryptographic systems, SENSU requires cryptographic calculation conducted under the user's supervision. In our previous system, the users were required to install a client system to use the electronic questionnaire system, which reduced the usability of the system. One approach to increase the usability of the questionnaire system is to make the electronic questionnaire system, web-based. However, blindly making a web-based questionnaire has no guarantee on protecting the privacy of the user, potentially threatening the safety of the user. This year, we propose a web-based questionnaire system using SENSU. We have proposed and compared several models that represent anonymous authentication system used with web-based systems. Based on this comparison, we have suggested how to build a web-based questionnaire system using SENSU, showing that the users' privacy could be protected without reducing the usability of the system.

† 株式会社 トヨタ IT 開発センター
Toyota InfoTechnology Center, Co., Ltd.
hikita@jp.toyota-itc.com

†† 独立行政法人 産業技術総合研究所
Advanced Institute of Science and Technology
{shunsuke.soeda,rie-shigetomi}@aist.go.jp

1. はじめに

近年の電子情報の普及に伴い，様々な種類の情報が容易に利用できるようになっている．同時に様々な情報漏洩問題も生じてきており，情報の扱う方法を検討する重要性が増してきている．そのような中，プライバシ保護を実現するための暗号プロトコルが様々な提案されている[2),4)]．SENSU[6)] はプライバシ保護を実現するための匿名認証プロトコルの一種， Refreshable Token Scheme[4),5)] を実装したシステムで，一回利用した権利を再利用することが可能なであるといった特徴を持ち，様々なサービスを実現することが可能である．

プライバシ保護を実現する上ためには，ある個人に関するプライバシ情報を，その個人自身が把握・管理できるようにすることが必要である．匿名認証もこの概念に基づいて設計されており，認証を受ける人が，自分の ID がどのように扱われているかを確認・管理できる仕組みとなっている．そのため，プライバシ保護を実現するためのシステムは，システムを利用する個人 (**利用者**) の側でも暗号計算を行うことような設計をすることが多い．例えば SENSU も，利用者で離散対数計算を行う設計になっている．

一方で，このような計算を利用者の側で容易に行えないような場合も考えられる．従来のプログラミング・シンポジウムのアンケートシステムでは，利用者の側で暗号計算を行ってもらっていたため，専用クライエントソフトウェアの利用を強制していた．これは利用者の利便性を大きく損ねるものであり，実際，改善の要望が強かった．また，利用する端末の種類によっては，そもそも利用者側が暗号計算を行だけの計算能力を持たない場合も考えられる．

本論文では，プログラミング・シンポジウムのための電子アンケートシステムの構築を念頭に置きつつ，利用者の利便性とプライバシ的な安全性を両立する方法について比較・検討を行った．利便性を確保するための方針としては，ウェブベースドなシステムをベースとし，プライバシ保護に関する暗号計算・秘密の保持の問題を解決するため，信頼できる第三者 (Trusted Third Party, **TTP**) を仮定した．このようなシステムを実現する方法には様々なものが考えられるが，本論文ではそれらを 4 つのモデルで表現した．また，その中で利便性を重視し，TTP へ強い仮定を要求するモデルを基本として，プログラミング・シンポジウムのためのウェブアンケートシステムを構築する方法について述べた．

2. 背　　景

本節では，電子アンケートシステムへの需要と，筆者らのプログラミング・シンポジウムでのプライバシ保護への取り組みについて述べる．

2.1 電子アンケートシステム

アンケートは，直接参加者からの声を集めることができる手段であるため，様々なシステムの運営を改善する方法として有効である．実際，多くの学会・研究会においても参加者からアンケートによるフィードバックを集めることで運営方針を検討することが行われている．アンケートを行う方法は複数考えられるが，一般的な方法はアンケート用紙を配布し回収する方法である．

このような，従来からの，紙を用いたアンケートの方法を紙ベース方式と呼ぶことにする．紙ベース方式では，アンケート用紙の配布を一人に一枚に限定することで，一人一票の投票も同時に行うことが可能となる．

