コンピュータセキュリティ 13－2
（２００１．５．２５）

二次元コードによる学生証のセキュリティ向上

小林 哲二　　増田 貴浩　　大川 貴史

日本工業大学

〒345-8501 埼玉県宮代町学園台 4-1-1 情報棟

あらまし　二次元コードは，バーコードを二次元に拡張したものであり，記録容量が大きく，誤り訂正機能もある．二次元コードは，近い将来，商品管理，身分証明書などの多くの分野に使用される可能性がある．二次元コードの応用として，大学における学生の身分証明書である学生証に二次元コードの Aztec Code を適用することを検討する．個人の文字情報と顔画像を二次元コードに格納して，二次元コード付き学生証を作成する方法，本人確認に利用する方法，及びセキュリティの問題点の解決方法についての考察を示す．

キーワード：　二次元コード，Aztec Code，学生証，本人確認，セキュリティ

Security Improvements for a Student Identification Card System using Two-dimensional Symbols

Tetsuji KOBAYASHI　Takahiro MASUDA　Takafumi OKAWA

Nippon Institute of Technology

4-1-1 , (Joho-Building), Gakuendai, Miyashiro-machi, Saitama-ken, 345-8501 Japan

Abstract　In recent years, two-dimensional symbols have appeared by extending the function of barcodes. Two-dimensional symbols have characteristics such as large recording capacity and error correction capability. Two-dimensional symbols will be used in many applications such that merchandize managements, identification systems, etc., in the near future. This paper investigates a student identification card system using Aztec Code for a two-dimensional symbol. A prototype system that uses two-dimensional symbols encoding both personal information and a facial photograph is described. Security improvements for the system are investigated.

Key words：　two-dimensional symbol,　Aztec Code,　student identification card,　personal identification,　security

1．まえがき

二次元コード(two-dimensional symbol)は，バーコードを二次元に拡張したものであり，二次元バーコードと呼ばれることもある[1],[2],[3].二次元コードは，バーコードと同様に，印刷可能なもの（紙，プラスチック等）に記録可能である．例えば，商品の詳細なデータを二次元コードに記録し，ラベルなどに印刷して商品に付加できる．二次元コードの生成はソフト（又はハード）によるエンコード（データを二次元コードに変換）とプリンタ印刷で行い，読取りとデコード（二次元コードをデータに変換）は，二次元コードスキャナによって行う．二次元コードは，バーコードに比べて記録密度が大きいために，印刷面に汚れや傷が生じると，誤って解読される可能性が大きくなるので，高機能な誤り訂正符号を二次元コードのアルゴリズムに組込むことによって，利用者が指定する度合いの誤り訂正を行えるようになっている．

二次元コードスキャナは，バーコードと二次元コードの兼用であることが多い．二次元コードは，比較的新しい技術のため，現在はバーコードほどには多く用いられていないが，近い将来，商品管理，身分証明書などの多くの分野に使用されてゆく可能性がある．この論文では，大学における学生の身分証明書である学生証に，二次元コードの Aztec Code を適用するときのセキュリティ向上について，従来の著者の研究（[9]～[13]）を元にして検討する．

2．バーコードと二次元コード

2．1 二次元コードの必要性

バーコードの問題点は，①1つのバーコードの情報量は最大でも数 10 文字であるので，格納するデータ量を増加したり，データ量が大きい画像をバーコードに記録したりすることが困難であること，及び②バーコードには，誤り検出機能はあっても誤り訂正機能がないため，バーコードに傷や汚れがあると，バーコードスキャナで読取りできないことが発生することである．二次元コードでは，これらの問題点が解決されている．二次元コードは，バーコードを縦に多重に積み上げた形状のスタック型二次元コード（例：PDF417）と，画像の画素に相当する位置に黒か白のパターンを格納してゆくマトリックス型二次元コード（例：QR Code，Aztec Code）に分類でき，それぞれの分類について，色々な種類の二次元コードがある．

2．2 二次元コードの比較と選択

一般的に，学生証の余白は少ないので，二次元コードは，記録密度が大きい必要がある．学生証の使用は過酷であることが多いので，誤り訂正能力が大きい必要がある．代表的な二次元コードである PDF417, QR Code，Aztec Code を比較する．

PDF417：スタック型である．最大で，英数字を 1850 字，数字を 2710 字，又はバイナリデータを 1108 バイトまで格納できる．

QR Code：マトリクス型である．最も高容量のモデル2では，最大で英数字を 4296 字，数字を 7089 字，又はバイナリデータを 2953 バイトまで格納できる．

