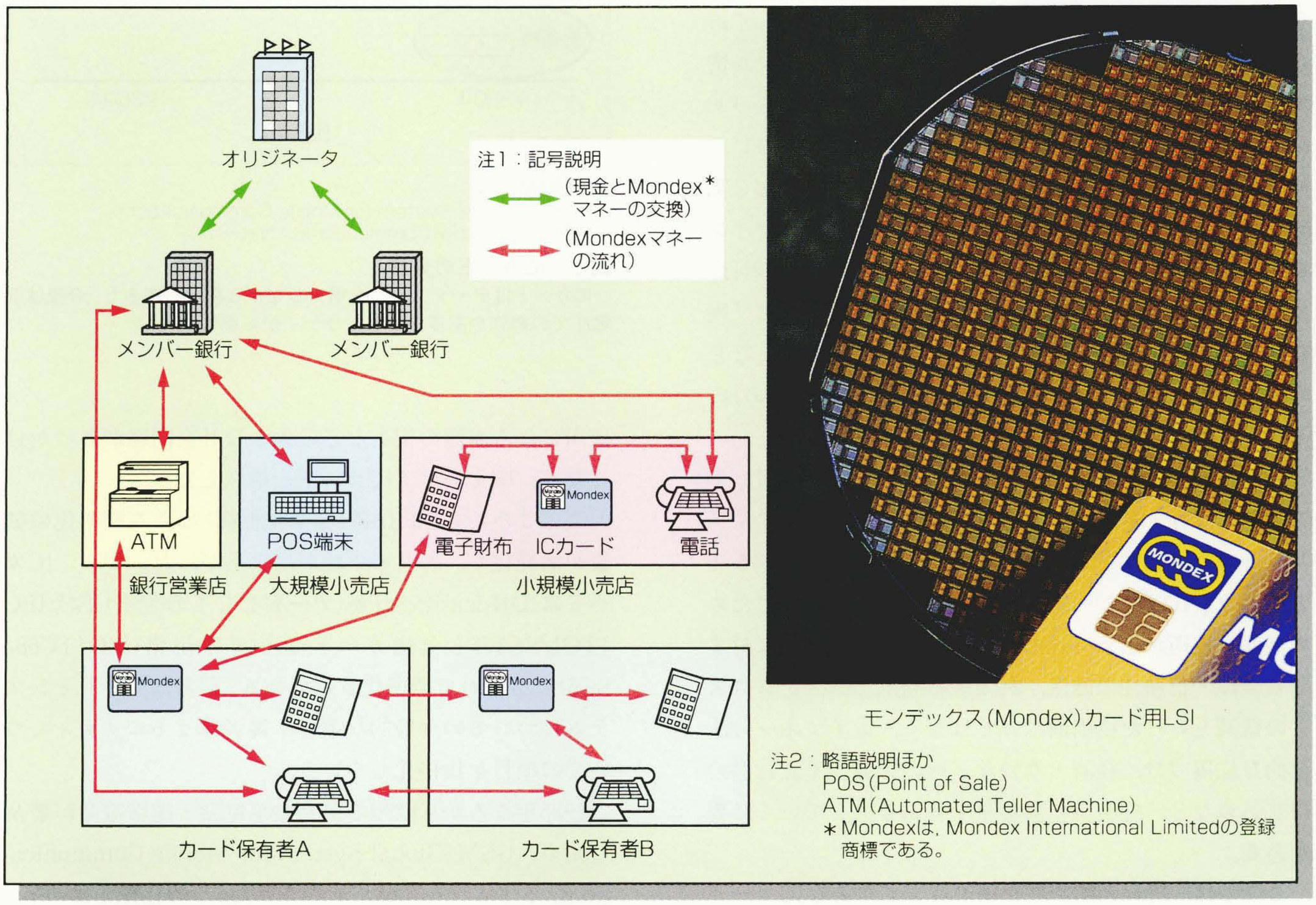
電子マネーとICカード用マイクロプロセッサ

IC Card Microprocessor for Electronic Money

佐藤恒夫* *Tsuneo Satô*
田中紀夫* *Toshio Tanaka*
中田邦彦* *Kunihiko Nakada*
竹島雅彦* *Masahiko Takeshima*
長崎信孝** *Nobutaka Nagasaki*



モンデックス（Mondex）カード用LSI

モンデックスの利用形態[1]とICカード用マイクロコンピュータのウェーハ

オリジネータ（モンデックスマネーの発行母体）からメンバー銀行が現金で購入したモンデックスマネーは，他銀行，小売店，カード保持者との間で流通する。モンデックスマネーのような電子マネーシステムではICカードの役割が重要であり，ICカードに使われるマイクロプロセッサには高いセキュリティが求められる。

