

高いセキュリティ機能を持つ通信機用ICカード

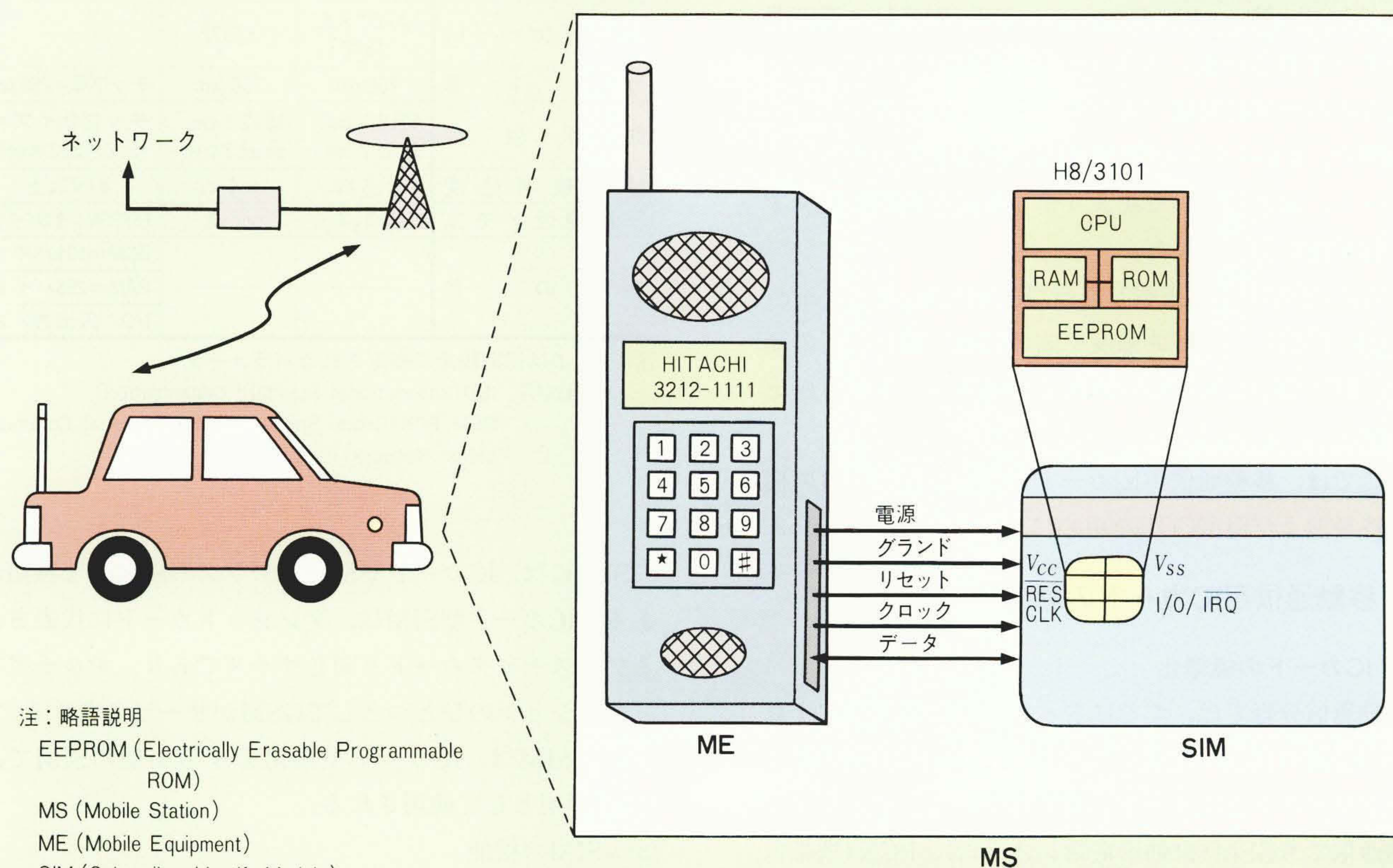
Microcomputers with High Security for Telecommunication Systems

佐藤恒夫* Tsuneo Satō

川下智恵* Norishige Kawashimo

山浦 忠* Tadashi Yamaura

竹島雅彦* Masahiko Takeshima



移動通信のシステム構成 ICカードを用いた移動通信システムの構成は、ハンディ機器とICカードから成る。

マイクロコンピュータ(以下、マイコンと略す。)内蔵のICカードは、高いセキュリティや大容量メモリを必要とする銀行カード、電話カード、IDカードなど多種多様なアプリケーションで採用されている。

さらに、移動通信用ICカードでは、携帯性やバッテリー駆動のため、低消費電力モードを備えた高性能マイコンが要求されている。

日立製作所は、大容量EEPROM(Electrically Erasable Programmable ROM)、低消費電力モード、高いセキュリティを特長としたHシリーズマイコンH8/3101を開発し、量産している。

さらに、高信頼度のICカード用薄型COB(Chip On Board)を開発し、実装技術での顧客ニーズにも対応している。

* 日立製作所 半導体事業部

1 はじめに

ヨーロッパを中心としたGSM(Group Special Mobile), PCN(Personal Communication Network)およびDECT(Digital European Cordless Telecommunication)の各移動通信システムでは、マイクロコンピュータ(以下、マイコンと略す。)内蔵ICカードの採用が決まり標準化が進められている。これらのシステムでは、大容量EEPROM(Electrically Erasable Programmable ROM)、低消費電力モードおよび高いセキュリティが要求されている。これらのニーズに対応するため、H8シリーズマイコンの展開で、8kバイトのEEPROM、低消費電力のスリープモード、および高いセキュリティ機能を内蔵したマイコンH8/3101を開発した。

