九州大学学術情報リポジトリ
Kyushu University Institutional Repository

QRコードと互換性を持つ二次元コードの大容量化と秘匿化に関する研究

寺浦, 信之

https://doi.org/10.15017/1866317

出版情報：九州大学, 2017, 博士（工学）, 課程博士
バージョン：
権利関係：

QR コードと互換性を持つ二次元コードの大容量化と秘匿化に関する研究

九州大学システム情報科学府

情報学専攻

寺浦　信之

平成 29 年 07 月

目次

本論文の概要

従前のバーコードを拡張した二次元コードは，1980 年代後半から 90 年代前半に開発され，今日ではさまざまな用途で使用されている．開発された二次元コードの中で，複数の二次元コードが国際標準となっている．その中で，代表的な二次元コードは QR コードである．QR コードは，従来産業用途に限定して使用されていたが，現在では，スマートフォンで読み取り，WEB 参照を行う主要な手段となっている．そして，情報システムの多様化や通信ネットワークの高速化による IoT 用途に向けて，大容量化と秘匿化の要求がある．大容量化では，文字情報だけでなく，音声や画像情報の収容がある．秘匿化では，特別なユーザにのみデータの読み取りを許し，他者にはデータを秘匿する情報提供の用途も存在する．例えば，産業用途ではコストや品質情報，医療用途での個人情報などである．

大容量化の手法として，二次元コードを構成する基本単位であるセルについて，従来の二次元コードにおける白黒の 2 色による 1 セル 1 ビットに対して，セルの多色化（いわゆるカラー二次元コード）による多ビット化が提案されている．多色化は，複数の色を用いてセルを符号化する手法である．2^n 色を用いる場合には，1 セル当たり n ビットを表現することが可能となり，多くの研究事例がある．これらの研究はセルに用いる色数を増大させ，主に多くの色を識別する手法の検討となっていた．しかし，多色化によって，白黒の既存の二次元コードとして識別した場合には，正しい白黒の二次元コードにはならず，互換性は失われる結果となっていた．

秘匿化の手法として，既存の二次元コードの記憶領域を 2 分割し，通常の領域の終端の背後に秘匿する暗号化データを配置する提案がある．この提案では，通常の領域を読み取る互換性があるが，二次元コードの領域を分割するため，通常の領域が減少する．そして，秘匿領域が単一であるため一人しかアクセスできず、複数領域への分割の実現が課題であった．

本論文の第 1 の課題は，既存の二次元コードと互換性を維持しながら，セルを多値化し，記憶するデータの大容量化を行うことである．セルの多値化の手法として，多色化と多領域化を採用した．多領域化は，セルを複数の領域に分割し，分割された領域を独立して符号化する手法である．第 2 の課題は，増加した記憶領域のデータを秘匿することである．第 3 の課題は，複数のユーザが複数の領域の二次元コードを読み取るに際して，アクセス制御を行い，特定の

ユーザにのみ情報提供を可能にすることである．

本論文は，二次元コードを構成する基本単位であるセルを，既存の二次元コードと互換性を維持しながら多色化と多領域化の手法を用いて多値化し，大容量化を図り，既存の二次元コードから増加した記憶領域をランダムマスク法によって秘匿する手法を提案し，さらに記憶領域を複数の領域に分割し複数のユーザのアクセス制御をする手法について検討を行ったものであり，6 章から構成される．

第 1 章は序論であり，本論文の背景と主要な研究課題について述べる．

第 2 章では，既存の二次元コードについて，その種類や識別手法について述べた．本論文で提案する手法は，マトリックス型の二次元コードすべてに適用可能であるが，QR コードを互換性維持の対象としたことを述べる．

第 3 章では，QR コードと互換性を維持しながら，多色化と多領域化の手法を併用し，大容量化を実現するセル構造を提案する．セルを 9 個の正方形のサブセルに分割し，互換性を維持する為に，中央のサブセルを白黒で符号化する．さらに，大容量化の為に，周辺部のサブセルをカラー8 色により符号化する．本論文で提案する二次元コードについて互換性確認試験及び識別性確認試験をした結果について述べる．

第 4 章では，QR コードと互換性を維持する領域は公開領域とし，増加した領域のみを秘匿領域とする手法について述べる．本論文で提案する大容量化方式では，仮想の白黒の二次元コードを重層していると見なすことができる．QR コードは誤り訂正を目的として，リードソロモン符号を用いている．リードソロモン符号では，誤り訂正能力を超えた誤りがある場合には復号できない特性を用いて秘匿化を行う．この仮想の QR コード（秘匿領域）の各セルに対して，乱数（秘密鍵）を XOR 演算することにより，リードソロモン符号の全データコード語に誤りを与え，正しいデータコード語への復号や推定を不可能とする秘匿化を行うことを述べる．

第 5 章では，二次元コードの記憶領域を多領域に分割し，複数のユーザのアクセス制御を行う提案手法を述べる．二次元コードを複数の領域に分割し，分割した領域を秘密鍵による秘匿化を行う．また，複数のユーザにそれらの領域のアクセス権を付与する．付与された領域の秘密鍵をユーザ毎に設定されるパスワードによってさらに秘匿化する．ユーザは自らのパスワードによってアクセスの許された領域の秘密鍵を入手し，領域にアクセスする．これらの手法に

より，複数ユーザのアクセス制御の課題を解決できたことを述べる．

第 6 章では，本論文の結論を述べ，今後の研究課題を示す．

本論文の概要（英語）

A Study on the High Capacity and Confidentiality of Two-Dimensional Codes Compatible with QR Code

Abstract:

Two-dimensional codes that extended the existing barcode were developed from the second half of the 1980s to the first half of the 1990s, and are currently used for various applications. Among the two-dimensional codes developed, several have become international standards. A typical two-dimensional code is the QR code. Although the QR code was previously used primarily for industrial applications, it has developed into the primary means of making a web reference readable by smartphone. Due to the diversification of information systems and high-speed communication networks, there is a demand for high capacity and confidentiality in IoT applications. With high capacity, in addition to character information, sound and image information can also be accommodated. In confidentiality, information can be provided in such a way that allows data to be read only by a specified user and to be hidden from others. Some cases where this is important include cost and quality information in industrial applications and personal information in medical applications.

As a method of increasing cell capacity, where the cell is a basic unit constituting a two-dimensional code, multicolor cells (so-called two-dimensional color code) have been proposed as a multi-bit configuration to replace conventional two-dimensional code, which uses one-bit cells with two colors, black and white. Polychromatization is a method of encoding cells using multiple colors. When 2^n colors are used, it is possible to express n bits per cell. There are many research cases on this subject. These studies have increased the number of colors used in a cell, focusing primarily on methods to identify additional colors. However, due to multicolorization, when a QR code is identified as an existing two-dimensional black and white code, it may be interpreted incorrectly, thus losing compatibility.

As a method of concealment, there is a proposal to divide the storage area of an existing two-dimensional code in two areas and arrange encrypted data to be kept secret behind the end of the normal area. In this proposal, there is compatibility to read the normal area. Because the area of the

two-dimensional code is divided, the usable area decreases. Due to there being only one confidential area, it is impossible to divide the area for access control of the confidential area.

This study focuses on three subject areas. The first is to create multi-valued cells while maintaining compatibility with existing two-dimensional codes and to increase the data storage capacity. As a method of creating multi-valued cells, multicolorization and multi-regionalization are adopted. Multi-regionalization is a method of dividing a cell into a plurality of regions and independently coding the divided regions. The second subject is to conceal the data located in the newly created storage areas. The third subject is to perform access control when a plurality of users read two-dimensional codes from a plurality of regions, while providing information only to a specific user.

In this study, a cell is multivalued by using a multicolorization and multi-regionalization method while maintaining compatibility with the existing two-dimensional code to increase its capacity. We propose to conceal the storage area increased from the existing two-dimensional code by using the mask pattern method. We also examine a method of dividing the storage area into a plurality of areas and performing access control on a plurality of users.

This thesis consists of the following six chapters.

Chapter 1 is an introduction and describes the background of this thesis and main research subjects.

In Chapter 2, we describe the existing two-dimensional code type and identification method. Although the method proposed in this thesis is applicable to all matrix type two-dimensional code, we describe that QR code is targeted for maintaining compatibility.

In Chapter 3, while maintaining compatibility with the QR code, we propose a cell structure that achieves high capacity by combining multicolorization and multilevelization techniques. The cell is divided into nine square subcells and the center subcell is encoded in black and white in order to maintain compatibility. Furthermore, in order to increase the capacity, the subcells in the peripheral portion are encoded using eight colors. The results of the compatibility check and discrimination confirmation tests on the two-dimensional code proposed in this study are described.

In Chapter 4, we describe a method of maintaining compatibility with QR

code as an open area and setting only increased areas as concealed. In the capacity enlarging method proposed in this study, it can be regarded as overlaying a virtual black and white two-dimensional code. The QR code uses a Reed-Solomon code for the purpose of error correction. For Reed-Solomon codes, concealment is performed using a property that cannot be decoded when there is an error that exceeds the error correction capability. An XOR operation is performed on a random number (secret key) for each cell of this virtual QR code (confidential area), thereby giving an error to all data code words of the Reed-Solomon code. We describe how to conceal and decrypt this code to make it impossible to decode and estimate correct data code words.

In Chapter 5, we describe a proposed method of dividing the two-dimensional code storage area into multiple areas and controlling multiple user access. The two-dimensional code is divided into a plurality of regions, and the divided regions are concealed with a secret key, where access rights to these areas may be granted to multiple users. The secret key for the granted area is further concealed by a password set for each user. The user obtains the area's secret key and accesses the area using his/her password. We describe that these techniques were able to solve the problem of multiple user access control.

In Chapter 6, we present the conclusions of this study and future research subjects.

本論文で用いる省略語などの説明

(1) QR コード

Quick Response コードを意味する二次元コードの名称である．日本のメーカが開発した二次元コードであり，日本，アジアを中心に普及しており，WEB アクセスの用途では，世界的に使用されている．

(2) SQRC

Security Quick Response Code の省略語であり，QR コードを開発したメーカが，QR コードを拡張して，QR コードにセキュリティ領域を追加した二次元コードの名称である．

(3) ID

IDentifier の省略語であり，識別子である．データの本体を記憶容量の大きな媒体に収容し，バーコードのような記憶容量の小さな媒体には ID のみを収容して，大きな媒体のデータ本体に ID を基にアクセス可能とする．

(4) RS 符号

Reed-Solomon 符号を意味する誤り訂正符号の名称である．QR コードの誤り訂正に用いられている誤り訂正符号である．

(5) ISO/IEC

ISO （ International Organization for Standardization）と IEC（International Electric Committee）が共同して作成した国際技術標準である．情報分野では標準作成のため JTC1（Joint Technical Committee 1）が設立され，二次元コード等に関する標準を作成している．

(6) RGB

色の表現法の１種であり，Red（赤），Green（緑），Blue（青）の三つの原色を用いて色を表現する加法混合の表現手法である．RGB は前記の色の頭文字である．

(7) POS システム

Point of Sales システムを意味するシステムの名称である．販売時点管理システムと呼ばれる．商品に貼付されているバーコード（JAN シンボル）に記憶されている商品番号を読み取って，販売価格に変換して販売する．現在，何か売れているのをリアルタイムに把握することができる．

第 1 章　序論

1.1　研究の背景

1.1.1　二次元コードの開発

二次元コードの第 1 号は，1982 年に開発されたベリコード[64] である．その後，続々と新たな二次元コードが開発されている．二次元コードの開発の目的は，大容量の光学的情報媒体の実現である．二次元コードに先立って，最初のバーコード（コード 2 オブ 5） [65]が 1970 年に開発され，その後幾つかのバーコードが開発されて，1970 年台後半には普及が進んでいた．しかし，バーコードは収容できるデータ量が多くても数十バイトに限定されており，収容するデータはデータの ID に限定され，データ本体は別途の大容量記憶媒体に収容されて,バーコードから読み取った ID からデータを参照するシステムとなっていた．

しかし，それではシステムが複雑となり，ソフトウェアの構成も複雑となるので，光学的情報媒体にデータ本体を収容するニーズが生まれ，それに対応するために二次元コードが開発された．二次元コードが開発されたのは，1980 年代から 1990 年代前半である．日本で開発された QR コードは 1994 年に発表されている．表 1-1 に代表的なバーコードと二次元コードの種類[64] [65]とその開発時期を示す．これらの形状等について第 2 章にて述べる．これらの二次元コードは，当時の技術で印刷し，撮像し，識別できる仕様となっている．現在では，1990 年代前半から既に 20 年以上の時間が経過し，二次元コードに関係する技術は格段の進歩を遂げている．

表 1-1　代表的なバーコードと二次元コードの種類とその開発時期

バーコード	二次元コード
1970年　CODE 2of 5　開発 1971年　JANシンボル開発 1972年　NW7開発 1974年　CODE39開発	1982年　ベリコード（マトリックス） 1987年　CODE49（スタック） 1987年　データマトリックス（マトリックス） 1989年　PDF417（スタック） 1994年　QRコード（マトリックス）

1.1.2　新しいニーズ

(1) 大容量化

新しいニーズの第一は，大容量化である．二次元コードでは，図 1-1 に示すように，セル数を多くすることにより，より多くのデータを収容可能である．ここでの大容量化は，二次元コードの同じ面積当たりの大容量化，すなわち高密度化である．

20 数字収容　　100 数字収容

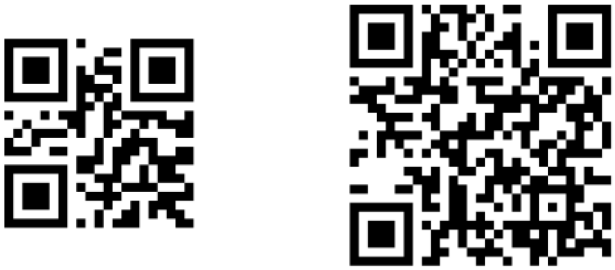


図 1-1　セル増加による大容量化

先に述べたように，データキャリアとしての二次元コードは，大きな容量のデータを収容できる必要がある．現在，データの受け渡しには，CD/DVD/USB メモリーなどが用いられている．これらには，数 GB という膨大なデータ量を収容可能である．これらが二次元コードで置き換えることが可能になれば，より安価にデータの受け渡しが可能となる．しかし，当面，数 GB や数 MB といった大きなデータ容量は実現し得ないが，より大きな記憶容量を実現することにより，用途の拡大が可能となる．その例として，音楽データや画像データがある．二次元コードに画像データを記憶させた例としては，パスポートへ顔写真画像を収容した例がある．この例では，8cm 四方程度の大きな白黒二次元コードが用いられていたが，高密度化を図ることでこれを小さくすることが可能になる．

本論文の主要な課題は，この大容量化，高密度化である．

(2) 秘匿化

また，二次元コードは当初から業務上での利用を前提としており，誰でも読み取り可能であることを当然としていた．しかし，二次元コードを読み取り可能なスマートフォンの普及によって，業務上の利用だけでなく，一般消費者の利用も普及してきている．これらの業務上及び一般消費者の利用において，誰でもが読み取り可能な利用の形態の他に，特別なユーザのみが読み取り可能で

ある利用形態のニーズが生まれて来ている．

(3) データ開示

新しいニーズの方向性の一つは，データ内容の開示である．二次元コードが携帯電話やスマートフォンで読み取り可能となり，一般消費者が自分の意志に基づいて読み取る機会が生まれてきている．その場合に，必要とされるのが読み取り対象のデータ内容の事前認知である．すなわち，読み取り対象にどのようなデータが格納されているのかを，事前に把握することである．

この目的のために，二次元コードのシンボル画像に視認可能な画像を重層し，重層した画像を目で視て，二次元コードの内容を開示する試みがなされている．これらの事例を図 1−2 に示す．

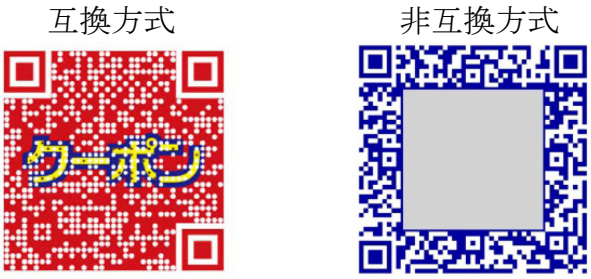


図 1-2　データ開示の事例

二次元コードに画像を重層させる方式としては，次の二つの方式がある．

①互換方式

②非互換方式

互換方式では，QR コードなど広く普及している二次元コードのシンボル画像に画像を重層させ，通常の読み取りソフトウェアで読み取らせる．この場合，セルと画像が重なっているため，通常の手順で作成した二次元コードの白セルが黒となったり，黒セルが白になる場合がある．このようなセルデータの破損になる場合には，セル色の読み取りエラーになるが，誤り訂正の範囲内の誤り率であれば，読み取り可能である．また，重層する画像に合わせてセル色を配置するなどの研究がなされている．

それに対して，非互換方式では，予め画像を重層させる領域を設定し，その領域にはデータを収容するセルを配置しない．このため，データ読み取りにはこれらに対応した特別なソフトウェアが必要となる．

（4）安全の確保

現在，スマートフォンなどで，WEB にアクセスするための URL 入力の手段として，二次元コードが多く用いられている．この仕組みを用いて不正なサーバに誘導することが行われており，二次元コードを用いた安全な WEB 誘導システムが必要とされてきている．

1.2　関連する研究

1.2.1 大容量化

収容データの大容量化を目的とし，セルを多値化する為の手段として多色化があり，多くの色の識別を目指す研究[9]-[36]がなされている．[10] [16]は色の識別手法として識別対象となる標準色をコード内に保持し，識別対象と標準色を比較することで識別を行っている．[15] [17]は，退色後の色空間で相互距離の最大化などを行い，識別対象間の比較で色を識別している．

表 1-2 に大容量化を目的とする多色化の研究事例を示す．

表 1-2　大容量化を目的とする多色化の研究事例

主研究者	研究機関	発表年	多重化	識別方式	互換性	評価試験	
						構造	最小セル (mm)
Hiroko Kato[9-14]	*Edith Cowan University*	2007-2012	Out of scope	相対	無	独自	---
助川[15]	名古屋工業大学	2008	RGB 加色混法	絶対	無	独自	記載無
寺田[16]	電気通信大学	2009	順データ色割当	相対	無	独自	0.67
遠藤[17-20]	神戸大学	2009-2012	QR重層	相対	無	QR	0.69
Grillo[24-28]	University of Tor Vergata	2010-2014	順データ色割当	相対	無	QR	0.69
古本[21-22]	神戸大学	2012-2014	グレイ4色	絶対	有	QR	2.86
菊池[23]	首都大学東京	2013	YCbCr 加色混法	絶対	有	QR	1.38

ここで，遠藤等の研究[20]は，現時点での多色化による大容量化の限界を示している．この研究では，32 色を用い，1 セル当たり 5 ビットを付与し，型番は 3, 6, 11, 16，誤り訂正レベルは M（15%）によってカラー二次元コード画像を作成し，それらをそれぞれ各辺 20㎜, 40㎜, 60㎜ で印刷し，710 万画素の撮像素子を具備するスマートフォンで撮像して JPEG 画像とし，それをパソコンで識別させた結果を示している．その識別結果を表 1-3 に示す．

表 1-3　32 色の場合の認識成功率（遠藤[20]を参考に作成）

印刷サイズ		型式			
		3	6	11	16
20mm	識別率	1%	0%	0%	0%
	セルサイズ	0.69mm	0.49mm	0.33mm	0.25mm
40mm	識別率	78%	44%	56%	4%
	セルサイズ	1.38mm	0.98mm	0.66mm	0.49mm
60mm	識別率	76%	70%	82%	20%
	セルサイズ	2.07mm	1.46mm	0.98mm	0.74mm

この実験結果では，セルサイズが 1㎜ 程度以上で，32 色カラー二次元コードが 80%程度読み取れている．ここで，認識成功率とされているのは，誤り訂正機能によって復号に成功した率であり，セル色の認識成功率ではない．

また，遠藤等の別の研究[19]において，16 色の場合には，100%の識別率が得られている．

1.2.2 互換性を考慮した大容量化

現在の白黒の二次元コードとの互換性を考慮したグレー及びカラー二次元コードの研究が見られる[21] [23]．

表 1-4 に互換性を考慮した大容量化を目的とする多色化の研究事例を示す．これらの研究は，互換性の維持をセルの明度によってのみ実現しているので，セルサイズが小さくなると互換性が失われやすい．

表 1-4 互換性を考慮した大容量化研究

<table>
<tr><th></th><th>符号化方式</th><th>互換性</th><th colspan="2">大容量化</th></tr>
<tr><th></th><th></th><th></th><th>セル
サイズ</th><th>ビット数／
セル</th></tr>
<tr><td>古本（2012）</td><td><table><tr><th>互換性</th><th>色</th><th>符号化</th></tr><tr><td rowspan="2">黒</td><td rowspan="2"></td><td>11</td></tr><tr><td>10</td></tr><tr><td rowspan="2">白</td><td rowspan="2"></td><td>01</td></tr><tr><td>00</td></tr></table></td><td>有り</td><td>2.86mm</td><td>2</td></tr>
<tr><td></td><td>セルサイズが小さくなると、
互換性失われる</td><td colspan="2">セルサイズが小さくなると、グレー色識別不可</td></tr>
<tr><td>菊池（2013）</td><td> 
(a) Y 成分. (b) C_b 成分. (c) C_r 成分.
表 2 明暗情報に対する YC_bC_r の設定値.
<table><tr><th>設計値</th><th>(Y_1, Y_2), ΔY</th><th>(C_{b1}, C_{b2}), ΔC_b</th><th>(C_{r1}, C_{r2}), ΔC_r</th></tr><tr><td>(a)</td><td>(120, 160), 40</td><td>(68, 170), 102</td><td>(60, 180), 120</td></tr><tr><td>(b)</td><td>(60, 160), 100</td><td>(102, 170), 68</td><td>(97, 170), 73</td></tr><tr><td>(c)</td><td>(80, 180), 100</td><td>(100, 160), 60</td><td>(82, 170), 88</td></tr></table></td><td>有り</td><td>1.38mm</td><td>3</td></tr>
<tr><td></td><td>セルサイズが小さくなると、
互換性失われる</td><td colspan="2">セルサイズが小さくなると、カラー8色を識別不可</td></tr>
</table>

1.2.3 秘匿化

表 1-5 に秘匿化を目的とする研究事例を示す．秘匿化では，電子署名と電子透かしを用いた研究が多く見られる[39]- [51]．

また，埋め草領域を用いて秘匿性と互換性を考慮した事例[38]が見られる．この事例については，1.3.2 節で紹介する．

表 1-5 秘匿化を目的とする研究事例

主研究者	研究機関	発表年	方式
小林[43-44]	日本工業大学	2002-2003	電子透かし
鈴木[42]	東京工科大学	2003	電子署名
女川[45]	公立はこだて未来大学	2006	電子透かし
原[38]	デンソー	2008	埋め草領域
新見[41]	九州工業大学	2009	電子透かし
小野[39],宮本[40]	鹿児島大学	2011,2014	電子透かし
Hsu[47]	National Central University (Taiwan)	2012	電子透かし
Vongpradhip[46]	Chulalongkorn University Bangkok	2012	電子透かし
苅田[50-51]	高知工科大学	2011-2012	電子透かし

1.3　課題

現在の技術レベルを前提にした新しい二次元コードを構想し，現在普及している二次元コードよりも大容量であって，さらにデータの秘匿機能を有する二次元コードを検討する．そこで留意したのは，既存の二次元コードとの互換性である．ここで互換性とは，既存の読み取り機器で既存のコードとして読み取れる性質のことである．

1.3.1　互換性を維持した大容量化

二次元コードを大容量化する研究は，関連する研究で述べたように，多くなされており，優れた研究も多い．しかし，それらの多くは既存の二次元コードとの互換性が考慮されていないため，実用化されても限定的であり，広く使用するには経済的社会的な制約がある．

現在も多くの用途でバーコードが用いられている．二次元コードの使用が望ましい用途でもバーコードが引き続き使われている場合がある．その一つが，商品に貼付されてコンビニエンスストアなどで読み取られて精算処理を行う商品バーコード（JAN シンボル）である．商品バーコードは商品コード（JAN コード）のみのデータしか記憶できないために，用途として POS システムのみで使用されている．しかし，これを二次元コードに置き換え，商品コードだけでなくその商品に関連するデータ，例えば定価や商品の詳細を説明する URL などを記憶させればより付加価値が高まり，用途も広がる．しかし，それが当面困難であるのは，商品バーコードと二次元コードの互換性がないからである．現在，世界中の商店には POS システムが導入されて，商品バーコードを読み取ることで精算処理を行っている．このために，すべての商品に商品バーコードが印刷され，すべての商店に商品バーコードを読み取るバーコードリーダが備わっている．そこで，商品バーコードを二次元コードに変更しようとすると，一斉にメーカは商品に二次元コードを印刷し，商店は二次元コードリーダを導入しなければならない．これには莫大なコストを要する．このコストに見合う付加価値を見出されるまで，二次元コードを用いた POS システムは導入されることはないと考えられる．

これと同じことが，既存の二次元コードを新しい高機能二次元コードに置き換える場合にも発生する．もちろん，置き換える付加価値が置き換えコストを

超える場合には置き換えられる．また，新規のシステムでも他のシステムと独立していれば導入されるだろう．しかし，そうでない場合には既存のシステムに組み入れられることは困難である．

（1）互換性の意味

一方，既存の二次元コードと互換性を有する場合ではどうだろうか．

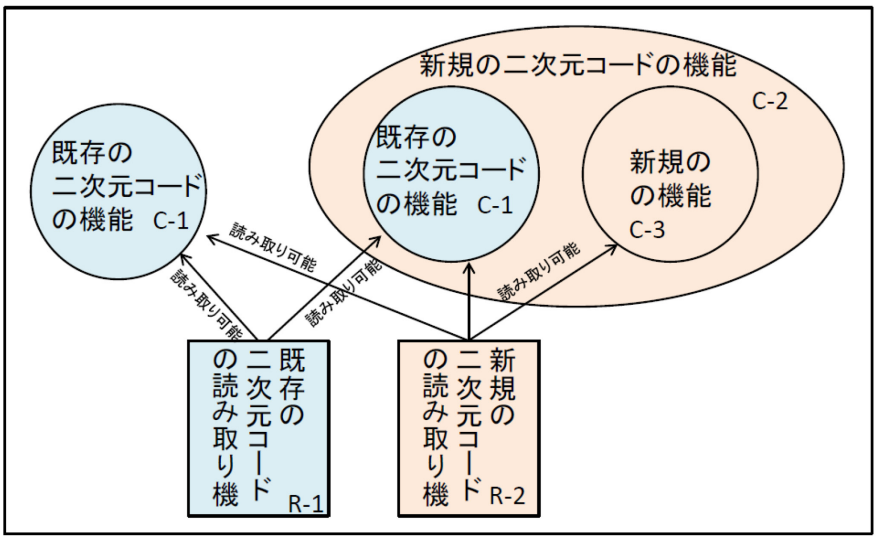


図 1－3　新規の二次元コードと読み取り装置

互換性の内容を示すために，図 1-3 に，新規の二次元コードとその読み取り装置の関係を示す．ここで，C1 は既存の二次元コードの機能であり，C2 は新規の二次元コードの機能である．C3 は，C2 の機能の中で，C1 以外の新たに追加された機能である．また，R1 は既存の二次元コードの読み取り装置であり，R2 は新規の読み取り装置である．