情報のディジタル化と広域ネットワークの急速な進展により，電子商取り引き，電子マネーシステムによるICカードをベースとしたキャッシュレス社会が到来しつつある。

ICカードには，改ざん，コピー偽造などの不正行為を防ぐための高度な技術が求められており，そのためにはICカードに使われるマイクロプロセッサが情報の機密性を保つうえで重要な役割を担っている。

日立製作所が開発した数々のICカード用マイクロプロセッサの中で“H8/3111”は，暗号処理の高速化を可能にするコプロセッサを内蔵していることにより，電子マネー用に適したマイクロプロセッサと言える。低電圧，低消費電力回路技術を採用し，チップサイズでは0.8ミクロンプロセスで19 mm^2を実現した。

*日立製作所 半導体事業部 **株式会社日立マイコンシステム

1. はじめに

情報のディジタル化と広域ネットワークの急速な普及によって電子商取り引き，電子マネーシステムの実用に向けた提案，実験が世界各地で行われている。電子マネーシステムは，貨幣(バリュー)を電子化するものと，決済を電子化するものに大別される。前者はICカード(スマートカードとも言う。)をベースにしたシステムであり，ICカードの内部に「現金」に相当するディジタル情報を蓄えておき，この情報を転送することによってバリューの授受を行うものである。この方式の主なものに，英国ナショナルウエストミンスター銀行ほかが提案し実験を行っている「Mondexシステム」[1]や，米国ビザインターナショナル社の“Visa Cash”などがある。後者は，インターネットなど広域のネットワークをベースに「現金」，「小切手」，「クレジットカード」，「口座振替」などの支払手段を代替しているシステムであり，主なものは，オランダデジキャッシュ社の“e-cash”がある。

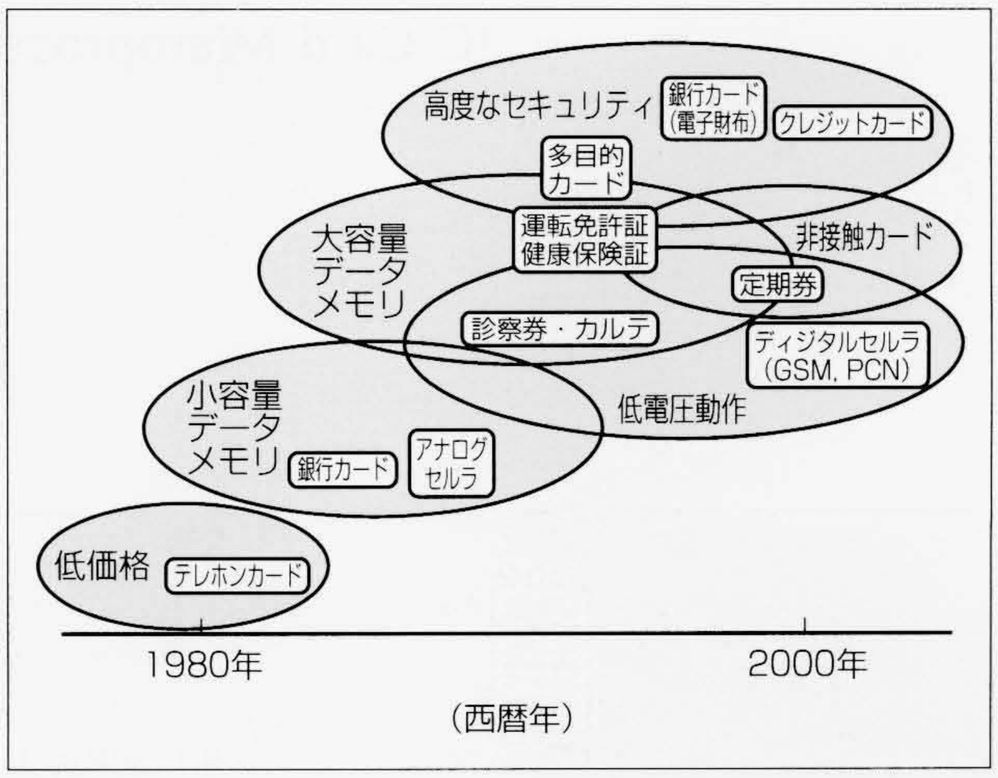
いずれの方式でも電子マネーシステムは，消費者，小売業者，銀行・金融業者それぞれにとって使いやすくメリットのある柔軟なシステムであることが要求される一方で，改ざん，コピー，偽造などの不正行為を防ぐための高度な技術が求められている。また，不正行為に対する安全性・信頼性の確保，利便性の向上，システムコストの低減といった技術面だけではなく，電子マネーの法律的な位置づけ，経済・為替などへの影響，不正行為の封じ込めなど，社会への影響を十分に考慮していく必要がある。

ここでは，情報の機密性を保つうえで重要なICカードに使うマイクロコンピュータについて，その開発思想と将来技術の展望について述べる。

2. 市場動向

ICカードは，クレジットカードや銀行のキャッシュカードと同じプラスチックカードにICチップを埋め込んだものであり，磁気カードには無い大きな記憶容量を持ち，それ自身で演算や処理ができる知能カードとして発展してきた(**図1**参照)。

