1. 総論—文明構造の変革と情報セキュリティ

辻 井 重 男[†]

1. マルチメディアネットワークによる 文明構造の変革

マルチメディアに関する議論の盛り上がりやインターネットの急速な普及は、人々に、情報ネットワークのパーソナル化と国際的ボーダレス化を実感させると共に、これまで、一部の研究者に専有されていた情報セキュリティに関する知識と技術を、広い分野の技術者に広げるという効果を生んでいる。

インターネットに象徴される情報ネットワークの地球的規模での浸透は、文明の構造や文化の概念を大きく変えていくものと予想される。文化の定義は、文化人類学者の数だけあるともいわれている通り、文明や文化を一義的に定義するのは難しいが、ここでは、文明とは、人類にとって普遍性のあるインフラストラクチャを意味するものとし、文化とは、あるグループに固有な思考形態、価値観、美意識や生活・行動様式等の総体を指すものとする。従来、国際的に普遍性のあるインフラストラクチャの中で、情報がらみのものとしては、印刷、郵便、電話、放送などがあり、これらの情報文明が各地域・民族間の文化交流に大きな力を発揮したことはいうまでもない。例えば、西洋文化が世界を制覇したかに見えたのは自由、平等、博愛といった近代の理念が無謬の真理であったためというより、印刷技術による情報普及能力によるところが大きかったというべきであろう。

しかし、これからの情報ネットワークの展開は、これまでとは質的に異なった影響を文明・文化の構造に与えるように思われる。文書・画像を含むいわゆるマルチメディアネットワークに誰もが自由にアクセスし、個人レベルで情報の受発信が可能な状況が地球を覆い始めている。情報ネットワーク化が国境を越えて

展開されるとき、法制度や慣行の国による違いが問題となってくる。例えば、米国では、著作権管理情報の虚偽表示、改ざん、除去についての規制があるが、日本の法律には規定がない（規制撤廃の流れと逆のことをいうようだが、情報財の流通を促進するという積極的な意味からも、このような規制は必要であろう）。

また、CALS (Continuous Acquisition and Lifecycle Support, 生産・調達・運用支援統合情報システム) に象徴されるような電子調達等の経済的インフラも国境を超えて整備される方向にある。情報ネットワークに税関という物理的関所を設けることはできない。情報ネットワーク社会では、物理的なレベルでのネットワークが国際的なインフラストラクチャになるのみでなく、その瞬時性と広域性から法制度や経済システムについても国際的合理性、透明性のあるインフラストラクチャの構築を促すことになるものと予想される。

CALS は、最近、Commerce At Light Speed の略ともいわれている通り、光速の商取引が行われる世界であり、そこでは、各国固有の法制度ではなく、世界法の下で運用することを決めている。また、種々の要因や歴史的経緯から、電子商取引における使用言語は、英語となる可能性が大きい。

情報ネットワークのボーダレス化は、このように、物理的なネットワークに止まらず、法制度、経済システム、更には言語までが、世界的文明インフラストラクチャとして肥大化することを意味している。

これまでの文明に比べ、格段に厚くなった文明層の上で人々の諸活動が展開され、文化層が形成されることになるが、このことは、文化の概念や構造にも影響を及ぼさずにはおかない。この点について若干付言しておこう。

明治12年、福沢諭吉は、その著「民情一新」において情報という言葉を初めて使用すると共に、電信や郵便がその後の日本に与える影響の大きいことを論じているが、実際、西洋文明の導入が日本文化に大きな変

[†] 中央大学

“Overview—Revolution of Civilization Structure and Information Security” by Shigeo Tsujii (Chuo University, Tokyo)

図 1 情報ネットワークのボーダレス化・パーソナル化による文明・文化構造の変化 (極論的概念図)

化をもたらした。それにもかかわらず、我々は、村落共同体的な情緒的連帯のもとに生活しており、欧米、特に米国とは異なる文化を保有している。しかし、CALSの中で談合することは難しい。今後の情報ネットワークの上で展開される経済活動は、我々の倫理観や談合体質を根本から変えていくことになるのではなかろうか。

人の心は簡単に変わるものではない。地域特有の気候風土の下で永年にわたって培われた民族の心が、情報ネットワークの普及位で変わるものだろうかという反論はもっともである。だが、民族やあるグループの平均値の差(分散)よりも個人差の方が大きいとも考えられる。個人が少数の帰属集団から解放され、情報ネットワークを通じて多くの集団に属し、人それぞれの個性によって生きるとき、文化の構造にも変化が生じよう。人々の信条や価値観、倫理観なども国や民族毎の差が減少し、個人の趣味、専門、価値観、美意識等によって結ばれた地球横断型の文化が21世紀を通じて育っていくものと思われる (図1)。

