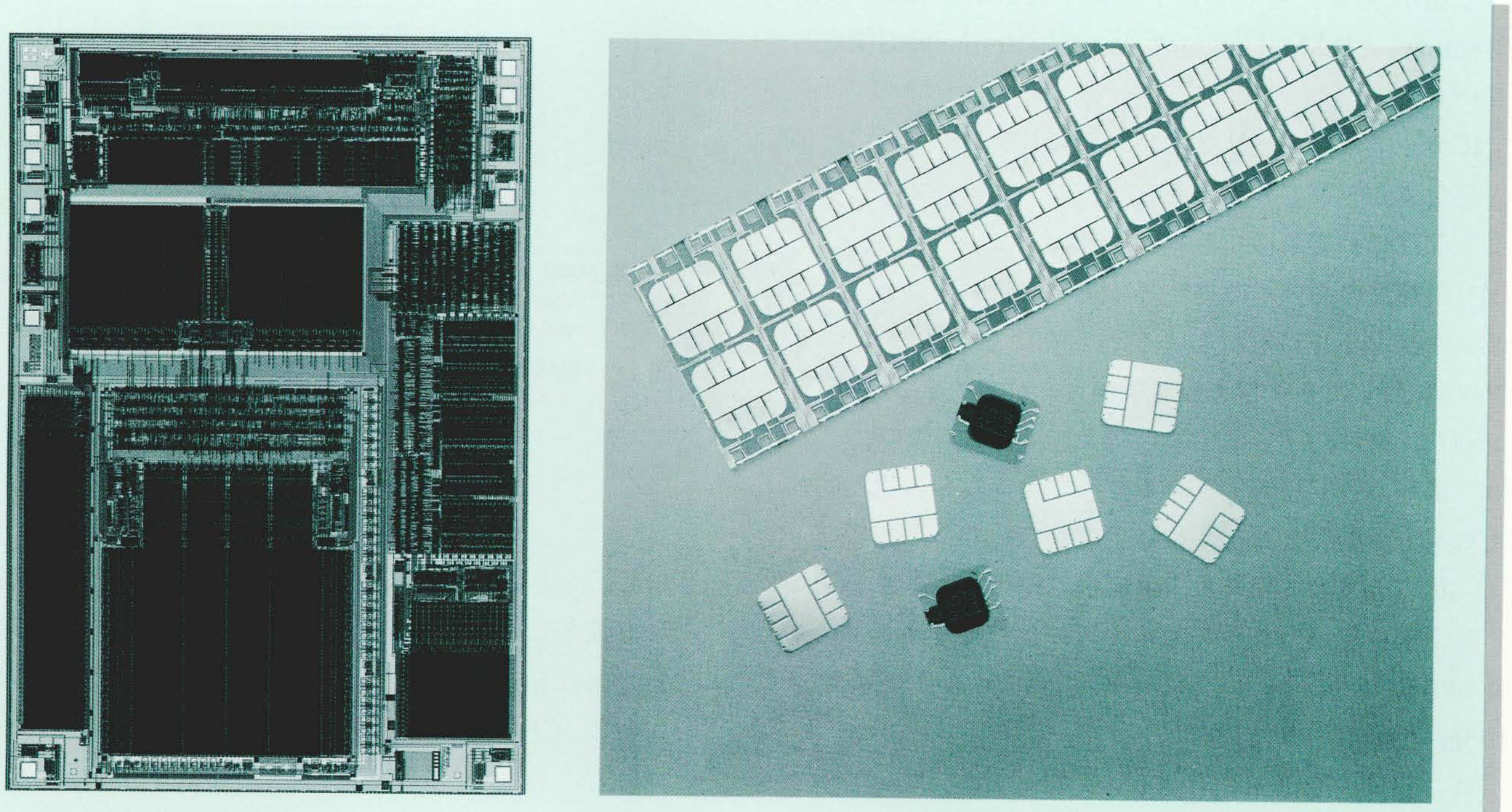
# ICカードを支える半導体技術

## Semiconductor Technology for IC Cards

中田邦彦 *Kunihiko Nakada*
北川信男 *Nobuo Kitagawa*
長崎信孝 *Nobutaka Nagasaki*



(a) 電子マネー用マイコン“H8/3111”　　(b) “H8/3111”のパッケージ

**電子マネー用マイコン“H8/3111”のチップ写真とそのパッケージ**
“H8/3111”は，べき乗剰余演算を高速に実行できるコプロセッサを内蔵したマイクロコンピュータである。チップを保護したり，外部との電気的接続を行うためにCOB(Chip on Board)またはCOT(Chip on Tape)にパッケージングされ，ICカードに組み込まれる。