ICカードの初めての実用化に踏み切ったのはフランスである[2]。フランスはICカードの基本特許を成立させたことに加え，日米やほかの欧州各国に比べてクレジットカードが普及せず，典型的な小切手社会であった。このため，事務コストの増大，オンライン化の遅れ，不正使用による多額の損失などの大きな社会問題がきっかけになり，国をあげてICカードを導入した。



注：略語説明
GSM(Global System for Mobile Communications)
PCN(Personal Communication Network)

図1　ICカードの発展
ICカードはデータメモリを増大しながら発展してきた。今後は低電圧での動作や高度なセキュリティが必要になる。

このころからISO(国際標準化機構)による標準化の動きが活発化し，普及の下地が出来上がった。現在，ICカードはID(Identification)カードとしての規格(ISO/IEC JTC1/SC17)と金融カードとしての規格(ISO/TC68/SC6)に分かれて標準化されている。前者はカードとシステムについての全般的な項目，後者はセキュリティについての項目を規格化している。

1985年ごろから欧州では自動車電話・携帯電話が普及し始め，GSM(Global System for Mobile Communications)と呼ばれる仕様が発表された。この仕様では，所有者のIDコードや各種サービス情報を蓄積するためにSIMCと呼ばれるICカードの使用が義務づけられており，大きなICカードの需要を持つ分野に成長している。

一方，最近のインターネットの普及により，電子マネーや電子商取り引きといった新分野・新事業が急速に伸びており，この決済方法の一つとしてICカードが使用されている。その代表的な例として，1995年7月モンデックス(Mondex)と呼ばれる世界初の電子キャッシュシステムの試行がイギリスで開始された。このモンデックス用ICカードには日立製作所が開発したICカード用マイクロプロセッサが使用されている。今後，1998年にかけて世界各地でモンデックスシステムが試行されることになっている。また，モンデックスではインターネットで情報提供を開始しており，いずれはインターネットを使

