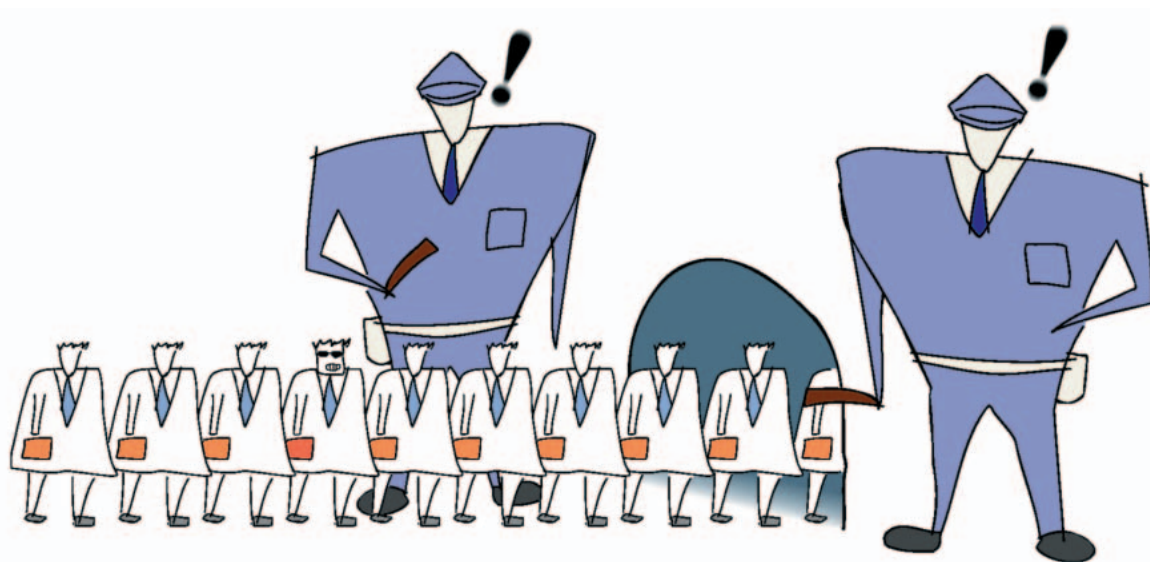


基礎技術 エレクトロニックコマースの

【第1回】 情報セキュリティの 最新業界動向

インターネット上でエレクトロニックコマースを行おうとする際の最大の問題点は電子決済におけるセキュリティだと言われて久しい。また、セキュリティ技術の仕様でもいくつかの規格が発表され、主導権争いが繰り広げられてきた。しかし、ここにきて業界の内部では統一規格策定に向けて活発な動きが見られるようになってきた。次第にその具体的な姿が見えてきた電子決済について、今回は最新の業界動向をレポートしてみたい。なお、次号ではその中心的な役割を果たすと思われるSET (Secure Electronic Transaction) について解説する予定である。

株式会社ビー・ユー・ジー
情報セキュリティプロジェクト代表
浅田 一憲





1 最新ニュースより

今年に入り、情報セキュリティー技術の分野でいくつかの新しい動きが現れてきた。まず、その中から注目すべき事件について見ていくことにしよう。

その1：RSADSI、Security Dynamics社に買収される

にわかには信じられないくらい重大なニュースが飛び込んできた。1996年4月15日、公開鍵暗号とRSA暗号方式をはじめとして数々のセキュリティー技術特許のライセンス権を持ち、BSAFEやTIPEMといったツールキットを通じてメジャーなセキュリティー機能入りの商用ソフトウェアのほとんどにライセンス供与を行っている世界でもトップクラスの情報セキュリティー技術専門会社RSA Data Security, Inc. (RSADSI) が買収された(図1)。買収したのは、Security Dynamics Technologies, Inc. という会社で、アメリカのマサチューセッツ州ケンブリッジにあるセキュリティー機器の専門会社だ(図2)。

