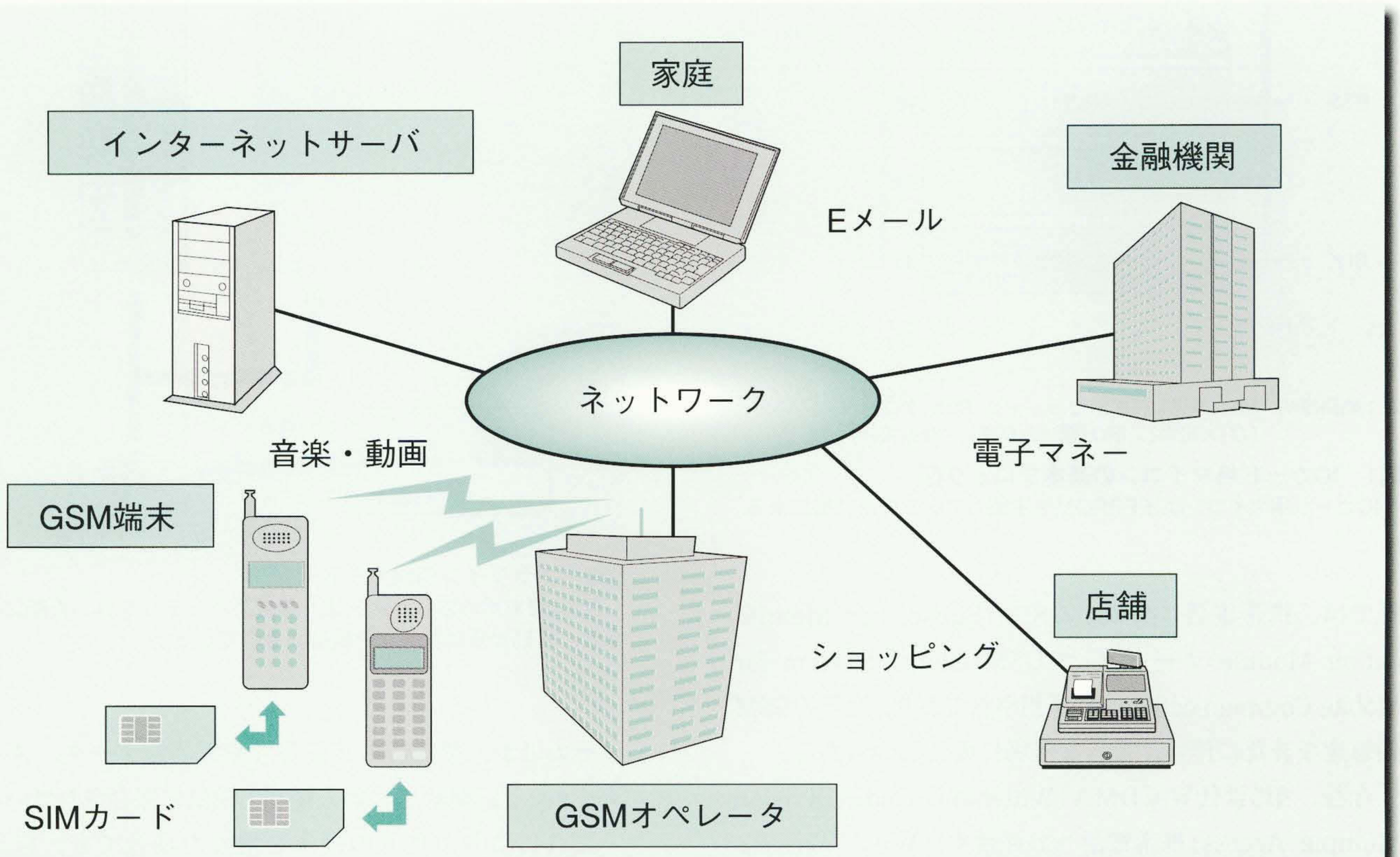
携帯電話におけるICカードの活用

—SIMカード用半導体への取組み—

IC Cards for Mobile Telecommunications

高本伸雄　*Nobuo Takamoto*



注：略語説明　GSM(Global System for Mobile Communications)，SIM(Subscriber Identification Module)

