コンテンツとハイパーリンクの構造

—超流通の現況と未来—

森 亮一[†]

1. ま え が き

筆者は、進行中のデジタル革命が史上唯一最大の革命であると考え、この革命をそれほど重大とする理由は、演算装置の進歩を支えるナノ技術を中心とする様々な関連技術が「共進性」を持つことである。現革命の最も重要な点は、技術の進歩が無数に生まれ、それらがすべて共進的に助け合って、現実には毎年4倍以上の猛烈な進歩がこれまでに50年間続き、その結果の性能の改善はすでに10の30乗倍に達していることである。12節で詳説するように、毎年4倍の継続は誤植ではない。

これまで共進性はほとんど生物だけが持つ神秘的な能力であった。有体物中心社会の長い歴史の中で、比較的容易に達成できる共進的な改善はほとんど尽くされてしまった。そこで、有体物では、日々の最良の設計の大部分は妥協点の発見になる。

例えば、自動車の燃費と定員と速度の全部を同時に改善する容易な方法は存在しない。そこで有体物の産業では、大きな進歩はめったにない。そのような進歩は「画期的」であり、この言葉そのものが「めったにない」ことを示している。画期的な進歩から次の画期的な進歩までは妥協と折衷の長い期間である。したがって、年平均10%を超えるような進歩は例外であった。このような環境が長く続いたから、社会も産業も学問も、画期的な成果だけが最も重要であるとするようになった。

超流通は現在の革命の次の段階を支える基盤技術である。以下では、超流通の現況に関して緊急と思われる次の2つの項目に言及し、デジタル革命の重要性について述べる。

- データコンテンツとプログラムコンテンツは別物であり続けるという思い込み。これについては9節で詳説する。
- 超流通ハイパーリンクの構造についての誤解。これについては10節で詳説する。

2. 超流通前夜

超流通の初出の3年前の「科学」1980年11月号(岩波書店, pp. 704~711)を一読されることを希望する。約20年前に、現在では誰の目にも明らかなデジタル革命がすでに始まっていることを指摘し、その方向と規模を述べたものである。20年前の記述のほとんど全部が、現在の状態にそのまま合致することが見られるであろう。読者が、以下の小論を読んで、もしその歯切れ良さに困惑したならば、筆者の20年前の歯切れ良さ、いやむしろ過激さには、書ききれなかった多くの理由も含めて、適切な根拠があったことを想起されたい。

3. 超流通の現況と資料

「日経エレクトロクス」1999/3/8号は、コンテンツ流通特集を組み、大手など6グループの事業計画などについて述べた。その中で「ここにきて、システム全体の基本的な枠組みがみえてきた」として超流通をあげた(p. 95)。1995年に米国WIRED誌は「2005年までには超流通のためのハードウェアがPCの標準的な構成要素になるだろう」と予測したが(Issue 3.06, 1995)、それが妥当であることが次第に明確になってきた。

超流通に関する最も新しい情報は、World Wide WebのSuperdistribution Resource Pageにある。

<http://sda.k.tsukuba-tech.ac.jp/SdA/WhatsNew.html>

印刷物としては、日本電子工業振興協会システムLSI技術委員会ソフトウェア超流通研究会とその前身による1988年以来的の報告書がある。1999年3月発行のものは資料が充実して推奨できる。その主な内容の最新版はWWWにある。森の論文66件、日本特許5件、外国特許3件、森以外の著者が超流通に言及した関連資料133件、その他、参考資料8件がある。いくつかの論文はダウンロードできる。

<http://sda.k.tsukuba-tech.ac.jp/SdA/SdAbib.html>

図1に超流通システムの構成例を示す。

超流通では、コンテンツを所有することに対して課金するのではなく、電気や電話などと同じように、利用者がどのくらい情報を利用したかを計測し、それに応じて課金する。

[†] 株式会社ナムコ

Copyright Protection of Digital Content and Technologies; (7)

“Copyright Protection of Digital Content and Technologies; (7) Structuring of Content and Hyperlinks with Superdistribution Technology” by Ryoichi Mori (NAMCO Limited, Tokyo)