ここで，互換性は以下の三つの条件を満たすことである．

①新規の二次元コードは既存の二次元コードの機能をすべて含む．

②既存の二次元コード C1 の読み取り装置 R1 は，新規の二次元コードの既存の二次元コードの機能部分 C1 を読み取り可能である．

③新規の二次元コード C2 の読み取り装置 R-2 は，既存の二次元コード C1 を読み取り可能である．

②が互換性の核心を成す機能である．

(2) 既存の利用形態

既存の利用形態について述べる．図 1-4 に既存の利用現場の二次元コードと読み取り装置の配置を示す．既存の利用現場 O-0 では，既存の二次元コード C1 とその読み取り装置 R1 が配置されており，それらがシステムを構成している．

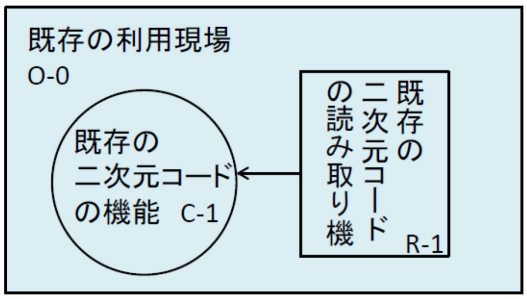


図 1-4　既存の利用現場

(3) 新規の利用形態

次に，既存の二次元コードと新規の二次元コードが混在して用いられる新規の利用形態について述べる．

A. 既存の利用現場

最初に，既存の利用現場について，図 1-5 に新規の利用現場の二次元コードと読み取り装置の配置を示す．既存の利用現場では既存の二次元コード C1 の読み取り装置 R1 が配置されている．そこで，既存の二次元コード C1 を読み取るとともに，新規の二次元コード C2 の互換部分 C1 を読み取る．この機能が互換性の必要な第一の理由となっている．

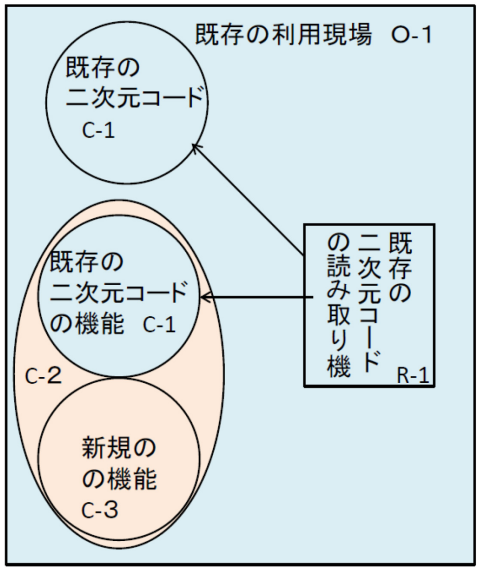


図 1-5　既存の利用現場に新しい二次元コード

次に，この機能の有用性について述べる．図 1-5 に二次元コードの発行元を加えた構成を図 1-6 に示す．ここでは，発行元として A 社，B 社，C 社が存在し，A 社，B 社は既存の二次元コードを発行し，C 社は新規の二次元コードを発行している．それらを混在して読み取る現場は，図 1－5 に示す利用現場と同じである．

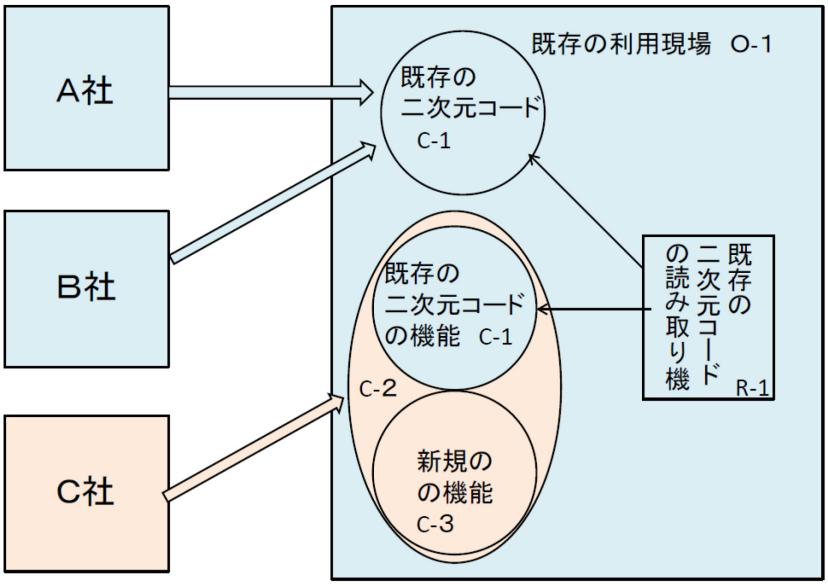


図 1-6　既存の利用現場システム

このシステム構成では，C 社は既存の二次元コードから新規の二次元コードに切り替えても，利用現場に何らの変更をすることなく，既存のシステム機能を維持することを示している．言い替えると，すべての発行元が一斉に新規の二次元コードに変更する必要がなく，逐次の拡張が可能であることを示している．この機能は，既に特定の二次元コードが普及している場合には，新規の二次元コードが普及する第一の必須の機能と言える．

B. 新規の利用現場

次に，新規の利用現場について，図 1-7 に新規の利用現場の二次元コードと読み取り装置の配置を示す．新規の利用現場では新規の二次元コード C2 の読み取り装置 R2 が配置されている．そこで，新規の二次元コード C2 を読み取るとともに，既存の二次元コード C1 を読み取る．この機能が互換性が必要な第二の理由となっている．

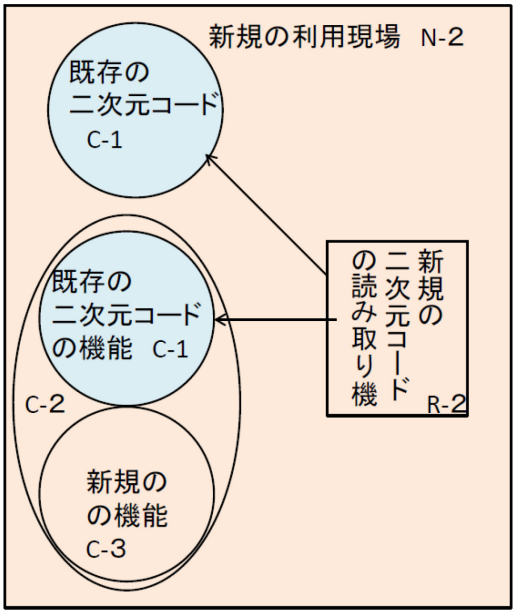


図 1-7　新規の利用現場に既存の二次元コード

次に，この機能の有用性について述べる．図 1-7 に二次元コードの発行元を加えた構成を図 1-8 に示す．ここでは，図 1-6 と同様に，発行元として A 社，B 社，C 社が存在し，A 社，B 社は既存の二次元コードを発行し，C 社は新規の二次元コードを発行している．それらを混在して読み取る現場は，図 1-7 に示す利用現場と同じである．

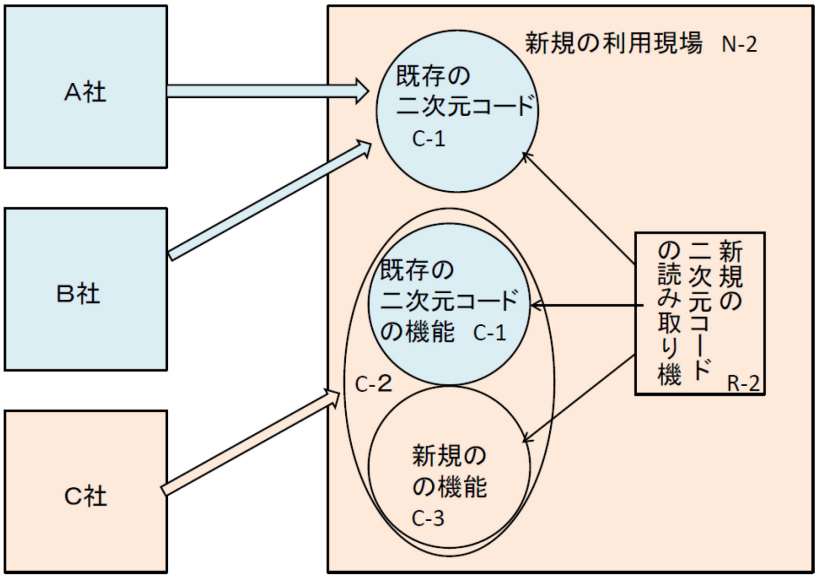


図 1-8　新規の利用現場システム

このシステム構成では，新規の利用現場で C 社から新規の二次元コードの発行を受け，新たに新規機能 C3 を用いた新しいシステムを稼働させている．この利用現場に A 社及び B 社の発行する既存の二次元コード C1 を受け入れ，A 社，B 社に対応する既存のシステムを維持することを示している．言い替えると，既存の二次元コードの発行元は何ら変更する必要がなく，新規の利用現場で利用可能であることを示している．この機能は，既に特定の二次元コードが普及している場合には，新規の二次元コードが普及する第二の必須機能と言える．

以上述べたように，実用を目指す二次元コードは既存の二次元コードの互換性を維持することは必要条件である．そこで，互換性を維持したまま大容量化を実現する手法の研究が第 1 の課題である．

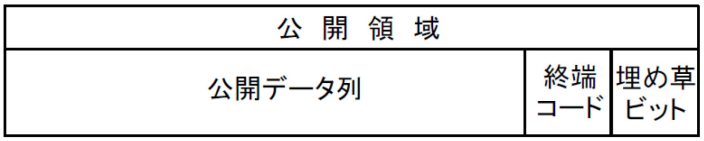
1.3.2　互換部を除く秘匿化

既存の二次元コードと互換性を維持しながら秘匿領域を有する白黒の二次元コード SQRC が提案されている[19]．

SQRC は，QR コードと同じ開発元が開発した二次元コードである．QR コードの仕様は，ISO/IEC の標準仕様[1]として規定され，公開されている．それに対して，SQRC は独自の仕様であり，そのデータ構造や暗号化方式は公表されていない．

SQRC は，図 1-9 に示すように，既存の二次元コードの領域を，公開領域と秘匿領域に 2 分割するものである．既存の二次元コードである QR コードは，利用データ領域の終端に終端コードを有している．QR コードの読み取り装置は，QR コードの読み取り時に，読み取ったデータに終端コードを検出すると，それ以降の領域のデータは無意味な埋め草ビットであると判断して，処理対象としない．SQRC は QR コードのこのようなデータ構成を利用し，終端コードの先の未利用領域に秘匿データを配置し，通常の QR コード読み取り装置から秘匿データを論理的に見えなくしている．

QR コードの構成



SQRC の構成

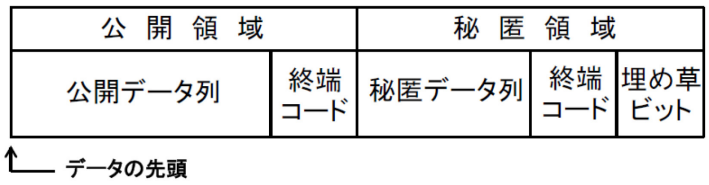


図 1－9　QR コードと SQRC のデータ構成

SQRC は秘匿領域に格納するデータを暗号化し，復号鍵は読み取り端末に予め記憶させることによって，公開領域データの読み取りと秘匿領域データの読み取りを実現している．しかし，大容量化を伴わないため，秘匿領域を設定するためにより大型の二次元コードを用いる必要があり，大きさの互換性は維持できない．

それに対して，本研究では，大容量化を伴う秘匿領域の設定が可能であり，互換性を維持する元の二次元コードと同じ大きさの二次元コードで実現できる．一方，大容量化した部分に限定した秘匿手法が必要となる．この秘匿手法の研究が第 2 の課題である．

SQRC は，データの秘匿に用いる二次元コードであり，その導入事例の多くは公表されていない．ここでは，WEB で公開されている二つの事例を紹介する．

第一の導入事例[62]は，劇団四季のスマートチケットである．この事例では，スマホやパソコンから WEB 経由でチケットを購入する際，モバイルチケットを選択した場合には，SQRC 画像が付されたモバイルチケットがスマホに配信される．ユーザは，会場の入場口でモバイルチケットを提示し，SQRC を入場口に設置されたリーダで読み取らせ，認証を受けることで入場手続きを行う．

第二の導入事例[63]は，ワインの在庫管理システムである．SQRC に在庫管理に必要な情報と共に，顧客に見せたくない情報を記録し，必要な情報をすべて記録することにより，管理業務の効率化を図っている．

1.3.3　アクセス制御

通常の QR コードは，図 1-10 上段に示すように，公開領域が 1 領域存在し，それに対応して公開領域を読み取るユーザも 1 つの構成であった．それに対して，前項に示した SQRC は，図 1-10 中段に示すように，公開領域と秘匿領域が 1 つの 2 領域であった．これに対応して，秘匿領域を読み取り可能と，読み取り

不可の 2 ユーザの構成であった．さらに，図 1-10 下段に示すように，秘匿領域が複数存在し，複数のユーザが許された秘匿領域のみを読み取り可能とするアクセス制御が実現できると，一つの二次元コードで予め設定された複数のユーザに必要な情報の提供が可能となる．

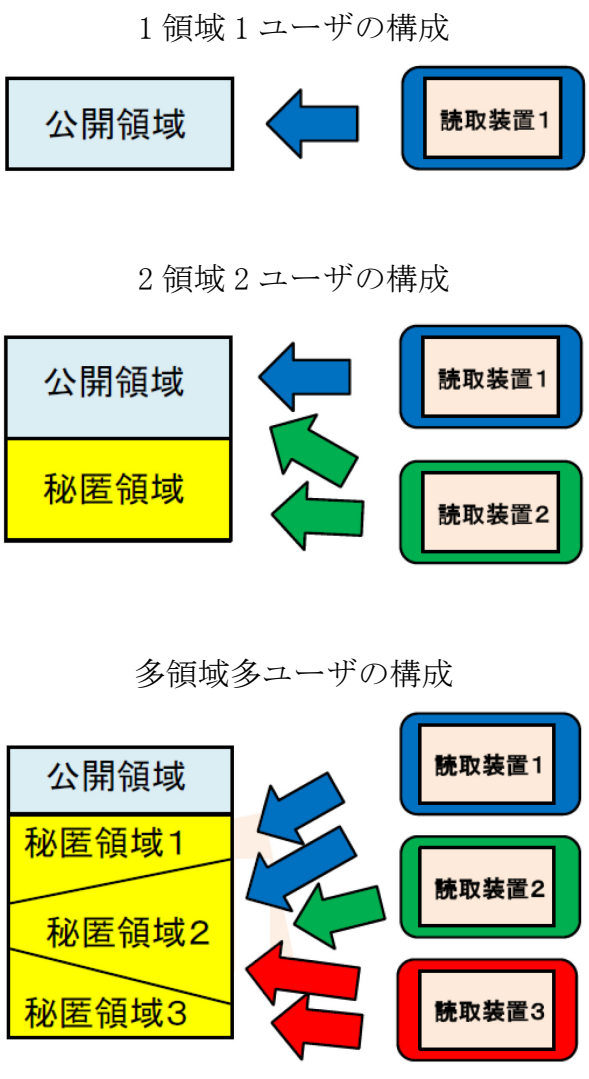


図 1－10　領域とユーザの構成

そこで，二次元コードを複数の領域に分割し，それらに複数のユーザにアクセスを可能とするアクセス方式の研究が第 3 の課題である．

第 2 章　既存の二次元コード

この章では，既存の二次元コードについて，その種類，応用，識別方式，誤り訂正方式を説明する．

2.1　既存の二次元コードの種類

第 1 章でも述べたように，最初の二次元コードはベリコードである．その後多くの二次元コードが開発されている．これらの二次元コードは，マトリックス型とスタック型に分類することができる．マトリックス型は，正方形でありセルと呼ばれる基本単位から構成されている．日本で普及している QR コード[1]や欧米で普及しているデータマトリックス[2]がその代表である．それに対して，スタック型は，バーコードを積み重ねた形状をしている．それらを表 2-1 に示す．

表 2-1　既存の二次元コード

スタック型	
マトリックス型	

これらの二次元コードはそれぞれ特長を有しており，それらの特長を活かす用途で用いられている．そして，これらの多くは ISO/IEC の国際標準に採用されており[1]- [5]，また特定の産業団体の業界標準になっている．

2.2　既存の二次元コードの応用

QR コードの用途は,

①データキャリア

②個人認証

③WEB 参照

である.

（1）データキャリア

データキャリアとしての使用は,QR コードが開発された本来の使用法であり,伝票や製品そのものに付され，物と情報の一体化手段として用いられている.バーコードと比較して大容量という特徴を活用している.

（2）個人認証

個人を特定するために，カード，チケットや病院での患者腕輪などで用いられており，人と情報の一体化手段としての利用法である.

（3）WEB 参照

QR コードはスマートフォンで読み取る用途では，日本のみならず，アジア，欧米でも用いられている.スマートフォンでの利用の主な目的は,WEB 参照である.WEB にアクセスするために必要となるURL をスマートフォンに入力するのは,煩雑であり，また入力ミスが発生する可能性が高いので，それらを簡単に入力する手段として用いられている.

2.3　既存の二次元コードの識別方式

ここでは，既存の QR コードの識別方式について述べる.

2.3.1　QR コードの構成

QR コードは,

①存在検出領域

②回転，変形補正領域

③データ管理領域

④データ領域

からなる.

これらの領域の配置を図 2－1 に示す.

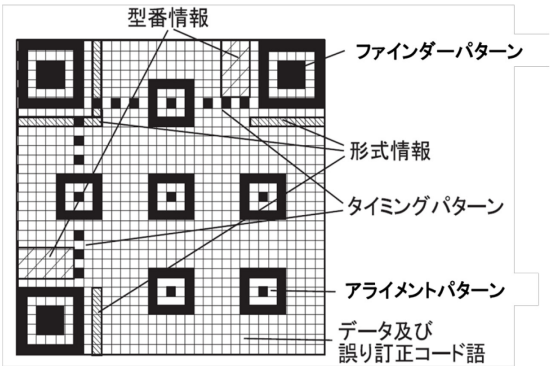


図 2-1 QR コードの領域配置

図 2−1 において，二次元コードの外周に白部として設定されているのが，クワイアットゾーン（QP)である．そして，左上部，左下部，右上部の 3 か所に設定されているのがファインダーパターン（FP)である．QP と FP が存在検出領域である．FP は黒部，白部，黒部，白部，黒部の長さの比率が 1:1:3:1:1 に設定されている．

左上部の FP と右上部の FP の間，及び左上部の FP と左下部の FP の間に設定されているのがタイミングパターン（TP)である．また，右下部に設定されているのがアライメントパターン（AP)である． AP はバージョンのサイズに対応して多数の AP が設定される．

データ管理領域は同じデータが二か所設定されており，

①マスクパターンの種別

②誤り訂正のレベル

を記憶している．この領域では誤り訂正として BCH 符号が用いられている．

上記の残りの領域がデータ領域である．データ領域は，誤り訂正を行うためにリードソロモン（RS)符号を用いており，データ部と訂正データ部から構成されている．訂正データ部の大きさは，予め設定された訂正率によって異なる．

QR コードはデータシンボルサイズが 8 ビット固定であり，8 ビットを単位として扱う．未割当のセルが 7 個未満存在する場合がある．これを残余ビットという．

2.3.2　識別ステップ

QR コードの識別ステップは次の 7 つの処理ステップからなる．

①存在検出処理
②ひずみ補正処理
③白黒判定閾値設定処理
④データ抽出処理
⑤マスク処理解除処理
⑥リードソロモン符号（RS 符号）による誤り訂正処理
⑦データ圧縮解除処理

以下に，各処理ステップについて述べる．

ステップ 1　存在検出処理

読み取り装置によって撮像した画像を，試みの閾値を用いて白黒画像化し，その白黒画像の中から黒白の長さパターンが 1:1:3:1:1 であるパターンを探索する．これらの探索により FP が検出できる．FP はどのような角度で直線を引いても 1:1:3:1:1 の比率になるので，比較的容易に検出できる．検出できない場合には，試みの閾値を適宜変更してリトライする．

ステップ 2　回転，変形補正処理

識別対象の QR コードのシンボルと読み取り装置の関係は，多くの場合正対せず，シンボル画像が回転した状態になっている．

そこで，FP の位置情報を元に回転補正処理を行う．併せて，QR コード全体の大きさ，セルサイズを推定する．これらの推定したサイズを基にして，TP と AP を検索し，撮像シンボル画像の変形を補正する．AP は当初の QR コードの仕様にはなかったが，ビール缶などの曲面に印刷された QR コードを読み取り可能とするために追加された．

ステップ 3　白黒判定の閾値設定処理

ステップ 2 で補正したシンボル画像から各セルの中央位置を計算し，中央位置の画素の RGB 値から明度 Bt を下記の式より計算する．

$$Bt = 0.299R + 0.587G + 0.114B \qquad (2\text{-}1)$$

QR コードの中で一番小さなバージョン 1 では,21x21 のセル構成となっており，441 個のセルが存在する．これより大きなバージョンではこれ以上のセルが存在する．これらのサンプリングしたセル中央部の明度の分布図を作成する．これらの分布図の例を図 2-2 に示す．

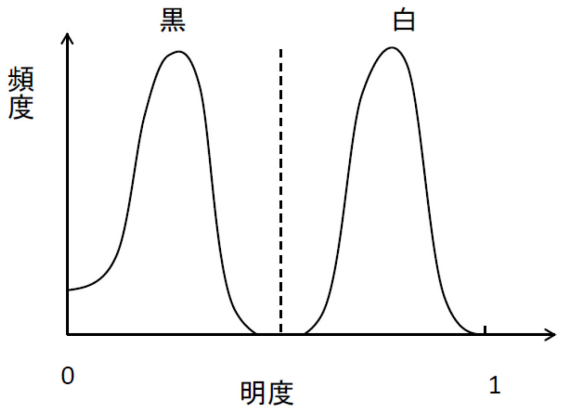


図 2-2 明度分布図

ここで，黒と白を分離する閾値 Bs を決定する．黒と白のピークの明度値の中央値などを採用する．

ステップ 4　データ抽出

次に，QR コードの黒白のアナログパターンから 1，0 のディジタルデータに変換する．ステップ 3 で決定した閾値 Bs を用いて，各セルの中央値のサンプリング値 Bt と比較し，

$$Bt > Bs \qquad (2\text{-}2)$$

の場合には，白と判定し，セルの値を 0 とする．また，

$$Bt < Bs \qquad (2\text{-}3)$$

の場合には，黒セルと判定し，セルの値を 1 とする．

上記の処理をデータ領域全体について行い，ビットマップを得る．

ステップ 5　マスク処理解除処理

ステップ 4 で決定した各セルのビットマップ BM に対して，マスク処理の解除処理を行う．マスクパターン MP は予め 8 個設定されており，QR コードのセイルパターンの生成時に用いたマスクパターンの種別を表す値がデータ管理部に記憶されている．マスク処理は次の目的から行われている．

①データ領域に 1:1:3:1:1 のパターンが出現しないようにする

②白黒のセルの比率をほぼ 1:1 にする．

データ管理部から MP を読み出し，ビットマップ BMa に対して EOR 計算を行い，MP を解除する．

ステップ 6　RS 符号誤り訂正

マスク処理を解除したビットマップ BMa から RS 符号のシンボルデータを配置し，誤り訂正処理を行う．

誤り訂正処理に成功した場合には，訂正後のビットマップ BMr からデータを取り出し，一連のデータ列とする．

ステップ 7　データ圧縮解除処理

QR コードでは，データの種別四つに対応しており，各種別毎に異なるデータ圧縮を行っている．これらの圧縮の解除処理を行う．データ種別を以下に示す．

①数字

②英数字記号

③漢字

④バイナリーデータ

数字は 3 数字を 10 ビットで，英数字は 2 文字を 11 ビットで，漢字は 13 ビットで表現している．

これらの処理により，QR コードの復号処理を完了する．

2.4　誤り訂正方式

QR コードでは，誤り訂正方式として，RS 符号を用いている．その誤り訂正のレベルは，表 2-2 に示すように，４つのレベルが規定されている．

表 2-2　ＱＲコードの誤り訂正レベル[1]

誤り訂正レベル	復元能力%(概数)
L	7
M	15
Q	25
H	30

また，セルの一辺の個数が型式として，規定されている．この型式と誤り訂正レベルの組み合わせに対応して，データコード語と訂正データコードの個数やその二次元コード内のセルの配置が ISO/IEC の規定[1]で詳細に定められている．これにより，種々の工夫の自由度は無くなっている．自由度が無いことによって，実際の読み取りにおいて混乱が生じていないのである．

第 3 章　互換性を維持した大容量化

3.1　はじめに

この章では，既存の二次元コード（QR コード）と互換性を維持しながら，記憶容量を拡大し，増加した部分を秘匿化するカラー二次元コードについて述べる．

ここでの互換性は，第 1 章で述べたように，本論文で提案する二次元コードの一部（互換部）を従来の二次元コードとして読み込めることである．また，大容量化は，同じコード形式，すなわち同じセル数で記憶するデータ容量を増加することであり，高密度化を意味する．二次元コードでは，コード形式を大型化し，セル数を増大させることにより収容するデータ量を増加させることができる．この場合は，データ収容密度はほぼ一定であり，高密度化にはなっていない．

以下では，互換性を維持した大容量化を実現するために低密度方式と高密度方式のカラー二次元コードを検討した結果について述べる．高密度方式は低密度方式のセル構造を拡張した方式である．

3.2　低密度方式カラー二次元コード

互換性を維持した大容量化では，上記のように低密度と高密度のカラー二次元コードを検討した．この節では，低密度のカラー二次元コードについて述べる．

3.2.1　セルの構造

既存の二次元コードとの互換性を維持しつつ，秘匿領域を追加するためには，二次元コードの基本単位であるセルの多値化を行う必要がある．多値化の手法として，多色化と多領域化が知られている．多領域化は，セルを複数の領域に分割し，それぞれに独立した情報を与える方式である．ここでは，互換性維持と秘匿化を目的とした大容量化のために，多色化と多領域化を併用する．そして，二次元コードとして，QR コード[1]を対象とする．この事例を図 3-1 左側に示す．QR コードのセルが白または黒の 1 ビットを表現しているが，それを多値化するために，図 3-1 右側に示すセルの構造を検討した．

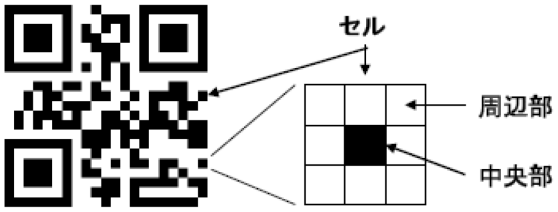


図 3-1　QR コードとセルの分割

図 3-1 右側は，セルを 9 個の同一面積の正方形の小領域（サブセル）に分割する．そして，中央部を互換部に，周辺部を新規の追加領域（秘匿部）に割当てる．互換部は，既存の読取装置で読取が容易になるように白色または黒色とする．周辺部は，大容量化のためにカラー色（多色）とする．

(1) 互換性の実現

スマートフォンの二次元コードの既存の読取りソフトウェアは，セルの切り出し後，各セルの中央部の画素の色が白色か，または黒色か，を判別している．そこで，互換部のデータの識別には，周辺部の寄与は小さい．

しかし，周辺部の色が，互換部と反対の色である場合には，誤って識別される可能性が高くなる[12]．すなわち，互換部が白の場合において，周辺部が黒の場合には，影響が大きくなる．