Security Dynamicsは、「SecurID」という可変暗証アクセスコントロールシステムで有名な会社である。「SecurID」の製品はファイアウォール用ソフトウェアとハードウェアのセットで、各ユーザーに配布するクレジットカードサイズの液晶表示機能付きカード上に刻々と表示される数字列と、ユーザーのPIN (Personal ID Number) の双方を入力した場合にだけ特定のネットワークにアクセスできるという仕組みになっている。この「SecurID」が大ベストセラーになったことで、Security DynamicsはNASDAQ (アメリカの店頭市場) に上場し、株式を公開後たちまち株価が暴騰して多くの資金を集めることができた。

今回、RSADSIはSecurity Dynamicsと株式の交換を行い、最終的にはSecurity Dynamicsの傘下に入る形となった。RSADSIのJim Bidzos社長は、株式会社ビー・ユー・ジーの質問に対して、「今回の買収に関しては、すべてが良いことばかりで悪いことは何もない。Securi-

ty DynamicsはもともとVeriSignの株主でもあり、非常に懇意にしている会社である。RSADSIとSecurity Dynamicsは業務が競合しておらず、一体となることで互いのビジネスの範囲を大きく広げることができる。買収を発表してから1週間でSecurity Dynamicsの株価は2倍近く高騰した。これも市場が我々の行動を評価している証拠である」

と上機嫌で答え、大変満足気だった。買収後もRSADSIは独立した会社として業務を行い、今までのRSADSIの方針は何ら変更されることはないということだった。

その2：VeriSignの強力ライバルが出現

VeriSign, Inc.は、1995年にRSADSIによって設立された会社である。電子印鑑は情報セキュリティー技術の中で最も重要な技術の1つであるが、VeriSign社はそれを使用する電子印鑑証明書発行システムの販売と発行サービスを行う会社である。

図1：2億ドルで買収されたことを伝えるRSADSIのホームページ



• April 22, 1996: An [open letter](#) from the CEOs of Security Dynamics and RSA Data Security.

• April 15, 1996: [Security Dynamics acquires RSA Data Security for \\$200 Million](#).

• Microsoft, Lotus, Banyan, Connectsoft, and many other vendors have endorsed S/MIME, RSA's new intervendor specification for secure interoperable e-mail! Download the S/MIME logo.

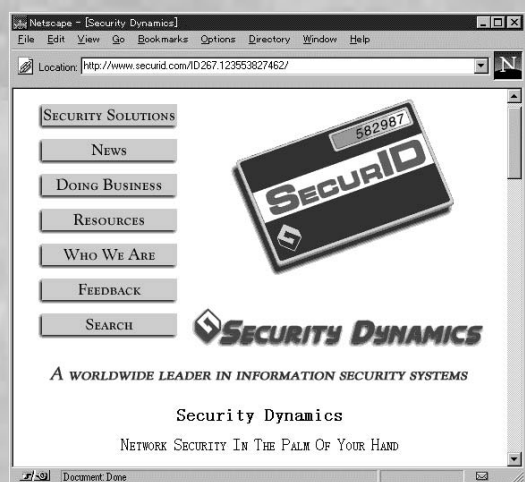


図2：Security Dynamics社のホームページを飾る同社のベストセラー商品「SecurID」

RSA直系の会社ということもあり大変に注目されてきた会社であるが、1996年になって、突如VeriSignの強力なライバルが出現してきた。AT&T、GTE、NOTEL、MCIなどの会社が同じく電子印鑑証明書関連ビジネスに参入することを発表したのである。