図1 超流通システムの構成例

所有に対して課金を行わないということは、そのデジタル情報をどのような経路で入手しても権利者の利益が損なわれないことを意味する。例えば、友人からコピーすることも正当な入手経路のひとつとなるので、超流通が実現した世界では不正コピーは原理的に存在しない。

他人からコンテンツをコピーして利用しても、コンテンツ提供者には適切な使用料が入る。つまり、そのようなコピー行為は、従来は海賊行為であったのとは全く逆に、歓迎される行為となる。

新規に生産する費用とコピーする費用との比がすでに100万を超えて、さらに劇的に変化し大きくなり続けることが基本的性質である情報財にとって、コンテンツ提供者の知らないところで自由にコピーされ、その利用に対する収益が提供者に自動的に支払われるというこの性質は、極めて望ましく重要なものである。

超流通技術が実現されれば、ほとんどすべてのソフトウェアが購入する前にすでに手元にあり（超供給）、面倒な手数なしに適切な管理の下で使用でき（超需要）、そして気に入らなければいつでも使用をやめ、また返品することが可能であり、これらのすべては、水道の栓を開閉するように、利用者の手元だけで行うことができる（超流通）。

超流通において流通するコンテンツには、その識別子や課金情報、権利者情報などが記載された超流通ラベル（Superdistribution Label）という電子的な情報が付加される。超流通ラベルは、データ部分と論理的に不可分でなければならない。

コンテンツを処理するハードウェアは、超流通ラベルリーダ（SDLR：Superdistribution Label Reader）を持ち、超流通ラベルに記載されたデータに基づいて適切な処理を

行う。最も典型的なものとしては、誰が誰のコンテンツを使用していくらの支払義務があるか（以下、使用記録）を記録・回収し、料金の精算を行うシステムが考えられる。

料金の精算には既存の流通網を利用したシステムなどが提案されているが、デジタルキャッシュなどを応用することもできる。

この使用記録の回収は、適切な頻度（例えば1ヵ月に1回程度）で行われればよいので、コンテンツ使用時にオンラインで接続されている必要はない。

利用者が使用記録の回収を拒んだ場合には、料金の支払いが滞ることになる。これを防止するために、多くの公共料金と同じように、滞納によるサービスの停止が適用できる。使用記録の回収が適切に行われない場合には、SDLRが、使用記録の回収以外のハードウェアの動作を停止することが考えられる。

超流通においては、従来の有体物の取引では不可能であったような、様々な課金の形態が可能である。試用課金、従量課金、自動買い取り、買い取り後の返金、特別許諾（各種割引など）、無料だが使用状況の報告を義務づけるものなどを実装できることが示されている。コンテンツの特色に応じて、単純な課金から複雑なものまで自由に選択することができる。

個々のコンテンツが超流通ラベルを持つことによって、あるコンテンツから他のコンテンツを利用する場合でも、個々のコンテンツで個別に課金処理を行うことができる。すなわち、複数のコンテンツがハイパーリンクされた状況でも適切な自動的課金ができる（ハイパーリンク課金）。

多数の素材を組合せるマルチメディアコンテンツの開発に適用すれば、煩雑な権利関係の個別交渉を不要とし、利

用許諾および課金の自動化ができる(コンテンツ利用自動許諾)。また、ソフトウェア部品単位の課金ができるので、ソフトウェア部品産業の実現が可能となる。

4. 看過の歴史

かなりの人々が、1970年代のマイクロコンピュータの出現、1983年の超流通の発明の両方の場合に、重要なトレンドを看過している。

このような誤りは、良い標準化を邪魔する可能性が大きい。後述するコンテンツとハイパーリンクについての看過も、1970年代と80年代の看過と同根と見られるので、過去の2例について略述して、説明の助けとする。

5. マイコンの重要性の看過(1970年代)

大形計算機が優位にあったとき、市場規模と社会での意義においてマイクロコンピュータが必ず追い越すという事実が看過された。当時すでにコンピュータ生産費用におけるソフトウェアの比率が高かったことと、同じソフトウェアが2倍のコンピュータで用いられれば、1台あたりのソフトウェア費用は半分になるという、誰にでもわかる事実が理解されなかったことが重要である。専門家の多くが、販売個数さえ増加すれば、優れたソフトウェアが非常に安価になるという、今では誰でも知っている事実を見過ごしたのである。

