ICカード応用とシステムLSI技術
Application of IC Cards and System LSI Technology

小田　広志
ODA Hiroshi

今から約20年前に，ビザ・インターナショナルがクレジットカードをICカードにする構想を打ち出した。そのねらいは言うまでもなく，カード普及に伴う偽造，不正利用での損害額を抑えることにあった。 日本では近年，ようやく“ セキュリティ ”に対する関心が高まってきているが，欧米諸国では十数年前から，製品に対するセキュリティ認証やセキュリティ評価にビジネスとして取り組んでいる企業があり，セキュリティ性を要求されるICカードはその対象とされてきた。更に拍車をかけているのが，ネットビジネス時代の到来である。このような環境のなかで，ICカード技術はいろいろな分野で応用され，進化している。

Visa International proposed a design for making credit cards into integrated circuit (IC) cards about 20 years ago. The purpose of such a change is to minimize damage due to forgery and unauthorized use accompanying the wide dissemination of credit cards. Increasing attention is now being paid to security in Japan, although companies in other countries already began to enter the business of security authentication and evaluation about 10 years ago with a focus on the secure characteristics of IC cards. The arrival of the network business era has further accelerated this trend. As a result, IC card technology is being applied in a variety of fields and has evolved accordingly.

1 まえがき

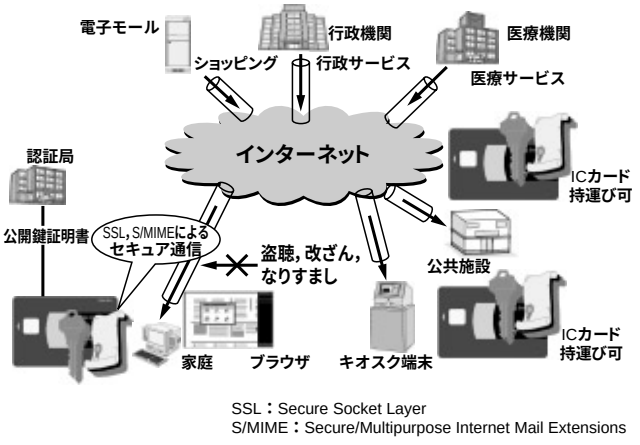
今，ICカードを利用した代表的なものといえば，携帯電話用SIM（Subscriber Identity Module：電話加入者識別モジュール）カード，電話用プリペイドカード，交通カード，金融カードなどが挙げられる。そして今後，新たな分野でよりセキュアなICカード利用が進んでいく。

その理由の一つには，インターネット環境における情報セキュリティ強化目的でのICカード利用があり，そこにICカードが持つ“ セキュリティ機能 ”や“ ID（IDentification）機能 ”が要求されるからである（図1）。

2 ICカードの分類

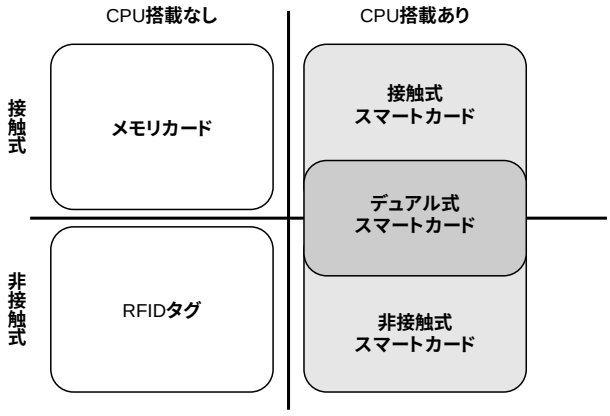
一般にICカードと呼ばれるもので，特にCPUを搭載したものを区別する意味でスマートカードと称している（図2）。

また別な観点から，リーダ・ライタとのデータのやり取りを接触式あるいは非接触式のいずれかの手段で行うかにより，接触式ICカード，非接触式ICカード及びその両方の機能



SSL：Secure Socket Layer
S/MIME：Secure/Multipurpose Internet Mail Extensions

図1．インターネット環境におけるICカード利用　インターネット環境においてセキュリティ性を高めるために，個人認証やデータの暗号化目的でICカードの利用が高まってきている。
Use of IC cards in Internet environment



