大学における講義評価のための匿名アンケートプロトコルとその試作

北川 隆[†] 岡 博文[††] 楫 勇一[†††]

本論文では，電子投票方式に関する理論的な研究成果を応用することで，大学における講義評価アンケートを電子的に実現することを考える．講義評価アンケートでは，回答者の匿名性確保や不正防止等，電子投票と共通するセキュリティ要件も多い．しかしその一方，講義評価アンケートは，大学という特殊な環境において実施されるため，通常の電子投票とはやや異なる前提条件の下で議論を行うことが可能である．そのため，通常の電子投票方式の実用化で大きな問題となる匿名ネットワークの実現法についても，講義評価アンケートでは，プロトコルの構成と運用上の工夫とである程度対応することが可能となる．本論文ではまず，匿名性，安全性および実現の容易性に配慮した講義評価プロトコルについて考察する．次に，考察したプロトコルに基づいて実装したWebベースのアンケートシステムについて紹介し，著者らの属する大学において実際に試用した実証実験の結果について述べる．

An Anonymous Questionnaire System for Rating Faculty Courses in Universities

TAKASHI KITAGAWA,[†] HIROFUMI OKA[††] and YUICHI KAJI[†††]

A fair and secure system for a faculty courses questionnaire (FCQ) in universities is discussed. An FCQ can be regarded as a special instance of the electronic voting for which a number of studies have been devoted for long years. However, there is slight difference between an FCQ and the general voting, and the difference makes realization of an FCQ system little bit easier than the realization of the general voting scheme. For example, in an FCQ system, it is possible to get around the serious problem concerning "anonymous network" by devising the protocol and its use. In this paper, a simple protocol for an FCQ is considered and its security is discussed. The paper also introduces a prototype Web-based FCQ system, and some results on the experimental use of the system in the authors' university.

1. はじめに

本論文では，主として情報セキュリティの観点から，大学等における講義評価アンケートシステムを電子的に実現する方法について議論する．

近年多くの大学において，学生が自分の受講した講義の内容を評価する，いわゆる講義評価がさかんに行われている[1)]．講義評価を実施する目的は多様であるが，たとえば評価結果を教官にフィードバックすることで，講義内容の改善や向上が期待できる．著者らの属する大学においても，数年前よりアンケート方式で学生による講義評価を行っている．本学では当初，試験実施時等にアンケート用紙を学生に配布し，試験の解答と同時にアンケート用紙の回収を行っていた．紙ベースでのアンケートの場合，教官の目の前で，試験の解答用紙だけを提出してアンケート回答用紙を提出しないのは学生も気まずく感じるのか，アンケート回収率（試験受験者に対するアンケート回答者数の割合）はほぼ100パーセントに近かった．しかし，紙ベースでアンケートを行った場合，集計等は手作業で行う必要があるため，アンケートの機械化・システム化による省力化の要望が出てきた．

この要望に対処するため，本学情報科学研究科では平成12年度より試験的にWeb上でアンケートを実施するシステムを導入し，約2年間の実験的な運用を行った．システムの導入により，当初の狙いどおり集計の手間自体は軽減したが，こんどはアンケートの回収率が極端に低下するという問題が発生した．ア

† 独立行政法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
†† NRIセキュアテクノロジーズ
NRI Secure Technologies, Ltd.
††† 奈良先端科学技術大学院大学
Nara Institute of Science and Technology

ンケート回収率が低下した原因としては，システムの安直な匿名性実現方式が考えられる．このシステムでは，回答者の匿名性を保証するために誰でも無記名で（個人認証を行うことなく）アンケート回答フォームに書き込めるようになっている．大学側では，誰がアンケートに回答して誰が回答していないのか把握できないため，学生にとっては，アンケートに回答しないことに対する心理的な障害が小さくなったものと考えられる．たとえば回答時に個人の認証を行う等，いわゆる記名式のアンケートにすれば回答率自体は向上すると考えられるが，記名回答では学生が批判的な意見を書きにくくなるのではないかとの懸念もある．もし，回答内容については匿名性が保証されているが，回答の事実については大学側で記録をとることが可能な方式があれば，講義評価等のアンケートには有用であると考えられる．

一方，同種の研究として電子投票プロトコルがある[6),8),9),11)]．講義評価アンケートは電子投票の特殊な場合と考えることができるが，電子投票と講義評価アンケートでは要求される事項や前提条件に異なる点も多い．また，現在提案されている電子投票システムでは，MIX-NET[5)] 等の匿名通信路が必要になることが多い．大学内において，結託を行わない複数のサーバによって MIX-NET を実現することは可能であるが，それらサーバの管理を大学が行うのであれば学生に対して説得力を持たない．

これらの理由から，本論文では大学での講義評価システムに適した電子アンケートプロトコルを提案する．提案方式は，既存の電子投票プロトコルの簡易版とも考えられるが，匿名通信路の問題にも十分考慮した方式となっている．さらに，Java を用いて Web 上にアンケートシステムを実装し，本学の講義評価アンケートの用に供することで，実証実験を行う．

本論文ではまず，2 章においてアンケートプロトコルを設計するうえでの仮定や，プロトコルに要求される性質について整理する．3 章では匿名性を保証しつつ，回答者と未回答者の識別が可能な電子アンケートプロトコルを提案する．4 章では提案したプロトコルに基づいて行った実装結果と実際に大学内で講義評価に用いた実験結果について述べる．

2. 準　　備

2.1 プロトコルに必要な性質

本章では，主としてセキュリティ的な観点から，講義評価のためのアンケートプロトコルが満たすべき性質を示す．以下では，アンケートの集計を行う大学側エンティティをサーバと呼び，アンケートに回答する学生をユーザと呼ぶ．