6. 超流通の必然性の看過(1983年から)

ここでも約10年間の看過期間があった。主要な産業の製品の代金回収に不具合があれば、研究対象として、また産業として、それが重要でないことなどあり得ない。にもかかわらず、速度を高め、機能を充実することが当時の正統な研究対象であって、ソフトウェアの代金を適切に、すなわち権利者にとって確実に、そしてユーザにとって便利に回収する、超流通のような電子技術の研究の重要性は約10年の間無視されたといつてよい。

7. 先見性と経営判断

上の2例は筆者の経験であるが、このような看過の例は多いであろう。それは無理もない。進行中のデジタル革命のような激動期では、先見性と経営判断の両立は極めて困難である。

人々は、有能であるほど、ふつう後者に投入される。なぜならば、いつ、何を、いくらで、どのように製造し、契約し、市場展開するかなどのあらゆる事柄は、その1つを誤るだけでも致命的になりかねず、しかも、完全な判断根拠なしに、充分とはいえない時間的余裕で次々と決定を求められるからである。このような経営判断をやり抜いて初めて、競争における勝者となる。したがって、迅速・適切な経営判断の能力が経営の神髄とされるのは妥当であろう。

一方、先見性は、充分に考え、可能な枝分かれを読み切ることによって正確になる。ところが、社会はそのような時間を許さない。例えば、メディア上の討論では、即座に返事できることが重要であり、散会後の答えは正しくても無効である。しかし、迅速な応答が正確であるという保証は全くないし、程度をこえて迅速な応答は大きな誤りを含む。

では、どうしたら良いのか。適切なチームを組むことが答であろう。そこでは、各種のスポーツのように、考えるよりも早く、反射的に体が動く神経を、生まれながらに、また訓練によって持つことが競技の神髄であり、そのような人々が中核プレイヤーである。同時に、実技はしないが、適切なコーチの有無がチームの勝敗を決めるだろう。

8. 現在の超流通システムの設計で特に留意されるべき要点は何か

2項目あげる。どちらも、有体物時代に刷り込まれた、もはや不用な思想の残滓である。

9. データコンテンツとプログラムコンテンツは別物であり続けるという思い込み

現在、超流通システムを設計開発中の人々の多くが、流通するのはデータだけであると考えている。その理由は、これまでがそうであったということであろう。アナログレコードも、CD-DAも単にデータであった。そもそも、それ以上の技術はなかったという理由でそうだったのである。コンテンツとしてプログラムを用いる技術的な水準も要請もこれまではなかった。

しかし、技術は急激に変わる。デジタルオーディオテープは、コピーできるという理由でコンテンツ提供者から拒否された。その同じ提供者がCDはコピーできるはずがないと考えてコンテンツを供給したが、現在CDをコピーする機械は5万円、媒体は200円以下になった。この変化に何年かかったかを考えてみれば、技術の急激な進歩を考慮しないシステム設計は社会の将来に対して有害であることがわかる。

プログラムを流通することの利点は数え切れない。流通するコンテンツとして、データもちろんあるだろう。当初は大部分かもしれない。しかし、データは知能がないから、その防御はプログラムに依存する。

プログラムであれば、それ自身が知能を持ち、アクティブである。自分がどの規格を満たすのか、どの規格を要求するのか、要求が満足されないときどうするのか、どのような価格で、どのような機能を提供する提供者がどこにいるのかをどのように探索するのか、どのように電子的で自動的な「入札」、「契約」を行うのかなどについて、システムの自由度は無限である。

すなわち、はじめからデジタルオブジェクト=プログラムにする方が自然である。これによって、個別的、能動

的な高度の機能の実現が可能になる。

プログラミング言語 JAVA によって、人々はアプレットを使う機会を持った。アプレットは、application の語尾を「小」を意味する接尾語 let にしたものである。application はかなりの主体性を持つ応用プログラム、例えば editor 等に用いられるのに対して、アプレットは明らかに将来におけるソフトウェア部品の意識を示しているといえるであろう。

人々はアプレットを使う機会を持ち、データでは困難だがプログラムならば容易にできることが多数あることを経験しているにもかかわらず、ネットワーク上で流通するのはデータだけであると考え、プログラムの流通を軽視している。