さらに、H8/3101を搭載した薄型COB(Chip On Board)を開発・量産し、機械的強度や曲げ強度に強いなどの高い信頼度を実現して、実装技術での顧客ニーズにも対応している。

ここでは、移動通信用ICカードの動向、H8/3101の機能・特長および薄型COBを中心に述べる。

2 移動通信用ICカードの動向

2.1 ICカードの標準化

移動通信分野では、すでにドイツでのC-NET(アナログ移動通信の自動車電話システム)で、EEPROM内蔵1チップマイコンをICカードに採用している。デジタル移動通信でもGSM(自動車電話システム)、PCN(携帯電話システム)、DECT(コードレス電話システム)でICカードの採用を決めており、標準化が進められている。

ICカードは、ISO(International Standard Organization)規格、IS7816で標準化が進められ、移動通信用ICカードの規格もこれに基づいている。移動通信のICカードに関しては、ETSI(European Telecommunication Standards Institute)が積極的にGSM、PCN、DECTの規格を決めており、これらの規格は類似している。ICカードの規格と日立製作所の対応を表1に示す。

2.2 GSMシステムでのICカード

ICカードを使うデジタル移動通信の代表であるGSMシステムは、前ページの図に示すようにMS(Mobile Station)と呼ばれ、メイン制御装置のME(Mobile Equipment)とICカードのSIM(Subscriber Identity Module)で構成している。

(1) SIMの概要

表1 ICカードの規格と日立製作所の対応 H8/3101は、ISOやGSM/PCNの国際規格に合わせて設計されている。

	ISO	GSM/PCN	H8/3101
電源電圧 V_{cc}	5V±5%	5V±10%	5V±10%
動作温度 T_a	0~+50℃	-25~+85℃	-25~+85℃
動作周波数 f_{clk}	1~5MHz	1~5MHz	1~10MHz
スリープモード	——	スリープモードあり	スリープモードあり
消費電流 I_{cc}	動作時	<10mA	<10mA
	スリープ時	<200μA	<100μA
プロトコル(ボーレート)	$1/D^* \times f/372$	$f/372$	——
カード厚	760μm	760μm	チップ厚=250μm
曲げ強度	短辺1cm, 長辺2cm	短辺1cm, 長辺2cm	チップサイズ=5.2×5.2mm ²
静電破壊強度	1.5kV	1.5kV	4kV以上
不揮発性メモリ	必須(す)	必須	EEPROM=8kバイト
その他	——	——	ROM=10kバイト
			RAM=256バイト
			I/O=入出力×2

注：* Dは初期設定で指定されるパラメータ
略語説明 ISO(International Standard Organization)
GSM/PCN(Group Special Mobile/Personal Communication Network)

SIMには、ICカード型SIMとプラグ型SIMの2種類がある。ICカード型SIMは、クレジットカードに代表されるプラスチックカードと同じサイズであり、マルチアプリケーションのひとつとしてGSMがサービスされる。プラグ型SIMは、ICカード型SIMよりも小型のSIMで、GSM専用として使用される。

(2) SIMの機能

GSMシステムでは、セキュリティに関する加入者情報の蓄積・管理、ユーザーPIN(Personal Identification Number)作成・管理など、GSMオペレーターのサポートやGSM加入者の承認・管理に必要な加入者情報をSIMで記憶している。さらに、課金情報、短縮ダイヤル・相手先固定ダイヤルのようなGSMサービスに必要な情報などもSIMが記憶する。

2.3 移動通信用ICカードマイコンの仕様

これらの情報蓄積のため、移動通信用ICカードマイコンはEEPROM内蔵が必須(す)である。さらに、それ以外のマイコンに対するニーズは次のとおりである。

- (1) 通信プロトコルなどを実現するための高速CPU
- (2) 機械的強度向上のための小さいチップサイズ
- (3) マルチファイル実現のための大容量EEPROM
- (4) 信頼性の高いEEPROM
- (5) GSM/PCN仕様に合致した電気的特性

日立製作所は、これらの物理的・電氣的条件を考慮し、ICカード用マイコンH8/3101の仕様を決定した。

3 H8/3101の機能と特長

3.1 ICカード用マイコンの展開

日立製作所は、1985年からICカード用マイコンの開発を始め、図1に示すように現在までに3品種を展開している。これらは、移动通信カード、IDカード、銀行・クレジットなどのマルチファイルを用いるアプリケーション用のカードで使用されている。

3.2 H8/3101の特長

現在、GSM/PCN仕様を満たし、マルチファイルに対応可能な大容量EEPROM内蔵1チップマイコンはH8/3101だけである。さらに、コンタクトレスカードにも対応するため、I/O(入出力端子)を1本追加し2I/Oとなっている。以下に、H8/3101の特長について述べる。

