ICカード・多目的利用の実現のための
JICSAP仕様とは？
JICSAP ICカード仕様(V1.1)改版について

ICカードシステム利用促進協議会

今回から「JICSAPスペシャルレポート」を再開する。再スタート第1回目の今回は、先般開示された「JICSAP仕様Ver1.1」について、開示までの背景や仕様の意義、また現在までの導入事例などについて報告する。
仕様開示後の10月15日には、改版説明会が開催され、JICSAP会員だけではなく関係ベンダー、さらには一般メディアなども参加、100名の定員が満席になる盛況となっていた。

1．はじめに

ICカードシステム利用促進協議会（以下JICSAP）は、平成10年7月、日本工業規格準拠JICSAP外部端子付きICカード仕様に関する最新の第1.1版を開示した。

JICSAPは、官民・業種など事業主体が異なっていても、自由にアプリケーションをICカードに搭載できる、広域・多目的利用ICカードの実現を目指して仕様の標準化を進めてきた。今回の新しい第1.1版では、国際整合性を図って制定されたJIS規格票に準拠し、互換性の確保のためにISO／IECではオプション扱いの規格を実装上必須とした項も付加された。

さらに、外部端子なしICカード（非接触密着型ICカード）の関係では、共通コマンドについてISO／IEC10536は、外部端子付きの規格（ISO／IEC7816－4）の適用を規定している。そのため、本仕様の適用が検討されている。

2．改版の背景

今回の改版は、次の2点が直接的な契機となって行われた。

1）ICカード広域・多目的利用実証実験実施のための通商産業省からの要望

通商産業省は、JICSAP仕様（Ver．1.0、発行ライブラリ仕様Ver．1.0）をICカード多目的利用実証実験（北海道・滝川市）で採用した。そこで一定の評価を得たことから、発行システムのセキュリティに依存しない、広域的かつ多目的利用が可能なICカードシステムの有効性、実用性を検討する新たなフィールド実験の実施を計画。平成9年から、岐阜県・益田郡をモデル地区として検討・開発に着手した。

実験にあたって要望された技術要件は、広域利用を考慮したセキュリティの確保にある。広域利用の環境では、カードシステム管理者やカード発行者が複数にまたがる可能性が高い。しかし、現状のカードシステムは、カード発行者の管理義務として、それぞれが独自の方法で情報のセキュリティを担保している。この方法をそのまま踏襲していては、複数のカードシステム管理者・カード発行者にまたがる広域利用のセキュリティを確保しにくくなることが想定される。

そのため、従来のカード発行時のコマンドによる情報セキュリティの確保以外に、暗号化などによって情報セキュリティを確保する方法（＝発行システム非依存型セキュリティシステム）の検討が急務となっていた。

将来的に、この「発行システム非依存型セキュリティシステム」が実用的に稼働することが証明されれば、ICカードの発行コマンドなどは非公開とする必然性が消え、その規格の統一などが進み、ICカードの品質の均一化や低廉化がさらに促進すると期待される。

2）健康保険証Cカード化実証実験実施のための社会保険庁からの要望

社会保険庁は、平成7年度から3年計画で熊本県・八代市をフィールドとした健康保険証のICカード化実験を実施してきた。この第2期実験で、JICSAPは、国際整合化が図られたJIS準拠のICカードでの実施を提案した。これに対し、同庁からは、

1.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

2.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化コマンドなどに関するJICSAP仕様上の機能についての技術要件が示された。

3．アピールポイント

ICカードのオペレーティングシステムは、世界的に金融業務での利用に関する研究開発が先行しており、実際にJAVAカード、MULTOSなどが製品化されようとしている。国内においては、従来の多目的利用に加えて、広域利用の実現が期待されてきた。

「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、広範囲にアプリケーションを利用できるという意味も含まれている。しかし、事はそう簡単ではない。1枚のカードで多くのアプリケーションを搭載すると、メモリ不足になってしまう。

その解決には、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、カードに記憶させればよい。JICSAP仕様によるICカードは、このパーソナルカードとも言うべき機能を実現するために、カード内にあるファイルの追加・再利用を可能にしたものである。

