社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2007－GN－64（5）
2007／6／1

紙答案と電子フィードバックを併用した講義支援および個人情報保護方法

Integrating paper and electronic media to enable feedback and personal information protection in class

市村　哲†　山下　亮輔†　中村　亮太†　上林　憲行†

† 東京工科大学　〒192-0982 東京都八王子市片倉町 1404-1
E-mail: †ichimura@cs.teu.ac.jp

あらまし　大規模講義ではその人数の多さゆえに，学生に十分な学習支援が困難であるという現状がある．講義と期末テストの実施で手一杯になってしまうことが多いが，学生は「演習やミニテストがあり自分の理解度を確認できる」,「講師からフィードバックが受けられる」講義を求めている．近年，IT 技術を利用して大規模講義の質の向上をめざす例が増えてきているが，ノート PC やネットワーク環境のトラブル等により，ミニテストや定期テストは紙で行なわなければならないのが現状である．そこで著者らは，大規模講義を支援することを目的とした研究活動の一環として，紙と電子メディアのそれぞれの長所を融合する講義支援システムの開発を試みた．構築したシステムは，2 次元バーコードと文字認識技術を利用したシステムであり，紙の答案に書かれた学籍番号や解答マークを文字認識およびマーク認識し，結果を PC に自動入力する機能を備えている．さらに，成績評価やコメントがかかれた答案用紙を複合機で一括スキャンして PDF ファイルとして Web サーバーに蓄積し，この PDF ファイルの URL を各学生に電子メールで自動送信する「電子フィードバック機能」を有する．加えて，個人情報保護のための仕組みとして，答案用紙をスキャンする際に，学籍番号，氏名，評価点欄などの領域で画像分割し，分割した部分画像毎に暗号化して保存する機能を提供している．
キーワード　教育支援システム，個人情報保護，紙と電子

Satoshi ICHIMURA†, Ryosuke YAMASHITA†, Ryota NAKAMURA†, and Noriyuki KAMIBAYASHI†

† Tokyo University of Technology　Katakura 1404-1, Hachioji-shi, Tokyo, 192-0982 Japan
E-mail: †ichimura@cs.teu.ac.jp

Abstract　Due to the large number of students, lectures in the auditorium are likely to be limited to delivering one-sided lecture and conducting final exam. However, it is apparently desirable for students to have opportunities to check their own progress or understanding level through frequent check-up. Some have tried to build information systems for online-test or taking attendance. However, paper could not be replaced by online system due to the inevitable trouble of students' laptop PC or computer network. For this reason, we developed an educational system where the merit of paper and electronic media were merged. The system automatically recognizes student's ID and check marks written in paper. 2-D barcode and character recognition technology were combined in the system for this purpose. The scanner reads each student's report annotated by the lecturer and creates PDF, and sends it back to each student via e-mail. For the personal information protection, the created PDF is entirely or partially encrypted through the RSA public-key cryptography.
Key words　Educational system, Personal information protection , Paper and electronic media

1. はじめに

教育の現場では，大規模講義（数百名以上の学生が教室に集合して受講する講義形態をここでは大規模講義と呼ぶこととする）において学生に十分な学習支援が困難であるという現状がある．例えば，私立大学では，数百名の学生が履修する講義を，TA(Teaching Assistant) 等のサポートなしに講師 1 人ですべて担当することも珍しくなく，講義と期末テストの実施で手一杯になってしまうことが多い．「わかりやすく満足できる授業」について本学学部生を対象としてアンケートを行った結果，少人数講義の方が大人数講義よりも学生の満足度が総じて高いことがわかった．少人数講義の満足度が高い理由としては，「演習やミニテストがあり自分の理解度を確認できる」，「講師からフィードバックが受けられる」などが多く挙げられた．

このような学生のニーズを受け，大規模講義であっても電子メディアを利用して学習支援サービスの質の向上をめざす例が増えてきている．例えば，著者らが所属する大学では，情報コンセントが各教室の各机に備わっており，また，学生全員が自分のノート PC を講義で利用することが義務づけられているため，この環境を利用して Web フォームを利用したレポート提出や，専用の出席確認ソフトを用いて出席確認を実施する講義が存在する（図 1 参照）．