ユーザの不正回答防止： 1 人のユーザが 2 回以上回答を行ったり，アンケートに回答する権利のないユーザが回答を行えないこと．

匿名性： サーバは，どのユーザがどの回答を行ったか特定できない（当て推量以上の確率で言い当てることができない）こと．

回答者と未回答者の識別： サーバは，どのユーザが回答を行って，どのユーザが回答を行っていないかを検出できること．

設問設定の柔軟性： アンケートの設問は多者択一方式に限定されず，たとえば回答者による自由記述が可能である等，柔軟に設定できること．

上で述べた性質は，通常の電子投票等とも共通する要求仕様である．一方，本研究で対象としている講義評価アンケートでは，以下の条件を仮定できる．

サーバの不正行為に関する仮定： サーバは，回答内容の改ざんや回答の水増し等，いわゆる「能動的攻撃」を行わないと仮定する．大学（サーバ）が講義評価アンケートを実施する目的は，学生の率直な意見を収集することであり，回答結果を不正に操作したとしても，大学として得るものはない．したがって，大学が能動的な攻撃を行う動機や必然性はきわめて低く，アンケートプロトコルは，これらの不正行為に対する耐性を有する必要はない．一方，サーバの「受動的攻撃」（正当に入手した情報から他の情報，たとえば誰がどのような回答を行ったか等の情報を導出するような攻撃）については，プロトコルとして耐性を有する必要がある．

通信路に関する仮定： サーバとユーザとの間には，盗聴や通報の改変ができないような安全な通信路が存在すると仮定する．大学内ネットワークはファイアウォール等により学外から保護されており，物理的にも大学の管理下にある．また，取り扱う情報の経済的な価値もそれほど大きくはないため，第三者による大規模な攻撃の対象となることもない．たとえば SSL[12)] 等の既存技術を利用することで，通信路については実用上十分な安全性が得られると考えられる．

通常の電子投票では必ずしも上記の仮定を置くことができないため，投票プロトコル自体が，たとえばサーバの能動的攻撃への保護機能や，通信メッセージの暗号化等の機能を有する必要があった．その意味で，

講義評価アンケートに要求されるセキュリティ要件は若干弱く，逆に，それら安全性実現のための機構の一部を省略することで，より簡潔で実現に適したプロトコルが得られる可能性がある．

2.2 既存の電子投票について

ネットワーク上で匿名の投票や選挙を行うための方式については，文献 6)，8) で提案されているブラインド署名[3),4)] を用いる方式や，文献 9)，11) 等で提案されている MIX-NET[5)] と呼ばれる匿名通信路を用いる方式等，多くの理論的な研究が行われている．MIX-NET は，匿名通信路を実現する一手法で，結託しない複数のサーバ（MIX サーバ）によって構成される．大学内に複数の MIX サーバを設置することは技術的には困難でないと考えられるが，学生に対し，大学が管理する MIX サーバが結託していないことを納得させるのは困難である．一方，ブラインド署名を用いる方式の場合には，投票者の匿名性を保つために，サーバと各投票者間に匿名通信路が必要である．匿名通信路については現在でもさかんに研究されているが，インターネット等の実用的な環境において匿名通信を実現する仕組みについては，残念ながらまだ確立されているとはいえない．また，ブラインド署名を用いる方式では，サーバの能動的攻撃を防止するため，公開掲示板のような仕組みが必要になることも多い．

3. アンケートプロトコル

3.1 概　　要

本研究では，ブラインド署名を利用することで，必要最小限の機能を持ったアンケートプロトコルを構成する．ブラインド署名を利用する方式については，前章で述べたように若干の問題点が知られているが，他の方式に比べて，より実用的なアプローチであると考えられる．プロトコルの構成にあたっては，たとえば文献 7) 等で提案されているような 2 フェーズ型プロトコルを基本として検討を行う．文献 7) のプロトコルでは，ANDOS（All-or-Nothing Disclosure of Secrets）プロトコルを利用することで，サーバ（集計者）から各ユーザ（投票者）に対して，投票権を有することの証明書を発行する．ユーザは，実際の投票内容にこの証明書を添付してサーバに送ることで，自分の投票の正当性を主張する．集計結果に関する情報は掲示板等で公開され，サーバの能動的攻撃はユーザによって監視される．

文献 7) の方式はシンプルで安全性が高い反面，少なくとも以下に示すような問題があると考えられる．(1) ANDOS プロトコルは，複数のユーザが同期・協力して実行する必要があるが，実際の投票者にそれを期待するのは現実的でない，(2) 公開掲示板が必要となる，(3) 匿名通信路が必要となる．本研究では，(1) に関して，ANDOS の代わりにブラインド署名を利用することで，各ユーザが非同期的に投票（アンケートに回答）できるようにする．また，(2) について，講義評価アンケートではサーバの能動的攻撃を想定外としているので，公開掲示板自体が不要となる．一方，(3) については依然として大きな問題であり，一般的な解決策を提示することは困難であるが，運用上の工夫で対応することを検討する．たとえば，ユーザがプロトコル実行の一部を他の計算機上で行うことで，回答者と回答内容の関連付けが事実上できないようにする等の対応を考える．そのためには，プロトコルの各操作の独立性をできるだけ高くしておき，各操作間でのデータの移行等の作業ができるだけ小さくなるよう，プロトコルおよびシステムを構成する必要がある．