Aztec Code：マトリクス型である．最大で，英字を 3067 字，数字を 3832 字，又はバイナリデータを 1914 バイトまで格納できる．

いずれの二次元コードも Reed-Solomon 符号を用いた誤り訂正機能を有している．任意のデータ容量に対する二次元コードの印刷面積は，Aztec Code が最も小さい．

文字および顔画像を二次元コードにして学生証に格納する場合，①二次元コードに格納する文字情報の選定，②二次元コードに格納する顔画像の形式，並びに③二次元コード付き学生証の利用方法と特徴，について明確化する必要がある．

二次元コードのない通常の学生証の一例では，有効領域が縦 58mm，横 89mm であり，余白は少ないため，学生証の顔画像を二次元コードにするには，学生証の書式を変更して余白を作り，更には，記録密度が大きい二次元コードを用いる必要がある．また，その場合でも，正方形の二次元コードとして記録できる余白は，縦横共に最大で約 3 cm である．これらの条件に対応するため，本研究では，比較的最近（1995 年）に発表され，従来の二次元コードに対して発生した不具合への改良がなされている二次元コードであると言われている Aztec Code を用いる．なお，他の二次元コードも原理的には適用可能である．Aztec Code は，AIM International によって，1997 年に標準化されている二次元コードである．Aztec Code は，印刷された状態では，二値画像であり，画素はモジュールと呼ばれ，黒画素がビットの1，白画素がビットの0を表す．二値画像は，ファインダパターン（中央の黒画素およびその周りを同心状に囲む正方形の白画素群と正方形の黒画素群），ファインダパターンに密着したオリエンテーションパターンとモードメッセージ，及びそれらの外側にあるデータレイヤで構成する．ファインダパターンとオリエンテーションパターンは，デコード

時の位置決め等に用いられる．モードメッセージにはデータレイヤ数，データレイヤ内のデータワード数，それらの誤り訂正チェックワードが格納される．データレイヤには，メッセージのデータとそれらの誤り訂正チェックワードが格納される．

3．二次元コード付き学生証の作成方法

学生証の作成手順の概要を図1に示す．まず，学生証のための個人の文字情報（テキストデータ）および顔画像（バイナリデータ）を二次元コードにする．次に，データベース管理ソフトなどを用いて，試作した学生証作成ソフトにより，学生証のデータを編集し，学生証を印刷して，二次元コード付き学生証が完成する．なお，バイナリデータはテキストデータに変換（例えば文献［7］にあるBASE64方式等を利用）してから二次元コードにエンコードしているが，この試作以外の場合として，直接にバイナリデータを二次元コードにエンコードすることも考えられる．

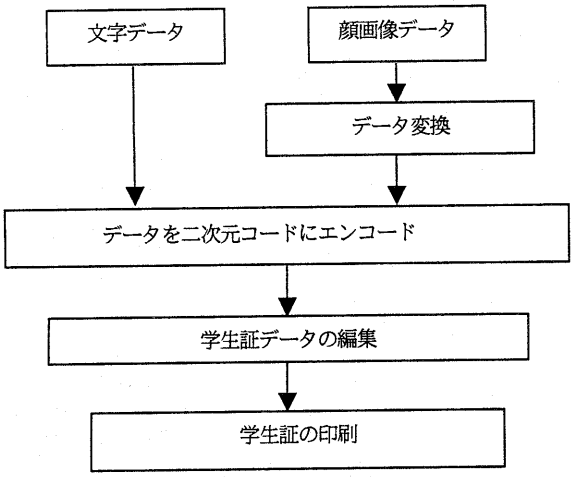

図1　二次元コード付き学生証の作成手順

学生証のサイズは，銀行や郵便局のキャッシュカードなどに類似したサイズ（約83mm×54mm）に設定している．学生証のデータ量は，個人情報の文字データや顔画像データの容量に依存する．試作したシステムでは，文字データの二次元コードの大きさは約10mm×10mm，顔画像データの二次元コードの大きさは約21mm×21mmである．図2は二次元コード付き学生証の例である．学生証は，ディスプレイ画面に表示されているのと同じ状態で印刷できる．図2における文字，顔写真，及びその他の印刷情報は，この論文のための架空のデータである．試作システムでは，顔画像に使用できる二次元コードの容量をできるだけ大きくするために，文字データと顔画像を，個別の二次元コードにしている．しかし，1つの二次元コードに格納することも原理的には可能である．操作性向上のためには，文字データと顔画像の二次元コードを1つに統合することが好ましい．

