平成１３年度

春季終了

修士（工学）学位論文

経済社会における情報流通に関する一考察

－　個人消費活動を事例として　－

A Study on Information Circulation System
in Individual Economic Activities

平成１４年1月１５日

高知工科大学　大学院　工学研究科　基盤工学専攻　起業家コース

学籍番号：１０５５１７１

大野　加恵
Kae Ohno

目　次

第一章　序論

１．１　緒言

ＩＴ（Information Technology／情報技術）革命は、１８世紀に英国で始まった産業革命に匹敵する歴史的大転換を社会にもたらすと言われ[1] [2]、国民生活において、多様なライフスタイルの実現や利便性の向上をもたらす鍵として、我が国社会全体から強い期待がある。

１８世紀にワットによって蒸気機関が発明され、その発明を改良発展させることによって、我々人間は社会や経済を発展させてきた。つまり、産業革命以降、現代までの技術革新の主役は常にエネルギーであったと言え、産業革命はエネルギー革命と言い換えることもできる。そして、エネルギーによって生み出される大量の生産物つまり物質を我々は持てるようになった[1]。エネルギーの集中管理と効率的分業によって、大量生産が可能になったからである。そして、その大量生産された物質を大量に消費する活動が経済社会の基盤であった。

一方、２０世紀末に始まったＩＴ革命がもたらすと期待される「高度通信情報ネットワーク社会」は[3]、「皆が情報を持てるようになる」社会であると言える[1]。万物は物質性と情報性の両面を持ちうるが、産業革命によって、我々は物質を持てるようになり、ＩＴ革命によって情報を持てるようになる。

ただし、ＩＴ革命以降の情報は、従来の情報とは異なり、情報がデジタル化されている。従来、情報を伝達するにはかなりのエネルギーや物質を消費していた。このため、情報の本質的特性である恣意的生成性、自由疎通性、処理・編集・加工の自在性等が制約されていた。しかし、ＩＴの発展により、情報がデジタル化されたことによって、この制約から解放され、情報本来の特性が顕在化されるようになった。つまり、情報が付加価値の源泉となるのである。このようなことから、産業革命の主役であったエネルギーにあたるＩＴ革命の主役は、デジタル化された「情報」であると言える。

産業革命の本質は、エネルギーを利用した生産装置を使い、労働生産性をあげ、経済社会を豊かにすることであったが、ＩＴ革命の本質は生活革命である[1]。皆が情報を蓄積し、処理・編集・加工などを行い、情報を交信することによって新たな情報の流れが生まれ、社会や生活の成り立ちそのものを変える。そして、社会や生活が変わる結果として経済効果が出現する。ＩＴはこのための基盤であり、「高度通信情報ネットワーク社会」実現にはマイクロプロセッサー、メモリーそしてインターネットが決め手となると言われている[1]。

万物は物質性と情報性の両面を持ちうると既に書いたが、情報とは本来、観念的なものであり、産業革命の主役であるエネルギー・物質とは独立な概念であるが[4]、万物のもう一方の特性である「情報」に、エネルギー保存の法則にとらわれない流れがあることに注目し、考察を行いたいと考えた。

１．２　研究の背景

エネルギーは複写をすることができないが、情報は複写をすることができる。しかも、情報は複写をしたからといって増えることはあっても減ることはない(2)。アナログ技術による複写は情報の劣化や雑情報の混入を許してきたが、デジタル技術は情報を数値化することによって、半永久的に蓄積し、処理・編集・加工などを可能にする。

２０世紀末頃からインターネットをインフラとしてネットワークで企業が繋がれるようになってきた。デジタル化された情報はネットワークを介して交信するには適している。受信した情報を蓄積し、処理・編集・加工し、新たな情報として発信することも可能である。また、従来のアナログ的処理に比べて正確かつ効率的に行える。ビジネス展開において、ネットワークで繋がれデジタル化された情報を交信することは、移動や紙、人件費等のコストを削減できる、ロスタイムが少ないなど明確なメリットがあり、１９９８年の企業間電子商取引は、８兆６２００億円に達している(3)。

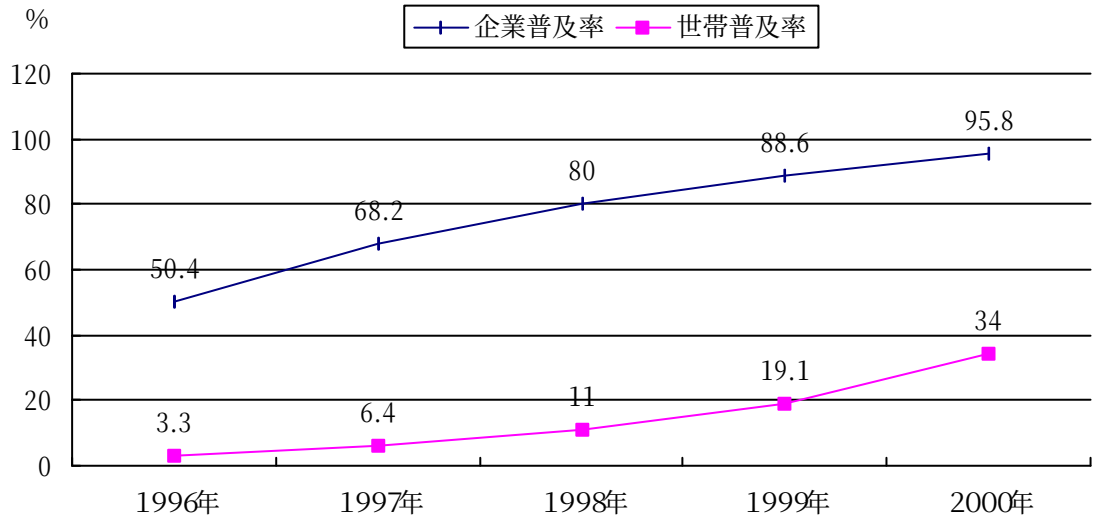


図１－１　我が国におけるインターネットの普及状況(3)

企業は、内部業務や外部業務もＩＴ化している。ＥＤＩ（Electronic Data Interchange）やＥＲＰ（Enterprise Resource Planning）、ＳＣＭ（Supply Chain Management）、ＡＳＰ（Application Service Provider）、ＩＤＣ（Internet Data Center）などがそれである。また、対消費者をも取り込んだＩＴ化も推進されている。最も代表的なものがＣＲＭ（Customer Relationship Management）である。ＣＲＭは、消費者の属性や購買履歴などの多様なデータを一元管理し、データ・マイニング手法によって分析し、販売や広告を行うものである。ＥＲＰやＳＣＭ、ＡＳＰ、ＩＤＣなどは企業内もしくは企業間での売買

や契約を対象としていたのに対して、ＳＣＭは、消費者のデータをＩＴによって企業活動に活かすところが異なっているが、企業が情報を蓄積し、処理・編集・加工を行う点で共通している(3)。

一方、個人がネットワークに接続し、主体となって情報を蓄積し、処理・編集・加工を行うことができているだろうか。

先にみたように、個人のインターネット接続率は企業と比較してまだ低い。ＰＣや携帯電話などの既存の情報端末は操作性が十分でなく、年齢や学歴、年収による普及率の偏りが大きい。

図１－２　インターネット利用率（世帯主年齢別）
%

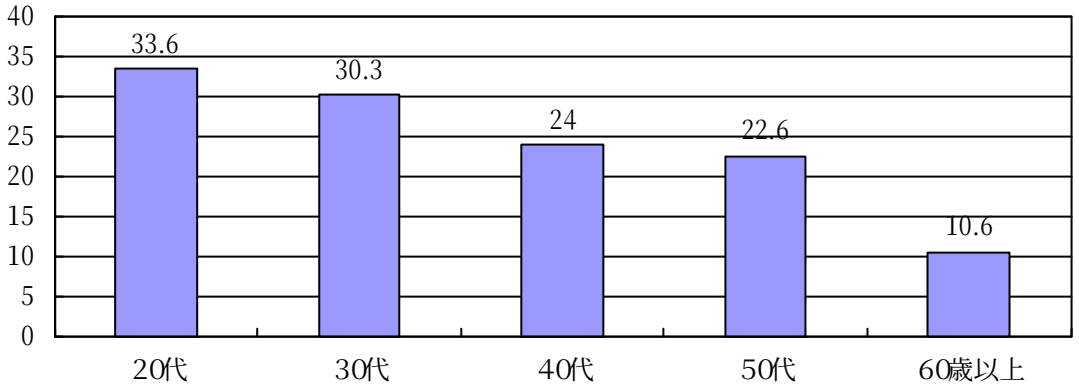


図１－２　インターネット利用率（世帯主年齢別）(3)

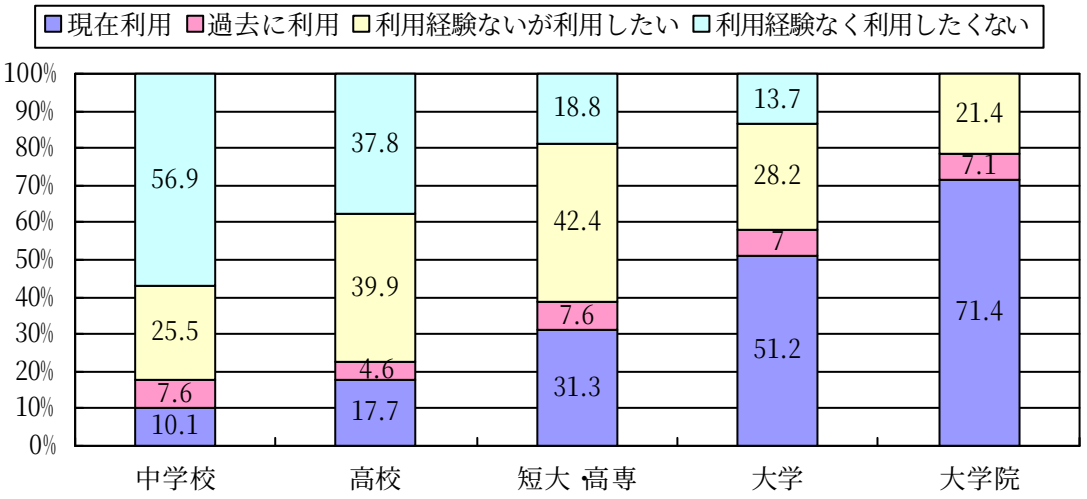


図１－３　インターネット利用率（学歴別）(3)

しかし、ＩＴ革命の本質は生活革命である。年齢や学歴にかかわりなく、皆が情報を蓄積し、処理・編集・加工などを行い、情報を交信することによって新たな情報の流れが生まれる。それによって、社会や生活の成り立ちそのものが変わり、結果として経済効果が出現する。経済効果を見る指標としてＧＤＰ（国内総生産）があるが、ＧＤＰの約６割を占めているのは、個人消費活動である。個人消費活動を通じて、容易に情報の蓄積、処理・編集・加工ができる仕組みを構築すれば、社会における新たな情報の流れを作ることが可能となる。

このためには、一般の消費者が簡単にネットワークに接続できる情報機器もしくは媒体とＩＴ環境が必要であると考え、個人消費活動を事例として、経済社会における情報流通について考察を行うこととした。

１．３　本研究の目的と意義

産業革命の主役であったエネルギーは複写ができないが、デジタル化された情報は複写をすることができる。しかも複写をすることによる劣化がない。これはデジタル情報特有のものである。ＩＴ技術の進展によって劣化しないデジタル情報の複写や活用を我々は２０世紀の後半から積極的に始めている。このことは、ビジネス社会において急速に広まり、先に見たように企業のＩＴ化は推進され、ＥＤＩやＥＲＰ、ＳＣＭなどのＩＴ技術を使ったシステムやさまざまなネットワークにおいてビジネスに利用可能なデジタル情報の共有、活用がされている。

しかしながら個人に目を転じて見ると、ＩＴ革命は生活革命であるにもかかわらず、個人が情報を持ち、十分に処理・編集・加工ができるようにはなっていない。つまり、ＩＴが企業側に留まっており、未だ生活者である個人のところまで十分に広まってきていない。このことから、ＩＴ革命の本質である生活革命を成すために、個人消費活動において個人が情報流通の環の中に入ることが可能な仕組みを作ることを本研究の目的とした。

本研究の成果によって、一般の消費者はＩＴ革命によって実現されると期待される「高度通信情報ネットワーク社会」の構成員となる選択肢をもつことができる。

また本研究の具現化により、社会における新たな情報の流れ、つまり新たな情報流通が実現される。このことは、社会や生活の成り立ちそのものに対しインパクトを与え、ひいてはＩＴ革命の本質である生活革命を実現する。筆者は、これらの実現による経済効果、社会的意義は大きいと考える。

第二章　個人消費活動における情報流通に関する考察

２．１　個人消費活動における情報流通の現状

国内の景気をみる指標としてＧＤＰ（国内総生産）があるが、ＧＤＰの約６割を占める個人消費活動における情報流通の現状の整理を行い、望まれる情報流通との違いを明らかにし、課題を抽出したい。

まず、個人消費活動を消費活動の場という軸で分類し、小売店などに直接行き消費活動をおこなう「Direct Shopping」と、自宅や職場にいながら消費活動を行う「Indirect Shopping」に大別する。そして、「Indirect Shopping」をインターネットの Web ブラウザを介して行う「Web Shopping」と以前からあるカタログやＴＶ・ラジオなどを介した従来の「Catalog Shopping」に分ける。

これら３つの消費活動において発生する情報には、消費活動に関する「購買情報」と消費活動を行う人に関する「個人属性情報」があり、これらは異なるセキュリティレベルで扱われないといけない。そしてこれらを「デジタル情報」とハガキやレシートなどの紙や電話通話などの「アナログ情報」に分類する。

表２－１　個人消費活動において発生する情報の分類

		購買情報		個人属性情報	
Direct Shopping		必須	店舗側でデジタル化	任意	店舗側でデジタル化
Indirect Shopping	Catalog Shopping	必須	店舗側がデジタル化	必須	店舗側がデジタル化
	Web Shopping	必須	消費者でデジタル化	必須	消費者でデジタル化

これら３つの視点で個人消費活動における情報流通の流れを考察する。ただし、「Direct Shopping」の場合は、決済方法によって店舗以降の情報の流れが異なるため、最も一般的な現金決済を対象とする。

「Direct Shopping」の場合は、対面販売が基本であるため物流がなく、このため個人属性情報を必ずしも必要としない。「Direct Shopping」と「Catalog Shopping」は個人属性情報を必須とするか否かの違いはあるが、その他の点においては同じある。これら２つと「Web Shopping」の違いは、店舗側から個人に還される購買情報や個人属性情報がデジタル化されているか否かである。

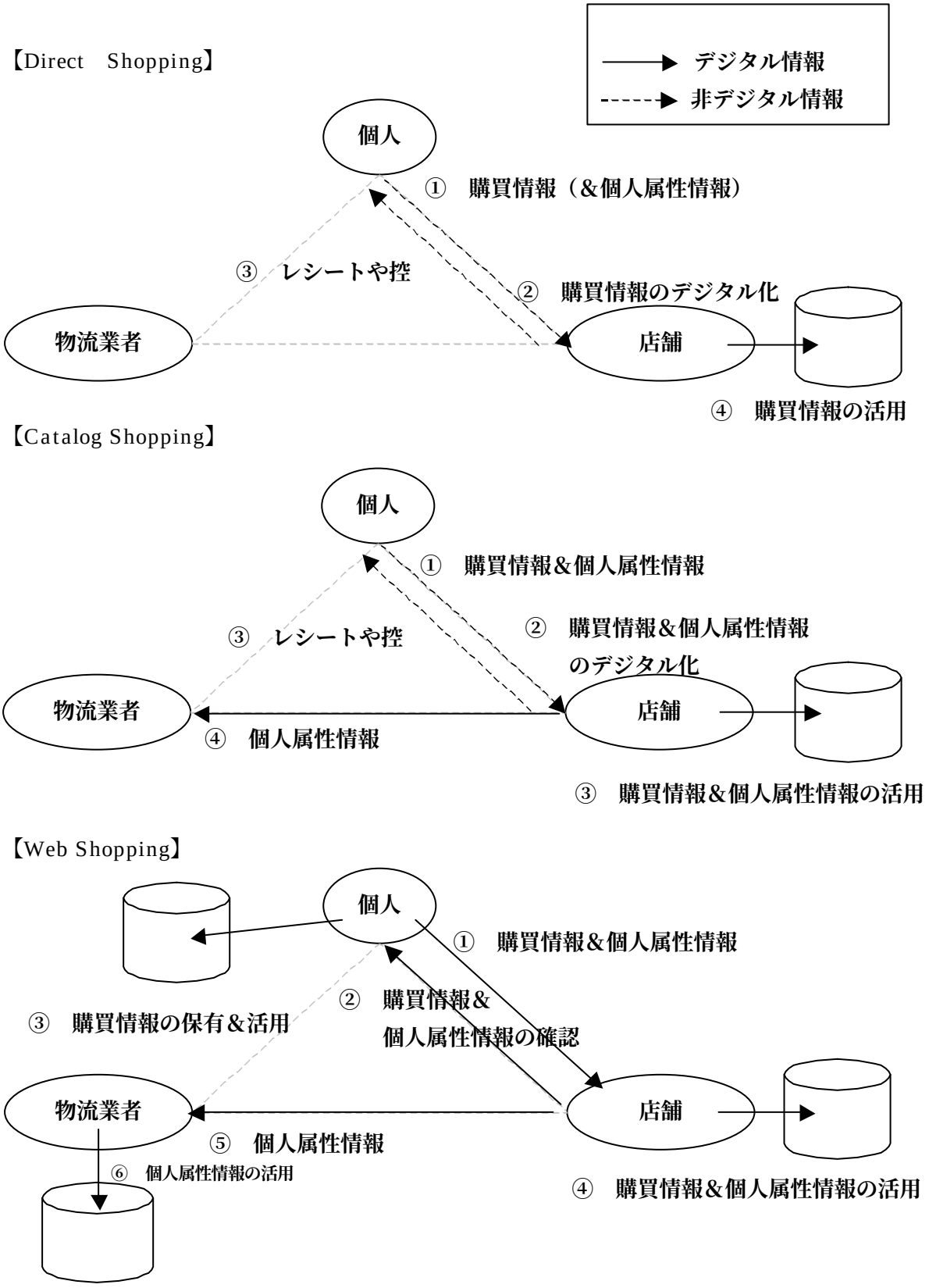


図２－１　個人消費活動における情報の流れ

「Web Shopping」の場合は、店舗に情報を渡す以前に自らＷｅｂで入力を行うため、その時点で情報はデジタル化される。また、「Web Shopping」の場合、購入確認のためのメールが店舗側から送られてくるが、メール情報もデジタル化された情報であるため、自らカット＆ペーストをしてそれらを蓄積、処置・編集・加工、検索することができる。「Direct Shopping」や「Catalog Shopping」の場合は、消費者と店舗との情報のやりとりは、対面、紙、音声であり、デジタル化された情報ではない。このため、消費者が購買情報を蓄積し、処理・編集・加工、検索をしようとする時は、デジタル化がまずおこなわなければならない。

次に店舗以降の情報の流れである。消費者がクレジットカードやデビットカードを使用した場合は、消費者のカードから個人属性情報を読み取り、クレジットカード会社や銀行に照会をする。現金決済の場合でも、購買情報、個人属性情報共にデジタル化され店舗にて売れ筋情報の分析や顧客マーケティングに活用される。また、ＥＤＩ（Electronic Data Interchange）やＳＣＭ（Supply Chain Management）、ＣＲＭ（Customer Relationship Management）などによって、企業間取引、企業活動に購買情報が活かされる。しかしながら、消費者は自らの購買情報や個人属性情報がどの範囲まで流通し、活用されているかは知ることができない。

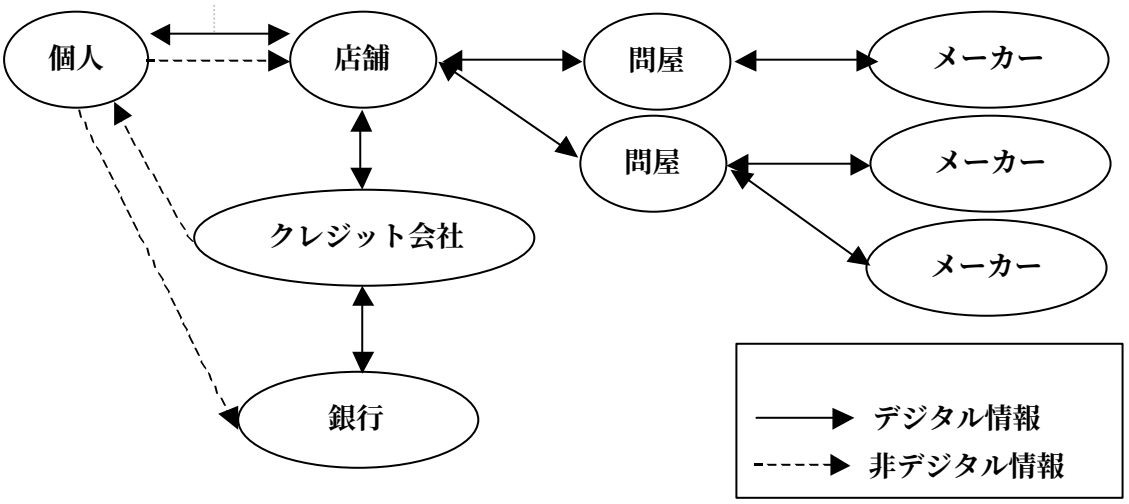


図２－２　Web Shopping における情報の流れ

企業間においては、デジタル情報の情報共有、情報交換を行うことは既に進んでいるが、個人は、「Web Shopping」を除いて、まだ情報流通の輪の中に入っていないことがわかる。また、消費者は購買情報、個人属性情報を一方的に店舗に吸い上げられている構図となっている。

表２－２　個人属性情報ファイルの内容（%）(5)

	１～５	６～８	９～10	11～13 18	14～15	16、21	20	22～23
	①基礎的内容	①の関連項目	②社会的地位	②の関連項目	③購買力	④嗜好	④の関連項目	⑤家族
卸売り・小売業	86.9	5.7	56.9	8.6	10.3	36.2	6.9	46.6
上記の内小売業	91.3	4.3	63.0	8.7	13.0	39.1	8.7	58.7
訪問販売会社	90.0	5.0	52.5	2.5	0	27.5	0	25.0
通信販売会社	88.3	7.1	45.8	4.2	6.3	37.5	4.2	27.1

①基礎的内容（１．氏名、２．住所、３．電話番号、４．性別、５．生年月日）
①の関連項目（６．身体、７．出身地、８．本籍）
②社会的地位（９．職業、10．勤務先）
②の関連項目（11．地位、12．学歴、13．経歴、18．叙位叙勲）
③購買力　　（14．収入、15．資産）
④嗜好　　（16．趣味、21．商品・サービスの購入歴）
④の関連項目（20．定期購読誌）
⑤家族　　（22．配偶者、23．家族）

個人属性情報の収集・蓄積・利用等について経済企画庁が行った実態調査（１９８５年実施）の個人消費活動に直接関係があると思われる業種について、そのアンケート内容を見て見ると、企業内におけるＩＴ浸透が十分でない時期から、情報蓄積がされていたことが分かる(5)。現在は、個人消費活動の場である店舗には、ほとんどＰＯＳ（Point Of Sale）システムが導入されているため、「④嗜好」「④の関連項目」にあたる「購買情報」は、ほぼ確実に保管、利用されていると言ってもよく、インハウスカードやクレジットカードの利用によって「個人属性情報」と「購買情報」は結びつけられ、企業内において活用されている。

しかしながら、情報主体である消費者には活用が容易な状態で情報が還されていない。また、消費者は自らの情報でありながら、その情報がどの範囲まで流通し、活用されているか分からない。

２．２　情報流通におけるエントロピーの考察(6) (7) (8) (9)

一般に用いられている情報の概念は、意味や内容を含めたものとして理解されている。万物は物質性と情報性を持ちうると既に書いたが、この場合の情報性も同様である。ビット単位での記号としてだけではなく、その記号のもつ意味や内容をも指している。つまり、人間の行動や社会活動から生まれ、意味のあるものごとについての「知らせ」が情報と考えられている。

個人の消費活動における購買情報は、店舗内の他部門、企業間取引や企業活動に活かされるが、消費者は自らの購買情報がどの範囲まで流通し、活用されているかを知らない。

仮に、個人が一日に消費活動で生み出す情報量が１０と過程すると、一日に１万人が来る店舗には１０万の情報量が集まる。店舗がＡという商品の販売成績について知りたいとする。１万人の一人一人が「買った」、「買わなかった」の２分の１ずつの確率を持つので、この場合のエントロピーは、

$$\frac{1}{2}\log_{10}100000 \quad = \quad \frac{1}{2}\ \log_{10}10^{5}\ = 2.5$$

となる。今ここで、10^{5}の情報の中に「時刻」があり開店時の１０時から正午までの来店者を抽出でき、その数が１０００人だった時、

$$\frac{1}{2}\ \log_{10}10^{4}\ =\ \ 2$$

となり、エントロピーが減少する。（対数ベースを２とすれば、ビット単位となるが、便宜上１０ベースで計算）情報のエントロピーとは、情報源の不確定性、曖昧さを表し、情報源から出ている情報の量ともいえるが、時刻という情報によって抽出したことによりエントロピーが減少する。企業は、保有する情報の不確実さ、曖昧さを可能な限り減少させたい。情報流通の中において、如何に保有する情報のエントロピーを減少させる情報を持つかが企業活動にとっては重要であり、企業が時刻といった周辺情報のみならず個人属性情報を収集させる。

