ソフトウェア工学 134－8
（２００１．１０．１８）

IC カードプラットフォームにおけるマルチ IC カード制御の提案

真壁 聡子、鈴木勝彦、山本修一郎

日本電信電話株式会社　情報流通プラットフォーム研究所
〒180-8585 東京都武蔵野市緑町 3-9-11
Telephon:0422-59-6137
e-mail:makabe.satoko@lab.ntt.co.jp

概要 最近、アプリケーションを複数搭載できるIC カードを運用するためのIC カードプラットフォームが大変注目されている。IC カードプラットフォームは、IC カードを管理するサーバ群と専用 IC カードとの組み合わせにより実現されている。しかし、IC カードプラットフォームとIC カードが 1 対 1 に対応していると、以下の問題がある。

・IC カード利用者は、異なる種別の IC カードを特定の IC カードプラットフォームで利用できない。
・サービス提供者は、IC カードプラットフォームごとにアプリケーションを開発しなければならない。
・カード発行者は、IC カードプラットフォーム専用の IC カードを発行しなくてはならない。

そこで、本研究では、複数のIC カードを１つのIC カードプラットフォームで収容するための実現方式を検討する。

A ploposal of multi smart card controls for smart card platforms

Satoko Makabe , Katsuhiko Suzuki , Syuichiro Yamamoto

Information Sharing Platform Laboratories,NTT
3-9-11,Midori-cho Musashino-shi,Tokyo 180-8585 Japan
Telephone:+81 422 59 6137
e-mail:makabe.satoko@lab.ntt.co.jp

Abstract In recent years, smart card platforms for managing multi-application purposed smart cards are paid to much attention. Each smart card platform is composed by a group of servers and the dedicated smart cards. The one-to-one relationship between smart card platform and smart card, however, produces many problems for the users of smart card platform s

In this paper, I discuss a achievement method to support multiple smart cards with the smart card platform.

1 はじめに

近年、電子商取引の普及に伴い、IC カードは高セキュリティ・高機能なデバイスとして大変注目されている。金融・通信分野では磁気カードの代替として既に実用化されており、公共・医療・交通分野でも今後適用されることが決まっている。これにより、IC カードの国内発行枚数は 2005 年までに 5 億枚を超え、各分野に適した IC カードが発行されると予測される。[1]

IC カード技術として、複数のアプリケーション（以降、AP）の搭載が可能な多目的 IC カード及び多目的 IC カード上にアプリケーションを運用する IC カードプラットフォームが大変注目されている。[1][2]

現在、提案または運用されている IC カードプラットフォームとして、NICE（Net-based IC Card Environment）[3]、MULTOS[4]、VOP / GP[5][6]がある。NICE は、現在我々が開発している IC カードプラットフォームであり、MULTOS は Mondex / MULTOS が、VOP/GP は VISA カード陣営が、それぞれ仕様の決定をしている。

各 IC カードプラットフォームは、IC カードを管理するサーバ群と専用 IC カードとの組み合わせにより実現されている。このため、IC カードプラットフォームと IC カードが 1 対 1 の関係になり、相互性がないため、IC カードプラットフォーム利用者に対して以下の問題が生じる。

- ■ IC カード利用者は、IC カードプラットフォーム上のサービスを利用したい場合、IC カードプラットフォーム専用の IC カードを所有しなければならない。
- ■ サービス提供者が、IC カードプラットフォーム上で IC カードサービスを提供する場合、
  - ① サービス提供者サーバ
  - ② 端末用 AP
  - ③ IC カードに搭載する AP

  を構築・運用しなければならない。
- ■カード発行者は、IC カードプラットフォームに応じたインタフェース・機能を持ったカードを発行しなければならない。

そこで、本研究では、我々が開発している NICE を対象としたマルチ IC カード制御の実現方式を検討する。

本研究により、従来は 1 対 1 だった IC カードプラットフォームと IC カードの関係を 1 対多にする新しいスキームを提案する。

2 NICE と IC カードの関係

2.1 NICE

NICE は、カード発行者（CI）、サービス提供者（SP）、AP ローダ（AL）、カード保有者（CH）、登録機関（RC）の役割分担に基づいたオペレーションモデルである。多様なビジネスモデルを成立させるために必要な共通的機能を具現化し、カードのハードや OS と独立なコンポーネントとして実装しているので、IC カードサービスの提供・運用者が容易にシステムを構築できる。また、IC カード利用者は、IC カード発行後のオンラインアプリケーション（AP）ダウンロード・AP 間ファイアウォール機能により、安全に複数のサービスを利用することができる。

