マルチメディア通信と分散処理　106－23
コンピュータセキュリティ　16－23
（２００２．２．１５）

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

宇田 隆哉†，伊藤 雅仁†，淡谷 浩平†，重野 寛†，松下 温†

†慶應義塾大学 理工学部 情報工学科 松下研究室

本論文は携帯型端末向け電子チケットシステムの提案である。本提案のシステムは商用に耐えうる強固なセキュリティを持ち、既存の携帯電話端末に特別なハードウェアを加えることなく、携帯型端末の機種を問わず電子チケットの発行から使用までを安全に管理できる。利用者は、携帯型端末からチケット発行サーバにアクセスし希望するチケットを購入した後、そ の携帯型端末画面上に電子チケットを表示し入場ゲートを通過する。本論文では、三次元パターン通信を用いることにより、電子チケットに付加した公開鍵暗号署名を任意の画面解像度を持つ端末上で扱うことを可能にした。本提案のシステムは、イベント会場の入場券や鉄道の切符などに幅広く利用可能である。

Digital Ticket System with 3-D Pattern Recognition for Cellular Phones

Ryuya Uda†, Masahito Ito†, Kohei Awaya†, Hiroshi Shigeno† and Yutaka Matsushita†

†Matsushita Laboratory, Faculty of Science & Technology, Keio University

A digital ticket 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 user can deal with everything related with a ticket such as issue, payment and showing with his cellular phone. He 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 no adding hardware module is needed. This system can be used for concert ticket, train ticket, etc.

1．はじめに

コンサートなどのイベントチケットや鉄道の切符を購入する場合、利用者はチケット販売店へ赴かなければならないのが現状である。近年では、電話や FAX、またインターネットなどからチケットを申し込むことも可能であるが、紙面のチケットを受け取るために手数料と送料が発生し、配送を待つために瞬時にチケットの利用が出来ないなど、コストと利便性の両面で様々な問題を抱えている。

このような状況を背景に、現在、様々なチケットに関する実験が開始されているが、すでに実用化されている Suica カード[12]のように IC カードを用いたものや、特殊なハードウェアデバイスを必要とするものでは、規格が統一されていない現在では個々のサービス専用のハードウェアを携帯せねばならず、利用者への負担が増大するだけで将来性に欠けていると言わざるを得ない。

一方、インターネットサービスが利用可能な携帯電話の契約者数が 2001 年 9 月末時点で約 4500 万人[13]を超える現在、携帯電話を用いたチケット販売に関する実験も開始されている。その中でも、既存の端末へハードウェアを追加することなく、携帯電話端末画面に一次元もしくは二次元バーコード[4][5][6][7][8][9][11]を表示することで電子チケットサービスを提供可能にする研究[14][15]もなされている。しかし、チケットの情報量は画面解像度の制約を受けるため、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の電子的なセキュリティに必要とされるビット数[2]には遠く及ばず、電子チケット自体が 1 枚の画像であるため単純な複製も容易であり、安全面に大きな問題を抱えていると言える。具体例としては、イープラスが行った実験[14]では扱われるデータは

10 進 8 桁のバーコードであり、ターゲットワンが行っている二次元バーコード方式[15]でも 18 から 34 キャラクタ程度に過ぎない。

そこで本論文では上記の点をふまえ、既存の携帯電話端末を用い、利用者がチケットの申し込みから利用までもを携帯電話端末のみで行える安全な電子チケット発行システムを提案する。本研究では、三次元パターンを用いて携帯電話端末の画面上にチケットの署名を表示することにより、公開鍵暗号[1]で一般的に安全と言われる 1024bit の電子署名[2][10]を利用可能にしている。また、チケット自体を一時的に発行される仮チケットと、実際に使用する本チケットに分離して扱うことにより、悪意のある第三者によってチケット署名が解析される時間を最小限に留めている。さらに、利用者を管理するユーザ ID と、イベント業者がチケットを管理するためのワンタイムユーザ ID を区別して扱い、顧客情報の流出も抑制している。本論文では、既存の携帯電話に専用のハードウェアを付加することなく、チケットの発行から使用までを 1024bit の公開鍵暗号に基づいて安全に行えるシステムを提案する。