GSMネットワークの中核を担うSIMカードの位置づけ

GSMを使った携帯電話端末に挿入され，加入者の電話番号ほかのIDや電話帳データ，各種サービス情報，認証などを管理するSIMカードは，携帯電話ネットワークのセキュリティを支える重要なコンポーネントとして位置づけられている。

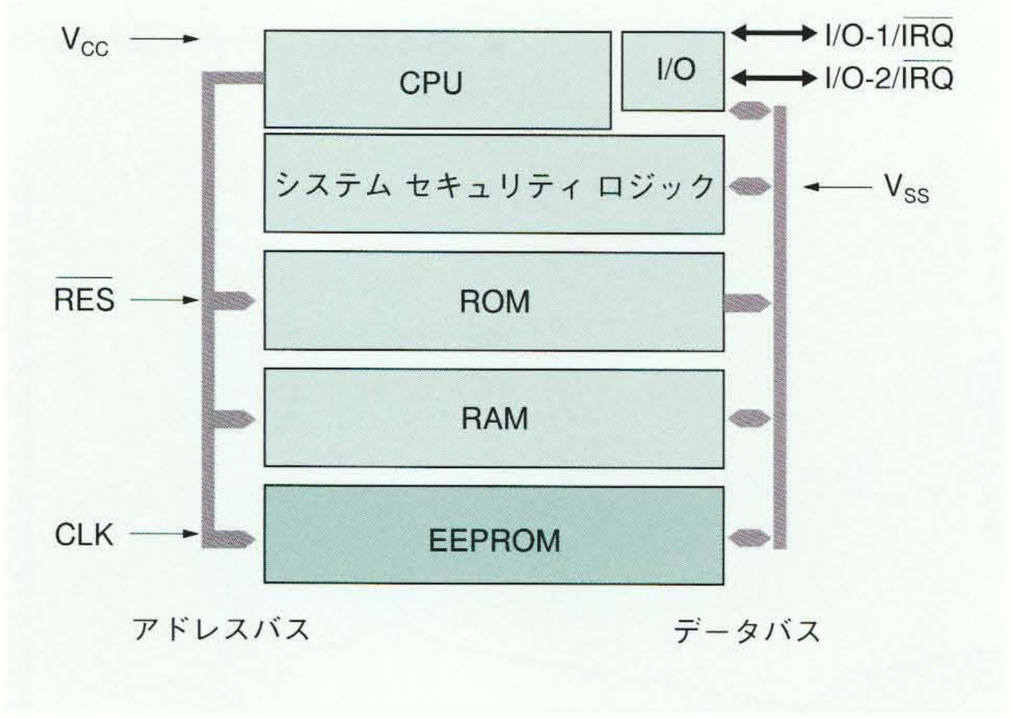
携帯電話の急速な普及に伴い，GSMに搭載されるSIMカードの市場も急成長を遂げ，ICカードの重要な市場の一つとなっている。また，多機能化が進む携帯電話は，近年，モバイルネットワークを支えるデバイスとしても重要視され，その携帯電話に搭載されるSIMカードでも，携帯電話の多機能化に伴う大容量メモリ化の一途から，ネットワークへのアクセスを考慮した，アクセスの高速化や高セキュリティ化などの要求が多様化しており，変革期に入っている。

今後，SIMカード用の半導体では，この携帯電話ネットワークを利用したさまざまなアプリケーションに対し，いかに高性能で使いやすく，セキュリティを確保した安全な製品を提供できるかがかぎとなる。

1　はじめに

ICカードは，クレジットカードなどに使用されている磁気カード大の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。このICチップは，各種処理を行うCPU(Central Processing Unit)，処理内容を指示するプログラムを格納するROM(Read-Only Memory)，処理データを一時保管するRAM(Random Access Memory)といったマイコンの基本要素に加え，各種プログラムや情報を格納するEEPROM(Electrically Erasable Programmable ROM)などの不揮発性メモリで構成している(**図1**参照)。