デジタル情報は簡単にいくらでもコピー（複写）することができ、無限の大量生産が可能である。これゆえに、物質のコピー（複製）という時とは意義が変化する。物質の場合にはコピー（複製）は偽物であるが、デジタル情報の場合は、オリジナルと同じ価値を持つ。しかもコピーして譲渡･伝達しても情報源から情報は失われない。このため、ＡからＢ、ＢからＣへ情報が流通し、広がっていったとしてもエントロピーは増大しない。情報以外のものは、広がっていくことによってエントロピーは増大していくが、個々の複写された情報はオリジナルと統一であるためエントロピーは増大しないが、受け取り側の情報付加によりエントロピーを減少させ得る。この情報の特質が、現時点では情報の活用者である企業側のメリットとしてのみ機能し、情報源である消費者の経済活動や社会生活において、エントロピーの減少させる方向に働いていないことが課題である。エントロピー増大を制御することこそ情報革命の持つ最大の使命と筆者は考える。

２．３　個人消費活動からみた情報流通の課題(1) (2) (10)

これまでの考察によって、以下の２つの問題点が明らかになった。

i. 消費者に購買情報や個人属性情報がデジタル情報で還されず、店舗以降における企業間の情報流通の中で使用、活用されていること
ii. 消費者は自らの購買情報や個人属性情報がどの範囲まで流通し、活用されているかを知ることができないこと

ＩＴ革命がもたらすと期待される「高度通信情報ネットワーク社会」は、「皆が情報をもてるようになる」社会である。そして、処理・編集・加工などを自在に行えるようになることである。しかし、現状を見る限りにおいて消費者は、その選択肢を持つに至っていない。

（１）高い携帯性と操作性

では、データを発生させた情報主体である消費者に、購買情報や個人属性情報をデジタル化した状態で還すにはどうすればよいだろうか。

方法は２つあると考える。

① 消費者自身が購買情報や個人属性情報を記録する媒体を持ち歩くこと
② 消費者の認証後、消費者毎に情報を保管するセンターにデータを送信し、消費者は任意の時に、自信のデータを自由に取り出し、処理・編集・加工できるようにすること

①も②も、消費者が簡単に持ち歩くことができ、誰でも使用できるモノでなければならない。

記録のためにはメモリを使用する。携帯性の高い記録媒体として、ＥＥＰＲＯＭやフラッシュ、ＳＲＡＭ、ＤＲＡＭ、ＦｅＲＡＭなどのメモリがある。これらは、メモリカード、スマートカード、コンパクトフラッシュ、非接触ＩＣカードなどで使用される。高い携帯性と操作性、そして維持が最も容易であるメモリは何であるか、以降の章で考察を行う。

（２）消費活動の場において使用される商品コード(11)

記録媒体に購買情報の記録がスムーズに行えたとしても、個々の店舗で異なる項目や項目順番が違っていては、編集・処理・加工の段階で、データを一定の形に整形するといった手間がかかる。消費活動はさまざまな場所で行われ、店舗によって導入されているＰＯＳシステムは異なり、手渡されるレシートや領収書のレイアウトが異なっているが、デジタルデータとなった購買情報の処理・編集・加工の効率を上げるためにも、共通した情報流通項目を共通したデータレイアウトで記録しなければならない。ここで、以下に現行のコード体系を整理する。

消費活動に関する「購買情報」と消費活動を行う人に関する「個人属性情報」がある。まず、「購買情報」にはどのような項目があるか。店舗で受け取るレシート、クレジットカードを使用した際のお客様控に記載され、消費者に渡されるものに記載されている項目がまず考えられる。購買詳細項目は消費活動の詳細な記録である。例えば、パン○○○円、電池△△△円、といった内容である。そして購買詳細項目は、家計簿に記載される。消費活動は一店舗だけではなく、さまざまな場所において行われるが、購買情報の処理・編集・加工を効率的に行うためには、後で寄せることができる何らかのキーが必要である。つまり、異なる場所で消費活動を行った場合でも、同一商品には、同一の商品コードがついていなければならない。

図２－３　ＪＡＮコードのコード体系

ＰＯＳ（ Point Of Sale：販売時点情報管理）システムでは商品に印刷してある商品コードを利用している。現在、日本で最も普及している商品コードは、ＪＡＮコードである。世界（アメリカ、カナダを除く）共通の商品コードとして ＥＡＮ （ European Article Number ）コードが１９７７年に制定されたが、これの日本における名称がＪＡＮ（ Japanese Article Number ）コードである。 ＪＡＮコードは日本の共通的な商品コードとなっており、流通情報システムの基盤となっている。ＪＡＮコードはバーコードとして商品に表示され、 ＰＯＳ（ Point Of Sale：販売時点情報管理）システム、受発注システム、棚卸・在庫管理システムなどが利用している。

ＪＡＮコードには、多くの商品分野に利用される「共通商品コード」のほか、雑誌用のコード体系である「共通雑誌コード」、書籍用のコード体系である「書籍ＪＡＮコード」や、「クーポン用ＪＡＮコード」、「料金支払帳票用ＪＡＮコード」がある。

「共通商品コード」は、１３桁（標準タイプ）または８桁（短縮タイプ）からなり、標準タイプでは、１３桁のうち最初の７桁（ただし、２００１年１月以降に新規登録の企業については９桁。７桁または９桁のうち最初の２桁は日本の国コードである「４９」また

は「４５」である）が「メーカーコード」、次の５桁（２００１年１月以降新規登録企業は３桁）が「商品アイテムコード」、そして、最後の１桁が誤読防止のための「チェック・デジット」である。通常、商品には、これらのコードを示す数字とともに、いわゆる「バーコード」と呼ばれる表示とあわせて、「ＪＡＮシンボル」が包装された商品上に表示されている。そして、このシンボルが、通常、ＰＯＳ端末によって読みとられる。

「メーカーコード」は、日本では財団法人流通システム開発センターが一元的に管理しており、各企業が財団法人流通システム開発センターに登録申請を行い、財団法人流通システム開発センターがコードの割り当てを行っている。また、「商品アイテムコード」は、ある一定の設定基準に基づいて、「メーカーコード」の割り当てを受けた企業が、小売業で単品レベルでの管理ができるような単位で設定し、自主的に付番している。なお、一度付番した「商品アイテムコード」の再利用にあたっては、通常では出荷停止後最低４年は空け、かつ、小売や卸売での流通在庫がなくなったことを確認することが企業に対して要望されているため、異なる商品が同一の「商品アイテムコード」を持つことは許されていない。消費財の大部分の商品には、ＪＡＮコードが付番されているが、消費財でありながら、ＪＡＮコードが付番されていない商品の種類の例として次の商品がある。

- 自動車部品（カー用品は除く）
- 自動車そのもの
- 住居関連（ホームセンターのような業態で扱われるような商品を除く）
- 生鮮食料品（加工食品については付番されている）

自動車部品、自動車そのものや住宅関連の消費財は、個人消費活動において扱うことが頻繁でないためマニュアル処理が可能であるが、生鮮食料品は、個人消費活動において最も頻繁に購入する商品であり、購買情報において占める割合も少なくないため、生鮮食料品のコードをどのように行うかが課題である。ただし、現在、ＪＡＮコードを持たない生鮮食料品もＥＤＩ化の推進から平成１２年に生鮮ＪＡＮコード化が決まっている。

ＪＡＮコードを一括管理しているデーターベースにＪＩＣＦＳがある。ＪＩＣＦＳで管理している具体的項目は下記のとおりで、登録は、主として商品メーカーが行っている。

- ＪＡＮコード（ＥＡＮコード、ＵＰＣコード）
- ＪＩＣＦＳ商品分類コード
- 正式（漢字）商品名
- カナ商品名
- 内容量・重量

➢　単品サイズ

近年の調査によれば、一般のスーパー・マーケットで取り扱われる食料品・日用品の８５～９０％ 、コンビニエンスストアでは９５％ 以上がＪＩＣＦＳに存在する。ＪＡＮコードが付与されているもののＪＩＣＦＳに登録されていない商品は、他社・店舗においてあまり取り扱われていない商品で、すなわち、店舗独自でＪＡＮコードが付与されている商品（インハウスコード商品とも言う)、あるいは、ある地域で独自に流通している商品である。なお、このようなＪＡＮコードが付与されているもののＪＩＣＦＳに登録されていない商品の具体的種類は、日配品、総菜、豆腐等である。

以上が現在、主にＰＯＳシステムで使用されているＪＡＮコードである。これらを踏まえ、以降の章で新しい情報流通項目とデータレイアウトについて提案を行う。

（３）セキュリティ対策

購買情報や個人属性情報が流通することによって、消費者が不利益を受ける、不安を感じるといったことがあってはならない。本人以外が情報の取出しを行うや、流通の過程において情報が漏洩する、改ざんされるといった不安を払拭する高いセキュリティが要求される。セキュリティ対策について以降の章で考察を行う。

（４）流通範囲のコントロール

セキュリティ対策は消極的な安全対策であるとも言える。では、消費者が積極的に購買情報や個人属性情報の流通範囲や活用について知り、コントロールするためにはどうすればよいだろうか。

デジタル情報は「０」と「１」で表現され、「０」と「１」が全く同様に並んだ同じ情報であったとしても、消費者と店舗（企業）によってその情報から得る情報量が異なり、一つの情報が消費者自身の発生させた購買情報と店舗側の販売情報といった二面を持つ。

例えば、消費者がチョコレート１箱を２５０円で買ったとする。この消費活動によって「チョコレート　１箱　２５０円」といったデジタルデータをＰＯＳ端末が生成する。このデータは消費者の消費活動によって生じたものなので消費者にとっては、「私の購買情報」である。一方、店舗は仕入れを行い、消費者に売った情報であるため「当店の販売情報」である。物質としてのチョコレートは、販売者である店舗から消費者へ所有権が清算によって移るが、「チョコレート　１箱　２５０円」という情報は、１つの情報でありながら所有者が２者いるということになる。これが、一つの情報が消費者自身の発生させた購買情報と店舗側の販売情報といった二面を持つということである。

この場合、消費者は「私の購買情報」として単独所有権を主張することは出来ない。そして、販売情報の分析や活用は、企業活動上妨げられるものではない。

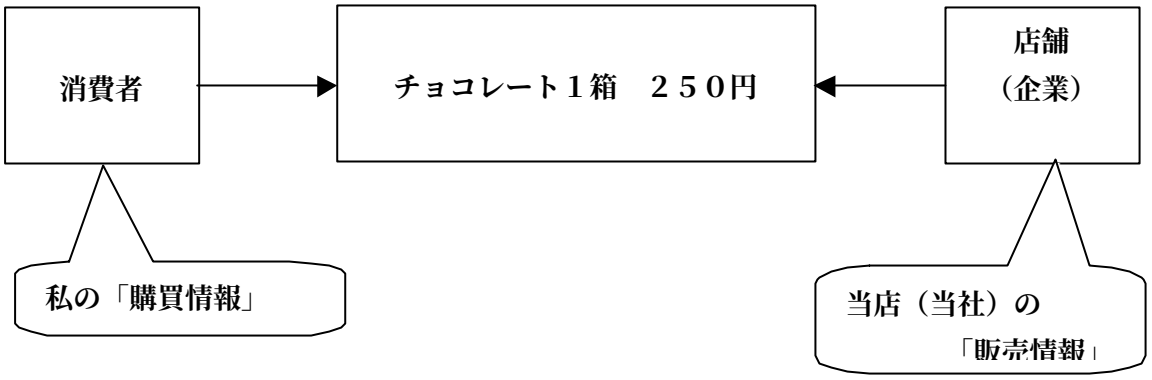


図２－４　消費活動の場で発生する情報の２面性

では、個人属性情報はどうであろうか。個人属性情報は、元々、消費者個人に属している情報である。これが、消費活動の場において消費者が意識した店舗（企業）以外に流通してしまう。

例えば、消費者がＡ社から購入した商品について、消費者はＡ社に顧客登録をしたつもりだが、Ａ社からＢ社、Ｃ社などに消費者の情報が知らない間に流通され、Ｂ社やＣ社で保有されてしまうといった問題である。

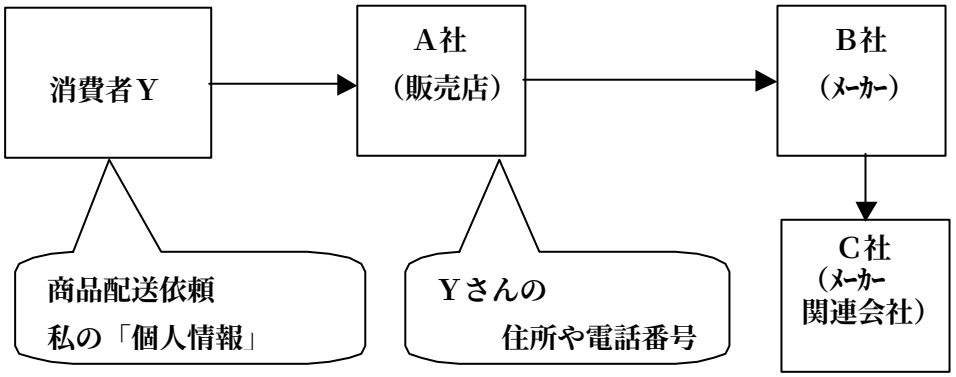


図２－５　消費者が知らないところに個人情報が流通

しかしながら、店舗（企業）は、多くの消費者が発生させた販売情報を消費者の個人属性情報や時刻といった周辺情報を使いエントロピーを減少させ、分析精度をあげたマーケティングを行いたい。このため、販売情報と個人属性情報の一部が一つとなり企業間で流通することも有り得、現に行われている。自らの情報をコントロールする方法について、以降の章で考察を行う。

第３章　個人消費活動における新しい情報流通システムの提案

２章での調査研究で抽出した課題の解決方法として、新しい情報流通システムの提案を行う。まず、情報流通項目、その後、セキュリティ、メモリ、そして情報流通範囲のコントロールに関する検討の後、個人消費活動における新しい情報流通システムの提案を行う。

３．１　情報流通項目(11)

第２章において行ったＪＡＮコードについての考察から、インハウスコードや、地域限定の商品等に国際標準コードにのっとったＪＡＮコードがついていない課題は残るが、ＪＡＮコードを使用すれば、約８割の「購買情報」はフォローできると判断する。

よって、購買情報を効率的に処理・編集・加工するためのキー項目としてＪＡＮコードを利用する。そして、ＪＡＮコードがない日配品、総菜、豆腐、生鮮食料品などを処理するための補助的情報として商品名を持つ。

この他に、レシートに記載される日時、店舗名、連絡先、レジ番号、レジ担当など、後から購買情報について店舗に問い合わせをするために必要な情報を持つ。

現金決済以外のキャッシュカードやデビッドカードなどの決済（以降「キャッシュレス決済」と呼ぶ）がある。最近は、ＰＯＳ端末で処理される小額決済の場合は、サインレスで処理が行われることがほとんどであるが、これらの「使用控え」をレシートとともに消費者が受け取るケースがほとんどである。このキャッシュカードやデビッドカードなどのキャッシュレス決済の場合も「使用控え」を購買情報とともに記録する。これは、今後、増えるであろうキャッシュレス、電子マネー時代の消費活動において、使い勝手のよい新しい情報流通システムとなることを考慮した。

レシートの場合、店舗はレシートに消費者へのお知らせを記載する、登録顧客の場合はポイント数を記載するなどを行っている。このため、店舗が自由に使用できる項目スペースを一定の長さ用意する。

以上のことをまとめたデータレイアウトを表３－１に記す。

表３－１　購買情報項目

項目名		例	データ必要長（バイト）
基本項目	消費活動年月日	YYYYMMDD	8
	時間	HHMMSS	6
	場所（店舗名）	○×△ショッピングセンター	４０
	店舗電話番号	03-1234-1434	14
	レジ番号	××	2
	レジ担当者名	○○○○	１０
キャッシュレス決済項目（現金決済時はなし）	会社コード	11111111	１０
	カード番号	1234-1111-2222-3333	２２
	有効期限	05/07	6
	支払い回数	一括	3
	伝票番号	1234567890	１０
	商品区分		3
	取扱区分		3
	処理通番		5
	承認番号		１０
購買詳細情報	商品点数（n）	n	2
	S_1	商品コード（商品名）１３桁＋７桁	２０
	S_1の外税金額	150	6
	S_2	商品コード（商品名）１３桁＋７桁	２０
	S_2の外税金額	198	6
	S_n	商品コード（商品名）１３桁＋７桁	２０
	S_nの外税金額	98	6
	外税金額合計	446	6
	消費税額	22	6
	内税金額合計	468	6
店舗使用項目	フリー欄１		２０
	フリー欄２		２０

基本項目エリアの合計バイト数＝８０

キャッシュレス項目エリアの合計バイト数＝７２

詳細購買情報エリアの合計バイト数＝２＋２６×商品点数＋２４＝２６（１＋商品点数）

店舗使用項目エリアの合計バイト数＝４０

次に「個人属性情報」である。「個人属性情報」のうち「基本属性」は、消費者へ還す情報ではなく、店舗がマーケティングのために欲しい情報であるため、ポイントなどの特典の代わりとして顧客情報を収集するハウスカードやポイントカードといった手法がとられている。このため、各店舗（企業）が独自のインハウスやポイントカードを発行するため、消費者は複数枚のカードを管理しなくてはならない。全て同じ記録媒体にこれらの機能をもたせれば、消費者は店舗毎に異なるカードを持つ必要がなく、利便性は高い。

表３－２　個人属性情報項目

項目名		データ長（バイト）
基本属性	氏名	20
	住所	40
	電話番号	14
	電子メールアドレス	20
	性別	1
	生年月日	8
金融機関情報（×　n）	（クレジットもしくはデビッドカード）会社コード	10
	カード番号	22
	有効期限	6

金融機関項目エリアの合計バイト数＝３８
基本属性エリアの合計バイト数＝１０３

１人の消費者が複数のクレジットカードを持っているケースが少なくない。この個人属性情報項目は、金融機関単位に作成することができる。

以上、購買情報と個人属性情報は以下のイメージで記録媒体に記録するものとする。

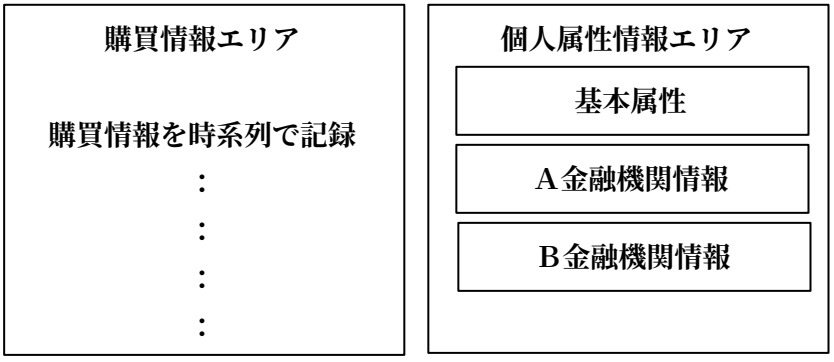


図３－１　流通情報データエリアのイメージ

３．２　システム構成要件

（１）高い携帯性と操作性

情報を記録する媒体は、消費活動の場に手軽に持っていくことができなければならない。第１章でも述べたが、ＩＴ革命がもたらす「高度通信情報ネットワーク社会」は、「皆が情報をもてるようになる」社会であり、当システムも情報機器の操作が苦手な人達も皆、情報をもてるようになることを目指している。

そのためには、記録媒体に邪魔になる程のバッテリーがついていては携帯に不便である。消費活動の場に必ず持って行く財布の中やいつも身につけている指輪やネックレス、時計といったモノに情報を記録できることが理想である。このため、可能な限り小型で低消費電力のバッテリーで動作する、もしくはバッテリーが必要ない記録媒体であることが要件となる。

（２）セキュリティ対策

近年のネットワーク構築はインターネットをインフラとしている。よって当システムもインターネットを通信インフラとして使用することを前提とする。

この場合、インターネット上で「他人の使用」、「不正アクセス」、「データ改ざんやコピー」、「通信データの盗聴」といった脅威が発生する。カード犯罪の犯罪発生の要因を見てみると、暗証番号の漏れが最も多く過半数を超えている。

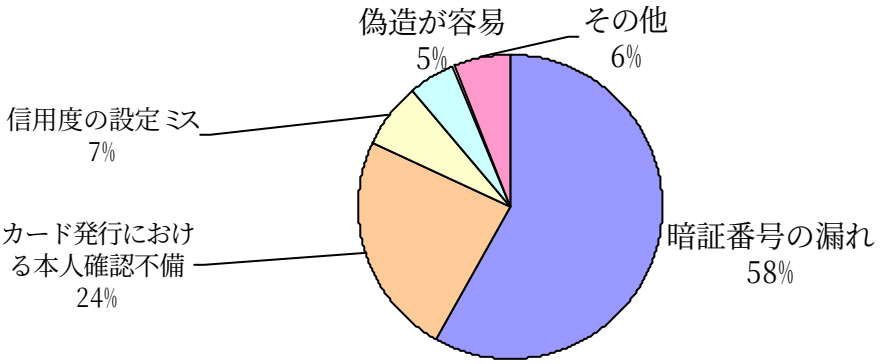


図３－２　カード犯罪発生の要因(12)

最も多い暗証番号の漏れを防ぐために、暗証番号を漏らさない、盗聴されない技術が必要である。また、仮に盗聴されたとしても、暗証番号が分からないような仕組みとしておく必要がある。このような技術として「認証技術」と「暗号技術」がある(13)。

いくら暗号化されていたとしても、毎回同じ形式に暗号化されていては、いずれは解読されてしまう。この危険を回避するために、毎回異なるパスワードの送信を行うのがワンタイムパスワード方式である(13) (14)。この方式を、新しい情報流通システムに使用することによって、高い認証面でのセキュリティを確保する。この時に、ＰＯＳ端末前で消費者を待たせることなく、本人であることの確認（認証）を行わなければならないため、出来うる限り処理の速いワンタイムパスワード方式を求める。

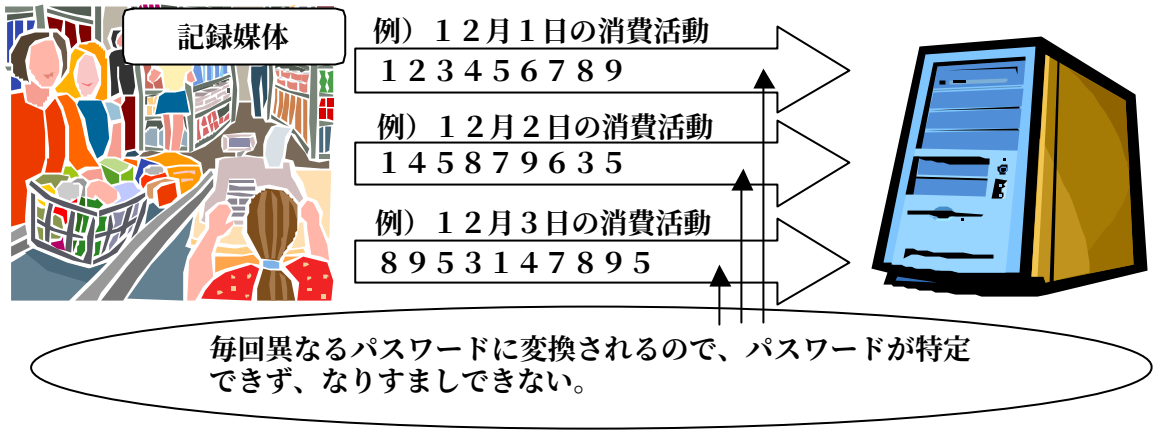


図３－３　ワンタイムパスワード

新しい情報流通システムでは、認証だけでなく、購買情報や個人属性情報も扱うため、これらの情報が仮に盗聴や漏洩したとしても解読できない状態にしておく必要がある。よって購買情報や個人属性情報を暗号化する。この場合も、ＰＯＳ端末前で可能な限り消費者を待たせない処理の速さが求められる。

購買情報と個人属性情報ではセキュリティレベルが異なる。購買情報は個人属性情報と結びつかない限り個人情報とはならない。よって個人属性情報には、より高いレベルのセキュリティ技術の適用が必要である。

