三次元パターン認識を用いた携帯型端末向け電子チケットシステム

E-TICKET ISSUING SYSTEM WITH 3-D PATTERN RECOGNITION FOR MOBILE TERMINALS

宇田　隆哉 [1)]　　市村　哲 [2)]　　伊藤　雅仁 [3)]
Ryuya UDA　Satoshi ICHIMURA　Masahito ITO

1) 東京工科大学　コンピュータサイエンス学部（〒192-0982 東京都八王子市片倉町１４０４－１
E-mail: uda @ cs.teu.ac.jp ）

2) 東京工科大学　コンピュータサイエンス学部（〒192-0982 東京都八王子市片倉町１４０４－１
E-mail: ichimura @ cs.teu.ac.jp ）

3) 東京工科大学　コンピュータサイエンス学部（〒192-0982 東京都八王子市片倉町１４０４－１
E-mail: masahito @ cs.teu.ac.jp ）

ABSTRACT. The electronic ticket issuing system for cellular phones is described in this paper. The system has strong security for commercial use and has flexibility to support any cellular phone and PDA. A cellular phone needs no adding hardware module. A user can deal with everything related with a ticket such as issue, payment and showing with his cellular phone. A user accesses to the ticket issuing server to get a ticket and shows that ticket holding his cellular phone to the ticket reader at an entrance gate. 3-D pattern is used in order to show a ticket, and its recognition is free from tilt, rotation and moving of a cellular phone during reading. This electronic ticket issuing system can be used for concert ticket, train ticket, etc. This system allows reentrance, and still more, this ticket can be used as a coupon ticket that is used any number of times.

1. 背景

通常，各種イベントや列車などのチケットを必要とする場合，チケット販売店で購入して，紙などのチケットを受け取る必要がある．近年では，電話，ファクシミリ，PC などでチケットを注文することも可能であるが，依然として紙媒体としてのチケットを取りに行くか，郵送で受け取る必要があり，手間や輸送コストがかかる．

一方で，携帯型情報端末，特にインターネットサービスが利用可能な携帯電話は，すでに多くの人が持ち歩くものとなっている．この携帯電話や，インターネット上でのチケットの購入サービスは，さまざまなチケット販売代行業者が始めている．

携帯型情報端末をチケットとする手法も登場しており，携帯型情報端末に非接触 IC チップや IrDA インタフェースなどを搭載し，認証，通信を行うことを想定した手法がある．このような手法では，その通信インタフェースが普及した場合には利用が期待できるが，現状で普及している携帯電話がそのまま利用できるわけではなく，規格が統一されないと複数のデバイスが混在し不便なものとなる．

携帯電話画面に 1 次元もしくは 2 次元バーコード [1, 2, 3] を表示することで認証する電子チケットの実験や商品化 [4, 5] も始まっている．二次元バーコードは QR コード [1] や CyberCode[2] に代表され，位置案内など様々なサービス [6, 7, 8, 9] に用いられている．しかし，端末の画面解像度の制約により，携帯電話端末の画面に表示可能な情報のデータ量は，一般的な電子署名である 1024 ビットの RSA 署名等 [10] を行うのに必要なビット数には遠く及ばず，また表示された画面が一枚の画像なため紙などへの複製も可能であり，安全面には問題があると言える．例として，イープラスが行った実験 [4] では，10 進 8 桁のバーコードである．自動販売機で用いられている 2 次元バーコードによる Cmode も，10 進 10 桁と容量は大きくない．ターゲットワンが行っている 2 次元バーコード方式 [5] でも最大でも 200 ビット程度に過ぎない．

本開発では，上記の点をふまえ，既存の携帯型情報端末を用いた安全な電子チケット発行システムを提案する．本システムでは，ユーザに対する利便性やシステムの安全性を高めるため，以下の点について考慮し，システムを構築する．

1) **チケットの受け取りなどに物理的な方法は用いないこと：**チケットを物理的に渡す，IC カードを公衆端末で書き換えるなどの方法では，ユーザの手間がかかるため，電子的な通信方法で携帯型情報端末にチケット情報を送信し認証に用い，操作は携帯型情報端末上で完結するようにする．携帯型情報端末以外に持ち運ぶものが増える，チケットを取り出す等の手間を避けるため，携帯型情報端末をチケットとして使う．
2) **従来の携帯型情報端末をそのまま使えること：**端末のコスト増加を避け，従来の端末のユーザも利用できるように，多くの端末が装備しているデバイスを用いてチケット情報を読み取り装置へ送信する．特殊な暗号モジュールなどによる端末側での処理も避ける．
3) **利用者のプライバシが保護されること：**通常，チケットは，イベント業者がチケット販売業者に委託する．いくらチケット販売業者がプライバシ保護に留意しても，イベント業者側からの顧客情報流出は考えられる．また，イベントの入場に必要なのは，正当なチケットを所有していることだけである．よって，イベント業者へは，チケットに関する情報のみを伝え，購入者の個人情報を一切伝えないことで，個人情報の流出や悪用の危険性を低減する．

4) **チケットの安全性が確保されていること：**チケットには，十分な長さの電子署名 [11, 12] を用いることで，そのチケットの真贋を確認できるようにし，安全性を確保する．

2. 目的

本開発では，既存の携帯型情報端末に特殊なデバイスを追加することなく，1024 ビットの RSA 署名 [13, 11] に加えその他のチケット情報を送信することができる三次元パターン通信を提案し，これを用いることで安全なチケットを実現する．

三次元パターン通信とは，携帯型情報端末の画面に複数の画像を順次書き換えていくことにより，任意のビット長のデータを送信する手法である．また，一般に市販されている携帯電話機に本提案方式を実装し，1024 ビットの RSA 署名および ID データを画面に表示して読み取る実験とその評価を行う．本開発の三次元パターンは，携帯型情報端末を持つ利用者の手が動いたり，端末画面が読み取り装置のカメラ部に対して水平または垂直に傾いた場合や，表示パターンに画像をオーバーレイした場合にも，正しく読み取ることが可能であることが確認できた．本提案手法では，現在広く普及している携帯電話をそのまま使用でき，IC カードのようなデバイスを新たに購入する必要がない．さらに使用する携帯型情報端末の画面解像度に依存することなく，必要なビット数を送信できるスケーラビリティを持った，安全な認証方式と言える．

3. 認証関連技術と関連研究

本開発では，電子チケットに電子署名 [11, 12] を用いて安全性を保証している．この技術が何かについて，簡単に説明する．

(1) 暗号

暗号とは，情報を一定の規則に従って他の表現に変えて，その規則を知らない者には元の情報を判らなくするためのものである．

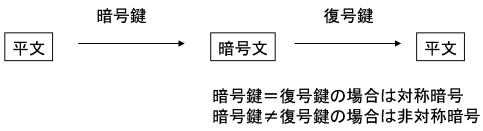

図 1: 暗号

暗号には，対称暗号（秘密鍵暗号）と非対称暗号（公開鍵暗号）の２つがある．図１において，暗号鍵と復号鍵が等しいものが対称暗号である．また，暗号鍵と復号鍵が異なり，片方の鍵で暗号化した情報は，その鍵と対になる鍵を用いないと復号化できないものが非対称暗号である．この対となる鍵の片方で暗号化したものは，もう片方の鍵で復号化できる．

対称暗号では，通信を行う二者間で鍵（秘密鍵）を共有しなくてはならないことから，鍵の安全な管理や配布の問題が生じる．もし秘密鍵が第三者の手に渡れば，通信は筒抜けになってしまうためである．そのため，通信相手の数が増えるほど管理すべき鍵も増え，鍵管理の問題が発生する．この対称暗号には様々な方式があるが，本開発では用いていないため，ここではその詳細は割愛する．

一方で，非対称暗号では，一つの片方の鍵（公開鍵）を複数の相手に渡してしまっても問題はなく，対になるもう一つ鍵（秘密鍵）だけを管理しておけばよい．そのため，一般的なネットワーク上でも安全に鍵の送信が行える．

代表的な非対称暗号には，いくつかの方式が存在する．

■RSA(Rivest, Shamir, Adleman) 方式 1978 年，MIT の Rivest，Shamir，Adleman によって考案された暗号方式 [13, 11] である．一般的に最も普及しており有名なものといえる．巨大整数を素因数分解するのは極めて困難であるという仮定に基づいており，実際に巨大整数の素因数分解を簡単に行う方法は，計算機の誕生以前から研究されているが，未だ発見されていない．

■ElGamal 方式 ElGamal によって考案された，数学の離散対数問題を暗号に応用したものである．この暗号鍵長を短くした電子署名方式の DSA(Digital Signature Algorithm) が，1991 年に NIST が公布した電子署名標準 (DSS: Digital Signature Standard) に用いられている．

■楕円曲線暗号 1985 年，Neal Koblitz と Miller が考案した暗号方式である．一般に 160 ビット鍵長の楕円曲線暗号は 1024 ビット鍵長の RSA に匹敵する強度と言われるが，楕円曲線問題自体はまだ研究途上といえる．

■一方向性ハッシュ関数 一方向性ハッシュ関数は暗号ではないが，特に非対称暗号と密接な関わりがある．安全な通信のためには情報を暗号化するだけでなく，情報が伝達途中で改竄されていないことを証明できる必要がある．そこで、メッセージの情報を凝縮する手法が用いられており，このときに一方向性ハッシュ関数が用いられる．

一方向性ハッシュ関数は，一方向性 (非可逆性) と，同値生成確率の低さを特徴とする．一方向性とは，入力された値からハッシュ値を計算するのは容易であるが，ハッシュ値から入力された値を求めるのが困難なことを示している．また，高速に計算が可能ではあるが，同じ値を生成させるためには膨大な計算量が必要とされるため，現実には困難であるといえる．

(2) 電子署名

電子署名とは，電子文書の正当性を保証するためにつける情報である．送信するデータに認証子と呼ばれる電子的なメッセージを付与し，送信者を認証し，他者によってデータの改竄が行われていないか検証することで，データの安全性を保証するものである．

2000 年 5 月に制定された電子署名及び認証業務に関する法律 [14] によると，第２条で,「電子署名」とは、電磁的記録（電子的方式，磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって，電子計算機による情報処理の用に供されるものをいう．以下同じ.）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう．

1) 当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること．
2) 当該情報について改変が行われていないかどうかを確認することができるものであること．

と定められている．

署名の実際の利用方法について解説する．送信者は，受信者に対して送信したいデータを一方向性ハッシュ関数に入力して，そのハッシュ値を求める．このハッシュ値は認証子と呼ばれる．これを自分の秘密鍵で暗号化し，データと暗号化された認証子を受信者へ送信する．また、受信者は送信者の公開鍵を受け取っておく．受信者が送信者の公開鍵で認証子を復号化し，得られたハッシュ値と，データを一方向性ハッシュ関数によって計算した値を比較して，一致すれば改竄がないことが確認できる．

