平成 13 年度

学士学位論文

モバイル端末を用いたチケット課金方式

The system for making ticket reservations using mobile phone terminals.

1020269　　越智 裕架子

指導教員　　清水 明宏

2002 年 2 月 8 日

高知工科大学 情報システム工学科

要 旨

モバイル端末を用いたチケット課金方式

越智 裕架子

インターネットを利用した様々なサービスが提供されている．

このうち，チケット予約サービスは，従来のチケット予約をインターネットに代替する事によって，ユーザの利便性を向上させているサービスとして，多く利用されている．しかし，最終的にユーザがチケットを受け取るという手間は不可欠であり，ユーザの利便性という観点から最適であるとはいえない．

この問題は，このサービスにおいて課金システムを付加する事によって解消できると考えられるが，この場合，個人情報をインターネット上でやりとりしなければならないため，個人情報の漏洩のという問題が発生する．また，暗号技術を組み合わせてクレジットカードで決済する方法は多く利用されているが，クレジットカードにはユーザに利用資格制限があり，子供が使えない等の問題がある．

そこで，本研究はこれらの問題を解決する新しい流通システムを提案する．提案方式ではまず，ユーザ制限のない，既存のプリペイド課金システムを用いる．更に，ワンタイムパスワード認証方式である SAS プロトコルを応用し，課金とチケット配信を同時に安全に行う事のできるチケット配信プロトコルを提案する．

提案プロトコルにより，ユーザの負荷を大幅に軽減するチケット配信サービス環境を提案する．さらに，提案プロトコルの中核処理となる課金システムのシミュレータを作成し，その有効性についてを検討する．

キーワード　インターネット，モバイル端末，チケット配信，課金，認証

Abstract

The system for making ticket reservations using mobile phone terminals.

The internet is widespread now . Many companies provide a lot of services . One thing of all , ticket reservations using mobile phone terminals . This system is more convenient than the usual ticket reservation systems .

However ,it does not save time because you still have to pick-up the ticket. That is why this sort of system is not optimal for many users. This problem can be solved if we are able to pay through the internet . This creates another problem . Private information might be leaked . Settlement of account through the inter-net is already available . But children are not able to use credit cards . Again it is not optimal for many users . This research solves these problems and proposes a new system for circulation .

First , it takes advantage of a system for circulation using a prepaid card .To address the problem as a main subject with the distribution of tickets , I will apply the one-time password authentication of SAS protocol ,from our research materials from last year . I propose a system for paying for and distributing tickets that is safe . In this proposal I have in view a plan to distribute tickets without to wasting time . A simulation program will be used to test the effectiveness of the core management paying system.

key words Internet , Mobile phone terminals , Distribution , Making a payment , Certification

目次

図目次

第１章

はじめに

数々の情報は電子化・デジタル化され，従来複雑であった作業もコンピュータによって高速な処理が実現されるという場面が多くある．現在, コンピュータはごく普通に私たちの身近に存在し，生活の一部として欠かせないものとなっているのが実状である．

これに伴いインターネットも広く普及している．今やインターネットは企業や研究者だけでなく，私たちの一般の生活において多くの場で利用されたりと，あらゆる層の人達の日常的なものとして溶け込んでいる．これはインターネットを利用したサービスが増えたほか, 学校教育等あらゆる場面で社会全体がインターネットを取り入れる動向にある事が言える．

そして，情報流通の形態として，飛躍的な普及率からその代表とも言える，携帯電話においては 2001 年 12 月データで 67,101,100 台となっている．この普及率は驚異的であり，その要因としてモバイル端末であるという利点や個人への浸透性に加えて，電話の機能を越え，メールやインターネットの利用が可能になっている事があげられる．現在は，固定電話を利用せず，家族でも個人単位で携帯電話を持つという人も少なくない．

こういった現状から，インターネットや携帯電話を利用したサービスはますます増加している．

その一つに，インターネットを利用したチケット予約サービスがある．これは航空券の予約等に利用されており，従来の電話予約をインターネットで代替する事によって，２４時間受付を可能にし，ユーザへの時間的利便性を向上させたサービスである．

しかし，このサービスの中で一点，物（チケット）のやりとりをするという作業は不可欠となっている．例えば，航空券の予約の場合として，予約等はインターネット上で処理されるにも関わらず，搭乗するまでにチケットを受け取るという手間はどうしても省くことがで

きない．これでは消費者の時間の制約が加わり最適とは言えない．

この，チケットを受け取る手間が不可欠である要因は，チケットと引き換えに支払いを行わなければならないためである．これより，支払いを予約と同じくインターネット上で処理する事ができれば，解消される問題と考えられる．しかし，支払いをするための課金システムをインターネット上の処理として付加する事は，予約処理のみの場合と異なり予約情報に加えて個人情報（口座番号等）をインターネット上に掲載しなくてはならないため，個人情報の漏洩の問題が発生する．このためセキュアなルートの確保が前提であり，最重要となる．現在既存のサービスとしては，クレジットを利用したインターネット決済がある．しかし，この場合クレジットは子供が利用できないため，ユーザに制限が加わり最適とはいえない．

本論文ではこのような問題を解消するべく，新しい流通システムのプロトコルを提案する．また，こうしたサービスを提供するに当たって，ユーザだけでなく，コンテンツ提供者側にとってもメリットがもたらせられるような，より実用性の高いシステム設計を行う．

そこで，既存のプリペイド課金システムを利用し，本研究の本質であるプリペイド後のチケット配信をセキュアに行うために，昨年度当研究室ですすめられていた SAS のプロトコルを応用し，課金とチケット配信を同時に安全に行う事のできるプロトコルを提案する．

