

# JICSAPの国内ICカード 標準化への取り組み

## 目 次

はじめに	1
1 . JICSAPの誕生と背景	2
2 . JISX6306共通コマンドの規格化	3
(1) 標準化対応組織	3
(2) 接触型ICカードの国際標準化	3
(3) 原案作成の組織と留意点	3
(4) JISX6306の規格内容	4
3 . 北海道滝川市向け仕様の開発	5
(1) 開発の背景と目的	5
(2) 仕様化にあたっての 基本コンセプト	5
(3) 仕様の特徴	5
(4) 主な規定内容	6
(5) コマンド体系	6
(6) 実証実験結果	6
4 . JICSAP仕様V1.0の開示	8
5 . 広域・多目的利用ICカードに向けた バージョンアップ	8
(1) バージョンアップの背景と目的	8
(2) 広域利用とは	9
(3) 広域・多目的利用ICカードの ユーザ要求	9
(4) 検討体制	9
(5) V1.1の主たる規定内容	10
(6) 一般公開説明会の開催	11
(7) 岐阜県益田郡での実証実験の開始	11
6 . 英訳JICSAP仕様の刊行	11
7 . 今後の取り組み	12

## はじめに

日本国内だけでもすでに2000万枚弱が使われているICカードは、これを取り巻く技術と環境の変化とともに、ようやく本格的な利用がされようとしています。

しかし、これまでは各メーカーやユーザーが、それぞれの目的や用途に応じて個別に仕様を設定し、開発しており、ICカードシステム間の互換性はまったくといっていいほどないのが実情です。

ICカードは高度情報社会や電子商取引（EC：Electronic Commerce）社会のキーコンポーネントであり、ICカードシステムは新しい社会システムともなり得る可能性を持っています。

これからICカードシステムがさらに発展し、社会的なシステムとして普及、定着していくためには、仕様の互換性や共通プラットフォームの技術環境の整備等、国際標準化動向と国際市場戦略をも視野に入れた標準化への取り組みの重要性が、一段と重みを増してきます。

99年はわが国のICカード市場の創造において、エポックメイキング的な年でした。3月にはNTTの公衆電話にICカードテレホンカード（スマートテレホンカード）が商用サービスとして登場し、高速道路にはETC（ノンストップ自動料金収受システム）が本格導入される初年度となりました。

いずれも全国規模のICカードシステムですが、さらに市民レベルで新しいICカード社会の到来を告げる、住民基本台帳法改正案の第145回通常国会での法案成立がありました。

法律が施行されると、希望する国民には市町村からICカードの「住民基本台帳カード」が交付されることとなりますが、交付を希望する国民を1人でもふやすためには、利便性が高く、プライバシーの保護を含め安心して使える、セキュリティ機能が十分な魅力あるICカードシステムを実現することが求められます。

そのためのICカードの技術環境としては、1枚の住基カードが全国津々浦々で使えること、サービス機能としては利便性と魅力を高めるキラー・アプリケーションの開発が決め手となります。現在、通産省が県の協力を得て岐阜県益田郡の五町村で行っている、広域・多目的ICカード実証実験の目的は、まさにここにあります。

JICSAP（Japan Ic Card System Application council：ICカードシステム利用促進協議会）は、かかる広域・多目的利用ICカードの仕様化にニューメディア開発協会との連携により取り組んできましたが、ここではJICSAP自体とその活動経緯を、標準化への取り組みを中心に述べます。

# 1. JICSAPの誕生と背景

カード社会のインフラストラクチャーとして期待されるICカードシステムにおいて、そのキーコンポーネントとしてのICカードの標準化が非常に重要であるとの認識は言を待たないでしょう。しかし、すでに動いているICカードシステムでは、互換性はほとんど考慮されていません。

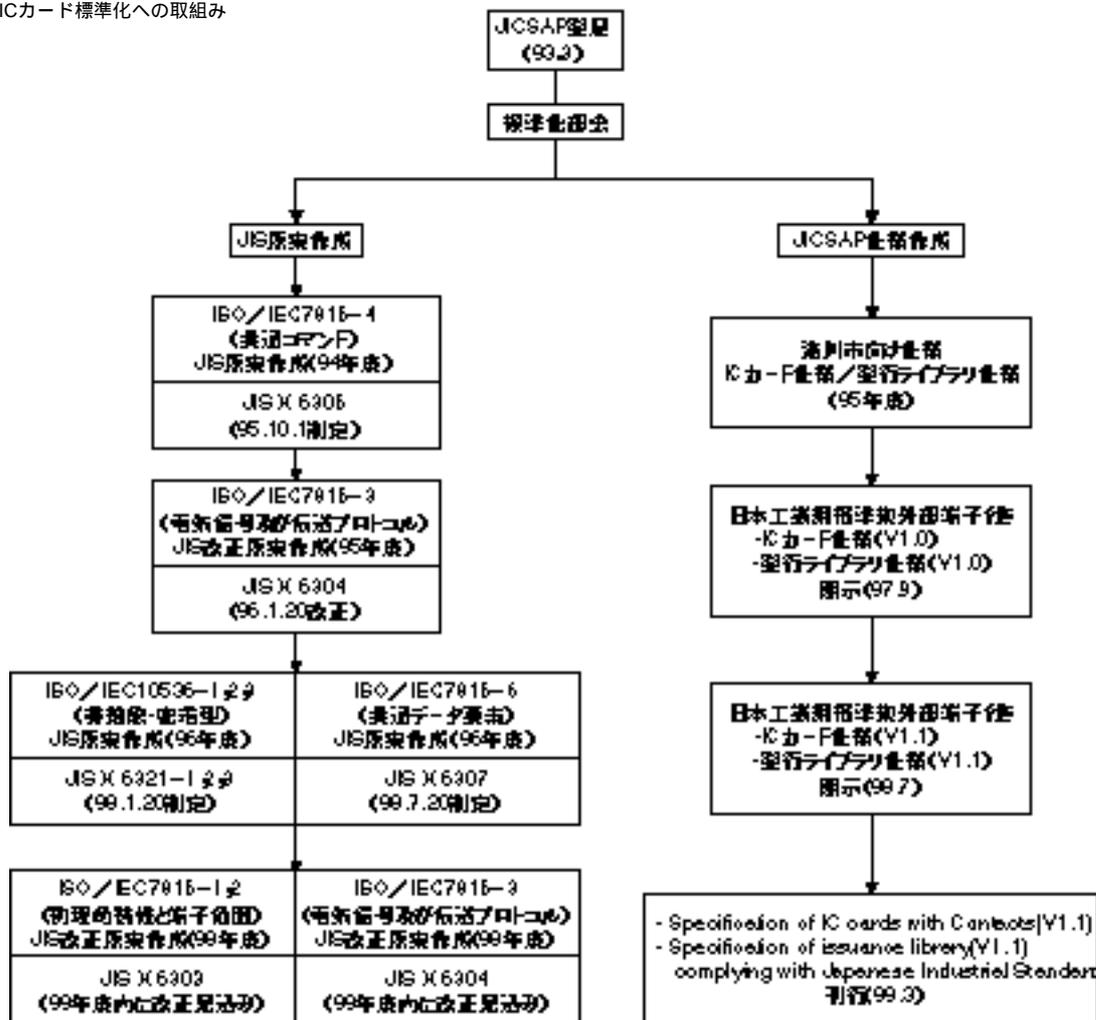
ICカードの標準化は、関係する組織の利害を調整し、透明性、公平性を確保しながら、グローバルかつ総合的に推進しなければなりません。ここから、メーカ、システムインテグレーター、利用者がバラバラに動くのではなく、互いに連携しあい、将来に向けてベクトル合わせができるような組織の必要性が浮上しました。