(3) 関連研究

携帯電話でチケット情報を扱える手法に関する研究としては，XML Ticket[15, 16, 17]，GSM-Ticket[18] 等が

ある．これらの研究では，チケットとして扱うべき情報が何であるか，どのようにサーバや業者との間でトランザクションが起きるか，などについて提案している．扱うチケットの幅は広く，航空券やイベントのチケット，ソフトウェアのライセンス，運転免許などあらゆるものを扱えるデータ構造を示している．これらの流通において，その権利を保証するものである．さらに，GSM-Ticket ではGSM 方式携帯電話に搭載される SIM(Subscriber Identity Module)[19, 20] への格納方法や使い方を示している．しかし，SIM として，RSA 公開鍵署名を処理できる拡張されたモジュールの使用を前提としている．さらに，チケットを確認する，いわゆるチケットの確認方法については，別の何らかのデバイスが必要であるとしている．つまり，従来の携帯型情報端末をそのまま用いているわけではなく，以下の問題を伴う．

- 携帯電話，携帯型情報端末にとっては負荷が大きい公開鍵署名処理のための専用モジュールをつける必要がある．
- 認証段階の近距離通信方式が必要．

同様の問題は，中尾らの提案する鉄道チケット [21] にも存在する．これは専用の暗号計算モジュールを内蔵させることを前提とし，近距離通信に赤外線による IrDA を用いている．

非接触 IC カードを用いてチケットとする方法も提案されているが，これは限られた用途でしか実用化されていない．商業的に成功しているものとしては，JR 東日本の Suica がある．定期と一体のものが普及しており，同社の鉄道を通勤や通学に用いる人に用いられている．機能としては，切符の購買から自動精算までを行い，取得は駅の窓口で一回だけですむ．カードの取得には 500 円のデポジットを必要とするが，返却時には戻ってくるため，特に利用者の負担は大きくなく，特に急いでいるときには煩わしい切符の購買や精算がなくなり，金銭のチャージも切符購買に比べてはるかに少ない頻度ですむことがメリットといえる．鉄道チケットとして新たな媒体を配布するのは，駅という場所だけであり，取得から消費までが場所的に完結した存在であることも普及の要因と思われる．

Suica では、磁気券をわざわざ取り出す煩わしさから開放されるという点，紛失時の再発行が受けられる点，急いでいるときに切符を買わなくてすむ点などが利点だが，磁気式化される前の定期券は見せるだけで済んでいた上，磁気式化後はプリペイド型のカードとしてイオカードが予め存在している．磁気式定期券に不満のある人々や，磁気式のイオカードを利用していた人が移行しただけとも考えられる．鉄道チケットであるため現状で 500 万枚の普及があるにすぎないとも言える．

鉄道ではなく興業チケットでは，1999 年から 2000 年にかけて、チケットぴあが大規模な IC カード配布による実験を試みたが [22, 23]，チケット業者としてはあまりメリットがなく，配布コストが高額になることから，現在では NTT コミュニケーションズと新会社を設立し，IrDA などによる認証を試みている．他にも，KDDI による二次元コードの実証実験や日立による IC カードの実証実験など様々なものがあり，認証のための近距離通信媒体として何を用いるのかが最大の問題となっている．

また，プリたまや icePAY[24] など，携帯電話に接続して使用する認証デバイスも存在したが，普及はしていない．使える場所があまりに限られているにもかかわらず，使用するためには携帯電話と一緒に肌身離さず持ち歩かなくてはならないためである．購買が携帯電話で行われる以上，このような外付けデバイスや IC カード等を用いるもの [25, 26, 27] は，デバイスの携帯の問題や，カード配布の問題があるため普及は難しい．

興業チケットや各種娯楽施設の入場券などの最大の特徴は，そのチケットが使われる機会が少なく散発的であり，趣味性が高いと言うことである [28]．そのため，専用のデバイスは交通系チケットなど他の分野に比べても特に普及しにくいといえ，携帯型情報端末に内蔵されている機能を有効に活用すべきであるといえる．

二次元コードを用いた従来手法の問題は第 1 節で述べたとおりである．そのため，本開発では画面を利用して高速に通信な通信を実現し，また，端末側での複雑な計算処理は行わないこととする．

4. 電子チケットシステム

本章では，電子チケットシステムの概要について述べる．

(1) システム概要

図 2 に，本システムの概要を示す．

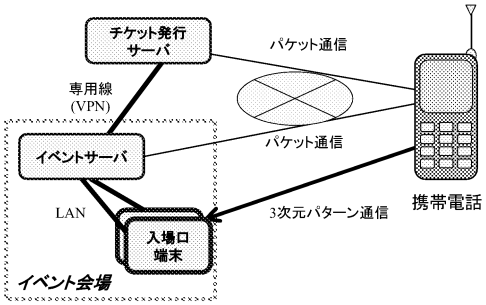

図 2: 電子チケットシステムの概要

システムには，ユーザの管理やチケットの販売などを行うチケット発行サーバと，イベントごとのチケットの認証を行うイベントサーバの 2 種類のサーバを用意する．チケット発行サーバとイベントサーバは，携帯電話網にインターネット経由で接続され，携帯電話はインターネットサービス機能を用いてサーバにアクセスする．チケット発行サーバは，ユーザのチケット購入や決済などを管理し，入場に用いるチケットとは別の，一時的なチケットである仮チケットの発行を行う．仮チケットには，本チケットの発行を受けるための URL を含む．携帯電話は仮チケットに記載された URL にアクセスし，入場に用いる本チケットを発行する．一方，イベントサーバはチケット発行サーバに専用線で接続され，販売されたチケットに関する情報を受け取る．イベント会場には入場口端末が用意され，イベントサーバと LAN で接続される．入場口端末は，3 次元パターン通信によって携帯電話から本チケットを受信し，本チケットの署名とイベントサーバに登録されているチケット情報を比較して，入場の可否を決定する．このとき，イベントサーバはチケットの無効化など，入場口端末における認証の制御も行う．

(2) ユーザ登録

チケット発行は，ユーザ登録，仮チケット発行，本チケット発行の 3 段階に分けられる．以下に手順に沿って処理を説明する．

ユーザは，まずシステムに登録を行い，ユーザ ID とパスワードを受け取る必要がある．そのため，チケット販売代行会社が管理するチケット発行サーバに携帯電話などでアクセスし，名前，住所，電話番号，クレジットカード番号などの決済情報を登録する．このとき，携帯電話の端末番号など，携帯電話端末を特定できるものを記録しておくことが望ましい．ここで，ユーザ ID とパスワードが生成され，利用者に通知される．ユーザ ID やパスワードなど，

ユーザのプライバシのかかわる情報は，プライバシ保護のため，チケット発行サーバのみで扱われ，以降は外部に送信されることはない．

(3) 仮チケット発行

図 3 に仮チケット発行の手順を示す．

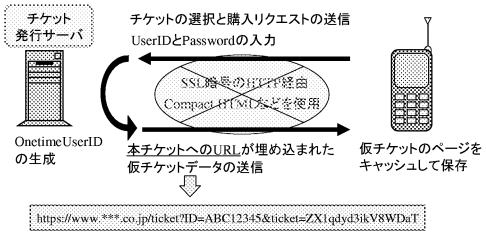

図 3: 仮チケット発行

チケットを購入したいユーザは，携帯電話を用いて，SSL で暗号化された HTTP プロトコルを用いてチケット発行サーバにアクセスする．ユーザは購入するチケットを選択し，購入を決定し，ユーザ ID とパスワードを入力する．チケット発行サーバは，この購入要求を受け取り，ユーザに対して，本チケットを受け取るための URL の記載された仮チケットページを送信する．例として，埋め込まれている URL は以下のようなものである．

https://www.***.co.jp/ticket?ID=
ABC12345&ticket=ZX1qdyd3ikV8WDaT

ユーザは仮チケットページをキャッシュするか，ブックマークとして記録しておく．仮チケットページは実際の入場には使わない一時的なものであり，購入した結果として受け取る引換券のようなものである．この仮チケットを用い，ユーザは後に入場に用いる本チケットを受け取る．

(4) 本チケット発行

図 4 に本チケットの発行手順を示す．

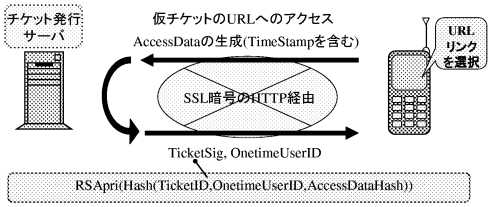

図 4: 本チケット発行

本チケットの発行は，チケット発行サーバが行う．ユーザは，先述の仮チケットに示されている URL を用い，本チケットの取得のためにチケット発行サーバへアクセスする．このサーバへのアクセス可能時刻は，入場開始など実際に電子チケットが利用され始める一定時間前へ制限することで，チケットの解析やねつ造などが可能な時間は短くなり，より高い安全性を実現することが可能となる．また，本チケットを紛失する機会が減少する．後述する三次元パターン通信では，Java を利用できる場合は Java を用いるのが速度などの点で最適であるが，機種によってはアプリケーションの格納数が少なかったり，古いアプリケーションを確認もなく上書きしたりするものがある．これによるチケットの喪失を予防できる．

本チケット発行時に，チケット発行サーバから，イベントにおいて唯一でありランダムに生成される OnetimeUserID と，チケットの内容に対応する TicketID がイベントサーバに渡される．さらに，チケット発行サーバではアクセス時刻のタイムスタンプなどの AccessData が生成される．この AccessData のタイムスタンプは，後に再発行が必要な際に用いられる．チケット発行サーバは，携帯電話に，TicketID, OnetimeUserID，AccessDataHash(AccessData のハッシュ値) から生成される署名 TicketSig と，OnetimeUserID を含んだ本チケットを送信する．ここで，ユーザのもとには AccessData は送信しないため，チケットの解析は一層困難となる．TicketSig は，TicketID, OnetimeUserID，AccessDataHash をつなげたもの，もしくは排他的論理和をとったもののハッシュ値を求め，このハッシュ値を RSA 秘密鍵で暗号化して生成される．

$$TicketSig = RSApri\{hash\{$$

$$Seq(TicketID, OnetimeUserID, AccessDataHash)$$

$$\| \; XOR(TicketID, OnetimeUserID, AccessDataHash)\}\}$$

さらに本チケットには，改ざんによる不正使用を防ぐために有効期限を定めておくのが望ましく，この有効期限内に使用しなかった場合には再発行の手続きを必要とする．チケット再発行のためには，AccessData に含まれるタイムスタンプが必要となる．ユーザが同じチケットの本チケットの再発行を要求したとき，チケット発行サーバは新しく生成した AccessData に基づいてチケットを再生成する．古いタイムスタンプを持つ AccessData からなる本チケットの情報は，イベントサーバ上で無効化される．