ここで，周辺部の反対の色が，中央部の識別に与える影響を評価した結果を図 3-2 に示す．

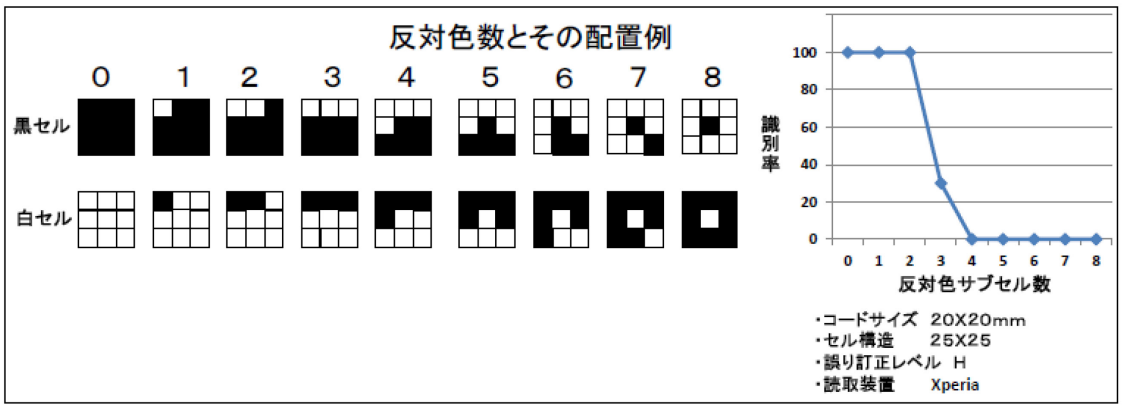


図 3-2　反対色サブセルの影響評価

この実験は，それぞれの反対色の個数の周辺部のサブセル配置を乱数で決めて配置した場合の識別結果である．

これにより，セルサイズが 0.8mm の場合には，反対色の個数が 3 個の場合で大きな影響があり，4 個以上では読み取れない結果となっている．また，周辺部の影響は，セルサイズが小さいほど大きくなる．

そこで，周辺部の色を白グループ色と黒グループ色に分類し，互換部が白色の場合には，周辺部を白グループ色を割り当て，黒色の場合には黒グループ色を割り当てる．ただし，これらのカラー色は，印刷される場合には，印刷時のインクの発色や経時劣化による変色で，白または黒グループの範囲に止まらない可能性がある．そこで，白または黒グループ色の周辺部への割り当ては，中央部の識別に与える影響を低減するための補助的な手法と言える．

(2) セルの多色化

ここでは，8 色を用いた場合について述べる．用いる色は，次のようにして選択した．

3.2.2 項で述べるように，距離尺度として RGB 空間でのユークリッド距離を用いる．この距離尺度では，RGB の三次元空間で相互に最も離れた色セットが識別が最も容易となる．そこで，相互に最も離れた位置は RGB 空間の立方体の端部であり，当該位置にある色を選択する．

表 3-1　カラー8 色の選択と符合化

色群	色コード	RGB			輝度	色	符号化データ
		R	G	B			
白グループ	000	255	255	255	1		00
	001	255	255	0	0.93		01
	010	0	255	255	0.79		10
	011	0	255	0	0.72		11
黒グループ	100	255	0	255	0.28		00
	101	255	0	0	0.21		01
	110	0	0	255	0.07		10
	111	0	0	0	0		11

選択した各色の RGB の具体値を表 3-1 に示す．表 3-1 に各色の輝度を示したが，輝度(Y)と RGB 値の変換式は，ITU-R BT.601[15]で規定されている次式を用いた．

$$Y = 0.299R + 0.587G + 0.114B \quad (3\text{-}1)$$

輝度の値を基に，各色を白または黒グループに分類した
図 3-3 に，低密度の場合のセルの色構成の例を示す．

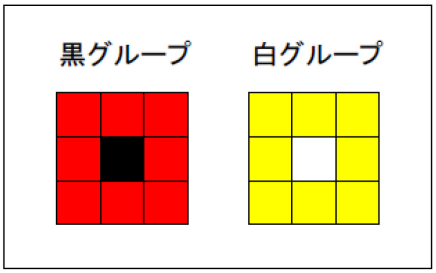


図 3-3　セルの色構成

この色構成の特徴は，互換性を維持するために中央部を黒または白で構成し，大容量化するために周辺部をカラー色で符号化したことである．この構成が，本研究の従来研究に対する基本的な新規点であり，工夫点である．

3.2.2　符号化

低密度構成におけるサブセルは，セル色によって，白グループまたは黒グループの 4 色によって符号化される．

(1) 色の符号化

4 色による符号化では 2 ビットを表現できる．図 3-4 に示すように，二つの同一サイズの白黒の二次元コードの同一位置のサブセルの値を表 3-1 の符号化データに基づき色を選択することにより符号化する．例えば，互換部が黒であるセルにおいて，サブセルが両方共に白 (0) の場合には 00 の 2 ビットを表現し，紫色に符号化される．

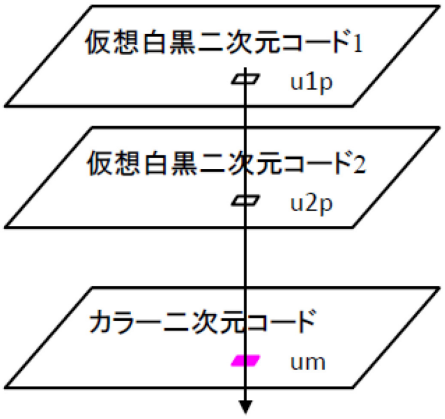


図 3-4　二次元コードの色符号化

(2) 仮想的な積層構造

選択した 8 色について，白グループと黒グループの色はそれぞれ 4 色であるので，新たに 2 ビットを表現できる．この色コードと保持するデータの対応は，表 3-1 の符号化テーブルに示されている．この例では，色コード 000 はデータ 00 を保持する．周辺部の 8 色の多色化によって，従来と同容量の既存領域と従来の 2 倍の容量の新規領域からなる二次元コードを表現する．

また，色コード 000 は，互換部が白（0）であり，周辺部が白白（00）であることを示している．

この構成は，一つのセルが 3 ビットを表現しているので，図 3-5 に示すように，既存の白黒の 2 次元コードが 3 層重なっているのと同等である．

以下では個々の仮想的な白黒の二次元コードを層と呼ぶ．

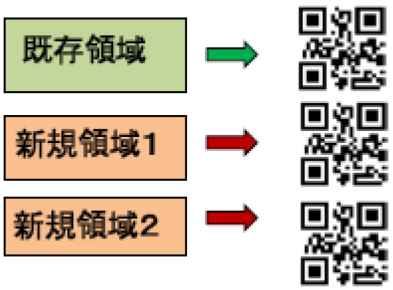


図 3-5 仮想的な積層構造

3.2.3　色識別手法

（1）比較法の採用

色を識別する手法としては，判別法[15][17]と比較法[10][16]がある．判別法は入力された画素の RGB 値に基づき予め定められた色集合から特定の色を判別する手法である．それに対して，比較法は，予め定められた色集合の色全てを二次元コードの中の定められた領域に設定しておき，それらの色集合と識別すべき画素色と比較することにより，一番近い色を選択する手法である．

カラー色を用いた二次元コードを紙に印刷する場合には，印刷に用いるインクやトナーによって，元の RGB 値から離れた色になったり，それらをスマートフォンで読取る場合には，用いられる撮像素子の特性によって，入力される RGB 値がさらに変化することが知られている[17]．さらに，印刷された色が経時劣化によって，変化することが想定できる．

そこで，本論文の提案では，これらの影響を回避できる比較法を採用する．比較法（パレット方式）は上記のインクによる発色の差異や経時劣化について，比較色（パレット色）とセル色が同様に差異が発生し，経時劣化するので，それらの影響を回避可能である．

パレット色を二次元コードの定められた位置に収容する．図 3-6 に示すように，白及び黒グループのパレット色は，それぞれファインダーパターンの白部または黒部に配置する．その比較対象の色群をここではパレットと呼ぶ．QR コードでは，定められた位置にファインダーパターンを有しているので，そこへパレットを配置する．また，これらのパレット色が汚れなどによって正しい色を表現できなくなる可能性があるので，三つあるファインダーパターンのすべてにパレットを設定する．

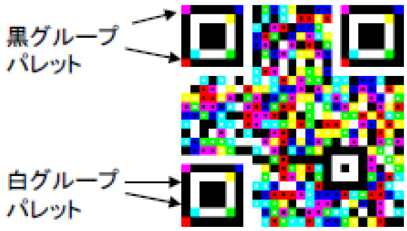


図 3-6　パレット色の設定

また，パレットのセルにおいても，中央部のサブセルの影響を符号化領域のセルと同一とするために，図 3-7 に示すように，セルを中央部と周辺部に分割し，中央部にはグループ色を配置し，周辺部にパレット色を配置した．ここで，図 3-5 に示した白グループパレットセルに描いた中央部と周辺部の境界線は，説明のために描いた線であり，実際には存在しない．

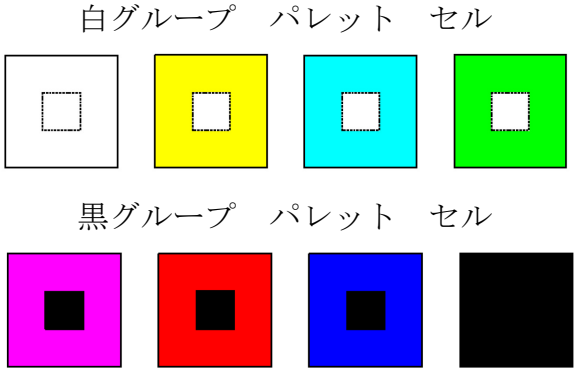


図 3-7 パレットのセル構造

(2) 識別処理

各セルの周辺部の色（以下，セル色と呼ぶ）を識別する識別処理は，撮像された画像をセルレベルに切り出した後，比較対象であるパレット色とセル色を抽出するデータ抽出処理と比較処理から構成される．

A．データ抽出処理

比較する対象は，パレット色とセル色である．パレット色はすべてのセルの比較に共通である．パレット色は，図 3-8 左図に示すように，パレットを構成するセルを 9 つの領域に分割し，さらにその中央部を 9 つに分割し，その中央の画素の RGB 値の平均値とした．比較はセル色とパレット色の，白または黒のグループ色の 4 色と行う．また，パレットは各ファインダーパターンの中に 3 セット設定している．3 セットに含まれる色を独立した色として扱い，仮想的に 12 色として比較し，最も距離の小さいパレット色を選択する．

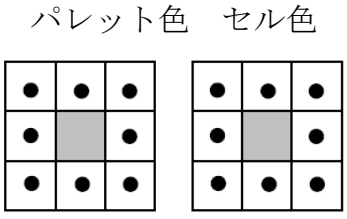


図 3-8　パレット色とセル色のデータサンプリング位置

セル色の RGB 値は，図 3-6 右図に示す周辺部の 8 個のサブセル領域の中央の画素の RGB 値の平均値とした.

Ｂ．比較処理

比較処理は，データ抽出処理で作成したパレット色 12 色とセル色の各 RGB 値を比較する．パレット色の RGB データ Cp は,

$$Cp = (Ri, Gi, Bi) \quad (3\text{-}2)$$

で表現できる.ここで,i は選択候補であるパレット色 12 色の指標である.Ri ,Gi, Bi は各パレット色の RGB 値であり，0 から 255 の間の値をとる.

同様に，セル色の RGB データ Cc は,

$$Cc = (Rc, Gc, Bc) \quad (3\text{-}3)$$

で表現する．i 番目のパレット色とセル色の RGB 値のユークリッド距離 Di は

$$Di = \sqrt{(Rc - Ri)2 + (Gc - Gi)2 + (Bc - Bi)2} \quad (3\text{-}4)$$

となる.

Di が最小値となるパレット色をセル色と同一と判定する.

3.2.4　提案アルゴリズム

この項では，本論文の提案の符号化と復号の処理について述べる．評価試験に用いた二次元コードは本項の符号化処理に従って作成した．また，評価試験に用いたソフトウェアは，復号処理のステップ 1 からステップ 5 に従って作成した.

具体的な処理内容を説明する前に，本論文で提案する低密度の二次元コードのデータ構成を示し，そこで示した記号の内容を説明する．データ構成を表 3-2 に示す.

表 3-2　低密度構成の二次元コードのデータ構成

項　目				データ部	訂正部
既存領域（第0層）		保持データ		d0	
		埋め込みデータ		d0f	d0fc
		白黒符号	前*	u0	u0c
			後*	u0p	u0pc
新規領域	第1層	保持データ		d1	
		埋め込みデータ		d1f	d1fc
		仮想白黒符号	前*	u1	u1c
			後*	u1p	u1pc
	第2層	保持データ		d2	d2c
		埋め込みデータ		d2f	d2fc
		仮想白黒符号	前*	u2	u2c
			後*	u2p	u2pc
	重層	カラー符号		*um*	umc

*前、後は、マスク処理の前、後を意味する

データ構成を示す表 3-2 において，収容するデータ D=(d0,d1,d2)は，既存領域（第 0 層）に収容する元データ d0，新規領域（第 1 層，第 2 層）に収容する元データ d1,d2 から成る．このデータを書式化したデータが Df=(d0f,d1f,d2f)である．例えば，d0f は d0 を収容するためのデータヘッダー（収容するデータのデータ種別，データ長）やデータの終わりを示す終端コードが挿入されている．また，データの種別によってデータ圧縮が行われている．そして，収容可能なデータサイズに比較して収容するデータが少ない場合には，終端コードの後ろには，埋め草ビットと呼ばれるデータパターンが埋め込まれる．この書式化したデータ Df=(d0f,d1f,d2f)のそれぞれの層に対して，RS 符号を用いた誤り訂正データ Dfc=(d0fc,d1fc,d2fc)が生成される．例えば，d0f と d0fc は RS 符号におけるデータコード語を構成する．

この Df と Dfc を予め定義された二次元コードの符号化領域のセルに配置し，白黒符号化したデータが U=(U0,U1,U2)と Uc=(U0c,U1c,U2c)である．U および Uc は df,dfc を単純に白黒に置き換えたデータではなく，データの配置された位置情報を含んでいる．この U,Uc に対して，マスク処理を行った結果が Up,Upc で

ある．このU0p,U0pcは，二次元コードの既存領域の中の符号化領域の白黒パターンを示している．UmとUmcは，それぞれU1とU2，U1cとU2cを符号化テーブル表3-1を用いてカラー色に置き換えたデータである．

次に，データの構成要素を用いて，具体的な処理について述べる．

(1) 符号化処理

ステップ1：データの準備

既存領域に収容するデータd0及び新規領域に収容するデータを各層に分配して得た各層に収容するデータd1,d2,からなる収容データD = (d0,d1,d2)を準備する．

ステップ2：各層の白黒二次元コード化

各層の収容データ D = (d0,d1,d2)を白黒の二次元コード化し，誤り訂正データを含めた二次元コードの白黒データ U = (u0,u1,u2)を得る．以下では，煩雑を避けるために，誤り訂正部分の説明を省略する．

ステップ3：マスク処理

ステップ2で得られた第1，第2層のデータについて，与えられた共通秘匿パターンで排他的論理和演算を行い(マスク処理については,第4章で詳述する)，白黒データU = (u0,*u1,u2*)を得る．

ステップ4：可変領域のセル色の決定

既存領域の各セルの白黒データu0に基づき，表3-1の白グループまたは黒グループの符号化テーブルを用いて，新規領域の各セルの白黒データ *u1,u2* を符号化し，周辺部のセルの色を決定する．

ステップ5：固定領域のセル色の決定

パレット色を割り当てられたセルに設定する．それ以外のファインダーパターンなどの固定領域は黒または白に設定する．

(2) 復号処理

ステップ1：画像入力と画像抽出

撮像装置によって，二次元コードを含む画像を撮像し，二次元コードに含まれるファインダーパターンを基に二次元コードを検出し，二次元コードの画像を抽出する．

ステップ 2：互換部の識別

撮像した二次元コードを白黒の二次元コードとして識別し，既存領域のセルの白か黒のデータ u0 を得る．

ステップ 3：パレット色の抽出

ステップ 2 で切り出したセルについて，パレット色が格納されているセルから，パレット色のデータを取得する．

ステップ 4：可変領域のセル色の識別

二次元コードの可変領域のセルの周辺部について，パレット色との距離を計算し，最小の色を当該セルの色として選択する．

ステップ 5：各層の白黒二次元コードに復号

新規領域について，各セルの互換部の白または黒の色に従い符号化テーブルによって復号し，二次元コードの白黒データ U=(u0, *u1. u2*)を得る．

ステップ 6：マスク解除処理

共通秘匿パターンで排他的論理和演算を行い秘匿の復号をして，白黒データ U = (u0, u1, u2)を得る．

ステップ 7：白黒二次元コードの復号

ステップ 4 で得られた二次元コードの白黒データ U = (u0, u1. u2.)から各層の二次元コードを復号し，各層に収納されたデータ D = (d0, d1, d2)を得る．

3.2.5　評価試験

(1) 互換性評価試験

セルの周辺部にカラー8 色を用いた場合について，スマートフォンを用いて既存領域の読取りの検証を行った．その検証の条件と結果について述べる．

①　試験条件

Ａ．二次元コード

二次元コードと印刷には，下記を用いた．

二次元コードの種類：	QR コード
型番	： 2（25x25 セル）
誤り訂正	： レベルH（30%）
データタイプ	： バイナリー
プリンタ	： MG6230（キャノン製）
印刷紙	： マット紙（コクヨ）

検証に用いた収容データは，読取り時に確認が容易な漢字及び ASCII 文字をとした．二次元コードに収容するデータを表 3-3 に示す．また，それらのデータを収容する二次元コードを図 3-9 に示す．

表 3-3　収容データ

コード番号	既存領域	新規領域
1	カラー2次元	01234567890123456789012345
2	カラー2次元	ABCDEFGHIJKLMNOPQRSTUVWX
3	ABCDEFGHIJKLM	01234567890123456789012345
4	0123456789ABC	ABCDEFGHIJKLMNOPQRSTUVWX
5	吾輩は猫であ	吾輩は猫である。名前はまだ
白黒	吾輩は猫であ	

図 3-9　検証に用いた二次元コード

ここでは，色の読取性の検証が目的であるので，カラー部の秘匿化（マスク処理）は実施しなかった．

表 3-4 に図 3-9 に示した各検証用二次元コードのセル周辺部の色の出現分布を示す．コード領域の 352 個のセルについて示した．各二次元コードについて，各色がほぼ一様に出現していることが判る．

表 3-4　色の出現分布

色 / コード番号	1	2	3	4	5	6	7	8
	白	黄	青緑	緑	ピンク	青	赤	黒
コード1	36	48	38	45	48	41	45	51
コード2	32	51	45	39	42	43	60	40
コード3	40	46	44	43	44	43	39	53
コード4	48	44	43	41	42	48	48	38
コード5	52	37	44	42	44	38	49	46

B．読取り機器

読取りには，下記のスマートフォン及び読取ソフトウェアを用いた．

スマートフォン　　：　GALAXY Note 2　(SAMSUNG 製)

読取りソフトウェア　：　表 3-5 の中に示す

②　検証結果

検証試験の結果を表 3-5 に示す．この結果について検討する．

表 3-5 互換性検証結果

			読取り率(%)						
コードサイズ (mm)			12	10	8	6	5	4	3
セルサイズ (mm)			0.48	0.4	0.32	0.24	0.2	0.16	0.12
アンドロイド	QRコード スキャナ	カラー	100	100	100	100	24	0	0
		白黒	100	100	100	100	100	100	0
	Code Scanner	カラー	100	100	100	100	60	0	0
		白黒	100	100	100	100	100	100	0
アイフォン	QRdeCode	カラー	100	100	100	0	0	0	0
		白黒	100	100	100	100	60	0	0
	ICONIT	カラー	100	100	100	0	0	0	0
		白黒	100	100	100	100	100	0	0

コードサイズが 8mm 以上の場合には，全てのカラーコード及び白黒コードで 100%の読取りができた．また，3mm 以下の場合は，全てのコードについて，読取が不可能であった．4mm の場合には，多くの場合読取が不可であった．カラーコ

ードと白黒コードで読取率に差がなく，十分な互換性を有していることが確認できた．そして，互換性が収容するデータへの依存性がないことが確認できた．

また，スマートフォンの機種や読み取りソフトウェアの違いによって，読み取り率に大きな違いが発生している．この違いの原因は，読み取りソフトウェアの開発方針の違いであると考えられる．開発方針には二つあり，一つは誤読み取りが無いように確実に読み取る方針であり，他方は可能な限り読み取る方針である．この方針が読み取りアルゴリズムの違いとなり，読み取り率の違いとなっている．

(2) セルレベル識別性の評価試験

① 試験条件

Ａ．検証サンプル

識別性の検証にも，図 3-7 に示し互換性検証で用いたコード 1 を用いた．

Ｂ．読取条件

読取りは，下記の条件で実施した．

スマートフォン	： GALAXY Note 2 (SAMSUNG 製)
照明	： 白色蛍光灯
二次元コードとの距離	： 55mm に固定
焦点合わせ	： スマートフォンによる自動焦点

② 検証方法

カラー部の識別は，スマートフォンでの処理とパソコンでの処理の 2 ステップで行った．

Ａ．スマートフォン処理

スマートフォンでカラー二次元コードを撮像し，従来の白黒の二次元コードとして，誤り訂正を含めて識別する．この処理に伴って，各セルを切り出し，各サンプリング値の表を作成する．この表に含まれるのは，図 3-1 右図に示す各セルを 9 分割した領域の中央値の各 RGB 値 ，図 3-6 左図に示すパレット色の 9 点の RGB 値及び誤り訂正後の各セルの白または黒の区別である．

Ｂ．パソコン処理

スマートフォンで作成した上記の表をパソコンに転送する．そして，そのデータをエクセル上の VBA でデータ抽出処理,平均値処理及び比較処理を行い，色

の識別処理を行った．識別率は，各セルの本来の色（正解色）との比較により算出した．

③　検証結果

従来の研究での評価は，コードレベルの読取率を用いる場合が多い．実用性を評価する場合には，適切な評価基準であるが，色の識別性を評価する場合には，次節で述べる誤り訂正の機能によって，誤りが見えなくなるので，ここでは個々のセルレベルでの誤り率を評価基準として評価する．

読取検証は図 3-7 に示した 5 個の二次元コードについて，コードサイズが 40mm から 10mm の二次元コードを作成し，それぞれについて 10 回づつ読取り，それぞれの読取について，読取率を計測し，それらの平均値を求めた．

QR コードのバージョン 2 は 25x25 セルの構成であり，セル数は全体で 625 個である．また，次節で述べるように総コード語は 44 であり，これに対応するセル数は 352 である．

コード識別に直接関与するのは，コード語領域である．また，ファインダーパターン，タイミングパターン及びアライメントパターンは，白色または黒色に固定されており，それらの識別はカラー色の識別には当たらない．そこで，コード語領域のセルを対象にして識別率を計測した．この結果を図 3-10 に示す．

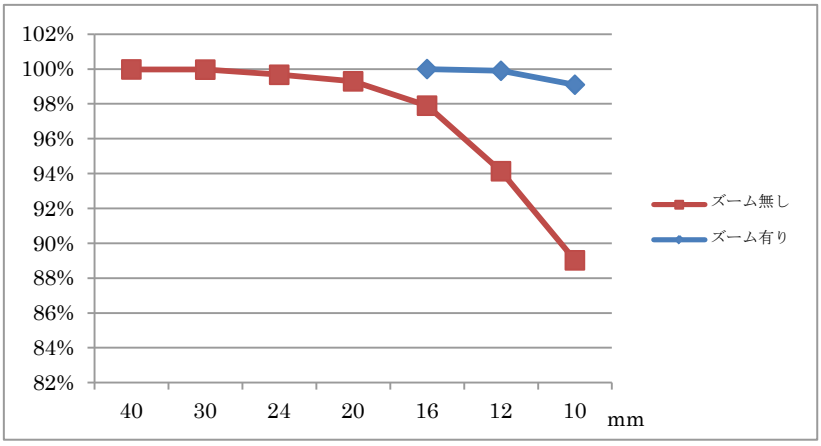
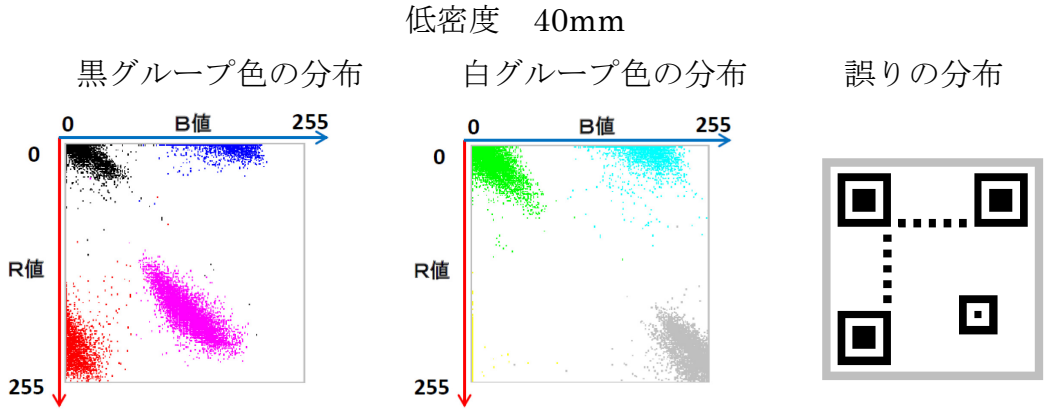


図 3-10　低密度構成の識別検証結果

この結果，20mm のコードサイズからセルレベルの誤りが多く発生していることが判る．また，識別を誤ったセルは，コード内の特定の位置に集中することなく，分散していた．そこで，コードサイズが小さくなるに従って，解像度が不足し，近傍のセルの色が混入してくるのが原因と考えられる．白黒の二次元コードの場合には，反対色が混入してもある程度までは識別可能であるのに対して，カラー色の場合には，色相が変化し，誤りが発生しやすい．

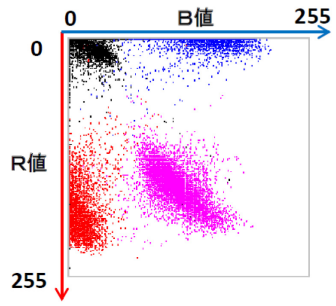
図 3-11 に，上記の識別試験で得られた各セル（周辺部の平均値）の RGB 値の分布と誤り位置を示す．図 3-11 では，コードサイズが 40mm～10mm の場合及びコードサイズが 20mm～10mm のズーム機能用いて拡大したそれぞれの場合を示す．それぞれのコードサイズについて，左図は黒グループ色の 4 色（黒，青，紫，赤）のサンプリング値（RGB 値）の R 値と B 値を平面にして示した．中央は同様に，白グループ色（白，黄，青緑，緑）の 4 色について示した．右図は誤り分布図であり，誤りの発生した位置（セル）とその位置のセル色（周辺部）を示す．誤識別した色の事例を図 3-12 に示す．

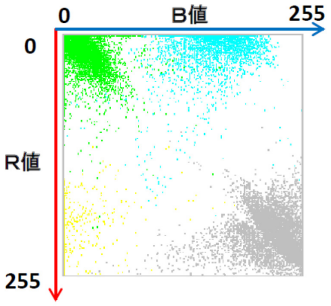
黒グループ色と白グループ色の分布は，5 個の二次元コードの各 10 回分の読み取りの全サンプリング値を示した．それに対して，誤り分布図は当該読み取りの平均的な誤り率の 1 回分の誤り位置を示した．