このため，磁気カードに比べて各種処理機能によるデータの流出や偽造を困難にするとともに，大量のデータの記憶を可能とし，通信・金融・医療・娯楽・公共・交通といった幅広い分野で採用が進んでいる。特に通信分



注：略語説明　Vcc(電源)，RES(リセット)，CLK(クロック)，
I/O(入出力)，IRQ(割込み要求)，Vss(接地)

図1　ICカード用マイコンの基本ブロック図
ICカード用マイコンは，EEPROMを搭載しているのが特徴である。

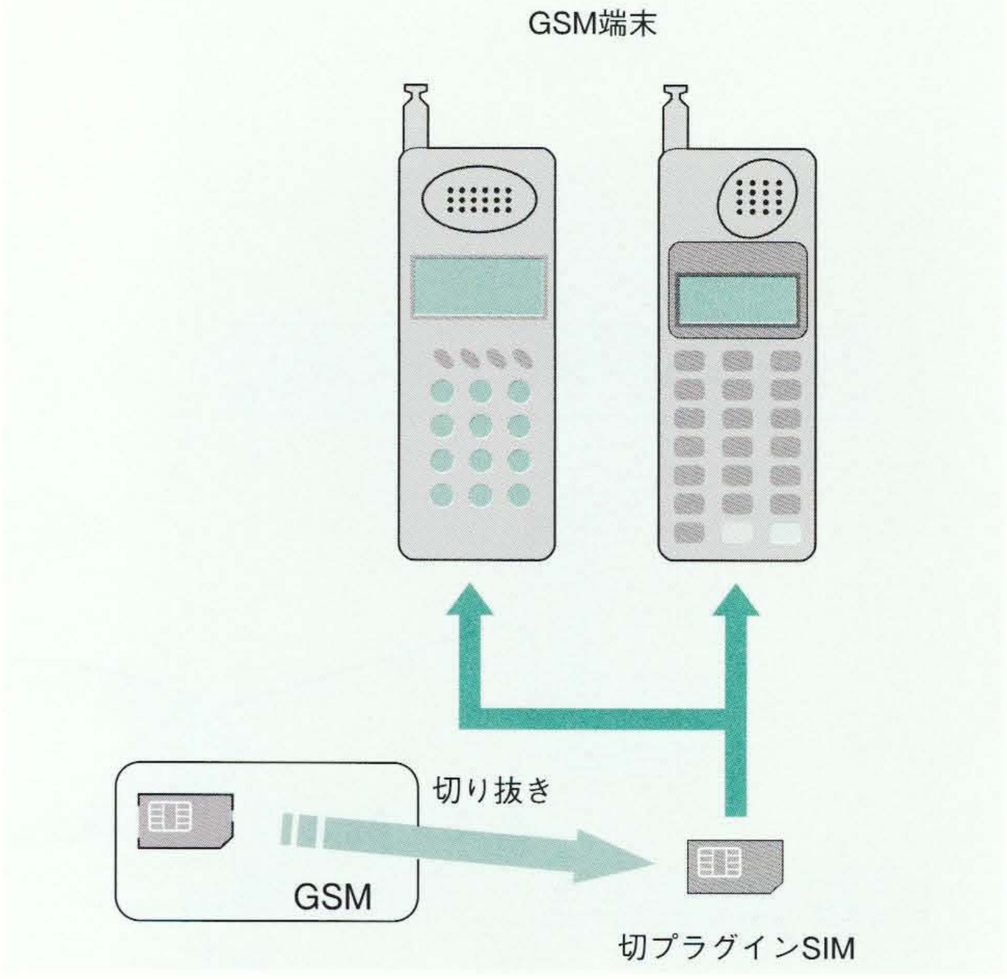


図2　プラグインSIMカード
GSM端末用のSIMカードは，通常，バッテリを外した面に挿入され，外部からは見えない構造になっている。

野では，携帯電話に搭載するSIM(Subscriber Identification Module)カードとしてGSM(Global System for Mobile Communications)に採用されており，近年のGSMの急速な普及に伴い，大きな市場に成長しつつある。