RFID：Radio Frequency IDentification

図2．ICカードの分類　一般にICカードと呼ばれているものは，CPU搭載の有無やデータ通信方法などにより分類される。
Classification of IC cards

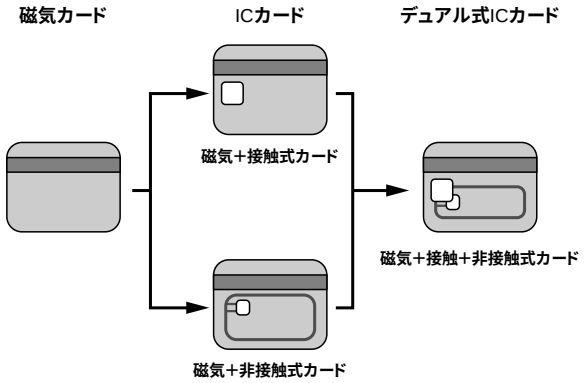


図3．ICカード進化のイメージ　従来の磁気カードからICカードへ移行する際，用途に応じて接触式あるいは非接触式カードでの運用が考えられる。将来はカード統合でのデュアル式カードへ移行するとの見かたもある。
Image of IC card evolution

を兼ね備えたデュアル式ICカードに分類される。

図3は，ICカードの進化をイメージしたものである。磁気カードからICカードへの移行期には，用途に応じて接触式と非接触式の2種類のカードが普及するが，様々な種類のカードを統合する動きから，将来はデュアル式ICカードへと移り変わっていくという見かたもある。

（注1）　Java及びその他のJavaを含む商標は，米国SunMicrosystems社の商標。
（注2）　米国ザイログ社の商標。

3 システム動向

ICカードシステムの特長の一つに，不揮発性メモリを搭載していることが挙げられる。用途に応じてそのメモリ容量は異なるが，この1～2年で飛躍的に大容量化が進んでいる。

その理由の一つとして，今年から日本で先駆けて実用化された次世代携帯電話サービスの普及が挙げられる。

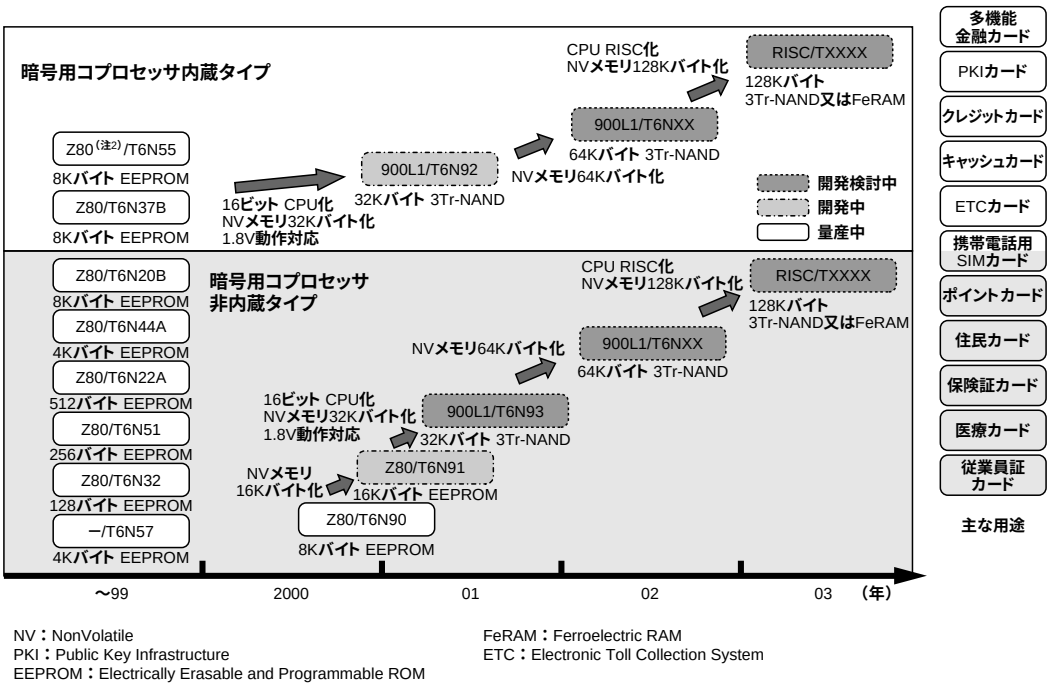
将来，ICカードは多様化するサービスを意識し，従来の通信速度をより高速化して大量の情報を蓄えることが容易となり，また，Java(注1)カードのような多目的用途に使えるオープンプラットフォームの実用化に期待が持たれている。

