# シリーズ

**シリーズ「電子政府を支える情報通信基盤技術」第８回**

# ユビキタスカード

㈱日立製作所MMCソリューションセンター長　村松　晃

## １　はじめに

ユビキタスという言葉がコンピュータの世界で初めて使われたのは、1988年、Xerox PARCにおける「Ubiquitous　Computing」の研究においてである。かれらはユビキタス、すなわち物理世界のいたるところでコンピュータが利用される未来世界について考察し実験したが、その最大の特徴は利用者がそれを意識しないで済むようにするコンセプトにある。これを実現するために、チップや端末（ポストイットのようなTab、ノートサイズのPad、黒板のようなBoard）などのハードウェアからネットワーク、ユーザインタフェース、アプリケーション、プライバシー、キャッシュ方式などあらゆる側面を研究対象にした（http://www.ubiq.com/weiser/researchreports.htm）。

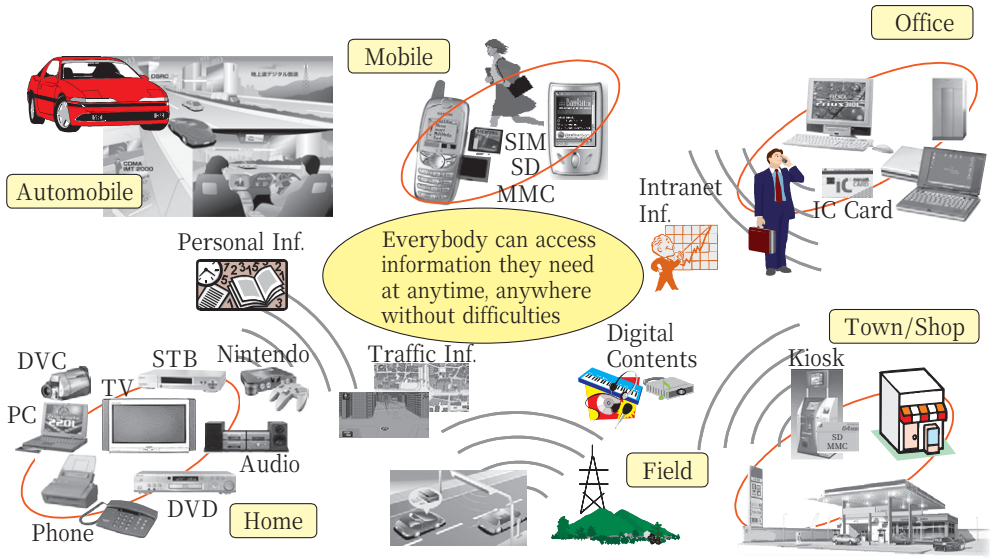
近年、この言葉は研究の世界でなく実業の世界で使われるようになってきた。最大の理由はワイヤレスネットワークと端末の進歩である。ｉモードに代表される携帯電話網を経由したインターネット接続サービスの成功に続き、３Ｇ携帯電話の登場で静止時で２Mbps、移動時でも384kbpsの広帯域が利用できるようになってきた。さらに高速な接続環境を求めるユーザーのためには屋外無線LAN環境が導入されつつある。またバッテリーの進歩により携帯電話も200時間を超える待ち受け時間が当たり前となり、さらにビジネスユーザーの要求を満たす軽量かつ高機能なPDAが普及し始めている。この驚異的な技術革新は生活のあらゆる分野に拡大し、いつでもどこでも誰でもコンピュータを意識せずに情報にアクセスできるようになると予想されている。

これはネットワークコンピューティングのパラダイムにおける第三の波である。第一の波は言うまでもなくメインフレームコンピュータとオンラインネットワークである。この波は1980年代に終焉に向かい、代わってクライアント・サーバーシステムとLAN、インターネットという現在われわれがその中で生活しているパラダイム―Webコンピューティング―に移行していく。これを第二の波とすれば、第三の波はすべてがIPネットワーク化（IPコンバージェンス）していく先に存在するユビキタスコンピューティングである。

