次世代ICカードシステム研究会設立

研究会会長　東京工業大学　大山教授インタビュー

昨年12月、「次世代ICカードシステム研究会」の設立設立総会が開催され、研究会が発足した。同研究会はエヌ・ティ・データ、日本電信電話が代表発起人として参加、さらに関連の企業15社が発起人として参加している。会長には、東京工業大学の大山永昭教授が就任。同教授は、JICSAPにおいても標準化部会の幹事をしておられる。そこで、今回のJICSAPスペシャルレポートでは、今回設立された次世代ICカードシステム研究会の活動内容や、さらにJICSAPとどのように連携を取っていくのかなどを中心に伺った。

（聞き手：本誌長岡二郎）

共通プラットフォーム作り

長岡：まず「次世代ICカードシステム研究会」では、どのような活動をされていかれるのかから伺いたいのですが。

大山：設立趣意書の目的の項には、「関係省庁等との情報共有、意見交換を通じて、次世代ICカードシステムに求められる実効性・実用性の高い共通プラットフォームを検討すると共に、次世代ICカードシステムの普及促進を図ること」とある通りです。ただ、この共通プラットフォームということについては、説明が必要でしょう。例えば接触型の7816の場合、カードの形状や電気的な特性は7816のパート1から3までで、パート4がコマンドにあたります。このコマンドが同じでないと、コンピュータシステムとの整合が取れません。ここの標準化はすでに終わってますので、標準化をしようと思っているわけではありません。まず各省庁でカードを利用する場合、これまでは各省庁用にカードを作ることが必要でした。しかしパソコンを見た場合、何々省庁用というのはありません。なぜ、カードは何々省庁用になっているのかというと、答えは言うまでもなく、リソースが足りないからです。もちろん各省庁がそれぞれの目的に向かってカードを使うのは当たり前の話ですから、限られたリソースを前提にすれば必然的にカードが異なってきてしまうわけです。同じ7816シリーズのパート4に準拠しても、リソースが足りないため異なるカードが必要になってしまうわけです。その結果、製造メーカーは、それぞれのユーザーに合わせたカードを作ることになりま

発起人企業

発起人代表	株式会社エヌ・ティ・データ
	日本電信電話株式会社
発　起　人	沖電気工業株式会社
	オリンパス光学工業株式会社
	ユニカ株式会社
	大日本印刷株式会社
	株式会社デンソー
	株式会社東芝
	凸版印刷株式会社
	日本アイ・ビー・エム株式会社
	日本電気株式会社
	株式会社日立製作所
	株式会社富士総合研究所
	富士通株式会社
	松下電器産業株式会社
	三菱電機株式会社
	株式会社リコー

す。ですから多品種になります。数はそんなに出ないことが多いので、少量生産になってしまいます。多品種・少量生産というのは、一番コストを上げることになります。ですから、この際、すべての要求が満たせるようなカードを開発し、それで各省やさまざまな場所でカードを使うことが実現できれば大量生産が可能になります。大量生産が可能になれば、コストダウンが実現します。さらに高機能にすれば、国際市場でも競争力がつきます。そういう仕掛けを作ろうとしているわけです。このきっかけとして、公的分野を最初に考えたわけです。各省のアプリケーションで必要な要求を明確にしてもらい、研究会で全部吸収できるカードの開発を支援するのです。そのためには、個別の開発部隊で行っても駄目で、各省の要求や技術動向等を情報共有をする必要があります。

長岡：すでにJICSAPや、ニューメディア開発協会など、さまざまな標準化のための組織がありますが、そこに今回、新たに研究会を立ち上げた背景は何ですか。

大山：それは非常に明瞭で、15省庁が参画してくれていることに表われています。すなわち15省庁に参画して頂くには、ニュートラルな組織であることが必要で、特定の省庁との関連の深い団体では、この目的を達成することは難しいのです。会の活動も、1年強の時限にしています。

長岡：JICSAPは具体的にはどういった形で参加されるのですか。

大山：JICSAPは、特別会員で入るのではないかと思います。それから先の話として、規格（案）なども出してもらえることも考えられます。また、標準化にかかわることが必要であれば、全部JICSAP側にお願いするつもりでいます。

