電子投票技術における他分野への応用の可能性 ～大学における相互評価システムの提案～

A1200334 宮島　麻由美

1　はじめに

現在大学教育において成績判定の資料として用いられているものは, 出席・レポートの提出・小テスト・定期試験などがあげられる. 学生を評価する場合, 上の資料だけではなくもっと多くの資料を用いて評価すべきである. 具体例をあげると「関心・意欲・成果」など, 教師が把握できない部分まで学生の内面を見る工夫を行うために, 学生同士の意見を教師の評価に反映させるための相互評価と, 自分を改めて見直すための自己評価を資料として用いる必要がある [9].

相互評価を実現するいくつかの要件がある. 誰が評価者か分からなくすることで匿名性を守る. 評価対象者は自分の評価された内容を教師以外の人が見れないようにすることでプライバシーを保護する. 集計がきちんと行われているかを検証できる. 教師は全員からの評価を得るために誰が未提出かを把握できる. 同じ人が二重に評価をすることを防止する. そして不当な評価に対しクレームをつけることができる. という以上６つの要件が挙げられる. これらの要件は選挙の要件と共通するものがある. そこで本研究では, 電子投票で用いられているミックスネット方式を利用して, 大学教育における相互評価システムを提案する.

2　ミックスネット方式による電子投票の実現 [7]

相互評価システムにはミックスネットと呼ばれる匿名通信路を介した電子投票方式を用いる. これは認証した投票者から暗号化された投票文を受け取ると, 全員の投票文を多段のセンター[1]からなるミックスネットを介してセンターに一括して伝達する方式である [6]. まず電子投票の実現のために必要な３要件を述べる.

2.1　投票の３要件

選挙において, 有権者の確認（認証）, 無記名性の確保, 選挙結果の正当性証明の３つの要件が必要である. １つ目の要件である有権者の確認は, 選挙権を持たない人の投票の防止と二重投票の防止を行う. 次の無記名性の確保は誰が誰に投票したか追跡できないようにする. 最後の選挙結果の正当性証明は自分の投票結果が選挙に反映されているか確認できるようにすることを目的とする.

2.2　ミックスネット方式について

ミックスネット方式は不在者投票で用いられてる方法を暗号化したものに似ている. 不在者投票の方法は, 投票者が投票用紙に記入し, それを封筒に入れる. この封筒を更に封筒に入れ, 外側の封筒には投票者の名前を記載する. 次に開票の方法は, 個々の投票について外側の封筒から内側の封筒を取り出す. 投票者の名前が書かれていない内封筒だけになった状態で, すべての投票者の封筒と混ぜ合わせる. この手順が票を追跡できなくしている. 最後に, 内封筒を開いて投票用紙を取り出し通常の開票に移る.

ミックスネット方式は, 各投票者は投票文を多重に暗号化（投票文を封筒に入れる）して, これに投票者自身の署名を施して（名前を記載）センターに送る. センターが１つだけだと無記名性が確保されないので, センターを複数設置する. 各センターはシャッフル（封筒の混ぜ合わせ）と復号（開封作業）を行う. この投票内容における暗号方式は公開鍵暗号方式を用いている. 暗号化で用いられる鍵を公開鍵, 復号化の鍵を秘密鍵と呼ぶ.

2.3　ミックスネット方式による投票の３要件の実現

一方ミックスネット方式では, 暗号処理を施した投票文に署名を付加するので, 有権者認証, 二重投票防止ができる. 無記名性の確保を実現するために, 各センターは有権者が暗号化した投票をシャッフルして復号する. 各段階の秘密鍵は別々の管理者が管理することで, 無記名性は確保できる[2].

正当性の証明は,「ゼロ知識証明 [3]」という技術を使うことで実現している. ゼロ知識証明を用いることで, 証明者が検証者にシャッフルおよび復号処理が正しく処理されているかを納得させるものであるが, 手順が終了しても検証者が自分で証明することはできないという性質を持つ.

[1] 投票集計所.

[2] 前提条件:各センターが結託しないこと.

3　大学における相互評価システムの提案 [2] [9]

授業における「関心・意欲・成果」の観点の評価にあたっては, プレゼンテーションの発表, 態度や行動, 作品の評価を学生の自己評価・相互評価などの多様な評価方法により継続的・総合的に行う必要がある. 自己評価とは, 学生が自らの学習を振り返り, その過程や成果について自ら判断し, その判断をもとに今後の学習を改善・調整することができるものである. 相互評価とは, 学生同士が相手の学びの課程や成果について判断しあうことである. これにより教師は, 学生同士の学びの課程や成果についての情報を得ることができ, 教師の一方的な判断や表面化された学生の姿のみではなく, より多くの資料を駆使して評価することができる.