## ２　ユビキタス情報社会とユビキタスカード

ユビキタスコンピューティングのパラダイムが支配する世界、すなわちユビキタス情報社会では、人々はコンピュータをコンピュータと意識することなく、オフィスや家庭といったホームポジションから離れた場所、例えば、自動車の中や公共施設、商店、街路等でも利用して情報をアクセスする。端末もPCや携帯電話だけでなくPDA、ITS連携車載情報端末、キオスク端末、自販機、ゲーム機、セットトップボックスなど、多種多様にわ

**図１　ユビキタス情報社会**




たる。したがって、どんな場所からでもネットワークに正しく接続してサービスを受けることができなくてはならない（図１）。そのために必要となるのがユビキタスカードである。

## ３　ユビキタスカード

ネットワークに接続して情報にアクセスする場合、通常何らかの認証が行われる。ダイアルアップの場合はISP（インターネットサービスプロバイダー）が契約者に付与しているIDとパスワードで認証される。また、構外から企業のイントラネットにリモートアクセスするためには、上記ISPによる認証とは別にRADIUSサーバー（リモートアクセスサーバー）によるID・パスワード認証が必要である。

一般にID・パスワード認証は低セキュリティであると言われているが、それは運用面において特に顕著である。パスワードに短い数字列や誕生日、恋人の名前などを用いることの危険性はつとに指摘されているが、改善されていない。なぜなら人はID・パスワードを記憶しなければならないからである。長い数字列や記憶しにくい文字列を採用する場合ふつう手帳などに記録するが、これを紛失したら一大事である。中にはポストイットに書いて机上のディスプレイに貼っておく人すらいて、これでは事実上ノーセキュリティである。また、ID・パスワード認証はキーボード入力が要求されることもユビキタスというコンセプトにそぐわない。これを解決すると期待されているのがユビキタスカードである。

ユビキタスカードは利用者本人の認証情報を格納した耐タンパー性のあるデバイスである。情報をアクセスするための端末にこれを挿入し、本人でなくては入力できない情報を入力してユビキタスカード内で本人認証（User　Verification）を行い、その結果をネットワークに送出して端末認証（Authentication）を行う。一般論としては、端末が信用できるものであれば端末における本人認証で十分であるが、２で述べたような多種多様な端末からネットワークに接続することを想定するとその仮定は成り立たない。そこで信用できない端末と信用できるカードとの組み合わせが求められることになる。本人認証のための情報としてもっとも簡便かつ間違いの少ないものは指紋など

の生体情報であることから、理想的なユビキタスカードは生体情報認証機能を持ったものとなるであろう。しかし本稿においてはこのような技術的側面でなくビジネス的側面について議論することとしたい。すなわち、現実問題としてどのようなカードが社会に受け入れられていくか、を以下では考察していきたい。

まず、ユビキタスカードの概要についてまとめると、これは本人認証と端末認証のための耐タンパーデバイス（ハッキングに抵抗する性質のあるデバイス）であることから、ICカード用チップが使用されるものと考えられる。また、いつでもどこでも利用できなくてはならぬことから、常に身に付けておける形状でなくてはならないし、対応する端末も自身が携帯できるものでなくてはならないであろう。英国の大学教授が自身の身体にチップを埋め込んで常にネットワークに接続できるようにしたという報道が先日なされたが、これは極端としても、携帯電話や腕時計などのモバイル用具と組み合わせて使えるものであることは当然であろう。このように見てくると、現時点では次の３点がユビキタスカードの候補であると思われる。

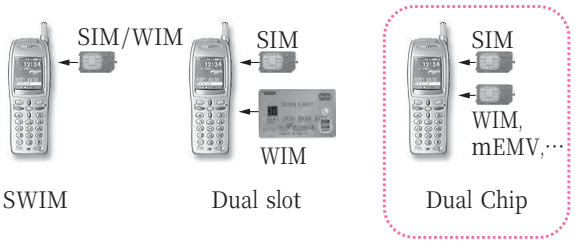
１）ICカード（ID１と呼ばれるフルサイズのもの）
２）SIMカード（ID０と呼ばれるGSM携帯電話用のもの）
３）セキュアメモリカード