筆者とて、これが暴論とはいわぬまでも極論であることは充分心得ている。例えば、言語は文化の基本的要素であるが、言語が簡単に変わらない以上、地域や民族特有の文化が消えるわけではなく、地域縦割型の文化が従来通り続くことはもちろんである。筆者が主張したいのは、地域縦割型の文化と直交する地球横断型の多元的文化も急速に成長していくのではないかということである。

以上を要するに、文明層が経済的、法制度的基盤を含む形で従来より格段に重層化し、かつ国際的に広域化し、その上で同じく国境を超えた広域的文化活動が展開されるような情報ネットワーク社会の到来が予想されることを述べたものであるが、このような社会の存立条件のひとつが情報セキュリティである。

情報セキュリティとは単に暗号による情報秘匿のような守りの技術を意味するのではない。それは、紙ペ

図 2 情報セキュリティ技術の構造

ースと対面ベースを主とする社会から、情報ネットワークが人々の活動の少なからぬ部分を支える社会へ移行しつつある現代において、認証、署名、相手確認等の技術を通して情報に信用を与える技術、情報の価値を保証する技術、要するに新しい社会の信頼関係を構築する技術なのであり、情報財の流通を促進する攻めの技術なのである (図2)。

2. ポストモダン暗号論

我々が日常生活の中で、ある物を秘密保管したり、文章にマル秘の印を押すことと、署名や捺印することと、どちらの機会が多いだろうか。明らかに後者であろう。情報ネットワーク社会における暗号の役割とし

でも、前者以上に後者に相当する機能が本質的に重要である。

暗号の歴史は古く、ギリシャ・ローマ時代にさかのぼるといわれているが、実はそれより古く約5千年前、ヘブライで単文字換字式暗号が使われていたという。古代から中世を経て16世紀には多表式暗号が発明され、第2次大戦にはこれが極限的發展を遂げ、大戦の推移に陰の主役を果たしたことはよく知られている。

このような数千年の歴史の中での暗号の主機能は、同一組織内における秘密伝達であった。シーザー暗号から第2次大戦中のエニグマ暗号や紫暗号まで、暗号方式はアルゴリズムの面でも、暗号文の自動作成等の実現技術面でも長足の進歩を遂げている。大戦末期には英国でドイツのエニグマ暗号解読のため、暗号解析機が作成され、一時はこれが世界初のコンピュータだとされたこともあった。しかし、このような進歩にもかかわらず、古代から今世紀中頃まで、暗号のパラダイムは変わらなかった。繰り返しになるが、暗号は同一組織内の守秘を第一義としていた。

このような暗号をモダン暗号ということにすれば、暗号の世界にパラダイムの拡大が起きてポストモダン暗号の時代に入ったのは1970年代であった。流行語としてのポストモダンはすでに古いが、現代思想としてのポストモダンには、近代合理主義に対する反省的あるいは批判的ニュアンスが強いのにに対し、筆者がポストモダン暗号というとき、それは、従来古典暗号の名で呼ばれることの多かった工業社会のモダン暗号を包含しつつ、パラダイムが格段に拡大した、情報文明インフラストラクチャの基盤となる暗号である。科学技術においてポストモダンというとき、それはモダンを包含しなければ意味がない。

どのようにパラダイムが拡大したのか。

- (1) 同一組織内で使用に限られていた暗号が、国際社会まで含めた公開的共通基盤技術となった。
- (2) 守秘を主な機能としていた暗号が、それと合わせて、人・モノや情報の真正性を保証し、情報に信用を付与して、情報財流通を促進するための認証機能、すなわち、署名・改ざん防止機能を持つこととなった。

の2点に要約されよう。

1973年、米国商務省は、不特定多数間での利用に供するため、アルゴリズム公開型共通鍵暗号を公募し、1977年、標準暗号DES(Data Encryption Standard)をFIPS(Federal Information Processing

Standard)として制定した。これと前後して、公開鍵暗号の概念が誕生している。古来、暗号化の鍵は当事者どうし(2者間)の共通の約束事であり、ペア毎に秘密に鍵を設定していた。このことは、暗号の常識であったから、公開鍵暗号が生まれるまでは、共通鍵方式という名称も存在しなかった。