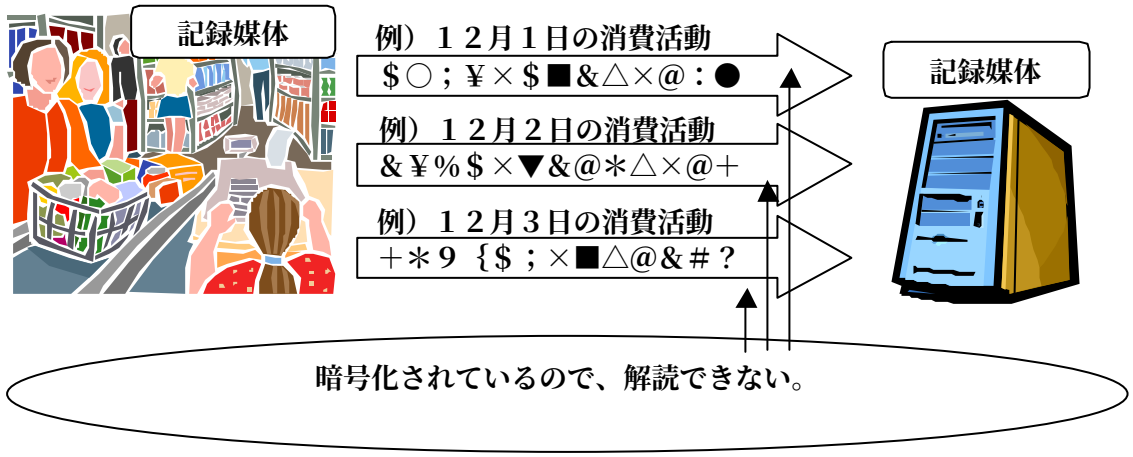


図３－４　暗号処理

（３）メモリ(15) (16)

「（１）高い携帯性と操作性」の中において、可能な限りバッテリーが小さい、もしくはバッテリーが必要ない記録媒体であることが要件となると書いた。通常、不揮発性メモリは、常に電力による刺激を与えることによってデータを保持しているが、当システムにおいては、バッテリー不要で記録データを保持することのできるメモリでなければならない。

「（２）セキュリティ対策」で書いたワンタイムパスワードは、毎回異なる認証情報を送信することによって安全性を高める。このため、ワンタイムパスワードは、その認証情報算出のため、毎回異なる情報を次の認証計算のために持っていなければならない。この為、Read/Write が可能なメモリの必要があるが、通常、メモリの Read/Write は破壊読出しによって行われる。この破壊読出しを行った場合、元の状態に書き直しておく作業が必要であり、セル毎に余分の配線を必要とし、高集積化には好ましくない。また、破壊読出しはセル毎の閾値余裕（ノイズマージン）のばらつきのため、記録情報が正しく読み出せなかったり、読み書きの間に一部が消えてしまったりする。つまり、一度、トラブルが発生すると、以降、認証が行えないことになり、システムの安定性が悪くなる。よって、高いシステムの信頼性の為には、記録してある情報を消すことなく読み書きを行う非破壊読み出しのメモリが必要である。

現在、想定している購買情報の固定エリアの合計長は１９２バイトである。これに、可変エリアである購買詳細情報の２６バイトが（１＋購入品目数分）追加される。例えば、１回の消費活動において３０品目を買うとすると約１Ｋのデータ量となる。

仮に、消費者の持つ記録媒体に購買情報を記録する方法をとるのであれば、ＰＯＳ端末前で消費者を待たせることなく、約１Ｋの情報を記録できなければならない。

また、一日に消費活動をする場は一箇所とは限らない。例えば、１日５箇所程度で消費活動を行うとする。消費活動の度にワンタイムパスワードは次回の計算のために情報の更新をするため、この場合、５×３０×１２＝１８００回／年の書き込みがメモリに行われることになる。ＰＣや街角端末からの処理などを考慮すると約５倍の１万回／年の書換え可能なメモリである必要がある。また、頻繁にメモリの交換を行うことは実用的でないので、できる限り長く、何度も書替えができるメモリである必要がある。

以上から、メモリの要件を以下のように整理する。

① バッテリー不要もしくは非常に小さい上に不揮発性
② 非破壊読出し
③ 実用性のある迅速な記録スピード
④ 最低でも１万回／年以上の書換え可能（10^4以上の書替え）

上記４点を満たすメモリは何であるか。現在、利用されているメモリには、ROM（Read Only Memory)、MASK－ROM、PROM(Programmable ROM)、EPROM(Erasable Programmable ROM)、EEPROM（Electrically Erasable Programmable ROM)、RAM（Random Access Memory)、DRAM（Dynamic Random Access Memory）そして最近になって実用化されたFeRAM（Filed Reconfigurable Memory）がある。これらの中から書替えが可能な不揮発性メモリを選び、フラッシュとともに比較を行った。

内部書込電圧、スタンバイ電圧ともに低く、１万回／年以上の書換え可能、つまり 10^4 以上の書替えが可能であり、読み出し、書き込み、書替えの時間が最も速いメモリは、FeRAMである。よって、FeRAMに関する技術動向を次章にて検証し実用化について検討を行う。

表３－３　ＩＣカードで使用されるメモリの種類と特徴(15)

メモリの種類	特徴
ROM	読み出し専用メモリ。通常、一度記憶されたデータの変更、消去はできない。
MASK－ROM	製造段階で記憶情報を印刷パターン化したROM。
PROM	プログラム可能なROM。
EPROM	紫外線を照射することにより、データを消去し、再書き込みが可能なROM。ただし、ＩＣカードの場合、カード内メモリに紫外線を照射することができない為、記憶内容の書替えは不可。
EEPROM	記憶内容を電気的に消去し、書替え可能としたROM。
RAM	情報の読み出し、書き込みが自由なメモリ。電源が切れると記憶されている情報が消去される為、カード化の場合バッテリーが必要。
FeRAM	情報の読み出し、書き込みが自由なメモリ。電源が切れても記憶されている情報が消去されない。バッテリー不要。

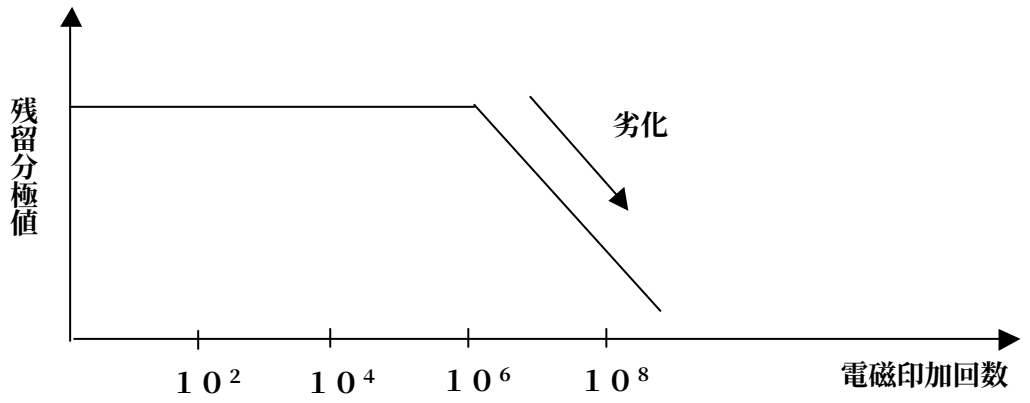


図３－５　疲労劣化特性 (24)

表３－４　不揮発性メモリの特徴比較(15)

	FeRAM	EEPROM	フラッシュ
内部書込電圧(V)	2	12	12
読み出し時間	75ns/byte	200ns/page	100ns/byte
書き込み時間	75ns/byte	10ms/page	10μs/byte
書替え時間	75ns/byte	10ms/page	10μs/byte (block:500ms)
書替え可能回数	10^{13}以上	10^{4}	10^{6}
ビット書替え	可	可	不可
セルサイズ	0．5	1	0.25
スタンバイ電流(μA)	≪1	≪1	≪1
アクセス性	ランダム	ランダム	ブロック消去
データ保持（年）	10	10	10

FeRAM；破壊読出しのため、読み出し時でも同一データの再書き込みが必要

EEPROM；page(数byte～数+byte)単位

フラッシュ；書替えは追記式のため、通常は書き込みと同じ。消去はブロック単位

（4）流通範囲のコントロール

２章において、「消費者は自らの購買情報や個人属性情報がどの範囲まで流通し、活用されているかを知ることができない」つまり、流通範囲のコントロールができない、ことが問題点であると指摘した。

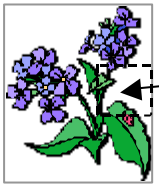
消費者が不安に感ずるのは、基本属性が自ら許可しない、知らない範囲まで広がっているという点である。つまりA店には、商品配達のために自宅住所や電話番号、氏名を教えたが、この情報がA店以外のBやCに漏れてしまう可能性がある。

個人属性情報のようなテキスト情報は、デジタルコンテンツと異なり部分的な複写、一部分だけの取り出しでも十分目的を果たせることが多い。例えば、生年月日は年月日まで全て分からずとも誕生月が分かっただけでも、マーケティング情報として有効に作用し得る。

個人属性情報：２００１年１２月１日生まれ　20011201　→　1201

⇒　１２月１日だけでも役割を果たせる

デジタルコンテンツ：



一部だけを取り出しても、あまり役にたたない

図３－６　テキスト情報とデジタルコンテンツの違い

また、テキスト情報は、画像や音声のデジタルコンテンツと異なり、透かし技術の適用やＤＡＴ／ＭＤなどの専用デジタル録音再生機器におけるＳＣＭＳ（Serial Copy Management System）を利用した二世代以降コピー不可といった技術も、現時点では適用できない。

では、テキスト情報である個人属性情報の流通範囲をコントロールするためには、どのような方法があるであろうか。具体的な例を引きながら考えてみる。

《　例　》

ASCIIコードの「ｲﾁﾛｳ」は、２進法で「10000010100100101011101110000011」である。

今、「10000010100100101011101110000011」の

１ビット目＋３２ビット目（1+1=0）、　８ビット目＋　９ビット目（0+1=1）、

１６ビット目＋１７ビット目（0+1=1）、２４ビット目＋２５ビット目（1+1=0）

とした値（0110）（仮に以降「雑情報」と呼ぶ）を、「ｲﾁﾛｳ」の各ワード「ｲ」「ﾁ」「ﾛ」「ｳ」の間に埋め込み「ｲ0ﾁ1ﾛ1ｳ0」とする。つまり、「10000010010010010110111011110000011 0」とテキスト情報が再構成される。このような仕組み（アプリケーションソフト）を開発すれば、雑情報が入っているために、専用のアプリケーションソフトがなければ、データを正しく読むことが出来ない。個人属性情報の扱いに対する協定などを作成し、それに同意する店舗（企業）のみに、専用アプリケーションソフトを配布するようにすれば、一定のコントロールはできる。しかし、専用ソフトを使って正しく読んだ店舗（企業）は、目視するだけではなく、コンピュータシステム内部で処理を行う為に雑情報を排除して扱うことを必要とする。そして、雑情報排除後のデータを他へコピーし、渡されてしまうと、以降は情報のコントロールができない。

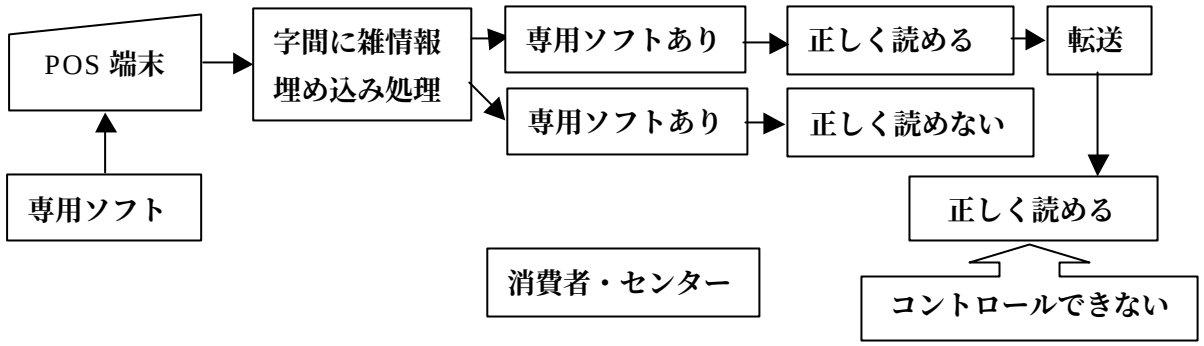


図３－７　雑情報埋め込み後

では、個々の情報を暗号化する場合はどうであろうか。最初に復号する時に消費者に鍵をもらいに行くといった仕組みを作ることによって､最初の段階における個人属性情報のありかを消費者は知ることができる。これによって、一定の管理する目的は達せられるが、復号の後に、他へコピーし渡されるケースも考えられる。この場合も上記と同様に、以降の流通経路に対してコントロールを行うことができない。

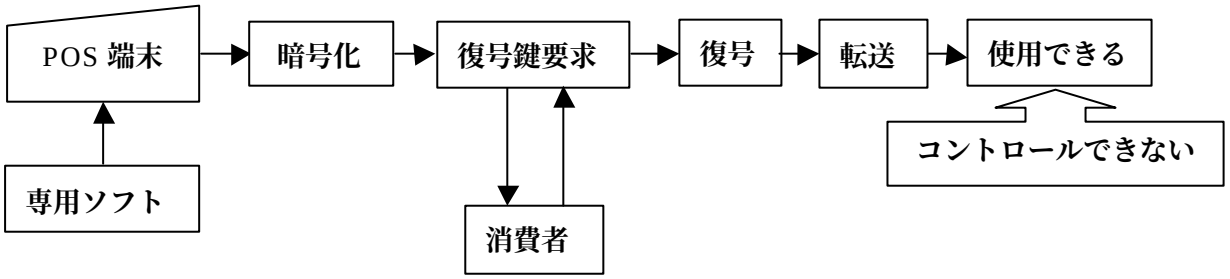


図３－８　暗号化－復号後

このようなことから、現時点では、「雑情報の埋め込み＋個々人ごとに暗号化を行う」といった技術的な対応と、雑情報の専用ソフトを入れる企業や店舗に対して、社会的責任と個人情報保護といった観点から規約や規制で縛る方法とを結びつけて行かなければならないのではないかと考える。

この方法は、さらに研究を重ねることによって有効な方法とすることができるかもしれないが現時点では当システム具現化のための技術的ブレイクスルーと成り得ていない。よって、今後の継続研究課題としたい。

尚、ＯＥＣＤ（経済協力開発機構）において１９８０年に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」いわゆる「ＯＥＣＤ８原則」

が採択され、国においては「個人情報保護基本法制に関する大綱」が平成１２年策定され、地方自治体においても「個人情報保護条例」が策定されつつあり、社会における個人情報取り扱いに関する法整備が進んでいる(5)。

ＯＥＣＤ８原則（25）

１．収集制限の原則
個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。

２．データ内容の原則
個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。

３．目的明確化の原則
個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。

４．利用制限の原則
個人データは、第 9 条により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。
（ａ）データ主体の同意がある場合、又は、（ｂ）法律の規定による場合

５．安全保護の原則
個人データは、その紛失もしくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

６．公開の原則
個人データに係る開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。

７．個人参加の原則
個人は次の権利を有する。（ａ）データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること。（ｂ）自己に関するデータを、（Ⅰ）合理的な期間内に、（Ⅱ）もし必要なら、過度にならない費用で、（Ⅲ）合理的な方法で、かつ、（Ⅳ）自己にわかりやすい形で、自己に知らしめられること。（ｃ）上記（ａ）及び（ｂ）の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異義を申立てることができること。（ｄ）自己に関するデータに対して異義を申立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

８．責任の原則
データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

３．３　実用化システム構想の提案

個人消費活動の場を「Direct Shopping」、「Catalog Shopping」、「Web Shopping」に分け、情報の流れを確認し、問題点、課題を抽出した。

ショッピングの３つの形態にはそれぞれの特徴があるが、以降は、最も日常生活において頻繁に消費活動が行われる「Direct Shopping」を対象とし、情報流通の実用化システム構想の提案を行う。

本研究の目的は、個人消費活動において、一版の消費者が容易に情報の蓄積・処理・編集・加工ができる仕組みを構築し、かつ、簡単にネットワークに接続できる情報機器もしくはＩＴ環境を具現化することにある。このことによって、消費者は高度通信情報ネットワーク社会の構成員となる選択肢をもつことができる。

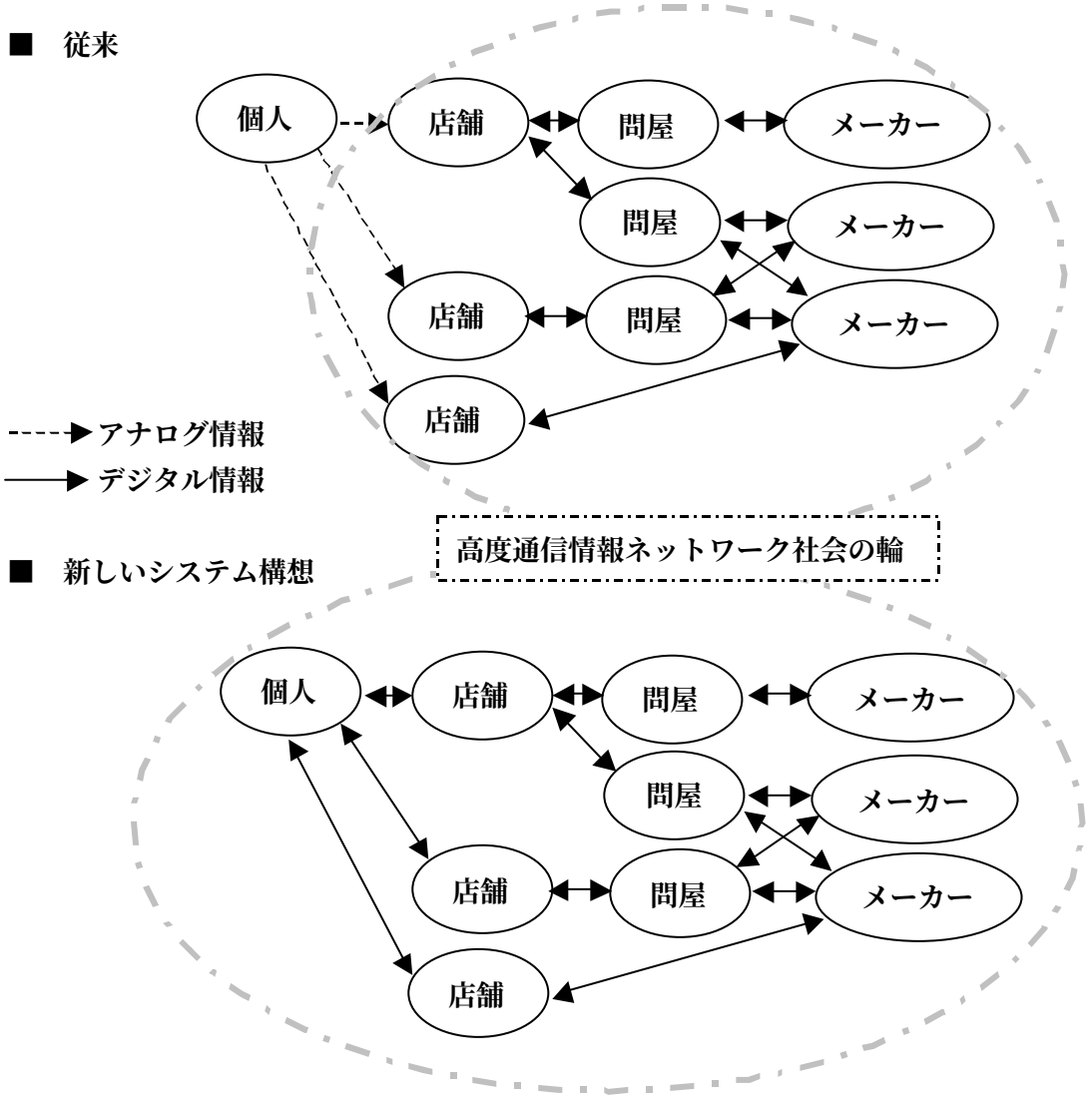


図３－８　従来と新しいシステム構想

ＰＯＳ端末にてデジタル化された購買情報を消費者が所有することができるようにする。所有する場所は、消費者が持参する記録媒体もしくはセンターとする。

記録の場合、消費者が持参した記録媒体が、持参した本人のものであるかどうかの認証が必要である。その後、情報の暗号化を行った後、記録する。

■　購買情報の記録

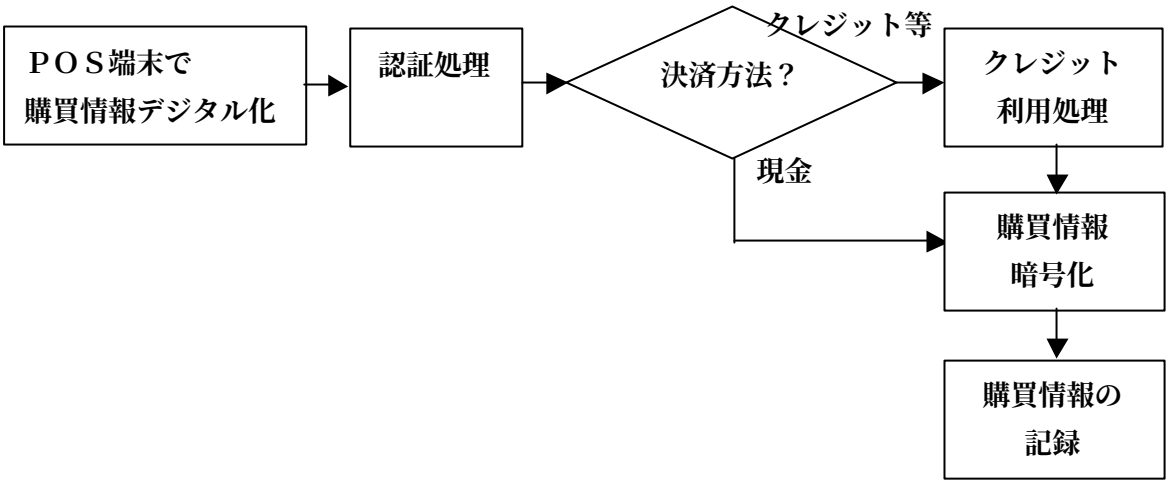


図３－９　記録処理ＪＯＢ構成図

記録した購買情報の処理・編集・加工の場合、記録時と同様に、まず、消費者が持参した記録媒体が、持参した本人のものであるかどうかの認証が必要である。その後、暗号化されている情報の復号を行い、別媒体への出力を行う。その後、データの処理・編集・加工を行い、記録媒体に購買情報を記録していた場合は、記録媒体から消去を行う。データの処理・編集・加工は、個人のＰＣで専用のアプリケーションソフトをダウンロードして行う方法と、街角に設置する端末の画面操作指示に従って行う方法の２方法を用意する。街角端末の使用によって、ＰＣなどＩＴ機器の操作が苦手な人たちも、高度通信情報ネットワーク社会の技術を利用することができるようになり、消費活動におけるデジタルデバイドが減少する。