これによって，ユーザ制限も加わらずチケットを取りに行く手間のない，すなわちユーザに時間の制約負荷を与えない，チケット配信サービス環境の構築を目指す．

そして，最も重要である課金システムのシミュレータを作成し，その有効性を検討する．

第 2 章

既存のチケット配信方式

2.1　電子チケット

現在チケット配信の新しい試みとして，電子チケットというものがある．これは携帯電話でチケットを購入し，その携帯電話がそのままチケットになるというシステムである．

イープラスとアランが共同で販売するこの電子チケットは，既に販売を開始しており販売しているチケットの 4 割強が電子チケットで売買された．

電子チケットの利点は，その手続きの速さにある．従来は予約して，紙のチケットの配送期間が必要なためカード決済の場合で 7 日前までというように受付期間が限られる．しかし電子チケットの場合，その直前まで受付，販売が可能である．

また送料の面でも，従来では 500 円程の送料が必要なため，1000 円程度の低価チケットの販売ができなかったが，電子チケットの場合送料を無料にできるため，チケットの価格に関わらず販売が可能になる．

この電子チケットは “ 携帯電話の Web ページに配信されるバーコード ” という形で提供される．購入からイベント入場までの流れは概略で次のようになる．

1. パソコン用 Web ページ，または電話でチケットの申し込みをする．
2. クレジットカードまたは銀行振込で決済を行う．
3. i モード端末宛てにメールを受信する．
4. 受信したメールに記載された URL を開くと，バーコードが表示される．
5. イベント入場口でバーコードを提示する．

これは，自動車の ETC のように列を待つことなく入場できるようになる．

ユーザーの携帯に配信されるメールは，ユーザーごとに異なっており，バーコードが記載されたページもユーザーごとに異なる．しかもバーコードのページを開こうとした場合，NTT ドコモが管理している UID（ユーザーの ID）によってチェックされるため，購入者以外がバーコードのページを開こうとしても開けないように工夫されている．

バーコード自体は単なる画像だが，パリティとチェック・デジットでチェックすることで，偽造もできないようになっている．

また，電子チケットでは各々のユーザーごとに後々までサービスを提供できる．例えば，入場したユーザーに道路の交通情報や天気情報，イベントの進捗状況を提供することができる．

こうした情報をユーザーのニーズに合わせて提供でき，マーケティングに生かせることは電子チケットの将来的なメリットといえる．

2.1.1　問題点

送料という形でユーザーにコストを負担させる紙のチケットと違い，電子チケットのシステムコストは販売者が負担しなければならない．

これは紙のチケットよりもコストがかかっているというのが実状である．しかし，これでは販売者にとっての負担があるため，一般的な普及に繋がるには遠い．

また，席番号がある場合の扱いや，チケットを二人分購入したい場合はどう対処するのかといった問題が残されている．

2.2　電子財布

日立製作所は，携帯電話の画面に 2 次元バーコードを表示して，チケット代わりに利用するサービスが開発されている．

2.2　電子財布

電子チケットや電子財布というと，Bluetooth や非接触の IC カードを利用した近未来のサービスが想像されることが多い．しかし携帯電話の画面を利用することで，新機能を備えた端末を必要とせずに電子チケットを実現することができる．

これは，インターネットに接続できる携帯電話でチケット販売サイトにアクセスし，2 次元バーコードの電子チケットを入手する．コンサート会場などで，チケット代わりに携帯電話を差し出し，バーコードスキャナで読み取って入場認証を行う．

ここで使う 2 次元バーコードは「QR コード」(Quick Response Code) と呼ばれるもので，従来のバーコードに比べて多くの情報を記録できるのが特徴であり，携帯電話の画面でも約数字 300 文字を記録する事ができる．

2 次元バーコードはそれ自体が誤り訂正機能を持っているため，全体の 30 %程度がうまく読み取れなくても，認証には問題ない．

このサービスに特に向いていると考えるものを下の図に示す．

実現される機能	流通	エンタテイメント	公共・交通
販売促進	クーポン・チラシ配信		電子回覧版
個人認証	会員証・ポイントカード	電子チケット	定期券・図書・診察カード
決済	領収書・請求書	モバイルコマース	公共料金請求書

コンサートのチケットなどに利用した場合，発送に時間のかかる紙のチケットと違い，公演の直前でもオンラインで購入が可能である．

また，携帯電話に新機能が追加されなくても，携帯電話の液晶は大きくなり，2 次元バーコードの表示に問題はない．また待ち受け画像などのダウンロードが普及したことから，イ

ンターネットにアクセスできる携帯電話にはデータの 2 次利用を防止する機能が搭載されており，電子チケットの複製や転送を防止できる．

そして，財布の中にあるたくさんのポイントカードを携帯にまとめられるだけでもメリットは大きい．

2.2.1　問題点

まず一つにコストの問題がある．

現在のところ，一般に普及しているとは言いがたい 2 次元バーコードを利用するため，スキャナだけでも 10 万円程度のコストが必要である．スキャナを接続するシステムの開発まで含むとかなりの金額になる．

もう 1 つの問題は，クーポンのように紙のチケットを切るのに比べると，2 次元バーコードは読み取りに手間がかかってしまう事である．ここが電車の定期券などにも採用しにくい理由で，非接触型の Bluetooth や IC カードなどが期待される分野でもある．

2.3　非接触 IC カードでのモバイルコマース

電子商取り引きは期待されながらも，その安全性が検証されていないため，なかなか一般化されないのが実状である．

しかしここで，携帯情報端末，非接触 IC カード，インターネットおよび無線パケット通信網を利用した電子商取引の安全性，即時性，有効性などを検証する事を目的に，実験が行われている．

これは総務省の認可法人である通信，放送機構（TAO）が進める「モバイル e-コマース」の研究開発において受託企業として 3 社が実施する．

これは，NTT ドコモ，ソニー，NTT データの 3 社は 2001 年 6 月 13 日，8 月 1 日より

札幌市を中心に行われた．実験にあたっては，約 300 名のモニターに携帯情報端末と非接触 IC カードが配布され，以下の実験が行われている．

- モバイル環境での電子バリューの購入
- 札幌市営地下鉄東西線 19 駅，南北線駅 1 駅（計 66 台）で，電子マネーを電子乗車券として利用
- 指定の自動販売機（8 台）での電子マネーによる飲料購入
- コンサート会場（SPICA ホール）で電子チケットとして利用

