

ICカード・多目的利用の実現のための JICSAP仕様とは？

1. 外部接点付きICカードの標準化動向

ICカードの普及には、“ICカード利用システムの目的、効果等について関係者間で共通の利益を得る”ための調整と“ICカードの物理的・機能的条件等について、基本部分での互換性を確保する”標準化の推進と仕様の決定が必要となっている。現在、前者についてはクレジットカード各社や銀行協会等で、後者は世界的には国際電気標準会議（IEC）国際標準化機構（ISO）、日本国内では日本工業標準調査会（事務局・通産産業省工業技術

院標準部）を窓口に、日本事務機械工業会や日本規格協会等複数の組織を通じて推進されている。

標準化に際しては、関係する組織の利害を取り払い、グローバルかつ総合的に推進することも重要だ。平成5年に発足したICカードシステム利用促進協議会（JICSAP）は、モノづくりの専門家とオペレーションの責任者が互いに情報交換を行い討議を重ねることを通じて、双方の都合だけで妥協しない、標準化について現実的な提案・開発活動を行っている。また、我が国では既に市民カードや住民健康カードのような行政カードや地域カードが実用化されている例もあり、今後はキャッシュカードのような金融機能や、公共交通機関や商店街での決済機能を持たせるなど、1枚のカードに複数の機能が折り込まれた「多目的利用」が確実にになっている。こうしたマーケットの変化を踏まえたコンセプト・メイクを具体化しなければICカードの普及はおぼつかない。ISO / 1EC7816の国際仕様のJIS化については、「x6306」として原案作成をJICSAPが担当し、多目的利用を前提とする提案を行った。

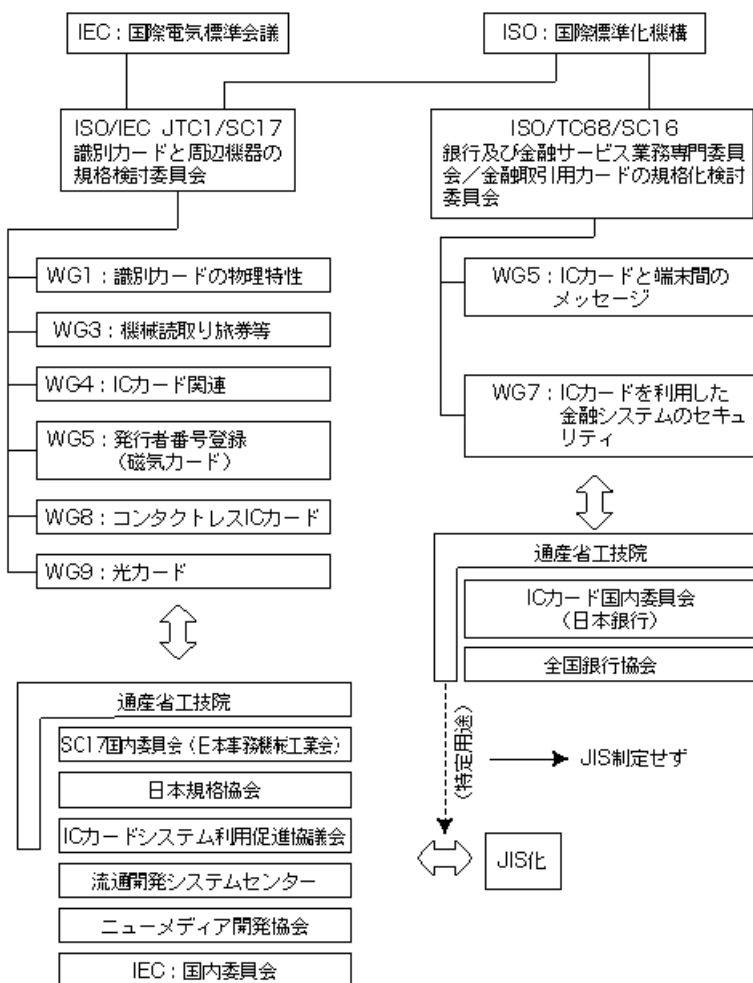
標準化の最重要テーマはセキュリティと、「コマンド」と呼ばれるプログラムの部分である。特にキャッシュカードを中心に金融分野での浸透が確実視される接触型（外部接点付き）ICカードの場合、多目的利用との兼ね合いから、ISO / 1EC7816では「オプション」として、カード発行者がその目的に応じてオリジナルに規定する形態、つまり“基本は共通するが付加機能については独自で決定する”内容となっている。