マルチメディアの急速な進展により，情報を正確に，しかも安全に伝えることがますます重要になってきている。中でもEC(Electronic Commerce：電子商取引)のように金融情報を扱うシステムでは，情報をいかに安全に伝達するかが課題となっている。そのキーデバイスの一つとして，最近，ICカードが着目されている。

ICカードは，高い性能はもちろんのこと，改ざんや複製などの不正行為に対して十分な防御手段(耐タンパリング性※1))を持つ必要がある。ICカードには，個人情報や金融情報を，内蔵の不揮発性メモリに格納するようになってきたため，信頼性が高いことも重要である。ICカードの耐タンパリング性と高い信頼性は，マイコン(マイクロコンピュータ)によって可能としている。

日立製作所は，1986年からICカード用マイコンを開発，生産してきた。1991年には，主にGSM(Global System for Mobile Communications)向けに8kバイトの不揮発性メモリ内蔵のマイコンを開発し，1995年には電子マネー用途として，暗号処理の高速化を実現するコプロセッサ内蔵のマイコンを量産化してきた。今後は，ICカードの汎用化，高機能化およびコンタクトレス化の流れに適した半導体を開発していく考えである。

※1)　耐タンパリング性：内部情報への不正アクセスなどに対する防御機能

## 1　はじめに

ICカードは薄いプラスチックカードにICチップを埋め込んだものである。特にICチップにCPU(Central Processing Unit)を内蔵したICカードは，別名「スマートカード」とも呼ばれている。ICチップは，CPUのほかに各種情報を格納する不揮発性メモリ，演算や種々の処理を指示するプログラムを内蔵したROM(Read-Only Memory)とRAM(Random Access Memory)で構成している。

ICカードは今や，社会インフラストラクチャーの一部と見なすことができる。そのために，ICチップには次のような点が必要条件である[1)]。

(1)　信頼性の高い不揮発性メモリを内蔵すること

(2)　中身を不正に解析しようとするたくらみ(タンパリング)に対してさまざまな対策が行われていること(耐タンパリング性)

(3)　薄いカードに実装されるため，曲げなどの物理的強度に対して耐えうるように封止されていること

(4)　広く普及するために，低価格で提供できること

日立製作所は，これらのニーズにこたえる形で，1986年からICカード用マイコン(マイクロコンピュータ)を開発，生産してきた。

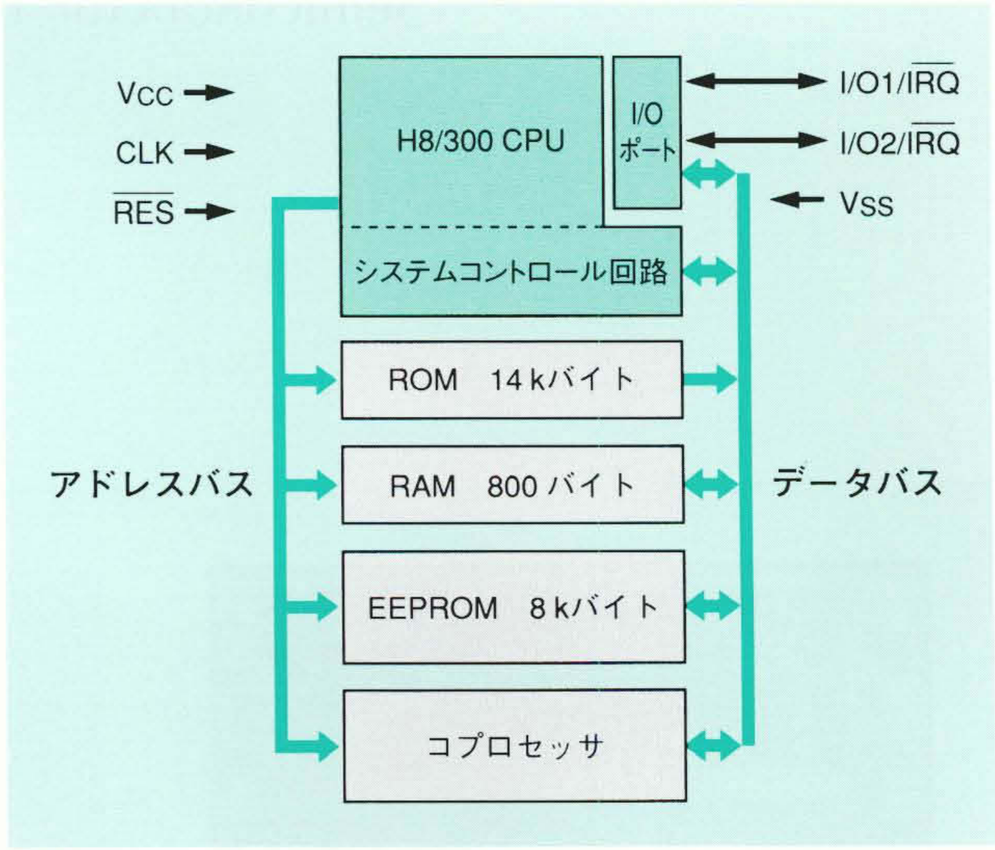
ここでは，ICカード用マイコンのマイコンアーキテクチャ，不揮発性メモリ技術，および耐タンパリング技術を中心に述べる。