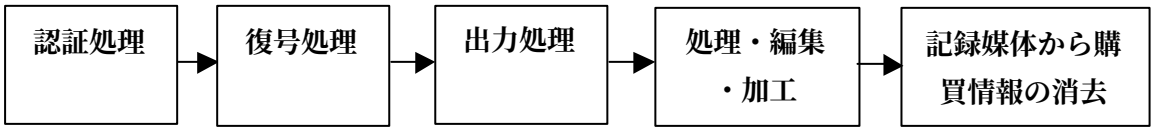


図３－１０　処理・編集・加工処理ＪＯＢ構成図

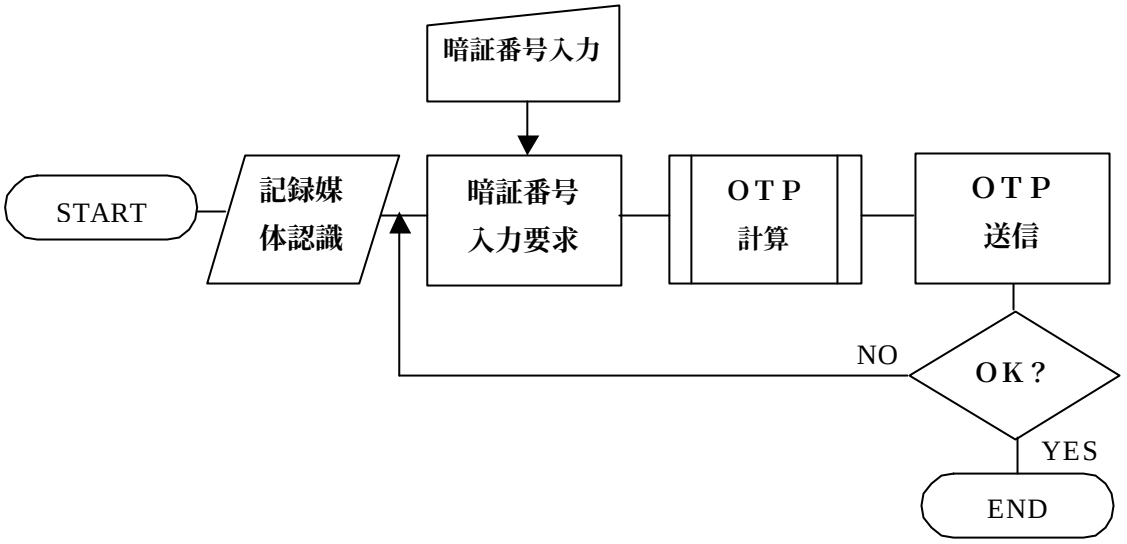


図３－１１　認証処理ＪＯＢフロー

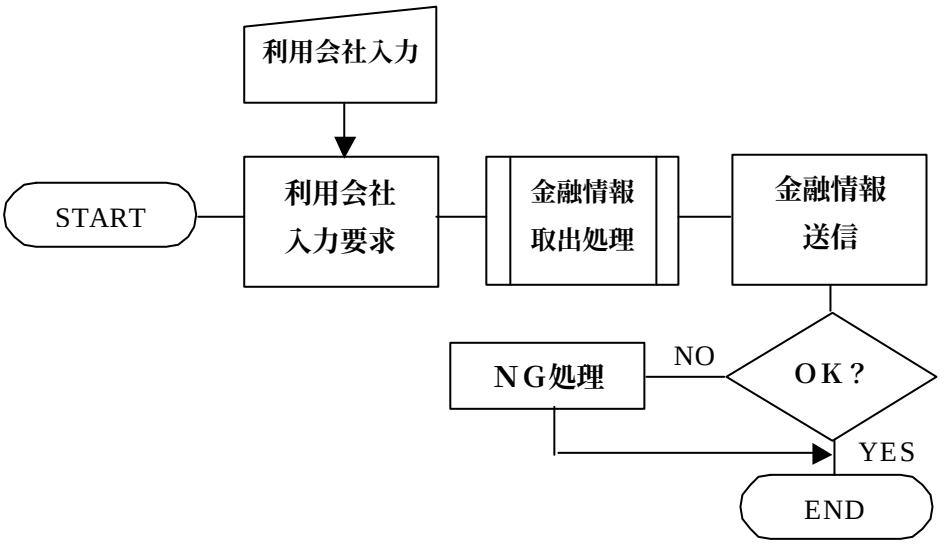


図３－１２　クレジット利用処理ＪＯＢフロー

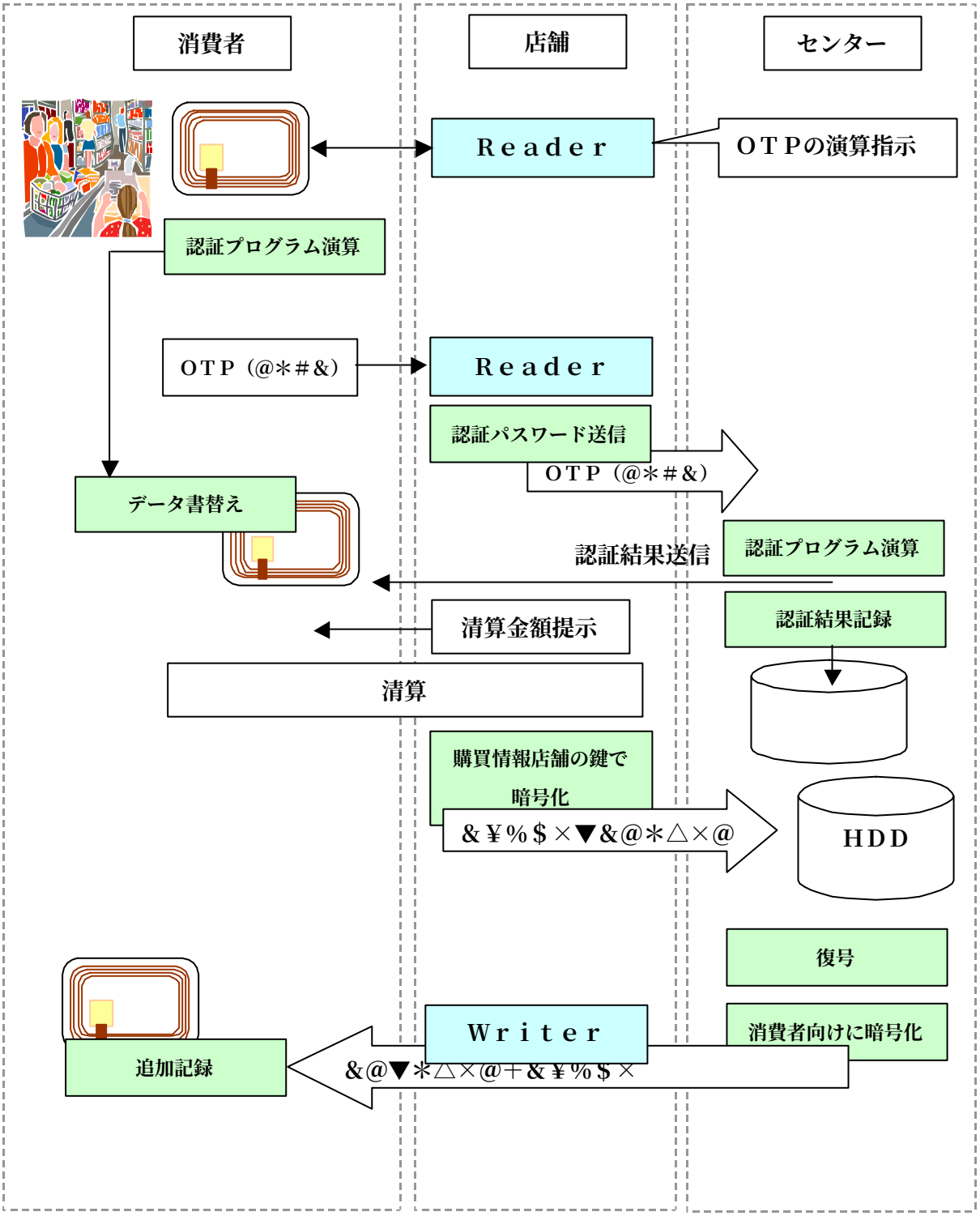


図３－１３　システム構想～個人認証・記録処理

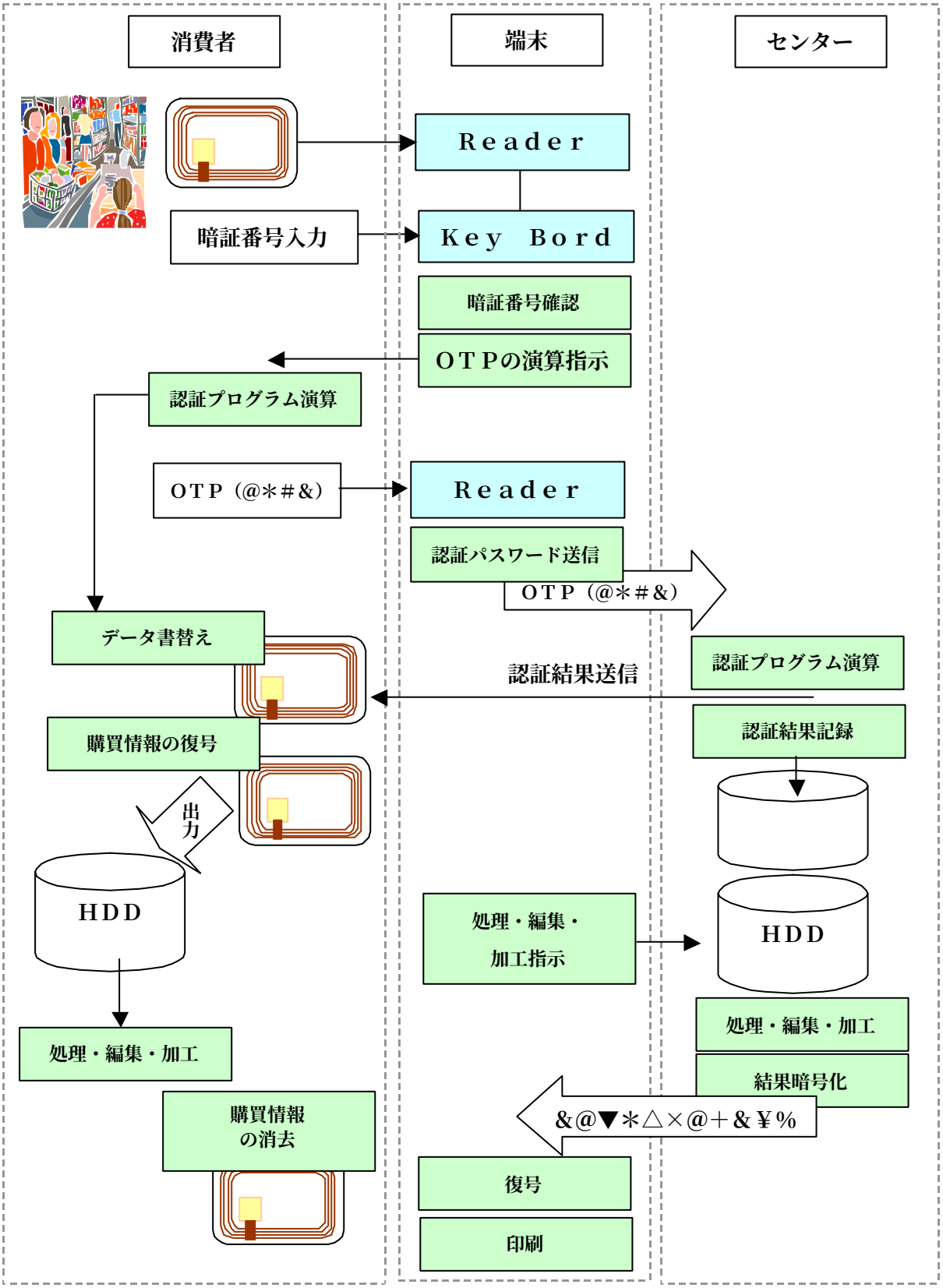


図３－１４　システム構想－個人認証・情報取り出し（復号）・消去処理

第四章　新システム具現化のための技術的ブレークスルー

前章において、個人消費活動における新しい情報流通システムの構成要件をあげ、構想の提案を行った。この章では、前章であげたメモリと高セキュリティについての技術的ブレークスルーを検討し、最先端の認証・暗号技術とメモリ技術の融合により当システムの実現を図る。

４．１　認証・暗号技術の適用によるシステム安全性の向上

まず、第三章で優位性の明らかになったワンタイムパスワード認証技術には主に３つの方式がある。この３つの方式の中で最も処理速度が速く、使用が容易な技術はどれか確認を行う。

次に、２つの方法に分けられる暗号技術の当システムへの適用について考察する。

（１）ワンタイムパスワード認証方式[10] [13] [14] [16]

ワンタイムパスワード方式には、フリーソフトウェアのＳ／ＫＥＹやＯＰＩＥ（One-time Passwords In Everything）、ＳｅｃｕｒＩＤ、ＳＡＳ（Simple And Secure Password Authentication Method）など３つの方式がある。

Ｓ／ＫＥＹは、Ｂｅｌｌｃｏｒｅで開発された一方向ハッシュ関数を基にしたワンタイムパスワードである。ＵＮＩＸシステムに実装されるもので、ハッシュ関数にはＭＤ４ハッシュやＭＤ５、ＤＥＳ－ＭＡＣなどがある。Ｓ／ＫＥＹは、三種類のデータを使用する。一つは、ユーザーがプログラムに対して入力する秘密のパスワードであり「パスフレーズ」とも呼ばれる。もう一つは「シード（種）」または「キー」と呼ばれるもので、二つの文字と五つの数字で構成される。最後の一つは「シーケンス番号」で、１以上の整数である。シーケンス番号は特に指定しなければ１００以下であるが、９９９９まで指定できる。

Ｓ／ＫＥＹは、まずシードとパスフレーズを連結し，それに対してシーケンス番号の回数だけ一方向ハッシュを繰り返し計算する。そしてその結果を６つの英単語に変換し、６４ビットの収まるよう変換処理を行う。プログラムは前回最後に受け付けられたワンタイムパスワードを記録しているので、前回のワンタイムパスワードと、 ユーザーが入力したワンタイムパスワードを一回ハッシュ関数にかけた結果とが一致した場合に、ユーザーを認証する。一方向ハッシュ関数を使うことにより，もし (ログイン等に成功した) ワンタイムパスワードが一回盗聴されたとしても、 次回以降に使われる複数のワンタイムパスワードを生成することは不可能である。シーケンス番号は認証が成功するたびに１ずつ減らされ、ユーザーとログインプログラム の間で同期が取られる。シーケンス番号が「０」となると、

初期化を行わなければならない。

ＯＰＩＥは、US Naval Research Laboratory(NRL)が開発したＳ／ＫＥＹの改良版である。ＭＤ４ハッシュやＭＤ５、ＤＥＳ－ＭＡＣなどをサポートし。Ｓ／ＫＥＹに比べ、セキュリティの改良を行っているが、基本的な計算方法は同じである。

ＳｅｃｕｒＩＤは、トークンと呼ばれる液晶表示をもったカード型やキーフォルダー型をしているハードを用いる。トークンは、６０秒毎に予測不可能なアクセスコード（パスワード）を生成し、認証サーバーと共用する。認証サーバーとＳｅｃｕｒＩＤは、常に時間同期が取られて（タイムシンクロナス方式）おり、ユーザーは液晶に表示されるパスワードを自ら入力するため、毎回異なるパスワードが生成される。ＳｅｃｕｒＩＤは液晶に表示されるパスワードを入力しなければならない為、面倒でありハード面でのコストもかさむのが問題である。

（株）日本システムディベロップメント　　シチズン時計株式会社

図４－１　トークン（例）

ＳＡＳは、シーケンス番号を決める必要がなく、このため、シーケンス番号の不足といったことが有り得ない。よって、半永久的に使用できる。また、Ｓ／ＫＥＹがシーケンス番号の回数分、暗号化の計算をしているのに対して、ＳＡＳは計算回数が少なく、パスワード生成時間がＳ／ＫＥＹやＯＰＩＥと比べて速い。

同じＣＰＵ、ＭＤ４ハッシュ関数を使用する場合（計算処理だけを比較すると）、シーケンス番号を９９９９と設定したＳ／ＫＥＹが１回の認証計算を行っている間に、５回計算のＳＡＳは１９９９回、３回計算のＳＡＳは３３３３回の認証計算を行うことができ、処理速度において圧倒的な優位性がある。よって、当システムでは個人認証にＳＡＳを使用する。

A：ユーザーＩＤ、Ｓ：ユーザーパスワード、ｎ：認証回数。０以上でなければならない。
N_n：n 番目の認証に対するランダムな数値、

E：ハッシュ関数。E_n^m とは N_n を使ってm回、$(S \oplus N_n)$をハッシュ関数で計算すること。

⊕：排他的論理和

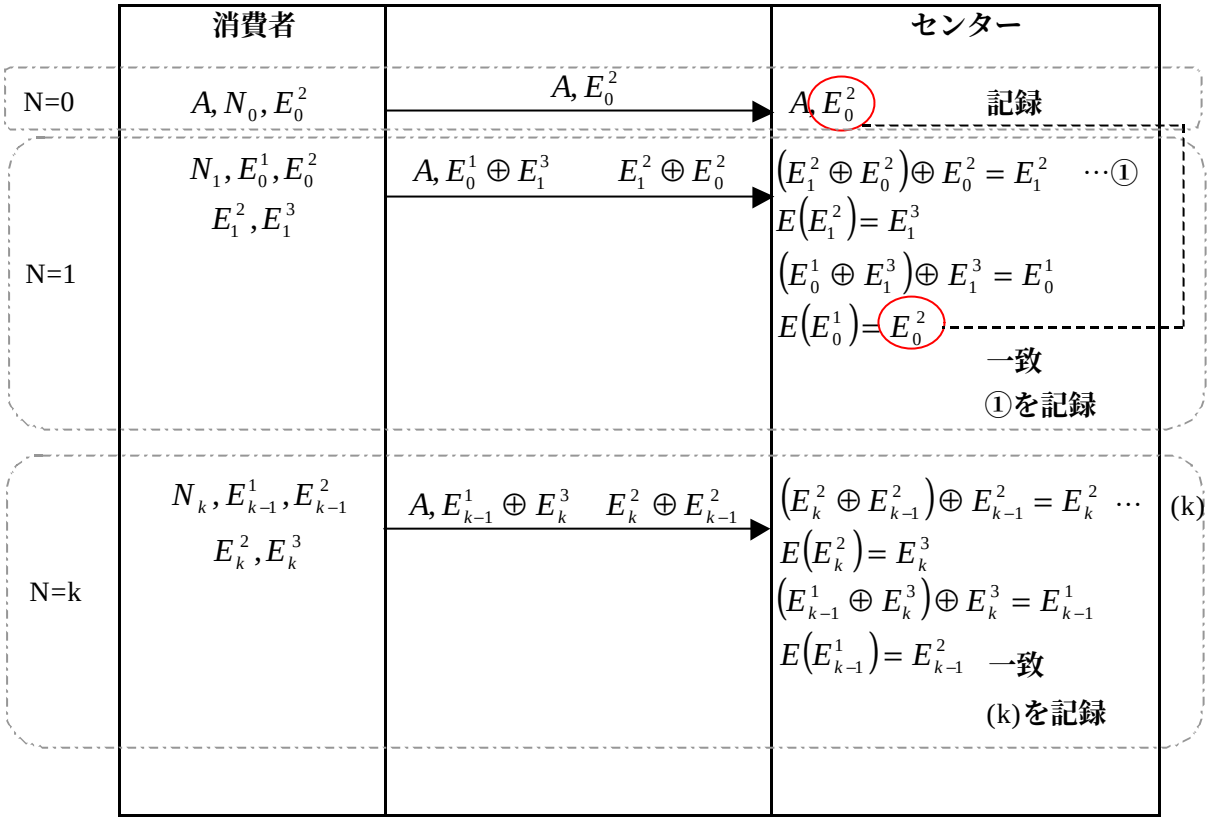


図４－２　ＳＡＳ[16]

表４－１　ワンタイムパスワードの特徴比較

	ＳＡＳ	Ｓ／ＫＥＹや ＯＰＩＥ	ＳｅｃｕｒＩＤ
シーケンス番号	不要	要（MAX9999）	―
計算回数	６４ビットを ５回もしくは３回	６４ビットを シーケンス番号と 同じ回数	―
設定のリセット	不要	要 （シーケンス番号を 使い切ると必要）	―
専用端末	不要	不要	要

（２）暗号技術の適用(4) (6) (10) (13) (14)

暗号化はアルゴリズムと鍵を用いて行う。その代表的なものが「共通鍵暗号方式」と「公開鍵暗号方式」である。

共通鍵暗号方式は、暗号化鍵E_k＝復号鍵D_k　であり、鍵を必ず秘密にしておかなければならない。この方式による代表的な暗号系として米国のＤＥＳ（Data Encryption Standard）暗号、ＮＴＴのＦＥＡＬ暗号、三菱電機のＭＩＳＴＹ暗号などがあげられる。

共通鍵暗号方式の特徴から、共通鍵暗号方式のアルゴリズムは、電子署名など原理的に公開鍵暗号でなければならない場合を除き、ほとんどすべての暗号の応用領域で利用される。

特に、大量のデータを暗号化する際は、必ず共通鍵が用いられている。不特定多数との暗号通信のように、共通鍵暗号でなく公開鍵暗号を使った方が良い場合も、通常は公開鍵を用いて共通鍵（セッション鍵）の交換を行い、データの暗号化そのものは共通鍵暗号アルゴリズムが用いられる。

キーは長いほど暗号解読に時間がかかる。現在では、６４ビット以上のキーを使用するのが一般的である。

公開鍵暗号方式は、暗号化鍵E_k≠復号鍵D_k　であり、暗号化鍵E_kは公開し、復号鍵D_kは秘密にする。共通鍵暗号方式に比べ、鍵管理面では軽減される。この公開鍵方式の代表的なものにＲＳＡ暗号、Ｅｌ Ｇａｍａｌ暗号、楕円暗号などがある。

公開鍵公式は、秘密鍵の配送がない、鍵管理が容易といったメリットはあるが、公開鍵暗号方式は、共通鍵暗号方式に比較して、暗号処理が低速である。このため、多量のデータの暗号通信には共通鍵暗号を利用し、共通鍵暗号に用いられる共通鍵の秘密配送と電子署名に公開鍵暗号を利用するのが一般的である。

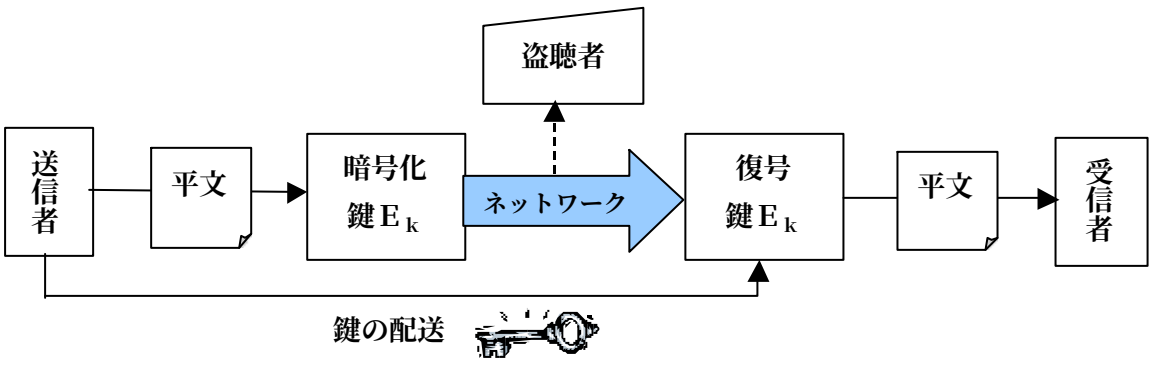


図４－３　共通鍵暗号方式

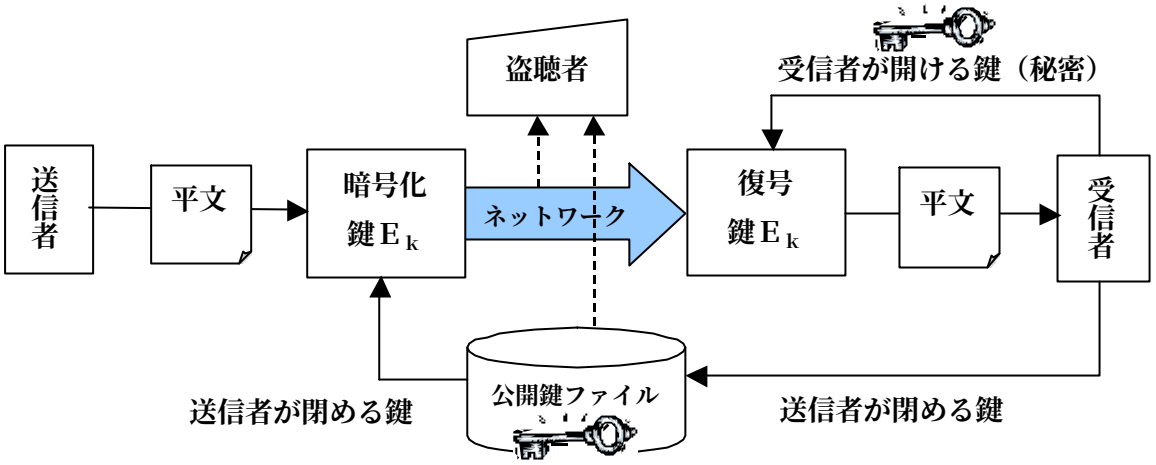


図４－４　公開鍵暗号方式

表４－２　主な共通鍵ブロック暗号方式の比較[9]

名称	キー長（bit）	ブロック長（bit）	段数	速度 ＊注記以外開発元公表速度
DES	56	64	１６	7.7Mbps(P5-90)＊1
Triple DES（２キー）	56×2 (57 相当)	64	１６×３	DES の３分の１
Triple DES（３キー）	56×3 (112 相当)	64	１６×３	DES の３分の１ 2.6Mbps(P5-90) ＊1
IDEA	128	64	8	DES の２倍 177Mbps(専用 LSI)
FEAL-*N*	64	64	N	7Mbps(P5-90)＊2 55Mbps(専用 LSI)
MISTY1 MISTY2	128	64	8＊3	20Mbps(P5-100)
MBAL	64	16-1024 byte	3	24Mbps(P5-133)
RC2	1-128 Byte	64	18	8Mbps(P5-90)
RC5	1-256 Byte	32,64,128	可変	24Mbps(P5-90)
Blowfish	32-448	64	可変	25Mbps(P5-150)
CAST	40-128	64	可変	26Mbps(P5-150) CAST-128

＊１：ＲＳＡ社製ＢＳＡＦＥツールキットによる値

＊２：ＦＥＡＬ３２の値

＊３：実際は入れ子構造の為、8(32bit)×3(16bit)×3(7.9bit)=72 段の S-box を用いる

表４－５　暗号アルゴリズムの分類と特徴の比較

		秘密鍵の配送	暗号化速度	主な用途
共通鍵暗号方式	暗号化の鍵と復号の鍵が同じか容易に類推できる暗号方式。	必要	速い	データの暗号化
公開鍵暗号方式	暗号化の鍵と復号の鍵が異なり、一方から他方への類推が実質的に不可能な暗号方式。	不要	遅い	電子捺印、鍵の配布

新システムではワンタイムパスワードによって本人認証を行うが、初期設定を安全な方法で行わねばならず、初期設定の送信時の暗号方式をどちらの方式にするか決め、鍵を定めなくてはならない。次に、消費活動時の購買情報の暗号方式と消費活動時の個人属性情報の暗号方式を決めなくてはならない。今まで確認した、暗号方式のメリットデメリットと、新システムの構成をかんがみ、「４．３　新システム実現への適用と検証」にて暗号方式や暗号鍵を何にするかについて述べる。