この、ISO / 1EC7816 - 4の国際仕様における「ICカードのファイル構造およびコマンドは全てオプションで、さらに個々のコマンドにおける様々な機能も全てオプションである」部分について、JICSAPの「x6306」では、最低必要なコマンドと機能を抽出し必須機能としての機能を制定。これによりJIS準拠ICカードの相互運用が可能な環境を確保され、多目的利用の道が開かれた。

さらに、通産省は、カード製造メーカー間の技

NTTデータ通信株式会社
技術開発本部
マルチメディア技術センタ
先端通信応用担当
岩瀬史幸氏

図 日本のICカード標準化組織とJICSAP



術の相互運用の可能性を実証する目的で、平成7年度に実証実験を(財)ニューメディア開発協会に委託し、北海道・滝川市で実施した。商店街カードシステムとしてのポイント機能、健康管理カードとして検診結果の記録管理を行うという、多目的利用をコンセプトとするICカードの仕様選ばれたのはJicsap仕様であった。

この“滝川市向け仕様”策定に当たっては、JICSAPが原案を作成したJIS準拠「x6306」を基本としながらも、そこで規定されていないISO/

IEC7816-4のコマンドや機能を必要に応じて組み込むとともに、国際標準化になっていないシステムの管理・運用コマンドを規定する方向で行われ、特にアクセス制御方法を明確化した。その結果、