## 2　マイコンアーキテクチャ

開発したICカード用マイコン“H8/3111”のブロック図を**図1**に示す[2)]。不揮発性メモリ“EEPROM(Electrically Erasable Programmable ROM)”にはデータを記憶することができ，8ビットCPUやROM・RAMにより，ICカード自身が能動的にさまざまなデータ処理を行うことができる。CPUが行う主要な処理は，EEPROM内のデータ管理，I/O端子による通信制御，送受信データの暗号化処理などである。

また近年，活発に提案，試行されている電子マネーなどの用途などでは，安全なディジタル通信の実現要求の高まりから，暗号処理が高度化してきている[3)]。暗号処理方式の概要について以下に述べる。

暗号化方式は数多くの方式が提案されているが，これらは「共通鍵暗号方式」と「公開鍵暗号方式」に大別される。共通鍵暗号方式は，暗号化鍵と復号化鍵とを同一にし，とも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。この方式は一般に，CPUだけでも高速処理ができるという利点を持つ一方，共通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るため，鍵管理に制約がある。




注：略語説明
Vcc, Vss(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1　H8/3111のブロック図**
H8/3113では，暗号計算用コプロセッサを内蔵したり，アドレスバスやデータバスにつながる端子をなくして，耐タンパリング性を高めている。

公開鍵暗号方式では，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り，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」を容易にするなどの特徴がある。特に電子マネーシステムでは，不特定多数間通信での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，「RSA暗号※2)」が一般に知られている。H8/3111は，公開鍵暗号処理を高速に実行するために，“$X^Y$ mod N”で表されるべき剰余演算を高速に計算するためのコプロセッサを内蔵している。演算性能はCPUによるソフトウェア処理にも依存するが，512ビットの“$X^Y$ mod N”の計算が約0.5秒で実行できる。

※2)　RSA暗号：米国のRivest, Shamir, Adelman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暗号方式

## 3　不揮発性メモリ“EEPROM”技術

日立製作所のEEPROMには，一般に採用されているフローティングゲート型と異なり，「MONOS(Metal-Oxide-Nitride-Oxide-Silicon)型」を採用している[4]。フローティングゲート型とMONOS型の断面構造を**図2**に示す。

フローティングゲート型の素子では，自由電子の状態でフローティングゲートに電荷を蓄積する。これに対して，MONOS型の素子は独自の3層ゲートの絶縁膜構造であり，その窒化膜中の離散的トラップ準位に電荷を捕まえることにより，同様の効果を持たせている。もしトンネル領域にピンホールや絶縁膜の欠陥などがあると，フローティングゲート型の素子では蓄積された電子がすべて流出し，記憶素子としての機能を果たさなくなる。一方，MONOS型の素子では，そのポイントだけが電荷蓄積効果を持たなくなるだけであり，記憶素子としてほとんど問題なく正常に機能する。

