住民基本台帳カード
― Java™ 言語を使ったアプリケーションに対応

National ID Card Supporting Java™ Applications

清水　博夫　　**福田　亜紀**

■ SHIMIZU Hiroo　　■ FUKUDA Aki

2003年8月から交付予定である住民基本台帳カード（以下，住基カードと略記）は，住民票の写しの広域交付，転入転出の特例及び本人確認業務などに利用され，住基カード用リーダライタと通信することで各業務を実現する。

今回，東芝は，住基カード向けの非接触ICカードをLSI及びカードオペレーティングシステムを含め新規に開発し，住民基本台帳仕様，JavaCard™（注1）仕様，及び近接型ICカードの標準であるISO/IEC14443 TypeB（ISO：国際標準化機構，IEC：国際電気標準会議）を基本仕様とした通信インタフェースに対応した。更に，セキュリティを高めるための耐タンパ性に優れた暗号処理を搭載していることを特長としている。

The national ID card, to be issued in Japan from August 2003, will be used for the issuance of copies of resident cards over a wide area as well as special registration measures for address relocations and verification of applicants. Each of these municipal services will be realized by accessing a reader/writer designed for the national ID card.

For the national ID card, Toshiba has developed a new contactless IC card with the card operating system contained in an LSI, enabling it to support multiple JavaCard™ applications. The communication interface of this IC card complies with ISO/IEC14443 Type B. Moreover, to ensure advanced security this IC card is equipped with an encryption process incorporating highly improved tamper-resistant functions.

1　まえがき

近年，非接触ICカードの普及は目覚ましく，交通システム，入退管理，物流管理に利用されている。更に，現在個人認証用としての用途などにも検討がなされている。また，（財）ニューメディア開発協会が中心となり，“近接型通信インタフェース実装規約 第1.1版”に基づいたIT（情報技術）装備都市研究事業の実証実験なども行われ，行政系に非接触ICカードが使用される可能性が広がり，実現に向かっている。

住民基本台帳ネットワークシステムは，各市町村で管理する住民基本台帳を基礎に，全国の市町村を電気通信回線で結び，住民基本台帳事務を効率化するために導入するものである。このシステムにおいて，住基カードは住民票の写しの広域交付，転入転出の特例及び本人確認業務に利用され，住基カード用リーダライタと通信することで，各業務を実現する。

また，追加発行可能なマルチアプリケーションカードとして，業務利用に必要な基本機能を備えるとともに，住民基本台帳法に基づいて定められた市町村の条例により，市町村の独自利用にも供される。

なお，行政系の非接触ICカードである住基カードは，2003年8月に交付される予定である。

（注1）　Java及びその他のJavaを含む商標は，米国Sun Microsystems, Inc.の米国及びその他の国における登録商標又は商標。

ここでは，東芝の住基カードの仕様，主要技術，及びその特長について述べる。

2　住基カードの概要仕様

住基カードの外観を**図1**に，概略仕様を**表1**に示す。

偽造防止のため，券面印刷にパール印刷やマイクロ文字を採用している。CPUは16ビット，メモリはROM，RAM，不揮発性メモリから成る。

図1．住基カード― 85.6×53.98×0.76 mmサイズのICカードである。
Sample national ID card

表1．住基カードの概略仕様
Basic specifications of national ID card

項　目	仕　様
外形寸法	85.60 × 53.98 × 0.76 mm
カード材	非ポリ塩化ビニル
磁気ストライプ	あり（JIS Ⅱ 型，隠ぺい）
エンボス	あり（点字エンボス）
偽造防止印刷	特殊インク（OVI，パールなど），マイクロ文字
CPU	オリジナル16ビットCPU
メモリ	ROM：128 Kバイト／RAM：4 Kバイト 不揮発性メモリ：32 Kバイト
インタフェース	非接触のみ，ISO/IEC14443 TypeBに準拠
伝送レート	106 kbps/212 kbps ただし，衝突防止処理中は106 kbps固定
最小動作磁界	4 A/m以下
最大動作磁界	7.5 A/m以上
主要機能	・JavaCard™によるマルチアプリケーション対応 ・暗号コプロセッサ搭載（RSA演算）

OVI：Optically Variable Inks

通信インタフェースは，近接型ICカードの標準であるISO/IEC14443 TypeBを基本仕様としている。なお，ISO/IEC14443は，13.56 MHzを基本周波数とした近接型非接触ICカードに関して規定しており，物理的特性，通信方式，衝突防止方式，通信プロトコルなどを定めている。

