

第1部

スマートカードが先導する、 e - Japanの行方と展望

～スマートカードが変える、暮らしを変える、ビジネスを変える～

(ICカードフェア2002における総括講演から)

- ◆年月日: 平成14年9月27日(金)
- ◆場 所: 科学技術館 地下1階サイエンスホール
- ◆講演者: 東京工業大学 教授・工学博士 大山永昭氏
フロンティア創造共同研究センター
共同研究機能情報系分野

これから、40分程でございますが、今後のICカード(スマートカード)の展開を含めまして、私自身の考えをお話し申し上げたいと思っております。事務局側から要望されました講演タイトルは、「スマートカードが先導する、e - Japanの行方と展望」とのことです。

e - Japanが何処へ行くのかというのは、我々みんなの関心事だと思います。ここに集まっている多くの方々には、スマートカードの普及により、きっと我々の暮らしが変わるのだろう、あるいは自分達の関係する情報技術なり情報システムが変わっていくのだろうというところに、期待を寄せているのではないかと思います。

画面の右上に、NICSS(ニックス)のロゴがあります。将来は、このロゴが入ったインターネット接続の各種電子機器を、世界中の製品に貼ってもらいたいと実は密かに思っているものでございます。

最初に、e - Japanをはじめとして、社会の情報化に関して、もう一度確認しておくことがございます。ここにもありますように、ITの導入というのは、単なる手段です。ITという新しい強力な武器を、あるいは便利な道具をいかに上手く使うかにかかっています。従って、使えない方にはお使いいただけようように何等かの支援をしなくてはなりませんし、使いたくない方も、ITの利便性を知ればお使いいただけるようになるのではないかと思います。

社会の情報化の目的は、我が国の繁栄の維持・発展であります。今のまま、日本経済が停滞しますと、多少定年が延びたとしても、きっと我々の子供達の



時代には、年金等社会保障のレベルが下がってしまうということもありえるのではないかと思います。従って我が国にとっては、社会全体のIT化の推進が必要であって、決して個別分野のIT化の議論をしているのではないということでもあります。

今、情報インフラを構築することは、そのためのブロードバンドであり、そのためのスマートカードということをまず、同じ思いに立っていただきたいと思うわけです。e - Japan重点計画は御存知の通り、「民間主導政府による環境整備」と書かれております。今のIT基本法は、後一年半程で改正を検討するということになっていますので、間もなく起草委員会が再開されると伺っております。

一方で、産業構造の変革に伴い、知的財産というものに対しても、大きくクローズアップされ、政府においては「知的財産戦略会議」というのが既に設置されています。更に「知的財産基本法」という法案を秋の臨時国会に提出し、来年早々には「知的財産戦略本部」を立ち上げるという主旨のことが言われております。

こういう大きな変化があるわけではありますが、民間主導政府による環境整備と言った流れから、経済不況の深刻化や、補正予算の必要性の論議とともに、

公的分野への投資への期待から、ある意味で電子政府・電子自治体が大きくクローズアップされてきています。

本来の目的からしてみれば、当然のことながらこの電子政府・電子自治体は、社会全体のIT化、即ち民の情報化の促進支援に繋がるように、上手くもっていかねければ、官側だけが小さな政府になっても、国全体の経済力・活力は落ちてしまうだろうと思うわけです。幸いにして、e-Japan戦略の中には、ICカード（スマートカード）は電子政府サービスを受ける標準インターフェースであると位置づけられています。自由と安全を保証する安全側のキーデバイス、これがスマートカードであるということになると思います。

今日は、そのスマートカードが普及して、その後更にどうなっていくのかということについて、今政府等で議論されている内容についてご紹介したいと思います。

スマートカードの中に入っている重要なデバイスは、実はカード形のものではなくてICチップでございます。この半導体をセキュアチップと呼んでおりますが、このチップの機能による安全性によって、インターネット社会における安全と自由が保証されてくるわけです。たまたま財布の中に入れるのにカードの形が便利なものであることや、更には国民全員にセキュアチップを内蔵した携帯電話を配るというわけにもいきませんので、スマートカードが位置づけられたということなのです。

住民基本台帳カード（住基カードと略称）については、まだまだ状況が正確に知られてない面がございます。住基カードは、社会のキーデバイスとして、あるいはきっかけとなり、それが省庁・自治体の壁を越えた行政連携カードとなって、より多目的に使えるように、世の中のインフラを整えようというのが今の考え方です。このような動きを実現するために、ニックスで作りましたフレームワークというものが採用されております。IT装備でも、この方式ののりつた各種システムが作られたということでもあります。更に、電子空間における本人確認のために、従来の記名捺印にあたる公的個人認証サービス（PKI）の普及が計画されています。

