

IC カード

～ FeliCa と JavaCard ～

大西 祥代, 細江 則彰

Sachiyo ONISHI, Noriaki HOSOE

1 はじめに

近年, 多くのカードが磁気カードから IC(Integrated Circuit: 集積回路) カードへと移行している。その背景には, 電子マネーが組み込まれた高度なセキュリティを要するカードや, 一枚で複数のサービスを提供するカードなど, 大量の情報を扱い, 安全性・信頼性が必要なカードサービスが登場していることがある。

この実現に欠かせないのが IC カードである。IC カードは磁気カードと比べ, 大容量の情報を記憶でき, 高い安全性を実現し, そして一枚のカードで複数のサービスを搭載できる拡張機能がある。IC カードには, CPU, OS, 通信に関する様々な技術が必要であるが, 本稿では FeliCa と Java Card という技術に注目する。

2 IC カード

IC カードとは, プラスチックカードに, CPU や IC メモリなどの IC チップを内蔵し, 情報を記録できるようにしたものである。これにより, 複雑な暗号処理と多様な機能の搭載が可能となり, 拡張機能も備えられる。また, 変造や解析が難しく, セキュリティ機能に優れている。

2.1 IC カードの種類

IC カードは以下のように分類することができる。

- 接触型

IC カードとリーダ/ライターが接触するタイプで, 通信傍受が強く, トランザクションも安定しているため, クレジットカードに用いられることが多い。

- 非接触型

カードとリーダ/ライター間で無線通信を行う方式である。ソニーが開発した FeliCa などがあある。

- 接触/非接触型

接触と非接触それぞれのインタフェースで 1 つの IC チップを共有するコンビカードと, IC チップを持つ 2 チップ型のハイブリットカードがある。

2.2 IC カードの構成要素

IC カードは以下の要素で構成されている。

- CPU
中央演算処理装置で IC チップの頭脳中枢である。
- ROM
プログラムなど書換えの不必要なデータを格納する。
- RAM
プログラム処理時など一時的処理のためにデータを格納する。
- EEPROM
バイト単位で内容の書き換え, 消去が可能な ROM。一般的なデータを格納する。

これらの要素により, 接触型カードは Fig. 1(a) に示す構造に, また, 非接触型カードは Fig. 1(b) に示す構造となっている。

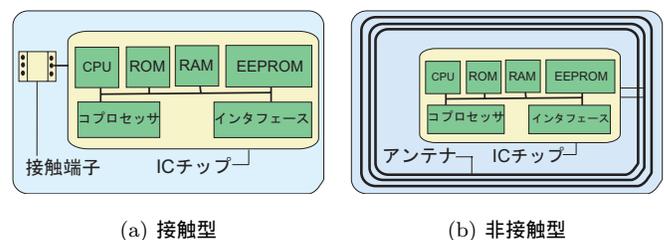


Fig. 1 物理的構造

3 IC カード技術

本節では, 日本が開発した非接触型 IC カードの技術 FeliCa と, 世界的に普及している IC カード技術の Java Card という 2 つの技術について述べる。

3.1 FeliCa

FeliCa とはソニーが開発した IC カード技術である。Edy, ICOCA, そして PiTaPa などで採用されている。

3.1.1 FeliCa の特徴

FeliCa の特徴は以下のようなことが挙げられる。

- 非接触型
- 携帯や時計などへの組み込みが可能
- 高い安全性を実現
- スピーディーなデータの送受信が可能
- 一枚のカードで複数種類のデータ管理

3.1.2 FeliCaによるマルチアプリケーション

FeliCaでは一枚のカードで複数の機能を搭載できる。各々のデータには個別のアクセス権を設定することが可能で、これによりアプリケーション間の安全な相互運用が実現される。Fig. 2のようにICカード内のファイルシステムは「エリア」と「サービス」の階層構造となる。エリアはフォルダに相当するもので、サービスは、データに対するアクセスの種類や権限を定義する。エリアやサービスに設定されるアクセスキーは、権限のないものがサービスにアクセスすることを防ぎ、アプリケーション・ファイアウォールを実現する。また、複数のアクセスキーを合成した縮退鍵を利用する。縮退鍵により、アクセス対象が複数にわたる場合でも、一回の相互認証で複数のファイルをオープンすることができる。

