

家保 具太 吉澤 正浩 富沢 雅彰 竹田 忠雄  
NTT 生活環境研究所

### 1. はじめに

多目的 IC カードのビジネスモデルとして、1 枚の IC カードに複数のサービス提供者のアプリケーション (AP) を搭載することにより、サービス提供者間でコストシェアによるコスト低減を図り、利用者の IC カードの利便性を向上させるビジネスモデルが検討されている [1]。このサービスを実現するためには、複数のサービス提供者からの AP に対して、AP の追加格納・削除を行なう 2 次発行や非接触型 IC カードの複数枚差しに対応できるアプリケーション管理カードマネージャ (APCM) が必要となる。

本稿では、多目的 IC カード向けの AP 管理モデルおよび APCM について検討する。

### 2. 従来 IC カードの APCM の問題点

図 1 に従来の AP 管理モデルを示す。このモデルでは、サービス提供者にある AP 管理モジュールにより IC カード毎に AP を管理し、IC カードに格納する全ての AP が一括して IC カードに転送される。APCM は受信した AP を IC カードのメモリに格納する。IC カードに格納する AP の構成情報 (AP 格納情報) はサービス提供者によって一元的に管理される。このモデルの問題点を以下に示す。

- (i) サービス提供者が、個人情報である AP 格納情報を管理 (利用者のプライバシーの侵害、サービス提供者と依存関係あり)
- (ii) AP の構成がネットワーク上を經由して IC カードに転送 (セキュリティ情報の漏洩)

### 3. 多目的 IC カード向け APCM の検討

上記従来モデルの問題を解決する手法として、図 2 に示す AP 管理モデルを提案する。本モデルでは、AP 管理モジュールを IC カードの APCM 上に搭載し、AP 格納情報を IC カードのメモリに格納し、APCM により AP を管理する。このモデルの特長を以下に示す。

- (i) IC カードのメモリにおいて AP 格納情報を管理 (利用者のプライバシーの保護、サービス提供者との依存関係なし)

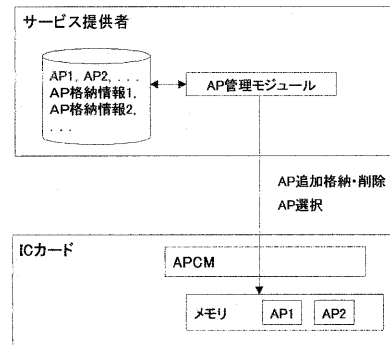


図 1. 従来 AP 管理モデル

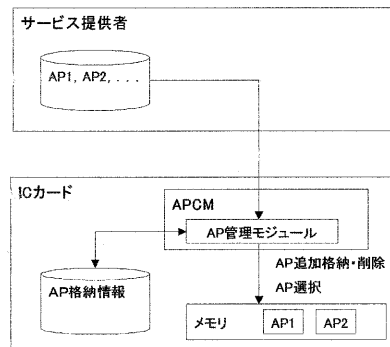


図 2. 提案 AP 管理モデル

- (ii) IC カード内 APCM の閉じた範囲内で AP 管理モジュールのみが AP 格納情報を使用 (セキュリティ情報の使用を制限)

本モデルでは、IC カードのメモリ上に APCM および AP 格納情報を格納し、IC カードの CPU で処理を行なうため、メモリ容量が多く、高性能な CPU を搭載する IC カードを要する。

### 4. AP 管理モジュールの検討

図 2 の AP 管理モデルの AP 管理モジュールでは、① AP の有効・無効判定、② AP の格納・未格納判定、③ AP の格納可否判定、④ AP の格納・削除、⑤ AP 格納情報の追加・削除、⑥ AP の選択、の処理を行なう。これらの処理を実現するために、AP 格納ブロック番号管理機能、AP フラグ管理機能、AP 格納空きブロック管理機能を追加