ニックスのフレームワークで作られた、公的な、あるいは行政連携のスマートカードは、他の目的でも使えるように、その機能および安全性が確保されております。従って、電気や水道、道路と同じように、それらが整備されることによって、新しい町ができ、人が集い、ビジネスが起きるといふ、そのためのインフラの一つになっていくだろうと期待されるものであります。こういう公的分野のものを進めるためには、当然のことながら、国際標準にも十分配慮する必要があります。簡単に言ってしまうと日

本発のデファクトあるいはモジュールの標準を推進するためにもEUとの連携や、それからグローバルプラットフォーム（GP）と呼ばれるVISA・Master Card等のクレジットカード会社等との技術提携が重要になってきます。

現在では、既にこの状況が整いつつあります。EUのSCC（スマートカードチャーター）との交流は、来年度以降、公的分野でのカード利用に主眼が移ってきており、我々日本と協力を進めることになっております。ニックスのフレームワークというのは、我が国が生んだ考え方であり、我が国の技術になっており、あまり知られていませんがこの技術はEUとの協力、GPとのMOU締結等を見てもおわかりのように、我が国の技術が世界をリードできるチャンスをもっているものです。もっと簡単に言えば、世界の中で日本にしかまだ製品がないということも言えます。これをいかに使って更なる飛躍、発展を遂げるかというのが、そして我々の生活が将来どんなに便利になるかというものを作り上げようするわけです。

先程も言いましたように、政府に知的財産戦略会議が設置されております。知財と言いますと、大抵、大きく二つ考えられます。一つは特許、もう一つは著作物です。もちろんブランドや衣装のようなものもございます。知財そのものの性質を考えてみますと、知的財産というのはまず人の知恵によって創出されるということなのです。従って我々が努力をしなければならぬと同時に、制度的に権利化するための保護をする必要があるということなのです。権利として成り立たなければ、富みにはならないということなのです。

そして3つ目が重要なのでありますが、即ち 創出、権利化、その次です。それは、流通です。知財は流通しなければ、使われない知恵になってしまいます。ここをいかに促進するかというのを知的財産戦略会議で議論がなされているところです。

ご案内の通り、著作物については、著作権者の方たちが、インターネット上に流すのを躊躇しているものがたくさんあります。これをどうやって解決するか、それも自由と安全の中でどう構築するかが、大事なポイントと思うわけです。インターネットを含めてネットワークが社会全体に広がっていくとき、利用者からみると先程から言うように、インターネットは自由に何にでも使えるからこそ、大きな価値を持っています。

ところが、一つ何かあれば、あるいは自分にとって大切な情報であれば、安全性についても配慮せざるを得ないということになります。システム全体を静的にどちらかの状態、すなわち自由で十分な安全性を確保する必要のない状態、あるいは安全ではあるが自由な使い方を阻害されてしまう状態が考えられます。ユーザーそれぞれの立場からみれば、コミュニケーションを取る相手との自由な合意のもとで、

安全性については必要なものを自分達で確保するという形になるのだらうと思います。

その意味では安全性のレベルは、例えばインターネットも今後はスタティックになるのではなくダイナミックに変化できるものが必要であると思うわけです。安全性のレベルは、コミュニケーションの都度決めても構わないのではないかと思います。その点、今のIPV6のような技術はどちらかという、スタティックな状況になっております。こういうものも、更なる情報技術の発展として考えたらどうだろうか。ということは、ダイナミックコントロールが必要になります。即ちリモートでお互いのコミュニケーションをはった上で、セキュリティーレベルを確保するというわけです。これを安全かつ確実にを行うために、新たなビジネスモデルができる可能性を考え、もしできれば当然権利化するということが今の流れかと思うわけです。

漠とした話が多すぎると、わかりづらくなりますので少し、具体的な話に入ります。機器及びコンテンツの認証、そしてそれらをインターネットから認証する新しい認証ビジネスを作り上げていきたいと思うわけです。