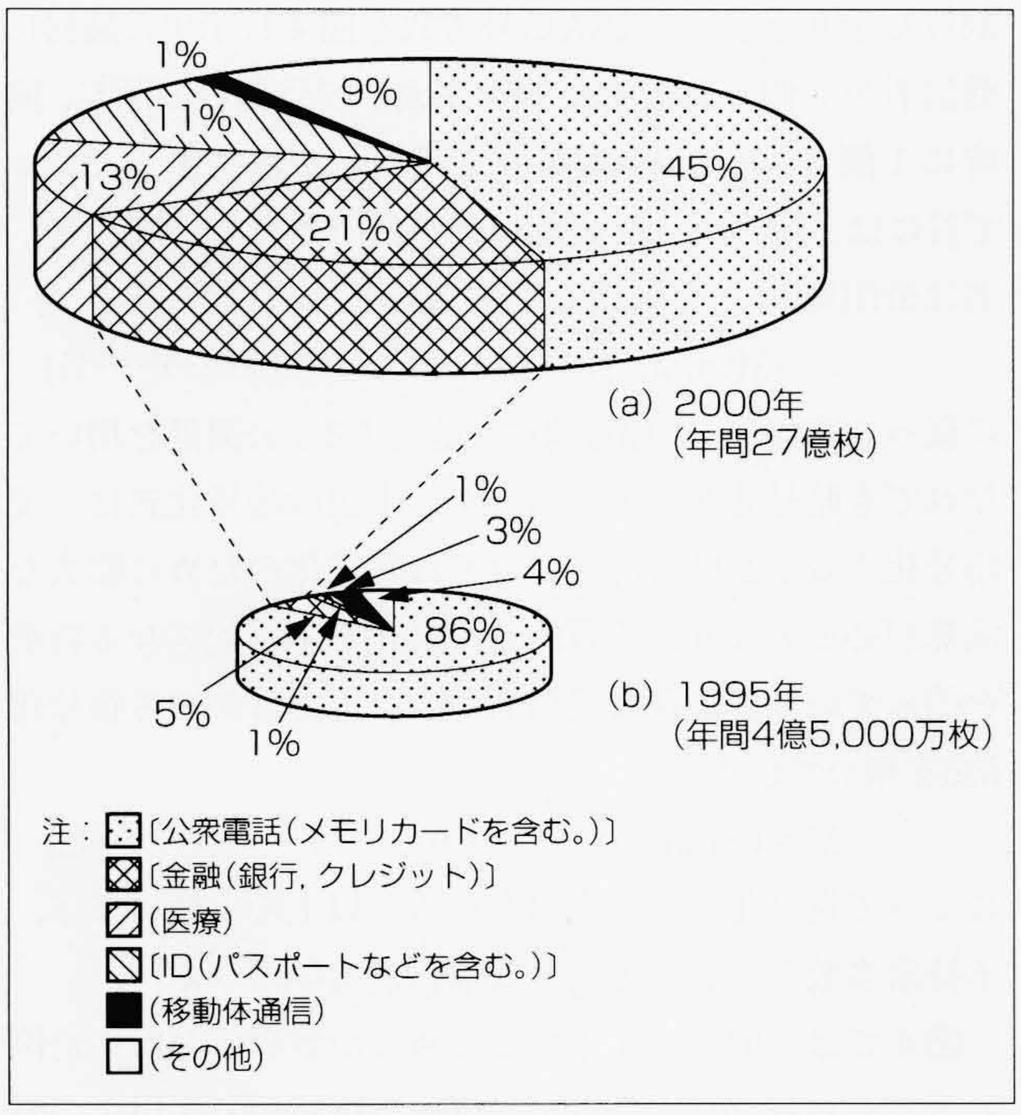


図2　ICカードの応用別市場動向
1995年には公衆電話用カードが約9割を占めているが，2000年にかけて金融向けカードの著しい成長が見込まれている。

ってモンデックスカード間で資金移動を行う計画もあり，簡単な支払システムからネットワークを使った本格的な電子商取り引き(エレクトロニックコマース)へ向けての準備を進めている。

一方，クレジット業界でもICカード化の動きが活発化しており，1995年にクレジットカードメーカーのビザインターナショナル社，マスターカードインターナショナル社，ユーロペイ社は三者合同でクレジットカードについてのICカード統一規格を発表した。これは三者の頭文字を取って「EMV規格」と呼ばれ，実質的に世界クレジットカード規格となっている。現在，クレジットカード各社はこの規格を基にICカード化を進めている。ICカードの応用別市場動向を**図2**に示す。現在の主要分野は公衆電話用テレホンカードが大部分を占めるが，2000年に向けてクレジットカードを含めた金融市場は，今後，最も注目されるICカードの市場である。

地域別に見ると，ICカード市場は欧州が一歩先んじた形になり，1995年でも世界の市場の約80%を占めている。近年，アジアでも先に述べたGSM仕様の電話を採用する国が増加し，これに伴って欧州カードメーカーのアジア進出が目立つようになった。アジアの地元メーカーとの合弁なども多くなってきている。またアジア各地では，例えば中国での貨幣管理(金カード)，韓国での政府発行書類のカード化(Tカード)などでICカードのトライアルが行われている。

3. ICカードによる電子マネー実現の課題と対応策

以上に述べたICカード市場の中で，特に今後の急速な市場成長が期待されている電子マネーについて，その実現上の課題と対応策を以下に述べる。

3.1　電子マネー実現の課題

ICカードを使用した電子マネーシステムでの送金の概念を**図3**に示す。現金に相当する残高情報(バリュー)がディジタル情報化されてICカード内の不揮発性メモリEEPROM(Electrically Erasable Programmable Read-Only Memory)に記憶されており，送金額がディジタル情報化されてICカード間で送受信される。送金額が双方のICカード内のバリューからディジタル演算処理によって減額・増額されてEEPROMの内容を更新する。

このときのICカード間での送受信は専用のリーダ・ライタの内部で行われるのに加え，電話回線やインターネットなどのネットワークを用いた通信による送金も，今後のアプリケーションでは幅広く行われることが考えられる。通信回線上の送金情報を改ざん，コピーするなどの不正行為を防止するために，電子マネーシステムでは通信情報を「暗号化」することが必須である。このときの暗号化・復号化はICカード内の演算処理によって行われるため，ICカードの機能・性能が電子マネーシステムの構築で重要な要因となる。電子マネーシステムに要求されるセキュリティ性を満たす暗号方式と，そのICカードによる実現方法について以下に述べる。