第一世代の超流通が実現し、第二世代へと進むときに、プログラムを処理できない超流通システムは、ユーザに敬遠され、市場での競争に敗れるだろう。超流通の発達とともに、コンテンツの最小単位の粒度は小さくなり、標準化され、権利者には確実な防御を、ユーザには便利さを提供するソフトウェア部品産業が誕生し成長するであろう。ハードウェア設計言語や、FPLA(Field Programmable Logic Array)の普及を考えれば、ネットワークによる流通は「ハードウェア」にまで及び、コンピュータシステムそのものがネットワークによってデジタル情報として流通する可能性もあろう。

10. 超流通ハイパーリンクの構造についての誤解

現在研究開発中のハイパーリンク可能な超流通システムのいくつかは、特定の不自由なハイパーリンク構造を強制するようである。これは誤りである。

超流通ハイパーリンク構造が確立されていない理由は、偶然ではなく、歴史的な刷り込みの影響である。次のたとえがよいであろう。

自動車を買うときはブレーキもいっしょに買い、自動車の代金は、ブレーキのそれを含む。ブレーキのメーカーは、実は最終的に代金を支払っている根源であるエンドユーザよりも、現実に代金を支払ってくれる自動車のメーカーに礼を尽くす。人類の歴史を通じて社会の構造やモラルもそのようになった。我々の生活のなかの構造の多くに、上下、親子、全体と部分という関係がある。

この思い込みは有害である。デジタル情報の超流通では、部品は必要に応じて購入し、返品し、廃棄できる。

自動車の部品であるエンジンの部品がまた自動車であるというような自由な構造は、有体物では起こらない。巨大なねじ構造の、ある部品のそのまた部品がねじであることはあっても、それは種類が同じだけであって、同一物ではない。有体物に特有な歴史的なこの刷り込みのために、親は子の上位にあって子の面倒をみるという考えから抜けられないのである。

製品の代金に部品の代金を含めるという、有体物の時には当然だった考えから脱却すれば、条件(普通は料金の請求)のついたリンクを、トリー状に限定されず、自由にグラフ状に飛び回る超流通ハイパーリンクが可能になる。

「自動車」メーカーは自動車の(ブレーキを含まない)代金を受け取り、「ブレーキ」メーカーはブレーキの代金を直接ユーザから受け取ればよいのである。ブレーキが必要ならば、適切な時点で購入する。不要になったら、返品あるいは廃棄する。

ハイパーリンクが有用であるのは、それが社会の自由な構造に対応できるからである。社会の構造を、木構造(親から子へ孫へ)、森構造(複数の木)などに限定できないことは明らかである。A から B にリンクし、B から C にそして C から A にリンクすることがあるだろう。またこのとき、B から C へのリンクを B が除去することがあるだろう。このような自由はハイパーリンク構造への基本的な要請である。

上のような理解が進めば、どのように入り組んだハイパーリンクでも、計算複雑度を増すことなしに単純明快に処理できることがわかるだろう。もし希望すれば、紹介料や割り引きを処理することも難しくない。

11. しかし、今のままのインターネットではできないのではないのか

今のままではできないこともあるが、そもそもインターネット自身がいつも改善されている。ルーチンの call には、成功、失敗、return value などがある。追加・拡張されるべき機能は、例えば、

サービス提供要求	Request For Services
提供サービスリスト	Available Services List
入札要求	Request for Bids
公認資格証明	Approved Capability Certificates

これらは今後の発展の当然の方向だろう。

12. 革命の驚くべき過小評価

デジタル革命の速度を、DRAM の集積度にならって 3 年間に 4 倍(10 の 0.6 乗)、したがって、毎年 1.6 倍(10 の 0.2 乗)であるという評価はかなり広く認められている。これは極めて過小な評価であり、誤まっている。デジタル革命の進歩は少なくともその 3 乗倍、すなわち、毎年 4 倍(10 の 0.6 乗)以上である。これは、集積度、速度、消費電力の進歩のすべてが助け合うことによるものである。以下に詳細に説明する。

まず、性能とは何かについて考察しよう。例えば自動車のレースでは、最近まで「性能＝早さ」であった。しかし社会は変化する。まず「総燃料消費量の上限」換言すれば「エネルギー効率の下限」が設けられた。次には、1 リットルで何キロ走るかの競争やソーラカーレースが誕生した。これらの新しいレースでは、通常は速度の下限が設け