このような考え方で、93年3月にJICSAPが設立されました。JICSAPの一つの特徴は、メーカやシステムインテグレータのような、ICカードシステムを開発・販売する側の組織だけではなく、シ

ステムを導入し、実際に活用して行く側の企業や団体も数多く参加しているところにあります。つくる側の論理では、どんなに参加者が多くても、技術からの発想という限界を脱しきれません。これに対して使う側は、ユーザオリエンテッドな発想ができます。また、ICカード社会の創造には、中央省庁との横断的な関係の確保、これに基づく政策プランナーとしてのアドバイス、支援・協力が重要となります。このため、通産省、郵政省をはじめ関係各省庁がオブザーバとなり、各省庁の外郭団体が会員として参加しています。こうした点で、運営面ではいわゆる工業会と性格を大きく異にしています。

JICSAPには現在、国内外75の企業・団体が参加し標準化に取り組んできていますが、これからも、モノづくりの専門家とオペレーションの責任者が一つのテーブルを囲み、互いに情報交換を行い討議を重ねることを通じ、ICカード社会に向けより現実的な提案をしていきたいと考えています。

ICカード標準化への取組み



## 2. JIS X 6306共通コマンドの規格化

通産省は大きく分けて三つの観点から、ICカードに対する取組みを進めています。一つは、工業技術院で取組んでいるJISなど標準化を行なう作業です。二つ目は、JICSAPなどが中心となって取組んでいる業界標準の策定作業やニューメディア開発協会による各種アプリケーションの開発と普及です。三つ目は、ICカードを実際にどのように活用して行くのか、アプリケーションレベルでの標準化です。

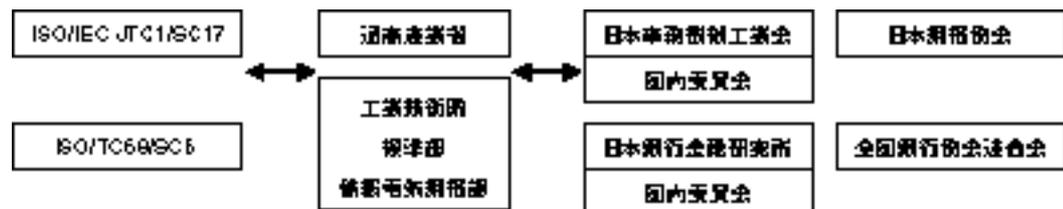
### (1) 標準化対応組織

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・機能的な条件等について、基本的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ります。

前者についてはクレジット各社や銀行協会等で、後者は世界的には国際標準化機構（ISO）、国際電気標準会議（IEC）、日本国内では日本工業標準調査会情報部会（事務局・通産省工業技術院標準部）で進められ、国内の関係する機関及びISO/IECの標準化組織はそれぞれ次のとおりとなっています。

一方、幅広い様々な分野でICカードが利用される動きが顕在化しており、わが国で動き出したITS（高度道路交通システム）の国際標準化では、92年ISOに専門委員会のTC/204が、保健医療情報分野でも98年にTC/215が設置されています。TC/215に対応する国内委員会は、98年6月に医療情報システム開発センター（MEDIS）に設けられ、TC/215にはJICSAPも委員として参加しています。

国内標準機関



### (2) 接触型ICカードの国際標準化

ICカードは1970年代にロラン・モレノ氏（フランス）並びに有村国孝氏（日本）によりほぼ同時期に発明されましたが、日本は製造面では最先端の位置にいると自負しているものの、利用面ではヨーロッパに大きく遅れをとっています。

遅れをとった理由は幾つかありますが、その一つに1枚のICカードの利便性、効率性を重視した、多目的利用に重点を置きすぎたのではないかという指摘があります。

通産省ではこうしたわが国のICカード市場の閉塞感を打開し、市場を立ち上げるため、接触型ICカードの国際標準化の中で、長年の懸案であった基本コマンド部分（ISO/IEC7816-4）の国際標準化策定によりやく見通しがついたことから、JICSAPにJIS原案作成作業を委託し、JIS X6306（外部端子付きICカード - 共通コマンド）が95年10月1日に制定されました。

### (3) 原案作成の組織と留意点

JICSAPでは原案作成組織として、東京工業大学 大山永昭教授を部会長とする標準化部会と多目的利用部会を設置し、標準化部会にはワーキンググループとしてシステム、カード、リーダ/ライタの三つの分科会を設け、標準化部会の調整は主査連絡会、全体の調整は合同部会で行う体制としました。