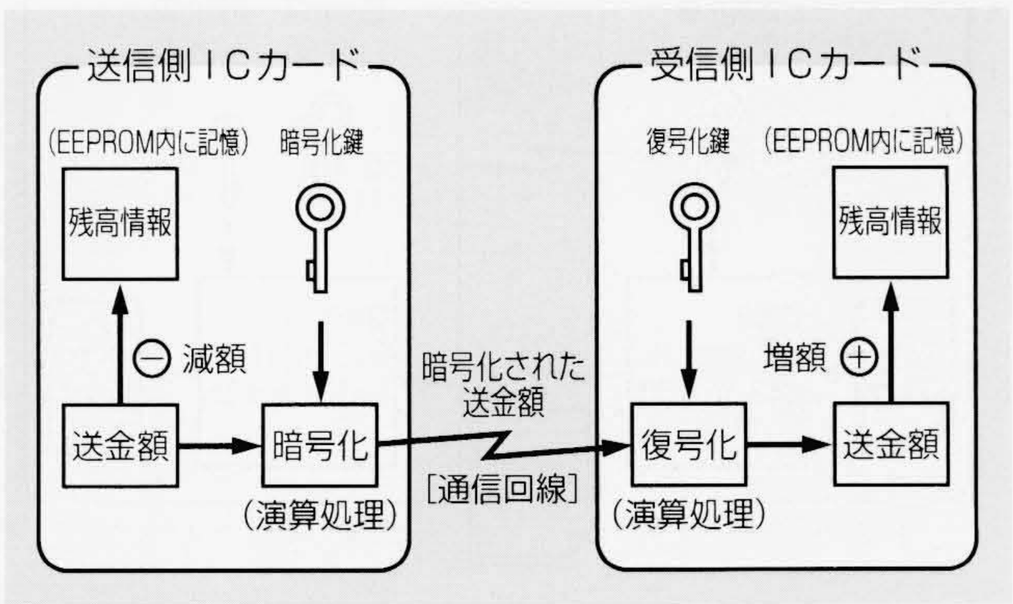


図3　ICカード間の電子マネーの送金
暗号化された送金額がICカード間で送受信される。残高情報は不揮発性メモリEEPROM内に記憶される。

3.2　暗号化技術

ディジタル情報の暗号化は，上述した電子マネーをはじめとする安全なディジタル通信の実現要求の高まりから，近年活発に研究され，数多くの暗号方式が提案されている[3]。これらは「秘密鍵暗号方式」と「公開鍵暗号方式」に大別される。

秘密鍵暗号方式は，暗号化鍵と復号化鍵とを同一にし，共に秘密鍵として管理する方式である。代表的な方式として国際標準にもなっているDES(Data　Encryption Standard)暗号が知られている。日立製作所は，秘密鍵暗号方式として1989年にMULTI2暗号を開発し，CS(Communication Satellite)ディジタル放送適用などで実用化している[4]。秘密鍵暗号方式は一般に演算速度が高速であるという利点を持つ一方，秘密鍵をあらかじめ送信者と受信者に配送しておく必要があり，鍵管理に制約のある場合がある。

公開鍵暗号方式は，異なる暗号化鍵と復号化鍵を使用する。暗号化鍵を公開することによって鍵管理を容易にし，同時に利用者が本人であることを確認して証明する，いわゆる「認証」を容易にする利点がある。特に電子マネーシステムでは不特定多数との間での通信における認証の実現が重要課題であり，その解決のために公開鍵暗号方式が使用されることが多い。一例として，1978年に米国のRivest，Shamir，Adlemanの3人によって考案され，その頭文字をとって命名された「RSA暗号」が一般に知られている[3]。

RSA暗号では$X^Y \bmod N$で表される剰余演算が用いられる。ここで X，Y，Nは整数であり，“mod N”はNで割った余りを表す。RSA暗号方式を**図4**に示す。最初に受信者が2個の公開鍵e，Nを生成して外部に公開し，同時に1個の秘密鍵dを生成して受信者が保持する。ここでNには2個の大きな素数の積が使用される。次に送信者は公開鍵e，Nを使用して平文Mを

$$C = M^e \bmod N \quad \cdots\cdots (1)$$

に従って暗号化し，暗号文Cを送信する。公開鍵を用いてだれでも暗号化が可能であるが，上記の暗号化式は一度暗号化すると公開鍵e，Nだけでは復号化のために膨大な演算が必要となり，実質的に復号化が不可能となる特徴を持っている。最後に受信者が，自分だけが知る復号化鍵dを用いてCを

$$M = C^d \bmod N \quad \cdots\cdots (2)$$

によって復号化し，平文Mを得る。以上の手順により，不特定多数との間での安全な通信が実現できる。

図4では理解しやすくするために小さな値を用いた例で示している。実システムでは鍵には512ビット以上の整数が使用される。そのため，暗号化・復号化には膨大な演算が必要になり，従来のICカードでは実用に耐え得る十分に速い処理速度が実現できないという技術的課題があった。以上はRAS暗号での例であるが，処理速度の問題は一般の公開鍵暗号方式での共通の課題であった。その解決策として日立製作所は，CPU(Central Processing Unit)の演算を補助して高速演算処理を行うコプロセッサを開発し，ICカード用LSIチップに内蔵した。これにより，多倍長の整数演算を利用した暗号処理をユーザーがソフトウェアで実現できるようになった。