2. 提案システム

本節では、電子チケットシステムの概要について述べる。本論文の電子チケット発行システムは、三次元パターン通信を用いて入場口端末での認証を行う。三次元パターンを用いることにより、画面表示可能なビット数の制限を無くし、一次元バーコードや二次元バーコードを用いた電子チケットでは不可能だった 1024bit の公開鍵暗号署名が使用可能となる。これにより、特殊な認証用ハードウェアモジュールを携帯電話端末に付加することなく、既存の携帯電話端末をそのまま利用した安全な電子チケットサービスが提供できる。

2.1 システム概要

図 1 に、本システムの概要を示す。

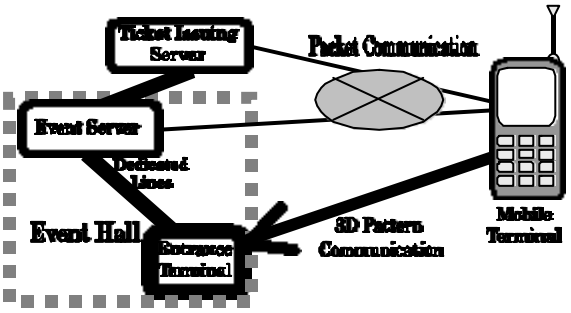

図 1 The relationship with each server and each terminal

本システムの利用者は、携帯電話端末を用いてチケット発行サーバにアクセスし、希望するチケットの発行手続きを行う。この時点では仮チケットが発行され、実際に使用する本チケットを得るには、次にイベントサーバへアクセスする。これらのアクセスは携帯電話端末のインターネットサービス機能を用いて行われる。チケット発行サーバは、信頼のおける機関によって運営される、ユーザのチケット購入や決済などを管理するサーバであり、一時的なチケットである仮チケットの発行を行う。チケットサーバはチケット発行サービスを通して 1 つであり、様々なイベント業者が運営するイベント多数のサーバと連携してサービスを提供する。一方、イベントサーバは、コンサートチケットや鉄道の切符といったイベント用のチケットを扱う業者によって管理されるサーバである。チケット発行サーバとイベントサーバ間は専用線で接続される。

入場口端末はイベント会場のゲートに設置されており、イベントサーバと LAN で繋がっている。利用者が電子チケットを使用する際には、携帯電話端末の画面に三次元パターンを表示し、そのパターンを入場口端末のカメラに翳すことで認証を行う。入場口端末は、三次元パターン通信によって得られた署名データと、イベントサーバのデータベース内のチケット情報とを比較し、利用者の入場の可否を決定する。このとき、イベントサーバは使用済みチケットの無効化など、入場口端末における認証に関する制御も行う。

3. チケット発行プロセス

本システムにおけるチケット発行のプロセスは、ユーザ登録、仮チケット発行、本チケット発行の 3 段階に分類される。

3.1 ユーザ登録

本システムのユーザ（利用者）は、まずチケット発行サーバにアクセスし、チケット発行サービスに対してユーザ登録を行う。この時点でそのユーザ固有の UserID 及び Password が発行され、以後、仮チケット発行及び決済に関わる一切のサービスの処理は、この UserID 及び Password を用いて行われる。登録されるユーザの個人情報は、氏名、住所、電話番号、クレジットカード番号など、決済を可能とするものである。このとき、携帯電話の端末番号など、可能であれば携帯電話端末を特定できるものも記録するのが望ましい。ユーザ登録で扱われた個人情報及び UserID、Password は、プライバシー保護のため本チケット発行サーバのみで扱われ、外部に送信されることはない。