ISO/JIS標準化を踏まえ、異なるユーザーでも共通した利用ができる。

公開性があり、長期にわたって陳腐化しない。誰でも使える容易性を持っていることを実現している。

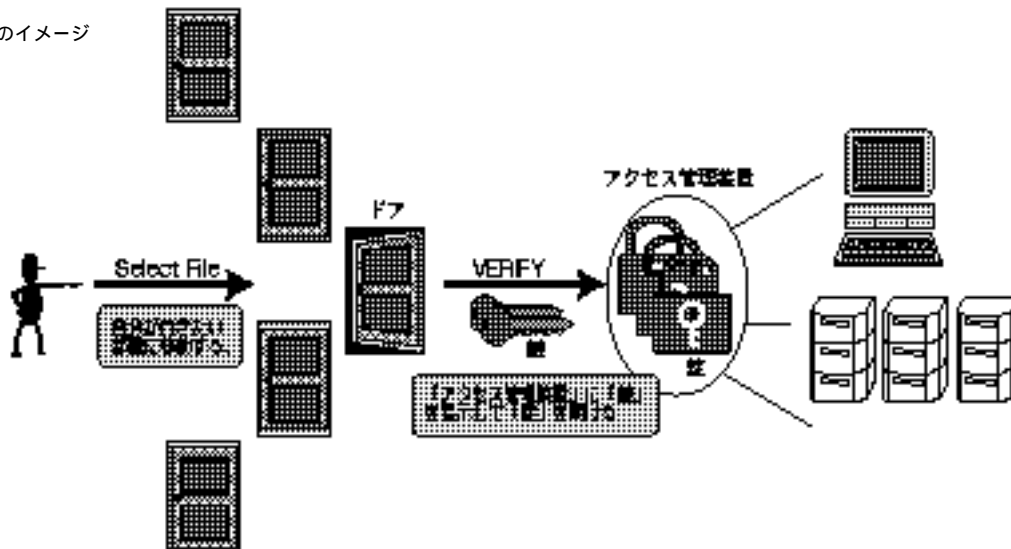
表 国際標準化の内容

国際標準規格シリーズ(ISO)などの名称 準拠項目	標準化項目(制定/改訂年)	JIS化項目
パート1	「カードの物理特性」 初版：1987年7月制定	JIS x 63 03 昭和63年7月制定
パート2	「端子の位置と寸法」 初版：1988年5月制定 現在定期見直しD16版審議中	JIS x 63 03 昭和63年7月制定
パート3	「電気特性及びプロトコル」 ・端子の電気特性 ・端子の活性化手順 ・アンサーリセット ・キャプタ伝送プロトコル (Y=0) ・ブロック伝送プロトコル (T=1) ・プロトコル選択手順 (PTS) 初版：1989年9月制定 PTSとT=1を除く全て AMD1：1992年12月制定 T=1部分のみ AMD2：1994年12月制定 PTS及びその他 修正案：3V電圧追加 IS発行準備中	JIS x 63 04 平成8年10月改訂 (AMD2まで部分)
パート4	「業界共通コマンド」 ・ファイル構造 ・セキュリティ基本構造 ・共通コマンド 初版：1995年9月制定	JIS x 63 06 平成7年10月制定
パート6	「アプリケーションID登録システム」 初版：1993年10月制定 AMD1：D16版審議中	JIS化なし
パート8	「業界共通データ要素」 初版：1996年4月制定	JIS原案作成済み(発行準備中)
パート7	「ISQGLデータベース関連コマンド」 D16版審議中	_____
パート8	「セキュリティ関連コマンド」 現在CD投票中	_____
パート9	「追加古機能コマンド」 現在WD作成中	_____
パート10	「同型式カード」 現在D16版審議中	_____
パート11	「セキュリティアークアクチャー」 現在WD作成中	_____

図a JICSAP仕様におけるコマンド一覧



図b アクセス管理方法のイメージ



2. 滝川市向け仕様の内容 ～ アクセス管理方法～

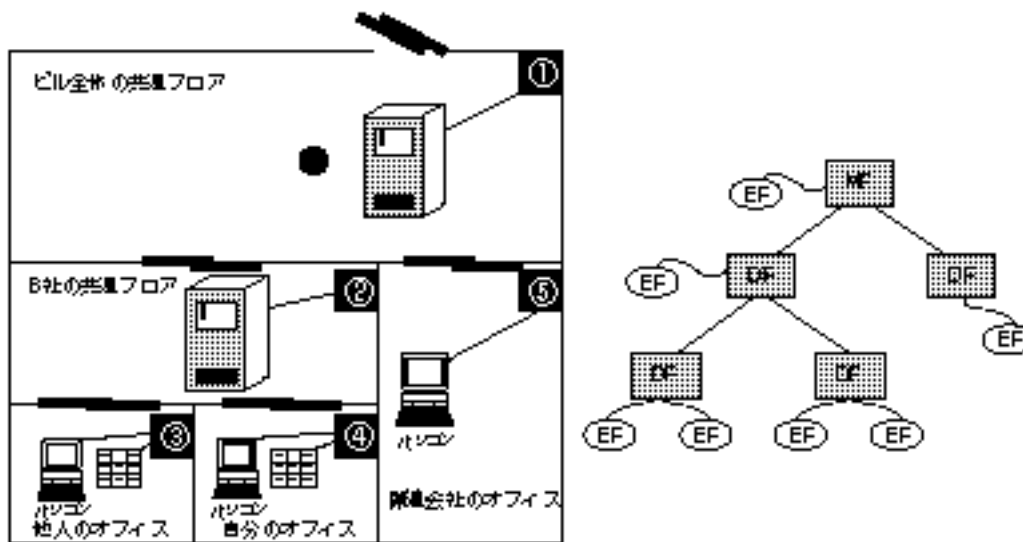
当該仕様のポテンシャルとして、カード内部へのアクセス制御を挙げることができる。セキュリティ上、ICカード内に設定されているデータは当然不当なアクセスを排除し、保護されなければならない。そのため、外部から命令（コマンド）があっても、それを実行しても構わないかを判断させ、不当なコマンドであれば排除する仕組みを盛り込んだ。これは、ICカードが実用される上で、基本的な仕様に位置づけられる内容といえよう。