ブラインド署名等を用いて正当性に関する証明をあらかじめ入手し，後日，以前の操作とは独立した環境において入手した証明を行使するという方式は，電子マネーの匿名性実現においてしばしば用いられるアプローチである．一方，著者らの知る範囲では，従来の電子投票に関する研究において，電子マネー型のシンプルな匿名性実現方式はそれほど重要視されてこなかった．原因はいくつか考えられるが，単純に操作の独立性を高める方式では，電子投票の研究において重要視されている「投票者による集計者監視」の仕組みとうまく整合しないことが考えられる．講義評価アンケートでは，集計者の不正監視が不要になるため，電子マネー型のシンプルな方式でも有効であると考えられる．

提案プロトコルはハンドル登録フェーズ，回答フェーズ，受領書送信フェーズの 3 つのフェーズからなる．ユーザはまずハンドル登録フェーズを実行し，その後回答フェーズを実行し，最後に受領書送信フェーズを実行する．各フェーズの概要は以下のとおりである．

ハンドル登録フェーズ：ユーザはランダムにハンドルを選び，ハンドルに対するサーバの電子署名を入手する．この際，ブラインド署名を用いて署名の計算を行うこととし，サーバがユーザとハンドルとの対応をつけることができないようにする．ハンドルに対する署名は，次の回答フェーズで利用する．

回答フェーズ：ユーザはハンドルとその署名を提示することで，自分に回答権があることをサーバに提示する（この際，自分の本名は明かす必要はない）．その後，サーバにアンケートの回答を送り，サーバからア

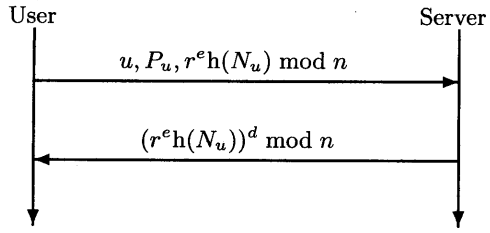


図 1 ハンドル登録フェーズ
Fig. 1 Handle registration phase.

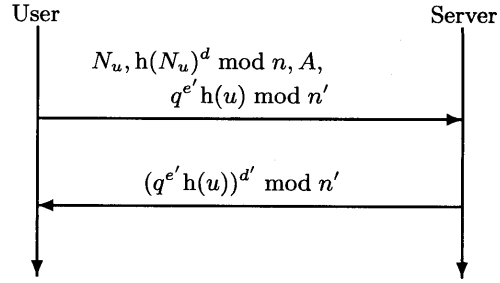


図 2 回答フェーズ
Fig. 2 Answer phase.

ンケートに回答したことを証明する受領書を受けとる．受領書の授受にもブラインド署名を利用し，たとえユーザが受領書を公開しても，そこから回答内容が露呈することはないようにする．

受領書送信フェーズ：ユーザは回答フェーズで手に入れた受領書をサーバに送信する．

3.2 プロトコルの詳細

以下では RSA ブラインド署名[3),4)] を用いた一実現法を示す．他のブラインド署名法を用いてもほぼ同様のプロトコルを得ることが可能である．

ハンドル登録フェーズ（図 1）

準備 サーバは RSA 暗号の鍵組を計算し，署名検証鍵（暗号化鍵）(e, n) を公開，署名作成鍵（復号鍵）d を秘密にしておく．またサーバは一方向性ハッシュ関数 h を定め，すべてのユーザに通知する．サーバは回答権のあるユーザに対し，ユーザ ID u と初期パスワード P_u を発行しておく．

(1) ユーザはハンドル N_u をランダムに作成する．ユーザは，ハンドル N_u にブラインド署名をもらうために乱数 $r(1 < r < n)$ を選び，$r^e \mathrm{h}(N_u) \bmod n$ を計算する．

(2) ユーザは ID u，初期パスワード P_u，ステップ (1) で計算した $r^e \mathrm{h}(N) \bmod n$ をサーバに送信する．

(3) サーバはユーザから送られてきた ID u と初期パスワード P_u をチェックする．もし，パスワードが正しくなかったり，そのユーザに回答権がなかったり，あるいはすでにハンドル登録フェーズを実行していたならば，プロトコルを終了する．

(4) サーバは $(r^e \mathrm{h}(N_u))^d \bmod n$ を計算し，ユーザに送信する．

(5) ユーザはサーバから受けとった $(r^e \mathrm{h}(N_u))^d \bmod n$ に $r^{-1} \bmod n$ をかけ，$\mathrm{h}(N_u)^d \bmod n$ を得る．$\mathrm{h}(N_u)^d \bmod n$ はハンドル N_u に対するサーバの署名となっているが，以降では，この $\mathrm{h}(N_u)^d \bmod n$ を回答用パスワードと呼ぶ．回答用パスワードは，次の回答フェーズで利用する．

回答フェーズ（図 2）

準備 サーバは RSA 暗号の鍵組を計算し，署名検証鍵（暗号化鍵）(e', n') を公開，署名作成鍵（復号化鍵）d' を秘密にしておく．これらの鍵はハンドル登録フェーズで用いた鍵とは異なるものを利用する．また，ハンドル登録フェーズと同様に一方向性ハッシュ関数 h を選び，すべてのユーザに通知する．一方向性ハッシュ関数は，ハンドル登録フェーズで用いたものと同じ関数でかまわない．

(1) ユーザは以下の 4 つのデータをサーバに送信する．
- ハンドル登録フェーズで選んだハンドル N_u
- 回答用パスワード $\mathrm{h}(N_u)^d \bmod n$
- アンケートの回答 A（自由に記述した文書でよい）
- 受領書を計算するためのデータ $q^{e'} \mathrm{h}(u) \bmod n'$．ここで，$q$ はユーザが任意に選んだ乱数で，$1 < q < n'$ とする．また u はユーザ ID を表す．