3.2 仮チケット発行

図 2 に仮チケット発行の手順を示す。

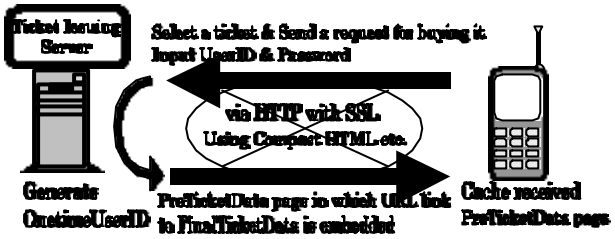

図 2 The Procedure for issuing PreTicket

チケット購入を希望するユーザは、携帯電話端末を用いて、SSL で暗号化された HTTP 上でチケット発行サーバにアクセスする。ここで、ユーザは購入するチケットを選択し、UserID 及び Password と共に購入要求を送信する。チケット発行サーバは購入要求を受け取ると、そのユーザに対し、購入したそのチケットの処理に関する手続きのみに有効となる OnetimeUserID と、一時的なチケットとして三次元パターンの埋め込まれていない仮チケットを発行する。仮チケットは、最終的な本チケットへアクセスするための URL リンクやアクセスコードなどを含む PreTicketData として、ユーザの携帯電話端末にキャッシュされ保存される。一例として、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を電子メールなどの形式でキャッシュするか、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、チケットを購入した証明として受け取る本チケットへの引換券である。ユーザは、購入したチケットをキャンセルするなどの場合を除き、このチケットに関してはこれ以後チケット発行サーバではなく、そのチケットを扱うイベントサーバと通信する。その時にはユーザの個人情報とは結びつくことのない OnetimeUserID 及び PreTicketData が扱われる。

3.3 本チケット発行

図 3 に本チケットの発行手順を示す。

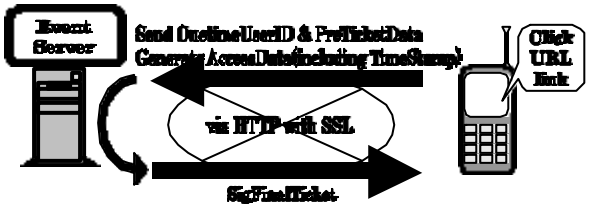

図 3 The Procedure for issuing FinalTicket

ユーザは、本チケットの発行が許可された後、3.2 節で説明した仮チケットを用いて、仮チケットに記載された URL から、そのチケットを扱うイベントのイベントサーバへアクセスし、本チケット発行手続きを行う。イベントサーバはイベントごとに設置されており、そのイベントに関連する入退場処理や三次元パターンを含む本チケットの発行などを管理する。コンサートなどのイベントの場合、イベントサーバは会場内に設置されており、イベント業者や会場運営者が管理する。イベントサーバの設置は浮動であり、本チケットの発行はイベントサーバ設置後にしか行うことが出来ない。しかし、イベントサーバへのアクセス可能時刻を設定することにより、本チケットの発行が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されるため、悪意のある第三者がチケットの解析や偽造を行うための時間が短くなり、より高い安全性を実現することが可能となる。

イベントサーバは、本チケット発行開始時刻前に、チケット発行サーバより OnetimeUserID や PreTicketData と本チケットの内容（FinalTicketData）との対応関係を通知されている。しかし、OnetimeUserID の発行はランダムであるため、イベントサーバを運営する業者にはユーザの個人情報が漏洩せず、イベントサーバを運営する業者の管理体制が杜撰であったり、悪意のある業者がイベントサーバを運営していたとしても、ユーザのプライバシーは保護される。

本チケット発行手続きにおいては、ユーザはイベントサーバに対して OnetimeUserID 及び PreTicketData を送信する。この時点で、ユーザのアクセス情報から AccessData が生成される。AccessData は、本チケットが有効期限切れになった場合などの再発行の際に用いるタイムスタンプを必ず含んでおり、これ以外の情報としては、携帯電話端末の端末 ID やアクセス元基地局の固有 ID など、任意の情報を含むことが可能である。イベントサーバは受信した情報を処理し、受信情報が正当であれば、入場時に使用される本チケットの署名である SigFinalTicket をユーザの携帯電話端末に送信する。

SigFinalTicket は、OnetimeUserID、AccessData、FinalTicketData の 3 つを連続的に結合させた値もしくは排他的論理和を計算した値に対してハッシュ計算を行い、そのハッシュ値をイベント用の RSA 秘密鍵で暗号化したデータである。今回は、一般に半永久的に安全とされる[10]1024bit の鍵を用いているが、各イベント毎に 512bit や 2048bit などの異なった強度の鍵や、RSA 以外の異なった公開鍵暗号アルゴリズムを用いることも可能である。また、OnetimeUserID、AccessData、FinalTicketData は、ハッシュ値を使用するため、各データ長はイベント毎もしくはチケット毎に任意で構わない。特に、座席番号情報やイベントの種類情報などを含む FinalTicketData の書式を任意とすることにより、スケーラビリティや拡張性を高めている。ユーザの端末に送信される情報は本チケット