このようにMONOS型の特徴は，データの保持特性に優れ，書き換えによる劣化が少ないことにある。また，これらの特性を維持しながら，素子のサイズを比例縮小することができる。これは，チップサイズを小さくすることが機械的強度の向上につながるので，ICカードには最適な技術であり，将来のいっそうの微細化プロセスにも適用できる。

## 4　耐タンパリング技術

### 4.1　異常動作時でのEEPROM誤書込み防止

端子付きICカードでは，各信号が端子を介してリーダ・ライタと接触している。そのため，カード使用中に信号の異常が生じた場合，これに起因するEEPROMデータの破壊や誤書込みを防止する機能をマイコンチップに内蔵する必要がある。

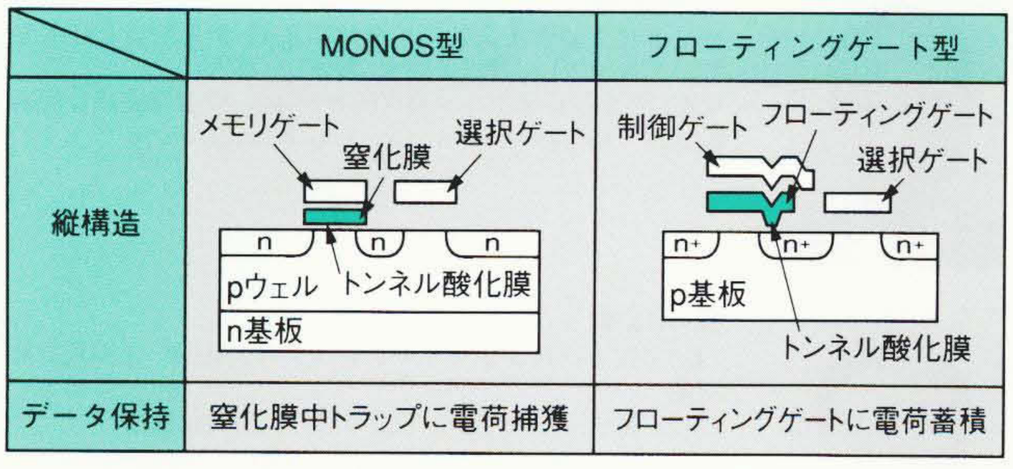



**図2　EEPROMメモリセル技術の比較**
フローティングゲート型ではフローティングゲートに電荷を蓄積することにより，MONOS型では窒化膜中に電荷を捕まえることにより，それぞれ記憶効果を持たせる。

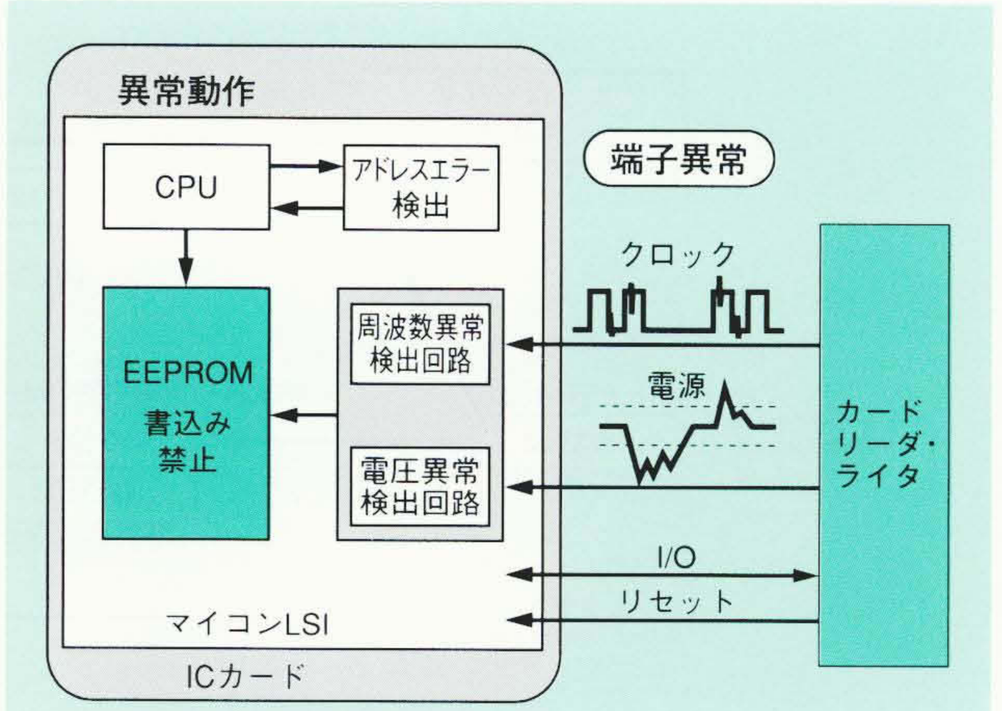



**図3　EEPROMの誤書込み・改ざん防止機能**
周波数異常検出回路と電圧異常検出回路などにより，EEPROMの誤書込みや改ざんを防止する。

異常信号の検出では，特に重要なクロックと電源端子に着目した。クロックにノイズが付加されたりクロックが停止したりするなどの異常には周波数異常検出回路が，電源の瞬断や高電圧印加などの異常には，電圧異常検出回路がそれぞれ作動する。それらの異常を検出すると，EEPROMへの書込みを即時に禁止する。さらに，CPU自身の動作を常に監視し，アドレスエラーなどの異常動作が生じた場合には，これを検出してCPUによる予定外の書込み実行を阻止する。