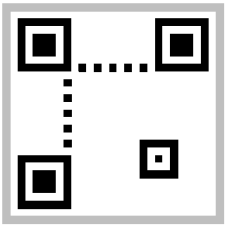


黒グループ色の分布　　白グループ色の分布　　誤りの分布

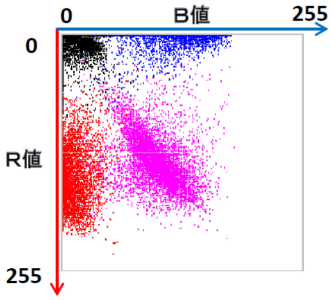
低密度　30mm

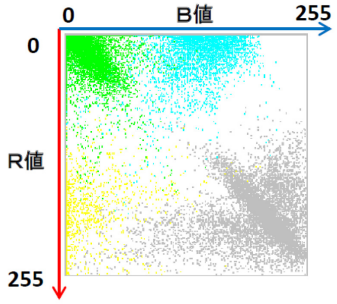


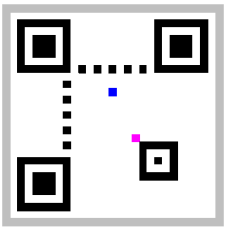




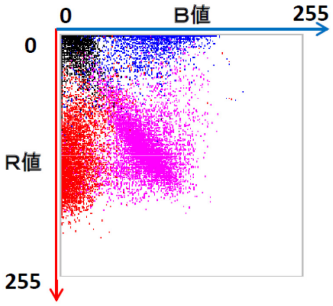
低密度　24mm

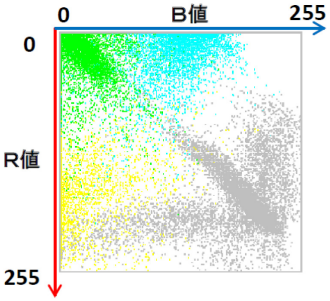


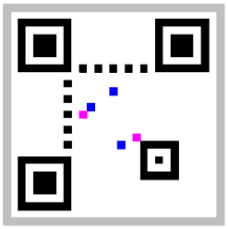




低密度　20mm

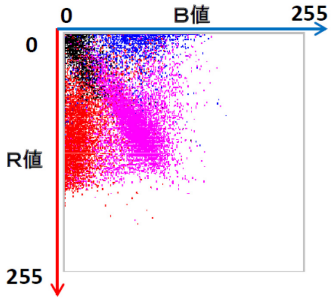


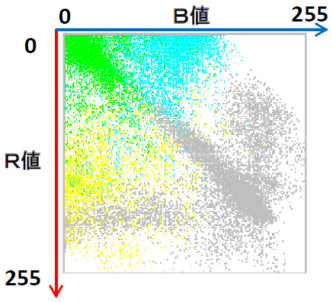


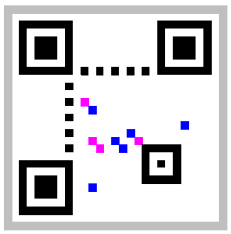


黒グループ色の分布　　白グループ色の分布　　誤りの分布

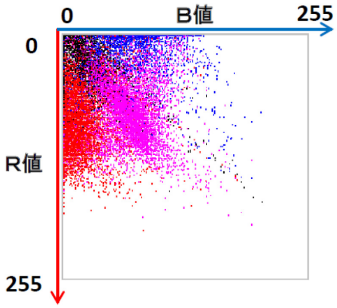
低密度　16mm

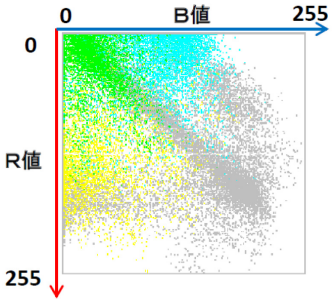


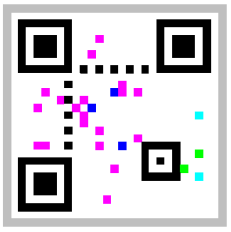




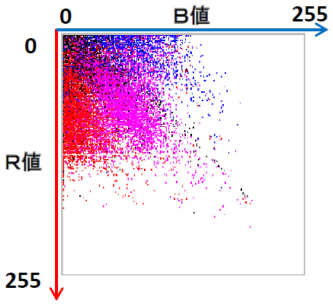
低密度　12mm

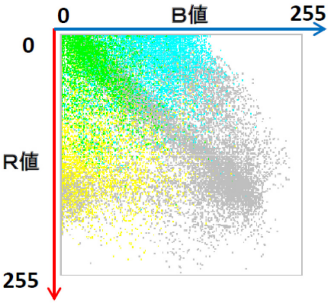


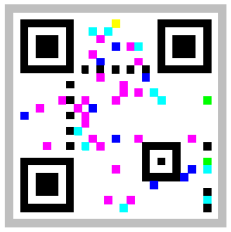




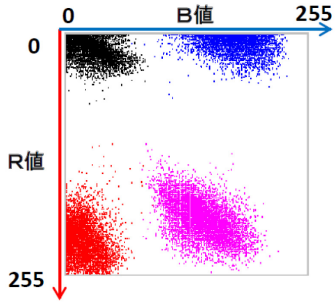
低密度　10mm

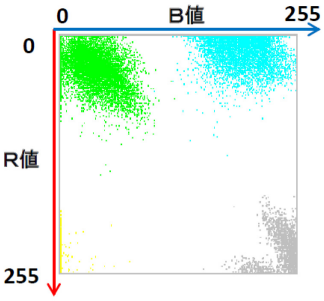


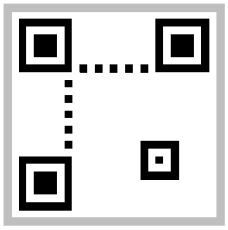




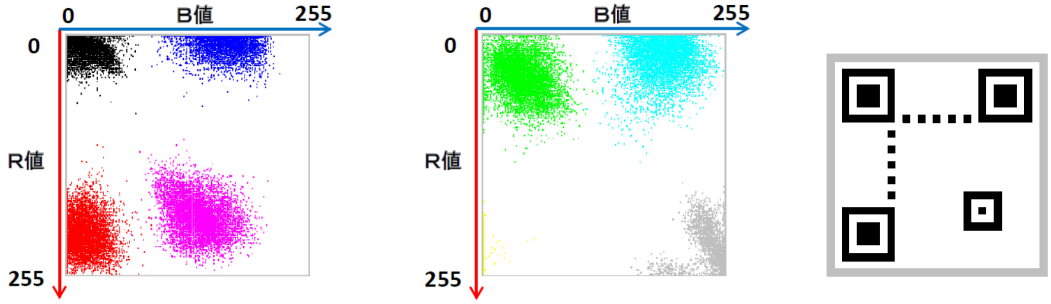
低密度　ズーム 20mm



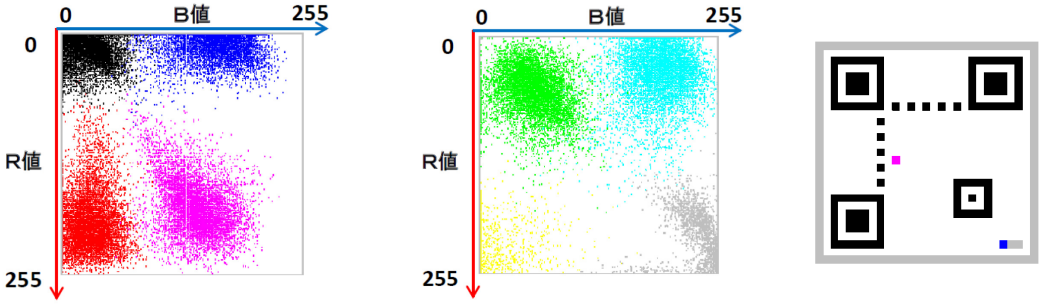




低密度　ズーム 16mm



低密度　ズーム 12mm



低密度　ズーム 10mm

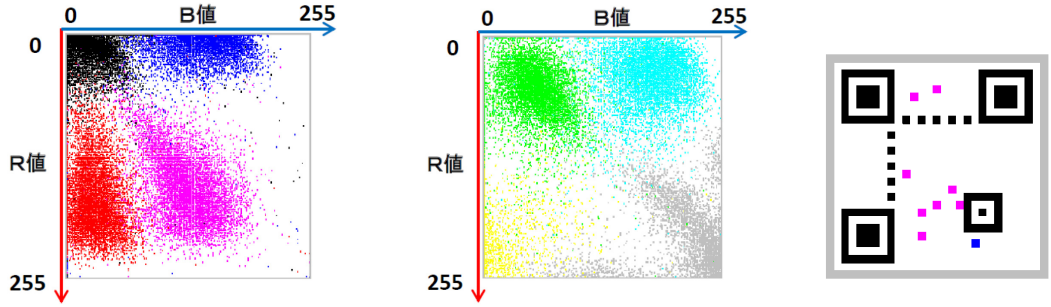
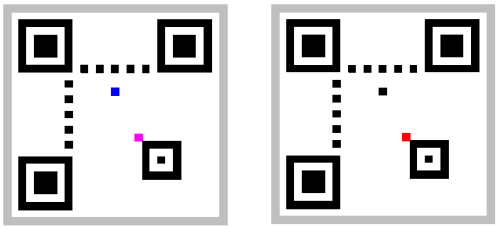


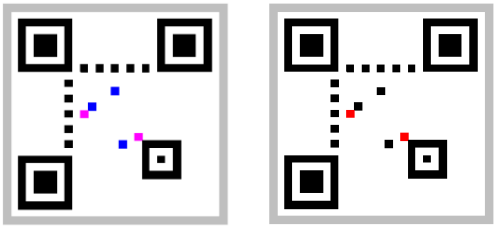
図 3-11 サンプリング値の分布（左図，中央）と誤り位置の分布（右図）

次に，誤り位置の分布で示した色が誤識別した色の事例を図 3-9 に示す．各コードサイズについて，左側が元の色，右側が誤識別した色を示す．例えば，低密度のコードサイズが 24mm の場合には，誤識別したセルは 2 か所であり，青を黒に，紫を赤に誤識別している．

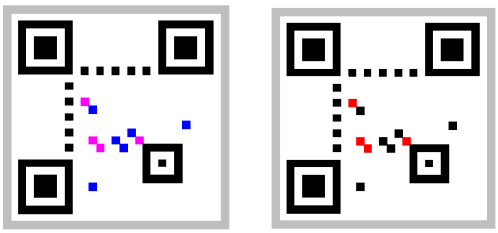
低密度 24mm



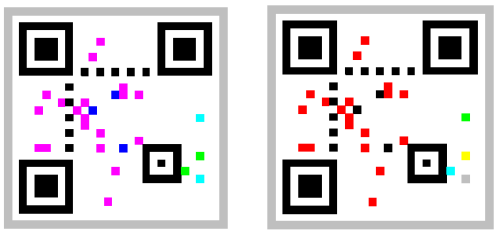
低密度 20mm



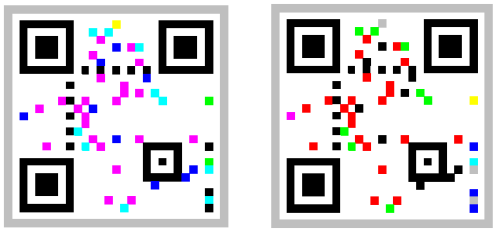
低密度 16mm



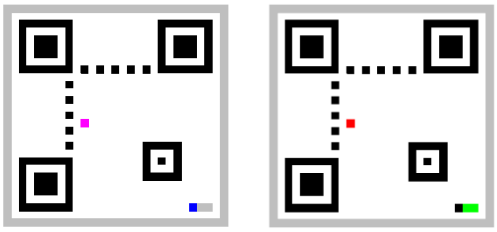
低密度 12mm



低密度　10mm



低密度　ズーム 12mm



低密度　ズーム 10mm

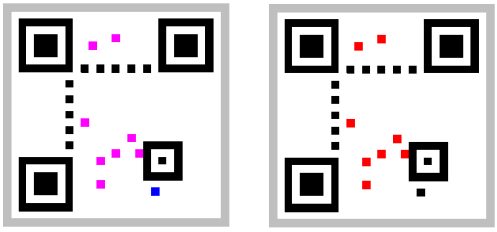


図 3-12　低密度構成の誤識別色の対照（左側　元の色，右側　誤識別色）

④検証結果の検討

Ａ．サンプリング色の分布

上記の図 3-11 において，コードサイズ 40㎜ と 30㎜ の場合には，誤識別は発生していない．この場合の各色の分布を見ると，他の色の分からほぼ完全に分離されている．それに対して，コードサイズ 24㎜ では各色の分布の重なりが発生していることが分かる．コードサイズ 20㎜ 以下では，さらに各色の分布の重なり領域は拡大しており，コードサイズが小さいほど重なり領域は大きい．

Ｂ．誤り分布と誤り色

誤りセルは，ほぼ一様に分布しており，偏りは見られない．それに対して，誤り色には偏りがある．これは，サンプリング色の分布の重なりの状態が各色で異なるためである．

(3) コードレベル復号シミューレーション

二次元コードでは，誤り訂正機能が具備しており，定められた誤り率以下であれば，誤り訂正が可能であり，正しく復号可能である．設定されている誤り訂正レベルでの誤り訂正数を表 3-6 に示す．この誤り訂正数以下であれば，コードレベルで正しく読取が可能である．すなわち，検証に用いた型番では，総データコード語数が，44 個である．誤り訂正レベルが，L，M，Q，H について，誤りのあるデータコード語数が，それぞれ 4 個，8 個，11 個，14 個以下であれば，すべての誤りを訂正し，コードレベルで正しく読取が可能である．

表 3-6　誤り訂正レベルによる誤り訂正数[1]

誤り訂正レベル	総コード語数	データコード語数	誤り訂正コード語数	誤り訂正数
L	44	34	10	4
M	44	28	16	8
Q	44	22	22	11
H	44	16	28	14

図 3-13 に，各セルがどのデータコード語に属するかを示す．白黒領域は固定部，黄色領域は管理部，緑色領域は未使用部である．

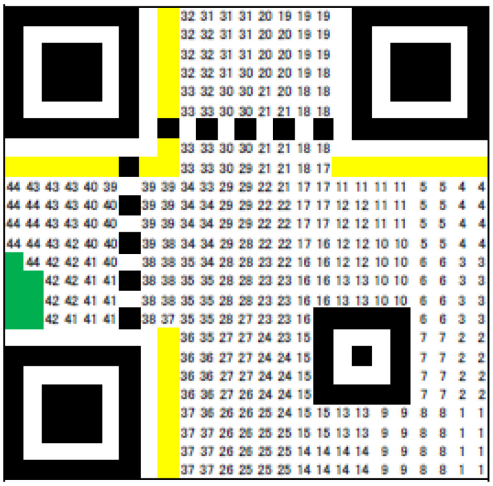
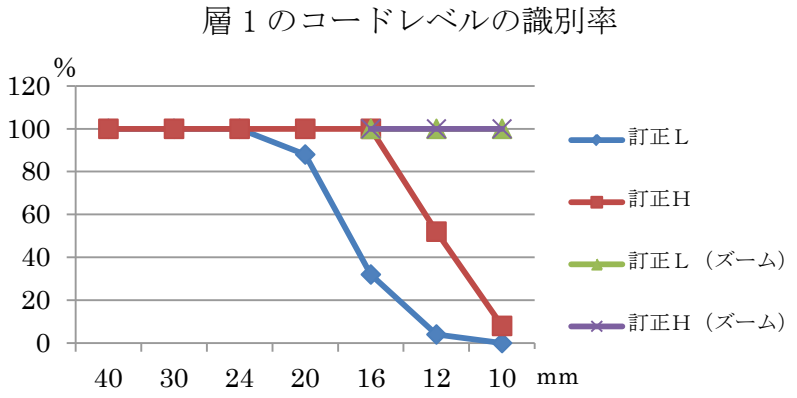


図 3-13　各セルの用途と所属するコード語番号

図 3-10 のセル周辺部の色の識別誤りを，復号後の層 1 と層 2 の二つの白黒の二次元コードの誤りに展開した．そして，それらの誤りセルがどのデータコード語に属するかを計測し，誤りセルの存在するコード語数をカウントした．この誤りコード語数と表 3-6 に示す各誤り訂正レベルの訂正可能な数と比較し，読取り可能性をシュミレーションした層 1 及び層 2 のコードレベルの識別率を，図 3-14 に示す．　層 1 と層 2 は，表 3-1 の符号化データの第 1 及び第 2 ビットで構成される仮想的な白黒の二次元コードである．



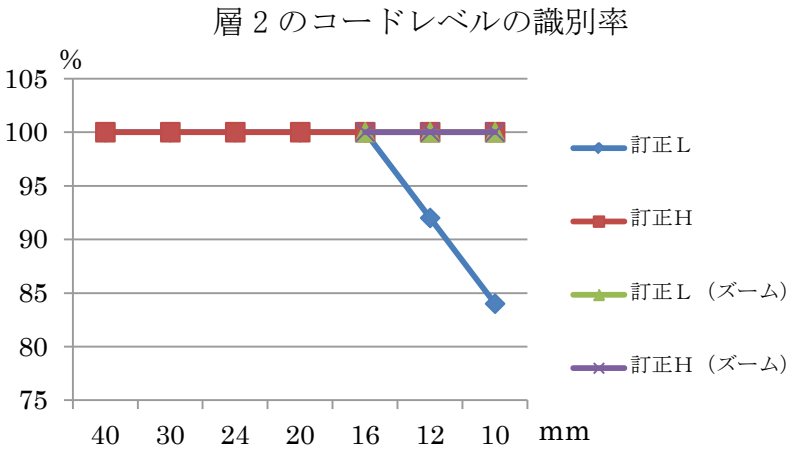


図 3-14　コードレベルの識別率

・シミュレーション結果の検討

図 3-14 に示す層 1 と層 2 の識別率に差がでるのは, 識別した誤り色によって, 層 1 と層 2 に及ぼす影響が異なるからである. 例えば, 白（符号化データが 00）を黄色（01）や青（10）と誤識別すると，それぞれ層 2，層 1 のみが誤り，層 1 と層 2 は正しい結果となる．また，緑（11）と誤識別すると層 1 と層 2 の両方が誤る.

図 3-14 の結果から，誤り訂正レベルが M, Q, H レベルでは 16mm，L レベルでは 20mm のコードサイズまで読取可能であることが判る．これはセル幅が 0.64 及び 0.8mm であり, 実際に白黒の二次元コードで用いられているセル幅の 1.5 倍程度である.

そこで，本論文で提案する構造のカラー二次元コードは，現状レベルの識別能力においても，若干コードサイズが大きくなるものの，コードサイズが 20mm で全ての誤り訂正レベルにおいて，100%の読取が可能であり，実用性があると判断できる.

また，RS 符号を用いた誤り訂正は，ブロック誤り訂正方式であり，データコード語単位の訂正となるので，誤りが特定の領域に集中した場合には，効率的に訂正することが可能である．それに対して，誤りが広く分散した場合には，訂正効率が低くなる.

3.3　高密度方式カラー二次元コード

この節では，高密度方式のカラー二次元コードについて検討する．高密度方式のカラー二次元コードは，前節で述べた低密度方式のカラー二次元コードのセル構造を拡張して，QR コードとの互換性を維持したまま低密度方式よりもさらに大容量化したものである．

3.3.1　セルの構造

既存の二次元コードとの互換性を維持しつつ，追加領域を追加するために，二次元コードの基本単位であるセルの多値化を行う必要がある．多値化の手法として，多色化と多領域化が知られている．多領域化は，セルを複数の領域に分割し，それぞれに独立した情報を与える方式である．

そこで，互換性と秘匿化を目的とする大容量化のために，多色化と多領域化を併用し，3.2.1 項で述べた低密度方式では，図 3-15 右側に示すセルの構造を検討した．この構造は，互換性とセルの多値化を同時に実現可能である．

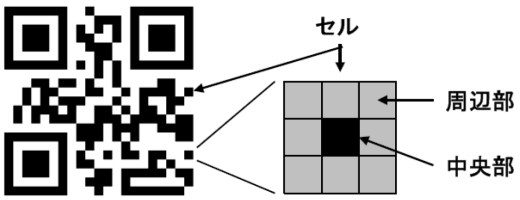


図 3-15　QR コードとセルの分割

(1) 低密度構成と高密度構成の差異

図 3-13 右側は，セルを 9 個の同一面積の正方形の小領域（サブセル）に分割する構造を示している．そして，中央部を互換領域に，周辺部を新規の追加領域に割当てる．中央部は，既存の読取装置で読取が容易になるように白色または黒色とする．周辺部は，大容量化のためにカラー色とする．

低密度方式では，周辺部を単一の符号化単位とする図 3-16 左図に示す構成としていた．それに対して高密度方式では，周辺部を構成する 8 個のサブセルを符号化単位とする図 3-16 右図に示す構成とする．

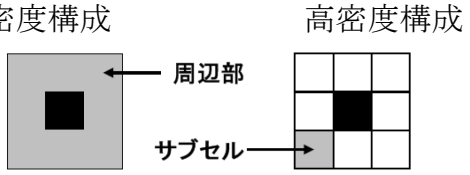


図 3-16　符号化単位

(2) 互換性の実現

既存のスマートフォンの二次元コードの読取りソフトウェアは，セルの切り出し後，各セルの中央部の画素の色，すなわち白色か，または黒色かを判別している．そこで，互換部のデータの識別には，周辺部の寄与は小さい．そこで，高密度方式においても，低密度方式と同様に，中央部を互換領域に割り当てることにより，互換性を実現する．

低密度方式では，周辺部のサブセルにはすべて同一の色が割り当てられたが，高密度方式では，各層に収容するデータに従って割り当てる色がサブセル毎に異なる．

(3) セルの多色化

ここでは，8 色を用いた場合について述べる．用いる色は，次のようにして選択した．

3.3.3 項で述べるように，低密度方式と同様に，距離尺度として RGB 値間のユークリッド距離を用いる．この距離尺度では，RGB の三次元空間で相互に最も離れた色セットが識別が最も容易となる．そこで，相互に最も離れた位置は RGB 空間の立方体の端部であり，当該位置にある色を選択する．

表 3-7　カラー8 色の選択と符合化データ

色群	色コード	RGB			輝度	色	符号化データ
		R	G	B			
白グループ	000	255	255	255	1		00
	001	255	255	0	0.93		01
	010	0	255	255	0.79		10
	011	0	255	0	0.72		11
黒グループ	100	255	0	255	0.28		00
	101	255	0	0	0.21		01
	110	0	0	255	0.07		10
	111	0	0	0	0		11

選択した各色の RGB の具体値を表 3-7 に示す．この表 3-7 は，低密度方式の場合の表 3-1 と同じである．

3.3.2　符号化

(1) 符号化原理

高密度構成におけるサブセルは，セル中央部サブセル色によって，白グループまたは黒グループの 4 色によって符号化される．

4 色による符号化では 2 ビットを表現できる．図 3-17 に示すように，特定の位置のサブセルを，二つの同一サイズの仮想的白黒二次元コードの同一位置のサブセルの値を表 3-11 の符号化データに基づき色を選択することにより符号化する．例えば，セル中央部サブセル色が黒であるセルにおいて，サブセルが両方共に白（0）の場合には 00 の 2 ビットを表現し，紫色に符号化される．

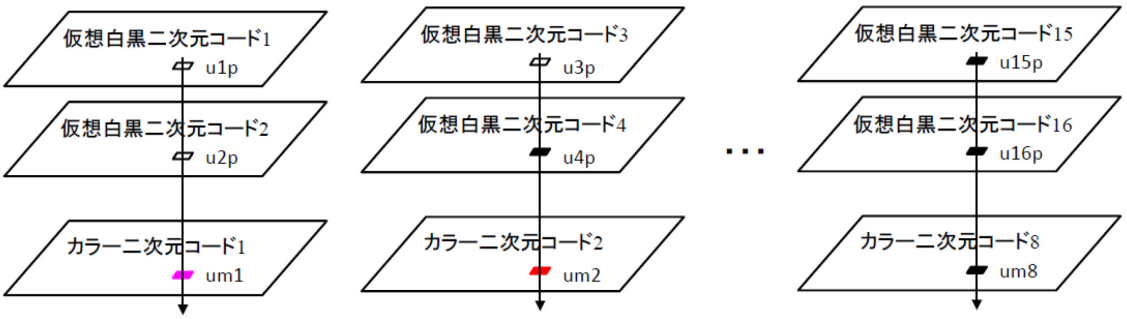


図 3-17　高密度方式の二次元コードの色符号化

ここで，図 3-17 中に記載の u1p～u16p 及び um1～um8 は，3.3.4 項の表 3-8 に示すデータである．

また，サブセルの番号は，図 3-18 に示す位置に割り振った．

1	2	3
4	0	5
6	7	8

図 3-18 サブセル番号に対応するサブセル位置

(2) 仮想的な積層構造

上記のように，選択した 8 色について，白グループと黒グループの色はそれぞれ 4 色であるので，新たに 2 ビットを表現できる．符号化領域が，低密度構成では 1 個，高密度構成では 8 個あるので，セル周辺部はそれぞれ 2 ビット，

16 ビットを表現する．そこで，本論文で提案する構造の二次元コードは，従来と同容量の既存領域と従来の 2 倍または 16 倍の容量の新規領域からなる二次元コードを表現する．

この構成は，一つのセルが 3 ビットまたは 17 ビットを表現しているので，図 3-16 に示すように，白黒の既存の 2 次元コードが 3 層または 17 層重なっているのと同等である．

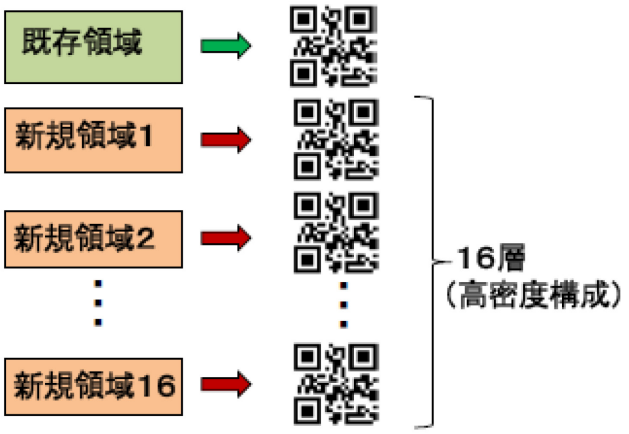


図 3-16 仮想的な積層構造

3.3.3 色識別手法

(1) 比較法

3.2.3 の低密度方式の比較法の項で述べたように，色を識別する手法としては，判別法と比較法がある．判別法は入力された画素の RGB 値から予め定められた色集合から特定の色を判別する手法である．それに対して，比較法は予め定められた色集合の色全てをコードの中の定められた領域に設定しておき，それらの色集合と識別すべきサブセル色と比較することにより，一番近い色を選択する手法である．高密度方式においても，低密度方式と同様に比較法を用いた．

また，パレットについても，図 3-20 に示すように，低密度方式と同じ構成を用いた．

図 3-20 高密度方式のパレット色の設定

(2)識別処理

各サブセルの色を識別する識別処理は，比較対象であるパレット色とサブセル色を準備するデータ抽出処理と比較処理から構成される．

①データ抽出処理

色識別処理で比較する対象は，パレット色とサブセル色である．パレット色はすべてのサブセルの比較に共通である．パレット色は，図 3-21 左図に示すように，パレットを構成するセルを 9 個の領域に分割し，中央部を除く周辺部 8 個の RGB 値の平均値とした．比較はサブセル色とパレット色（各グループ色の 4 色）とで行う．また，パレットは，図 3-20 に示すように，各ファインダーパターンの中に 3 セット設定している．3 セットに含まれる色を独立した色として扱い，仮想的に 12 色として比較し，最も距離の小さいパレット色を選択する．

データ部のサブセルは，図 3-21 右図に示すサブセルの中心の RGB 値とする．

パレット部　　データ部

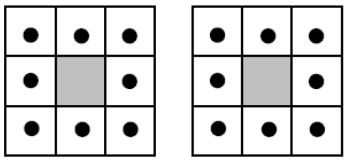


図 3-21　データ抽出位置

②比較処理

比較処理は,データ抽出処理で作成したパレット色 12 色とサブセル色の各 RGB 値を比較する．パレット色の RGB データ Cp を,

$$Cp = (Ri, Gi, Bi) \tag{3-5}$$

と表現する．

ここで，i は選択候補であるパレット色 12 色の指標である．Ri ,Gi，Bi は各パレット色の RGB 値であり，0 から 255 の間の値をとる．

同様に，サブセル色の RGB データ Csc は,

$$Csc = (Rsc, Gsc, Bsc) \tag{3-6}$$

で表現する．ここで，SC はサブセルの番号であり，1 から 8 の値である．そこで，i 番目のパレット色とセル色の RGB 値のユークリッド距離 Di は

$$Di = \sqrt{(Rsc - Ri)2 + (Gsc - Gi)2 + (Bsc - Bi)2} \tag{3-7}$$

となる．

Di が最小値となるパレット色をサブセル色と判定する．

3.3.4　提案アルゴリズム

ここで，本論文の提案の符号化と復号の処理について，高密度構成の場合について述べる．表 3-8 に，高密度構成の二次元コードのデータ構成を示す．

表 3-8　高密度構成の二次元コードのデータ構成

項　目				データ部	訂正部
既存領域（第0層）		保持データ		d0	
		埋め込みデータ		d0f	d0fc
		白黒符号	前*	u0	u0c
			後*	u0p	u0pc
新規領域	第1層	保持データ		d1	
		埋め込みデータ		d1f	d1fc
		仮想白黒符号	前*	u1	u1c
			後*	u1p	u1pc
	第2層	保持データ		d2	d2c
		埋め込みデータ		d2f	d2fc
		仮想白黒符号	前*	u2	u2c
			後*	u2p	u2pc
	重層1	カラー符号		um1	um1c
新規領域	∫				
	第15層	保持データ		d15	d15c
		埋め込みデータ		d15f	d15fc
		仮想白黒符号	前*	u15	u15c
			後*	u15p	u15pc
	第16層	保持データ		d16f	d16fc
		埋め込みデータ		u16	u16c
		仮想白黒符号	前*	*u16*	*u16c*
			後*	*u16p*	*u16pc*
	重層8	カラー符号		um8	um8c

*前、後は、マスク処理の前、後を意味する

(1) 符号化処理

ステップ 1：データの準備

既存領域に収容するデータ d0 及び新規領域の各層に収容するデータ d1..d16, からなる収容データ D = (d0, d1..d16)を準備する.