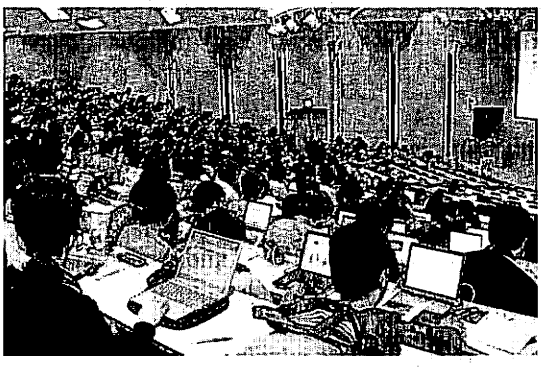

図 1　大規模講義風景
Fig. 1　Lecture in the auditorium

しかしながら，現状，電子メディアだけに頼ることができない問題がある．例えば，著者らが担当する約 480 名の大規模講義（メディア学部の必修科目「キャリアデザイン」）では，毎回 5 名〜10 名程度の学生が，修理中，持参し忘れた，原因不明でフリーズした等のトラブルにより講義中に PC を使えない状況である [1]．また，講師がレポートを採点する時，数百名分の文章を PC のディスプレイ上で読んで採点すると非常に疲れてしまうのが現実である．このため，ミニテストや定期テストは紙で行なわなければならないのが現状であり，全て手作業となるため教育スタッフの負担は大きいままである．

以上の背景から，大規模講義を支援することを目的とした研究活動の一環として，紙と電子メディアのそれぞれの長所を融合するシステムの開発を試みた [2]．紙にはリスクに対する耐性があり，かつ，読みやすく，また，記述内容を証拠として残せるメリットがある．一方，電子メディアには情報を整理しやすく，学生に対して個別フィードバックなどの情報伝達を行いやすい特徴がある．

今回構築したシステムは，2 次元バーコードと文字認識技術を利用したシステムであり，紙の答案に書かれた学籍番号や成績評価を文字認識およびマーク認識し，結果を PC に自動入力する機能を備えている．さらに，成績評価やコメントが書かれた答案を高速複合機で一括スキャンして PDF データとして Web サーバーに蓄積し，この PDF の URL を各学生に電子メールで自動送信する機能（「電子フィードバック機能」）を有する．

さらに構築したシステムは，個人情報保護のための仕組みとして，答案用紙をスキャンした際に作成される画像データを暗号化して保存する機能を有している．公開鍵が 2 次元バーコードで紙に印刷されており，この紙をカバーシートとして答案用紙の束と一緒に複合機に読ませることで，答案用紙を簡単に暗号化できる．また，答案用紙をスキャンした画像をそのまま 1 枚の画像として保存するのではなく，学籍番号，氏名，評価点欄などの領域で画像分割し，分割した部分画像毎に異なる鍵で暗号化して保存する機能も提供している．例えば，TA がスキャン画像を見る際には，学籍番号と答案内容の画像だけが見え，一方，氏名や評価点の画像は暗号化されたままで見ることができない．

本論文では，構築したシステムの設計，実装，評価について述べる．

2. 背景と問題点

私立大学における講義は，大教室で行われる大規模講義であることが多い．大規模講義は極めて一般的であり，理系学部，文系学部を問わず多く見受けられる．しかしながら，実験や演習といった一部の例外を除けば，TA 等のサポートスタッフが割り当てられることはまれであり，講師がその講義に関わる運営をすべて 1 人で行わなければならないのが普通である．このような理由から，講師が学生に対して一方的に講義するだけの授業にならざるを得ないのが実情であり，例えば，学生数が数百名を超える講義において出席カードを配って学生の出席をとることさえ困難である．通常は，定常的に行われる講義と，期末テストの実施に終始することが多い．

一方，著者らが所属する大学が全学生に対して継続的に実施している授業評価アンケートの結果からは，少人数制の講義と比較して，大規模講義対する学生の満足度が低いことが明らかとなっている．少人数制講義の満足度が高い理由として，学生らは，「演習問題やミニテストがあり自分の進度/理解度を確認できる」，「演習の解答や解説が随時行われる」，「自分がやったことに対して講師からフィードバックが受けられる」などの工夫が行なわれていることが多いことを挙げている．少人数制講義においては実施可能なこれらの教育手法が行えないことが大規模講義の問題であると推測できる．