JIS原案作成に当たって特に配慮されたことは、建設、クレジット業界で使用されているICカードおよびIDカード等一般企業で使用されているS型ICカード（ICカード関連16社が決めた国内暫定標準）との、相互運用性と国際標準との整合性でした。

このため、検討組織には関連団体にも委員として参加してもらうことで透明性、公平性の確保に配慮しました。

(4) JIS X 6306の規格内容

国際標準で定めたコマンドの規格の範囲は、各国の要求を広く取り入れたオプション形式であるが故に、その規格数は膨大となっています。このため、現在のICカードメモリ容量では、すべてをカードにインプリメントできないため、ISO準拠であってもメーカー間で異なるコマンドをインプリメントする可能性があり、各社のICカードの互換性が必ずしも確保できないことが大きな問題となりました。

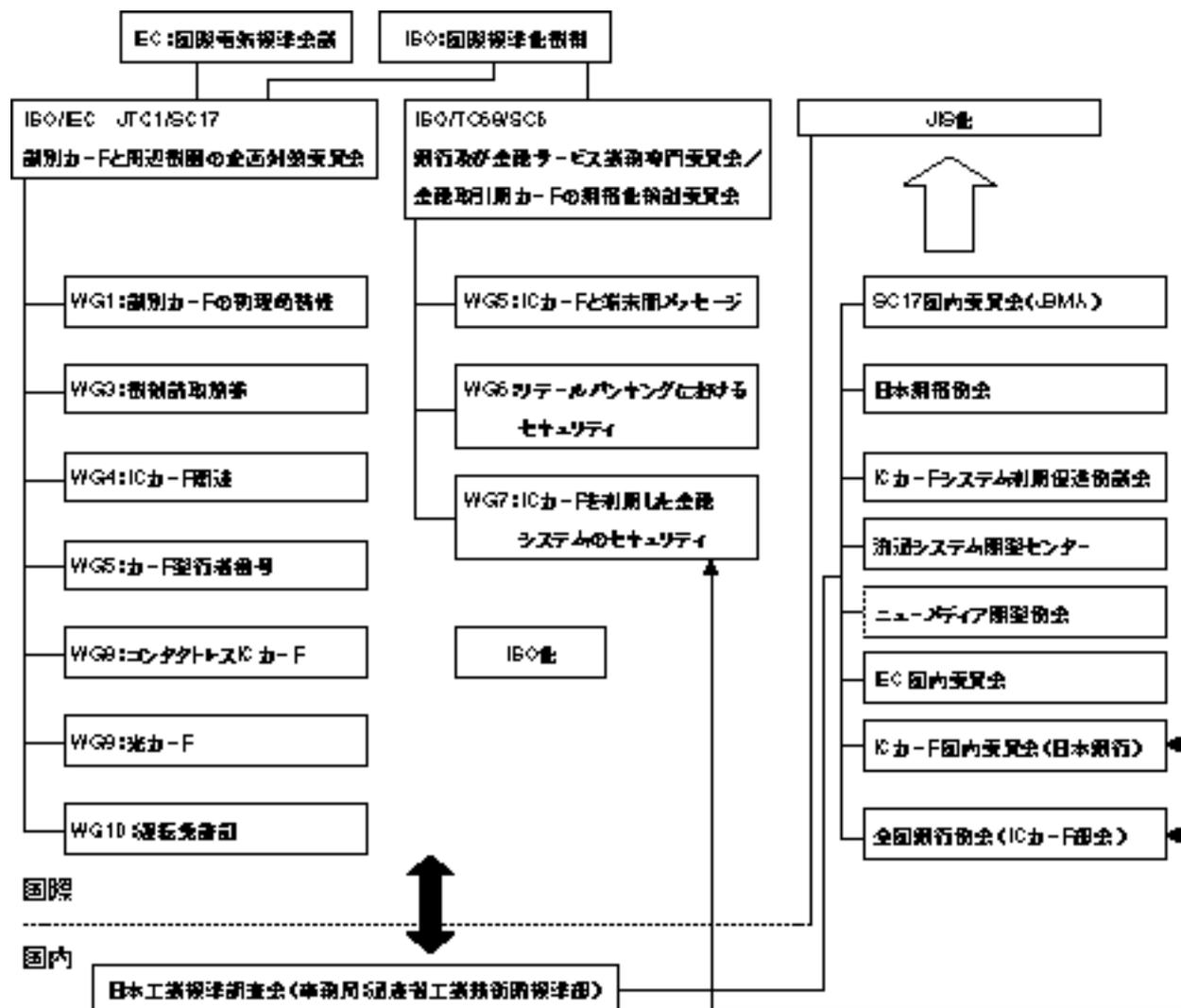
しかし、JICSAPでは、JIS原案を制定するに当たって、  
**JIS準拠カード間での最低限の互換性を確保すること。**

**各業界が国際標準案に基づいて、これまで検討してきた規格案は可能な限り尊重すること。**

の2点に特に留意することとし、カードの相互運用性を確保するための方策を検討しました。

その結果、これまで各業界ですでに検討されてきた規格を最大限活用し、かつそれらの間の相互運用性を確保するため、JISカードとして最低限の機能を持たせる基本コマンドを規定し、それ以外のISO / IEC 7816 - 4で規定されるコマンドについては、各メーカ、ユーザが自由に選択できるオプション機能ととして扱うこととしました。これにより、JIS準拠カード間であれば、必須コマンドで必要最低限の相互運用性を確保することを可能としました。

ICカードの国際標準化組織



基本コマンドの比較

基本コマンド		ISO / IEC 7816 - 4	JIS X 6306
1	READ BINARY		-
2	WRITE BINARY		-
3	UPDATE BINARY		-
4	ERASE BINARY		-
5	READ RECORD(S)		
6	WRITE RECORD		-
7	APPEND RECORD		
8	UPDATE RECORD		
9	GET DATA		-
10	PUT DATA		-
11	SELECT FILE		
12	VERIFY		
13	INTERNAL AUTHENTICATE		
14	EXTERNL AUTHENTICATE		
15	GET CHALLENGE		
16	MANAGE CHANNEL		-