ステップ 2：各層の白黒二次元コード化

各層の収容データ D = (d0, d1..d16)から RS 符号のデータコード語を構成し, 誤り訂正データコード語を生成して二次元コードを作成し, 白黒データ U = (u0, u1..u16)を得る.

ステップ 3：マスク処理

ステップ 2 で得られた白黒データ U= (u0, u1..u16)について, 与えられた共通秘匿パターンで排他的論理和演算を行い, 白黒データ U = (u0, *u1..u16*)を得る.

ステップ 4：可変領域のセル色の決定

新規領域の各セルの白黒データ u0 に基づき, 表 3-7 の白グループまたは黒グループの符号化データを用いて, 新規領域の各セルの白黒データ U = (*u1..u16*)を符号化し, 周辺部の 8 個のサブセルの色を決定する.

ステップ 5：固定領域のセル色の決定

パレット色を定められたパレット部に設定する. ファインダーパターンなどの固定領域は黒または白に設定する.

(2) 復号処理

ステップ 1：画像入力と画像抽出

撮像装置によって, 二次元コードを含む画像を撮像し, 二次元コードに含まれるファインダーパターンを基に二次元コードを検出し, 二次元コードの画像を抽出する.

ステップ 2：互換部の識別

撮像した二次元コードを白黒の二次元コードとして識別し, 既存領域のサブセルが白か黒のデータ u0 を得る.

ステップ 3：パレット色の抽出

ステップ 2 で切り出したセルについて, パレット色が格納されているセルから, パレット色のデータを取得する.

ステップ 4：可変領域のセル色の識別

二次元コードの可変領域のサブセルについて，12 個のパレット色との距離を計算し，最小の色を当該サブセルの色として選択する．

ステップ 5：各層の白黒二次元コードに復号

新規領域について，各セルの互換部の白または黒の色に従い符号化テーブルによって復号し，二次元コードの白黒データ U=(u0,*u1..u16*)を得る．

ステップ 6：マスク解除処理

共通秘匿パターンで排他的論理和演算を行い秘匿の復号をして,白黒データ U = (u0, u1..u16)を得る．

ステップ 7：白黒二次元コードの復号

ステップ 4 で得られた二次元コードの白黒データ U = (u0, u1..u16)から各層の二次元コードを誤り訂正を経て復号し，各層に収納されたデータ D = (d0,d1..d16)を得る．

3.3.5　評価試験

(1) 互換性評価試験

セルの周辺部にカラー8 色を用いた場合について,スマートフォンを用いて既存領域の読取りの検証を行った．その検証の条件と結果について述べる．

Ａ．試験条件

検証サンプル

検証用の二次元コード及び印刷には，下記を用いた．

二次元コードの種類：	QR コード
型番	： 2（25x25 セル）
誤り訂正	： レベル H
プリンタとインク	： MG6230，純正品（キャノン製）
印刷紙	： マット紙（コクヨ）

検証に用いた収容データは，読取り時に確認が容易な漢字及び英数字をとした．二次元コードに収容するデータを表 3-9 に示す．また，それらのデータを収容する二次元コードの例を図 3-22 に示す．この検証では，色の読取性の検証が目的であるので，新規領域の秘匿化（ランダムマスク処理）は実施しなかった．

表 3-9　高密度構成の収容データ

コード番号	既存領域	新規領域
1	カラー2次元	012345678901234567890123456789..... 01234567
2	カラー2次元	ABCDEFGHIJKLMNOPQRSTUVWXabcdef.... defghijklmnopqrstuvwxyz
3	ABCDEFGHIJKLM	012345678901234567890123456789..... 01234567
4	0123456789ABC	ABCDEFGHIJKLMNOPQRSTUVWXabcdef.... defghijklmnopqrstuvwxyz
5	吾輩は猫であ	吾輩は猫である。名前はまだ無い。どこで生.....しかもあとで聞くとそれは書生と

高密度コード 5

図 3-22　検証に用いた二次元コードの例

B．読取条件

読取りは，下記の条件で実施した．

スマートフォン　　：GALAXY Note 2　(SAMSUNG 製)

　　：IPhone5S　(Apple 製)

読取りソフトウェア　：表 3-10 の中に示す

照明　　：白色蛍光灯

二次元コードとの距離　：焦点の合う最短距離

表 3-9 の 5 個のカラー二次元コードについて，各二次元コードのサイズの画像を印刷し，各コードサイズについて各 10 回読み取りを行った．

C．検証結果

検証試験の結果を表 3-10 に示す．この結果について，検討する．

表 3-10 互換性検証結果

			読取り率(%)						
コードサイズ (mm)			12	10	8	6	4.8	4	3.2
セルサイズ (mm)			0.48	0.4	0.32	0.24	0.2	0.16	0.12
アンドロイド	QRコードスキャナ	低密度	100	100	100	100	24	0	0
		高密度	100	100	100	100	76	34	0
		白黒	100	100	100	100	100	100	0
	Code Scanner	低密度	100	100	100	100	60	0	0
		高密度	100	100	100	100	90	58	0
		白黒	100	100	100	100	100	100	0
アイフォン	QRdeCode	低密度	100	100	58	0	0	0	0
		高密度	100	100	100	14	0	0	0
		白黒	100	100	100	100	60	0	0
	ICONIT	低密度	100	100	100	0	0	0	0
		高密度	100	100	100	100	100	0	0
		白黒	100	100	100	100	100	0	0

コードサイズが 10mm 以上の場合には，全てのカラーコード及び白黒コードで読取率が 100%であった．また，3.2mm 以下の場合は，全てのコードについて，読取率が 0%であった．アンドロイド OS (NOTE2)の読取ソフトウェアを用いた場合，若干白黒コードのほうが読取率が高い．しかし，大差なく，ほぼ互換性があると言える．一方，アイフォン上の読取ソフトウェアを用いた場合，小さなセルサイズでの白黒コードそのものの読取率が低い．また，カラーコードとの読取率の差が，アンドロイド系よりも大きい．

現在，実用されている白黒コードの多くは，セルサイズが 0.4mm（バージョン 2 では，コードサイズが 10mm）以上である．このサイズの場合には，カラーコード，白黒コードのすべてが 100%の読取率であるので，試験した全ての読取ソフトウェアで実用的に互換性があると言える．

(2) サブセルレベル識別性評価試験

セル周辺部のサブセルの識別性の検証を行った．その検証の条件と結果について述べる．

A. 試験条件

検証サンプル

識別性の検証にも，表 3-9，図 3-22 に示す互換性評価試験で用いたコードサンプルを用いた．

読取条件

読取りは，下記の条件で実施した．

スマートフォン	：	GALAXY Note 2 （SAMSUNG 製）
照明	：	白色蛍光灯
二次元コードとの距離	：	55mm に固定
焦点合わせ	：	スマートフォンによる自動焦点

B．検証方法

カラー部の識別は，スマートフォンでの処理とパソコンでの処理の 2 ステップで行った．処理内容は，低密度の場合と同様である．高密度の場合には，8 個のサブセルについて処理を行っている．

スマートフォン処理

スマートフォンでカラー二次元コードを撮像し，従来の白黒の二次元コードとして，誤り訂正を含めて識別する．この処理に伴って，各サブセルを切り出し，各サンプリング値の表を作成する．この表に含まれるのは，各サブセルの中心の各 RGB 値，パレットの 24 点の RGB 値及び誤り訂正後の各セルの白または黒の区別である．

パソコン処理

スマートフォンで作成した上記の表をパソコンに転送する．表のデータをエクセル上の VBA でデータ抽出処理での平均化処理及び比較処理を行い，色の識別処理を行った．識別率は，各セルの本来の色との比較により算出した．

C．検証結果

サブセルレベル

ここでは，低密度構成の場合と同様に，個々のサブセルレベルでの誤り率を評価基準として評価する．

読取検証は,表 3-9 のコード 5 について行った．また，コードサイズが小さい場合には，ズーム機能を用いて拡大した画像について識別を別途行った．倍率は，それぞれ 2.3 倍(20mm)，2.9 倍(16mm),3.9 倍(12mm)，4.3 倍(10mm)である．

コード復号に直接関与するのは，データコード語領域である．ファインダーパターン，タイミングパターン及びアライメントパターンは，白色または黒色に固定されており，それらの識別は，カラー色の識別には当たらない．そこで，データコード語領域のサブセルを対象にして，識別率を計測した．

高密度構成の識別結果を図 3-23 に示す．

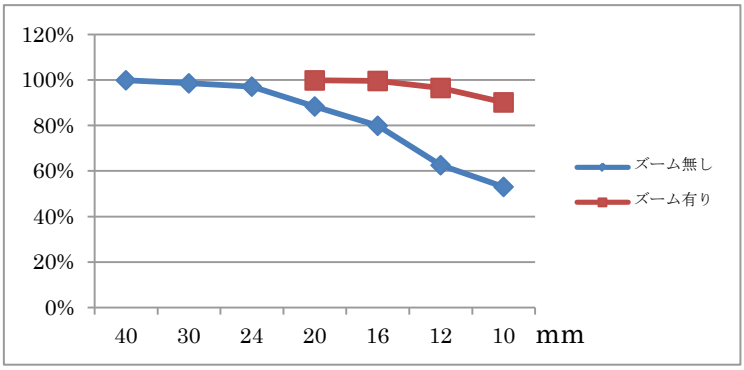


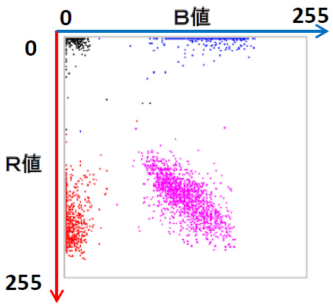
図 3-23　高密度構成の識別検証結果

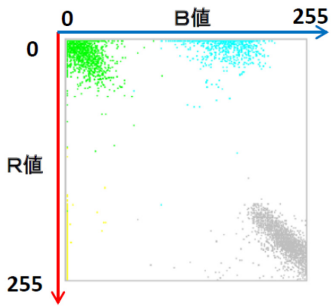
コードサイズが 24mm までは，ほぼ 100%の識別率であるが，20mm よりも小さくなると識別率が低下してくる．ズーム機能を用いると，低密度構成と同様に，識別率は大きく改善し 20mm, 16mm でほぼ 100%の識別率に回復する．

次に，各色の RGB 値の R と B の値の分布図を図 3-24 に示す．この図は，読み取り対象の 5 種類の二次元コードについて，5 回実施した読取のすべての計測値をプロットした．

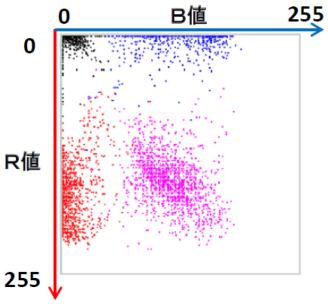
高密度　40mm

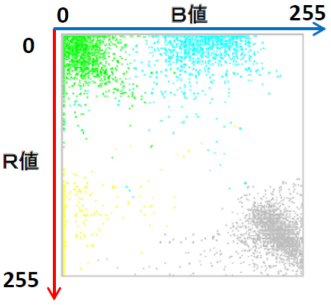
黒グループ色の分布　　白グループ色の分布　　誤りの分布



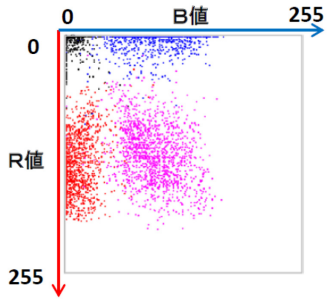


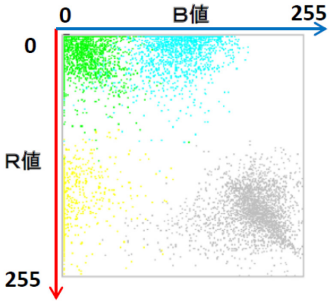
高密度　30mm



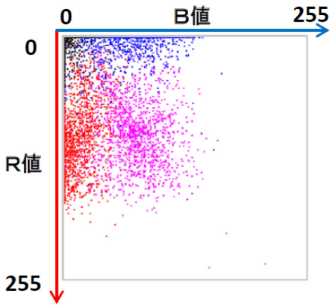


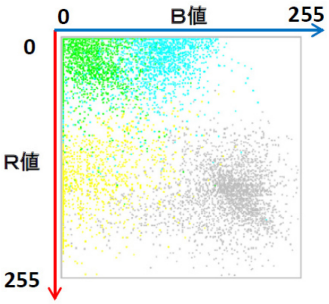
高密度　24mm



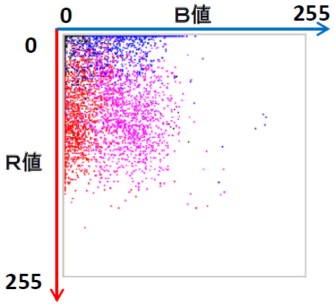


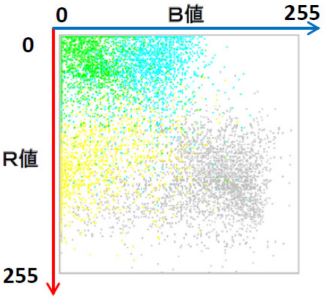
高密度　20mm



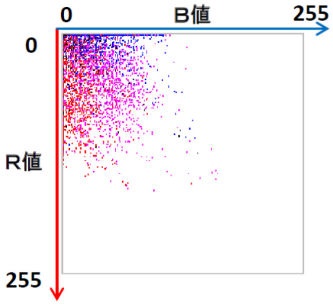


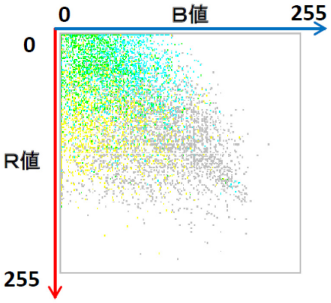
高密度　16mm



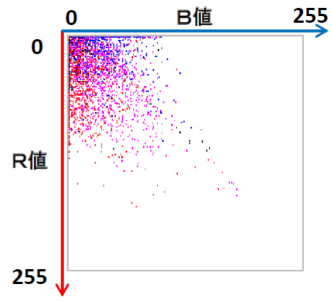


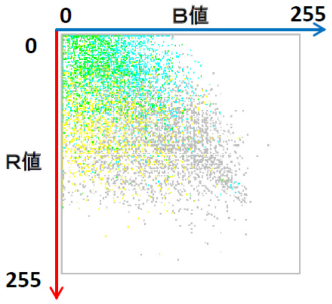
高密度　12mm



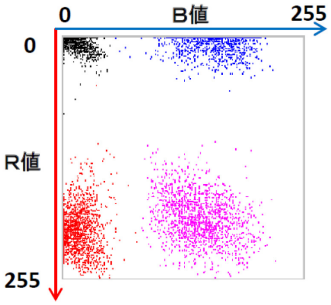


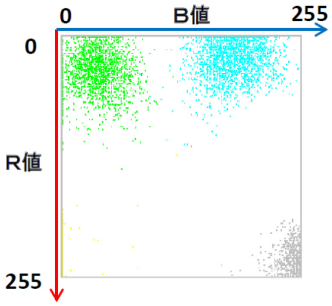
高密度　10mm

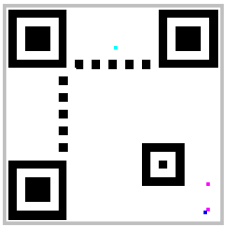




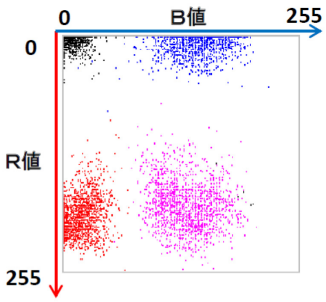
高密度　ズーム 20mm

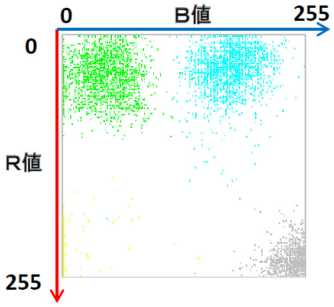


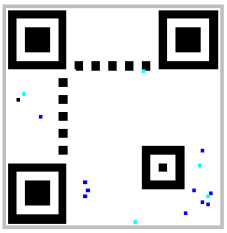




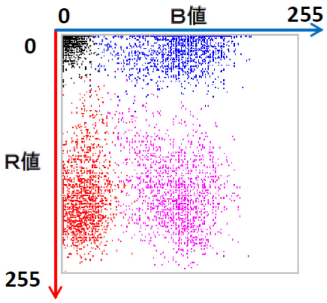
高密度　ズーム 16mm

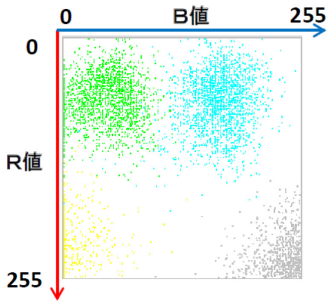






高密度　ズーム 12mm





高密度　ズーム 10mm

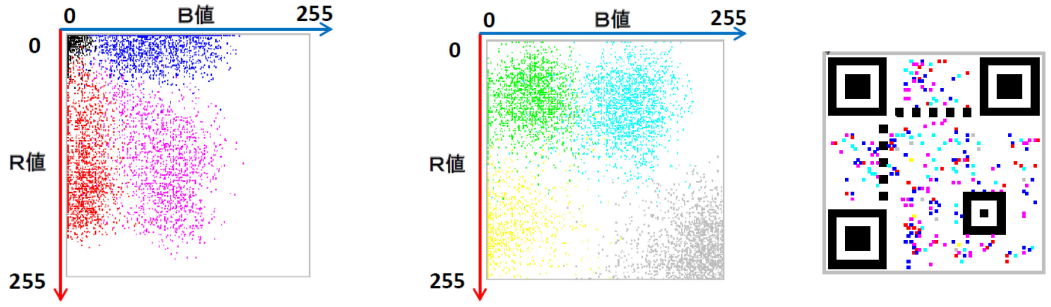
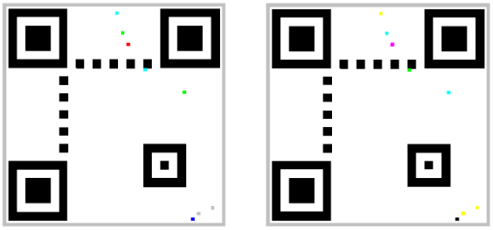


図 3-24　高密度構成のサンプリング色の分布

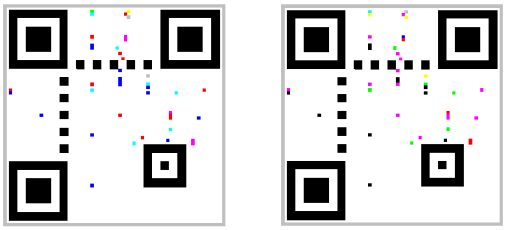
次に，誤り位置の分布で示した色が誤識別した色の事例を図 3-25 に示す．高密度方式では，サブセル単位で独立して符号化されているので，誤識別もサブセル単位で発生する．そこで，セルの中の該当するサブセルの位置を示す．

各コードサイズについて，左側に元の色，右側に誤識別した色を示す．例えば，高密度のコードサイズが 40mm の場合には，誤識別したサブセルは 8 か所であり，上部の 3 箇所では，青緑を黄に，緑を青緑，赤を紫に誤識別している．

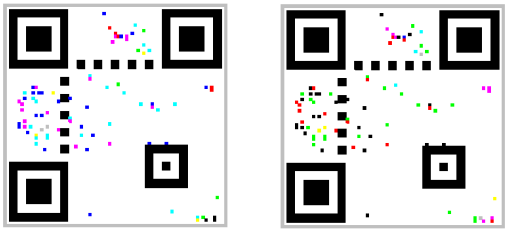
高密度　40mm



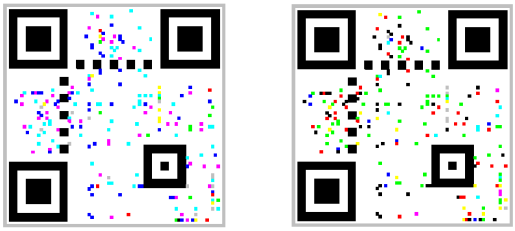
高密度　30mm



高密度　24mm



高密度　20mm



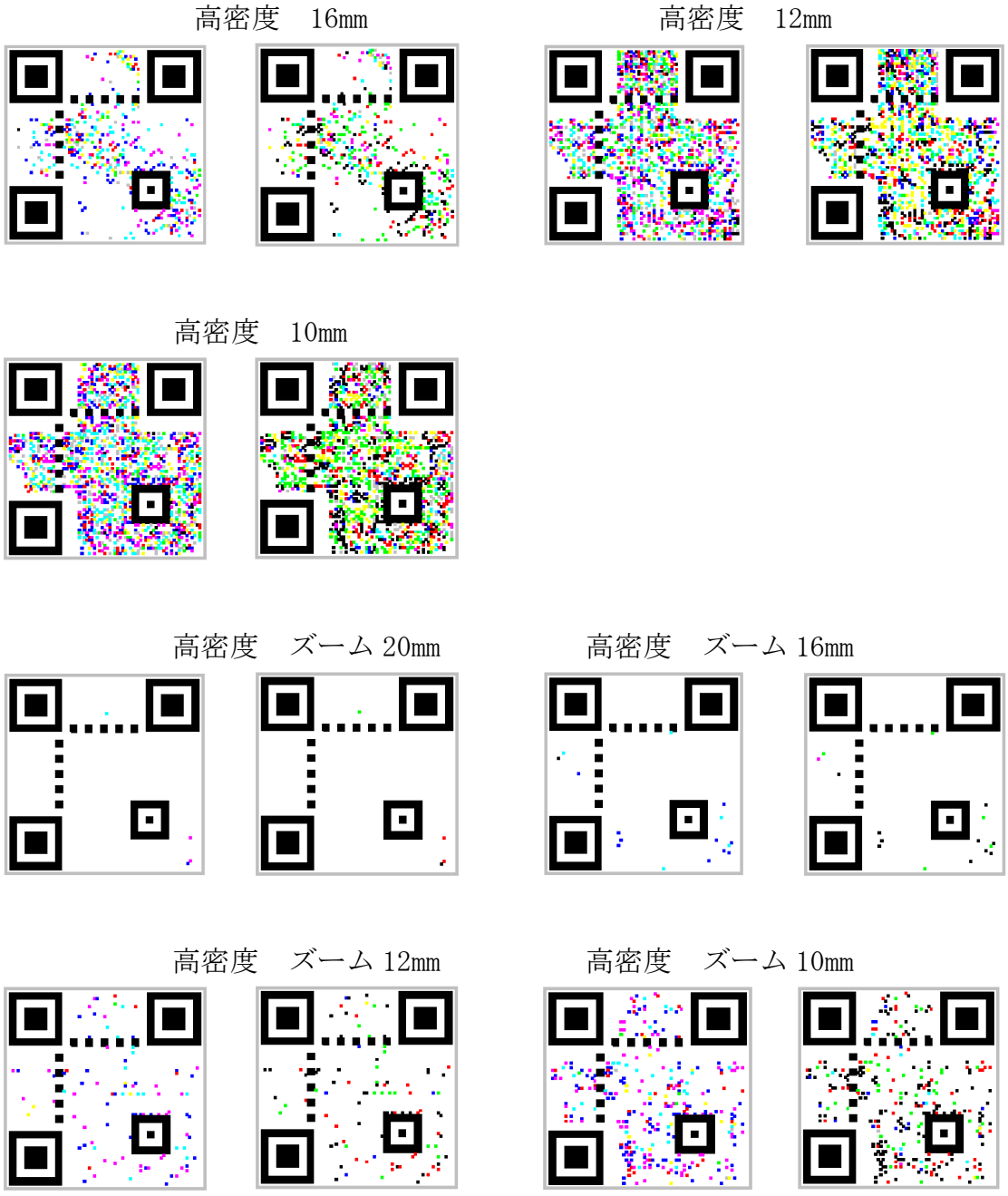


図 3-25　高密度構成の誤識別色の対照（左側:元の色，右側:誤識別色）

20mm のコードサイズの識別率は 88.4%であり，8 個のサブセルについて平均 327.4 個の誤りが発生している．それに対して，ズームを用いた場合では，識別率は 99.8%であり，誤りサブセル数が平均 5.4 個に減少し，大幅な改善となっている．スマートフォンのズーム機能は，ディジタルズームであり，同じ画像を

拡大表示しているに過ぎない．従って，図 3-24 に示した RGB 値の縮退は，スマートフォンの OS による画像処理が主な原因であると言える．

D.　高密度化の要素技術

高密度化には，印刷時と読み取り時の要素技術が必要である．ここでは，その要素技術について検討する．

①密度

印刷時の要素技術として印刷の精密度がある．印刷の密度は DPI(Dot Per Inch) で表現される．DPI 値が大きくなると，同じ形状の高密度カラー二次元コードをより小さなサイズで印刷することが可能になり，また同じサイズでより大きな形状を印刷可能になる．