一方で，紙を利用せず，電子的にアンケート (電子ベース) を行う方法も考えらる．紙ベース，電子ベースそれぞれの利点や欠点があると考えられるが，プログラミング・シンポジウムは性格上，紙ベース方式よりも電子的ベースの方が良いと考えられる．

まず，参加者の多くが電子的な端末を持参している上，その扱いに習熟している．日常的にも，紙ベースの処理よりも電子ベース処理が多い，電子ベース方式の方が紙ベース方式よりも抵抗が少ない参加者も多いと考えられる．

また，運営者から見ても，紙ベース方式の場合，回収した後のアンケート用紙の集計作業は一枚一枚の確認のため煩雑であり，人為的ミスが起こりやすいことも問題がある．その他にも環境保護の面 (電子ベース方式に完全に移行すれば紙の消費を抑えることが可能)・「個人情報保護」の面 (かさばる，記入済のアンケート用紙を適正に管理しないといけない) などでも電子ベース方式が紙ベース方式よりも優れている．

しかし，プログラミング・シンポジウムにおけるアンケートについて，紙ベース方式と同等の機能を持つ電子ベース方式のものを提供するた

図 1 へぇぶぅボタンデモ (第 45 プログラミング・シンポジウム)

めには，大きな課題がある．従来の紙ベースのアンケートは，賞の選考の参考にするための投票を兼ねており，同様なことを電子ベース方式で実現するためには，多重投稿を禁止するための仕組みを導入する必要がある．一方で，より真意に近い回答を確保するためアンケートは匿名で行いたいという需要や，紙ベース方式と同じくらい容易に利用できるようなシステムにしたいといった需要も存在する．

以上をまとめるとプログラミング・シンポジウムで必要とされるアンケートシステムは以下の要件を満たす事が必要と考えられる．

- 電子的にアンケートへの回答が出来る
- 匿名性が担保されている
- 多重投稿が防止できる

2.2 プログラミング・シンポジウムにおける取り組み

筆者らは，2003 年より，Refreshable Token Scheme[4),5)] を基にしたシステムの提案，及びそのデモをプログラミング・シンポジウムにて行ってきた．当初は，2ch のような匿名掲示板システムのデモを行っていた[6)]．その際に，匿名性は掲示板よりも直接他の人を評価するようなシステムに必要であるとの指摘いただいた．そこで，翌年，発表の人気度を測るシステム「へぇぶぅボタン」(図 1) の提案を行い，そのデモを行った．

また同時に，Refreshable Token Scheme を基とした匿名認証ライブラリ作成プロジェクトを立ち上げ，SENSU プロジェクトとした[3)]．

プログラミング・シンポジウム向けの電子アンケートシステムは 2005 年より提供している．このシステムは SENSU を用いることで，ユーザのプライバシを守る工夫を行っていた．この従来の電子アンケートシステムは TTP を一切仮定せず，3.2 節で説明するような利用者側の暗号計算と秘密の保持を，利用者の端末で行う前提で設計されていた．これを実現するために，利用者には専用のクライエントソフトウェアを端末にコピーして利用してもらう仕組みを採用していた．準備した専用のクライエントソフトウェアは Microsoft Windows 用のものと，Linux 用ののものと二種類あった他，それ以外の環境の人や，プライバシが本当に確保されているか確認したい人のためにソースコードでも提供していた．しかし，専用クライエントソフトウェアの使い勝手について，不満を感じる利用者も少なくなかった．また，他の環境 (例えば MacOS X) 向けのクライエントソフトウェアも準備されていない等の問題点があった．

3. 匿名認証システム

本節では，匿名性を保証しつつ，認証を行う匿名認証プロトコルについて説明した後，匿名認証プロトコル Refreshable Token Scheme を実装した SENSU について説明する．

ここでの匿名性とは，匿名 FTP などで行われているような無認証とは違うもので，暗号技術等を利用して，利用者自身が匿名であることを確認できる性質を指す．また，ここでの認証とは，利用者が正当な秘密鍵を保持しているかどうかの確認をする手順のことである．

3.1 暗号を利用した匿名認証プロトコル

暗号を利用した匿名認証プロトコルは，既存に普及している同様な仕組みと比べ，様々な特徴を持つ．既存の方式としては，ワンタイムパスワードを利用した方式や仮名を利用する方式が挙げられる．