の署名であり、本チケットの具体的なデータである FinalTicketData はユーザの端末には送信されないため、悪意のあるユーザによるチケットの解析・改竄・偽造は一層困難となる。

さらに本チケットには、改竄による不正使用を防ぐための有効期限が定められている。イベント会場の入り口が混雑していたり開場時刻に遅刻するなどして、本チケットを有効期限内に使用できなかった場合は、本チケット再発行の手続きが必要となる。このとき、ユーザのアクセスにより新たな AccessData が生成され、同じ OnetimeUserID によるチケットが複数存在した場合でも、古いタイムスタンプを持つ AccessData に基づくチケットから順にイベントサーバ上で無効となってゆく。

4. 入場管理

4.1 入場

図 4 に入場の手順を示す。

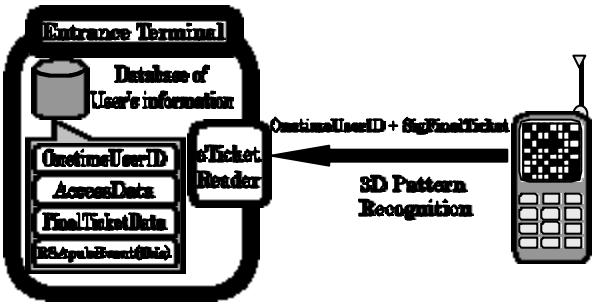

図 4 The procedure for entrance

入場口端末は事前にチケットに関連するデータをチケット発行サーバより受け取っている。図 4 に示すように、そのデータは OnetimeUserID、AccessData、FinalTicketData 及びそのイベント用公開鍵暗号ペアの公開鍵である。これらのデータは、本チケットがユーザに再発行される場合は、その都度必要に応じて部分的に更新される。

ユーザは、入場ゲートを通過する際に、入場口端末のチケット読み取り装置に対し、携帯電話端末の画面に表示された三次元パターンを提示する。三次元パターンとして送信されるのは OnetimeUserID 及び SigFinalTicket であり、入場口端末は読み取り装置から受け取った SigFinalTicket をイベントサーバの公開鍵で復号化し、イベントサーバの OnetimeUserID、AccessData、FinalTicketData のハッシュ値と比較する。このハッシュ値が同一のものであれば、読み取った OnetimeUserID は正統なものであるため、ユーザにゲートの通過を許可する。

4.2 再入場

本システムはユーザの不正な再入場も防ぐ仕組みを持つ。一例として、一度入場したユーザが他人の携帯電話端末を複数台借りて退場し、それらの端末を別の人間に渡した後、彼らと共に入場するような不正行為が挙げられる。

そこで本システムでは、ユーザの入場時に OnetimeUserID をロックし、ロックされた状態ではチケットは使用済みとして扱われ、チケットの二重使用を禁止している。そして、ユーザがイベント会場から一時退場する場合は退場口端末に三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。
ユーザの再入場時には、入場口端末は OnetimeUserID を再ロックする。この退場口端末は入場口端末と兼用で、ゲートの通過方向で役割を切り替えることも可能である。

5. 三次元パターン通信

三次元パターンは利用目的や性質において、バーコードとは一線を画すものである。
バーコードが物体の識別用に印刷することを想定して作られた印[4][5]であるのに対して、三次元パターンでは時間軸を使用することにより、
表示デバイスや読み取り装置の解像度・色数などに制限されることなく、
任意の長さのデータを送信可能な通信手段である。
本論文では電子チケットの証明に用いているが、一般的な通信手段として
汎用性に富んだものであると言える。

5.1 二次元バーコード

図 5 に示すように、二次元バーコードはセルの集合で表現された模様である。

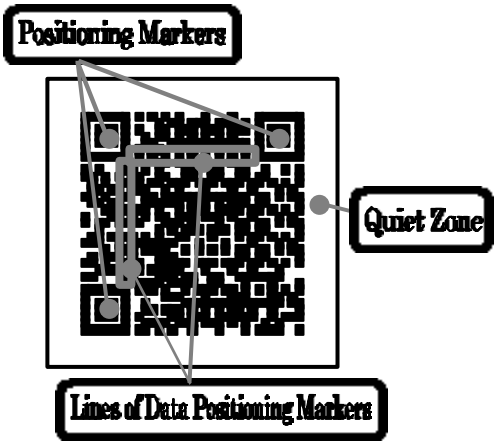

図 5 2-D barcode

黒と白に塗り分けられたセルは、それぞれ“0”と“1”を表しており、ひとつのセルで 1bit のデータを表現する。そして、それらのセルが縦軸と横軸に沿って平面上に配置されている。