(1) スリープモード

GSM/PCNでは、待機時(スリープ時)の消費電流を低減するため、ICカード用マイコンはスリープモードを内蔵することが必須である。また、バッテリーの寿命を考慮し、消費電流はスリープ時で200 μ A以下、動作時でも10 mA以下の必要があるが、H8/3101は、これをすべて満たしている。スリープモードからの復帰は、I/Oが共通になっている割り込み端子で行っている。割り込み端子とI/Oを共通にすることにより、I/Oからの次データのスタートビットの立ち下がりエッジを検出し、スリープモードから直ちにアクティブモードに遷移し、データ受信す

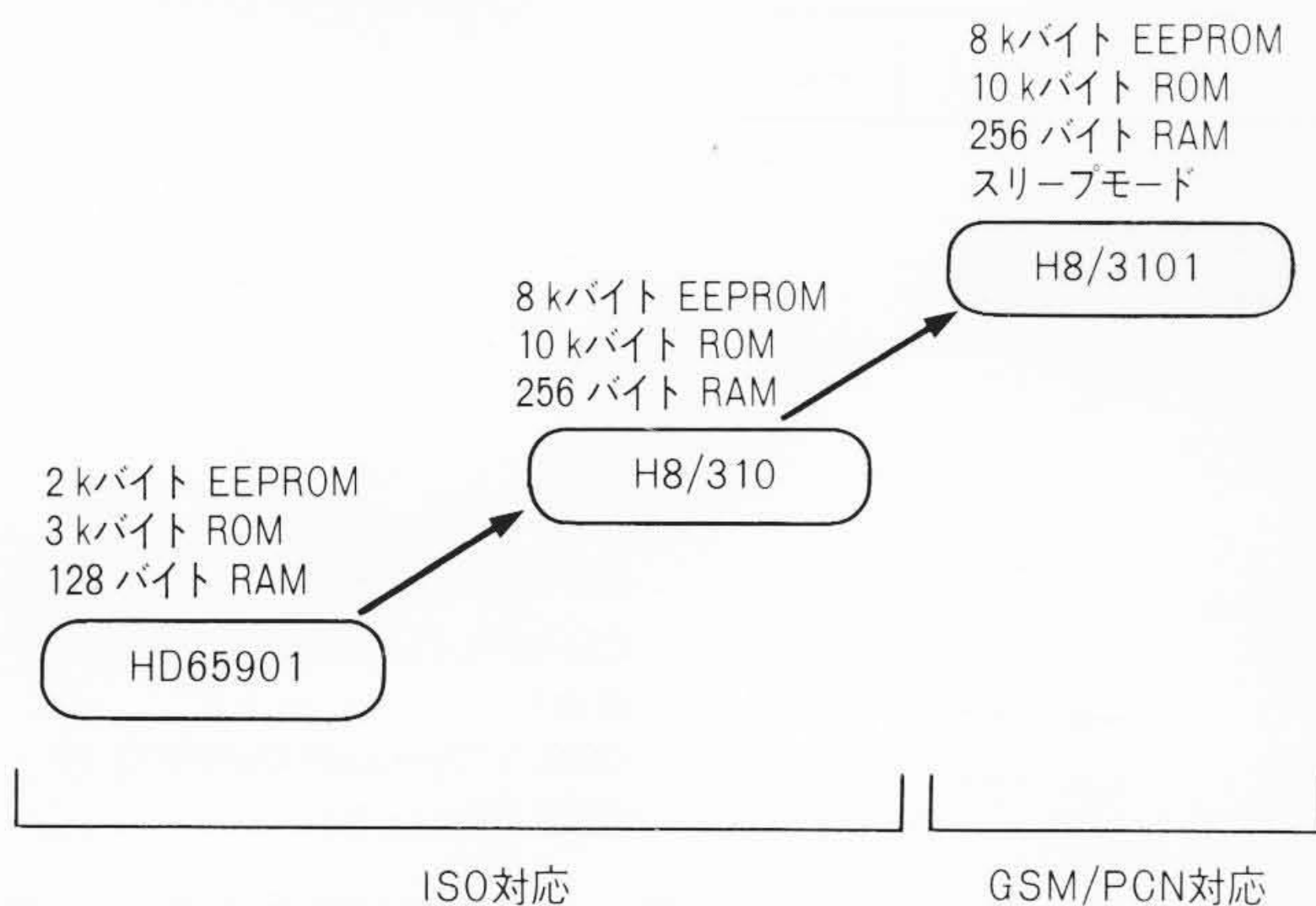


図1 ICカード用マイコンの展開 日立製作所では不揮発性メモリEEPROM内蔵のICカード専用マイコンを用途に応じてそろえている。

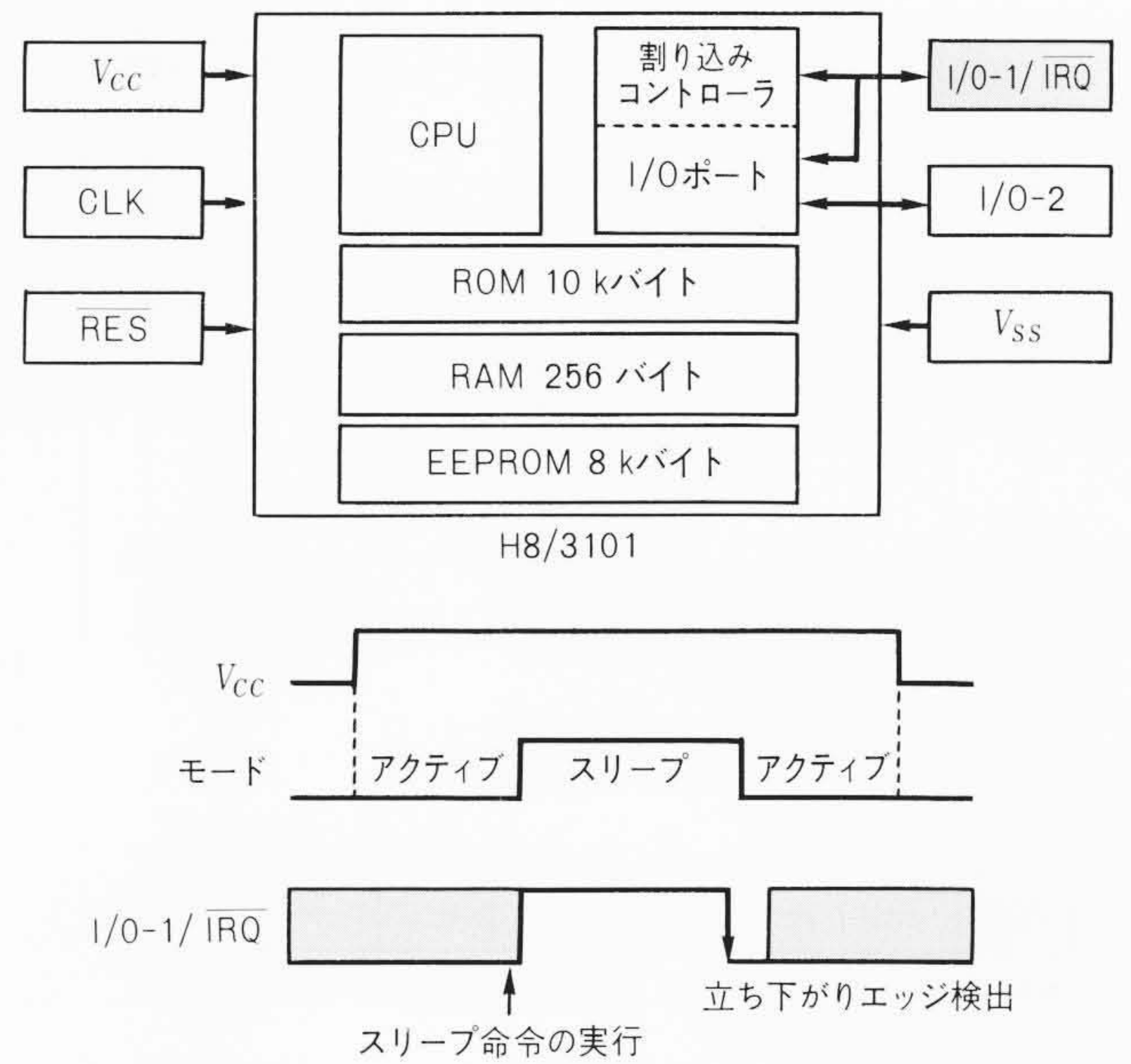


図2 H8/3101とスリープモード H8/3101は8ビットCPUと大容量メモリを内蔵し、ソフトウェアによって消費電力の少ないスリープモードにすることができる。

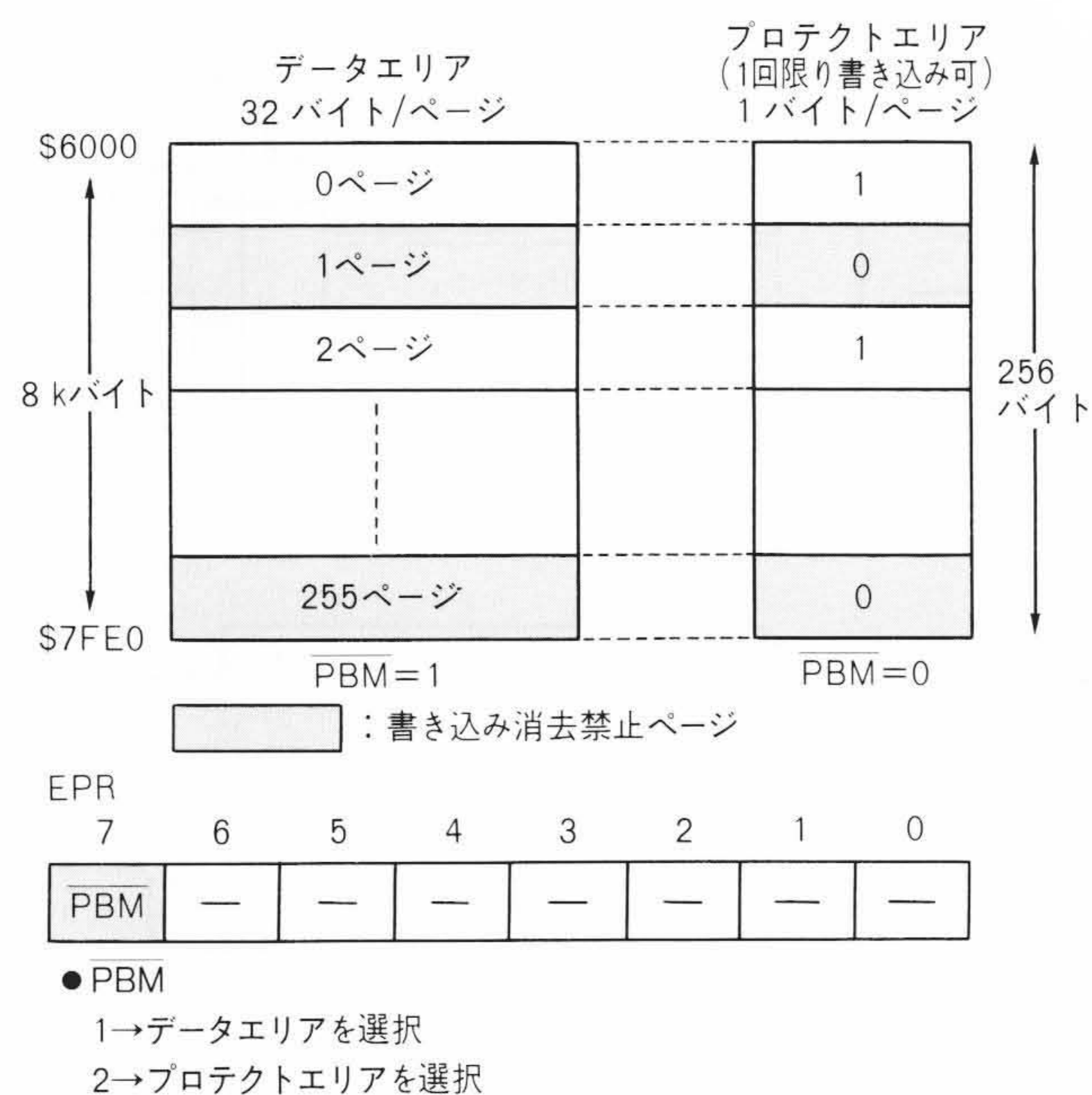
ることができる。H8/3101のブロック図と、スリープモードの概要を図2に示す。