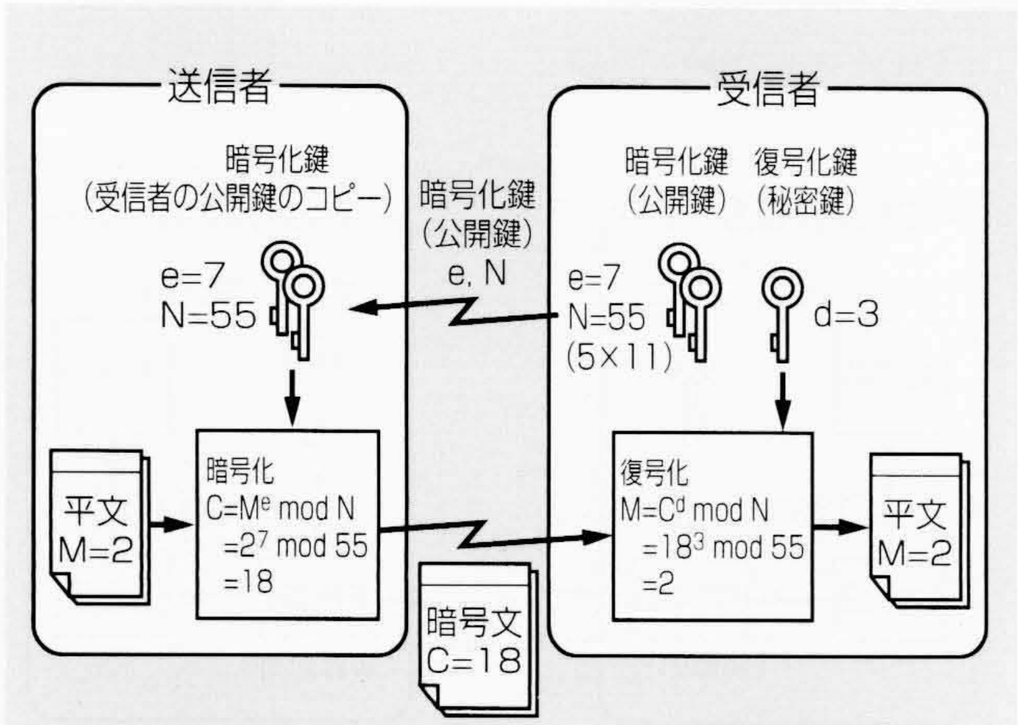


図4　RSA暗号方式と演算例
公開鍵を用いて暗号化された暗号文Cは，復号用の秘密鍵を持つ受信者だけが復号化できる。

4．ICカード用マイクロプロセッサのLSI設計技術

日立製作所は，1986年にICカード用としてEEPROMを内蔵した初めてのマイクロプロセッサ“HD65901”を開発した。この製品のEEPROMは2kバイトであった。ICカード用途の多様化，情報量の増加に伴って大きな容量のメモリの必要性が高まり，1989年には日立製作所オリジナルCPUである“H8”を核に，大容量の8kバイトEEPROMを内蔵したH8/310シリーズを世界で初めて製品化した。現在，8kバイトはICカードの標準EEPROMサイズになっている。1995年にはチップサイズ18 mm^2に高機能を集積し，GSM仕様の3V動作にも対応可能なH8/3102を開発した[5]。各マイクロプロセッサの機能一覧を**表1**に示す。

これらのマイクロプロセッサの開発を行ううえでの主

表1　H8/310シリーズの仕様一覧

従来製品ではメモリ展開品だけのラインアップであったが，今回金融市場向けコプロセッサ オン チップ品をラインアップした。

製品名		H8/310, H8/3101	H8/3102	H8/3103	H8/3111
CPU		H8/300CPU			
メモリ	EEPROM	8kバイト	8kバイト	16kバイト	8kバイト
	マスクROM	10kバイト	16kバイト	20kバイト	14kバイト
	RAM	256バイト	512バイト	512バイト	800バイト
I/Oポート		2	2	2	2
コプロセッサ		———	———	———	搭載
動作電圧，動作周波数		5.0 V(10 MHz)	5.0 V(10 MHz) 3.0 V(5 MHz)	5.0 V(10 MHz) 3.0 V(5 MHz)	5.0 V(10 MHz) 3.0 V(5 MHz)
消費電流	動作中	20 mA (10 MHz, 5 V)	20 mA (10 MHz, 5 V)	20 mA (10 MHz, 5 V)	20 mA (特殊モード時)
	スリープ時	最大100 μA*	最大100 μA	最大100 μA	最大100 μA
パッケージ		COB，ウェーハ，チップ，SOP-10	COB，ウェーハ，SOP-10	COB，ウェーハ	COB，ウェーハ

注：略語説明など　ROM(Read-Only Memory)，RAM(Random Access Memory)，I/O(Input-Output)
COB(Chip on Board)，SOP(Small Outline Package)
＊(H8/310はスリープモードなし)

な要素技術は次のとおりである。

(1)　不揮発性メモリEEPROMプロセス技術
(2)　低電圧，低消費電力回路技術
(3)　サブミクロンプロセス技術
(4)　セキュリティ技術

なお，セキュリティ技術は，内蔵メモリの不正読み出し，情報改ざん，またはチップそのものの偽造などを防止する技術である。暗号処理に適したコプロセッサの内蔵もこの一つであり，詳細は省略するが，LSI技術でもさまざまなくふうを凝らしている。

