

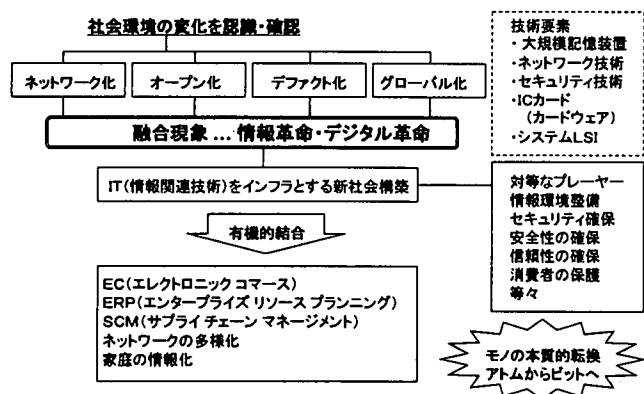
「次世代ECを進めるキーテクノロジー」

平松雄一（沖電気工業株式会社）

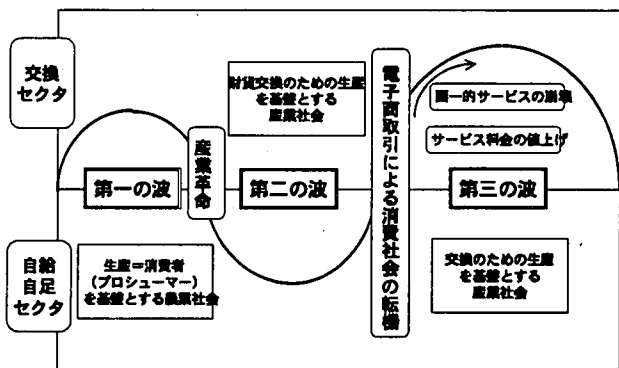
電子商取引（エレクトロニック コマース：EC）は、「インターネットを中心とするネットワークを活用した商品やサービスを売買」することと定義されている。確かにスタート時点では、ネットワーク上の売買取引や口座振替指示のためのものであった。しかし、現在ではデジタル化された商品、即ち電子情報もそのターゲット商品として仲間に加わり、その範囲は拡大している。

このECは、社会インフラの本質的転換、即ち現物（アトム）から情報（ビット）への変化により必然的に誕生したものと言える。この歴史は新しく、10年に満たないものである。日本では、1995年度通産省が第一次補正予算として公募した「エレクトロニック コマース推進事業」がその緒である。B to C をターゲットに、この予算総額100億円である。またその直後にB to B をターゲット第二次補正予算として217億円を投資している。

社会環境の変化



第三の波 生産=消費者（プロシューマ化）の復活



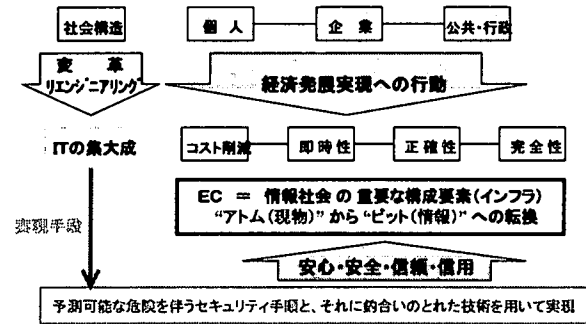
このECは、これまで歴史上で語られてきた産業革命に匹敵する、大きな動きとして捉えることが必要であろう。それはこの対象が産業界の大企業や銀行・金融機関のみとせず、中小企業や生活者（個人・消費者）までも含む社会全体としているからである。そしてその基盤は、インターネットを中心とするネットワークに根差し構築されていることに他ならない。また、これを可能にしたキーは、IT（インフォメーション テクノロジー：情報技術）によるデジタル化である。そのためこの動きを情報革命・デジタル革命として表現することもできる。しかし、ITは新社会構築の実現手段であり、目的ではない。

これまで産業界を中心とするデジタル化は、コンピュータ出現と同時に情報のデジタル化を進めてきた。しかし、このECの動きは伝票等のデータのデジタル化であり、商品・産業の本質的情報化ではない。今の動きは、商品そのものをデジタル化して、新たなビジネス誕生へと動いている。これが産業界において合従連衡へと結びつき、メガバンク誕生や異業種・異分野企業の合併等となり現在の社会現象の一つとなっている。

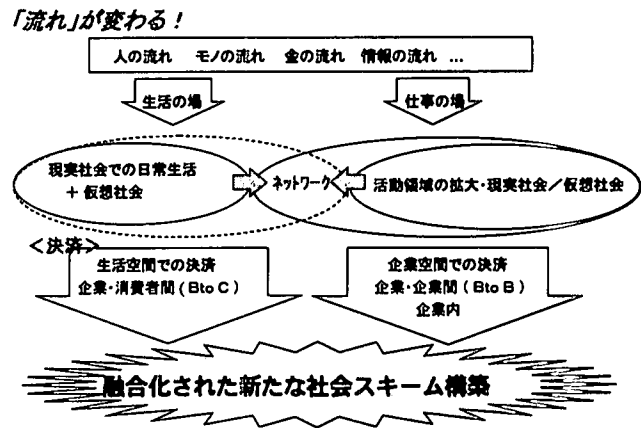
このEC市場規模は2003年でB to B 約70兆円、B to C 約2.5兆円と予測されている。規模的には前者が圧倒的なものとなるが、その情報化への動きとしては、前者はある程度IT技術を駆使して今日に至っているのに対し、後者はまったくと言っていいほど手付かずの状