(2) サーバはユーザから送られたハンドル N_u から $\mathrm{h}(N_u)^d \bmod n$ を計算し，回答用パスワードと一致することを確認する．パスワードが一致し，かつハンドル N_u を持つユーザからまだ回答を受けとっていないならば，回答 A を受理する．もし，以前に同じハンドルを持つユーザが回答をしていた場合には回答は受理せず，プロトコルを終了する．

(3) サーバは回答を受理したのち，$(q^{e'} \mathrm{h}(u))^{d'} \bmod n'$ を計算しユーザに送信する．

(4) ユーザはサーバから送られてきた $(q^{e'} \mathrm{h}(u))^{d'} \bmod n'$ に $q^{-1} \bmod n'$ をかけて，$\mathrm{h}(u)^{d'} \bmod n'$ を得る．これが受領書となる．

受領書送信フェーズ

ユーザは受領書をサーバに送信する．

3.3 プロトコルの安全性について

3.2節で紹介したプロトコルは，文献7)で議論されているような通常の電子投票プロトコルから不要な機能を削除して，簡単化したものと考えることもできる．本節では，たとえ前述のような簡単化を行ったとしても，講義評価アンケートの実現に要求されるセキュリティ要件は損なわれていないことを示す．

3.3.1 不正回答防止

ユーザによる不正回答としては，1人のユーザが2回以上回答をする多重回答と，回答権のないユーザが回答を行う非権利者による回答が考えられる．提案プロトコルにおいて回答をサーバに受理してもらうには，ハンドルとそのハンドルに対する回答用パスワードが必要となるため，不正を行おうとするユーザは，本来ならば入手できないはずの回答用パスワード（および対応するハンドル）をあらかじめ入手しておく必要がある．一方，提案プロトコルにおいて回答用パスワードを発行できるのはサーバのみである．サーバは，回答用パスワードの発行にあたってつねにユーザの正当性を検査するため，ユーザがサーバから不正に回答用パスワードを入手することはできない．また，サーバの助けを借りずに回答用パスワードを構成することは，電子署名を偽造することに相当するため，(RSA署名が安全である限り）ユーザがこれに成功することはない．よって，ユーザが不正に回答用パスワードを入手・構築することはなく，不正回答を行うことはできない．

3.3.2 匿 名 性

ハンドル登録フェーズにおいて，ユーザはID u，初期パスワード P_u，$r^e \mathrm{h}(N_u) \bmod n$ をサーバに送っている．ここで，ハンドル N_u は一方向性ハッシュ関数によって処理され，しかもブラインド化乱数 r がかかっているため，サーバはこれらの情報からユーザ u のハンドル N_u を知ることができない．投票終了後，サーバはアンケートの回答に利用されたすべてのハンドルを知ることができるが，それでもハンドル登録フェーズでは $\mathrm{h}(N_u)$ をブラインド化して送っているため，サーバはユーザ u が使用したハンドルを求めることはできない．

次に，回答フェーズでは，ユーザはハンドル N_u とアンケートの回答 A を送っているため，サーバはハンドルと回答とを対応付けることが可能である．しかし，先に述べたように，サーバはハンドルとユーザIDの対応をつけることができないため，結局ユーザIDとアンケートの回答を対応付けることはできない．また，受領証の発行にもブラインド署名を用いているため，受領書送信フェーズでユーザが受領証をサーバに送信しても，受領証の情報からユーザIDと回答とを対応付けることはできない．

上述したプロトコルにおける唯一の懸念は，回答フェーズにおいて，サーバがユーザのIDを特定できないことを保障しなければならない点にある．現実世界のコンピュータネットワークの多くでは，自分が現在通信している相手が誰なのか，ある程度特定することが可能である．もし，悪意を持ったサーバがこの特質を悪用すると，ユーザとその回答内容の関連付けが可能となってしまう．たとえば，あるユーザがハンドル登録フェーズと回答フェーズを同一の計算機上でほぼ同時刻に行ってしまうと，サーバに大きな手がかりを与えることになる．理想的には，回答フェーズの実行にはいわゆる匿名ネットワークを利用することが推奨される．しかし残念ながら，匿名ネットワークはまだ研究段階の技術であり，本原稿執筆段階において実用的・標準的な方式が確立されているとはいえない．事実，ネットワークの匿名性の問題は，電子投票プロトコルの実現における最大の技術的課題の1つであると考えられる．

本研究では，この問題に対し，運用上の工夫で問題を回避することを検討する．上述したアンケートプロトコルは，従来の電子投票プロトコルに比べて非常にシンプルなものとなっており，各フェーズ間で継承しなければならない情報はきわめて少量である．もし，ユーザがそれら継承すべき情報を自分の手で直接取り扱うことができれば，ユーザは各フェーズを好きなときに好きな計算機から実行することが可能である．たとえば，ハンドル登録フェーズおよび受領証送信フェーズは自分専用の計算機から実行し，回答フェーズのみ，自分が特定されないような計算機を利用することで，擬似的に匿名ネットワークを実現することが可能である．実際，回答フェーズの実行においてはユーザIDの提示は要求されないため，たとえば大学内に設置されている（認証なしで誰でも利用可能な）共有パソコンを利用することや，大学とは無関係のインターネットプロバイダ経由でサーバにアクセスすること，あるいは，近年増加している無線LANのホットスポットを利用すること等により，上記のような運用を行うことは十分現実的であると考えられる．

3.3.3 回答者と未回答者の識別

回答フェーズを実行したのち，ユーザは受領書 $\mathrm{h}(u)^{d'} \bmod n'$ を入手できる．ユーザはサーバの秘密鍵 d' を知らないので受領書を偽造することは不可能で