中でも一番の注目株はGTEである(図3)。GTEは世界第4位の電話会社であるが、内部に政府システム部(Government System Division)という部門があり、そこで15年も前からアメリカの政府(National Security Agency)で使用するCA*(Certification Authority)システムを開発して提供していた。GTEはカナダ政府にも同様のシステムを提供しており、すでに200万通を超える電子印鑑証明書を発行してきた実績がある。そこで培ってきたCAの技術を商用利用できることになり、1996年1月のRSAコンファレンスで初めて発表を行った。それ以前は、アメリカ政府との秘密保持契約のために、CAシステムを開発していることはいっさい公にしていなかった。彼らのシステムの総称はCyberTrustという。さすがにアメリカ政府で使用されているだけあって高機能で高信頼のシステムである。早

くもMasterCard Internationalがオーストラリアのキャンベラで行っている電子小切手実験に採用されて稼働しているほか、SET(インターネット上でカード決済を安全に行うためのプロトコル)のシステムでも採用される見通しである。

クレジットカード会社では、VISA InternationalがVeriSignに出資しており、SETにはVeriSignのシステムを採用すると思われる。これにより、クレジットカード関連のCAサービスでは、VISA-VeriSign組とMaster-GTE組の2陣営ができるかもしれない。GTEは、彼らのCA技術を金融関係ではクレジットカード決済、電子小切手や電子現金の発行、ホームバンキングなどに利用するほか、一般向けにはNetscapeやMicrosoft、Oracleなどのインターネット用サーバーやナビゲーター用の証明書の発行サービスに使用していく意向のようだ。すでに、EMV(ICカードの標準規格:後述)仕様の電子小切手用CAも完成して稼働しているという素早さで、多くのクレジットカード会社や銀行などがGTEのCyberTrustを採用する可能性が高くなっている。また、NSA以外の政府機関もCyberTrust

*CA: 電子的な印鑑証明の発行機関。場所や使用目的に応じて複数設置され、それらが階層構造を形成する

の採用を検討している。

一方、Netscape社は、4月にNetscape Certificate Serverというサーバーを発表した。このサーバーは名前のとおり、会社内などのインターネットで小規模に使用する電子印鑑証明書の発行(CA構築)機能を持っているサーバーである。これに続いて、6月に発売すると噂されているNetscape Navigator3.0では、サーバーのみならずユーザー側でも電子印鑑や電子印鑑証明書を使用できるようにする。このサーバーは特別なハードウェアを使用せずすべてソフトウェアで証明書の発行を行うので、VeriSignやGTEなどの専門業者に委託発行してもらう場合に比べて、セキュリティが弱い、公共性がない、発行に時間がかかるなどの欠点はあるが、手軽で安価に証明書を発行できるので小規模な会社の社員証などに向いており、大変画期的な商品であるといえる。

また、Microsoftも独自にCA用ソフトウェアを開発していると噂されており、クレジットカード会社ではAmerican Express Travel Related Services Company, Inc.(AMEX)との提携も行った。

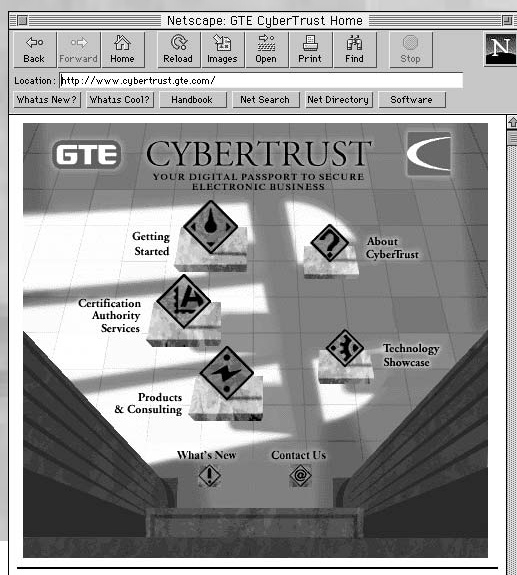


図3: CyberTrustを開発したGTEのホームページ



RSADSIは、これらのVeriSignのライバル会社に対しても差別することなくセキュリティ技術のライセンスを与える方針であり、CA業界は一気に戦国時代に入るかもしれない。