図2　二次元コード付き学生証の例

4．二次元コード付き学生証による本人確認

二次元コード付きの学生証を用いて，本人確認を行なう方法と考察を述べる．

4．1　学生証による本人確認手順

二次元コード付き学生証による本人確認システムは，二次元コードスキャナが接続されたコンピュータであり，コンピュータには，本人確認用の試作ソフトを起動しておく．本人確認手順を次に示す．

［ステップ1］：学生証に印刷してある二次元コードを二次元コードスキャナで読取る．

［ステップ2］：二次元コードスキャナから読取った情報の内，個人の文字データはそのままコンピュータの表示にそのまま利用できるが，顔画像データもテキスト形式になっているので，テキスト・バイナリ変換ソフトを用いて顔画像のテキストデータをバイナリデータに変換して，バイナリデータの顔画像にする．

［ステップ3］：本人確認機能を用いてディスプレイに表示して，次のように本人確認を行う．検査者は，学生証の提示者の顔，学生証の顔写真，及び学生証の二次元コードから得られる顔画像と文字データを用いて，本人であるかどうかの判定を実施する．検査者のチェック事項は後述する．　　（手順終）

本人確認手順の概要を図3に示す．

本人確認のセキュリティ向上のための検査者による検査事項を表1に示す．表1は，表の各行ごとに検査目的に従って検査者の検査の有無を表している．表1の説明を以下に示す．

（1）　学生証に対する通常のチェック

これは，二次元コードのない学生証でも，一般的に行われる通常のチェックである．①実際の顔と学生証の顔写真との照合チェック，及び②実際の人物と学生証の文字情報との照合チェックを行う．

（2）　学生証の偽造に対するチェック

これは，二次元コード付きの学生証の偽造検出のために行うチェックである．学生証とディスプレイ画面の両方を見て行う．①学生証の顔写真と学生証の二次元コードから取得して表示した顔画像との照合チェック，及び②学生証に印刷された文字情報と，学生証の二次元コードから取得して表示した文字情報との照合チェックを行う．なお，これらのチェック（表1では，括弧付きの（有））は，二次元コードに格納したデータをデータベースに登録しておいて，二次元コードから読込んだデータと直接に照合する機能をシステムに追加することによって，不要にできる（後述する）．

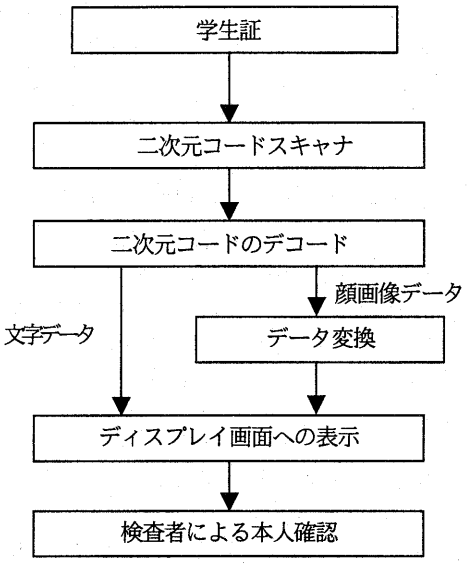

図3　本人確認手順の概要

表1　検査者による検査事項

検査事項／検査目的	実際の顔と学生証の顔写真の照合	実際の人物と学生証の文字情報の照合	学生証の顔写真と学生証の二次元コードから得た顔画像の照合	学生証の文字情報と学生証の二次元コードから得た文字情報の照合
通常の検査	有	有	無	無
顔写真の偽造検出	無	無	(有)	無
文字データの偽造検出	無	無	無	(有)
二次元コードの偽造検出	無	無	(有)	(有)

4．2　本人確認についての考察

(1) 適用効果：　二次元コード付き学生証を使用することにより，学生証の偽造と記載事項の改ざんに対処できる．

(2) 運用形態：　試作システムでは，1台の本人確認用コンピュータを単独で運用する場合だけに限定している．拡張として，1台のサーバと1台以上の本人確認用クライアントを接続する構成が考えられる．