(5) 入場管理

a) 入場

図 5 に入場の手順を示す．

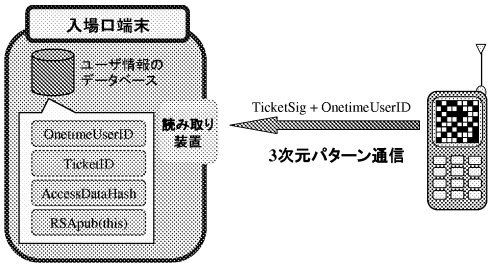

図 5: 入場手順

入退場などの管理を行うのがイベントサーバである．イベントサーバは，イベントごとに会場内に用意されており，イベント業者や会場運営者が管理する．イベントサーバは，チケット発行サーバより OnetimeUserID や TicketID と本チケットの対応関係を通知されている．しかし，どのユーザがどの OnetimeUserID を発行されたかなどは一切通知されないため，イベント業者が購入者を特定をすることは不可能であり，ユーザのプライバシは保護される．

この入場口端末は，TicketSig の生成に使われた秘密鍵の対になる公開鍵を渡されている．ユーザが入場するとき，電子チケット読み取り装置に 3 次元パターンを提示する．入場口端末は，読み取り装置から OnetimeUserID と TicketSig を受け取り，TicketSig を公開鍵で復号化する．このとき，イベントサーバからチケットに関する情報である TicketID, OnetimeUserID, AccessDataHash を受けとる．復号された TicketSig が，TicketID, OnetimeUserID, AccessDataHash のハッシュ値と一致した場合，すなわちつぎの式が成立した場合，入場口端末は入場を許可する．

$$RSApub(this)\{TicketSig\} =$$

$hash(TicketID, OnetimeUserID, AccessDataHash)$

ここで，入場に用いられた電子チケットが一時的に無効化されない場合，1 人で 2 つの携帯電話を持って退場し，再度別の人間と 2 人で入場し，また 1 人で 2 つの携帯電話を持って出ることを繰り返せば，何人でも入場できてしまう．そのため，入場口端末は入場を許可した後，そのチケットの OnetimeUserID をロックするように，イベントサーバに通知する．

(6) 再入場

ユーザがイベント会場から一時退場するとき，退場口端末に 3 次元パターンを提示し，そのユーザの OnetimeUserID をアンロックすることで，一時的退場と再入場を可能とする．ユーザが再入場するときには，入場口端末は再度 OnetimeUserID をロックする．この退場口端末は，一時退場が少ない場合，入場口端末と兼用でもよい．

上記のように，イベントサーバは本チケットの発行と入退場の認証の制御を行っている．1 チケットあたりのチケット発行サーバとの通信は 1 回限りであるのに対して，チケットの認証のたびに入場口端末と通信を行うため，会場内に設置するのが適切である．

5. 三次元パターン関連技術

本提案の三次元パターンは，携帯型情報端末の画面に表示することに特化したものであり，その特性を生かしている．技術的には，バーコードや二次元コードの応用的なものであり，可能な限り速く画面を書き換えることで短時間で大量のデータを送信することを可能としたものである．

ここではまず，バーコード，二次元コードの説明を行う．

(1) バーコード

バーコードは，小売業界においてチェックアウトを早く正確に行うための入力手段として発展した自動認識技術で，現在では，流通，物流，製造， 行政，医療等，幅広い分野で利用されている．店頭で販売されるすべての型番商品にはバーコードがつけられるほど普及している．この普及の背景には，コンピュータシステムの普及の中で，高い読取率， 高い読取信頼性，高い操作性，安価なメディアや読取装置の要求が高まり， バーコードがこれらの課題を実現していたからである． 一般にバーコードと称される縞状の一次元のバーコードは，二次元コード (シンボル) と対比させてリニアコード (シンボル) とも呼ばれており，バーコードは，情報を幅が変化する平行かつ長方形のバーとスペースの配列により，エンコードされたシンボルと定義されている．

a) バーコードの構成

バーコードは，スタート キャラクタ，データ キャラクタ，チェックデジット， ストップ キャラクタ及び，これらの前後に付くクワイエットゾーンから構成されている．また，バーコードは， キャラクタ間ギャップのある独立型 (ディスクリート型) シンボルと，キャラクタ間ギャップのない連続型 (コンティニアス型) シンボルがある．また，細太の 2 種類のバー (またはスペース) で構成される 2 値レベル型シンボルと数種類の太さのバー (またはスペース) で構成されるマルチレベル型シンボルがある．連続型シンボルやマルチレベル型シンボルの方が，情報密度が高い反面，読み取りには独立型シンボルや二値レベルシンボルに比べて読み取り装置の精度が必要である．バーコードの読み取りには，レーザを用いたラインスキャナや，カメラを用いたスキャナが用いられる．カメラを用いたタイプでは，二次元コードに対応できるものが多い．

図 6 にバーコードの構成を示す．このバーコードは Code 128 と呼ばれ，コンティニュアス型，マルチレベル型である．

図 6: バーコードの構成

バーコードは現在 100 種類以上の規格があるといわれるため，規格の詳説は割愛する．

(2) 二次元コード

バーコードには，情報量を多くできない，情報化密度が低い， シンボルが大きい，汚れたら読めない，読取方向に制限がある等の問題点があった．これらを解決すべく開発されたシンボルが二次元コードである．二次元コードは，バーコードが一次元で情報化されているのに対し，x および y 方向の二次元で情報をエンコードしたシンボルと定義することができる．

二次元コードは，バーコードと共存する形で，流通，物流，製造，行政，医療等，幅広い分野で利用されている．二次元コードの最大情報量は，通常は 1K バイト以上あるため，EDI データを伝票やラベルに印刷し，紙ベースでの EDI に使用されている． また，最小シンボルサイズを数ミリ四方にすることができるため，小物製品の管理にも用いられている．さらに読取方向に制限がないことから宅配貨物の自動仕分にも使用可能である．二次元コードでは，バーコードとは異なり，誤り訂正機能により多少の汚れに対しても確実な読取が可能となっており，その誤り訂正量はコードによって異なるが，可変であるものが多い．バーコードと比較して，収納できる情報量が多くキャラクタだけではなくバイナリコードを使用できるため，顔写真やサインを二次元コードにした ID カードの作成や，一般的な電子チケットサービスの実験にも用いられている．コカコーラと NTT ドコモが行っている自動販売機の決済サービス Cmode にも，二次元コードの QR コードが用いられている．ただしその中身はバイナリコードではなく，10 進 10 桁のただの数字列であり，二次元コードの持つメリットはあまり生かされていないといえる．

a) 二次元コードの構成

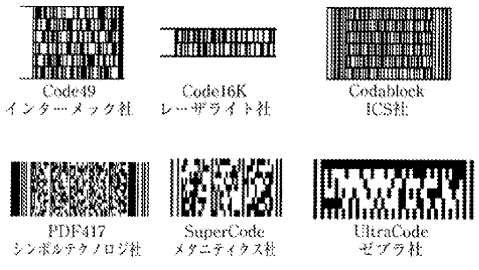

図 7: スタック型コードの種類

二次元コードは，バーコードを積み上げた形のスタック型二次元コードと碁盤のマスに黒い石 (セルという) を置いたようなマトリックス型二次元コードがある．

スタック型二次元コードは， 図 7 に示すように，バーコードのようにスタートコードやストップコードと，これ

らの前後に付くクワイエットゾーンから構成されている．横方向に見た場合，１次元のリニアバーコードと同じ形状であるため，バーコード用のラインスキャナなどでも読みとることができるというメリットを持つ．

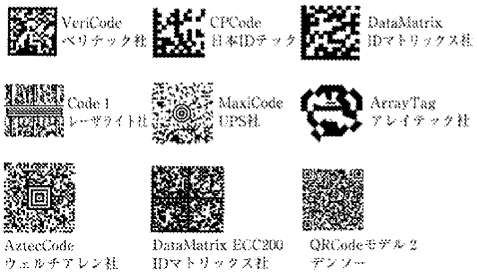

図 8: マトリックス型コードの種類

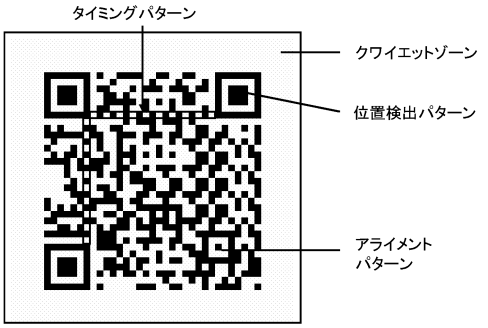

図 9: QR コードの構成

マトリックス型二次元コードは，図 8 に示すように，四角，またはＬ型ガイドセルがあるタイプやユニークな形の切り出しマークを持つタイプがあり，これらのガイドセルや切り出しマークによって位置や向きを判断し，回転や傾きに耐性を持たせている．画像処理が必要となるため，バーコード用のラインスキャナでは読みとることはできず，CCD カメラなどによってシンボルを読みとる．

図 9 に二次元コードの例を示す．近年携帯電話で多く用いられている QR コードであり，マトリックス型に分類される．

(3) 誤り訂正符号

本節では，三次元パターン通信における通信の信頼性を高める技術として用いる誤り訂正符号について，前提とする通信路のモデルについて説明し，誤り訂正符号とは何であるか，どのような種類のものが存在するか，そして本開発で用いる代表的な誤り訂正符号について述べる．

a) 通信系のモデル

符号理論における通信系のモデルを図 10 に示す．ここでは，通信とは，相手に情報を送ったり，情報を記録したりすることと定義する．また，情報としては離散的なものについて取り扱うとする．

以下に図 10 に示した通信系のモデルの定義を説明する．

■情報源　情報源からは，送りたい情報として 0,1 の情報ビット列が発生する．次に接続される符号器では情報ビット列を k ビットごとのブロックに区切るため，ここでもビット列は区切って考える．これを通報と呼び，$\mathbf{i} = (i_1 \cdots i_k)$ で表す．

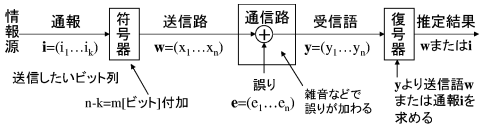

図 10: 通信系のモデル

■符号器　符号器からは，通報 $\mathbf{i}$ に対応した n ビット $(n > k)$ のビット列 $\mathbf{w} = (w_1 \cdots w_n)$ が出力される．すなわち，符号器で $m = n - k$ ビットの冗長ビットを付加されることになる．この n を符号長といい，k を情報ビット数という．$\mathbf{w}$ を符号語，この操作を符号化という．