まさかと思ったRSADSIの買収劇と、独占の道を走っているかのように思われたVeriSign社にも多くの手強いライバルが出現したことは、これから情報セキュリティ技術が爆発的に普及することの前触れであると思われる。特に突如彗星の如く登場したGTEのCyberTrustは業界を再編させる力さえ持っていそうだ。このように多くの企業がこの分野のビジネスに参入してくるということは、ユーザーにとっては多くの選択肢の中から自分の目的に合ったものを選べるようになることを意味し、大変喜ばしいことであると思う。

その3：MicrosoftのコードサインとCryptoAPI

1996年4月、Microsoftは電子コードに著作権者やベンダーがデジタル印鑑を捺印し、使用者がそれを確認できるコードサインと呼ばれる新技术をWindows95やNT上

でサポートすることを発表した(図4)。コードサインの実用化により、ワープロなどの商用ソフトウェアはもちろん、シェアウェア、ニュースクリップや株価情報、音楽、絵画などのあらゆるコンテンツをインターネットからダウンロードする形で購入ができるようにするための下地ができる。

コードサインでは、国際規格であるX.509バージョン3形式の電子印鑑証明書をPKCS#7のフォーマットで使用する。コンテンツ提供者は、コンテンツに会社名、住所やD-U-N-S番号を入れ込み電子印鑑を押して提供する。電子印鑑証明書は、ポリシー別に分かれたCAに発行してもらう(図5)。

現在のところ、VeriSignとGTEがコードサイン用CAの運営に名乗りを上げている。コードサインは、デジタル化されたすべてのコンテンツに使用でき、既存のコンテンツ流通を根底から変えてしまう大きな可能性を持っている重要な技術である。

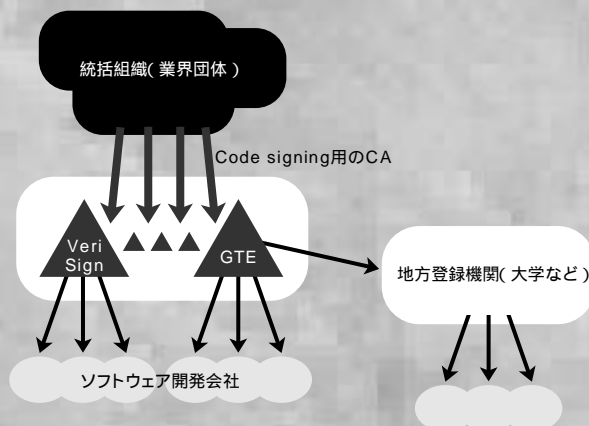
また、Microsoftは1996年2月にCryptoAPIという、Windows95やNTから暗号ライブラリにアクセスするための標準APIを追加することも表明している。Windows上

で動作するアプリケーションがこのCryptoAPIを呼び出すことによって、さまざまな暗号機能を利用することができる。これは、現在のように各アプリケーションがRSADSIから個別にBSAFEやTIPEMのライセンスを受ける必要がなくなるということの意味している。つまり、MicrosoftだけがRSADSIのライセンシーとなり、アプリケーションはCryptoAPIを利用するだけになる、という構造である。このような形になると、Windowsのアプリケーションはアメリカの輸出規制の枠にとらわれなくなり、自由に世界中に輸出できるようになる可能性が高い。コードサインにしてもCryptoAPIにしても、「さすがMicrosoft」と思わせるようなキーポイントを押さえており、今後のMicrosoftの動向が注目される。

図4：コードサインの仕様について解説しているMicrosoft社のホームページ



図5：コードサイン運営のための組織構成



2 電子決済の動き - クレジットカード時代へ

インターネット上での電子決済は、情報セキュリティ技術が使用される一大分野である。インターネットが既存の流通を大きく変えてしまうことは紛れのない事実であるが、そこで行われる決済も既存のものとは変わっていくはずだ。ここでは今後の電子決済の動きを展望してみよう。