ユーザーは，携帯端末から無線パケット通信（DoPa）を利用してサーバにアクセスする．認証を行い，サーバから電子マネーが発行されたら，携帯端末内に格納する「チャージ」と呼ばれる作業を初めに行う．その後携帯端末に接続されたカードリーダーを用いて非接触 IC カード電子マネーを移し替える．

これによりユーザーはクレジットカード大の非接触 IC カードを持つだけで，地下鉄の乗車や自動販売機からの商品購入が可能となる．

※ コンビニを通していくらかの金額を課金センタにプリペイドし，データを登録する．IC カードは，CPU やメモリ，暗号機能を組み込んだカードである．扱える情報量が多く，セキュリティに優れることから電子マネーや会員カードなどへの応用が期待されている．非接触型 IC カードは，さらにアンテナと無線機能を内蔵し，ポケットなどに入れたままで外部と通信し，電子マネーなどの決済に利用できる．

2.3.1　問題点

ここでもコスト面での問題が挙げられる．

非接触 IC カードは高性能であっても，それをスキャンする機械が高価なため，これを利

用しようという提供者が少ないために，なかなか普及に至らない．

　また，電子商取り引きにはまだ問題が残されており，安全性が実証されないままでは消費者は利用できないといった問題があげられる．

第 3 章

チケット配信方式

3.1 概要

本研究で扱うチケット配信サービスについて，全体の概要を簡単に説明する．ここでは映画のチケット購入の場合を例としてあげる．

この配信方式では以下を利用する．

- コンビニ
- ユニークな数（Na) の記載されたカード
- 課金センタ

※ Na というのは，最寄りの駅やコンビニといった，ユーザの身近にある場所に置かれたカードである．これにはユニークな数が記載されているだけで，元々は無価値のカードである．

ユーザ ：
コンビニを通していくらかの金額を課金センタにプリペイドし，データを登録する（第 3 章 3.2 に示す）．

ユーザ ：
どこにでも置かれている，無価値の Na（ユニークな数) が記載されたカードを取得する．

3.1 概要

ユーザ ：

雑誌やホームページ等から，チケットの欲しいコンテンツを選択し，またその URL 情報を取得しておく．

ユーザ ：

3. で取得した URL より，携帯電話等からそのホームページを閲覧し，予約情報，ユーザ ID，Na の数字情報を課金センタに送信する．

課金センタ：

受信したデータからユーザを照合し認証する．認証成立なら予約情報分の金額が，ユーザのプリペイド金額より引き落とされる．

課金センタ ：

プリペイド金額からの引き落とし後，Na の記載されているカードに予約情報分の金額を登録する．

ユーザ ：

当日，Na の記載されているカードを映画館で提示する．

映画館 ：

Na の数字より，課金センタと検証を行い，認証成立すれば Na の記載されているカードを映画のチケットとして利用できる．

※ 4.5.6 については，第 4 章より詳しく説明する．

このチケット配信方式の特徴を挙げる．

まず一つに，どこにでも置いてある Na の記載されたカードは元々無価値であるが，ユーザと課金センタとの間で認証し，課金センタでプリペイド金額からの引き落としが終了しデータが書き換えられた後，カードに予約情報分の金額が再登録される（３章．６の部分）．この時点で，それまで無価値であった Na が記載されたカードが，予約情報分の価値を持つチケットに変わるという点である．