そこで電子投票の暗号技術を用いた相互評価システムの提案を行う[3]. この提案では, 完全な匿名性が確保しつつ誰が未提出か明らかにすることができる. この匿名性により, 教師や学生が誰からの評価か分からないことで周りの目を気にせず, 自分の自由な発言が可能になる. 加えて, 復号化の処理を行った教師と学生が不正を行っていないか調べることが出来るので, 自分の発言がきちんと反映されているか調べることができる. さらに, 根拠のない評価に対するクレームをつけることができるようにする. これによって, 根拠のない評価の抑止力となる.

3.1　相互評価システムの要件

相互評価システムを実現する上でも, 選挙と同様に, 有権者（この場合学生）の確認（認証）, 無記名性の確保, 選挙（この場合評価）結果の正当性証明の３つの要件を果たされなければならない. まず学生の確認は関係者以外の送信, 又は同じ学生が二重に評価内容を送信していないか確認するため. 次に無記名性の確保は, 誰が評価内容を書いたのか追跡できないようにするためである. 最後に評価結果の正当性証明は, 評価システムが正当に行われているか確認できるようにする.

加えて相互評価システムは他の要件として, 評価対象者は自分の評価された内容を教師以外の人が見れないようにすることでプライバシーを保護する, 教師は全員からの評価を得るために誰が未提出かを把握できる, そして不当な評価に対しクレームをつけることができるという３点も加えられなければならない.

[3]本研究における相互評価には, 自己の評価を含むものとする.

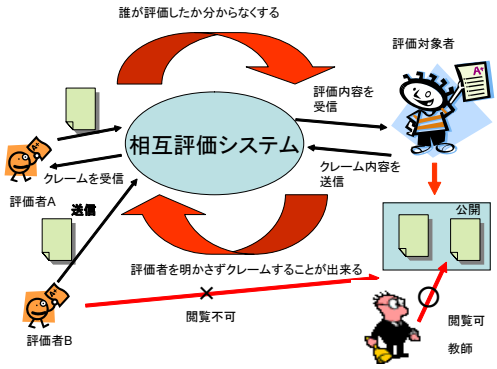

図 1: 相互評価システムの流れ

3.2　相互評価システム

このシステムの流れを図１に示す. まず評価する学生（評価者）は自己評価を含む評価[4] を教師の鍵と評価される学生（評価対象者）の鍵で二重に暗号化したものを, 教師に送信する. ミックスネット方式におけるセンターの役割は教師の管理するコンピュータが担う. コンピュータは受け取った評価を教師の鍵で復号化し, 全ての評価内容をシャッフルして, 評価対象者に送信する. 評価対象者は受け取った評価を自分の鍵で復号化し内容を確認する. そのうちの根拠のない評価に対して, 教師を通して評価者にクレームをつけることができる. また, 評価内容にクレームがあったからといって, 評価の内容を変えるかどうかは評価者に委ねられる. ただし, このクレームは何回やっても終わらない場合が考えられるため, 一回だけと限定する. このクレームに関して, 評価対象者はクレーム先を知ることはできない. クレーム先を知ることができるのは教師だけだが, 教師はそのクレームの内容を知りえない. クレームの内容を知ることができるのは, クレーム先の評価者である. このクレームは, 教師を通して評価者に届けられるので, 教師に不信感を持たれるのを避けようとし, 根拠のない評価が減ることが見込まれる.

クレームに対する返答が終了した段階で, 評価対象者は自分の評価内容をシャッフルして教師のみに公開する. 不正がないか確認するために, 評価者は評価内容を暗号化したものを公開し, 教師と評価対象者は処理したものを公開する. この相互評価システムによって, 評価内容を見ることができるのは, 評価対象者と教師のみである. この二人は評価内容を見ることができるが, 誰が評価したかを知ることはできない.

[4]評価内容は５段階評価と何故その評価をつけたのかの理由を示す.

3.2.1 [PIK93] によるミックス方式の匿名のチャネルを用いた相互評価の仕組み

ここでは, ミックスネット方式を用いた相互評価システムの定義を以下に行う. ただしクレーム用の鍵ペアは新たに生成し直すものとする.