公開鍵方式では個人毎に、秘密鍵とこれに対応する公開鍵を用意する。公開鍵方式を守秘(いわゆる暗号、あるいは狭義の暗号)に用いるときは、受信者Aが公開している公開鍵で、誰もがAに暗号文を送ることができる。このとき、暗号化鍵は公開されており、暗号通信に先立つ鍵の秘密配送という煩わしさが無い。しかし、公開鍵方式の本領は、その認証機能においてより顕著に発揮される。公開鍵方式を認証に用いるとき、秘密鍵は、その人の手書き署名や実印に相当すると考えてよい。公開鍵は、その署名や実印がその人のものであるという本人確認(一般にはカードや端末を含めた人やモノの真正性確認)の手段に当たる。つまり、発信者Bが個人の秘密鍵で作成した暗号文は、秘密鍵とペアになっている公開鍵のみで検証することができるため、受信者は発信者Bが本人であることを確認することができる。このように考えると、従来の公開鍵方式という名称は必ずしも適切ではないように思われる。やや長くなるが、

共通鍵方式⇒共通秘密鍵方式

公開鍵方式⇒個人秘密鍵方式

と呼び変えれば概念的にはより明快であろう。“何故、鍵を公開して暗号になるのか?”というような暗号の面白さを説明するには、公開鍵方式という名称は面白いが、秘密なしに暗号方式が成立する筈もない。秘密鍵を個人が専有していて、オープンな放送型ネットワーク社会に適応させた方式が、公開鍵方式なのである。

さて、マルチメディアが高速ネットワークを流れる時代にあつて、複雑な権利関係の下で、原作者と改訂者に適切な権利を認めつつ、情報財をスムーズに流通させるため

- (1) 情報の価値に対する認識と情報通信倫理の高揚
- (2) デジタル情報財に適した法制度の整備
- (3) 認証・署名、情報秘匿、課金等を適正に行うための技術的システムの導入

を急がねばならない。(3)の技術的システムの基本技術がポストモダン暗号であり、情報セキュリティ技術である。

ハードウェアの急激な価格低下に対して、潜在的に

はより大きな量産効果が期待できる筈のソフトウェアについては生産性が上がっていない。ソースコードレベルで部品化・再利用が行われても、組織内に閉じている限りは大きな効果はなく、それらの部品を電子オブジェクトとして市場に供給し、対価を得ることができるようなシステムが確立されて始めて、ソフトウェアの流通と低価格化が実現されよう。

また、近頃騒がしいマルチメディアも、その素材を利用者が自由に処理・加工・編集し、これをネットワークを介して再び流通させ得るようなシステムが必要であろう。情報自由化時代を迎えて、我々は、情報価値の認識と情報通信倫理感を高めるといった精神的構造改革をベースに、上記のようなシステムを、法制面と技術面から確立していくことが急がれている。

デジタル情報の姿をした知的財産に対しては、複製をもって著作権侵害とするコピーライトの発想、あるいは印刷技術を前提とした法制度は改めるべきときにきており、利用に対する対価徴収権を基本とする法制度が適合していると思われる。

このような法制度の下で、情報財の流通を促進し、そのパイを大きくして単価を下げる技術的システムとして、いわゆる超流通システム (Super Distribution) が注目されている。超流通システムは、1983 年以來、森亮一氏によって提唱されてきた概念であり、大よそ次のような構成となっている²⁾。

超流通システムは、情報財 (以下、ソフトウェアと呼ぶ) の利用に応じて課金する従量制のソフトウェア流通システムである。料金決済を電子的に行うために必要な情報が超流通ラベルとして、ソフトウェアに付加される。超流通ラベルとして、次の 2 項目が含まれる。

- (1) ソフトウェア ID: 個々のソフトウェアを識別し、利用料金の支払先を区別する情報
- (2) 使用記録: ソフトウェアの利用状況を表す情報であり、超流通センターに回収され、それに基づいて料金の決済が行われる。

超流通ラベルは料金決済の基礎となるもので、その改ざんは超流通システムにとって脅威であり、改ざん防止のために暗号が用いられる。また、利用情報の秘匿、認証子生成・確認等のため、暗号技術が駆使され、超流通システムは、暗号と情報セキュリティシステムそのものといっても過言ではない。

最近、暗号化された情報を CD-ROM に多数記録し、料金支払いに応じて鍵を配るシステムも商用化されているが、このようなシステムを、いわば、インダストリアルプラットフォームとして、体系化したの

が、超流通の概念であるといえよう。

情報社会とは、有体財と同等以上に情報財が流通する社会であることを考えると、情報財流通促進剤としての情報セキュリティ技術は、守りの技術であると同時に攻めの技術と認識されるべきであろう。