符号長 n，情報ビット数 k の符号を (n, k) 符号という．符号長と情報ビット数の比 R を符号化率といい，次式で定義される．

$$R = \frac{k}{n} \tag{1}$$

これは，符号の能率を表し，高いほど符号長が短くなり望ましいが，一般に同一の符号化方式を用いた場合，符号化率が高いほど冗長性が低いため誤りに弱くなる．

■通信路　通信路は送信語 $\mathbf{w} = (w_1 \cdots w_n)$ が入力されると，n ビットの受信語 $\mathbf{y} = (y_1 \cdots y_n)$ を出力する．ここで，雑音などによる誤りが加えられ，

$$\mathbf{y} = \mathbf{w} + \mathbf{e} \tag{2}$$

となる．通信路に送り出された符号語を送信語という．また，$\mathbf{e}$ は誤りパターンと呼ぶ．

■復号器　復号器では，$\mathbf{y}$ を元に，符号器で行った演算に応じた演算を行い，いずれの符号語が送信されたかを推定する．

b) 誤り訂正検出符号

誤り訂正符号 (ECC：Error Correcting Code) とは，通信路で生じた誤りを訂正することを目的として，通報に適切な冗長性を付加したものである．同様に，誤り検出のみを目的とする誤り検出符号 (EDC：Error Detecting Code) がある．この二つの符号に本質的な差はなく，通信系における符号の使われ方の違いである．両者を併せて誤り制御符号と呼ぶ．

通信系において，これらの符号は FEC(Forward Error Correction)，ARQ(Automatic Recovery Quotient)，誤り修正の 3 通りの使われ方をする．まず，受信側では誤り訂正符号もしくは誤り検出符号で誤りを検出する．FEC と呼ばれる通信系では，その誤りを誤り訂正符号の能力により復号器で訂正し，元の通報を復元する．送信側は復号器が正しく訂正を行っている限り，再送する必要はない．ARQ と呼ばれる通信系では誤りの検出のみを行い，誤りがある場合は送信側にデータの再送を要求する．この方法は，簡潔かつ確実ではあるが，リアルタイム性が要求される場合や単向通信路では利用できない．誤り修正では，検出の後，データの性質を利用して他の正常な部分から誤ったデータの正しい値を推測する．主として映像・音声データの視聴覚補正などに用いられ，正しい通報が復元されるわけではない．

c) ブロック符号と畳込み符号

誤り訂正符号は，ブロック符号と畳込み符号の 2 種類に大別することができる．それぞれ，次のような定義によって分類される．

■ブロック符号　(n, k) ブロック符号は，情報のビット系列を k ビットごとのブロックに区切り，各ブロックに対して独立して誤り訂正符号による符号化を施す．この際，k ビットの情報系列は n ビットの符号語に符号化される．各ブロックへの符号化の計算は独立しており，前後のブロッ

クの影響を受けない．この操作を，情報ビット系列 k ビットごとに繰り返し行う．

■畳み込み符号　k/n 畳み込み符号は，k ビットで区切られたブロックが符号化され，n ビットの符号語となる点ではブロック符号と変わりはない．しかし，ブロック符号と異なるのは各符号語が過去にわたる複数のブロックもかかわって逐次的に決定されるという点にある．つまり，前後のブロックの内容が異なれば，同じ k ビットを与えても異なる n ビットの符号語が生じることとなる．

d)　**誤り訂正**

■ハミング距離と最小距離　ここでは，まずハミング距離 [29] を例を挙げて説明する．ハミング距離は $d(\mathbf{u},\mathbf{v})$ で表され，

$$\left.\begin{array}{rcl}\mathbf{y} & = & (10100)\\ \mathbf{w_1} & = & (11100)\\ \mathbf{w_2} & = & (01111)\end{array}\right\} \tag{3}$$

のとき，$\mathbf{y}$ と $\mathbf{w_1}$ は 1 カ所，$\mathbf{y}$ と $\mathbf{w_2}$ は 4 カ所異なっており，

$$\left.\begin{array}{rcl}d(\mathbf{y},\mathbf{w_1}) & = & 1\\ d(\mathbf{y},\mathbf{w_2}) & = & 4\end{array}\right\} \tag{4}$$

である．

n ビットのビット列のうち符号語として使用されるのは $\mathbf{w_1},\mathbf{w_2},\cdots\mathbf{w_m}$ の M 種類である．この符号を構成する相違なる符号語間の距離の最小値を最小距離といい，d_{min} で表す．すなわち，

$$d_{min} = mind(\mathbf{w_i},\mathbf{w_j}) \quad i \neq j \tag{5}$$

である．

■誤り訂正　符号語から距離 t 以下のビット列の集合を，半径 t の小球で表す (図 11).

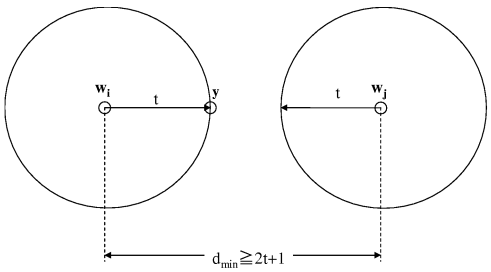

図 11: 最小距離と誤り訂正能力

各符号語を中心として半径 t の小球は，

$$d_{min} \geq 2t+1 \tag{6}$$

であれば，共通部分を持たない．送信語として $\mathbf{w_i}$ を送り，t ヶ所以下の誤り (これを以下，t 重誤りと呼ぶ) を生じて $\mathbf{y}$ が受信されたとすると，$\mathbf{y}$ は $\mathbf{w_i}$ に一番近いので，この誤りは一番近いものに訂正される．t 重の誤りまでは訂正可能な符号を，t 重誤り訂正符号という．

■リードソロモン符号　今までの符号はビット単位で誤り訂正を考えてきたが，現実には t が大きくなると符号の効率が悪くなり，実用性に乏しくなる．

リードソロモン符号 [30] では，すべてをバイト (これは 8 ビットに限らず，2^n ビットである) で表す．ハミング距離も，バイト単位で二つのベクトルの対応する要素を比べて，バイト単位に何カ所間違っているかで示し，符号の最小距離もこのバイト単位で測ることとなる．誤りもバイト単位に考える．$e_i = 0$ であれば，そのバイト y_i は誤りなしであり，$e_i \neq 0$ であれば，そのバイト y_i は誤りである．

この符号は，符号長 $n = 2^m - 1$，情報点数 $k = n - 2t$，最小距離 $2t+1$ であり，t 重バイト訂正が可能である．RS 符号は，同一の最小距離を持つ $GF(2^m)$ 上の線形符号のなかで最小の検査点数を持つ．線形符号の最小距離と検査点数の関係を与えるシングルトン限界式を満足する最大距離分離符号 (MDS 符号：Maximum Distance Separable Code) となっている．

たったの 3 ビットの誤りでも，すべて異なるバイトに発生した場合は 3 重バイト誤りになる．逆に 3 ビットの誤りがすべて同一のバイトで発生した場合は，1 重バイト誤りとなる．

e)　**インタリーブ**

連続して起きる誤り，すなわちバースト誤りにより，符号の誤り訂正限界を超えてしまうことは少なくない．再送が行われない限り，もはや正しい情報を復元することはできない．しかし，可能な限り多くの符号長の中に均等に誤りが分散すれば，誤り率が低い限り，長いバースト誤りの訂正可能となる確率は大きくなる．

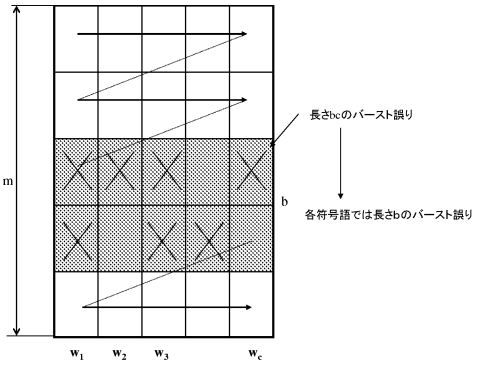

図 12: インターリーブ

たとえば，長さ b 以下のバースト誤りを訂正できる (n,k) 符号 C があるとする．この符号語を c 個，列方向に並べる．c 個の各符号語を図 12 の矢印のように行方向に操作して並べ直し，通信路に送り出す方法をインターリーブという．この並べ直し方は一例であり，実際には，目的に応じて適切なものを決定する．

網掛け部分にバースト誤りが生じても，各符号語に分散される．それが符号 C で訂正可能であれば，この誤りは訂正可能となる．従って，全体を一つの符号語と見て (nc,kc) 符号であり，長さ bc までのバースト誤りに対処することが可能となる．このような方法は一般的に用いられており，コンパクトディスクやディジタル放送にも使用されている．

6.　三次元パターンの要件

三次元パターンは，基本的には二次元コードを時間とともに書き換えたものであるが，実際にこれをチケット用として用いるためには，ただ単に時間とともに画面を書き換えればよいというものではなく，特に読み取り処理においていくつかの制約が存在する．

現状，自動改札機等でのゲートの認証時間は 0.5 秒程度であり，これを超えると渋滞が発生すると言われている．本システムでも同様に，ゲートにおけるパターン通信及び認証時間があまりに長くなってしまうと，渋滞の発生や必要な窓口数の増加等を招き，入場に支障をきたす．本研究のチケットにおける通信データ量は，電子署名として 1024bit，チケットのデータとして 512bit，合計で 1536bit である．これを可能な限り速く送受信する必要がある．

三次元パターン通信では，時間とともに画面が書き換え

られてしまう．バーコードなどの CCD スキャナやレーザスキャナでは，数回のスキャンを行いコードが読めるまで繰り返すことで読み取りを行える．一回で読みとる率（FRR:First Read Rate）が 10%を超えている場合には，いずれ読み取りは完了する [31]．しかし，画面が書き換えられてしまう上，待ち時間に制約のある本システムでは何回も読むわけにはいかない．そのため，FFR は可能な限り 100%に近づける必要がある．

また，表示画素と CCD 素子の干渉によってモアレが発生する場合が多い．これも時間とともに変化しない二次元コードであれば，手ぶれなどで発生位置が変化するため，フレーム間の平均化によって低減することが可能である．三次元パターン通信では，約 1 フレーム撮像後にはすでに画面の書き換えが行われているため，単独のフレーム内で処理を完結しなくてはならない．

一般的に，時間軸を含む三次元処理は，時間による変化の検出など，時間軸方向の相関性を用いて認識等を行うものであるが，本開発の三次元パターン通信では，むしろ時間軸が読み取り処理の制約となっている．

ここでの三次元パターンという名称は，時間変化を伴うコードの表示に対する呼称を意味するものと定義する．

7. 実装

本提案の三次元パターンは様々な携帯型情報端末の画面上に表示可能である．ここではデバイスとして最も有力な携帯電話端末の画面上に表示した場合の実装について説明する．図 13 に実装を示す．

図 13: 実装画面

現在主流となっている一般的な携帯電話では，120×160 ピクセルの画面解像度を持ち，その内 120 × 130 ピクセルの解像度部がアプリケーション側からの操作により任意に描き変え可能となっている．もちろん，携帯電話端末の解像度がこれ以外の機種も存在するが，本提案の三次元パターンは任意の画面解像度を持つ端末において有効である．