マルチアプリケーションに対応するため，JavaCard™仕様を用いて実現することとした。また，暗号アルゴリズムとしては，DES（共通鍵暗号）及びRSA（公開鍵暗号）を採用しており，RSA暗号演算を実行するためのコプロセッサを搭載している。

3 ハードウェア構成

住基カードのハードウェア構成を**図2**に示し，その特長を次に述べる。

住基カードは，LSIとループアンテナで構成しており，LSI内部は，CPU，メモリ，コプロセッサ，無線通信制御部（RF部），変復調回路，及び電源部から成る。

CPUは各機能の制御を行っており，メモリは，作業領域であるRAM，制御コードを搭載するROM，データの書換えが可能な不揮発性メモリの3種から成る。

また，住基カードでは，暗号機能（コプロセッサなど）を駆使して重要なデータを保護している。具体的には，証明書検証，認証，セッションキー設定，パスワード照合を行わなければデータを読み出せるアクセス条件が成立せず，更に，読み出されるデータはセッションキーで暗号化されているため，万一，盗み取られたとしても，それがどのようなデータであるのか判別することは極めて困難である。

ループアンテナ，RF部，変復調部では，住基カード用リーダライタとの送受信を行っている。

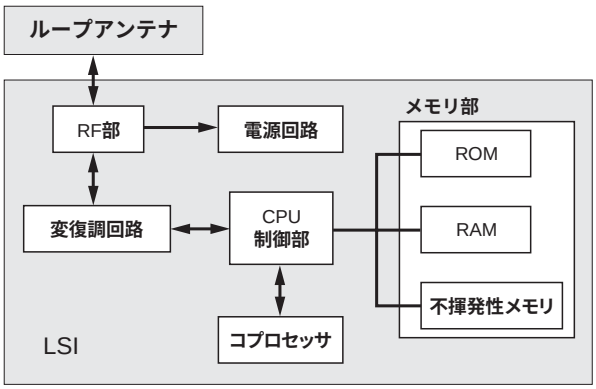

図2．住基カードのハードウェア構成 ― ループアンテナとLSIで構成している。
Hardware configuration of national ID card

住基カード用リーダライタからの電磁波を住基カードで受信する場合は，ループアンテナで10％ASK（Amplitude Shift Keying）に変調された電磁波を受信し，RF部にてフィルタやアンプを通過後，復調回路にてA/D（Analog-to-Digital）変換されたNRZ（Non-Return to Zero）符号化信号を，制御部にて復号化することにより信号を受信する。

住基カードから住基カード用リーダライタへ送信する場合は，制御部にてNRZ-L（L for level）符号化した信号を，変調回路やRF部にてD/A（Digital-to-Analog）変換し，サブキャリア847.5 kHz BPSK（Binary Phase Shift Keying）に変調された電磁波が，ループアンテナから送信される。

また，住基カードはバッテリーレスであり，リーダライタからの電磁波から電源を生成する。電源部では，ループアンテナで受信した電磁波を整流した後，平滑化コンデンサやシャントレギュレータなどにより，安定な電源を生成している。

次に，今回のハードウェアの特長を以下に挙げる。

RF特性を向上させ，多種類ある住基カード用リーダライタとの互換性を取るため，共振周波数や帯域幅を変更した多種多様なループアンテナを設計し，最適化設計を行った。また，カード化後，住基カードの変調度などのRF特性を変更できるように，抵抗などのパラメータを可変に設定できる機能を追加した。

これらの機能の追加により，互換性試験にも対応することが可能となった。また，各種パラメータを変えるごとに，LSIを新たに開発する必要がなくなった。

4 ファームウェア及びファイルの構成

住基カードのファームウェア及び不揮発性メモリ内のファイルの構成を**図3**に示す。ファイル構成としてアプリケーション層の中のカードドメイン（CD）がルートディレクトリであり，