(3) 検査者の負担軽減：　検査者の目視チェックを軽減する将来的方法として，顔認識技術と組み合わせて検査事項の顔の照合に関する項目を自動化することが考えられる．

5．二次元コード付き学生証のセキュリティ向上

不正者が，不正者本人の顔写真に対して二次元コードを作成するためには，学生証の作成システムを偽造または不正使用する必要があるから，二次元コードの付かない学生証よりも二次元コード付き学生証は偽造の困難性が大きい．一般に，身分証明書においては，顔写真のすり替えを防ぐために物理的に写真に割印を行うことが多いが，二次元コードに割印を直接行っても，二次元コードのデコード時のノイズになるだけであるので，無意味である．学生証の情報である個人の文字情報，顔写真，二次元コード及び学生証記録媒体（用紙等）を，すべて偽造されると，前述した本人確認機能をすり抜けられてしまう．

このような高レベルの偽造学生証への対策と考察を述べる．なお，この検討は，学生証が重要な用途にも用いられることを考慮すると，意義がある．

（1）対策案と考察

【方式1（コンピュータに元の情報を保持する提案方式）】：学生証の二次元コードに格納した元のデータ（文字データおよび顔画像）を，本人確認を行うコンピュータ又はサーバのデータベースに保持する．学生証を提示された時に，二次元コードから得た学生証のデータと，元のデータとの一致性をチェックする．元のデータの代わりに，そのデータをファイルのハッシュ関数などで短縮した値によって一致性をチェックしてもよい．

[方式1の考察]：この方式は実現が容易であり，かつ，本人確認のチェックを自動化できる効果がある。1人の学生証の全情報のデータ量をM，学生数をNとすると，本人確認を行う1つのコンピュータで保持するデータ量は，M・Nである．従って，学生数が多い場合は，本人確認を行うコンピュータで保持するデータ量が大きくなる．クライアント・サーバの構成の場合に，サーバだけに学生証のデータを集中して保持する場合は，クライアントへの必要情報を必要時にダウンロードすればよい．一致性のチェックは，ファイルのハッシュ関数などを用いて短縮値により行った方が，照合処理時間を短縮できる。

【方式2（共通鍵暗号による暗号化方式）】：二次元コードにするデータは，暗号化してから[8]，二次元コードにして印刷する．印刷された二次元コードを二次元コードスキャナで読取った直後に復号化する．

[方式2の考察]：共通鍵を不正者が取得した場合および不正者が暗号解読を完了した場合を共に除いて，学生証の偽造はできない．共通鍵は，本人確認を行うコンピュータに秘密に保持する．

【方式3（公開鍵暗号による暗号化方式）】：二次元コードにするデータは，公開鍵暗号の公開鍵で暗号化してから二次元コードにし，その二次元コードを二次元コードスキャナで読取った直後に公開鍵暗号の秘密鍵により復号化する．秘密鍵は，本人確認を行うコンピュータに秘密に保存する．

[方式3の考察]：秘密鍵を不正者が取得した場合および不正者が暗号解読を完成した場合を共に除いて，学生証の偽造はできない．

【方式4（メッセージ認証方式）】：共通鍵暗号により，二次元コードにする前に元のデータのメッセージ認証子を作成しておき，元のデータとメッセージ認証子を共に二次元コードにする．二次元コードをデコードした後で，データ中のメッセージ認証子の正当性を検証する．メッセージ認証子を作成するための暗号鍵は，本人確認を行うコンピュータに秘密に保存する．

[方式4の考察]：　メッセージ認証のための暗号鍵を不正者が取得した場合または不正者が暗号解読をした場合を共に除いて，学生証の偽造はできない．メッセージ認証子のためのデータ量の増加がある．

【方式5（ディジタル署名方式）】：公開鍵方式を用いて，二次元コードにする前に元のデータのディジタル署名を作成しておき，元のデータとディジタル署名を共に二次元コードにする．二次元コードをデコードしたときには，データの中にあるディジタル署名の正当性を検証する．本人確認を行うコンピュータにはディジタル署名検証のための公開鍵だけを保存する．

[方式5の考察]：ディジタル署名生成のための秘密鍵を不正者が取得した場合または不正者がディジタル署名アルゴリズムを暗号解読した場合を除いて，学生証の偽造はできない．秘密鍵は，本人確認を行うコンピュータとは別の場所に保管しておけばよいので，方式2，方式3，および方式4よりも鍵管理が安全である．

ディジタル署名データのためのデータ量の増加がある．

【方式６（顔画像に電子透かしのデータを埋込む方式）】：顔画像を二次元コードにする前に，顔画像に電子透かしのデータを埋込んでおく．本人確認を行うときに，顔画像に埋込まれたデータの正当性をチェックする．

[方式６の考察]：顔画像にディジタル署名を付加することと機能的には同じである．ディジタル署名に比べて，二次元コードのデータ量が増加しないという長所がある．安全性は，電子透かしのアルゴリズムにも依存する．