...規定 - ...留保

### 3. 北海道滝川市向け仕様の開発

JIS X 6306の制定により、JIS準拠ICカードの相互運用性が可能な環境が確保され、国内市場拡大の道が開かれました。

#### (1) 開発の背景と目的

通産省はニューメディア・コミュニティ構想に基づく地域情報化施策の一つとして、商店街カードシステムの導入調査を行い、ICカードを用いた情報システムの検討を行っていました。その調査結果を踏まえ、ニューメディア・コミュニティ構想応用発展地域に指定され、商店街の活性化に積極的な検討、取組みを行っていた北海道滝川市に白羽の矢をたて、ICカードシステムモデル事業を、95年に滝川市で行うことを決定しました。

このモデル事業は、次の三つのテーマを主眼にしていました。

#### ISO / IEC国際標準準拠ICカードの導入

#### メーカ各社製造ICカード関連機器の相互運用性の検証

#### 多目的利用ICカードシステムの実現

とくに、はこれまで技術的に実現できなかった複数のアプリケーションサービスを、JIS X 6306の制定を受け、公共・民間分野において一枚

のカードで提供することを可能にする多目的利用をめざしたもので、国内初のシステムとして注目すべきものでした。JIS X 6306の共通コマンドは前述したように、メーカ間の最低限の互換性を確保するために規格化したものですが、滝川市向け仕様では、多目的利用という、さらに高度なICカードの機能、仕様化が要求されました。

通産省はJIS X 6306の原案を作成したJICSAPに協力を要請し、ニューメディア開発協会が実証実験を担うことになりました。

#### (2) 仕様化にあたっての基本コンセプト

JICSAPが原案を作成したJIS X 6306を基本としながらも、そこでは規定されていないISO / IEC7816 - 4のコマンドや機能のうちから、多目的利用実現の基本要件となるセキュリティに関するコマンドを必要に応じて組み込むとともに、国際標準化と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い、とくにアクセス制御方法を明確化し、次の点を実現しました。

**ISO / JIS標準化を踏まえ、異なるユーザ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がある。**

上記に加え、国内各地で稼働、実運用に供されているICカードシステムの運用に支障が発生しないよう考慮することとしました。

#### (3) 仕様の特徴

本仕様はカード製造者、リーダー/ライター製造者、システムインテグレータ等のICカードシステム関係ベンダー間の、アプリケーションレイヤでの相互の互換性を、多目的利用の場面で取ることを目的に制定され、多目的利用に供せられるよう、運用業務面（発行処理、キーのアンロック業務等）では、運用者が同一のユーザ・インターフェースで操作できるよう配慮されています。

多目的利用ICカードは複数のファイルを格納するため、ファイル間の不当なアクセスを防止するためのファイルの独立性の確保が必要となります。このため、滝川市向け仕様では、JIS X 6306にファイルの管理・運用セキュリティ対策のコマンドを追加していますが、JIS規格（X 6303 / 6304 / 6305 / 6306）を遵守しています。

また、ICカード発行システムを共通化するための「発行ライブラリ仕様」も決めています。

#### (4) 主な規定内容

##### ・伝送仕様について

ISO規格では、ATRの伝送仕様およびPTSの伝送仕様が、3.5712MHzの9600bpsで固定化されており、以降のサブシーケント伝送に関しては、ATR中のパラメータおよびPTSにより伝送条件を変更可能としています。本仕様では、リーダー/ライター側の処理を容易にするために、ATRおよびサブシーケントの伝送仕様を同一(3.5712MHzの9600bps固定)としています。

##### ・ファイル構造について

###### a. ファイル構造

DF間共通の情報を格納する「共通ファイル」を実現するために、最低2レベルのDFをサポートしています。

###### b. 基礎ファイル(EF)構造

「レコード構造」だけでなく、大量のデータを効率的に格納できる「透過構造」も採用しています。

レコードの形式は、メモリの有効活用を考慮し、他業界においても使用されている簡易符号化TLVフォーマットを採用しています。このレコード形式を採用するに当たり、レコード番号指定に加え、レコードIDによる指定方法を採用しています。

##### ・セキュリティ構造について

a. セキュリティ属性については、各アクセス種別ごとに、4つのアクセス当事者のキー、及び4つのアクセスノードキーの組み合わせを設定できる範囲で十分ではないかとの意見もありました。しかし、様々な設定条件があることを考慮し、より多くのキーの組み合わせを設定できるようにしています。その結果、ICカードのリソースを考慮し、上記の各々7つのキーの組み合わせを設定できます。

b. 暗号方式については、1つの方式を規定することも考えられましたが、現時点では暗号方式を1つに限定できないため、搭載される暗号方式を規定するのではなく、単一の暗号方式を搭載することとし、カード内に記録された「カード識別子」により、搭載された暗号方式を識別する方法を採っています。

##### ・コマンドについて

a. ISO規格にて規定されているコマンド以外にも、カードの運用形態を考えた場合に必

要であると想定されるコマンドを、「準システムコマンド」として規定しています。

b. 上記以外のファイル生成系コマンドについては、どのベンダーカードかを意識することなく、ファイルを生成することができるように、規定すべきではないかとの意見もありました。しかし、これらコマンドは、カード内のOSにて制御されるファイル管理方法に大きく影響し、これを規定することは各ベンダーの独自性を否定する恐れがあります。

そのため、これら発行機に適応したプログラムを、発行機にインストールすることにより対処することとしています。また、該当カードが、どの発行プログラムに対応するかは、カード内に記録された「カード識別子」情報を読み出すことにより、判別する方法を採っています。