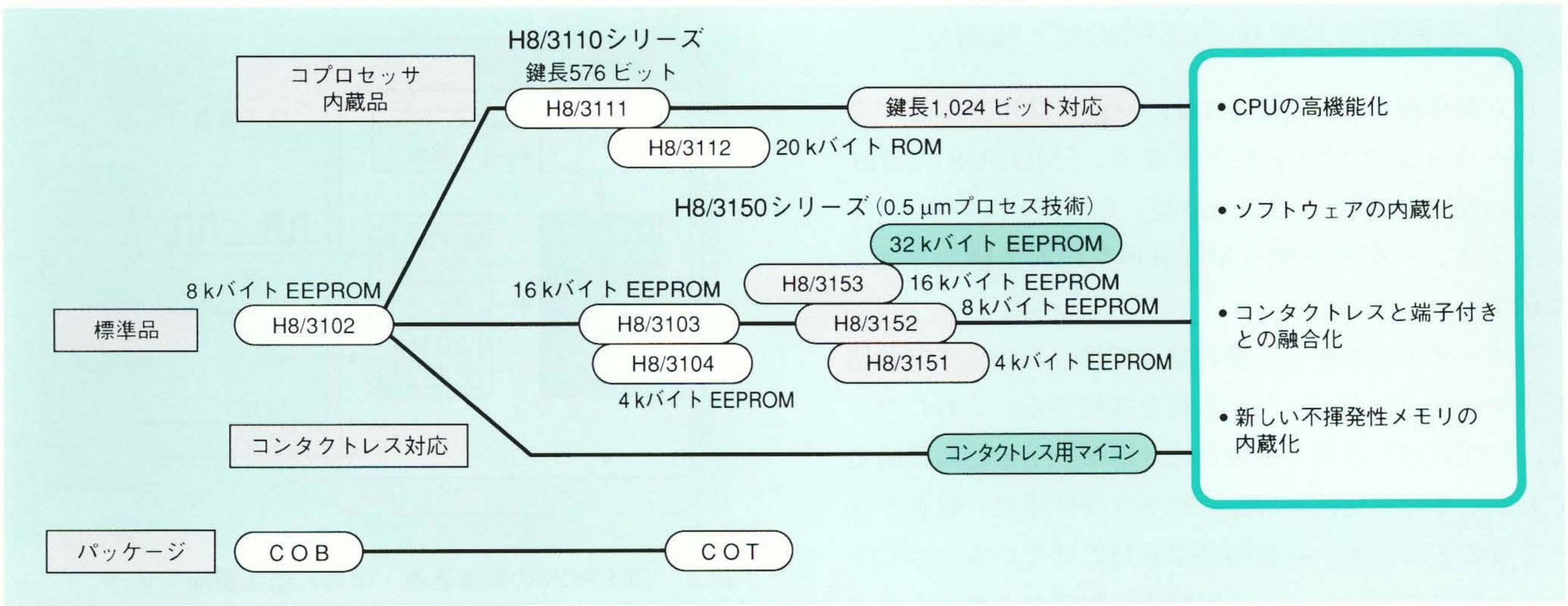
### 4.2　意図的なEEPROM改ざんの防止

最近，ICカードに与えるクロックや電源電圧を規定値外に設定して内蔵のマイコンを意図的に誤動作させ，この誤動作をモニタすることによってマイコン内部のプログラムを解析する手法が危険視されている。プログラムが解析されれば，EEPROMへの書込み手順が判明し，EEPROMに記憶されている情報を改ざんされるおそれが生じる。

これを防止する一つの手段として，周波数異常検出回路や電圧異常検出回路が有効である。マイコンの異常動作を未然に防止するには，そこに至る前にマイコンの動作をロックすることである。EEPROMへの誤書込みと改ざん防止機能を**図3**に示す。

## 5　ロードマップ

日立製作所は，1995年に5Vと3V動作を可能にした“H8/3102”を開発した。このH8/3102をベースとして，三つの流れに分けて製品化を行う(**図4**参照)。第一は，




注：略語説明ほか　COB(Chip on Board), COT(Chip on Tape), (量産中), (開発中), (計画中)

**図4　ICカードマイコンのロードマップ**

従来のCPUとメモリだけの標準マイコンをベースに，暗号処理を高速化するためのコプロセッサ内蔵のマイコンと，外部との通信に端子を持たないコンタクトレス対応のマイコンも充実していく。

CPUとメモリで構成する標準的なマイコンである。メモリ容量4 kバイトから16 kバイトまでのバリエーションをそろえた。1998年には，より耐タンパリング性の高い「H8/3150シリーズ」を製品化する。第二に，コプロセッサを内蔵した「H8/3110シリーズ」を製品化していく。暗号の鍵長が1,024ビットに対応した製品を1998年にも量産化していく。第三は，コンタクトレスカード用マイコンである。外部との通信に端子を持たない特徴を生かし，鉄道・地下鉄などの改札や入退室のようなトランスポーテーション分野への応用をねらう。

## 6　おわりに

ここでは，ICカード用マイコンを特徴づける不揮発性メモリ技術と耐タンパリング技術を中心に述べた。