況にある。そこで、ここでは未開拓である B to C にも焦点を当て述べてみたい。

エレクトロニクス（電子商取引）の目指すもの



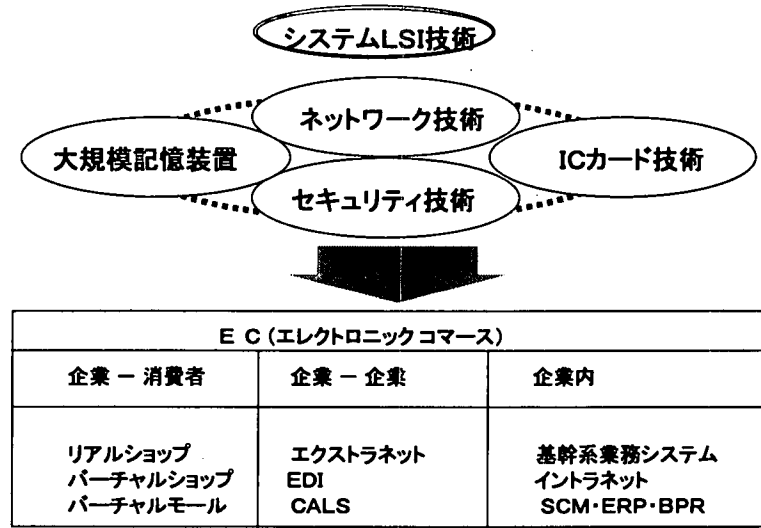
社会構造の変化(決済分野)



EC導入により社会構造の変化、特に決済分野においては、その「流れ」を替える大きなうねりとなっている。ネットワーク上に形成される新社会の参加者・プレーヤーは、行政・企業・小売店・生活者（個人・消費者）等々であり、総て対等に活動できることとなる。このため基盤（プラットフォーム）として、新たにネットワーク・コミュニケーション・セキュリティ・プレゼンテーション等々に対する課題解決が浮上する。これが次世代ECにも結びつくキーテクノロジーである。

ここで手段として活用されるキーテクノロジーの幾つかを紹介する。

EC社会を支える技術



○ ネットワーク技術

インターネットは、既に理解いただいているように特定企業が営利のために運営しているネットワークサービスではない。非営利の目的で規約が定められ「国際的に標準化された通信手順や手続き」のことである。この規約や標準に基づく限り、企業や団体・生活者（個人・消費者）は、自由に情報の交換がインターネットを通じて可能となっている。

最近では、デジタル伝送路等の新技術の普及、通信事業へ新規参入の一層の増大、NTTの再編、国内外の業務区分の撤廃と通信会社の合併及び連携の動き等、通信環境は急速かつダイナミックに変化している。一方、生活者を含む通信利用者は、豊かな生活の実現や精神的ゆとりの確保を求めて、便利・迅速・多様な情報通信サービスへのニーズが増大している。社会経済面では、経済のボーダレス化が一層進み、また、高齢化社会の到来や地球環境の保全等の社会環境変化と共に、ネットワークの重要性がより一層喚起されている。

インターネットの急激な発展は、米国における国防技術を背景として通信・コンピュータ及び基本ソフトウェア技術の蓄積と公開の上に成り立っている。この分野はアプリケーションの自由かつ多様な展開に資するものが比較的多く、注目すべき技術が豊富に存在していると言える。

インターネットをこれだけ普及させた立役者は、電子メールでありマルチメディア情報を簡単に扱うことができるWWWである。この画期的な仕組みが、ネットワークを大衆化させ、急激な利用ユーザ数の増加を引き起こしている。

一方、大衆化するが故にセキュリティ対策も求められるところである。特に、第三者の介入を受ける可能性があり、安価な通信ができる反面接続しているだけで発生する脅威がある。

- ・ 不正な利益をあげようとする第三者からの脅威
- ・ システムの混乱を狙った攻撃・脅威
- ・ 機密情報への不正なアクセスを意図した脅威
- ・ 個人情報悪用した成りすまし・否認・改竄等の脅威
- ・ 商取引での相手認証の確保 … 認証・電子署名・暗号化 等々