ワンタイムパスワードを利用した方式とは，認証が必要なたびに，TTP(ワンタイムパスワード発行団体) によって発行されたワンタイムパスワードによって認証を行う方式である．また，TTP(仮名発行団体) が発行した権利書，つまり仮名 (Pseudonym) を利用する方式を利用する方法も存在する．どちらの方法でも，TTP は利用者の確認を行う (個人を特定する) が，どのようなサービスを提供されたのかは知らず，また，サービス提供者は提供されたサービスは知っているが，誰に提供したのかについては特定できない．このようにして，提供されたサービスと提供された個人が結びつかないようになっている．

しかし，これらの方式は，TTP とサービス提供者が結託してしまえば匿名性は保証されない．特に，仮名を利用する方法に関しては，一旦仮名と個人とが結びつけられてしまったら，その

個人に関する匿名性は完全になくなってしまう．

一方，暗号に基づいた匿名認証は，権利発行者であっても匿名性を破ることが不可能である．従来の方式では，TTP とサービス提供者とが結託しない仮定が必要であったが，匿名認証の場合にはその保証は必要ない．そのため，サービス提供者と権利発行者が同一主体でも匿名性に問題は生じない．

匿名認証システムの多くはゼロ知識証明等の技術を基礎として構成されており，知識のあるユーザは自分で計算プロトコルと確認することで，実際に匿名性が保証されていることを確認できる．

なお，本論文で述べる TTP を利用して匿名認証を行う場合，TTP に関する仮定は従来の方式と同じだけ必要であり，この点だけに注目すれば従来と同じ強さの仮定が必要である．しかし，利用者が信頼できる第三者機関を見つけることができなかった場合，自分の端末で専用アプリケーションを用いて認証を行う選択肢をとることも可能なので，匿名認証を利用したシステムの方がプライバシ保護の観点では優れている．

3.2 SENSU プロトコル

SENSU は，繁富が提案した Refreshable Token Scheme を基とした匿名認証ライブラリプロジェクトである[4)~6)]．

暗号を基とした匿名認証プロトコルとしては，Blind Signature や，Group 署名など様々な種類が提案されている[1),2),4)]．その中でも，Refreshable Token Scheme は，匿名 TOKEN と呼ばれる権利証を認証に利用する．ここで，この TOKEN は下記のセキュリティ要件を満たしている:

Definition1

- (Anonymity, Refreshability) この匿名 TOKEN は，Refresh 機能を持ち，匿名でありながら権利の更新をすることができる．
- (Double-Use Traceability) 二重使用者を不正利用と仮定し，匿名で二重 TOKEN を提示してた場合は，たとえ Refresh 後であっても，名前を追跡することができる．
- (Unforgeability) 権利証は，権利作成者以外の人が作成することができない

暗号を基にした匿名認証プロトコルは様々提案されているが，下記の理由により，プログラミング・シンポジウムのシステムにおいては，SENSU を利用する．

- Refresh することができるため，一回投稿したアンケートを取り下げた上で，改めて投稿することが可能である．また，その際に ID を提示する必要はないため，これを匿名のうちに行うことが可能である．
- 既に開発が行われており，容易に利用でき，他の匿名認証プロトコルを改めて実装することと比べてコストが低い．

4. 匿名認証を使用したウェブアンケートシステムのモデル化

本節では，匿名認証を使用したウェブアンケートシステムを実現する方法について説明する．匿名認証を行おうとした場合，サービス提供者側の方だけでなく，利用者の方でも暗号計算を行う必要がある．一方で，ウェブアンケートシステムの端末では様々な理由により，暗号計算を行うことができなかったり，できたとしても制限がかかる場合がある．例えば，携帯電話のような端末ように，端末自体の計算能力が限られている場合がある..

