ICカード・多目的利用の実現のための JICSAP仕様とは？
広域多目的ICカードと次世代ICカード

凸版印刷株式会社
金融・証券事業本部 カードセンター 寄本 義一

はじめに

JICSAP仕様は、現在ICカードの国内標準仕様の位置づけとなっており、その仕様の検討に当たっては、国際／国内で標準化の検討メンバーが集まり、国内のアプリケーションユーザの要求と国際／国内標準規格を基に仕様書を作製している。

JICSAP仕様における多目的利用の運用場面での各カード製造会社間の互換性については、ニューメディア開発協会が行った滝川市システムで実証済みである。

今回は、その仕様（日本工業規格準拠JICSAP外部端子付きICカード仕様 第1.0版）との互換性を保ちながらも、JICSAP仕様の一つの発展型として、同じくニューメディア開発協会が行う岐阜県益田郡での広域・多目的利用ICカード仕様を検討したので、その紹介を行い、さらに次世代JICSAP仕様について述べる。

標準化とバージョンアップ

システムの構成要素を標準化することは、そのシステムを利用目的に沿って速やかに開発出来るばかりか、運用、さらには保守も容易となる。システム機器間のインタフェースが標準化され、ハードウェア、ソフトウェアの両面で互換性を持つ様になると、それに合致する機器をどのメーカーから購入しても、システムに組み込むことが可能となり、その製品寿命も長くなるのでメーカーは大量生産による低価格化と安定を供給することが可能となり、ユーザも安心して利用出来る様になる。しかし、システムの構成要素のある部分が技術の進歩によってグレードアップして行くような場合、ユーザはシステム全体において最小条件の互換性をとりながらも、システムに使用する機器全体の効率化、利便性を向上させるための見直しが必要となってくる。また、ISO/JISの標準規格の改正あるいは、ユーザアプリケーションの必要から仕様が修正・追加されることも考えられる。

JICSAP仕様が次第に変更されていくことに互換性と言う点で不安を持れる方もあるかと思うが、ファイルの構成要素とセキュリティ、運用/準システムコマンドなどのICカードの機能を規定した「JICSAP 外部端子付きICカード仕様 第1.0版」を互換性を保つための基本とし、それに、それぞれユーザの要求をオプション機能として追加していく方法を取っている。これらは発行ライブラリと共にバージョン管理されている。

広域・多目的利用ICカードのユーザ要求

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より示されたユーザ要求は以下のような事項であった。

(1) 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および業務削除処理が可能なシステムに使用する。

(2) ICカードに対する新機能要求

・業務サービスごとの独立性確保すること： 既存の業務サービスのために生成されたファイル

に設定された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。
→対応方法：業務ファイル(DF)をMF配下の2階層とする。上位DFはMFにある創生系のアクセスキーを照合することで創生出来る。次にそのDFの配下にファイル創生用のIEF（パスワード/キーをしまうファイル）を同様のアクセス権のもとに創生/パスワード/キーを設定し、下位DF（実際の業務サービスに使用する）の創生のために用いる。この様にする事で、MFのセキュリティが下位のDFのセキュリティに影響を与えない仕組みを作った。なお、パス上で、同じパスワード/キーが存在してはならない事としている。

- 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。

→対応方法：要求機能はカードメーカ毎の個別機能で実現するが、発行ライブラリのDLLを用いて、それらの機能を統一する方法とする。また、業務一覧表によってカード内にどのファイルが存在しているを確認することが可能となる。

- ICカード認証機能
- カード発行者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。
- 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。
- 上記機能が、ネットワークを通じて安全に行われること。

→対応方法：要求機能は「カード認証、外部認証」に、トリプルDES、RSAを使用出来るように基本仕様に追加し、それらに使用するキーの設定/変更が可能なように、発行ライブラリに機能を追加する。

(3) ICカードの発行に関する要求

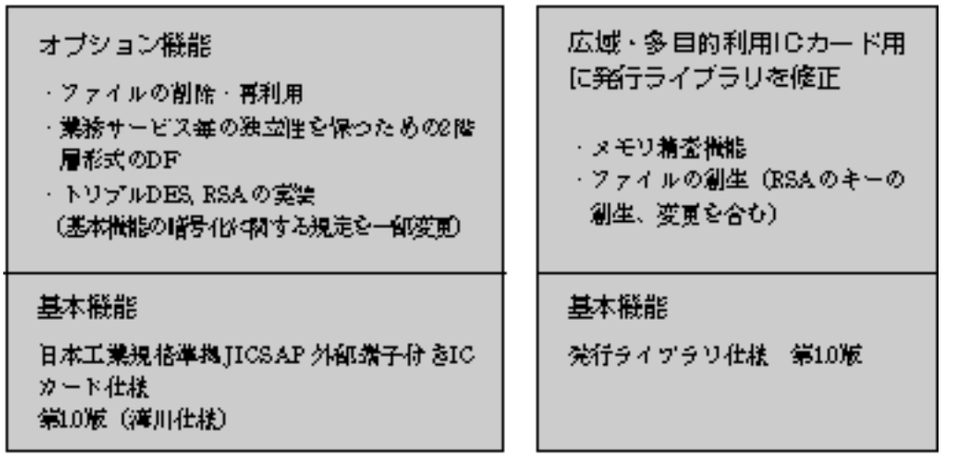
- カード発行者およびサービス提供者は、ICカード製造メーカーを意識することなく、カード発行処理、または業務発行処理をする事が可能なこと。
- サービス提供者は、そのICカードに業務発行処理可能であることをチェックするために、ICカード内のメモリ残容量を精査可能なこと。