具体的な戦略と目標という形で申し上げますと、つい先日、内閣府に作られた経済再生諮問会議からの要望で、情報家電、ブロードバンド、ITと呼ばれるタスクフォースが設置されました。その時に、私が使った資料の中で、現実のソリューションとしてのスマートカードを用いた戦略があります。スマートカード戦略は、日本の国力あるいは富を益すためのものです。現在世界最高レベルになりつつあるスマートカードシステム産業を、なんとか確固たる産業にしたい。そして2005年までに国際市場の50%のシェアを取っていきたい。今の日本のスマートカードを輸出産業としてみると、残念ながら少ないものであります。ここをなんとかしたいと考えています。更には日本発の国際標準を獲得し、スマートカードのマルチアプリケーション機能というものを世界中に根付かせたいというのが、考え方でございます。幸いにして、内閣府のタスクフォース担当の方たちからは、積極的な反応を頂いております。現在は素案でありますので、皆様方の御意見も含めて議論をさせていただければと思っています。スマートカードが広がりますと、認証、カードの場合には発行登録システム等様々なものが実用化されてきます。

次はカードの形状にこだわるのではなく、機能と安全性にこだわったセキュアチップの戦略を進めたいと思います。インターネットに接続される全ての電子機器にチップを埋め込むという考えです。

そして新たな認証ビジネスを作ることで、IT社会は世界に広がると思います。ここに「e-ethics(情報倫理)：自由と安全」と書いてあります。情報倫

理、自由と安全を目標とした考え方、倫理観及び技術、制度及び技術という様々な組み合わせがあるとと思いますが、これらを日本から作り上げていく必要があるのではないかと思うわけです。

住民基本台帳カード(住基カード)について説明を致したいと思います。私自身、住基カードの基本的な機能設計に関与しました。マルチアプリケーションが搭載可能な住基カードは、ここにありますようにCPU付きのものであるということです。単なるメモリーカードではございません。従って、誤解を避けるためにこれからはスマートカードと呼びたいと思っております。スマートカードの上に、住民基本台帳アプリケーション(住基アプリ)と呼ばれる機能を搭載すると、これが住基カードと言うわけです。

住基アプリを搭載したスマートカードには、一般ユーザーから見た時のものとしては、既に配布されております11ケタのコードのみが書き込まれます。この11ケタのコードを守るために、3つの鍵と錠のペアが入ります。その一つは、住民の方が直接キーインするパスワードです。安全性の面からはアルファベット・特殊記号を入れて8文字以上にしようと言われていますが、長くなれば記憶するのは無理ですね。4桁か、あるいは8桁でも語呂合わせで覚えることが可能かとも思いますが、パスワードは本人が覚えられる範囲に入れていただくということになります。

パスワードというとカード全体のパスワードだと思っている方がいますが、この場合は住基アプリ用のパスワードになります。他のアプリケーションにつきましても同じように異なるパスワードを設定することが可能ですし、鍵も別に設定することができます。

住民基本台帳は、ご案内の通り、自治体の窓口に行きますと、窓口側の端末とカードの間で情報のやり取りがなされます。この時に端末側には認証の鍵・認証用の錠というセットを持っています。カード側には、認証用の錠Aで鍵Aがこちらを開け、カードの中の認証鍵Bが認証用の錠Bを開けます。これ本当は正確ではなくて、共通鍵のように見えますが、具体的には電子署名と同じ非対称鍵暗号方式、それも通常使われている署名のレベルのものが2組使われています。従って、スマートカードの種類によっては処理に少し時間がかかるかなということが起きるかもしれません。でも家のドアに3つ鍵をかければ、開閉に時間がかかりますよね。この場合にはそんな仕掛けになっています。こういった各種の鍵がアプリケーションの目的に応じて格納されます。各種アプリケーションとしては、条例事項であります。IT装備研究事業で検討されました延100以上のアプリケーション利用が可能になる方向で現在検討されています。年内には、地方条例をこういう風に作ってくださいという難型を総務省自ら発行することにな

っています。繰り返しですが、アプリケーション毎に鍵が違うということを知っておいて頂きたいと思えます。これだけの機能を持ったカードはそんなにいくつもありません。

更に電子署名本人の署名もオンライン申請申告に必要です。そのため、現在公的個人認証サービスと言われるものが、新しい法律として、国会に提出されています。平成14年秋の国会で成立すれば、我々住民全員が希望すると、自治体から電子署名のサービスを受けることが可能になります。予定では平成15年からでございます。この署名の秘密鍵及び公開鍵証明書こういったものが、この他のアプリのところに入ってまいります。既に住民基本台帳と電子署名だけで、マルチアプリケーションになっています。当然パスワードも、違うものが入られるようになっております。