それらの商品に使用されるスマートカードは，従来の8Kバイト，16Kバイトの不揮発性メモリを搭載した製品から32Kバイト，64Kバイト製品へ移行しており，この先1～2年後には128Kバイト以上の不揮発性メモリを搭載した製品化が予想される。

図4及び図5は，当社の接触式スマートカード用LSIと非接触式ICカード用LSIの製品トレンドである。

4 システム要素技術

スマートカード用LSIシステムの基本構成は，CPU，不揮発性メモリ，プログラムROM，データRAMのほかに暗号処理



NV：NonVolatile
PKI：Public Key Infrastructure
EEPROM：Electrically Erasable and Programmable ROM
FeRAM：Ferroelectric RAM
ETC：Electronic Toll Collection System

図4．当社における接触式スマートカード製品トレンド　次世代携帯電話サービスに伴ない，ICカードが搭載されるなど，将来に向けてより情報データの増大化，高速処理化への要求が強まってきている。それに使用されるLSIも大容量不揮発性メモリーや高速処理可能なCPUが要求される。
Trend in Toshiba contact type smart card products

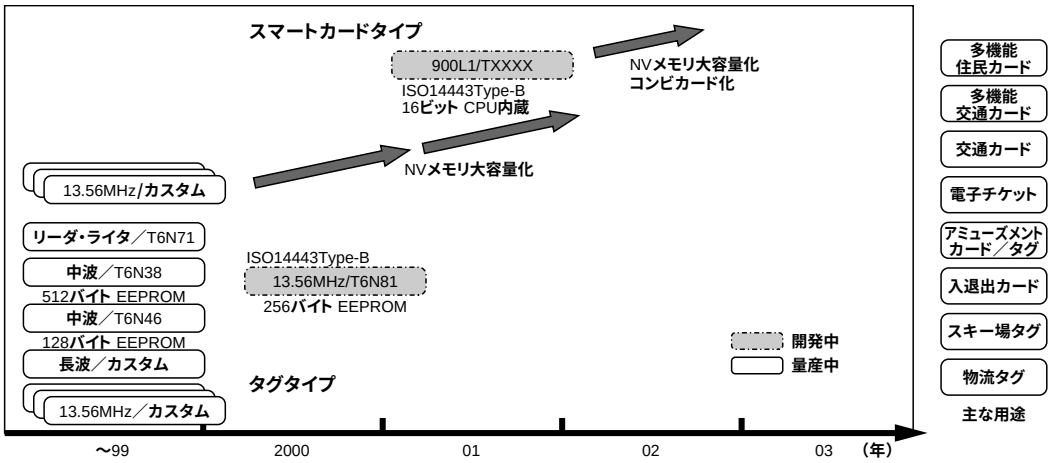


図5．当社における非接触式ICカード製品トレンド　接触式カード同様，高機能化への移行が予想される。
Trend in Toshiba noncontact type IC card products

回路としてDES（Data Encryption Standard）やコプロセッサを必要に応じて搭載している。

また，耐タンパ（tamper：不正行為）技術においては回路，レイアウト，プロセスなどで対策を講じている。

なお，接触式と非接触式で大きく異なるところはデータの送受信回路で，前者はシリアル入出力ポート，後者は無線アナログ回路を搭載している。接触式スマートカードにおいて，次世代携帯電話用SIMカードやJavaカードの普及に合わせて，製品の高機能化が進んでいる。

そういった状況下において，半導体メーカーの課題は高機能化実現と相反し，既にISO（国際標準化機構）／IEC（国際電気標準会議）7816で決められている接触式スマートカードやICモジュールのサイズから，そこに搭載されるLSIチップのサイズは一般的に最大5×4mmに抑える必要がある。