ある．また，詳細は割愛するが，ハンドル登録フェーズと回答フェーズで異なるRSA鍵を利用しているため，ユーザは，ハンドル登録フェーズの署名機構を悪用して受領書の偽造を行うこともできない（もし両フェーズで同じ鍵を利用すると，受領書が偽造される可能性がある）．したがって，受領書を保有していることは，アンケートに回答したことの証明となる．逆に，受領書を提示できないユーザは，アンケートに回答していないものと判断できる．

4. アンケートシステムの実装と評価

4.1 実証実験の目的と概要

前章でも議論したように，一定の前提条件のもとでは，提案したアンケートプロトコルは実用上十分な安全性を有すると考えられる．一方，現実の世界でアンケートシステムを実現する際には，前章で考えたような前提条件を実現することが難しかったり，あるいは何らかの理由で，プロトコル中の操作を他の操作で置き換える（近似する）必要が生じたりすることもある．通常，これらの要因はプロトコルの安全性を損なう方向に働くと考えられるが，その影響がどの程度のものになるのか，事前に予測することは難しい．本章では，提案プロトコルの試作と実証実験を通じて，プロトコル実現の際の問題点の抽出と，現実環境における提案方式の安全性について考察を行う．また，電子的な講義評価アンケートを実際に利用する場合，安全性以外の問題についても考慮する必要があるが，本研究では以下に述べる3つの点に的を絞り，実証実験を通じて評価を行った．

安全性要件以外で評価すべき点の第1は，プロトコルのユーザビリティである．前章でも述べたように，提案方式において匿名性を確保するためには，（匿名ネットワークが利用可能でない限り）プロトコルの各フェーズを独立に，異なる計算機上で実行する必要があり，ユーザに若干の負荷をかけることとなる．実証実験を通じて，ユーザの負荷がどの程度のものとなるのかを評価する．

評価すべき点の第2は，提案方式のスケーラビリティである．一般に，大学には多数の学生が在籍し，同時に複数の講義科目を受講している．したがって，講義評価アンケートシステムは多数の回答を処理する必要があり，システムが対象とする規模によっては，サーバにかかる負荷が問題になる可能性もある．提案方式が比較的大規模な使用にも耐えるか否かを検証するため，試作したシステムの処理性能の計測や，実証実験中の動作ログ解析等を行う．

実証実験で評価する最後の点は，アンケートの回収率である．論文の冒頭でも書いたように，本研究の目的は匿名性を確保しつつ，高い回収率が実現できるような電子アンケートシステムを実現することである．アンケート未回答者を識別可能であるという提案方式の特性がアンケート回収率にどの程度影響するかを評価する．

安全性に加えて以上3点の評価を行うため，2種類のシステムを試作し，2種類の実験を行った．システムの試作にあたっては，鍵長1024ビットのRSA暗号を利用した．一方向性ハッシュ関数はMD5[10]を，通信路の保護にはSSL[12]を用いた．提案方式では，ユーザ（学生）の側でもブラインド署名等の計算が必要になるため，ユーザの計算機上でなんらかのプログラムを実行する必要がある．本研究では，ユーザの利便性や保守の手間についても検討し，ユーザ側プログラムをJavaアプレットとして実装した．したがって，ユーザの視点からは，Webブラウザを使用する延長として提案システムを利用することが可能である．また，特別なソフトウェアのインストールや設定等の作業が不要になるため，ユーザは自宅の計算機や街中に設置されているインターネット端末からでも，アンケートに回答することが可能となる．一方，サーバ（大学）については，Javaアプレットとの親和性を考え，Javaサーブレットにより実装を行った．システム内容の詳細については，それぞれの実験の節において述べる．

4.2 実　験　1

4.2.1 本実験の概要

実験1ではユーザビリティ評価を行う．本実験で用いる試作システムでは，提案プロトコルの各フェーズごとに別のプログラム（Javaアプレット）を準備してユーザに提供する．ユーザは，自分の手でフェーズ間のデータ移行を行うことになる．比較的小規模な講義科目において，実際の受講学生に本システムを利用してもらい，使用感等について聞き取り調査を行った．

ただし，大学では1人の学生が多数の科目を受講していることが多いため，前章で述べたプロトコルを科目ごとに実現するのでは，被験者（学生）にとっての負荷が重くなりすぎるなるのではないかと考えられる．そこで，学生の負荷軽減を目的として，回答用パスワードの内部構造に科目情報が反映されるようプロトコルを若干変更して，提案方式の試作を行った．変更内容については割愛するが，この変更により，学生はハンドル登録フェーズを1度実行するだけで，すべての受講科目に対する回答用パスワードを得ることができる．一方，本変更によりプロトコルのセキュリ

ティ的要件はやや低下する．複数の学生が結託して不正を行ったり，1人の学生が，自分の回答権を犠牲にして受講していない科目の回答用パスワードを得たりすることが可能になる場合がある．また，学生は複数科目にわたって同一のハンドルを使用することになるため，どのハンドルがどの科目のアンケート回答に使われたかを分析することで，ハンドルと学生の実体との推測が可能になるおそれもある．本格的な選挙であればこれらは大きな問題であるが，講義評価アンケートでは一般の選挙ほどの安全性は要求されないことを考慮し，ここではユーザの利便性を優先することとした．