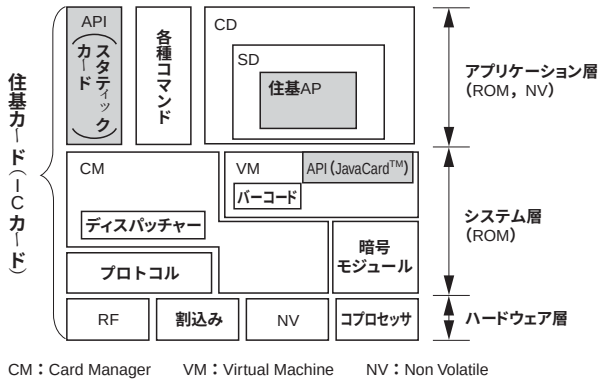

図3．住基カードのファームウェアの構成 ― アプリケーション層に住基APが搭載されている。

Firmware configuration of national ID card

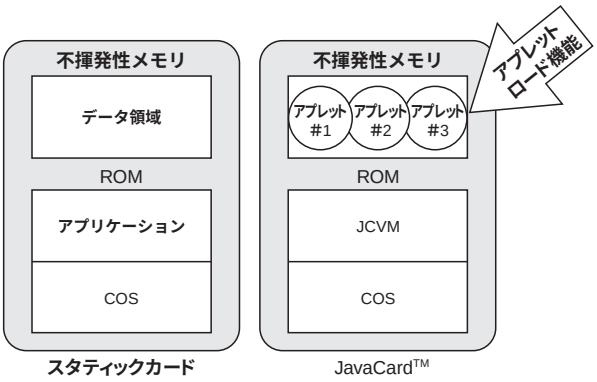

図4．スタティックカードとJavaCard™の比較 ― JavaCard™はアプレットを追加できる。

Comparison of static card and JavaCard™

サービスドメイン（SD）は，住基アプリケーション（住基AP）が格納されているディレクトリである。ICカードでは，通常，アプリケーションはディレクトリ単位で管理されている。住基APも一つのディレクトリであり，ディレクトリ内には，JavaCard™アプリケーション（アプレット），又は複数のファイルを格納することができる。

JavaCard™アプリケーションから使うことのできるAPI（Application Programming Interface）を2種類用意している。一つはJavaCard™APIであり，もう一つはスタティックカードのAPIである。JavaCard™APIは，Sun Microsystems, Inc.が規定したJavaCard™ 2.1.1仕様に準拠している。JCRE（JavaCard™ Runtime Environment），JCVM（JavaCard™ Virtual Machine），JavaCard™APIは，既にSun Microsystems, Inc.の互換性試験にも合格したカードから，ソースコードを流用している。JavaCard™アプリケーションから使うことのできるスタティックカードのAPIは，住基AP内のファイルにアクセスするために必要な機能をAPI化したものである。暗号モジュールは，DESとRSAがあり，どちらも，外部機関で耐タンパ性の評価を行い，安全性が確認されたカードから，ソースコードを流用している。

ICカードを大別すると次のようになる（**図4**）。既存のICカードとしては，アプリケーションを追加できるタイプ（JavaCard™）と，アプリケーションの追加ができず，ROMを開発した時点でサポートするアプリケーションが決まってしまうタイプ（スタティックカード）の2種類がある。スタティックカードは，不揮発性メモリ内にファイルシステムを構築し，ファイルへのアクセス制御を行うことでアプリケーションの実現を行う。アプリケーション間のファイアウォールは，COS（Card Operating System）が管理している。

Java™アプリケーションを実行できる環境を構築するためには，JCRE，JCVM，JavaCard™APIを提供する必要があるため，ROMに格納するプログラムが大規模になる。

これに対し，スタティックカードのメリットは，少ないROMリソースで多機能なアプリケーションを提供できることと，不揮発性メモリの使用量が少なくて済むことである。なぜならば，スタティックカードは，実行プログラムをROMに持っており，不揮発性メモリ内にはファイルのみが格納されるのに対し，JavaCard™は，不揮発性メモリ内に実行プログラムとデータを格納するため，同じデータサイズであれば，実行プログラムを不揮発性メモリに格納している分だけ，不揮発性メモリを多く使用することになる。

今回開発した住基カードは，これら2種類のタイプのICカードを合わせた仕様となっている。すなわち，JavaCard™仕様を用いたアプリケーション追加と，スタティックカード仕様による高いメモリ効率を可能としている。

カードに搭載するアプリケーションを記述する言語としてJavaCard™仕様を採用した理由を次に述べる。アプリケーションの追加を行う場合に，アセンブラでアプリケーションを開発し，カードにダウンロードすることも可能である。ところが，アセンブラで開発されたアプリケーションでは，アプリケーション開発者用に提供されているAPI以外に，ROM，RAMあるいは不揮発性メモリへの直接アクセスにより，セキュリティ情報に関連するプログラム又はデータを操作することが可能となってしまう。したがって，悪意のある第三者が用意した盗聴用のアプリケーションをダウンロードすることで，メモリから住基AP内のデータを直接盗み出すことができるようになってしまう。

これに対し，JavaCard™では，JCREやJCVMにより管理された実行環境上でのみ，アプリケーションが実行可能となっている。もし，盗聴用にアプリケーションをダウンロードしたとしても，提供されているAPIではメモリに直接アクセスできない。また，JavaCard™の仕様として，自分以外のアプ