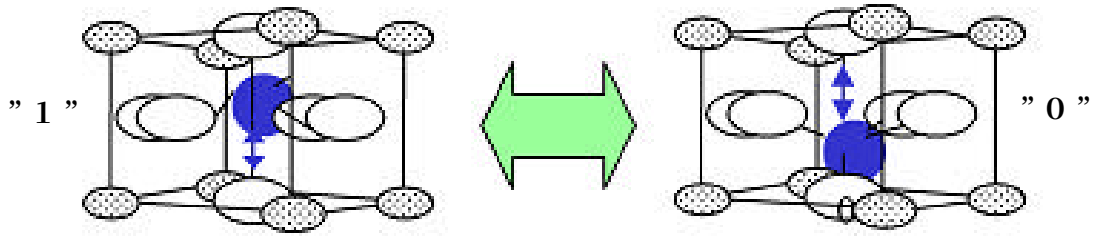
４．２　フィールド・リコンフィギュラブル・メモリ（Filed Reconfigurable Memory）内蔵携帯端末用プロセッサによるユーザー情報管理の高機能化[15] [18] [19]

第三章で優位性の明らかになったＦｅＲＡＭ（Ferroelectric Random Access Memory）の技術動向を見ていく前に、フィールド・リコンフィギュラブル・メモリ（Filed Reconfigurable Memory）、ＦｅＲＡＭの構造と原理について整理をする。

従来、ＬＳＩは記憶専門のメモリと計算専門のマイクロプロセッサに別れており、情報機器の中で機能を果たしてきていた。しかし、１９８０年代以降、電子回路の構成を変えて機能を変更できる素子が注目されるようになった。「回路を変更すること＝論理回路を変更すること」から、リコンフィギュラブル（ある形に合わせ動的に再構成できる）論理ＬＳＩと呼ぶようになった。これを小型化し、モバイル端末で使用できるようにしたのが、フィールド・リコンフィギュラブル・メモリである。リコンフィギュラブルとして、ＤＲＡＭ、ＥＥＰＲＯＭ、フラッシュメモリなども使用されるが、その性能の優位性から、ＦｅＲＡＭを用いたほうが使い勝手が良いと言われ、情報通信分野での活躍が期待される。

ＦｅＲＡＭ（Ferroelectric Random Access Memory）は、ＤＲＡＭのキャパシタ部分を強誘電体薄膜で置き換え、記憶機能を持たせたものである。強誘電体とは、例えば強チタン酸ジルコン酸鉛＝PZT(Pb(Ti,Zr)O3)などの金属有機物を加熱・酸化処理して得られた薄膜材であり、その特徴として、薄膜内に自発的な電気分極を持っているが、その分極は、電場をかけることによって電極の方向を変える性質を持っている。この性質を利用して、

薄膜にかける電場をある方向から逆方向にしていくと自発分極の反転がおこり（ヒステリシス現象)、かける電圧の正負を切り替えることにより正（ｐ）極または負（ｎ）極の電荷を薄膜表面に誘起することができる。そして、強誘電導体は自発分極をしているので、一旦反転させておけば、その状態が記憶されたままとなる。



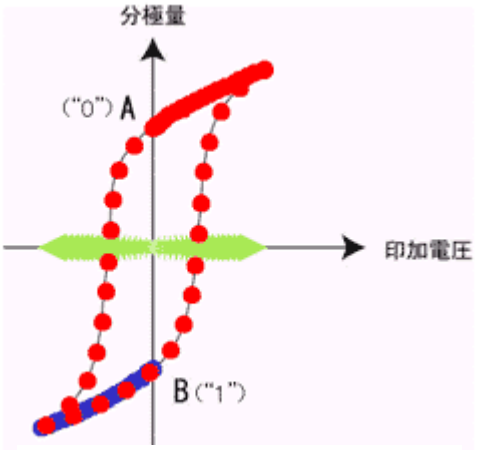


図４－６　ヒステリシス現象

ＤＲＡＭでは１メモリセルあたり１Ｔ／１Ｃ構造が一般的であったが、ＦｅＲＡＭに１Ｔ／１Ｃ構造も用いるとメモリ情報の検出レベルが約半分以下となるため、ＤＲＡＭ並みの安定動作が難しくなる欠点があった。このため、初期のＦｅＲＡＭでは２Ｔ／２Ｃ（２トランジスタ／２キャパシタ）構造であったが、この構造では必然的にセル面積が大きくなるために、大容量化し難いという欠点があった。このため、セル内に新たに基準電位の発生回路を設ける、信号ノイズを低減させるなどの技術開発されたことにより 基本的にはＤＲＡＭと同様に１つのメモリセル内に１Ｔ１Ｃ（１トランジスタ／１キャパシタ）型の構造が実現できているが、ＦｅＲＡＭではキャパシタに強誘電体を配しているため、不揮発性の特性を有する。以上がＦｅＲＡＭの構造と原理である。

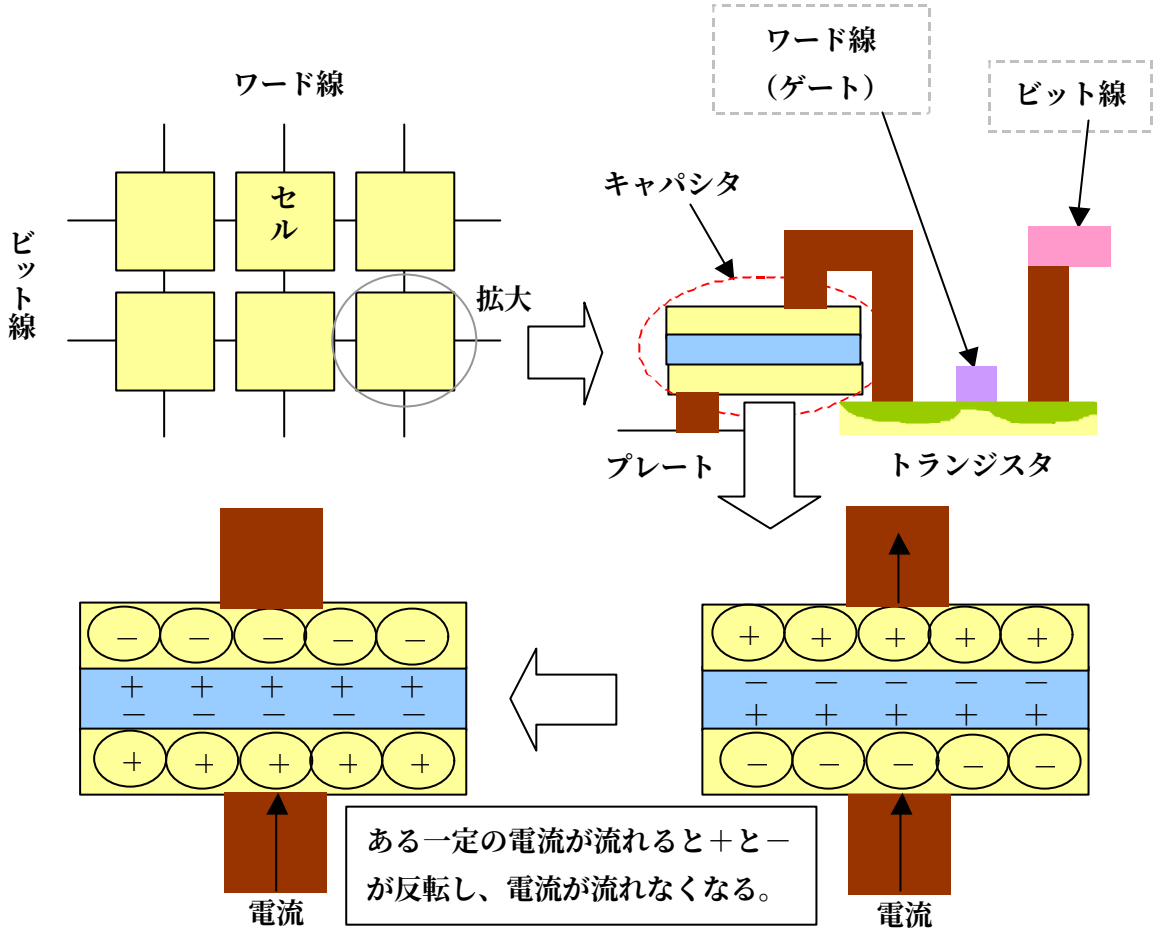


図４－７　ＦｅＲＡＭの構造

１チップは複数のセルで構成されている。セルのサイズを小さくすれば、１チップに搭載できるセル個数が多くなるため容量を上げることができる。

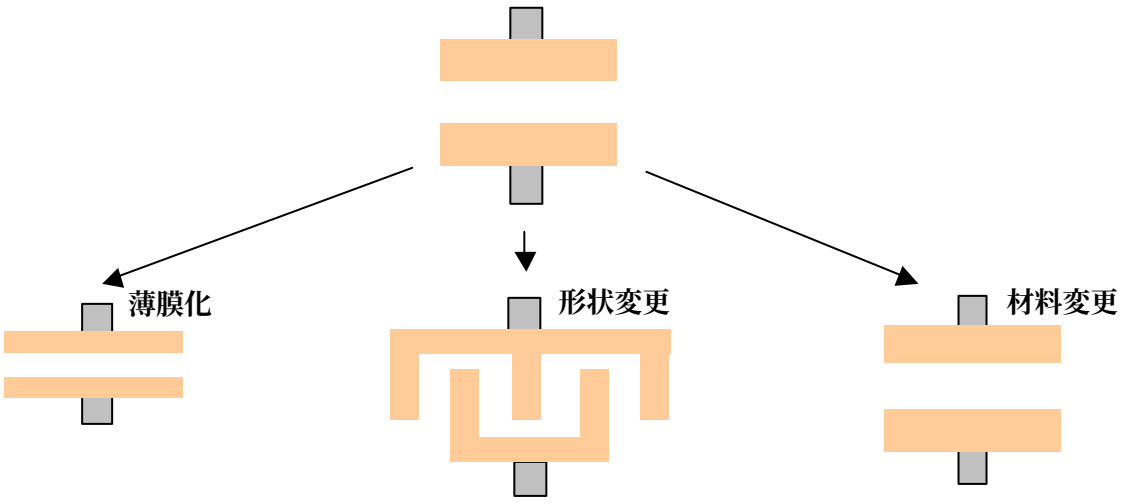


図４－８　容量値増加の手法

ＦｅＲＡＭは、基本的には現在のＤＲＡＭと同じ１Ｔ１Ｃ（１トランジスタ／１キャパシタ）型のメモリセルをとる。ＤＲＡＭが設計ルールの微細化、積層化、材料変更などによって容量値の増加を行ってきたことを考えると、ＦｅＲＡＭもまた、微細化と積層化、材料の変更により大容量化が可能である。また、積層構造化によりセル面積を小さくすることによって、ワンチップに複数のＦｅＲＡＭを搭載することができる。

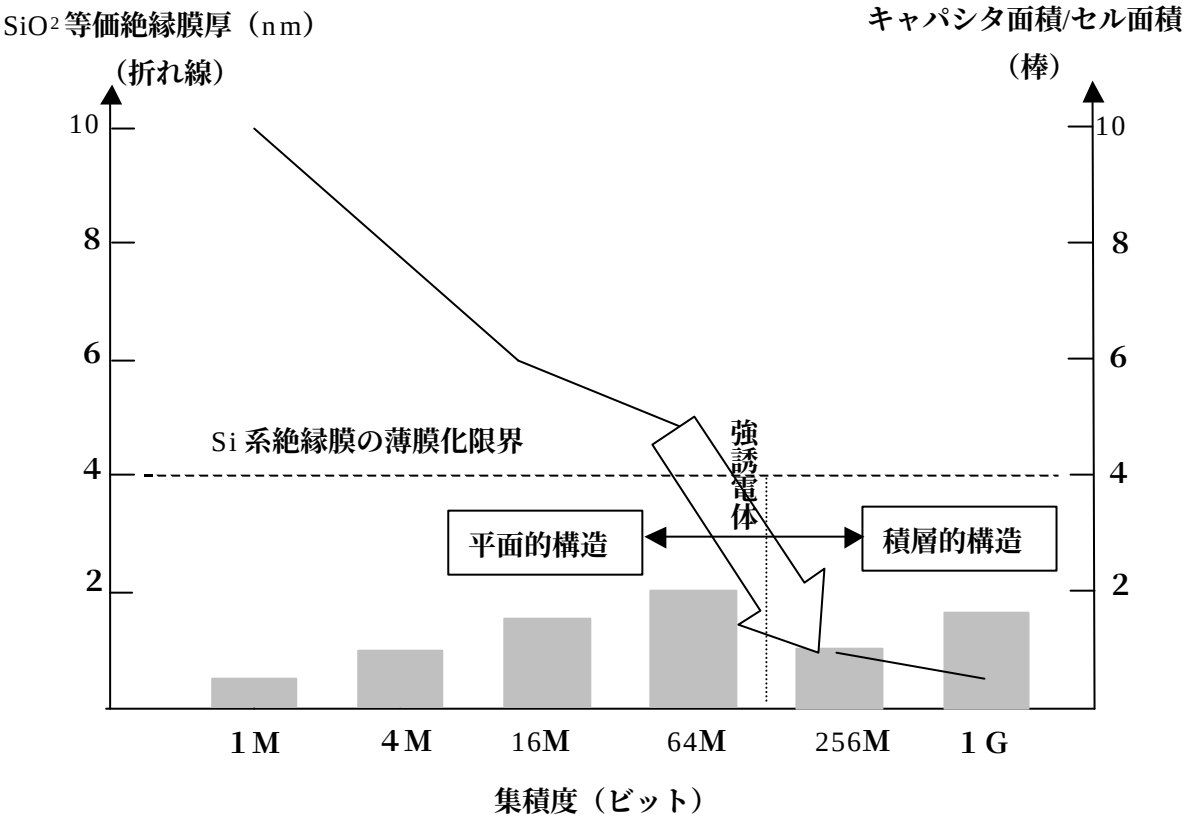


図４－９　強誘電体膜厚と集積度、キャパシタセル面積の関係

現在、ＦｅＲＡＭの主流である１Ｔ／１Ｃ型のセル情報読み出しでは、強誘電体の分極量変化に伴う分極電流を読む方式であるため、必然的にセル情報は読み出しサイクル毎に壊れる「破壊読み出し」となり、同一サイクル内での再書き込みが必要になる。「破壊読出し」の場合、読み出し途中でＩＣチップへの電源供給が切れるなどのトラブルが発生した場合、データが欠落するなどの問題が生じる可能性がある。このようなことから、「非破壊読み出し」（NDRO：Non-Destructive Read Out Memory）を実現するセル構造やセンス回路に関する研究が積極的に行われるようになった。そして、積層構造化を行うことによって、１Ｔ／１Ｃよりもメモリサイズを小さくすることができ、また、「非破壊読み出し」のため「破壊読出し」よりも高速に処理が行える技術が開発された。

表４－６　ＦｅＲＡＭテクノロジーの変遷(15)

製品	64Kビット	256Kビット	16Mビット	256Mビット	１Gビット
設計ルール	1.0μm	0.8μm	0.35μm	0.18μm	0.13μm
デザイン	２T/２C	１T/１C	１T/１C	１T/１C	１T/１C

表４－７　ＦｅＲＡＭセル面積の変遷(19)

セル面積 (μm)	設計ルール (μm^2)	容量 (μm^2)	縦横比率
1.9	0.35	1.0	0.1 - 0.2
1.0	0.25	0.5	0.35
0.5	0.18	0.25	0.8
0.3	0.13	0.1	2.5

このように、ＦｅＲＡＭは小電力で不揮発性を保つといった優れた特性を持ち、微細化、非破壊読み出しの技術の進展により、大容量も実現しつつある。今後、現在使用されているオンチップ、オフチップでの様々なメモリと置き換えられていくことは自明である。

４．３　新システム実現への提案と検証(20)

（１）暗号技術の適用

①　初期設定時の暗号方式

ワンタイムパスワードの初期設定情報は必ず安全に送信されなければならない。初期設定時には、消費者自ら暗証番号の設定を行う必要があるため、街角専用端末を用いる。街角専用端末に公開鍵ファイルを入れておき、初期設定情報を安全に暗号化しセンターへ送信する。

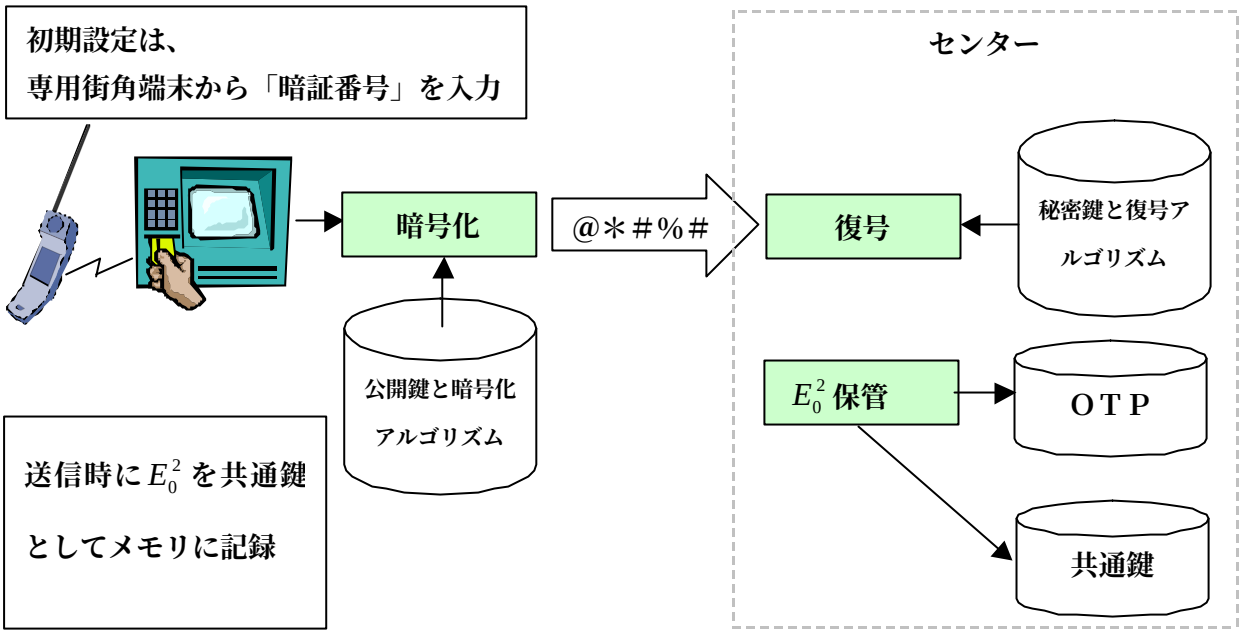


図４－１０　初期設定処理

②　購買情報の暗号方式

メモリに記録する購買情報の暗号方式は、E_0^2を使った共通鍵方式とする。

ＰＯＳ端末において「店舗－センター」単位で管理する共通鍵方式で暗号化し、暗号化した購買情報をセンターに送信する。センターはその情報を保管すると共に、それを一旦復号し、消費者毎に共通鍵として管理しているE_0^2でもう一度暗号化し、店舗のＰＯＳ端末経由で消費者のメモリに送信する。復号も個人認証後、E_0^2を使い行う。

③　金融機関情報のセキュリティ

個人属性情報内の金融機関情報は、購買情報よりもセキュリティを高くしなければならない。購買情報は毎回同じ共通鍵のE_0^2で暗号化するが、個人属性情報は金融機関などの任意の場所で暗号化したものをメモリにあらかじめ記録することとする。その暗号方式をセンターは知らない。そして、店舗（企業）と金融機関が直接に通信を行うものとする。

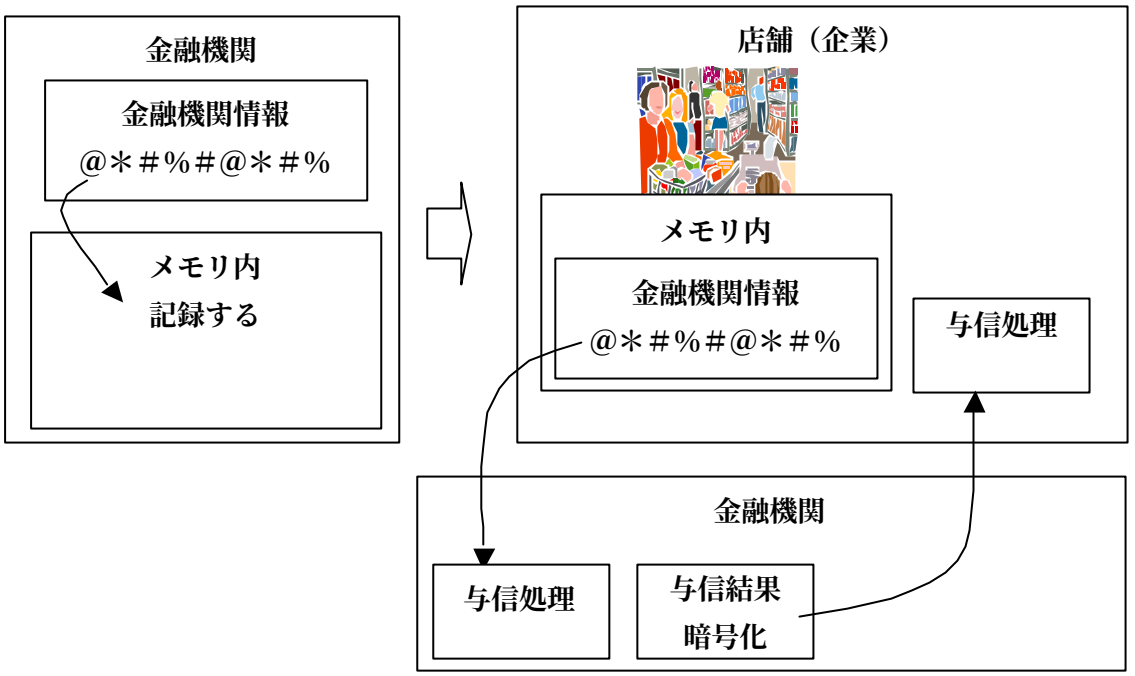


図４－１１　金融機関情報のセキュリティ

（２）ＩＣカードへ非破壊読み出しＦｅＲＡＭ搭載

ワンタイムパスワードの使用のためには、毎回、書替え可能なメモリが記録媒体に搭載されている必要がある。また、消費活動の場に欠かせない財布とともに、必ず携帯できる大きさである必要がある。バッテリー不要のＦｅＲＡＭ搭載のＩＴ機器として携帯電話やＰＤＡなどが現時点では考えられるが、高齢者層での利用者が少ない、財布に入る大きさではないなどの課題がある。そこで普及しつつあるＩＣカードに最も使用されているＥＥＰＲＯＭの代わりに非破壊読み出しＦｅＲＡＭをＩＣカードに搭載することを提案し、筆者の提案する本システムの最も基本的な特徴としたい(23)。

ＥＥＰＲＯＭは内部書込電圧が１２Ｖ、書き換え可能回数が10^4のため、ワンタイムパスワード方式の毎回書替え要求に応えることができないが、非破壊読み出しＦｅＲＡＭは内部書込電圧が２Ｖと低く、書き換え可能回数が10^{13}のためワンタイムパスワード方式のハード要件を十分満たしている。

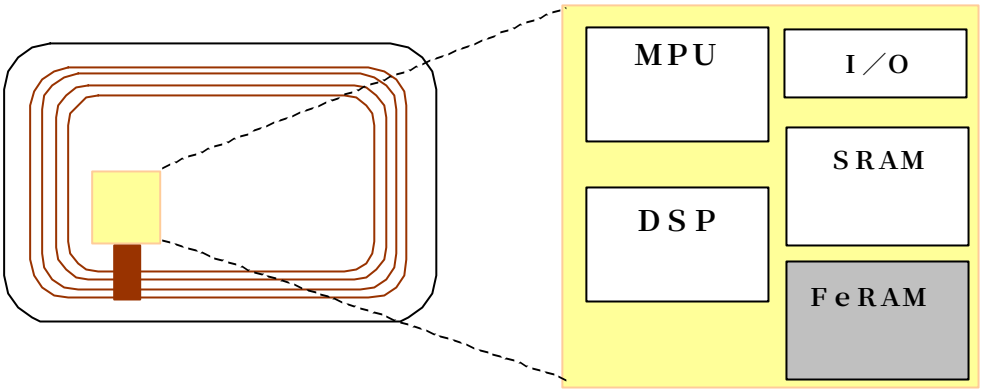


図４－１２　ＩＣカードへ非破壊読み出しＦｅＲＡＭ搭載

また、破壊読出しのように電源遮断などのトラブル時に発生する可能性のあったデータ欠落などがなくなり、ユーザーの情報管理の高機能化が安定的に行える高い安定性から非破壊読み出しＦｅＲＡＭが適している。

（３）通信速度の検証

インターネット通信インフラとして使うことを前提としている。そこで、ＰＯＳ端末・店舗（企業）とセンター間、街角端末とセンター間における通信速度を検証する。各ＰＣやサーバーでの処理時間はＣＰＵやその他マシンの状態によって異なるため、計算対象としない。また、通信速度もルーターなどの周辺機器の性能にも左右される。