4.2.2 試作システムについて

本実験で用いる試作システムでは，プロトコルの各フェーズごとに，それぞれ独立したプログラム（Javaアプレット）を用意する．各フェーズを担当するプログラムはそれぞれ独立しているため，ハンドルや回答用パスワード，受領書等の中間情報をなんらかの方法で直前フェーズから受け取る必要がある．一方，ユーザの計算機保護のため，Javaアプレットによるユーザ計算機のリソースアクセスは強く制限されており，たとえば上記の中間情報をユーザ側計算機上のファイルとして残すことはきわめて困難である．したがって，ユーザは自分自身の手で，ハンドルや回答用パスワード，受領書情報等を取り扱う必要がある．本来ならば，これらの情報はできるだけ乱雑で大きな2進値であることが望ましいが，ユーザの取扱いの利便性を考え，以下のように対処することとした．まずハンドルは，ユーザ自身によって好きな文字列を選定することとした．機械的にハンドルを選定する場合と比較して，異なるユーザが同一のハンドルを選ぶ確率が若干増加する可能性があるが，ユーザ自身はハンドルを覚えやすいという利点がある．また，回答用パスワードおよび受領書については，S/Key等の使い捨てパスワードの実装で見られるように，2進値をハッシュして適当な英単語に置き換える手法を採用することとした．

サーバ側では，RSA鍵転送，ユーザ認証および回答用パスワード発行，回答受付および受領書発行，受領書受付の各機能ごとにJavaサーブレットを用意し，ユーザ側Javaアプレットからの要求に応じてサービスを提供する．これらサーブレットの構成は，後述する実験2のものとほぼ同様であるため，詳細はそちらで述べることとする．

4.2.3 実験の詳細と結果

実験1は，平成13年度第IV期に開講された小規模な講義科目において，前項で述べたシステムを利用して行った☆．被験者の数は12人で，必ずしもセキュリティの専門知識を有していない．アンケートの実施にあたっては，プロトコルの概要や試作システムの使い方等について簡単な説明を行い，アンケート回答期間として約1週間を設定した．学生は操作方法等をおおむね理解したようであり，操作上の問題で回答できなかったというケースはなかった．ただし，回答用パスワード等の中間情報の取扱いが面倒である，回答科目数が多いときには学生の負荷が大きくなりすぎるのではないか等，操作性に関して疑問を投げかけるコメントも何件か寄せられた．

また，ハンドルとして自分のユーザ名や本名を使用する者や，同一の計算機上ですべてのフェーズを実行する者も多くみられた．少なくとも今回の実験では，匿名性実現のために余計な手間をかけるよりも，より簡便に操作ができることを望む学生が多数を占めることが分かった．本実験では被験者数も少数であり，観察された傾向を単純に一般化することはできないが，より多くのユーザに利用してもらうためには，システムの操作性が非常に重要であると考えられる．その意味で，提案方法をそのまま実現し，データ移行等の作業をすべてユーザに任せてしまうのは，残念ながらあまり現実的であるとはいえない．

本問題を解決するための一手法として，ICカード等のデバイスを利用し，大学における事務作業や手続きとリンクして，アンケート実施に必要な情報の授受を行うことが考えられる．たとえば，学期の最初の履修登録作業の一部として，事務局の端末等でハンドル登録フェーズを実行することを考える．ハンドルの選択や，一連のブラインド署名関連の計算等はICカードが行い，ハンドルと回答用パスワードはカード内に蓄積しておく．学期終了時には，個人の端末とICカード内に蓄積された情報を用いて回答フェーズを実行し，受領書は再度ICカード内で記録する．成績発行時には，事務局の端末等で受領書の確認を行えば，アンケート回答者と未回答者を識別可能である．以上のようにICカードを利用することで，ユーザは中間情報に触れる必要がなくなり，操作性は格段に改善すると考えられる．また，ユーザは無意識のうちに，各フェーズで異なる計算機を利用することになるため，匿名性の実現上も好ましいといえる．

4.3 実 験 2

4.3.1 本実験の概要

実験2では，より多くの被験者を対象とし，スケー

☆ 著者らの大学では，1年を4つの期にわけて講義を行っている．

ラビリティとアンケート回収率の評価を行う．本来であれば，前項でも考察したように，ICカード等を導入して操作性を改善してからスケーラビリティ評価を行うべきところであるが，今回の実験ではそこまでの環境設定が難しいこと，サーバの負荷を評価するためには，ICカードの有無は本質的でないことを考慮し，スケーラビリティ評価に特化したシステムを試作して利用することとした．本実験で使用する試作システムでは，ユーザはすべてのフェーズを同一のプログラム（Javaアプレット）内で実行する．したがって，通信ログ等を解析することにより，どの学生がどの回答を行ったか追跡することが可能である．一方，ユーザは中間データに触れる必要がないため，ユーザが利用するプログラムの操作性は格段に向上する．匿名性の問題は，先にも述べたようにICカード等の導入で解決できること，今回の実験の目的を考えると，操作性を高めて，より多くの学生に実験に参加してもらうことのほうが意義が大きいことをふまえて，次項で述べるようなシステムを構築した．

4.3.2 試作システムについて

本実験では，ユーザに対して1個のJavaアプレットを提供する．この1つのアプレットが，ユーザ認証，ハンドル選定，回答用パスワードの取得，回答の送信と受領書の構築等，いっさいの作業を行う．ユーザは中間情報に触れる必要がないため，実験1のシステムに比べて，使いやすさは格段に上昇することが期待される．また，ユーザが署名鍵，ハンドル，回答用パスワード，受領証情報等に直接触れる必要がないため，実験1で考えたような，セキュリティを若干犠牲にして操作性を高める工夫をする必要がなく，安全性の観点からも優れていると考えられる．