3. 国際ボーダレス化と国家の情報セキュリティ政策

人々の経済的活動は、国境を越えて、ボーダレス化し、電子商取引 (Electronic Commerce) や CALS を活用して、Virtual Cooperation が設立される動向にある。こうした活動を円滑に行うためには、情報ネットワークや電子伝票のプロトコルに止まらず、法制度まで含めて統一されていることが望ましい。暗号方式についても然りである。暗号の場合、絶対安全性を保証することが難しいので、1 つの標準に決めない方がよいという考え方もあるが、この議論は別として、仮りに米国政府の標準暗号が信頼性が高そうであるからといって、各国ともそれに右へならえというわけにはいかないお家の事情も存在する。お家の事情とは、ナショナルセキュリティもあり、また、国民の心情、倫理観あるいは価値観もからむ根深い事情である。暗号方式だからといって単純な技術の問題に収まる話ではなく、国際軸と国家軸という直交座標の中で妥協点を見出すという 21 世紀の課題を背負う話なのである。このような視点から、最近のクリントン・ゴア政権の暗号政策について考えてみよう。

米国では第 2 次大戦後も暗号政策には軍の強い影響がうかがわれるが、民間での利用が進むにつれ、政府は、麻薬売買やテロリスト活動などにもその利用が及ぶことを懸念している。そして、NII (National Information Infrastructure) 計画の一環として、1993 年 4 月、クリントン政権は、Skipjack と呼ばれる非公開アルゴリズムを用い、裁判所の許可の下で、暗号化された通信内容を解読し得る仕組みを導入する構想を発表した。この仕組みは KES (Key Escrow System) と呼ばれており、プライバシー保護の観点から、通信内容に対する守秘の必要性が高まる一方、通信内容の秘匿は、ネットワーク犯罪において、法の執行を妨げるという相容れない課題を解決しようとするものといわれている。KES は暗号鍵保管標準 EES (Escrowed Encryption Standard) として米国連邦政府標準 FIPS (Federal Information Processing Standards) の認定を受けているが、法的強制力はないものと位置付けられている。

また、FIPS は、“国家機密ではないが取扱いに注

意を要する情報 (Unclassified but sensitive information)”を対象として、米国政府内での取扱標準を定めるものであり、民間企業や個人を直接コントロールするものではないが、暗号機器の市場を通して、間接的に民間に大きな影響力をもっている。

歴史をさかのぼれば、米国の暗号技術はもともと国家安全保障の立場から機密情報 (Classified information) を秘匿する手段として、NSA (National Security Agency, 国家安全局, 国防総省の下部機関) の一元的管理の下におかれていた。1965年に制定された Automatic Data Processing Equipment Act により機密情報は NSA が、取扱注意情報は NIST (National Institute of Standards and Technology, 商務省の下部機関) が管理するという線引きがなされたが、NSA の高度な技術力や様々な経緯から、米国の暗号文化には軍を中心とする国家主導の色彩が強い。こうした背景もあって、KES 構想に対しては“政府が保管鍵を用いてプライバシーを侵害するのではないか”といった批判が、民間サイドや学識経験者から出されており、クリントン政権も KES 構想を強行する構えではなく、今後の実施形態はなお不明な点が多い。

そうはいつても、米国政府は NII の世界化、すなわち、GII (Global Information Infrastructure) 構想も提案しており、その中には KES のような概念も含まれるとすれば、国際的な影響も大きなものがある。例えば、米国あるいは米国人がからむ犯罪が米国外でなされた場合の法の執行については Long arm protection といった言葉も聞かれ、各国の文化や法制度の違いから、当分、様々な摩擦を生ずることも予想される。KES 構想は、テロリストや麻薬に対する取締りをひとつの目的としているが、筆者はこの点には大きな疑問を禁じ得ない。何故なら、このような不正行為を行おうとするものは、政府推奨の標準暗号を用いず、共通鍵暗号、公開鍵暗号を含めて独自に選んだ暗号方式を使用できるからである。これに対する米国政府側の見解は、標準暗号の装置は低価格だからということであるが、これは犯罪者の得ばかりし利益や、ソフトウェアによる暗号通信の場合を考えると、説得力のある回答とはいえない。また、バーチャルカンパニー等において、企業等の金の出入りが暗号化されてネットワークを流れた場合、政府は税の徴収が難しくなるという問題の解決策として KES を考えているとの推測もなされているが、これは、不可視性という情報化社会の特質にからみ、かつ、ボーダレス化と合わせて国家の存立基盤にも影響を与えかねない深刻な課

題を我々に突きつけている。

我が国は、治安維持については、戦前・戦時の警察のあり方への反動から、戦後、警察力を弱体化したこともあり、また、権力に対するアレルギーもあって、犯罪捜査よりも通信の秘密を重視する傾向にあり、米国の KES のような構想は、日本では猛反対を受けることは目に見えている。

