ICカード用LSIの技術動向と今後の課題

Technical Trends in IC Card LSIs and Issues Requiring Future Solutions

長谷部　信一
S. Hasebe

ICカードは，海外では1980年代から使用されてきたが，ここにきて全世界的に普及するきざしを見せはじめている。当社でもICカードの開発を80年代から手掛けている。

ここでは特にICカードに使用されるLSIを中心に，ICカード用LSI製品のラインアップ，プロセス，LSIのセキュリティ技術，サイト（カードの製造工場）セキュリティについて取り上げる。これからの課題としては，製品のラインアップ面では，現状の8ビットCPUを内蔵した製品以外に，ハードウェアの機種依存性をなくすためにJavaCard(注1)カードに対応できる製品の開発が必要である。プロセスの面では，より高機能なLSIとするために，シュリンク（縮小化）を進める必要がある。セキュリティ技術の面では，偽造防止のために周波数検知回路，温度検知回路，電圧検知回路を内蔵し，アタッカ（不正な解析者）の技術より一歩進んだ改ざん，偽造を防ぐ耐タンパ回路を取り入れる必要がある。

IC cards have been in use in various countries since the 1980s, and will soon be diffused worldwide. Toshiba has been developing IC cards since the 1980s.

This paper describes our IC card LSI lineup and processes, LSI security technologies, and site security. With regard to the LSI lineup, although the 8-bit CPU is currently used, LSIs that can be used for a JavaCard must also be rapidly developed. In connection with processes, chip shrinkage technology must be introduced to realize higher performance. And in the realm of security, frequency detection, temperature detection and voltage detection need to be implemented in IC card LSIs.

1 まえがき

ICカードは80年代に，欧州，特にフランスでテレホンカードとして使用されたのが最初である。これに使用されたLSIにはCPUなどのコントローラは搭載されず，不揮発性メモリ(注2)と書込み・読出し回路を1チップ化した単純なものであった。日本では，テレホンカードに磁気ストライプのものが導入され，それによるインフラが整備されたため，ICカードタイプのテレホンカードの普及が遅れた。しかし，磁気ストライプのカードでは特別な方法によりデータが視認でき，偽造などの被害が発生したため，また海外でのICカードの発展もあり，ICカードへ切り換える動きが出てきた。

2 ICカード用LSIの動向

2.1 製品のラインアップ

ICカードにはデータをリーダライタと端子を接触させてやり取りする接触式カードと，非接触でデータをやり取りする非接触式カードがある。非接触式カードは仕様が各社各様であるために，現在LSIは主にカスタム用として開発している。ここでは，仕様が明確になっている接触式カードについて述べる。

ICカードの用途は，大きく三つに分類できる。それに対応する当社のLSIを示したのが**表1**である。ローエンドモデルは単純なポイントカードであり，使用する不揮発性メモリ容量も少なくて済むものである。

ハイエンドクラスは，主に金融，バンキング，保険証などメモリ容量がより大きく，またセキュリティも最高のものが要求される。ミドルクラスは，この両者の中間に位置するものである。

表1．ICカードの用途と当社LSI対応
IC card applications and corresponding Toshiba LSIs

用　途	当社LSI
[ハイエンドクラス] 銀行（キャッシュカード），ECカード， 健康カード（病院の診療記録など）	T6N29A その他，新製品開発中
[ミドルクラス] IDカード	T6N20A，T6N24 その他，新製品開発中
[ローエンドクラス] テレホンカード，ポイントカード	T6N32，T6N22A その他，新製品開発中

EC：Electronic Commerce（電子商取引），ID：Identification Data

（注1）　JavaCardは，米国Sun Microsystems社の商標。
（注2）　EEPROM (Electrically Erasable and Programable ROM) およびFRAM (Ferroelectric RAM)。

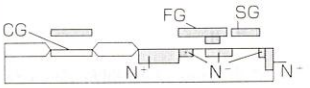
当社のICカード用LSIは，基本的に8ビットCPUをコントローラとして，その周りに不揮発性メモリ，システム全体をコントロールするプログラムを内蔵するマスクROM，途中計算結果などを保存するRAMを配置した構成にしてある。その他，ハイエンドクラスでは暗号を使用してデータの改ざんなどを防ぐ必要があり，そのためのコプロセッサを内蔵している。現在では，公開鍵(かぎ)暗号方式が使用される可能性が高く，この暗号データが1,024ビットと演算量が大きく，ソフトウェア的に処理すると時間がかかりすぎるため，専用の計算回路を内蔵している。また，偽造対策としては，耐タンパ(tamper resistance)回路を内蔵している。現在，世界的にCPUは，インテル系8051の改良品と，モトローラ系6805の2種類が使用されている。当社は前者に近いZ80(注3)をCPUとして採用している。これは，Z80がかなり知名度があり，開発用ツールなどが豊富にあるためと，CPUのコアサイズが比較的小さいために採用した。よく知られているように，CPUをコアにすると解析されやすいのではないかとの懸念については，簡単には偽造できないように対策してあるので偽造はほぼ不可能となっている。