サーバ側では，実験1と同様，RSA鍵転送，ユーザ認証および回答用パスワード発行，回答受付および受領書発行，受領書受付の各機能ごとにJavaサーブレットを用意し，ユーザ側Javaアプレットからの要求に応じてサービスを提供する．実験では，パーソナルコンピュータ（AMD Athlon 1 GBプロセッサ，主記憶容量512 MB，OSはFreeBSD 4.5-RELEASE）上にサーバを構築した．Javaサーブレットのコンテナとしては，tomcat（バージョン3.2.3）を採用し，署名の作成および検証にはJavaのBigIntegerオブジェクトを使用する．サーブレットの機能，プロトコル上での役割，性能は以下のとおりである．ただし，以下で述べる実行時間の中には，サーブレット起動のためにOSやコンテナ（tomcat）で消費される時間は含まれない．時間の計測にあたっては，JavaのDateオブジェクトを使用して実時間を計測した．したがって，同じ環境であっても，サーバの負荷状況によっては実行時間に多少の変動があるものと考えられる．

- RSA鍵転送：3.2節各フェーズの「準備」段階における，鍵を公開する機能を提供するサーブレットである．クライアントとなるJavaアプレットから講義科目名を受け取り，対応する科目のアンケート回答に使用される鍵（ハンドル登録フェーズ用と回答フェーズ用）を返送する．本サーブレットは，1秒あたり約400のリクエストを処理することが可能である．単純計算では，1リクエストの処理に必要となる時間は約2.5ミリ秒となる．
- ユーザ認証および回答用パスワード発行：ハンドル登録フェーズの第3および第4ステップに相当する機能を提供するサーブレットである．ユーザIDおよび初期パスワードとしては，学内で統一的に管理されている学生のユーザ名とログインパスワードを利用する．本サーブレットは，Javaアプレットからユーザ名，パスワード，講義科目名，ブラインド化されたハンドルパスワード（ステップ2の$r^e h(N_u) \pmod n$）を受け取り，パスワードが正しいか，その学生が指定された講義を受講しているか，まだ回答用パスワードを受け取っていないか等を検査し，問題がなければ署名を作成してクライアントに返送する．本サーブレットの実行には，1リクエストあたり約200ミリ秒が必要となる．ただしこの時間の中には，パスワード認証を行うためにNIS（YP）データベースを参照する時間も含まれている．ユーザ認証機構をネットワークに依存しない形で実現すれば，効率は改善可能である．パスワード認証にかかる時間を除外すると，実行時間は約120ミリ秒となる．
- 回答受付および受領書発行：回答フェーズの第2および第3ステップに相当する機能を提供するサーブレットである．クライアントから，ハンドル，回答用パスワード，講義科目名，設問への回答，受領証計算のための情報（$q^{e'} h(u) \pmod{n'}$）を受け取り，ステップ2で定められた検査を行った後，受領証に署名をして返送する．本サーブレットの実行には，1リクエストあたり約220ミリ秒が必要となる．この処理では，回答用パスワードの検査と受領証への署名を行う必要があり，実行時間のほとんどが，BigIntegerオブジェクトのベキ乗剰余演算に使われていると考えられる．
- 受領書受付：受領書送信フェーズに相当する．クライアントからユーザ名と受領書を受け取り，受

領書の正しさを検証して記録する．受領書の正しさを確認してから記録するため，1リクエストあたり約100ミリ秒が必要となる．

各サーブレットの実行時間は数百ミリ秒単位であり，クライアントからのリクエストに対して，きわめて短時間で各処理を完了することが可能である．数秒おきにリクエストが来るような環境であれば，サーバにはほとんど負荷がかからないと予想される．万一，あるサーブレットの処理中に他のリクエストが到着した場合でも，サーブレットコンテナが別スレッドを生成して処理を行うため，ユーザに対する処理が滞ることはない．

4.3.3 実験の詳細と結果

実験2は，平成14年度第I期，第II期に開講されたすべての講義を対象とし，原則として受講生全員参加で実施した．第I期の講義の場合，少なくとも1つの講義を履修している学生165人が対象となり，開講科目数は20科目である．履修登録件数は全部で1383件であった．第II期では，学生数164人，科目数25で履修件数は1616件であった．第I期，第II期の講義期間終了後，それぞれ約1週間の期間を設定してアンケートに回答するよう学生に依頼した．ただし，学生には事前に，アンケートに回答したかどうかが担当教官には把握できる旨をアナウンスした．

その結果，第I期については680件，第II期については559件の回答が寄せられた．履修登録数に対するアンケート回収率は，それぞれ49%，35%となった．実際には，学期途中で講義を放棄する学生が少なからずいるため，最後まで出席していた学生数に対する回収率は，これよりも大きな値となる．前年度同時期には，セキュリティ的要件を考慮しない無記名電子アンケートシステムを使用していたが，そのときの回収率はそれぞれ6%，17%であった．昨年度と比べて回収率が大幅に上昇しており，所期の目的は達成したことになる．

動作ログを確認したところ，サーバに到着するリクエストは，多いときでも数十秒から数分おきであった．この程度の規模のアンケートであれば，通常のパーソナルコンピュータ程度でもまったく問題なくサーバとして利用可能である．実際，著者らの主観的な判断ではあるが，アンケートシステム稼働中でもサーバ計算機のパフォーマンス低下はみられず，性能的にはまだ余裕があると思われる．もっと規模の大きなアンケートであっても，現システムで十分対応可能であると予測できる．

4.4 実験の総括

2つの実験を通じて，セキュリティ以外の要件について，提案プロトコルの評価を行った．実験1の結果より，提案プロトコルに忠実に従うと，ユーザの負荷が大きくなることが明らかとなった．しかし，この問題については，本文中でも述べたようにICカード等を併用することで回避可能であると考えられる．近年，私立大学を中心とした多くの大学において学生証をICカードに置き換える動きがあることを考慮すると，この問題回避法は十分現実的であると考えられる．一方，実験2を通じて，提案方式のスケーラビリティについての検討を行った．著者らの属する大学の規模であれば，通常のパーソナルコンピュータであっても，余裕をもってサーバの役割を果たすことが可能である．また，今回の実験でアンケート回収率を向上させることに成功したが，これは，試作システムが有する未回答者識別機能を，学生が強く意識しているためと考えられる．