開発ではなく、各省庁の要件を整理する

長岡：ただ予算面から見ると、開発には費用が足りないのではないでしょうか。

大山：この研究会では開発は行いません。各省庁別々で実施します。例えば郵政省では、14443ベースの無線カードシステムを、10億円程度の予算を投入して開発します。また通産省では、約16億5000万円の開発予算を別途用意しています。つまりニーズが明確になってシステムに対する要求定義が決まると、開発はそれぞれできるようになっているのです。そこまでの仕掛けは作ります。両省とも開発が終わるのがちょうど来年度いっぱいですから、会の活動もこのタイミングに合わせています。

長岡：通産省のほうはアドバンスドICカードですか。これは16億5000万円に包含されているものなんですか。

大山：そうです。

長岡：また「プラットフォーム」という表現に戻りますけれど、これはファイル構造の規定ということになるのですか。

大山：ファイル構造を規定する必要は全くありません。それは、アプリケーションごとに決めれば良いことです。例えばこう考えていただければ良いと思います。例えば今、3つのサービス形態があるとします。公的、民間、どちらでも構いません。この3つが、1枚のカードに相乗りするためには何が必要なのかを考えます。各サービスにおける要求は全部違うことがあるので、カードの仕様は、全てをカバーすることが必要になります。相乗りした状況をカード側から見ると、各アプリケーションは独立していますので、それぞれ専用のシステムで構いません。各アプリケーションでは鍵の管理などを行なっていますので、カードに記録された情報の安全性は保たれます。そうすると、ある程度高い値段でも、例えば1000円でも20個のアプリケーションを搭載すれば1つのアプリケーションあたりの値段は50円になるわけです。

長岡：するとカードにアプリケーションを追加した場合、どこかに持っていかないとその機能が乗らないとなると、最初に何かを乗せるとなるとあちこちに行かないといけない。そういう意味では、追加のアプリケーションをネットワークともうまく連動して、搭載する仕組みを作ることが必要になりますね。

大山：その通りです。
長岡：さまざまな機関のカードが1枚化されると自分たちでセキュリティなどを抱え込みたい部分が出てきますね。
大山：それぞれにやってもらいますから、中は完全に独立させます。
長岡：例えば、暗号アルゴリズムは独自で持ちたいと思った場合にはどうすればいいのですか。
大山：暗号アルゴリズムは、ダウンロードを可能にしたいと思っています。
長岡：なるほど。

非接触ICの近接型にする理由

長岡：金融機関などでは、接触ICカードということが言われていますが、非接触ICカードとされるのは、10年先を見越してのことでしょうか。
大山：10年先ではなく、3年先を見ています。ですから、来年度いっぱいで方向性を出そうとしています。
長岡：特に14443（近接型）にされる理由はどこですか。
大山：今は近接と言ってる人が多いのと、もう1つはやはりテレホンカードの動きです。電話機とうまく合わせ込めるかどうかは、大変な違いなんです。ですから、私はできれば14443系統で電話機と兼用できるかたちが良いのではないかと思っています。
長岡：近接型のタイプ的A、BそれからCと言われるものがありますが、どれを利用するのかの絞り込みをされるのですか。
大山：絞り込む必要があるのかどうかは分かりません。というのはそれぞれ特性が違いますから、必然的に目的によって何を利用するのかが異なることが有り得ます。タイプ別の組み合わせができれば良いのではないかと考えています。
長岡：それは技術的には可能ですか。
大山：技術的には可能と聞いています。
長岡：海外の標準化動向への働きかけもされているのですか。
大山：これから始めるところです。ただ標準仕様は、ISOが行ないますから、別のレベルで調整をする必要があると思っています。