この公的個人認証サービスは個人としての自然人としての人の存在、氏名、住所等を証明するものです。それをベースにその人が持っている、法定資格ライセンスの認証も、このサービス上に載る予定です。例えば、法定資格については医師・薬剤師の方、行政書士、税理士の方、まだ他にいっぱいありますが、いわゆる士業の方、法定免許を持っていないとやってはいけない業がいっぱいございます。消防等においても、有資格者の人が直接報告しなければならないものがございます。

こういったものについての資格認証の「しかけ」として、この二つが組み合わされます。すなわち、住民の方が住基カードをはじめとする機能及び安全性で十分認められているものをお持ちいただきますと、窓口申請し秘密鍵が入ってまいります。もう一方の公開鍵は都道府県レベルに提供されてここから電子署名の公開鍵証明書が知事の署名のもとで電

子データとして送られてきます、あるいは手渡されます。この証明書はカードの中にしまうことも可能です。ある人が窓口に行って秘密鍵をもらうと同時に、公開鍵の証明書が発行されて、LG-WAN経由だと思えますがすぐに公開鍵がカードに入るのではないかと思います。

この証明書を持っている方はこれで電子署名ができるわけですが、資格認証の方は、属性証明機関ないしは資格証明機関、例えば医師のような場合には厚生労働省の管轄です。厚生労働省が責任をもって自ら資格認証属性証明機関を作るか、何処かに委ねるか、更にはアウトソースするというようになります。そこに対して、電子的に申請を致します。これもインターネット経由で構いません。もらった方は、住民の方の氏名・住所が公開鍵証明書によって書かれ、本人の意志であることが電子署名によって確認され、その結果、属性証明書送付機関は自らのデータベースと照合し、申請者が有資格者であれば、無事、資格あるいは属性証明書を、電子的に発行することになります。ここにもやはり属性証明機関の長ないしは医師の場合だと、厚生労働大臣の署名で発行されるはず。この辺は色々な考え方、やり方がありますが、電子的な証明書が出てくる。その結果、この方は必要に応じて、本人の自然人としての署名と有資格者としての署名、その場合には、秘密鍵で署名をし、公開鍵証明書で本人を署名し、この証明書とのリンクによって資格を証明するという形でやり取りができるようになるでしょう。もちろん属性証明機関から、ペアの鍵をもう1個発行する方法もありえます。この辺は費用対効果によって決まってくると思います。

スマートカードのインフラ化の目的は、ビジネス環境を向上させることです。新規ビジネスを創出し、利便性を向上していくためにも、スマートカードは専用システムにしません。次世代のスマートカードの機能としてはまず、マルチアプリケーションになっています。安全性についてはファイアーウォール等様々な方式でその安全性が確保され、更にはその機能は第三者によって確認をされるということです。民間利用のカードは必ずしもそうではないものもあるかと思いますが、公的分野で行政連携及び住民基本台帳で使うものについては一定のレベルをクリアした、認定されたカードでないと利用できないということになります。更に非対称鍵暗号方式を持っていること、非接触インターフェースを有する事ということになります。もちろん国際標準準拠でなければな



りません。

スマートカードを用いたアプリケーションの運用の仕方は、ニックスフレームワークと呼ばれるものです。世界最先端の技術云々と書いてありますが、必要なことはサービスの追加・削除、ソフトウェアのダウンロード・削除等がPKIを用いてやられていること、更にそれによってオンイン・オフライン問わず、オンサイトでできるようなっていることです。

そして、そのPKIを使った相互認証はチップとチップの間でもできるように作られているということです。ドライブのソフトウェアは正しい手順にしなければ、相互認証できませんので、フェイルセーフ(fail-safe)からみれば、チップでも構わないということになるわけです。

繰り返しになりますが、住基カードを手にした利用者が、新たに自治体が許可したサービスを利用したいと思えば、サービス提供者の窓口でメンバーシップが確認された後に、このカードを利用してサービスを受けることができるということです。今までは、サービス提供の目的毎に、新しいカードが発行されていました。カードにアプリケーションを追加できる、管理用の鍵が階層化して作られているというのが大事なポイントであります。

おわかりの通り、サービスを追加するのは、このサービス利用者とサービス提供者の了解によるものです。住民の側からみれば便利なカードになりますし、それからカード発行している自治体にとっては、住民の満足だけでなく、サービス提供者がカードの利用を選んでくれば、カードの場所貸し代としての費用の回収が可能になっていきます。こういった仕組みは、自治体によって考え方が異なりますが、仕掛けとしてはこうなっています。サービス提供者の方たちは、自らカードを発行する手間もなく、更にはそのカードの費用を安い値段で相乗りさせてもらえる、安全性及び機能の高いカードが使えるというわけです。