5. ま と め

大学等における講義評価アンケートを念頭におき，匿名性の保証と回答者・未回答者の識別が可能なアンケートプロトコルを提案した．また，提案したプロトコルに基づいてアンケートシステムの実装を行い，実際に講義評価アンケートとして試験的に運用を行った．本論文において議論した方式は講義評価だけにとどまらず，さまざまな場面で応用が可能であると考えられる．たとえば，外国の学会における役員選挙等では，投票率を上げるため，投票した人に抽選で景品を授与するような試みもさかんに行われているが，提案方式はそのような選挙にも応用可能である．また提案方式は，電子的な投票方式と従来の紙ベース投票方式とを併用する際にも有用である．大規模な選挙や投票等では，技術的な経過措置として，あるいはデジタルデバイドに対する配慮として，電子投票と紙ベース投票の両者を実行し，その集計結果を合算して最終的な投票結果とするような運用が現実的であると考えられる[2)]．その際には，電子的に投票を行った投票者が紙ベースの投票には参加しないよう，電子投票を行ったか否かの識別が必要となる．提案方式を利用すれば，投票の匿名性を確保しつつ，上記識別が可能となる．ただし，二重投票を行おうとするユーザは，受領書を提出しない可能性があるため，提案法そのままでは安全であるとはいえない．ハンドル登録フェーズの実行をもって投票を行ったと解釈することも考えられるが，受領書の取扱いについて，提案方式にはまだ改善の余地があ

ると考えられる．

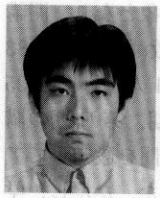
電子投票・アンケート方式についてはこれまでも多くの研究が行われてきた．しかし，実際にそれらの方式を実現するためには，たとえば法律的な問題や道徳的な問題等をクリアする必要があり，実証実験すらままならないというのが現状であった．今回，大学という比較的小さなコミュニティにおいてではあるが，いわゆる電子アンケート方式を現実の用に供するべく試みた．アンケート回収率の観察を続行する等，今後も長期的な評価が必要ではあるが，本研究で行った試みは，今後の電子投票方式の実用化研究に些少ながらも貢献するものと考えられる．

謝辞 実証実験に協力いただきました，奈良先端科学技術大学院大学情報科学研究科に感謝いたします．また，実験結果の記述について有用な意見をいただいた査読者の方々に感謝いたします．

参考文献

1) 朝日新聞：ベストティーチャー選び，1月5日（夕刊）(2002).
2) 朝日新聞：ネット投票で行使率が上昇，5月22日（朝刊）(2002).
3) Chaum, D.: Blind signatures for untraceable payments, *Proc. Crypto'82*, pp.199–203, Plenum Press, Santa Barbara California (Aug. 1982).
4) Chaum, D.: Security without identification: transaction systems to make big brother obsolete, *Comm. ACM*, Vol.28, No.10, pp.1030–1044 (1985).
5) Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).
6) Fujioka, A., Okamoto, T. and Ohta, K.: A practical secret voting scheme for large scale elections, *Proc. AUSCRYPT'92*, Gold Coast, Queensland, Australia, LNCS 718, pp.244–251 (Dec. 1992).
7) Nurmi, H., Salomaa, A. and Santean, L.: Secret ballot elections in computer networks, *Computers & Security*, Vol.10, pp.553–560 (1991).
8) Ohkubo, M., Miura, F., Abe, M., Fujioka, A. and Okamoto, T.: An improvement on a practical secret voting scheme, *Proc. ISW'99*, Kuala Lumpur, Malaysia, LNCS 1729, pp.225–234 (Nov. 1999).
9) Park, C., Itoh, K. and Kurosawa, K.: Efficient anonymous cahnnel and all/nothing election scheme, *Proc. EUROCRYPT'93*, Lofthus, Norway, LNCS 1334, pp.248–259, (May 1993).
10) Rivest, R. and Dusse, S.: The MD5 message-digest algorithm, Network Working Group Internet Draft, RSA Data Security Inc. (1991).
11) Sako, K. and Kilian, J.: Receipt-free mixtype voting scheme — a practical solution to the implementaion of a voting booth, *Proc. EUROCRYPT'95*, Saint-Malo, France, LNCS 921, pp.393–403 (May 1995).
12) OpenSSL, "The Open Source Toolkit for SSL/TLS." http://www.openssl.org/

(平成14年12月27日受付)
(平成15年7月3日採録)



北川 隆（正会員）

平成9年東京工業大学工学部情報工学科卒業．平成11年奈良先端科学技術大学院大学博士前期課程修了．平成14同後期課程研究指導認定退学．現在，独立行政法人産業技術総合研究所特別研究員．情報セキュリティに興味を持つ．電子情報通信学会会員．

岡 博文

平成12年岡山大学工学部電気電子工学科卒業．平成14年奈良先端科学技術大学院大学博士前期課程修了．同年NRIセキュアテクノロジーズ株式会社入社．

楫 勇一（正会員）

平成3年大阪大学基礎工学部情報工学科卒業．平成4年同大学大学院修士課程修了．平成6年同大学院博士課程修了．同年奈良先端科学技術大学院大学情報科学研究科助手．平成10年同助教授，現在に至る．博士（工学）．符号理論，情報セキュリティ，オートマトン理論等に関する研究に従事．IEEE会員．