Ｃ＆Ｃ賞　表彰式典　講演資料

万里の長城 胡を防がず

内部情報漏洩に備えてＭＥＬＴ up 止揚

中央大学　研究開発機構　辻井 重男

２０１４年１１月２６日

（デジタルフォンレジック研究会　辻井著コラムより）

このところ、組織内部からの情報漏洩が深刻な話題となっている。筆者も、ベネッセの監視委員会（社長の諮問機関）の委員長を仰せつかり、身を引き締めている。デジタルフォンレジック研究会の佐々木良一会長も、読売新聞の「論点」で[「内部犯罪」想定も必要]と題して、企業の情報漏洩対策を論じておられるが、（２０１４年１０月３０日朝刊)、件数は別として、被害額では、内部漏洩が全被害額の半分を超えていると言う統計も報告されている。実態はそれを上回るかも知れない。

万里の長城、胡を防げず、明王朝は内部から崩壊した。Fire Wall を高くするだけでは、内部情報漏洩は防げない。本丸、即ちデータ本体・データベースを守ることを真剣に考えねばならない。企業などの従業員の５４％がデータベースへのアクセスログを取られていることを気にしているが、経営者・管理者は、情報漏洩対策の中で、アクセスログによる監視の重要性を１９位に位置づけているというアンケート結果も出ている。組織的に意識合わせをした上で、情報漏洩対策に取り組まねばならない。

さて、ＯＣＢＭの普及に伴って、情報社会のＤＡＤAism が浸透し、MELT up を図ることの重要性が緊急さを増している。

（「何のことか。勝手な略語ばかり並べて分からないではないか。」「失礼しました。これから説明します。」）

ＯＣＢＭは 「Open data, Cloud, Big data, My number」の略である。一般に、Digital 技術、特に Big data の拡大・浸透により、社会的機能や構造を連続化、つまり、Analog 化が進む。個人情報について言えば、Big data の拡大浸透は、その特定度（Identifiability ）と機微度（Sensitivity）を連続化している。ヨーロッパの ENISA では、各々を４段階に分類した上で、個人情報の重要性を７レベルに整理している。

この現象を私は、ＤＡ変換と呼んでいる。若かりし頃、取り組んだ技術的なＤＡ（Digital to Analog ）変換ではなく、社会的なＤＡ変換である。この社会的ＤＡ変換現象が進むと、法的規制が必要になる。２０世紀までは特に必要としなかった個人情報保護法などが、２１世紀になって制定されるようになった。法制度は、解釈の幅はあるにせよ、懲役何年、罰金何万円というように、社会的な意味での Digital 的存在である。その役割は大きいが、万能ではなく、上記の ENISA の分類に対応して法制度を定めて運用することは難しい。最

後に頼れるのは、人間のAnalog的な倫理（Ethics）,モラル、意識、心理、自己規制、行動規範、Management能力などである。こうして、Digital技術は、社会的機能・構造をAnalog化し、それが、法制度という社会的digital化を進め、最後に、人間というAnalog的存在に頼るというＤＡＤＡプロセスを生むことになる。これが、私が勝手に使っている「情報社会のDADAism」である。

私は、ＩＰＡ（独立行政法人 情報処理推進機構）で、小・中・高の生徒達から応募された情報セキュリティ標語の選考委員長を務めているが、数年前、ある中学生が「アナログの心受け継ぎデジタルへ」という標語で、応募してきた。「何を言っているのか分からない」という選考委員もいたが、私は、背負った子に浅瀬を教えられた気がして、強く推薦し入選させた。情報社会の DADAism は、ＤＡＤＡプロセスでは終わらず、Analog 人間からDigital技術へのFeed back が大事なのである。

ここで、余談１つ。この頃、スマホから目を離さない子連れの若いお母さんをよく見かける。最近のセキュリティ標語では、小学生から「お母さん、スマホより僕の顔を見てよ」という類のものが多くなった。これも、母親が、背負う子に浅瀬を教えられている例だろう。

さて、Big data をはじめとするＯＣＢＭ現象は、自由を拡大する。自由には様々は意味があるが、それはさておき、１９世紀の初め頃、哲学者ヘーゲルは、「歴史とは自由の拡大のプロセスであり、自由の拡大に伴って矛盾も拡大する」と述べている（加藤尚武著「哲学原理の転換」（未来社２０１２年１０月）。ヘーゲルに言われるまでもなく、我々は、例えば、表現の自由と児童ポルノ規制のなど様々な矛盾相克に悩まされ続けている。歌の文句ではないが、「この世の中、右を向いても左を見ても、矛盾と相克の絡み合いじゃございませんか」と言わんばかりである。

