ICカード・多目的利用の実現のための JICSAP仕様とは？ 発行ライブラリ仕様

1．カード発行への提言

現在、ICカードの運用方法として、広域多目的に利用することが急速に展開しつつある。文字通り広域的な環境で、複数のアプリケーションにICカードを利用しようとする構想である。ICカードシステム利用促進協議会（JICSAP）では、このような利用場面を想定したファイル管理方式およびセキュリティ機構を実現できるようなICカード仕様を平成9年に規定した。これがJICSAPのICカード仕様である。

さてICカードは、カード製造から破棄に至る過程において、その時点での特有な機能が要求される。このICカードの一生を、カードライフサイクルと呼ぶ。

一般的に、ICカードのライフサイクルは、主に以下のようなステージで構成される。

(1)カード製造ステージ

ICカードを製造するステージであり、製造者に関連する情報を格納する。この時、「カード識別子」と呼ばれるカード製造者に割り当てられた情報も格納される（この情報が、今回の発行システムを実現するキーアイテムとなる）。

(2)カード一次発行ステージ

カード製造ステージから渡されたICカード内のメモリに対し、ファイルを割り当て、かつ運用時に必要なキーデータを登録する。また必要に応じて、運用に必要となる運用基本情報等を格納する。これにより、要求するアプリケーションレベルのカスタマイズを行う。

(3)カード二次発行ステージ

カード一次発行ステージにより構築された、メモリ内のファイルに対し、カード所持者の個人情報等を格納することにより、所持者レベルのカスタマイズを行う。また、必要に応じて、カード所持者に与える暗証番号等を書き換える。

(4)カード運用ステージ

カード所持者が、システムでカードを運用する。

(5)カード終結ステージ

カードを、アプリケーションで利用不可能な状態に遷移させる。

JICSAPのICカード仕様は、このうち「カード二次発行ステージ」「カード運用ステージ」および「カード終結ステージ」の各場面を想定し、以下の二種類のコマンド群を規定したものである。

(1)ユーザコマンドおよび関連機能

(2)準システムコマンドおよび関連機能

上記コマンドのうち“ユーザコマンド”は、ISO/IEC 7816-4にて規定されているコマンドの中から、想定されるシステムの中で利用される頻度が高いものを検討し、選択されたものである。なおこれらのコマンドセットは、JIS X6306で規定するコマンドおよび諸機能を包含している。

また“準システムコマンド”は、ISO/IEC 7816-4には規定されていない。しかし、想定されるシステムを運用する上で、さらに必要であり、かつ標準化の際にカードの実現方法上の違いによる諸問題を伴わないものを抽出し、仕様化したものである。

さて一次発行処理は、通常、ICカードが実装する「一次発行処理用コマンド（以下、発行コマンドと呼ぶ）」を利用してファイルの創成が行われる。このコマンドの仕様（コマンドによってカードに伝達しなければならないパラメタ、フォーマット等の規定）は、ICカード内において実際にどのようにファイルを管理しているかという「ファイル管理の実現方法」に依存する。この実現方法についてはICカードメーカーの裁量にゆだねられている。従ってメーカー間で異なる方法を採用している。このため、適用される発行コマンド仕様自身が、メーカ間で異なっているのが現状である。

従来、カードメーカーによるICカード供給は、主に以下の2つの方法によりなされている。

(1) あらかじめ運用が想定されているアプリケー

株式会社東芝
柳町工場
技術管理部
飯島康雄氏

ションの提供者から、これらの運用に必要なファイル（アプリケーションデータを、体系的に格納するためのメモリの区切り）情報を入手し、これによりカードメーカーが一次発行処理を行う。この後、アプリケーション提供者が二次発行処理を行う。

(2) カードメーカーが、専用の発行装置をアプリケーション提供者に提供し、アプリケーション提供者はこれを使用して一次発行および二次発行処理を行う。

前者の方法は、カードを一次発行する時点で、運用されるアプリケーションが想定できることを前提としており、また後者は、アプリケーション提供者に対し専用発行装置を提供することが前提となっている。

さらに前者の方法は、アプリケーション提供者の運用思想の下で作成されたファイルおよびセキュリティ情報を、カードメーカーが何らかの手段で入手し一次発行を行わなければならず、この点から言えば、セキュリティ面や、アプリケーション・プライバシー面での問題は残される。アプリケーション提供者は、カードメーカーといえども重要なデータを開示したがらない。また情報を公開されたカードメーカーにとっては、提供された情報に対する管理を慎重に行わなければならず、その負担も少なくない。お互いに、「手離れ」が良いカードを求めようとする。

さて同一のカードメーカーが、同一仕様のICカードをアプリケーション提供者に供給する場合、特に（2）の方法を採用すれば、アプリケーション提供者側で任意のファイル管理方法をカードに設定することが可能である。ただし近年では、公平性および透明性を重視した運用を目指すアプリケーションが検討されており、その背後にある、他社メーカーによるカード供給を視野に入れると、カードの発行場面で問題が生じてくる。