インターネットと電子決済

ネットワークの使用方法や使用できる技術が進むにつれて、決済の仕方も進歩してくる。現在は、既存の通信販売と同じように、インターネット上で最も簡単で問題の少ない決済方法は銀行振り込みである。近いうちに、銀行振り込みはインターネットを足回りとして使用できるようになり、家庭のパソコンを使った、文字どおりのホームバンキングが実現するだろう（ちなみに今のホームバンキングは一般の人が簡単に使用するのにはいろいろと面倒だ）。そのときには、インターネットホームバンキングは、インターネット上で行われる売買の決

済に使用されるだけではなく、現実世界での企業や個人の普通の商取引でも多く使用されるようになる。銀行の店舗や銀行員などは今ほどは必要でなくなるかもしれない。振り込み手数料も大きく値下げされるであろうし、キャッシュフローも今より少なくなると思われる。日本ではインターネットホームバンキングの普及には、エレクトロニックコマースに対する銀行の動きが鈍いため、かなり時間がかかる模様で、他の決済方法に先を越されて顧客を多く失うことになるかもしれない。

クレジットカード決済へ

そのホームバンキングよりもっと急速に実用化されつつあるのがクレジットカード決済である。

クレジットカードは、使用者にとって便利になればなるほど不正利用や犯罪の問題が発生してきていた。通信販売などでカード番号を知らせるだけで買い物ができるようになったり、スーパーの食品売場ではサイ

ンレスでカードが使用できたりと、クレジットカードはどんどん便利に使用できるようになった。しかし、一方ではそれだけ不正利用や犯罪の温床を作ってきたことなる。

ネットワークを使用しての電子決済では、「盗み見」、「なりすまし」、「しらばくれ」、「改ざん」の問題がつきまとう。インターネットでクレジットカード決済を行うことは新たな不正や犯罪を招く恐れがある。しかも、デジタルワールドでは、一瞬の間に多くの店で不正が行われる可能性があり、危険度は今までとは比べ物にならないほど高い。

あるお店へのアクセスをすべて監視して通信データ中のカード情報を盗み見し、1か月分1000人のカード番号を使用して10分間に1000件の店で不正な買い物をするとか、WWWサーバーを立ち上げて詐欺目的の店を開き、商品を販売しているふりをしてカード情報だけをせしめ、ある日突然ネット上から消えてしまい、その後の捜索もできないなど、今までに考えられなかったさまざまな問題が出てきそうだ。

3 クレジットカードのICカード化とインターネット決済

クレジットカード犯罪のような問題を情報セキュリティ技術で解決し、今後ますます増えていくインターネット上の決済を自分のところで押さえようと考えているのがクレジットカード会社やソフトウェア会社である。また、クレジットカード会社は、これを契機に実際の加盟店で起きている不正利用の問題も一気に解決しようとしている。

実用段階に入った「EMVカード」

世界最大のクレジットカード会社VISAと2番目のMasterCard、加えてヨーロッパのEuroPayは、既存の磁気ストライプ入りのクレジットカードを5年後くらいをめどにすべてICカード（Smart Card）に変更しようとしており、統一規格を制定した。この規格は、EMV規格（EuroPay、MasterCard、Visaの頭文字をとった）と呼ばれて

おり、規格に準拠したカードはEMVカードと呼ばれる。

現在、EMV規格では、RSA暗号方式を唯一の暗号方式として制定しており、カードやカードリーダーにはRSAの技術が使用される。クレジットカードが磁気カードからEMVカードに変更されることによって、カードの偽造が現在より飛躍的に難しくなる。また、カード中には所持者の電子印鑑証明書が安全に保管されているので、電子



的にカード所有者の本人確認ができる。将来的には、カード単体で電子印鑑の捺印もできるようになり、電子小切手の機能も入るようになる。EMVカードは、不正利用の防止の役割を果たすにとどまらず、クレジットカードを使用する機会を大幅に増加させることになるだろう(図6)。