3.1　概要

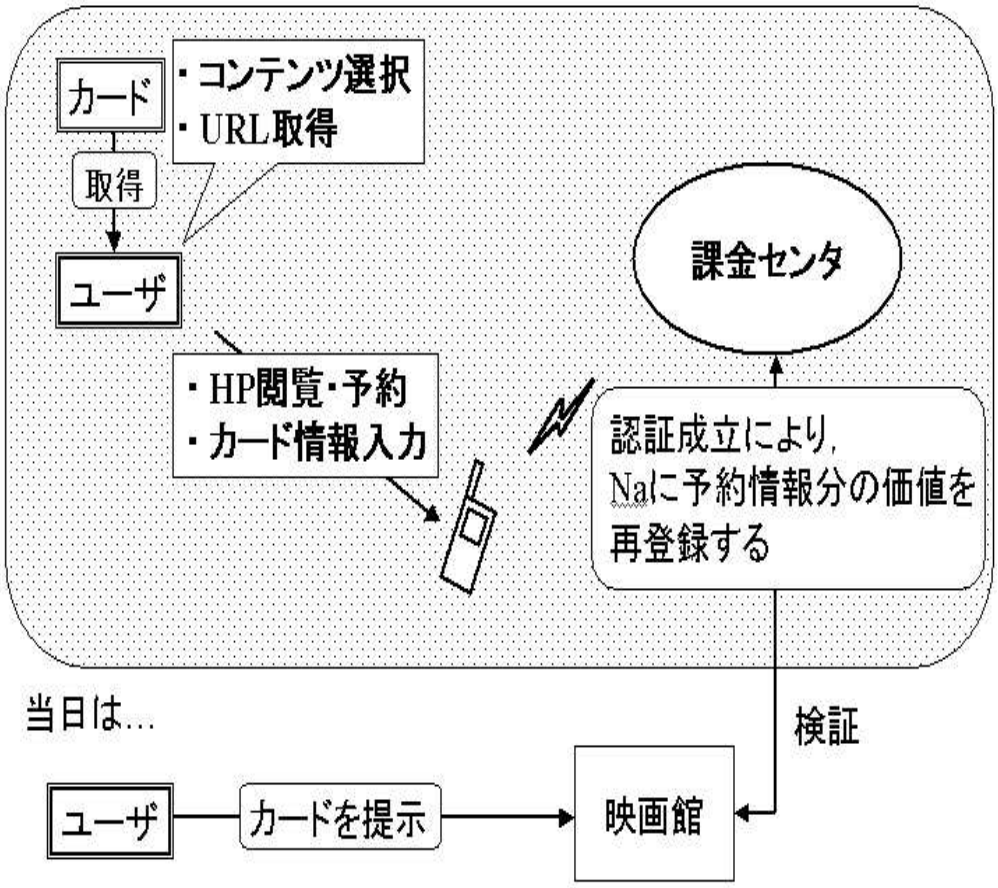

図 3.1　チケット配信方式の概要

これはすなわち，チケット自体に価値を持たせるのではなく，ユニークな数に価値を持たせる事によって，カード（チケット）に汎用性を持たせている．自分の手元にあるチケットを指定して，価値を持たせる事で，チケットを受け取る手間を省いている．

また，モバイル端末（ここでは携帯電話）からの操作を可能にする事によって利用する場所を選ぶ事がないため，ユーザの利便性を向上している．

そして，インターネットに課金を付加した既存のシステムとして，クレジットカードを用いたインターネット決済というものがある．

このシステムの利用に当たって，クレジットカードは子供の利用ができないため，ユーザ制限が加わってしまうという問題がある．そこで，本研究で利用するシステムには，プリペイド課金システムを採用した．

また，このシステムは安全性がすでに検証されている，ワンタイムパスワード認証方式である SAS 認証方式をベースにシステム設計を行った．これより，インターネット上に個人情報を掲載した際に起こる，個人情報の漏洩の問題を解決している．

そして，本研究で提案するチケット配信システムはユーザだけでなく，コンテンツ提供者側にとってもメリットがもたらせられるような，より実用性の高いシステム設計を行うとしている．そのため，2 章で挙げた既存システムの問題点に共通してあげられた問題であるコスト面を考慮する必要がある．

ここで本研究で提案したチケット配信システム全体で，コストのかかる媒体といえば Na（ユニークな数字）の記載されたカードであるが，これは数字のかかれただけの紙媒体とし，ごくわずかのコストですむ．このシステム全体のメリットとして低コストであるという事があげられる．

こういった特徴を一環し，ユーザに最適なチケット配信方式を構成した．

3.2　プリペイド課金方式

先ず，本研究の前段階（2.2（1）の部分）となる，プリペイド課金方式（登録フェーズ）について説明する（図 3.1）．

これは本研究で扱うチケット配信方式における登録フェーズに当たる部分であり，既存のシステムとして現在も利用されている．

登録フェーズは，ユーザ・コンビニ・課金センタの 3 者間でのやりとりとなっている．ここでは，コンビニでプリペイドし，同時にユーザＩＤ・プリペイド金額，そして本研究であるプリペイド後のチケット配信システムを利用する際に使用する認証用のデータの課金センタへの登録を行っている．

3.2 プリペイド課金方式

利用する情報を以下に示す.

- ユーザ ID： ユーザ固有の番号
- XID： カード固有の番号
- Xmask： 安全に認証情報を送るための番号
- E_0^2： 認証情報
- ￥3,000： プリペイド金額

ユーザ ：

プリペイド金額としてコンビニに 3,000 円分の支払いを行う.

コンビニ ：

ユーザ所有の携帯電話に XID・Xmask を送信する.

コンビニ ：

課金センタに XID・Xmask とユーザがプリペイドした￥3,000 の情報を送信する.

ユーザ ：

携帯電話によって，XID と・E_0^2・ユーザ ID を課金センタに送信する.

この時，E_0^2，ユーザ ID を安全に配送するために，これにコンビニから受け取った Xmask を排他的論理和で足して暗号化し，それを課金センタに送信する.

課金センタ ：

ユーザから受信した XID と，コンビニから受信した情報を照合し，Xmask を使って認証情報を復号する．※

課金センタ ：

￥3,000，復号された E_0^2，ユーザ ID が登録される.