当然のことながら、複数種類のカードが供給される発行者側からは、「同一の装置を使用して、同一のオペレーションで、メーカーを意識することなく複数メーカのカードを発行したい」という要求がある。従来の方法だと、複数メーカーのカードを採用する場合、採用されるメーカーから、自社カード専用の発行装置を事前に供給してもらう。そして発行時に、混在する複数メーカーのカードの中から発行対象に選ばれたカードが、どのメーカーから供給されたカードかを判断し、さらに対応する発行機で発行するという作業を行うことや、発行現場では、物理的に複数の発行機を設置しなければならないといった必要が出てくる。このような煩わしさ、非効率さを回避したいという要求は、至極当然のことである。

特に広域・多目的運用の背景にある技術として、あらゆる発行環境（利用環境、設置環境等）を想定すると、同一のプラットフォームで、同一のマンマシン・インタフェースを介して、カードの仕様面での相違を意識せずに、共通の環境でICカードを使用することが望ましい。

JICSAPでは、このような諸問題を解決するために、ここに示す「発行ライブラリ仕様」をまとめ上げた。

2．発行ライブラリ仕様の概要

本仕様の技術的着眼点は、各カード仕様に対応する「カード発行用ドライバ」を用意し、これにより異なる発行仕様を伴うカードでも、同一の発行装置で発行できるようにすることである。例えば、パソコンのOS上にインストールされる、各プリンタ毎に存在するプリンタドライバの様なものである。ただ概念的に異なるのは、操作者が利用したいプリンタドライバを操作によって選択するのに対し、カード発行用ドライバは、現在発行装置にかかっているカードの種別を自動判別し、適合するカード発行用ドライバを選択してカード発行する点である。この概念が、先に紹介した「被発行カードの種別を意識することなく」発行処理が可能となる理由である。

この発行システムに実現される機能は、以下の通り。

・DFを生成する機能
　アプリケーションファイルを、発行情報に基づいてカード内に生成する機能。

・WEFを生成する機能
　運用のためのデータを格納するためのファイルを、発行情報に基づいてカード内に生成する機能。

・キーデータを登録する機能
　アプリケーションデータおよびシステムを保護するための認証用キーデータ（カード所持者の暗証番号等も含まれる）の設定、およびこれを格納するファイルの生成を、発行情報に基づいて行う機能。

３．発行システムの構成

図1に、発行システムの構成例を示す。

図中の発行アプリケーションプログラムとは、発行システム全体を管理するものであり、操作者の指示等に従って、主に以下の機能を果たす。

1）発行データの入力指示および発行データの格納
2）カードに対応する発行ライブラリを使用し、発行データからコマンド群データを作成
3）コマンド群データにより、カードを発行

ここにある発行データとは、ICカードを発行するために必要な、カード内に構築すべきファイルの構造情報である。アプリケーション提供者は、発行アプリケーションの指示に従って、自身のアプリケーション運用に必要なファイル構成およびセキュリティ要件等を入力し、発行データを作成する（図中（a)。発行データフォーマットについては後述)。

なおこの発行データは、発行ライブラリ仕様で規定される「発行データ共通フォーマット（発行コマンドとは別のフォーマットを有する)」に従って、例示するようにHD内に保存される。

また必要に応じて、発行ライブラリの機能であるサイズ精査機能で、この発行データにより入れ子関係になっているファイルのサイズ等を精査し、ファイル間でのサイズの不整合を実際のカード発行処理に先立って検査することもでき、発行処理の効率化向上を促している。

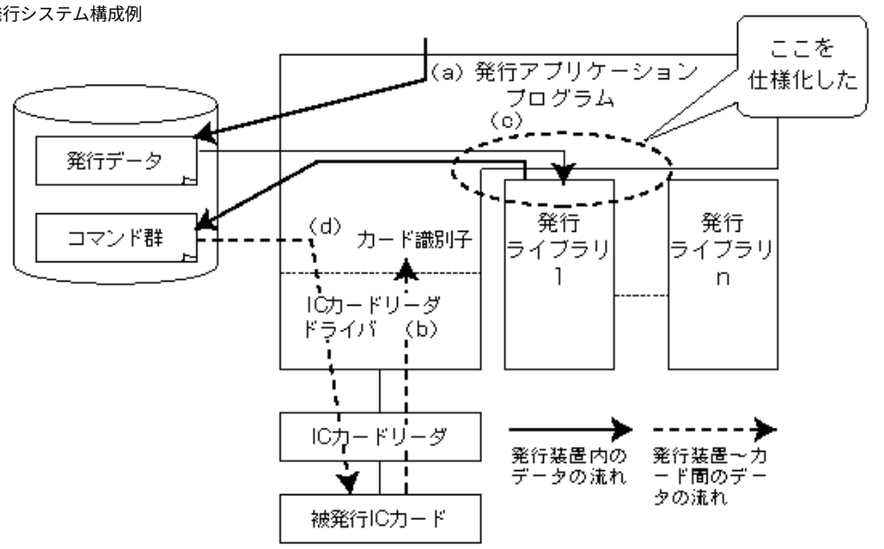
さてこの発行データを用いた、実際の発行動作を説明する。まず発行アプリケーションプログラムは、被発行カードがICカードリーダに挿入されたことを確認して、当該カードから「カード識別子」を読み出す（図中（b))。この情報は、1バイトのバイナリデータで構成されており、これにより、対応する発行ライブラリを検索する。なおこの情報の管理および登録は、JICSAP事務局が行っている。またこの情報は、発行ライブラリ機能関数名の一部（他の部分は共通）となっているため、今回使用する関数名は、当該カード識別情報から容易に生成する事ができる。