図 5 に示されている二次元バーコードはデンソーが開発した QR コード[6]と呼ばれるものである。画面隅に配置されている大きな 3 つのセル及びその大きなセル間を繋ぐ帯状の領域は位置マーカと呼ばれるもので、スキャナに対してバーコードの位置を特定するために使用される。位置マーカよりも外周の白い領域はクワイエットゾーンと呼ばれ、スキャナが位置マーカを判別する際に認識し易くするために存在する。

5.2 三次元パターン

本論文で提案する三次元パターンは、データを画面の縦軸、横軸、時間軸に沿って
三次元に配置したものである。本研究で携帯電話端末画面に実装した
三次元パターンの構成を図 6 に示す。

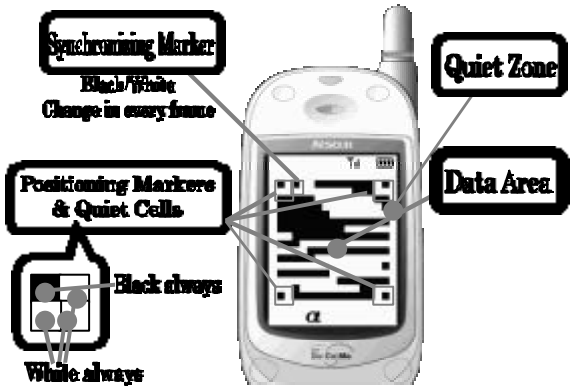

図 6 3-D pattern

三次元パターンは、画面外部から表示領域を識別するためのクワイエットゾーンで周囲を囲まれており、四隅に位置マーカ、上端にフレームの変化に追従するための同期マーカ、そしてそれ以外の部分にデータ領域を持つ。

位置マーカは、表示画面の位置を検出するために用いられる。通常、二次元バーコードにおいては、印刷物のたわみ、折れ等に対応するために、複数の位置マーカを埋め込んでいるもの[6][8][11]が多い。一方、液晶画面はたわむことはなく、傾きや回転によって発生する変形は線形であるため、四隅の位置が特定できれば画面内の各セルの位置は特定可能である。そのため、本研究では位置マーカは四隅のみに配置し、その分 1 画面中に表示可能なデータ量を増加させている。位置マーカは、読み取り中は常に携帯電話端末画面の四隅の位置を読み取り装置に対して通知しているため、読み取り中に端末画面が平行移動したり上下左右の向きが変化してもパターン認識に問題はない。さらに、位置マーカによって、三次元パターンの読み取り開始前もしくは読み取り中に、読み取り装置のカメラのレンズ面に対して端末の画面が平行でなくなったとしても、4 点の位置マーカから端末画面の傾きを計算し、正しく三次元パターン認識が行えるようにしている。

同期マーカは、奇数フレームと偶数フレームで白と黒の反転を繰り返す。読み取り装置は、同期マーカの変化を検出することで、画面の書き換えを検知する。これは、携帯電話端末の種類によって、画面を描き変える速度が異なるため、複数フレームに渡って偶然同じパターンが表示された場合と、同一のフレームが長時間表示されている場合とを区別する必要があるからである。本実装では読み取り装置は毎秒 30 フレームの速度で画像処理を行っており、同期マーカの色が反転した時点でフレームが切り替わったものとして処理を行っている。なお、読み取りを開始するフレームとしてプリアンブルフレームを用意した。プリアンブルフレームでは位置マーカ以外の全てのセルが白の状態になっている。また、同期マーカは、画面の上下の向きを特定するためにも使用している。

本研究による実装では、携帯電話端末画面上に三次元パターンを表示する際に、i モード端末では i アプリ、J-SKY 端末では PNG 画像の連続表示を用いたが、Java アプリケーションやアニメーション GIF 画像など、場合により様々な手段を用いて携帯型端末の画面で三次元パターン通信を行うことが可能である。

