

ICカードを使ったシステム開発の基礎

藤田 崇

鉄道の定期券、クレジット・カード、入退室用管理カードなど、ICカードの応用分野はどんどん広がっている。本章では、このICカードを使ったシステムを開発するための基礎知識を紹介する。ICカードの分類から、ファイル・システム、カードとの通信、ICカード操作のためのAPIまでを解説する。
(編集部)

はじめに

ICカードにはICチップが埋め込まれています。ICチップは、CPUやメモリ、ROM、EEPROMが搭載された半導体集積回路です。ソフトウェアとしては、OSやカード・アプリケーションが搭載されます。ICチップだけで一つのコンピュータといえます。現在普及しているICカードは、外部インターフェースという点から接触型と非接触型に分けられます。

接触型は、主に金融機関のキャッシュ・カードやクレジット・カードなどに利用されています。非接触型は、交通機関や携帯電話などに利用されています。最近では、両方のインターフェースを1チップの中に実装したデュアル・インターフェース型と呼ばれるものもあります。搭載しているOSという点で見ると、専用OSとマルチ・アプリケーションOSに分けられます。専用OSは、OSとカード・アプリケーションがROMに焼き込まれたもので、データのみEEPROMに格納されます。マルチ・アプリケーションOSは、VM (Virtual Machine) と呼ばれる汎用OSがROMに焼き込まれており、複数のカード・アプリケーションとデータがEEPROMに格納されます。カード発行後にカード・アプリケーションを追加したり、削除したりすることができます。専用OSが搭載されているカードはNative型ICカード[図1(a)]、マルチ・アプリケーションOSが搭載されているカードはプラットフォーム型ICカード[図1(b)]とも呼ばれます。

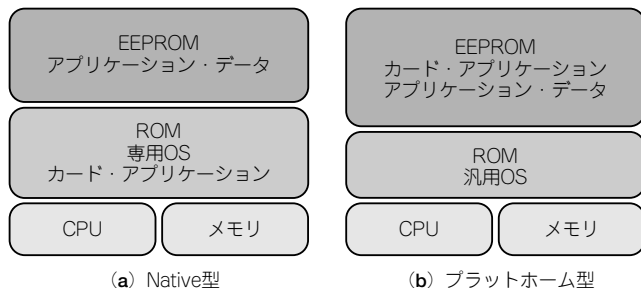


図1 カード・タイプ

ション OS は、VM (Virtual Machine) と呼ばれる汎用 OS がROMに焼き込まれており、複数のカード・アプリケーションとデータがEEPROMに格納されます。カード発行後にカード・アプリケーションを追加したり、削除したりすることができます。専用OSが搭載されているカードはNative型ICカード[図1(a)]、マルチ・アプリケーションOSが搭載されているカードはプラットフォーム型ICカード[図1(b)]とも呼ばれます。

1. システム構成

一般的なICカードを扱うシステムは、PCSC Working Groupを中心に策定された「Interoperability Specification for ICCs and Personal Computer Systems」⁽⁴⁾を元に構成されます。図2に主なコンポーネントと構成例を示します。



図2 システム構成例

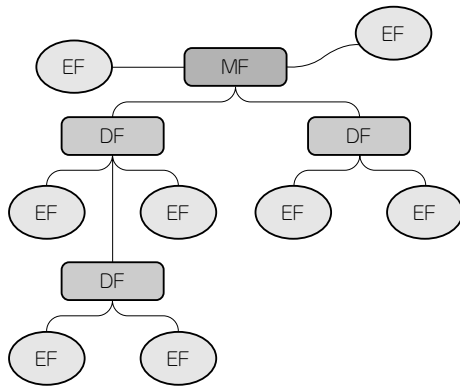


図3
ファイル構造

表1
ファイル識別子

識別子	用途
3F00	MFの識別子
2F00	DIR (EF) の識別子
3FFF	パス指定時に利用
FFFF	未使用

ビス・プロバイダに相当する PKCS#11 (Cryptoki) API の開発手順などを紹介します。

2. ファイル・システム

● 概要

ISO/IEC 7816-4⁽¹⁾においてICカード内のファイルは、図3のような階層的なファイル・システムとして規定されています。

MF (Master File) はカード内に一つだけ存在するファイルで、一般的なファイル・システムではルート・ディレクトリに相当します。DF (Dedicated File) は、ファイル階層の区切りを表すファイルです。一般的なファイル・システムのディレクトリに相当します。しかし、このファイルそのものには読み書きできるデータはなく、一般的なファイル・システムのディレクトリが持っているような下位階層のエントリ情報を持っていません。

EF (Elementary File) は、バイナリ・データを格納するファイルです。通常、ファイル・サイズは作成時に決まる固定長になります。一般的なファイル・システム上のファイルのように、追加するとファイル・サイズが増えていくようなことはありません。

(1) ファイル識別子

ファイルは2バイトのコードで識別します。予約されている識別子は表1のとおりです。

特定のファイルを指定するには、このファイル識別子を必要分連続して記述します。これをパスと呼びます。カードがワイルド・カードをサポートしている場合は、途中の階層に3FFFをワイルド・カードとして指定できます。パスの指定は、MFからの絶対パスを指定するか、カレントDFからの相対で行います。なお、DFは1～16バイトまでの文字列で識別可能ですが、パスに含めることはできません。

(1) ICC (IC カード)

ICカードは規格や標準が幾つか存在し、用途に応じて構成方法が異なります。ベンダによっても違いがあります。

(2) IFD (Interface Device)

ICカードと通信するためのデバイスを表します。いわゆるICカード・リーダー/ライターに相当します。IFDとホスト間のインターフェースには、RS-232-C、USB、PS/2などが用いられます。

(3) IFD ハンドラ

IFDと通信するためのハンドラです。デバイス・ドライバに相当しますが、単純なデータの転送を行うだけでなく、コマンドの送信と応答の受信までをまとめて処理する必要があります。プラットフォームによっては、入出力(RS-232-C、USBなど)用のデバイス・ドライバとIFDハンドラを分離して実装する場合があります。

(4) IFD リソース・マネージャ

複数のIFDを管理するためのコンポーネントです。

(5) ICC サービス・プロバイダ

ICカードにアクセスするためのAPIを提供するコンポーネントです。ICカード側の相違はこの階層で隠ぺいされます。PKI (Public Key Infrastructure) 機能、つまり認証、署名・検証、暗号・復号などの機能は、この部分で提供されます。代表的なAPIとして、CryptoAPI⁽⁹⁾、PKCS#11 (Cryptoki) API⁽³⁾、GSC-IS BSI/XSI⁽⁸⁾などがあります。

(6) アプリケーション

ICカードを利用するアプリケーション・プログラムです。ICCサービス・プロバイダやICCリソース・マネージャが提供するAPIを利用して実装します。以下、ICカードを扱うための基本的な項目を確認した後、ICCサー