(2) EEPROMへの書き込み保護

GSM/PCNでは、セキュリティキー、PINコードの保護のため、1回限りの書き込み可能なメモリ内蔵の要求がある。しかし、EPROM(UV Erasable Programmable ROM)とEEPROMを同じチップ上で混在させることはプロセス技術上難しいので、H8/3101では図3に示すようにEEPROMを用いて1回限りの書き込み可能なメモリを実現した。EEPROMを32バイトごと1ページに分け、各ページに1バイトのプロテクト領域を設けた。このプロテクト領域は、外部から書き込みはできるが消去ができない構造になっている。このプロテクト領域のデータが初期値の‘1’状態のときは、実際のデータ領域へは自由にアクセスできるが、一度‘0’書き込みを行うとそのプロテクト領域に該当するデータ領域は、書き込み・消去が恒久的に禁止され、読み出し専用となる。プロテクト領域への書き込みは、EPR(EEPROM Protect Register)のPBMビット(Protect Bit Mode bit)でプロテクト領域を選択し、その後は通常のEEPROMへの書き込み・消去と同様の手順で行う。

(3) 書き込みシーケンス

EEPROMの信頼性を損なう原因として、誤書き込



注：略語説明 PBM (Protect Bit Mode)
EPR (EEPROM Protect Register)

図3 EEPROMへの書き込み保護 EEPROMの不当な書き込みを防止するため、32バイトごとにプロテクトをかけることができる。このプロテクトの設定は1回だけである。

み・誤消去がある。これを防ぐため、H8/3101では、図4に示す書き込みシーケンスを導入した。H8/3101は、外部から入力するCPUのリセット回路とは別に、EEPROM専用のリセット回路を内蔵し、常時EEPROMがリセット状態になるようにした。このリセット状態から書き込