図 13 の例では，実データを埋め込んでいるデータエリアに対しては 3 × 3 ピクセルで 1 セルを構成し，各マーカに関しては 6 × 6 ピクセルで 1 セルを構成している．

(1) 位置マーカ

図 13 の端末画面四隅に存在するのが位置マーカである．位置マーカは読み取り装置が，端末の位置を検出するために用いられる．読み取り装置は，まず位置マーカを検出し，各マーカの位置を求めてから他のデータの読みとり処理を行う．ユーザは端末を手に持った状態で読み取り装置のカメラにかざすため，読み取り中に端末画面がカメラに対して傾いたり動いたりするが，読み取り中の傾きや動きも位置マーカによって検出できる．液晶や有機 EL などを用いた携帯型情報端末の画面は，紙面と異なりたわまないため，二次元バーコードよりも位置マーカを少なくしデータエリアを増やすことができる．本提案の三次元パターンでは，4 点のみの位置マーカにより端末画面の傾きや動きを検出していることが特徴である．位置マーカに関する読み取りの詳細は 8. 章で述べる．

クワイエットゾーンは位置マーカよりも外周に位置する常に白いエリアである．また，位置マーカの周囲 1 セル分の領域はクワイエットセルであり，これらのエリアを常に白くすることにより，位置マーカの捕捉を可能にしている．端末画面の縁は画面外の領域と接しており，端末外装の色や素材などによって，読み取り装置が画面外の領域をマーカとの連結成分として捕らえてしまうことがある．このような事態を避けるために位置マーカの周囲を常にクワイエットゾーンとし，確実に位置マーカを捕捉できるようにしている．

(2) 情報ゾーン

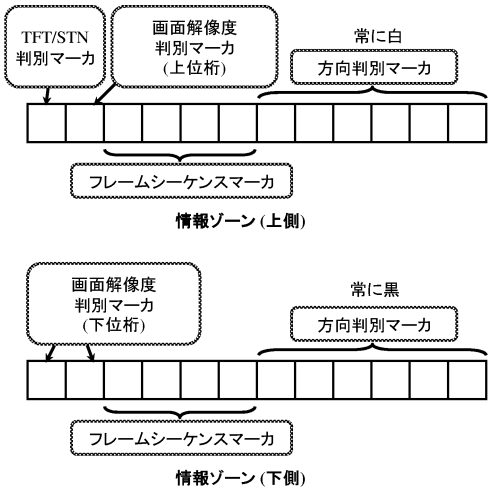

図 14: 情報ゾーン

図 13 中の情報ゾーンは図 14 に示すように分割されている．

情報ゾーンは以下のマーカを含む．

- **TFT/STN 判別マーカ**
- **画面解像度判別マーカ**
- **フレームシーケンスマーカ**
- **方向判別マーカ**

TFT/STN 判別マーカは，端末画面の種類が STN 液晶かそれ以外（TFT，TFD，有機 EL）かを判別するためのものである．本実装では STN 液晶を 0（黒）とし，それ以外の画面を 1（白）としている．フレームの更新検出はフレームシーケンスマーカを参照することによって行っており，STN 液晶は他の素子に比べて残光時間が非常に長いという特徴を持っているため，STN 液晶以外の画面ではフレームシーケンスマーカの更新を確認後 1 フレームだけ捨てて次のフレームから処理に入るが，STN 液晶の場合は数フレームを捨てて残光が無くなってから読みとり処理を行っている．なお，STN 液晶画面を持つ端末では故意に

フレームの描き変え時間を遅くしている．描き変える速度に応じてどの程度残光の影響が出るのかは (3) 節に示す．

画面解像度判別マーカは，上端側の情報ゾーンに 1 セル，下端側に 2 セルで合計 3 ビットを用意している．本実装では 3 ビットを用いて 8 通りの画面解像度を登録可能としている．図 13 では画面解像度判別マーカは 0 で，一般的な端末解像度である 120×130 ピクセルの場合を表している．これらのマーカは機種によって異なる値となる．コードを発行するサーバと端末は通常は HTTPS を用いて通信を行うため，サーバは HTTP ヘッダに含まれる User-Agent ヘッダから機種を判別してこれらのマーカを変更する．

フレームシーケンスマーカは図 14 に示すように上端側および下端側の情報ゾーンに同一のものが表示される．フレーム番号を読み誤ってしまうと，エラーにより読み取り処理が行えなくなるのではなく，フレーム番号を誤って処理を行ってしまうため，画面欠けや万一の読み誤りを考慮して上下に同一の信号を表示している．本実装ではフレームシーケンスマーカは上下端の情報ゾーンにそれぞれ 4 ビットずつ設けてあり，16 フレームまでのフレーム数に対応している．

方向判別マーカは，画面の上下左右の向きを示すために用いられる．このマーカは上端側と下端側で色が反転しており，図 14 に示すように本実装では上端側が常に白，下端側が常に黒であり，方向判別マーカの存在する側が向かって右側となっている．方向判別マーカもフレームシーケンスマーカと同様，読み誤ってしまうとエラーにより読み取り処理が行えなくなるのではなく，画面の向きを誤って処理してしまうため，画面欠けや万一の読み誤りを考慮して上下に同一の信号を表示している．

(3) 拡張情報ゾーン

本実装では未定義の領域である．画面解像度の種類やフレーム番号の表示などが現在の情報ゾーンだけでは足りなくなった場合に使用するために空白としている．

(4) データエリア

データエリアは，三次元パターンを用いて実際に通信を行うデータを表示する領域である．図 13 の実装ではデータセルの大きさを 3×3 ピクセルで 1 セルとして表現しており，データエリアにはクワイエットセルの 16 セル分を除いて $32 \times 35 - 16 = 1104$ セルが存在している．よって，1 フレームあたりのデータエリアのビット数は 1104 ビットである．ただし，1 セルを 3×3 ピクセルで構成した場合には読み誤りが発生する確率がある程度あるため，本実装では誤り訂正符号（ECC）とインタリーブを用いて最大で 30%までの読み誤りを訂正可能としている．ECC とインタリーブの構成に関しては 10. 節で詳細を説明する．また，読み誤りがどのような状況下においてどの程度発生するのかに関しては，11. 節に評価としてまとめて示す．

8. 読み取り処理

本提案の三次元パターンが二次元バーコードと最も異なる点は，時間軸を用いていることである．時間軸を用いることにより，画面解像度や画面の大きさにより 1 画面あたりの情報量が制限されていても，送信可能なデータ長に制限がなくなるというメリットがあるが，様々な端末での使用を可能とするため，二次元バーコードには無いいくつかの処理が必要となる．

(1) 二値化

図 15 に示すように，液晶や有機 EL など画面と読み取り装置側の CCD との干渉でモアレが発生する場合がある．

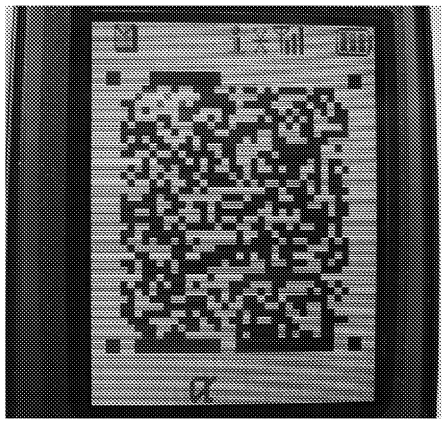

図 15: モアレの発生

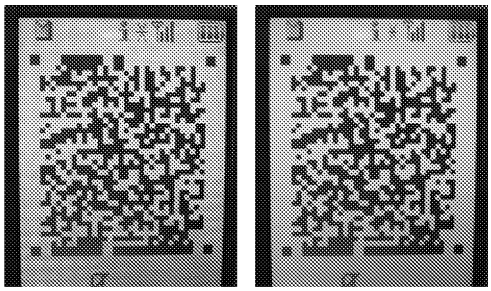

図 16: 中央値フィルタによるモアレの除去

モアレや欠陥画素，画面に付着した汚れによるノイズなどの影響を軽減させるため，図 16 に示すように，ノイズ除去フィルタとして中央値フィルタを用いた．これは，9. 節で詳細について述べるが，半透明の広告画像を重ねた場合の除去についても同様である．

ノイズ除去の後，二値化を行って位置マーカの検出を行う．ここで，位置マーカが黒であることと，後の (5) 節で述べる残留しているモアレの影響を避けるため，閾値を最大輝度の 15%という低い値に固定している．また，この二値化画像は位置マーカの検出のみに用い，他のセルの値の読み取りは二値化を行う前のノイズ除去後の画像図 16 を用いて行う．

(2) マーカパターン検出

図 17 に示すように，二値化処理の後，連結成分を検出し，位置マーカを検索する．

位置マーカは正方形であり，正方形の周囲長は $4\sqrt{\text{面積}}$ と等しいため，各連結成分の面積に対して平方根を取り，それを 4 倍した値がそれぞれの連結成分の周囲長と等しいものが位置マーカの候補に絞られる．ただし，実験により，中央値フィルタを通したフレーム画像では，正方形の角がとれて丸みを帯びてしまっているため，4 倍ではなく 3.6 倍以下になるものを位置マーカ候補としている．図 18 に示すように，候補の中から最外周に位置する 4 点を位置マーカとして決定し，4 点の内部の平均からをセル読み取りの閾値を決定する．

(3) シンボル位置の決定

携帯型情報端末は，撮像面に対して常に平行な向きに置かれるとは限らない．実際の利用では，ユーザは携帯電話

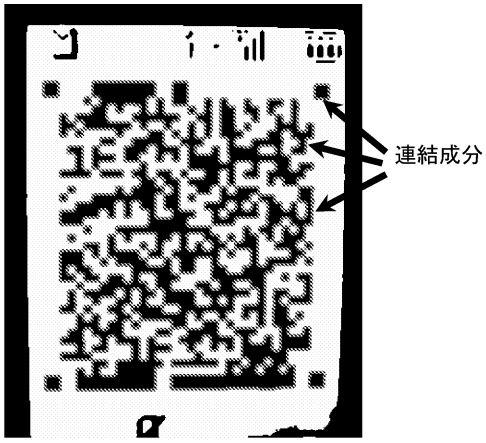

図 17: 連結成分の表示

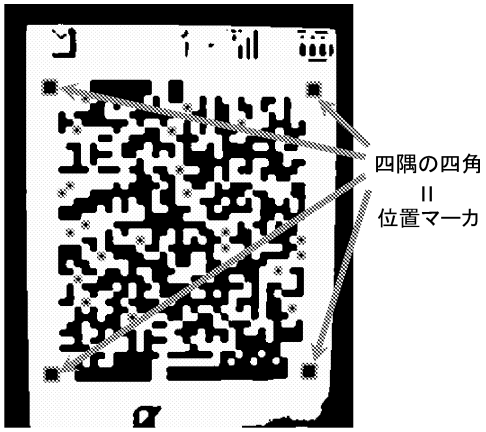

図 18: 位置マーカの検索

などの端末を読み取り装置のカメラ部にかざすが，人間の手によってかざされるため，画面が撮像面に対して少なからず非平行に傾く．しかし，液晶画面は紙面と異なりたわまわないため，四隅の各位置マーカから単位ベクトルを求めることで，この線形ひずみを補正している．データセルに関しては，線形ひずみを補正した座標にあるセルの値からデータを読み取っている．撮像面に対して垂直方向に傾いた場合の読み取り精度に関しては，(2) 節で述べる．