これによって，半導体メーカー各社はその実現に向けてより微細化プロセスを採用し，一定のチップサイズで高機能化を実現するために研究・開発を進めている。

もちろん，プロセスだけでなく，システム回路の縮小化も併せて検討を進めている。

ここでは，進化するICカードに対し，半導体システム技術をどのように実現していくかについて述べる。

4.1　不揮発性メモリ技術

当社では，大容量化が進むなかチップサイズを抑えるためにNAND（Negative AND circuit）型フラッシュメモリ技術をベースにセルサイズを小さくした独自の3Transistor（Tr）-NANDメモリを開発し，32Kバイト以上の不揮発性メモリとして採用している。

図6は，当社における3Tr-NANDメモリと他メモリセルサイズとの比較であり，**図7**はこれらの不揮発性メモリ技術導入でのプロセストレンドである。

不揮発性メモリ大容量化での課題は，LSIのチップ占有率の高い不揮発性メモリ回路をいかに小さく，かつ安価なものにするかであり，各半導体メーカーの手腕にかかっている。言いかえれば，容量に応じた適正な不揮発性メモリ技術の選択が鍵（かぎ）となる。

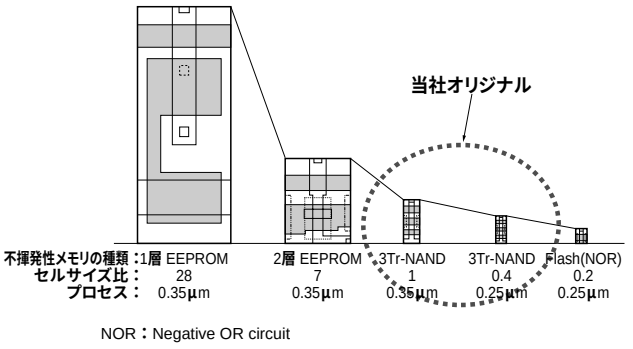


図6．不揮発性メモリサイズ比較（当社比）　NAND型フラッシュメモリ技術をベースに，ICカード用メモリとして従来のEEPROMと比較してセルサイズの縮小を実現した。
Comparison of nonvolatile memory size（ratio of Toshiba）

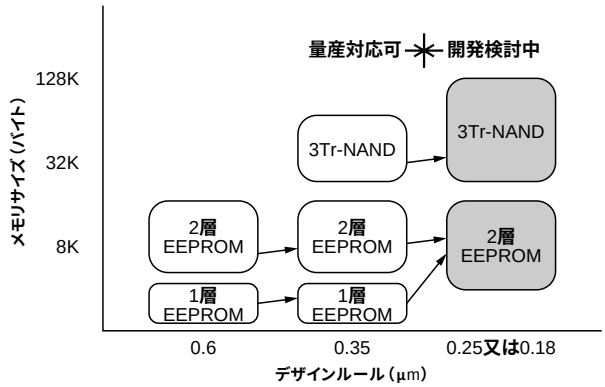


図7．各種不揮発性メモリでの微細化プロセストレンド　各種不揮発性メモリで将来の大容量メモリ化に対応するために，微細化プロセスの開発を進めている。
Trend in finer processes for various nonvolatile memories

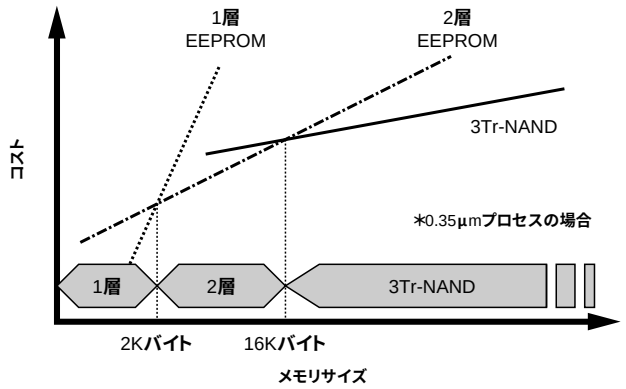


図8．不揮発性メモリサイズに応じたメモリ技術採用イメージ　メモリサイズ及び各種メモリ技術でのコストのクロスポイントを見極め，最適なメモリ技術を選択することで全体のコストが抑えられる。
Image of technologies adopted according to nonvolatile memory size