次に電子機器との接続を説明しましょう。ご案内の通り情報家電と言う考え方が推進されています。情報家電には冷蔵庫や洗濯機等の、白物家電もあれば、様々なものがございます。更には住宅や自動車のようなものも、それぞれがホームオートメーションの一部として、それぞれがインターネットに接続されていくだろうと思われれます。その時に、外出先からもアクセスできるのは、便利な利用方法であります。更に新しいソフトウェアのダウンロードによって、利用している製品の機能アップもできるようになります。万が一、製品に不具合が出たときには、ソフトウェアの入れ替えを商品の回収なしでできるというメンテナンス機能が可能です。それがリモートメンテ、あるいはリモートサービスという言い方になります。こういった効果が期待できますが、

インターネット接続ということは、ウィルスを流しこまれるかもしれない、あるいは他の人がリモートサービスシステムに入り込み、予期せぬいたずらをするかも知れません。このことに関しては、やはり安全確実な方策を検討したいと思います。

これが先程から言っている、安全性の確保のところでは、そのためには利用者と情報機器との相互認証が必要です。必ず対等な立場でお互いに正当な接続相手であることを確認するというのが基本になります。この相互認証のためには、先程の住基カードとCS(コミュニケーションサーバ)の間でやった、相互認証と同じ仕掛けが使えます。重要なことは鍵の配送です。すなわち、白物(情報)家電は、自分で買って購入してはじめて本人のコントロール下におかれます。ですから鍵はプレインストールできないというのがわかります。もちろん量販店で自由に購入できるように、標準的な機器の認証方式にしていきたいと思います。機器の認証とは、その機器が間違いなく自分が希望しているものかどうか、これを確実にすることです。

こういった要求がどの程度の頻度で起きるのか、登録し鍵を1回配送すればまたしばらく使えるようになるのか、まだまだ検討の余地はありますが、少なくとも鍵配送、登録、鍵の配送のための登録認証局が必要になってきます。

この仕掛けが次世代のセキュアチップと管理システムによって実現されます。この同じ仕掛けが、間もなく日本において、公的な分野における住基カードとして出てくるわけです。だからこそ、その技術を民間にも開放し、更に使いやすい世界を作ろうというのが今の構想であります。

今、機器の認証方法をご説明しました。デジタルの世界では当然のことではありますが、機器を認証するにも特定のための機器のID番号、その機器の正当性を確認するための暗号鍵という、どちらもデジタルデータが必要になります。これは、情報家電等の物理的な物についている必要は特になくて、デジタル情報そのものに対しても、同じやりかたが可能になってまいります。暗号化に対するレベルとか別の手段も必要になりますが、論理的なあるいは体系だった利用方法としては、機器でもデジタルデータでは同じ「かたち」になります。

そこで知財の中でも重要な課題になっている著作物の流通について考えてみたいと思います。

現在日本の権利関係では著作権法は法的にほぼ完備していて、これ以上手が打てないと言われております。東南アジア等諸外国ではまだこの著作物に対する権利を認めていない国もございますので、特許についても同じですが、この辺は十分な配慮をしなければなりません。そうは言っても内政干渉するわ

けにいきませんし、国際ルールのもとで彼らも知財に対する十分な保護をしていただきたいということかと思えます。

一方デジタル情報はご存知の通り、コピーしても劣化しないという最大の特徴をもっています。この特徴を維持して何等かの形で安心して、利用者・権利者の双方が満足した形でなんとか、この情報の流通を図りたいと思います。

幸いにして、人の認証はできるようになります。更にその人の、オンラインによる、あるいは意思を明確にするための電子署名も間もなく整備されます。そうなると、このデジタルデータの購入という本質は、一種のデジタルデータの属性情報になります。物を買ったという属性情報で表されるということですから。法定資格ほどではありませんが、属性のやり方もわかっています。

従って、登録認証局が設置されれば、知財著作物であるコンテンツ等に対しては権利者に対して、利用者が費用を払うことで利用の許諾を受けた、その許諾が正当に受けている人かどうかを電子空間で保証・確認することによって、可能性が出るようになります。コピーされたときに、それが不当なやりかた、不正行為であれば法的な対応が可能です。もちろん例えば「電子すかし」という技術を使う話もありますし、そういった防御方法も考えておく必要もあります。機器・メディアに対してコピー防止機能をかける方法もあります。デジタル署名によって、コピー防止機能もダイナミックなコントロール下での対応が可能になる場合が予測されます。これは便利な方式です。普段は、コピーもなんでも自由ですが、ある契約のもとにおいては、コピーができなくなっている。その安全性を両者、すなわち権利者及び利用者の両方が信用する第三者によって守られる。これが認証ビジネスになると予測している理由です。