今後，第3世代W-CDMA(Wideband Code Division Multiple Access)携帯電話への採用や，WAP(Wireless Application Protocol)による携帯電話のネットワークアクセスの普及により，このSIMカードの重要性が増していくことが予想される。

ここでは，このSIMカードの役割と今後の動向，および日立製作所の半導体への取組みについて述べる。

2　SIMカードの役割

前述したように，SIMカードは，GSMに採用されて以来，欧州を中心に急速に発展している。

その形状には，通常の磁気カードの大きさの「ID-1 SIM」のほか，切手大の切り込みがあり，携帯電話ユーザーが切り取って携帯端末に挿入する「プラグインSIM」と呼ばれるタイプがある。最近は，携帯端末の小型化の要求が強いことから，プラグインSIMが主流となっている(**図2**参照)。

SIMでは，携帯電話サービスプロバイダによって契約者のID(電話番号)やSMS(Short Message Service)などの契約サービス情報，サービスを受けるためのアプリケーションプログラムなどが書き込まれ，契約者に渡される。契約者はそのSIMを携帯端末に挿入することで，自分の電話として契約したサービスを受けられるようになる。

そのほか，契約者の暗証番号や電話帳データ，メールデータなど，契約者の個人情報もSIMに保存されている。

これにより，他人の端末を借りた場合でも，自分のSIMを差し込むだけで，自分の電話として自分の契約サービスや，保存されている情報を使用することができる。また，端末を新たに買い換えた場合にも，SIMを入れ替えるだけで新しい端末を使用することができ，SIMを取り出した古い端末に，個人のプライバシー情報が残ることもない。

さらに，サービスを変更または追加したい場合にも，SIMにはSTK(SIM Tool Kit)と呼ばれるアプリケーションの管理システムがあり，GSMサービスプロバイダに申し込めば，OTA(Over the Air)サービスによってSTKに対応したデータが携帯電話を介してSMSを利用して送信される。そのため，申し込んだサービスのアプリケーションダウンロードがショップに赴くことなく可能である。

このように，GSMのサービスの大部分は，SIMカードによって支えられている。

3　SIMカードの動向

3.1　ネットワーク接続への対応

現在，わが国では，携帯電話でのEメール送受信や，ウェブサイト閲覧がブームとなっている。しかし，GSM

では，まだSMSが主流である。WAPを使用した，ネットワークに接続できる端末も出ているが，魅力的なサービスを提供できずにおり，今後，テキストベースから画像ベースへ，また，モバイルショッピングなどのEC(Electronic commerce)に対応するためのセキュリティ向上が図られ，普及していくものと思われる。

このWAPに対して，SIMカードでは，WAPブラウザの搭載が進み，セキュリティ強化のため，WAPサーバへの接続に「RSA暗号」を使用した認証が求められている。このWAPへの認証機能を“WIM(WAP Identification Module)”と呼び，この機能を搭載したSIMは“SWIM”と呼ばれる。

このように，SIMにブラウザ機能と認証機能を持たせることにより，新しいデバイスの追加なしに，安全にネットワークに接続することが可能となる。

3.2 第3世代携帯電話への対応

第3世代の携帯電話では，主に欧州でW-CDMA，米州では“CDMA2000”が主流となると見られている。W-CDMAではSIMカードの搭載が規格上必須となっているが，CDMA2000では，これがオプションとされており，搭載の義務はない。この第3世代に搭載されるSIMを“USIM(Universal Subscriber Identification Module)”と呼ぶ。

第3世代では，携帯端末と基地局間のデータ通信速度が最高で2.4Mビット/sと高速化が図られるため，WAPなどのネットワークを利用した，音楽・映像の配信サービスの充実が考えられる。

これに対し，SIMには複数のアプリケーションを搭載することになるため，マルチアプリケーションOS(Operating System)の搭載が進められており，この中でもJava※) OSが主流となってきている。当初，ICカードでは，このJava OSは，各OS開発者が独自に開発し，互換性のないものであった。最近は，Javaカードフォーラムによって標準化が進み，互換性の確保が進められている。