られている。このような観察から、社会が求める「性能」は変わっていくことが明らかであるが、現在および近い将来に最も求められるであろう性能について考えてみよう。

そのひとつを A としよう。 A は一定時間当たりの処理容量であり、自動車でいえば速度×可搬重量(乗用車ならば定員)である。コンピュータでいえば、 A は演算速度×集積度となろう。他のひとつ B は一定エネルギー消費当たりの処理容量である。

これら2つの代表的な性能 A と B とを、1つの性能 Q に換算評価することが望ましい。何故ならば、早くさえあればエネルギー資源をいくら浪費してもよいとか、一定限度以下ならばエネルギー消費の程度を問わないのは、今後の社会の中心的要請に一致しない。これは道徳論ではない。例えば、世界中で用いることができるナビゲータその他の腕時計形の装置の実用化とその便利さは、明らかに大きくエネルギー効率 B に依存する。

Q を A と B のどのような関数にするべきか。次の条件は充分適切と思われる。

(1) A が一定の時、 Q は B に正比例する。

(2) B が一定の時、 Q は A に正比例する。

この条件(1)と(2)を承認するならば、 Q は A と B との積に比例係数を乗じたものとしてよい。蛇足であるが、 A と B との積の平方根はだめである。どちらの条件も満足しないから。正比例すなわち線形関係は単純で魅力的であり、より複雑にする理由は見当たらない。

まず、平面形の集積回路において、チップ面積を一定とし、集積度が n の2乗倍になったときには、素子の寸法は n 分の1になる。演算速度は、光が1素子を通過するのに要する時間で決まるので n 倍になる。すなわち、集積度が n の2乗倍大きくなると、演算速度の限界は n 倍速くなる。これにより、性能 A は、 n の3乗倍で進歩することになる。

次に性能 B について考えよう。放散できる熱量は、表面温度が同一である限り、面積あたり不変である。ゆえに集積回路の消費電力はチップ面積あたりほぼ同一である。したがって、 n の2乗の集積度の上昇は、1素子あたりの消費電力が n の2乗分の1に改善されていることを意味する。これと速度が n 倍になることを考えると、1演算当たりの消費電力は n の3乗分の1になる。これは性能 B の n の3乗倍の進歩である。

上の A と B の2つは本来は互いに独立である。例えば、自動車では、 A と B は拮抗する。しかし集積回路では、拮抗ではなく共進するのである。集積度が大きくなることは、「集積度×速度」の向上による演算能力、すなわち A の3乗の進歩だけをもたらすのではない。同時に、1単位演算あたりの消費電力は、「集積度×速度」の逆数に比例して減少する。すなわち、1単位演算あたりの消費電力は、 n の3乗分の1になるという進歩が同時に実現される。もしそうでなければ、その集積回路チップの発熱量は

前よりも大きくなるからである。

以上のことから、現在の集積回路技術において、集積度の n の2乗倍の進歩が実現されているときには、 A と B の積である性能 Q については、 n の6乗倍という、はるかに大きい進歩が実現されているのである。このことは、従来の有体物の社会の閉塞状況の根本原因である拮抗とは正反対の、きわめて重要な基本的性質である。

有体物でも、かつて種々の共進的な進歩が存在した。それらは純金の露頭のようなもので、掘尽くされるまでは、多くの人々はそこに「投資」を集中した。そして、何万年かの間に、掘り出しやすいものの多くは収穫されてしまったのである。

デジタル情報という新しい露頭は、大きな危険と同時に、有体物とは比較にならない多くの超越した利点を持つ。そこでの共進的な進歩が掘尽くされるのに、これから何百年かかるのか、15節で言及する。

性能が1桁変われば状況は一変する。年に0.2乗ならば1桁の進歩には5年かかる。秋葉原の様子が一変するのに5年かかるか。もちろんNoである。1年で4倍の進歩とすれば、1年8ヵ月で1桁の進歩が起きる。1年8ヵ月は秋葉原の様子が一変するのに5年より明らかに近い推定だといえよう。