端末で暗号計算を行うことができない場合は，TTP に暗号計算を依頼する方法が考えられるが，この場合には利用者の秘密を TTP に渡すことになるため，TTP に関しては強い仮定が必要となる．つまり，利用者の端末にどの程度の計算能力があるか (どの程度暗号計算を行うことが可能か)，TTP を利用することができるか等の仮定により，実現可能な方法，より良い方法は異なる．ここでは 4 つの方法について説明し，それぞれの利点と欠点について説明する．

4.1 専用アプケーション

ここでは，匿名認証のための暗号計算を行う専用アプリケーション等を利用する方法 (図 2) について述べる．このモデルでは，匿名認証に必要な計算やデータの保管について，利用者側で必要なものを，全て利用者の端末上で実現できると仮定する．なお，ブラウザにプラグインを追加するの方法も専用アプリケーションを利用するモデルの一種として考える．

専用アプリケーションモデルでは，匿名認証にかかわる処理は全て利用者の管理下で行う．利用者の秘密鍵の生成や保管・秘密鍵を利用した暗号計算は全て端末上で行うため，TTP を仮定する必要がない．このモデルは，利用者の秘密鍵を外部に渡す必要がないため，安全性に関す

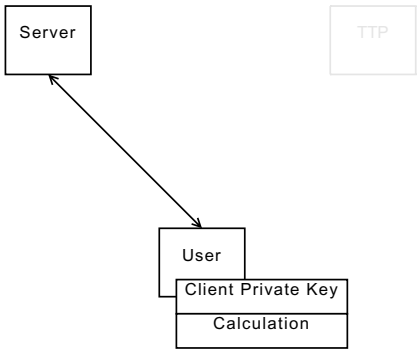

図 2 専用アプリケーションを利用するモデル

る仮定を少なくすることが可能である．

一方で，利用者の端末は暗号計算を行うため，端末の処理能力が処理にかかる時間に影響する．そのため，計算能力が低い端末では利用することが難しい可能性がある．また，暗号計算を行うためのプログラムやプラグインを別にインストールすること必要があるため，利用者の心理的な抵抗もあると考えられる．

匿名認証技術が一般化し，匿名認証に関する統一的な規格が策定されれば，それに基くアプリケーションやプラグインが普及することが考えられ，そうなった場合には別プログラムをインストールする心理的な障壁はなくなる．また，近年の計算機の能力の向上には目覚しいものがあるため，将来的には計算能力が問題となる場合も減ると考えられる．

4.2 アプレット

ここでは，サーバから端末にダウンロードされて実行されるプログラム (アプレット) で，匿名認証に関する端末側の処理が行われるモデルについて述べる (図 3)．このモデルでは，利用者の端末上で必要な計算を行うことが可能だが，通信やデータの記録については制限されていると仮定する．なお，JavaScript 等のブラウザ上で実行されるスクリプト言語もこのモデルで扱う．

アプレットは，実行される端末のハードウェア的なアーキテクチャに様々なものが考えられることもあり，中間言語で配布され，その中間言語を実行する仮想的なアーキテクチャ(仮想マシン，VM) で実行されることが多い．そのため，実行速度は専用アプリケーションモデルと比べて遅くなることが多い．また，サーバから提供されたコードが信用できるとは限らないため，アプレットの実行には様々な制限がかけられることが多い．例えば，Java の Applet や Adobe Flash 技術を利用した場合，(原則として) 端末のローカルファイルにデータを記録することも，アプレットを提供したサーバ以外のサーバと通信することもできない．

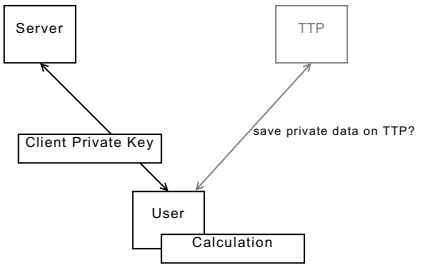

図 3 アプレットを使用するモデル

アプレットは，表現できる計算の自由度は高いため，暗号計算に必要な計算を行うことが可能である．また，多くの場合にはウェブページをアクセスすれば自動的にダウンロード・実行されるため，ウェブベースドシステムの簡便性を損ねる要素は少ない．

一方で端末のローカルファイルに情報を記録することができないため，匿名認証に利用する秘密は，メモリ上にセッション単位の寿命で保管することになる．そのため，セッション中に計算が中止されるような事故が発生した場合は，利用者の秘密鍵や計算途中の TOKEN 等，認証に必要な権利自体が失われてしまうこともありうる．