公共の情報：$p = kq + 1$ (p, q は互いに素)

$q = (g')^k \bmod p$ (g'は $\bmod p$ の生成限)

教師の公開鍵:$y_t = g^{x_t} \bmod p$

教師の秘密鍵:$x_t \in Z_q^*$

評価対象者 i の公開鍵: $y_{s_i} = g^{x_{s_i}} \bmod p (i = 1, 2, ...)$

評価対象者 i の秘密鍵:$x_{s_i} \in Z_q^* (i = 1, 2, ...)$

評価者 a の公開鍵 (クレーム用) :$y_{s_a} = g^{x_{s_a}} \bmod p (a = 1, 2, ...)$

評価者 a の秘密鍵 (クレーム用) :$x_{s_a} \in Z_q^* (a = 1, 2, ...)$

評価内容:m

クレーム内容:c

電子署名:$S_{s_i} (i = 1, 2, ...)$

宛先の情報:A_{s_i}

3.2.2 暗号化されたメッセージ

評価者 i は, 乱数 r_0 を生成し, 評価内容 m にクレーム用の公開鍵を付加したものを次のように暗号化し電子署名を付加する.

$$G_1 = S_{s_i} \| A_{s_i} \| g^{r_0} \bmod p \quad (1)$$

$$M_1 = (y_t \cdot y_i)^{r_0} \cdot (y_{s_a} \| m) \bmod p \quad (2)$$

を教師に送る[5].

3.2.3 メッセージの処理

教師は電子署名 S_{s_i} を確認し, 正当な評価である場合は, 乱数 r_1 を生成する. そして, 教師の秘密鍵 x_t を使用して以下の計算をする.

$$G_2 = G_1 \cdot g^{r_1} \bmod p = g^{r_0 + r_1} \bmod p \quad (3)$$

$$M_2 = M_1 \cdot y_t \cdot {y_i}^{r_1} / G_1^{x_t} \bmod p = y_i^{r_0 + r_1} \cdot (y_{s_a} \| m) \bmod p \quad (4)$$

教師は他の学生から得た評価内容をまとめ, 宛先 A_{s_i} ごとに分類し, その中で置換処理する. その後, 宛先別に評価内容を送信する.

評価対象者は以下の計算をする.

$$y_{s_a} \| m = M_2 / G_2^{x_{s_i}} \bmod p \quad (5)$$

これによりクレーム用公開鍵 y_{s_a} と評価内容 m を得る.

[5]ただし || は連結を表す.

3.2.4 クレーム処理

評価対象者は, 根拠のない評価についてクレームを出すことができる. 評価対象者は評価内容に付加してあった公開鍵 y_{s_a} を使って以下のようにクレームの内容を暗号化したもの C と, G_2,M_2 を教師に送る.

$$C = y_{s_a} \cdot c \bmod p \quad (6)$$

このとき,G_2,M_2 も一緒に送るのは教師がクレーム先を判別するためである. 教師はクレームの内容を, クレーム先である評価者に送る. クレームをもらった評価者はクレームの内容を読み, 必要に応じて評価内容を変更した評価を暗号化した M_4 を教師に送る.

$$M_4 = A_{s_1} \| y_i \cdot m \bmod p \quad (7)$$

教師は M_4 を送信するだけで置換や復号は行わないものとする.

3.2.5 クレーム処理の暗号方式

クレーム処理には公開鍵暗号方式を用いる. もし共通鍵暗号方式を用いた場合, すべての学生が同じ鍵を持っていることになり, 復号が可能となってしまう. その点公開鍵暗号方式を用いた場合, 学生がクレーム内容の暗号文を盗み見ても, 復号の鍵が異なるので暗号解読はできないのである.

3.3 集計の正当性の検証

集計の正当性を検証するために, 復号の正当性とシャッフルの正当性をそれぞれ分けて検証する. (G_i,M_i) の組と,(G_{i+1},M_{i+1}) が与えられるが, 最初の段階では $G_i^{x_i}$ として送られている. 教師と学生は各々の正しさを証明する.

3.3.1 復号の正当性

G が与えられ, 最初の段階で, 復号を行い,$H = G^x \bmod p$ を生み出すことから成る. そして (G,g,$y = g^x \bmod p$) が与えられている.

1. 証明者は,$r \in Z_{p-1}$ を一様に選ぶ.

$$y' = g^r \bmod p \quad (8)$$

$$G' = G^r \bmod p \quad (9)$$

. 検証者は,(y',G') を送る.

2a. 1/2 の確率で, 検証者は証明者に r を明らかにすることを頼む.

2b. 1/2 の確率で, 検証者は証明者に $r' = r - x$ を明らかにすることを頼む. 検証者はチェックする.

$$y' = g^{r'} \cdot y \bmod p \quad (10)$$

$$G' = H \cdot G^{r'} \bmod p \quad (11)$$

3.3.2　シャッフルの正当性

定数 g,w と

$$A = \begin{pmatrix} a_i^{(1)} \\ a_i^{(2)} \end{pmatrix}$$

が与えられ, 二番目の段階は, 生成された r_1,r_2,... と置換の Π と生成された一組のセットから成っている.

$$B = \begin{pmatrix} {a_{\Pi(i)}}^{(1)} \cdot g^{r'_{\Pi(i)}} \bmod p \\ {a_{\Pi(i)}}^{(2)} \cdot \omega^{r'_{\Pi(i)}} \bmod p \end{pmatrix}$$

G と $a_i^{(2)}$ は最初の段階の M/H のものを引用する. 証拠は, 与えられた (A,B,g,w),B は A からの生成されることができることを見せることから成り立っている.