ここでは，3章で述べた暗号処理の高速化を可能にするコプロセッサを内蔵し，電子マネー用に適した新しいマイクロプロセッサ“H8/3111”のLSI設計技術について述べる。

4.1　EEPROMのプロセス技術

日立製作所のEEPROM素子はMONOS(Metal-Oxide Nitride-Oxide Silicon)型と呼ばれ，一般に採用されているフローティングゲート型EEPROM素子とは異なる独自のサンドイッチ構造をしている。MONOS型EEPROM素子の断面構造を**図5**に示す。ナイトライド膜とトンネル酸化膜との界面に電子あるいは正孔を捕獲し，メモリMOSトランジスタのしきい値電圧を変化させることによってデータ“0”，“1”を保持する。

MONOS型EEPROMの特長は，電子がナイトライド膜と酸化膜との界面に存在するトラップ準位に捕獲されるために，データの保持特性に優れ，書き換え回数の劣化が少ないことである。また，このメモリ素子はこれらの特性を維持しながら，サイズを比例縮小できる。これはチップサイズを小さくすることが信頼性などに影響するICカードに最適なEEPROM技術であり，将来の0.35ミクロンプロセスにも適用できる技術である。

4.2　低電圧，低消費電力回路技術

新しいGSM仕様(Version11.12)では，3V動作が義務づけられている。今後のGSM用カードだけでなく，電子マネーカードでも携帯用電子財布など電池駆動の機器でICカードを使うことも多くなる。できる限り低い電圧で動作することが必須の技術である。EEPROM回路の消費電力低減について例をあげると，一般の単体EEPROMメモリでは読み出し回路に差動型を使用してお