6. 実装及び評価

本システムの実装においては、チケット用に有効な表示範囲が 120x130 の画面解像度を持つ一般的な i モード端末と J-SKY 端末を用いて、三次元パターンの 1 セルの大きさを 7×7 画素、1 フレームあたり 17×16 セルとした。そのため、1 フレームで 223bit のデータを送信可能である。三次元パターン通信を用いた本電子チケットシステムでは、十分な安全性を実現することを前提に、OnetimeUserID 部に 512bit、SigFinalTicket 部を 1024bit とし、合計 1536bit をプリアンブルフレームを含み 8 フレームで送信している。読み取りには市販の DV カメラを用い、DV 圧縮信号を IEEE1394 で送信し、360×240 画素（約 8 万画素相当）の解像度でデコードした。各フレームの切り替え速度は携帯電話端末の機種と状態に依存するため、数台の携帯電話を用いて測定したところ、通信開始から認証までの時間は高速な端末で 1.6 秒から 2.2 秒程度、遅い端末で 6 秒程度であった。

7. まとめ

本論文では、携帯電話を用いて、特別な追加デバイス等を付加することなく、公開鍵暗号に基づく安全な電子署名を用いた電子チケットを利用可能なシステムと、そのシステムを実現するための三次元パターン通信を提案した。本システムでは、ユーザはチケットの購入から利用までを、既存の携帯電話端末を用いて行うことができる。

本システムでは、ユーザのプライバシーにかかわる個人情報や決済情報などは、通信キャリアなどが管理する認証局を兼ねたチケット発行サーバでのみ扱われ、イベントサーバに対しては 1 回限り使用される OnetimeUserID を用いることで、ユーザの個人情報流出を防いでいる。また、三次元パターンが埋め込まれた本チケットは、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、攻撃者に解析・改竄を行う時間を与えない。そして、公開鍵暗号に基づく電子チケットの署名はサーバ側で行われ、ユーザの携帯電話端末上では暗号・復号の計算を行わないため、演算能力が低くメモリ領域の少ない端末であっても、特別なハードウェアモジュールを追加することなく本システムによるサービスが利用可能となる。

本システムが提供するサービスでは、中途退場や再入場に関しても安全に処理することが出来、チケットの使用状況はイベントサーバ側で管理されるため、クーポンチケットのような回数券としての利用も可能である。また、本研究の三次元パターン通信は、端末画面の解像度に依存せずに任意のビット長を持つデータ列を送信可能とする技術であるため、本論文の電子チケット発行システムは、画面の書き換えが可能であれば携帯電話端末の機種を選ばず、i-mode、J-SKY、au などのブラウザフォン、さらには PDA、携帯型 PC など様々な端末で利用可能である。

最後に、今後の課題としては、三次元パターン通信の速度向上が必須だと言える。通常、自動改札のようなゲートを通過する際には、認証に掛かる時間が 0.5 秒程度でないとスムーズに入場列が流れないと言われている。今後は、読み取り装置や信号形式の改良によって、高速化と読み取りエラー[3]に対する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。

参考文献

1) 櫻井幸一, "暗号理論の基礎", 共立出版株式会社,1996.

2) 辻井重男, "暗号と情報セキュリティ", 昭晃堂, 1990.

3) ヴェラ・プレス, "符号理論入門", ワイリー・ジャパン・インコーポレイテッド, 1984.

4) 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.

5) 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.

6) 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", 情報処理学会第 52 回全国大会, Vol.2, pp.253-254, 1996.

7) 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, MBE96-73, pp.85-92, 1996.

8) 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, HCS98-39, pp.1-8, 1999.

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, MBE94-148, pp.79-84, 1995.

10) Rivest, R.L., Shamir, A., Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptsystems", Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

11) Jun Rekimoto, Yuji Ayatsuka, "CyberCode: Designing Augmented Reality Environments with Visual Tags", Designing Augmented Reality Environments (DARE 2000), 2000.

12) ＪＲ東日本: Suica, http://www.jreast.co.jp/suica/

13) 総務省総合通信基盤局: インターネット接続サービスの利用者数等の推移【平成 13 年 10 月】(速報), 2001.

14) エンタテインメントプラス: イープラス, http://www.eplus.co.jp/

15) ターゲットワン: モバイルワン, http://www.target-one.co.jp/.