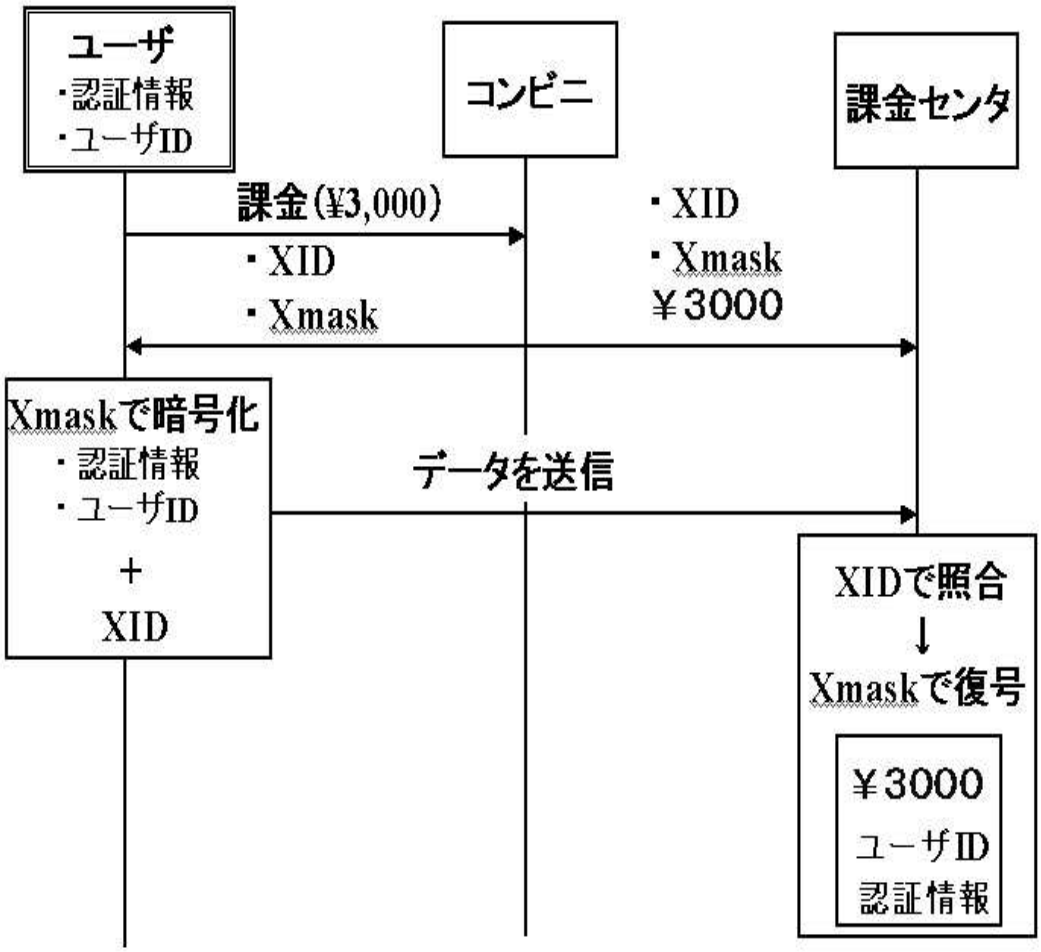

図 3.2　プリペイド課金方式の概要

※ XID・Xmask はペアの情報になっており，XID を鍵として，ペアの Xmask によって復号を行っている．

E_0^2 は一回目の認証情報として課金センタに登録した．登録した認証情報は携帯電話にも保存されており，その後のチケット配信システムを利用する際に利用する．この時，チケット配信システムを利用する度に，E_0^2，E_1^2，E_2^2... というように，認証情報は書き換えられる．