#### (5) コマンド体系

コマンド一覧表

順番	コマンド名
ユーザーコマンド	1 READ BINARY
	2 WRITE BINARY
	3 UPDATE BINARY
	4 READ RECORD (S)
	5 WRITE RECORD
	6 APPEND RECORD
	7 UPDATE RECORD
	8 SELECT FILE
	9 VERIFY
	10 INTERNAL AUTHENTICATE
	11 EXTERNL AUTHENTICATE
	12 GET CHALLENGE
準システムコマンド	1 LOCK DF
	2 UNLOCK DF
	3 UNLOCK KEY
	4 CHANGE KEY
	5 ERASE ALL RECORDS

色のついている部分はJIS X 6306で規定されていることを示します。

#### (6) 実証実験結果

滝川市ICカードシステムは商店街カードシステム(ポイント機能、駐車場ポイント機能)、健康管理システム(血圧、脈搏等の記録管理)からスタートしました。

上記システムは、計画通り96年2月に運用に入り、96年度で終了しました。

その検証・評価結果はニューメディア開発協会により、97年3月に「平成8年度電源地域における多目的利用ICカードシステム運用調査報告書（財団法人電源地域振興センター）」としてまとめられました。

実験終了後は滝川市に自主的な運営が移行しましたが、現在は34,000枚を超えるカードが発行され、商店街の加盟店も100店を上まわり、磁気

ストライプを利用してのクレジット機能が付加され、隣接地域への拡大が検討されています。

なお、実証実験中の96年10月には早くも、実験に参加した沖電気工業がシステムインテグレーターとなり、滝川市向け仕様（その後JICSAP仕様V1.0として制定）に基づき、駒ヶ根市商店街プライベート型電子マネーカードシステムを商用サービスとして実現させています。このシステムは電子マネーサービス並びにポイントカードサービスを併設して開始され、サービスのアクセス端末とし

#### 滝川市多目的利用ICカードシステム

##### システムの内容

システム	サービスの内容	稼働日	事業主体
商店街ポイントカードシステム	<ul style="list-style-type: none"> <li>・ポイント機能</li> <li>・駐車場ポイント機能</li> <li>・クレジット機能 (H9.4からクレディセゾンと提携契約)</li> <li>・プリペイド機能(H10.10から)</li> <li>・釣り銭積立機能(未稼働)</li> </ul>	平成8年2月	滝川情報事業協同組合 (げんきカード会)
健康管理カードシステム	<ul style="list-style-type: none"> <li>・健康データの測定結果に基づき保健婦が健康指導/相談</li> <li>・市民の健康状態に合わせた運動処方を書く</li> <li>・医学的検査/体力測定データの記録と健康の度合いの変化の把握</li> <li>・測定結果を「健康度測定総合結果」に記録し通知</li> </ul>	平成8年6月	滝川市保健課 (保健センター)

##### 利用状況

人口(滝川市)	48,000人	月間カード売上平均	5億円
商圏人口	75,000人	月間ポイント総発行数	500万円
カード発行枚数	34,146人	月間ポイント総利用数	400万円
加盟店数	110店	月間利用回数	15万回
店舗端末台数	147台	月間利用会員数	21,000人

##### 導入経過

- ・平成元年7月 通産省からニューメディアコミュニティ構想応用発展地域に指定
- ・平成3年3月 商店街・観光・流通・技術の情報化の指針策定
- ・平成6年3月 商店街カードシステムの導入に関する調査
- ・平成6年8月 小売業者に対するカードシステム導入意向調査を実施
- ・平成7年1月 多目的利用ICカードシステムモデル事業の地域指定
- ・平成7年4月 滝川情報事業協同組合設立

##### 導入の背景

- ・消費者のライフスタイルの変化への対応
- ・郊外型大型店、CVS、DSへの対応策
- ・消費者ニーズへの対応
- ・既存商業の連携の強化
- ・消費者とのコミュニケーション

##### 今後の課題

商店街ポイントカード	健康管理カード
<ul style="list-style-type: none"> <li>魅力あるイベントの企画</li> <li>顧客情報等の情報活動</li> <li>仮想商店街の構築</li> <li>新たな業種・業態店の加盟店募集</li> </ul>	<ul style="list-style-type: none"> <li>システムの拡充</li> <li>健康測定器の拡充</li> <li>市内健康づくり施設等での測定を可能に</li> </ul>

て金融機関のATMと各店舗POSを使用してリロード機能も当初から実稼動しています。

このことから、滝川市のモデル事業は予想以上の成功をおさめたといえますが、駒ヶ根市のシステムではその後、駒ヶ根市役所での住民票や印鑑証明書の交付手数料にも利用でき、また電子マネー並びにポイントのカード間移動等も可能となり、リージョナルペイメントシステム、コミュニティカードとして地元住民の日常生活に密着した完成度の高いサービスが提供され、近隣の飯島町にもそのサービス領域が広がっています。

#### 4 . JICSAP仕様V1.0の開示

JICSAPでは97年3月の滝川市多目的利用ICカード実証実験の検証・評価を受け、直ちに仕様公開に取組み、97年9月にJICSAP仕様V1.0として開示しました。

通産省は、96年2月に開始された滝川市の多目的利用ICカード実証実験が順調に推移していること、国内市場でのICカードシステム間の相互運用性を一日でも早く確立して行くことが望まれること等から、滝川市向けJICSAP仕様の早期公開を期待していたものと思われま。

この点で開示は遅過ぎたとの批判が一部ありましたが、すでに市場に出まわっているICカードの存在、見切り発車で公開したあとに不具合が発生した場合の影響など、JICSAPとしては慎重に対処せざるを得ない面があったことは否めません。

しかし、開示以降は、広域利用に向けたバージョンアップ作業に着手していたこともあって報道発表こそ見送りましたが、カード専門誌の月刊カードウェブに「JICSAPスペシャルレポート」ページを開設し、98年2月からJICSAP仕様V1.0の連載解説を始めました。また、98年3月には東京国際展示場（東京ビッグサイト）で開催された、日本経済新聞社によるSECURITY SHOWにはじめて出展し、仕様書を公開するなど、JICSAP仕様の普及に向け活動を本格化しました。