前提　：　通信インフラをＩＳＤＮ６４Ｋ(bps)
①　認証　　認証データ　：６４ビット　⇒　８バイト　⇒　往復：０．００２秒
②　店舗からセンターへ送信
　　購買情報データ　：約１Ｋバイト　･･･　０．１２５秒　⇒　往復：０．２５秒
　　∴　①＋②＝０．２５２秒
③　書き込み　７５ns　×　１Ｋバイト　＝７５×１０$^{-6}$　秒（一瞬である）
１０台のＰＯＳ端末から全く同時にトランザクションが発生した場合も通信速度は約３秒程度である。よって、日商約１０００万円の大型小売店であってもＩＳＤＮ６４Ｋの回線が１本あれば、十分に処理は行える。扱うデータがテキストであるため、現通信技術でも十分実用性のあるスピードが確保できることが明らかである。また、ブロードバンド化の普及が飛躍的に伸びていることを付記しておく。

このため、ＩＣカードのメモリに購買情報を記録せずに、購買情報をセンターに送信し保管する方が、データ記録容量面でも制限がなくまたバックアップを常にとっておけるため、実質的である。

第五章　新システムを用いたビジネスの提案

５．１　ビジネスモデル

第三章、第四章において、個人消費活動を情報流通システムの中に入れる新たなシステムの提案を行い具現化の技術的ブレークスルーについてみた。ここでは、この新システムを用いた新たなビジネスの提案を行う。

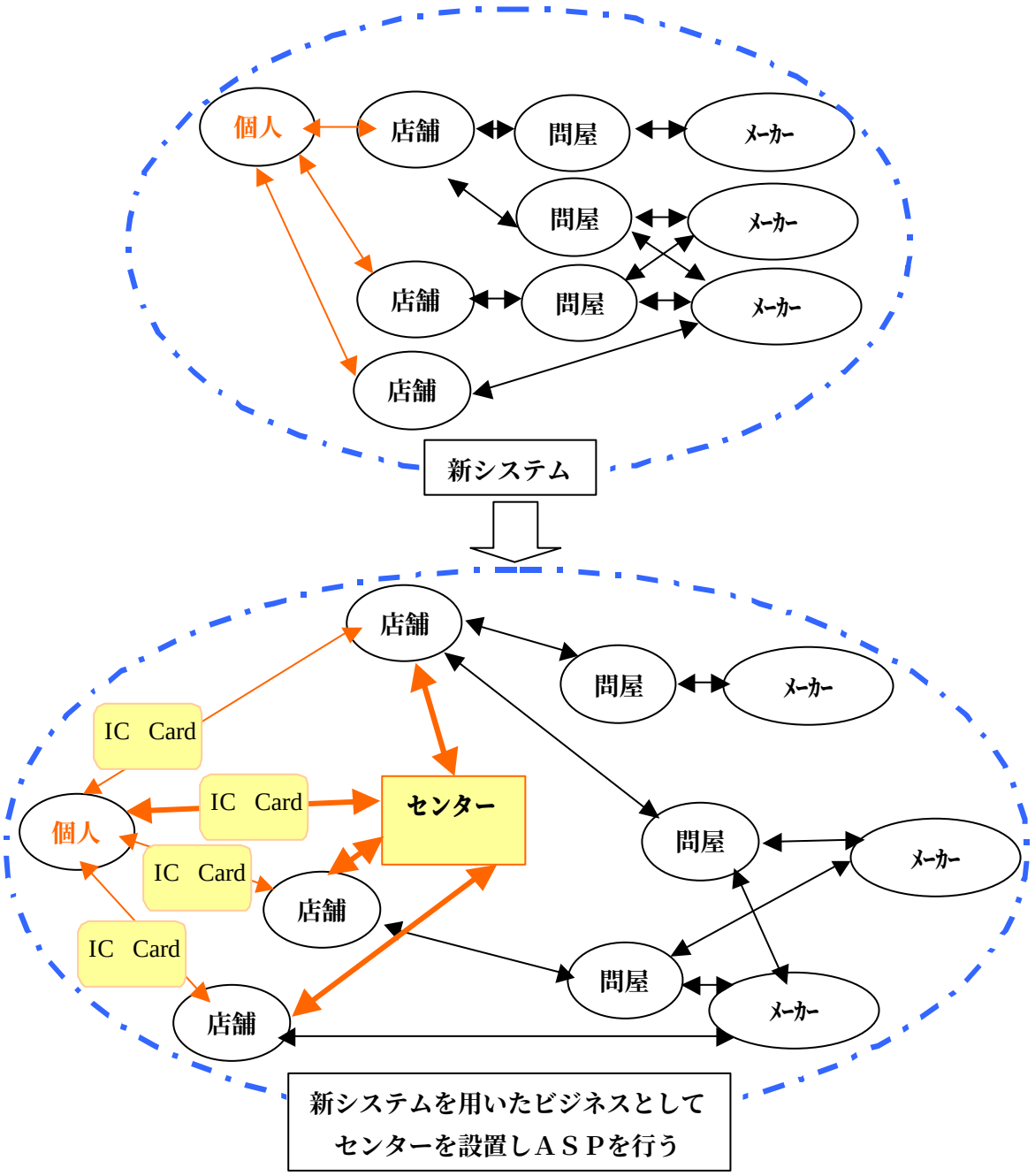


図５－１　新システムを用いた新たなビジネス概念図

（１）事業の名称

販売情報管理システムのＡＳＰ（Application Service Provider）事業および購買情報集計分析サービス

（２）事業の概要

①　製品・サービス概要

《消費者に対して》
（Ａ）消費活動情報自動集計・分析サービス
《店舗に対して》
（Ｂ）販売情報管理システムのＡＳＰ

このシステムによって、

- **消費者　･･･　面倒な家計簿作成をしなくとも、正確な情報で家計管理を行うことができる。時間の節約にもつながり、多忙な人には利便性が高い。**
- **店舗もしくは企業･･･　少ないシステム投資でＰＯＳシステムを初めとする販売管理システムを手に入れることができると共に、自社内だけでは分からない他者との比較などの統計データも手に入れることができる。**

（Ａ）消費活動情報自動集計・分析サービス　について

（ア）製品・サービスの構成

ＩＣカード　＋　消費活動情報の集計・分析　＋　アドバイザーの紹介

（イ）サービス概要

消費者がＩＣカードを使用するだけで消費活動情報の集計・分析が自動的に行うサービス。消費者は、家計簿記載の手間や時間がかからず、有効に時間を使うことができる。また、記入ミス、入力ミスがなく、正確にマネーフローを把握することができる。システムでフォローを行う以外の消費活動情報は、ＰＣ利用者は自ら入力ができるが、入力フォーマットをソフトで用意しているため入力が容易である。

集計結果や分析結果について、消費者が希望すればアドバイスを専門家から受けることができる。

消費活動情報の集計・分析には以下の２つのサービスを用意する。

- ＰＣで専用ソフトをダウンロードすることによって自分で集計・分析できる
- ＰＣか使えない場合も街角端末で集計・分析の指示ができる

購買情報は商品単位であるが、一定の期間で費目などの一定のグループで集計する。多種多様な家計簿があるが、当システムでは、客観的なデータとの比較、分析が行い易いことを考慮し、総務庁「家計調査」の費目分類に順じて費目を定める。表５－１の項目には、「光熱費・水道代」や「保健医療」もあるが、小売店だけでなく広範な意味での消費活動が行われる場所に当システムを導入することによってフォローする。「家賃地代」や「光熱費・水道代」、「通信」のように銀行口座やクレジット会社から自動的に支払いがされるものも少なくない。この場合は金融機関との提携によって順次取り込んでいく。

具体的なサービスメニューは以下のとおり。

- 詳細データ印刷　…　購買情報の時系列リストを出す。
- 月次集計表作成　…　「○日〆」と〆日を指定できる。指定日から１ヶ月遡って集計と比率を計算する。
- 年次集計表作成　…　「◇月◇日〆」と〆月日を指定できる。指定日から一年遡って集計と比率を計算する。
- 推移表作成　…　月もしくは３年間の集計数字の推移表を作成する。
- 調査データとの比較表作成　…　総務庁「家計調査」や貯蓄広報委員会「貯蓄と家計に関する世論調査」、総理府「国民生活に関する世論調査」など調査されたデータと比較し、該当消費者のポジションがどこにあるかをわかるようにする。

  総務庁の家計調査調査では、県別、世帯内容（単身、勤労、農業など）に統計数値がある。単に費目単位の比較ではなく、消費者の居住地域、世帯構造などに細分した比較を行い、目安となるようにする。

  当システム内において希望者のデータ蓄積が一定できた段階で、システム内部においてもデータ分析を行い、比較ができるようにする。

消費者が簡単に街角端末（プリンター付き）や専用ソフトから、これらのメニューを手順に従って選択していくだけで、メニューに示す表を作成する。街角端末を設置することによって、パソコンを扱うことが出来ない消費者も集計・分析表を手に入れることができる。

表５－１　支出費目分類

費目	項目	費目	項目
食料	穀類	被服及び履物	和服
	魚介類		洋服
	肉類		シャツ・セーター
	乳卵類		下着類
	野菜・海草		生地・糸類
	果物		他の被服
	油脂・調味料		履物類
	菓子類		被服関連サービス
	調理食品	保険医療	医薬品
	飲料		健康維持用摂取品
	酒類		保健医療用品・器具
	外食		保健・医療サービス
住居	家賃地代	交通通信	交通
	設備・修繕維持		自動車等関係費
光熱・水道代	光熱		通信
	電気代	教育	
	ガス代	教養娯楽	教養娯楽用耐久財
	他の光熱費		教養娯楽用品
	上下水道料		書籍・他の印刷物
家具・家事用品	家庭用耐久財		教養娯楽サービス
	室内装飾・装飾品	その他の消費支出	諸雑費
	寝具類		こづかい（使途不明）
	家事雑貨		交際費
	家事用消耗品		仕送り金
	家事サービス	以上	以上

図５－２　サービスアウトプットイメージ

■　明細データ印刷

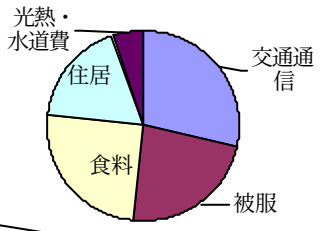
例）1 月・2002 年　明細表

購買日	品目	金額	費目	店舗名
2002.01.05	牛乳	198	食料	○○スーパー
2002.01.05	牛肉（200ｇ）	750	食料	○○スーパー
2002.01.06	食パン	205	食料	△△マート
2002.01.07	セーター	10,000	被服	□□百貨店
：	書籍	2,000	教養・娯楽	□□百貨店
：	：	：	：	：

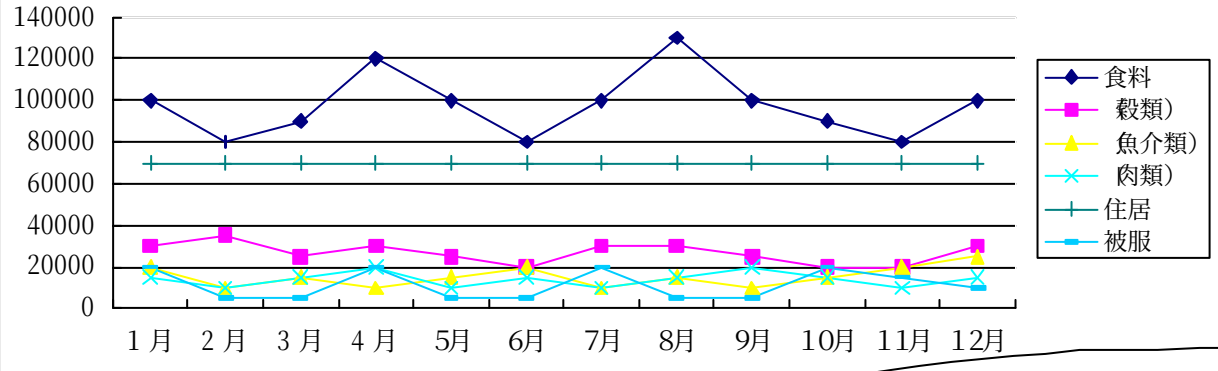
■　月次集計表作成・年次集計表作成

例）1 月・2002 年　集計表

費目	金額	支出に占める割合	対前月比	対前年同月比
食料	100,000	33 %	+5 %	+8 %
住居	70,000	23 %	+0 %	+0 %
光熱・水道費	20,000	7 %	-3 %	+2 %
：		XX %	+X %	+X %
：		XX %	-X %	-X %



■　推移表作成



（B）販売情報管理システムのＡＳＰ　について

（ア）製品・サービスの構成

ＰＯＳシステムや販売管理システムのＡＳＰサービス　＋　情報の分析　＋　コンサルティング

（イ）サービス概要

現在、各企業や店舗単位でシステム構築しているＰＯＳシステムや販売管理システムのＡＳＰサービス。各企業や店舗にはＰＯＳ端末、ＩＣカード Reader/Writer など必要最低限の情報機器を用意し通信回線でセンターとつなぎ、センターのシステムやデータベースを使う。希望企業、店舗から解析情報の提供をうけ、一店舗だけでなく複数店舗の分析を行い、企業や店舗に提供する。

② 製品・サービス価格

製品名		価格
ＩＣカード発行手数料（１枚）		５００円
年会費（１枚）		５，０００円
ＰＯＳ端末リース料金（１台・月）		３０，０００円
ＩＣカード Reader/Writer リース料金（１台・月）		５，０００円
日商：１０００万円以上	ＡＳＰ利用初期導入費	２，５００，０００円
	ＡＳＰ利用料金（年額）	１５，０００，０００円
日商：５００万円以上	ＡＳＰ利用初期導入費	１，５００，０００円
	ＡＳＰ利用料金（年額）	９，０００，０００円
日商：２５０万円以上	ＡＳＰ利用初期導入費	１，０００，０００円
	ＡＳＰ利用料金（年額）	６，０００，０００円
日商：１００万円以上	ＡＳＰ利用初期導入費	５００，０００円
	ＡＳＰ利用料金（年額）	３，０００，０００円
日商：１００万円未満	ＡＳＰ利用初期導入費	２５０，０００円
	ＡＳＰ利用料金（年額）	１，５００，０００円

③　現状と当システム導入後

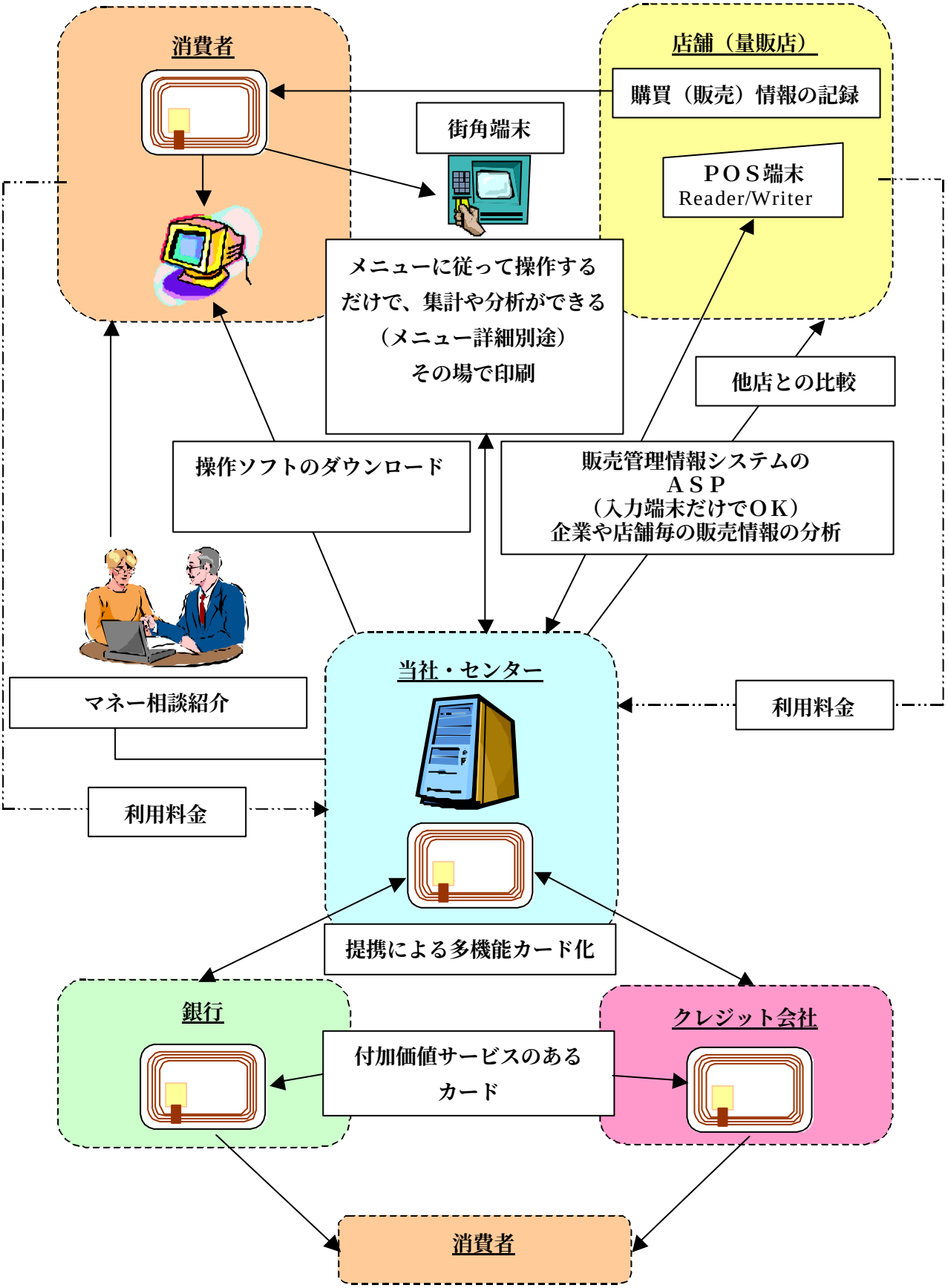
現状		当システム導入後
消費者	家計簿をつけないために家計管理ができない	ＩＣカードに購買情報の記録を行うだけ
	家計簿をつけるのに時間がかかる	必要ない
	家計簿をつけていても分析できない	必要ない
企業（店舗）	ＰＯＳシステムや販売管理システムの構築に資金がかかる	低コストでシステム構築ができる
	機器の入れ替えが困難	リースの為機器は最新のものに変更可能
	システム保守要員のコストがかかる	当社センターで行うため必要ない
	販売データの十分な分析ができていない	多様な視点で分析可能

④　ビジネスモデル

当社は、ＰＯＳシステム・販売管理システムに関するのＡＳＰおよびその付帯サービス（情報の分析・コンサルティングなど）に関する契約を消費者の購買活動に関係する店舗（企業）と結び、その利用料を日商金額に応じて受け取る。また、ＩＣカード Reader/Writer やＰＯＳ端末を初めとするＰＯＳシステムや販売管理システムで使用する情報端末のリースもしくはレンタルを行う。

消費者は、ＡＳＰサービス契約店舗や情報機器リース・レンタル店舗（企業）で使用でき、購買情報を自ら処理・編集・加工できるＩＣカードの利用契約を当社と結び、ＩＣカード年会費を支払う。契約消費者は購買情報の処理・編集・加工のための操作ソフトを当社サーバーから無料でダウンロードし使用することができる。また、ＰＣ操作などのできない人たちは、街角端末を使用し、事前に用意されているメニューに従って操作を行うだけで、購買情報の記録、編集や分析を行った資料を手にすることができる。これらのサービス料金は全てＩＣカードの年会費に含まれており、別途、料金を徴収しない。これらに加え、契約消費者に対して購買記録や分析資料を元に、マネー相談の専門家を紹介する。専門家への支払いは別途生じるが、消費者は積極的に資産管理や運用についての情報を得、活動を行うことができる。

ＩＣカードは単に購買情報の記録の為にもちいるのではなく、銀行やクレジット会社といった金融機関と提携を行い、多機能ＩＣカードとして利用ができる。購買情報は金融機関から直接引き落とされているケースが少なくないため、金融機関との提携によって、より正確な購買情報の把握、分析を行うことができる。


消費者
店舗（量販店）
購買（販売）情報の記録
街角端末
ＰＯＳ端末
Reader/Writer
メニューに従って操作する
だけで、集計や分析ができる
（メニュー詳細別途）
その場で印刷
他店との比較
操作ソフトのダウンロード
販売管理情報システムの
ＡＳＰ
（入力端末だけでＯＫ）
企業や店舗毎の販売情報の分析
当社・センター
マネー相談紹介
利用料金
利用料金
提携による多機能カード化
銀行
クレジット会社
付加価値サービスのある
カード
消費者

５．２　市場と戦略

（１）市場

①　ターゲット（顧客）

《消費者》　…　全勤労者

《店　舗》　…　最終的には全消費活動の場においてＩＣカードが使用できるよう、ＩＣカード Reader/Writer　を設置するが、まず、最も消費活動が盛んに行われる大型小売店（量販店）をターゲットとする。

②　ターゲット（顧客）分析

《消費者》

アンケート結果（詳細は付録参照）を元に、ターゲット（顧客）分析を行う。
現在、家計簿を「つけている」人は２５．８％であり、つけていない理由は、「必要がない」が４１．３％、「面倒でできない（つけ始めても長続きしない）が３４．７％、「時間がない」が１３．２％となっている。

家計簿をつけている人と「仕事や家事、通勤などの時間以外で自由に使える時間」との関係を見てみると、１週間に１０時間以上自由時間がある人が家計簿をつけている割合が高いことが分かる。

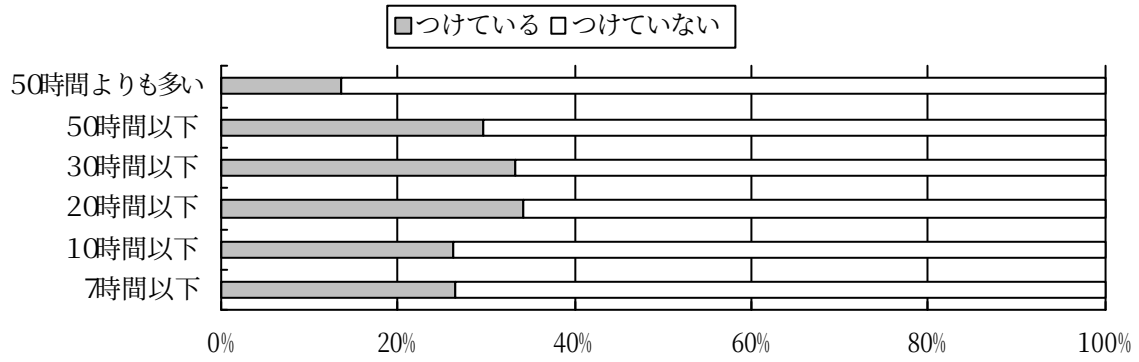


図５－１　家計簿記帳と自由時間の関係

家計簿をつけている人のうち、１日の家計簿に係わる時間は、３０分までが最も多く、５０．０％であるが、１時間までの人も３１．０％いる。１週間の仕事や家事、通勤などの時間以外で自由に使える時間が１０時間以下の人は全体の２６．４％で、自由時間がほとんどない人が多い。「家計簿をつける時間がない」と答えた人の３分の２が、１週間に自由に使える時間が１０時間以下である。よって、自由時間の少ない勤労世帯は当システム

の主要なターゲットと考える。

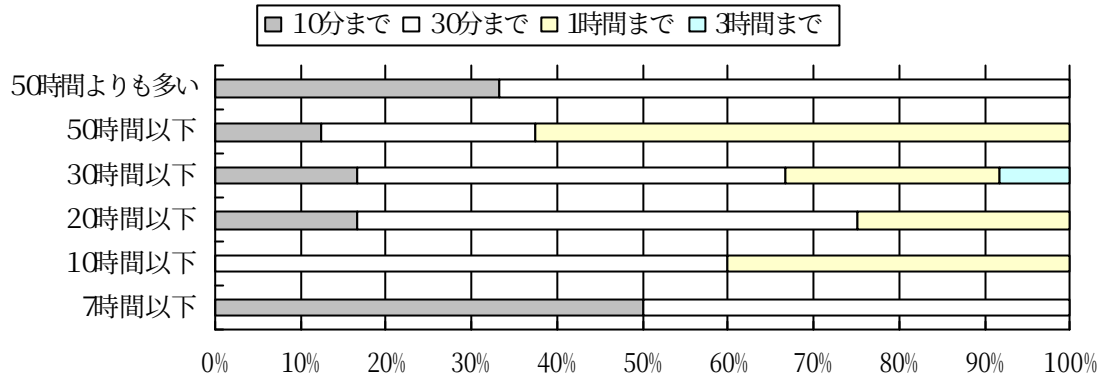


図５－２　仕事や家事、通勤などの時間以外で自由に使える時間（１週間）と家計簿に係わる時間（１日）の関係

家計簿記載単位は、「費目単位」が最も多く６６．７%、「細目単位」が１６．７%、「店舗単位の合計金額」が１６．７%となっており、「店舗単位の合計金額」で記載している人の４２．９%が、もう「少し細かな単位で記載したい」と思っているが、「費目単位」で記載している人の７１．４%は、現在の記載内容で満足している。よって、当システム行う集計は費目単位で行うこととした。