今年に入ってVISAがアメリカのアトランタでVISA Smart Cash、MasterCardがオーストラリアのキャンベラでMasterCard Cashという電子小切手の実験を開始している。VISAの使用しているICカードはEMV準拠ではないが、MasterCardはEMVを独自に拡張したICカードを使用している。両陣営とも今の実験に続けてニューヨークやイギリスで実験を行い、すべてのクレジットカードをできるだけ速やかにICカードに切り替えていくことにしている。

電子決済の統一規格「SET」

VISAとMicrosoftは、1995年9月27日にSecure Transaction Technology (STT)というクレジットカードを使用した電子決済規格を発表した。2日後の9月29日、

Master CardとNetscape、GTE、IBMらは、Secure Electronic Payment Protocol (SEPP)という規格を発表した。これらは発表の直前まで共同で統一仕様の検討がなされていたが、ぎりぎりになって別々の規格として発表されることとなった。STTもSEPPも、買い手の個人情報やクレジットカード番号は店の人にも見せないようにする、クレジットカード会社には個人が何を買ったのかという購買情報は渡らないようにするなどの個人のプライバシー保護を考慮したシステムになっており、使用するセキュリティ技術もほとんど同じといってよいほど似かよっている。両者とも電子印鑑技術を使用し、クレジットカード番号と電子印鑑証明書の対応付けによって本人を確認する。理論的には、カード番号とデジタルデータである電子印鑑証明書の発行だけで、プラスチックのカードを発行せずにソフト的なクレジットカードを発行することもできるようになる。

世界1位と2位のクレジットカード会社の決済方法が別だということは両者にとっても、利用者にとっても決して好ましいことではない。1996年2月1日、VISAとMaster

Cardは、両者が新しいクレジットカード決済の統一規格Secure Electronic Transaction (SET)を作成することを発表した。2月23日には「Review Draft For Comment」という最初のバージョンのスペックも公開された(図7)。内容は、Master陣営のSEPPをベースに一部VISA陣営のSTTで使っている技術を入れ込んだようなものになっており、この統一規格がVISA側がMaster側に歩み寄った結果実現したということが推測できる。SETの規格制定には、GTE、IBM、Microsoft、SAIC、Terisa、VeriSignも協力会社として参加している(図8)。

もともとVISAとMasterCardがインターネット上のカード決済規格制定で折り合えなかったのは、エレクトロニックコマースの分野で首位を独走するNetscapeが、追いかけてくるMicrosoftに対して非常に大きな不快感と不安感を持っていたことにあったと思われる。しかし、最後には、使用するユーザーや加盟店のことを考えて協調する路線をとってくれたことになる。これらの規格を作成する際にRSADSIの技術者もアドバイザーとして参加しており、セキュ

図6：クレジットカードの用途を拡大するEMVカード

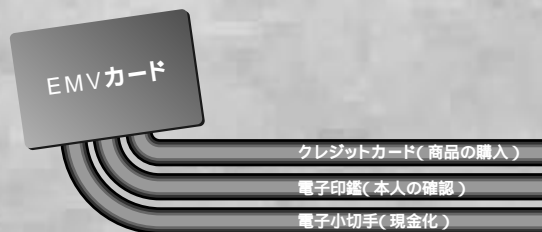
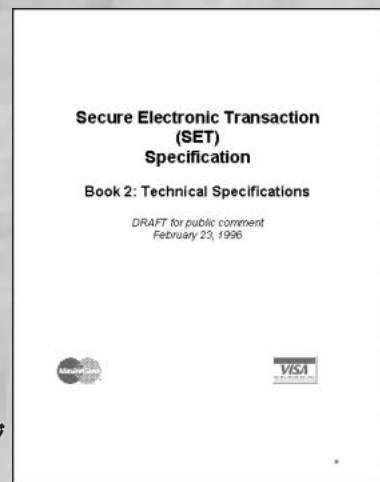