また，既存GSMとの互換性の確保も重要視され，USIMカードには，GSMアプリケーションのプログラムやデータも搭載される。

このように，USIMカードには，(1) 大容量メモリと，(2) それに格納される大量のデータを扱うための高速データ処理，(3) 高速データ転送，および (4) 高セキュリティが要求される。

4 カード用マイコンへの取組み

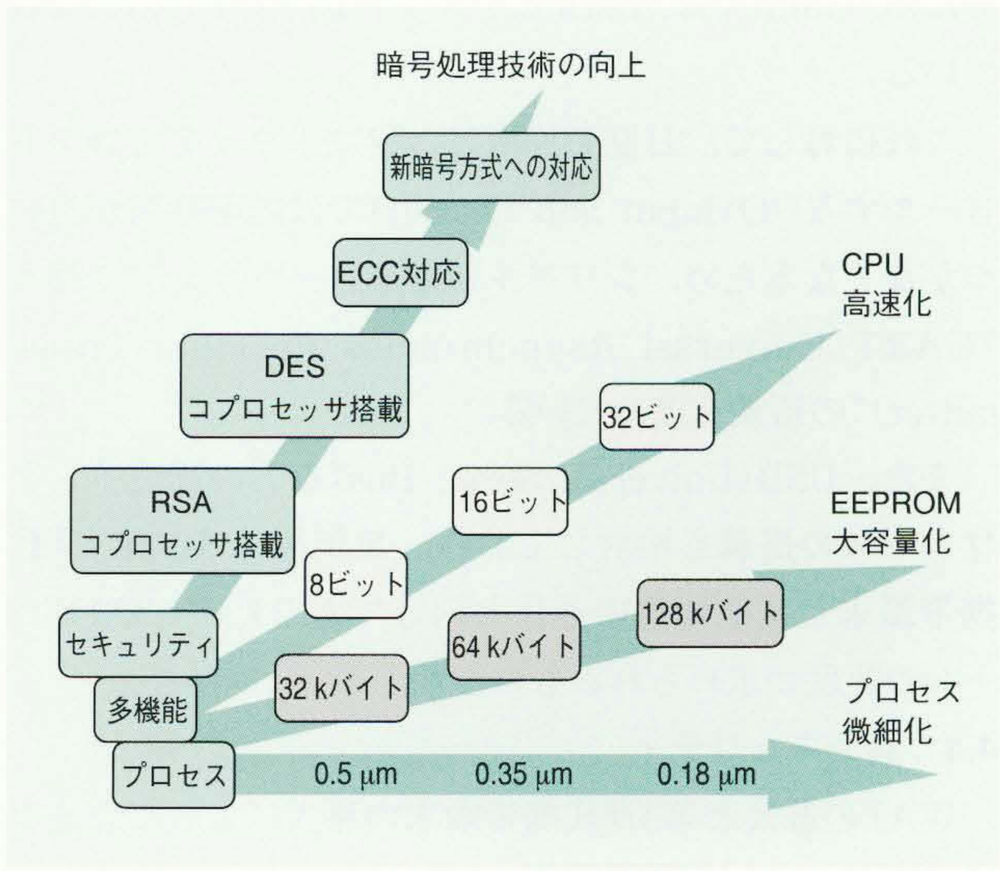
日立製作所は，前述したSIMカードに対する要求を満たすためのさまざまな取組みを行っている(**図3**参照)。

4.1 大容量・高速EEPROM

SIMカードの多機能化に伴い，アプリケーションプログラムや，データを格納する不揮発性メモリの大容量化が進んでいる。

この不揮発性メモリには，EEPROMを使用するのが一般的である。しかし，RAMに比べてEEPROMのデータの書き換え速度は遅く，処理速度向上の妨げとなっている。

このため，日立製作所は，このEEPROMに一般に採用されているフローティングゲート型とは異なる，MONOS(Metal-Oxide-Nitride-Oxide-Silicon)型と呼ばれる独自の方式を採用している。この方式は，フローティングゲート型に比べて信頼性が高く，メモリセルの小型化に適している。この特性を生かして，プロセスの微細化により，大容量化への対応，書き換え速度の高速化を図っている。