なお、同年4月には全銀協が、国際標準化及びJIS規格化の進展に対応し、技術的な仕様を全面的に改定、これを「全銀協ICカード標準仕様」として発表しています。

改訂にあたっての基本的な考え方の一つには、国際標準規格に準拠したICカードで多目的利用を実現することが含まれています。

#### 5 . 広域・多目的利用ICカードに向けたバージョンアップ

滝川市における多目的利用ICカードシステムのモデル事業で、異なるカードベンダー間の互換性及び1枚のICカードによる多目的利用が可能であることが実証されました。

一方、97年9月のJICSAP仕様V1.0の開示により、JICSAP仕様のICカードが特定のアプリケーション用ではなく、汎用的にどんなアプリケーションにも対応可能な機能を持っており、ファイル構成が必要に応じて自由設計できることから、いわゆるカスタム仕様にも使えるJIS準拠のICカードということも、システム開発者に理解されるようになってきました。

こうしたことから、S型（16社暫定仕様）を使用してきた自治省の地域カードシステムにV1.0が提案されるなど、JICSAP仕様ICカードを採用する動きが次第に顕在化してきました。

ちなみに、現在公開されている国内ICカード仕様のほとんどがJICSAP仕様を参照しており、建設ICカード、全銀協ICカードなどは、運用場面でのセキュリティ設定が一致していれば、ファイル内のデータと交換が可能です。

さて、こうした中で、98年3月住民基本台帳法改正案が国会に提出されました。法案は政府が金融再生法案の処理を優先させたことなどから、結果として審議は先送りされることになりました。しかし、法案には希望する国民に市町村から「住民基本台帳カード」が交付されることが盛り込まれており、そのカードはICカードが有力視されていることから、同法案の提出は、行政サービス分野における本格的かつ全国規模のICカードシステムの登場を予告するものでした。

##### (1) バージョンアップの背景と目的

今回のバージョンアップには上記のような背景があり、直接的には通産省及び社会保険庁からの協力要請を受け、ニューメディア開発協会との連携により実施されました。

##### (通産省)

情報インフラストラクチャ及びそれらを利用した各種サービスの提供が急速に普及する中で、サービス利用者にとっての利便性を向上させるため、次の課題について速やかに対応する。

ア．利用者の利便性を拡大し、かつICカードの普及を促進するために、1枚のICカードを複数の

目的に使用可能で、かつICカード製造メーカーの新規参入、サービス提供者の新規参加、および複数の主体によって発行されたICカードの相互運用が容易に可能な環境を整備する。(多目的に利用可能なICカードシステムの環境を整備する課題)

イ. 公共・民間分野で、様々なサービスをネットワークを通じて提供するニーズが高まりつつあるが、同時に、サービス提供者とサービス利用者が相互に確認するための情報や、サービスに係わる個人情報の安全を確保する必要性も高まっている。そのため、相互認証や個人情報の管理を、ICカードを利用することによって安全に実現するための、基礎技術を整備する。(ICカードのネットワーク環境での課題)

#### (社会保険庁)

JICSAPからの提案を参考に、熊本県八代市で実施してきた健康保険証ICカード化実験の第2期実験(98年10月を予定)において、JIS準拠のICカードに切替えることを検討する。

##### ア. 発行コマンドの完備性

発行ライブラリの導入・運用についての現状と課題、DFの生成機能など

##### イ. セキュリティ機能

現行システムより高いセキュリティレベルを確保するための相互認証、鍵の管理、セキュアメッセージング暗号コマンドなどに対する機能

#### (2) 広域利用とは

「広域」とは、全国どこでも利用できる、という地域的汎用性はもちろん、複数のアプリケーションを広範囲に利用できるという意味も含んでいます。

しかし、1枚のカードのメモリ容量には一定の限界があるため、すべてのアプリケーションを搭載しようとする、メモリ不足になる恐れがあります。この解決には、利用する時点で、カード利用者が必要とするアプリケーションだけを選び、カードに記憶させることができればよいし、不要となったものが削除でき、その領域を再利用できればなおよろしいといえます。

バージョンアップしたJICSAP V1.1は、カード内にあるファイルの追加・削除・再利用を可能とし、パーソナルカードとも言うべき機能を実現した仕様となっています。

#### (3) 広域・多目的利用ICカードのユーザ要求

広域利用では、上記の技術要件のほか、住民基本台帳ネットワークを例にとれば、全国の各市町村が「住民基本台帳カード」発行主体となって、複数のカードメーカーやシステムインテグレータに発注して行くことや、市町村以外の複数の民間サービス提供者がこれに相乗りする利用形態が想定されるため、こうした場面でのファイルの独立性とセキュリティ機能、認証機能がとりわけ重要となってきます。

広域・多目的利用のICカード仕様として、ニューメディア開発協会から示された主たるユーザ要求は以下のような事項でした。

##### ア. 要求事項

1枚のICカードで、カード利用者の要求や、提供されるサービスの変化に対応して、いつでも、どこでも、またいくつでも、業務発行処理、業務サービスの利用及び業務削除処理が可能なシステムとする。

##### イ. ICカードに対する新機能要求

- a. 業務サービスごとの独立性を確保すること  
既存の業務サービスのために生成されたファイルに設定されているアクセス権が侵されるような鍵の設定を、ICカードが許可しない機能を持つこと。
- b. 業務サービスを削除する機能を持つこと  
1つの業務サービスに関わるファイルを登録する領域であるDFを単位に、削除可能で、削除したファイルの領域に他の業務サービスを登録可能とする機能を持つこと。
- c. ICカード認証機能
- d. カード発行者が自らが発行した広域・多目的利用ICカードを1枚単位で確認できること。
- e. カード発行者が業務発行を許可したサービス提供者を確認できること。
- f. 上記機能が、ネットワークを通じて安全に行なわれること。

##### ウ. ICカードの発行に関する要求

- a. カード発行者およびサービス提供者は、ICカード製造メーカーを意識することなく、カード発行処理、または業務発行処理をする事が可能なこと。
- b. サービス提供者は、そのICカードに業務発行処理可能であることをチェックするために、ICカード内のメモリ残容量を精査可能なこと。