(4) 二重像の除去

三次元パターンは二次元バーコードと異なり画面を描き変えるために，残光の問題が発生する．フレームシーケンスマーカが変わって次のフレームを示しても図 19 のように前のフレームの残光が残っている状態で処理が行われると，読み誤りを生じる．

そこで，二重像のフレームを除去するために，読み取り中に画面の描き変わりから STN 以外は 1 フレーム，STN では数フレーム待って処理を開始する．STN とそれ以外の判別は，(2) 節の TFT/STN 判別マーカを用いて行う．なお，STN 液晶画面を持つ端末では，三次元パターンの描き変え速度が，その端末が持つ STN 液晶の残光時間を超えないように予め描き変え速度を遅くしている．STN 液晶画面を持つ端末の，残光による影響と読み取り精度に関しては，(3) 節で述べる．

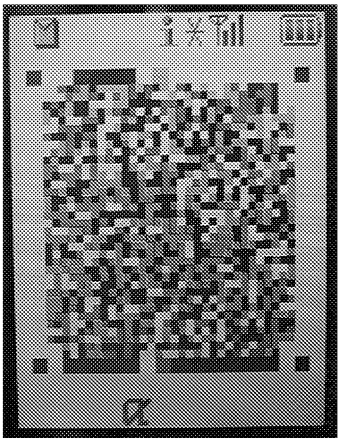

図 19: 二重像

図 20: 二値化画像のモアレ

(5) モアレの影響の軽減

位置マーカによって，線形ひずみを補正した座標にあるセルの画素値をもちいてデータを読み取ることは (3) 節で述べた．求められた座標の画素値は，中央値フィルタによって周囲の画素と平均化されているが，モアレによる画素値への影響を完全になくすことができているわけではない．位置マーカ検出の際には二値化の閾値を低くしているために問題は生じないが，閾値を白と黒の中間になるようにした場合，この閾値で二値化すると，図 20 に示すようなモアレの残存を確認できる．このモアレが読み誤りの原因となる．これは光学的なフィルタを用いるか，強力な平均化フィルタを掛けることで減少させられるが，面積の小さいセルが検出できなくなるなどの弊害がある．モアレは端末や角度，後述のオーバーレイによって発生量が変化するため，セルの画素値の平均を求めるなどの方法では部分毎に値が変わってしまい正しく読みとれない．図 20 からも，部分毎に発生の仕方が異なることが表れている．

この現象は，液晶の表示画素間の黒い隙間によって起きているため，黒いセルには影響を及ぼさないが，白いセルに重なって現れることに着目した．本手法では，セルの値を判定する際，セル中心とその周囲の画素値がすべて閾値

以下であれば黒，一つでも閾値を超えていれば白と判定することで，モアレの影響をほとんど受けない読み取りを可能としている．

9. 画像のオーバーレイ

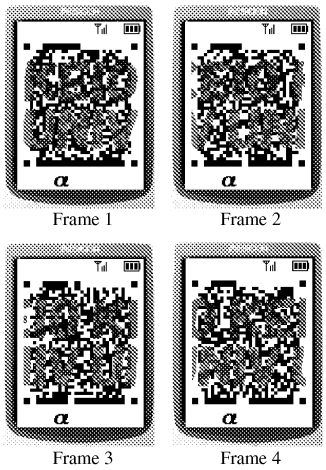

図 21: 画像のオーバーレイ

本提案の三次元パターンは，表示に使用するデータを白黒二値のセルで表現しているため，任意の画像をオーバーレイすることが可能である．図 21 は，三次元パターンに広告画像をオーバーレイした一例である．

画像のオーバーレイによる読み取り精度の詳細に関しては (4) 節で述べるが，図 21 のような画像を各フレームに重ねても，問題なくデータを読みとることが出来ている．そして，図 21 にも示しているように，重ねる画像をフレーム毎に変えてアニメーションさせることも可能である．画像の不透明度を上げるほど読み誤りが発生しやすくなるが，三次元パターン自体に誤り耐性を持たせているため，誤り訂正可能な範囲であれば読み誤りによる影響はないと言える．図 21 では，70%の不透明度で画像を三次元パターンの上にオーバーレイしている．不透明度と読み誤り率に関する詳細は (4) 節で述べる．

本実験では，上部が赤（RGB 値:255,0,0），下部が青（RGB 値:0,0,255）の 2 色画像を半透明化して三次元パターンにオーバーレイしている．なお，あまり色数が多い画像を重ねられないのは，三次元パターンの読み取りによる制約ではなく，実験に使用した数台の携帯電話端末のメモリ領域が少なく，容量の大きい画像データを同時に数多くバッファリングできないためである．

10. 読み誤りに対する耐性

本実装における読み取り率は 11. 節にて述べるが，携帯電話端末画面上に表示した三次元パターンには読み誤りが生じる．本実装は (4) 節よりデータエリアのセルを 3×3 ピクセルで構成している．各マーカは，データエリアのセルの 4 倍の面積である 6×6 ピクセルを用い読み誤りを防ぎ，さらにフレーム間で変化しないものは複数フレーム間の一致を，フレーム間で変化するものは同一フレーム内に 2 個表示し両者の一致を検査することで誤りを排除している．ここで，データエリアのセルも 6×6 ピクセルにしてしまうと，1 フレームあたり表示可能なビット数が 1104 ビットの 1/4 の 276 ビットになってしまう．そこで，本実装では誤り訂正符号（ECC）[32] とインタリーブを用いて三次元パターンのデータエリアで生じる読み誤りを訂正している．

(1) 誤り訂正符号

誤り訂正符号（ECC）は冗長ビットを付加することにより受信誤りを訂正することを可能とするものである．本実装では三次元パターンのデータエリアに表示されるビット列に対して短縮化リードソロモン (10,4) 符号,$GF(2^4)$ を使用している．(4) 節の実装では，データエリアには 1 フレームあたり 1104 ビットのデータを表示できる．データ 4 バイト (この符号では 1 バイトは 4 ビットを意味する) に対し，6 バイトの検査記号を付加し，合計 10 バイトのブロックの 3 バイトの誤りの訂正を可能としている．よって，本実装の三次元パターンは，最大では 30%の読み誤りが訂正できる．ただし，ECC の適用により，1 フレームあたりに埋め込まれている実データは 441.6 ビットとなり，1104 ビットの 40%まで減少する．しかし，ECC を用いないで 4 倍の面積のセルにして読み誤りを低減させた場合はデータ量が 25%になってしまうのに対して，本符号を適用した場合はデータ量の 40%を使用できるため，有利であるといえる．また，表示面積の大きなセルを用いた場合でも，端末画面の傾きや汚れ，光などの要因による読み誤りがなくなるわけではない．

マーカセルに関しては，読み誤った場合でも問題が起こらない工夫をしている．位置マーカでは一度捕捉したマーカの近辺の座標を再捕捉すれば誤りが減る．フレームシーケンスマーカ、方向判別マーカに関しては，上下の情報ゾーンに同一の信号を表示するようにして両者の一致性を検査している．TFT/STN 判別マーカや画面解像度判別マーカはフレームごとに書き換わらないため，読み誤りは少なく，また読み誤った場合はその後の読み取り自体が続行できない．このような対策により，マーカの読み誤りは起こりにくく通信品質への影響は少ない．しかしデータエリアのセルは読み誤りの 1 ビットの読み誤りでも致命的である．特に，鍵などのデータを表示した場合は認証で弾かれてしまうため，1 ビットでも誤りがあってはならない．特に，1 セルあたりの構成ピクセルを少なくして 1 フレームあたりの表示ビット数を上げた場合，誤り訂正は必要不可欠である．

(2) インタリーブ

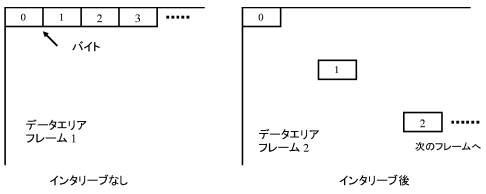

図 22: インターリーブ

(1) 節で述べたとおり，本実装では，ECC は情報 4 バイトに対して 6 バイトを付加して 10 バイトとしているが，全体の読み誤り率が 30%以下でも，この 10 バイト中に 4 バイト以上の読み誤りが発生すればそのブロックは誤り訂正が行えない．そのため，バイト単位でのインタリーブを用いて読み取り時のバーストエラーを分散させている．本提案では、このインタリーブを三次元に行っている．すなわち，連続した記号は各フレーム内で x 軸と y 軸方向，さらに各フレーム間に分散するようにしている．また，1 つの記号に含まれる 4 ビットは並べて表示される．

記号数の素因数にならない数を乗算して，その剰余をとることで，重複なく記号を分散できる．これを数式で表すと，全部で 1104 バイトの記号が存在するため，掛ける数

を 113 とすると，i 番目の記号の位置 P_i は，

$$P_i = 113 \cdot i \bmod 1104 \tag{7}$$

となる．i を 0 から数えると，図 22 の様に，連続する記号の位置は 1 フレーム 1 行 1 列，1 フレーム 13 行 5 列，1 フレーム 26 行 7 列，2 フレーム目 8 行 1 列…となる．

三次元パターンにおける読み誤りは，画面の傾き，書き換えやリフレッシュによる横方向のバースト誤り，液晶画面に付着したゴミ，外光による画面反射の影響による局所的な誤りが支配的であり，連続した読み誤りが出やすい．

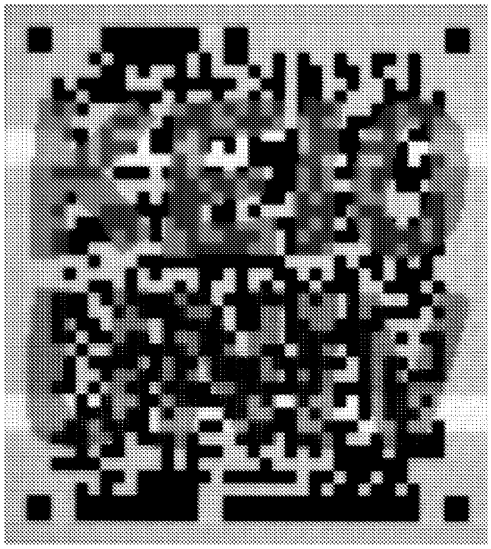

図 23: リフレッシュの様子

特に，画面リフレッシュの横方向の誤りは多く発生する．残光の短い有機 EL で見られる横方向のリフレッシュによる残光の態様を，図 23 に示す．この画像はわずかに電子シャッタの開放時間を伸ばしているため，実際にはより細い線となる．