不揮発性メモリサイズに応じたメモリ技術採用のイメージを図8に示す。

4.2　CPUの選択

ICカードの多様化により，今後，様々なアプリケーションのダウンロードが容易となるJavaカードでは，より高速処理可能なCPUが必要になってくる。

既に半導体メーカー各社は，縮小命令セットコンピュータ（RISC）CPU搭載製品の開発を行っており，今後の多機能カードへの採用が期待されている。当社のスマートカードに搭載されるCPUのトレンドを図9に示す。

4.3　セキュリティ技術

ICカードシステムの特長の一つとして，情報の機密性を高め，外部からの物理的不正アクセスを防ぐための暗号処理回路や耐タンパ回路の搭載が挙げられる。

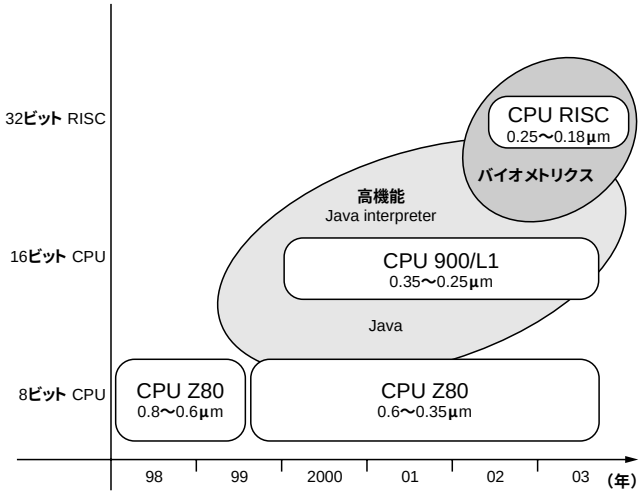


図9．スマートカード搭載CPUトレンド　ICカード用に搭載されるCPUは，情報データの大容量化に伴い高速処理可能なRISC系に移行している。
Trend in smart card CPUs

暗号方式には共通鍵暗号と呼ばれるDES，Triple-DES，AES（Advanced Encryption Standard）や，公開鍵暗号と呼ばれ世の中で広く使われているRSA（Rivest-Samir-Adleman：この方式を発明した3人の頭文字をとって称している），楕円（だえん）曲線暗号などの方式があり，それらはスマートカード用LSIの中のハードウェア及びソフトウェアの協調により実装されている。

なお，ハードウェアとしての処理エンジンはコプロセッサであり，この回路の処理能力で暗号処理速度が決まる。

より高速化を図るため，外部からの供給クロックに対し，内部で周波数逓倍回路を設けている。

また，一般的には暗号鍵長を長くすれば，より情報の機密性は高くなるが，前述のコプロセッサの処理負担が大きくなり処理速度が遅くなる。こうした問題を克服しようと，各社では新たな暗号処理の開発も進められている。

耐タンパについては，一般的に次のような工夫が施されている。

(1)　セキュリティセンサ
　(a)　高，低電圧検知
　(b)　高，低周波数検知
　(c)　高，低温度検知
(2)　不法アドレスアクセス検知
(3)　イオンインプラROM
(4)　多層メタル配線
(5)　微細プロセス
(6)　その他

5　あとがき

海外においては携帯電話をはじめ，金融，交通などの分野でICカードが広く使われているが，国内においても昨年から今年にかけて，これらの分野でICカードの利用が広がってきている。

情報ネットワーク時代におけるセキュリティ技術基盤として，ICカードを利用したシステムがこれからもいろいろな分野で考えられている。

今後も，様々な用途に安心して使えるICカード用として，よりセキュリティ性の高いコンパクトなシステムの開発，製品化に努めていきたい。

小田　広志　ODA Hiroshi
セミコンダクター社 システムLSI事業部 システムLSI統括第一部参事。ICカード用LSI開発業務に従事。
System LSI Div.