一方，読み取り時の要素技術として撮影画像の画素密度がある．スマートフォンなどでは，1200 万画素の撮像機能を有した製品ある．撮影画像の画素密度は，撮影対象の二次元コード画像の画像全体に対する大きさの比率で決まる．印刷時に高密度で印刷されていても，読み取り時，低画素密度で撮像した場合，印刷された高密度な情報を識別することができない．

従って，印刷と読み取りのバランスのとれた高密度化が必要となる．

②色の再現性

高密度二次元コードのサブセル色の識別は，サンプリングしたサブセル色の RGB 値とパレット色の RGB 値のユークリッド距離を基準にしている．RGB 値で指定した色が正確に印刷されていなければ，RGB 空間が縮小し，他の色との距離が短くなる．そして，サブセル色間の距離が短くなり，正確に撮像されたとしても誤認識の可能性が高まる．例えば，赤は RGB(255,0,0)で指定されるが，それが印刷されて RGB(240,0,0)相当となる場合である．また，撮像時にも，正確に印刷されたサブセル色を再現しなければ，RGB 空間が縮小する．そこで，サブセル色間の距離が短くなり，誤認識の可能性が高まる．従って，高密度カラー二次元コードの識別には，印刷時と撮像時の色の再現性が技術要素となる．

(3) コードレベル復号シミュレーション

二次元コードでは，誤り訂正機能が具備しており，定められた誤り率以下であれば，誤り訂正が可能であり，正しく復号可能である．検証に用いた型番では，総データコード語数が，44 個である．誤り訂正レベルが，L，M，Q，H について，誤りのあるデータコード語数が，それぞれ 4 個，8 個，11 個，14 個以下

であれば，すべての誤りを訂正し，コードレベルで正しく読取が可能である．

図 3-23 に示したサブセルの色の誤識別を，復号後の奇数層と偶数層の二つの白黒の二次元コードの誤りに展開した．そして，それらの誤りセルがどのデータコード語に属するかを判定し，誤りセルの存在するデータコード語数を計測した．この誤りコード語数と各誤り訂正レベルの訂正可能な数と比較し，復号可能性をシュミレーションした．訂正可能を 100，訂正不可能を 0 としてその平均値を計算した．奇数層及び偶数層のコードレベルの識別率を図 3-26 に示す．奇数層と偶数層は，表 3-7 の符号化データの第 1，第 2 ビットで構成される仮想的な白黒二次元コードである．

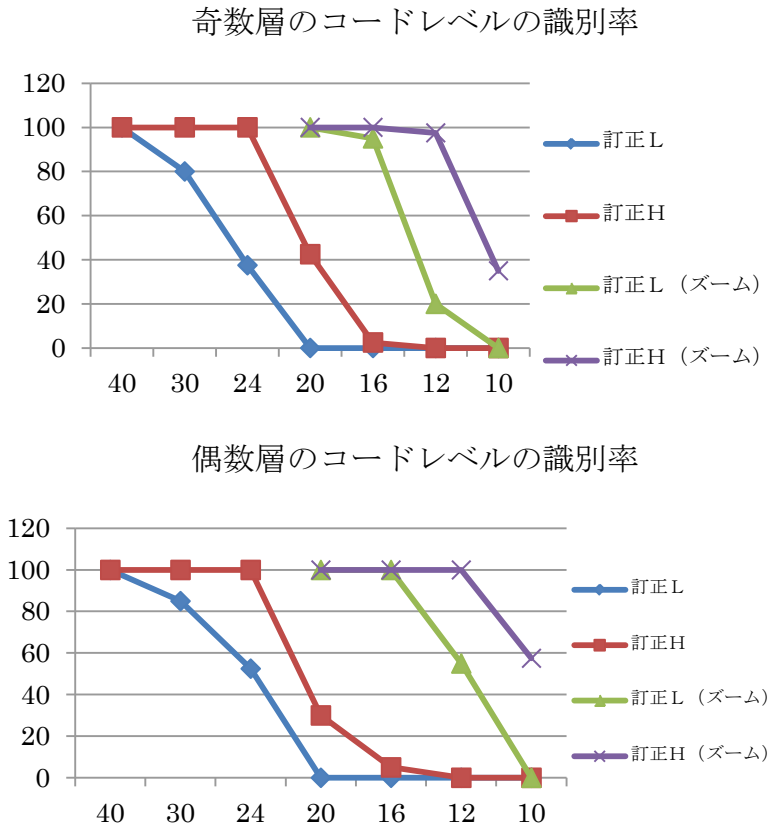


図 3-26　高密度構成のコードレベルの識別率

図 3-26 に示す奇数層と偶数層の識別率に差が出るのは，識別した誤り色によって奇数層と偶数層に及ぼす影響が異なるからである．例えば，白（符号化データが 00）を黄色（01）や青（10）と誤識別すると，それぞれ偶数層，奇数層のみが誤り，奇数層と偶数層は正しい．また，緑（11）と誤識別すると奇数層と偶数層の両方が誤る．

図 3-14，図 3-26 の結果から，低密度構成では誤り訂正レベルが H レベルの場合では 16㎜，L レベルの場合では 24㎜ のコードサイズまで読取可能である．また，ズーム機能を用いれば 10㎜ についても読取可能である．高密度構成では誤り訂正レベルが H レベルの場合では 24㎜，L レベルの場合では 40㎜ のコードサイズまで読取可能である．また，ズーム機能を用いればそれぞれ 12㎜，16㎜ についても読取可能である．

そこで，本論文で提案する構造のカラー二次元コードは，現在用いられている二次元コードのセルサイズが 0.4㎜ （型番 2 ではコードサイズが 10㎜）程度であることから，現状レベルの識別能力においても，低密度構成では実用レベルにあり，高密度構成ではコードサイズが若干大きくなるが，実用性があると判断できる．

第 4 章　ランダムマスク法による秘匿

4.1　はじめに

既存の二次元コードとの互換性を維持する既存領域と，追加のデータ領域である新規領域を有する二次元コードにおいて，新規領域を秘匿化するために，ランダムマスクを用いる手法を提案する．

QR コードで用いられているマスク処理は，予め定められた 8 個のマスクパターンによって，読み取り性向上を目的に行われている．それらと区別するために，ここでは秘匿化を目的とした処理をランダムマスク処理およびその処理方式をランダムマスク法と呼ぶ．

4.2　秘匿領域を有する二次元コードの脅威

情報セキュリティにおける 4 大脅威は，

①盗聴
②なりすまし
③改ざん
④否認

である．

ここでは，秘匿領域を有する二次元コードについて，上記の脅威を基に検討し，秘匿領域を有する二次元コードの脅威を明確にする．

また，二次元コードの発行者は，信頼できると仮定する．

4.2.1　盗聴

盗聴とは，通信中のデータを不正な手段を用いて盗み取ることである．秘匿領域を有する二次元コードでは，秘匿領域に保持するデータの読出しに相当する．従って，情報セキュリティにおける盗聴は，本論文の対象とする秘匿化への脅威である．

4.2.2　なりすまし

なりすましとは，他人の名前や盗用した ID やパスワードを利用し，その人のふりをして，悪意のある行為をすることである．秘匿領域を有する二次元コードでは，秘匿領域を偽造し，正規に製作された二次元コードになりすませることに相当する．従って，情報セキュリティにおけるなりすましは，本論文の対象とする秘匿化への脅威である．

秘匿領域を有する二次元コードの偽造は，次の 3 つの行為からなる．

①偽作

②複製

③複写

偽作は，正規品と同じ二次元コードを新たに作り出すことであり，秘匿領域のデータを正規品と同じルールで作り出すことである．

複製は，正規品を基に，正規品と同じ二次元コードを作ることであり，秘匿領域のデータを基にした正規品と同じものを作ることである．

複写は，正規品を基に，複写機を用いて正規品と同じ二次元コードを作ることである．

偽作，複写，複製の関係を図 4-1 に示す．

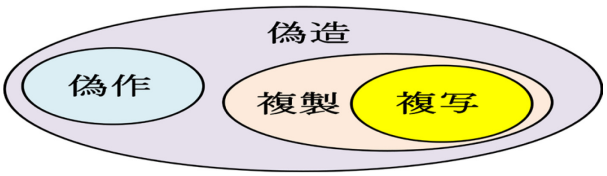


図 4-1 偽造の内容

ここで，複製及び複写は，二次元コードの情報操作では防ぎ得ない行為である．それに対して偽作は，秘匿化手法によって防ぎ得る行為であると言える．

そこで，秘匿領域を有する二次元コードにとってのなりすましは，上記で述べた偽作である．

4.2.3 改ざん

改ざんとは，データの内容を権限のない者が勝手に書き換えることである．秘匿領域を有する二次元コードでは，改ざんに相当する行為は存在しない．

秘匿領域を有する二次元コードは印刷された状態で，製作者から利用者に提示される．印刷された二次元コードを他のデータに書き換えることは不可能である．すなわち，白と黒のセルからなる通常の QR コードにおいて，単に白セルを黒セルに，あるいは黒セルを白セルに置き換えても，誤り訂正の範囲内であれば，正しいデータが読み出される．また，誤り訂正の範囲外であれば，誤りが検出され，正規のデータ以外に復号される可能性は存在しない．

本論文で提案する多色手法では，複数の仮想的な白黒の QR コードの重層構造をなっており，セルの色を変更すると，仮想的な白黒の QR コードの対応するセルの白と黒の反転となり，上記の白黒の QR コードと同じ結果となり，仮想的な白黒の QR コードを正規のデータ以外に書き換える可能性は存在しない．

また，目的のデータを記憶する二次元コードに置き換える場合は，上記の偽作に相当する．そこで，秘匿領域を有する二次元コードでは，改ざんに相当する脅威は存在しない．

4.2.4　否認

否認とは，電子商取引などにおいて，取引に関わり実行した操作を否定する行為のことである．これに相当する秘匿領域を有する二次元コードでは，発行者は信頼できるので，否認に相当する行為は存在しない．

従って，秘匿領域を有する二次元コードでは，否認に相当する脅威は存在しない．

4.3　QR コードの構造

ここでは，二次元コードの事例として，QR コードを取り上げる．QR コードの構造を図 4-2 に示す．QR コードの構造について，第 2 章で詳しく述べたので，ここではランダムマスクによる秘匿化を述べるに際して必要な点について，その概略を説明する．

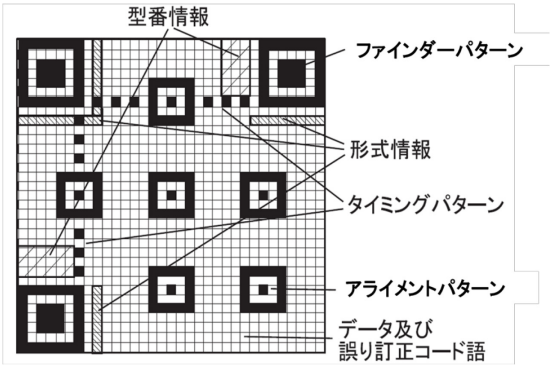


図 4-2　QR コードの構造

QR コードには，記憶するデータによって変化する可変部と変化しない固定部とがある．

①　固定部

固定部には，撮影した画像の中から二次元コードを識別し，その範囲を確定し，回転角や曲がりの補正を行うためのパターンが埋め込まれている．

ファインダーパターンは，三隅に設定されたパターンであり，二次元コード

の存在を識別するためのパターンである．その中心を横切る走査線は，どの方向の走査でも 1:1:3:1:1 の長さの白黒パターンとなる．これにより，位置と回転角を判別する．タイミングパターンは白と黒のセルが交互に配置されており，セルの座標を判別する．アライメントパターンは，飲料容器などの曲面上に印刷された場合の画像の歪みを補正するのに用いる．

② 可変部

可変部には，データを保持し，誤り訂正を可能とするデータコード語部，訂正データコード語部及び管理データ部がある．

管理データ部には，QR コードの大きさ（バージョン）を示す型式情報部と誤り訂正レベルとマスクパターンの情報を示す形式情報部がある．

4.4 マスク処理

QR コードの読出しを確実にするために，白と黒のセルをバランスよく配置され，また，ファインダーパターンに見られる黒白黒黒黒白黒のパターンが出現しないことが望ましい．

マスク処理はデータコード語領域（型式情報及び型番情報を除く）で，データパターンとマスクパターンとで順に XOR 演算による白黒変換を行わせる．

マスクパターンの条件式を表 4-1 に，それぞれの条件式に対応するパターンの例を図 4-3 に示す．ただし，見やすくするために，機能パターン部を併せて示す．

表 4-1 マスクパターンの条件式

マスクパターン番号	条件
000	(x+y)mod 2 = 0
001	X mod 2 = 0
010	Y mod 3 = 0
011	(x+y)mod 3 = 0
100	((x div 2)+(y div 3)) mod 2 = 0
101	(xy) mod 2 + (xy) mod 3 = 0
110	((xy) mod 2 + (xy) mod 3) mod 2 = 0
111	((xy) mod 3 + (x+y) mod 2) mod 2 =0

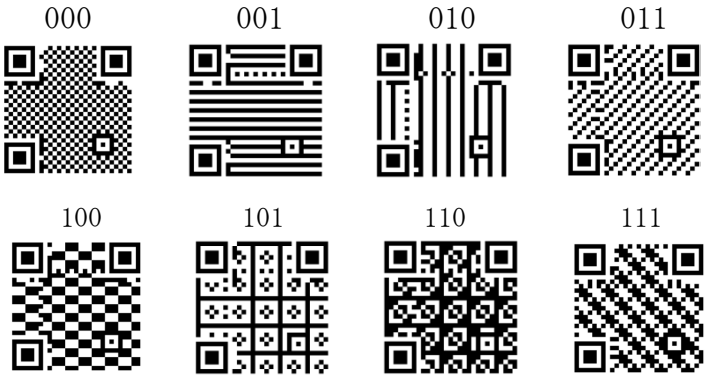


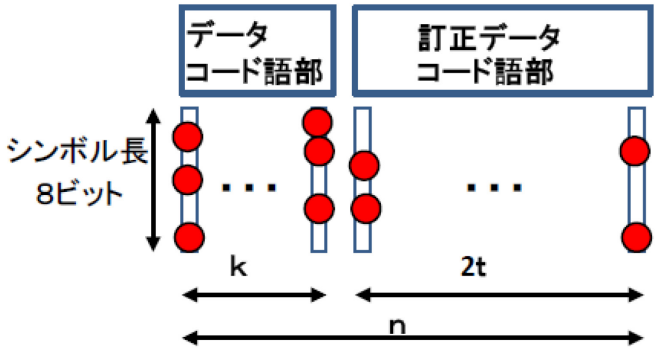
図 4-3　マスクパターンの図示

4.5　ランダムマスクを用いた秘匿化

多値セル型二次元コードの新規領域に記憶するデータを秘匿化する手法として，ランダムマスク法を提案する．

ランダムマスクによる秘匿化は，QR コードの誤り訂正に用いるリードソロモン符号（RS 符号）の特性を用いた秘匿化である．RS 符号は，ブロック型の誤り訂正符号であり，予め定義された誤り訂正能力の範囲内の誤りについては，その誤りを訂正することが可能である．しかし，その能力を超えた誤りについては，誤りを訂正することができない．従って，各データコード語に誤りを発生させる行為を，誤りデータビットの位置を共通鍵とする秘匿化として捉えることができる．

RS 符号において，t 個のデータコード語の誤りまで訂正可能とすると，図 4-4 に示すように，t 個を超えるデータコード語に誤りを発生させれば，訂正できず復号できない．その誤りの発生を 4.3 節で説明したランダムマスクを用いて行うことが可能である．



n: データコード語総数
k: データコード語数
t: 訂正可能データコード語数
●: 誤りビット

図 4-4　ランダムマスクによる誤り発生

ここでは，確実に復号を不可能とする為に，全データコード語に誤りを発生させる．また，データコード語を構成するビットについて，平均的に半数のビットを反転させる．攻撃者からの推定を避けるために，乱数を用いて反転ビットを決定する．そして，すべての新規領域について，乱数によって発生させた値と仮想的二次元コードのセルの値との XOR 演算を行う．

マスクパターンの本来の目的は，データ部のセルの白黒の配置がファインダーパターンと同じ 1:1:3:1:1 とならないようにするなど二次元コードの存在と位置を確実に識別する白黒配置を作成することである．これらの目的は，セルレベルの処理よって達成されるので，互換部であるセルの中央部のサブセルで構成する仮想的な二次元コードに規定のマスクパターンを適用することにより目的を達成できる．セルの周辺部を構成する 16 個の仮想的な二次元コードはどのような白黒のパターンを有していても，カラーに符号化されるときには中央部のサブセルに従って白グループまたは黒グループの色となり，マスクパターンの目的は達成される．従って，新規領域の 16 個の仮想的な二次元コードについて，任意のマスクパターンを選択することができる．

すなわち，互換性を維持するために互換部の QR コードについては通常のマスク処理を行い，セル周辺部から構成される秘匿部である仮想的な QR コードについてはランダムマスク処理を行う．

４．６　偽造検出システムの構成例

ランダムマスク法を用いた秘匿化を活用した医薬品の偽造検出システムの構成例を図 4-5 に示す．

このシステム構成では，印刷会社で医薬品の包装箱やアンプルに貼付するシールを印刷する場合を想定している．包装箱やシールには，ランダムマスク法を用いた秘匿領域を有するカラーQR コードが印刷されている．公開領域には医薬品の品番が記憶され，秘匿領域にはシリアル番号が記憶されている．秘匿化

のために乱数を発生させてランダムマスク値とし，シリアル番号を秘匿化して記憶させて印刷する．同時に，真偽判定サーバに，品番とランダムマスク値を紐づけて記憶する．

真偽判定をするとき，消費者はスマートフォンを用いて，医薬品に貼付されたカラー二次元コードを読み取る．読み取ったデータを真偽判定サーバに送信する．真偽判定サーバは，公開領域から医薬品の品番を復号し，品番と紐付けられたランダムマスク値を読み出す．そして，ランダムマスク値を用いて，秘匿領域の復号を行う．復号して得たデータが，予定していたデータであれば，正規品と判定し，予定していたデータと異なれば偽作（偽造）品と判定する．

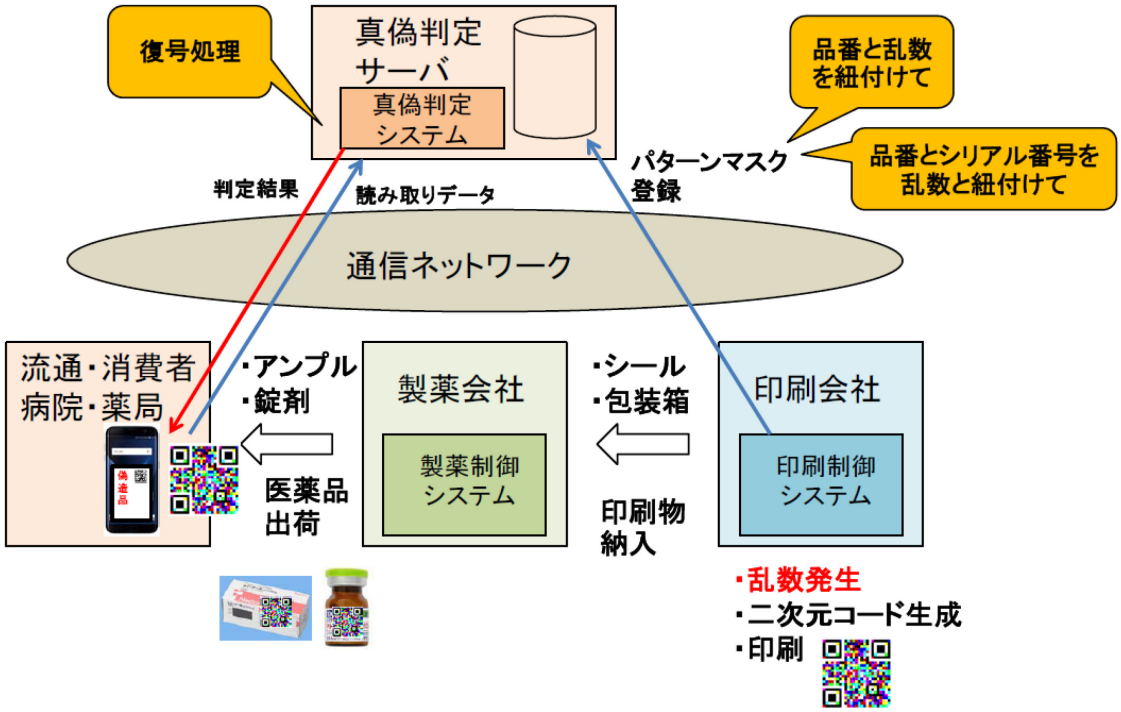


図 4-5 偽造検出システム構成例

4.7　安全性の検討

4.5節で述べたランダムマスクを用いた秘匿化は，RS符号の誤り訂正の特性を用いた秘匿化である．しかし，RS符号は本来誤り訂正の目的で用いられており，復号時のランダムマスク値が正しくなくとも，誤り訂正の機能によって正しく復号される場合がある．そこで，安全性が低下することが懸念されるので，安全性の検討を行う．

4.7.1　訂正可能確率の検討

ここでは，ランダムマスク処理によって生成したデータコード語が，正しく復号される確率を計算する．

(1)ランダムマスク値を選択しない場合

ランダムマスク処理に用いるランダムマスク値は乱数を発生させることにより得る．この値をランダムマスク処理の対象となるデータコード語と無関係に採用する場合について検討する．

ランダムマスク処理によって，各データコード語に誤りを与えるが，誤りのあるデータコード語がｔ個以下である場合には，誤り訂正の能力によって，正しく復号される．その確率を計算する．

データコード語が誤りを含まない確率Psは

$$Ps = (1/2)^8 \qquad (4\text{-}1)$$

である．

n個のデータコード語の中からｍ個を選択する組み合わせの数Nは，

$$N = nCm \qquad (4\text{-}2)$$

そこで，n個のデータコード語の中からｍ個のデータコード語が誤りを含まない確率Pmは，

$$Pm = nCm \times Ps^n \qquad (4\text{-}3)$$

そこで，誤りの無いデータコード語がｍ個以下である確率Pは

$$P = \sum_{k=1}^{m} nCk/2^{8n} \qquad (4\text{-}4)$$

具体的な二次元コードの各型番について計算した結果を表4-2に示す．誤り訂正レベルは最大の訂正能力を有するレベルHである．

この結果により，訂正可能確率は無視できる程度であることが判る．

表 4-2　訂正可能確率

バージョン	データコード語数	訂正データコード語数	訂正可能確率
2	16	28	2.2×10^{-95}
3	26	44	1.9×10^{-151}
4	36	64	3.9×10^{-215}

(2) ランダムマスク値を選択する場合

次に，乱数の発生によって得たランダムマスク値について，全てのデータコード語に誤りを発生させるランダムマスク値を選択する場合について検討する．

ランダムマスク処理を行う場合には，既にランダムマスク処理の対象となるデータコード語は作成済である．そこで，図 4-6 に示すフローチャートのように，全てのデータコード語に誤りを発生させるランダムマスク値を選択することが可能である．すなわち，乱数発生により得たランダムマスクによるランダムマスク処理後，データコード語に誤りのないデータコード語が一つでもあれば，再び乱数を発生させ新たなランダムマスク値を得る．

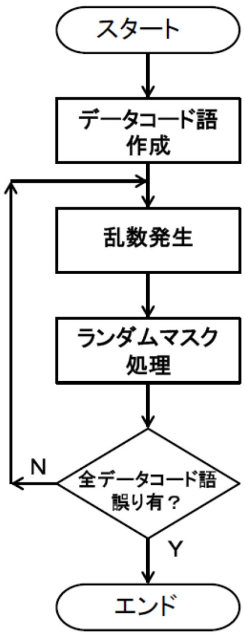


図 4-6　ランダムマスク値の選択処理

このような処理を行えば，ランダムマスク処理を行った結果，全てのデータコード語に誤りがあることを保証することが可能である．

そこで，ランダムマスク値の選択処理を行う場合には，全てのデータコード語に誤りが含まれ，RS 符号による誤り訂正能力の限界を超えるので，訂正可能確率はゼロとなる．

4.7.2　誤り訂正による脆弱性

正しいランダムマスク値を適用しなくとも，誤り訂正機能により復号できる場合がある．そこで，攻撃者によるラウンドロビン攻撃において，一つの復号可能なランダムマスクあたりの場合の数は減少する．これにより，誤り訂正機能によって脆弱性が発生する可能性があるので検討する．

①硬判定の場合

攻撃者が復号の為に用いる復号鍵としてのランダムマスク値は，次の領域に区分することが可能である．

A. RS 符号の復号処理で訂正できる結果となる場合

1. 正しいデータに復号される場合（A1）
2. 正しくないデータに復号される場合（A2）

B. RS 符号の復号処理で訂正できない結果となる場合（B）

これらの三つの場合は，ランダムマスク値の数理空間の中で図示すると図 4-7 となる．

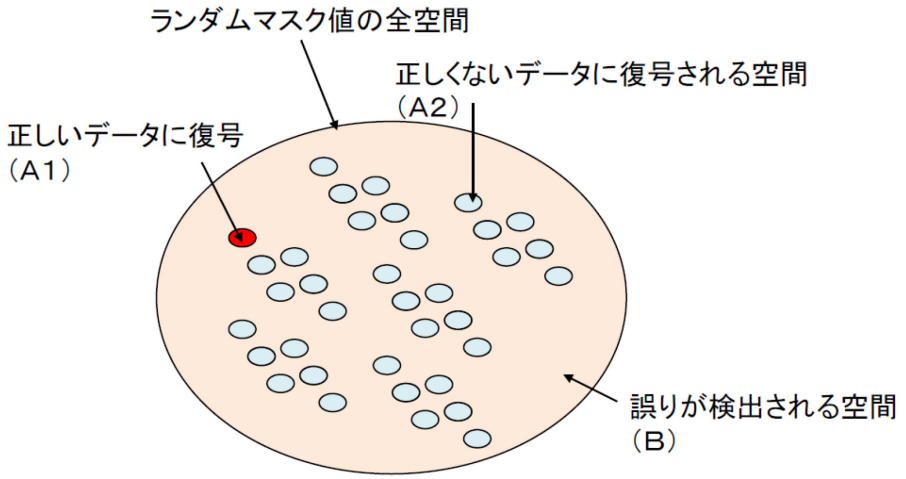


図 4-7 ランダムマスク空間

ここで，上記の三つの場合の数を検討する．それぞれの場合の数を以下のように表現する．

Np:すべての場合の数

NA1: 正しいデータに復号される場合

NA2: 正しくないデータに復号される場合

NB: 訂正できない場合

これらの場合の数には，次の関係が成立する．

$$Np = NA1 + NA2 + NB \qquad (4\text{-}5)$$

１）特殊な場合

ここで，一般的な場合の式を導出するために，特殊な場合について検討する．ここでは，図 4-8 に示す全データコード語数 n が 4，訂正データコード語数が 2 の場合について，検討する．