システム動向としては，現在，各社ごとに異なるLSIを使用するときに，開発環境をそのたびに変更する必要がでてくるが，このような不都合をなくすために，開発言語としてJava(注4)を使用するようになると考えられる。Javaのアプレットと言われるプログラムをICカードに乗せて動作させるが，これは中間言語であり，カードはそのアプレットを解釈しながら動作する必要があるので，そのために必要な処理能力はより高いものとなる。これに対して8ビットCPUでは困難であり，16ビット，32ビットCPUを使用したシステムに移行すると考えられる。

2.2 LSIプロセス技術

現在，当社では最新のCMOS，プロセスルール0.6 μm一層ポリシリコンEEPROMまたは，プロセスルール0.6 μm二層ポリシリコンEEPROMで量産対応している。図1に一層ポリシリコンEEPROM，図2に二層ポリシリコンEEPROMの断面構造を示す。一層ポリシリコンEEPROMは電荷を保持するフローテングゲートを一層ポリシリコンにより形成したもので，二層ポリシリコンで形成したものに比べてプロセスが簡単になる。しかし，メモリセル自体は大きくなるため，不揮発性メモリの容量が4Kバイト以下のものに使用する。二層ポリシリコンEEPROMではメモリセルを最適に構成することができるが，一層ポリシリコンEEPROMよりもプロセスが複雑になるため，コストアップになり，チップサイズを小さくする要求が強い4Kバイト以上のものに使用する。

(注3) Z80は，米国ザイログ社の商標。
(注4) Javaは，米国Sun Microsystems社の商標。

プロセスルール		0.6 μm
構造		
電圧(V_{PP})		5～1.8 V (20 V)
ゲート酸化膜膜厚	トンネル酸化膜	90 Å
	高耐圧トランジスタのゲート酸化膜	400 Å
トンネル領域		1.2×1.0 μm^2
セルサイズ		129 μm^2
スレッショルド電圧	消去時	＞0(注入) V
	ライト時	＜−3.0 V
書込みセル電流		＞40 μA

CG : Control Gate　SG : Select Gate
FG : Floating Gate　N : Negative Layer

図1．一層ポリシリコンEEPROMセル構造　二層ポリシリコンで形成したものに比べて，プロセスが簡単になる。
Structure of 1Poly EEPROM cell

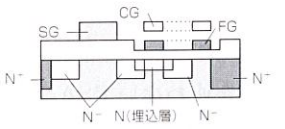
プロセスルール		0.6 μm
構造		
電圧(V_{PP})		3—5 V (20 V)
ゲート酸化膜膜厚	トンネル酸化膜	90 Å
	高耐圧トランジスタのゲート酸化膜	400 Å
	酸化膜・窒化膜	250 Å
トンネル領域		1.0×0.6 μm^2
セルサイズ		36 μm^2
スレッショルド電圧	消去時	＞0(注入) V
	ライト時	＜−3.0 V
書込みセル電流		＞50 μA

図2．二層ポリシリコンEEPROMの構造　一層ポリシリコンで形成したものに比べ，プロセスが複雑になるためコストアップになる。しかし，メモリ容量が大きくできるので4Kバイト以上に使用される。
Structure of 2Poly EEPROM cell

EEPROMに要求される性能としてエンジュランスとリテンション性能がある。エンジュランスはEEPROMに何回データを書込み・読出しをしても問題ないかを示す性能であり，EEPROMでは10^5回が現在世界の標準である。また，リテンションは書き込んだデータが＋85°Cで何年消去されないで保持されるかを示す能力であり，現在の世界標準は10年である。これらの値は，今後ますます大きく，また長くなっていくものと考えられる。さらにLSIに要求される項目としては，チップの厚みがある。カードにLSIを内蔵するためには，薄いチップが使用者からみれば好ましいのであるが，チップが薄くなればなるほど割れやすくなるので，現在は250 μmで対応している。非接触カードの場合に

は，チップが完全にカードに入ってしまうために，チップ厚は100 μm以下にする必要がある。また，将来的には50 μm以下にする必要がでてくるものと推測される。カードには，持ち歩くためにいつも応力がかかるが，この応力がかかってもチップが割れないためには，経験上，チップ面積は25 mm²以下でなくてはならない。高機能化のために素子数増加，チップ面積が増える要因はあるものの減る要因は何もない状況において，今後は，よりいっそうのチップサイズのシュリンクを進めるとともに，チップ面積を縮小させるために，3層アルミ配線により配線エリアを縮小する必要がある。