部屋毎に「アクセス管理装置」が置かれ、そこに設置されている全ての端末機器類へのアクセスを管理しているオフィス为例とする。「アクセス

管理装置」は複数の錠の集まりで、これらの錠に合った鍵を使うことでアクセスが許可される構造である。従って、特定の端末にアクセスしたくても、アクセス管理装置に置かれた端末の「錠」に合う「鍵」がなければどうにもならない。

実際のICカードでは、自分の希望する部屋に行く = 「SELECT」、アクセス管理装置に鍵を入れて開錠する = 「VERIFY」のコマンドが使われている。なお、カード全体はMF (Master File = 主ファイル)、部屋のことは「DF」(Dedicated File = 専用ファイル) 部屋にある端末機器類のように実際にアクセスする対象を「EF (Elementary File : 基礎ファイル)」と呼んでいる。

図c カードの基本的な構造



カードの基本的な構造

さらにあるオフィスビルを例に、「部屋に行きアクセスする」シーンを当てはめながら、カードの基本的な構造を紹介する。

自分の部屋、同僚の部屋で構成された自社オフィスと 関連会社のオフィス、ビル共用フロアの合計4つの空間を持つビルを想定する。

この状況では、他社と共用空間を設ける必要はないが、自社の2部屋以外にコミュニケーションのために共用フロアを設けたい。もちろん、そのフロアは他社と共用せず、自社内部だけで設置した。その結果、ビルには5つの部屋ができる。ICカードでいえば部屋 = DF (Dedicated File = 専用ファイル) が2階層設定できるファイル構造となっている。

また、各部屋には、アクセスの対象となるパソコンや自動販売機つまりEF (アクセス対象の基礎ファイル) が設置され、これらは各部屋に設置された「アクセス管理装置」によって管理されている。

現在の施錠状態と自分がいる位置をICカードのファイル構造に示すと、図のようにアクセス管理装置と 自分の部屋 = DF + 2つのEF、 同僚の部屋 = DF + 2つのEF、 自社の共通フロア = DF + 1つのEF、 関連会社のオフィス = DF + 1つのEF、

ビルの共通フロア = MF (主ファイル) + 一つのEFで構成され、自分の現在位置であるビル共用部 = MFのみ開錠状況 “カードへのアクセス開始時には” ということになっている。

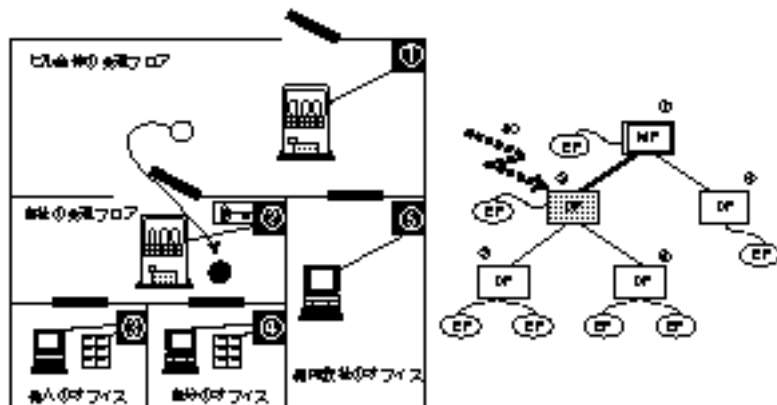
自動ロック機能

次に、このビルには利便性提供とセキュリティ確保のため、「ドアは人間が入ると施錠されず開いたままになる」「部屋からいったん出て他の部屋に移動した場合、元の部屋のドアは自動的に閉まり施錠される」機能があると想定する。