上述のどの方式も本人確認ソフトに組み込めば自動的に行えるので，検査者への影響はない．以上の考察から，実現の容易性では方式１の元のデータを保持する方式がよい．状況に応じて他の方式も用いるとよい．

（２）　その他のセキュリティ技術

二次元コードの記憶媒体としての特徴は，①紙，プラスチック，金属などの印刷可能な媒体であればよい，②印刷面積が記録量に比べて小さい，及び③二次元コードを見たり，コンピュータに読込んだりしても，デコードしなければ意味不明であることである．二次元コードのセキュリティ関連技術として，例えば，複数の二次元コードに認証データや暗号鍵を分散して格納し，読み出し順序を所有者だけの秘密にする方法（國米の文献[6]）が提案されているが，多数の二次元コードを印刷する必要があるために，学生証では余白が少ないので使用できない。この他に，二次元コードのアルゴリズムに，暗号／認証／電子透かしのアルゴリズムを融合させること，印刷の工夫等が考えられるが，多様な研究が必要であるので，本稿の対象外である．

６．むすび

二次元コードのAztec Codeを学生証に適用することを検討して次の結果を得た．これらの結果は，他者の二次元コード関係の文献（例えば[1]～[6]）では記述されていない。

（１）　個人の文字情報と顔画像を二次元コードのAztec Codeにすることによって，二次元コード付き学生証を作成するための機能を，データベース管理システムなどを有効利用して実現する方法を考察し,実現例を具体的に示した．

二次元コード付き学生証は，学生証の機能拡充を低コストで行うのに有効であるが，二次元コードスキャナのコスト低下が普及に重要な要素である．また，バーコードの機能は二次元コードで包含でき，ＩＣカードは二次元コードと併用も可能である．

（２）　学生証の所有者の本人確認のセキュリティ向上のために，学生証に印刷してある二次元コードを二次元コードスキャナで読取り，その内容をディスプレィに表示して，本人確認を行う機能を考察した．本人確認のために，コンピュータに元の情報を保持して二次元コードから得た情報と照合する方式によって，検査者の負担を少なくできることを示した．更に，この方式は，二次元コード付き学生証の偽造に対するセキュリティ向上にも効果があることを示した．

参考文献

[1] International Symbology Specification － Aztec Code，AIM International，Dec. 1997.

[2] 平本純也：“知っておきたいバーコード・二次元コードの知識”，日本工業出版，Feb. 1999.

[3] 黒沢康雄：“二次元コードの特徴と種類”，月刊バーコード８月増刊号，日本工業出版,pp.77-85, Aug. 1999.

[4] 井籐 久男：“顔写真検証システム”，特許公開平11－198573，公開日July 27，1999.

[5] 丸橋光夫ほか：“ＩＤカード及び個人認証システム及びその方法”，特許公開平6-155971，公開日June 3，1994.

[6] 國米 仁：“記憶照合による個人認証手法（囮混在秘匿方法）”，コンピュータセキュリティシンポジウム 2000論文集，pp.213-218，情報処理学会，Oct. 2000.

[7] 笠野英松（監修）：“インターネットＲＦＣ事典”，pp.241-245（BASE64），アスキー，May 1999.

[8] B. Schneier: “ Applied Cryptography”, second edition, John Wiley & Sons, Inc., 1996.

[9] 小林哲二：“二次元バーコード応用のセキュリティ”，1998 年暗号と情報セキュリティシンポジウム予稿集，9.3.A，pp.1-8，Jan. 1998.

[10] 小林哲二：“証紙類の部分的電子化とセキュリティ”1999 年暗号と情報セキュリティシンポジウム予稿集，W4-3.8，pp.395-400，Jan. 1999.

[11] 増田貴浩，北澤考紀，並木正次，小林哲二：“二次元コードを用いた学生証と誤り訂正特性”，1999年信学会情報・システムソサイエティ大会,講演論文集, D9-3, p.71, Sept. 1999.

[12] 増田貴浩，高橋 徹，長竹 孝文，神 憲祐，大川 貴史，小林 哲二：“二次元コードによる学生証と本人確認”，信学技法，OFS99-72，pp.35-40，Mar. 2000.

[13] 大川貴史，増田貴浩，小林哲二：“二次元コードとＩＣカードの学生証への適用”，信学会，情報・システムソサイエティ大会,講演論文集,D-9-3,p.96，Sept. 2000.