また，セッションを越えての処理が現実的でないため，いくつかのサービスの実現が不可能となる．一回投稿したアンケートの再投稿のようなサービスをを利用するためには，センションを越えて秘密を保持しておく必要があるが，アプレットを利用した場合にはそれは難しい☆．

4.3 計算外注モデル

ここでは，匿名認証のための暗号計算を，TTP で行う方法 (図 4) について述べる．このモデルでは，利用者側の秘密については端末の方で保管し，必要に応じて TTP に渡す一方で，匿名認証に必要な利用者側の計算は TTP 上で行うと仮定する．また，後に述べる認証アウトソーシングモデルと異なり，TTP とサーバとが直接通信

☆ ユーザがコピー アンド ペーストで必要な情報をメモしておく方法等が考えられるため，不可能ではない．

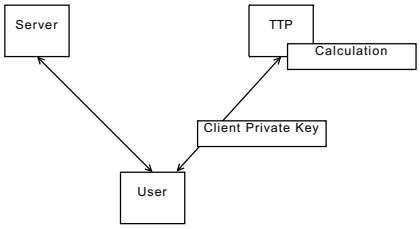

図 4 計算外注モデル

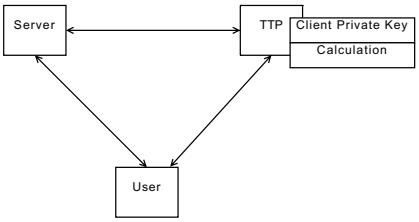

図 5 計算アウトソーシングモデル

しないと仮定する．このモデルでは，端末が外部の TTP サーバに計算を委託する方法や，認証を行うためのスマートカード利用する方法等を扱う．

計算外注モデルでは，認証に必要なデータは端末で管理し，認証に関する暗号計算が必要になるたびに，端末から TTP へと計算に必要なデータを渡す手順をとる．TTP は計算が終了したら，端末に結果を返すとともに，端末から受け取ったデータは破棄する．

このモデルでは，サーバとの通信は端末を必ず経由する．そのため，利用者は自分の秘密情報がどのように扱われているかが理解し易い．また，端末では暗号計算を行わないため，端末の計算能力が低くても実現することが可能となることが挙げられる．

一方で TTP を仮定する必要があるため，セキュリティに関する要求は前に述べた二つのモデルより厳しくなる．また，端末にデータを管理する能力や，必要に応じてサーバ・TTP と通信する必要があり，例えばウェブベースドシステムで実現しようとすれば利用者に煩雑な操作を要求することになる．

4.4 認証アウトソーシングモデル

ここでは，匿名認証のための処理を全て TTP で行う方法 (図 5) について述べる．このモデルでは，匿名認証に必要な計算や情報の保管のうち，利用者に関係するものは全て TTP の上で実現する．また，認証に関する通信も TTP とサーバとの間で直接行われると仮定する．

認証アウトソーシングモデルでは認証に関する手順は TTP とサーバの間で行い，端末は，その時点での計算の経過を示すデータのみを各サーバとやり取りする．計算の経過を示すデータが盗聴された場合，権利も盗まれてしまうため，端末とサーバとの通信にはセキュアチャネルを用いる必要がある．

この方法では，端末が認証に必要な機能は基本的なデータ通信機能だけになるため，例えば計算の経過を示すデータを URL の形で与えれば，ウェブブラウジング機能のみを登載した端末でも利用することが可能となる．

一方で，TTP とサーバが直接通信するため，利用者側からサーバと TTP が結託していないことを確かめることが非常に難しい．その上，暗号計算や利用者の秘密が全て TTP 上に置かれるため，利用者は実際にどのように認証が行われているかを把握することも困難である．そのため，TTP に関しては非常強い仮定を置く必要がある．

4.5 比　　較

本節では，いままで見てきた 4 つの手法について，以下の観点から比較を行う．

- ユーザの利便性
- 実装にかかるコスト
- セキュリティ

4.5.1 ユーザの利便性

専用アプリケーションについては，アプリケーションをダウンロードして使用するという手間がかかるので利便性やアプリケーションの信頼性面でユーザに対して抵抗を与えると考えられる．