図7：SETの仕様書。MasterCardのホームページ(<http://www.mastercard.com>)からダウンロード可能



リティー面から見ても比較的完成度の高い規格としてできあがっている。

1996年5月中には、SETの次のバージョンが発表される予定である。次バージョンでは、あまり根本的な変更はなく、各証明書の無効リスト（Certificate Revocation List）のさまざまな配布方法や処理の途中結果を照会する機能など、SETのシステムが実稼動したときに発生する細かい問題に対応した拡張がなされる予定で、より現実的で洗練された規格になるだろう。

SETは、インターネットクレジットカード決済の決め手であり、この規格が世界統一規格として普及することになるだろう。日本でのエレクトロニックコマースプロジェクトなども、ほとんどがSETに準拠した規格を採用することになるとと思われる（IBMのカード決済方式を使用するテレコムサービス協会など、独自色を打ち出した実験もある

が）。

株式会社ビー・ユー・ジーもSET規格の制定について意見を提出したり、SETシステムの開発を行ったりと、SET関連業務に力を入れており、金融関係会社などと打ち合わせをしながら複数のシステムや機器の開発を進めている。ほかにも、MicrosoftやNetscapeをはじめとする多くのベンダーがSET関連ソフトウェアの開発に力を入れている。RSADSIもSET Toolkit（仮称）というソフトウェア開発ツールキットを開発中で、完成し次第ソフトウェアベンダーに提供する予定である。また、RSADSIではSETのインプリメンテーションが正しく行われているかどうかを検証するテスト機関の運営も予定している。もし、RSADSIの思惑どおりSETテスト機関が設立されると、SET関連製品を開発するベンダーはインターオペラビリティのためにRSADSI純正

のSET Toolkitを使用しなければならない状況になることも予想される。その場合、SET Toolkitは、BSAFEとTIPEMに続いて重要な役割を担うことになると思われる。

このようなクレジットカード業界の素早い動きにより、ネットワーク決済の本命はホームバンキングを飛び越えてクレジットカードへ移りつつある。特に、間もなく登場するEMVカードはクレジットカードの可能性を大きく広げるものであり、多くのエレクトロニックコマースアプリケーションは、EMVカードを電子決済のためだけではなく、単なる印鑑としても使用するようになるかもしれない。そのときには、概念上分かりにくかった電子印鑑技術も、EMVカードを印鑑と見なすことによって「物」として扱える印鑑を得ることになり、一般の人々からも信用を得ることができるようになるだろう。