A Study of the smart card application manager for the multi-purpose smart card

Tomota Ieyasu, Masahiro Yoshizawa, Masaaki Tomizawa, Tadao Takeda

NTT Lifestyle and Environmental Technology Laboratories

3-1 Morinosato Wakamiya, Atsugi, Kanagawa, 243-0198, Japan

し、そのときの IC カードメモリの構成および AP 格納情報の項目について以下で述べる。

IC カードのメモリ内の構成は、AP 格納情報と AP 格納領域と AP 退避領域からなる (図 3)。AP 格納領域と AP 退避領域は同一の大きさであり、指定された一定の大きさのブロックで構成され、このブロック単位で AP の格納・削除を行なう。ブロック単位で管理することにより、AP の追加格納位置の決定や AP 格納領域の空き領域の判別をブロック番号の処理に簡略化できる。

次に、本稿で提案する機能について述べる。

AP 格納ブロック番号管理機能とは、入力された APID をもとに AP 格納情報の AP 格納ブロック番号を参照して AP を選択したり、追加格納した AP の格納位置である AP 格納ブロック番号を AP 格納情報に追加したり、AP フラグが無効である AP を削除するときに、AP フラグが有効の AP を AP 格納領域の先頭から再格納するために AP 格納ブロック番号を付け直したりする機能である。AP を削除するときには、AP 格納領域にある AP フラグが有効な AP のみを AP 退避領域に格納し、AP 格納領域のデータを消去して、AP 退避領域の全ての AP を AP 格納領域に格納する処理を行なうため、AP 格納領域と AP 退避領域の AP 格納ブロック番号を同一にしておけば、AP 退避領域に格納したときの AP 格納ブロック番号を利用することができる。

AP 格納フラグ管理機能とは、AP をメモリから削除する代わりに AP 毎のフラグを無効に設定して AP にアクセスできなくしたり、AP フラグを有効に設定してアクセス不能となっている AP を再度アクセス可能にしたりする機能である。両機能ともに、メモリ消去に時間を要する不揮発性メモリを搭載する IC カードの場合には、実際にメモリ消去を行なう頻度を減少させて処理を高速化するのに有効な機能である。

AP 格納空きブロック管理機能とは、AP を追加格納するときに、AP 格納領域に空きブロックがあるかを検証し、追加格納する AP が要するブロック数が空きブロック数よりも少ない場合に自動的に

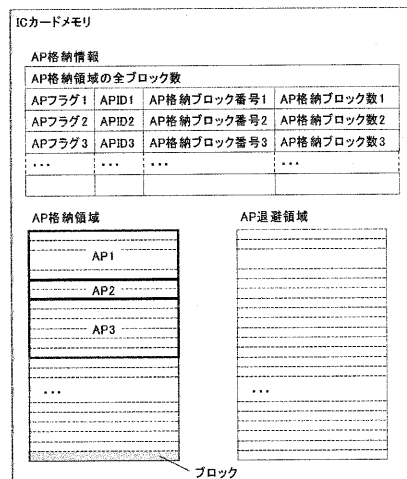


図 3. IC カードのメモリ内の構成

に AP フラグが無効となっている AP を削除する機能である。

## 5. 評価

本稿で提案した AP 管理モデルと従来モデルの比較結果を表 1 に示す。提案モデルでは、個人情報 IC カード内から外部に読み出されることなく管理され、利用者はサービス提供者に依存することなく IC カードに格納する AP を管理できることから、多目的 IC カードに適したモデルであることが確認できた。

## 6. まとめ

多目的 IC カードに適した AP 管理モデルと、そのモデルでの APCM について検討した。検討の結果、大容量メモリと高性能 CPU を搭載した高機能 IC カードが前提となるが、利用者が複数のサービス提供者からサービスを選択して IC カードに格納し多目的に利用できることから、提案モデルは多目的 IC カードのビジネスモデルに適していることがわかった。

今後は、IC カードに格納されている AP 管理情報のバックアップや IC カード紛失時のリストア等のライフサイクルを検討する予定である。

## 参考文献

- [1] IC カードシステム利用促進協議会、“日本工業規格準拠 JICSAP 外部端子付き IC カード仕様対応 発行ライブラリ仕様”、1998

表 1. 提案モデルと従来モデルの比較評価

	提案モデル	従来モデル
AP 格納処理	IC カードが受信するのは格納対象の AP のみ	IC カードに格納される全 AP を受信
AP 格納情報の使用範囲	IC カード内に限定	サービス提供者内に限定
多目的 IC カードへの適用性 (総合評価)	複数のサービス提供者からの AP 提供に対応	特定のサービス提供者からの AP 提供に限定