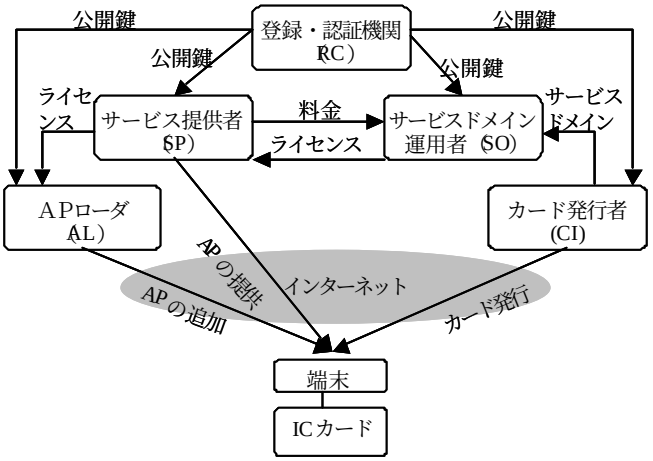

図１ NICE モデル

2.2 NICE の IC カード管理機能

NICE が IC カードに要求する機能である IC カード管理機能を表１に示す。

表１ NICE の IC カード管理機能表

IC カード管理機能	機能概要
AP 追加	IC カード発行後に NW を介して AP を追加する
AP 削除	IC カード発行後に NW を介して AP を削除する
SD 管理	AP の格納されるカード領域（メモリ）を管理する
ライフサイクル管理	カード及び AP の生成から廃棄までの状態を管理する（状態：Card Block, Card Unblock 等）
プロファイル管理	IC カード上のカードのメタ情報を管理する（メタ情報：カード識別情報、カード認証情報、カード資源情報等）
鍵・証明書管理	認証・暗号通信をするための鍵・証明書を管理する
認証・暗号通信	鍵・証明書を利用して、認証・暗号通信を行う

2.3 IC カード

表１の NICE の IC カード管理機能を全て満たす IC カードとして、ELWISE カード（with NICE-CM）がある。また、市場で普及している IC カードとして、MULTOS カード、VOP/GP カード、JICSAP カード[7]、FeliCa カード[8]、IC テレホンカード[9]等がある。これらの IC カードは、複数の AP を利用できるマルチ AP カードであるという共通点を持つ。しかし、各 IC カードによって特徴及び適用分野が異なる。表 2 に各 IC カードの概要と適用分野をまとめる。

2.4 NICE/IC カードの対応関係分析

NICE を対象としたマルチ IC カード制御を実現するために、

①**2.2 章で挙げた IC カード管理機能と、IC カード管理機能を IC カード内で処理する IC カード OS/CM（以降、CM）機能との対応関係**

②対象となる IC カードのカードアクセス方式

を分析し、**問題点を抽出する。**

2.4.1 分析結果①

①の分析結果を以下に示す。

1. NICE の IC カード管理機能を実現する CM コマンドがない。（表 3.A 参照）
2. AP 追加機能を実行する処理手順が、各 IC カードによって異なる。（表 3.B 参照）
3. 認証/暗号通信機能の実現可能レベルが、各 IC カードによって異なる。（表 3.C 参照）

さらに、各コマンドのパラメータを調査した結果、以下のことが分かった。

4. 同一機能を実現するコマンドはあるが、コマンド名及びコマンドのパラメータが異なる。（表 3.D 参照）
5. コマンドのパラメータの中に、NICE が管理していないデータがある。

表 2 IC カードの概要と適用分野

	仕様策定者	概要	適用分野
ELWISEカード（NICE専用カード）	NTT	1MBの大容量フラッシュメモリを持ち、高速入出力インタフェース＆複数暗号方式をサポートしたICカード	医療分野（電子カルテ） 公共分野（地方自治体発行カード、電子パスポート、免許証
MULTOSカード	MAOSCO	MasterCard等が推奨するEMV準拠のOSを搭載した高セキュリティICカード	金融分野（キャッシュカード、クレジットカード、電子マネー等）
VOP/GPカード	VISAカード陣営中心	VOP/GPプラットフォーム専用ICカード	金融分野（キャッシュカード、クレジットカード、電子マネー等）
JICSAPカード	ICカード利用促進協議会	ISO/IEC標準規格をベースにし、複数産業で利用可能な国内標準ICカード	公共分野（地方自治体発行カード等） ID分野（学生証、社員証等）
FeliCaカード	ソニー	業界最高速の処理スピードを持つ非接触ICカード	交通分野（鉄道・地下鉄・バスの乗車券等）
ICテレホンカード	NTT	公衆電話に必要な機能（認証・度数減算・番号記録）のみを持つ非接触ICカード	通信分野（テレホンカード）