また、アプリケーションを記憶する「アプリケーション占有ファイル」（DF）が、他のDFから完全に独立しており、ひとつのアプリケーションに専用のICカードとして利用できる。

これらの工夫によって、地域だけでなく、経営スタイル（官民）・業種が全く異なった事業主体の提供するアプリケーションが自由にICカードに搭載され、生活の広い範囲での活用を可能としている。

4．JICSAP仕様（Ver1.0）導入事例

1）多目的利用ICカードシステム（通産省）

通産省・(財）ニューメディア開発協会は、平成6年度から3年間、北海道・滝川市で、異なるメーカーのシステムで運用される、複数サービスの相互運用性の検証を通じて、公共・民間を問わない様々な業務サービスの提供が1枚のカードで可能なICカードシステムの実証実験を行った。現在、行政サービスとして同市の健康管理、民間サービスでは商店街のポイントサービスなどに対応した「げんきカード」として運用されている。

2）社会保険庁の医療保険カード

平成7年度から、熊本県八代市で健康保険証のカード化のあり方を検討するため、被保険者証機能に加え、健診情報、健康づくり情報などの記録も可能な、ICカードによる「医療保険カード」の導入実験を行っている。ICカード化のメリットは、被保険者にとって、①被扶養者を含め、加入者一人一人に交付された方が使い勝手が便利、②ICカード化により常時携帯が可能で緊急時に役立つ、③健康意識の向上、健康管理への関心醸成で受診機会が拡大する――などが挙げられている。また、医療機関にとっても、①健診情報などの収録が可能になり、カルテなどへの転記ミスの防止、②事務作業の軽減、③資格確認上のトラブル防止、④汚損による記号番号の読みとりミスの防止――などのメリットがある。

実験では八代市の人口約10万8000人に対し、約8万人に発行された。第1次実験は平成9年度で終了したが、平成10年度以降も引き続きシステムを継続、将来的には実験結果を踏まえ、全国規模での導入を進めていく考えである。

3）長野県駒ヶ根スタンプ協同組合、赤穂信用金庫

駒ヶ根協同組合では、商店街、地域の活性化、

図1　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準拠	従来の多目的利用ICカード JICSAP V1.0準拠
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）名および直下の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なったので、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る。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（データの隠ぺい、データの完全生確認）	―
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

大型店対策を目的に、平成8年度からポイント機能、プリペイド機能のついたICカード「つれてってカード」の発行を開始している。このカードは、商店街の加盟店140店での買い物にプリペイドカードによる支払いが可能で、ポイントも付与される。また、赤穂信用金庫と提携した「しんきんつれてってカード」では赤穂信金のATMからプリペイド入金ができ、キャッシュカードとしても使用できる他、今年9月からは駒ヶ根市役所での住民票や印鑑証明請求の支払いに電子マネーカードとしても利用できるようになっている。現在、発行枚数は約2万枚に達し、今年7月には近隣の飯島市にも広がっている。

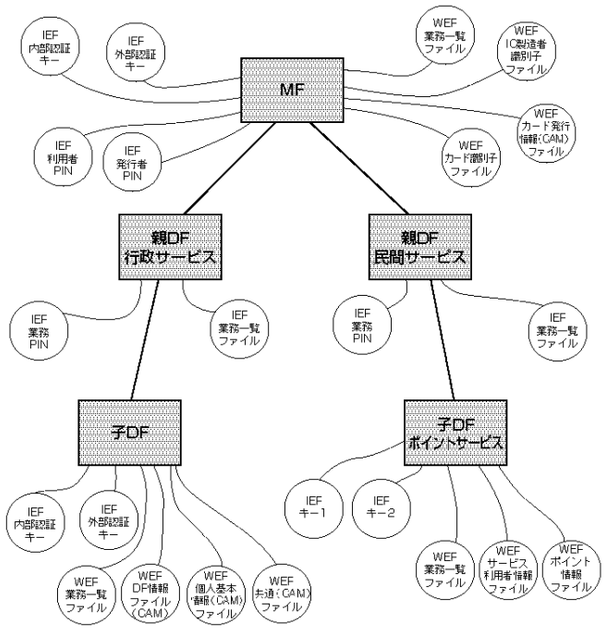
5．JICSAP仕様の概略

1）従来の多目的ICカードとの互換性

運用コマンドはJICSAPVer1.0準拠ICカードと上位互換を持つ。発行コマンドを除き、運用コマンド・準システムコマンド、およびファイルのアクセス権および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る。