1. 証明者は, 様に $t_i \in Z_{p-1}$, 乱数の置換 λ と

$$C = \begin{pmatrix} {a_{\lambda(i)}}^{(1)} \cdot g^{t_{\lambda(i)}} \bmod p \\ {a_{\lambda(i)}}^{(2)} \cdot \omega^{t_{\lambda(i)}} \bmod p \end{pmatrix}$$

を選ぶ.

2a. 1/2 の確率で, 検証者は λ と t_i を明らかにすることを証明者に求める. 検証者は,C は,A,λ,t_i によってこの方法で生成されているかチェックする.

2b. 1/2 の確率で, 検証者は $\lambda' = \lambda \circ \pi^{-1}$ と $t'_i = t_i - r'_i$ を証明者に求める. 検証者は次のような方法で C は B で生成されていることをチェックする.

$$B = \begin{pmatrix} b_i^{(1)} \\ b_i^{(2)} \end{pmatrix}$$

$$C = \begin{pmatrix} {a_{\lambda(i)}}^{(1)} \cdot g^{t_{\lambda(i)}} \bmod p \\ {a_{\lambda(i)}}^{(2)} \cdot \omega^{t_{\lambda(i)}} \bmod p \end{pmatrix}$$

4　おわりに

この大学の相互評価システムを用いることにより, 学生は紙媒体以上に相手に的確な評価を下すことが可能になる. これにより教師は学生に関する多くの資料を得て学生を評価できる. そして学生も評価しあうことで互いに刺激し合い, 自分の学習の行動を振り返り, 今後自分の行動を改善し, 学習意欲や学習成果の高揚が期待できる. そして教師自身も, 学生の授業への関心・意欲・成果についての評価が悪ければ, 自分の学習指導の問題点も確認できる. つまりこの相互評価システムは単に教師から学生への評価に資料として役立つだけではなく, 学生の学習意欲が向上することと教師の指導の向上に繋がることが期待される. また企業で相互評価システムを用いることも可能である. 例えばプロジェクトチームを組んで仕事をする場合, 相手に言いにくい発言も気兼ねなく言い合えるようになる. このようにお互いを高めることができるこのシステムにより, プロジェクトマネージャーは, チームのメンバーの特性を知ることができ, 一人一人の相手に対する意見を反映させることでコミュニケーションを管理し, その上であるミッションへ向かって問題を解決していくことを円滑に進めることができる. このように相互評価システムは大学教育以外の場所でも多様な使用の可能性を秘めたものである.

しかし, 大人数教育にこのシステムを導入した場合, 学生の発表や作品などの学習の成果に対する評価は可能であるが, 学生一人一人に対する授業の関心や意欲まで目が行き届かないという相互評価そのものの課題が解決できていない. 今後,e-learnig などを用いて, 大人数教育に対応できるシステム作りが課題となる.

参考文献

[1] Choonsik PARK, Kazutomo ITOH and Kaoru KUROSAWA,“ Efficient Anonymous Channel and All/Nothing Election Scheme”, Advance in cryptrogy,EUROCRYPT’93,pp.248-259,1993.

[2] Kazue Sako, Joe Kilian, “ Receipt-Free Mix-Type Voting Scheme ”, Advances in cryptology, EUROCRYPT’95,pp.393-403,1995.

[3] Douglas R.Stinson, 暗号理論の基礎, 共立出版株式会社,1996.

[4] 岡本 龍明, 山本 博資, 現代暗号, 産業図書,1997.

[5] 佐古 和恵,“ 公平性とプライバシー保護 ”, 電子情報通信学会誌, vol.83,No.2,pp.112-116,2002.

[6] 佐古 和恵,“ 電子投票と電子入札 ”日本オペレーションズ・リサーチ学会,pp.514-519,2002.

[7] 宮内 宏, 尾花 賢, 森 健悟,”電子投票の実現”, 電子情報通信学会誌,vol.86,No.5,pp.331-336,2003.

[8] 北川 隆, 岡 博文, 楫 勇一“ 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 ”, 電子情報通信学会誌, vol.44,No.9,pp.2353-2362,2002.

[9] http://www.educ.pref.fukuoka.jp/kensyu/tyouken/h14/05teramoto.pdf, 古橋　透. 学習指導の改善をめざす中学校英語科の目標に準拠した評価の在り方.