以上のことは、我々の社会が、有体物社会における、メリットが拮抗しあう産業製品群から、一転して、これまで神の手のみが、すなわち、何億年という長い間のゆらぎの積み重ねのみが実現できた、生物のみに特有であった、共進的良さをもった産業製品が我々をささえる基盤になったことを意味する。

13. このことが、史上はじめて始まったことが重要である

従来の産業製品は非生物的で、共進性がなく、各メリットは拮抗的であった。例えば、自動車の積載量、速度、燃費の関係をみれば理解できる。したがって、最良点は妥協による中途半端な解となり、その結果すぐに閉塞状態に達する。極めてまれな高度なブレイクスルーのみが、この閉塞状況の突破をもたらす。そのため、従来の社会では、高度な成果といえば困難なものに決まっており、ついには何も良い結果をもたらさなくとも、高度に困難であるだけで評価されるような風潮になった。

デジタル革命の世界では、毎年4倍の、したがって10年で100万倍、20年で1兆倍の進歩がある。そこで、的を射た質の良い「思いつき」の価値が極めて高くなる。芸術の世界に似てきたといえる。いかに難行苦行しようと、資質のない人には良い芸術が作れないのと同様なことが、産業の中心的分野で起きようになっていく。進歩の最基礎部分が生命体的なものに、共進的なものになったことは、人類史上はじめてである。この進歩は今後長く続

14. いろいろなコンテンツ流通が発表されている。どれも似ていて、どれも良いのではないか

よく見れば根本的な多くの相違がある。次の性質を持たなければ、コンテンツ流通の社会基盤にはなり得ない。

電灯を点滅するたびに電力会社に手続きをする必要がなくては行けない。

家を建てた時ただ一度、またはクレジットカードを作る時にただ一度契約をするのと同様な手続きは良いだろう。それによって毎回の煩雑な手順を取り除くことができるならば。

水や電気として、ボトルウォーターも乾電池も有用である。しかし、それらは社会基盤ではない。

使うために煩雑な手順を必要とするものは駄目である。煩雑な手順とは、権利者またはユーザにとって面倒で、除去できる一切の手順である。

15. デジタル革命の本質

デジタル革命の影響の大きさを示そうとして、産業革命や津波あるいは集中豪雨に例える場合があるが、どれも不適切である。産業革命はエネルギーの工業生産を可能にしたけれども、質量・エネルギー保存則が核心であることには変わりがなかった。その意味で、産業革命はデジタル革命の初期微動であると例える方がむしろ適当である。

津波や集中豪雨などで「緊急対策」と呼ばれるものの多くは、実は単なる「緊急避難」にすぎない。最悪の事態は長く続かないことを我々は経験的に知っているので、本格的対策が事態の峠が過ぎてからになるのは、これまでは自然であった。デジタル革命の場合に同様な対応は致命的である。なぜならば、この革命の激烈さは今後100年以上にわたって継続する明瞭な理由があるからである。デジタル革命では、今すぐに根本的かつ長期的対策を立て、至急に実行を始めることが正しいのであって、従来のような緊急避難で乗り切ろうとすれば、大きな誤りになる。

デジタル革命の激烈さが長く続く理由は、世界中の人間と資本がデジタル情報の分野に流入を続けるからである。ますます多くの人々が、デジタル情報の分野が有利な投資先であることに気づいて、自分とその財産を投入する。それは、ある時間の遅れをともなつて結果として現れ、さらに正のフィードバックを引き起こす。津波や集中豪雨と違って、デジタル革命は「絶対的な」限界に達するまで止まらない。1980年の筆者の上述の論文の図1から見られるように、現在の速度でナノテク化が進むとして、人間の技術が「神の手」すなわち自然が数十億年の偶然のゆらぎによって創ったナノ構造の水準と比較できる程度になるまでに、100年以上にわたって進歩が続くだろう。鳥のように飛ぶことの次にはジェット機を発明したように、さらに進むのではないかと思うが、その前までだけ

でも認識に値する。

もしデジタル革命を無理に集中豪雨に例えるならば、それは降りが毎日前日より強くなる、そして止むことのない豪雨である。その結果としては、「陸地などというものはなくなる」という例えの方が良いであろう。その時でも有体物は確かに存在するであろうが、それは情報の海の上に浮くハウスボートのようなものだろう。