このようにして登録された，金額・認証情報・ユーザ ID のデータを利用して，この後の，本研究の本質となるチケット配信方式へと繋げる．

3.3　課金部分の概要

本研究の本質であるプリペイド後のチケット配信方式において，以下に説明する（図 4.1 に示す）．

ここではユーザ所有の携帯電話と課金センタの 2 者間で通信が行われている．

モバイル端末（ここでは携帯電話を想定する）を用いて，予約とプリペイド金額からの引き落としその他，従来のチケットの予約・発券・支払にあたる部分を行っている．

課金センタには予め，ユーザ ID・プリペイド金額情報（￥3,000）・認証情報が登録されているものとし，予約金額は￥2,000 とする．

ここでは以下を利用する．

- ユーザとユーザ所有の携帯電話
- Na（ユニークな数) の記載されたカード
- 課金センタ

ユーザ ：

ユーザ ID と，認証情報によって暗号化した予約情報，Na（ユニークな数字）を課金センタに送信する．

課金センタ ：

受信したユーザ ID からプリペイド課金した際の登録者リストと照合し，一致したユーザ ID で，その認証情報から暗号化された 2 つのデータを復号する．

3.3 課金部分の概要

課金センタ ：

認証が成立したら，暗号化されていた予約情報，Na を復号する．復号した Na に予約情報を登録する．

課金センタ ：

プリペイド金額から予約情報分の金額を引き落とした金額と，次回認証用データを元の登録データから書き換える．

ユーザ ：

利用する際は，Na の記載されたカードを映画館で提示し，映画館と課金センタで検証を行い，成立すれば Na の記載されたカードを映画券として利用できる．

3.3　課金部分の概要

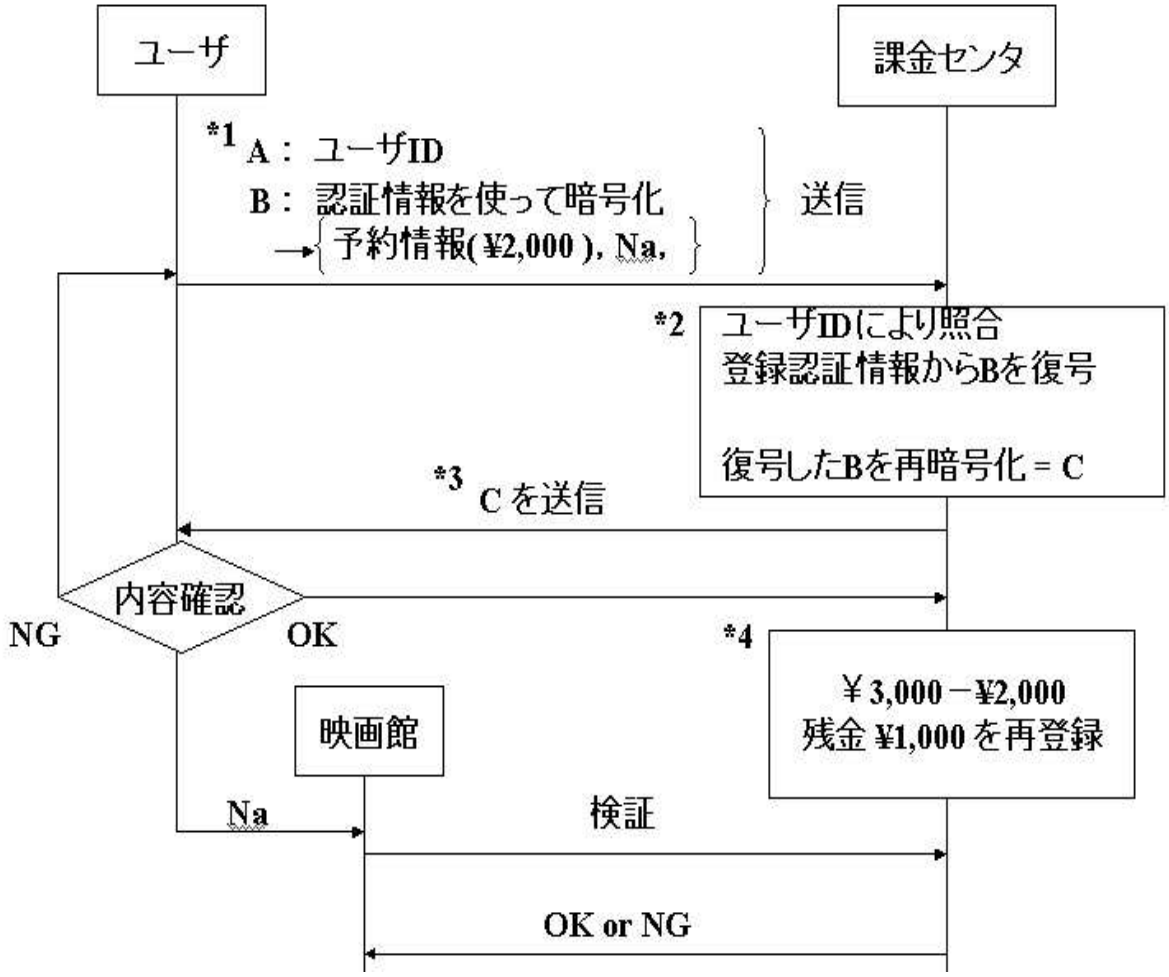

図 3.3　課金部分の概要

第 4 章

プロトコルの設計

4.1 SAS 認証方式

第 5 章で述べた課金部分は，SAS 認証方式システムをベースとした．これより，本研究のベースとなった SAS 認証方式について説明する．

利用する情報は以下に示す

- A : ユーザ ID
- S : パスワード
- N : 乱数
- E_0^2 : 認証情報

まず，登録フェーズ $(n = 0)$ の流れは以下の通りである．

User: $E_0^2 = E^2(S \oplus N_0)$ を計算する．

User: A, E_0^2 を Host に安全なチャネルを用いて送信する．

Host: A, E_0^2 を 保存する．

次に認証フェーズ $(n = k)$ の説明を行う．流れは以下の通りである．

User: 以下のデータを計算し，A と共に Host に送信する．

$E_k^1 \oplus E_k^3 + 1$, $E_{k+1}^2 \oplus E_k^2$

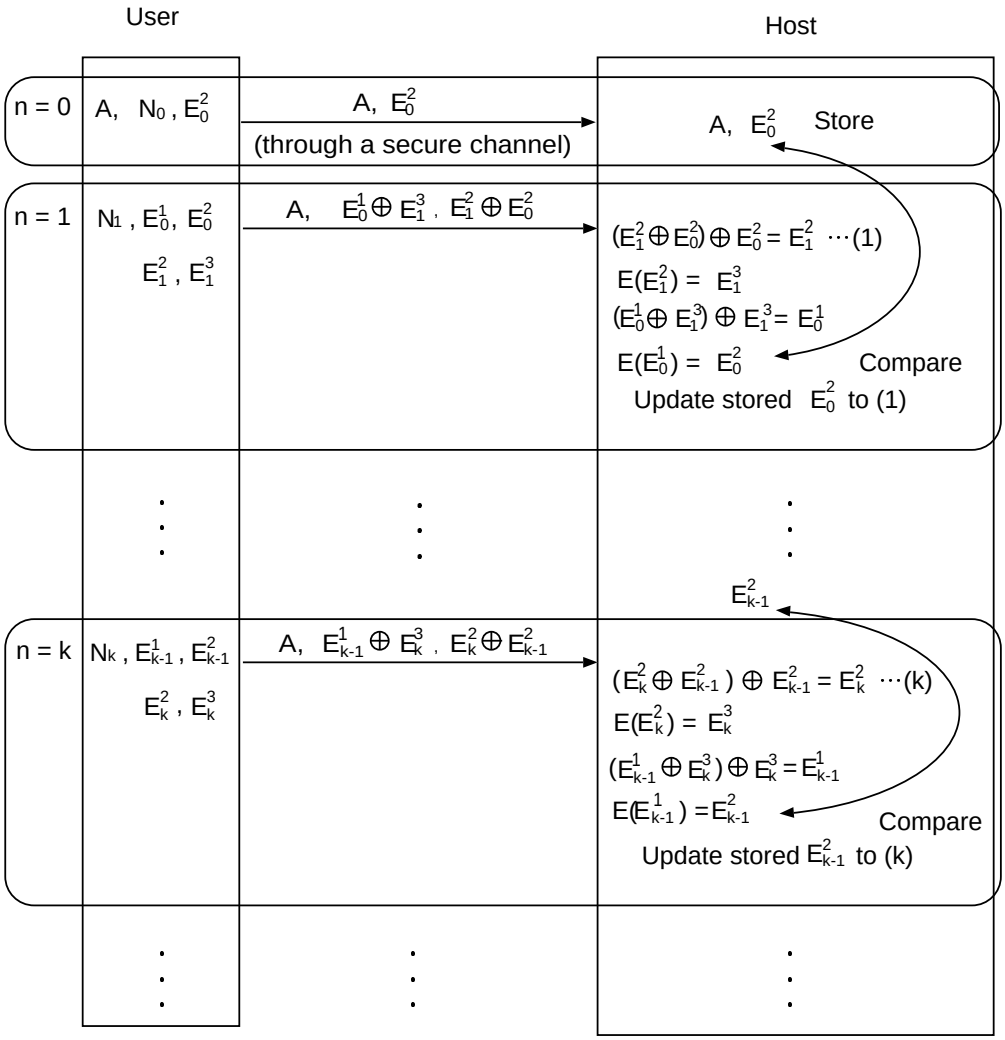

図 4.1 SAS の登録，および認証フェーズ

Host: $E^2_{k+1} \oplus E^2_k$ と，保存されている E^2_k との排他的論理和を取り，以下を取得する．

E^2_{k+1}

Host: E^2_{k+1} にハッシュ関数を適用する．

$E(E^2_{k+1}) = E^3_{k+1}$

取得した E^3_{k+1} を $E^1_k \oplus E^3_{k+1}$ と排他的論理和を取り，今回認証用中間データ E^1_k を取得する．E^1_k にハッシュ関数を適応し，保存している E^2_k と比較する．一致すれば，User は認証され，次回認証フェーズのために，E^2_k を E^2_{k+1} に更新する．