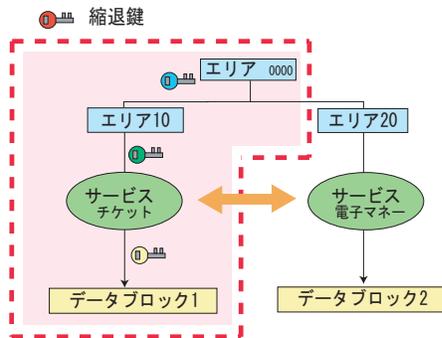


Fig. 2 FeliCaのマルチアプリケーション

3.2 Java Card

JavaCardは、米国SunMicrosystems社が開発したICカードのプラットフォームである。Javaの命令群の中からICカードで利用するのに必要なものをピックアップし、APIで提供する。米国国防総省の身分証カードとしても採用されるなど、全世界で約3億枚の発行実績があり、デファクトスタンダードとなっている。

3.2.1 Java Cardの特徴

JavaCardの特徴は次のようなことが挙げられる。

- カード発行後にサービスの追加・削除・更新が可能
- Java言語によるアプリケーションの開発が可能
これまでカード・ベンダーに依存していたアプリケーション開発がカード事業者自らできるため、開発期間の短縮および開発コストの削減ができる。
- 安全なマルチアプリケーション環境を実現
アプリケーション同士の相互干渉が起きないJava言語の特性により、1枚のカードで独立した複数のサービスプログラムを書き込むことが可能となる。

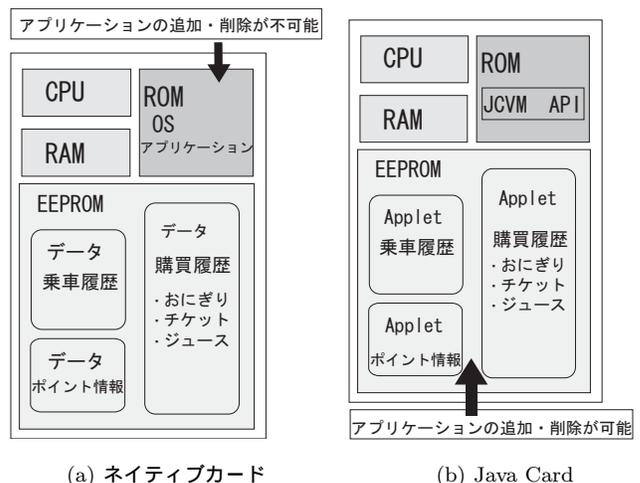
3.2.2 Java Cardによるマルチアプリケーション

Fig. 3(a)は専用OSが用いられるネイティブ(専用)カードである。これには次の問題点がある。

● 各カードメーカーごとに固有のカードOSを搭載し、アプリケーションを開発する際のAPIも固有の仕様であるため、アプリケーションが特定のOSにしか対応できず、サービスの多様性を妨げる。

- OSとアプリケーションが一体化した形でROMに格納するのでアプリケーションの追加・削除ができない。

そこで特定のOSに依存しないプラットフォームであるJava Cardを用いることで、追加・削除・更新が可能なマルチアプリケーションを実現する。Fig. 3(b)にJava Cardを示す。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、JCVMやAPIの提供が必要で、これらはROMに格納する。そしてEEPROMにアプレットを追加・削除する。ネイティブカードと比べると、EEPROMに実行プログラムを格納する分、メモリ効率が悪くなるという問題点もある。



(a) ネイティブカード (b) Java Card
Fig. 3 ネイティブカードとJava Cardの比較

4 今後の展望

今後もICカードによる様々なサービスが展開されていくが、現存するサービスを利用しつつ、新たなサービスを導入していくことになる。新旧どちらのサービスにも対応するための有効な手段として、接触型/非接触型カードの普及が考えられる。接触型でJavaCardを採用することにより、新サービスのアプリケーションをカードにダウンロードすることができる。また、非接触型でFeliCaなどを搭載し、現在の交通乗車券のサービスや電子マネーのサービスをそのまま使うことができる。このような複数のサービスを統合できるカードが発展していくと考えられる。

参考文献

- 1) <http://www.sony.co.jp/Products/felica/>
- 2) http://jp.sun.com/newsletters/innercircle/03_07_22/feature03.html
- 3) http://www.dnp.co.jp/bf/ic_card/index.html