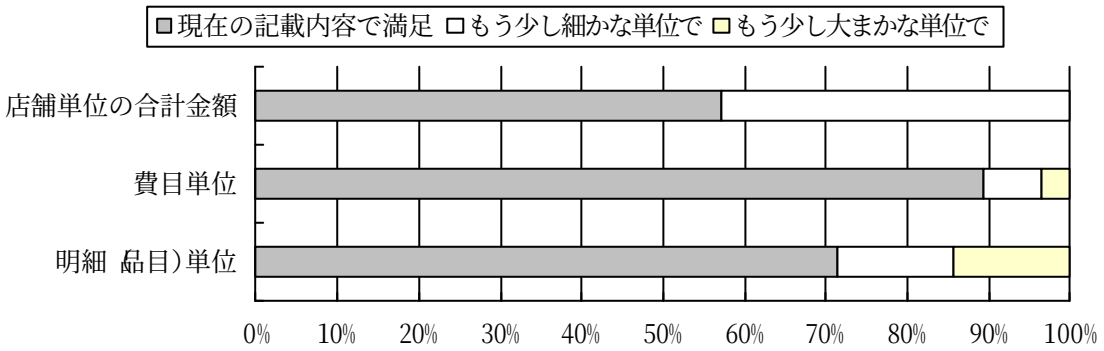


図５－３　家計簿記載単位と希望記載単位の関係

家計簿をつけている人のうち、「集計も分析も行っている」人は１９．０%にすぎず、「集計だけを行っている」人が５７．１%、つけているだけで、「集計や分析をおこなっていない」人が２１．４%であり、約８割の人が、記載している情報を家計管理に生かせていない。そして、買い物情報から自動で家計簿を作成する仕組みを利用するかといった質問について、「利用したい」、「是非、利用したい」の合計は３９．６%である。

以上のことから、消費者の約４～６割に当システムの潜在的ニーズがあるものと考える。

《店　舗》

自社システム構築の場合、構築コストがかかる上、システムのハード、ソフト共に減価償却の対象となるため、財務諸表に与える影響が大きい。メーカー系などの流通業では、販売管理や在庫管理システムをアウトソーシングで構築し、保守まで任せているところもある。通信速度が速くなり、高いセキュリティ確保がなされれば、自社内システム構築から、アウトソースや標準的ソフトの若干のカスタマイズによるＡＳＰ、ＢＳＰなどを利用するようになる。

また、通信回線のブロードバンド化により、データ通信速度に問題があったがために社内に構築していたシステムを外部に出すことができるようになった。また、高いセキュリティ技術により、外部にデータを出すことの不安が少なくなってきている。加えて、単独の企業内だけで情報を保有し、分析するだけでは、業界や周辺業界の動きに対応しきれなくなってきており、企業や業界の枠を超えて市場分析を行う必要がでてきている。

自社開発のＰＯＳシステムや販売管理システムに比較し、新しい機器への対応が早く、システム構築期間が短く、また、コストを損金処理できるため、財務上のメリットが大きい。

また、インハウスカードの発行コスト、維持コストも大きいため、当システムの利用によって、現在以上の情報入手、分析が行えればメリットは大きく、ニーズはあると考える。

③　市場規模

《消費者市場規模》　･･･　９２０億円／年　市場

平成１２年の国勢調査によると全国の世帯数は４６３８万世帯であり、一般世帯人員は1億２４８２万人である。②の市場分析結果から、一般世帯の４割を潜在市場規模と見る。　⇒　約１８５５万人

ＩＣカード発行手数料　･･･　５００円　×　１８５５万人　＝　　９２億円
ＩＣカード年会費　･･･　　５０００円　×　１８５５万人　＝　９２０億円

《店舗市場規模》　･･･　４５０億円／年　市場

日商１０００万円以上の大型小売店は、全国で約３０００店舗。日商金額の小さな小売店数が把握できないため、この数値を使用。リース料金は考慮しない。

初期導入コスト　･･･　２５０万円　×　３０００店舗　＝　７５億円
ＡＳＰ利用料　･･･　１５００万円　×　３０００店舗　＝　４５０億円／年

④　参入障壁

低い。ＰＯＳシステムや販売管理システムの開発を既に行っているシステムベンダーはＡＳＰサービスの展開が行い易く、ノウハウの蓄積がある。販売管理のシステムアウトソーシングによる開発、保守は既に行っている企業もある。

既にクレジットカードは一部ＩＣカード化されているが、店舗に設置されているＩＣカード Reader/Writer と入出力インターフェイスが異なるため、機器の共有ができない。このため、店舗側に新たなＩＣカード Reader/Writer を設置することを嫌がられる可能性がないとは言えない。

（２）戦略

（Ａ）量販店のインハウスカードと提携しプロトタイプ作成

アンケート結果（詳細は付録参照）によると、日常的な買い物を行う量販店が、「決まっている」が２２．７%、「だいたい決まっている」が６９．３%で、９２．０%の人が、ほぼ決まった量販店で買い物をしており、７５%程度の人が３店舗以内の固定的な量販店で買い物をしている。

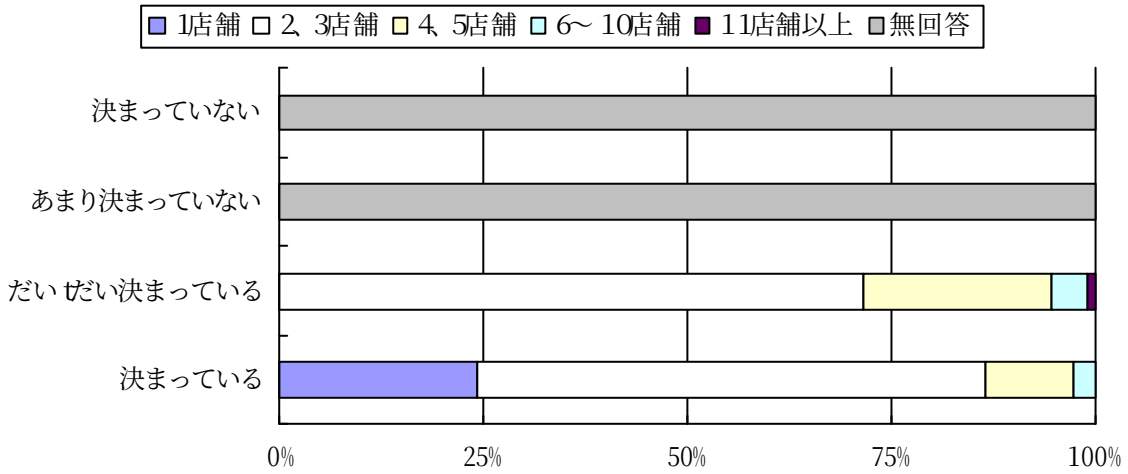


図５－４　日常的に買い物をしている量販店とその店舗数の関係

回答者の居住地と最も良く行く店の関係を見ると、どの地域も、自宅と会社の通勤路が少なく、自宅から４キロ以内の店で固定的に買い物をしている。

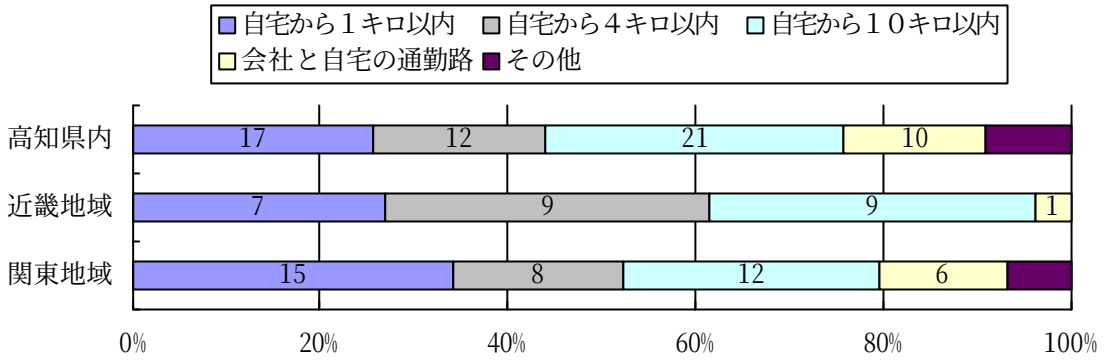


図５－５　回答者の居住地と良く行く店の場所の関係

以上のことから、中小規模の都市で多くの店舗を展開する量販店がある地域を選び、量販店のインハウスカード（会員ポイントカード）と提携する。

現金決済中心の人が８２．２％と多く、また、量販店の会員カードは「現金決済のみ」が４６．０％と最も多いため、まず、現金決済のみで使用できるプロトタイプを作成する。その後、地域銀行やクレジット会社と提携し、キャッシュレス決済ができるようにする。

（B）財務諸表改善

自前でＰＯＳシステムや販売管理システムを構築する場合、一時的にシステム構築コストがかさむ上にメンテナンスコストも必要であるが、機器のリースとＡＳＰの組み合わせであるため、損金処理ができる上に必要資金の平準化ができ、財務諸表の改善につながることをアピールする。

（C）ソフトパッケージソフトのカスタマイズと独自データベースによる分析

ＰＯＳシステム、販売管理システムは既存のパッケージソフトを基本とし、当システムの独自サービスをカスタマイズする。

当システムの独自性は、店舗や消費者に提供するデータ分析結果にある。また、政府の調査結果と共に、消費者の購買情報を蓄積しデータベースを作成すること、それらに専門家の分析を加味することによって、データ分析を深く、広く行う。

（D）機器リースのみから開始し消費者指示を獲得

既に稼動しているＰＯＳシステムや販売管理システムがあるので、ＡＳＰを利用しない店舗に対しては、ＩＣカード Reader/Writer のリースのみを行い、まずは消費者の利便性を高め、指示を獲得する。

（3）マイルストーン

① プロトタイプシステム構築および実証実験　　２００２年４～１２月
　実験用ＩＣカード　･･･　５０００枚
　実証実験店舗数　･･･　３店舗（Reader/Writer 設置のみ･･･５台）
② サーバー導入標準パッケージソフトの選定、カスタマイズ
　　２００２年７～９月
③ プロトタイプシステムの評価及び修正　　２００２年１０月～２００３年３月
④ サーバー内システムの本格的構築　　２００２年１０月～
⑤ 本格始動　　２００３年　１月～

２００２年				２００３年				２００４年				２００５年			
	①														
		②													
			③												
			④												
			⑤												

（4）必要資金

単位：千円

２００２年	２００３年	２００４年	２００５年	２００６年
４０，２００	４４，８８０	９０，１６６	１７４，７５９	３４０，１５６

（5）売上金額

単位：千円

２００２年	２００３年	２００４年	２００５年	２００６年
０	３４，０００	９３，５５０	１８０，１００	３９７，４５０

（6）キャッシュフロー計画

単位：千円

年	2002年	2003年	2004年	2005年	2006年
売上合計	0	34，000	93，550	180，100	397，450
直接経費合計	35，200	38，280	80，716	156，470	299，601
間接経費合計	5，000	6，600	9，450	18，289	40，555
費用合計	40，200	44，880	90，166	174，759	340，156
利益	－40，200	－10，880	3，384	5，341	57，294
グロスキャッシュフロー（税引前）	－40，200	－51，080	－47，696	－42，355	14，939
ネットキャッシュフロー（税引後）	－40，200	－51，080	－49，388	－46，718	－18，070

初年度は、システム構築や実証実験のため、売上はなく費用のみかかる。

税引き前では３年目に単年度黒字となり、グロスキャッシュフローの赤字は５年目で消え、ネットのキャッシュフローも６年目で黒字になる計画とする。

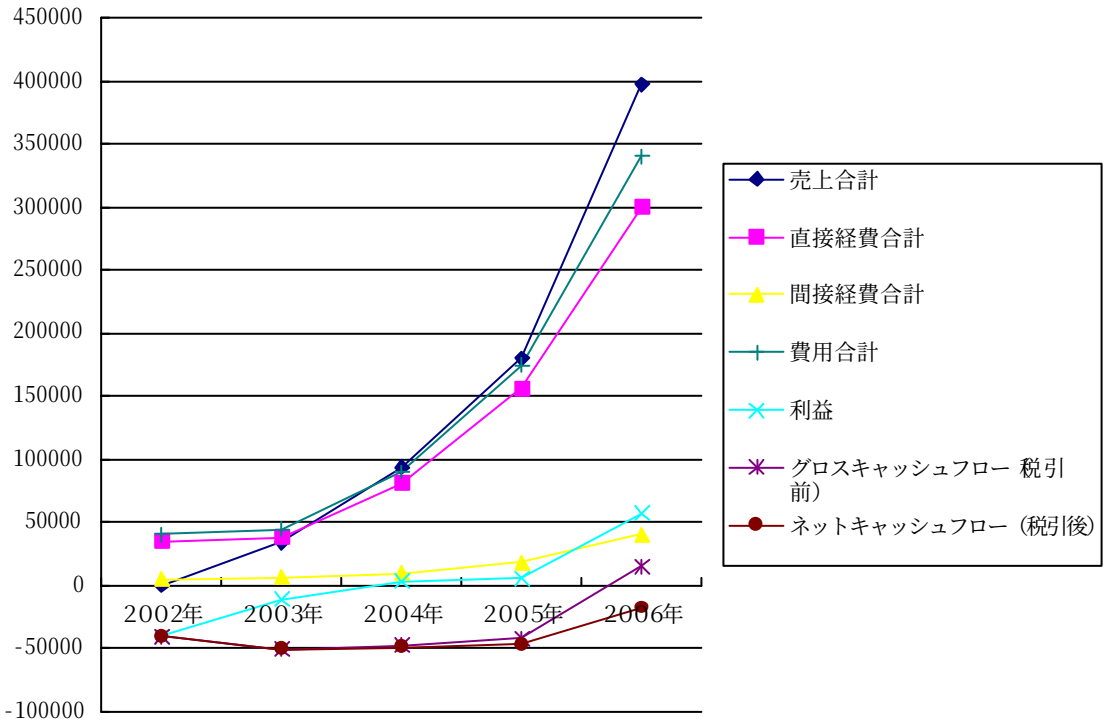


図５－４　キャッシュフロー

５．３　実現への課題

（１）ＩＣカードを非接触タイプにするか接触タイプにするか

小電力でのデータの読み書きが出来る特徴を持ったＦｅＲＡＭは非接触タイプに適していると言える。しかし、現在のワンタイムパスワードのプロトコルは接触タイプによる読み書きを前提としている。このため、非接触タイプの場合には Reader/Writer とＩＣカードに入れるプロトコルの拡張が必要となる。これらの機能分担の整理を行うと以下のようになる。

非接触タイプの場合、ＩＣカードとは Reader/Writer が離れているため、この間をデータが行き来する間に、データを盗まれる可能性がある。しかし、ワンタイムパスワードは、個人の暗証番号の入力を必要としている。ＩＣカードには携帯電話のような入力インターフェイスがついていないため、離れている Reader/Writer からパスワードを入力する必要が生じる。よって、Reader/Writer で暗証番号を暗号化してＩＣカードに送信する必要がある。

この場合、ＩＣカードにワンタイムパスワード計算のプロトコルを入れるだけでなく、暗証番号の復号のプロトコルを入れる必要がある。また、暗証番号の暗号化をそのように行うか、鍵を何にするか等を検討しなければならない。

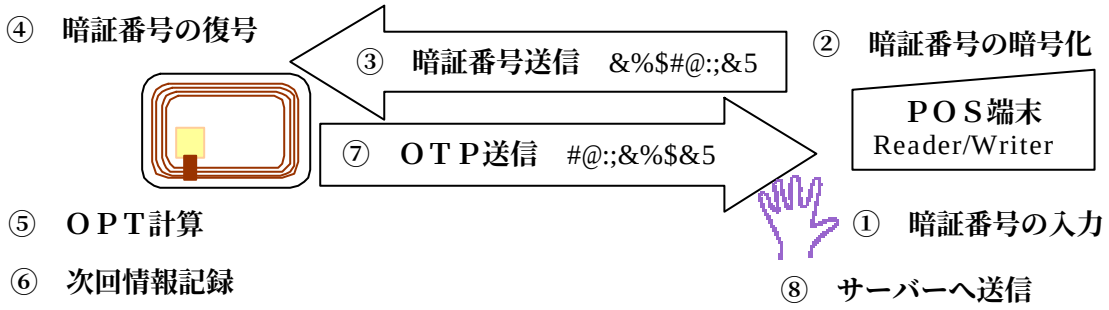


図５－５　非接触タイプの処理の流れ

（２）通信経路のトラブル対策

インターネットを通信インフラとする場合、通信経路上のトラブルや、通信速度の遅滞が発生する。インターネット上の通信経路のトラブルや通信遅滞にどのように対応し、システムの安定稼動を保つかが課題である。

（３）普及における課題

２～３の量販店のインハウスカードとして提携を行うことが重要であるが､競合する量販店の協力を得られるかがある。また、量販店、小売店の大部分に、既にＰＯＳ端末が導入され、販売管理システムが稼動している。量販店の場合、数千万円の投資によって構築した販売管理システムである。また、現状、自社構築を行った販売管理システムの使い勝手に大きな不満を持っていない場合は、新しいＡＳＰによるシステムの導入を行う判断をしない。よって、消費者が当システムを導入している量販店を選ぶ、財務諸表面での改善が図れるなどの積極的な理由が必要になる。

新システムをＡＳＰで利用する場合は問題ないが、現システムから新システムへの変更をせずに、消費者の利便性を高めるために当システムの Reader/Writer やＰＯＳ端末のデータ生成、データ変換プログラムの一部を変更しなければならない。この場合、ＰＯＳシステムのメーカーや種類によって、仕様が異なるため、個別にカスタマイズしなければならずロードが大きくなる。このロードによって発生するコストを店舗側に求めると、新システムの導入はなされないため、当ビジネスモデルの中において吸収しなければならない。

消費活動の場は多岐に渡る。量販店や小売店だけでなく、外食産業、ガソリンスタンド、美容院、病院…など多数ある。消費者にとって、この多岐に渡る消費活動の場、全てにおいて、購買情報を記録できるＩＣカードが使用できることが最も望むべきものである。購買情報を記録できるＩＣカードが使用できる消費活動の場を如何に広げていくか、マーケティング戦略上の課題は大きい。

金融機関（銀行やクレジット会社）との連携を行うことによって、よりスムーズな消費者への普及が進むと考えるが、既にクレジット会社各社では、磁気カードのＩＣカード化が始まっている。そして、既存のＩＣカード Reader/Writer の入出力インターフェイスは主にＥＥＰＲＯＭを対象としている。当システムで使用するＩＣカードは、ＦｅＲＡＭを既存のメモリ（ＥＥＰＲＯＭ）に換えて使用するため、新しいＦｅＲＡＭを用いたＩＣカード用 Reader/Writer が必要であり、既存カードとの相互共用を実現させる技術開発が必要である。

第六章　結論

６．１　実験・評価項目

最後に、当システムの実験項目をあげる。

① ＦｅＲＡＭと Reader/Writer との通信可能距離（非接触の場合）
② ＦｅＲＡＭと Reader/Writer との通信速度
③ 外的環境による通信の安定性
　例）温度、湿度、間に紙が挟まっている場合や、複数ＩＣカードを同じ財布に入れている時などの通信の安定性について。
④ ワンタイムパスワードに使用するデータの読み書きの安定性
　例）処理を繰り返し行っても、常にデータが正しい場所に書き込まれるかどうか。
⑤ メモリ内のデータエリアとプログラムエリアの非干渉
　ＦｅＲＡＭには、プログラムエリアとデータエリアがあり、プログラムエリアにはワンタイムパスワード計算のためのプログラム、暗証番号復号のプログラムなどが記録される。データエリアには、次回認証計算に使用する情報や暗号鍵を毎回記録する。これらが互いに干渉しないか、データが正しいエリア、ポジションに記録され、正しく読むことができるか。
⑥ 非接触タイプの場合、プロトコルの拡張が必要であるため、その検証

以上を中心として実験を行っていく予定である。

６．２　結語

ＩＴ革命の本質は生活革命であるとし、皆が情報を蓄積し、処理・編集・加工などを行い、情報を交換することによって新たな情報の流れが生まれ、社会や生活の成り立ちを変えるといった視点に立ち本研究を行った。そこで、高度通信情報ネットワーク社会の環の中に十分入っていない個人に目を向け、個人消費活動における情報の流通について考察した。

その結果、最先端技術である認証・暗号技術とそれを高い操作性で実現するメモリ技術を融合することによって、消費者が個人消費活動の場を通じて高度通信情報ネットワーク社会の環の中に入る選択肢を持つことができると考え、新しいシステムの提案を行った。言い換えれば、本研究はソフトに対する理解とそれを実現するハードに対する理解の融合の上にたって成されたものである。

この新しいシステムによって、消費者は個人消費活動の場を通じて情報流通の環の中

に入る選択肢を持つ。今後は、提案した新しいシステムのフィールドで実証実験を行っていく。これからは、認証・暗号技術、メモリ技術のみならず情報機器の処理能力が益々あがって進歩していく。また、ブロードバンド化し、IPV6 の技術が確立され、普及することによって、情報を持ち歩くから、高いセキュリティに守られた場所にデータを保管しておき、いつでもどこでもアクセスし、処理・編集・加工の指示が行えるユビキタス化が進んでいくと考える。

本研究で課題となった情報の流通については一定の成果を出せたと考えるが、情報のコントロールは今後の継続研究課題とした。ユビキタス化が進むにつれ、情報が流通することのメリットと共に、どこまで情報が広がっていくか分からないといった不安が残る。ＩＴ革命によって生まれる情報弱者への対応とともに、情報社会に対する不安を法律や規則など社会的に縛るだけでなく、技術的な研究をより進めていく必要がある。

謝　辞

本論文を結ぶにあたり、本研究をご指導、サポート下さった方々に心からの感謝の意を表したい。

主担当教官である加納剛太教授には、筆者の不案内な分野である半導体やメモリについて最先端の知識や情報をご教授頂いた。そして、理解を深めるための様々な資料、文献をご紹介下さり、その上に、論文の構成、表現など細部に亙って懇切丁寧にご指導、叱咤激励をして頂いた。

情報システム工学科の清水明宏教授には、起業家コース担当ではないにもかかわらず、認証、暗号技術について多忙な時間を割いて丁重にご指導下さった。また、論文作成に参考となる情報流通やネットワークに関する論文、文献などご紹介頂き、非常に参考になった。心から感謝している。
副担当である宮沢和夫教授にもお忙しい中、ディスカッションの時間を頂き、貴重なコメントを頂戴した。

濱口智尋教授、田路則子東京総合研究所主任研究員には、プレゼンテーション資料やその内容について貴重なコメントを頂戴したり、参考論文の紹介などを頂いたりと大変お世話になった。

現在のＰＯＳシステムや流通システムの構成、現場での課題などについて、富士通高知システムエンジニアリングのＳＥである山中鈴野氏、高木知弘氏に色々と教えて頂き、当システム構想をビジネスとして考える時に大変参考になった。お二人からヒヤリングを行うことを快く許可して下さった三ッ橋四郎富士通高知システムエンジニアリング社長には深謝したい。
ビジネスプランを検討するにあたって行った、買い物に関するアンケートにご協力頂いた起業家コースの学生を始め数多くの皆様にも心からお礼を申し上げたい。
当システムのフィールド実験についてご検討頂いた松下電器産業株式会社の大槻達男氏にも感謝している。今後、フィールド実験を行うにあたり、引き続きご協力を頂ければ厖大な幸せである。

平成１４年１月吉日
大野　加惠

《参考文献》

引用番号	文献名・著者名	出版社名他
(1)	「ＩＴ革命　－　ネット社会のゆくえ　－」 西垣通　著	岩波新書 平成１３年5月１８日 第一版発行 平成１３年9月　5日 第三版発行
(2)	「ＩＴ革命の虚妄」 森谷正規　著	文藝春秋 平成１３年1月２０日　第一版発行 平成１３年3月２０日　第四版発行
(3)	「情報通信白書」	平成１２年版 平成１３年版
(4)	「暗号」 辻井重男　著	講談社選書メチエ １９９６年4月１０日　第一版発行 １９９９年4月　8日　第五版発行
(5)	「プライバシーと高度情報化社会」 堀部政男　著	岩波新書
(6)	「暗号と情報社会」 辻井重男　著	文藝春秋 平成１１年１２月２０日 第一版発行
(7)	「構想力の時代　デジタル家電で」日本が勝つ」 水野博之　著	東洋経済新聞社 ２０００年6月２２日
(8)	「メタファーの記号論」 菅野盾樹　著	けい草書房 １９８５年4月３０日　第一版発行
(9)	「「暗号利用技術ハンドブック」	http://www.ecom.or.jp/qecom/
(10)	「インターネット取引は安全か」 五味俊夫　著	文藝春秋 平成１２年7月２０日　第一版発行
(11)	「知っておきたい　バーコード・二次元コードの知識」 平本純也　著	日本工業出版
(12)	「多目的利用ＩＣカード社会における望ましいシステムとあるべき標準化に関する調査研究報告書」	昭和６３年3月発行 昭和６１年カード犯罪の態様別状況と分類（日本国内）から作成