自由の拡大、安心安全の向上、プライバシーの保護は、互いに矛盾する場面が多い。この矛盾を可能な限り解消し、高度均衡を図る手段を日々、探求するのが、我々の使命である。そのためには、３つの止揚を図らねばならないので、私は、１０数年来、三止揚（drei aufheben)と唱えてきたが、最近は、より具体的に、MELT up と呼ぶことにしている（付記参照）

MELT とは、M; Management, E; Ethics, Law, Technology であり、この４者を強連結・密結合させて、三止揚を図ろうと言うことである。この中で、特に難しいのが、Ethics と Management である。

抽象的な話ばかりで具体的提案が無いではないか、と言われそうなので、暗号の例を１つ挙げておこう。

１９８０年代から９０年代にかけて、暗号は、軍事・外交だけでなく情報社会にも役立つのかという意味で、話題性を持っていた。拙著「暗号―ポストモダンの情報セキュリティ」
（現在、「暗号と情報セキュリティと改題。講談社学術文庫」）を野田聖子郵政大臣（当時）

謹呈したところ、「こういう本が読みたかったのよ」と云って読んでもらった。また、大蔵省（現在、財務省）に呼ばれて暗号の講演をした際、法学部卒の局長さん達から「あなたの本は良く分かった。しかし、素数って、そんなに沢山あるのですか」と玄人裸足の質問を受けたりもした。

その後、暗号が社会的基盤として活用されるようになると、新技術の宿命として、話題性がなくなり、縁の下に入って、社会的関心も薄れてきた。正しく利用されていれば、それで良いのだが、情報系技術者にすら、ＲＳＡ暗号が正しく理解されておらず、素数の使い回しという、素因数分解にその安全性を依拠するＲＳＡ暗号にとって、とんでもない使われ方おしていることもあるようだ。暗号研究者の間では、暗号復活という声も上がっているがどうだろうか。暗号化し情報をクラウドに保管した場合、統計処理なども、暗号化したまま、加算・乗算をして結果を求める手法が、暗号学会では活発に行われているが、行政、医療や企業などで利用が進むことを期待している。

中央大学研究開発機構では、独立行政法人 情報通信開発機構（ＮＩＣＴ）からの組織暗号などをテーマとする委託研究を、私がリーダーとなって進めている。組織暗号は、暗号化文書を受け取った組織内で、暗号化伝送処理を行うシステムである。My Number の導入に伴って、自治体からの要請も増えるものと考え、現在、長野県や新潟県の自治体で、実証実験を展開している。

古い話だが、第一次大戦では、ドイツ発の暗号化情報が不必要に平文に戻されたため、アメリカ参戦のきっかけとなり、連合国勝利の要因となった。この逸話は、昨今の内部情報漏洩防止にも活かされねばならない。

内部情報漏洩対策としての Management には、不満分子を減らすというような組織経営のレベルから、技術を手抜きせず、正しく使うというレベルまで、多様な段階があるが、蟻の一穴から情報が漏れて、九仞の功を一簣（いっき）に虧く（かく）ことの無いよう、コストや効率を考慮しながら、綿密な対策表を作成することが要請される。

付記　　ヘーゲルと弁証法・止揚

私は勝手な解釈で、止揚（aufheben）という用語を使ってきたが、ヘーゲル哲学の立場から見て正しい使用法かどうか自信が無い。元々、aufheben というドイツ語は、「持ち上げる」という意味である。第一次大戦後、敗戦国ドイツはハイパーインフレ状態で、円高マルク安が進む中、日本からカント・ヘーゲルを学びに行く学徒は、若き日のハイデガーを家庭教師に雇うという贅沢も出来たという時代である。そんな中、訪独したある哲学学徒が、下宿に付いた途端、おかみさんから、「一寸、その荷物 aufheben してよ」と云われて、がっくりしたという話を聞かれた方も多いだろう。

本文中にも引用した加藤尚武先生の「哲学原理の転換」によれば、「弁証法という言葉には、いままで、いろいろ誤解があった。ヘーゲルの弁証法は正反合の弁証法であるとよく

教科書に書いてあるが、正反合という用語例がヘーゲルの書いたもののなかに、一つも存在しないということは、京都大学の酒井修教授が証明しており、世界的にも認められている（上記１０７頁）」とのことである。

私としては、正反二つの要請があるとき、初めから「バランスですね」と諦めず、可能な限り持ち上げて（MELT up して）、高度均衡を図るべきであるという意味で、止揚と言う言葉を使用している。

最後に駄洒落を１つ。本コラムのタイトルを、当初は、「万里の長城 胡を防がずー内部情報漏洩に備えてＭＥＬＴ up しよう」としていたが、「しよう」と打ち込んだとき、うっかり仮名漢字変換を押してしまったところ、「止揚」と出てしまい、「MELT up によって止揚しよう」と言う意味で、「・・・ＭＥＬＴ up 止揚」とした次第である。私のパソコンでは、「止揚」の方が「使用」より使用頻度が高かった結果である。