ICカードはクレジットカード、銀行カード、住基（住民基本台帳）カードなどとして今後日本社会の情報インフラを形成するカードである。また、すでに一部の企業では社員証などに応用されている他、JR東のSuicaカードのような交通系カードとしても導入が始まっている。身分証、金融カード、交通カードとして誰もがパスケースや財布の中に入れて持ち運ぶICカードは、たしかにユビキタスカードの有力な候補である。しかし、いくつかの疑問点も存在する。第一は、いくらインフラが整備されても、ICカード端末が世の中に満ち溢れるわけではないから、いつでもどこからでもアクセスできるためには前記したように携帯電話などと組み合わせて使えなくてはならない。しかしICカードはその条件を満たす大きさではない。また、本人認証情報とともに持ち運ぶであろう様々な個人情報を格納するには、数十キロバイトというメモリ容量はあまに小さい。

SIMカードについては日本ではあまりよく知られていないが、実は発行されたすべてのICカード中最大の枚数はこの形態が占めている。その理由は欧州やアジアで利用されているGSM携帯電話が採用しているからで、今後次世代携帯電話に移行していくと日本でも普及していくと見られている。この大きさは携帯電話や腕時計など小型の端末と相性がよく、メモリ容量が小さいという問題はあるが、ユビキタスカードの候補として最有力である。しかしながら、SIMカードには一つビジネス面で大きな課題がある。それはカードの発行者が携帯電話サービス事業者（MNO：Mobile Network　Operator）に限定されるという点である。利用者の認証をMNOに依存しなくてはならないことには、欧州の金融機関などから異論の声が上がっている。このため、欧州の携帯電話ベンダーのノキアは、ビザインターナショナル、ノルデア銀行と組んで二枚のSIMカードを利用する携帯電話を開発した。彼らによれば、モバイルコマース用携帯電話には①すべてをSIMカードで行うSWIM方式、②ID１のICカードを挿入できるデュアルスロット方式、③二つのSIMカード用スロットを持つデュアルチップ方式の三種類があり、金融機関など独自に利用者認証を行いたいと考えるサービスプロバイダーにも受け入れられるもっともエレガントなソリューションはデュアルチッ

プ方式である（図２）。

**図２　モバイルコマース用携帯電話の方式**

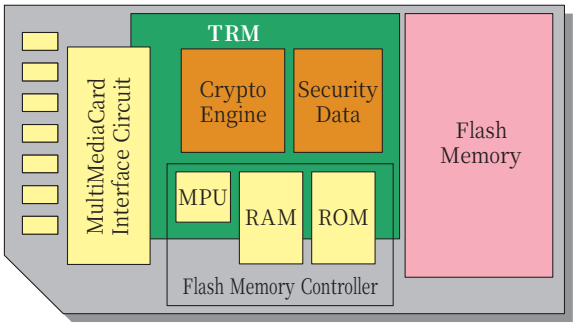



## ４　日本におけるユビキタスカードの展開とセキュアメモリカード

しかしながら、日本においてはすべての携帯電話端末はMNOブランドであり、かれらが端末ビジネスを支配しているために、デュアルチップ方式あるいはデュアルスロット方式の端末が登場する可能性は小さいと言わねばならない。なぜなら、このような端末は携帯電話を単なる土管（conduit）として利用するものであり、MNOに付加価値をもたらさないからである。そこで注目されるのがセキュアメモリカードである。