(13)	「インターネットセキュリティ入門」 佐々木良一　著	岩波新書 １９９９年3月１９日　第一版発行
(14)	「未来ネット技術シリーズ　情報セキュリティ技術」 伊土誠一　監修	電気通信協会
(15)	「消えないＩＣメモリ　－ＦＲＡＭのすべて－」 川合知二　著	工業調査会
(16)	「電子情報通信学会技術研究報告書」	OFS2001 - 39 - 50 オフィスシステム　2001 年 11 月 19 日
(17)	「暗号利用技術ハンドブック」	http://www.ecom.or.jp/qecom/
(18)	「無線アクセスのすべて」 武藤佳恭　監修	翔泳社 ２０００年8月１０日　第一版
(19)	「Integrated Ferroelectrics 」	１９９９，Vol. ２７，pp.291-314
(20)	「ＩＣカード　しくみと広がる世界」 玉田丈夫・穐山晴臣・桑原正幸　著	１９８９年7月１０日　第一版
(21)	「カードビジネスのすべて」 細貝康夫　著	日刊工業新聞社 １９９０年2月２８日　第一版
(22)	「暮らしと金融なんでもデータ　平成１２年度版」	貯蓄広報中央委員会
(23)	特願２００１－０８３１０６	
(24)	PANASONIC　資料より	
(25)	http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/recm_privc.htm	

《 アンケート集計結果 》* 単純集計 ＊

アンケート実施期間　　平成１３年８月３１日～９月１０日
有効回答数　　１６３名

1. 回答者の属性

□ 性別

		回答数	構成比
(1)	男性	76	46.6%
(2)	女性	87	53.4%
	計	163	100.0%

□ 年齢構成

		回答数	構成比
(1)	１８歳～１９歳	0	0.0%
(2)	２０歳～２５歳	10	6.1%
(3)	２６歳～３０歳	15	9.2%
(4)	３１歳～３５歳	21	12.9%
(5)	３６歳～４０歳	34	20.9%
(6)	４１歳～４５歳	22	13.5%
(7)	４６歳～５０歳	21	12.9%
(8)	５１歳～６０歳	30	18.4%
(9)	６１歳～７０歳	8	4.9%
(10)	７１歳以上	2	1.2%
	計	163	100.0%

□ お住まいの地域(地域)

		回答数	構成比
(1)	北海道・東北	2	1.2%
(2)	関東	48	29.4%
(3)	中部	3	1.8%
(4)	近畿	28	17.2%
(5)	中国	5	3.1%
(6)	四国(高知以外)	5	3.1%
(7)	高知	70	42.9%
(8)	九州・沖縄	2	1.2%
	計	163	100.0%

□ 同居人の有無

		回答数	構成比
(1)	有	127	77.9%
(2)	無	36	22.1%
	計	163	100.0%

□ 同居人有無で「有」の場合：どのような方と同居されていますか？（複数選択可）

		回答数	構成比
(1)	配偶者	97	47.5%
(2)	親	32	15.7%
(3)	子供	67	32.8%
(4)	親類	2	1.0%
(5)	友人	3	1.5%
(6)	その他	3	1.5%
	計	204	100.0%

□　職業

		回答数	構成比
(1)	会社員	74	45.4%
(2)	パート・アルバイト	12	7.4%
(3)	農林水産業	0	0.0%
(4)	自営業	16	9.8%
(5)	無職（専業主婦を含む）	32	19.6%
(6)	その他	29	17.8%
	計	163	100.0%

□　職業：その他の内容

		回答数	
	公務員	13	
	学生	6	
	大学教員・教員・大学職員	6	
	会社役員・経営者	3	
	アルバイト	1	
	合計	29	

□　通勤

		回答数	構成比
(1)	通勤はない	38	23.3%
(2)	バイクや自家用車	58	35.6%
(3)	徒歩、自転車	18	11.0%
(4)	電車、バスなど公共交通機関	44	27.0%
(5)	その他	4	2.5%
	無回答	1	0.6%
	計	163	100.0%

□　通勤：その他の内容
徒歩・自転車・車・公共交通機関を交互に利用

□　通勤時間はどのくらいですか？（片道）

		回答数	構成比
(1)	通勤はない	38	23.3%
(2)	３０分以内	69	42.3%
(3)	１時間以内	37	22.7%
(4)	１．５時間以内	12	7.4%
(5)	２時間以内	4	2.5%
(6)	２時間よりもかかる	0	0.0%
	無回答	3	1.8%
	計	163	100.0%

□　仕事や家事、通勤などの時間以外で、ご自身で使える自由な時間はどれくらいありますか？（１週間で）

		回答数	構成比
(1)	７時間以下	24	14.7%
(2)	１０時間以下	19	11.7%
(3)	２０時間以下	35	21.5%
(4)	３０時間以下	36	22.1%
(5)	５０時間以下	27	16.6%
(6)	５０時間よりも多い	22	13.5%
	計	163	100.0%

２．買い物について

Ｑ１－１　日常的な買い物をする量販店(例：スーパーマーケット、ショッピングセンター等）は決まっていますか？

		回答数	構成比
(1)	決まっている	37	22.7%
(2)	だいたい決まっている	113	69.3%
(3)	あまり決まっていない	10	6.1%
(4)	決まっていない	3	1.8%
	計	163	100.0%

Ｑ１－２　Ｑ１－１で「決まっている」「だいたい決まっている」：決まっているお店は何店舗位ですか？

		回答数	構成比
(1)	１店舗	9	6.0%
(2)	２、３店舗	104	69.3%
(3)	４、５店舗	30	20.0%
(4)	６～１０店舗	6	4.0%
(5)	１１店舗以上	1	0.7%
	計	150	100.0%

Ｑ１－３　Ｑ１－１で「決まっている」「だいたい決まっている」：最も良く行くお店はどこにありますか？

		回答数	構成比
(1)	自宅から歩いて行ける範囲（１キロ以内）	40	26.7%
(2)	自宅から自転車で行ける範囲（４キロ以内）	31	20.7%
(3)	自宅からバイクや車で５～１０分位の範囲（１０キロ	48	32.0%
(4)	会社から自宅への帰り道に	21	14.0%
(5)	その他	10	6.7%
	計	150	100.0%

□　その他の内容
- ＊　郡部在住。休日に高知市内まででかける
- ＊　電車でいける範囲
- ＊　生協通販
- ＊　勤務先
- ＊　遠くても専門店
- ＊　会社から歩いていける範囲
- ＊　近所の店及び自宅への帰り道にある店
- ＊　車で１５分以上かかります

Ｑ１－４　Ｑ１－１で「決まっている」「だいたい決まっている」：最も良く行くお店は、何が気に入っていますか？（複数選択可）

		回答数	構成比
(1)	場所（自宅から近い等）	99	37.1%
(2)	価格	65	24.3%
(3)	店員の応対（サービス）	17	6.4%
(4)	ポイントサービス等の付加サービスの充実	28	10.5%
(5)	その他	58	21.7%
	計	267	100.0%

□　その他の内容（複数記述の場合は分けてカウント）
* 品揃え　31
* 品質　7
* 営業時間（夜遅い）　3
* 店内の状況（清潔、明るい等）
* 買う計画がなくても、多くの商品を眺めて楽しめる
* 雰囲気。
* 商品の展示方法
* 新鮮さ・安全なものを扱っている。
* 商品の安全性
* スーパーですが魚が一匹二匹と選んで買えたり野菜果物も・・・・
* 生活用品が１店で済ませることが出来るから
* 品並べがなれている
* 店舗面積が小さく商品のまとまりが良い。
* ペットのえさの種類の多さと価格
* 好みにあった物が比較的安く売っている。
* 通勤経路上　商品が揃っている（スーパー）
* 生鮮食品が新鮮だから。お総菜が工夫されているから。
* お惣菜がおいしい。
* 商品がその店でしか販売されていない
* ほかに存在しないから
* カードをもっているので現金がいらない
* カードが使える
* 駐車場が広い　駐車場から道路に出やすい
* 駐車場がある。
* 駐車場があり、銀行、郵便局などがあるから
* 駐車場に入りやすい。
* 公立図書館が同じ敷地内にあるから
* 夏は暑いし、冬は寒いから遠くへは行きたくない

Ｑ１－５　量販店の会員カードを持っていますか？

		回答数	構成比
(1)	現金決済のみ	75	46.0%
(2)	クレジット決済のみ	10	6.1%
(3)	現金・クレジット決済両方	36	22.1%
(4)	持っていない	42	25.8%
	計	163	100.0%

Ｑ１－６　量販店での支払いは何が中心ですか？

		回答数	構成比
(1)	現金	134	82.2%
(2)	クレジット決済ができる量販店の会員カード	17	10.4%
(3)	一般のクレジットカード	12	7.4%
	計	163	100.0%

Ｑ１－７　家計簿を個人的につけていますか？

		回答数	構成比
(1)	はい	42	25.8%
(2)	いいえ	121	74.2%
	計	163	100.0%

Ｑ１－８　Ｑ１－７で「はい」：パソコンの家計簿ソフトを使用していますか？

		回答数	構成比
(1)	はい	10	23.8%
(2)	いいえ	32	76.2%
	計	42	100.0%

Ｑ１－９　Ｑ１－７で「はい」：記入や入力の際参照するのはレシートですか？

		回答数	構成比
(1)	はい	42	100.0%
(2)	いいえ	0	0.0%
	計	42	100.0%

Ｑ１－１０　Ｑ１－７で「はい」：量販店での買い物の場合、記入や入力はどういった単位で行っていますか？

		回答数	構成比
(1)	明細（品目）単位（例：牛乳や卵、靴下等）	7	16.7%
(2)	費目単位（例：食物、被服、保健衛生等）	28	66.7%
(3)	店舗単位の合計金額	7	16.7%
(4)	その他	0	0.0%
	計	42	100.0%

Ｑ１－１１　Ｑ１－７で「はい」：Ｑ１－９の記入や入力の単位で満足していますか？

		回答数	構成比
(1)	はい	34	81.0%
(2)	もう少し細かな単位で	6	14.3%
(3)	もう少し大まかな単位で	2	4.8%
	計	42	100.0%

Ｑ１－１２　Ｑ１－７で「はい」：レシートが出ないところでの買い物の金額はどのように記録していますか？（複数選択可）

		回答数	構成比
(1)	覚えておく	26	45.6%
(2)	メモしておく	12	21.1%
(3)	合計値で処理をする	5	8.8%
(4)	大体の金額で処理する	7	12.3%
(5)	気にしない	2	3.5%
(6)	記載しない	0	0.0%
(7)	その他	5	8.8%
	計	57	100.0%

Ｑ１－１３　Ｑ１－７で「はい」：クレジット使用の家計簿記入や入力はどのようにしてい

		回答数	構成比
(1)	クレジットカードは使わない主義である	12	28.6%
(2)	家計簿記入、入力要領に従って記入、入力	6	14.3%
(3)	現金と同じように記入、入	16	38.1%
(4)	わからないので記入や入力をしていない	3	7.1%
(5)	その他	5	11.9%
	計	42	100.0%

Ｑ１－１４　Ｑ１－７で「はい」：家計簿を月単位、年単位で集計し、分析していますか？

		回答数	構成比
(1)	集計も分析もしている	8	19.0%
(2)	集計はしているが分析までは	24	57.1%
(3)	集計も分析もあまりやってい	9	21.4%
(4)	その他	1	2.4%
	計	42	100.0%

Ｑ１－１５　Ｑ１－７で「はい」：家計簿に係わる時間は１日でどれくらいですか？

		回答数	構成比
(1)	１０分まで	7	16.7%
(2)	３０分まで	21	50.0%
(3)	１時間まで	13	31.0%
(4)	３時間まで	1	2.4%
(5)	５時間まで	0	0.0%
(6)	５時間以上	0	0.0%
	計	42	100.0%

Ｑ１－１６　Ｑ１－７で「いいえ」：家計簿をつけない理由は何ですか？

		回答数	構成比
(1)	必要がないから	50	41.3%
(2)	面倒でできない（つけ始めても長続きしない）	42	34.7%
(3)	時間がない	16	13.2%
(4)	その他	13	10.7%
	計	121	100.0%

□　その他の内容
* エクセルに使用金額だけ入力しています。
* 何を買ったかすぐ忘れる（レシートも無くす）ので誤差が多すぎてやめた
* つけていたが、有効でないので止めた
* ほとんどがカード決裁で、請求書が送付されて来る
* 家内はつけていると思います
* 妻がつけている
* 前に家計簿をつけて、生活費を把握済
* 家内の把握で私にはわかりませんので現在の所信頼しています。
* 毎月の出費がだいたい決まっているから
* 会社の帳簿でせいいっぱい
* 家計簿の活用方法が良く解らず、あまりつける意味を感じない
* 家計簿をつけること自体、思いついていなかった。
* 必要なお金は出て行くしかないから

Ｑ１－１７　あなたの買い物情報から家計簿を自動的に作成し、分析してくれるサービスがあれば利用しますか？

		回答数	構成比
(1)	ぜひ利用したい	15	9.2%
(2)	利用を検討したい	48	29.4%
(3)	自分でやるので必要ない	15	9.2%
(4)	多分利用しない	55	33.7%
(5)	利用しない	30	18.4%
	計	163	100.0%

Ｑ１－１８　Ｑ１－１７で「ぜひ利用したい」「利用を検討したい」：サービス利用時に、何で個人認証が行われると良いと思いますか？

		回答数	構成比
(1)	カード	32	50.8%
(2)	携帯電話	16	25.4%
(3)	パームやＰＡＤなど、その他の携帯端末	2	3.2%
(4)	腕時計やペンダントなど、身につける情報端末	2	3.2%
(5)	その他	11	17.5%
	計	63	100.0%

□　その他の内容
＊　物理媒体は何でも良い。サービス提供側で個人についての生活の詳細が判別できないこと
＊　指紋
＊　特になし
＊　指紋と暗証番号など、二つ以上の方法を組み合わせる
＊　パスワードで十分です
＊　生体（指紋）＆知識情報(password)&所持品情報(CARD)
＊　体（部分・臭い・声etc）
＊　（携帯に入る？）ＰＨＳ
＊　音声とか指紋など

Ｑ１－１９　Ｑ１－１７で「ぜひ利用したい」「利用を検討したい」：作成済み家計簿はどのような形で欲しいですか？

		回答数	構成比
(1)	Ｗｅｂで確認したりパソコンで印刷	6	9.5%
(2)	Ｗｅｂでダウンロードも	38	60.3%
(3)	街角記帳機で印刷する。（銀行のATM記帳のイメー	5	7.9%
(4)	月１回郵送されてくる	10	15.9%
(5)	わからない	1	1.6%
(6)	その他	3	4.8%
	計	63	100.0%

□　その他の内容
＊　家の場合：ＰＣ、外出時：パームやＰＡＤ
＊　外部媒体を使用しない個人固有の環境だけを使用したもので参照できれば良い
＊　パソコンを持っていないので、上記２番目と４番目などの組み合わせ

Ｑ２－１　携帯電話を持っていますか？

		回答数	構成比
(1)	はい	127	77.9%
(2)	いいえ	36	22.1%
	計	163	100.0%

Ｑ２－２　パームやＰＡＤなど、その他の携帯端末を持っていますか？

		回答数	構成比
(1)	はい	17	10.4%
(2)	いいえ	146	89.6%
	計	163	100.0%

Ｑ２－３　情報化社会で、こういうことが実現されると良いのに・・・と思うことがあれば、お書きください。
＊　精神的強化
＊　携帯電話の完全カーナビ化
＊　買い物をするときに、今月の予算を超えたら警告がでたり、ダイエット中に一定以上のカロリーを摂取すると、それ以上たべないように警告がくる。
＊　世界中どこでも使用できる端末がほしい
＊　子供の運動会などを遠く離れたところからでも見える（安く、簡単に）ようになれば、仕事場で観戦する。
＊　個人ID制。もうすべてのIDは統一し、指紋他での認証で一発OKにしてほしい。どうせ年金その他でがっちり個人情報なんて抑えられてるし。
＊　必要以上の機能アップより通信料金をやすくすること。
＊　インターネットインフラの充実によるメディアの統合（ラジオ、テレビ、新聞等の情報も全てインターネットで）
＊　家計簿の診断と適切な指導が適時受けられるシステムの提供
＊　年寄りに使いやすい携帯電話。今の携帯は年寄り向きでは無い。しかし、一番必要ではないか。数カ所の指定登録電話で、押すだけで繋がるタイプがいい。当然にこちらから居場所確認も出来なければ意味がない。

* 人口の少ない地方にも、インターネットの常時接続できるようになって欲しい。
* ＩＤカード一枚で戸籍から保険証等々兼ねる事ができれば今のようにいちいち変更しなく
IT時代になっても田舎はサービス対象外です。一部の人の利益や便利さでは全国的には
* 満足行くサービス提供にはならないと思います。例：電波の入らない地域や光ファイ
バーケーブルの使えない人たち
* 情報技術を上手に使った生涯学習社会
* 常に端末を携帯するのではなく、必要時に鳥が持ってきて、使用し又鳥に返すような方法
* 近くの催し物や、便利やさん情報
* 呼び出し音も、人が話している声も聞こえない携帯電話
* メールやファイルに分散しているデータを関連付けて、新たなデータベースを作ってくれ
* 子供の様子が保育園から定期的に画像配信される（一部、サービスが実施されているが
* パソコンの場合、機能の充実だけでなく、使いやすさなどの充実も考慮に入れるべきだ
と思う。（高齢者用など）
* セキュリティーシステムの構築
* パソコンや携帯電話でのテレビの放送日やビデオのレンタル在庫の検索サービス
* 思い（脳波の動き）が自動的にイメージや文字に変換できる。
* 各社の検索エンジンがエシュロンクラスの能力を持ち、いかなる情報も無料で入手でき
るようになること
* 振込、支払いのネット決済
* 低価格で速いネットワーク環境。
* 現在のLap top PCの重量が半分になること。
プライバシーの侵害になるかもしれませんが、大金を出して利用するもの、生命等に関
* 係して利用するものの的確な情報。病気治療の適した医師や病院の紹介。裁判に適した
弁護士の紹介や、腕のいい大工さん等の情報が得られること。
* リアルなバーチャル体験ができるようになればいい。（たとえばショッピングのとき
に、パソコン内でリアルな自分を作ってバーチャル内で試着できるようにするとか）
* 家の戸締まりが携帯電話で確認できる。留守中不審者が家に入ってきたら携帯電話に通報
* 故障の少ない、起動の早いウェアラブルパソコンで、いつでもどこでも連絡・情報管
理・仕事がこなせること
* ユビキタス遠隔地映像コミュニケーション
* 一部行われているが、国内外で現金なしで商品決済。身に付ける情報端末特に眼鏡の形
態をモニターとしTVやパソコン画像を見ること。
* 情報料の低価格化
* スタートレックのように、都度ＴＶ電話や会議がこの場で（PC）でできれば
* 銀行や郵便局へ行かなくても、お金の出し入れや振り込みなどが、無料で出来ればと思う
* ＰＣ等情報端末の無線化
* 根本的なインフラの整備、並びに低価格化
* 立体映像が送れるようになったら面白いと思う。動画のもっと先の感じ。実物大じゃな
くていいから。
* 不要情報の排除（不要の宣伝メールが数多く舞い込むのを防ぎたい）
* 国際的なコミュニケーションにおける自動翻訳サービス。
* 人がお互い思いやり、第六感も素直に使える穏やかな世の中。
* 海外の情報はよく入ってくるのに、東京では近辺の事故、事件、火事などの情報はほと
んど入らない。
* 与えられる「便利」のなかで、自分が必要なものを選ぶのみ。総論としては「情報化」
してほしくない。
* 病気の時の病院の情報。修理、どこに頼めばいいのか。
* 家計簿サービスと同様な、事業経費の領収書を集め整理する作業に変わるもの
* 低価格の携帯電話、パソコン機器
* ショッピングに行かなくても欲しいものを出前してくれるサービス
* 在宅勤務。でも本当は良くないことですね。情報化は考え方を誤ると人間性を奪います。
* 携帯電話で買物の決済ができればいい。各店舗発行の個々のポイントカードを持ち歩く
のはたいへん
* 通信速度の向上。機器の小型化。仕様の統一。
* 心の交流が円滑になればいいと思う
* 住所と電話番号とメールアドレス等、アドレス情報の管理の一元化
* 必要としている情報の自動抽出、検索機能
* 情報のクラスタリングと連関の自動抽出

＊　音楽配信など、もっと安く利用できたら良い
＊　個人にとって有用/無用な情報の区別ができる今まで以上の検索機能を持ったものがほし
＊　ＰＨＳだけを持っています。よって、携帯とＰＨＳが変わらずに利用できるサービスで会って欲しい。（何事においても。）
＊　職安に出向かなくても求人情報が閲覧できる。図書館に出向かなくても端末デリバリしてもらって借りる。在宅勤務
＊　今までの情報化をよりよく活かす社会(ソフトの問題？)→結局「人間」なんだと思う・・
＊　キー入力以外の入力装置など。ウエアラブルなPC
＊　痴漢、ひったくり見張り番＆通報サービス
＊　独居老人や視覚障害者に使いやすい携帯電話の開発と、点字版マニュアル
＊　老人も銀行のATM位の操作で利用できるようなパソコンの普及
＊　季節・その日の天気に合わせた、毎日の献立のレシピが届くと良いと思う。
＊　キャッシュレスですべて決済できる
＊　秘密を守る

Ｑ２－４　情報化社会で、懸念されることがあれば、お書きください。

個人データ・個人情報の漏洩	46
個人情報の流出・悪用	10
セキュリティの問題	9
誰かに勝手に個人情報を管理されること	4

□　以下、上記に分類したものに加えて具体的に。

＜セキュリティについて＞
＊　情報漏洩。システムではなく人災だからこればかりは防ぎようがない。
＊　情報の真偽性。個人やネットのセキュリティー。人を傷つけることも簡単に出来ます。幼い子供などは現実感が無くなるのではないのでしょうか。
＊　とにかく、機密保持という概念が日本でまったく、論議されずに進んでいること。教育の現場では、まずこのことからスタートすることが肝要。
＊　セキュリティーとスピードとユビキタス化
＊　口座引き落とし決済の場合のセキュリティー
＊　情報コントロールが外部の悪意や不用意に操作されること
＊　知的所有権の侵害
＊　ハッカー対策と秘密保持
＊　情報の流出とトラブルによる紛失。
＊　セキュリティ、ウイルスなどについて、安全はNet環境の実現。
＊　何よりも心配なのは個人情報の流出、カードのスキミングのようなことが起こる可能性が０でないのは不安。
＊　１００％の保護策は絶対に有り得ないと思います。

＜情報過多について＞
＊　情報が多くなりすぎて個人で自分の情報管理ができなくなること。（オーバーフロー）
＊　情報過多
＊　情報が膨大になることです
＊　情報に踊らされること。
＊　便利すぎる、情報氾濫などのような、過度のサービス提供
＊　情報が多すぎて自分で情報や状況を判断する力が無くなってきていると思う。流されている事が多いと思う。
＊　情報過多による真実の歪曲化
＊　情報量が抱負過ぎて消化しきれない。スピードばかりが求められ生活にゆとりがなくなってきている。

＜コミュニケーションの問題について＞
＊　最近、Eメールによるコミュニケーションの欠点を実感します。「便利」より「懸念」を常に感じます。
＊　実際酒を飲んだり、話したりすることでできる信頼関係
＊　コミュニケーションの希薄化。対面での話が苦手となる。
＊　人間関係が希薄になる
＊　取り残される人たちに対する処置、嫌いな人、能力的に難しい人両者
＊　人間同士のふれあいの欠如

＜健康について＞
＊　視力低下、電磁波など健康面への悪影響

＜社会について＞
＊　失業率の拡大(募集と希望のアンバランス)
＊　ネットワークの高速化が進んでいるが、災害などでネットワークが途切れた場合の影響が、今まで以上に大きいのではないか？
＊　情報化社会では、飯は食えない　生産性（食料や生活に必要品）のあり方
＊　人員削減
＊　サイバーテロの増加
＊　国家政府による個人情報管理への懸念。
＊　インターネットによる犯罪が急増していること
＊　ウイルスの進入・情報化社会について行けなくなること

＜その他＞
＊　NTTには、健全な推進能力があるのかどうか不安
＊　ウイルスなど迷惑メールの発信をすること
＊　ハード偏重
＊　ウイルス。悪徳商法
＊　作業をした実感がないため、やったかやらなかったかの記憶が残らない。相手の顔が見えないので、信用できるかの判断が難しい。
＊　何かが完全に欠落すること。本当に大切なものが見えなくなること。
＊　迷惑メールのようなものはいらない
＊　通信環境(インターネット、電話)の整備不足および利用料金の高価なところ。
＊　ドコモの迷惑メールのようなものが蔓延すること。また、発信元が無責任な情報を自由に流しても罪にに問われない　今の無法状態では、この先問題が多いのでは。
＊　内容が正しくなかったり、偏った情報が瞬時に共有化されて、皆がその情報が正しいと思い込んでしまうこと。その結果、自分で考えたり、疑問を持ったりする能力が失われ