2）ファイル管理

図2　広域・多目的利用ICカードファイル配置例



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だが、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。

3）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るが、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る。このパーシャル名による誤selectを防止するために定義した。

例）DF名“1234”と“123”が存在した場合にselect“123”指定するパーシャル名の対象は“1234”&“123”となるため、どちらがselectされるか判断できない。

そのためDF直下の本業務一覧ファイルにDFを記録しておき、その内容でDF名を確認する方式をとる。

4）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する。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とする。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ある。

5）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、再利用が可能である。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）と削除を同じアクセス種別にした。（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する。）

・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。

6）暗号化方式（認証用）

ICカードに複数の暗号化アルゴリズムを搭載で

きる仕様である。対象鍵暗号方式として、新たにトリプルDESを実装している。

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）を実装する。

7）セキュアメッセージング機能

セキュアメッセージ機能は、ユーザーニーズへの早急な対応を行うために、1.データの隠蔽、2.データの完全確認、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んだ。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る。

なお、詳細機能については以下のように規定している。

1.CCS作成時のパディングルール

ISO規格に従い、必ずはじめに‘80’、以下を‘0’でパディングすることにした。

2.暗号化、CCS作成時に利用できる暗号関数

暗号関数は、発行ライブラリにおける「IEF創生情報データオブジェクト」に暗号関数識別情報フィールドを追加し、ユーザーが発行時に選択できるように柔軟性を高めた。

3.暗号化機能モード

ISO7816－4のデフォルトモードはECBモードだが、CBCにも配慮し、カードでは暗号モードを選択できるようにした。

なお、ECBモードを使用すると、パディング部分の平文データが固定的になり、セキュリティが低下するおそれがあるが、ISO準拠のユーザーニーズも否定できないことから、両モードを併記することとした。

4.暗号化、CCS作成の単独機能

ユーザーのセキュリティポリシーに柔軟に対応できるように、単独の暗号機能、CCS確認機能を選択できるようにした。

6．AID付番管理、IC製造者識別子ファイルの登録の義務化

JICSAP仕様Ver.1.1では、カード発行者、アプリケーションサービス提供者、および利用者が設定するセキュリティ要件を超えて、カードに記録されているデータにアクセスするコマンド機能が、ICおよびICカード製造処理過程以外に存在してはならないと規定されている。

このため、ISO9992－2および全銀協ICカード標準仕様（改訂版）に準拠し、セキュリティ監査証跡のために、MF直下にEF－ID＝2F11のIC製造者識別ファイル（WEF）について、1.埋込者／IC組立業者識別子、2.IC製造者識別子、3.製造者ICタイプ識別子の設定を推奨している。

埋込者／IC組立業者識別子はCCEEAで表されCCおよびIC製造者識別子は、ISOで管理されているが、国内での流通が想定されるカードには国番号以外の基準がない。このため、関係する国内標準団体と協議し、当協議会が付番管理責任を担うことになり、別途Ver1.1に反映させる。また、ISO/IECから勧告されていたICカードAID（アプリケーション識別子）の国際付番管理制度についても、平成11年1月にJIS制定され、（財）日本規格協会が付番登録センターとして機能することが決定したことから、併せてVer1.1に反映する。

7.JICSAP仕様今後の方向性

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ある。

2000年～2001年頃に期待される本格化に向け、我が国のICカード市場では、今後ICカードおよ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る。

今後、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、また各種実証実験からは本格展開に必要となる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る。

JICSAPではICカード（システム）に特化したミッションを受け、ICカードの一層の普及拡大に向け、より使いやすく、わかりやすいカードへと発展させていく。