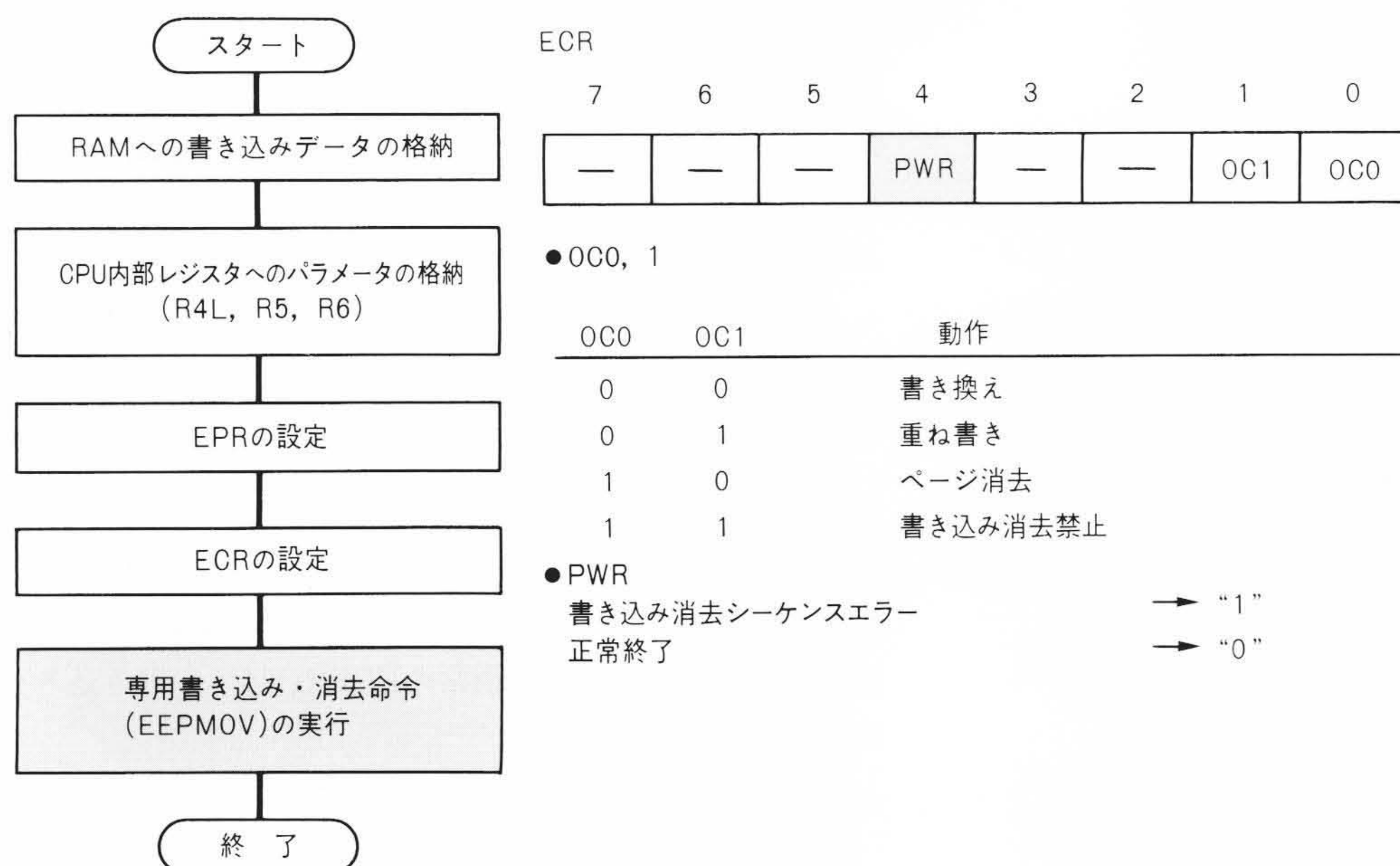
みシーケンスに従った場合だけリセットが解除され、EEPROMへのアクセスが可能となる。さらに書き込みにRAMやレジスタにデータを書き込む命令と異なった専用命令を使用するため、マイコンが暴走しても誤書き込み・誤消去を防止できる。

一方、書き込み・消去中の電源電圧低下も、EEPROMのデータ保持を悪化させ信頼性を損なう原因となる。この対応として、H8/3101に低電圧検出回路を内蔵した。低電圧検出回路はEEPROMの書き込み・消去中に電源電圧の低下を検出すると、直ちにEEPROMをリセット状態にし、ECR (EEPROM Control Register) のPWRビット (Power bit) をセットする。ユーザーは書き込み終了後に、このPWRビットをチェックすることにより、書き込み中に電圧低下がなかったかを知ることができる。

以上のように、EEPROMへのアクセスに特殊なシーケンスと専用命令を取り入れ、さらに低電圧検出回路を内蔵することで誤書き込み・誤消去の防止を実現し、セキュリティの高いEEPROMとした。

4 ICカード用COB

ICカードには、カード表面にコンタクト部を持たない非接触型カードと、IS7816に準拠したコンタクト部を配置した接触型カードの二つのタイプがある。移動通信用ICカードは接触型であり、カード表面に配置したコンタクト部を通し、カードに埋め込まれたマイコンとICカードリーダ/ライタ間で通信を行う。このICカード用モジ



注：略語説明
ECR (EEPROM Control Register)
EEPROM (EEPROMへの書き込み命令)
OC0, 1 (Operation Control 0, 1)
PWR (Power Bit)

図4 EEPROM書き込みシーケンス 専用命令と一定のシーケンスをとることにより、誤書き込みを防止することができる。

ルールとして、コンタクト部とマイコンを一体化したCOBが用いられる。

ICカードでは、薄いプラスチックカード内にCOBを収めなければならないという制約がある。カードの厚さはISOで0.76 mmと規定されているので、COBとプラスチックカードとの接着部およびカード部の厚さを考慮すると、COBとしては0.6 mm程度の厚さが必須となる。

これに反し、カードは利用者によって携帯されることが多いため機械的ストレスを受けやすく、カードにしたときの機械的強度の向上や高信頼性を確保することが、COBとしては重要なポイントとなる。