表 3　IC カード管理機能 / IC カード対応分析表

NICEにおけるICカード管理機能			MULTOSカードコマンド分析	VOP/GPカードコマンド分析	JICSAPカードコマンド分析	FeliCaカードコマンド分析
AP追加			B	B	B	B
AP削除			D	D	D	D
AP選択			D	D	D	A
SD管理	SD生成		A	A	A,D	A,D
	SD削除					
	SD変更					
	配下ＳＤ取得					
ポリシ管理	ポリシ設定		A	A	A	A
	ポリシ削除					
	ポリシ取得					
ライフサイクル管理	参照	カード	A,D	A,D	A,D	A
		AP,SD				
	更新	カード				
		AP,SD				
プロファイル管理	取得	カード	A	A,D	A	A
		その他(ＳＤ，AP)				
	変更	カード				
		その他(ＳＤ,AP)				
鍵/証明書管理	更新		A	A	D	D
認証/暗号通信			A	C	C	C

2.4.2 分析結果②

②の分析結果を以下に示す。

1. 端末･IC カード間初期処理機能が異なる。
2. 端末･IC カード間の伝送プロトコル方式が異なる。

2.4.3 課題抽出

分析結果①、②から問題点をまとめ、課題を抽出する。

■IC カード機能の問題点

レベル１:IC カードが機能を持っていない。

レベル２:IC カードが機能を持っているが、コマンド名及び処理手順が異なる。

レベル３:IC カードが機能を持っていて、コマンド名及び処理手順も同じであるが、コマンドに含まれるパラメータが異なる。

■ IC カードハードウエアの問題点

IC カードアクセス方式が異なる

これらの問題点は、IC カードごとに異なる。よって、本研究の課題は、IC カードの機能毎に異なる問題レベルを統一的に解決する方式を実現することである。

3 提案

NICE の構成要素より、マルチ IC カード制御の実現方式として、以下の２方式が考えられる。

① IC カード側で解決する方式

② サーバ側で解決する方式

以降では、この2方式の考察、比較結果を述べる。

3.1 CM エミュレータ方式

IC カード側で解決する方式として、CM エミュレータ方式を提案する。CM とは、IC カードとサーバが協調したオペレーションを行うための IC カード上のミドルウエアであり、NICE-CM は NICE の要求機能を IC カード上で実現している。この NICE-CM のエミュレータを他の IC カードに AP として搭載する。

CM エミュレータの機能を、以下に２つ挙げる。

- NICE サーバから送られてくるコマンドの既存カードOS/他 PF-CM 用コマンドへの変換
- 既存カードOS/他 PF-CM が持っていない機能の補充

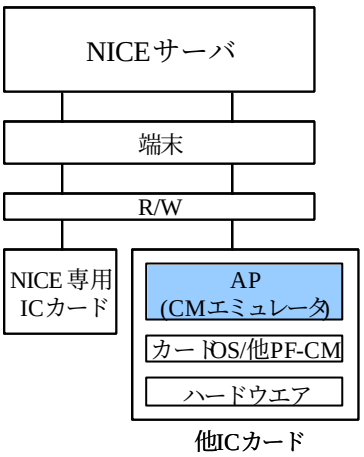

図 2　CM エミュレータ方式

3.2　アダプタ方式

サーバ側で解決する方式として、アダプタ方式を提案する。アダプタは、サーバ側に構築され、各 IC カードの機能及びコマンド差を吸収し、NICE カード以外の IC カードから NICE を利用可能にする。