符号語一つを構成するビット群は，4 ビットが正方形となるように並べた方がシンボル間距離が短いため印刷物などでは好ましく，実際の 2 次元バーコードも同様であるが，横方向の読み誤りが支配的であるため，本開発では 4 ビットを行方向に並べている．

(3) 再読み取り

三次元パターンではフレームの表示を繰りかえしているので，以上の方法によって誤り訂正を行ったのち，訂正不能な誤りが存在する場合は，繰り返し表示されるフレームから，誤りの存在する部分の再読み取りを行う．これはランダム誤りや，発生位置が変化するバースト誤りに有効である．しかし，画面上のゴミや濃すぎるオーバーレイなどで繰り返し表示されるフレームの同一箇所に生じる誤りに対しての効果は期待できない．

11. 評価

本提案の三次元パターンにおける認証速度及び精度について定量的に評価する．読み取り装置のカメラは，試作機では 6.1cm × 6.6cm の矩形断面の筒型構造となっており，開口部に携帯電話端末をかざして用いる．開口部から内蔵カメラのレンズまでの距離は 32cm であり，直接太陽光や照明光がレンズに入射することはない．使用時の外観を図 24 に示す．

実際の読み取り装置では，金属製の本体の上に FRP 成形品を乗せ，曲面形状に変更している．取り付けられたカ

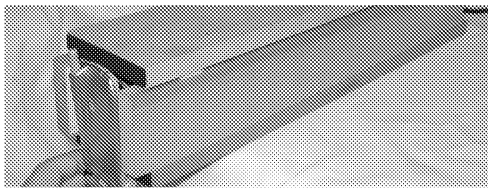

図 24: 読み取り装置 (試作品)

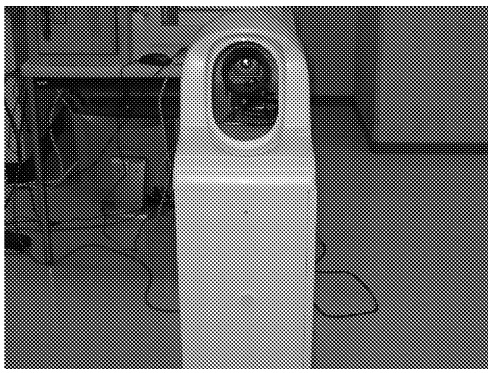

図 25: 読み取り装置

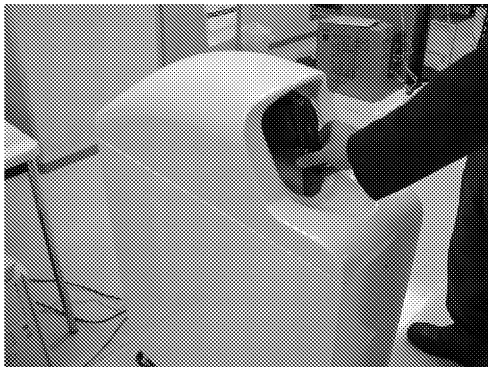

図 26: 使用時

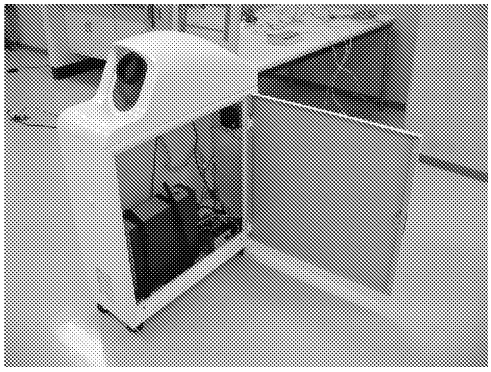

図 27: 内部構造

メラはわずかに上向きの傾きをもっているが，使用時は読み取り窓周囲に外乱光入射防止のための暗幕の貼付を行い，携帯端末を当てた時に画面以外の光が入射しないようになっているため，光学的は試作機と同様と見なせる．

両者で使用しているカメラは同一であり，1/3 型カラー CCD を用いた 640 × 480 画素のカメラ (SONY DFW-V500) であり，レンズは 25mm の単焦点レンズを用いている．カメラは IEEE1394 端子を通じて画像処理用の PC へと接続されている．実験は通常の蛍光灯照明のある屋内で行う．読み取り装置に光源はなく，すべての実験においてバックライトやフロントライトなどは点灯状態とする．消灯した場合には読み取り不能となるため，再度携帯のボタンを押すことで点灯させる必要がある．

(1) 認証速度

三次元パターンを用いて認証に使用した場合の認証速度について評価を行った．実運用での安全性を考慮し，本評価においては，ID 部に 512 ビット，データ署名部に 1024 ビットの RSA 公開鍵署名を用い，合計 1536 ビットを三次元パターン通信で読み取り装置に認識させ，読みとった三次元パターンから認証を行う．表 1 に認証に要するまでの時間を示す．この測定では、各携帯電話端末は可能な限り速く画面の描き変えを行っている．なお，STN 液晶を用いている P503iS に関しては，最大速度で画面を描き変えると，残光の影響でフレームシーケンスマーカを認識できないため，測定結果が出ていない．STN 液晶の残光を考慮した読み取り評価は (3) 節に記す．

表 1: 認証に要する時間

端末	時間 (ms)
N503i	0.40
D503i	0.33
SO503iS	0.44
P503iS	–
N2001	0.40

表 1 より、STN 液晶を除いては一般的な携帯電話端末で 0.44 秒以内の認証が可能であることが実証された．これは，現在使用されている鉄道の自動改札機と同程度の時間で三次元パターンの読み取りから認証までが行えることになる．

(2) 画面角度と認識率

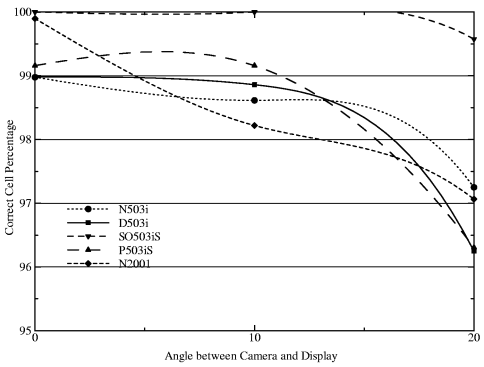

図 28: 画面角度と認識率の関係

図 28 は，携帯電話端末画面を読み取り装置の開口部から浮かせることで，カメラに対して傾けた場合の認識率の変化を示している．各機種各条件で 30 回の測定の平均値である．

傾きがない状態ではどの端末も 99% 以上の認識率を示している．機種によって角度がなくてもわずかに誤りが発生しているが，これは，横方向に行単位のバースト誤りが生じる場合が多いためで，画面の書き換えやリフレッシュ等の影響によるものと思われる．(2) 節に示すとおり，三次元パターンにはインタリーブを用いており，読み誤りのバイトは分散するため，横一列に誤りが発生しても問題はない．角度とともに誤りは徐々に増加するが，すべての機種において，20 度でも 96.3%以上の認識率を示している．画面が 30 度近い傾きを生じると，位置マーカの形状が長方形に変化し，マーカの検出が困難になるため，読み取り処理そのものが困難となる．特にフロントライトを持つ機種である D503i や N503i では，角度によってカメラ内にフロントライトが写り込み，妨害要因となるため，光源が見える方向に傾けた場合，この現象が起こりやすい．

実験においては位置が検出できる範囲では訂正不能な誤りは全く発生しなかった．三次元パターンは，少ない位置マーカで傾きにも対応することが可能であり，また送信ビット数に上限がないことから，誤り訂正に用いる検査ビットにも多くのビットを使用でき，誤りに耐性を持たせることができる点で二次元バーコードに対する優位性が伺える．

(3) STN 液晶の認識率

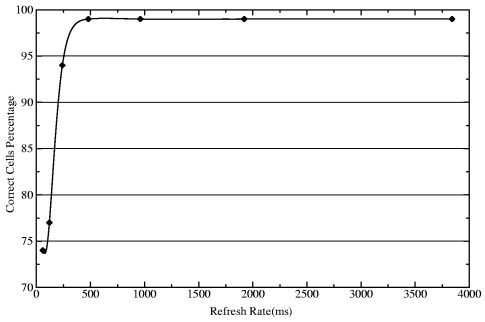

図 29: STN 液晶における描画速度と認識率の関係

STN 液晶は，TFT 液晶や TFD 液晶，有機 EL などと比較すると残光時間が非常に長い．そのため，P503iS 端末では，端末が描き変えることが可能な最大限の速度で三次元パターンを描画処理すると，残光の影響で正しく認識することが出来なくなる．図 29 は，P503iS における描画速度と三次元パターンの認識率を測定した結果である．

リフレッシュレートが 120ms の辺りからかろうじてフレームシーケンスマーカの読み取りが可能であったが，この状態では読み取り率は 75%未満と低い．500ms 以上では認識率に変化がないため，この端末の STN 液晶では約 0.5 秒で残光の影響が無くなることがわかる．(2) 節に示したとおり，STN 液晶を判別するマーカを設けているため，読み取りに時間はかかるものの対応が可能であり，本開発の他の評価において P503iS は画面書き換えに 500ms のウェイトを掛けて実験を行っている．

(4) 画像のオーバーレイによる認識率

図 30 は，画像のオーバーレイによる三次元パターン認識率の変化を示したものである．測定にあたりオーバーレイに用いた画像は，9. 章にあるように，図 21 に示される赤 (255,0,0) と青 (0,0,255) の 2 色画像である．図 30 の横軸はオーバーレイ画像の不透明度を表している．不透明度はオーバーレイ画像と三次元パターンの濃さの比率で求められ，不透明度 100%の時，画像の下にあるセルは見えな

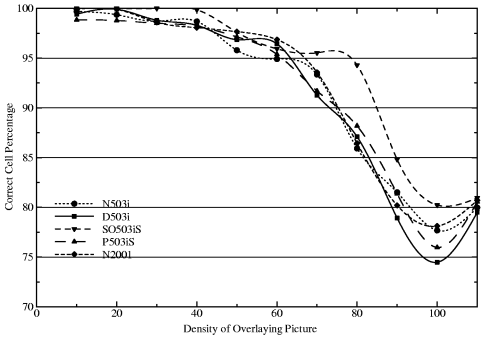

図 30: オーバーレイ画像と認識率の関係

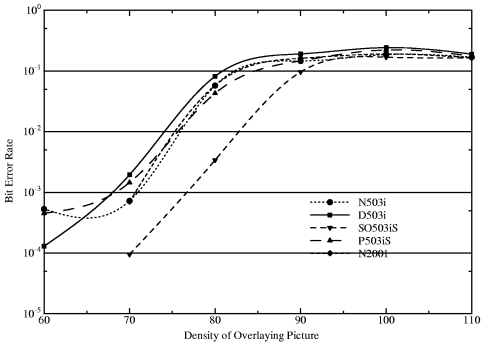

図 31: 訂正後の誤り率

くなる．なお，2 色のオーバーレイ画像と同一の形状のものの画素値を黒 (0,0,0) にして三次元パターンに不透明度 100%で重ねた場合を，グラフでは不透明度 110%の位置に記述した．