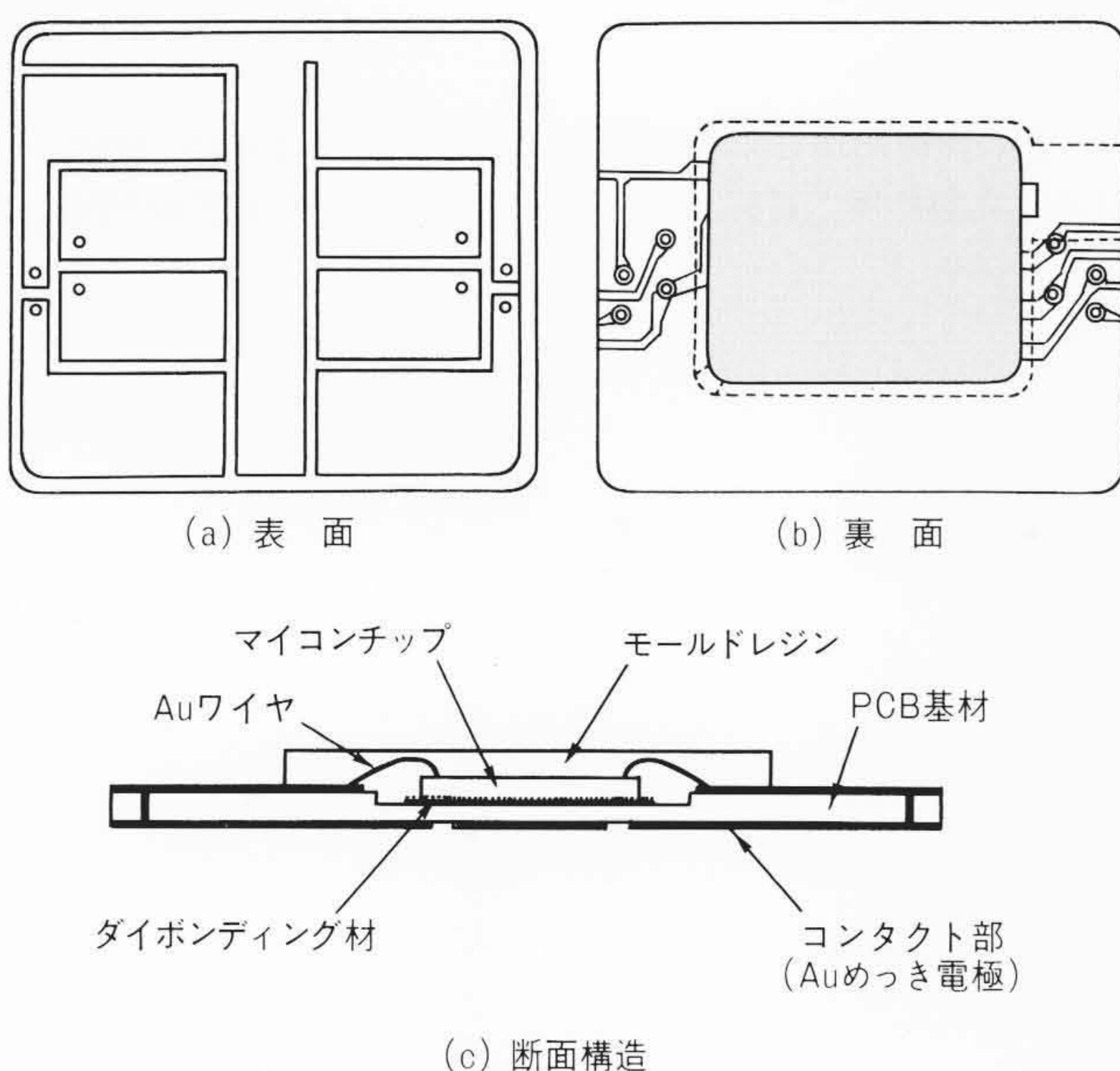
以上から、次の3点がICカード用COBに対する技術的課題となる。

- (1) 0.6 mmの薄型COBの実現
- (2) 機械強度・曲げ強度の向上
- (3) 高信頼性の確保

4.1 COBの構造

H8/3101で使用したCOBの外形および断面構造を図5に示す。

ICカード用COBは、表面にコンタクト部を設けたPCB (Printed Circuit Board) 基材上にマイコンチップを接着し、Auワイヤで結線した後、トランスファモールドに



注：略語説明 COB (Chip On Board), PCB (Printed Circuit Board)

図5 H8/3101COBの外形 ICカード用のCOBは厚さの精度が要求される。

よってチップ表面を封止した構造とした。このCOBの特長は次のとおりである。

- (1) PCB基材は、表面にAu(金)めっきを施したコンタクト部をパターン化したハードPCBを用いている。コンタクト部のAuめっきは、外観品質および電極パターン面の強度の点から有利な硬質Auめっきを採用し、また、裏面のパターン部は、ボンダビリティの点から軟質Auめっきを適用した。表裏面間はスルーホールによって接続をしている。さらに、COBの薄型化に対応するため、チップマウント部に凹み加工してある基材を採用した。
- (2) ワイヤボンディング工程では、通常のボンディング方式では、レジ