(4) 検討体制

ユーザ要求に基づき、JICSAPは標準化部会に「カード発行処理基盤技術検討分科会」、ニューメディア開発協会は「ICカード等広域・多目的利用研究会」に「広域利用検討ワーキンググループ」と「システムインテグレーションワーキンググループ」を設置し、取組みました。なお、検討作業の効率化と透明性、公平性を期し、広域利用検討ワーキンググループには公募によるJICSAP会員が委員として参加しています。

(5) V1.1の主たる規定内容

JICSAP仕様V1.1の運用コマンドは、V1.0との上位互換性を持ち、発行コマンドを除き、運用コマンド・準システムコマンド及びファイルのアクセス権とセキュリティ要件を一致させることにより、双方のICカードで共通の業務サービスが利用できます。

以下、V1.0とV1.1の規格内容の関係、V1.1の主たる追加・変更機能を示します。

**ア．ファイル管理**

ICカードに記録されているデータにアクセスするのがコマンド機能ですが、カード発行者、サービス提供者、およびカード利用者が設定するセキュリティ要件を超えて、ICおよびICカードの製造処理過程以外に存在しないこと。

セキュリティ対策としてスーパーバイザコマンドのICカード内の存在を禁止し、そのセキュ

リティ監査証跡を担保するため、ISO9992 - 2及び全銀協ICカード標準仕様（98年4月改訂版）に準拠し、MF直下に「IC製造者識別子ファイル」の設定を推奨しています。

**イ．業務一覧ファイル**

DF削除機能を適用する場合、対象とするDFをSELECT FILEコマンドでカレント状態にする必要がありますが、SELECT FILEコマンドのDF削除対象とは異なるDFがカレント状態となる可能性があります。

このパーシャル名による誤セレクトを防止するため、DF直下の業務一覧ファイルにDFを記録しておき、その内容でDFを確認する方式をとっています。

**ウ．DFのセキュリティ上の独立性**

DF創生時、当該DFおよび直接の上位・下位DFに存在する、IEFの創生を禁止することにより、セキュリティ上の独立を実現しています。また、業務発行処理の際、1階層目のDFにはDFの創生を管理するキーを記録することとし、業務サービスの提供時に使用するDFは2階層目のDFとします。なお、その際に当該業務サービスに係わるファイルのセキュリティ要件は、独自の設定が可能です。

**エ．DFの追加、削除、再利用機能**

オプションとして、DF単位での追加および削除、再利用が可能です。なお、DF削除のアクセス種別は以下の理由から、創生系（発行）

JICSAP ICカード仕様比較表

項目	広域・多目的利用ICカード JICSAP V1.1	従来の多目的利用ICカード JICSAP V1.0
1. 運用コマンド・準システムコマンド	JICSAP V1.0準拠	JICSAP V1.0準拠
2. 業務一覧ファイル管理（オプション）	自DF（MF）名及び直下のDF名をWEFに記録する	JICSAP V1.1準拠可能
3. DFのセキュリティ上の独立性	当該DFおよび当該DF直接の上位・下位DFに存在する、IEFと同一区分のIEFの創生を禁止することにより、セキュリティ上の独立を実現	JICSAP V1.0準拠
4. DF単位での追加 / 削除 / 再利用（オプション）	・追加 / 削除可能 ・削除した部分は再利用可能 ・発行DLLを用いる	追加のみ可能
5. 認証系暗号化方式（オプション）	複数の暗号化方式を搭載できる仕様としたので、Triple-DESとRSAを実装	DES、FEAL、RSAのうちのいずれか1つの暗号方式を搭載でき、DESを実装
6. セキュアメッセージ（オプション）	CHANGE KEYコマンドに対してのセキュアメッセージ機能を実現（データの隠蔽、データの完全性確認）	
7. 発行処理	・JICSAP発行ライブラリ仕様V1.1準拠 ・発行DLLを用いる	JICSAP発行ライブラリ仕様V1.0準拠

と削除を同じアクセス種別にししました。(アクセス種別については、今後不都合があれば継続して検討します。)

- ・発行した者のみが削除可能とする。
- ・DFを二階層化することにより、一階層目のDF配下のIEFを照合しないとDFの削除ができないファイルデザインを推奨することにより、DFを発行したサービス提供者以外の削除を妨げる。

#### オ．暗号化方式(認証用)

ICカードに複数の暗号アルゴリズムを搭載できる仕様です。対象鍵暗号方式として、新たにトリプルDESを実装しています。

暗号化：暗／復／暗

復合化：復／暗／復

非対象鍵暗号方式には、RSA(512ビット)を実装します。

#### カ．セキュアメッセージング機能

セキュアメッセージング機能は、ユーザーへの早急な対応を行なうために、

1. データの隠蔽、
2. データの完全性の確認、
3. データの隠蔽かつ完全性の確認、

という3つの機能をCHANGE KEYコマンドに適用するという条件付きで盛り込みました。当該仕様では、セキュアメッセージング機能の相互運用性を考慮し、カード上に1~3全ての機能を実装することを推奨しています。

#### (6) 一般公開説明会の開催

広域・多目的利用ICカード仕様は、JICSAP仕様V1.1として98年7月に開示され、98年10月文京区シビックセンターでの一般公開説明会において報道機関にも公開されました。

V1.0の際は報道発表を見送りましたが、今回は、当初から実証実験への多数企業からの提案、参加を期し、早期開示が求められていたこと、民間分野で活発化しているシステム提案への配慮等から、早期開示に加えて、一般公開説明会の実施まで踏み込みました。

#### (7) 岐阜県益田郡での実証実験の開始

JICSAP仕様V1.1を採用して、98年10月に岐阜県益田郡の5町村(金山町、下呂町、小坂町、萩原町、馬瀬村)を対象に、実証実験がスタートしています。

実験は、電源地域の振興をめざし、電源地域振

興センターが通産省・資源エネルギー庁からの委託を受けて実施している「電源地域指導事業」の一環として、ニューメディア開発協会により進められています。

岐阜県では、産学官による「ICカード導入研究会」を設置し、実験システム導入のための基本的なガイドライン「産学官ICカード導入研究会調査・研究報告書(99年3月)」をまとめています。同報告書は、観念的な見方や理論先行しがちな現状の打開には、実践こそが突破口、「住民基本台帳ネットワーク構想」に先がけて地域から実践することのメリットを生かし、今後国レベルで進むICカード利用システムをリード、サポートする役割を担いたいとする考え方が背骨になっています。