注：略語説明
ECC(Elliptic Curve Cryptography)
DES(Data Encryption Standard)
RSA(Rivest，Shamir，Adelman)

図3 ICカード用マイコンの開発ロードマップ
高機能化するSIMのニーズに対応するため，ICカード用マイコンでは，動作速度やメモリ容量など，いっそうの進化が図られている。

※) JavaおよびすべてのJava関連の商標およびロゴは，米国およびその他の国における米国Sun Microsystems, Inc.の商標または登録商標である。

4.2 高速・低消費電力CPU

SIMカードの高機能化に伴う，Javaなどのマルチアプリケーション OSの搭載により，CPUにも高速化が要求されている。

しかし，バッテリ駆動の携帯端末に搭載されるSIMカードには，低消費電力化という相反する命題があり，規格でも最大消費電流が規定されている。

高速化の手段としては，処理ビット数の拡大や，クロックの高速化，パイプライン処理，命令の最適化などが図られている。

また，この高速化に伴って増加する消費電流を抑えるためには，(1) プロセスの微細化，(2) 動作電圧の低減，および (3) 必要なブロックだけを動作させるブロック選択動作が有効な手段である。

日立製作所は，0.35 μmプロセスを使用した，16ビットCPU搭載の「AE-4 シリーズ」をすでに発売しており，今後も，0.18 μmプロセスの採用と，32ビットCPU搭載の「AE-5シリーズ」の開発により，いっそうの高速化と低消費電力化を図っていく計画である。

4.3 高速データ転送

取り扱うデータ量の増加により，携帯端末とSIMカード間のデータ通信にも高速化が要求されている。

これまでのSIMでは9.6 kビット/sが主流であったが，近年は，100 kビット/s以上の速度が要求されている。このため，USIMでは，156 kビット/sが規格上で必須となっている。

これに対して，日立製作所は，ソフトウェアでコントロールするI/O(Input and Output)では処理時間が追いつかなくなるため，シリアル通信をハードウェアで行う“UART(Universal Asynchronous Receiver-Transmitter)”の搭載を進めている。

また，USB(Universal Serial Bus)などの高速インタフェースの搭載も検討しており，数年後には，第3世代携帯端末と基地局間の通信と同等である1 M～2 Mビット/sの速度が求められるものと考える。

4.4 高セキュリティ

WAPの普及と第3世代携帯端末の導入によって急速な進展が予想されるECに対応するために，偽造や情報改ざんなどの不正行為を防ぐ防御手段が重要性を増している。

このため，日立製作所は，まずネットワーク上での情報のセキュリティとして，「AE-4 シリーズ」にDES(Data Encryption Standard)アクセラレータを標準搭載としたほか，RSA暗号やECC処理に適したコプロセッサ搭載品のラインアップを拡充し，各種暗号処理に対応している。

次に，ICチップ内の情報のセキュリティとして，CPUの誤動作を防ぐため，異常な動作環境を検出する電源電圧・クロック周波数検出器や，メタル層でのチップ配線のシールド，内部データの暗号化などのさまざまな対策を二重三重に施している。

また，日々進歩しているチップの解析技術に合わせて，研究所で最新技術を開発しているほか，第三者機関による評価を通じて対策を施している。

5 おわりに

ここでは，ICカードのアプリケーションを代表するSIMカードについて述べた。

SIMカードは，携帯電話ネットワークの中で，サービス・セキュリティの向上に欠かせない中核を担うデバイスとして，今後もますます発展していくものと考える。

日立製作所は，このSIMカードのニーズに合ったICカード用マイコンの開発をさらに進めることにより，今後，(1) 大容量・高速不揮発性メモリ，(2) 32ビット高速・高機能CPU，および (3) 各種周辺機能を搭載したマイコンを提案し，携帯電話の利便性と安全性の向上に貢献していく考えである。

参考文献

1) 株式会社シーメディア：モバイル総覧(2000)

執筆者紹介

高本伸雄
1992年日立製作所入社，半導体グループ ICカードビジネスユニット 所属
現在，ICカードマイコンのマーケティングに従事
E-mail：takamoto-nobuo @ sic. hitachi. co. jp