2.3 LSIのセキュリテイ技術

2.3.1 LSI暗号技術　暗号では，これまで20年以上使用されてきた秘密鍵暗号方式のDES (Data Encryption Standard) に代わり，公開鍵暗号方式が採用されようとしている。この場合，暗号の強度の関係で512～1,024ビット長の鍵が使用されるが，この鍵の生成などを純粋にソフトウェア処理すると，カード内部の8ビットマイコンでは処理時間が膨大なものとなるために，時間短縮のために専用の計算器を搭載する必要がある。この計算器の性能は，現在，512ビットのCRT(注5)(Chinese Remainder Theorem：中国人剰余定理) を使わないRSA signature(注6)の処理時間で比較される。この処理時間は，平均で約200 msとなっている (標準化比較条件：512ビット，RSA signature without CRT)。

今後，より暗号強度を高くするためには，鍵長をもっと長くする必要があり，2,048ビット程度まで伸びるものと推測される。また，現在のものより10倍程度処理速度を向上させるために，方式自体の変更も検討する必要がある。IC自体は98年に現状の4倍に高速化する予定である。ただし，ビット数を大きくせずに，暗号強度を高くすることができ，かつその方式が特許取得されていなければ，それが望ましく，その辺について各社検討を進めている。当社では，システム対応も含めて，99年には現状の16倍の高速化対応をする予定である。

2.3.2 耐タンパ技術　現在，開発中のLSIは，磁気カードで発生したような偽造問題が発生しないように耐タンパ回路を内蔵している。耐タンパとはアタッカがLSIを解析し，その動作を解析して，中のデータを改ざん，偽造することを防止する回路，しくみのことで，銀行，クレジットカード用LSIはこのタンパ回路を内蔵していないと採用されない。耐タンパ回路について，さまざまな論文が発表されているが，ここまで実施すればタンパ回路はパーフェクトであるといったことはなく，アタッカの技術の進歩に合わせて，一歩先を進んでいる必要がある。LSIとしても，日進月歩のこのタンパ技術に対応していく必要がある。

タンパ回路の例としては，①周波数検知回路，②温度検知回路，③電源検知回路などがある。周波数検知回路については，アタッカがCPUへのクロックを1命令ごと入れながら解析する手法をとることが考えられ，この解析を防ぐために低周波検知回路を内蔵している。また，LSIはどんな温度でも動作するというわけではなく，必ず最適な動作温度というものが存在する。この動作温度外になったときに動作が保証できなくなるため，温度検知回路を設け，規格温度外ではLSIの動作を停止させる。同様に規格電圧以外の電圧を印加して動作が不安定になることを防止するために，電源電圧のモニタ回路を内蔵させている。これにより，正常以外の電圧ではLSIは動作しないようにしてある。

以上のような回路のほかに，配線スクランブルがある。アタッカが少しでも解析に手間取るようにアドレスライン，バスラインにスクランブルをかける。また，あるビットは1層目，他のビットは2層目といったように縦方向でもランダムにスクランブルをかけると，解析の困難度が上がる。かつ，耐タンパ性向上のため配線はできるだけ短く，各ブロックを詰めて配置する必要がある。

今後，耐タンパ性能は，先ほども述べたように日進月歩で進化するために，つねに情報を集めてLSIにフィードバックする予定である。

2.4 サイトセキュリティ

ICカード用LSIでは，LSI自体のセキュリティが必要なのはもちろんのこと，LSIを量産する工場のセキュリティも必要である。製造している場所に誰でも自由に入れるようでは論外であり，LSIの途中工程にあるものも，作業終了後は金庫に保管して計数，チェックをする必要がある。不良品も解析の材料にならないとも限らないので破砕し，その証拠を残しておく必要がある。構内，工程にはCCTV (Closed-Circuit TeleVision) などで24時間，監視する必要がある。製品の輸送も厳重にすることが必要で，金融カード用LSIには，金融機関などの現金輸送車と同等なセキュリティ管理が必要である。

3 あとがき

ICカード用LSIとして現状の概要，今後の動向についてまとめた。ICカードがまさにビジネスとして立ち上がろうとしている。このビジネスチャンスに乗れるように市場からの仕様・セキュリティ要求を適宜取捨選択して，関連部門と連携を取りながら，迅速に対応していきたい。

(注5)　余り (剰余) 演算を高速で行うアルゴリズムの一種。
(注6)　公開鍵暗号方式の一種。

長谷部　信一　Shin'ichi Hasebe

半導体システム技術センター 映像情報システムLSI第一技術部主務。
ICカード用LSIの開発に従事。
Semiconductor System Engineering Center