さればとて、日本国民の間でプライバシー保護に対する意識が高いかといえそうではなく、これはこれで問題なのだが、この点も含めて、このような日本と欧米の文化の相違をどのように乗り越えて、国際的情報文明インフラストラクチャを構築していくのか、今後、長期的視点から考えていかねばならない。

それにしても政府が自国の経済活動や犯罪行為を把握しようとすれば、政府の定めた標準暗号以外の暗号方式の使用を禁止しなければならず、しかも、これらの諸活動が国境を超えて行われるとすれば、そのような暗号政策を国際的整合の下に行わねばならない。これは極論かも知れないが、我々はそのような極限状況についても考えをめぐらしておく必要がある。

一方、米国政府の暗号政策のもうひとつの柱として輸出規制があり、これは、1994年3月のココム規制廃止後も、国防上や法律執行手段を保持する観点から続けられている。しかし、暗号技術を利用したソフトウェアについては、インターネット等のコンピュータネットワークを通じて流出している。ここにも、ネットワークを流れる情報については、税関も水際作戦も無力であるという情報化社会の特徴がうかがわれる。

以上のような米国の状況に対して、我が国の政府の対応はどうだろうか。第2次大戦中、日本政府の暗号技術のレベルはかなり高かったようであるが、米国政府が暗号による勝利を高らかに謳いつつ、戦後もその勢力を温存し拡充することができたのに対し、敗戦国日本が落ち込んでしまったことは想像に難くない。

第2次大戦中に蓄積された外務省や陸海軍の暗号技術は、戦後も対応する機関に引き継がれていると推測されるが、学会や民間企業における暗号研究は、それらとはほとんど関わりなく行われているといつてよい。これまで郵政省、通産省あるいは警察庁などにおいて暗号に関する調査研究などは行われてきたものの、日本としての標準暗号制定の是非、安全性に関する評価や体系化の推進方策に関する議論は最近までほとんど行われてこなかった。

最近の情報通信基盤整備、マルチメディア、更にはインターネットの動き等に対応して、日本政府も暗号等の情報セキュリティ政策に本格的に取り組み始めた

ようである。

郵政省では、1995年2月、郵政省内に「マルチメディア社会におけるセキュリティ技術に関する調査研究会」(委員長 中央大学 辻井重男)を設けて、上記の課題に関する議論を深めるとともに、通信放送機構において、暗号技術に関するプロジェクト研究をスタートさせている。また、通産省では、1994年10月、セキュリティ・プライバシー問題検討委員会(委員長 鶴沢元青山学院大学学長)を設置し、1995年7月の報告書にハッカー・ウィルス対策基準の抜本的改訂、プライバシー保護に対する民間部門を対象とした法的措置、電子計算機システム安全対策基準の大幅改訂、コンピュータセキュリティ評価の実施方策、公開鍵の登録システムの実証実験の実施、エレクトロニック・コマース・プロジェクトの実施等を盛り込んだところである。

4. む す び

21世紀の人類社会は、文明・文化の諸相において、国際軸と国家軸の直交する座標軸の中での相克の時代であるように思われる。情報セキュリティも例外ではなく、というより、情報文明の基盤としての情報セキ

ュリティに関して、我々はそのような悩みを日々経験している。

小文はそのような視点からまとめたものであるが、舌足らずの面も多く、どの程度筆者の感ずるところをお伝えできたか心もとないが、多少とも会員諸氏の御参考になれば幸いである。

(1995年8月10日受付)

【参 考 文 献】

- 1) 辻井重男：“現代暗号の不思議”，信学誌，78，3，pp.292-297 (Mar. 1995)
- 2) 森ほか：“電子情報通信学会，情報セキュリティ研究会，超流通および関連する応用分野特集”(Sep. 1994) (ISEC 94-13-22)
特に，大滝：“超流通アーキテクチャにおける開発環境について”(ISEC 94-14)
- 3) 通産省オープンシステム環境整備委員会セキュリティ分科会平成6年度報告書
- 4) 辻井，笠原編著：“暗号と情報セキュリティ”，昭晃堂 (Mar. 1990)

つじ い しげ お
辻井 重男 昭和33年，東京工業大学工学部電気工学科卒業。同年，日本電気(株)入社。昭和40年，山梨大助教授。昭和46年，東京工業大学助教授。昭和53年，同教授。平成6年，中央大学教授。情報通信システム，暗号理論，デジタル信号処理の研究に従事。博士(工学)。