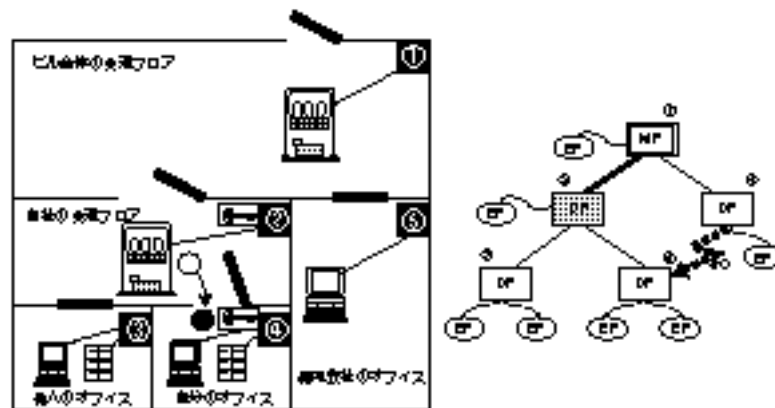
そうすると、現在位置のビル共用フロアから自社共通フロアに入り、その自動販売機を利用するには、アクセス管理装置を開錠しなければならない。さらに、自分の部屋に移動して、パソコンにアクセスするにも当然対応するアクセス管理装置の開錠が必要になる。

この状況では、「ドアは人間が入ると施錠されず開いたままになる」ために、自社の共用フロアの錠は閉められていない。つまり、現在自分がいる部屋の内部にある他の部屋に移動する場合には、現在の部屋のドアは閉められない。しかし、