このようにセキュアチップを使えば、ニックスフレームを拡張することで、家電製品やコンテンツ等の利用・流通に対応できそうだとこの見えてまいります。この図は、電子機器にセキュアなチップが入っていて、製造者は出荷時にリモートサービス、リモートメンテのための鍵を入れ込むということになります。

機器を購入するときには、利用者が登録認証センターに対して私がこの機器を買いましたと登録することで相手確認がされ、その該当機器に必要な情報が書き込まれます。その時に、製造者キーと機能をコントロールするための鍵、あるいは保証するための鍵、更には所有者である人を特定するための鍵、ここにはスペースの関係で書いていませんが、利用者の鍵、こういったものが組み込まれます。

これもマルチアプリケーションであることは、すぐに見てわかります。そして、最後に本人にアクセ

スキーが渡ります。これで、ひとたびセットされるとインターネット経由で、機器と本人との直接の相互認証によって、コミュニケーションが開始されるというものです。

更にコンテンツを買う場合には単に購入という行為は使用許諾の登録だけになります。言い方を変えますとこの方式では音楽や映像などのための円盤(媒体)は不要であるということです。ただ、そうは言ってもすぐ全部がこの方式になるとは思いません。CDやDVDの(コンテンツ)販売店の良さというのはまた別にありますから、そこはすみ分けだろうと思います。

購入登録がされると、購入者は利用する際の本人登録を申し込みます。そうすると、この人が誰か、それからその人の許諾を確認した上でセンターに配信要求をします。多分、この登録認証センターは今この認証業務と同じくらい、あるいはそれ以上の社会的な信用を得る必要があるかもしれません。この辺は今後の議論になると思います。

コンテンツデータセンターは指定されたところに対してデータを提供します。この時にアクセス、すなわちこの機器の機能は登録認証センターのランチと様々な形でダイナミックにコントロールされることが予測されます。音楽の場合はリモートで聞く人はいないと思いますが、コンテンツの再生はこのキーによって、ボタンを押すと音が出てくる、こういったやり方があるだろうと思うわけです。

以上のことをまとめますと、インターネット経由でのアクセスコントロールには機器及び両者の相互認証が有効となります。相互認証用には、認証鍵の配送が必須であって、スケーラビリティを考えれば、当然PKIの利用となります。相互認証を確実に行うには、機器と利用者の登録が必要です。利用者というときの基本は自然人としては、公的個人認証サービスを使う方法もありますし、民間の認証局も考えられます。

ただ、絶対に必要なのは、人・もの・コンテンツ全てが登録されていなければ特定はできないということです。更に、登録削除、鍵の配信などを行う登録局が必要で、この技術はまさにIT装備をはじめとして、経済産業省の支援によって作られてきた技術です。それが間もなく住民基本台帳カード、それから行政連携カードとして、世の中に広がっていく可能性を持つスマートカードの中にあるセキュアチップとその管理運用システムによって実現されそうだとこのことです。

ここは最初に申し上げましたように、日本がアドバンテージを取っている部分です。まさに自由と安全を守られる電子空間が作られるということからも、我が国にとって非常に重要な戦略の位置づけができるのではないかと思います。そのためにも、認証

ビジネスを新しい形で展開していこうと思います。かつてアメリカにおいて日本車や日本の半導体が得た評判のように、「最高の品質のものは、日本製である」というのがございました。車は安全・安心だから使える。砂漠の中を一人で走っていて、壊れたら殆ど死と直面します。そのような時に、故障の多いアメリカ車には乗りたくなかったという気持ちはよくわかります。同じことで、今後インターネットに接続される電子機器は、ニックスフレームワークとは言いませんが、セキュアチップが入っていることで安全性が確保され、認証局によって我々の安全や

権利が保障されるというのを作り上げていったらどうでしょうか。きっと今よりも楽しい世界が、あと5年くらいの間には花を開きはじめると思うわけです。

以上で私が申し上げる、生活を変える、そのきっかけとしてのスマートカードの現状、それから将来への一つの流れをご説明させていただきました。今後益々この分野が発展するのを私も祈念するものがございます。

ご静聴ありがとうございました。

(文責：IT装備都市研究事業推進室)