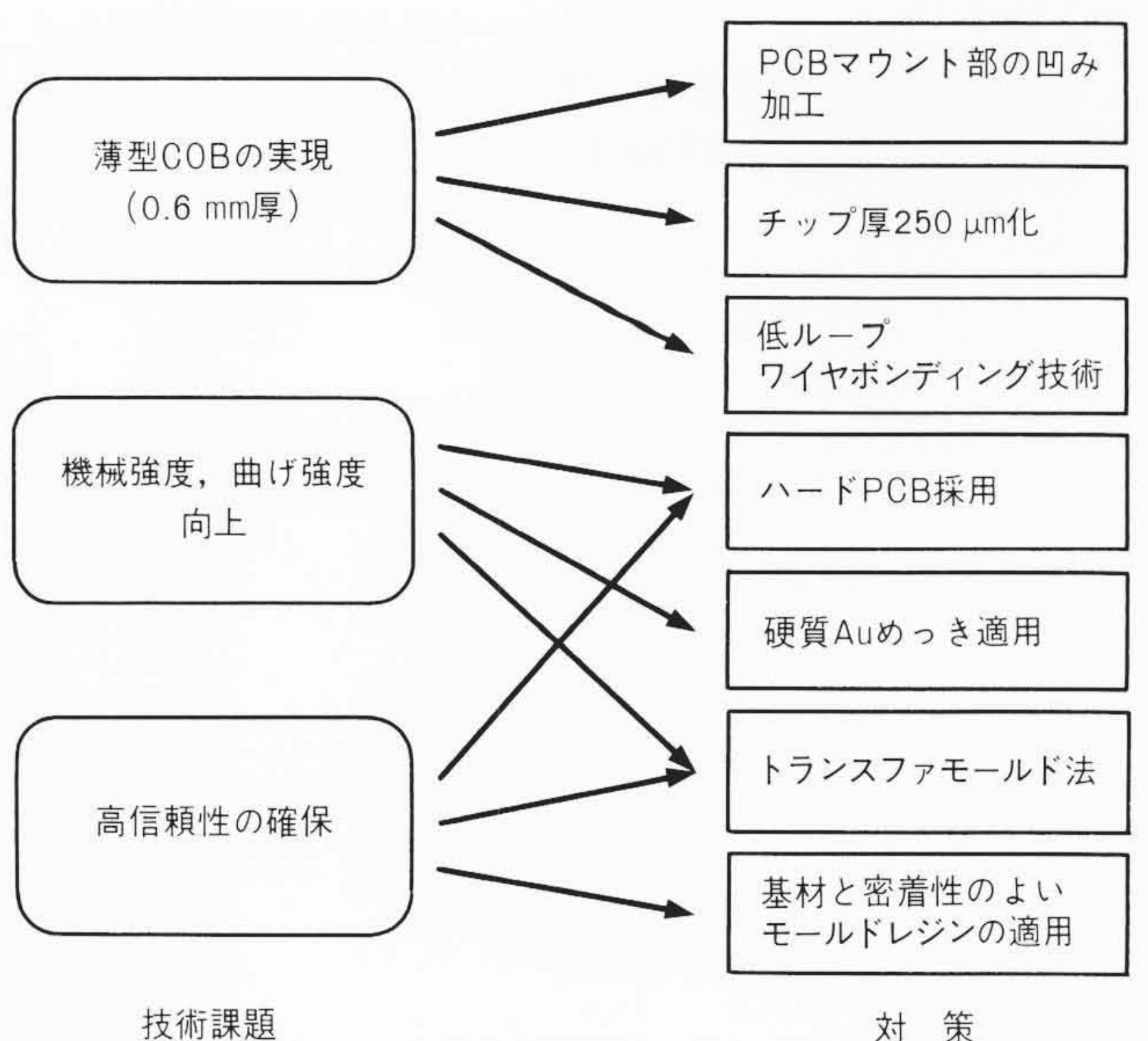


図6 ICカード用COBの課題と対策 COB開発にあたっては、技術課題を解決するためにさまざまなくふうを施している。

選択した。

以上をまとめて図6に示す。これらにより、薄型でかつ高信頼性を持つICカード用COBを実現することができた。

4.2 COBの信頼性

H8/3101に適用したICカード用COBの信頼性試験結果を表2に示す。

信頼性試験に関しては、高温動作、高温放置、低温放置、高温・高湿放置、温度サイクル寿命と、いずれも良好の結果が得られた。これは通常のプラスチックモールド品と同等のレベルにあり、薄型のICカード用COBとして高い信頼度を持つことを確認することができた。

5 おわりに

現在、ヨーロッパではようやくGSMの実用化のめどがついたところであるが、次世代へ向けた動きが早くも始まっている。

一方、国内では限定された用途、地域でのICカードの利用が行われているが、通信網への応用はこれからの段階である。

次世代GSM用ICカードには、

- (1) 動作電圧：2.7～5.5 V
- (2) 消費電流：動作時；1 mA以下、スリープ時；10 μ A

表2 COBの信頼度試験結果 ISO規格に十分満足する信頼性を持っている。

試験項目	試験条件	試験個数	故障数
高温動作	$T_a = 125^{\circ}\text{C}$ $V_{cc} = 5.5\text{ V}$ $t = 1,000\text{ h}$	22	0
高温放置	$T_a = 125^{\circ}\text{C}$ $t = 1,000\text{ h}$	22	0
低温放置	$T_a = -55^{\circ}\text{C}$ $t = 1,000\text{ h}$	22	0
高温・高湿放置	$T_a = 85^{\circ}\text{C}$ $\text{RH} \geq 85\%$ $V_{cc} = 5.5\text{ V}$ $t = 1,000\text{ h}$	22	0
温度サイクル寿命	$-55 \sim 25 \sim 150^{\circ}\text{C}$ 100サイクル	22	0

以下

- (3) メモリの大容量化

の3点の要求がある。

また、シリアルインタフェース、タイマなどの周辺機能のハードウェア化も重要である。次世代ICカード用マイコンでは、これらの移動通信システムからのニーズを考慮して、プロセス、周辺機能、チップサイズの設計を検討していく。

参考文献

- 1) 和田，外：シリコンファイルへの道を開くフラッシュメモリの開発，日立評論，72，12，1227～1234(平2-12)
- 2) GSM規格11.11 ETSI TC GSM(1990-3)
- 3) ISO規格7816(Part1 1987，Part2 1988，Part3 1989)
- 4) 日立製作所：H8/3101 ハードウェアマニュアル(平4)