リケーションにアクセスするためには，アクセスされる側のアプリケーションにアクセス許可を求める必要があり，アクセスされる側のアプリケーションは，アクセスを許可していないアプリケーションに対して，データを渡さない仕様になっている。住基APは，外部からのアクセスを許可していないことで，住基AP外から住基AP内のデータを読み出すことは不可能となっている。

住基AP以外のアプリケーション追加の要求があった場合に備えて，開放できる不揮発性メモリをできるだけ広く確保しておく必要がある。住基アプリケーションをJavaCard™のAPIのみで開発してしまうと，ファイルシステムへアクセスするための機能も不揮発性メモリ内の実行プログラムに入ってしまう。これを回避するために，スタティックカードで使用するファイルシステムへアクセスするために必要な機能をAPIとして用意し，そのAPIを使えば，効率よくJava™言語を使ったアプリケーションが開発できるようになる。ファイルの創生は，外部からのコマンドによって行う。Java™言語を使ったアプリケーションにおいて，創生されたファイルへの読出し，書込みなどを行うには独自APIを使う。これにより，Java™言語を使ったアプリケーションと同じディレクトリ内に，スタティックカードと同等なファイルシステムを構築できる。

図5は，当社独自の仕様として搭載したメモリへの書込み処理フローを示している。非接触ICカードは，動作に必要な電源を，アンテナを介して外部から供給している。このため，リーダライタとカード間の電波の状態により，電源が不安定な状態となりやすい。電源が不安定になった場合に問題となるのが，不揮発性メモリへの書込み処理である。当社の住基カードでは，不揮発性メモリの書込み前にいったんバッファ領域に書込みを行い，その後，書込み対象となる領域に書込みを行っている。もし，バッファ領域の書込み中に電源が落ちてしまっても，本来の書込み対象エリアは書込み前の状態を保持している。また，バッファ領域の書込み後，本来の書込み対象領域に書込み中に電源が落ちてしまっても，次にカードが起動した時点でバッファ領域から本来の書込み対象領域への書込みを実施して，書込み後の状態としている。これによりカード内のデータは，たとえ書込みの失敗があったとしても，書込み前か書込み後のいずれかの状態が保証されている。

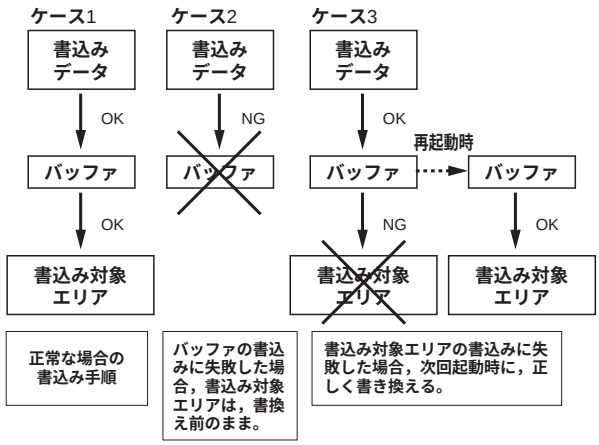

図5．不揮発性メモリへの書込み ― 正常ケースと異常ケースの処理フローである。カード内のデータは書込み前か，書込み後の状態が保証される。
Writing to flash memory

5 今後の課題

住基カードなどの非接触ICカードは，多方面のシステムで活用される機会が多くなるため，リーダライタが異なると通信できなくなるなどの問題が起きないように，互換性を高める必要がある。そのためにも，互換性に影響する規格にないパラメータを検討していく必要がある。また，通信時間短縮のため，高速伝送レート化が規格化されつつあり，今後対応していく必要がある。

また，住基カードは個人情報を扱うものであり，非常に高いセキュリティ性が要求されている。ISO/IEC15408に基づいたチップとファームの評価を行い，公的に認められた高いセキュリティを備えた製品としていく。

6 あとがき

今回，住基カード向けの非接触ICカードを開発したことにより，JavaCard™仕様によるマルチアプリケーション対応，近接型非接触ICカードの標準であるISO/IEC14443 TypeBに準拠した通信インタフェース対応，及びセキュリティを高めるための耐タンパ性に優れた暗号処理への対応が可能となった。これらの機能をより高め，今後の製品にも反映させていきたい。

清水　博夫　SHIMIZU Hiroo
社会ネットワークインフラ社　システムコンポーネンツ事業部
カードシステム部。ICカードシステムの開発に従事。
System Components Div.

福田　亜紀　FUKUDA Aki
社会ネットワークインフラ社　システムコンポーネンツ事業部
カードシステム部。ICカードシステムの開発に従事。
System Components Div.