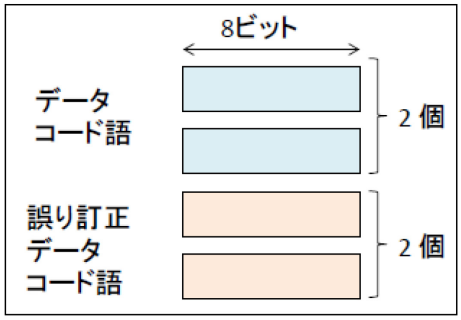


図 4-8 特殊な場合のデータコード語構成

2^{32} の符号空間中の点のうち，符号として選ばれるのは 2^{16} の点である．１つの符号の点について，その周りの訂正可能な点の数は，

$$NA1 = (2^8 - 1) \times {}_4C_1 \qquad (4\text{-}6)$$

従って，ある符号を選んだとき，その点に訂正される（元の符号を含む）店の数は $2^8 \times {}_4C_1$ である．ここで，その符号が誤る全ての場合を考えると，その符号に訂正される以外の $2^{32}-2^8 \times {}_4C_1$ の点に誤れば，誤訂正または誤り検出となる．その中で，誤訂正される点の数，他の符号に訂正される NA2 は

$$NA2 = (2^8 - 1) \times {}_4C_1 \times (2^{16}-1) \qquad (4\text{-}7)$$

となる．NB は，復号処理で誤りが検出される場合であり，すべての場合から上記を除いた場合であるので，

$$NB = 2^{32} - NA1 - NA2 \quad (4\text{-}8)$$

$$= 2^{32} - (2^8-1) \times {}_4C_1 \times 2^{16} \quad (4\text{-}9)$$

となる．

２）一般式

次に，一般的な場合について，検討する．ここで，一般的な場合として，図 4-9 に示す全データコード語数 n が k, 訂正データコード語数が 2t の場合について，検討する．

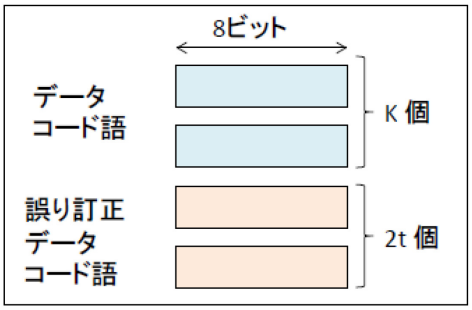


図 4-9 一般的な場合のデータコード語構成

A. t 個のコード語が誤っている場合

誤っているコード語の場合の数は， 誤っているのは，t 個のコード語であるので，（2^6-1）^{t} 通りとなる．コード語は n 個のコード語中任意の t 個のコード語あるので，nCt 通りある．そこで，

$$NA1 = (2^6-1)^t \times nCt \quad (4\text{-}10)$$

となる．

また，訂正可能であるのは，本来のデータ以外のすべてのデータについても同じ場合の数であるので，

$$NA2 = (2^8-1)^t \times nCt \times (2^k-1) \quad (4\text{-}11)$$

となる，

B. 1 個から t 個のコード語が誤っている場合の合計

訂正可能な場合は，1 個から t 個の誤りのあるデータコード語数の場合であるので，これを合計すると，それぞれ以下のようになる．

$$NA1 = \sum_{i=1,t} nCi \times (2^8-1)^i \quad (4\text{-}12)$$

$$NA2 = \sum_{i=1,t} nCi \times (2^8-1)^i \times (2^{8k}-1) \quad (4\text{-}13)$$

QR コードでよく使用されるバージョン 1,2,3 の場合について，NA1,NA2 を数値計算した結果を表 4-3 に示す．

表 4-3　バージョン 1,2,3 の場合の数値計算結果

型番	訂正レベル	RSブロック構成	マスクパターン数	正しい訂正可能数	誤った訂正可能数	
1	L	(26,19,2)	4.1×10^{62}	2.1×10^{07}	1.2×10^{53}	
	M	(26,16,4)	4.1×10^{62}	6.3×10^{13}	2.2×10^{52}	
	Q	(26,13,6)	4.1×10^{62}	6.3×10^{19}	1.3×10^{51}	
	H	(26,9,8)	4.1×10^{62}	2.8×10^{25}	1.3×10^{47}	
2	L	(44,34,4)	9.2×10^{105}	5.7×10^{14}	4.4×10^{96}	
	M	(44,28,8)	9.2×10^{105}	3.2×10^{27}	8.5×10^{94}	
	Q	(44,22,11)	9.2×10^{105}	2.3×10^{36}	2.2×10^{89}	
	H	(44,16,14)	9.2×10^{105}	5.7×10^{44}	1.9×10^{83}	
3	L	(70,55,7)	3.8×10^{168}	8.4×10^{25}	2.4×10^{158}	
	M	(70,44,13)	3.8×10^{168}	9.2×10^{44}	8.4×10^{150}	
	Q	(35,17,9)x2	3.8×10^{168}	3.2×10^{29}	2.8×10^{70}	1ブロックについて評価
	H	(35,13,11)x2	3.8×10^{168}	2.9×10^{40}	5.8×10^{71}	

誤り訂正によって，正しく復号可能なランダムマスクの場合の数は増大するが，誤訂正の場合の数は，それを大きく上回っており，多くの場合に誤訂正する結果となり，誤り訂正による脆弱性はないと判断できる．

②軟判定の場合

軟判定の例として，最尤推定の場合について，検討する．

ここでは，一般的な場合として，図 4-9 に示す全データコード語数 n が k，訂正データコード語数が 2t の場合について，検討する．

最尤推定では，硬判定で復号可能な複数の符号空間の中の符号領域の中で，より近い領域に推定する．これを誤りのあるデータコード語数が Ne の場合について，図 4-10 に示す．

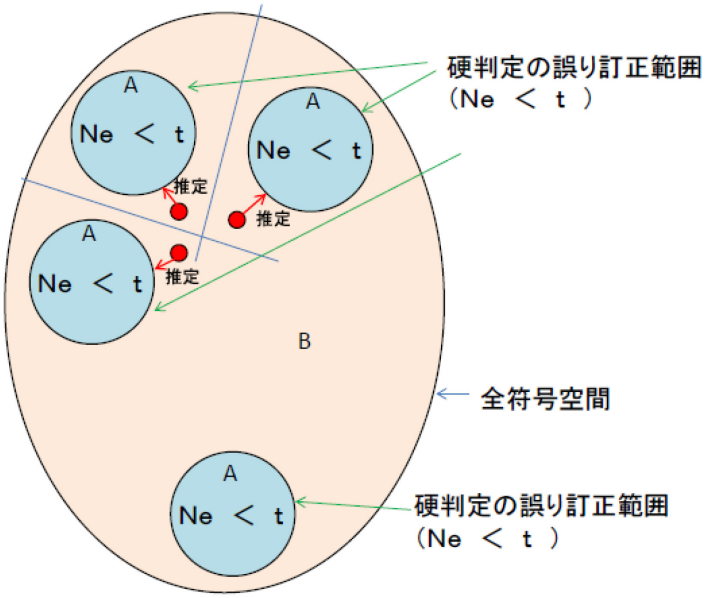


図 4-10　最尤推定における推定

図 4-10 において，データコード語の中で誤りがあるデータコード語数 Ne が訂正可能な誤り数 t よりも少なく，硬判定で訂正可能な範囲（A 領域）を青色で示し，ランダムマスク処理をされたデータコード語の位置を赤色で示す．データコード語の位置によって，より近い A 領域に推定する．

1) ランダムマスク復号処理をしない場合の推定

ここで，ランダムマスク処理によって，すべてのデータコード語に誤りがある場合には，データコード語の位置は正しいデータコード語から遠い位置となる．この状況を図 4-11 に示す．ここで，硬判定で正しく訂正可能な範囲（A1 領域）を青色で示し，誤って訂正する範囲（A2 領域）を紫色で示す．

この場合には，必ず近傍に存在する A2 領域を推定することになるので，正しいデータコード語に復号されることはない．

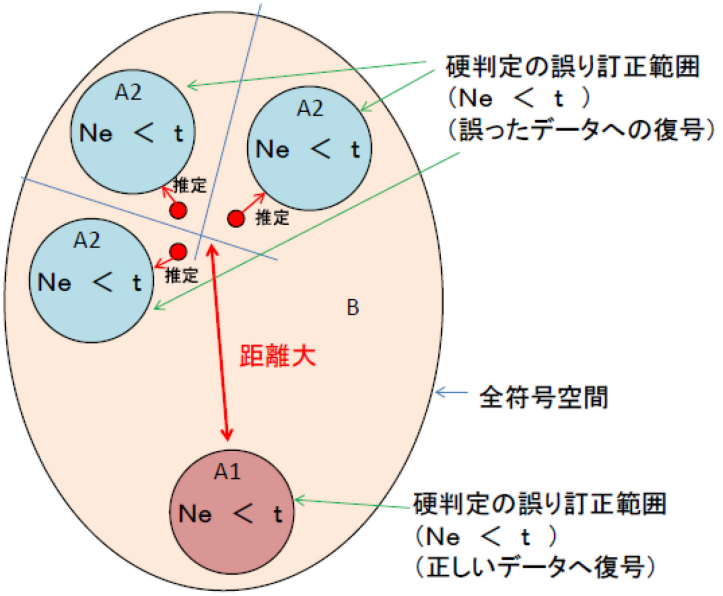


図 4-11 最尤推定における全データコード語に誤りがある場合の推定

2) ランダムマスク復号処理をする場合の推定

ランダムマスク復号処理を行った後のデータコード語の位置は，仮定するランダムマスク値によって，図 4-12 に示すように全符号空間の任意の位置をとることが可能である．この場合においても，正しいデータコード語の近傍には誤って訂正する範囲（A2 領域）は大量に存在しており，正しいデータコード語を推定する確率は，硬判定の場合と同じ程度であると考えられる．

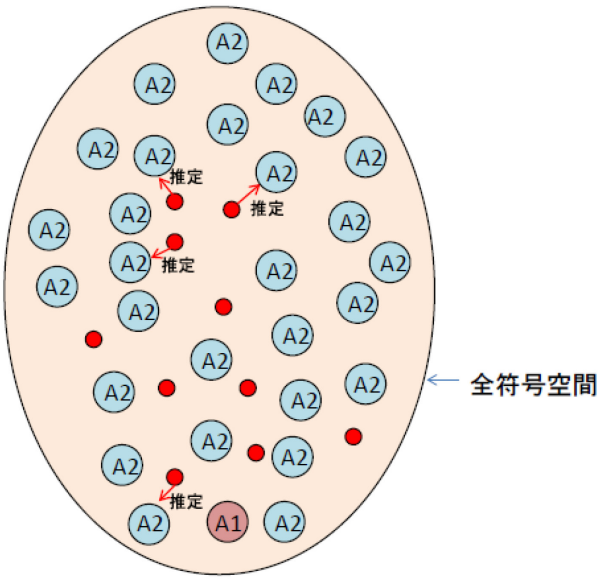


図 4-12 最尤推定におけるランダムマスク復号処理をした場合の推定

データゴード語の長さは8ビットであるので，2^8-1の誤りパターンがある．そこで，データコード語数がnであれば，そのパターン数は$(2^8-1)^n$となる．n=44の場合は全パターンは2^{352}となり，全数検索されても計算量的安全性を有する．

そこで，軟判定においても，誤り訂正による脆弱性はないと判断できる．

第 5 章　多領域分割とアクセス制御

5.1　はじめに

既存の二次元コードとの互換性を維持する既存領域と，追加のデータ領域である新規領域を有する多値セル型二次元コードにおいて，新規領域を複数のデータ領域に分割し，複数のユーザがアクセス権を付与されたデータ領域のみを読み取ることができるアクセス方式の検討を行う．

単に二次元コードに秘匿領域を設定し，その復号鍵を有する端末のみが読み取り可能とする SQRC が提案されている．この方式は，図 5-1 のように，データ領域と読み取り者が 1 対 1 の関係では有効である．

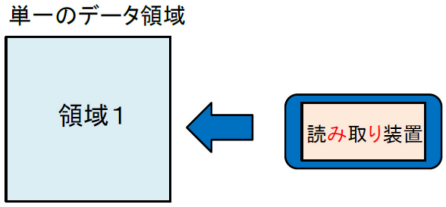


図 5-1　データ領域と読み取り者が 1 対 1 の場合

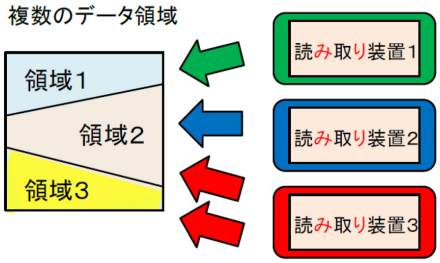


図 5-2　データ領域と読み取り者が N 対 M の場合

5.2　アクセス制御の必要性

一方，二次元コードのデータが複数の領域に区分されており，複数の読み取り者毎に読み取り範囲が異なる図 5-2 に示す場合の対応は想定されていない．この機能が実現できれば二次元コードの活用分野を拡げることができる．そこで，この場合に対応可能なシステムを検討する．

秘匿性のある二次元コードを開発するために，二次元コードの基本要素であるセルを多値化して二次元コードを大容量化し，新たに作り出した領域を秘匿

化する．複数のユーザに対して，二次元コードに収容されている複数の区分されたデータ領域へのアクセス制御を行う．ユーザが複数の異なる区分された領域を読み取るために，複数の復号鍵を用いることなく，一つのパスワードで許されたアクセス領域を読み取り可能とする．

5.3　領域分割

2.4 節で述べたように，多値セル型二次元コードは 17 個（層）の仮想的な白黒の二次元コードから構成される．ここで，互換領域（層）を除く 16 層を用いて秘匿領域を構成する．この構成を表 5-1 に示す．

表 5-1　秘匿領域のデータ構成

<table>
<tr><th colspan="2">領域名</th><th>収容データ</th></tr>
<tr><td colspan="2">管理領域（非秘匿化領域）</td><td>ユーザの秘匿化された
復号キイ、層の割り当て</td></tr>
<tr><td rowspan="4">データ領域
（秘匿化領域）</td><td>データ領域1</td><td rowspan="4">アクセス制御の区分毎の
収容データ</td></tr>
<tr><td>データ領域2</td></tr>
<tr><td>⋮</td></tr>
<tr><td>データ領域n</td></tr>
</table>

秘匿領域は，管理領域とデータ領域に分割される．管理領域はユーザ毎のパスワードに対応するランダムマスク値やデータ領域に対する層の割り当てデータを収容する領域であり，層単位で構成されランダムマスクによる秘匿化を行わない領域である．データ領域はアクセス制御の区分毎に設定されたデータを収容する領域であり，層単位で構成され，ランダムマスクによる秘匿化を行なう領域である．

データ領域は，アクセス制御の区分毎に n 個に分割され，各データ領域を構成する層は，同一の秘匿化鍵で秘匿化される．各データ領域に割り当てられる層は，当該データ領域に収容するデータ量によって自動的に割り当てられ，管理層に記憶される．また，各データ領域の秘匿化に用いるランダムマスク値は乱数によって生成する．

5.4　アクセス制御

5.4.1　複数ユーザへのアクセス権割り当て

m 人のユーザに対して，n 個のデータ領域に対するアクセス権の割り当てを行う．ここでは，一般的な記述の前に，ユーザ数 3，データ領域数 4 の場合のアクセス権の割り当て例を表 5-2 に示す．

表 5-2　各ユーザへのアクセス権の割り当て

データ領域名	割当層	ユーザA	ユーザB	ユーザC
データ領域1	1～4	○		
データ領域2	5～8	○	○	
データ領域3	9～10	○	○	○
データ領域4	11～15			○

この例では，ユーザ A はデータ領域 1,2,3 に，ユーザ B がデータ領域 2,3 に，ユーザ C はデータ領域 3,4 に，それぞれアクセス権が付与されている．そして，表 5-2 の割当層に示された層が，それぞれのデータ領域に割り当てられる．これらの同一のデータ領域に割り当てられた層は同一のランダムマスクによって秘匿化される．

データ領域 n のランダムマスク値を *Pn* とすると，この例では，4 つの乱数によって生成されたランダムマスク値 *P1, P2, P3, P4* が生成され，秘匿化に用いられる．

一般的に，データ領域数 n，ユーザ数 m の場合のアクセス権の割り当て表は，表 5-3 のようになる．

表 5-3　一般的なアクセス権の割り当て

データ領域名	割当層	ユーザ1	・・・	ユーザM
データ領域1	各データ領域のデータ量によって割り当て	・・	・・	・・
データ領域2		・・	・・	・・
⋮		・・	・・	・・
データ領域N		・・	・・	・・

5.4.2　ユーザ毎のパスワード設定

表 5-2 の例の場合，ユーザ A は 3 つのデータ領域にアクセス権が付与されており，それらのデータ領域の 3 つのランダムマスク値 *P1, P2, P3* を知る必要がある．しかし，一つの多値セル型二次元コードについて，複数の復号鍵（ランダムマスク値）を管理するのは煩雑である．そこで，1 人のユーザが多値セル型二次元コードを一つのパスワードでアクセスする方法を検討する．

ユーザが一つのパスワードで複数のランダムマスク値を知得していると同様な処理を可能とする為には，多値セル型二次元コードの中にユーザに付与されたデータ領域のランダムマスク値を記憶している必要がある．また，それらを記憶する層はランダムマスクによって秘匿化されていない必要がある．そして，記憶されるランダムマスク値はそのままの値を記憶している場合，全ての者が読み取り可能であり，秘匿化への復号鍵の役割を果たすことができない．そこで，共通鍵であるパスワードで秘匿化されたランダムマスク値を記憶する．

表 5-4　パスワードと秘匿化ランダムマスク

ユーザ名	パスワード	収容ランダムマスク値	秘匿化ランダムマスクセット
ユーザA	PWa	*P1, P2, P3*	*EPa*
ユーザB	PWb	*P2, P3*	*EPb*
ユーザC	PWc	*P3, P4*	*EPc*

これらを整理すると，表 5-4 のように，ユーザ A はパスワード PWa を付与され，ランダムマスク値（*P1, P2, P3*）をパスワード PWa によって秘匿化し，秘匿化ランダムマスク *EPa* を得て，表 5-1 の管理領域に格納する．管理領域は全ユーザの秘匿化ランダムマスク値 *EPa, EPb, EPc* を収容する．管理領域に割り当てる層の数は *EPm* を収容するに足る層数が割り当てられる．

5.4.3　安全性の検討

各領域のデータは，複数の仮想的二次元コードに分割されて収容されている．データを収容する仮想的二次元コードは，乱数によるランダムマスクで秘匿化されている．乱数によって発生させたランダムマスクは，パスワードによって

秘匿化されて記録されている．従って，パスワードを知らなければ，それぞれの領域でランダムマスクを総当たり方式で復号を試みる必要がある．そこで，ランダムマスクは必要な安全性によって任意の長さを選択できるので，計算量的安全性を有する．

5.4.4　アクセス制御処理のまとめ

アクセス制御処理の全体をまとめる．全体の処理の流れを図 5-3 に示す．ここでは，二つの秘匿領域（領域１，領域２）に対して，三者のユーザ（ユーザ a，ユーザ b，ユーザ c）がアクセスする場合について述べる．ユーザ a，b，c は，それぞれパスワード A，B，C が付与されており，ユーザ a は領域 1，2 に，ユーザ b は領域 1 のみに，ユーザ c は領域 2 のみにアクセス権が与えられているとする．

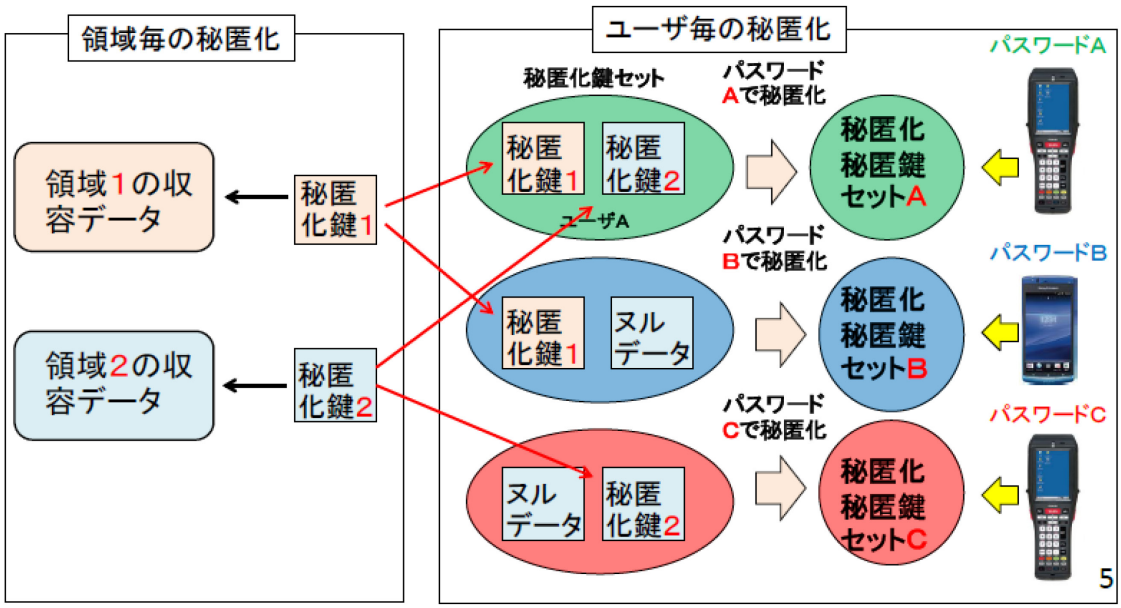


図 5-3　アクセス制御処理の流れ

①領域毎の秘匿化

はじめに，領域毎の秘匿化処理を行う．領域 1 及び領域 2 に収容する秘匿すべきデータついて，それぞれの領域の秘匿化鍵 1 及び秘匿化鍵 2 を用いて秘匿化し，領域 1 及び領域 2 に収容する．

②ユーザ毎の秘匿化

次に，ユーザ毎の秘匿化処理を行う．ユーザにアクセス権が与えられた領域の秘匿化鍵をユーザ毎のパスワードで秘匿化し，秘匿化された秘匿化鍵セットをユーザ毎に設定された秘匿化鍵セット位置に収容する．

例えば，ユーザ a は領域 1 と領域 2 の両方のアクセス権を付与されているので，秘匿化鍵 1,2 をパスワード A で秘匿化し，対応する位置に収容する．一方，ユーザ b は，領域 1 のみのアクセス権を有するので，秘匿化鍵 1 とヌルデータを秘匿化して対応位置に収容する．

③ユーザの秘匿領域へのアクセス

ユーザが秘匿領域にアクセスする場合には，各ユーザに割り当てられた秘匿化鍵セット収容位置から秘匿化鍵セットを読み出し，各ユーザのパスワードによって秘匿化鍵セットを領域毎の秘匿化鍵に復号する．そして，各領域の秘匿化されたデータを読み出し，各領域の秘匿化鍵を用いて復号し，各領域のデータを得る．

ここで，秘匿化鍵がヌルデータである場合には，アクセス権がないとして，その領域の処理は行わない．

5.5　提案アルゴリズム

符号化と復号の処理について具体的に説明する．秘匿化に無関係の誤り訂正処理については省略する．

ここで，既存領域に収容するデータ *d0* 及び秘匿データ領域に収容するデータ *d1,..,dn* からなる収容データを D = (*d0, d1,..,dn*) とする．これらのデータを各層に配置したデータ *ld1,..,ld16* からなる収容データを LD=(*ld1,..,ld16*) とする．また，この各層の収容データを白黒符号としたデータ *ud0,ud1,..,ud16* からなるデータを UD=(*ud0,ud1,..,ud16*) とする．そして，この白黒符号をカラー化したデータ *cd1,..,cd8* からなるデータを CD=(*cd1,..,cd8*) とする．

これらの個別のデータ配置を表 5-5 に示す．

表 5-5　データの配置

<table>
<tr><th colspan="3">項目</th><th>収容
データ</th><th>層(白黒)
レベル
データ</th><th>カラー
レベル
データ</th></tr>
<tr><td colspan="3">既存領域</td><td>d0</td><td>ld0</td><td></td></tr>
<tr><td rowspan="5">新規領域
(秘匿化領域)</td><td colspan="2">管理領域
(非暗号化領域)</td><td></td><td>ld1,..,ldj</td><td rowspan="5">cd1,..,cd8</td></tr>
<tr><td rowspan="4">データ領域
(暗号化領域)</td><td>データ領域1</td><td>d1</td><td rowspan="4">ldj+1,..,ld16</td></tr>
<tr><td>データ領域2</td><td>d2</td></tr>
<tr><td>⋮</td><td>d3,..,dn-1</td></tr>
<tr><td>データ領域n</td><td>dn</td></tr>
</table>

5.5.1　符号化処理

ステップ 1：データの準備及び圧縮

二次元コードに収容するデータの種別（英数字，漢字，バイナリー）毎に圧縮を行い，データ D = (*d0, d1,..., dn*) を準備する．

ステップ 2：既存領域の二次元コードの生成

既存領域のデータ *d0* について，通常の白黒二次元コードの生成処理を行い *1d0* 及び ud0 を得る．

ステップ 3:管理領域の割り当て

ユーザ毎の秘匿化ランダムマスク及び層の割り当てデータを記憶する管理領域のデータ量を計算し，新規領域へ必要な層数を割り当てる．

ステップ 4:データの領域分割

n 個のデータ領域について，それらを新規領域の 16 層の内，管理領域に割り当てた層以外の層に割り当てる．

ステップ 5:ランダムマスクの生成と秘匿化

n 個のデータ領域に適用するランダムマスク *P1,..., Pn* を乱数を用いて生成する．それらを各ユーザのパスワード PWn を用いて秘匿化し *EPa,..., EPm* を得て，管理領域データにセットする．

ステップ 6：新規領域の二次元コードの生成

ステップ 3 で，各データ領域に割り当てた層に．当該データ領域のデータを設定し，LD=(*1d1,..., 1d16*) を得る．その後各層にランダムマスク *P1,..., Pn* を用

いてランダムマスク処理を行い，UD=(*ud1,..,ud16*)を得る．

ステップ 7：サブセル色の決定

UD=(*ud1,..,ud16*)について，表 3-7 の符号化テーブルを用いてサブセル色を決定し，最終的な多値セル型二次元コードの各サブセル色 CD = (*cd1,..,cd8*)を得る．

5.5.2　復号処理

ステップ 1：画像入力，画像抽出

撮像装置によって，二次元コードを含む画像を撮像し，二次元コードに含まれるファインダーパターンを基に二次元コードを検出し，二次元コードの画像を抽出する．

ステップ 2：セル色の識別

二次元コード画像から各セルを切り出し，セルの中央部及び周辺部のサブセル色の識別を行い，多値セル型二次元コードの各サブセル色 CD=(*cd1,..,cd8*)を得る．

ステップ 3：白黒二次元コードに復号

表 3-7 の符号化テーブルを用いて，サブセルの色コード CD=(*cd1,..,cd8*)から各層の各セルの白または黒の色を復号し，二次元コードの白黒符号 UD=(ud1,..,ud16)を得る．

ステップ 4：既存領域の復号

既存領域の白黒符号 *1d0* から通常の白黒の二次元コードの復号処理を行い，収容データ *d0* を得る．

ステップ 5：新規領域の復号

ステップ 5-1:管理領域の読み取り

新規領域の内，ランダムマスク処理がされていない管理領域から，ユーザ m の秘匿化ランダムマスク *EPm* を読み取り，データ領域の構成を得る．

ステップ 5-2:ランダムマスクとデータの復号

ステップ 5-1 で得た秘匿化ランダムマスク *EPm* を，入力されたパスワード PWm を用いて復号し，割り当てられた層のランダムマスク *Pi,..,Pj* を得る．ここで，*i,..,j* はユーザ m がアクセスを許可された領域番号である．*Pi,..,Pj* を用いて白黒符号 UD=(*udk,..,ud1*)の復号処理を行い LD=(*1dk,..,1d1*)を得る．ここで，*k,..,1* はユーザ m がアクセスを許可された層番号である．LD=(*1dk,..,1d1*)からアクセスが許された収容データ *di,..,dj* を得る．