以上のような状況から，著者らは，大規模講義であっても一

方的な講義に終始しないことが重要と感じており，担当講義において数々の工夫を行ってきた．本論文では，特に，本学メディア学部の大規模講義である「キャリアデザイン」において，著者らが実践した方法，および，その実践のために構築したシステムについて述べる．本講義は必修科目のため，受講学生数は約 480 名であり，大規模講義の中でも特に履修者数の多い講義となっている．なお，本講義は演習の性質も備えているため，数名の大学院生 TA が付与されている．

システムを導入する前までの「キャリアデザイン」の講義では，毎週ミニテスト (「自己チェックシート」) の答案を紙で集め，講師と TA とによって評価結果およびコメントを手書きで追記し，次週以降に各学生に返却するようにしていた．この方法では，成績入力のために答案を学籍番号順に並び替えるだけでも毎週膨大な時間が必要であることが問題となっていた．また，答案を各学生に返却する際，答案を学籍番号順で 50 名分ずつの山に分けておき，各学生に自分の答案を探すように指示していたが，全員に返却するためには少なくとも 15 分〜20 分の時間が必要となっていた（図 2）．加えてこの返却方法には，遅刻や欠席をした学生に返却できない，他の人の答案を間違って持ってゆく学生が存在するといった問題があり，講義が混乱してしまうことがしばしばあった．

図 2　答案用紙返却時の混雑
Fig. 2　Returning report to students

3. 紙と電子メディアの融合機能

3.1 機　　能

本システムによって実装した紙と電子の融合機能について述べる．学生が用いる 2 次元バーコード付き答案用紙は図 3 のようなものである．バーコードとしては，ゼロックス社が開発した「グリフ」[8] を利用した．グリフは斜め線模様であり，右上がりか右下がりかでビットの ON/OFF を表す．今回の実装では，スキャンした答案用紙をどのルールによって処理すべきかを示すための ID としてグリフが利用されている．グリフの代わりに QR コード等の他の 2 次元バーコードで代替しても構わない．

一方，チェックボックス内の塗りつぶしマークや，学籍番号の数字は，画像処理によって自動読込みされる．数字記入枠については，長方形枠内に 6 個の点が配置されており，この点を線で結んで 0 から 9 までの数字を書かせるものである．数字をブロック体で書くことを強制することで，読み取り誤りを減少させている．グリフコードの作成・認識，および，数字の文字認識は富士ゼロックス社からモジュール [9] の提供を受けた．

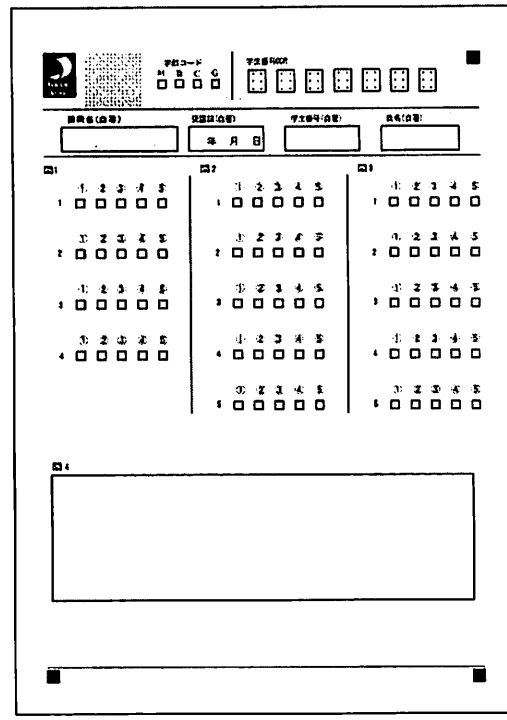

図 3　グリフシート
Fig. 3　Glyph sheet

以下に典型的なシステムの利用シナリオを示す．

（1） 学生は，答案用紙であるグリフシートに，学籍番号，氏名，および，解答内容を鉛筆で記入する．

（2） 回収したグリフシートに講師や TA が赤鉛筆でコメントを追記する（図 4 参照）．評価者用の評価点記入欄がある場合，講師や TA はこれにも記入する．

（3） 講師がグリフシートを複合機でスキャンすると，システムによって電子ファイル（PDF）が作成されると共に，学籍番号と評価点が文字認識される．これと同時に，作成された PDF にはランダムかつユニークな URL が割り当てられ，Web サーバ上に配置される．そしてシステムは，自動読み取りした学籍番号と評価点，および，PDF に割り当てた URL を対として記録し，CSV ファイルに一括出力する．