日立製作所は，1986年以降その時々のニーズに合ったICカードマイコンを提供してきている。今後は，ICカードに適用することを目的に，(1) 汎用OS(Operating System)などのソフトウェアを内蔵し，各種アプリケーションの出し入れが可能なマイコン，(2) CPUを16ビットや32ビットへ高機能化し，高速処理を実現するマイコン，(3) RAM並みの高速書き換えを可能とする不揮発性メモリ内蔵マイコン，(4) 従来の端子付きとコンタクトレスを融合し，それぞれの特徴を補完したマイコンなどを開発する計画である。

これからも，より使いやすく，より信頼性の高いICカード用マイコンを開発していく考えである。

## 参考文献

1) 株式会社シーメディア：ICカード総覧(1997-9)
2) 佐藤，外：電子マネーとICカード用マイクロプロセッサ，日立評論，**78**，11，793～798(平8-11)
3) デジタルマネーのすべて，日経BP社(1997)
4) S. Minami：A Novel MONOS Nonvolatile Memory Device Ensuring 10-Year Data Retention after $10^7$ Erase/Write Cycle：IEEE Transactions on Electron Devices, Vol. 40, No.11(1993-11)

## 執筆者紹介

**中田邦彦**
1982年日立製作所入社，半導体事業部 システムLSI本部 第二システムLSI設計センタ 所属
現在，ICカードマイコンLSIの設計・開発に従事
E-mail：knakada@cm. musashi. hitachi. co. jp

**北川信男**
1981年日立製作所入社，半導体事業部 システムLSI本部 第二システムLSI設計センタ 所属
現在，ICカードマイコンのマーケティング・製品企画に従事
E-mail：kitagawa@cm. musashi. hitachi. co. jp

**長崎信孝**
1980年株式会社日立マイコンシステム入社，第一LSI設計部 所属
現在，ICカードマイコンLSIの設計・開発に従事
E-mail：nagasaki@hitachi-mc. co. jp