5.6　想定用途

本論文で提案する多値セル型二次元コードの複数ユーザへのアクセス制御の想定用途について述べる．

5.6.1　商品情報

想定用途の第一は，商品情報のユーザを限定した提供である．この事例のユーザ例，データ例及びそのアクセス権の付与例を表 5-6 に示す．

表 5-6　商品情報提供の場合のアクセス権割当の例

データ領域名	製造者	物流	販売店	消費者
商品名、 商品番号	○	○	○	○
製造年月日 製造ロット番号	○		○	
検査結果	○			
販売期限	○		○	
消費期限	○	○	○	○
連絡先	○	○	○	

この例で示すように，販売店や消費者に知られたくない情報を，知らせる必要のあるユーザにのみ的確に提供することが可能になる．

5.6.2　偽物検出

想定用途の第二は，偽物検出である．この事例のユーザ例，データ例及びアクセス権の付与例を表 5-7 に示す．

表 5-7　偽物検出の場合のアクセス権割当の例

データ領域名	製造者	販売店	消費者	偽造者
商品名、 商品番号	○	○	○	○
ブランド名	○	○		
シリアル番号	○	○		

この例では，多値セル型二次元コードの作成時に，偽造者が販売店に付与された復号鍵を知らないので，当該販売店向けの多値セル型二次元コードを作成できない特性を用いている．誤った秘密鍵を用いて作成した多値セル型二次元コードでは正規品であることを示すデータを読み取ることができないので，偽物であることが知れる．

また，ブランド名などの秘匿化されたデータは，乱数によるランダムマスクで秘匿化されて仮想二次元コードに収容され，符号化テーブルによって色符号化されてカラー二次元コードのサブセルとして印刷されている．上記の乱数によって発生したランダムマスクもパスワードで秘匿化されて仮想二次元コードに収容され，同様にカラー二次元コードのサブセルとして印刷されている．これらを規定された方法以外で作成または改変すると，それらは全て偽造品と判定されるので，偽物検出を無効にすることはできない．

5.7　実験結果

5.5.1 で説明した符号化処理をパソコン上に，復号処理をスマートホン上に実装し，多値セル型二次元コードの作成及び読み取りの実験を表 5-8 に示す条件で行った．作成した多値セル型二次元コードの例を図 5-4 に示す．

表 5-8　試験条件

項目	条件
バージョン	バージョン4（29x29セル）
コードサイズ	40x40,30x30 (mm)
誤り訂正	レベルH
印刷紙	マット紙（コクヨ）
スマートフォン	GALAXY Note 2 (SAMSUNG製)
照明	室内の天井照明
焦点合わせ	スマートフォンによる自動焦点

図 5-4　多値セル型二次元コードの例

読み取り実験の結果，データ量が少なく多値セル型二次元コードに収容でき，窓際など明るく，二次元コードの明度分布が一様な読み取り条件が良い場合には，予定したとおり，複数のデータ領域の中から複数のユーザがアクセスが許されたデータ領域を読み取ることができた．しかし，次の二つの問題点が明らかになった．

(1) データ配置の非効率

データ量が多い場合に，データ量が収容能力以下であるにも関わらず，収容できない場合が発生した．これは，データ領域を層単位で配置したからである．特定の層にはデータ領域が不足する一方，他の層では未使用のデータ領域が存在する場合が発生した．データ配置の効率を向上させるためには，データ領域の配置を層単位ではなく，別の単位で配置する必要がある．

(2) 読み取り性能の不足

多値セル型二次元コードの読み取りを，第 3 章では白色蛍光灯による照明を用いて実験を行い，二次元コードの 7 つのサイズについて，その読み取り結果を示した．この読み取り試験結果は，照明があり，且つ二次元コードのセルサイズが比較的大きい場合には，安定して読み取り可能であることを示している．

今回は，照明のない実使用環境で実施した．領域数，データ内容の異なる 2 つの二次元コードを作成し，それぞれ一辺を 40㎜ と 30㎜ とした場合について，3 つの読み取り環境で各 10 回の読み取り試行を行った結果を表 5-9 に示す．

表 5-9　読み取り試験結果

二次元コードサイズ(mm)		読み取り率（%）		
		室内窓際（明度分布無し）	室内中央（明度分布有り）	
コードサイズ	セルサイズ		点灯無し	点灯有り
40	1.4	100	5	10
30	1.0	95	10	15

この結果，スマートホンの影など二次元コード内に明度分布が発生しない場合には，前記の実験結果とほぼ同じ結果が得られた．一方，天井照明とスマートホン及び読み取り対象の二次元コードの位置関係で，スマートフォンの影により二次元コード内に明度分布が発生する場合には，大きなサイズの二次元コードで読み取り率が低下した．また，スマートフォンの照明を点灯した場合にも，照明が不均一となり，明度分布が発生した．この場合に対応するためには，読み取り時に明度補正機能が必要である．

第 6 章　結論と今後の課題

6.1　結語

本論文では，QR コードと互換性を持つ二次元コードについて，多色化と多領域化の手法を用いてセルの多値化を行い，もって二次元コードの大容量化を行い，増加した領域について秘匿化する提案を行った．

第 3 章では，セルを 3x3 構成の 9 個のサブセルに区分し，中央部のサブセルと周辺部のサブセルに分割する．中央部のサブセルを QR コードと互換性を持たせるために白黒で符号化し，周辺部のサブセルを大容量化のために 8 色のカラー色で符号化する方式（低密度方式）の提案を行った．そして，互換性及び識別性の実験を行い，実用的な大きさで互換性を有し，識別可能であることを示した．

さらに，上記の周辺部のサブセル（8 個）を独立してカラー色で符号化する方式（高密度方式）の提案を行った．低密度方式と同様に，互換性及び識別性の実験を行い，実用的な大きさで互換性を有し，識別可能であることを示した．

第 4 章では，第 3 章で提案した二次元コードにおいて，周辺部のサブセルが構成する 2 個（低密度）または 16 個（高密度）の仮想的な QR コードについて，ランダムマスクを用いて秘匿化する手法（ランダムマスク法）を提案し，その有効性を確認した．

第 5 章では，第 3 章で提案した高密度方式の二次元コードについて，第 4 章で提案したランダムマスクによる秘匿化を適用し，さらにユーザに割り当てたアクセス権に対応する秘匿化鍵をユーザのパスワードでさらに秘匿化することにより，アクセス権の制御を行う方式を提案した．この方式に基づく高密度方式のカラー二次元コードの画像を作成し，スマートフォン上に読み取りソフトウェアを実装し，読み取り試験を実施してその有効性を確認した．

6.2　今後の課題

6.2.1　微細サブセルの識別性能の向上

今後の課題の第 1 は，微細サブセルの識別性能の向上である．スマートフォンを用いた読み取り試験の結果，ある程度の大きさのサブセルまでは誤りなく識別可能であるが，それ以下では識別誤りが発生する．読み取り試験データの解析の結果，微小セルの識別誤りの原因は，周辺のサブセル色の混入であることが明らかになった．スマートフォンの OS は撮像した画像をアプリケーションソフトに受け渡すときに，画像圧縮を行う．画像圧縮を行う場合に，周辺の画素との平均化処理を行うが，平均化処理がサブセルの内部だけでなく，周辺のサブセルを含んだ領域で行う．そこで，注目するサブセルの代表値に周辺のサブセルの影響が及ぶ．すなわち，これが周辺のサブセル色の混入である．

そこで，サブセルの色の識別には，サブセル内部領域に限定した平均化処理が必要である．

6.2.2　明度補正

二次元コードの表面に対して，白色光を一様に投光した場合には，スマートフォンを用いた読み取り試験の結果，実用的な大きさの二次元コードまで識別ができることを示した．しかし，二次元コードの表面にスマートフォンの影が差すなどの原因で，二次元コードの表面の明度が一様ではなく，明度分布を有する場合には，きわめて識別率が低下することが明らかになった．これは，ファインダーパターンに設定したパレット色と識別対象サブセルの明度が異なる場合には，印刷されている色が同じであっても，異なる色として判断されるためである．

そこで，明度が異なっていても，同一の色と判定可能な明度補正処理が必要である．

6.2.3　アクセス制御のネットワーク対応

第 5 章で提案した二次元コードへのアクセス制御は，二次元コード内部に記憶させたアクセス制御データ（表 5-2 の管理領域）に基づき行った．このアクセス制御データを図 6-1 のように，ネットワークに接続されたサーバに記憶することで，アクセス制御をダイナミックに行える可能性がある．例えば，新規

のユーザが出現した場合のユーザ追加や既存のユーザのアクセス領域の変更などである．

また，データ領域のデータについても，二次元コードに収容するのは，実際のデータではなく秘匿化されたコンテンツ ID とし，実際のデータはコンテンツ ID と対応させてサーバに記憶させれば収容データサイズの限界を無くすことも可能である．

アクセス制御データやコンテンツの変更の鍵の管理などネットワーク化することの諸課題について，今後の検討課題としたい．

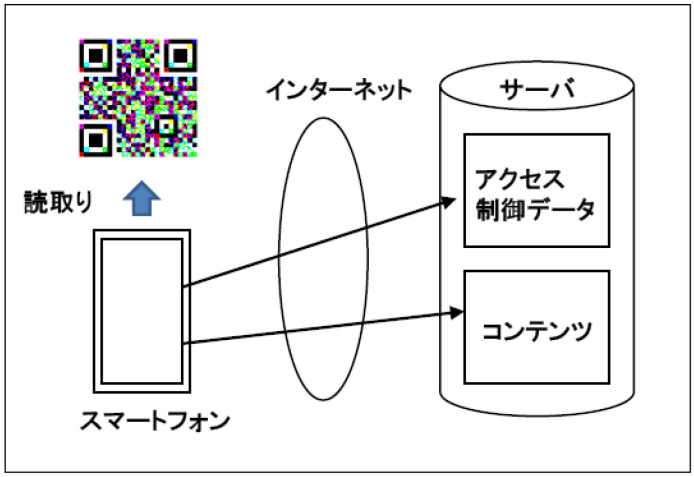


図 6-1　ネットワーク二次元コード管理システム

謝辞

本学位論文の執筆にあたり，九州大学システム情報科学研究院教授櫻井幸一先生には，社会人博士課程に入学以来6年の長きに渡って，学会発表での論文の内容の議論，指導から論文の書き方までご指導いただき，また本学位論文では論文の構成から，まとめ方にいたるまでご指導を賜りました．遅々として進まない研究，なかなかまとまらない論文作成に対して，暖かく指導いただきましたことに深く感謝の意を表します．

また，広島修道大学経済科学部教授井上徹先生には，膝を交えて親しく誤り訂正理論のご指導をいただきました．名古屋大学准教授岩田哲先生には，研究初期のご指導をいただきました．NIU / Science & Technology Intelligence の Mike DAVD 教授および Security Assurance at Salesforce.com, Inc. の Kurt SAUER 副社長には，本学位論文の英文概要にアドバイスをいただきました． 東京理科大学工学部教授岩村惠一先生および国立情報学研究所コンテンツ科学研究系教授越前功先生には，学位論文作成指導だけでなく，情報処理学会コンピュータセキュリティシンポジウムなどの成果発表を聴講いただき，質問，討議を通じてご指導を頂戴いたしました．九州大学教授岡田義広先生および准教授安田雅哉先生には，本学位論文の予備審査において，疑問点を指摘し，内容に踏み込んだ議論を通じてご指導を頂戴しました．ここに深く感謝の意を表します．

生涯学習開発財団より平成２４年度博士号取得支援助成金の授与を受けました．ご支援に感謝致します．

最後に，社会人博士課程での研究と会社の業務の両立を支えてくれた妻美樹子，幼少の頃より学業を見守ってもらった亡父清，母照代に心より感謝致します．

参考文献

参考文献は，国際標準，大容量化，秘匿化，その他の順に記載した.

1) ISO/IEC 18004:2006 Information technology -- Automatic identification and data capture techniques -- QR Code 2005 bar code symbology specification.

2) ISO/IEC 16022:2006 Information technology -- Automatic identification and data capture techniques -- Data Matrix bar code symbology specification.

3) ISO/IEC 15438:2015 Information technology -- Automatic identification and data capture techniques -- PDF417 bar code symbology specification

4) ISO/IEC 16023:2000 Information technology -- International symbology specification -- MaxiCode

5) ISO/IEC 24778:2008 Information technology -- Automatic identification and data capture techniques -- Aztec Code bar code symbology specification

6) ISO/IEC 24778:2008 Information technology -- Automatic identification and data capture techniques -- GS1 Composite bar code symbology specification

7) ISO/IEC 15415:2011 Information technology -- Automatic identification and data capture techniques -- Bar code symbol print quality test specification -- Two-dimensional symbols.

8) https://www.itu.int/rec/R-REC-BT.601/en.

9) Hiroko Kato, Keng T. Tan, Pervasive 2D Barcodes for Camera Phone Applications, IEEE Pervasive Computing, vol.6, no.4, pp.76-85,2007.

10) Hiroko Kato, Keng T. Tan, Douglas Chai, Development Of A Novel Finder Pattern For Effective Color 2D Barcode Detection, Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications. ISPA2008, IEEE Computer Society, pp.1006-1013, 2008.

11) Hiroko Kato, Keng T. Tan, Douglas Chai, Novel colour selection scheme for 2D barcode. Proceedings of 2009 International Symposium on Intelligent Signal Processing and Communication Systems, pp.529-532.2009.

12) Hiroko Kato, Keng T. Tan , Douglas Chai, Novel colour selection scheme for 2D barcode. Proceedings of 2009 International Symposium on Intelligent Signal Processing and Communication Systems, pp.529-532, 2009

13) Hiroko Kato, Keng T. Tan, Douglas Chai, Barcodes for Mobile Devices, Cambridge University Press, 2010.

14) Keng T. Tan,Hiroko Kato, Designing a Color Barcode for Mobile Applications, IEEE Pervasive Computing, vol.6, no.4, pp.50-55,2012.

15) 助川修司, 伊藤正都, 近藤圭佑, 大囿忠親, 新谷虎松, QR コードの多色化による 2 次元コードの大容量化について:情報処理学会全国大会講演論文集 第 70 回平成 20 年(4), pp.845-846, 2008.

16) 寺田遼平, 藤本敬介, 中山泰一, カラー二次元コードを高解像化するための認識アルゴリズムの実現と評価, 信学技報, SS2008-57,PP.55-60,2009.

17) 遠藤裕介, 恩賀嶺, 廣友雅徳, 森井昌克, カラー多重化 QR コードの提案と評価, 信学技報 LOIS2009-25, IE2009-66, 2009.

18) 遠藤裕介, 廣友雅徳, 森井昌克, カラー多重化 QR コードの改良と評価, 信学技報 LOIS2010-5, 2010.

19) 遠藤裕介, 廣友雅徳, 森井昌克, 高密度情報化を可能とする QR コード符号化方式について, FIT2010 , RO-006 第 4 分冊 PP.151-156, 2010.

20) 遠藤祐介,廣友雅徳, 佐治勇樹, 渡辺優平, 森井昌克, 多値二次元コードにおける高階調度認識アルゴリズムの提案,電子情報通信学会論文誌 D Vol.J95-D No.11 pp.1935-1943, 2012.

21) 古本啓祐, 渡辺優平, 森井昌克, グレースケール多重化二次元コードとその応用, 信学技報 ICSS201-5, 2012.

22) 古本啓祐, 森井昌克, 多値二次元コードを利用した視覚障害者対する音声

支援,情報処理学会研究報告 Vol. 2014 -SPT -8 No.13,pp.71-76,2014.

23) 菊池真徳, 藤吉正明, 貴家仁志, 標準 QR コードと互換性を有するカラーコードの検討, 信学技報 EMM2013-11, PP61-66,2013.

24) Antonio Grillo, Alessandro Lentini, Marco Querini, Giuseppe F. Italiano, High Capacity Colored Two Dimensional Codes,Proceedings of the International Multiconference on Computer Science and information Technology pp. 709-716, 2010.

25) Marco Querini, Antonio Grillo, Alessandro Lentini and Giuseppe F. Italiano, 2D Color Barcodes For Mobile Phones, International Journal of Computer Science and Applications, Vol. 8 No. 1, 2011, pp.136-155.,2011.

26) Marco Querini, Giuseppe F. Italiano, Color Classifiers for 2D Color Barcodes, Proceedings of the 2013 Federated Conference on Computer Science and Information Systems, pp.611-618, 2013.

27) Marco Querini, Giuseppe F. Italiano, Color Classifiers for 2D Color Barcodes, IEEE Transl. Federated Conference on Computer Science and Information Systems , pp. 611-618,2013.

28) Marco Querini, Giuseppe F Italiano, Reliability and data density in high capacity color barcodes,Computer Science and Information Systems (ComSIS), PP.1595-1615,2014.

29) Kris Antoni Hadiputra Nurwono, Color Quick Response Code for Mobile Content Distribution,Proceedings of MoMM2009, 2009.

30) Harish.N,Embedding, a Large Information In QR Code Using Multiplexing Technique.Taraksh Journal of Communications , Page No. 6 , Vol. 1 Issue 1, 2014.

31) Orhan Bulan, Henryk Blasinski, Gaurav Sharma,Color QR Codes Increased Capacity Via Per-Channel Data Encoding and Interference Cancellation, Society for Imaging Science and Technology, pp.156-159, 2011.

32) Orhan Bulan and Gaurav Sharma, Improved Color Barcodes via Expectation

Maximization Style Interference Cancellation, IEEE Transl. Acoustics, Speech and Signal Processing , March 2012 pp.1509-1512,2012.

33) Homayoun Bagherinia, Roberto Manduchi, A Theory of Color Barcodes, IEEE Color and Photometry in Computer Vision Workshop, pp.806-813, 2011.

34) Takuma Shimizu, Mariko Isami, Kenji Terada, Wataru Ohyama, Tetsushi Wakabayashi, Fumitaka Kimura, Color Recognition by Extended Color Space Method for 64-color 2-D Barcode, MVA2011 IAPR Conference on Machine Vision Applications, pp.259-262, 2011.

35) 山本稔貴，2 次元カラーコード画像の色認識に関する研究，三重大学修士論文，2008.

36) 勇まり子，拡張色空間法による 2 次元カラーコード画像の色認識に関する研究，三重大学修士論文，2011.

37) Guy Adams, Steven Simske, Stephen Polland, 2D code sub-coding density limits, NIP27: 27th International Conference on Digital Printing Technologies and Digital Fabrication, pp.696-699, 2011.

38) 原昌弘，二次元コードの生成方法およびその読取装置，特開 2008-299422.

39) 小野智司，電子透かしを用いたカラー二次元コードの複製検知:電子情報通信学会論文誌. D，情報・システム J94-D(12)，pp.1971-1974，2011.

40) 宮本龍二,前原武,谷山大介,小野智司,中山茂,二次元コードの複製検知を目的とした印刷画像電子透かしの進化的生成,情報処理学会研究報告 MPS -92 No 23, 2014.

41) 新見道治，反復型可逆的情報ハイディングを利用した大容量二次元コード，2009 年電子情報通信学会総合大会，S21-S22 ，2009.

42) 鈴木敬嘉，宇田隆哉，伊藤雅人，市村哲，田胡和哉，星徹，松下温，二次元コードを用いた公開鍵署名による郵便物認証，情報処理学会研究報告 2003-CSEC-23，pp.77-80，2003.

43) 小林哲二，二次元コードのセキュリティ向上と応用，FIT2002，PP.225-226,

2002.

44) 小林哲二，二次元コードの電子透かしと応用，情報処理学会第 65 回全国大会，PP3-213-214，2003.

45) 女川穂高，三上貞芳，長野章，高木剛，鳴海日出人，桑原伸司，若林隆司，2 次元コードへのすかしコード導入による信頼性の確保，FIT2006，PP.201-202，2006.

46) Sartid Vongpradhip, Suppat Rungraungsilp, QR Code Using Invisible Watermarking in Frequency Domain, 9th International Conference on ICT and Knowledge Enginerring, pp.47-52, 2012.

47) Fu Hau Hsu, Min Hao Wu, Shiuh Jeng Wang, Dual-watermarking by QR-code applications in image processing, Proceedings of the 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, UIC-ATC 2012, pp.638-643, 2012.

48) Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, Sartid Vongpradhip, Data Hiding Method for QR Code Based on Watermark by compare DCT with DFT Domain, International Conference on Computer and Communication Technologies , ICCCT2012, PP.144-148, 2012.

49) Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl ,QR Code Seurity, Proceedings of the 8th International Conference on Advances in Mobile Computing and Multi-media, MoMM2010. pp.430-435, 2010.

50) 苅田光一郎，清水明宏，QR コードへの電子透かし実装に関する研究，信学技報 LOIS2011-16，IE2011-49，EMM2011-09，PP.7-10，2011.

51) 苅田光一郎，清水明宏，二次元コード認証方式に関する研究，高知工科大学修士論文，2012.

52) Steven J. Simske, Jason S. Aronoff, Margaret Sturgill, Revenge of the Physical - Mobile Color Barcode Solutions to Security Challenges, 2010

Optical Document Security, San Francisco, 2010.

53) 田尻 昌之 ,谷山 大介,小野 智司 ,中山 茂 ,視認性と品質を考慮した二次元コードのモジュールパターン最適化,情報処理学会研究報告 MPS -92 No.2, 2013.

54) 暴 満粟 ,藤吉 正明 ,貴家 仁志, カラー情報付加による QR コードの多機能化,映像情報メディア学会技術報告 36(39), PP.1-4, 2012.

55) 荻原学, デザイン二次元コード, 電子情報通信学会誌 Vol.94 No.4, pp.341-343, 2011.

56) 青山直樹 ,渡辺優平,森井昌克, 埋め草コードを利用した QR コードの高誤り訂正, FIT2013, 第 4 分冊 pp.509-514, 2013.

57) 西村芳一, データの符号化技術と誤り訂正の基礎, ＣＱ出版社, 2010.

58) 和田山正, 誤り訂正技術の基礎, 森北出版, 2010.

59) 財団法人国際情報化協力センター, アジア諸国における二次元シンボルを使ったサプライチェーンに関する調査研究報告書, システム技術開発調査研究, 21-R-8,2010.

60) 清水隆史, 笹岡秀, リードソロモン符号のテーブル参照軟判定復号法の検討信学技報, IT2004-67 , ISEC2004-123, WBS2004-182 , 2005.

61) 西田豊明, https://www.ii.ist.i.kyoto-u.ac.jp/wordpress/wp-content/uploads/2015/03/pub-note-09-2015.pdf (2017.06 参照)

62) https://www.shiki.jp/tickets/guide/system/guide/smart/ (2017.06 参照)

63) http://www.khwayz.jp/case_001.php (2017.06 参照)

64) 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, 2006.

65) 日本自動認識システム協会, よくわかるバーコード・二次元シンボル, オーム社, 2010.

索引

査読付き論文リスト

1) Teraura, N. and Sakurai, K.：Preventing the access of fraudulent WEB sites by using a special two-dimensional code, Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp.645-650, (2012).

2) Teraura, N. and Sakurai, K.：Information hiding of two-dimensional code by multilayer optical method, 10th IEEE International Symposium on Parallel and Distributed Processing with Applications, pp.770-777, (2012).

3) Teraura, N. and Sakurai, K.： Information Hiding in Subcells of a Two-Dimensional Code, The 1st IEEE Global Conference on Consumer Electronics, pp.661-665, (2012).

4) Teraura, N. and Sakurai, K.：Confidentiality of 2D Code using Infrared with Cell-level Error Correction, International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 2, N^{o} 1, pp.23-31, (2013).

5) Teraura, N. and Sakurai, K.：Evaluation of the Identity and Compatibility of Multi-valued Cells in Two-dimensional codes using Smartphones, IEEE 7th International Conference on Service-Oriented Computing and Applications, pp.253-259, (2014).

6) Teraura, N. and Sakurai, K.：Proposal of Multi-value Cell structure High Density Two-dimensional codes and Evaluation of Readability using Smartphones, New Technologies, Mobility and Security (NTMS), 7th IFIP International Conference on, pid1162546-D, (2015).

7) 寺浦信之, 櫻井幸一: 多値セル型二次元コードでの多分割領域への複数ユーザのアクセス制御, 情報処理学会論文誌, Vol.57, No.9, pp.1965-1973, (2016).

8) Teraura, N., Ito, K., Kobayashi, D., Sakurai, K.： Evaluation of Gamma Ray Durability And Its Application on Radiation Environment, Proc. of The 6th annual IEEE International Conference on RFID Technology and Applications (RFID-TA2015), pp.147-152, (2015).

学会等での発表リスト

1) 寺浦信之, 櫻井幸一: 多層式光学的情報媒体による二次元コードの情報ハイディング, コンピュータセキュリティシンポジウム(CSS2011), pp.211-216, (2011).

2) 寺浦信之, 櫻井幸一: 二次元コードによる不正 WEB 誘導への対策, 2012 年暗号と情報セキュリティシンポジウム(SCIS2012),4E1-6,(2012).

3) 寺浦信之, 櫻井幸一: セルの微細分割による二次元コードの情報ハイディング, 第 11 回情報科学技術フォーラム(FIT2012), K-045, (2012)

4) 寺浦信之, 櫻井幸一: グレー及びカラー化による二次元コードの情報ハイディング, コンピュータセキュリティシンポジウム(CSS2012), pp.211-216, (2012).

5) 寺浦信之, 櫻井幸一: 商品コード用バーコードの互換性を維持した秘匿化と大容量化, 信学技報, vol. 112, no. 293, EMM2012-83, pp. 117-122, 2012 年 11 月.

6) 寺浦信之, 櫻井幸一: バーコードの互換性を維持した大容量化と秘匿化及び誤り訂正の導入, 信学技報, vol. 112, no. 357, PRMU2012-77, pp. 43-48, 2012 年 12 月.

7) 寺浦信之, 櫻井幸一:互換領域を有する暗号付二次元コードへのセルレベルの誤り訂正の導入, 2013 年暗号と情報セキュリティシンポジウム(SCIS2013),2C3-2,(2013).

8) 寺浦信之, 櫻井幸一: 互換領域を有する多色多領域方式の高密度二次元コード, 第 12 回情報科学技術フォーラム(FIT2013), K-045, (2013).

9) 寺浦信之, 櫻井幸一:RS 符号データコード語にマスクパターンを適用した多値化二次元コードの秘匿化, コンピュータセキュリティシンポジウム(CSS2013), pp.809-816, (2013).

10) 寺浦信之, 櫻井幸一: 多値化二次元コードのハイブリッド暗号による秘匿, 2014 年暗号と情報セキュリティシンポジウム(SCIS2014),4F1-4,(2014).

11) 寺浦信之，櫻井幸一：秘匿領域を有する多値セル構造の二次元コードの互換性と識別性のスマートフォン実装による評価，コンピュータセキュリティシンポジウム(CSS2014)，pp.1276-1283，(2014)．

12) 寺浦信之，櫻井幸一：秘匿領域を有する高密度二次元コードの互換性と識別性に関するスマートフォン実装による評価，2015 年暗号と情報セキュリティシンポジウム(SCIS2015),1B2-2,(2015)．

13) 寺浦信之，井上徹，櫻井幸一:高密度二次元コードのブロック誤りとランダム誤りに対応する二重誤り訂正システムの検討，第 14 回情報科学技術フォーラム(FIT2015)，K-045，(2015)．

14) 寺浦信之，櫻井幸一:多値セル型二次元コードのデータ領域分割と分割領域への複数ユーザのアクセス制御，コンピュータセキュリティシンポジウム 2015(CSS2015)，3C1-1，(2015)．

15) 寺浦信之，岩村惠市，越前功，櫻井幸一： 二重符号化二次元コードのマスクパターン秘匿化への RS 符号を用いた誤り訂正の影響検討，信学技報，vol.117，no.40，EMM2017-12，pp.67-72，(2017)．