一致しなければ認証は拒否される．

SAS では認証を行う度に次回用鍵の登録を行うので Lamport と違い，パスワードの再設定の必要がない．また処理量も軽量である．安全性に関しても，既存のワンタイムパスワード認証方式で問題であった認証情報の再利用攻撃やサービス不能攻撃に対して耐性がある．

4.2　認証・課金プロトコル

第 6 章で述べた SAS 認証方式を応用し，認証及び課金部分のプロトコルの設計を行った．

このプロトコルについて，以下に説明する（図 5.2 参照）．

利用するデータは以下である．

- ID : ユーザ ID
- Na : カードに記載された，ユニークな数字
- R　: 予約金額
- E_0^2 : 認証情報

ユーザ　:

ID,

$E1_0 \oplus E_1^3$，$E_1^2 \oplus E_0^2$,

$E(Na, E_0^2)$,$E(R, E_0^2)$ を課金センタに送信.

課金センタ　:

ID によって照合する.

$E_1^2 \oplus E_0^2 \oplus E_0^2 = E_1^2$

$E(E_1^2) = E_1^3$

$E_0^1 \oplus E_1^3 \oplus E_1^3 = E_0^1$

$E(E_0^1) = E_0^2$

ここで出たデータと登録データの認証情報を照らし合わせる.

課金センタ　:

Na，R を E_0^2 で復号する.

課金センタ　:

Na に R の情報を登録する.

またプリペイド金額から R を引き，次回認証用データとして E_1^2 を登録する.

課金センタ　:

データ書き換え登録完了確認メッセージの送信.

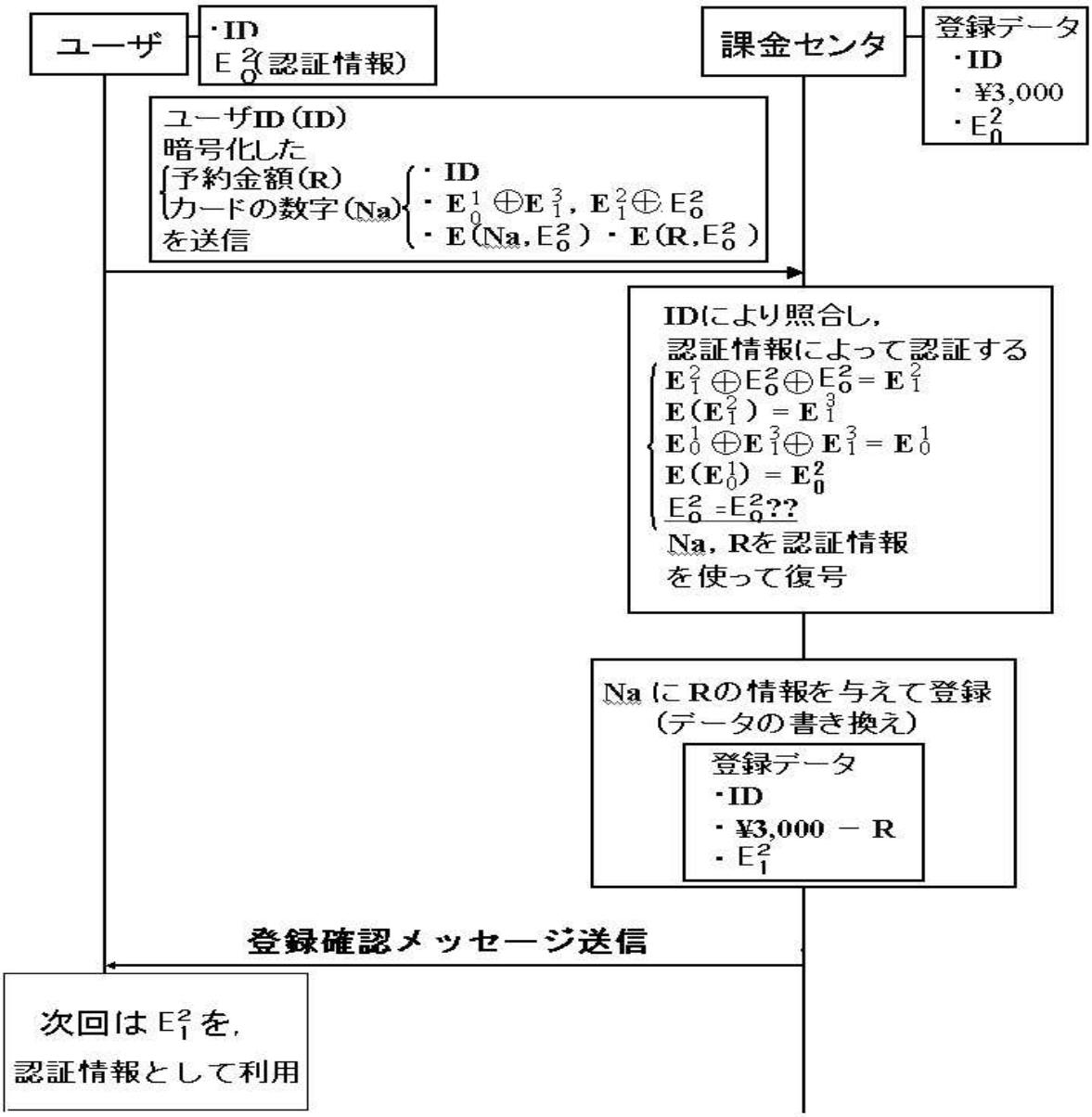

図 4.2　認証，課金プロトコル

第 5 章

シミュレータ

5.1 目的

これまでに提案したプロトコルに沿って，有効性を検証するためにシミュレータを作成する．

本研究ではモバイル端末を利用する点に優位性があるため，爆発的な普及を遂げその代表といえる携帯電話において，現在広く利用が見込まれる Java でのシュミレータを作成する．