（4） 各学生宛メールの本文に，各自の PDF にアクセスするための URL が自動記入される．講師が送信ボタンが押されると各学生にメールが一斉送信される．

（5） 学生は，受け取ったメール中の URL をクリックして，コメントや評価点が追記された PDF をダウンロードする．

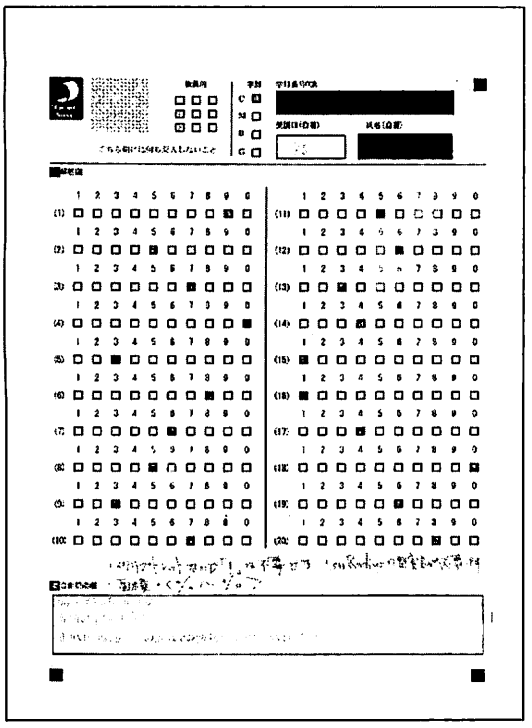

図 4 追記コメント（下部の手書き）
Fig. 4 Annotation by lecturer

3.2 実験と評価

キャリアデザインの講義において，半年間，本システムを実運用した．その結果，システムを導入することで，教育スタッフと受講学生の双方に以下のメリットがあることが確認できた．
教育スタッフの利点： 480 名分のデータを学籍番号に並び替える作業を省くことができる．学籍名簿に各学生の点数を転記する作業を正確かつ素早く行える．答案を各学生に返却する際に必要となっていた時間を無くし，本来の講義時間として利用できる．各学生の答案 (PDF) を時系列で並べて表示できるため，つまづいた箇所等を分析することができる．
受講学生の利点： 次回の講義前に答案が返却されるため，次回講義前までにコメントを確認できる．答案返却時の混乱が発生せず，返却答案を確実に入手できる．

一方，顕在化した問題点としては，学籍番号の読み取り誤りが存在し，それを確認するための作業が必要となったことが挙げられる．学籍番号のすべての文字が正しく認識できた場合を正常認識と見なした場合，480 件中の約 50 件に何らかの認識誤りが認められた．読み取り誤りが発生した答案用紙には，学籍番号が未記入のもの，学生が間違って違う数字を記入してしまったもの，記入文字の濃度が足りない等も含まれている．

そこで，第 3 回講義からは，各学生の学籍番号をあらかじめ記入したグリフシート（PDF）を生成して Web サーバに配置し，その PDF の URL を各学生にメール送信し，PDF を印刷して毎回の講義に持参させるように周知した．このシートに答案を記入させて回収した結果，紙が破損したり，学籍番号欄が汚れていることによるエラーはわずかに残ったが，これらを除けば学籍番号に認識誤りを含むものは 0 件となった [1]．図 5 に，手書きで記入された学籍番号の例，予め印刷した学籍番号の例を対比して示す．

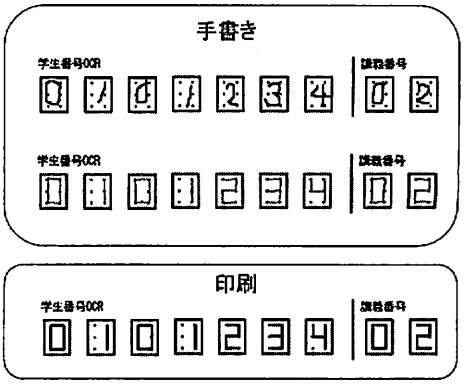

図 5 手書き数字と印刷数字
Fig. 5 Handwriting and printed number

4. 個人情報管理機能

4.1 基本機能

学籍番号と氏名とが対となって外部公開されると個人情報漏洩の問題としてみなされる現状において，個人情報をセキュアに管理することは極めて重要である [3] [4]．前述の紙と電子メディアを融合した講義支援システムにおいても，答案用紙をスキャンして作成した PDF ファイル（学籍番号と氏名が対となった画像データ）を教育スタッフ側で共有した際に，個人情報が漏洩する可能性がある．すなわち，答案用紙が紙の形態のままであれば情報漏洩に対する対策を講じる必要性はほとんどなかったが，それをスキャンして電子データに変換したためにその必要性が生じたと言える．

この問題意識から，答案用紙をスキャンした際に作成される画像データが暗号化して保存されるようにシステムを改良した．この際，数百名の答案用紙をスキャンするような高速な複合機は学部や学科で共有利用されることが想定できる．そこで，複数のユーザが簡単かつ安全に画像データを暗号化できるようにするために，公開鍵暗号方式と 2 次元バーコード技術を組み合わせた暗号化方法を構築した．

画像の暗号化には 1024 ビットの RSA 公開鍵暗号方式を用いている（本実装では，.NET Framework 標準の PublicKeyCryptography モジュール [5] を用いた）．暗号化の際に公開鍵を用い，復号化の際は，この公開鍵とペアとなる個人の秘密鍵でこの暗号を解く（正確には，データ自体は共通鍵で暗号化し，その共通鍵を公開鍵で暗号化して暗号化データと共に受信者に送信するハイブリッド暗号化方式を用いている）．

答案用紙を暗号化する際に，暗号化に用いる自分の公開鍵をシステムに入力する必要があるが，本システムでは，複合

機に紙を読み込ませる操作だけでこの処理が行えるようになっている．具体的には，公開鍵が 2 次元バーコード（QR コード）[6] [7] で紙に印刷されており，この紙をカバーシートとして答案用紙の束と一緒に複合機にスキャンさせることで，答案用紙を暗号化できるようにした．図 6 は公開鍵を QR コードに変換した例である (誤り訂正符号が 15 %加えられている)。

図 6　QR コード表示された公開鍵の例
Fig. 6　QR code of public key

以下に，典型的な利用シナリオを述べる．ここで述べるシナリオは，本システムを利用するのが講師のみであり，答案用紙全体を 1 つの鍵で暗号化する場合である．なお，答案用紙スキャン時，前述の通り学籍番号や評価点が文字認識されるが，ここでは説明を省略する．

4.1.1　事前準備

講師は，本システムを使い公開鍵と秘密鍵のペアを生成する．この時，秘密鍵が自分の PC にセキュアに保存されると共に，公開鍵が QR コードとしてカバーシート (A4 用紙) に印刷される．講師は作成されたカバーシートをプリンタで印刷しておく．このカバーシートを利用して暗号化した答案用紙画像を復号化できるのは秘密鍵を持つ講師のみである．

4.1.2　答案用紙スキャン時

答案用紙の束の上に上記カバーシートを重ね，この束を複合機の ADF に載せスキャンを開始する．この時複合機がビットマップ画像を作成するが，本システムは，カバーシートに印刷された公開鍵を利用してこのビットマップ画像を暗号化する．

具体的には，システムはランダムな共通鍵を生成し，この共通鍵でビットマップ画像を暗号化してネットワーク共有フォルダーに保存する．そしてこの時用いられた共通鍵をカバーシートに印刷された公開鍵で暗号化し，ビットマップ画像と一緒のフォルダーに保存する．

4.1.3　答案用紙閲覧時

答案用紙閲覧時，講師はネットワーク共有フォルダーから暗号化されたビットマップ画像と，暗号化された共通鍵とを入手し，自分が保持している秘密鍵で暗号化された共通鍵を復号化する．そして，この復号化された共通鍵で暗号化されたビットマップ画像を復号化する．これによってビットマップ画像の内容を閲覧できる．

学生にフィードバックする際には，ビットマップ画像を PDF データに変換し，前述の電子フィードバック機能を用いてメール送信するようになっている．

4.2　応用機能

さらに，講師と TA が個人情報を共有する状況に対応するため，学籍番号，氏名，評価点欄などを領域で画像分割し，分割した部分画像毎に暗号化して保存できるようにした．この時，講師と TA の両方の公開鍵で個人情報を暗号化する．これにより例えば，TA は学籍番号と答案内容の画像だけが見えるが，講師は学籍番号と答案内容の他，学生氏名や評価点の画像も見えるようになる．

以下に，典型的な利用シナリオを述べる．ここで述べるシナリオは，本システムを利用するのが講師と TA であり，答案用紙全体を複数の鍵で暗号化する場合である．

4.2.1　事前準備

講師は講師用の公開鍵・秘密鍵のペアを作成し，この時，講師用の秘密鍵は講師の PC にセキュアに保存される．TA も TA 用の公開鍵・秘密鍵のペアを作成し，TA 用の秘密鍵は TA の PC にセキュアに保存される．講師の公開鍵と TA の公開鍵はお互いに共有されている．

説明を単純化するため，ここでは，学籍番号と答案内容を画像領域 A，氏名と評価点を画像領域 B と分けたと仮定する．そしてカバーシートを作成する際，講師は画像領域 A および B，TA は画像領域 A が見えるようにしたいとシステムに入力する．するとシステムは，講師の公開鍵，と TA の公開鍵，および，各公開鍵でどの画像領域を暗号化するかを記憶した情報を，カバーシート 1 枚に QR コードとして連ねて印刷する．

4.2.2　答案用紙スキャン時

講師は，答案用紙の束の上に上記カバーシートを重ね，この束を複合機の ADF に載せスキャンを開始する．この時システムは，画像領域 A（学籍番号と答案内容）を暗号化する共通鍵 A と，画像領域 B（氏名と評価点）を暗号化する共通鍵 B を作成し，共通鍵 A で学籍番号と答案内容を暗号化し，共通鍵 B で氏名と評価点を暗号化する．そして，講師の公開鍵を利用して共通鍵 A と共通鍵 B を暗号化し，暗号化された共通鍵 A1 および B1 を作成する．また，TA の公開鍵を利用して共通鍵 A を暗号化し，暗号化された共通鍵 A2 を作成する．

答案用紙の各領域を暗号化したビットマップ画像と，暗号化された共通鍵 A1，B1，A2 は，同一のネットワーク共有フォルダーに保存される．

4.2.3　答案用紙閲覧時

答案用紙を閲覧する際，講師は，ネットワーク共有フォルダーから，暗号化された共通鍵 A1 と B1 を入手し，自分が保持している秘密鍵を用いて共通鍵 A，共通鍵 B を取り出す．そして，共通鍵 A と共通鍵 B をもちいて画像領域 A（学籍番号，答案内容）および，画像領域 B（氏名，評価点）を復号化する．

一方 TA が答案用紙を閲覧する際は，ネットワーク共有フォルダーから，暗号化された共通鍵 A2 を入手し，自分が保持している秘密鍵を用いて共通鍵 A を取り出す．そして，共通鍵 A をもちいて画像領域 A（学籍番号と答案内容）を復号化する．TA が暗号化された共通鍵 B1 を入手しても，TA の秘密鍵では共通鍵 B を取り出すことができないため，TA は画像領域 B

（氏名および評価点）を閲覧することはできない．

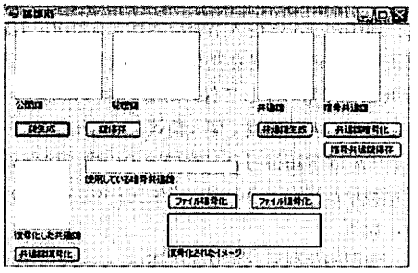

図 7　講師用ツールの画面デザイン
Fig. 7　Software for lecturer

4.3　実装システム

実装したソフトウェアの画面デザインを図 7 に示す．図 7 は講師用のツールを示しており，講師用の公開鍵・秘密鍵ペアを作成する機能や，暗号化されたファイルを復号化する機能の他，講師が答案用紙スキャン時にファイルを暗号化するための機能（共通鍵生成，共通鍵暗号化，ファイル暗号化の各機能）を兼ね備えている．

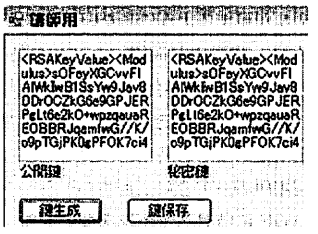

図 8　鍵ペア作成
Fig. 8　Creating key-pair

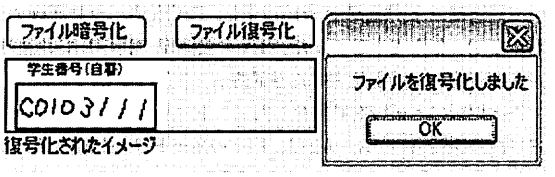

図 9　暗号化された学籍番号の復号化
Fig. 9　Decoding encrypted student's id

図 8 に，講師が公開鍵・秘密鍵ペアを作成した様子を示す．また，図 9 には，暗号化された学籍番号の領域を復号化した様子を示す．

5. ま と め

大規模講義を支援することを目的とした研究活動の一環として，紙と電子メディアのそれぞれの長所を融合する講義支援システムの開発を試みた．電子メディアを利用した講義支援システムは多く提案されているが，パソコンまたはネットワーク環境のトラブルによって，ほぼ毎回，授業が混乱してしまうのが現状である．そこで今回，リスクに対する耐性があり，かつ，読みやすいという紙のメリットと，情報を整理しやすく，伝達しやすいという電子メディアのメリットを融合するシステムを構築した．

2 次元バーコードと文字認識技術を利用することにより，採点処理，成績処理を効率化することができた．半年間の実運用の結果，この効率化により，教育スタッフは本来の教育業務により多くの時間を使えるようになったことがわかった．また，成績評価やコメントが追記された答案を PDF で各学生に電子フィードバックできるようにしたことで，それまで紙で返却していた際に生じていた授業の混乱が発生しなくなった．答案にコメントや評価結果を追記してこまめに学生に返却することは，学生の勉学への動機付けとなる可能性がある．

また，答案用紙をスキャンして電子データに変換したために生じる個人情報漏洩防止の必要性に関し，公開鍵暗号方式と 2 次元バーコード技術を組み合わせた個人情報管理機能を提案した．講師と TA が個人情報を共有する状況にも対応できるようになっている．この個人情報管理機能については実装と動作検証が終了した段階であり，今後，実際の授業で運用して行きたいと考えている．

文　献

[1] 小山内，神林，長井，上林，市村，山下，田丸，三浦: 大教室講義における個別フィードバックを支援する複合的なメディアを活用した教育サービス -サービス設計と運用方法-，第 69 回情報処理学会全国大会，6ZA-5 (2007).

[2] 松本，山下，上林，市村: 紙と電子情報を併用した講義のための個人情報保護手法，第 69 回情報処理学会全国大会，1Z-7 (2007).

[3] 大学教育と情報：個人情報保護への留意点と対策，私立大学情報教育協会，Vol.14，No.2　(通巻 111 号) pp. 2 − 18, (2006).

[4] 大学教育と情報：個人情報保護への留意点と対策（2），私立大学情報教育協会，Vol.14，No.3　(通巻 112 号) pp. 2 − 17, (2006).

[5] PublicKeyCryptography モジュール，Microsoft 社: http://msdn2.microsoft.com/ja-jp/library/xct38ftb(VS.80).aspx

[6] QR Code Image，Psytec 社: http://www.psytec.co.jp/freesoft/

[7] Open Source QR Code Decode Library, http://sourceforge.jp/projects/qrcode/

[8] Johnson, W., Jellinek, H., Klotz L. Jr., Rao, R. Card, S.: Bridging the Paper and Electronic Worlds: The Paper User Interface, ACM Conference on Human Factors in Computing Systems (ACM CHI'93), pp.507-512, (1993).

[9] DocuShuttle，富士ゼロックス社: http://www.fujixerox.co.jp/product/docushuttle/