アプレット，計算外注モデル，認証アウトソーシングモデルについては一般的に利用されているブラウザを利用するため，導入に関する抵抗は少ないと考えられる．一方で計算外注モデルに関しては，秘密鍵ならびに TOKEN をユーザが明示的にアップロード指示，ダウンロードという作業を行う必要があり，作業に対しての抵抗が有る可能性がある．

アプレット，認証アウトソーシングモデルに関してはユーザ作業は初期コードの入力だけであることから導入への抵抗は少なく，ユーザ利便性が高いと考えられるが．

4.5.2 実装にかかるコスト

SENSU ライブラリは現在 C で実装されている．

そのため，ネイティブ C で実装可能な計算外注モデルと認証アウトソーシングモデルに関しては，既存のライブラリを流用できるため，実装するためのコストが少なく済む．また，実行時には Web サーバ側で実行されるので，クライアント側での検証作業についても負荷は少ない．

専用アプリケーションの場合，昨年までのように端末 OS 別に SENSU アプリケーションを用意する場合はプラットフォーム分のアプリケーション開発・検証作業が必要となる．昨年の場合は Windows, Linux の 2 プラットフォームについてアプリケーションを用意したが，OS 毎の検証だけでもそれなりの負荷がかかった．

Java アプリケーションにすれば，1 プラットフォームで Java VM をサポートした OS をサポートできるが，SENSU ライブラリは C で書かれているため，ライブラリを全面的に Java で書き直す工数が加算されるという問題が存在する．

アプレットについても基本的には 1 プラットフォームで対応できるメリットがあるが，Java アプリケーション同様に，ライブラリ回りを全面的に Java で書き直す必要がある．

4.5.3 安 全 性

ここでは，各モデルを，セキュリティ(ここでは頑健性のような意味) とプライバシの観点から比較する．まず，全てのモデルは SENSU の安全性に依存する．

専用アプリケーションモデルは，他に仮定を置いていないため，安全性は SENSU のみに依存する．

アプレットモデルは，利用者が，プログラムをサービス提供者側から提供されるために，プライバシに関して正しく動作しているのかを確認することが難しい．また，セキュリティに関しても，計算やネットワークが遮断された場合，再び権利を発行してもらうためには匿名性を犠牲にしなければならない可能性がある．

計算外注モデル，および，認証アウトソーシングモデルに関しては，TTP に関する仮定が成り立つかどうかが問題となる．なお，多くの場合，サーバは端末よりも頑健にできているため，認証アウトソーシングモデルのセキュリティは高い可能性がある．

5. プログラミング・シンポジウム電子アンケートシステム

2.2 節で述べたとおり，従来行われてきた専用アプリケーションを用いたアンケートシステムには利用者の利便性を損ねるという問題点があった．そこで，今年度のプログラミング・シンポジウムの電子アンケートシステム (以下本システム) はウェブベースドなシステムとして構築することにした．今回比較したモデルの中では専用アプリケーションモデル以外のモデルが適用可能であると考えられるが，その中で 4.4 節で説明した認証アウトソーシングモデルを採用した．アプレットモデルでは利用者の認証用データの保存場所に関する問題を解決する必要がある．また，計算外注モデルを採用した場合，ウェブベースドシステムとして実装しようとした場合，ユーザに煩雑な操作を要求する一方で，TTP を必要とすること自体は認証アウトソーシングモデルと同じであるため，利用者に訴える利点があまりないのではないかと考えた．

ここでは，本システムの概要について述べる．本システムでは，サーバ上にサービス提供者のための SENSU プログラムが，TTP 上に利用者のための SENSU プログラムがインストールされている．計算の経過を示すデータは URL として表現され，利用者が必要な URL で TTP にアクセスすることで，TTP 上で SENSU プログラムが実行され，認証を行う仕掛けとなっている．

5.1 登録・TOKEN の発行

各利用者には，権利を受け取るための URL(権利 URL) が事前に与えられる．権利 URL は利用者ごとに異なるものが与えられており，TTP をアクセスするためのアドレスになっている．