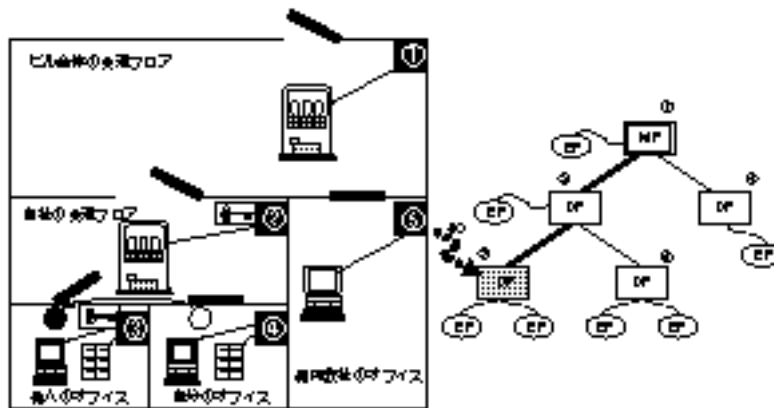
【図d：自動ロック機能 : 自社の共通フロアに移動した状況】



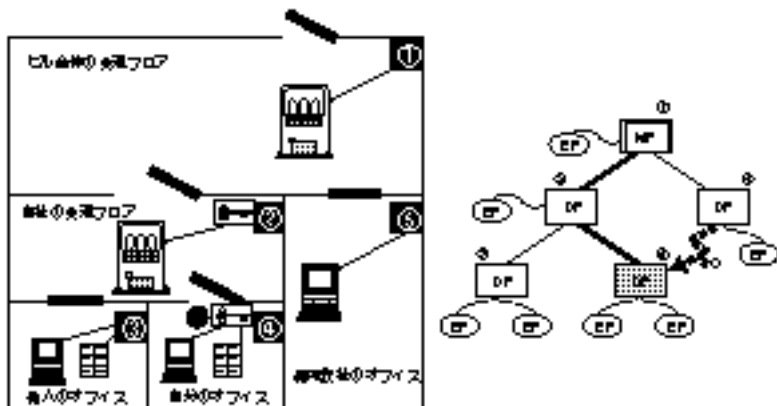
【図d 自動ロック機能 : 自分のオフィスに移動した状況】



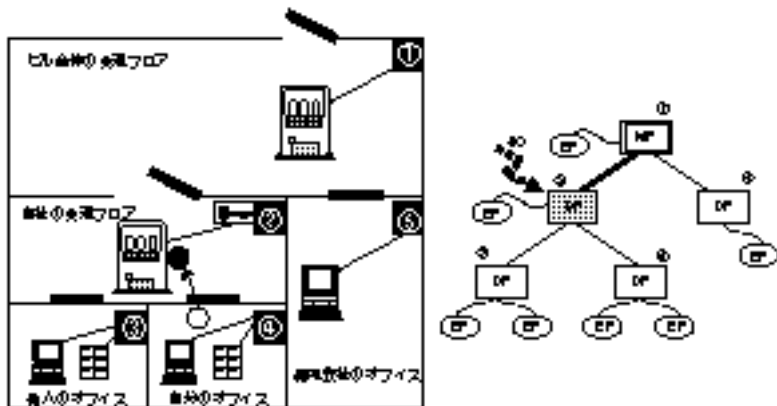
【図d 自動ロック機能 : 同僚の部屋に移動した状況】



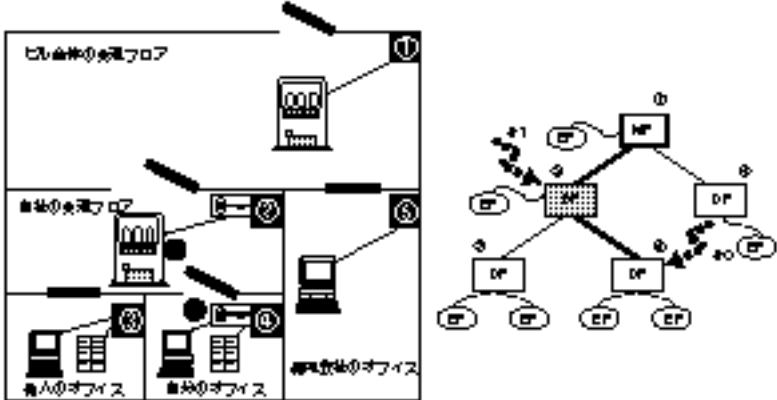
【図e：ダブルDFオープン：自社の部屋にいる状況】



【図e：ダブルDFオープン：自社共通フロアへ移動した状況】



【図e：ダブルDFオープン：自分の部屋と自社共通フロアとに同時アクセス】



自社であっても同僚の部屋に移動すると、「部屋からいったん出て他の部屋に移動した場合、元の部屋のドアは自動的に閉まり施錠される」機能が働き、自社の共通部分は開錠されたまま、自分の部屋の鍵は閉じられる。これを自動ロック機能という。

ICカードで実際のアクセスには、次のように構成される。

図dを参照

(ビルの共通フロア)
 SELECT [# 0](自社の共通フロア)
 VERIFY [# 0](の錠をあけるための鍵)
 自社の共通フロア内の自動販売機にアクセスする
 (自社の共通フロア)
 SELECT [# 0](自社の部屋)
 VERIFY [# 0](の錠をあけるための鍵)
 自分の部屋のパソコンにアクセスする
 (自分の部屋)
 SELECT [# 0](同僚の部屋)
 VERIFY [# 0](の錠をあけるための鍵)
 同僚の部屋で資料を探す

* 図中の矢印と [# 0] を「論理チャンネル」と呼び、カード内部へのアクセス手段を示す。

ダブルDFオープン

同僚の部屋で資料を発見し、自分の部屋に戻ってパソコンに向かって。コーヒープレイクに自社の共通フロアにある自動販売機を利用したい。しかし、自動ロック機能が作動し、自分の部屋に戻るためには再度開錠が必要となる。これでは二度手間が煩わしい。

そこで、現在自分がいる部屋の開閉状態を保持したまま、他の部屋の利用が可能になるよう、「ダブルDFオープン」を導入した。これによって、最低2つの部屋をそのままに他の部屋で用事を済ます環境が確保される。

具体的には、これまで使用していた [# 0] の論理チャンネルの他に、別の論理チャンネルをサポートすることで具体化している。

ICカードでの実際のアクセスには、次のとおり。

図eを参照

(自分の部屋)
 SELECT [# 0](自社の部屋)
 VERIFY [# 0](の錠をあけるための鍵)
 自社の共通フロア内の自動販売機にアクセスする
 (自社の共通フロア)
 SELECT [# 1](自社の共通フロア)
 * [# 0] を使用して自分の部屋での用事も継続できる。