図 30 は，オーバーレイ画像の不透明度の増加とともに三次元パターンの認識率は低下することを示している．完全に黒となっている場合の値が，赤青 2 色の画像の不透明度 100%の値よりよいのは，表示するパターンを完全に黒でつぶしてしまうことで，色信号が周囲のセルに干渉する現象がなくなり，オーバーレイ画像近辺の読み誤り率が低下するためと推測される．

誤り訂正後の誤り率を，図 31 に示す．本実験において，50%以下の濃度ではすべての機種で，60%では一部の機種で誤り訂正不能な状態が発生しなかったため，図 31 に現れていない部分がある．図 21 では，不透明度 70%で画像をオーバーレイしているが，この濃度では，オーバーレイされた画像の影響により訂正不能な誤りが発生することが数回に 1 回程度起こる．しかし，誤りの量が少なく，発生位置にランダム性が高いため，再度の表示で同じ部分が欠落することはほとんどない．そのため，一回の再読み取りで補間することができる．時間的には多少影響があるものの，認証は可能である．これは (3) 節に示した再読み取りが有効に作用しているといえる．不透明度 80%以上では，SO503iS 以外の機種は認証不能であった．訂正後の誤り率が大幅に増加するとともに，オーバーレイ画像が同じフレームの同じ場所の画素が高い確率で読み取り不能になるため，誤り訂正できない部分の読み直しができないためである．また，訂正前と訂正後の誤り率を比較してもあまり改善が見られない．このような広い面積に繰り返し発生する誤りは，本提案の誤り訂正の限界を超えているといえる．なお，オーバーレイ画像が静止画の場合であっても動画の場合であっても，図 30 のグラフはほとんど変化することはない．これは同程度の面積がオーバーレイの影響を受けているならば，影響を受けるビットの位置に依存しないということである．オーバーレイ画像の縦方向の幅がセル数の 30%未満の 9 セルであれば，たとえデータエリアを塗りつぶしても訂正可能であり，横長の画像の影響は少ない．これらのことは，(2) 節で述べたインタリーブが正しく機能していることを示している．

12. まとめ

本開発の三次元パターン通信による認証は，鍵のビット長を制限されることなく，1024 ビット以上の RSA 公開鍵署名も使用することが可能である．署名をつける元となるデータの長さにも制限はない．また，表示されるデータのビット長は，端末の画面解像度に依存することなく，異なる解像度の端末でも同様のビット数の送信が可能である．そして，三次元パターンを実際に現行機種の携帯電話端末に実装し，11. 節で認証に掛かる時間や読み取り精度を評価することにより，認証デバイスとして実用に足るものであることを確認した．三次元パターンを用いた既存の携帯電話端末は，STN 液晶の機種を除いて 0.44 秒以下で認証可能である．手ぶれによる読み取り中の移動や傾きにも対応し，読み誤りに対する耐性もある．また，広告用の画像をオーバーレイした場合でも，濃度が濃すぎなければ認証が行われることも確認された．

また，本システムでは，ユーザのプライバシにかかわるユーザ ID や決済情報などは，チケット販売業者の管理下にあるチケット発行サーバでのみ扱われており，一回限りの OnetimeUserID を用いることで，ユーザの個人情報の流出を防いでいる．また，本チケットは，イベント開始の一定時間前になるまで取得できないため，攻撃者が解析やねつ造を行う時間をほとんど与えない．署名などはサーバ側で行い，ユーザ側の携帯電話では暗号化も復号化も行なわないため，暗号モジュールなどの追加ハードウェアを携帯電話に搭載する必要がなく，普遍的に利用できる．中途退場，再入場も可能であり，クーポンチケットのような回数券利用も，サーバ側で管理している情報を利用して実現可能である．本開発の三次元パターン通信を電子チケットに用いることで，既存の携帯電話端末に認証用デバイスを追加することなく，安全なサービスが可能となった．サービスが携帯電話からの操作で完結することも，大きな特徴の一つである．

今後の課題として，3 次元パターン通信の速度の向上があげられる．現時点の通信速度は，最大で約 4kbps(誤り訂正後) 程度と他の認証機器と比べて極端には速くはないため，鉄道の自動改札のような用途での利用を考えた場合には，現状では速度が十分であるか検討の余地がある．また，小規模なイベントにおいても，読み取りが早く確実な方が待ち時間は減少し，読み取り装置の数も減らすことができる．現状では，モアレ等の各種妨害により，1 画素単位での通信や輝度，色信号を用いた通信などは実現できていないが，このような要素も含めた高速化を目標の一つとしたい．

今後は，読み取り装置や信号形式の改良によって，高速化と信頼性の向上を進めて行くとともに，本システムをイベントのチケットや各種入場ゲートなど，認証が必要な部分で実際の運用を行い，本方式の実用性を検証していく予定である．

13. 参加企業及び機関

なし。

14. 参考文献

[1] 長屋隆之, 山崎知彦, 原昌宏, 野尻忠雄. 高速読取り対応 2 次元コード [QR コード] の開発, 1996.

[2] Jun Rekimoto and Yuji Ayatsuka. CyberCode: De-

signing Augmented Reality Environments with Visual Tags. Proceedings of Designing Augmented Reality Environments(DARE 2000), pp. 1–10, 2000.
[3] 中村英雄, 牧野秀夫, 山宮士郎, 前田義信, 廣野幹彦. 簡易読み取りを目的とした分割型二次元バーコードの検討. 電子情報通信学会技術研究報告, Vol. HCS98, No. 39, pp. 1–8, 1999.
[4] イープラス. http://eee.eplus.co.jp/.
[5] モバイルワン. http://www.target-one.co.jp/.
[6] 尾形利文, 牧野秀夫, 石井郁夫, 中静真. 非可視型バーコードを用いた視覚障害者用位置案内装置の研究. 電子情報通信学会論文誌, Vol. J80-D-II, No. 11, pp. 3101–3107, 1997.
[7] 牧野秀夫, 森下文仁, 阿部好夫, 山宮士郎, 長谷川勝, 石井郁夫, 中静真. 非可視型バーコードを用いた視覚障害者用物体案内方式の研究. 電子情報通信学会論文誌, Vol. J80-D-II, No. 11, pp. 3094–3100, 1997.
[8] 関涼子, 牧野秀夫, 渡邊新二, 石井郁夫, 中静真. 非可視型 2 次元コードを用いた画像処理と音声案内-顔写真コード化と図書案内への応用. 電子情報通信学会技術研究報告, Vol. MBE96, No. 73, pp. 85–92, 1996.
[9] 菅原哲也, 牧野秀夫, 石井郁夫, 中静真. 2 次元マークを用いた視覚障害者用物体案内装置. 電子情報通信学会技術研究報告, Vol. MBE94, No. 148, pp. 79–84, 1995.
[10] 辻井重男, 笠原正雄. 暗号と情報セキュリティ. 昭光堂, 1990.
[11] Douglas R. Stinson. CRYPTOGRAPHY: Theory and Practice. CRC Press Inc., 1995.
[12] 辻井重雄, 笠原正雄. 暗号と情報セキュリティ. 昭晃堂, 1990.
[13] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptsystems. Communications of the ACM, Vol. 21, No. 2, pp. 120–126, 1978.
[14] 電子署名及び認証業務に関する法律. （平成１２年法律第１０２号）, 2000.
[15] Ko Fujimura and Yoshiaki Nakajima. General-purpose Digital Ticket Framework. 3rd USENIX Workshop on Electronic Commerce, pp. 177–186, 1998.
[16] Ko Fujimura, Yoshiaki Nakajima, and Jun Sekine. Xml ticket: Generalized digital ticket definition language. The W3C Signed XML Workshop, 1999.
[17] Ko Fujimura, Hiroshi Kuno, Masayuki Terada, Kazuo Matsuyama, Yasunao Mizuno, and Jun Sekine. Digital-Ticket-Controlled Digital Ticket Circulation. 8th USENIX Security Symposium, pp. 229–238, 1999.
[18] Antonio Mana, Jesus Martinez, Sonia Matamoros, and Jose M. Troya. GSM-Ticket: Generic Secure Mobile Ticketing Service. Gemplus Developer Conference, pp. 1–7, 2001.
[19] Digital cellular telecommunications system (Phase 2+) : Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 8.3.0), 2000.
[20] Digital cellular telecommunications system (Phase 2+) : Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.14 version 8.3.0), 2000.
[21] 中尾寿朗, 荒尾真樹, 藤本幸一, 細野雅彦, 谷口正宏, 石川達也. モバイル端末を利用した鉄道デジタルチケットシステムの開発. 情報処理学会研究報告, Vol. 2001, No. 83, pp. 15–22, 2001.
[22] ぴあ (株). 次世代型デジタル・チケット利用システム. IPA 平成 10 年度補正事業産業・社会情報化基盤整備事業, 1999.
[23] ぴあ, 2000 年に電子チケット流通の実験開始. 日経エレクトロニクス 1 月 4 日号, No. 733, pp. 33–34, 1999.
[24] icePAY Japan. http://www.icepay.co.jp/.
[25] 吉田哲, 山下哲也, 橋本勝憲, 板橋達夫, 豊田充, 吉田敏之. 非接触 IC カードと携帯情報端末を利用した E コマースシステムの開発. 情報処理学会第 62 回全国大会予稿集特別トラック, Vol. 5, pp. 89–96, 2001.
[26] Pierre Bieber, J. Cazin, Pierre Girard, Jean Louis Lanet, Virginie Wiels, and Guy Zanon. Electronic Purse Applet Certification, Vol. 32. Electronic Notes in Theoretical Computer Science, 2000.
[27] Pierre Bieber, J. Cazin, Pierre Girard, Jean Louis Lanet, Virginie Wiels, and Guy Zanon. Checking Secure Interactions of Smart Card Applets. ESORICS 2000, pp. 1–16, 2000.
[28] モバイル電子チケットのビジネス要件・機能要件. 電子商取引推進協議会 モバイル EC-WG モバイル電子チケット TF, 2002.
[29] R. W. Hamming. Error detecting and error correcting codes. Bell System Technical Journal, Vol. 29, pp. 147–160, 1950.
[30] I. S. Reed and G. Solomon. Polynomial Codes over Certain Finite Field. Journal of Society of Industrial Application Math, Vol. 8, pp. 300–304, 1960.
[31] 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, 2001.
[32] Vera Pless. Introduction to the Theory of Error-Correcting Codes, 3rd Ed. Wiley-Interscience, 1998.