利用者がウェブブラウザを通じて権利 URL にアクセスすると，TTP は サーバと通信し，SENSU の登録作業を行う．その際に TTP では利用者の秘密鍵等の情報を生成保存され，サーバにはその秘密鍵に対応する公開鍵が登録される．また，同様に TTP とサーバとの間で TOKEN 生成の手順が実行される．TTP は利用者に，その TOKEN を利用する際に必要な URL(TOKEN URL) を送り，利用者は端末に TOKEN URL を保存する．

5.2 アンケートの回答

利用者がアンケートに回答する際には，まずサーバ上で回答を作成し，その回答に関連付け

られた URL(回答 URL) を受け取る．次に，利用者は TOKEN URL で TTP にアクセスし，そこに回答 URL を入力する．

ここから TTP はサーバと通信を行い，SENSU の権利の利用の手順を実行することで，上の回答 URL に関連付けられた回答を有効にする．その際に，サーバは上の回答を取り下げるための無効化 URL を作成し，TTP に渡す．TTP は無効化 URL と用いた TOKEN 等と関連付けられた URL(回答認証 URL) を作成し，利用者に送る．利用者はこの回答認証 URL を保存する．

5.3 回答の取り下げ・TOKEN の再発行

利用者が回答を取り下げる際には，まず回答認証 URL で TTP にアクセスする．すると TTP は回答の取り下げの要求をサーバに行う．サーバは正しい回答取り下げ要求であることが確認できたら，回答を破棄するとともに，TTP と通信して SENSU の TOKEN の再発行の手順を行う．

ここで生成された TOKEN は最初に発行されたものと同等のものであり，TTP は TOKEN を保存するとともに，利用者に TOKEN URL を送る．利用者は TOKEN URL を保存する．

6. おわりに

本論文では，プログラミング・シンポジウム向けのウェブアンケートシステムを題材とし，匿名認証を用いたウェブベースドなシステムの実現方法や利点についての考察を行った．

まず，従来の紙ベースのアンケートシステムで実現していた機能や問題点について整理した後，電子アンケートシステムの課題を述べた．次に，従来から筆者らが取り組んできた，プログラミング・シンポジウムにおける匿名認証システムの利用について説明した後，従来の電子アンケートシステムの問題点について述べた．

続いて匿名認証システムについて説明した後，匿名認証を用いたウェブベースドシステムについて，考えられるモデルを 4 つ提示し，それぞれの利点・欠点をウェブアンケートシステムに利用することを前提にして議論した．更に，最も利用者の利便性に配慮した認証アウトソーシングモデルを基本とし，どのようにウェブアンケートシステムが実現できるかについて，簡単に説明した．

最後に，今後の課題をいくつか述べる：

- **SENSU の普及** SENSU を様々なアプリケーションに利用するとともに，標準として推進する．また，ウェブブラウザのプラグイン等を準備し，利用し易くする．
- **導入できる技術の検討** 各モデルについて，他の技術が導入できないか検討してみる．例えば計算外注モデルについて，依頼計算のような枠組みを導入できれば，TTP への仮定を弱められる．

参考文献

1) J. Camenisch and I. Damgard. Verifiable encryption and applications to group signatures and signature sharing. In *Tech. Rep. RS-98-32, Department of Computer Science, University of Aarhus*. Brics, Dec. 1998.
2) D. Chaum. Blind signatures for untraceable payments. In *Proc. of CRYPTO'82*, LNCS, pp. 199–203. Springer, 1982.
3) SENSU Project. In *http://aatoken.aitea.net*.
4) R. Shigetomi, J. Furukawa, A. Otsuka, K. Martin, and H. Imai. A provably secure refreahable partially anonymous token and its applications. In *IEICE Transactions on Fundamentals Special Section on Discrete Mathematics and Its Applications*. IEICE, 2006.
5) R. Shigetomi, A. Otsuka, T. Ogawa, and H. Imai. Refreshable tokens. 情報理論とその応用シンポジウム 2002, 2002.
6) Rie Shigetomi, Shunsuke SOEDA, Toshiro HIKITA, and Takahide Ogawa. An implementation of anonymous authentication system. In *Proceedings of Programming Symposium 2003*, 2003.