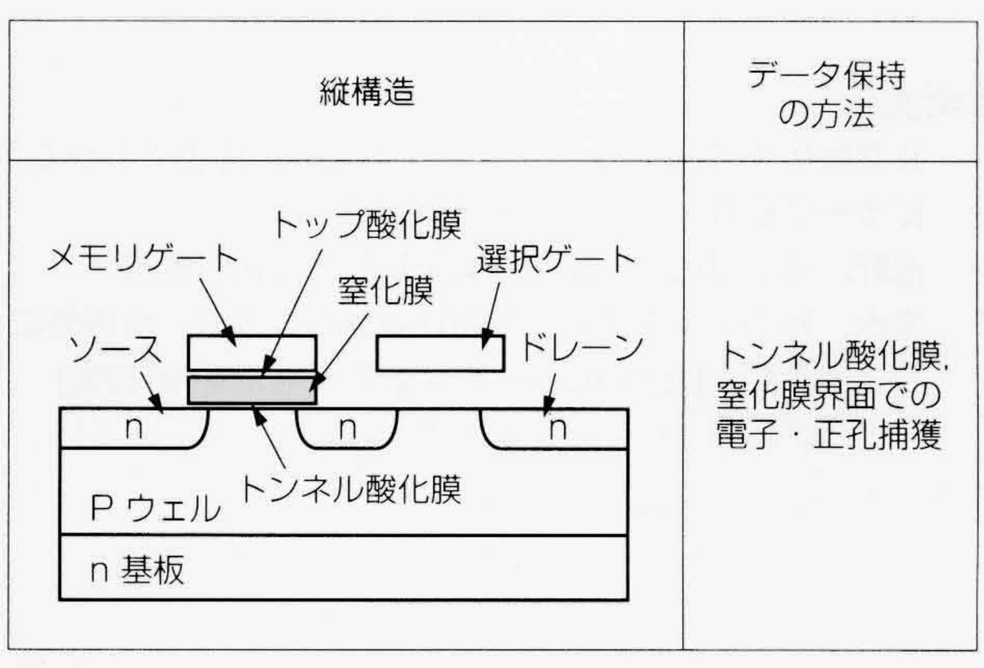


図5　MONOS型EEPROM素子の縦構造

日立製作所独自のMONOS型EEPROM素子は，データ保持や書き換え回数の特性に優れる。

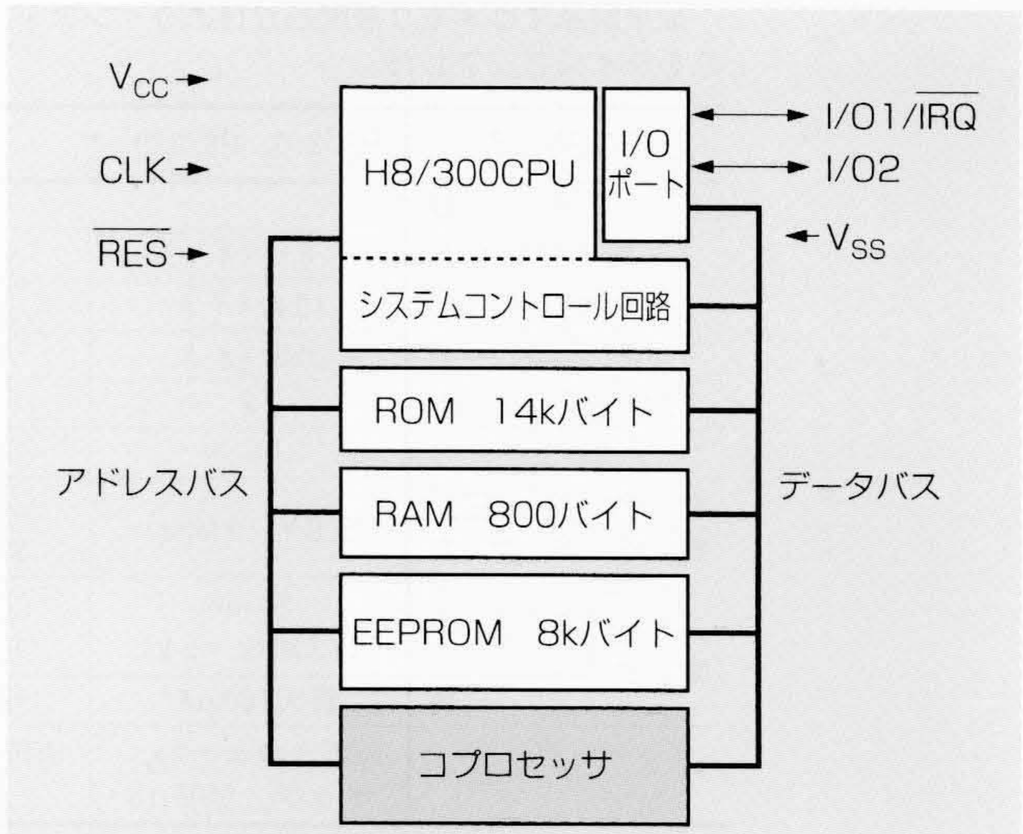
り，高速動作が可能な反面，数十ミリアンペアの定常電流が流れ，ICカード用には適さない。そこで，読み出し回路に電圧センス方式のCMOS(Complementary Metal-Oxide Semiconductor)帰還型回路を採用し，低電圧動作域でも確実に動作する回路設計技術を採用している。

さらにH8/3111では，暗号処理に適したコプロセッサを内蔵するにあたり，制御用メインCPUと時分割で実行する動作モードを設け，消費電力の増加を抑えるくふうをしている。

4.3 サブミクロンプロセス技術

ICカードの形状や曲げ強度についてはISOで規定されており，チップの機械的強度を考えると，チップサイズを小さくすることがこの規定を満足する一つの手段である。一般にそのサイズは25 mm^2以下と言われているが，暗号用プロセッサや多くの機能，大きなメモリサイズを内蔵しながら，できるだけ小さくまとめることが必要である。H8/3111では，0.8ミクロンプロセスを採用して19 mm^2を実現した。今後さらに0.5ミクロン，0.35ミクロンといった微細加工プロセス技術の改良を進めていく。

以上3章，4章で述べてきた設計技術を結集して電子マネーに最適なH8/3111を1996年に開発し製品化した。H8/3111の機能ブロック図を**図6**に示す。



注：略語説明
V_{CC}, V_{SS}(電源), CLK(Clock；クロック)
RES(Reset；リセット), I/O(Input/Output；入出力)
IRQ(Interrupt Request；割込み要求)

図6 H8/3111の機能ブロック図
H8/3111では，高いセキュリティ性を実現するために暗号処理用コプロセッサを内蔵し，外部端子も極力少なくした。

5. おわりに

ここでは，電子マネーに使用されるICカード用マイクロプロセッサの設計技術について主に述べた。

ICカードはわれわれの経済生活を大きく変える可能性を秘めている。それは従来の「お金」の価値観を変え，世界で共通に使える「マネー」というものに変えていくきっかけになるものである。ICカードの普及のために解決すべき課題はまだ多くあるが，さまざまな試みの中で，それはいずれ解決されていくと考える。このためには，ネットワークや端末機器のインフラストラクチャーのいっそうの充実はもちろんのこと，ICカードに使われるマイクロプロセッサの進化が不可欠である。

日立製作所は，このICカードの心臓部である，小さくて高機能を実現するマイクロプロセッサチップの技術開発を進めるとともに，システムにすぐに組み込めるソフトウェアの内蔵，新しい不揮発性メモリの導入などによって，「より使いやすく，より便利に，より安心な」ICカード用マイクロプロセッサを開発していく考えである。

参考文献

1) 日立製作所 新金融システム推進本部：図解よくわかる電子マネー，日刊工業新聞社(1996)
2) ICカード総覧，シーメディア(1995)
3) 池野，外：現代暗号理論，電子通信学会編(1986)
4) 宝木，外：マルチメディア向け高速暗号方式，情報処理学会，マルチメディア通信と分散処理研究会(1989-1)
5) 日立製作所：H8/3102ハードウェアマニュアル(1995)