アダプタの機能を、以下に挙げる。

- IC カードが持っていない機能の代行
- 各 IC カードに対応するカードコマンドの生成
- カードコマンドの順序管理

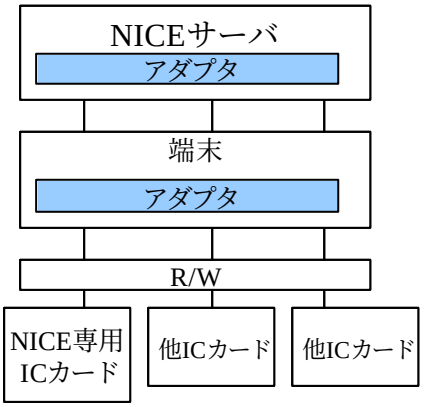

図 3　アダプタ方式

3.3　方式案の評価

＜3.1　CM エミュレータ方式＞＜3.2　アダプタ方式＞を適用性、セキュリティ、保守性に関して評価する。

(1)適用性

両方式の NICE への適用性を評価する。

■　CM エミュレータ方式

AP を搭載することが可能な IC カードへの適用を考えた場合、搭載する CM エミュレータは AP として制御可能な機能（PIN 認証等）しか持つことができない。このため、AP として制御不可能な AP 追加等の機能は、既存の CM 及びカードOS の方式を利用する必要があり、AP として搭載できる機能が限定される。また、データしか格納できない IC カードは、プログラムを追加することができないので、この方式を適用することができない。よって、2.4.3 章で抽出した問題に関して、IC カード機能の問題点は AP 搭載可能な IC カードでは解決することができるが、AP を搭載不可能な IC カードで解決することができない。また、IC カードハードウエアの問題点は、AP として搭載する本方式では解決できないと考えられる。

■　アダプタ方式

アダプタ方式は、IC カード側の機能を変更することなく、サーバ側の機能を拡充するだけなので、IC カードの性能や機能に影響されることなく適用できる。よって、2.4.3 章で抽出した問題は全て解決できると考えられる。

(2)セキュリティ

NICE に両方式を適用した場合の NICE 全体のセキュリティを評価する。

■CM エミュレータ方式

耐タンパである IC カード内で処理することができるため、非常に安全に処理をすることができる。

■　アダプタ方式

これまで IC カード内で閉じていた処理を、サーバ側で行う。サーバはハード的な耐タンパではないため、システム全体のセキュリティは低くなる。

(3)　保守性

NICE 要求機能の追加・変更に伴うシステム更新の容易性を評価する。

表 4 方式案の評価

	アダプタ方式	CMエミュレータ方式
適用性	○ サーバの機能拡充のみで、ICカードの性能や機能に影響されないため	△ ・APとして搭載できる機能しか持つことができないため ・データしか処理できないカードでは、プログラムであるAPを追加することもできないため
セキュリティ	△ サーバはハード的な耐タンパではなく、システム全体のセキュリティが低くなるため	○ 耐タンパであるICカード内で処理ができるため
保守性	○ アダプタの管理のみ	× 各ICカードの管理

■CM エミュレータ方式

システム更新方法は2通りある。1つは、IC カードに格納していた既存 CM エミュレータを NICE の AP 追加機能を用いて更新する方法である。もう1つは、既存 CM エミュレータを削除し、新 CM エミュレータを追加する方法である。どちらにしても、CM エミュレータの更新・削除・追加処理は各 IC カードに対して行わなければならないので、保守管理領域が広くなり、保守性は低い。

■アダプタ方式

NICE 要求機能の追加・変更に伴うIC カード機能の追加・変更は、IC カード機能を代行するアダプタを更新すればよいので、保守性に優れている。

CM エミュレータ方式とアダプタ方式を比較評価した結果、アダプタ方式が 2.4.3 章で挙げた問題点を全て解決し、**適用性の点で優れていることが分かった。**

4.おわりに

本稿では、VOP/GP **カード、**MULTOS **カード、**JICSAP **カード、**FeliCa **カードを対象とし、マルチ** IC **カードを制御するための問題点を抽出した。また、**IC **カードプラットフォームにおけるマルチ** IC **カード制御方式として、**CM **エミュレータ方式とアダプタ方式を提案した。さらに、**CM **エミュレータ方式とアダプタ方式を比較評価することにより、アダプタ方式が適用性の点で優れていることを明らかにした。**

今後は、アダプタ方式を具体化していく予定である。

5 参考文献

[1] “IC カード総覧”,株式会社シーメディア 2000

[2] 山本,竹内,細田, “ネットワーク指向 IC カードプラットフォーム”,NTT R&D Vol.49,No.12,2000

[3]竹内,平田,霍,”情報流通サービスをさまざまなシーンに広げる IC カードプラットフォーム”,NTT 技術ジャーナル,Vol12,No.10,2000

[4] MULTOS, http://www.multos.com/

[5] VISA Open Platform http://www-s2.visa.com/

[6]GlobalPlatform,http://www.globalplatform.org/

[7] IC カード利用促進協議会（ICSAP）http://www.jicsap.com/

[8]FeliCa,http://www.world.sony.com/JP/Electronics/felica/

[9] IC テレホンカード http://www.ntt-east.co.jp/ptd/icpublic