カードの機能を保証する組織も

長岡：CPUは32ビットにされますか。
大山：それは、開発の方のテーマであって、この研究会のテーマではありません。特に、インフラで利用するのであれば、カードの能力の話だけで議論しても意味がなくて、本当に使えるのかどうか、使えてどういう利便性があるのか、ということにシフトしないと無理です。この研究会はこれらのことを議論する場なのです。そこで一番大きい問題は、相乗りができるかどうかです。相乗りをするためには、セキュリティの部分をどう保持していくのかが重要です。つまりあるサービス提供者が、独自のセキュリティをかける場合、そのセキュリティ機能に対する責任はサービス提供者にあります。しかし現実にはカードメーカーがその部分を補っていることがあります。すなわち、カードメーカーとサービス提供者が一対一の場合は良いのですが、複数対複数になると従来の方式では不可能なのです。この課題に対する解決策も今度の夏までに明らかにするつもりです。
長岡：そうしますと、第三者的な組織も必要になってくるわけですか。
大山：いや、それは議論がまた別なのです。少なくともカードの機能を保証する所が必要になります。見掛けは全部同じになりますから、このカードは相乗りできるのかどうかということは、当然サービスを提供する側にとっては不安です。ですから、そのカードの機能を保証する所が必要になるわけです。
長岡：それは例えばどういったものが考えられるでしょうか。
大山：1つ考えられるのは、ニューメディア開発協会があります。ただその点についてはまだ議論

していません。
長岡：機能の保証というのはAIDとの管理とは別の動きなのですか。
大山：AIDというのは、ファイルのアドレスというか名前だけですから、AIDではカードの機能は保証できません。
長岡：カードの機能を保証して、万が一破壊された場合は、どうなるのですか。つまりトラブルが起きたものに対して保証するという意味なのか、そのトラブルが起きないようなカードを保証するのかといったことですか。
大山：後者です。その仕掛けをこのカードは持っていますという保証になります。
長岡：すると、認定マークではないですけれども、似たようなものも必要になってくるということですか。
大山：なるかもしれません。ただ、目で見て必要なのか、電子的なもので必要なのかというのは、これからの検討課題です。

今後、１年間の進行方法は？

長岡：それらを含めて、プラットフォームを共通化していこうということですね。
大山：研究会では、各省庁からの要求が明確にできれば良いと思います。それからどれぐらいの値段で実際のものが出てくるかというのは、また別のプロセスになるでしょう。
長岡：今後、どういった方法で進行されていかれるのですか。
大山：年内（1998年）に第2回目の理事会を開催する予定です。そこでは役割分担と進め方を決めます。
長岡：分科会を設けられるのですか。
大山：分科会を作るかは、研究会で相談をすることになると思います。
長岡：ただ意見を聞いていると、「ああでもない、こうでもない」といろんな出てくる可能性もあります。
大山：さまざまな意見を聞いて対応できてしまうかどうかも、大きな鍵です。もちろん全部1つの仕様で書けたら面白いですがね。
長岡：かなり、力仕事になりますね。
大山：そうですね。

バーチャルの世界へのアクセスにICカードが有用な理由

大山：1つ期待しているのは電子レベル、例えば各省庁から電子的に証明書が出てくると面白いと思っています。というのは、公衆電話で必要な証明書が取れてしまうからです。そういう世界ができるかもしれません。
長岡：いわゆる、税務署に行ったり、市役所に行ったりというのではなく、公衆電話の端末でできてしまうということですね。
大山：そうです。これができたらすごいですね。
長岡：そうですね。それをやりつつ、かつプライバシーも守るようなところの仕組み作りが大切ですね。
大山：カードというのは、自分の情報をコントロールするにはすごく有効なツールになると思うのです。自分の意志でしか動かないように作れるわけですから。だから、プライバシー保護のためにも、コントロール権の面からも、カードを使うというのは分かりやすいのです。
長岡：ひょっとしたら、それらがうまく先行できるようであれば、1つの行政ホームページがあって、例えば厚生省とかとあって、クリックすればそこにリンクをして飛んでいくというようなことも、技術的には可能ですよね。
大山：そうです。そして、その飛び先は基本的にはカードの中に入っていても良いし、少なくとも認証の鍵はカードの中に入っていれば良いのです。ただし、その番号はすべてのカードで同じである必要は全然なくて、ばらばらでも全く問題ありません。それぞれの所にいったら、そのままの番号を使えば良いわけですから。
長岡：なるほど、わかりました。カードはそういった分野での有効性が高いということですね。本日はお忙しい中、ありがとうございました。