16. コーヒーとガソリン

コーヒーとガソリンを保管する時には、それぞれ別な容器を使う。1つの容器に両方を入れておいて、使うときに分別する方法(容器を1つ節約できる)よりも、容器を別にして混じらないようにする(分別の手数と装置を節約できる)方が良いからである。

このように有体物では別なものは別に取り扱うのが自然である。例えば、ガソリンとコーヒーは混ぜない。しかし、デジタル情報では別なものの情報も同じ装置で取り扱うのが自然である。コーヒーの在庫量とガソリンの在庫量を取り扱うために別なコンピュータを用いる必要はない。このことがコンピュータとデジタル情報の便利さ重要さの決定的な理由のひとつである。農業、漁業、自動車産業などの何をとっても、それらの産業のある部分は特有であるが、ある部分は情報処理である。

漁業を例にとろう。「操業地まで安全な天候のもとで往復できるルート」、「操業地で魚群を探索する技術」、「漁獲作業をいつ止めるか、どの港に行くか、どの市場に送るのが最も有利かの計算」、「何割を活魚、何割を冷蔵、何割を冷凍とするのが最も有利かの計算」は情報処理であつて、他の分野の情報処理と基本的に同じ技術である。このように、あらゆる産業の半分は結局は情報処理である。そこで、そのためのコンピュータシステムの生産は、デジタル革命の進歩とともに、他のハードウェア、例えば、農業のための農地や灌漑施設、自動車工場のための生産ライン、などの総和に匹敵する産業規模になる。

これだけであれば、GDPの例えば50%がコンピュータシステムになるだろう、で話は終わる。けれども実際にはその先がある。コンピュータシステムを研究・開発・設計・製造する技術と、量産されたそのシステムを効率良く利用する技術とは、関係はあるが別のものである。

これは、自動車を研究・開発・設計・製造する技術と自動車を運転・利用する技術とが、関係はあるが別なものであると同様である。現在および将来の社会では、コンピュータを作る人々の数に比べて、使う人々の数の方が圧倒的に多い。これは他の産業分野でも同様である。漁業のための各種装置を効率良く使用することはひとつの教育である。この教育のかなりの部分は現在でもデジタル情報処理である。マルチメディア技術やバーチャルリアリティ技術の進歩によって、教育はますますデジタル情報処理の直接の応用になっていく。これらのことを考慮すると、

GDP の例えば 4 分の 3 がコンピュータシステムの生産とデジタル情報処理とであるという状況が起こるだろう。

17. 保存則のない世界へ

質量・エネルギー保存則は重要な物理法則のひとつであるが、情報には質量・エネルギーのような保存則がない。このことの正の影響は大きく、それについての人々の理解はまだ充分とはいえないことは、上述した通りである。さらに一方で、負の影響についての多くの人々の理解には、まだ根本的に欠けたところがあるように思われる。

読者の財布が、私のポケットにあれば他所にはないのは、保存則による。飛行士が、月面に居れば地球に居ないのも、保存則による。犯罪が起きた時、証拠は現場にあって、たぶん読者のポケットにはない。これも保存則による。

保存則の有無によって、次のような違いが起きる。財布を金庫にしまうと、原理的に独立な 2 種類の防御機能が実行される。第一に、金庫によって財布を盗むことが妨げられる。第二に、金庫をあけて財布があれば、それは財布が盗まれていないことの証明になる。この 2 つは「直交する」すなわち「互いに独立な」事象である。その証拠に、情報を金庫にしまう場合を考えてみるとよい。金庫にしまうことによって、情報を盗むことを妨げる防御機能は働くが、金庫をあけてそこに情報があっても、情報が盗まれていないことの証明にはならない。

18. セキュリティにおける直交性

ある会社の社長 P が身分証明書を紛失または盗まれたとする。この場合に「あの P は身分証明書を持っていないが、しかし我社の社長である」という確認が身分証明書と独立にできるならば、その社のセキュリティは、身分証明書による座標に加えて、直交する別のひとつの座標を持っている。この時また、「あの T は我が社の社長の身分証明書を持っているが、しかし我が社の社長ではない」ことを確認する手段があれば、これも身分証明書による座標と直交するひとつの座標である。