○ セキュリティ技術

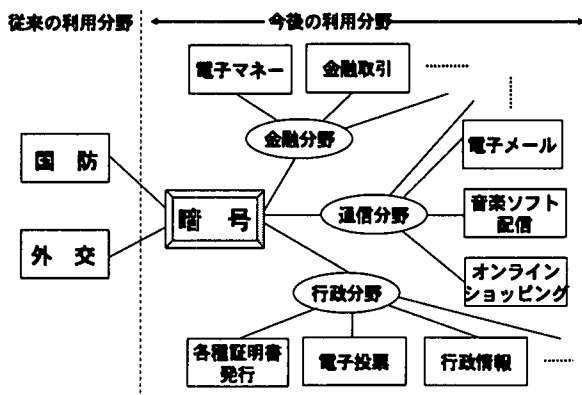
ECにおけるセキュリティは、極めて重要な技術である。この技術はともすれば暗号化技術として捉え勝ちであるが、ECにおいては、すべての構成要素と共に運用まで含むトータルなシステムとして、セキュリティ確保を如何に行うかが重要であろう。

持つべきセキュリティ機能は、次の通りである。

- ・ 情報発信者の正当性確認 …………… 発信者の認証・否認防止
- ・ 受信した情報の正当性・完全性の確認 …… 情報の改竄防止
- ・ 第三者への情報漏洩防止 …………… 情報の漏洩防止
- ・ 正当な受信者への情報到達確認 …………… 受信者の認証と否認防止

これらを認証・電子署名・暗号化技術を使用して情報の安全性・完全性を確保する。このことにより安心・安全・信頼・信用に応えるEC社会を構築することができる。

広がる暗号の用途



21世紀のデジタル暗号技術

1999. 8. 9. 米国商務省技術標準局発表 電子商取引の普及のカギ
次世代暗号技術 AES (Advanced Encryption Standard)

最終選考候補2001年までに最終決定

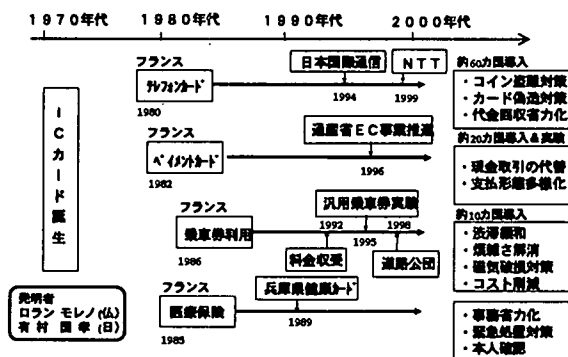
暗号名	開発主体	国名
① MARS	IBM	米国
② RC6	RSA社・フィラズ	米国
③ Rijndael	J. デー・マ氏ら2名	ベルギー
④ Serpent	R. アダ・ツ氏ら3名	英国・イスラエル
⑤ Twofish	B. シュナイア氏ら6名	米国
選外 EPOC	NTT	日本

○ ICカード技術

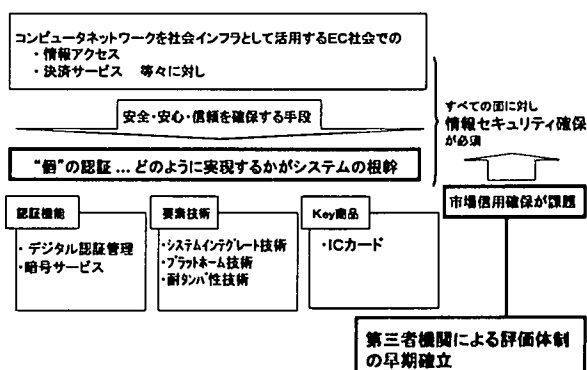
公衆電話のICカード化並びにJR東日本・乗車券類のICカード化等ここに来て大きな動きを見せている。ECにおいては、個の認証を行う手段として早くからICカードを使用することが検討されてきた。しかし、ICカードコスト並びにその有効性を発揮するキラーアプリケーションが見出せなかったことからこれまで停滞していた。ここに来て、既存カードである磁気カードの変造・偽造に伴う犯罪の多発化からICカード化への動きが加速化している。特に、個の認証ツールとして、生活者（個人・消費者）のID並びに運用時における個人IDとして活用されようとしている。

ICカードは、これまでの磁気カードとは異なり、オフラインにてもその有効性を発揮することができることから、運用コスト低減並びにセキュリティ確保にその威力が発揮されようとしている。また利用者からは、安心・安全・信頼できるカードとして老若男女から理解を受け、B to Cを中心に各種のシステム構築が全国各地で進められている。情報環境が充分でない地域においても、このICカードを活用することができる。

ICカード進展の背景



EC社会におけるICカードの重要性とその評価



ICカードは、EC社会を維持する極めて重要な媒体であり、これまでの接触型ICカードと共に、非接触型ICカードもより使いやすい形で身近なものとなろう。

いずれにしろ、EC社会は人の集合の上に成り立つものであり、その各プレーヤーが如何に安心・安全・信頼・信用を担保し、行動することができるかに掛かっている。その実現に向けて、法整備と共にIT技術が手段として役立つことを願う次第である。