→対応方法：ICカードのカード識別子からカード製造メーカー/仕様バージョンを発行機が特定し、DLLにより、そのメーカ毎のメモリ精査、ファイル創生コマンドを用いて、発行処理を行うものである。それらの仕様は発行ライブラリに記述されている。

今後のJICSAP仕様について

現在、国内外ではICカードのオペレーションシステム（以下OS）の開発が盛んに伝えられてい

広域・多目的利用ICカード仕様の構成



る。パソコンで言う、WINDOWSやMAC OSのような汎用OSである。汎用OSに近いものをICカードに組み込み、自らプログラムをICカードに組み込みたいと言う要求がある事への対応である。このJICSAPスペシャルレポートの中で何回も述べているが、JICSAP仕様のICカードは、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いる。しかも、ファイル構成は、必要に応じて自由設計だから、所謂カスタム仕様にも出来る。昨年JICSAP仕様が公開されたので、システム開発者の理解も得られるようになったと思う。

また、現在公開されている国内ICカード仕様のほとんどがJICSAP仕様を参照している。建設ICカード、全銀協ICカードなどは、運用場面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ある。

次に国内で一番利用されているJICSAPカードの基本的な機能仕様を変えることなく、次世代JICSAPカードの可能性を考えてみたい。

ICカードの機能アップの可能性について

ICカードは超小規模のコンピュータシステムである。使用されているマイクロプロセッサのほとんどがチップサイズの関係から8ビットのマイクロプロセッサで、1kB前後のRAMと20kB程度のプログラム用のROMを持ち、ユーザがデータファイルを書くことの出来るEEPROMが標準的には8kBとなっている。ミスプリントではない、「kB」である。しかしこれだけのメモリリソースでICカードのOSは通信を制御し、データの暗号化、ファイルのアクセス管理、パスワードチェック等のセキュリティ要件、データの読書き等のコマンド機能を実現しているハイテク製品でもある。

近年の半導体技術の進歩、特に半導体集積率のアップは目覚しいものがあり、電子1個で記憶するものまで出現しそうである。ICカード用では演算用コプロセッサのついたものが出現している。しかし、JAVAカードの特集等を読んでいると、「現在のチップではかなり限定された機能となるが、近い将来‥…」と言う記述によく出会う。

以降では、それ程の進歩が無くても実現可能な広域・多目的カードの次世代機能の候補をあげてみる。

●ファイルの追加・削除：現在ファイルの削除・再利用については、JICSAP仕様では、オプション扱いとなっている。ファイルが物理的な構成で出来ている場合は、多くの処理時間を要するからである。汎用記憶メディアの殆どが、ファイルの削除・再利用が可能となっており、それらは、ファイルがFile Allocation Table(FAT)でOSによって管理されている。しかし、ICカードではメモリ リソースの関係でその採用が遅れている。そこで、端末にあるコンテンツ アクセス メソッド（CAM）がその働きを代役している。CAMに多くのデータを転送、処理した後にまた転送してICカードに戻すと言う処理時間を短縮し、セキュリティ確保の点からも、ICカード内部で処理すると言う事を早急に検討しなくてはならない。また、FAT管理の採用によりファイルの創生、削除機能がシンプルとなり、発行機側の負担も軽減する。また、OSが未使用領域も含めてICカード内全てのメモリ管理を行うので業務一覧表も自動的にICカードのシステム管理ファイルとして作製されるようになる。

●伝送時間の高速化 ：つい最近まで、確かに9600bpsの伝送速度がよく使用されていたが、他の機器を見ると、モデムも56kbpsの時代である。9600bpsでは1文字送るのに約1.1msかかる。現在のところ、JICSAP、建設、全銀協、EMV仕様では、9600bpsとなっているが、国内メーカー製のマイクロプロセッサの実力から、最低でも倍の19200bpsは可能と思われる。処理の高速化の1つとして検討したい。

●ポイントカード機能について： ユーザから「高度な暗号化が出来るマイクロプロセッサで足し算、引き算が出来ないはずはないでしょう」と言われて答えに窮するが、ポイントカード用として加減算のコマンド機能を検討したい。

以上の様に、今後も時代の趨勢と要求に合致するJICSAP ICカード仕様を検討したいので、関係各位のご理解とご協力をお願いしたい。