

## 多目的なICカードを共通的に利用するためのミドルウェア(1) ～課題の抽出と、対策およびアーキテクチャの検討～

2G-8

石原 達也, 麻野間 利行, 青木 恵, 才所 敏明  
株式会社 東芝 S I技術開発センター

### 1. はじめに

情報インフラが整備されたオープンなネットワーク上で、今後は、電子商取引、行政、医療、金融、教育などのさまざまなサービスが提供されていくことが予想される。それらのサービスにおいてセキュリティの確保は必須の課題であり、ICカードの利用、さらには1枚のカードでいろいろなサービスを受けることができるようになることが期待されている。しかし、各アプリが個別にカードにアクセスしていたのでは、そのような共通化は困難で、また、カードとの通信自体が煩雑であるという問題がある。そこで、カードを共通にかつ簡便に利用できるミドルウェアを提案する。

### 2. ミドルウェアの概要

通常、利用者がICカードを利用者個人の端末で利用するとき、そのカードの種類にあわせて個別の機能モジュールをインストールする必要がある。この煩雑な手順はICカードの簡便な利用にとって大きな障害となっている。

そこで、ミドルウェアのアーキテクチャとして、ICカードさえ受け取れば個別の機能モジュールをインストールせずに、ネットワーク上から動的にダウンロードし、すぐに利用できる環境の実現を検討した。

カードの形状や通信プロトコル、通信データユニットなどのカードの基本仕様は、ISO7816 という国際標準で決まっている。そして、カードの個々の機能を利用するカード命令、例えば署名生成などの機能を利用するためには、その基本仕様ベースに各ベンダが個別に決めたコマンドにより執り行う必要がある。

上位のアプリケーションがカードと直接通信する場合は、このISO7816に関する知識、プロトコルの違いへの対応、ベンダ毎のカード命令の詳細などを知る必要がある。また、カードに一度に送信できるデータ量や一度に行えることは少量であるため、一つのことを行うのに数回に分けてカードにアクセスする必要がでてきたりと煩雑である。

そこで、この煩雑さを避けて、カードの機能を簡便に利用できるようにするために、カードのある機能単位ごとに、対応する上位インタフェース、例えば、暗号/署名生成要求や電子マネーの引き出しといったものを、定義して、上位アプリはそのインタフェースさえたればカードの機能を利用できるように間を仲介することがミドルウェアの基本的役割となる。

### 3. 課題

これまでのカードでは、先ほど説明したようにISO7816で基本的なカードコマンドが決められているとはいえ実際にはベンダごとやカードの種類ごとに同じ機能であっても命令が異なっており、またそれらの命令は発行後に変更できなかったもので、同じ機能でも、カードの種類ごとにミドルウェアが必要になっていた。

つまり例えば、同じ署名インタフェースであっても、カードの種類が異なるとそれぞれ個別の機能モジュールが必要になっていた。

このため、今後カードが多目的に利用され機能が増えていく、と機能モジュールが乗算的に増えていくことになる。

よって、個別に作成している機能モジュールを共通化することが必須であると考えられる。

そこで、機能モジュールを共通化するとき発生する、課題を抽出した。

#### 1) プラットフォームの違い

これは主に OS の違いを指している。通常、複数のプラットフォームに対応したミドルウェアを作成する場合、プラットフォームごとにミドルウェアを作成するのが一般的である。

## 2) カードドライバの違い

カードドライバはベンダごとに異なっている。

## 3) カードの種類の違い

同じ機能であっても実際の命令はカードの種類ごとに異なる。また発行後は変更できない場合が多い。カードの種類によってはアプレット管理機能に差異がある場合もある。

## 4. 対策

機能モジュールを共通化するときが発生する、課題に対し、その対策を検討した。

1) 2) については、OpenCard Framework[1]や pc/sc[2]など従来からある考え方を応用し、3) については、従来に無い考え方を導入した。

### 1) プラットフォームの違い

→Javaを利用

プラットフォームと独立な言語そして実行環境を使うことにより、プラットフォームの違いを吸収できる。

### 2) カードドライバの違い

→ドライバ制御部による違いの吸収

個別の機能モジュールの下にミドルウェアのコアとなる部分を置き、そこにドライバの違いを吸収する機能を用意することでカードドライバへの依存性を排除。

### 3) カードの種類の違い

→機能毎にカードコマンドを共通化

Java カードのように発行後にプログラムを搭載することで機能を変更できるカードに限定し、カードの命令セットをあらかじめ決定しておく。

→アプレット管理機能の差をカード制御部で吸収

カードの抽象インタフェースを定義して個々のカードアプレット管理機能の違いを吸収。

それぞれを実現する基本的なアーキテクチャを検討した(図1)。

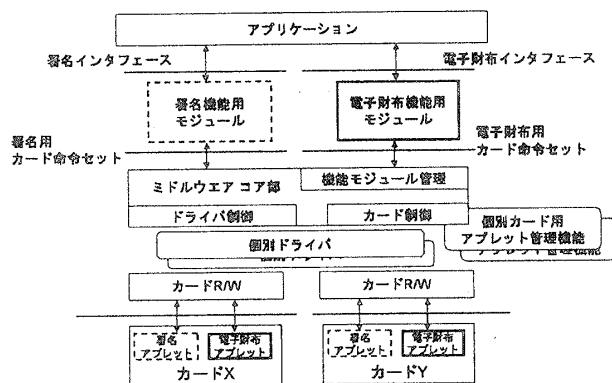


図1 基本的なアーキテクチャ

## 5. おわりに

多目的なICカードを共通的に利用するために必要な、機能モジュールの共通化における課題を抽出し、対策およびそれを実現する基本的なアーキテクチャを検討した。

## 6. 謝辞

本研究は、通信・放送機構の委託研究「マルチメディアネットワーク共通化技術の研究開発」によるものである。

関係各位のご支援に感謝する。

## 参考文献

[1] OCF Documentation :

<http://www.opencard.org/index-docs.html>

[2] PC/SC Workgroup Documents :

<http://www.smartcardsys.com/doc/content.html>