さて発行アプリケーションが、適合する発行ライブラリを見つけると、このライブラリにより、先に保持しておいた発行データを、ICカードが解読できるコマンドフォーマットに変換する（図中(c))。このようにして得られたコマンドデータ群を、ICカードリーダを介して順次、被発行カードに送信することにより（図中（d))、発行作業は完了する。

４．発行データのフォーマット概要

ここで発行データの概要を説明する。JICSAPのICカードが採用しているファイル構造は、MF（マスタファイル）を根幹としたツリー構造をなしており、利用目的に応じて枝葉（枝はファイル

図1　発行システム構成例



間の関連、葉は作業ファイル）を構成する。一次発行処理とは、いわばメーカーから提供された丸裸の木に対し、枝葉をつける作業に似ている。

図2は、あるICカードに構成されるべきファイル構造を示している。まずこのファイル構造のうち存在するDFに注目し、すべてのDFに対し、その上下に接触するファイル群を図3のように分離する。この図において波線の矩形で示されているDFは、そのファイルの実体はそれではなく（エイリアス）、矢印で関連づけられた太線の矩形で示された、同一DF番号を有するDFが実体であることを示す。

さてこれらの分離した各部分は、そのすべてが、実体のないDFを頂点に、その直下に位置するファイル（EFおよびDF）で構成されていることがわかる。これを便宜上、「ファイルの基礎パターン」と呼ぶことにする。逆に、このファイルの基本パターンの組み合わせで、あらゆるファイル構造が構成できることになる。

JICSAPではこの規則性に注目し、この特徴を発行データの基本構造として採用した。これは、図4に示される基本パターンをデータ列化し、このデータ列を「テンプレート」というデータの基本グループとして定義づけた。さらに図中の各ファイルに位置する部分に、対応するファイルを創成するために必要なパラメタを設定することとした。

このとき汎用性・柔軟性を考慮し、データ形式としてTLV構造を採用することとし、それぞれのデータ要素の意味づけの相違により、異なるタグの値を定義した。

図2　ファイル構成例

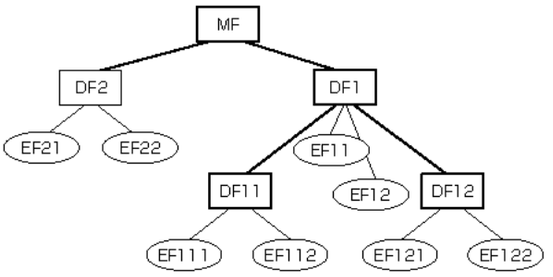


図3　基本パターンにより関連ファイルを分離

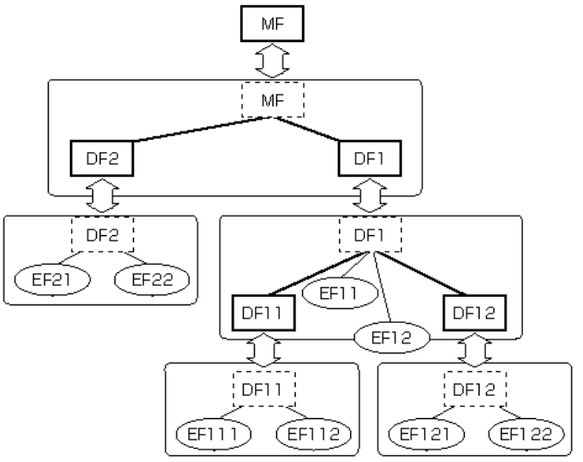


図4　基本パターンの一般形式

5．発行ライブラリ仕様の普遍性

ICカードの普及を活性化させる一つの要因として、利用ツールの普及・拡大があげられる。ここで紹介した発行システムも、その一因である。さてこれらの発行システムに利用される発行ライブラリは、ICカードメーカーが一次発行を行いたいアプリケーション提供者に配送される。考えられる配送形態は様々であるが、現在整備されているインターネット等を利用することにより、遠隔的にしかもスピーディに遂行することも可能である。

今回の仕様作成作業の合間に懸案となっていた発行コマンドの統一は、現状の技術動向等を鑑みるとカードメーカー間の調整等で困難な面があり、実施するに至らないでいる。しかし、将来的な展望を考えると可能なことかもしれない。その時点で、おそらく各メーカ独自の発行ライブラリと併用する形で、「共通に利用できる発行ライブラリ」が作成され、これに基づいたカード発行処理がなされるであろう。この発行ライブラリ仕様は、現状のメーカ間の発行機能仕様面での相違を吸収し、さらにこの共通発行ライブラリをも受け入れられる、柔軟性、普遍性のある仕様であると考えている。