セキュリティを構築する時、このように直交する複数の座標が実用上不可欠であることは明らかである。しかし、その必要は我々の経験によって認められるのであって、セキュリティに関する厳密な証明、すなわち、公理に基づく証明でその必要が導き出されることはない。なんとすれば、厳密な証明では、公理が正しいか否かについての議論は原理的に不可能だからである。

デジタル情報技術は著しく若い。秘密鍵暗号方式や公開鍵暗号方式におけるこれまでの高度な議論は、ほとんどが厳密な証明に基づいている。それに対して、デジタル革命が実現する社会のセキュリティは、そのような厳密な技術に加えて、それと直交する多様性のあるセキュリティを不可欠のものとして求める。

厳密な暗号は、計算機技術のひとつの中核として正当な注目を得て推進されているが、それと直交する多様性のあるセキュリティは、全く異なる発想と、破壊されたセキュリティの実例と、ユーザの快適さについての今後の長い経験と知識の集積によって提供され改善されていく性質のものである。

19. セキュリティの最大の穴は人間である

セキュリティの最大の穴が人間であることについては、専門家の間でも異論はないように思われる。「セキュリティの鎖はその中の最も弱い輪で切れる」こともまたよく知られた事実である。これら 2 つの表明が事実であるならば、この穴をふさぐための電子技術の研究・開発が、セキュリティにとって最も重要なはずである。実際にそうなっているだろうか。答えは No であるように見える。

この穴をふさぐための電子技術がまだない理由を検討しよう。原子力の例を考える。物理的な式やマニュアルの記述があっても、人間がそれを適切に守るとは限らない。そして実際そのようにして事故が起こった。にもかかわらず、この課題への取り組みは最重要なものとは設定されなかった。その理由は、おそらく原子力の場合、万一事故が起こった時の悪影響は恐るべきものなので、そのようなことが起こらないようにすること、すなわち、人間が穴になることがないように物理的、機構的に対策することに力点がおかれたためであろう。それでも現在になってみると、人間という穴をふさぐことが投資対策として最大の価値があったことが明らかであるように筆者には見える。

ネットワークセキュリティでは、原子力のような致命的で長期に影響する事故の可能性が本質的に小さいと考える人々がいるかもしれない。しかし、次のことを忘れてはならない。原子力の事故では、事故がより一層凄惨になることを希望する組織や人々は殆どないことを前提にできる。ネットワークセキュリティではそうではない。巨大で、優れた能力を持ち、そして存在そのものも知られていない組織が事故を計画し、事故の拡大に努める可能性がある。また、そのような組織による小手試しなどがあっても、それによる損失が巨大すぎて隠蔽できなくなるまでは、被害を受けた機関自身が隠蔽につとめる可能性も存在する。

20. デジタル情報のセキュリティの重要度は増す一方である

他の例を考えよう。デジタル革命以前において、なるべく多様な直交する防御機能が必要であるという認識とその実践とが目立たなかった理由は、特段の措置をしなくとも、それがほぼ自動的に行われたからである。例えば事件があったとすると、そこで血液、DNA、指紋などの証拠が「自然に」発生する。犯人がそれを避けようとして手袋をしたりしても、ある金庫が破られたとき、それを破った人間が金庫の近くにいたであろうことは確かであった。

図2 デジタル情報のセキュリティの重要性は増す一方である

デジタル革命によって、このような確かさはどんどん少なくなる。一方で、適切に設計されていないシステムでは、証拠を抹消し改竄することがますます容易になる。ここでもやはり、人間という穴をふさぐことが最も重要であると筆者は考える。そのための電子技術が、ネットワークセキュリティのための新しい技術分野になるだろう。

社会におけるデジタル情報の重要度と、必要なセキュリティの種類は、図2に示すように変化していくことは明らかである。

〔文献と資料〕

3節にあげた URL と報告書の論文・資料リストを見られたい。

もり りょういち
森 亮一 東京大学工学部卒業。同大学院(旧制)特別研究生。スタンフォード大学客員研究員。通商産業省電子技術総合研究所論理システム研究室長。筑波大学情報学類長。筑波技術短期大学教授。神奈川工科大学情報工学科長など。(株)ナムコ顧問。筑波大学名誉教授。工学博士。