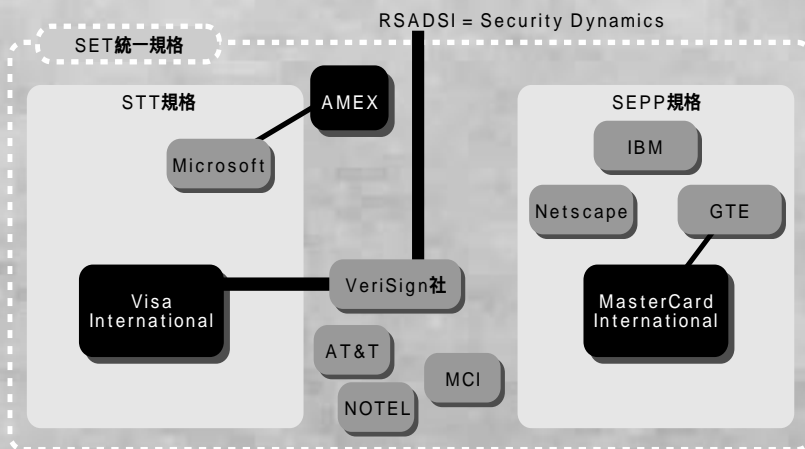


図8：セキュリティー技術における覇権争いはSET統一規格によって終結する？



図9：電子現金MONDEXのホームページ



4 電子決済方法の今後

クレジットカード決済の次に実用化が予想されるのが、デビットカード、電子小切手、電子現金などである。

クレジットカード決済の次には、デビットカードと電子小切手が実用化されるだろう。デビットカードとは銀行のキャッシュカードをクレジットカードのように使用できるようにしたものである。加盟店でデビットカードを使用して支払いを行う場合、その場で会員の銀行口座を確認し、支払おうとしている金額以上の残高がある場合はその場で引き落とす。1回ごとにその場で引き落としを行うので取りはぐれが少ない。デビットカードは主にヨーロッパで普及しているが、これもICカード化されようとしている。近々、イギリスでICカード化したデビットカードの実験も行われようとしており、こちらも楽しみである。

このままていど電子小切手のほうも主流はEMVカードになりそうで、またまたクレジットカード会社が一步リードといったところだ。EMVを利用した電子小切手の実験は、アトランタとキャンベラに続いて、ニューヨークで1996年末にCITIBANKとChemical Bankと合併したばかりのChase Bankの2行が行う予定である。この実験は10万人規模で行われ、VISAとMasterの

カードが混在して使用される予定で、同時期に同地域で行われる2大ブランドの実験を観察することによってどちらが進んでいるかを冷静に比較できるよいチャンスになるだろう。

電子小切手の後には本命の電子現金の実用化が待っており、ネットワーク重視型の社会の到来に合わせて技術もどんどん進んでいく。電子現金に関しては現在実用化のための技術が急ピッチで開発されているところであり、今しばらくは技術革新時期である。普通にいても実用化はしばらく先になりそうだ。

最近何かと騒がれているMONDEX（図9）なども電子現金の一種であるが、現在得られている情報から判断した著者の個人的な意見としては、今のMONDEXはどうしても信頼するに足りだけの技術的な根拠が得られず、このまま普及するようなことがあれば電子決済の将来に大きな不安を残すことになると思う（ただし、これはあくまでも著者の持つ限られた情報の中で判断した個人的な見解であることを再度お断りしておく。また、仮にこの見解が正しいとしても将来改善されるかもしれない）。最近、日本の多くの銀行もMONDEXを採用するという動きがあると聞いているが、セキュリティ面を慎重に評価したうえで冷

静に行動してほしいところである。電子現金の基本特許を世界中で持つNTTもMONDEX陣営に参加すると新聞などで報道されたが、それは誤報であることが後に確認されている。一度発行してしまえば半永久的に流通する電子現金は、クレジットカードなどは比べ物にならない高いセキュリティレベルが求められる。また、日本の現金である日本銀行券は日本銀行に信用があるから通貨として成り立っているわけで、現金には信用が一番大切である。一度でも事故があると、電子現金というものの自体が信用を失い、取り返しのつかないことになりかねないので電子現金の実用化は慎重に行ってほしい。もちろん、技術は日々進歩しているので、電子現金に十分な安全性を低コストで実現できるようになる日はすぐそこまで来ている。

そのような意味からも、今はクレジットカード決済が「旬」の時期であるといえる。また、クレジットカード業界の次の一手、EMVカードによる電子小切手は利用者にとってはMONDEXとほとんど変わらなく利用できるうえに、セキュリティ面でもMONDEXより優れたものが普及すると思われ、こちらのほうが本命に思える。

5 最後に

ホームバンキング、クレジットカード、デビットカード、電子小切手、電子現金というネットワーク上の新しい決済方法が次々実用化されていっても、これらの決済方法はすべて共存して使用されることになるだろう。実社会と同じように目的に合わ

せて最適な決済方法が選択できるようになれば、私たちの生活はますます便利になっていくはずだ。

本稿に関するお問い合わせは、電子メールにてinfosec@bug.co.jpまでお願いします。



[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp