# 独自のＱＲコードを用いた出席管理システムの開発と実践

先名健一　　麻布大学非常勤講師
1729manifold@gmail.com　sakina@azabu-u.ac.jp

## １．はじめに

近年、大学の講義における出席確認として、ICTの活用は一般的な流れであるが、従来の出席確認、即ち、点呼、出席カード、小テスト、レポートなどによる方法も依然利用されている[1]。麻布大学の場合､学生証のICタグを利用したシステムを設置した経緯があるが、業者構築のシステムの高コストと大学の実情に合わない使い勝手の悪さ、更に代理出席問題などから現在は使われていない。

以下で報告する出席登録システムは、機能的にはシンプルであるが、セキュリティが高く低コストでかつ自由度の高いシステムの構築を可能にする。

## ２．デジタル署名アルゴリズム

偽造･改ざんの検出が可能な独自のQRコード(以下、DSQRコード）は、デジタル署名アルゴリズムに基づいている。以下、簡単に説明すると、まず、採用した署名アルゴリズムに従って公開鍵 Kp と秘密鍵 Ks を生成し、メッセージ M のハッシュ値、乱数 r 及び Ks から署名 sig を生成する。次に、受取ったメッセージ M'(M とは限らない)の検証では､M'、署名 sig'及び Kp を使い､矛盾が存在しないかを検証する。デジタル署名アルゴリズムのなかで、署名値の長さが最も短くて済むのが、楕円曲線デジタル署名アルゴリズム（以下、ECDSA）である。例えば、RSAデジタル署名ではECDSAの１０倍以上の鍵長の署名が必要になる。ECDSA は有限体上の楕円曲線上の点からなる巡回群を用いており、巡回群の大きさを大体 $10^{50}$ 以上にすると現実的に離散対数問題が解けないという性質を使う。

## ３．DSQR コード

DSQR コードは、QR コードに ECDSA によるデジタル署名を埋め込んだもので、QR コードの偽造や改ざんの有無が検知できる。具体的には、まず有限体上の楕円曲線とその上の点 G（ベースポイント）を設定する。次に、乱数を発生させ、それを秘密鍵 Ks とする。このとき、公開鍵 Kp は Kp=Ks*G により決まる。なお、Kp は２つの整数の組からなる。メッセージを含めた QR コードデータのハッシュ値 h、乱数 r などを使い、署名値 sig を生成する。そして、元の QR コードに sig を排他的論理和で埋め込み DSQR コードが作られる。例えば、7H 型の QR コードをベースにして、160 ビット×２の sig を QR コードに埋め込み、更に、アルゴリズムを少し変えることで、偽造・改ざんの検出の他に、パスワード（以下、PW）と秘密言葉（以下、SW）が使えるようにできる。図１は、DSQR コードの一例である。メッセージが「M17000」、PW が「azabu123」、そして SW として「臨床検査」が格納されている。ただし、PW は QR コードに直接格納されている訳ではないので解読されることは殆どあり得ない。また、通常の QR コードリーダで読むと、メッセージのみしか表示されない。このように、DSQR コードを使うと、コードの真正性だけでなく PW による個人認証も可能になる。また、SW と PW を共に使用することで、通信相手との相互認証を可能にする。

図１　DSQR コード

## ４．出席登録及び確認システム

写真１は講義に使用している出席登録の装置で、PC と２台の Web カメラ（CP-01）からなる簡単なものである。図２のように学生がスマートフォンに表示した DSQR コードを Web カメラにかざすと、直ちにコードの真偽判定が実行され、正規のコードのときのみ出席登録が実行される。９０名ほどのクラスでは４～５分の時間で出席登録が完了する。出席データは１クリックで PC 保存の Excel ファイル

に書き込まれる。なお、Excel ファイルは学生課が作成した名簿ファイルを転用している。

写真１　出席登録装置

図２　出席登録

図３は学生が自分の出席状況や成績を確認するための出席管理システムの概要である。ここで使用するサーバはレンタルサーバ業者が提供している最も安価な VPS である。また、データベースには、各学生の DSQR コードと出席データが格納されている。

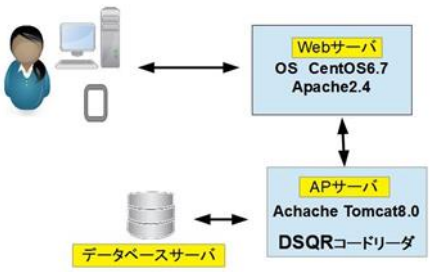


図３　出席管理システムの概要

図４は上記システムのログイン画面である。最初に、学生はログイン画面の「QR コードの取得（学生)」をクリックして自分の DSQR コードをダウンロードしておく。この DSQR コードは出席登録や出席確認の際に使用する。また、教員は「出席情報更新（教員)」をクリックして出席データが記録された Excel ファイルを適時サーバにアップロードしておく。学生が自分の出席状況や成績を確認するときは、以下の手順に従う。なお、このとき、学生/サーバ間で実質的な相互認証が同時に行われている。

❶「出席確認（学生)」をクリックする。
❷自分の DSQR コードを送信する。
❸DSQR コードが真正判定のとき SW が返される。SW が正しいことを確認して PW を送信する。
❹PW が正しいとき、科目名の入力画面になる。
　その後、出席状況と成績が表示される。

ここで特筆すべきことは、個人の ID/PW はデータベースに保管されていること、更に DSQR コードという画像を介して ID/PW を確認するログイン方式を採用していることである。このシステム形態は SQL インジェクションを含む情報漏洩などに対して原理的な耐性がある。今回の運用においても出席管理システムには不正を試みるアクセスが毎日多数あるが、何の問題もなく稼働している。そのためシステム監視の必要性を感じていない。また、本システムは学内ネットワークとは独立しているため、教員サイドに立った自由度の高いシステム設計を可能にする。

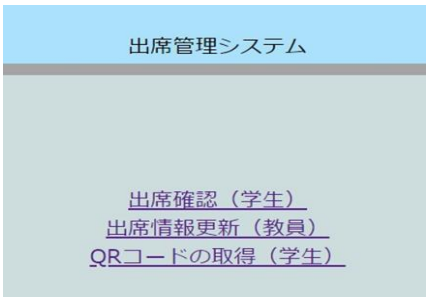


図４　出席管理システムのログイン画面

## ５．おわりに

シンプルな構成でかつ安全性の高い出席管理システムを構築し、講義で実践した。その結果、教員のデータ集計の負担軽減及び学生の出席・成績確認に大きな効果があった。

参考文献

1. https://gakumado.mynavi.jp/gmd/articles/50421
2. 先名健一 : 個人認証機能を有するデジタル署名型 QR コード、信学技報、EMM2017-11、pp.61-66、2017.