携帯電話が単なる通話装置からパーソナル情報端末に変貌していくにつれ、端末で保持されるデータは着メロ、壁紙、Javaアプレットなど有償無償を含め増大の一途である。とくにＪフォンの写メールにはじまって、KDDI、NTTドコモと日本の主要なMNOはデジカメ付携帯電話を市場に投入した。このため端末に搭載される高価なフラッシュメモリの容量も増大し、端末コストの上昇を招いている。日本においては携帯電話端末は販売奨励金を付加して仕入れ値より安く売られるので、このコスト上昇分をそのままストレートに実売価格に転嫁することができない。そのため、メモリ増大のコストを契約者に負担させるべく、メモリカードのスロットを付した端末が登場した。この動きはまだ初期段階にあるが、おそらく2003年モデルからは多数のメモリカードスロット付携帯電話が市販されるようになると思われる。

**図３　SecureMultiMediaCardの実現例（日立製作所）**




一方、メモリカードにセキュリティ機構を搭載する動きが始まっている。マルチメディアカードの普及団体であるMMCA（MultiMediaCard Association）を例に取ると、2001年６月にｅコマース用SecureMultiMediaCardの仕様が、2001年12月にコンテンツ保護用SecureMultiMediaCardの仕様が発表されている（http://www.mmca.org/、図３）。前者は従来ICカードに実装されてきたWIM（WAP Identity Module）をマルチメディアカードに実装するもので、これはハードウェア的にはメモリカードにICカードチップを導入することと同義といってよい。日本はデジカメの発達に伴ってメモリカードでは世界の先端をいっており、メモリスティック、SDメモリカード、マルチメディアカードなどが大量に流通しているが、ここに上記のようなセキュリティが入ってくると、携帯電話がオープンなVPN（Virtual Private Network）端末と化することが予想される。

## ５　ユビキタスカードの応用

先に述べたように、本人認証と端末認証のための耐タンパーデバイスであるユビキタスカードは、その中に認証のためのキーや証明書が格納されるが、メモリカードベースのユビキタスカードでは数メガバイトから数百メガバイトもの不揮発性メ

モリが別途格納用に利用できる。人がつねに持ち運ぶものといえば財布や定期入れ、時計、手帳などが思い浮かぶが、これらの中には鍵や印鑑のほか種々の個人情報やセキュリティデータ、生活記録などが含まれている。住所や生年月日は言うに及ばず、名刺、家族の写真、クレジットカードやポイントカード、領収書、クレジット使用履歴、預金通帳、ポートフォリオなど、種々雑多ではあるが常に持ち運び大切に管理されるこれらのデータが、恐らくユビキタスカードに安全な形態で格納されることになるであろう。また、業務用途では、業務固有の基本データをこのカードに入れて持ち運ぶことが可能である。SecureMultiMediaCardでは、フラッシュメモリ領域にこれらセキュリティが必要なデータを暗号化して格納し、PIN（暗証番号）認証の後、カード内の鍵で復号化される。仮に落としても、暗証番号がなければ読み出すことができない。

また、メモリカードはすでにPC、PDA、デジカメ、プリンタなどの様々な情報機器で利用されているが、今後携帯電話、自動車、セットトップボックス、キオスク端末などにも展開されていく。したがって、これら機器間でデータを安全に移動させるブリッジ機能も重要な用途になるであろう。このように、認証、秘密通信、暗号化コンテンツ管理、セキュア・ブリッジングなどの特性を活かして、いまコンシューマ用途向け、業務用途向けにユビキタスカードの様々な応用が開発されつつある（図４）。

## ６　おわりに

誰もがいつでもどこでも手軽にネットワークに接続してサービスを受けることができるユビキタス時代の必須デバイス「ユビキタスカード」について考察し、日本市場においてはMNOが発行するSIMカードとならんでセキュア・メモリカードがユビキタスカードの有力候補であることを述べた。セキュア・メモリカードはWIM認証機能を備え、VPNを構築するための基本機能を具備しているとともに、大容量メモリを活用して様々な個人情報や業務情報を安全に格納し、携帯し、ブリッジングすることができる。2003年以降、徐々にこのようなユビキタスカードの導入が始まるであろう。

**図４　ユビキタスカードの応用イメージ**