5.2 作成範囲

シミュレータの作成範囲は，以下の部分に示す通りである．

client :

ID,

$E1_0 \oplus E_1^3$,$E_1^2 \oplus E_0^2$,$E(Na, E_0^2)$,

$E(R, E_0^2)$ を課金センタに送信．

server :

受信したデータと一致する ID を登録データから検索し，そのユーザの認証情報を抽出する．この認証情報から以下の手順を行う

$E_1^2 \oplus E_0^2 \oplus E_0^2 = E_1^2$

$E(E_1^2) = E_1^3$

$E_0^1 \oplus E_1^3 \oplus E_1^3 = E_0^1$

$E(E_0^1) = E_0^2$

ここで出たデータと登録データの認証情報を照らし合わせて一致するか調べる．

server：

Na，R を E_0^2 で復号する．

server：

Na に R の情報を登録する．また登録データの金額から R を引き，次回認証用データとして E_1^2 として書き換え，登録する．

server：

データ書き換え登録完了確認メッセージの送信．

client：

データ書き換え登録完了確認メッセージの受信．

次回認証用のデータ E_1^2 を保存．

現在は，一通りの全体の動きとしては完成しているが，細かい動作について認証部分が調整段階のため評価に至っていない．

今後このシミュレータを完成させ，以下についてを評価する．このシミュレータによる評価項目としては以下とする．

- プロトコルの安全性の検証

  プロトコルの安全性については，本研究で設計したプロトコルにおいて実装上の問題はないかを検証する．

  これは，擬似的に問題を発生させる事によってその安全性を検証する．

5.2 作成範囲

- 処理速度の調査

  処理速度は，携帯電話を所有する総ユーザ数 67,101,100 台（2001 年 12 月データ）で設定し，どの程度の処理速度であるか調査する．

- 認証情報のデータ長，各種パラメータの設定

  認証情報 E_0^2 のデータ長は，このシステムにおいて最適な長さはどの程度なのか，安全性を含め，処理速度の関係等からも検討していく．
  また，Na（ユニークな数字）の記載されたカードにおいても，処理速度等から検討し最適な桁数の設定を行う．そして，携帯電話を所有する総ユーザ数からサーバ容量の設定も行う事が必要である．

- ユーザインタフェースの設計

  プリペイド課金を行って，課金センタにデータを登録する場合，予約や確認メッセージの受け取りの際の携帯電話のインタフェースの設計を行う．

第 6 章

むすび

本研究はモバイル端末を用いたチケット課金方式と題して，インターネット上に課金システムを付加する事によってチケットを受け取る手間のない，ユーザに最適なチケット配信方式を提案した．

また，既存のチケット配信方式における共通の問題であったコストの面に関しても，本研究で提案したチケット課金方式では極めて低コストに設計する事ができた．これは，一般的に普及される可能性が高く，実用化に即しているといえる．

今後の研究課題としては，現在作成中の中核処理にあたる課金システムのシミュレータを完成させ，評価項目であるプロトコルの安全性の検証，認証情報のデータ長，各種パラメータの設定，処理速度の調査，ユーザインタフェースの設定を行う．

またｉアプリ（携帯端末にのせて）での，より実装に近い実験を行う．

ｉアプリを選択している理由は，現在携帯電話会社 3 社ともに Java の動く電話を販売しているが，アプリケーションを配信するには，一般にキャリア参入サイトからでないとできない．しかし，ドコモのｉアプリのみ開発環境が公開され，ユーザが個人でアプリケーションを配布が可能であるため，ｉアプリを選択する．

そして，インタフェースの設定の検討が挙げられる．

URL をを携帯電話に入力する場合，例えば老人が利用する時は，数字を一つ一つ間違えずに入力するのは困難である．

そこで，現在色々なサービスへの利用が期待されている，バーコードスキャン装置の利用を提案する．

これは，URL 情報をバーコードの形式に変換しておき，例えば雑誌の端等に記載されて

いるとする．そして，これを携帯電話の外付けになったバーコードスキャン装置を用いてスキャンで入力が行われ，ホームページを閲覧する事ができる．

この入力方法によって間違える事なく入力する事ができ，老人や子供への利用も広がる．

また，この方法を用いて本研究で利用した Na（ユニークな数字）を携帯電話に入力する際も同様の事がいえる．

本研究は課金方式の設計と共に，流通システム全体の大きな範囲でプロトコルを提案したので，処理プログラムの設計からインタフェースまで考えるべき点は多く存在する．そのため，ユーザはもちろんコンテンツ提供者にとっても最適といえるシステム設計は案を尽きない．

本研究ではその基盤を作成したとして，今後更に研究を深め，ユーザだけでなくコンテンツ提供者にとってもより最適である方法を提案し，実用性の高いシステム設計を行う必要がある．

謝辞

本学情報システム工学科 清水明宏教授には，卒業研究を含め，学生生活全般に渡ってのご指導，貴重な御教示を賜った．ここに深謝申し上げる．

また，清水研究室学部生 上岡隆氏をはじめ研究室の方々には，有益な御議論を頂いた．心より感謝する．

参考文献

[1] $http://www.alan.co.jp/news/release_alan010925_0.html$

[2] $http://www.qrcode.com/$

[3] $http://www.nttdocomo.co.jp/new/contents/01/whatnew0613a.html$

[4] 上岡隆, 清水明宏, ”ワンタイムパスワード認証方式 SAS の安全性に関する検討” 電子情報通信学会技術研究報告書, $OFS2001-48, No.435, pp.53-58, 2001$