なお、八代市の健康保険証ICカード化第2期実験も、計画どおり98年10月から、JICSAP仕様に基づくICカードに全面切換えしスタートしています。

## 6. 英訳JICSAP仕様の刊行

JICSAPではここ3年連続して、ICカード先進地域の欧州電子マネー動向をターゲットに調査団を派遣し、帰朝報告会や報告書により調査結果を発表してきました。

このような海外活動で、情報収集活動だけではなく、日本からの情報発信も積極的に行ってほしいとの声が、毎回調査団に現地参加しているJETROや訪問先からでています。

JICSAPではこうした要望に積極的に対応していく必要があると考え、ドイツに在住する邦人コンサルタントとの契約を結び、必要な情報をコンサルタントを介して発信していく体制を作るとともに、情報発信の第一候補としてJICSAP仕様の英訳に取り組むこととし、99年3月に刊行しました。

英訳JICSAP仕様を第一候補とした主たる理由を以下に示します。

#### ア．わが国のICカード関連技術のPR

先に、日本は製造面では最先端の位置にいると自負しているものの、利用面では欧州に大きく遅れをとっているとの指摘をされました。しかし、広域・多目的利用の観点からは、利用技術面においてもJICSAP仕様の有用性と普及性は国際的にみても高いと考えられ、現に海外からの照会も寄せられています。

このため、英訳途中の英訳版スケルトンを、通産省の要請で出席した第10回日仏エレクトロ

ニクス・ラウンドテーブル（98年11月5日～6日）をはじめ、照会先に配布し、完成した英訳仕様書は入手希望があった内外の企業にすでに提供されているほか、ISO/TC215のHealth Cards WGでも紹介しています。

また、99年6月に国際標準として規格化されたISO 15408に対応して、わが国のソフトウェア及び電子機器・部品等のセキュリティ評価基準の作成に取組んでいるICカード取引システム研究開発事業組合（ICCS）では、JICSAP仕様をモデルとしたプロテクション・プロファイル原案の国際整合性の検証を、欧州の評価認証機関に英訳仕様書を付して依頼することを検討しています。

#### イ．ISO/IECへの標準化提案

広域・多目的利用ICカードの開発では「次世代ICカードシステム」の方向性を見極め、必要な技術開発と普及を行う目的が込められていました。

この流れを受け、さまざまな調整を経て98年12月に「次世代ICカードシステム研究会」が設立されました。同研究会はニューメディア開発協会との連携の中でシンクタンクとして機能し、通産省の「アドバンスドICカードシステムの開発」プロジェクトをはじめ各省庁との情報交換を通じ、JICSAP仕様をベースとした次世代ICカードシステムの実現をめざしており、国際デファクトスタンダードとしてISO/IECに提案できる成果を挙げたいとしています。

95年に結ばれたWTO/TBT協定により、ICカードをはじめすべてのJISなどの国家規格は世界貿易の障害になるとして、WTO加盟国は国際規格に準拠して、国家規格を策定することが義務づけられることになりました。以降わが国でも国際標準とJISの整合性がJIS原案作成においても重要視され、規格化においてはややもすると受け身的な対応となっています。

ISO/IECの国際標準化は1国1票の多数決原理で進められるため、標準化提案にあたっては理解国を確保することが決め手となりますが、以前から言語の問題がわが国にとって最大の課題だと指摘する意見もあります。

JICSAPでは、広域・多目的利用ICカードの実装規約としての英訳仕様書が次世代ICカードの提案に反映され、ISO/IECの国際標準化プロセスでの活用につながり、国際市場への拡大の一助となることを期待しています。

## 7．今後の取組み

ICカードは高度情報化社会における重要な要素技術の1つで我が国が得意とするハイテク商品であり、またICカードシステムは新しい社会システムとなり得る可能性を有し、かつ国家経済における投資効果も大です。

「住民基本台帳カード」をはじめ公共・民間分野での大規模システムの本格導入に向け、我が国のICカード市場では、今後ICカード及び関連機器の標準化とICカード採用システムの増加とが相俟って、ICカードの低廉化と多機能・高機能化が進むものと予想されます。

また、技術面ではネットワーク機能とともにCPUやMEMORYの飛躍的な技術革新によって、これまでのカードリソース上の制約から大きく開放される可能性が期待され、さらに各種実証実験からは本格展開に必要なICカードシステムの運用・制度・法律などについても新しい、貴重な情報が得られるものと考えられます。

現在、JICSAPをはじめICカードの標準化に関係する機関、団体では、2000年度のJIS原案作成候補を絞りつつありますが、接触、非接触どちらが主流になるかは別として、国際標準化が遅れている非接触型のJIS化については、次世代ICカードが非接触の近接型（ISO/IEC14443）を前提にしているほか各分野で、近接型が主流となる形勢となっていること等から、国内の市場動向に合わせ、何等かの大きな決断を迫られるかもしれません。また、これから明らかになる次世代ICカード仕様とJICSAP仕様との関係整理も大きな課題になることでしょう。

この場合、様々な分野にICカードシステムがその適用分野を拡大して行き、技術革新のスピードも急速であることなどから、国内ばかりでなく、ISO/IECの場をも視野に入れ、まずは企業レベルの利害を乗り越え国内標準としての統一を図り、それを国際標準化につなげていくような戦略的取組みが肝要です。

JICSAPではかかる情勢と考え方を踏まえ、また工業標準化法が改正され、従来にも増してJIS原案作成委員会の透明性、公平性が重視されるようになったこと等から、99年8月に委員構成を大きく見直し、質・量的な充実を図りましたが、ICカードに特化したミッションを受け、今後も期待に沿えるよう標準化活動に取組んで行くこととしています。